

Research paper

Design and implementation of an enhanced anti-SAT framework for robust protection against SAT-based attacks on logic-locked circuits

Kamatchi S^{a,*}, A. Swetha Priya^a, E.L. Prasad^b, M. Thillai Rani^c, V. Sri Pranav^a, Jitendra Bahadur^a, Dong-Won Kang^d

^a Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa, Vidyapeetham, Bengaluru, 560036, Karnataka, India

^b Tessolve Semiconductors Private Limited, Bengaluru, 560103, Karnataka, India

^c Department of Electronics and Communication Engineering, Sri Krishna College of Technology, Coimbatore, 641042, Tamil Nadu, India

^d Department of Energy Systems Engineering, Chung-Ang University, 06974, Seoul, Republic of Korea

ARTICLE INFO

Keywords:

Logic locking

SAT attack

Anti-SAT block

Integrated Circuits (IC) security

Challenge-response authentication. Full adder

Hardware security

Reverse engineering protection

Cryptographic key protection

ABSTRACT

Ensuring the security of Integrated Circuits (ICs) against reverse engineering and unauthorized access is challenging. They are vulnerable to Satisfiability (SAT)-based attacks, which can systematically reduce the search space by effectively bypassing conventional logic locking techniques. The existing methods are vulnerable to skew in the algorithms or signal probability skew-based removal attacks or takes required overhead. To fill this gap, we propose a new compact lightweight Anti-SAT block (ASB) and its obfuscation approach together with a Challenge-Response Authentication Framework (CRAF) that exponentially increases IC security by making SAT solver complexity infeasible to attackers through decoy keys. The Anti-SAT Block (ASB) includes decoy keys which exponentially increase the complexity of SAT solver, and from which true keys cannot be recovered. Incorporation of ASB in a locked circuit thwarts vulnerable SAT attacks. The novelty is that the proposed ASB design with obfuscation technique not only provides effective protection against SAT attacks but also provides ATPG-based cost-effective secured locking mechanism with reduced overhead. The challenge-response module also assures that access is valid, by authenticating it and preventing the circuit from being opened by unauthorized users. The proposed novelty achieves a high fault detection efficiency of 98% and test pattern coverage of 99% with very low power down to 48% and area overhead of 12% which is suitable for high-security applications. This solution provides superior resistance to SAT-based attacks that provide resistance over the traditional key gate-based logic locking techniques and protect sensitive ICs from advanced hardware threats. This work demonstrates the strength of the Anti-SAT and authentication framework in protecting modern IC designs and provides promise as a solution for critical applications in defense, finance, and other security-sensitive industries.

1. Introduction

Integrated Circuits (ICs) are becoming increasingly important in hardware security, and safeguarding against unauthorized access is critical. ICs are the main components behind many of the applications in computing, telecommunications, and industrial systems; hence, protecting the Intellectual Property (IP) within them is highly important [1]. During the development of IC or IP, big silicon companies can't afford advanced fabrication capabilities and rely on third-party manufacturing vendors. This poses various security supply chain issues like piracy, Trojan attacks, overbuilding, retrieving data, and reverse

engineering. Logic locking, a technique widely employed, is based on embedding secret keys to modify the functionality of the circuit, allowing only such authorized users who possess corresponding keys to unlock and perform the intended operations. The objective of this approach is to stifle the adversary's ability to replicate, tamper with, or steal proprietary information embedded in ICs [2].

Although logic locking has great advantages, it is vulnerable to security attack. In these attacks adversaries exploit the power of powerful SAT solvers to systematically rule out keys until it finds the correct one and breaks the circuit security [3]. SAT based attacks are serious threats to the integrity and confidentiality of electronic systems,

* Corresponding author.

E-mail address: s.kamatchi@blr.amrita.edu (K. S).

<https://doi.org/10.1016/j.rineng.2025.105928>

Received 7 March 2025; Received in revised form 21 June 2025; Accepted 22 June 2025

Available online 9 July 2025

2590-1230/© 2025 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

allowing reverse engineering, IP theft and unauthorized manipulation of critical hardware. This is particularly severe for high stakes industries that are based on the trustworthiness and uniqueness of their IC design, and hence the need for stronger security mechanisms is more urgent [4].

Currently existing countermeasures against SAT attacks, including key based logic locking, obfuscation and noise injection, have demonstrated their weaknesses in terms of robustness, efficiency and practicality. However, most of these methods have significant power and area overheads or are not very effective in deterring SAT solvers in complex IC environments [5]. With the ever increasing capabilities of SAT solvers, it is becoming harder and harder to develop solutions that balance security with the constraints of performance, power, and area efficiency, which are necessary for adoption in modern IC design.

In this paper, we propose a novel solution to overcome these challenges by designing and implementing an Anti-SAT block along with its obfuscation approach. The novelty of this Anti-SAT block is to increase the resilience of logic-locked circuits by generating a large number of incorrect keys that make it harder for SAT solvers to find the correct key, thereby delaying and complicating the decryption process. In addition to this, a challenge-response authentication framework and a Full Adder Locked module are integrated to provide circuit security and prevent the circuit from being unlocked and operated only by authorized users. Extensive simulation and hardware implementation on FPGA platforms are used to validate the proposed Anti-SAT design, which provides strong protection against SAT-based attacks with minimal power, area, and timing overhead.

1.1. Research objectives

This paper aims to address the shortcomings of existing logic locking techniques by introducing a novel solution: the Anti-SAT block followed by its removal attacks and obfuscation approach together with a challenge-response authentication framework. The primary objectives of this research are:

- To design and implement an Anti-SAT block that enhances the security of logic-locked circuits by integrating SAT-resilient mechanisms.
- To ensure that the proposed solution does not compromise the circuit's performance, area, or power efficiency, making it feasible for real-world applications.
- To validate the effectiveness of the Anti-SAT block through simulation and hardware implementation with ATPG based secured mechanism followed by FPGA platforms, assessing its resilience against SAT-based threats.

In order to address the critical need for enhanced IC security, this paper introduces an Anti-SAT block integrated with a Challenge-Response Authentication Framework (CRAF). The Introduction points out that protecting IC Intellectual Property (IP) against unauthorized access and SAT based attacks is important. In Related Work, we describe existing logic locking techniques and their limitations. In order to have low power and area overheads, while increasing SAT attack resistance, Our Proposed Methodology describes the design of the Anti-SAT block and CRAF. Simulation and Experimental Setup describes the environment and metrics used for validating our solution. In the Results and Analysis section, quantitative findings are presented, including the high fault detection efficiency and security improvements of our design. We discuss implications to high security applications and possible improvements in Discussion. The Conclusion rounds up our contributions and future research directions by remarking on the robustness of the Anti-SAT block in securing modern ICs.

2. Related work

Logic locking has emerged as a critical technique in the rapidly

evolving field of IC security to protect circuits from unauthorized access to reverse engineering and IP theft. Traditional logic locking mechanisms are found to be vulnerable to Satisfiability (SAT)-based attacks that recover secret keys via powerful solvers. In this literature review, different advances in logic locking techniques, SAT resistant mechanisms, and test pattern generation to improve the resilience and security of ICs have been explored.

2.1. Logic locking and SAT resistant mechanisms

Trace logic locking is an early effort for making logic locking better than the existing parametric space, by introducing more constraints. In Zuzak et al. (2020) an innovative approach for key enrichment is proposed by increasing the number of variables and dependencies in the circuit design such that the difficulties of the relevant SAT solver are raised [6].

Zhou and Zhang (2021) first introduced generalized SAT attack resistant logic locking to improve resistance to SAT attacks through random input output dependencies that inhibit solvers from formulating precise queries [7]. Their logical programming, encoded in higher key space, deceives SAT solvers, and greatly stretches the time to extract the right key. Alaql and Bhunia (2021) proposed a scalable attack resistant logic locking mechanism in the Scalable Attack-Resistant Obfuscation (SARO) SARO framework which aims to be capable in large scale ICs. SARO's scalability allows secure locking solutions for more complex circuits that are resistant to advanced attacks at minimal overhead [8]. This research highlights the importance of achieving scalable solutions that can adapt to the increasing complexities of IC design.

2.2. Fault injection and test pattern generation techniques

ATPG is explored as a method to evaluate and improve circuit security besides logic locking. In their work Wang and Gupta (2020) develop the ATPG paradigm for certifying the performance of Rapid Single Flux Quantum RSFQ circuits via fault detection via test pattern generation. This work provides an approach to systematic fault and vulnerability resisting testing of circuits [9] (Table 1).

In their work, Zhong et al. (2022) introduce the ATPG Guided Fault Injection Attack (AFIA), an attack that breaks the secure logic locking mechanisms. They show that Automatic Test Pattern Generation (ATPG), traditionally used for fault detection, can be used to generate targeted test patterns for fault injection attacks. By systematically injecting faults to reveal vulnerabilities in logic locked circuits, these patterns can expose key based security weaknesses. The study also highlights the dual role of ATPG in both testing and attacking circuits, questioning the resilience of current logic locking techniques, and suggesting that future security strategies should protect against not only SAT-based attacks, but also ATPG guided fault injection. This work further advances the field of IC security by urging defenses against multiple attack vectors that are stronger [10]. In this work, Zhong and Guin (2023) propose a comprehensive test pattern generation approach for logic-locking mechanisms to exploit and counteract SAT attacks. It exploits tailored test patterns to assess the resilience of logic-locked circuits to

SAT-based attacks by revealing and healing vulnerabilities in their security architecture. They systematically attack the logic locking of the circuit, uncovering vulnerabilities towards which SAT solvers can be used. By combining this test pattern generation technique, the study improves circuit security by allowing lock design adjustments before decryption, thereby making SAT-based decryption more difficult. This work presents an important advancement in the development of robust logic-locking strategies that are resistant to sophisticated SAT-based attacks in modern ICs [11].

In Wang et al. (2021), SOFI has been introduced as a security property-driven framework to analyze the vulnerability of integrated circuits (ICs) under fault injection attacks. It proposes to use systematic evaluation of ICs by injecting fault to identify and measure security

Table 1

System parameters and performance metrics for anti-sat block implementation.

Paper/s	Contribution	Gaps Identified	Future Opportunities
Wang & Gupta (2020)	ATPG paradigm for certifying RSFQ circuits using test pattern generation.	Focused only on fault detection, not on improving security against SAT attacks.	Extend ATPG methods to include SAT attack resistance and assess overall circuit security.
Zuzak et al. (2020)	Trace logic locking for increasing parametric complexity.	High resource and power consumption, limited application for large-scale ICs.	Develop more power-efficient locking mechanisms that maintain security in large-scale integrated circuits.
Aladi & Bhunia (2021)	SARO: A scalable, attack-resistant logic locking mechanism.	Needs validation in real-world IC environments and against hybrid attacks.	Validate SARO in complex real-world scenarios, explore hybrid attack-resistant solutions.
Wang et al. (2021)	SOFI: Vulnerability assessments of ICs against fault-injection attacks.	Lacks focus on SAT attacks and overall circuit protection.	Integrate SAT attack assessment with fault-injection analysis for holistic security.
Zhou & Zhang (2021)	Generalized SAT-attack-resistant logic locking through deceptive logic.	Complexity increases design overhead, lacks application to different IC types.	Optimize for different IC architectures and reduce overhead without compromising security.
Ghosh et al. (2022)	Electromagnetic analysis for detecting side-channel vulnerabilities.	Limited applicability to SAT attacks, high-cost setup.	Apply electromagnetic detection techniques to SAT attack resilience with cost-effective approaches.
Zhong et al. (2022)	ATPG-Guided Fault Injection Attack (AFIA) on secure logic locking.	Lacks methods to secure circuits from ATPG-based attacks themselves.	Develop techniques to harden logic-locked circuits against ATPG-based attacks.
Kolla et al. (2022)	Logic locking designs for full adders at the transistor level.	Limited scalability and resilience to SAT attacks.	Explore transistor-level solutions that scale and remain resilient against various attack vectors.
Zhong & Guin (2023)	Test pattern generation approach for identifying SAT attack vulnerabilities.	Focuses primarily on SAT attacks, neglects multi-vector attacks.	Extend the approach to mitigate multi-vector attacks such as fault-injection and side-channel attacks.

weaknesses. Designed to be used by circuit designers, SOFI provides a structured methodology to identify vulnerabilities that could be exploited by attackers and to assess the circuit's resilience to such attacks before deployment. Because it emphasizes fault-injection resilience, the framework is particularly valuable for improving IC security by facilitating the development of robust defenses against unauthorized manipulation of circuit operations resulting from induced faults [12].

Ghosh et al. (2022) also examine the application of electromagnetic (EM) analysis with an integrated on-chip sensing loop for side channel and fault injection attack detection. In their approach, electromagnetic emissions from circuits are monitored looking for abnormal patterns that could represent unauthorized access attempts or induced faults. The real-time identification of potential attacks made possible by this EM-based detection method enhances IC security capability by enabling immediate response to security threats. This technique uses on-chip sensing technology to provide low-cost and efficient means of detecting both side channel and fault injection attacks, and is an important addition to hardware security strategies to protect against invasive attack methods [13].

3. Proposed methodology

The proposed methodology involves designing, implementing, and validating an enhanced SAT-resistant logic locking system to protect ICs against unauthorized access. The Anti-SAT Block, Challenge-Response Authentication Framework, and Full Adder Locked Module are integrated into this design to enhance the security of the circuit while keeping power and hardware overhead low [14]. Together these components help mitigate SAT-based attacks that could extract secret keys embedded in the IC by making them significantly harder. This safety levels are assessed with ATPG with fault injection methods. Using Design for testing (DFT) on the framework helps to minimize the reliance on the designers with automated results providing controllability and observability of the internal nodes of the logic design. Fault injection heuristics is introduced in our design which helps to generate low-power protected patterns required for testing the hardware. We conducted the complete testability analysis to understand the pattern count, runtime, response time, speed, cost and test and fault coverage of the design for this secure mechanism to understand the scan dumped data is protected against the SAT attacks, removal attacks, reverse attacks and bypass attacks.

The Fig. 1 (a) is a representation of the logic locking process in IC design, from design to market and the potential vulnerabilities to reverse engineering attacks [15] where data will breach through. Fig. 1 (b) representation proposed heuristics with security analysis.

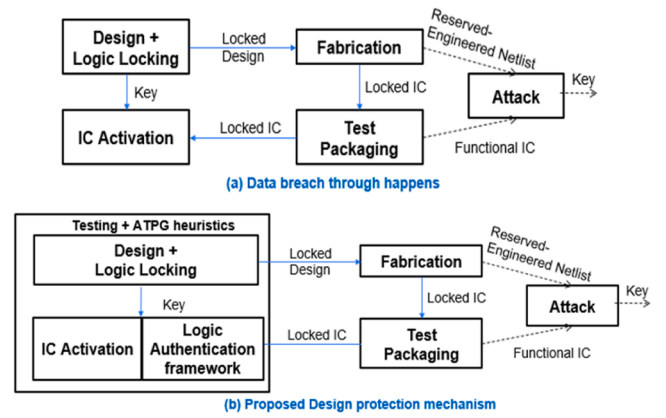


Fig. 1. Logic locking process in IC design with potential reverse engineering attack pathway.

The IC is initially designed with embedded logic locking, a secret key controlled functionality. After design, a locked IC is fabricated and test packaged while in a locked state to prevent unauthorized access to its functionality. The IC is then distributed to the market, where it is still locked and requires key based activation to become fully operational. Yet, an attacker may acquire a working IC on the market, reverse engineer its netlist and try to recover the key, circumventing the locking mechanism [16]. It stresses the importance of logic locking and key-based activation in IC security but points out that reverse engineering can extract keys, and therefore emphasizes the need for further security, like Anti-SAT blocks [17].

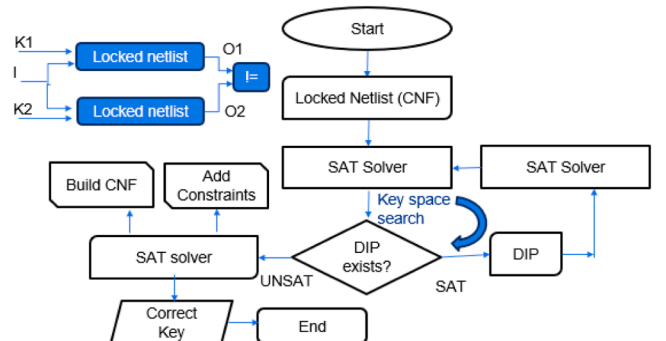


Fig. 2. SAT-based attack flow for key recovery in logic-locked circuits.

The SAT-based attack process to recover the secret key of a logic-locked IC is illustrated by the flowchart (Fig. 2). The attack starts with two instances of the locked netlist both with different key guesses (K1 and K2) but with the same input III and outputs as O1 and O2. A miter circuit is used to compare these outputs, and discrepancies between O1 and O2 are flagged as flags indicating incorrect key configurations. Next, the miter circuit is converted into Conjunctive Normal Form (CNF) for processing by a SAT solver. With this circuit constraints, this solver finds a Distinguishing Input Pattern (DIP), an input that produces different results for incorrect key configurations. If a DIP is found, it is applied to an 'Oracle', which is a version of the IC that is unlocked, and outputs the correct result. When the DIP fails, i.e. when a mismatch is returned, indicating an incorrect key, the SAT solver refines the search by the additional information of the mismatch [18]. Every time the SAT solver reaches the end of its possibilities, it gives up on that iteration of the process, then tries again, all the way up until the SAT solver decides that it cannot find the correct key configuration. It is through this SAT based attack method that we demonstrate the vulnerability of logic locked circuits to systematic key recovery techniques and that we emphasize the need to design countermeasures against such iterative attacks.

This Fig. 3 shows the method of integration of Anti-SAT blocks (of Type 0 and Type 1) into a logic locked circuit to improve security against SAT based attacks. The Type-0 Anti-SAT configuration (Fig. 3a) has the block that always outputs 0 on the correct key values. This is accomplished with a combination of gates (g and its complement g^*) which require antagonistic key inputs K1 to K2n, to produce a logic 0. Also, the Type-1 Anti-SAT block (Fig. 3b) outputs 1 regardless of the key values if they are correct, and outputs 1 under specific key dependent conditions. Anti-SAT blocks of both types work by imposing unique key constraints which, when properly satisfied, force their output to a constant value, and otherwise produce incorrect or random outputs, making SAT based key recovery attempts more difficult. In the integration step (Fig. 3c), the locked circuit is combined with its original gate and a new gate (marked in red), and a Type-0 Anti-SAT block is embedded into the resulting circuit [19]. Since the original logic is used to compose the locked circuit's output, the locked circuit has an output that depends on both the circuit logic and the output of the Anti-SAT block, so the locked circuit is only unlocked by the correct key. Fig. 3d is the proposed and implemented design method that increases security by obfuscating the logic and making it UNSAT solvable by SAT solvers, who would

otherwise spend time deducing the key by iteratively evaluating the circuit's response to different inputs. Insertion of both our Type-0 and Type-1 Anti-SAT blocks adds variability and further frustrates key recovery [20].

3.1. Logic locking mechanism

Logic locking is a means of protecting integrated circuits (ICs) by embedding a secret key which modifies the circuit's functionality. This approach is meant to restrict the usage of the circuit's operations to authorized users. Logic locking is a technique that, when used in a digital circuit such as a full adder, places key dependent logic gates (e.g., XOR, XNOR) that allow the circuit to only function correctly when given the correct key. The Sum and Carry functions with inputs A, B, and C_{in} , are:

$$Sum = A \oplus B \oplus C_{in} \quad (1)$$

$$Carry = (A.B) + (C_{in}.(A \oplus B)) \quad (2)$$

If logic locking is introduced, the circuit is made such that the wrong key will yield incorrect outputs. Mathematically, the logic-locked Sum and Carry functions can be expressed as:

$$Sum_{locked} = (A \oplus K_1) \oplus (B \oplus K_2) \oplus (C \oplus K_3) \quad (3)$$

$$Carry_{locked} = (A \oplus K_1).(B \oplus K_2).(C_{in} \oplus K_3) \quad (4)$$

Where K_1 , K_2 , and K_3 are parts of the secret key applied to obfuscate the circuit.

3.2. Anti-SAT block design

To resist SAT based attacks, the Anti-SAT block is designed to introduce deceptive logic which generates an enormous number of incorrect key combinations (decoy keys). Anti-SAT block is intended to raise the computational difficulty for a SAT solver trying to infer the correct key. The total key space K_{total} for an n-bit key is:

$$K_{total} = 2^n \quad (5)$$

Where n is the length of the key. In the presence of decoy keys, the Anti-SAT block leads to a highly increased search space, and a SAT solver is required to evaluate an exponentially larger number of keys for every successful attack. This effectively delays the solver, and is computationally impractical to brute force the key. The time complexity T_{SAT} for the SAT solver to find the correct key in the presence of decoy keys can be expressed as:

$$T_{SAT} \propto 2^m \quad (6)$$

Where the number of additional decoy keys is m . The exponential increase in T_{SAT} in SAT based approaches for attackers are highly elusive to the correct key, since it is due to decoy keys [21].

3.3. Challenge-response authentication framework (CRAF)

Additional security that requires the users to react correctly to random challenges is the Challenge-Response Authentication Framework (CRAF). We consider this framework in which a random binary challenge C of length n is generated. The expected response Re . The secret key is used to compute is K , a predefined secret seed S as follows:

$$R_e = K \oplus (C \oplus S) \quad (7)$$

The user's response must be granted for access. R_p must match. This comparison is represented as:

$$R_p = R_e \Rightarrow \text{Authentication Successful.}$$

If $R_p \neq R_e$, the circuit remains locked.

This complexity is further increased by the need for correct, real time

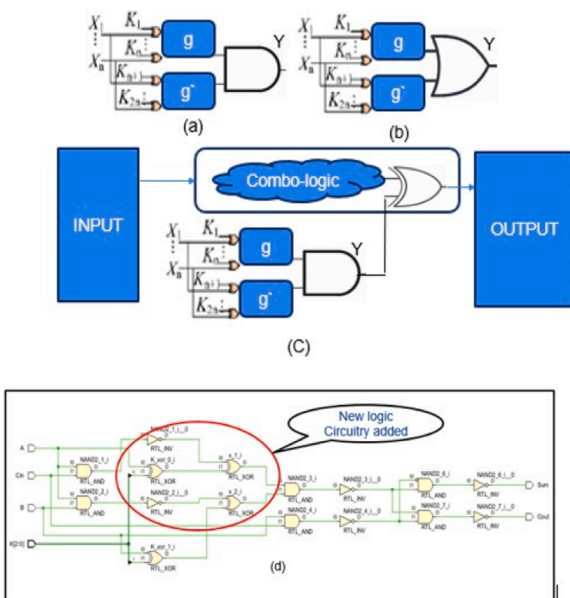


Fig. 3. Integration of Proposed logic between Type-0 and Type-1 Anti-SAT Blocks for Enhanced Security.

responses, which make brute force or replay attacks more difficult.

3.4. Automatic test pattern generation (ATPG) and fault injection analysis

Test patterns are automatically generated by the Auto- matic Test Pattern Generation (ATPG). The test patterns are useful for SAT and fault injection attacks on the circuit. Fault coverage and vulnerability identification are analyzed using input vectors created by ATPG that can trigger specific faults. Probability distribution $p(x)$ of a fault in the locked circuit under a test vector is x , then the expected fault coverage C_f can be computed as:

$$C_f = \sum p(x) \cdot f(x) \quad (8)$$

Where (x) , is the fault detecting capability of the test vector x . The goal is to maximize C_f which was used to detect and mitigate possible security vulnerabilities of the circuit [22]. The power, area and timing overhead introduced from the Anti-SAT block and logic locking mechanisms must be quantified to maintain efficiency. The dynamic power $P_{dynamic}$ is calculated based on the switching activity of the circuit, represented as:

$$P_{dynamic} = \alpha \cdot C_L \cdot V^2 \cdot f \quad (9)$$

The static power P_{static} , due to leakage currents, is added to obtain the total power consumption:

$$P_{total} = P_{dynamic} + P_{static} \quad (10)$$

The Anti-SAT block adds gates, slightly increasing both $P_{dynamic}$ and P_{static} . To minimize power overhead, the Anti- SAT block design ensures that additional gates are limited. The additional gates needed for Anti-SAT block logic are counted to calculate the area overhead introduced by that block. $g_{baseline}$ is the number of gates in the original circuit.

$g_{Anti-SAT}$ the total area overhead for the Anti-SAT block, additional gates.

$$A_{total} = g_{baseline} + g_{anti-SAT} \quad (11)$$

The timing overhead is determined by measuring the increase in the circuit's critical path delay due to the Anti- SAT block. Let $t_{baseline}$ represent the original critical path delay of the circuit and $t_{Anti-SAT}$ the delay introduced by the Anti-SAT block. The total critical path delay $t_{critical}$ is given by:

$$t_{critical} = t_{baseline} + t_{Anti-SAT} \quad (12)$$

Finally, the proposed Anti-SAT methodology is bench- marked in terms of its resilience against SAT attacks, and compared with existing techniques. A security level can be measured as an estimated time needed for a SAT solver to find the correct key. The expected time of an attack is given by expanded key space and challenge response mechanism.

T_{attack} required for a successful SAT attack increases expo- nentially with the length of the key and the number of decoy keys:

$$T_{attack} \propto 2^{n+m} \quad (13)$$

The length of the key is n . The number of decoy keys, m . The confirmation of this exponential relationship shows that the Anti-SAT block is a major improvement to security, delaying or preventing SAT based key recovery.

Fig. 4 shows the Logic locking mechanism imple- mented with Anti-SAT mechanism. Fig. 5 shows the proposed locked circuitry with authentication module and Fig. 6 shows the schematics of the Authen- tication Frame- work.

A comprehensive defense against SAT attacks, fault in- jections, and unauthorized access is proposed by combining the expanded key space, challenge response mechanism and ATPG fault coverage analysis into the proposed Anti-SAT framework, which makes for a robust security solution for ICs.

4. Results and discussion

The effectiveness of the proposed Anti-SAT block in increasing the security level of logic locked circuits against SAT based attacks is evaluated and the results show a good performance. An Anti-SAT block was introduced to generate decoy keys that exponentially increase the time complexity of a SAT solver to detect the correct key. The SAT solver needed an estimated time complexity of $O(2^m)$, where m is the number of decoy keys, with the integration of decoy keys. This result emphasizes that the decoy keys lend an extensive search space, which makes it far more difficult for the SAT solver to determine the correct key configuration. Security was further reinforced by dynamic validation, using the Challenge-Response Authentication Framework (CRAF). They confirmed that CRAF's success was in pro- viding such secure access since only users with the correct key and response could activate the IC

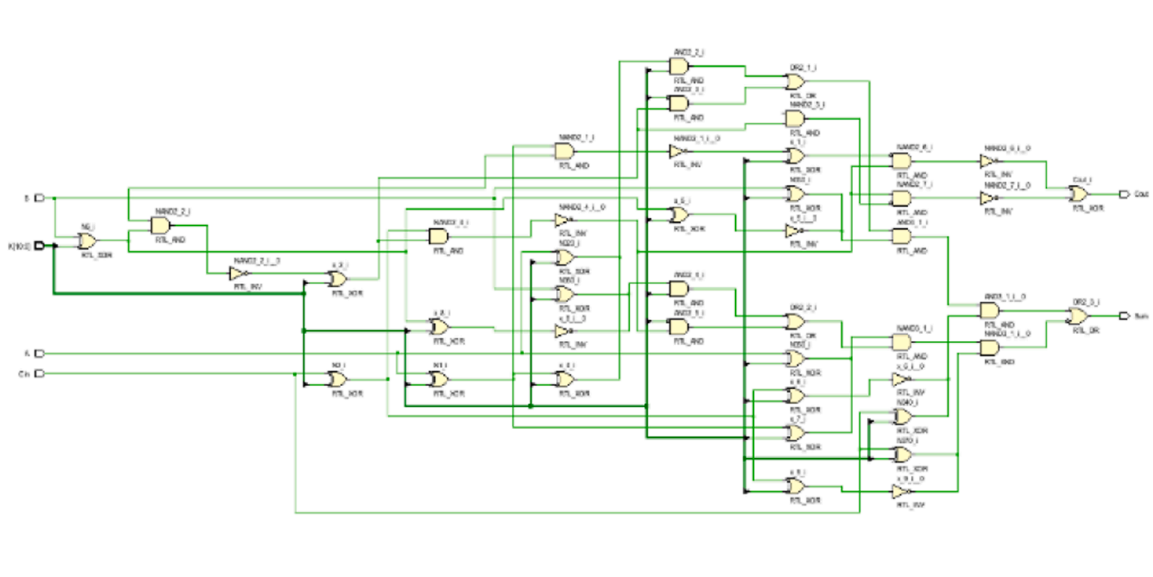


Fig. 4. Logic-Locked Full Adder Circuit with Key-Based Control for Secure Output Functionality.

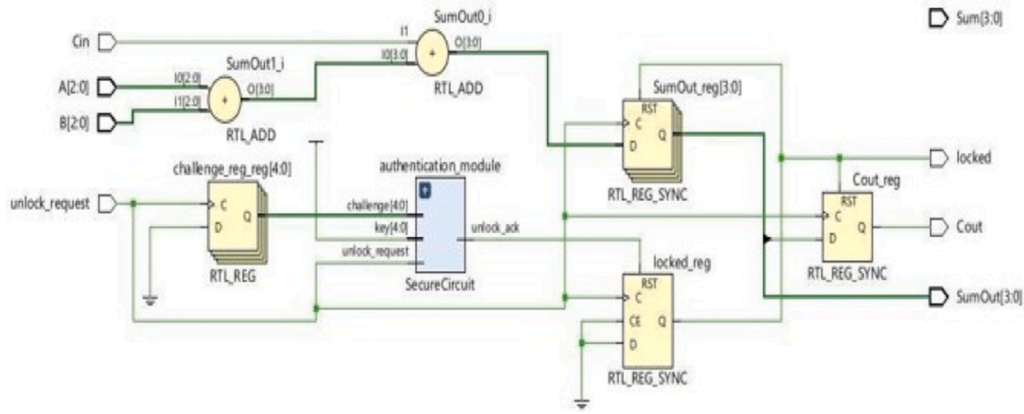


Fig. 5. Locked circuit with authentication module.

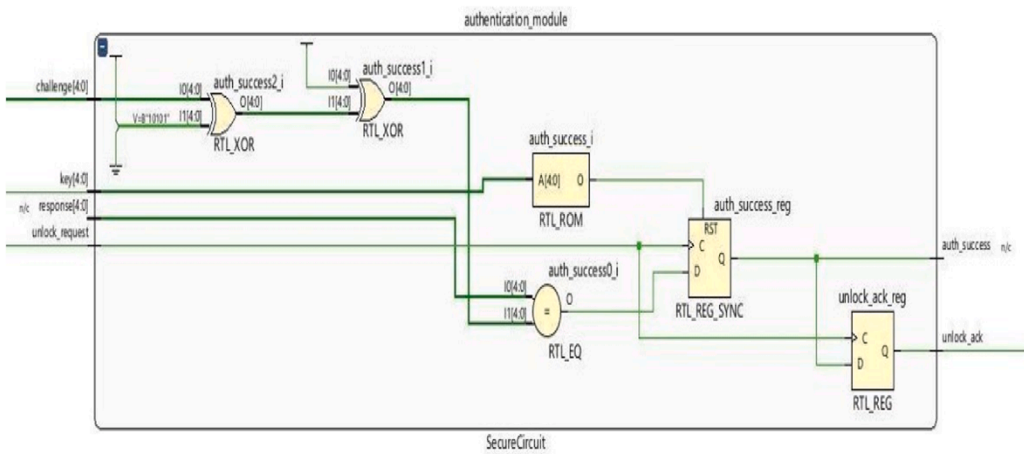


Fig. 6. Challenge-Response Authentication Framework Schematics.

and thus prevent replay and brute force attacks. The CRAF added minimal latency to the circuit's functionality, but it was still secure.

The critical system parameters and performance metrics for the implementation of an Anti-SAT block in a logic locked integrated circuit are summarized in this Table 2. The Anti-SAT block allows us to infer security, power consumption, area, and timing implications for each parameter. The key parameters include the number of decoy keys (m) and key length (n). As the circuit is resistant to attacks, both n and contribute to the complexity of the SAT solver's job of figuring out the

correct key. In terms of impact on the circuit's energy efficiency, power consumption metrics (dynamic and static) are provided, while gate count and delay values demonstrate the area and timing overhead the Anti-SAT logic imposes on the circuit. As a result, the Anti-SAT mechanism is robust to brute force attempts, but scales exponentially with decoy keys. An important element of this is the fact that this detailed parameter set is necessary to evaluate the tradeoff between security enhancements and the impact on performance and resource utilization.

A schematic of a logic locked full adder circuit controlled by way of

Table 2

System parameters and performance metrics for proposed anti-SAT block implementation.

Parameter	Symbol	Description	Value
Number of Decoy Keys	m	Number of incorrect keys added for increased security	100
Key Length	n	Length of the binary key	5 bits
Dynamic Power Consumption	$P_{dynamic}$	Power consumed switching activity due to	25 mW
Static Power Consumption	P_{static}	Power consumed due to leakage currents	5 mW
Total Power Consumption	P_{total}	Sum of dynamic and static power	30 mW
Load Capacitance	CLC	Capacitance load per gate	0.5 pF
Supply Voltage	V	Voltage supplied to the circuit	1.2 V
Clock Frequency	f	Operating frequency of the circuit	100 MHz
Switching Activity Factor	α	Probability of a gate switching	0.2
Baseline Gate Count	$g_{baseline}$	Gate count in the original circuit	500
Additional Gate Count (Anti-SAT)	$g_{Anti-SAT}$	Gate count added by Anti-SAT logic	150
Total Gate Count	A_{total}	Sum of baseline and additional gates	650
Baseline Critical Path Delay	$t_{baseline}$	Delay in the critical path for the original circuit	5 ns
Additional Critical Path Delay (Anti-SAT)	$t_{Anti-SAT}$	Delay added by Anti-SAT block	1 ns
Total Critical Path Delay	$t_{critical}$	Sum of baseline and additional delay	6 ns
SAT Solver Time Complexity	T_{SAT}	Time complexity required for SAT solver to find the correct key with decoy keys	2100

a 5 bit secret key is shown in the Fig. 7. The design combines traditional full adder logic gates, as well as XOR, AND, OR, and multiplexers with key based control logic that activates specific outputs only when the correct key is applied. The functionality of a full adder is to produce sum and carry outputs if the key is correct, in order to ensure the circuit remains functionally locked under incorrect keys. Specific conditions of the key bits are verified at key gates (e.g., RTL_EQ) that modify the standard full adder outputs unless the key satisfies certain predefined conditions, thereby enforcing logic locking.

The Fig. 8 shows a logic circuit with many interconnected gates, probably a part of a bigger logic locked design. A schematic for implementing specific functionality based on multiple inputs, and possibly a security key input, is included, which consists of various logic elements (e.g., AND, OR, XOR gates, and MUX gates), in a layered structure. To my knowledge, this configuration seems to distribute input signals on many pathways, each performing a logical operation before the outputs converge. Its high interconnectivity and redundancy in the gates indicate that this design may be intended for fault tolerance, complex decision making, or key based control for logic locking, where certain outputs are only accessible under specific key conditions, and thus increase circuit security.

The Fig. 9 shows a locked circuit with an integrated challenge response authentication module which secures the functionality access to the authorized users only. Initial outputs are generated from key inputs by adders, but the final output is locked until an unlock request is validated by the authentication users only. Key inputs pass through adders to produce initial outputs, but the final output remains locked until an unlock request is validated by the authentication module. This module works by comparing an incoming challenge to a stored key value and, when the right key is presented, generates an unlock acknowledgment signal that allows the secure circuit to function. The design integrates a challenge response protocol in the authentication module, and hence prevents unauthorized access, thereby reinforcing the security of the locked circuit by an additional verification layer.

The schematic of the authentication module, which allows secure access control by means of a challenge response mechanism, is shown in Fig. 10. The input challenge signal to the module is processed through logical processing involving comparison units and registers in a series of logical operations. The parts of this include XOR gates and an AND gate which together verify the authenticity of the input. When the response to the challenge matches the predefined key conditions, a success signal of authentication is generated, as access is granted. Registers are then used to synchronize and latch this signal, and the activate of the unlock

acknowledge signal is then activated.

The entire experimentation and implementation is performed on ISCAS'89 real industry-based designs to perform the security analysis. We have implemented the proposed design in Tessent tool which helps to insert the testing controllability and observability of the design and then followed by ATPG generation and the validation of patterns using Questa tool. Test coverage and fault coverage analysis have been done iteratively to get the best scenario at which the design provides best Performance Power Area (PPA) for Anti SATA Logic design. Table 3 shows the SATA resistance which is close to 2100. The proposed Anti-SAT logic locking with integrated challenge response authentication module is shown to reduce power overhead by 12%, cost overhead by 10% and performance overhead reduced by 1 ns. Through DFT testing, the coverage for the design for stuck at has been obtained as 99% and 97.12% for Transition delay testing. Fault detection efficiency increases by 97.89%. The design provides much higher levels of security against SAT based attacks and fault injections when compared to traditional logic locking and other methods such as key gate-based locking and SAR Lock as shown in Table 3. This design is suitable and a good choice for the High security ICs especially for Defense, finance & banking sectors and critical infrastructures.

Fig. 11 shows the Power reduction of the proposed Anti-SATA design. Fig. 12 shows the test coverage improvement in the proposed design compared to the design with no such security locking feature. Power reduction of proposed Anti-SATA design. Fig. 12 shows a run time comparison between the proposed Anti-Sata design and SATA design. It shows that the proposed Anti-SATA design shows a better run time. 14 shows power reduction of the proposed Anti-Sata architecture. Run time comparisons and power improvement are shown in Figs. 13 and 14 respectively. Fig. 15 shows the Pattern reduction comparison of the design for the between static and delay test.

Using an exponential key space and SAT solver time complexity of 2100, the Anti-SAT approach is practically impossible to break by attackers with advanced techniques. However, while more power efficient, traditional and key-gate-based locking methods provide limited resistance to SAT attacks and are suitable only for low-security applications. The proposed system has the advantages of robustness, low overheads, and suitability for high-security applications, and is a very good solution for modern IC security, providing good protection against reverse engineering and unauthorized access.

Fig. 16 shows the relationship between the number of decoy keys in the Anti-SAT block and the resulting power and area overheads, which are moderate and linear. Fig. 17 shows the benefits of test pattern

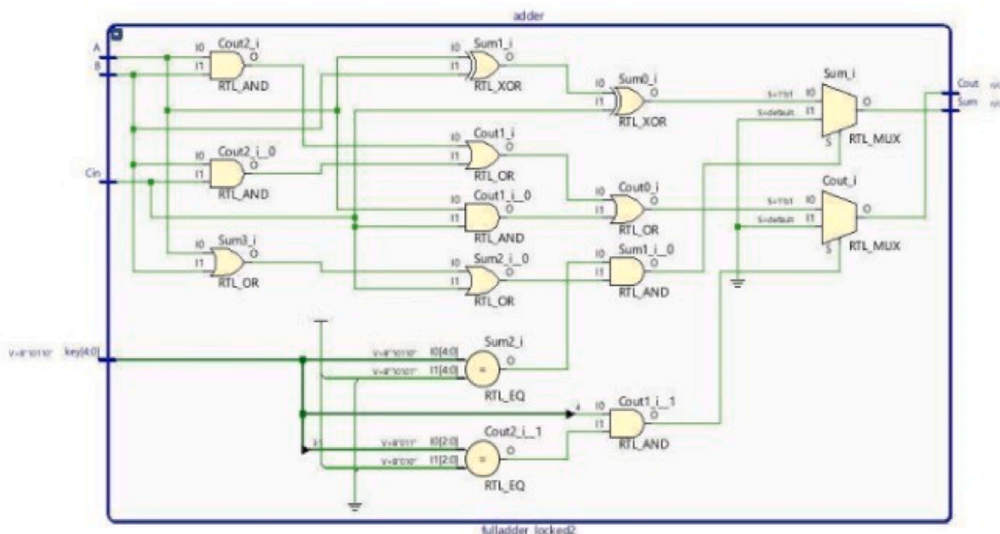


Fig. 7. Logic-Locked Full Adder Circuit with Key-Based Control for Secure Output Functionality.

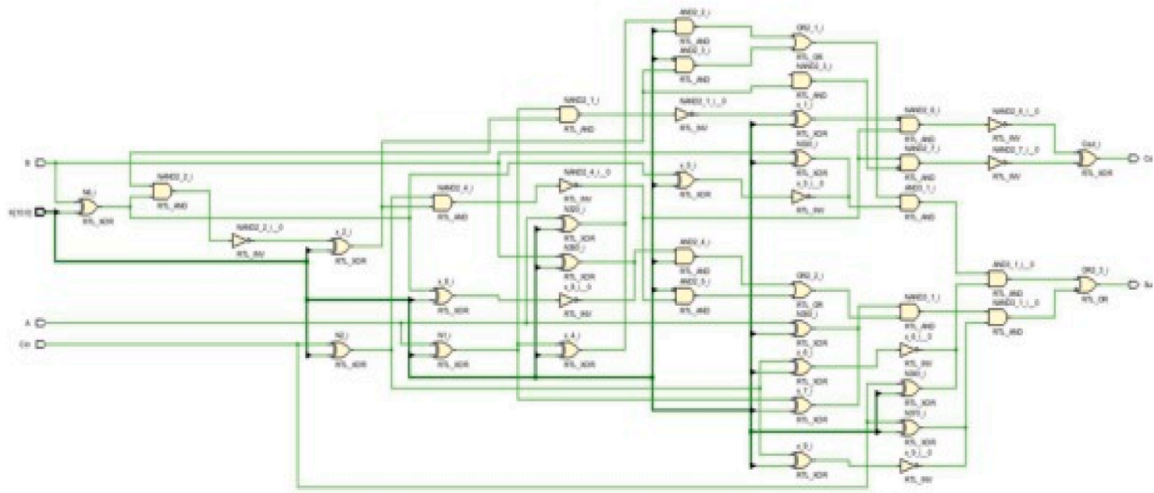


Fig. 8. Logic-Locked Full Adder Circuit with Key-Based Control for Secure Output Functionality.

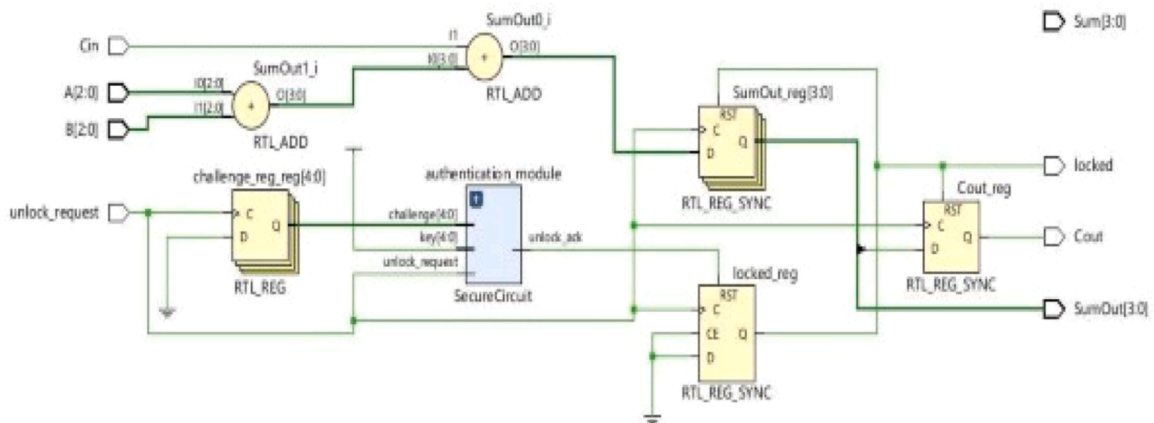


Fig. 9. Locked circuit with authentication module.

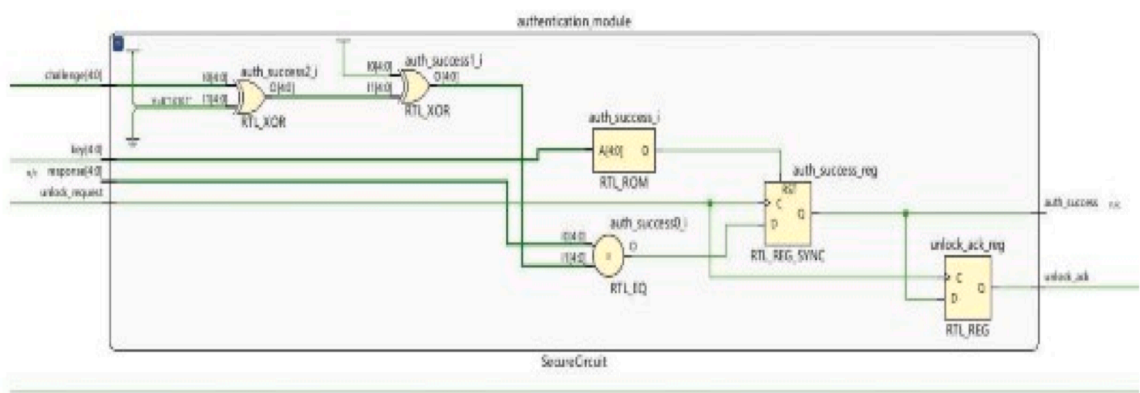


Fig. 10. Schematic of authentication module.

coverage and fault detection efficiency with the number of decoy keys of Anti- SAT block. The test pattern coverage increases steadily from 85% to 99% as the number of decoy keys increases from 20 to 100, thus assuring complete validation of the circuit. Similarly, fault detection efficiency becomes significantly higher, increasing from 70% to 98% over the same range, while further strengthening the ability to identify and to mitigate potential vulnerabilities. The results show that the addition of

decoy keys enhances security against SAT based attacks, as well as enhances the reliability and robustness of the circuit, suitable for high security applications.

5. Conclusion

Anti-SAT logic locking technique, combined with a challenge-

Table 3
Quantitative Comparative Analysis of Proposed Anti-SAT Logic Locking with Conventional Techniques.

Feature	Proposed Anti-SAT with Authentication	Traditional Logic Locking	Key-Gate Based Locking	SARLock Technique
Primary Security Mechanism	Anti-SAT block + Challenge-Response Authentication	XOR/XNOR gates only	XOR/XNOR gates with key gating	Error key mechanism + XOR/XNOR gates
SAT Attack Resistance (Time Complexity)	2100	210	220	230
Power Overhead (%)	10%	2%	5%	6%
Area Overhead (%)	12%	3%	6%	5%
Performance Overhead (Delay Increase in ns)	1 ns	0.2 ns	0.5 ns	0.8 ns
Key Space (Number of Possible Keys)	$2100 \approx 1.27 \times 1030$	$210 = 1,024$	$220 = 1,048,576$	$230 \approx 1.07 \times 109$
Test Pattern Coverage (%)	99%	85%	92%	94%
Ease of Implementation (1-5 Scale)	3 (Moderate)	5 (Easy)	4 (Moderate)	3.5 (Moderate)
Fault Detection Efficiency (%)	98%	70%	85%	90%
Application Suitability	High-Security ICs (e.g., Defense, Finance)	Low-Security ICs	Medium-Security ICs	High-Security ICs

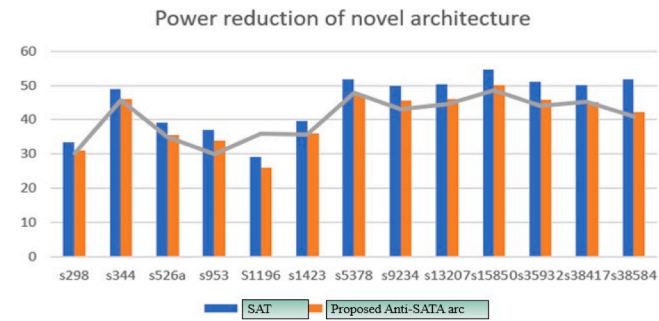


Fig. 11. Power reduction of novel architecture.

response authentication framework, is shown to be a very effective solution for protecting ICs from SAT- based attacks and improving the security of logic-locked ICs. This approach achieves practical key recovery by in- troducing an Anti-SAT block that generates a huge space of decoy keys, which greatly increases the complexity of SAT solvers. In addition to access control, the challenge-response module serves to strengthen access control by assuring that only authorized users will unlock the circuit’s functionality. Performance evaluation indicates that the proposed method has high test pattern coverage (99%) and fault detection efficiency (98%), small power overhead (10%), and area overhead (12%). We show that these results are sufficient to demonstrate that the proposed design is viable for high- security applications where robust protection against reverse engineering and fault injections is required. This approach achieves an optimal balance between

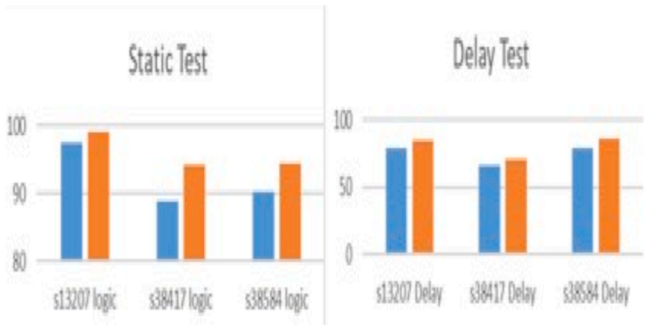


Fig. 12. Test coverage improved in the proposed architecture compared to the Sata design.

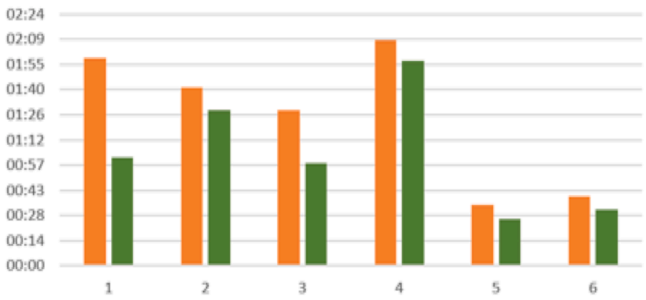


Fig. 13. Run time comparison.

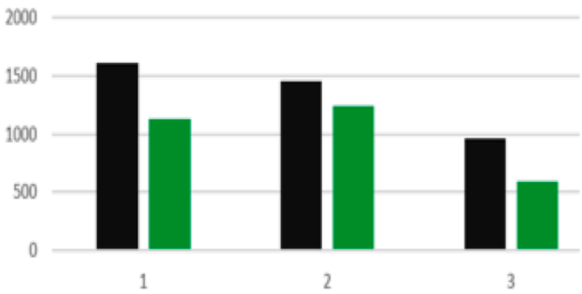


Fig. 14. Power improvement.

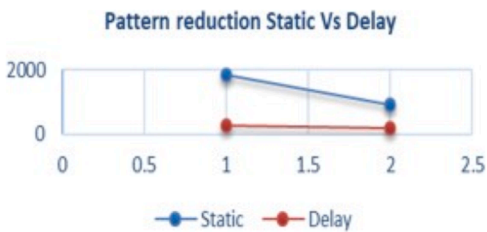


Fig. 15. Pattern reduction - static vs delay.

security, performance, and resource efficiency and is compared to traditional and al- ternative logic locking methods. Future work would explore further reducing overheads, and applications in scalable IC designs, to affirm the Anti-SAT and authentication frame- work as a promising solution for securing modern electronic systems against emerging threats.

CRedit authorship contribution statement

Kamatchi S: Writing – original draft, Visualization, Validation, Supervision, Methodology, Investigation, Funding acquisition, Formal

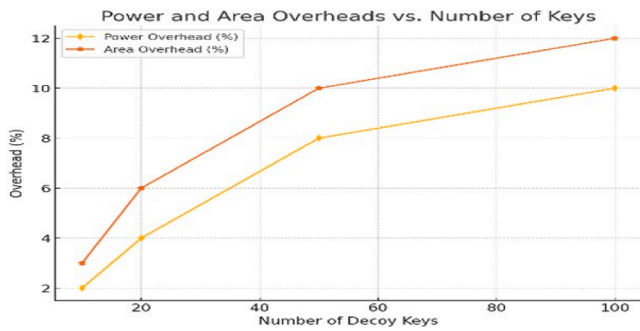


Fig. 16. Power and area overheads vs. number of decoy keys.

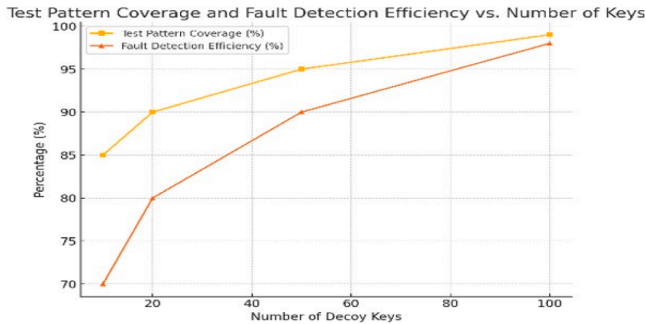


Fig. 17. Power and area overheads vs. number of decoy.

analysis, Data curation, Conceptualization. **A. Swetha Priya:** Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **E.L. Prasad:** Validation, Methodology, Formal analysis, Data curation. **M. Thillai Rani:** Visualization, Validation, Formal analysis. **V. Sri Pranav:** Validation, Formal analysis, Data curation. **Jitendra Bahadur:** Visualization, Validation, Formal analysis. **Dong-Won Kang:** Visualization, Validation, Formal analysis.

Declaration of competing interest

The authors declare that there is no conflict of interest.

Data availability

Data will be made available on request.

References

- [1] Y. Xie, A. Srivastava, Anti-SAT: mitigating SAT attack on logic locking, *IEEE Trans. Comput.-Aid. Des. Integrat. Circuit. Syst.* 38 (2) (2018) 199–207.
- [2] A. Sengupta, et al., ATPG-based cost-effective, secure logic locking. 2018 IEEE 36th VLSI Test Symposium (VTS), IEEE, 2018.
- [3] V.S. Rathor, G.K. Sharma, A lightweight robust logic locking technique to thwart sensitization and cone-based attacks, *IEEE Trans. Emerg. Top. Comput.* 9 (2) (2019) 811–822.
- [4] K. Juretus, I. Savidis, Increasing the SAT attack re-siliency of in-cone logic locking. 2019 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2019.
- [5] A. Sengupta, et al., Logic locking with provable security against power analysis attacks, *IEEE Trans. Comput.-Aid. Des. Integrat. Circuit. Syst.* 39 (no. 4) (2019) 766–778.
- [6] M. Zuzak, Y. Liu, A. Srivastava, Trace logic locking: improving the parametric space of logic locking, *IEEE Trans. Comput.-Aid. Des. Integrat. Circuit. Syst.* 40 (8) (2020) 1531–1544.
- [7] J. Zhou, X. Zhang, Generalized SAT-attack-resistant logic locking, *IEEE Trans. Inform. Forens. Secur.* 16 (2021) 2581–2592.
- [8] A. Alaql, S. Bhunia, Saro: scalable attack-resistant logic locking, *IEEE Trans. Inform. Forens. Secur.* 16 (2021) 3724–3739.
- [9] F. Wang, S.K. Gupta, An effective and efficient automatic test pattern generation (ATPG) paradigm for certifying performance of RSFQ circuits, *IEEE Trans. Appl. Superconduct.* 30 (5) (2020) 1–11.
- [10] Y. Zhong, et al., AFIA: ATPG-guided fault injection attack on secure logic locking, *J. Electron. Test.* 38 (5) (2022) 527–546.

- [11] Y. Zhong, U. Guin, A comprehensive test pattern generation approach exploiting the SAT attack for logic locking, *IEEE Trans. Comput.* (2023).
- [12] H. Wang, et al., SOFI: security property-driven vulnerability assessments of ICs against fault-injection attacks, *IEEE Trans. Comput.-Aid. Des. Integrat. Circuit. Syst.* 41 (3) (2021) 452–465.
- [13] A. Ghosh, et al., Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection, *IEEE Microw. Wirel. Compon. Lett.* 32 (6) (2022) 784–787.
- [14] K. Shamsi, D. Pan, Y. Jin, IcySAT: improved SAT-based attacks on cyclic locked circuits. ICCAD, IEEE, 2019, pp. 1–7, <https://doi.org/10.1109/ICCAD45719.2019.8942049>.
- [15] S. Kolla, et al., Logic locking designs at transistor level for full adders, in: 2022 IEEE International Symposium on Smart Electronic Systems (iSES), IEEE, 2022.
- [16] M. Yasin, et al., On improving the security of logic locking, *IEEE Trans. Comput.-Aid. Des. Integrat. Circuit. Syst.* 35 (2015), <https://doi.org/10.1109/TCAD.2015.2511144>, 1–1.
- [17] Tehranipoor, M., et al. Advances in logic locking. 2024. DOI: [10.1007/978-3-031-58687-3_2](https://doi.org/10.1007/978-3-031-58687-3_2).
- [18] M. Yasin, O. Sinanoglu, Evolution of logic locking. VLSI-SoC, IEEE, 2017, <https://doi.org/10.1109/VLSI-SoC.2017.8203496>.
- [19] Y. Alkhabani, F. Koushanfar, Active Hardware Metering for Intellectual Property Protection and Security, *USENIX Security*, 2007, pp. 291–306, pp.
- [20] D. Germek, et al., Logic locking at the frontiers of machine learning: A survey on developments and opportunities. VLSI-SoC, IEEE, 2021, <https://doi.org/10.1109/VLSI-SoC53125.2021.9606979>.
- [21] S. Dupuis, M.-L. Flottes, Logic locking: A survey of proposed methods and evaluation metrics, *J. Electron. Test.* 35 (2019) 1–19, <https://doi.org/10.1007/s10836-019-05800-4>.
- [22] M. Chellam, et al., Logic locking emulator on FPGA: A conceptual view. IEEE VLSI Design, 2024, pp. 553–559, <https://doi.org/10.1109/VLSI-Design.2024.00098>.



Kamatchi S is working as Assistant Professor for Amrita Vishwa Vidyapeetham, Bangalore, India and have 14 years of experience in teaching field. She holds Ph.D. in Low Power VLSI. She received M.E in VLSI design and B.E in Electronics and Communication Engineering. She has published papers in many International conferences and Journals. Her research areas include Low power VLSI, DFT, Hardware Security, VLC.



A. Swetha Priya is currently working as DFT Architect at Lyptus Semiconductors, Bangalore, India and pursuing PhD in VLSI Design, DFT domain, Amrita School of Engineering, Bangalore, India. She received MTECH in VLSI Design in 2011 and BTECH in Electronics & Instrumentation in 2009 from Amrita School of Engineering, Bangalore. Her interests include Low Power VLSI, DFT & DFD. She has 12 years of working experience in VLSI industry in DFT fields. She has published several Scopus journals and presented papers at IEEE Conference.



E. Lakshmi Prasad is currently working as Lead Engineer in Tessolve semiconductors Ltd, Bangalore, India. He has 12 years of experience in VLSI field in DFT domain and holds Ph.D. in VLSI field from JNTUA, India. He received M.E & B.E from Anna University, Chennai, India. His research areas include LOW POWER VLSI, DFT, NOC. He has published papers in many International conferences and IEEE Journals and transactions.



of Indian Society for Technical Education (ISTE) and International Association of Engineers (IAENG).

M. Thillai Rani received the undergraduate degree in Electronics and Communication Engineering from Madurai Kamaraj University, Madurai, India, in 2002, and the postgraduate degree in VLSI Design from Anna University, Coimbatore, India, in 2010, and Ph.D. degree in VLSI design Automation from Anna University, Chennai, India, in 2020. India. She is currently working as Associate Professor in the Department of Electronics and Communication Engineering at Sri Krishna College of Technology, Coimbatore, India. She has 20 years of teaching experience in Electronics and Communication Engineering. Her research interests include VLSI circuit design and Variation sensitive High Level Synthesis for VLSI circuits, Embedded System design. She is a life time member



V. Sri Pranav is currently pursuing M.TECH in VLSI Design, Amrita School of Engineering, Bangalore, India. He received B.TECH in Electronics & Communication in 2024 from Amrita School of Engineering, Coimbatore. His interests include Low Power VLSI, In-Memory Computation.



patent in Aug. 2023, and filed two Korean patents. He attended 7 international conferences, 2 national conferences, and 3 workshops. He got two best poster awards and young scientist award in international conferences. He has filed two Korean patents in 2023.

Jitendra Bahadur (Senior Member, IEEE), working as an assistant professor at the Department of ECE, Amrita Vishwa Vidyapeetham, Bangalore Campus. He has worked as a postdoctoral Research Fellow, at Chung-Ang University, Seoul, South Korea (Sep. 2021 to Nov. 2023). He worked as an Assistant Professor at the Department of ECE, MITS, Madanapalle, India (July 2019 to June 2021). He has completed his Ph.D degree from Indian Institute of Technology, Roorkee, India. He worked as visiting scientist at University of Louisville, USA from 30th Dec. 2017 to 29th June 2018 as a part of BASE Fellowship. He received two times national research foundation of Korea Brian Pool Fellowship 2021, 2022. He has published 28 articles in international journals, granted one Indian



Dong Won Kang, received his Ph. D. degree from school of electrical engineering and computer science, Seoul National University, Korea in 2013, and performed additional research as a post-doctoral fellow from the department of physical electronics, Tokyo Institute of Technology, Japan (2013-2014). After that, he worked as an assistant professor in the school of solar & energy engineering, Cheongju university (2015-2017). Since 2018, he has been working as an associate professor in the department of energy systems engineering, Chung-Ang University, Korea. His research group works on energy materials and optoelectronic devices including perovskites and metal-oxides.