Journal of Electronic Testing (2023) 39:141–153
https://doi.org/10.1007/s10836-023-06061-y

Design of INV/BUFF Logic Locking For Enhancing the Hardware Security

R. Naveenkumar[1,2] · N. M. Sivamangai[1] · A. Napolean[1] · S. Sridevi Sathya Priya[1] · S. V. Ashika[1]

Received: 28 November 2022 / Accepted: 26 March 2023 / Published online: 5 May 2023

Abstract
An increasingly popular method for defending an integrated circuit (IC) against theft, excess production, and the Hardware Trojans (HT) is logic locking. The majority of popular logical locking approaches were also susceptible to the SAT attacks. Although it has been reported that there are a number of SAT-resistant logical locking methods, such as Anti-SAT blocks (ASB), that lengthen the amount of time it takes to figure out the correct key, the current methods are possibly susceptible to removal attacks based on signal probability skew (SPS) or have a high design cost. It is suggested to use an INV/BUFF key model that produces an optimized design with less overhead than XOR/XNOR. The suggested method can significantly enhance logical locking without compromising security. Moreover, it reduces the area, power, and time overheads, respectively, by 2.76 %, 12.92 %, and 12.7 % in comparison to the XOR-based technique.

Keywords Hardware Security · Integrated circuit · Logical locking · Signal probability skew (SPS) · And Anti-SAT attack

1 Introduction

In today's world, third-party manufacturing process outsourcing in the production of chip is necessary, even for the greatest silicon companies, keeping a foundry with modern fabrication capabilities is expensive. Because the offshore some of the foundry may be untrustworthy, it offers significant security risks from numerous threats like Intellectual property (IP) theft, Reverse engineering (RE), overbuilding, and, Hardware Trojan (HT) [1]. The IC industries lose billions of dollars each year as a result of supply chain assaults. Various design-for-trust strategies, including logic locking and camouflaging [2] have been found to mitigate the aforementioned threats. By including extra key gates, such as XOR/XNOR, into the architecture, logic locking and encryption has gained recognition as a successful way for locking the functionality of the design in recent years multiplexer (MUX) , as well as by deploying new key-gates/ look-up tables (LUTs) in place of the original design [3]. Only when the correct key is pressed does the design work properly. An attacker cannot explore the right key values as the key bits are stored in a chip with a temper-proof memory. Logic locking security is at risk if an intruder may expose the right key in a timely manner. Notably, the very effective SAT assault has been revealed that may disclose the correct key within a matter of hours, also with enormous key sizes [4]. By employing distinguishing input patterns (DIPs), this approach iteratively removes all wrong key combinations.

Motivation of Research Work Various SAT-resistant techniques, like ASB, the availability of ASB makes the amount of SAT repetitions required to make the SAT assault exceedingly difficult. The AES circuit-based SAT-resistant technique necessitates substantial design overhead, but the Anti-SAT block-based method is sensitive to SPS-oriented removal, AppSAT, and bypass assaults. However, employ designed withholding with wire entanglement to obscure the Anti-SAT block against the aforementioned assaults. However, because of the usage of MUX and LUTs, this solution necessitates substantial overhead with design [5]. As a

Responsible Editor: C. A. Papachristou

✉ R. Naveenkumar
naveentamil256@gmail.com

N. M. Sivamangai
nmsivam@gmail.com

A. Napolean
nepojustin@gmail.com

S. Sridevi Sathya Priya
s.d.s.priya@gmail.com

S. V. Ashika
ashikas@karunya.edu.in

[1] Department of ECE, Karunya Institute of Technology and Sciences, Coimbatore, Tamilnadu 641114, India

[2] Dept. of ECE, Karpagam Academy of Higher Education, Coimbatore, India

result, in this research, we suggest innovative ASB design and obfuscation methods that can successfully conceal the ASB from functional/ structural analysis and SPS-based removal assaults with minimal complexity.

Hardware Security The manufacture of integrated circuits is currently outsourced to foreign foundries by a large number of semiconductor businesses, including Apple. Outsourced assembly and test (OSAT). Amkor can also provide test, assembly, and packaging services in addition to fabricating integrated circuits. To lessen their design effort and adhere to stringent time-to-market requirements, even design houses may acquire and employ third-party intellectual property (3PIP) cores. A number of (perhaps unreliable) agents have access to the priceless IP or the actual IC in a worldwide and dispersed IC supply chain. Rogue individuals may be able to take advantage of important knowledge or endanger the trust in the IC design flow as a result of the enhanced access to essential assets. As a result of globalization, challenges and vulnerabilities related to hardware security have appeared at several levels of the IC supply chain.

A. Reverse engineering (RE) is the function of retrieving an IC's design and technological information utilizing imaging techniques. Reverse engineering is a service provided by organizations like Chip Works. To obtain confidential information, such as cryptographic keys, RE can be used in conjunction with probing techniques.
B. IP Piracy: IP piracy is the term for the improper or unauthorized IP usage (e.g. net list or files of GDS-II). Important IP cores might be stolen by an attacker and passed off as genuine, just like with software piracy. Over $4 billion is lost every year to IP infringement in the semiconductor business.
C. Overbuilding: IC piracy takes the shape of excessive construction at an unreliable foundry. Overproducing ICs might allow a dishonest foundry to sell the extra units illegally. The cost of the foundry is only slightly increased when more integrated circuits are built using the same set of masks; the foundry may sell those ICs for less than the original IC Company would charge.
D. Hardware Trojans (HT): An IC can have modest, difficult-to-detect circuitry inserted by malicious parties in the design house or foundry that might leak confidential information or interrupt services while the IC is operating [6]**.** Since a Trojan's footprint might be rather small, it can be challenging to check for Trojans in a circuit, especially in the absence of a gold-standard (Trojan-free) reference. 3PIP utilised in the design or mask modification during production are the likely origins of Trojans.
E. Counterfeiting: Falsely created counterfeit integrated circuits (ICs) are copies of the real ones that seem very similar to the real ones. Out-of-spec, noted, and recycled counterfeit integrated circuits are a common sight in abandoned electronic equipment. Over 5% of all commercially available ICs are fakes. For the semiconductor business, fake ICs raise major reliability and security issues.

The objective of the work is for ensuring the security of traditional logical blocking methods against SAT assaults, it has been created to produce the ASB with minimal overhead using the INV/BUFF key-gate. To avoid SAT threats, it is suggested to use a practical logic obfuscation technique with minimal space, power, and efficiency overheads. On a conventional benchmark circuit, experimental assessments are shown.

Methodology The strong Anti-SAT Block (ASB) design/ integration approach is presented, which successfully thwarts the functional/structural modelling elimination attack by using certain circuits of the locked existing circuit. Authors present an ASB obfuscation method which effectively defeats the SPS-based removal assault while needing minimal effort. In addition, to increase output corruptibility, we present a technique that randomly places the ASB in a locked configuration. Moreover, by locking the design and creating the ASB, a new lightweight INV/BUFF key-gates design is created to minimize overhead over XOR-based key-gates.

The authors suggest a novel lightweight ASB architecture and obfuscation approach. The suggested ASB design and obfuscation approaches reduced area overhead by 25.5% and 22%, respectively, based on testing results on ISCAS-85 benchmarks. Not only does it successfully increase logic locking security, but it also greatly decreases design overhead [7]. A novel class of analogue Trojan may interact with digital and analogue macros to carry out hardware attacks during fabrication time. These large delay-based analogue Trojan circuits. It can be challenging to identify analogue Trojans since they can start up without any digital input signal and operate in a variety of on-chip power domains. To initiate an attack against an IC's PMU unit in order to build a kill switch [2]. A logic locking approach is created to safeguard the IC from hackers in order to increase hardware security. Key gates are generated using the Pseudo Random Number Generator (PRNG) to conceal the attackers. The PRNG output is utilised to produce the input of the circuit which can be used for automated testing. The suggested method decreases the area as well as the delay. These strategies are insecure and result in power excessive consumption [8]. To combat piracy, overbuilding, and RE attacks, use an effective logic obfuscation approach. A low-overhead logic obfuscation approach for preventing an attacker both the layout-level geometry and the gate-level netlist of IP/

IC are taken from RE. Prevent piracy and overbuilding by protecting IP/IC [9].

A True Random Number Generator (TRNG) it is possible to create a reliable TRNG architecture with just one PLL and three on-board primitives as well as a few additional basic logic units (e.g. 2 Counters, 8 D-type Flip-Flop, and 17 LUT. utilised for initial system-wide synchronization and post-processing tasks. The final system throughput will be reduced if the relative phase shift regulation of the FF input signals is not resolved to the best of one's ability. This will need a more intensive post-processing of the raw bitstream [10]. Reduce the number of duplicated key inputs and streamline SAT issues. A key checking procedure that increases the amount of faulty keys removed on every SAT-solving repetition. This approach can crack 10 benchmark circuits that were previously impossible to crack in one hour. It is immune to SAT-based assaults. The last improvement makes it possible for a SAT attack to overcome the cyclic logic encryption method, which locks a circuit by creating cycles and is resistant to the initial SAT attack [3]. A unique DFT approach that successfully boosts design protection to Trojan attacks while needing minimum overhead. The simulation findings demonstrate that the suggested key-gates lower per-gate area and energy by 34.2 and 35.1 %, respectively, when compared to stack-based key-gates. This removal attack approximates the absolute difference of probability skew (ADS) of distinct gates' inputs and recognize the gate with the maximum ADS (a gate whose inputs are oppositely skewed) as belonging to the ASB. It is possible that it will be ineffective in preventing piracy, overdevelopment, and RE [11]. CamoPerturb is a countermeasure to the decamouaging assault that combines logic perturbation with IC camouflage. CamoFix, a distinct camouflaged block, fixes the disturbed minterm, restoring the design's functionality. Reviving IC camouflage and making it useful against reverse engineering are both achieved by CamoPerturb [12].

To break the ASB, use a SPS attack. SPS attacks allow for the removal of ASB by recognizing their output gates, although if the blocks are architecturally / functionally obfuscated. The proposed method decreases both the area and the latency. SPS attacks become more effective as key size increases [13]. The ASB is used for improve the security of the traditional logic locking mechanisms to SAT attacks. Address the ASB's susceptibility to different removal attempts and study obfuscation strategies to avoid these type of removal assaults. Effectively counter the SAT assault and other removal attacks [14]. In addition, outline the assessment criteria used in the literature to evaluate the efficacy of hardware obfuscation approaches. Device metrics that assist designers in quantifying and quickly assessing the success of obfuscation during the early design stages are highly needed. The maintainability of hardware obfuscation techniques has received little attention [15]. Strong Anti-SAT (SAS) is a method of ensuring significant application-level effect by assigning a collection of key minterms enhanced corruptibility. Strong Anti-SAT protects processors from SAT attacks by assuring exponential SAT attack complexity and strong application-level effect when an incorrect key is used. Comparing Strip functionality logic locking (SFLL) to Strong Anti-SAT (SAS), Strong Anti-SAT delivers stronger security and less hardware overhead [16].

Full-lock logic locking systems are SAT-resistant. Every time the SAT solver iterates, more recursive DPLL calls are required due to full-lock SAT resistance causing each iteration to take an extremely lengthy time to finish. If the incorrect key is used to activate Full-Lock, the output is highly corrupted. It's resistant to removal and algebraic assaults [17]. A novel logic encryption approach that uses XOR/XNOR key gates to withstand the SAT attack. Compared to the modern XOR/XNOR-based logic encryption strategy, the method provides superior security for protecting against the SAT attack. By encrypting a total of 22 benchmark circuits, which can be successfully decoded within 10 minutes, they become impossible to break within 1 hour [1]. Time is being analyzed in order to induce a transition in functional Trojans. The approach raises net transition probabilities above a certain level. Smaller Trojans have the potential to be completely activated and cause functional faults [18].

In order to assess the defences from HT, IP piracy, and modern threat models, cutting-edge countermeasures, and metrics have been established. Systematizes the present understanding in this developing subject, including a threat model categorization, cutting-edge defences, and assessment metrics for significant hardware-based assaults. Using the target threat model and the accompanying metrics, the countermeasures may be contrasted with one another by structuring the threat/defense scenarios [6]. Encrypting the design by introducing extra gates that provide accurate outputs only when certain inputs are introduced to these gates. A designer can use this approach to controllably corrupt the outputs. To be more specific, this strategy aims for a Hamming Distance (HD) 50 % between the right, erroneous outputs (ideal situation) if incorrect key is used to increase uncertainty for an attacker. When compared to random logic encryption, the 50% HD objective is accomplished with a lesser number of extra gates. Each iteration of this job introduces a single key-gate. In big designs, this insertion may be computationally costly [5]. Demonstrate how an adversary can decrypt the obfuscated netlist in a time that

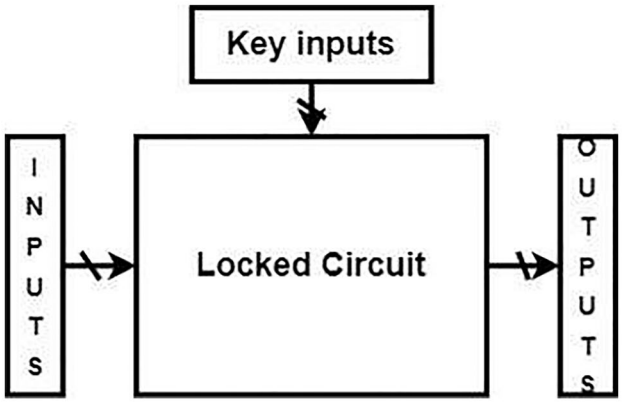


Fig. 1 Overview of logic locking

is linear to the number of keys by exposing the key values to the output. Create methods to close this security issue and make obfuscation genuinely exponential with respect to the amount of entered keys. By manipulating only the inputs and monitoring the results, IC testing approaches enable designers and testers to probe into the design. One way an attacker may circumvent logic obfuscation is by using this capability [19]. Quantitative security assurances are offered by SAR Lock and SFLL (Secure Function Logic Locking) against SAT elimination and approximation attacks. There isn't any latency overhead as well as the area overhead is about 10%, showing the usefulness and efficacy of SFLL. Logic locking solution that is affordable and logically safe against all assaults [20].

Timing SAT attacks that circumvent the protection offered by modern delay locking countermeasures. Highlight the speedy de-obfuscation of delay-locked net lists using the suggested Timing SAT attack. Within a sufficient length of time, de-obscure the functionality of such delay-locked architectures [21]. A smart initial key-gate selection method provides more security. Improve both security levels and run-time by accelerating the check for pairwise secure key-gate sites. A circuit may be made more secure against IP theft and reverse engineering assaults by adding more pairwise secure key gates. To determine how long it takes to break a circuit, formal analysis is necessary [22]. Develop a fault analysis-based logic encryption technique to analyze fault propagation in IC testing. When a faulty key is used in the design, fault analysis-based logic encryption obtains 50% HD between the right and matching incorrect outputs. This method has the benefit that each chip already comes with a distinct decryption key [23]. The connectivity cyclic obscurity strategy underlies SAT attacks. The security of cyclic obfuscation must be further assessed since cyclic circuits are not amenable to SAT attacks. As a result, it is essential to use oracle-guided assaults that can simulate such circuits. An important future approach is the thorough characterization and execution of the layout level utilizing fake gates. SAT attacks are utilised in logic locking and IC camouflaging [24].

Compared to previous methods, logic locking safeguards the circuit at the foundry level, from SoC integrators, and from hackers. To prevent SAT attack, ASB might be embedded in the design. With minimal cost, anti-SAT blocks may successfully counter SPS-based removal attempts. The SAR lock decrease the amount of various input patterns needed to find the secret key. Strong Anti-Sat is an efficient locking method that achieves great locking effectiveness without sacrificing security.

2 Logic Locking Techniques

Whenever the correct key is inserted into on-chip memory, a logic circuit restores the original functionality. As shown in Fig.1, to address the special functionality of an IC design, more key inputs (key-inputs), on-chip memory, and additional key used (key-gates) are supplied. An IC with

Table 1 logic locking assaults and their analyses

Attack	Sensitization [15]	Signal probability skew [24]	App SAT [25]	SAT [26]
Attack location	Producer or Consumer	Producer or Consumer	Producer or Consumer	Producer or Consumer
Threat model	Netlist-locked	Netlist-locked	Netlist-locked	Netlist-locked
	IC based functional level		IC based functional level	IC based functional level
Attack method	Own separate key bit sensitivity for main outputs	Determine output by using the signal skew as a trace.	When SAT assaults are combined with random oracle queries, It is possible to limit multi-layered defences to single-layered defences.	Using distinguishable input patterns, get clear of wrong keys
Attack defense	Encrypted using strong logic	TT lock, SFLL	Anti-SAT, SAR Lock	Anti-SAT
Type of attack	Algorithmic attack	Removal attack	Approximation attack	Algorithmic attack
Type of defense	Pre-SAT	Post - SAT	Post - SAT	-

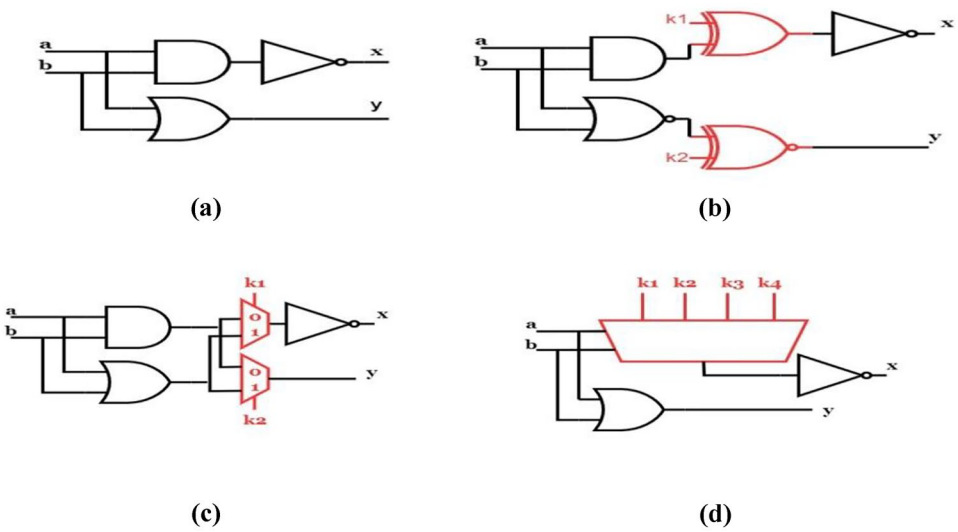


Fig. 2 Logic locking types (**a**) Initial-netlist (**b**) XOR/XNOR-oriented method locking (**c**) Locking logic with Mux (**d**) Locking method using the LUT

key functions (inputs) are connected with on-chip memory can operate only successful, when it is programmed with a reliable secret. Tamper-proof chip security must be fitted to ensure that functional chip's internal signals cannot be inspected by an unlicensed foundry.

Logic Locking Attacks Authors discuss several attacks on logic locking approaches in this section. Table 1 contrasts several attacks in logic locking. Attack location, models, its strategy, and defence against the attacks.

Logic locking types: It may be divided into three main groups depending on the key-gate types: XOR/XNOR , Mux based key gates , and look-up tables (LUTs) based logic locking. Figure 2 depicts the IC design procedure with locking.

The locked-netlist travels into the unprotected design stages. When key is not there, design and specifications are lost, the IC is faulty, and incorrect outputs are produced. To unlock a locked IC, The chip memory has to be entered using the correct key.

3 Proposed INV/BUFF Key Model Technique

Modern integrated circuit (IC) development cannot avoid outsourcing the production process to a third party because maintaining a foundry with sophisticated fabrication skills

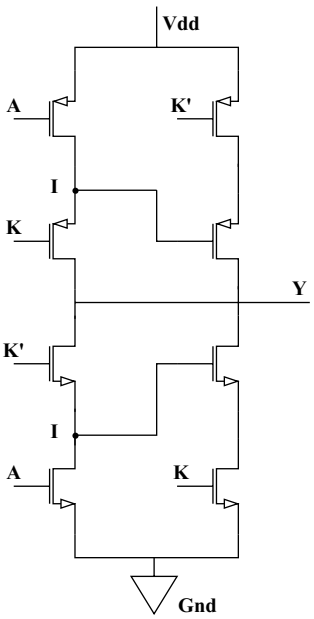


Fig. 3 INV/BUFF oriented key model proposed

Key	Input	Output
K	A	Y
0	0	1
0	1	0
1	0	0
1	1	1

Schematic design

Truth table

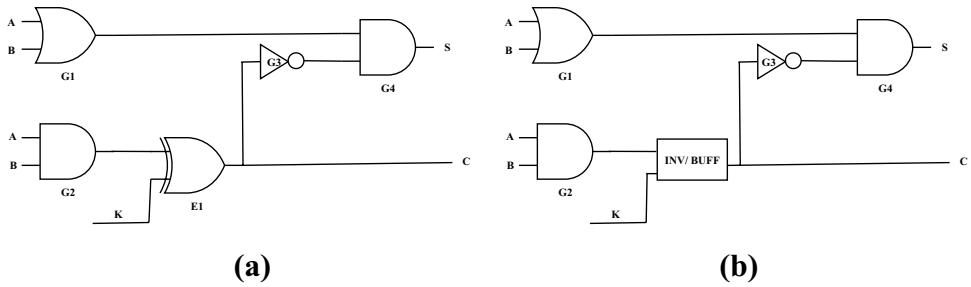


Fig. 4 Utilizing both (**a**) an XOR oriented key model (E1) and (**b**) a suggested INV/BUFF oriented model a functional key K = 0, a half-adder circuit may be locked

is too expensive, even for the major silicon manufacturers. Since the offshore foundry might not be reliable, it raises serious security issues for a variety of threats, including IP theft, overbuilding, hardware Trojans (HT), and reverse engineering. In the proposed design is in RTL level (Design level).

The proposed INV/BUFF key-gate design, gate level symbol, and Truth Table are depicted in Fig. 3. The suggested key-gate, like XOR/XNOR-based key-gates, having correct keys K = 0 and K = 1, can function as an inverter or buffer, respectively. With a valid key K = 0 or K = 1, the proposed key-gate can serve as an inverter or buffer, similar to XOR/XNOR based key-gates. The second level PMOS and NMOS of the schematic are turned ON/OFF by the input I, which is a value for an intermediate wire indicated in the diagram with a bullet point. This structure can also serve as

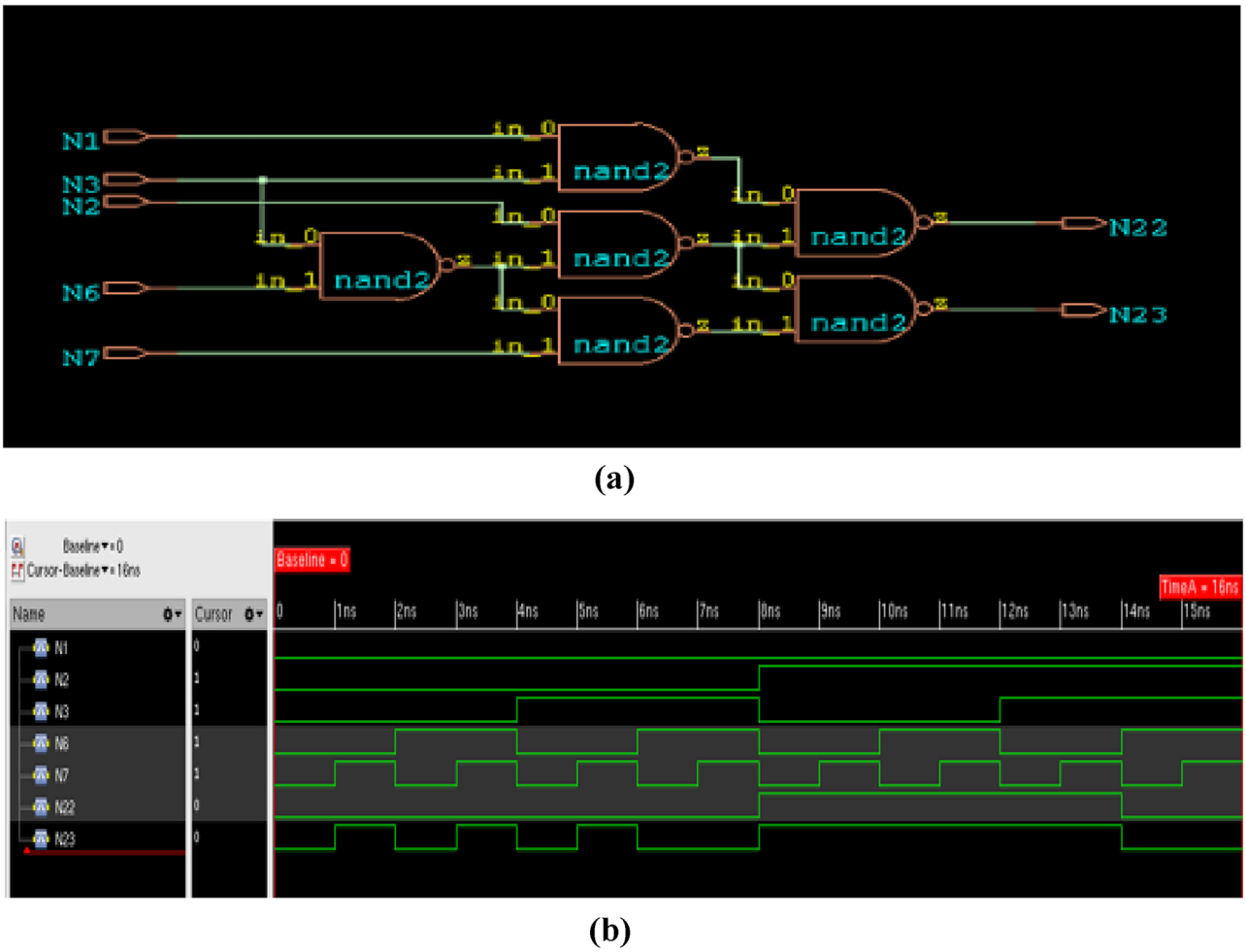


Fig. 5 **a** Schematic of C17 circuit. **b** Output waveform of C17 circuit

an inverter and buffer with the distinct valid keys K = 1 and K = 0, respectively (inverting the key-inputs). As a result, an attacker faces a difficulties when exploring the proper key on the netlist at the gate level.

An XOR/XNOR-oriented key model has the same locking as the key model proposed. As a result, INV/BUFF based key model may easily be used in most current locking methods for locking the functionality of the design while simultaneously producing the Anti-Sat Blocks in alternative of the XOR/XNOR model. Figure 4(a) and (b) demonstrate by combining the XOR and the suggested INV/BUFF key model, a half adder can be locked. Only when the genuine keys K = 0 and K = 1 are used do both locked circuits work properly.

Furthermore, the suggested key-gate may be used for locking the functionality of design either by adding an inverted gate (INV/BUFF) to an existing gate or by substituting an existing inverter within the design. Its reasonable key size, and suggested key gate may significantly minimize design overhead because it only needs ten transistors less overhead than XOR/XNOR design, because it needs 12 transistors. Moreover, because it has comparable functional behavior to the XOR/XNOR key model, the suggested key model may be employed in the creation of the feature ASB. Furthermore, the suggested key-gate has two distinct functions while utilizing a similar physical structure. As a result, image processing-based reverse engineering cannot provide direct knowledge of design functionality.

4 Results and Discussion

The proposed INV/BUFF-oriented locking blocks' security levels are tested. The level of security is determined by amount of SAT-attack repetitions. Moreover, power and

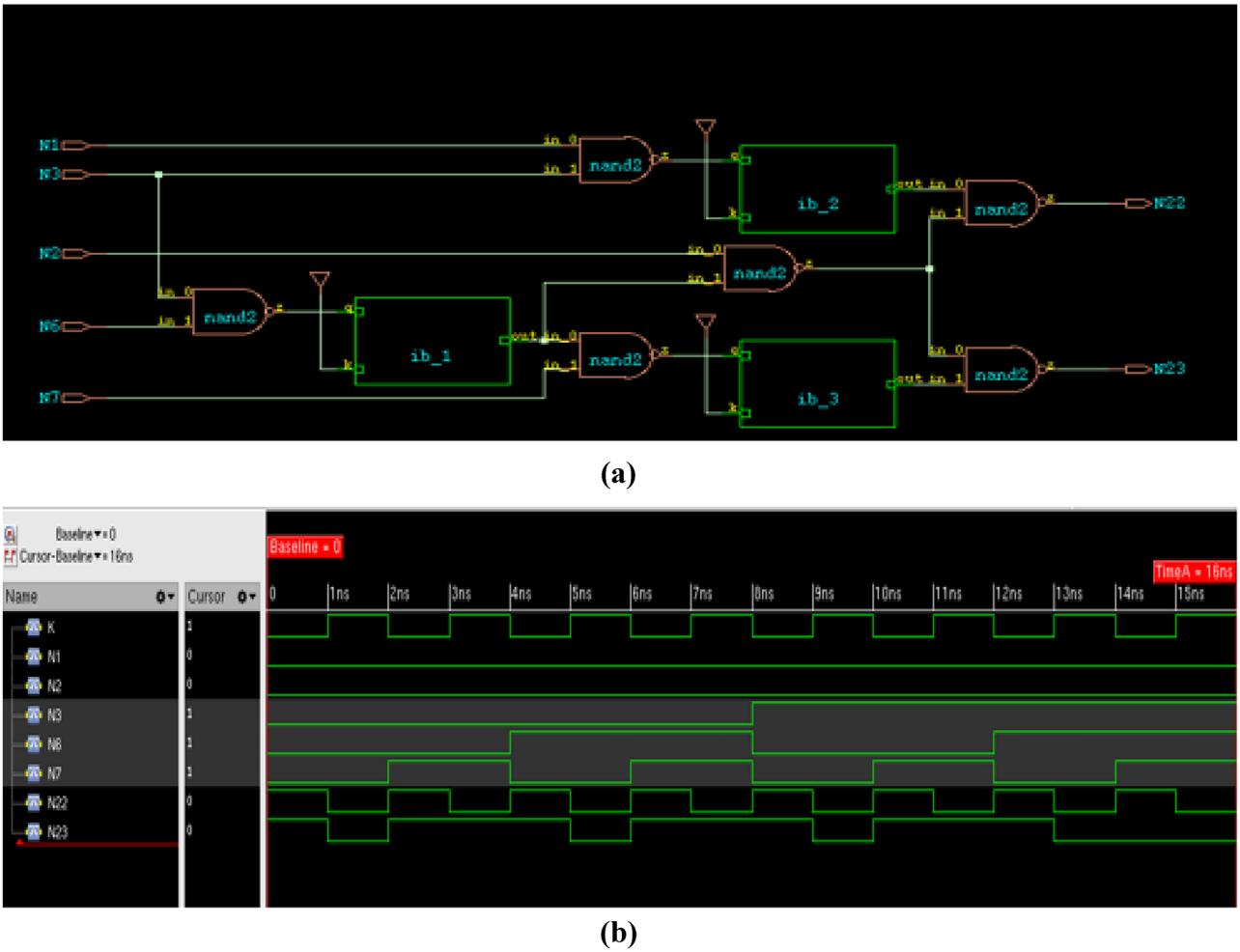
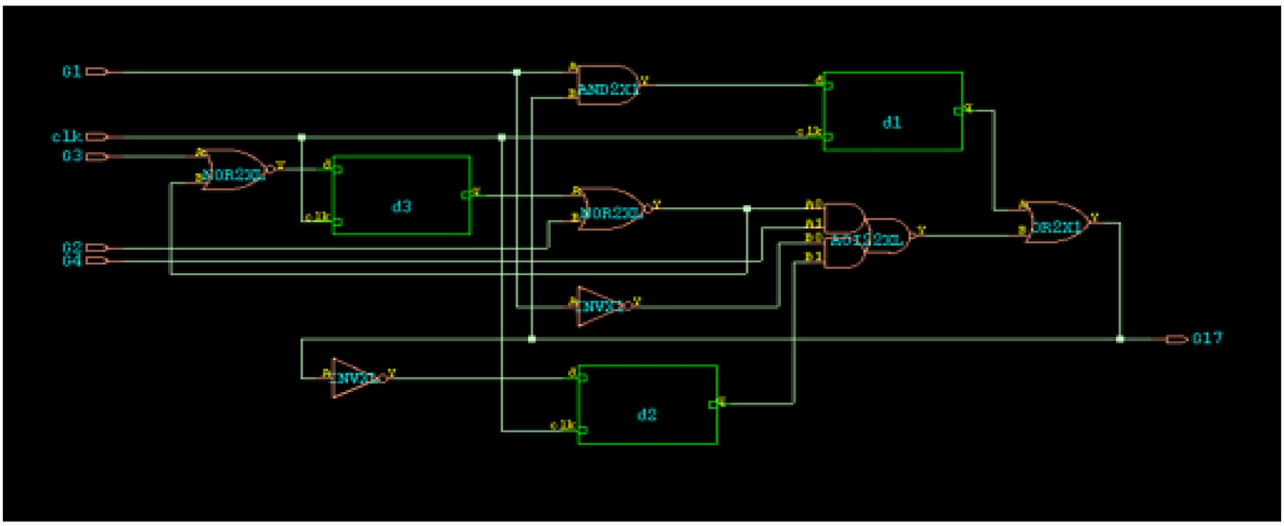
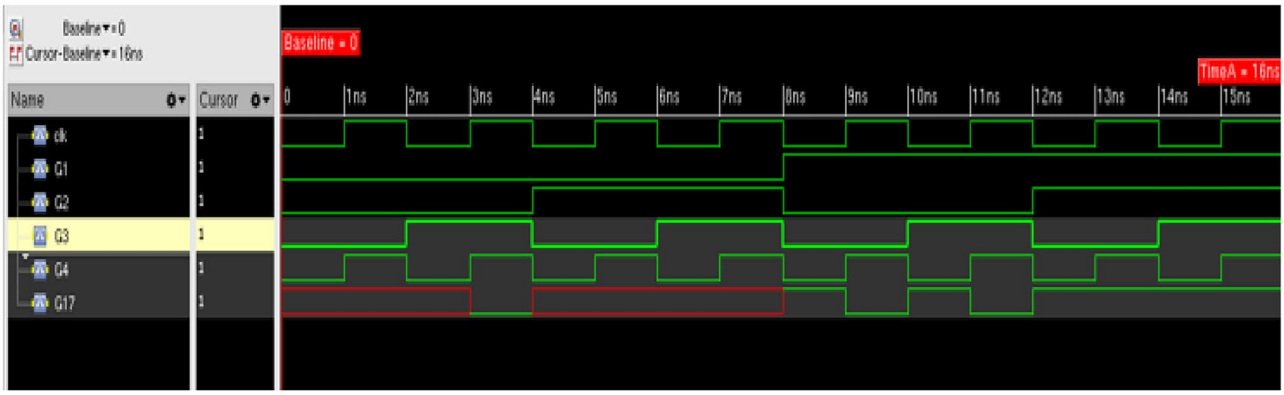


Fig. 6 **a** Schematic of C17 circuit with INV/BUFF. **b** Output waveform of C17 circuit with INV/BUFF



(a)



(b)

Fig. 7 **a** Schematic of s27 circuit. **b** Output waveform of S27 circuit

area are calculated. The following schematics and results are obtained by using Cadence IC6.1.8.

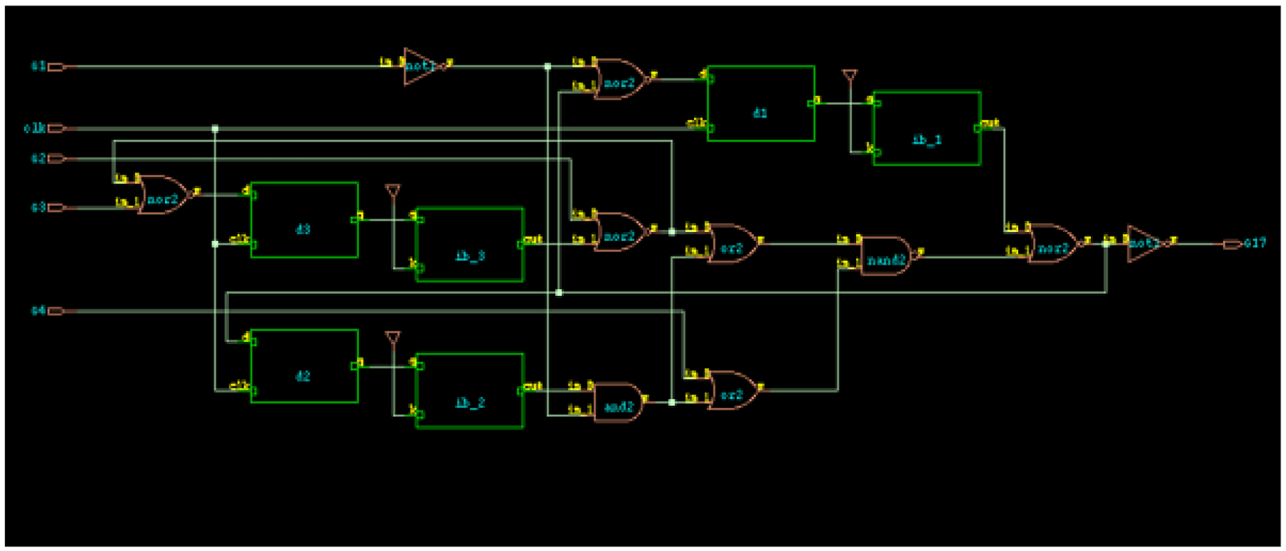
Analysis of C17 Benchmark Circuit Analysis of C17 benchmark circuit with various encryption methods integrated with Anti-Sat block along with obfuscation. C17 is a basic benchmark circuit has 5-inputs and 2-outputs. Figure 5a shows the schematic of C17 benchmark circuit. Figure 5b shows the output signal.

The design for the C17 benchmark circuit with INV/BUFF-based logic locking is shown in Fig. 6a, and the outputs for the correct and wrong keys are shown in Fig. 6b. The key size for the circuit is 3.

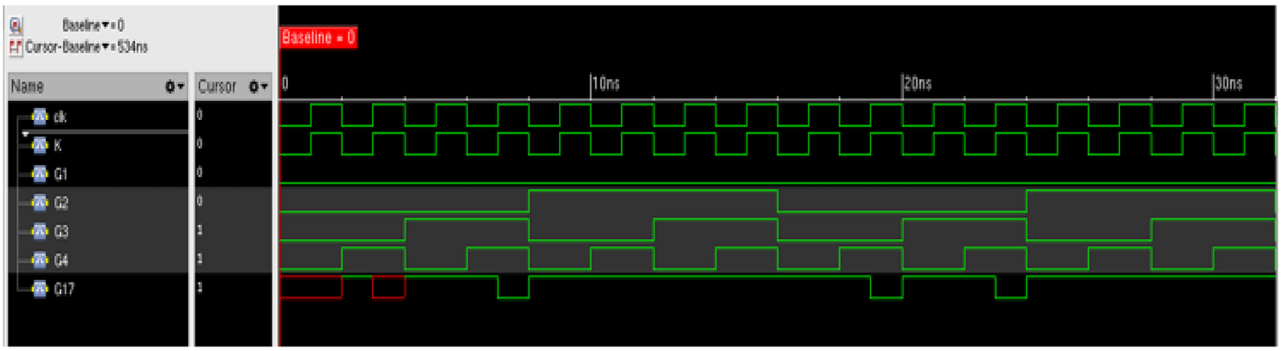
Figure 6a, key bits are mentioned (K) in INV/BUFF, Moreover N1 to N7 represents C17 circuit inputs. The wave form correct functionality represented at 15ns (When Key K=1, and the inputs of C17 circuits N1=0, N2=0, N3=1, N6=1, N7=1, the output N22=0 and N23=0 it means shows the correct C17 output). When K=0, with same input condition, the output of C17 is bad output signal, it is shown in Fig. 6b at 0 to 1 ns.

Analysis of S27 Benchmark Circuit Analysis of S27 benchmark circuit with various encryption methods integrated with Anti-Sat block along with obfuscation. S27 is a basic benchmark circuit with 5 inputs and 1 output. Figure 7a depicts the schematic of S27 benchmark circuit. Figure 7b shows the output waveform for S27 benchmark circuit.

Figure 8a show the schematic of S27 benchmark circuit with INV/BUFF based logic locking. Fig. 8b show the correct and wrong key outputs. The key size for the circuit is 3.



(a)



(b)

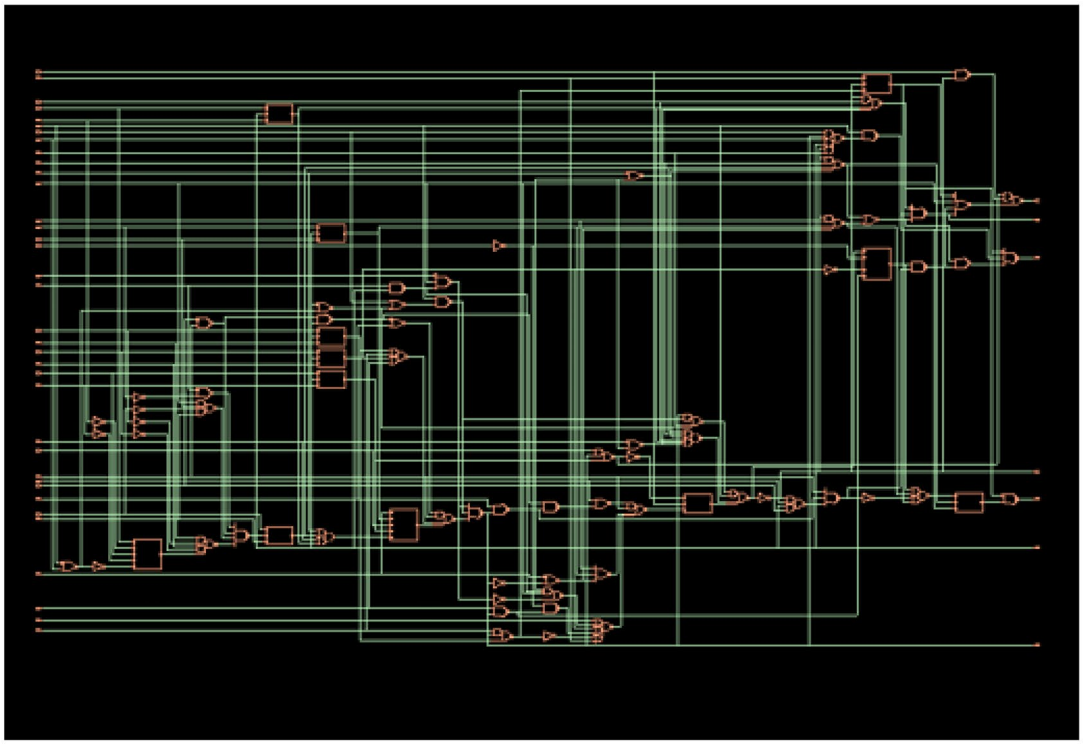
Fig. 8 **a** Schematic of S27 circuit with INV/BUFF. **b** Output waveform of S27 circuit with INV/BUFF

Analysis of C432 benchmark circuit with various encryption methods integrated with Anti-Sat block along with obfuscation. C432 is a basic benchmark circuit with 36 inputs and 7 outputs. Figure 9a shows the schematic of C432 benchmark circuit. Figure 9b shows the output waveform for C432 benchmark circuit.

Figure 10a show the schematic of C432 benchmark circuit with INV/BUFF based logic locking. Fig. 10b show the correct and wrong key outputs. The key size for the circuit is 10.

When the number of inverter key and input key is high, for example Fig. 10a (C432- 36 inputs with 10 inverter key) design the reverse engineering is very difficult. Since number of iteration will be more (time taken to reveal the correct key). In future author have a plan to work on structural and functional obfuscation of the cell along with this proposed work.

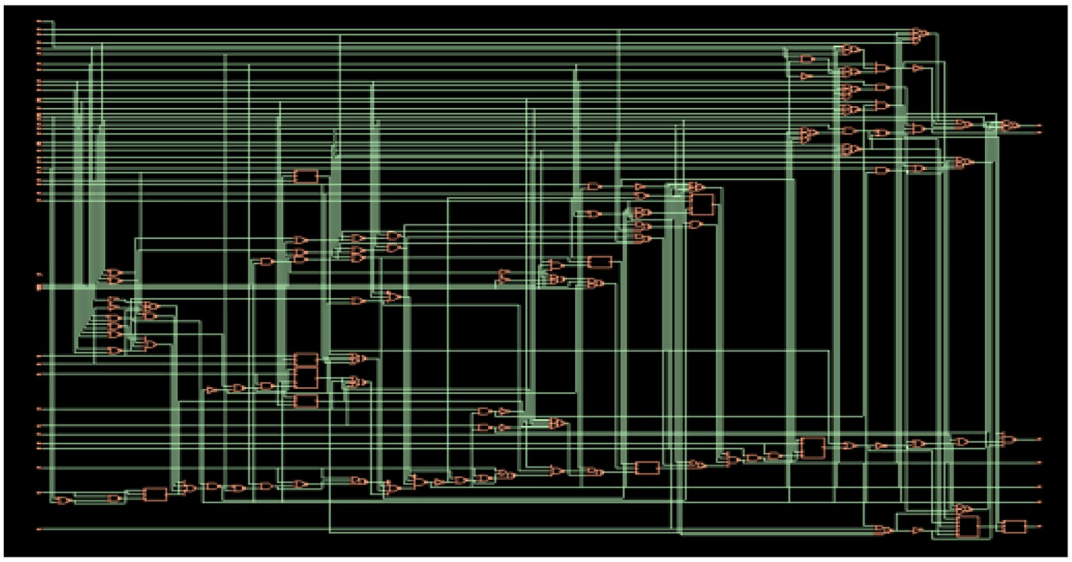
In Table 2 represents the analysis with various encryption methods with regard to area, power, and delay.



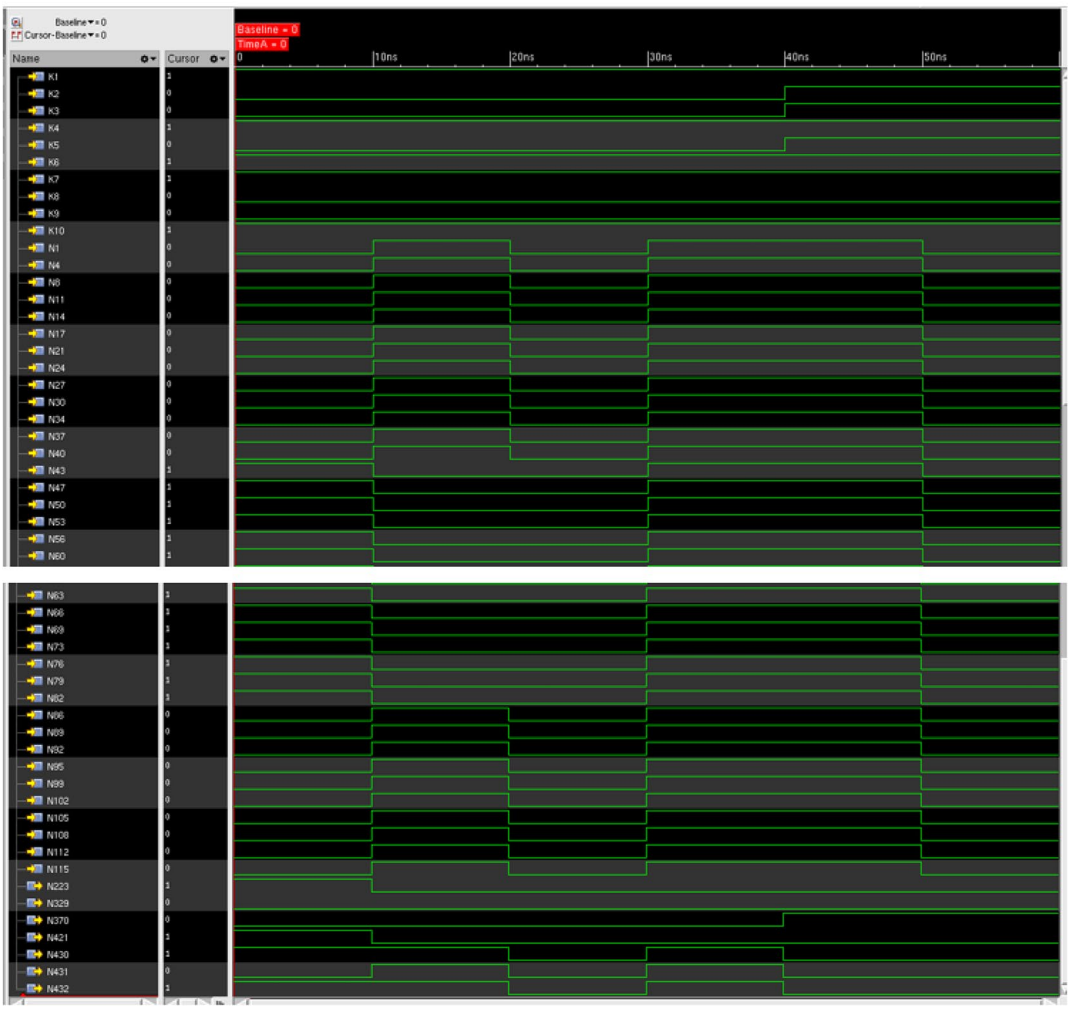
(a)

(b)

Fig. 9 **a** Schematic of C432 circuit. **b** Output waveform of C432 circuit



(a)



(b)

Fig. 10 **a** Schematic of C432 circuit with INV/BUFF. **b** Output waveform of C432 circuit with INV/BUFF

Table 2 Analysis of C17, S27 and C432 benchmark circuit

Parameters	Area (μm)	Power (nW)	Delay (ps)	Key size
Original circuit				
C17 [14]	16.652	425.567	210	
Logical Locking				
XOR	43.143	1534.732	563	3
Proposed INV/BUFF	40.873	1271.107	523	3
Original circuit				
S27	73.419	2312.269	361	
Logical Locking				
XOR	98.397	3696.829	452	3
Proposed INV/BUFF	96.126	2914.329	361	3
Original circuit				
C432	348.931	10998.072	3602	
Logical Locking				
XOR	524.532	19336.581	4861	10
Proposed INV/BUFF	520.747	19253.383	3971	10

5 Conclusion

The authors present a novel lightweight INV/BUFF-oriented locking strategy. A novel INV/BUFF key-gate design is suggested, which minimizes overhead while improving the design over XOR/XNOR gates. The analysis is done in C17, S27, and C432 benchmark circuits and it is observed that INV/BUFF key produces less amount of power, area, and delay in comparison to the XOR-based obfuscation method. The proposed approach, on average reduces 2.76 %, 12.92%, and 12.7% of area, power, and delay overhead over XOR-based technique respectively.

Author Contributions Statement The first author wrote the manuscript, and the second author supervised, third, fourth and fifth author- done the proof reading.

Data Availability Not Applicable.

Declarations

Research Involving Human and Animal Participants Not Applicable.

Competing Interests Nil.

References

1. Rostami M, Koushanfar F, Karri R (2014) A Primer on Hardware Security: Models, Methods, and Metrics. Proceedings of the IEEE 102:1283–1295. https://doi.org/10.1109/JPROC.2014.2335155
2. Ashika SV, Sivamangai NM, Naveenkumar R, Napolean A (2023) Importance of logic locking attacks in hardware security. In: Proc. Int Conf Intel Data Comm Technol Internet Things (IDCIoT), pp 156–160. https://doi.org/10.1109/IDCIoT56793.2023.10052782
3. Roy JA, Koushanfar F, Markov IL (2008) EPIC: Ending piracy of integrated circuits. In: Proc. Design, Automation Test Europe, pp 1069–1074. https://doi.org/10.1145/1403375.1403631
4. Subramanyan P, Ray S, Malik S (2015) Evaluating the security of logic encryption algorithms. In: Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp 137–143. https://doi.org/10.1109/HST.2015.7140252
5. Khaleghi S, Zhao KD, Rao W (2015) IC piracy prevention via design withholding and entanglement. In: Proc. 20th Asia and South Pacific Design Automation Conf., pp 821–826. https://doi.org/10.1109/ASPDAC.2015.7059112
6. Naveenkumar R, Sivamangai NM, Napolean A, Janani V (2021) A survey on recent detection methods of the hardware trojans. In: Proc. 3rd International Conference on Signal Processing and Communication (ICPSC), pp 139–143. https://doi.org/10.1109/ICSPC51351.2021.9451682
7. Patooghy A, Aerabi E, Rezaei H, Mark M, Fazeli M, Kinsy MA (2018) Mystic: Mystifying IP cores using analways-ON FSM obfuscation method. In: Proc. IEEE Comp Soc Ann Symp VLSI (ISVLSI), pp 626–631. https://doi.org/10.1109/ISVLSI.2018.00119
8. Liu B, Wang B, (2014) Embedded reconfigurable logic for ASIC design obfuscation against supply chain attacks. In: Proc. Design. Automation Test Europe Conf Exhibition (DATE), pp 1–6. https://doi.org/10.7873/DATE2014.256
9. International Chamber of Commerce, Impacts of counterfeiting and piracy to reach us $1.7 Trillion by 2015. [Online]. Available: http://www.iccwbo.org/News/Articles/2011/Impacts-ofcounterfeiting-and-piracy-to-reach-US$1-7-trillion-by-2015
10. Roy JA, Koushanfar F, Markov IL (2010) Ending Piracy of Integrated Circuits. Computer 43:30–38. https://doi.org/10.1109/MC.2010.284
11. Rajendran J, Zhang H, Zhang C, Rose GS, Pino Y, Sinanoglu O, Karri R (2015) Fault Analysis-Based Logic Encryption. IEEE Transactions on Computers 64:410–424. https://doi.org/10.1109/TC.2013.193
12. Rajendran J, Pino Y, Sinanoglu O, Karri R (2012) Security analysis of logic obfuscation. In: Proc. Design Automation Conf., pp 83–89. https://doi.org/10.1145/2228360.2228377
13. Naveenkumar R, Sivamangai NM, Napolean A, Nissi GA (2022) Hardware obfuscation for IP protection of DSP applications. J Electron Test 38(1):9–20. https://doi.org/10.1007/s10836-022-05984-2
14. Naveenkumar R, Sivamangai NM, Napolean A, Puviarasu A, Saranya G (2022) Preventive Measure of SAT Attack by Integrating Anti-SAT on Locked Circuit for Improving Hardware Security. In: Proc. 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp 756–760. https://doi.org/10.1109/ICCES54183.2022.9835923
15. Shamsi K, Li M, Pan DZ, Jin Y (2019) KC2: Key-Condition Crunching for Fast Sequential Circuit Deobfuscation. In: Proc. Design, Automation Test Europe Conf Exhibition (DATE), pp 534–539. https://doi.org/10.23919/DATE.2019.8715053
16. Shamsi K, Li M, Meade T, Zhao Z, Pan DZ, Jin Y (2017) AppSAT: Approximately deobfuscating integrated circuits. In: Proc. IEEE Int Symp Hardware Oriented Security Trust (HOST), pp 95–100. https://doi.org/10.1109/HST.2017.7951805
17. Massad ME, Garg S, Tripunitara MV (2015) Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes. NDSS. https://doi.org/10.14722/NDSS.2015.23218
18. Yasin M, Mazumdar B, Sinanoglu O, Rajendran JJ (2017) Security analysis of Anti-SAT. In: Proc. 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), pp 342–347. https://doi.org/10.1109/ASPDAC.2017.7858346
19. Jemimah Rinsy J, Sivamangai NM, Naveenkumar R, Napolean A, Puviarasu A, Janani V (2022) Review on logic locking attacks

in hardware security. In: Proc. 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, pp 342–347. https://doi.org/10.1109/ICDCS54290.2022.9780725
20. Xu X, Shakya B, Tehranipoor MM, Forte D (2017) Novel Bypass Attack and BDD-based Tradeoff Analysis against All Known Logic Locking Attacks. IACR Cryptol ePrint Arch 2017:621. https://doi.org/10.1007/978-3-319-66787-4_10
21. Yasin M, Rajendran JJ, Sinanoglu O, Karri R (2016) On Improving the Security of Logic Locking. IEEE Trans Computer-Aided Design Integrated Circuits Syst 35:1411–1424. https://doi.org/10.1109/TCAD.2015.2511144
22. Lao Y, Parhi KK (2015) Obfuscating DSP Circuits via High-Level Transformations. IEEE Trans Very Large Scale Integr (VLSI) Syst 23:819-830. https://doi.org/10.1109/TVLSI.2014.2323976
23. Xie Y, Srivastava A (2019) Anti-SAT: Mitigating SAT Attack on Logic Locking. IEEE Trans Computer-Aided Design Integ Circuits Syst 38:199–207. https://doi.org/10.1109/TCAD.2018.2801220
24. Xie Y, Srivastava A (2016) Mitigating SAT Attack on Logic Locking. IACR Cryptol ePrint Arch 2016:590. https://doi.org/10.1007/978-3-662-53140-2_7
25. Shamsi K, Li M, Meade T, Zhao Z, Pan DZ, Jin Y (2017) AppSAT: Approximately deobfuscating integrated circuits. In: Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp 95–100. https://doi.org/10.1109/HST.2017.7951805
26. Liu Y, Zuzak M, Xie Y, Chakraborty A, Srivastava A (2020) Strong anti-SAT: Secure and effective logic locking. In: Proc. 21st International Symposium on Quality Electronic Design (ISQED), pp 199–205. https://doi.org/10.1109/ISQED48828.2020.9136983

R. Naveenkumar is a research scholar at the department of electronics and communication engineering at the Karunya Institute of Technology and Sciences, Tamilnadu, India. He got his M.E. degree from Sri Shakthi Institute of Science and Technology, India, in 2014. He has 7 years of teaching experience, 3 years of research experience, and 1 year of industry experience. He has a number of international high impact journal publications and conference proceedings papers to his credit. He has presented several research papers in international and national conferences. His research interests are in hardware security of microelectronics. He is a member of MISTE, MIEANG, MIRED, and MSDIWC.

N. M. Sivamangai is an Associate Professor, Department of ECE, Karunya Institute of Technology and Sciences, India. She received her Ph.D. degree from Anna University, Chennai, India in 2011. She has 13 years of teaching experience. She was instrumental in the fabrication of IC jointly with Indian Institute of Science - Bangalore, in the year 2008. Her research interests are to design and test high performance semiconductor memories and to design VLSI based systems.

A. Napolean is working as a researcher in Electronics and Communication Engineering at Karunya University Coimbatore. He worked in VSB Engineering College from 2008 to 2017. He obtained M.Tech. degree in Sensor System Technology from Vellore Institute of Technology University in the year of 2002. He completed his M.Sc. physics degree from Bharathiar University in 2006. He completed his Bachelor of Science in Physics in 2004 from Manonmaniam Sundaranar University- Tirunelveli. His research experience is in the fields of nano materials, electronic devices, and nano-scale memory devices. He has a number of international high impact journal publications and conference proceedings papers to his credit. He has teaching experiences in various departments like Electronics and Instrumentation, apart from Physics. He is a member of MISTE, MIEANG, MIRED, and MSDIWC.

S. Sridevi Sathya Priya is an Assistant Professor, Department of ECE, Karunya Institute of Technology and Sciences, India received her Bachelor of Technology degree in Electronics and Communication Engineering form Madras University, Madras, India in 2001. She got her M.E degree from Karunya Institute of Technology and Sciences, India in 2006. She received her Ph.D degree from Karunya Institute of Technology and Sciences, Coimbatore, India in 2017. Her research interests include Hardware security, Cryptographic systems, Internet of things, Artificial Intelligence, and parallel processing architecture.

S. V. Ashika is a post graduate scholar, Department of ECE, Karunya Institute of Technology and Sciences, India. Her research interest is analog and digital circuit design.