Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Reverse Engineering Protection for the Hardware design using Input/output Locking System

Dinesh cholkar[1] , Jitendra Ahir[2] and Laxmi Singh[3]

[1]PhD. Scholar, Department of Electronics & Communication Engineering, Rabindranath Tagore University (RNTU), Bhopal

[2,3] Professor, Department of Electronics & Communication Engineering, Rabindranath Tagore University (RNTU) , Bhopal

Article History:

Received: 14-01-2025

Revised: 15-03-2025

Accepted: 21-03-2025

Abstract:

Technology has increased dramatically in the effectiveness of the attacks. There are different measures, at the logic lock (LL) level and at the chip level etc. The emergence of satisfaction (SAT)-based functional queries, and 3-D at the board level at the board level forced attacks at the board level. The Encryption/Decryption Module can improve overall security of the strategy. To determine the accurate key for a particular blocked circuit attacker will try. If the target is to attack attempts to output a circuit that calculates function. One way the two goals relate to is that a critical recovery of a particular blocking circuit means recovery of the circuit. However, the opposite may not be true. The researchers propose locking mechanisms in response to attacks on previous mechanisms, with another investigator having immediate impact. This input design applies to opened ICs and buttons that are avoided from off base yield. The calculation proceeds to discover exceptional input designs and kills untrue keys until the fitting key is found. The vital values for these entryways are "0" or 1. An inverter can be included to the same flag line as turning the key esteem. The thought of this approach is to anticipate the other party from speculating key values based on the entryway sort, as they don't know in case the over is portion of the first circuit or on the off chance that it has been included within the handle of rationale locking.

Keywords: Logic locking ,PCB, Security.

1. Introduction

The considerable threat of attackers pronounces hardware design pronunciation at all stages of the manufacturing lifecycle. In the case of a re attack, malicious actors have access to internal design details such as their own design .For combating RE threats. LL technique uses structural and functional design transformations to prevent attackers from preventing information. LL can be used[1].

Threat scenarios taking into account previous work include (i) blocked veiled circuits and (ii) unreliable foundry receiving black box original circuits. "Blackbox access can be saved and determined at the same time. This scenario is not (II) because it is possible to purchase a functional IC and attack another copy of the IC. If the target is to attack key recovery.

To determine the correct key for a particular blocked circuit attacker will try. If the target is to attack attempts to output a circuit that calculates function. One way the two goals relate to is that a critical recovery of a particular blocking circuit means recovery of the circuit. However, the opposite may not be true. The

researchers propose locking mechanisms in response to attacks on previous mechanisms, with another investigator having immediate impact[2].

To realize locking technology, Iolock is based on the JTAG architecture (co-test action group). It consists of blocking modules that encrypt/decrypt information. The lock module communicates with the Key Management Unit (SME) to maintain company keys. The SME contains an LFSR module (linear feedback shift register) that creates key locks and unlocks. Using small businesses, instead of using fixed static keys, designers can include dynamic key mechanisms in which encryption/decryption keys change over time. This increases the security provided by the Iolock framework.

Periodic dummy-The addition of logical elements resulted in periodic covering increasing complexity [3]. The Striped Function LL (SFLL) passes through satellite attacks by stripping the function from the original circuit and causing an to defeat satellite attacks using cascade keyblocks and/or gates, increasing complexity and damaging the consequences of resisting .It is important to recognize the opportunity to safely transfer keys into programming, while also keeping confidentiality from third parties for the safety of the system. Improving the middle security of potential manufacturers. The unique FSKP key available to enhances the secure boating process. This approach includes security programming, critical approval[5].

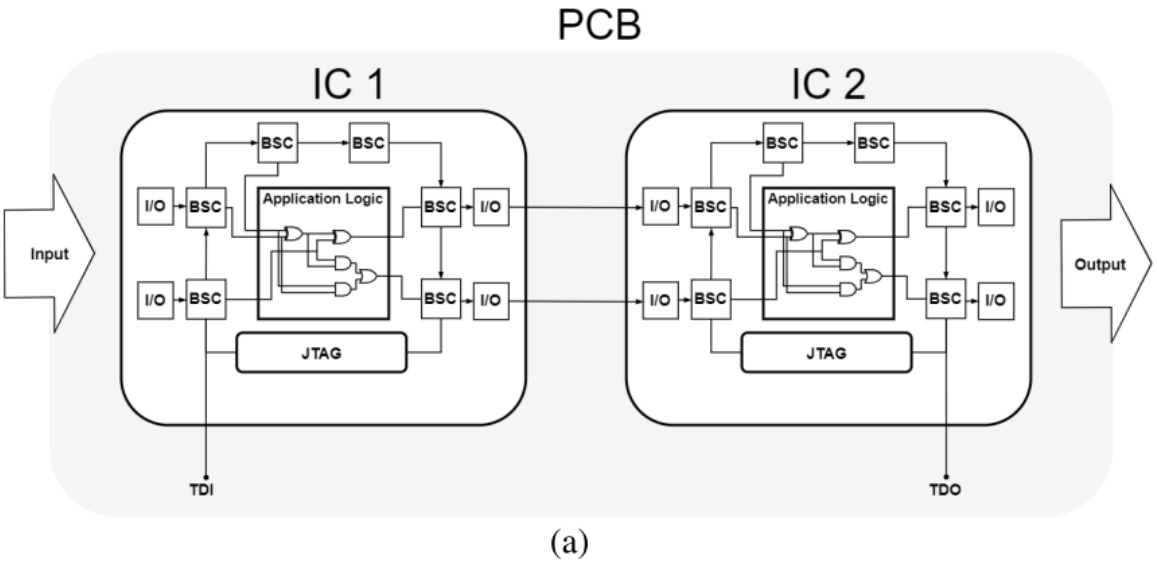
SAT attacks are also improved by improving defense against attacks and countering them. This leads to a tractor between the attacker and the defender.

This task uses stream ciphers to encrypt the connections of commercial devices (COTs) that protect data transferred from attackers based on malicious activity. However, the method only aims to attack at the PCB level. This is because they aim to sleep for the kids, leaving a gap in attacks at IC level. Additionally, using LFSRs will cause the system to take risks. Furthermore, connections such as buses can match interior communication monitoring and data manipulation. Bus snooping attacks involve observing communication between the components of the system[6].

The operation and function of the circuit are essential. This is because you can ensure that the replicated circuit works correctly. It is important to protect the circuit. This is important because it rejects the ability to check the ability of the replicated device to repeat it. Although it was a disruptive and expensive process in the past, advances in imaging technology have made it possible to design 3D imagery and process automation of devices[7,8].

2. Methodology

In the methodology, analyze I/OLock for the security purpose at the hardware. I/OLock realizes “security” by “encrypting the outputs” and “decrypting the inputs” across the “I/O boundaries” of an IC at an abstract level.



.

Fig.1 . " ICs on a PCB" interacting design.

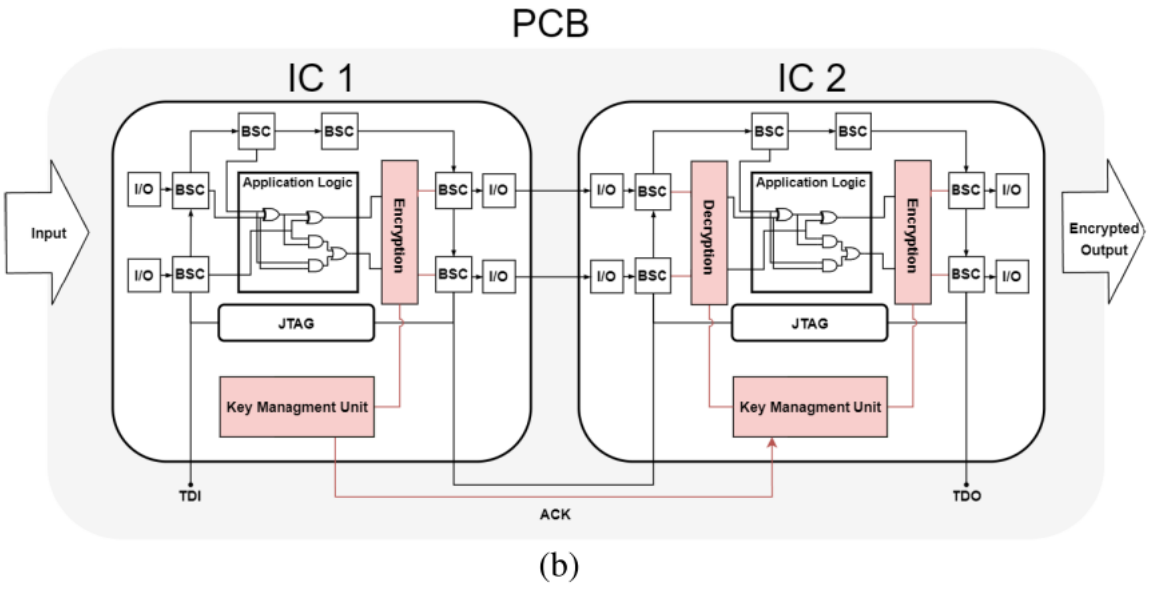


Fig. 2. "I/OLock" countermeasure design.

3. Simulations and Results

After implementing the implementation and assessing the safety and functionality of the proposed I/O lock system. Determines the efficiency of the system in combating such attacks. To see its functionality and to get a detailed understanding of the company, we ran hardware and simulation estimates on the system. I used an LL test bench for my review. These testbenches run LLs with simple XOR gates corresponding to random keys. We then applied our system and evaluated it on these testbenches to determine resistance to attacks.

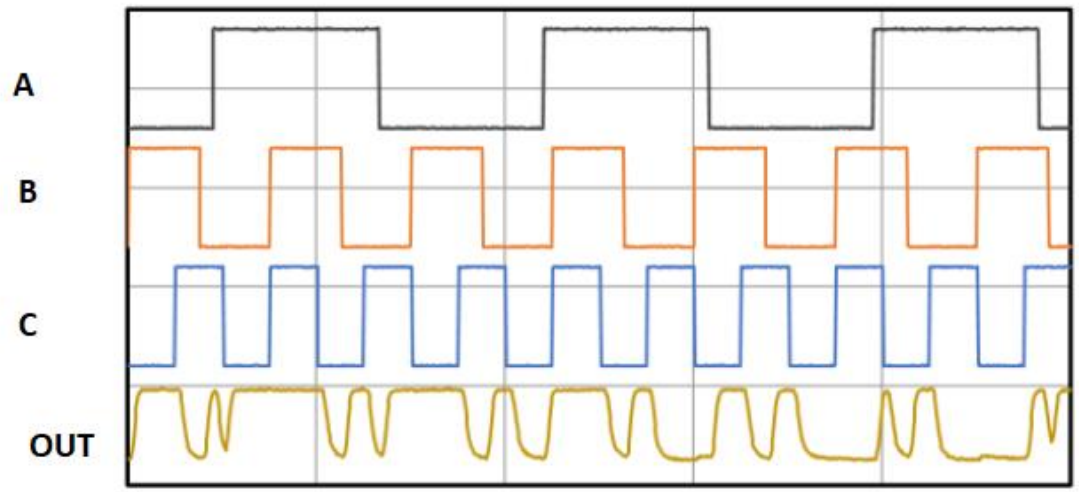


Figure 3:Test bench waveform with locking scheme.

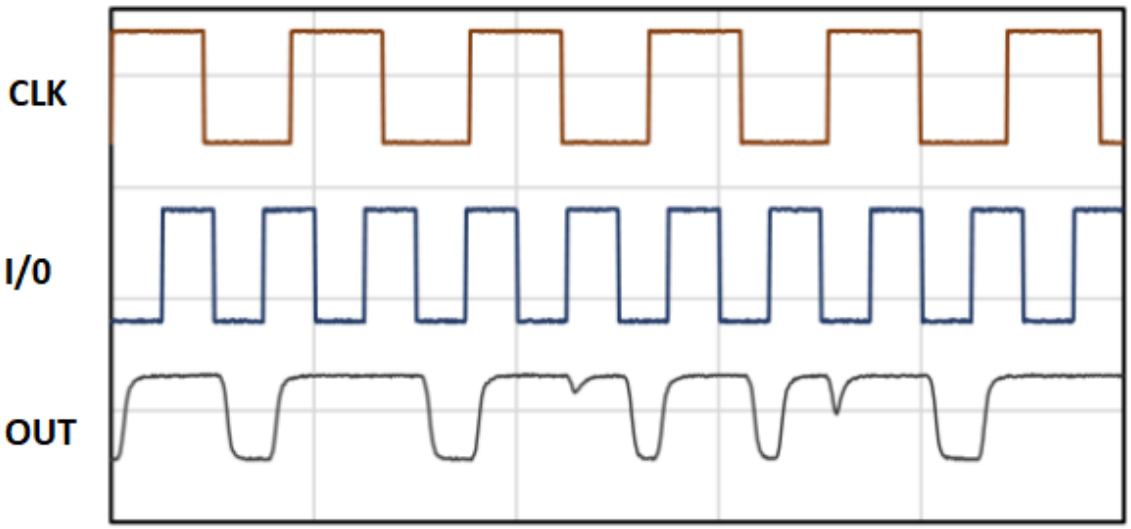


Figure 4:Test bench waveform to resistance the attacks.

The system was run and tested endlessly to define whether the system would remain to connect over a long period of time while using it. The figure shows the waveforms of the simulated experiment. The output matches the original circuit structure if the decoded, it can be concluded that the system works correctly. In this experiment, the system was allowed for 24 hours and counted the number of errors that happened. Since no errors have been found, the system can ride the key on the bike, and conclude that the E/A of the circuit can be decrypted/encrypted without disrupting the functional logic.

Additionally, signals were used to examine possible attacks on the system. You can manipulate signals to disrupt functionality, cause system errors, and indulge in confidential information. To analyze this, we took three different attacks into consideration.

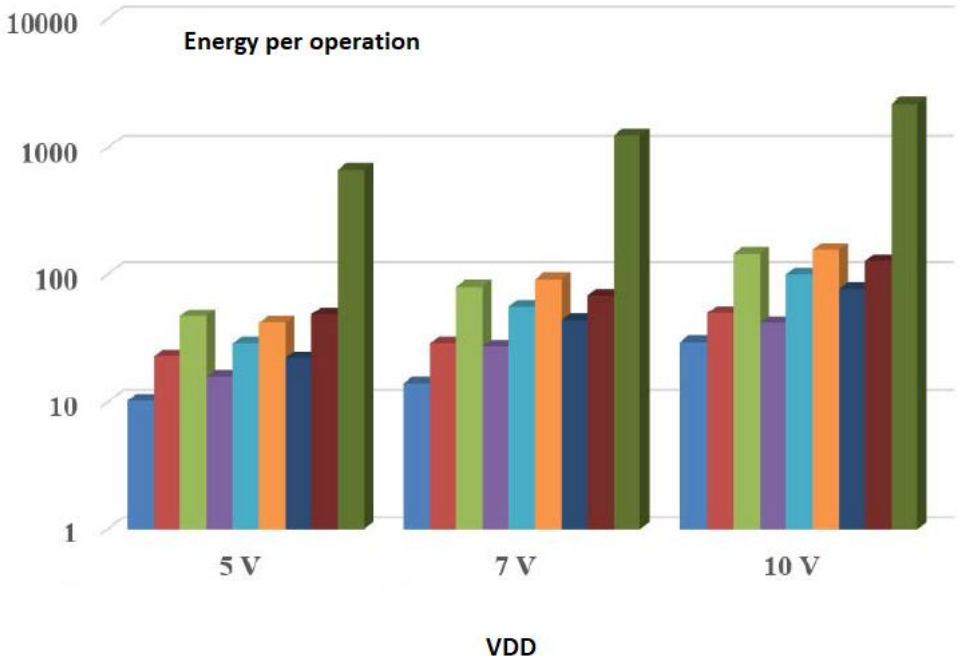


Figure 5: Energy per operation of proposed circuits from measurement results versus supply voltage

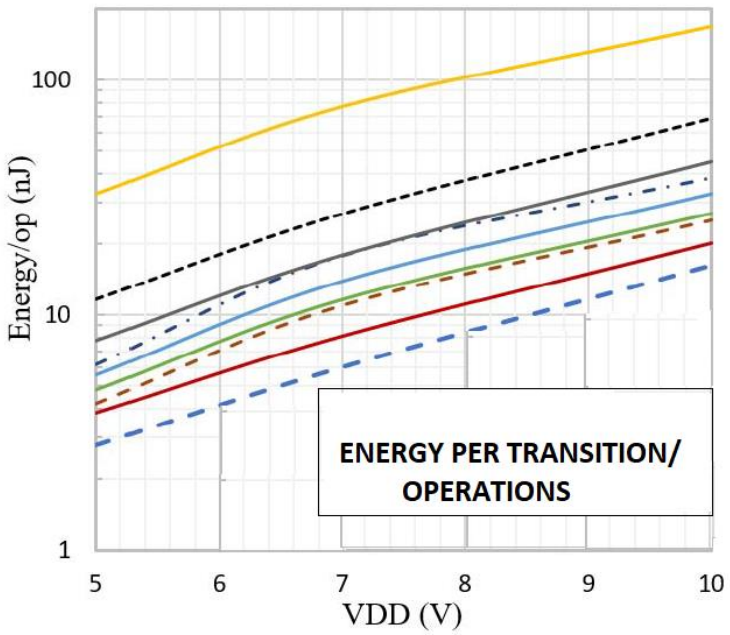


Figure 6: Energy comparison chart

4. Conclusion

At the PCB levels, I/O Lock has been installed and that prevents “RE attacks” by blocking I/O signals. To protect hardware from reattacks shown that I/O lock can be used as an independent or mutual with the fundamental LL technology. We evaluated the overhead costs of I/O lock and showed that area, delay and power are only minimal. We analyzed I/O lock's security through both hardware experiments and software simulation. Give the mathematically quantified its security assurance. Our results show that I/O lock presents a scalable, robust and low monitoring solution that can prevent reattacks at both the chip and PCB level. Additionally, we've covered how I/O Lock can protect against other hardware attacks. In the unreliable microelectronics supply chain, investigating the effectiveness of I/O lock against other threats, developing corresponding automation tools and, reducing overhead.

References

[1] T. Hoque, P. Slpsk, and S. Bhunia, “Trust issues in COTS: The challenges and emerging solution,” in Proc. Great Lakes Symp. VLSI, Sep. 2020, pp. 211–216.

[2] T. Hoque, J. Cruz, P. Chakraborty, and S. Bhunia, “Hardware IP trust validation: Learn (the untrustworthy), and verify,” in Proc. IEEE Int. Test Conf. (ITC), Oct. 2018, pp. 1–10.

[3] T. Hoque, P. Slpsk, and S. Bhunia, “Trust issues in microelectronics: The concerns and the countermeasures,” IEEE Consum. Electron. Mag., vol. 9, no. 6, pp. 72–83, Nov. 2020.

[4] M. Banga and M. S. Hsiao, “Hardware IP trust,” in The Hardware Trojan War. Berlin, Germany: Springer, 2018, pp. 75–100.

[5] K. Shamsi, M. Li, K. Plaks, S. Fazzari, D. Z. Pan, and Y. Jin, “IP protection and supply chain security through logic obfuscation: A systematic overview,” ACM Trans. Design Autom. Electron. Syst., vol. 24, no. 6, pp. 1–36, Nov. 2019.

[6] S. Dupuis and M.-L. Flottes, “Logic locking: A survey of proposed methods and evaluation metrics,” J. Electron. Test., vol. 35, no. 3, pp. 273–291, Jun. 2019.

[7] M. Yasin and O. Sinanoglu, “Evolution of logic locking,” in Proc. IFIP/IEEE Int. Conf. Very Large Scale Integr. (VLSI-SoC), Oct. 2017, pp. 1–6.

[8] P. Subramanyan, S. Ray, and S. Malik, “Evaluating the security of logic encryption algorithms,” in Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST), May 2015, pp. 137–143.

[9] K. Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan, and Y. Jin, “AppSAT: Approximately deobfuscating integrated circuits,” in Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST), May 2017, pp. 95–100.

[10] J. Rajendran, Y. Pino, and R. Karri, “Security analysis of logic obfuscation,” in Proc. 49th Annu. Design Automat. Conf., 2012, pp. 83–89, doi: 10.1145/2228360.2228377.Authorized licensed use limited to: Rabindranath Tagore University - Bhopal. Downloaded on May 02,2024 at 06:07:22 UTC from IEEE Xplore.