# Logical Locking System for Improved Hardware Security

N.Divya(M.E-II VLSI-Design)
*ECE Department, Syed Ammal Engineering College, Ramanathapuram*
Dr .S. M.H. Sithi Shameem Fathima, M.E. Ph.D..,
*Professor , Syed Ammal Engineering College, Ramanathapuram*

*ABSTRACT: Reuse-based system-on-chip (SoC) design using hardware intellectual-property (IP) cores has become a pervasive practice in the industry. However, these techniques incur high overheads, and integrated circuit (IC) camouflaging cannot provide any protection for the gate-level netlist of the third party intellectual property (IP) core or the single large monolithic IC. In order to circumvent these weaknesses, this brief elaborately analyzes these hardware security techniques and proposes a novel practical logic obfuscation method by random generators to prevent an adversary from RE both the gate-level netlist and the layout-level geometry of IP/IC and protect IP/IC from piracy and overbuilding. Xilinx 12.1 tool has been used to verify existing and proposed results .*

**Keyword:** *System on chip(soc), Intellectual Property(IP)*

## I INTRODUCTION

Recent trends in micro electronics technology have gradually changed the strategies used in VLSI circuits. Establishing an efficient methodology is one of the key to design VLSI chip successfully. The design of microelectronics system is strongly influenced by the fact that transistor and featured size, density and frequency have increased.

Due to the ever increasing complexity of constructing and/or maintaining a foundry with advanced fabrication capabilities, many semiconductor companies are becoming fabless. Such fabless companies design integrated circuits (IC) and send them to an advanced foundry, which is usually off-shore, for manufacturing. Also, the criticality of time-to-market has forced companies to buy several IC intellectual property (IP) blocks to use them in their systems-on-chip. The buyers and sellers of these IP blocks are distributed worldwide.

- A chip design house buys an IP core from an IP vendor and makes an illegal copy or "clone" of the IP. The IC design house then sells it to another chip design house (after minor modifications) claiming the IP to be its own.
- An untrusted fabrication house makes an illegal copy of the GDS-II database supplied by a chip design house and then illegally sells them as hard IP.
- An untrusted foundry manufactures and sells counterfeit copies of the IC under a different brand name .
- An adversary performs postsilicon reverse engineering on an IC to manufacture its illegal clone.

## II RELATED WORKS

The proposed obfuscation cell (OC) is composed of an inverter and a multiplexer. The structure is shown in Fig., where the key is a select input of the multiplexer (because of the key's importance, a distribution framework must be established so that the IP designer can securely unlock each IC).

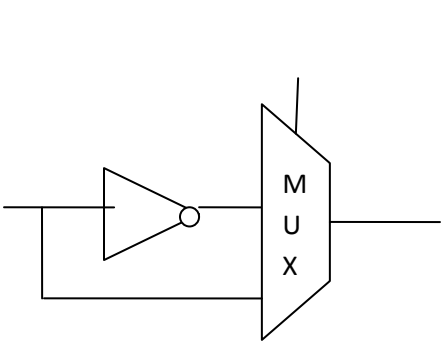


Fig.1 Structure of an OC

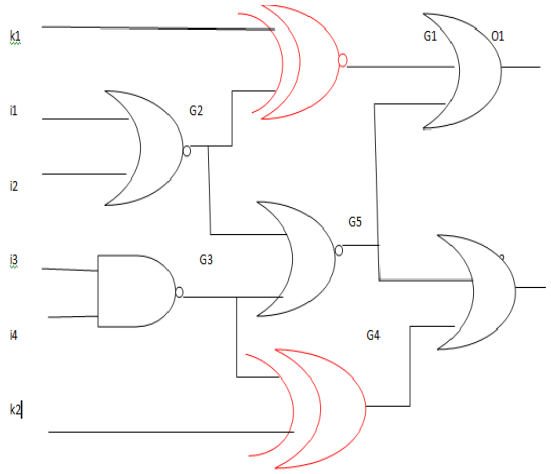


Fig.2 Circuit obfuscated with the combinational logic obfuscation method

gate-level netlist by RE, the secret key bits of inserted gates would be leaked: if the inserted gate is XOR, key bit would be 0; if is XNOR, the key bit would be 1.

In order to avoid this problem, we must replace some XOR gates with XNOR gates and inverters and, similarly, replace some XNOR gates with XOR gates and inverters, however, which incurs very high area and power overheads due to the redesign of the logic. The obfuscation structure proposed in this brief does not need to redesign the logic and the low overhead of the structure is demonstrated on standard benchmark circuit.

## III PROPOSED METHOD

The goal of hiding countermeasures is to make the physical characteristics of integrated circuits independent of intermediate values and operations performed during cryptographic applications. Among hiding countermeasures, essentially distinguish strategies one based on the randomisation of the execution of cryptographic algorithms one or more Pseudo Random Number Generators (PRNGs) are also included to generate the masks, which should be updated at each step of the datapath for a more efficient masking scheme. Prng used to generate key values to overcome the limitations of manual insertion values

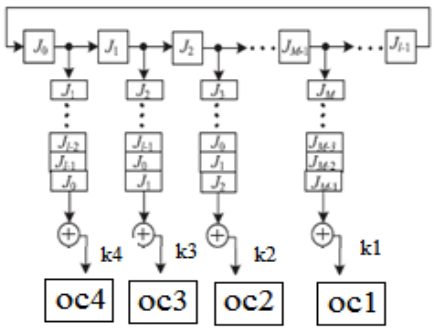


Fig.3. OC with pattern generation

Test pattern generation is the process of defining an effective test set which will drive the circuit under test so that the faults in the circuit will cause a different response at the primary outputs from the non-faulty outputs. The algorithms used in test pattern generation are usually directed to non-functional testing, which concentrate on propagating any available faults on the circuit nodes to primary outputs. This type of testing is termed fault oriented testing. Test pattern generation is strongly related to fault modeling. The proposed has been simulated and the synthesis report can be obtained by using Xilinx ISE 12.1i. The various parameters used for computing existing and proposed systems with Spartan-3 processor are given.

Jiliang Zhang studies of hardware security aim to thwart piracy, overbuilding, and reverse engineering (RE) by obfuscating and/or camouflaging. However, these techniques incur high overheads, and integrated circuit (IC) camouflaging cannot provide any protection for the gate-level netlist of the third party intellectual property (IP) core or the single large monolithic IC. In order to circumvent these weaknesses, this brief elaborately analyzes these hardware security techniques and proposes a practical logic obfuscation method with low overheads to prevent an adversary from RE both the gate-level netlist and the layout-level geometry of IP/IC and protect IP/IC from piracy and overbuilding. Traditionally, the IC design is written without any concern of obfuscation, and hence IC design is vulnerable to RE, piracy, and overbuilding. Given a gate-level netlist of the design, goal is to modify the original netlist to produce an obfuscated netlist, which is functionally equivalent to the former when correct key is given. An obfuscated gate-level netlist is synthesized into the layout geometry for manufacturing. An adversary buys the obfuscated IC

on the open market and then obtains the gate-level netlist by image processing-based RE. However, the functionality of obfuscated cells cannot be identified. The modified netlist reacts with a silicon physical unclonable function (PUF), and it can exactly perform the same as that of the design as long as the correct license is issued by the IP/IC designer. This means that only the chips authorized by the designer can guarantee the correct functionalities. Hence, the proposed obfuscation framework can prevent IC from RE, piracy, and overbuilding.

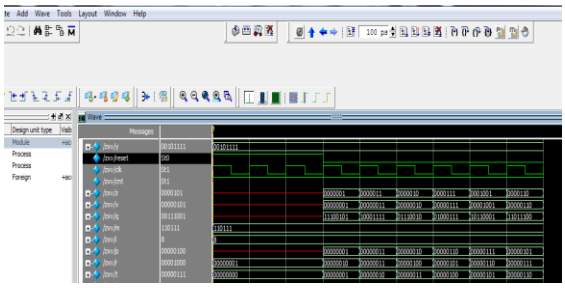

Fig.4 simulation of proposed random generator

| S.no | Parameter | Existing method | Proposed method |
|---|---|---|---|
| 1 | Slice | 2 | 1 |
| 2 | LUT | 3 | 2 |
| 3 | IOB | 8 | 6 |

patterns in OC

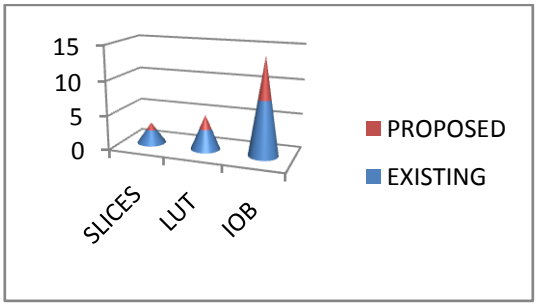


Fig.5 performance analysis of existing and proposed

## V CONCLUSION

In order to circumvent the weakness like Piracy, Overbuilding and Reverse engineering this work provides the solution with the help of the hardware security techniques using a novel practical logic obfuscation method and random generators to prevent an adversary from Reverse engineering. It includes the gate-level netlist and the layout-level geometry of IP/IC. This work protects IP/IC from piracy and overbuilding. The Proposed work achieved the high security and area reduction than the existing techniques. The results were implemented on Xilinx 12.1 tools.

## *REFERENCES*

1. Jiliang Zhang,"(2015) A Practical Logic Obfuscation Technique for Hardware Security," IEEE Trans. Very Large Scale Integrations. (VLSI) Syst.,vol. 23, no. 5, pp. 819–830.
2. Zhang .J, Lin Y., Lyu Y, and. Qu G, ( 2015)"A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing," *IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1137–1150.*
3. Lao. Y and K. K. Parthi K. K,( 2015) "Obfuscating DSP circuits via high-level transformations," IEEE Trans. Very Large Scale Integration. (VLSI) Systems.,vol. 23, no. 5, pp. 819–830.
4. Rostami.M,Koushanfar.F, and R. Karri,(2014) "A Primer on Hardware Security: Models, Methods, and Metrics," Proceedings of the IEEE 102(8), vol. 102, no. 8, pp. 1283–1295.
5. Rajendran.J, Pino.Y, Sinanoglu O., and Karri.R, ( 2012) "Security analysis of logic obfuscation," in Proc. 49th ACM/EDAC/IEEE Design Autom. Conf.,, pp. 83–89.
6. Koushanfar.F,(2012)"Provably secure active IC metering techniques for piracy avoidance and digital rights management," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 51–63.
7. Torrance.R and James.D,(2011) "The state-of-the-art in semiconductorreverse engineering," in Proc. 48th ACM/EDAC/IEEE DesignAutom.Conf. (DAC), Jun. 2011, pp. 333–338.
8. Roy J. A. Koushanfar.F, and Markov I.L, (2010)"Ending Piracy of Integrated Circuits," Computer, vol. 43, no. 10, pp. 30 38.
9. Baumgarten, Tyagi.A, and Zambreno.J, (2010)"Preventing IC piracy using reconfigurable logic barriers," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 66–75.
10. Chakraborty.R.S and Bhunia.S,(2009) "HARPOON: An obfuscation based SoC design methodology for hardware protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 28, no. 10*,pp. 1493–1502.

11. Roy.J, Koushanfar.F, and Markov.I.L,(2008) "EPIC: Ending Piracy of Integrated Circuits," in Proc. Design, Automation and Test in Europe, pp. 1069–1074.

12. Alkabani.Y,Koushanfar.F, and Potkonjak.M,( *2007)* "Remote activation of ICs for piracy prevention and digital right management," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design, pp. 674–677.*