STACK BASED CONFIGURABLE LOGIC GATES TECHNOLOGY FOR IP CORES

D.Keerthana[1], K.Rajesh[2]

[1]*PG scholar, SSM Institute of Engineering and Technology, Dindigul*
[2]*Assistant professor SSM Institute of Engineering and Technology, Dindigul*

---***---

Abstract - Nowadays Logic locking is a promising proactive defense strategy against intellectual property (IP) piracy, counterfeiting, hardware Trojans, reverse engineering, and overbuilding attacks. Logic encryption is also preventing the hardware Trojans insertion which has the entire design is no longer known to an adversary and also making it more difficult to insert a Trojan without causing unintended actions which is more readily detected. To provide a method to increase IC security against a multitude of threats in combinational logic encryption, the current logic encryption techniques has a high usage of power, and area. In this paper, a novel gate level implementation of logic encryption is proposed which is significantly reduces the per-gate overhead of encrypting a gate. Logic encryption method is presented for enhancing security against such threats. In this paper, a novel stack based configurable gate level logic encryption technique is presented with reduced per-gate overheads significantly. The proposed technique also expands the search space of a key sequence and also by increasing the difficulty for an adversary to extract the key value. The proposed technique has been implemented with the comparison of benchmark circuits and also results as a minimum overhead of area and delay increment.

Key Words: Encryption, stack, key gate

1. INTRODUCTION

Due to the drastic increase of complexity in IC fabrication and/or maintaining a foundry with advanced manufacturing capabilities, many semiconductor companies are becoming fabless. Such companies designed integrated circuits (IC) and send the IC's to an advanced foundry, which is usually an off-shore manufacturing. Criticality of recent trend has forced companies to buy several IC intellectual property (IP) blocks to use it in their systems-on-chip and overall the IP blocks are distributed worldwide.

Globalization of the IC design industry has led to different kinds of hardware attacks. An attacker can reverse engineer the functionality of an IC/IP and then steal and claim ownership of the IP. Some of the unauthorized IC fabrication company may also overbuild ICs and sell the IC illegally. Finally, the unwanted circuits may insert malicious circuits into the design without the knowledge of designer. Therefore, the semiconductor industry loses $4 billion annually due to the attacks. Such attacks have led IP and IC designers to re-evaluate in hardware's trust.

Each and every IC/IP designer has an additional responsibility to protect an individual design. If a designer is able to cover the IC's functionality while it passes through the different, potentially untrustworthy design flow, these attacks can be thwarted. To overcome these issues, the logic encryption concept is proposed. Logic encryption is the process of hiding the functionality and the implementation of a hardware design by inserting some additional gates called *key-gates* into the original design. In order to find a correct functionality, the valid key has to be supplied to the encrypted design. By applying a wrong key, the encrypted design will produce wrong outputs.

In this paper, the NAND/NOR stack based logic encryption is proposed to reduces the area, power, and performance overheads of utilizing the stack-based approach. This paper is structured as follow: Section II illustrated the literature survey based on proposed approach. In section III presented a preliminaries approach based on logic locking methodology. Section IV presented the experimental results and discussions and section V concluded the paper.

II. LITERATURE SURVEY

Yingjie Lao et al [1] presented an approach to design obfuscated circuits for digital signal processing (DSP) applications using high-level transformations, a key-based obfuscating finite-state machine (FSM), and a reconfigurator.

Lannanluo et al [2] proposed a binary-oriented, obfuscation-resilient binary code similarity comparison method based on a new concept, longest common subsequence of semantically equivalent basic blocks, which combines rigorous program semantics with longest common subsequence based fuzzy matching.

Marc et al [3] proposed two factors i.e., proposed the hybrid diversification approach for protecting embedded software and second one is to provide statistical metrics to evaluate the protection. Diversification can be achieved by combining hardware obfuscation at the micro architecture level and also software-level obfuscation techniques used to insert in the embedded systems.

Anirban et al [4] presented a novel structural obfuscation methodology which is used for protecting a digital signal processor (DSP) IP core at the architectural synthesis design stage.

Milena et al [5] proposed a reputation aware localized adaptive obfuscation for mobile opportunistic networks. This method comprises of two complementary techniques: one is opportunistic collaborative testing of nodes' obfuscation behavior (OCOT) and another one is multidimensional adaptive anonymisation (AA).

Jaya et al [6] proposed to protect all the hardware state with a low-cost state- deflection-based obfuscation method. This method is dynamically deflects state transitions from the original transition path to a black hole cluster if a wrong key is applied.

Xueyan et al [7] proposed a set of quantitatively evaluable metrics particularly facilitated by a recently circuit partition attack (CPA) and the powerful SAT-based attack (SATA).

Anirban et al [8] presented an obfuscation methodology of transient fault secured circuits. The approach presented obfuscates fault secured DSP circuits such that the functions of the resulting hardware become non-obvious to an adversary i.e., hindering reverse engineer process.

Sandhya et al [9] proposed a technique for hardware obfuscation named as dynamic functional obfuscation. This Hardware obfuscation is used to a set of countermeasures used against IC counterfeiting and illegal overproduction.

III. PRELIMINARIES

Jiliang Zhang et al [10] proposed a hardware security for the thwart piracy, overbuilding, and reverse engineering (RE) by obfuscating and/or camouflaging. These methods are incur high overheads, and integrated circuit (IC) camouflaging which cannot be provided any protection for the gate-level netlist of the third party IP core or the single large monolithic IC. In order to overcome these issues, the hardware security techniques and a practical logic obfuscation method are presented 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.

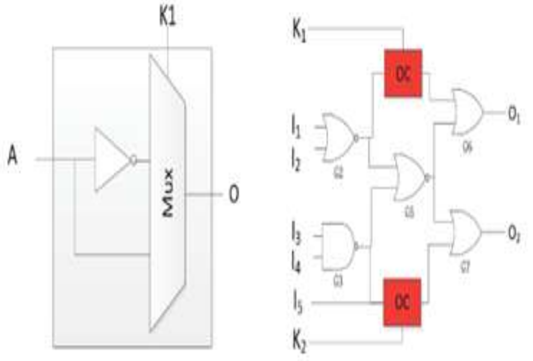
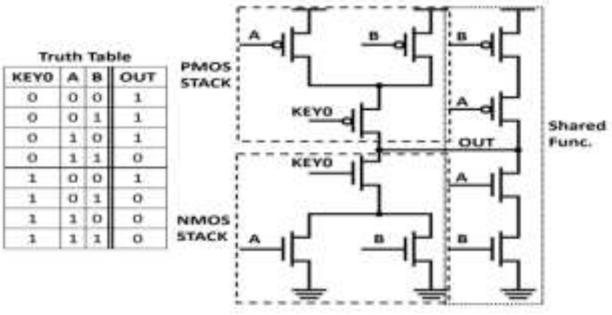


Figure 1: Structure and circuit of an OC

Traditionally, the IC design is developed without any concern of obfuscation, and hence IC design is vulnerable and threatened by the attackers by using RE, piracy, and overbuilding. The figure 1 is given a gate- level netlist of the design, which is modified the original netlist by including an obfuscated cell (OC). An obfuscated gate-level netlist is synthesized into the layout geometry for manufacturing. The functionality of obfuscated cells cannot be identified to the attacker. The combinational logic obfuscation technique is used to thwart piracy, overbuilding, and RE attacks. The attackers can be extracted the gate-level netlist by circuit-extraction-based RE, which cannot infer the obfuscated logic functions. A PUF response can be used to XOR with the configuration of OCs that is used to generate a device-dependent license to prevent piracy and overbuilding attacks of the IC.

IV. PROPOSED SYSTEM

in this section, the proposed system is described, an area of research aimed at ensuring secure and reliable ICs for critical applications is logic encryption in an IC. To increase the security of IC, the current implementations of XOR or the look-up table (LUT) methods, have high per gate overheads. A reduction in the hardware gate overhead is required to implement logic encryption in a wide variety of applications. Novel gate level designs for logic encryption are described.



Truth Table

KEY0	A	B	OUT
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Figure 2: proposed structure of stack based NAND/NOR gate.

The proposed topology is shown in Fig 2, is named as stack-based NAND/NOR gate. It is the process of ability of a key input to turn on/off the PMOS/NMOS logic stacks. If the KEY0 is 0, then the PMOS stack is activated allowing the gate to behave as a NAND gate. If the KEY0 is set to 1, then the NMOS stack is turned on allowing the gate to behave as a NOR. This disconnection of the logic stacks depending on the value of the input key which reduces power consumption and limits the degradation in performance. The NAND/NOR stack-based topology has two important characteristics in the following:

Firstly, the proposed has the ability to share common input/output combinations between implemented logical functions. In this process, the Implementations that do not require negated inputs. For example, when inputs A and B are either 0 or 1, the NAND and NOR gates generated the same logical output, permitting shared functionality as indicated by the fine dashed box (shared func.). To eliminate the key transistor, reduce the area, power, and performance overheads of utilizing the stack-based approach.

The second factors of the NAND/NOR topology, is not requiring negated inputs of A and B, which removed two additional inverters from the circuit and also reduced the overhead of the proposed topology. In case of NAND/AND stack-based topology was implemented instead, then the negated inputs are required which has the same input combinations must either turned on a PMOS or NMOS stack depending on the key value.

A useful IC with the key stacked in its memory is utilized as a oracle to distinguish the inaccurate keys in an iterative fashion. Be computational intricacy of the attack is expressed as far as the quantity of DIPs produced by the SAT attack. Be most recent research on logic locking have concentrated on shielding against the SATattack.

The SAT-attack flexible logic locking which guaranteed the quantity of proportionality classes of keys is exponential in the key length. Extensively, these recommendations all offer the structure appeared in Figure. A circuit is presented in which "flips" the output refer to this part as the 3D cube stripping unit. The output of this circuit is then altered to inversion by a key-dependent circuit which refers to as the programmable usefulness restoration unit. The last circuit in figure is ensured to have an exponential number of equivalence classes of keys and guaranteed a SAT attack versatility. Starting proposal of lines were Anti-SAT and SARLock. Against SAT was defenseless to the signal probability skew (SPS) attack while SARLock was helpless against the Double DIP attack and the Approximate SAT attack. The two plans are powerless against evacuation and sidestep attacks. TTLock and Secure Function Logic Locking (SFLL) to the best of the information, SFLL is the main combinational logic locking plan flexible to the entirety of the above attacks. The weakness that recognize in the state of art locking strategy SFLL-hd. This helplessness is a final product of the way that previous tools synthesized are security-negligent.

It is obvious from the netlists, the SFLL is resynthesized their netlists to conceal the secured hardware designs; the basic attacks can recognize the protected design in all the cases, thus separating the secret key. Until a genuine security aware tool is grown, any defense that depends on customary CAD tools will be defenseless. By inspiring avulnerability in a best in class logic locking strategy that has been solid up to this point, the work emphasizes a significant shortcomings, i.e., the requirement for the improvement of a security aware synthesis tool, along these recognizing a significant research flow. The strategy that upgrades Anti-SAT expands the network between the recently included blocks and the first logic to prevent basic evacuation attacks. This upgrade strategy is of no utilization for SFLL-hd either the attack expects and scans for stepping a hamming separation checker installed into the original circuit for usefulness stripping.

V. RESULTS AND DISCUSSION

In this section, the proposed circuit are simulated and synthesized by using xilinx12.1 which is occurred a low area than the traditional methodologies. In this method, the schematic of proposed circuits are layout and output waveform which is shown in the fig.3 and 4. The experimental results are given in Table 1 Then the RTL schematic and gate netlist of the proposed are shown in fig.5 and 6 respectively. From the figure 7 and 8, the simulation output for the proposed logic locking is shown with the corresponding digital waveform.

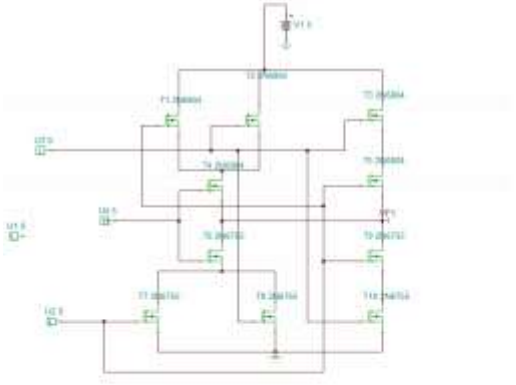


Figure 3: proposed circuit

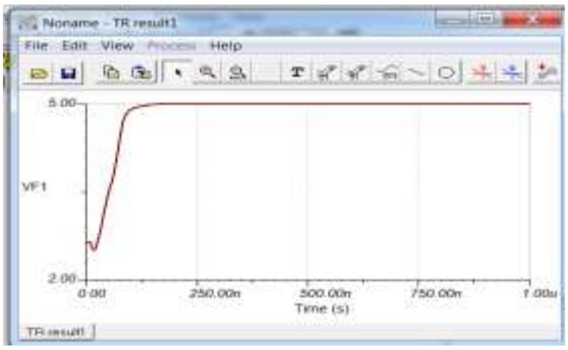


Figure 4: output of key gates

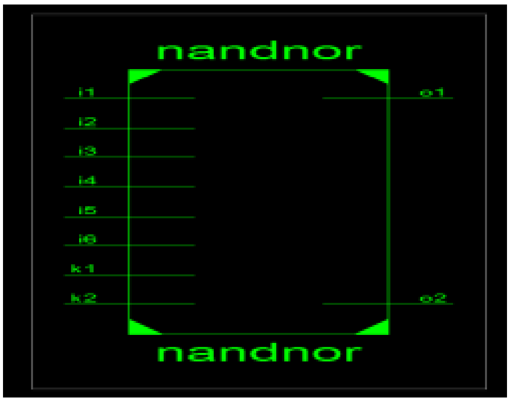


Figure 5: RTL schematic

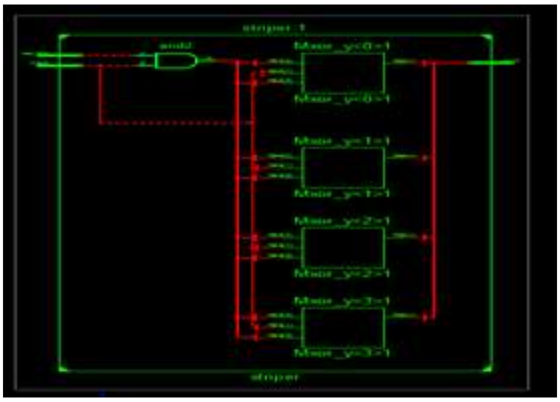
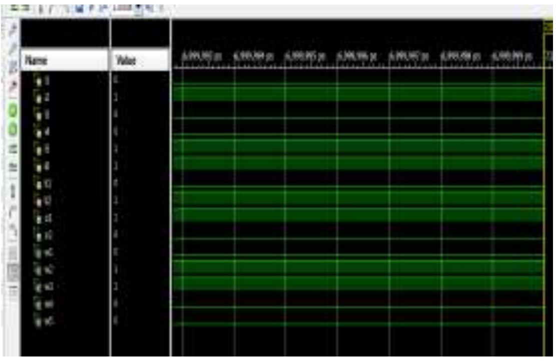


Figure 6: Gate netlist



I

Figure 7: simulation result

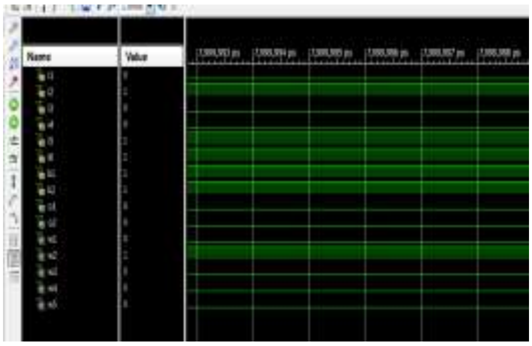


Figure 8: Encrypted output

VI. PERFORMANCE ANALYSIS

In this section, the comparison of proposed and the conventional methods are presented A synthesis report for the proposed circuits are showed in the fig 9. From the Fig 10, it clearly shows that there is a considerable reduction in time and area based on the implementation results which have been done by using Spartan-3 processor. The proposed algorithm significantly reduces area when compared to the standard benchmark with the traditional methods

Figure 9: synthesis results for the proposed

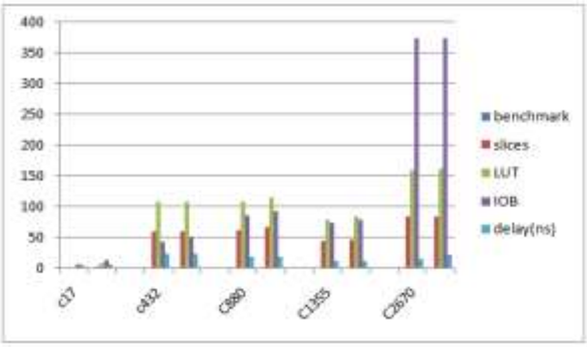


Figure 10: performance chart

VII. CONCLUSION

In this paper, the proposed attack based NAND/NOR based on Functional Analysis attacks using Logic Locking algorithms is implemented. These attacks are identified the locking key used structural and functional analysis. The Experimental results showed that the proposed method succeeded against existing system of bench mark circuits which is the only combinational locking algorithm resilient to all known attacks. The proposed operation in the locked design tools to implement the functionality strip operation. It is clear that the experimental results are showed the considerable reductions in the slices count and clock period time. The performance analysis of proposed are successfully simulated and may in future the hardware implementation can be done using SPARTAN-3 FPGA Board.

REFERENCES

[1] Yinjie.B et al “Obfuscating DSP Circuits via High-Level Transformations”, IEEE Transactions on Integrated Circuits and Systems, vol. 34, no. 6, pp.961–971, April 2018.

[2] Lannanluo.S et al “Semantics-Based Obfuscation-Resilient Binary Code Similarity Comparison with Applications to Software and Algorithm Plagiarism Detection,” IEEE Design & Test of Computers, vol. 27,no. 1, pp. 10–25, Jan 2017.

[3] Marc.G et al “Hybrid Obfuscation to Protect Against Disclosure Attacks on Embedded Microprocessors,”IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 51–63, Feb2016.

[4] Anirban.S et al “DSP design protection in CE through algorithmic transformation based structural obfuscation,” USENIX, Mar 2015, pp. 495– 510.

[5] Milena.G et al “Reputation Aware Obfuscation for Mobile Opportunistic Networks,”IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, May 2015.

[6] Jaya Dofe.S et al “Novel Dynamic State-Deflection Method for Gate-Level Design Obfuscation,”vol. 64, no. 2, pp. v f b x 410–424,Dec.2015.

[7] Xueyan.M et al “Towards a Formal and Quantitative Evaluation Framework for Circuit Obfuscation Methods,”USENIX Association, April 2007, pp. 20-26.

[8] Anirban.S et al “Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature,”IEEE Transactions on Information Forensics and Security, pp. 55–78, Jan 2013.

[9] Sandhya.M et al “Key-Based Dynamic Functional Obfuscation of Integrated Circuits Using Sequentially Triggered Mode-Based Design,”IEEE Transactions on Information Forensics and Security, Vol. 5,Feb2012.

[10] Zhang, J. “A Practical Logic Obfuscation Technique for Hardware Security”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 24(3), 1193–1197, 2016.