Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 4, 2020

Review Article

SECURED NETLIST GENERATION USING OBFUSCATION TECHNIQUE

M. Hemachand[1], E. Prabhu[2]

[1]Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. maddihemachandu@gmail.com
[2]Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. e_prabhu@cb.amrita.edu

Received: 05.12.2019 *Revised: 14.01.2020* *Accepted: 09.02.2020*

Abstract
Researchers have been conducting research in the field of hardware security for giving the security to the net list. Even camouflaging of the integrated circuit (IC) is not providing any security to the gate level net list. Abundant obfuscation techniques are available but they are not conquering the problem. While using the obfuscation techniques the factors like power, area and cost are given importance. Obfuscation used in this work reduces power, area and cost. In the design if the obfuscation used in this work is inserted, reverse engineering can't extract the gate level net list. Experiments shows that the design with the obfuscation gives less variation in power and area when compared to design without obfuscation.

Keywords: Hardware Security, Logic Obfuscation, Overbuilding, Physical Unclonable Function (PUF), Piracy, Reverse Engineering (RE).

DOI: http://dx.doi.org/10.31838/jcr.07.04.167

INTRODUCTION

Integrated circuits are playing a vital role in the present electronic world. So attackers are using criminal methods for retaining the information in the integrated circuits. Plagiarism of the integrated circuit has become a very common practice these days due to reverse engineering. Reverse engineering has become a threat to the semiconductor industry. Because of this the fame of integrated circuit designers is going down. Reverse engineering can be done using free tools or with less cost. So maximum attackers are using this to extract the net list. Using the plagiarized integrated circuit may even cause damage to the system[3]. By using this for research on integrated circuits the researchers may get the unfair results. As there is no security for the net list, the distrust designer is making a large number of integrated circuits and advertising the integrated circuit in a criminal manner. By using the reverse engineering they can extract net list and loot the information about the integrated circuit. They can also add some extra circuit which can damage or copy the information of the system. Due to the plagiarized integrated circuits, the wealthy relation between the designers and the clients will be broken, and because of this, there will be less hope on designers. To overcome this problem the designers should add some additional security to the design so that, only clients can access the design. The security can be given to the design by two types. They are authentication and obfuscation. The authentication process consists of a physical unclonable function whereas obfuscation means addition of an extra circuit.

LITERATURE SURVEY

A. Reverse Engineering (RE)

Reverse engineering is a process of decoding for exposing the designs and architecture of any circuit [4]. Reverse engineering is the hierarchical analysis method. Generally reverse engineering is used to verify the design of the circuit which the clients have given to designer. By using the reverse engineering the following can be done:

- Identify the technology which was used in the design of the circuit.
- The gate level net list extraction of the design.
- Changing the functionality of the design[12].
- Identify the components and boards present in the design.

By using reverse engineering, the details of the circuit can be known which can be used in an illegal manner. There is a huge damage to both designers and clients because of this[6].

B. Cam-ouflage

Cam-ouflage means adding some extra circuit to the design which will provide security to the design[10]. It is mainly used in the integrated circuit while possessing the layout information of the integrated circuit. By adding the cam-ouflage gates in the design, even if anyone try to apply the reverse engineering technique, they can't get the information of the device. By somehow if they get the information of the device also, it gives the information of the cam-ouflaged circuit only, that is it won't give any information of the original device[9]. To prevent integrated circuit from the reverse engineering approaches, any of these cam-ouflaging approaches can be used:

- Flexibility to the reverse engineering: By using this the attacker cannot know whether the device is cam-ouflaged.
- Corrupted outputs: The cam-ouflaged device net list should dominate the output of the net list of the original device.

Integrated circuit cam-ouflaging has an advantage. The unused spaces in the design will be occupied by the cam-ouflaged design and it will just look like as if it is an original part of the device.

C. Obfuscation

Obfuscation is nothing but addition of an extra circuit to the device without changing the functionality. Obfuscation is a two level approach. They are system level and circuit level [1].

System level approach

Very Few approaches in the system level comes under classical obfuscation approach. The remaining approaches are just general approaches.

- Component obfuscation: Mostly reverse engineering approaches focuses on the component identification. This approach is used to give more security to the components.

By changing the logic gates at the input and output sides it provides security [8].

- Obfuscation with programmable logic: In this technique, a subdivision of the gates is replaced by the physical unclonable functions. Physical unclonable functions are very unique. These are connected to the FPGA to duplicate the function of recovered logic.
- FSM modification: In this approach FSM will generate a key. Only the correct input sequence key will pass the information about the device[2].
- Logic encryption: In this approach additional gates are added to the security key as an input to design. When the key given by the client matches with the security key, the device not only shows the correct output but also the correct information about the device. When the key given by the client is different from the security key, the device shows a corrupted output[11].

Chip level approach

Circuit level obfuscation approach is to build or repair the cell libraries for changing the functionality of the gates. In this level, random circuits are added to the design.

- Cam-ouflaged cells: In this some dummy gates or wires are added to the structure.
- Filler cells A group of logic cells joined together is called a dense network. In this approach, some dense networks are connected. By adding the denser network to the design, there is no change in functionality.

D. Physical unclonable function

The unique nature of the Physical unclonable function (PUF) is due to micro structure present in it[5]. Due to the introduction of some physical factors to the PUF its structure is in micro state. Because of this, it is unstable and undisciplined. The PUF generates random key every time. So that, it gives more security to the device. Features of the PUFs are given as follows:

- The response to various challenges is Constant and sudden. It should stay constant for same challenge over multiple observations.
- Any two Physical unclonable functions should not generate the same key.
- Physical unclonable function may damage because of noisy aggression. So the damaged PUF can be identified by attackers easily.

The PUFs are analog PUFs, memory PUFs and digital PUFs[7]. The inputs given to the PUFs are called challenges, whereas outputs of the PUFs are known as responses. So PUFs is a challenge-response pair. Based on the challenges and responses PUFs can belong to any of these following categories:

- PUFs having limited number of the challenges and responses are known as weak PUFs.
- PUFs having large number of the challenges and responses are known as strong PUFs.

CONTRIBUTIONS

The contributions done were explained briefly as given below.

- Net list extraction for the original circuit.
- With no much area and power reduction, an obfuscation technique was proposed for preventing the reverse engineering techniques and from third parties.
- Obfuscation technique was demonstrated for the benchmark circuits.

PROPOSED METHODOLOGY

Integrated circuits were fabricated without using obfuscation in the olden days. Now a days design engineers are facing issues due to the reverse engineering done by attackers. So there is a need for the designers to secure the net list from them by using suitable obfuscation techniques .After inserting obfuscation circuit in the original circuit the area and power should not increase when compared to the circuit without obfuscation. The functionality of the integrated circuit should not change after inserting the obfuscation .If any hacker tries to extract the net list after inserting obfuscation, they can't identify the functionality of the particular integrated circuit. When the correct key is given by the designer, the key reacts with the Physical unclonable function. By this original functionality can be detected by the designer only.

A. Obfuscation Structure

The proposed obfuscation circuit consists of linear feedback shift register. The linear feedback shift register will be acting as shift register. The output will be taken at each clock. The output will be seen until the linear feedback shift register complete the number of states which depends on the seed. The seed which is given to the linear feedback shift register acts as a key for the protection of the integrated circuit. In gate level net list the obfuscation structure can be inserted in any wire. The obfuscation structure is shown in Fig.1.

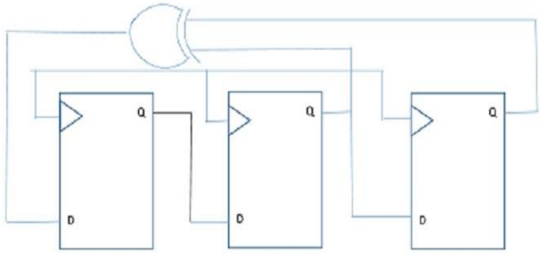

Fig. 1: Proposed obfuscation structure

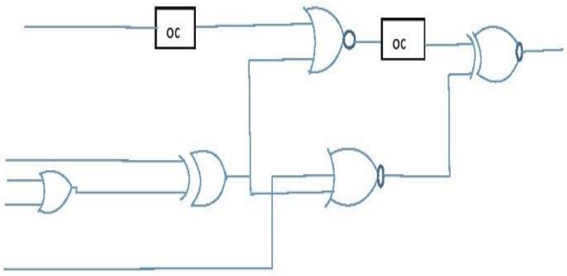

Fig. 2. Proposed inserted obfuscation structure

B. Reverse engineering

Reverse engineering is miss used by the attackers for stealing the information of the integrated circuit. The following are the procedures usually adopted by attackers:

- They extract the gate level net list of the designs by using the reverse engineering.
- The attackers adds some circuit to steal the information.
- They steal the information of the customers.

The wires of the gate level net list are inserted into the linear feedback shift register. If the attackers try to extract the gate level net list by reverse engineering, the functionality of the design will be changed. This happens because of the inserted obfuscation circuit. The attackers can't decode the functionality of the integrated circuit. The seed will be given by the designer to the linear feedback shift register. It will undergo an xor operation to produce a key based on the polynomial degree. If Xor and Xnor are used as obfuscation circuits, the key will be 0 by default to the Xor and 1 is used as key to the X nor. If the attackers use some random keys it is not safety to the design. When the proposed obfuscation circuit is used for obfuscation, the key cannot not be find out by the attackers. The net list will be displayed only after the giving proper key. Obfuscation circuit is inserted into the design and it is shown in Fig.2.

C. Gate level net list

Generally all the gates of the integrated circuit can be seen by anyone when the reverse engineering technique is applied. By using reverse engineering, when the obfuscation circuit is inserted in the design all the gates present in the design are not visible to the attackers. This security to the net list is achieved by inserting the obfuscation.

The proposed flow chart for providing security to the net list of the design is as shown in Fig. 3

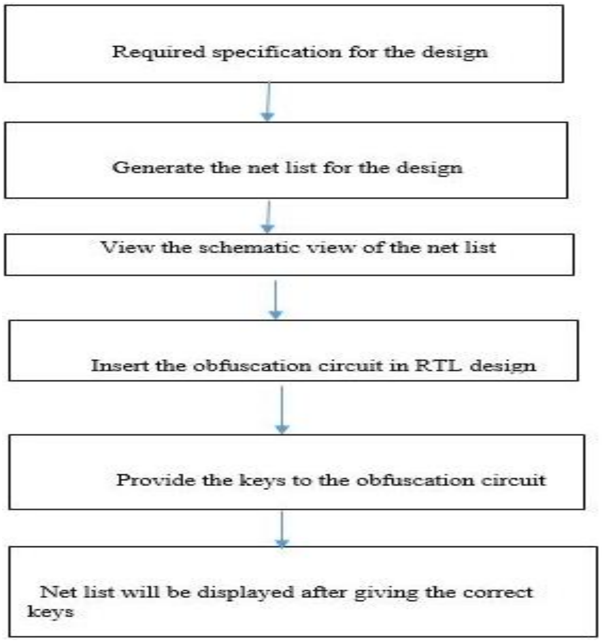
Required specification for the design
Generate the net list for the design
View the schematic view of the net list
Insert the obfuscation circuit in RTL design
Provide the keys to the obfuscation circuit
Net list will be displayed after giving the correct keys

Fig. 3: Proposed Flowchart

RESULTS

For ISCAS'89 benchmark circuits, experiments are conducted with and without obfuscation techniques. The computation of power and area of the benchmark circuits for with and without obfuscation is done in Synopsis Design Compiler. For some circuits the power and area will not vary much. The area is also not varying much. The percentage overhead of the power and area will not vary much when compared to benchmarks circuits for with obfuscation and without obfuscation.

Table 1: Power comparison for different benchmark circuits

Circuit	Without obfuscation Power(µW)	With obfuscation Power(µW)
s298	35.7943	35.9987
s344	84.377	84.895
s420	46.1600	46.5
s510	48.5420	48.94
s820	33.2230	33.885
s1196	145.877	146.001
s5378	269.24	269.99
s9234	344.98	345.001
s3854	7228.42	7228.95

Table 2: Area comparison for different benchmark circuits

Circuit	Without obfuscation Area(µm*µm)	With obfuscation Area(µm*µm)
s298	860.588	861.05
s344	959.988	960.002
s420	1027.158	1027.201
s510	1245.894	1246.010
s820	1469.9844	1470.00001
s1196	2829.180	2830.0101
s5378	2936.546	2936.956
s9234	7830.582	7830.998
s3854	85049.0526	85049.120

The percentage overhead of the benchmark circuits are negligible when compared to with and without obfuscation. The percentage overhead of the power and area are as shown in Fig. 4 and Fig. 5.

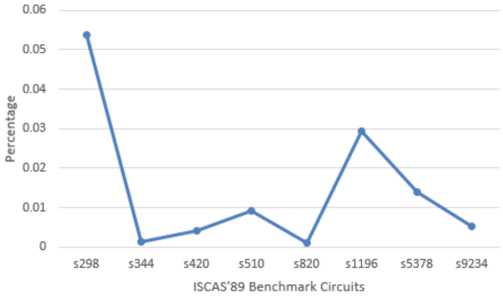

Fig. 4: Percentage overhead of area

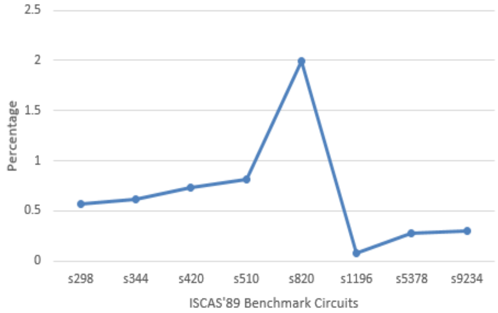

Fig. 5: Percentage overhead of power

CONCLUSION

By using the obfuscation technique, the security can be provided to the design without effecting the functionality. Only a negligible change in power and area are observed. Due to this the attackers cannot plagiarize the design and malfunctioning of the design is also prevented.

REFERENCES

1. Jiliang Zhang,"A Practical Logic Technique for Hardware security" IEEE Trans. Very Large Scale Integr. (VLSI) syst, vol.24, no.3, pp.1193- 1197, Feb 2016.
2. Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote activation of ICs for piracy prevention and digital right management," in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design,pp. 674–677 ,Nov. 2007
3. Charan, J., Goyal, J.P., Saxena, D.Effect of Pollypill on cardiovascular parameters: Systematic review and meta-analysis(2013) Journal of Cardiovascular Disease Research, 4 (2), pp. 92-97.
   DOI: 10.1016/j.jcdr.2012.11.005
4. R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," inProc. 48th ACM/EDAC/IEEE Design Autom. Conf. (DAC), pp. 333–338, Jun. 2011.
5. Chavda HV, Patel CN, Anand IS. "Biopharmaceutics Classification System." *Systematic Reviews in Pharmacy* 1.1 (2010), 62-69. Print. doi:10.4103/0975-8453.59514
6. L.W. Chow, J.P. Baukus, and W.M. Clark, "Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line

terminating on field oxide," U.S. Patent 7294935, Jul. 25, 2002

7. J.-L. Zhang, G. Qu, Y.-Q. Lyu, and Q. Zhou, "A survey on silicon PUFs and recent advances in ring oscillator PUFs," J. Comput. Sci. Technol., vol. 29, no. 4, pp. 664–678, Jul. 2014.
8. G. Suhand S. Devadas, "Physicalunclonable functions for device authentication and secret key generation," in Proc. Design Automation Conf. (DAC), pp. 9–14,2007
9. R. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," in Proc. Int. Conf. ComputerAided Design (ICCAD), pp. 674–677,2008
10. J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouaging," in Proc. ACM / SIGSAC Conf. Comput. Commun. Secur., pp. 709–720, 2013.
11. Veena, V., Prabhu, E., Mohan, N. "Improved test coverage by observation point insertion for fault coverage analysis," (2019) Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019, art. no. 8862789, pp. 174-178.
12. A.P.V and Ramesh S.R. "An Approach towards Logic Synthesis by Functional Decomposition", International Journal of Engineering Research and Applications, vol. 2, no. 3, pp. 324-330, 2012.