ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

Obfuscated Circuit Using Pseudo Random Masking Generator

A. Manimekalai[1] , R.Geeta [2], Dr.K.Ramasamy[3]

P.G Scholar, Department of Electronics and Communication Engineering, P.S.R Rengasamy College of Engineering for Women, Sivakasi, Tamilnadu, India[1,]

Assistant Professor, Department of Electronics and Communication Engineering, P.S.R Rengasamy College of Engineering for Women, Sivakasi, Tamilnadu, India[2],

Professor, Department of Electronics and Communication Engineering, P.S.R Rengasamy College of Engineering for Women, Sivakasi, Tamilnadu, India[3]

ABSTRACT: The economic process of Integrated Circuit (IC) design flow, rogue elements in the supply chain can thief ICs, overbuild ICs, and insert hardware trojans. The nonstop drive of Moores law to increase the integrating level of silicon chips has presented superior challenges to the reverse engineer, change simple teardowns, and demanding the approval of new and more sophisticated practical exercise to analyse chips. Hardware encoding embedded in chips adds a whole other level of difficulty to IC investigation.In this project propose applicative logic obfuscation method with low operating cost to prevent an adversary from RE both the gate-level netlist and the design-level geometry of IP/IC . Use a random number generators to mask logic vaue efficiently.our proposed scheme has been coded in HDL and simulated using Xilinx 13.2.

KEYWORDS: *Hardware security,overbuilding, logicobfuscation,pseudorandom generator(PRNG),physical unclonable function,reverse engineering.*

I.INTRODCUTION

New trends in micro electronics engineering have stepwise varied the scheme used in VLSI circuits.Found an cost-effective methodology is one of the key to designing VLSI chip successfully. The organisation of microelectronics system is powerfully influenced by the concept that transistor and featured sizing have endlessly influenced, while denseness and frequency have increased.

Due to the constantly increasing quality of constructing and/or maintaining a foundry with beforehand fabrication capabilities, many semiconductor companies are comely fabless. Such fabless combanies creating the integrated circuits(IC) and send them to an modern manufactory, which is usually off-shore, for fabrication Also, the criticality of time-to-market has affected companies to buy several IC intellectual property (IP) blocks to use them in their systems-on-chip. The purchase and sellers of these IP blocks are distributed worldwide.[1]

Unfortunately, new tendency in IP piracy and reverse engineering activity to make false ICs have lifted serious concerns in the IC designing world organization. IP piracy can take various kind , as illustrated by the following scenarios.

1) A chip design building buys an IP core from an IP marketer and form an illegal text or “clone” of the IP. The IC design building then sells it to another chip design building (after minor modifications) demand the IP to be its own.

2) An untrusted fabrication building form an illegal text of the GDS-II information activity by a chip design building and then illegally sells them as hard IP.

3) An untrusted manufactory manufacturing and sells false copies of the IC under a various brand name .

4) An individual performs postsilicon reverse engineering on an IC to manufacturing its illegal clone.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

New works in the hardware security goal to spoil the copyright infringement, overbuilding, and RE by obfuscating and/or camouflaging. However, they suffer from various issues. Below we will present these method in detail and analyze the limitations of them.

II.EXISTING SYSTEM

Jiliang Zhang survey of hardware protection aim to spoil highjacking, overbuilding, and reverse engineering (RE) by obfuscating and/or camouflaging. However, these method obtain high overheads, and integrated circuit (IC) camouflaging cannot provide any safety for the gate-level netlist of the third party intellectual property (IP) core or the single large monolithic IC. In order to circumvent these failing, this brief elaborately study 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 highjacking and overbuilding.[1]

Traditionally, the IC designing is written without any interest of obfuscation, and therefore IC designing is vulnerable to RE, highjacking, and overbuilding. Granted a gate-level netlist of the design, our destination is to alter the original netlist to make an modify netlist, which is serviceable equal weight to the former when exact key is granted, An modify gate-level netlist is alteration into the layout geometry for fabrication.[3] An person purchase the obfuscated IC on the open market and then discovery the gate-level netlist by visual aspect processing-based RE. All the same, the practicality of modify cells cannot be identified. The altered netlist reacts with a silicon physical unclonable function (PUF), and it can precisely execute the same as that of the design as long as the right license is issued by the IP/IC designer. This means that only the chips authorized by the designer can assurance the correct functionalities. Hence, the proposed obfuscation construction can keep IC from RE, highjacking, and overbuilding.[2]

A.OBFUSCATION STRUCTURE

Fig.1 Shows the Obfuscation cell is composed of an inverter and a multiplexer.Obfuscation cell is used to lock each IC.

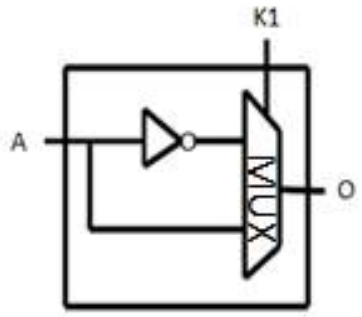


Fig.1. structure of an OC

As shown in Fig.2(a),a circuit obfuscated with the combinational logic obfuscation method in [7]by inserting a XOR gate .It obviously shows that if an adversary extracts this gate level netlist by RE ,the secret key bits of inserted gates would be leaked.

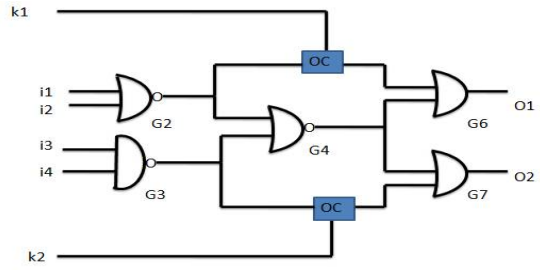
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017



In Fig.2(b),G4 and t1 are the key gates; an attacker can sensitize the key bits K1 and K2 to the ouputs O1 and O2 to obtain the key values by applying a specific input pattern.

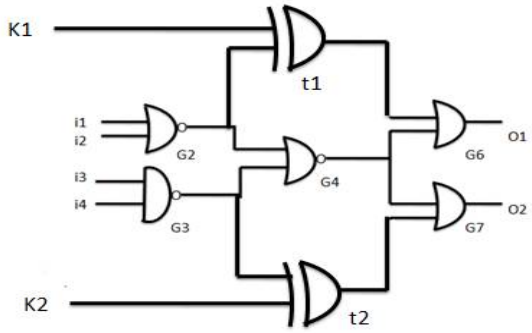


Fig.2 (a) An example of obfuscating a getlevel netlist with two OCs.(b) circuit obfuscated with the combinational logic obfuscation method.

B.PUF –based Obfuscation and the Generation of Licences

We use the configuration of OCs of obfuscated design to interact with the PUF response in order to generate a chip-dependent license to prevent piracy and overbuilding attacks and provide the pay-per-device licensing service. An attacker with no information about the key of the OCs cannot compute the correct license to unlock the pirated/overproduced chips. Hence, the designer is the only one who can issue the license to activate the chip. When the chip is powered on, the PUF response will XOR with the license to generate the correct configuration for OCs, then the generated configuration is stored in the flip-flops to unlock the chip. . The attackers can pull out the modify gate-level netlist by RE, but the extracted netlist does not include the key bits.

We use the PUF response[4] to unlock the role of the chip. The designer infrequently work out the error correcting code (ECC) to set for any bit flips to the PUF output (response) because the PUF output is hard to keep perfectly stable due to the noise or other sources of physical quality. Note that, we do not study the operating cost of employ PUFs and ECC methods[6] in this brief.Here the combinational logic obfuscation method to spoil piracy, overbuilding, and RE operation. Although the attackers can pull out the gate-level netlist by circuit-extraction-based RE, they cannot generalize the obfuscated logic functions. The only mode is to complete test all design of OCs by the infeasible brute-force attack[9]. Therefore, the obfuscation method in this brief not only resists visual aspect processing-based RE but also incurs low area and power overheads. In Fig.3,A PUF response can be used to XOR with the configuration of OCs to generate a device-dependent license to prevent highjacking and overbuilding attacks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

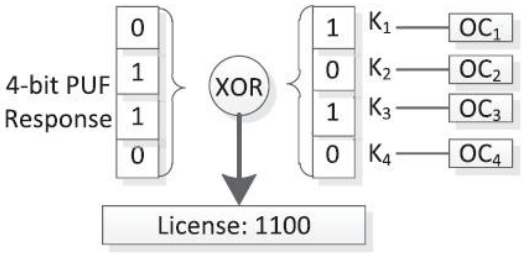


Fig.3.PUF-based obfuscation and the generation of the licences.

III . PROPOSED SYSTEM

The destination of secrecy countermeasures is to make the physical characteristics of integrated circuits independent of intermediate values and function performed during cryptographic applications. Among secrecy countermeasures, basically separate scheme: one based on the randomisation of the carrying out of cryptographic algorithms one or more Pseudo Random Number Generators (PRNGs) [8] are also consider to create the masks, which should be updated at each step of the datapath for a more economical masking scheme. PRNG in Fig.4,is used to create key values to beat the limitations of automatic insertion values .

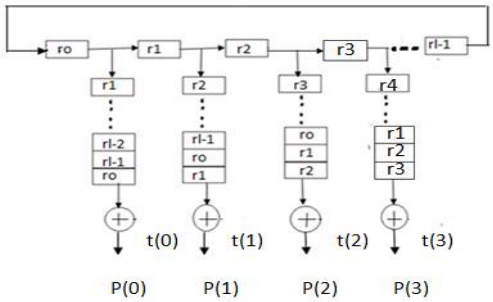


Fig.4.Pseudo random test pattern generator

A. PSEUDORANDOM TEST PATTERN GENERATION:

A pseudorandom number generator (PRNG), also best-known as a settled random bit generator (DRBG), is an algorithm for make a sequence of numbers whose properties approximate the properties of sequences of random numbers. The benefit of settled tests is, they supply a compact test set that are targeted to the detection of the defined fault list; and the obvious disfavour is the extended computing cost and complexity.

B.PSEUDO RANDOM GENERATOR WITH OC

A masking counter measure that conceals intermediate values with random values throughout circuits.In Fig.5,A hiding countermeasure that efficiently randomizes the execution of operations at the data-path level.The pseudo random generator provides the key values to an obfuscated circuit.Finally the proposed method provides high security in hardware design.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

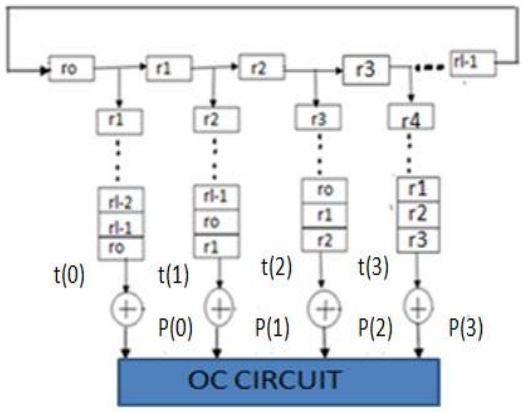


Fig. 5.Oc With Pseudo Random Generator

IV. EXPERIMENTALRESULTS

A . EXPERIMENTAL SETUP

we performed a set of experiments to evaluate the overhead of implementing the obfuscation technique.The experiments are performed on the circuits which are described in verilog format from the ISCAS benchmark.The synthesis was performed using xilinx 13.2.

B. EXPERIMENTAL ANALYSIS

Table 1 gives the synthesis summary conducted on ISCAS benchmark circuits.The columns number of slices,IOB and delay are the parameters of the original design and obfuscated design .The area is less compared to the existing obfuscation method.The delay is also reduced for different benchmark circuits with proposed method.

TABLE ISLICES, DELAY, IOB FOR OUR PROPOSED OBFUSCATION METHOD

Circuits	Existing Method			Propoesd Method		
	Slices	IOB	Delay	Slices	IOB	Delay
S400	2	9	6.697	1	7	6.236
S38417	2	9	7.535	1	7	7.337

The S400 circuithas slices and IOBs are high compared to proposed method as shown in Fig.6.The delay is calculated as 6.236ns in our proposed obfuscation method.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

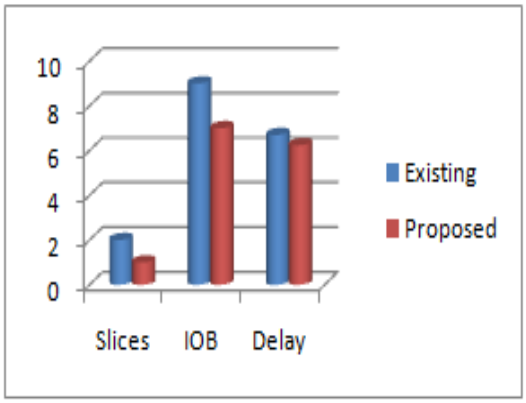


Fig .6. S400 benchmark circuit comparision

In S38417 benchmark circuit the slices and IOB usage is large compared to our proposed method is shown in Fig.7.The delay is measured as 7.336ns in our proposed system.

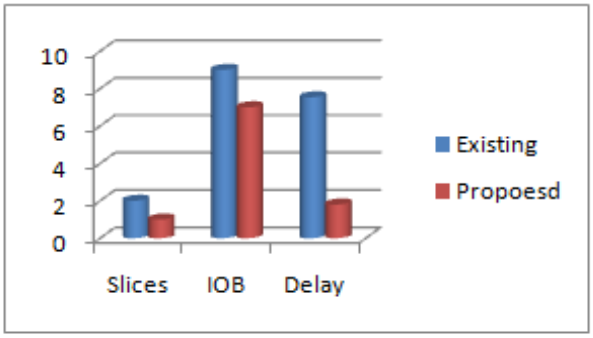


Fig.7.S38417 benchmark circuit comparision

C.PERFORMANCE ANALYSIS

The performance analysis in Fig.8.shows the difference between existing system with proposed system.The difference is made by using slices,IOBs and Delay.

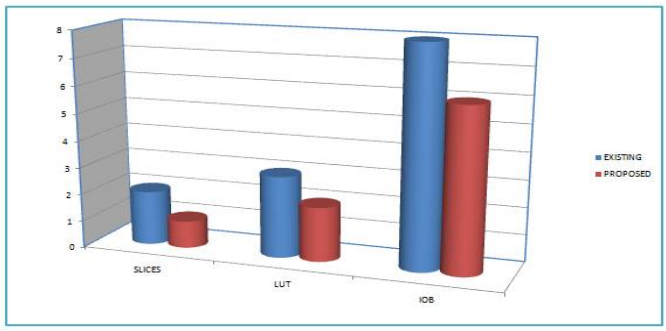


Fig. 8. performance analysis of obfuscated method

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

D. Simulation Result

The simulation result of existing obfuscated circuit in Fig.9,shows,when the correct key is given to an circuit then only output is generated by the circuit using OC.

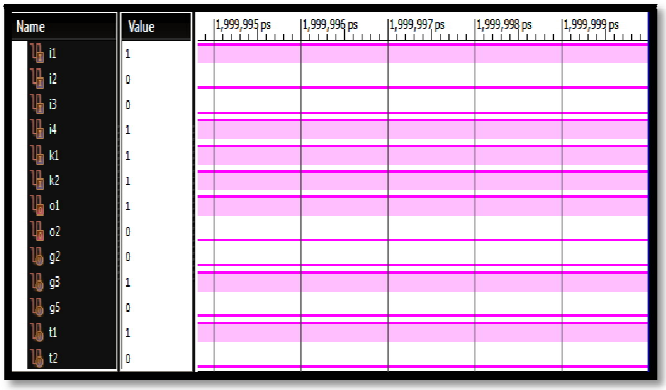


Fig.9.Simulation Result of existing obfuscated circuit

The simulation result of our proposed system in Fig.10.shows the Two level masking security using Pseudo Random Generator(PRNG).

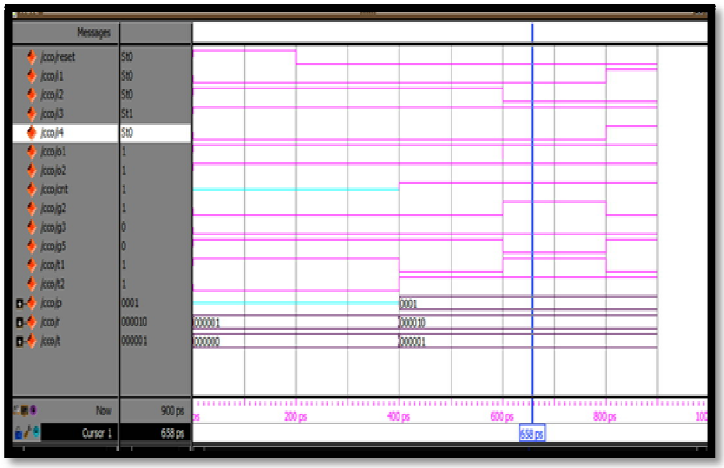


Fig.10.Simulation Result of proposed obfuscated circuit with pseudorandom generator

V. CONCLUSION

Logic obfuscation is weak when the inserted key-gates are isolated or their effect can be muted. If mutable gates are employed, then the attacker is able to determine the key bits within a second. However, it can be strengthened by inserting key-gates with random masking generators such that their effects are not mutable . our proposed obfuscation technique in this brief not only resists image processing-based RE but also incurs low area and power overheads. A PUF response can be used to XOR with the configuration of OCs to generate a device-dependent license to prevent piracy and overbuilding attacks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Special Issue 1, March 2017

REFERENCES

[1] Jiliang Zhang,"A Practical Logic Technique for Hardware security,"*IEEETrans.Very Large Scale Integr.* (VLSI)*syst.*,vol.24,no.3,pp.1193-1197,Feb 2016.

[2] Yingjie Lao, Bo Yuan, Chris H. Kim , and Keshab K. Parhi , " Reliable PUF-based Local Authentication with Self-Correction, IEEE *Transactions on Computer-Aided Design of Integrated Circuits and Systems*,vol. 12, no. 5, pp. 1120-1130, Jun 2016.

[3] Muhammad Yasin *and Ozgur Sinanoglu* , " Transforming Between Logic Locking and IC Camouflaging," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*,vol. 28, no. 8, pp. 978-981, 2015.

[4] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "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, 2015.

[5] *Srivatsan Chellappa, and Lawrence T. Clark* , " SRAM-Based Uniqe Chip Identifier Techniques, " IEEE *Transactions on very, large scale integration* (vlsi) *systems*,vol. 12, no. 5, pp. 1137–1150, oct .2015.

[6] Muhammad Yasin , A.Ozgur Sinanoglu, Jeyavijayan (JV) Rajendran, and Ramesh Karri , " On Improving the Security of Logic Locking , IEEE *Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 11, no. 6, pp. 870-890, Jun 2015.

[7] Y. Lao and K. K. Parhi, "Obfuscating DSP circuits via high-level transformations," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*,vol. 23, no. 5, pp. 819–830, May 2015.

[8] Florent Bruguier, Pascal Benoit, Lionel Torres, Lyonel Barthe, Morgan Bourree,and Victor Lomne, "Cost-Effective Design Strategies for Securing Embedded Processors, IEEE *Transactions on Emerging Topics in Computing*,vol. 8, no. 9, pp. 1150-1180 sep 2014.

[9] Koushanfar,Y. Lao and K. K. Parhi "Provably secure active IC metering avoidance and digital rights management," *IEEE Trans.Inf Forensics Security, vol. 7, no. 1, pp. 51–63, Feb.* 2014.

[10] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, " Security analysis of integrated circuit camouflaging," in *Proc. ACM/SIGSAC Conf. Comput. Commun. Secur.* 2013, pp. 709–720.

[11] L.W. Chow, J. P. Baukus, B. J. Wang, and R. P. Cocchi, "Camouflaging standard cell based integrated circuit," U . S. Patent 8 151 235, Apr. 3, 2012.

[12] R. Torrance and D. James, "The state - of - the - art in Semiconductor reverse engineering ," in *Proc . 48th ACM/EDAC/IEEE Design Autom.Conf. (DAC)*, Jun. 2011, pp. 333–338.

[13]R.S.Chakraborty and S. Bhunia, "HARPOON: An Obfuscation based SoC design methodology forhardware protection," *IEEE Trans. Comput. -Aided Design Integr. Circuits Syst., vol. 28, no. 10*,pp.1493–1502, Oct. 2009.

[14] J. A. Roy, F. Koushanfar, and I. L. Markov , " EPIC : Ending piracy of integrated circuits," in *Proc. Design, Autom. Test Eur.*, 2008, pp. 1069–1074.

[15] Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote activation of ICs for piracy prevention and digital right management," in *Proc. IEEE/ACMInt. Conf. Comput.- Aided Design*, Nov. 2007, pp. 674–677.