Journal of Critical Reviews

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

A SURVEY ON PHYSICAL UNCLONABLE FUNCTIONS AGAINST COUNTERFEITING IN SEMICONDUCTOR SUPPLY CHAIN

Kurra Anil Kumar[1], Nelakuditi Usha Rani[2]

[1]Department of Electronics and Communication Engineering
[2]Vignans foundation for science Technology & Research University, Vadlamudi-522213, Andhra Pradesh,India
Email : kakumar94@gmail.com[1] , usharani.nsai@gmail.com[2]

Received: 01.01.2020 ***Revised: 03.02.2020*** ***Accepted: 05.03.2020***

Abstract
In recent years, hardware security becomes the biggest concern in the semiconductor manufacturing community, due to enormous increasing the fabrication cost of Integrated circuits which raises several issues like cloning, overbuilding of ICs, IC piracy etc. Hence to combat these vulnerabilities, a set of techniques has been proposed like hardware watermarking, fingerprinting, PUFs, etc. this paper mainly addresses the importance of physical unclonable and gives the significance of the strong PUFs and weak PUFs in detecting and identifying the cloned and overproduced ICs.

keywords: Hardware security, Physical unclonable functions, hardware watermarking.

DOI: http://dx.doi.org/10.31838/jcr.07.04.477

INTRODUCTION

As the globalization of the semiconductor industry, the cost and complexity of fabrication of Integrated Circuits(ICs) are increase enormously. As a results, numerous set of global companies offshore their designs to the other countries where the labour cost and production values are cheaper. Hence it is clearly evident that this niti-gritty at the bottom level rise to many security issues. Especially issues like Overbuilding, cloning, piracy and Tamper are the major problems, which constantly affecting the economy of the global semiconductor supply chain and also impacting the authentication and security[1]. Figure 1 depicts the pitfalls in the fabrication of IC in the semiconductor supply chain.

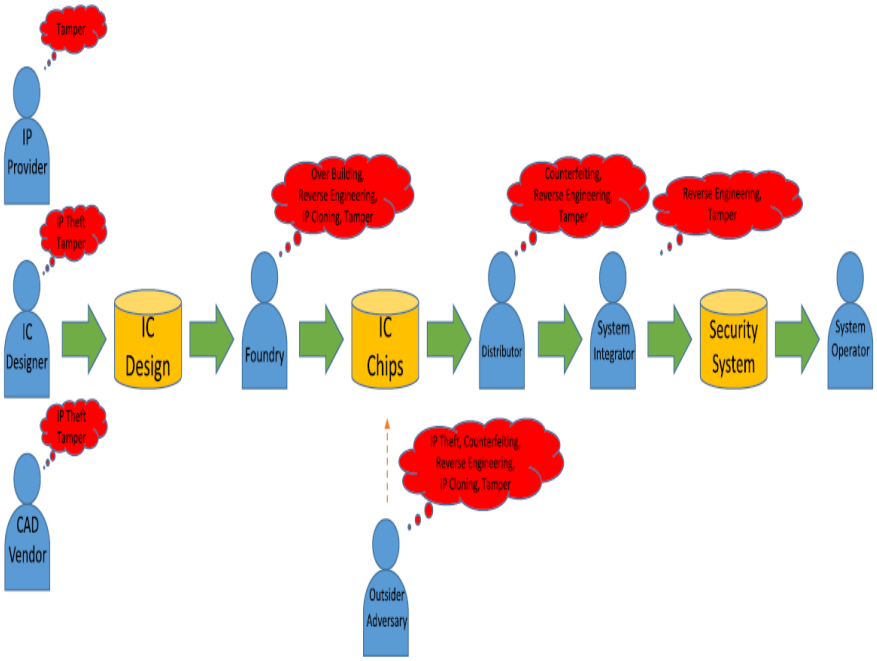

Figure 1: semiconductor supply chain risks.

In order to mitigate these vulnerabilities, there are many techniques has proposed like watermarking, fingerprinting, Physical Unclonable Functions(PUFs), formal verification, obfuscation, etc. The kind of security risks is varied from phase to phase. The counterfeit mechanism is used to identify the issues in each phase are indicated by the table1, respectively[2-3]. Out of these several counterfeiting techniques, physical unclonable functions are one of the technique which is widely and effectively used to control and counterpart the secure vulnerabilities like overbuilding and cloning of integrated circuits. The rest of the paper is organized like section 2 describes the importance of PUF and its characteristics, and section 3 explores the different classification of PUFs and its significance and finally, section 4 concludes the summary of PUFs.

Table 1: Supply chain security risks and Mitigation techniques.

Security risks	Mitigation Techniques
Over-building	Watermarking, fingerprinting, Physical Unclonable Functions(PUFs)
Cloning	Physical Unclonable Functions(PUFs), Watermarking, fingerprinting.
Tamper(IC Design)	Formal verification, detection, obfuscation

PHYSICAL UNCLONABLE FUNCTIONS

The concept of PUF has been introduced by Pappu in the year 2001. During the fabrication of Integrated circuits by utilizing the uncontrollable and unavoidable process variations at the nanoscale level it generates the secret keys. These keys are mainly generated due to the process variations, and by utilizing those keys, we can easily identify whether the device is cloned or overbuild. Any PUF circuit is triggered by the set of stimuli such as the input and the output generated from PUF is called the response. Respectively. Figure 2 depicts the mechanism of applying the input and response generated from the PUF[4-6]. Mathematically, PUFs are irreversible (one way) probabilistic challenge(C_i)-response (R_i) functions and can be expressed by (1).$PUF \equiv C_i \leftarrow R_i : \forall_i \leftarrow [0,1]^*$

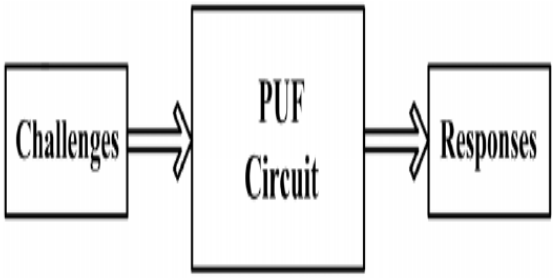

Figure 2: Challenge response mechanism in PUFs.

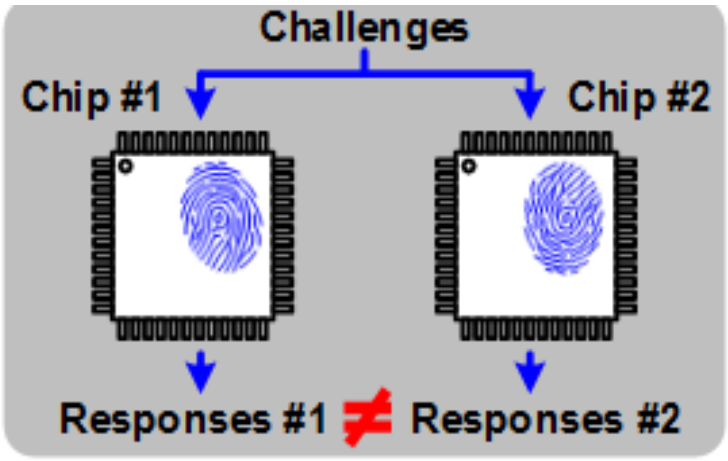

Figure 3.CRP behaviour of ICs

The kind of applying each challenge to the PUF even though it is the same the response generated from the IC is quite unique and unpredictable. Hence in a short form the each IC will act as a device fingerprint, and figure 2 depicts the CRP behaviour of the ICs. The type of variations that occurred in each IC can be mainly divided into two types, such as technology parameters and Non-technology parameters. technology parameters occur during fabrication of ICs which is unavoidable and uncontrollable, on the other hand, Non-technology parameters which are inherent and depends on voltage(V) and temperature(T) respectively[7]. "PUF response is always a characteristic function of Integrated Circuit(IC) and not possible to clone the exact device with same characteristics. The stored on physical chip parameters leads to remarkable security advantages and More importantly, the behaviour of each PUF should be dynamic and unique nature"[8].

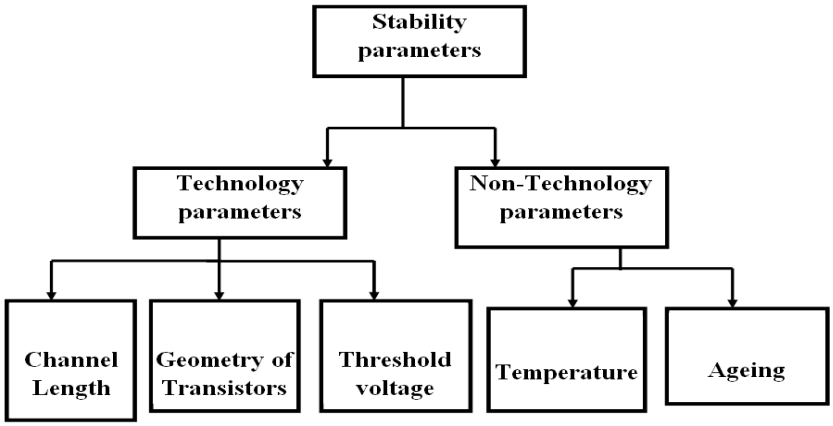

Figure 4: Classification of process variations in ICs.

Classification of PUFs

Depending upon the applied set of challenges and generated set of responses, PUFs has been broadly classified into two types such as the strong PUFs and weak PUFs. Strong PUfs are the PUFs having the large set of CRPs and susceptible to the invasive attacks and on the other hand weak PUFs are the PUFs having the limited set of CRPs and which are not affected by any kind of attacks. Table 2 represents the basic differences between strong PUFs and weak PUFs, respectively[9-10].

Table 2: Representation of PUFs based on CRPs

WEAK PUFS	STRONG PUFS
Limited number of CRPs	Large number of CRPs
Responses are stable from noise and environment variations for multiple readings	Response generated from an each challenge could be strong enough to environmental variations (better reliability).
Output response should be preserve private	No restriction to preserve the output response
Susceptible to invasive attacks	Not susceptible any attacks
Response is strong enough and depends on intrinsic process variations.	Not feasible to manufacture two PUFs with the same responses
Example: Anderson PUF	Example: Memory based PUFs, delay based PUFs.

In this section, we are going to give a brief overview of the strong PUFs such as arbiter PUF and ring oscillator PUF. An Arbiter PUFs are more generally timing-based PUFs and it's having exponential number of challenges. The basic architecture of the arbiter PUF consists of an N number of switching elements which are connected cascaded with each other, the switching block consists of two inputs and two outputs based on applied challenge and internal process variations, the response could be transfer either straight or cross, and an arbiter should be connected at the final stage of the delay network which decides the final response based on settling time of the input to the arbiter. It was recognized that the response could be estimated by summing up the delays at individual stages by using the additive linear delay model. Figure 5 illustrates the basic architecture of the arbiter PUF[9].

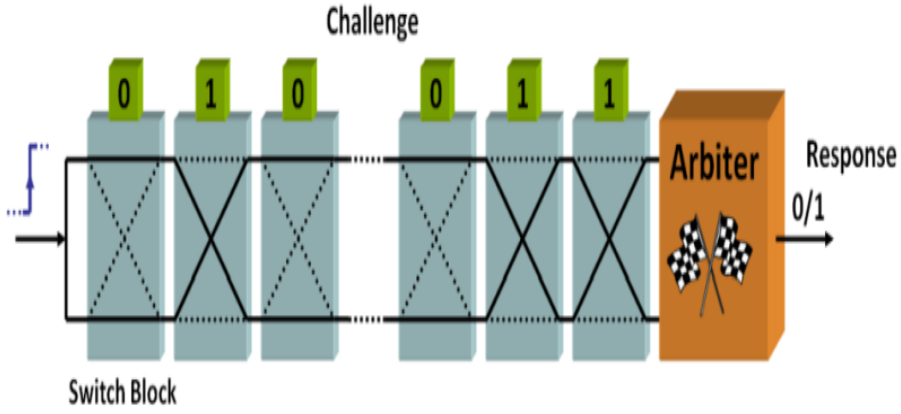

Figure 5 : Basic arbiter PUF architecture.

On the other hand, ring oscillator, PUF is another class of strong PUFs. It can use different approaches to measure the uncontrollable random variations. The architecture mainly consists of the three blocks such as delay line, edge detector and counter. The final response of the delay line is feedback to the input, which creates an asynchronous oscillating loop. The frequency of the oscillator is accurately measured by using the delay line. And the frequency could be altered at each and every iteration due to its random nature even it is sensed by using the edge detector and counter. Edge detector can be used to detect the edges of the periodic oscillations and counter can count the total number of oscillations over a period of time, respectively. Figure 6 depicts the basic architecture of the ring oscillator PUF[11-12].

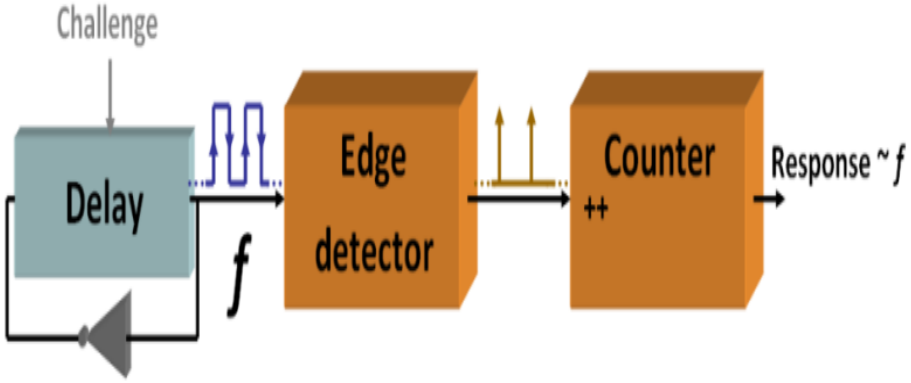

Figure 6: Ring oscillator PUF architecture.

CONCLUSION

Hardware security is one of the biggest concern in the hardware cryptography, especially in VLSI supply chain. Day by day, the usage of the electronics devices are increasing in a rapid rate; as a result, security is one of the primary concern. Hence to avoid and control these critical issues there are several mechanisms were proposed out of the physical unclonable functions are one of the emerging field and protects from the cloning, overproduction of illegal ICs and authentication of electronic devices respectively. In this paper we mainly focused on the strong PUFs and its importance in hardware security.

REFERENCES

1. D. Forte and A. Srivastava, "Manipulating manufacturing variations for better silicon-based Physically Unclonable Functions," in 2012 IEEE Computer Society Annual Symposium on VLSI, Aug 2012, pp. 171–176.
2. R. Kumar, S. N. Dhanuskodi, and S. Kundu, "On manufacturing aware physical design to improve the uniqueness of silicon-based physically Unclonable Functions," in 2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems, Jan 2014, pp. 381–386.
3. Sadulla, S., Anil Kumar, K., and Surendar. A.,:High secure buffer based physical unclonable functions (PUF's) for device authentication.: Telkomnika 17.1 (2019)
4. Kumar, S.S,. Guajardo, J., ; Maes, R. ; Schrijen, G.-J. ; Tuyls, P. "The butterfly PUF protecting IP on every FPGA IEEE International Workshop on Hardware-Oriented Security and Trust (HOST) PP 67 - 70 (2008)
5. Abhranil, M., Vikash Gunreddy, G., Patrick Schaumont: A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions: IACR Cryptology ePrint Archive, pp 657-659 (2011)
6. Anil Kumar, k.,Usha Rani, N., :A Decoder-Mux Based Arbiter Physical Unclonable Functions for Low Cost Security Applications: International Conference on Communication and Electronics Systems (ICCES). IEEE, (2019)
7. Kurra, Anil Kumar, and Usha Rani Nelakuditi" A Reliable Current Starved Inverter based Arbiter PUF Architecture for Iot Applications" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: PP 2249 -8958, Volume-9 Issue-1S5, December (2019).
8. Alkabani, Y., Koushanfar, F., and Potkonjak, M.: Remote activation of ICs for piracy prevention and digital right management,:in Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, ser., pp. 674–677 (2007)
9. Anil Kumar, K.,Usha Rani. N.:A secure arbiter physical unclonable functions (PUFs) for device authentication and identification.:indonesian Journal of Electrical Engineering and Informatics (IJEEI) 7(1):104-114 (2018)
10. Vallabhuni, Rajeev Ratna, et al. "Design of Comparator using 18nm FinFET Technology for Analog to Digital Converters." 2020 7th International Conference on Smart Structures and Systems (ICSSS). IEEE, 2020.
11. Anil Kumar, K., Usha Rani N.:Design of a Reliable Current Starved Inverter Based Arbiter Physical Unclonable Functions (PUFs) for Hardware Cryptography.:Ingénierie des Systèmes d Inf. 445-454 (2019)
12. Pittala, S. K., & Rani, A. J. (2017). Design of an Energy Efficient Multiplier Using Complementary Energy Path Adiabatic Logic. *The Annals of "Dunarea de Jos "*University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics, 40(1), 27-32.