Authentication of IC based on Electromagnetic Signature

Mosabbah Mushir Ahmed, David Hely, Romain Siragusa, Nicolas Barbot, Etienne Perret, Maxime Bernier, Frédéric Garet

Authentication of IC based on Electromagnetic Signature

Mosabbah Mushir Ahmed*, David Hely*, Romain Siragusa*, Nicolas Barbot*, Etienne Perret*§,
Maxime Bernier†, Fredric Garet†
*Univ. Grenoble Alpes, LCIS, Valence, France
Email: mushir-mosabbah.ahmed@lcis.grenoble-inp.fr
§Universitaire de France, Paris, France
†University of Savoie Mont Blanc, IMEP-LAHC, Chambery, France

***Abstract*—IC Counterfeiting is becoming serious issue. The approach discussed here is to use Electromagnetic (EM) input to an IC and measure its EM input output response. The idea is to extract a signature from EM response which should be unique to one IC. The main purpose of this work is to show that it is possible to authenticate electronic chips from a non-intrusive method, based on the use of RF waves. IC authentication can be performed using Physical Unclonable Function (PUF). PUF are based on process variation inherent to semiconductor fabrication process. EM based authentication is also based on the same principle. Nevertheless, unlike PUF such a method does not need dedicated circuitry and thus may have lower cost of implementation and may be easier to industrialize. This work first focuses on FPGA which are a common target of counterfeiting. We first prove that FPGAs are sensitive to EM excitations and find the optimum configuration using a lightweight marker not as complex as PUF to optimize the sensitivity to EM excitation. Finally, a post processing is performed on the EM measurement to get the FPGA signature which is later used for authentication. The post-processing operations are being developed in order to deal with aging effects and other measurements issues commonly seen with RF measurement.**

I. Introduction

Trust in Integrated Circuits (IC) is very important since ICs are the root of the system trust. But in recent years there has been growing number of incidents related to the trust of IC. These trust issues related to the ICs have become a source of major concern in different application areas like telecommunication, medical, space, military and banking [1]. The malicious or fake ICs can cause permanent or temporary damage to the hardware platform reducing the reliability of the system. In [1] Guin et al. discussed how the counterfeit is becoming the biggest challenge for the semiconductor industry. The ICs are used in different application ranging from small industry, household products to the defense, banking and space exploration applications.

Many methods have been developed to detect and avoid the counterfeit of IC. Based on the process variation the most known and commonly used method is Physical Unclonable Function (PUF) method. It exploits the inherent variability of IC for the purpose of authentication [2]. From [3]-[4], the process variation is an inherent variability which comes during the manufacturing process of the integrated circuits. As the scale of technology in the CMOS era is going down (less than 100nm) the variability in the physics of the devices such as transistor and other elements are getting more pronounced. This process variation during the manufacturing process comes due to much reason like random dopant fluctuations (RDF), variations in the critical dimensions during lithography, variation in the gate oxide thickness etc. Intrinsic variability of an IC due to the manufacturing defects can be exploited and use to create a fingerprint for the IC, which could be used for the purpose of the authentication.

Our idea is to use electromagnetic (EM) based technique wherein a guided RF wave interacts with the physics of IC, the response of the interaction could be used to create a unique identifier for that IC which could be used for the authentication purpose. Each IC has its own unique parameters. No two ICs even built on the mask have same physical characteristics. This differentiation comes due to the manufacturing variations.

II. Guided RF approach for IC authentication

Radio Frequency (RF) is any electromagnetic wave whose frequencies extend from 3 kHz to 300 GHz. The guided RF wave utilizes the manufacturing variation features. Each IC interacts with RF input wave and produce a unique signature. Each response can be stored in a database and when required it can be used to authenticate an IC.

The guided wave traverse in the IC, a part of it reflects back and some part is absorbed or refracted. Based on the physical variations in the IC, amount of reflections, refractions and absorption differs. This difference gives each IC a unique identification. In the ICs, the amount of reflection, absorption or refraction of the input wave depend on the process variations. The process variation like lithographic defects, variation in gate oxide thickness etc. causes a variability in the physics of ICs even from the same mask. This results in a different and unique response for each IC when a guided RF wave interacts with it. This could be further utilized for the purpose of authentication.

The chip could also be interrogated using the plane waves (radar approach) but we chose to use guided waves. Guided wave is more effective in the way the amount of the power injected would be much higher than the plane wave approach. There is higher probability of loss of power when using plane wave. In radar approach the waves may interfere with the environmental noise, or it may disperse from the surface (package) of IC and not get inside the chip at all.

III. Measurement Objectives, Post-Processing and Methodology

The objective of measurement using guided RF wave is to measure as much of data when ICs interact with guided RF wave in order to highlight the differences which could be used as a signature. Some key measurement objectives are:

1) Excite the IC (in ON state) with a guided RF signal.
2) Measure the amount of transmission and reflection (S-Parameters) of the RF wave due to interaction with the IC.
3) Measure other non-linear effects coming due to the interaction of IC with RF.
4) Measure the amount of internal coupling in the IC.

After the measurement steps, the S-Parameters would be subjected to post-processing. The post-processing (Correlation, Cosine-Similarity etc.) of the data would be instrumental in getting unique response for each IC. The data obtained after the post-processing of the response could be stored in a database for future uses. We propose the following methodology, for the authentication purpose after the post-processing of results

1) Database of S-Parameter can be made for an IC of say for example 'x123' series (from a vendor A) after its manufacturing.
2) Same IC could be tested with same RF signal input during the course of its lifetime to see the correlation of the results over the course of time.
3) Another IC ('x123') from the same vendor with exact same technology, configuration and manufacturing mask (as in step i) is excited with same RF signal.
4) Values of S-Parameter are obtained of the IC (described in step (iii)), and this value is compared with the first IC value (described in step (i)).
5) Necessary post processing can be done and then it can be seen how unique are the two values, of same ICs of exact same configuration, technology and vendor.

IV. Measurement Issues to consider

The effect of measurement error and noise cannot be neglected while doing the measurements. Measurement error could cause a drift from the actual results. Similarly measurement noise can make output response very noisy and affect the efficiency of post-processing in obtaining a unique response. We must also take into account the aging of transistors and noise inside the IC. Below we have highlighted some of the key measurement issues that have to be taken into account:

1) Measurement has inevitable noises.
2) Electrical devices like Transistors are prone to many physical variations due to constant. electrical, thermal stress and noise.
3) Electrical and Thermal stresses cause reliability issues like HCI and NBTI.
4) During measurement constant electrical stress at high frequency can cause shift in the output over period of time of the same IC.
5) This variation over period cannot be ignored during the measurement and must be taken in account during post processing.

V. Future Work

As part of future work we have developed a Printed Circuit Board (PCB) for the measurement purpose as shown in Figure 1. For initial measurements we have chosen a FPGA as IC under test. For the RF input and output connections the board has SMA connectors. For line impedance matching 50 Ohms resistors are used between SMA connectors and FPGA pins.

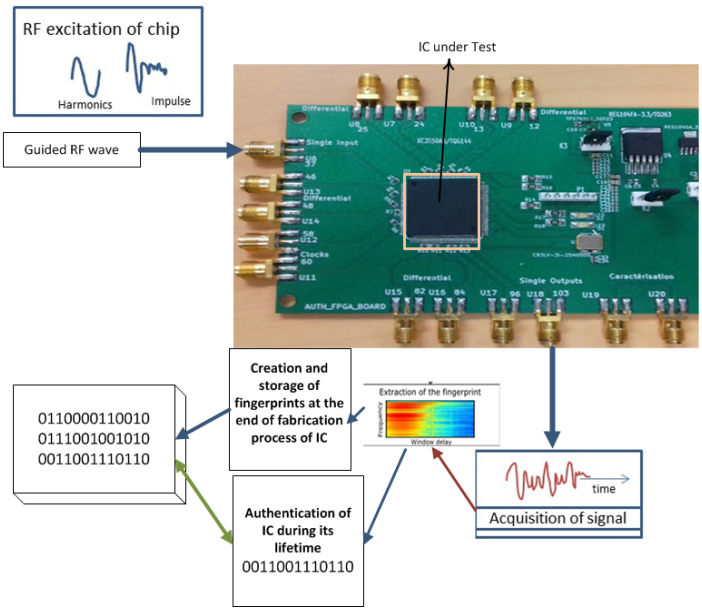

Fig. 1. Proposed hardware model of EM based authentication with a testbench. This testbench is specifically made to use RF signal as excitation to the IC.

We attempt to do repeatable measurements on a number of FPGAs and ASICs in different RF frequency ranges with different input power levels and observe the output for each case. From results obtained the required post-processing would be done to find the unique fingerprint of the IC.

References

[1] Ujjwal Guin, Student Member IEEE, Ke Huang, Member IEEE, Daniel DiMase , John M. Carulli, Jr., Senior Member IEEE , Mohammad Tehranipoor, Senior Member IEEE ,and Yiorgos Makris, Senior Member IEEE, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain" , proceedings of IEEE(volume:102, issue:8), pp 1207-1209

[2] Jim Aarestad, Philip Ortiz, Jim Plusquellic and Dhruva Acharyya, "HELP: A Hardware-Embedded Delay PUF", IEEE 2013 CEDA, SSCS and TTTC, pp 17-19

[3] Dina Kamel, "Transistor-level Design of Low-Power Nanoscale Digital Circuits for Secure Applications" July 2012, PhD Dissertation, pp 69-72

[4] Swaroop Ghosh and Kaushik Roy, "Parameter Varaition Tolerance and Error Resiliency: New Design Paradigm for the Nanoscale Era", IEEE Proceedings October 2010, pp 1718-1728.