HAL
open science

SALWARE: Salutary Hardware to design Trusted IC.

Lilian Bossuet, David Hely

To cite this version:

Lilian Bossuet, David Hely. SALWARE: Salutary Hardware to design Trusted IC.. Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE 2013, May 2013, Avignon, France. ujm-00833871

HAL Id: ujm-00833871

https://ujm.hal.science/ujm-00833871v1

Submitted on 13 Jun 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SALWARE: Salutary Hardware to design Trusted IC

Lilian Bossuet[1], David Hely[2]

[1] *Laboratoire Hubert Curien, UMR CNRS 5516*
University of Lyon, Saint-Etienne, France
Lilian.bossuet@univ-st-etienne.fr

[2] *Laboratoire de Conception et d'Intégration des Systèmes, Grenoble Institute of Technology*
F-26902, Valence cedex 9, France

***Abstract*—Fabless semiconductor industries are facing the rise of design costs of integrated circuits. This rise is link to the technology change and the complexity increasing. It follows that integrated circuits have become targets of counterfeiting and theft. The SALWARE project aims to study (theoretically and experimentally) salutary hardware design in order to fight against theft, illegal cloning and counterfeiting of integrated circuits. Salutary hardware means an embedded hardware system, hardly detectable / circumvented, inserted in an integrated circuit or a virtual component (Intellectual Property), used to provide intellectual property information (eg watermarking or hardware license) and / or to remotely activate the circuit or IP after manufacture and during use.**

***Index Terms*—salutary hardware, IP protection, IC counterfeiting, IP watermarking.**

I. Introduction

The microelectronics industry is facing increased costs of production of integrated circuits. This increase is due to the decrease in technology and the increasing complexity of systems (e.g. the transition from 32nm to 28nm technology is accompanied by a 40% increase in manufacturing costs with 300 mm wafers in diameter and a 30% increase in manufacturing costs with 450 mm wafers). For several years, this has led to a sharp increase in the number of companies with no means of production (fabless companies) and the relocation of production. In addition, integrated circuits manufactured today are produced with high added value in a highly competitive industry. Moreover, their time-to-market is increasingly tight. This makes them the targets of counterfeiting and theft.

In recent years, the issue of counterfeiting of integrated circuits has increased considerably. For example, the number of counterfeit electronic circuits collected by U.S. Customs from 2001 to 2011 has increased by around 700 [1]. Between 2007 and 2010, U.S. Customs collected 5.6 million counterfeit electronic products [2]. Overall, the estimation of counterfeiting is about 7% of the semiconductor market [3] which represents a loss of about $ 10 billion per year for the legal industry. It is therefore crucial and strategic to implement research projects to protect the intellectual property of IC designers.

To summarize the threat model of IC during manufacturing and life, Fig. 1 shows a simplified life cycle of an IC from a fabless designer to recycling. This cycle includes many threats to intellectual property from the designer: netlist theft, IP theft, mask theft, chip over-production (overbuilding), untested device theft, discarded device, reverse engineering, device counterfeiting, cloning, relabeled-repackaged-falsified "like new device".

We propose to fight against theft, illegal cloning and counterfeiting of integrated circuit by designing salutary hardware (*salware*). Salware is from the opposite of malware (malicious hardware) but can use the same technique, strategy and means. Salware means an embedded hardware system, hardly detectable, hardly circumvented, inserted in an integrated circuit or an IP, used to provide intellectual property information and/or to remotely activate the circuit or IP after manufacture and during use. IP Watermarking, PUF for IC authentication, remote activation, logic encryption, FSM encryption, memory encryption, bus encryption, hardware metering, VHDL obfuscation, bitstream encryption (FPGA), are some on the well-know salwares. In this short paper, we don't want to give a state of the art of these usual salwares. We want to discuss a new strategy to design salware by studying malware. Following section present some ideas that we want to investigate in order to find new efficient salwares.

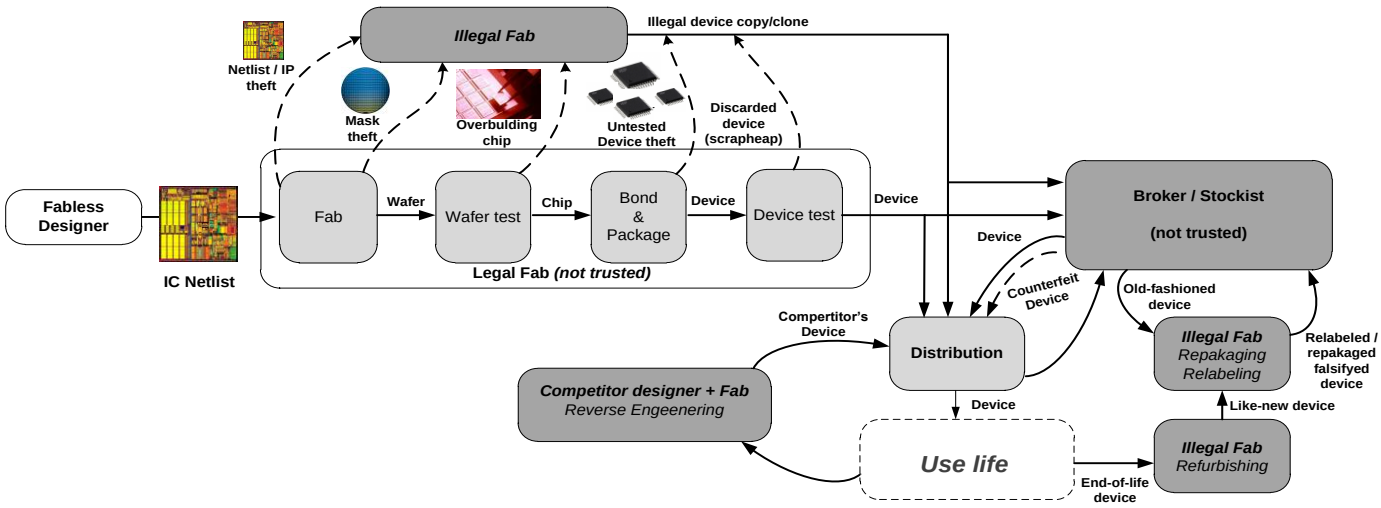

Fig. 1 - simplified life cycle of an IC from a fabless designer to recycling with threat model

II. New strategies for salware design

In the area of security, a means of attack can also be a means of protection. The techniques used to attack and to defend have always been very close. Investigating ways of attacks and malicious hardware is the strategy that we propose to develop new efficient salware. At a first glance, three options can be considered: hardware trojans, backdoors and side channels. Other means of attack / malware can be also investigated.

A. Hardware Trojan Spirit

Small, hardly detectable, hardware Trojans are able to disable a part of a device or to allow information leakage without degradation of the system performance. According to our proposed definition, such characteristics are required to design efficient salware. Embedding a Trojan inside an IP in order to protect it during evaluation was recently proposed [4]. This work proposes to modify the IP finite state machine in order to disturb the normal functional behavior of the IP. With such salware it is possible to putt an “expiry date” on the FSM control and to sell evaluation IP (temporary license). It is a time-based activation mechanism of Trojan [5], [6]. Others activation mechanism can be used to disturb the IP in case of illegal use such as expired hardware license or illegal copy. For example, a salware based on Trojan principles can use a PUF response to disturb or not an IP. Such physical-condition-based activation can permit to link an IP to a hardware implementation (hardware license).

As we have previously said, hardware Trojan can be designed to change the functionality of the infected device but also to silently leak information. Designing salware with a Trojan spirit could be a new opportunity to design IP watermarking. Watermarking techniques to fight against illegal IP copy and to allow IP traceability are already well-study. Recent study has shown that inserting watermarking during synthesis of IP netlist allows obtaining best results [7]. Embedding Trojan during the synthesis process is also an efficient way to design powerful and optimized Trojans. To conclude watermarking techniques could be efficiently improve by using Trojan mechanism to silently leak intellectual property information (mark).

Last but not least, hardware Trojan can be inserted in all location on the device: processor, hardware accelerator, memory, bus, i/o, NoC, power supply, analog part. That is really interesting to extend current works on salware which are often limited to logical gate, FSM, data-path and bus.

B. Official Backdoors

A recent work claimed that a backdoor was inserted into an FPGA [8]. This paper whipped up a storm on web before publication. Incriminated firm claimed that the inserted hardware was not malicious but salutary! This short story shown that malicious and salutary hardware are really close. Sometimes it is hard to distinguish them. Designers have to keep in mind that embedded salutary hardware could be misconstrued.

C. Side Channel Emission

The side channel attacks are well-known attacks in the field of cryptographic engineering. Most of the dynamic characteristics of both hardware and software implementation of cipher can be used for side channel analysis: the computation time, power consumption, electromagnetic radiation, optical radiation and even the produced sound during computation. The above descriptions are mainly oriented for side channel analysis. Such attack techniques can be used to read intellectual property information from the device to the verification process (watermarking checking).

Some published works proposed to use side channel as a communication channel to extract intellectual property. Thermal channel was used in [9] to allow a communication from an embedded tag to a remote receiver. Power consumption was used in [10]. Other side channel information can be efficiently used to transmit information about the IP. From example, like thermal channel, electromagnetic channel allows contactless checking. To conclude, side channels have to be used to design salware with discreet communication means.

VI. Conclusion

Investigating malicious hardware design and behavior is an opportunity to improve salutary hardware. Salware project aims at to design efficient intellectual property protection by follow this strategy. We hope to find new ways of protection, more efficient, more useful, more secure and low cost than state of the art existing protections.

References

[1] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012.

[2] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org

[3] M. Pecht, S. Tiku. Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, May 2006.

[4] Narasimhan, S.; Bhunia, S.; Chakraborty, R.S., "Hardware IP Protection During Evaluation Using Embedded Sequential Trojan," Design & Test of Computers, IEEE , vol.29, no.3, pp.70,79, June 2012

[5] Karri, R.; Rajendran, J.; Rosenfeld, K.; Tehranipoor, M., "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," Computer, vol.43, no.10, pp.39,46, Oct. 2010.

[6] Tehranipoor, M.; Koushanfar, F., "A Survey of Hardware Trojan Taxonomy and Detection," Design & Test of Computers, IEEE , vol.27, no.1, pp.10,25, Jan.-Feb. 2010

[7] B. Legal, L. Bossuet, "Automatic low-cost IP watermarking technique based on output mark insertion". Journal of Design Automation for Embedded System, Springer, Vol. 16, No. 2, pp. 71-92, June 2012.

[8] S. Skorobogatov, C. Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip". Cryptographic Hardware and Embedded Systems, CHES 2012, Springer, Lecture Notes in Computer Science Volume 7428, pp. 23-40, 2012.

[9] Marsh, C.; Kean, T.; Mclaren, D., "Protecting designs with a passive thermal tag," Electronics, Circuits and Systems, 2008. ICECS 2008. 15th IEEE International Conference on , vol., no., pp.218,221, Aug. 31 2008-Sept. 3 2008

[10] Georg T. Becker, Markus Kasper, Amir Moradi and Christof Paar, "Side-channel based watermarks for integrated circuits, " IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010.