Salutary Hardware to Design Trusted IC

Lilian Bossuet

Université de Lyon – Laboratoire Hubert Curien – UMR CNRS 5516 – Saint-Etienne, France

Ecole d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes
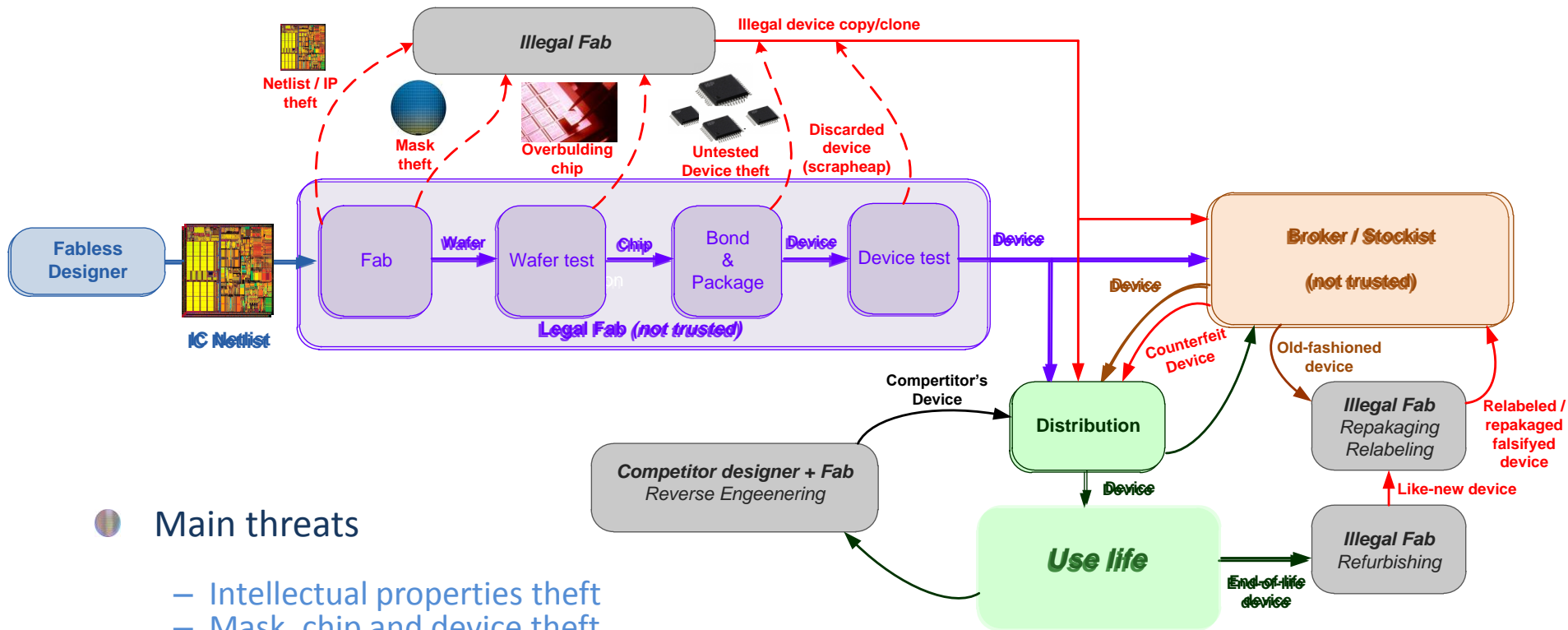
January 2014, Ottawa, Canada
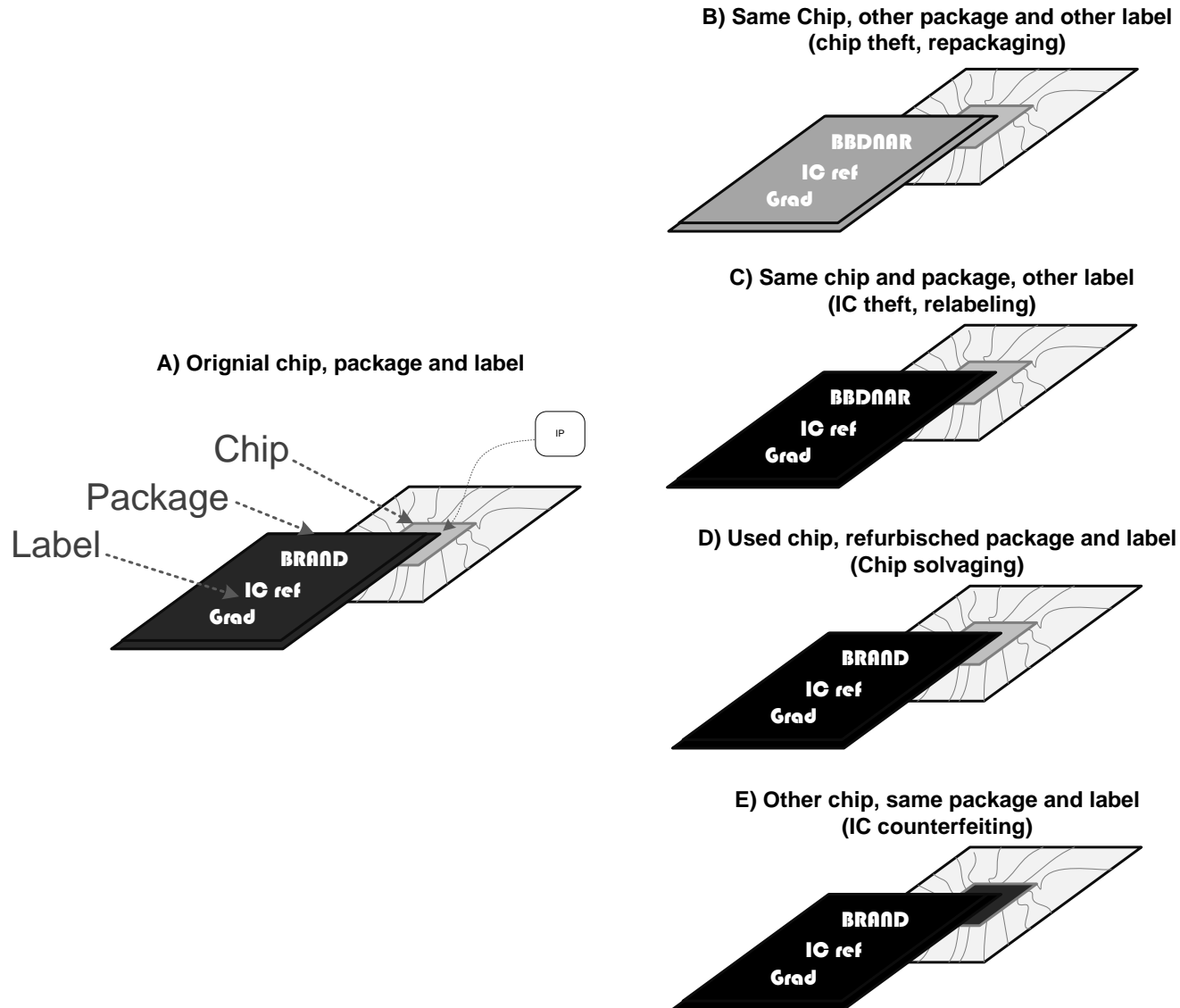
SALWARE

why ?

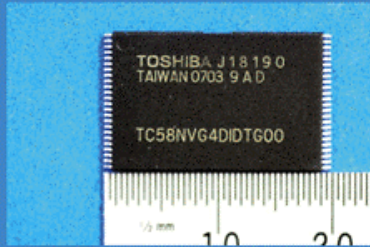# Threat model during manufacturing, supply chain and use life

Main threats

- Intellectual properties theft
- Mask, chip and device theft
- Overbuilding
- Illegal copy, cloning
- Counterfeiting
- Illegal refurbishing, repackaging, relabeling
- Reverse engineering
- Functional modifications (DRM violation, unlocking)

Definition

B) Same Chip, other package and other label (chip theft, repackaging)

BBDNAR
IC ref
Grad

C) Same chip and package, other label (IC theft, relabeling)

BBDNAR
IC ref
Grad

A) Orignial chip, package and label

Chip
Package
Label

IP

BRAND
IC ref
Grad

D) Used chip, refurbisched package and label (Chip solvaging)

BRAND
IC ref
Grad

E) Other chip, same package and label (IC counterfeiting)
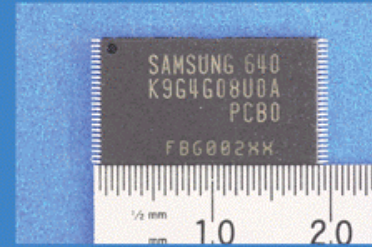
BRAND
IC ref
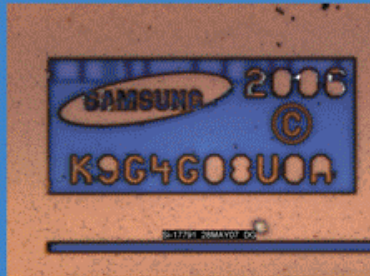Grad

Example of counterfeiting flash memory

Counterfeit Toshiba Part
Package Marking
TC58NVG4D1DTG00

Toshiba 56nm 16Gb MLC NAND
Flash Part Package Marking
TC58NVG4D1DTG00

Samsung 65nm 4Gb MLC NAND
Flash Part Package Marking
K9G4G08U0A

Counterfeit Toshiba Part
Die Markings

Toshiba 56nm 16Gb MLC NAND
Flash Part Die Markings

Samsung 65nm 4Gb MLC NAND
Flash Die Markings

One counterfeit device (left) had Toshiba markings but a Samsung die inside. You can see the actual Toshiba device markings on the second device. The Samsung die can be seen in the third image.

The rise of electronic device counteirfetings

studies [1-2]

wireless)

Nombre de références saisies

1500

1200

900

600

300

0

2001 · · · 008 · · · 2009

FIGHT AGAINST COUNTERFEITS
Setting the International Standard(s) in the

Supply & Demand Chain Executive
Special Edition/July-August 2011
Solutions-based intelligence for Supply Chain ROI
COUNTERFEIT
The Crisis
Critical strategies to meet the growing challenge

IEEE SPECTRUM
FOR THE TECHNOLOGY INSIDER
TEACHING A COPTER TO FLY ITSELF
A full-size craft goes solo P. 24
THE QUANTUM TRANSISTOR
Can it keep Moore's Law alive? P. 30
DAVID SARNOFF'S SECRET CACHE
Treasures of a remarkable life P. 42
DRONES INVADE BURNING MAN
Read about them at SPECTRUM.IEEE.ORG
FAKE
Scavenged chips passed off as new are cropping up in U.S. military equipment. Are they in passenger jets and cars, too? P.36
IEEE

BOGUS!
ELECTRONIC MANUFACTURING AND CONSUMERS CONFRONT A RISING TIDE OF COUNTERFEIT ELECTRONICS
By Michael Pecht & Sanjay Tiku

EE Times
CMP
Fake NEC company found, says report
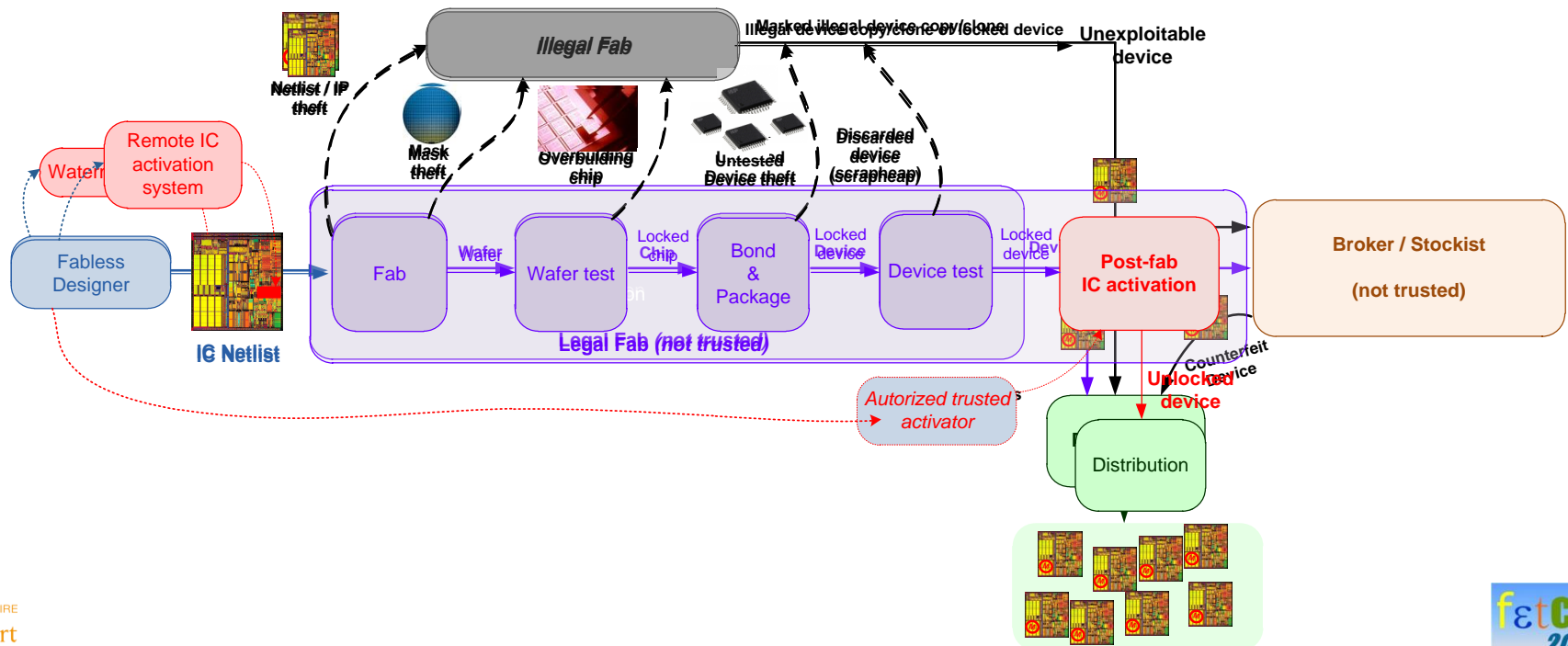
SALWARE

what ?

Salutary hardware to design trusted IC

- SALWARE definition

  Salutary hardware (SALWARE) is a (small piece of) hardware system, hardly detectable (from the attacker point of view), hardly circumvented (from the attacker point of view), inserted in an integrated circuit or an IP, used to provide intellectual property information and/or to remotely activate the integrated circuit or IP after manufacture and/or during use.

Salutary hardware to design trusted IC

- **M**ALWARE definition

  Malicious hardware (MALWARE) is a (small piece of) hardware system, hardly detectable (from the user point of view), hardly circumvented (from the user point of view), inserted in an integrated circuit or an IP, used to provide attacker hidden information and/or to remotely inactivate the integrated circuit or IP after manufacture and/or during use.

- Hardware Trojan
  - Small, hardly detectable
  - Disable a part of a device => remote activation
  - Information leakage => IP watermarking
  - Time-based activation mechanism => IP expire date (temporary license)
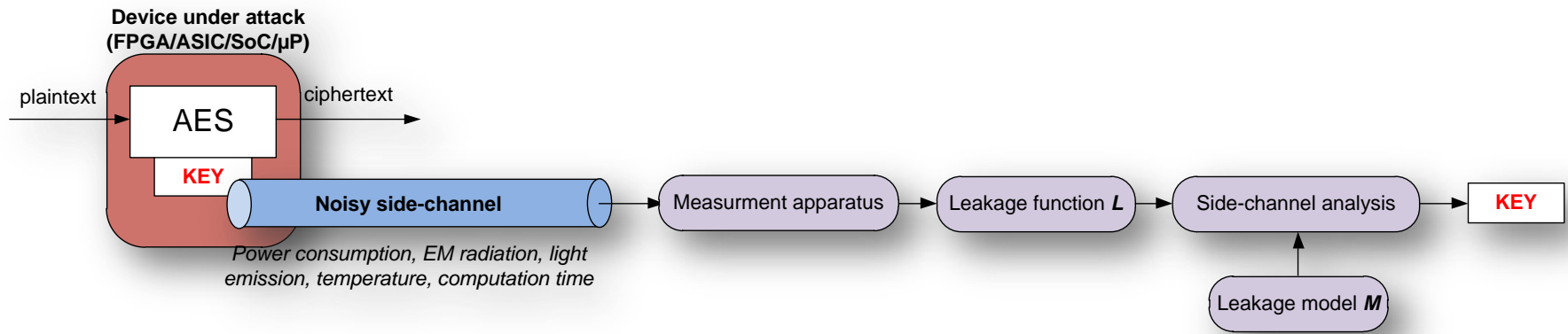
- Backdoors
  - Malicious / salutary ???

- Side channel
  - Typical SCA attacks on cipher => IP watermarking
  - Trojan detection

Side-channel attacks

- Side-channel key recovery (side-channel)
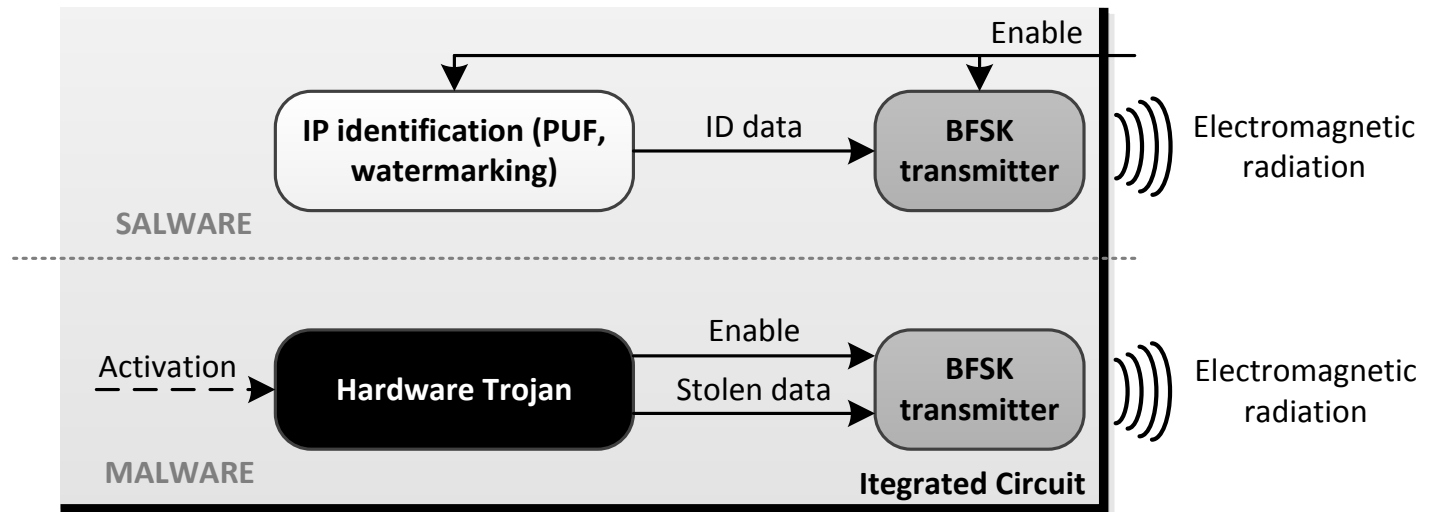 - Attacker aims to get back the secret key

Device under attack (FPGA/ASIC/SoC/µP)

plaintext → AES → ciphertext

KEY

Noisy side-channel

Power consumption, EM radiation, light emission, temperature, computation time

Measurment apparatus → Leakage function *L* → Side-channel analysis → KEY

Leakage model *M*

Example

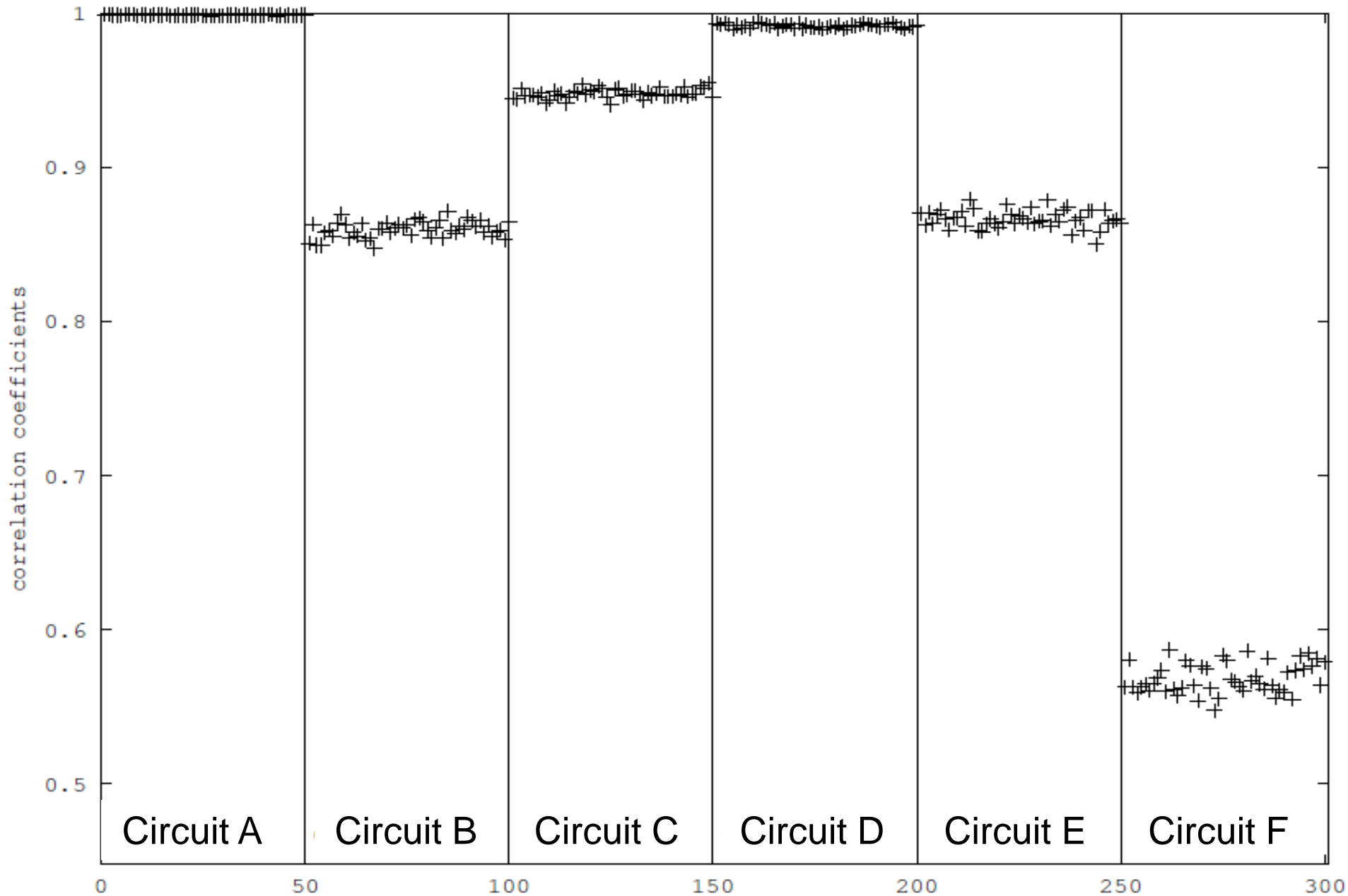- Side channel used to IP protection
  - IP information transmission
    - ID (from PUF)
    - Watermark

- Side channel to send IP watermarking
  - EM Channel (contactless, local)
  - BFSK transmitter (logical)
    - 200 / 300 Mhz
  - Adapted to FPGA implementations
    - Tests in progress
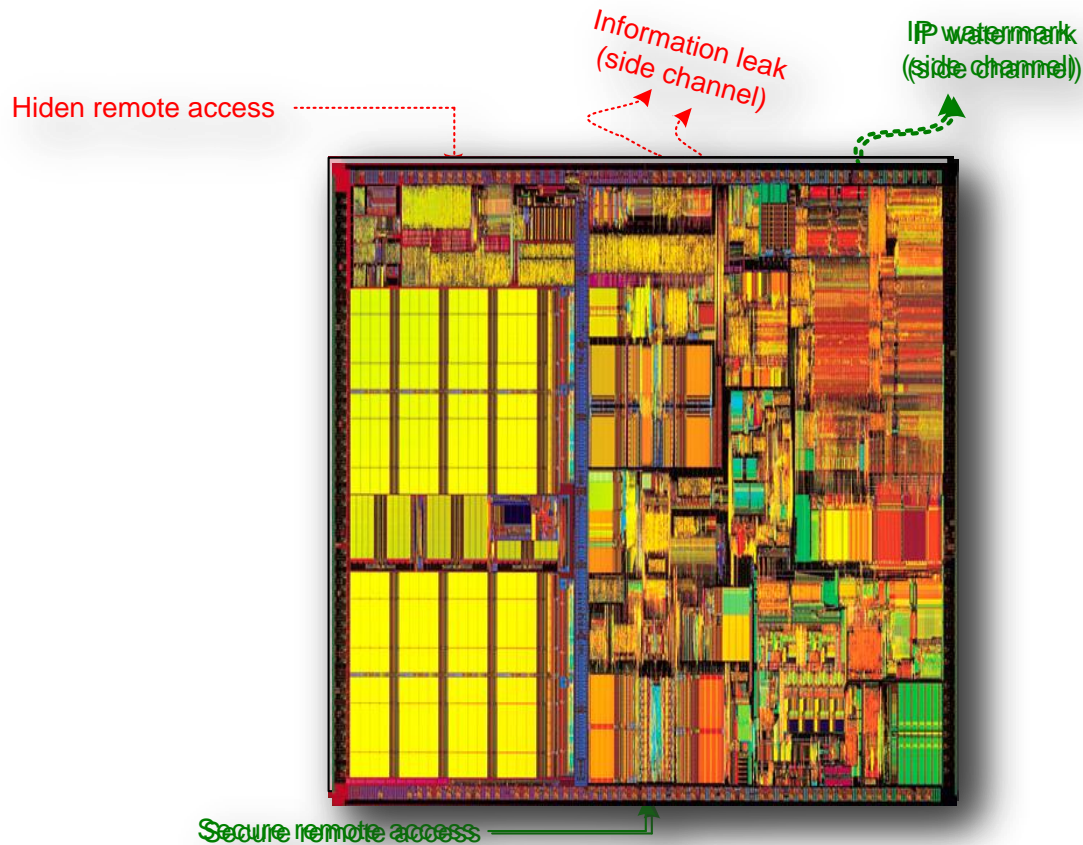   - Microsemi / Altera

Example

Salware / Malware

- *Salutary Hardware* vs *Malicious Hardware*

Hiden remote access

Information leak
(side channel)

IP watermark
(side channel)

Secure remote access

- *Investigating MALWARE design and behavior as a opportunity to improve SALWARE*
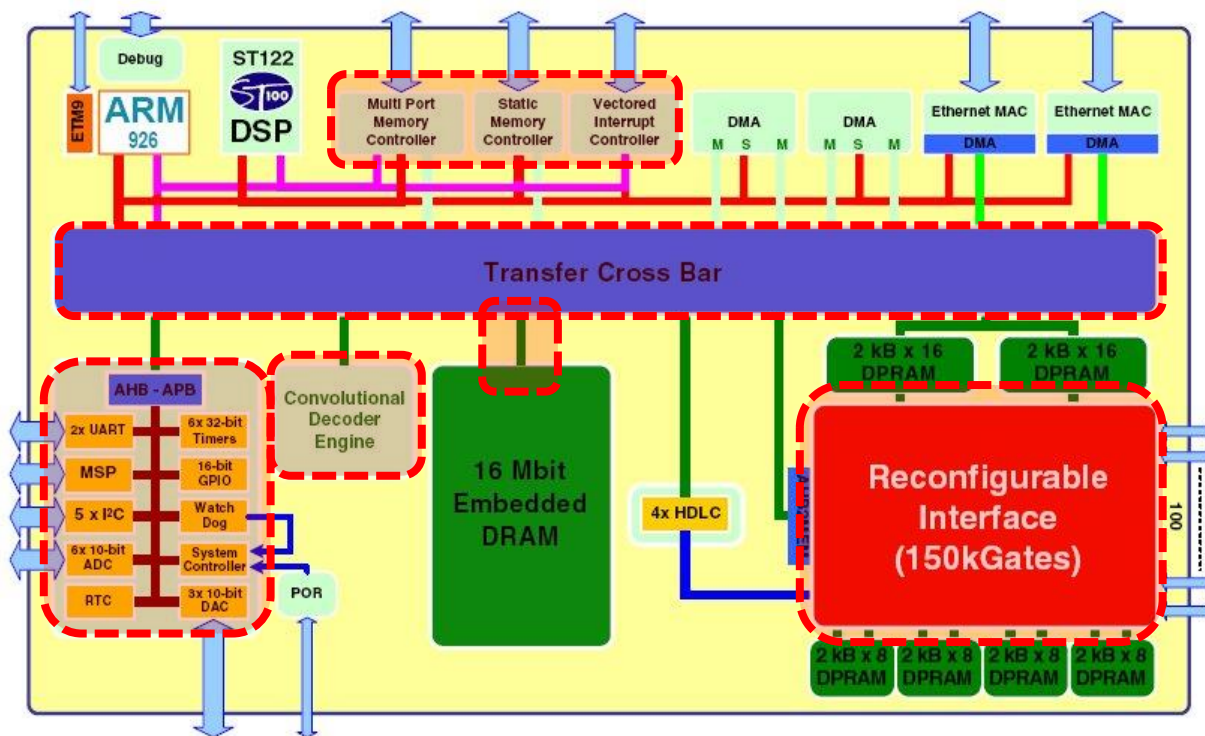
http://www.univ-st-etienne.fr/salware/
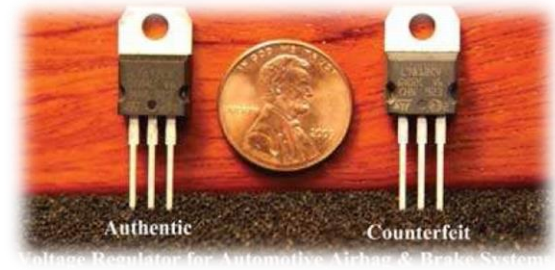
Blocage fonctionnel

- Actions de blocage dans un SoC
  - Contrôleur (FSM / interruption / mémoire)
  - Réseaux de communications internes : bus de données / Cross Bar / NoC
  - Mémoires RAM (bus @ / bus data)
  - Paramétrage/calibration (bloc analogique et mixte)
  - Configuration (eFPGA / multi-mode-IP)

Source STMicroelectronics – STW22000 microcontroller

Counterfeiting in figures

- 10 % of the global word market
  - Cost : 200 billion $ per year in USA
  - Impact : 250 000 employments loss per year in USA
- In 2008 , the number of counterfeiting seizures of the European customs was 178 million of products.
  - Watch, leather goods, article of luxury clothing, medicine, tabacco, electronics products
- Estimation of counterfeiting of the word semiconductor market is around 7% [1]
  - Financial loss of 10 billion $ per year for the word market
- From 2007 to 2010, the number of seizures of electronic devices counterfeiting of the US customs was 5.6 million [2]
  - Numerous counterfeiting of military-grade device and aerospace device [3,4]

Authentic   Counterfeit
Voltage Regulator for Automotive Airbag & Brake System

fake card   genuine card

[1] M. Pecht, S. Tiku. Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, May 2006
[2] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org
[3] S. Maynard. Trusted Foundry – Be Safe. Be Sure. Be Trusted Trusted Manufacturing of Integrated Circuits for the Department of Defenses. NDIA Manufacturing Division Meeting, October 2010
www.trustedfoundryprogram.or
[4] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012

Example

- Trojan insertion for IP protection during evaluation
  - Case Western Reserve University

  - Trojan insertion by IP's FSM modification
  - Re-synthesis of IP with Trojan
  - Time-activated Trojan
  - Trojan signature use as a digital watermarking (in case of illegal IP copy)

[1] Seetharam Narasimhan, Rajat Chakraborty, Swarup Bhunia, "Hardware IP Protection During Evaluation Using Embedded Sequential Trojan," IEEE Design & Test of Computers, 08 June 2011.