Fighting against theft, cloning and counterfeiting of integrated circuits

Lilian Bossuet

Associate Professor, head of the secure embedded system group

University of Lyon, Jean Monnet University, Saint-Etienne

Laboratoire Hubert Curien – CNRS UMR 5516

SÉMINAIRE

Confiance numérique

- Jeudi 3 mars 2016 -

Protection of the intellectual property of the fabless designers

why ?

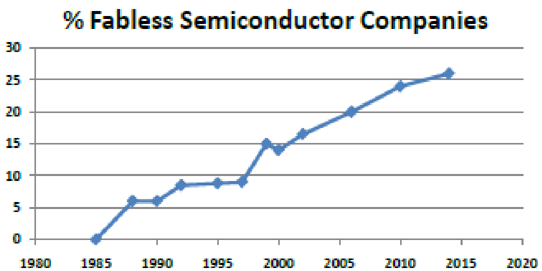
Semiconductor market

- Market increase
  - + 45% from 2009 to 2015 (336 billion of US $)
- SoC manufacturing cost rise
  - SoC complexity increase (*add value increase*)
  - +40% from 32nm (92 M€)=> to 28nm (130 M€)
  - Reduction => 30% with 450mm wafer [ITRS 2011]
- Manufacturing changes
  - Outsourcing of the manufacture and the design (mainly in Asia)
  - Fabless semiconductor companies increase
- Characteristics of counterfeiting targets
  - High add-value products
  - Rapid functional obsolescence
  - Long design time
  - Cheap ways to design counterfeiting
  - Limited risks to the counterfeiter

Taiwan Semiconductor Manufacturing Co., Ltd.

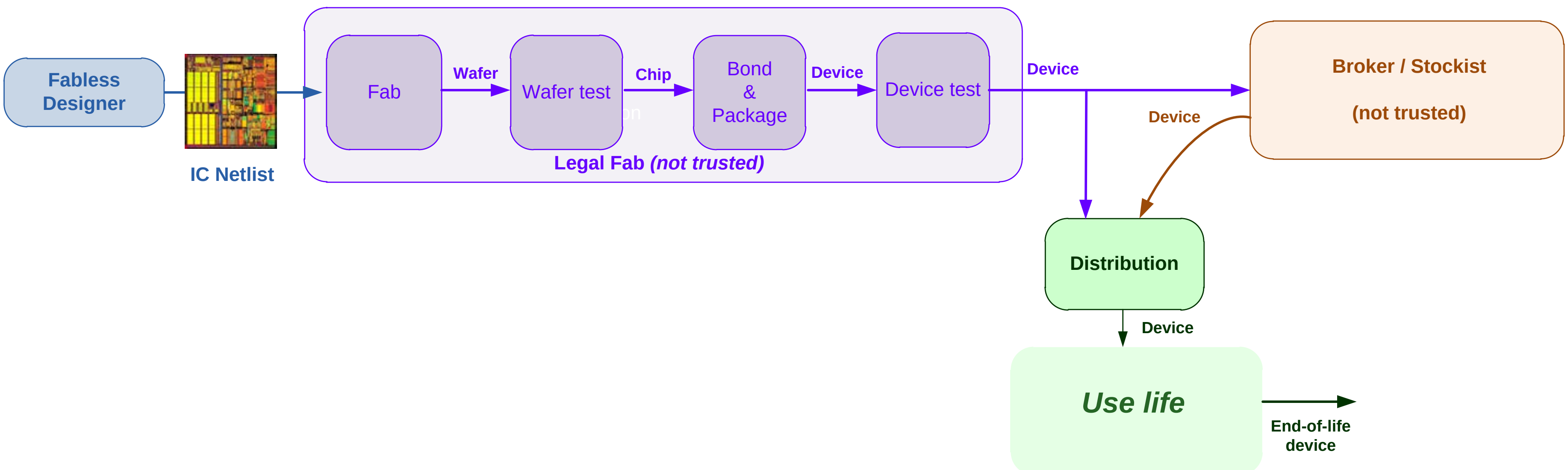
Tech.	Transistors	Manufacturing costs
130 nm	9 millions	9 millions €
90 nm	16 millions	18 millions €
65 nm	30 millions	46 millions €

Rapport Saunier, 2008

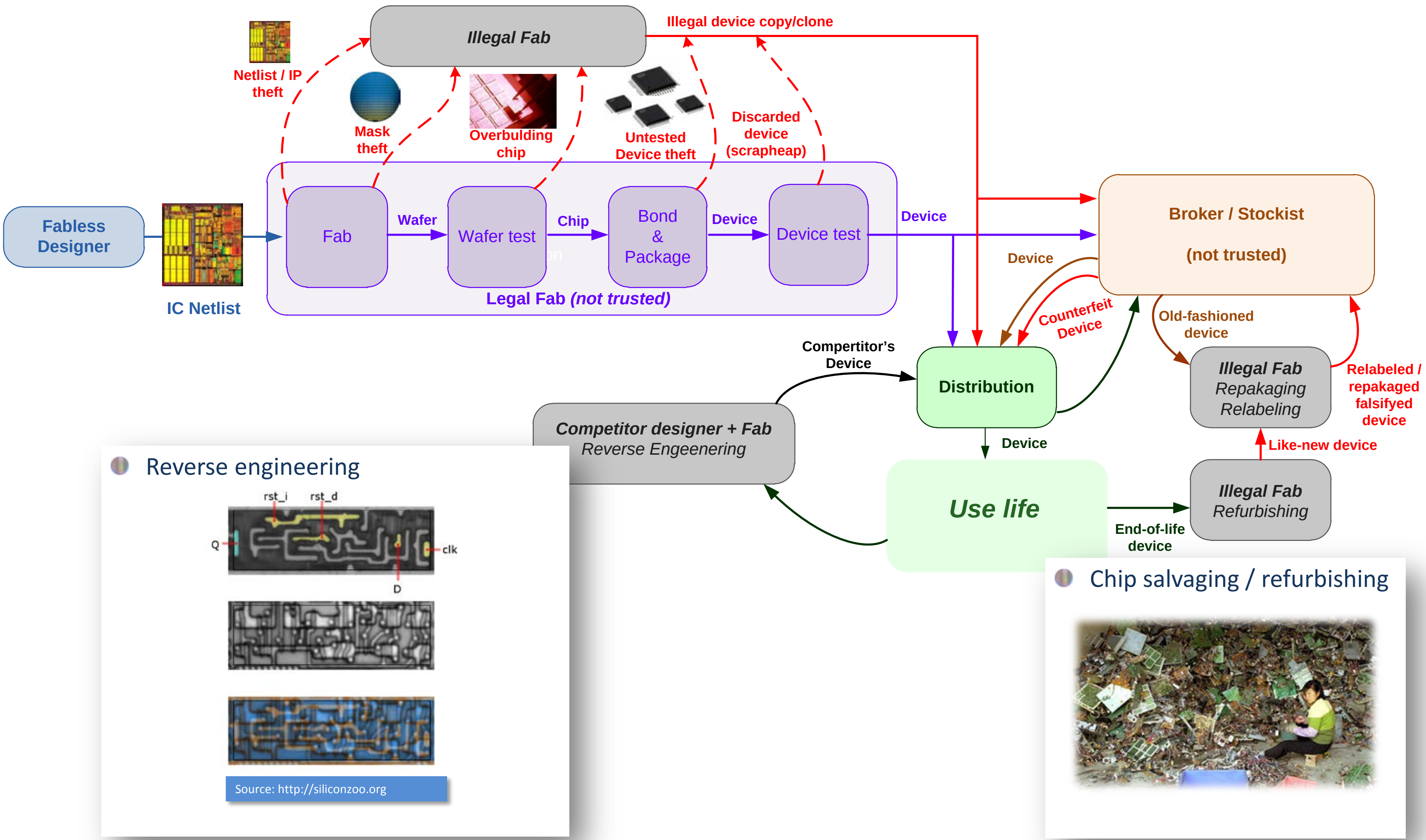


F. Koushanfar 2011

Threat model during manufacturing, supply chain and use life

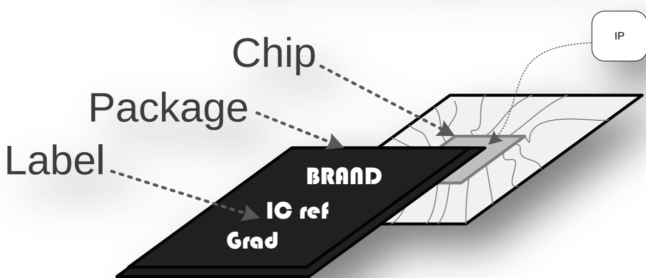


Threat model during manufacturing, supply chain and use life

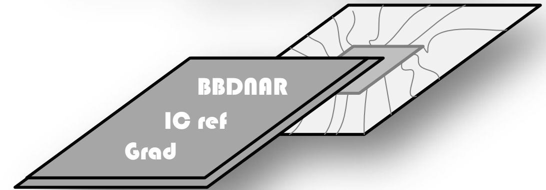


Definition

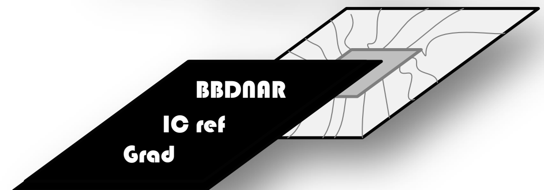
A) Orignial chip, package and label



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



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

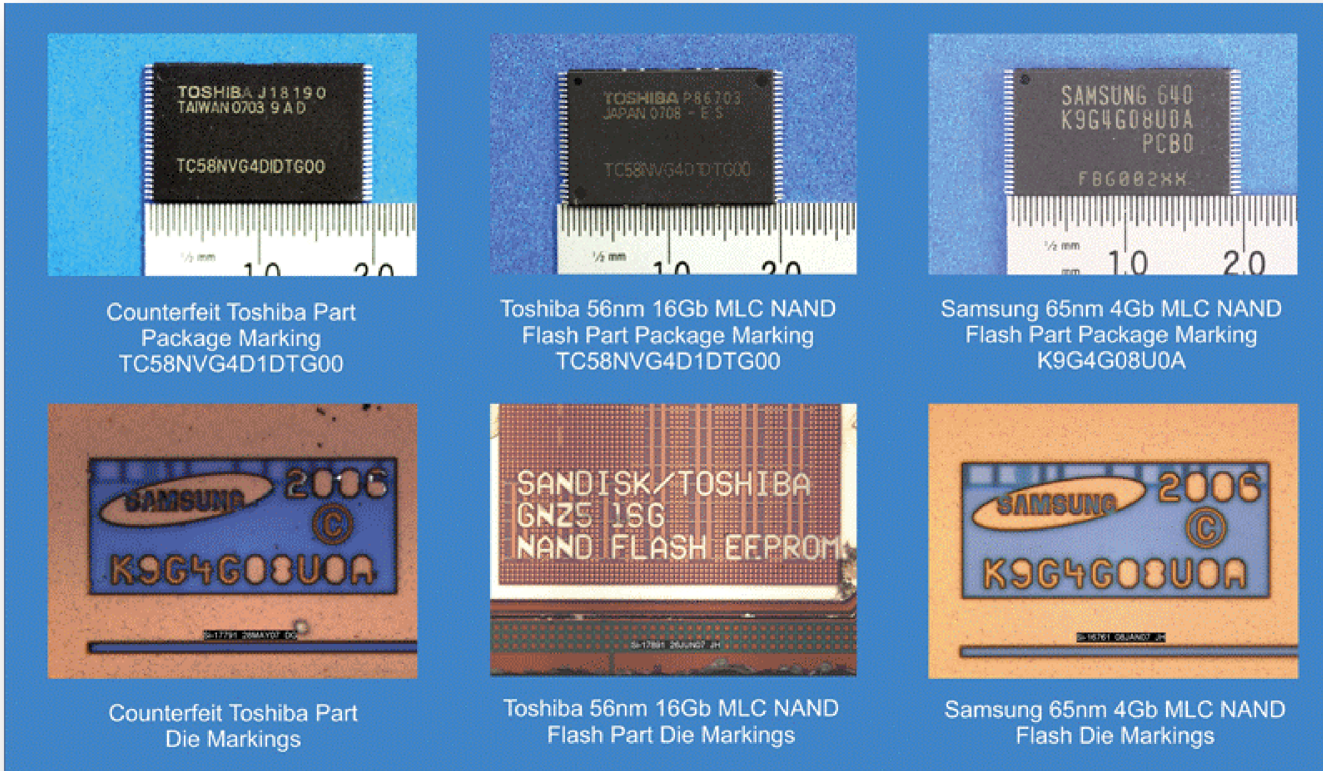


D) Used chip, refurbisched package and label
(Chip solvaging)

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

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Example of counterfeiting flash memory



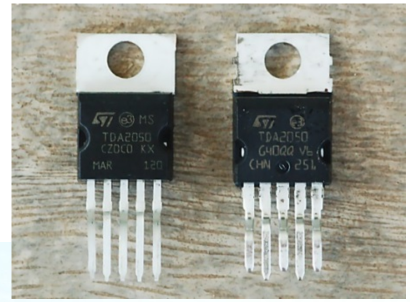
One counterfeit device (left) had Toshiba markings but a Samsung die inside. You can see the actual Toshiba device markings on the second device. The Samsung die can be seen in the third image.

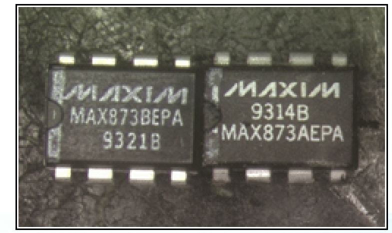
Source : EE Times, August 2007

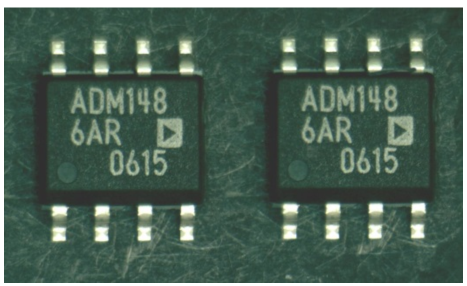
More examples ….

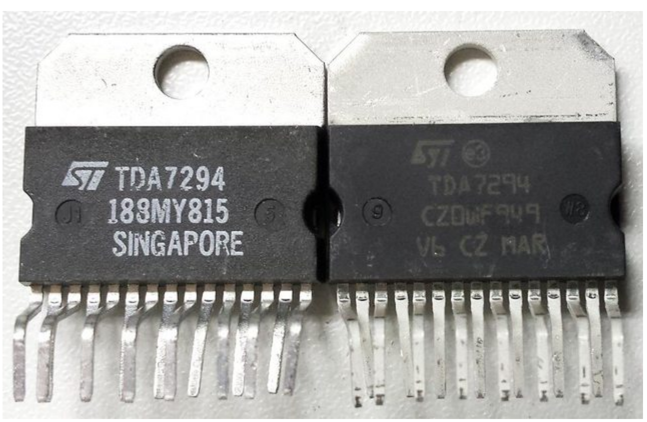
Real

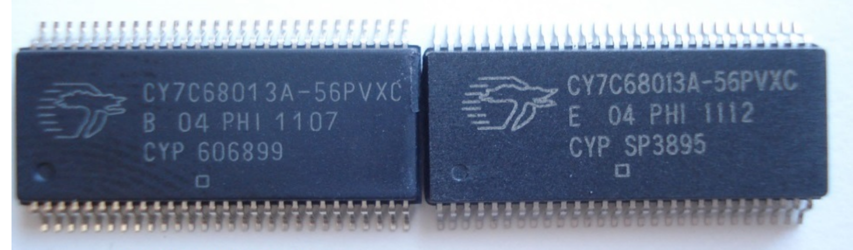
Fake





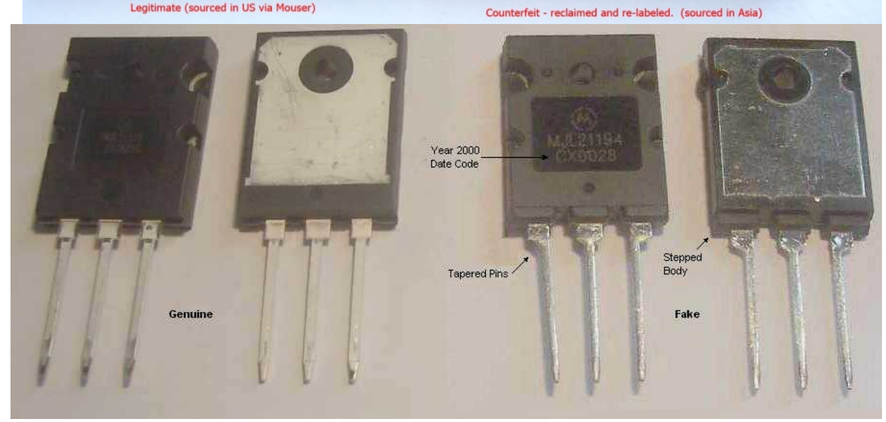






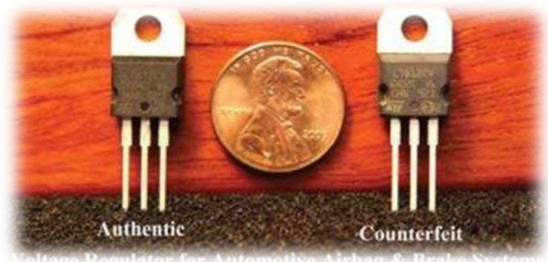
Legitimate (sourced in US via Mouser)

Counterfeit - reclaimed and re-labeled. (sourced in Asia)



Counterfeiting in figures

- In 2008 , the EU's external border control secured 178 million of counterfeit items
  - Watch, leather goods, article of luxury, clothing, pharmaceuticals, tabacco, <u>electronics products</u>



- Estimation of counterfeiting of the word semiconductor market is between 7% and 10% [1]
  - Financial loss of 23,5 billion $ in 2015 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]

[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

Amazing stories

- Fake NEC compagny
  - 2006 [1,2]
  - 50 counterfeit products (NEC or not)
    - Home entertainment systems, MP3 players, batteries, microphones, DVD players, computer peripheries …

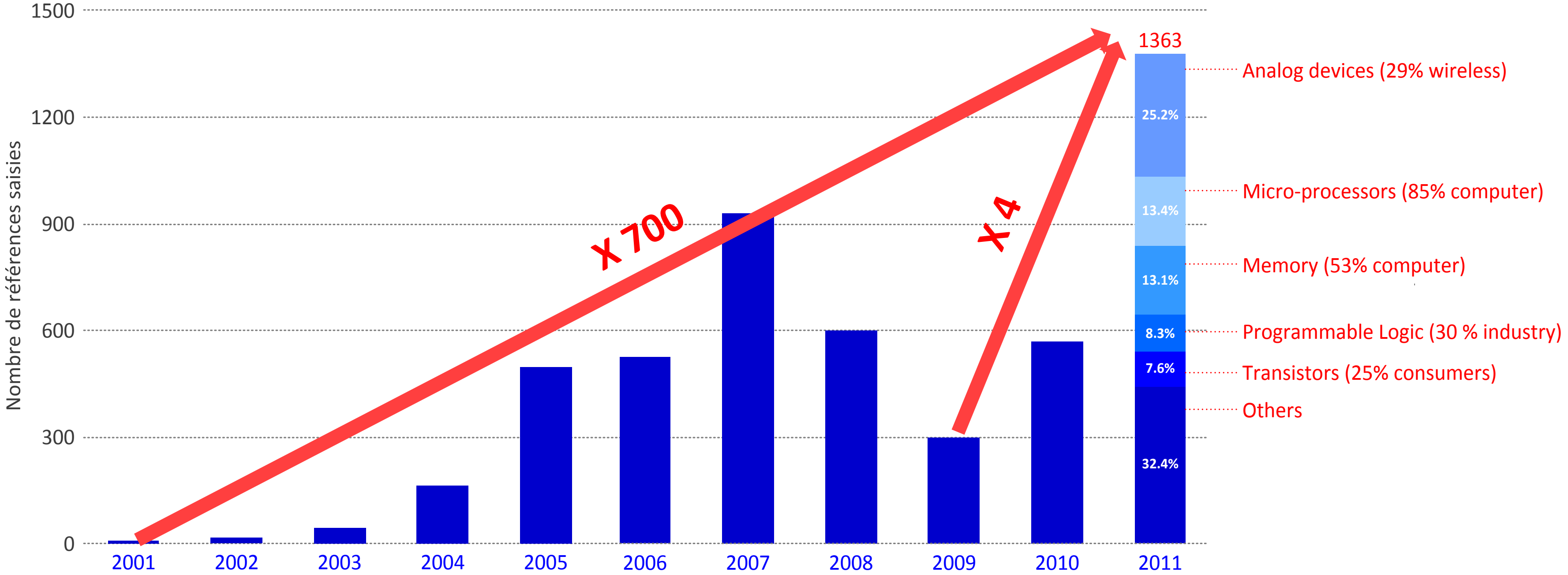
- VisonTech (USA)
  - From 2006 to 2010, VisonTech sell more than 60 000 counterfeit integrated circuits [3]
  - VisionTech customers: US Navy, Raytheon Missile System …

Advanced Micro Devices	$34,900.00
Altera	$7,611.00
Analog Devices	$75,580.66
Cypress Semiconductor	$33,446.00
Freescale	$40,021.00
Infineon Technologies	$10,036.00
Intel	$100,889.50
Intersil	$1,857.30
Linear Technology	$32,018.75
Maxim	$1,596.34
Mitel	$2,645.93
National Semiconductor	$5,943.80
NEC	$24,842.07
Peregrine Semiconductor	$2,640.00
Philips Electronics	$1,639.50
Renesas	$2,400.00
Samsung Electronics America	$77,165.00
STMicroelectronics	$18,619.21
Texas Instruments	$92,899.58
Toshiba	$2,424.00
Xilinx	$22,235.76
Total	$591,411.40

[1] Next Step for Counterfeiters: Faking the Whole Compagny, New York Times, May 2006 http://www.nytimes.com/2006/05/01/technology/01pirate.html?pagewanted=all
[2] Fake NEC compagny, says report, EE Times, April 2006 http://www.eetimes.com/electronics-news/4060352/Fake-NEC-company-found-says-report
[3] http://eetimes.com/electronics-news/4229964/Chip-counterfeiting-case-exposes-defense-supply-chain-flaw

The rise of electronic device counteirfetings

- Target and evolution
  - From US statistical studies [1-2]



[1] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012
[2] IHS-ERAI http://www.ihs.com/info/sc/a/combating-counterfeits/index.aspx

The rise of electronic device counteirfetings

[1] C. G... IEEE Spectrum, June 20...
[2] IHS-... ...ihs.com/info/sc/a/combating-counterfeits/...

Consequences of electronic products counterfeiting

- Economic damage
  - For legal provider: money losses
  - For purchaser: diagnostic/repairs
    - Ex: 2,7 million of US $ for US Navy missile systems
- Social damage
  - Employment losses
- Customer dissatisfaction
- Reliability decrease
- Security not guarantee
  - Potential malware insertion (hardware trojan)
- Environmental pollution
  - Non-compliance with legal standards

CURRENT INDUSTRIAL SOLUTIONS 1/2

Counterfeiting physical detection

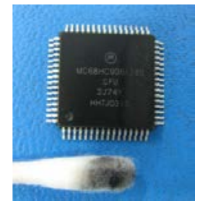
Counterfeiting physical detection

- Industrial means of detection
  - Marking permanency testing, visual inspection

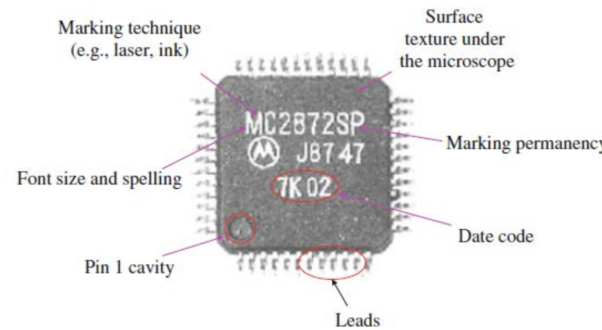
Before

After

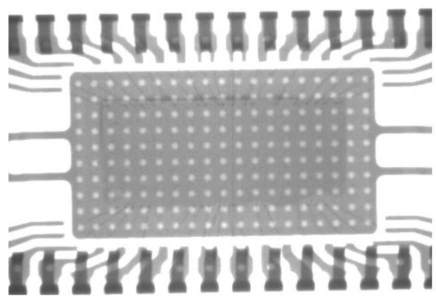
Fake Atmel

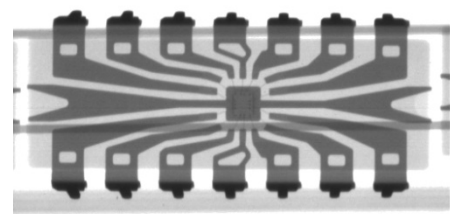


Fake Motorola

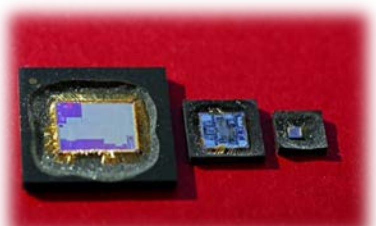


  - X-ray inspection



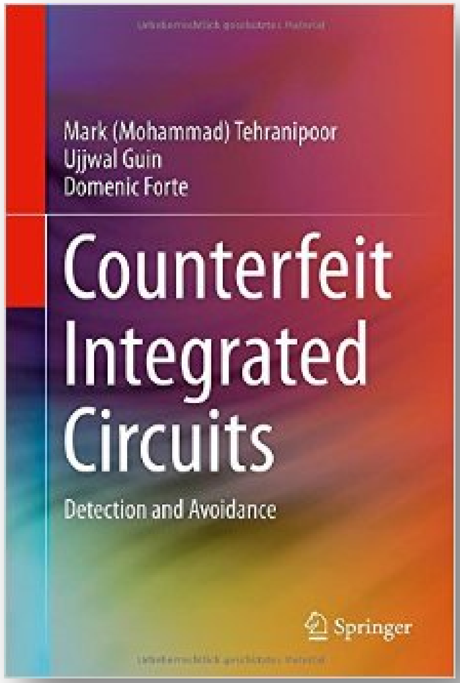


  - Unpackaging and high resolution optical inspection (reverse-engineering)



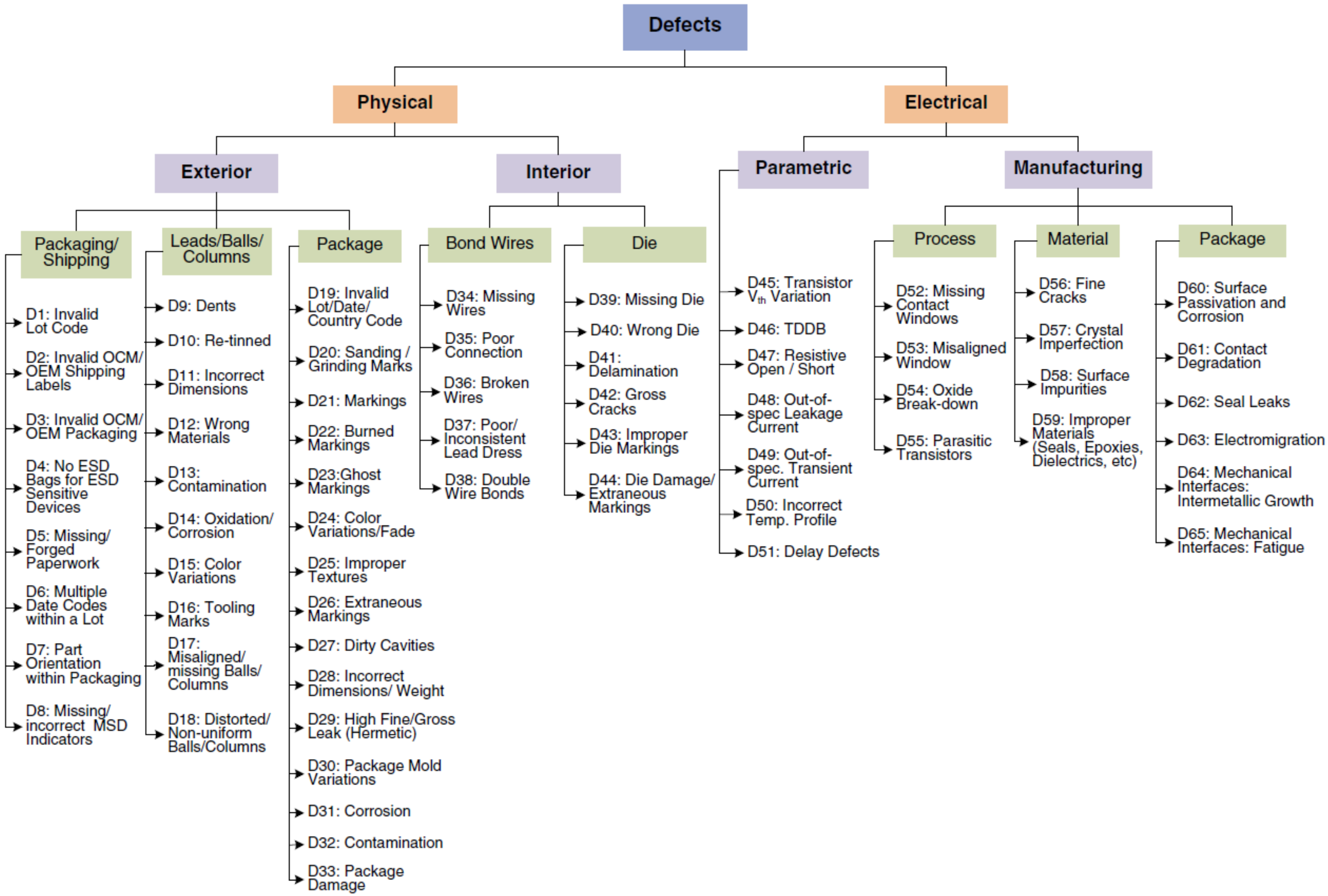
More information on counterfeit parts detection [TGF2015]

- Springer, 2015 – University of Connecticut, USA

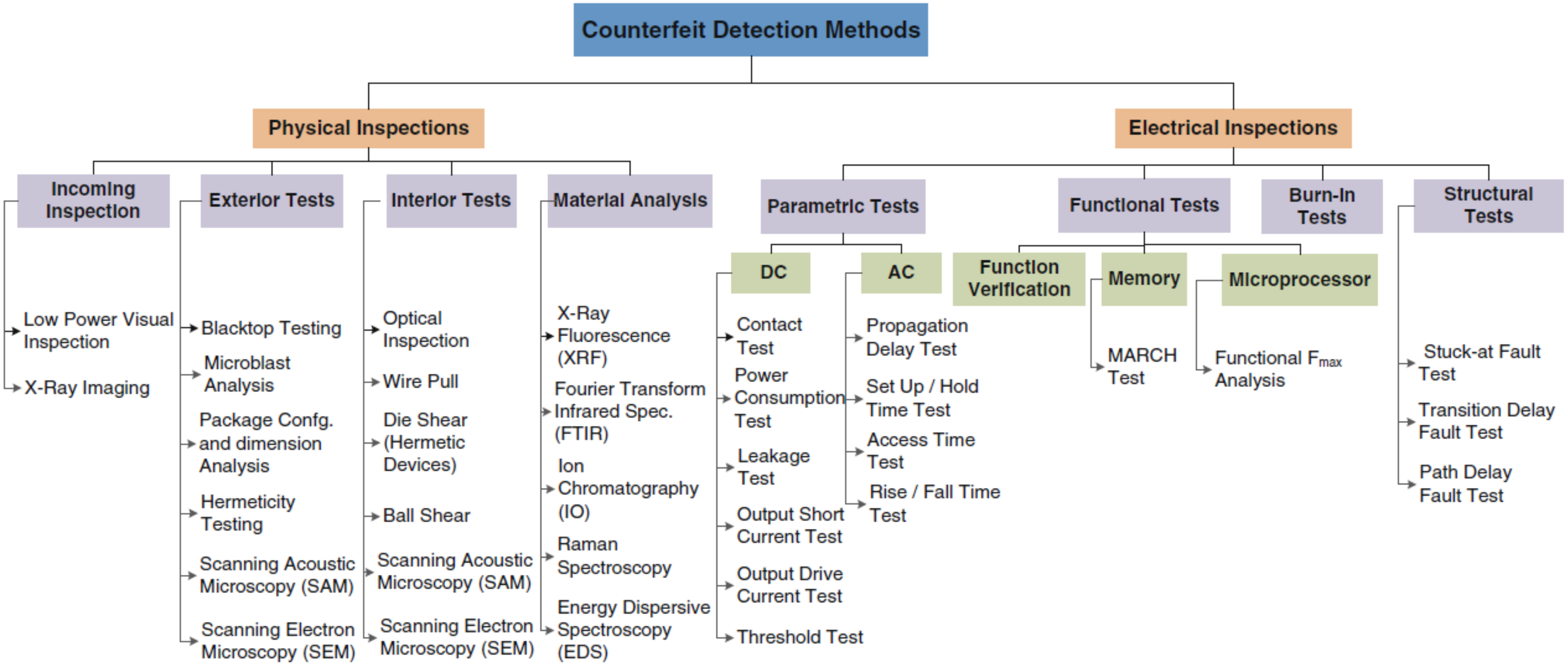


LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Taxonomy of defects in counterfeit components [TGF2015]



Taxonomy of counterfeit detection methods [TGF2015]

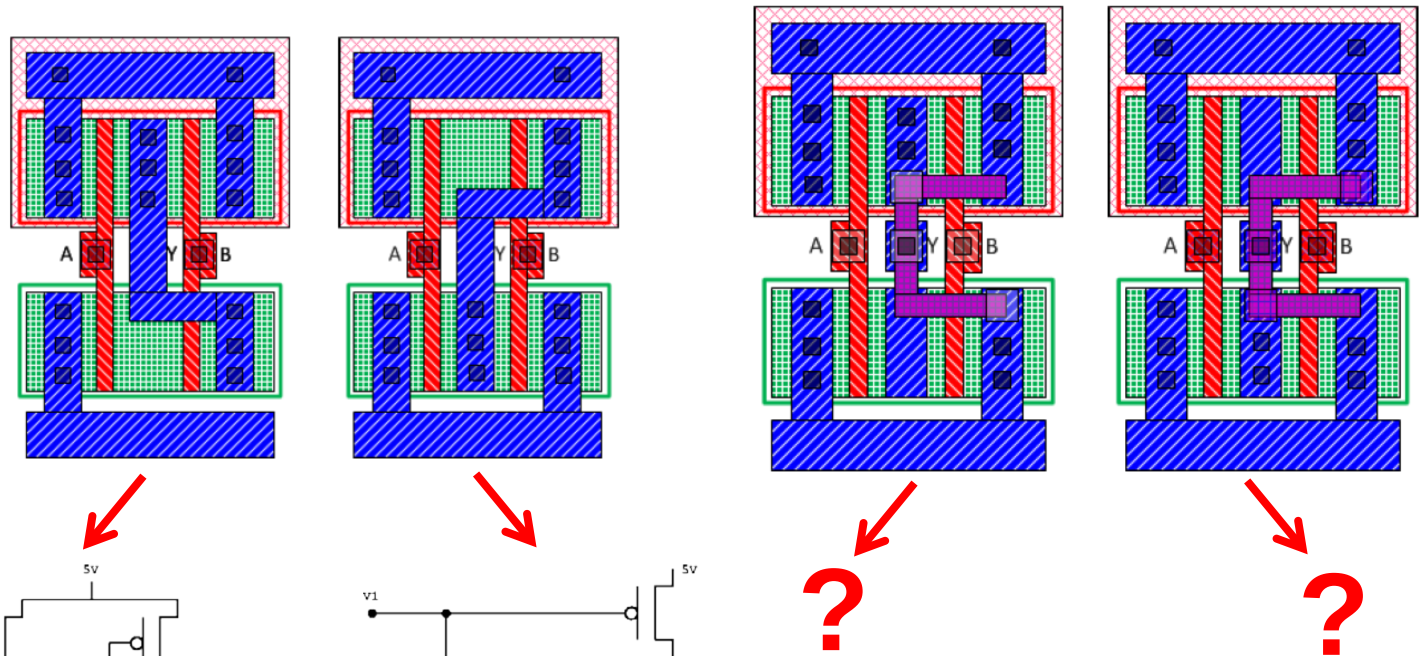


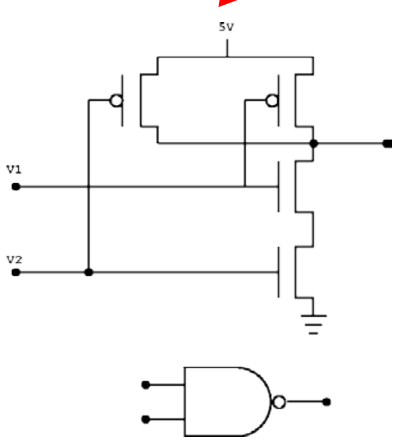
CURRENT INDUSTRIAL SOLUTIONS 2/2

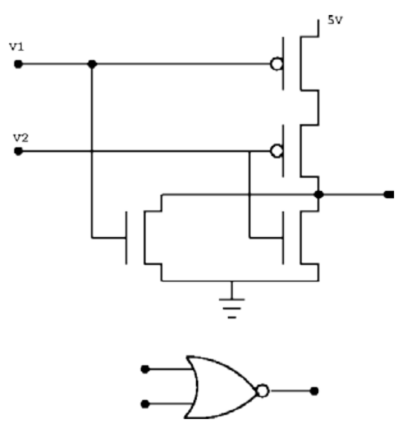
Protection against the reverse engineering

Circuit Camouflaging 1/2

- Definition: *set of means to physically hide details of a system from an optical inspection (which could use image processing techniques) without any modification of the system behavior*







J. Rajendran, M. Sam, O. Sinanoglu, R. Karri. *Security analysis of integrated circuit camouflaging*. ACM Conference on Computer & Communications Security, pp. 709 – 720, 2013.

Circuit Camouflaging 2/2

- Technology from SypherMedia International
http://www.smi.tv/solutions.htm

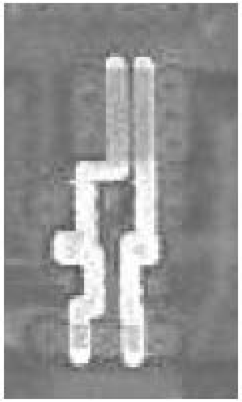


Figure 1: *Conventional 2 input NOR Gate*

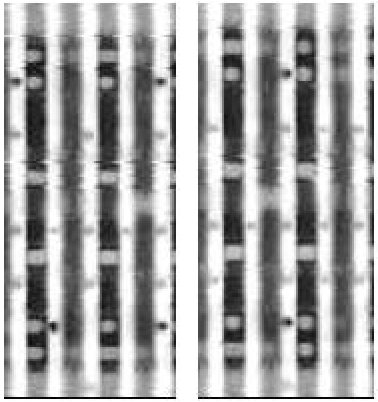


Figure 2: *SML 2-input NAND and NOR Gates*

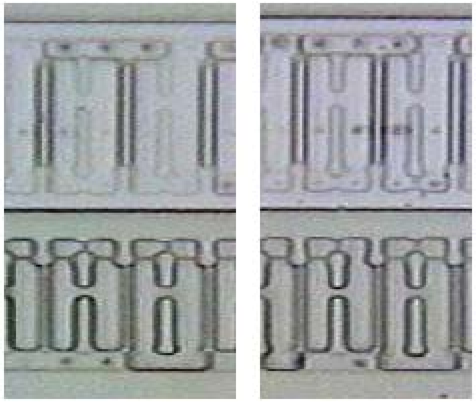


Figure 3: *SML 2-input NAND and NOR Gates without Metal*

SyperMedia Library – Circuit Camouflage Technology. SMI Data Sheet, 2012.

HARDWARE SOLUTION : SALWARE

what ?

Salutary hardware to design trusted IC

- SALWARE definition

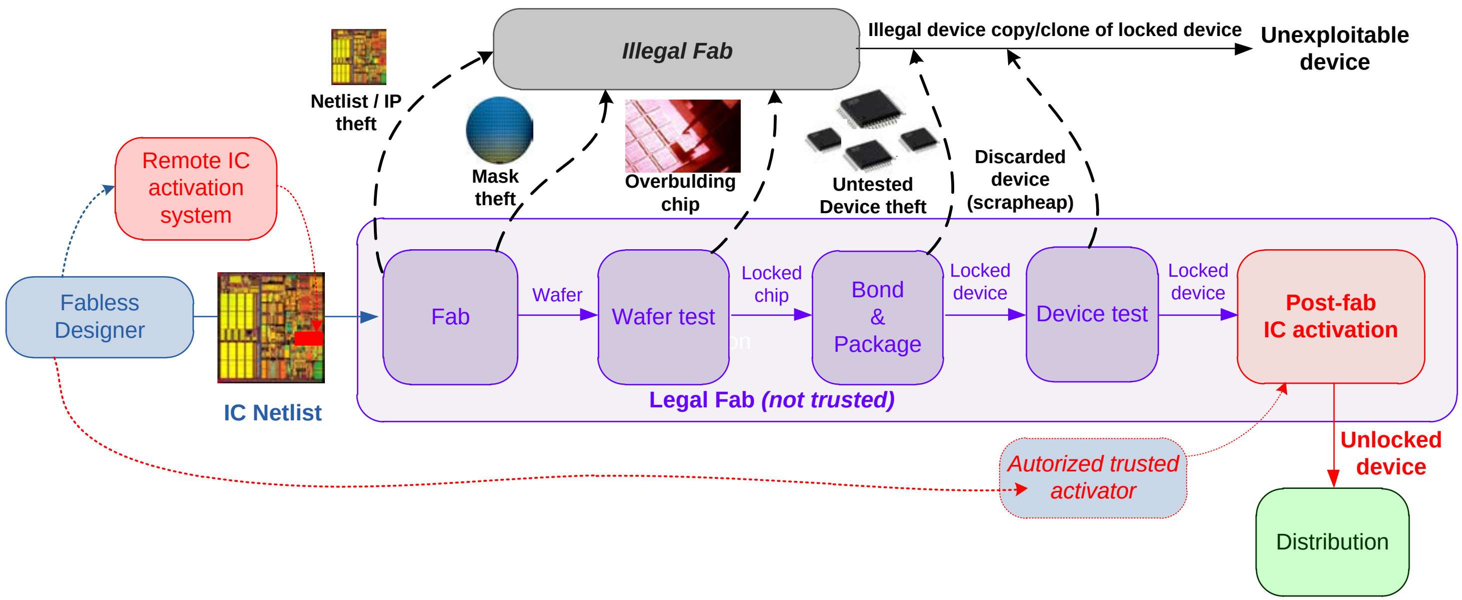
Salutary hardware (SALWARE) is a (small piece of) hardware system, hardly detectable (from the attacker point of view), hardly circumvented (from the attacker point of view), inserted in an integrated circuit or an IP, used to provide intellectual property information and/or to remotely activate the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

ACTIVE SALWARE

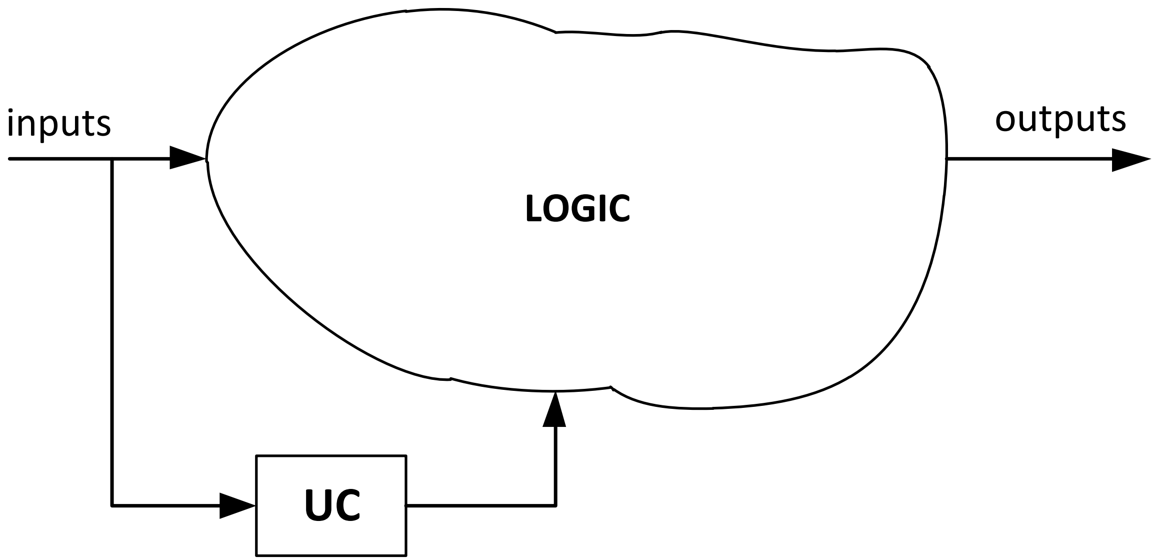
protection

IC Activation (locking/unlocking)

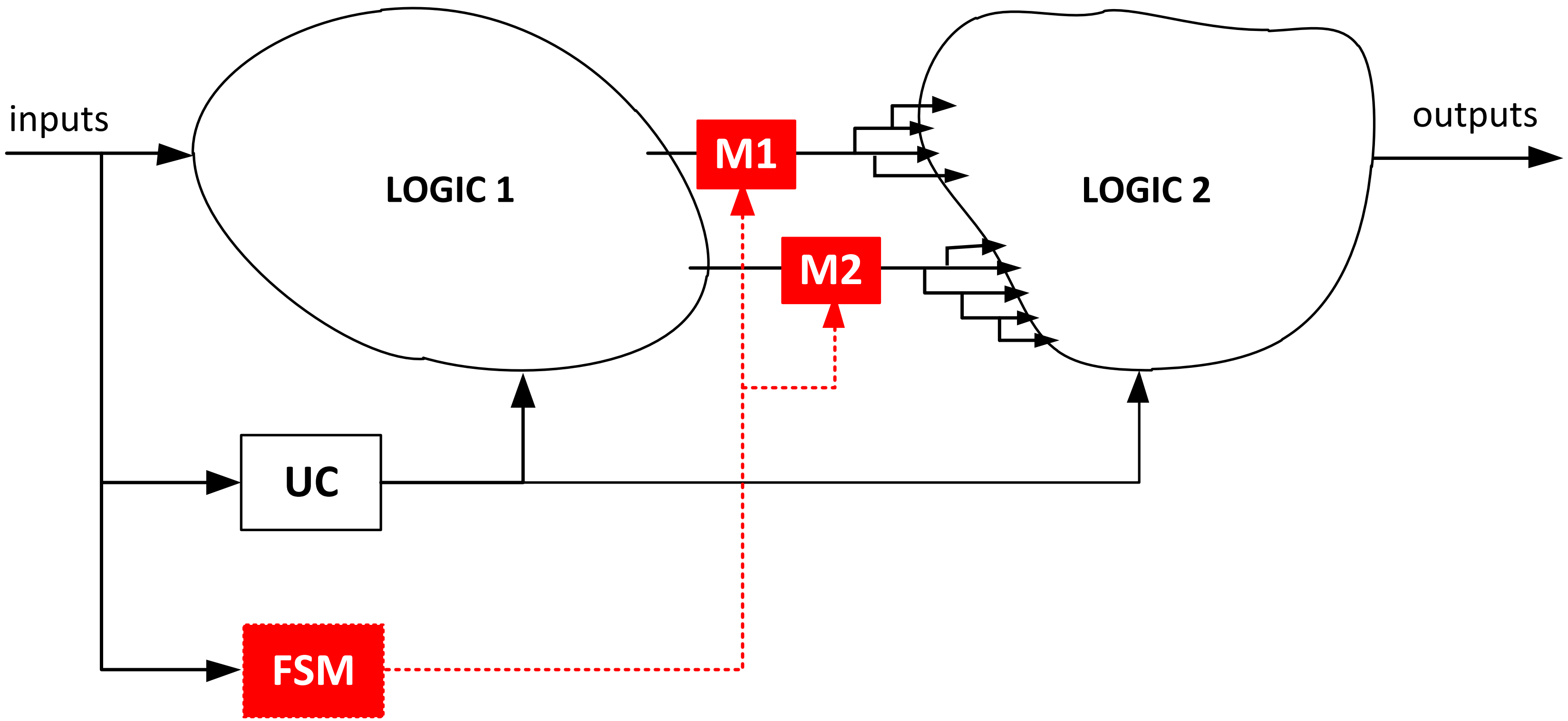
- (remote) activation after manufacturing (during life?)
  - Stolen devices or clones are not exploitable
  - Need cryptographic protocol to secure the activation scheme
  - Many solutions
    - Logic “encryption”, FSM “obfuscation”
    - Data-path “encryption” (BUS, NoC)
    - Antifuse-based on-chip locks
    - FPGA bitstream encryption



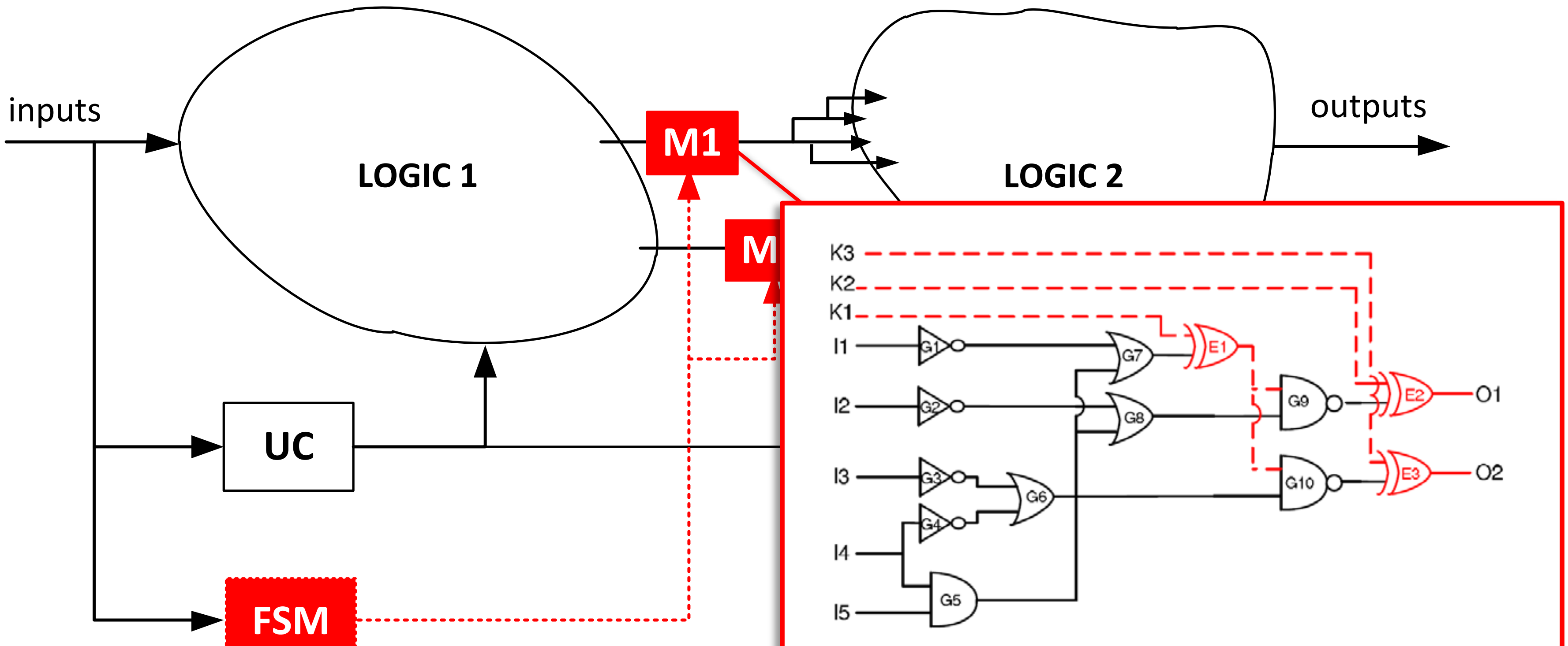
Logic *encryption*



Logic *encryption*

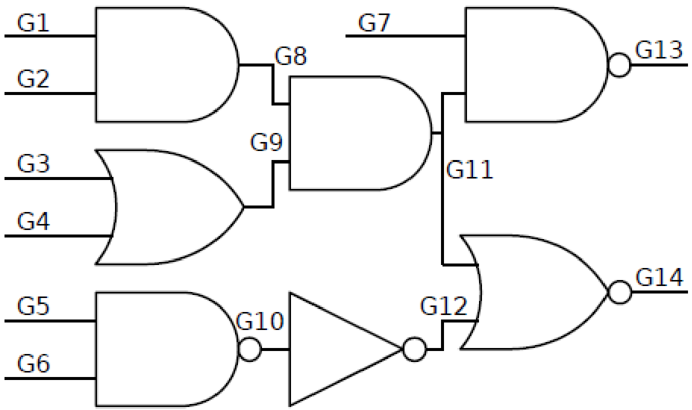


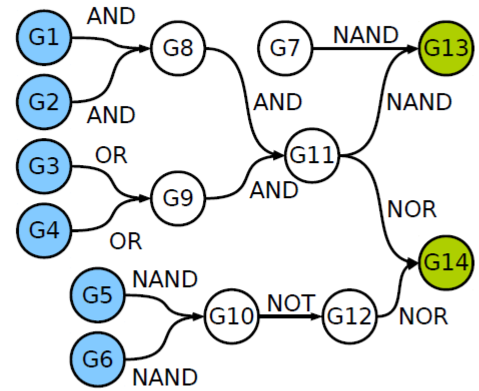
Logic *encryption*

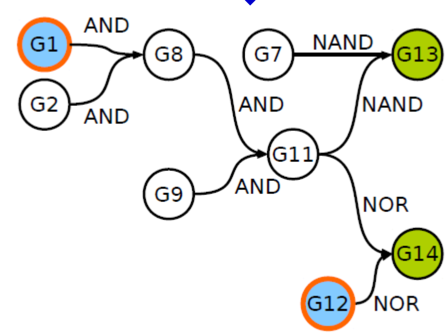


J. Rajendran, Y. Pino, O. Sinanoglu, R. Karri. *Logic Encryption: A Fault Analysis Perspective*. DATE 2012

Logic locking



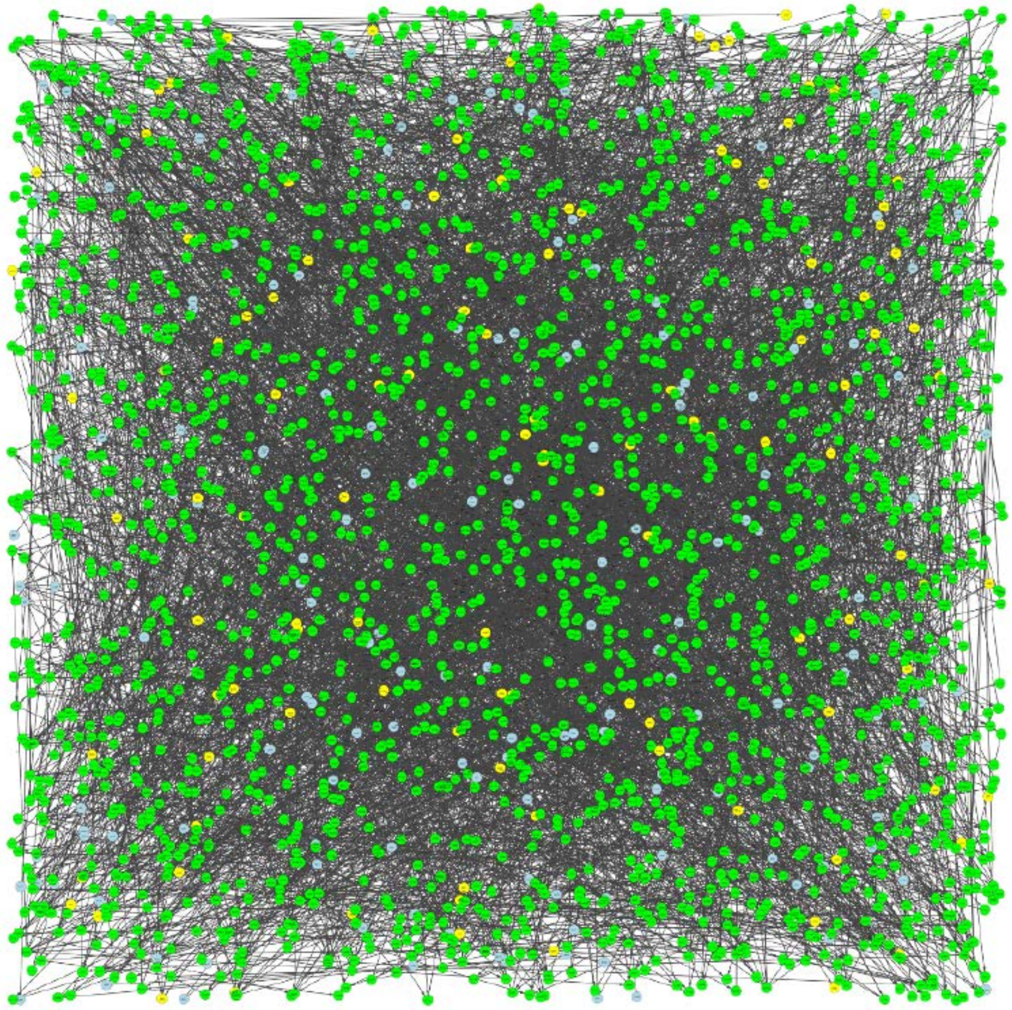




B. Colombier, L. Bossuet, D. Hely. *Reversible Denial-of-Service by Locking Gates Insertion for IP Cores Design Protection.* ISVLSI 2015.

Graphe analysis

- Benchmark ISCAS'85
  - 9-bit ALU
  - 2362 nodes
  - 178 inputs
  - 123 outputs

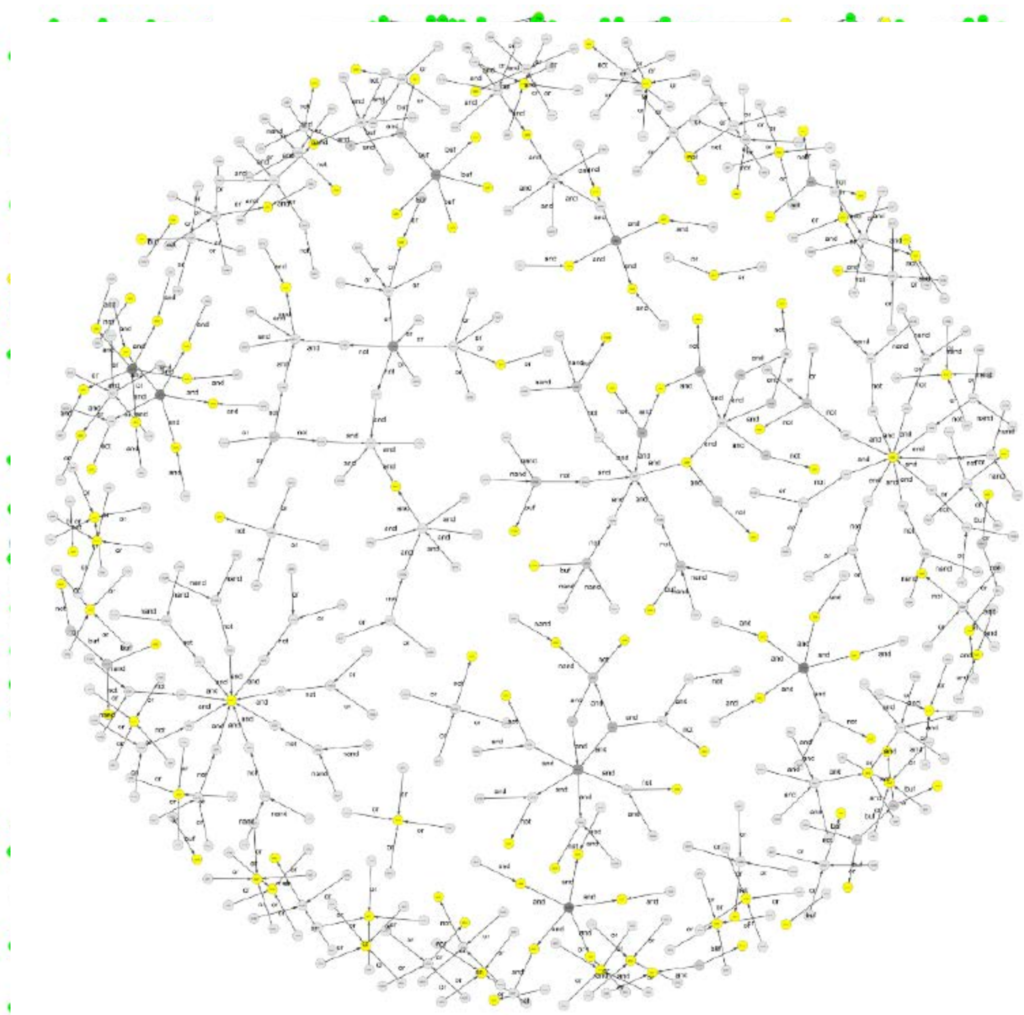


B. Colombier, L. Bossuet, D. Hely. *Reversible Denial-of-Service by Locking Gates Insertion for IP Cores Design Protection.* ISVLSI 2015.

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Graphe analysis

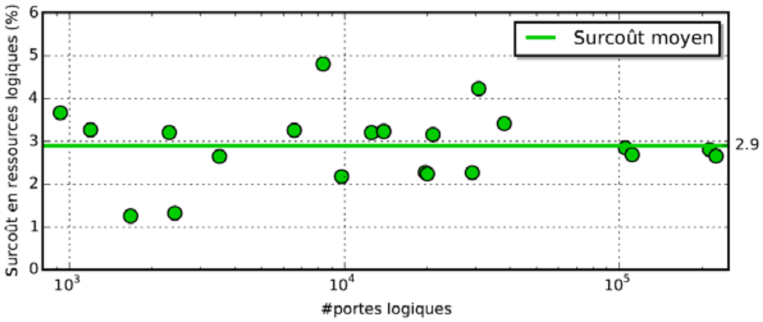
- Benchmark ISCAS'85
  - 9-bit ALU
  - 2362 nodes
  - 178 inputs
  - 123 outputs



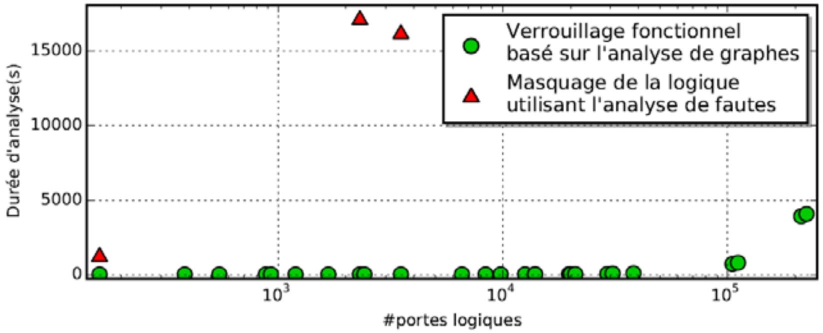
B. Colombier, L. Bossuet, D. Hely. *Reversible Denial-of-Service by Locking Gates Insertion for IP Cores Design Protection.* ISVLSI 2015.

Comparison with logic "encryption"

- Area overhead ≈ 3%
  - 20 netlists from ITC'99 benchmark
  - From 1K à 225K logic gates



- Analysis delay
  - Rajendran et al. Use faults propagation analysis
  - Our method is scalable

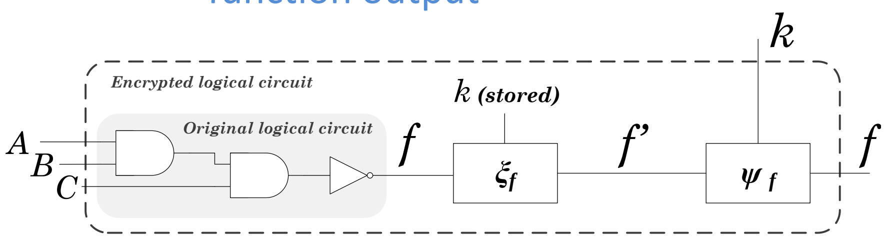


B. Colombier, L. Bossuet, D. Hely. *Reversible Denial-of-Service by Locking Gates Insertion for IP Cores Design Protection.* ISVLSI 2015.

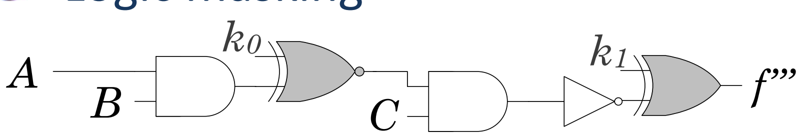
J. Rajendran, Y. Pino, O. Sinanoglu, R. Karri. *Logic Encryption: A Fault Analysis Perspective*. DATE 2012

A formal foundation for logic protection schemes

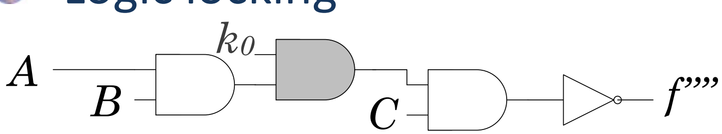
- Logic encryption
  - Formally : encryption of the Boolean function output



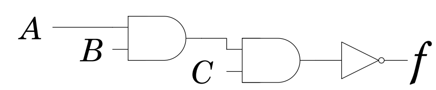
- Logic masking



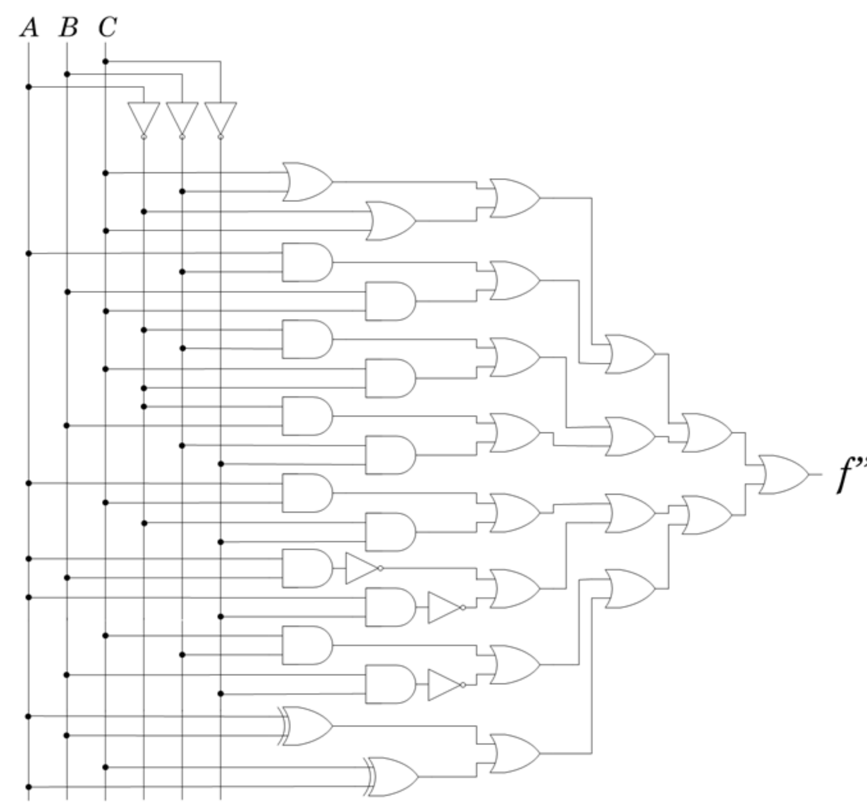
- Logic locking



- Logic obfuscation
  - Develop and obscure



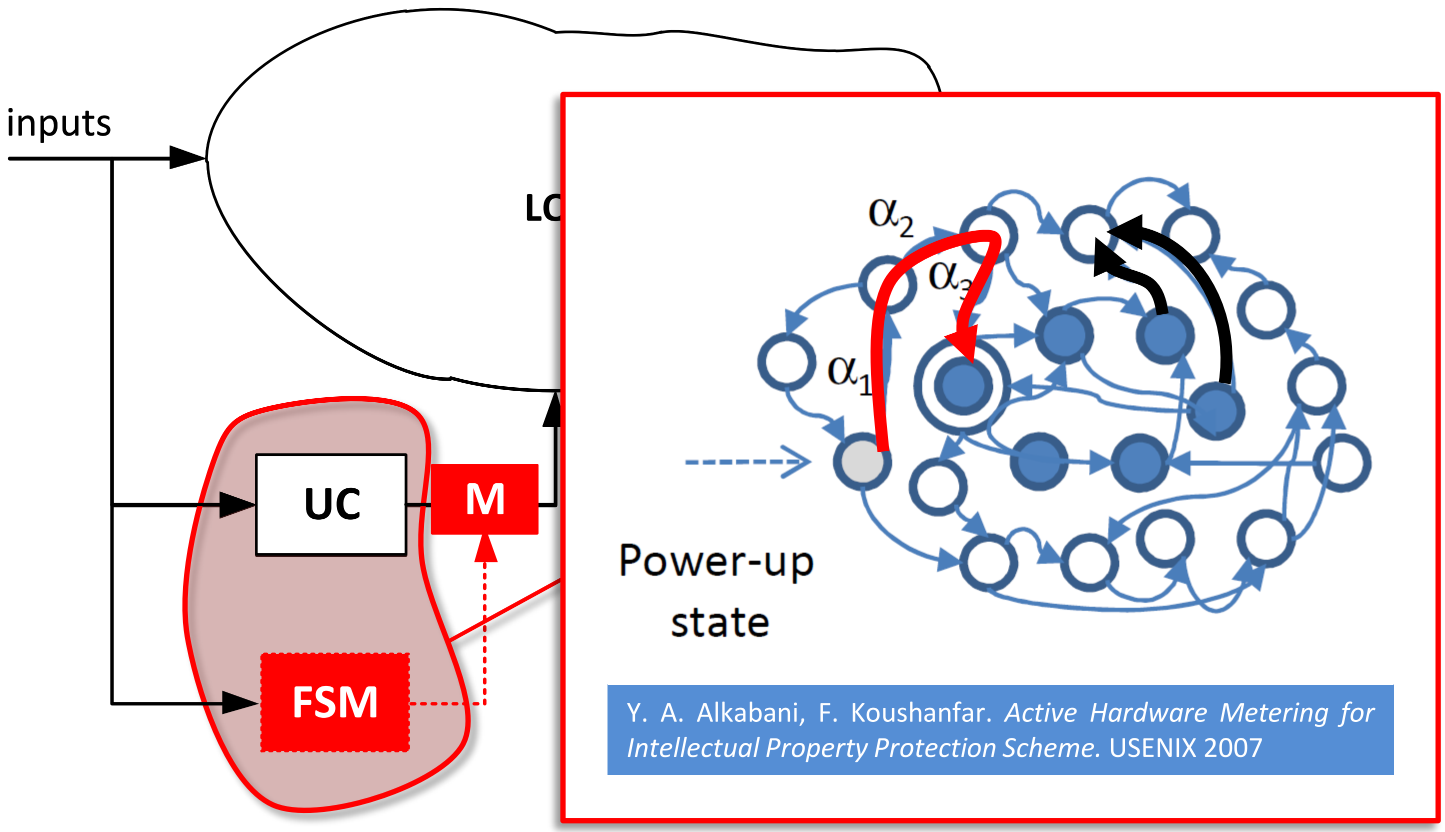
(a) Original Boolean function implementation



(c) Boolean function implementation after a second step of logical obfuscation

B. Colombier, L. Bossuet, D. Hely. *From Secured Logic to IP Protection.* Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, *to be published soon*.

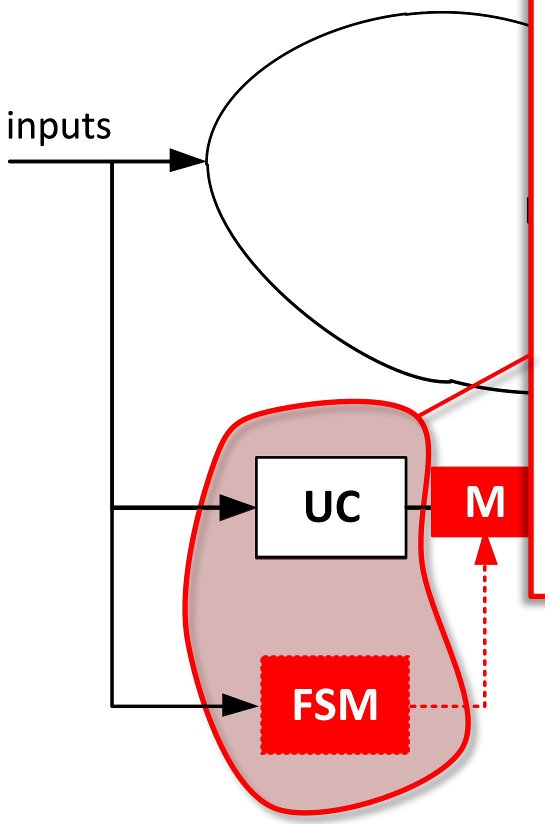
FSM *obfuscation*



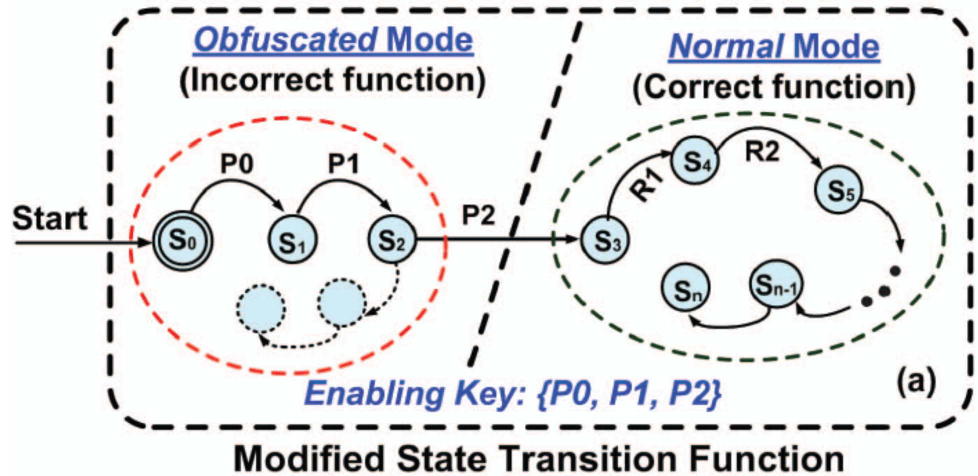
FSM obfuscation

Only one key for a set of devices!!!!

FSM *obfuscation*



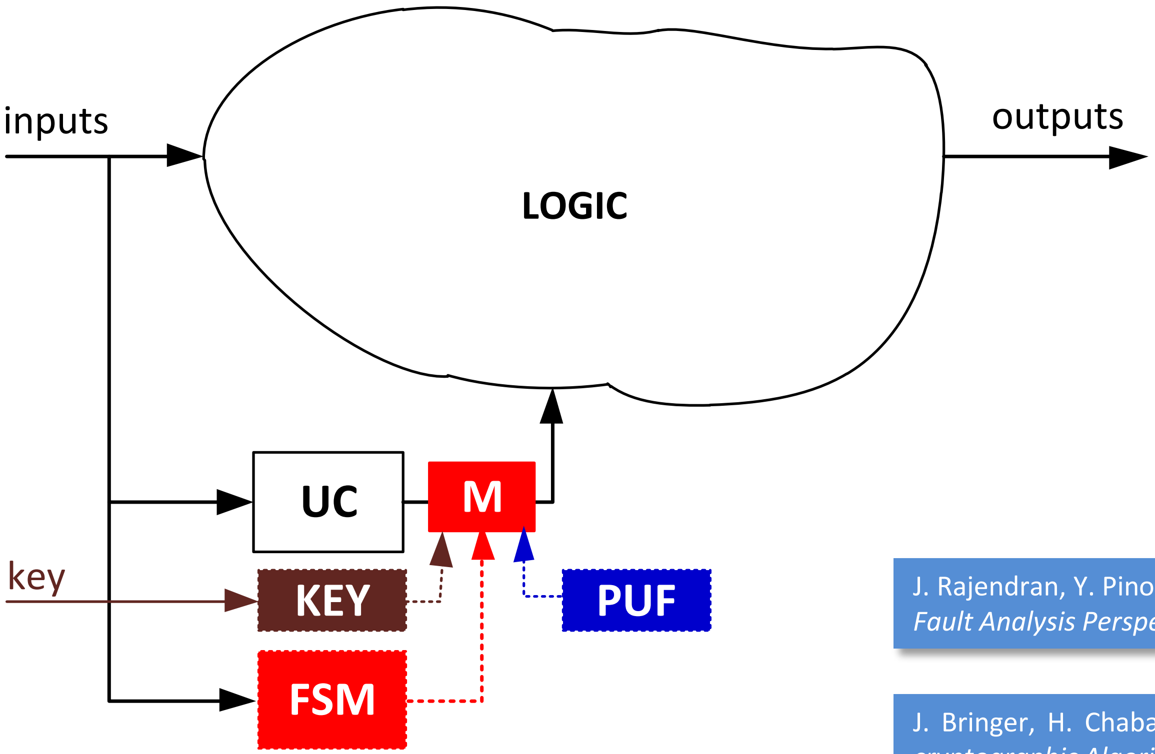
FSM obfuscation



R. S. Chakrabotry, S. Bhunia. *Security Through Obscurity: An Approach for Protecting Register Transfert Level Hardware IP*. In Proceedings of HOST 2009

FSM *obfuscation*

- FSM *obfuscation* – output register *encryption*
  - Dedicated Key per device
  - Needs an device identification (PUF)



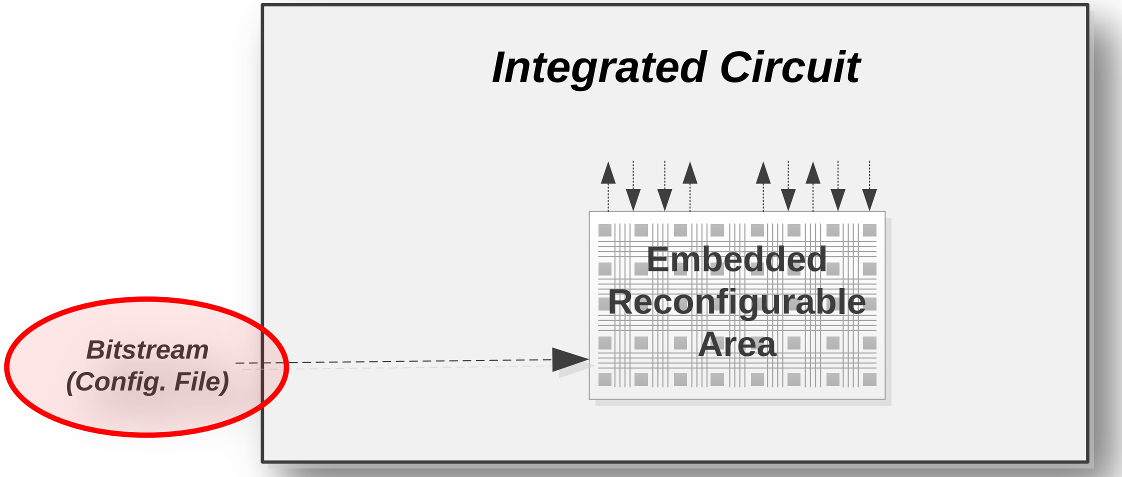
J. Rajendran, Y. Pino, O. Sinanoglu, R. Karri. *Logic Encryption: A Fault Analysis Perspective*. DATE 2012

J. Bringer, H. Chabanne, T. Icart. *On Physical Obfuscation of cryptographic Algorithlms*. INDOCRYPT 2009

Y. Alkabani, F. Koushanfar, M. Potkonjak. *Remote Activation of Ics for Piracy Prevention and Digital Right Managment*. ICCAD 2007

Design obfuscation

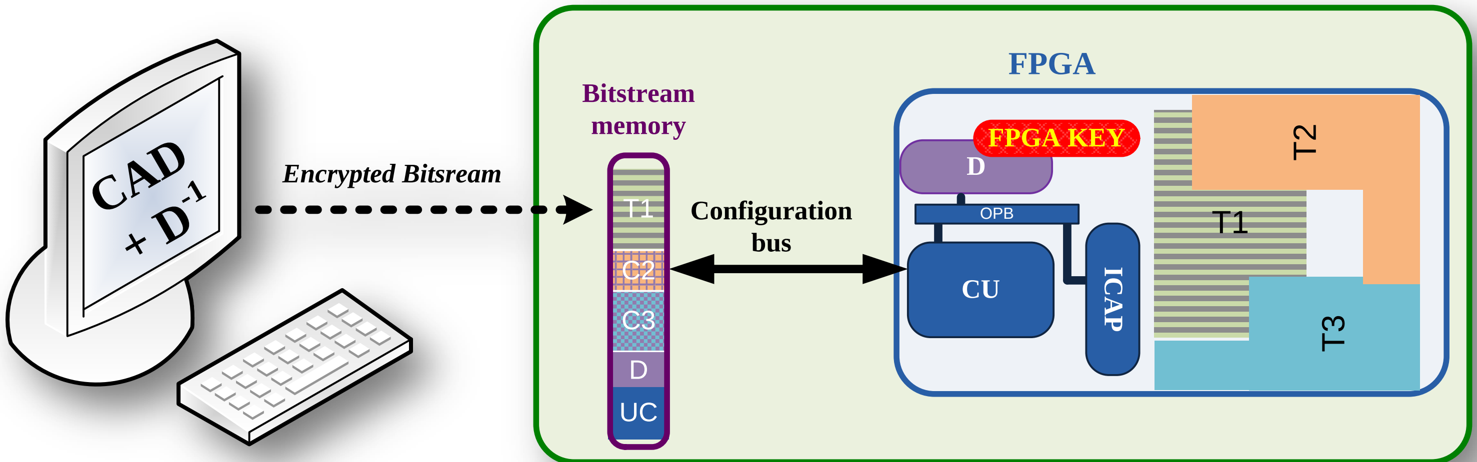
- Obfuscation by using reconfigurable area
  - Countermeasure to reverse-engineering
  - "High-information" parts have to be included in the reconfigurable area
    - Control Unit
    - Processor instruction decoder
  - Need encryption of the bitstream
    - Anti-cloning
    - One bitsream (encrypted) by device (one secret key by device)



B. Liu, and B. Wang. *Embedded Reconfigurable Logic for ASIC Design Obfuscation Against Supply Chain Attacks*. DATE 2014

Security of FPGA bitstream (SRAM and FLASH)

- Encryption of the FPGA bistream
  - Threats: probing / cloning / reverse-engineering / replay /denial
  - Solutions: partial and dynamic reconfiguration [1]-[2], embedded cipher with hash function [3], remote update protection [4], anti-replay [5], disposable config. [6] …



[1] L. Bossuet, G.Gogniat and W. Burleson. *Dynamically Configurable Security for SRAM FPGA Bitstreams.* RAW, IPDPS 2004

[2] A.S. Zeineddini, and K.Gaj. *Secure partial reconfiguration of FPGAs*. FPT 2005.

[3] Y. Hori, A. Satoh, H.Sakane, and K. Toda. *Bitstream encryption and authentication with AES-GCM in dynamically reconfigurable systems.* FPL 2008

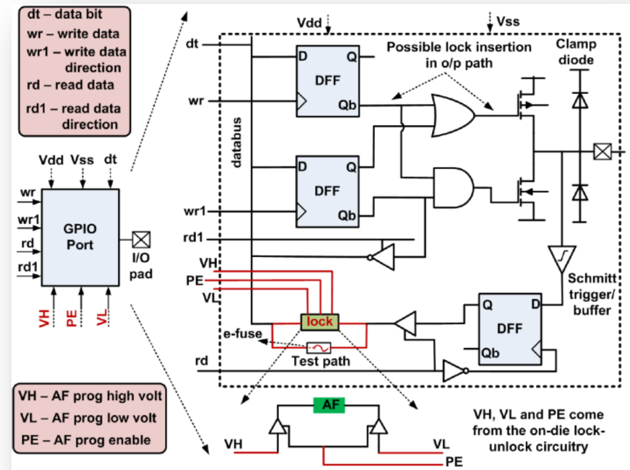
[4] S. Drimer and M. G. Kuhn. *A Protocol for Secure Remote Updates of FPGA Configurations.* ARC 2009.

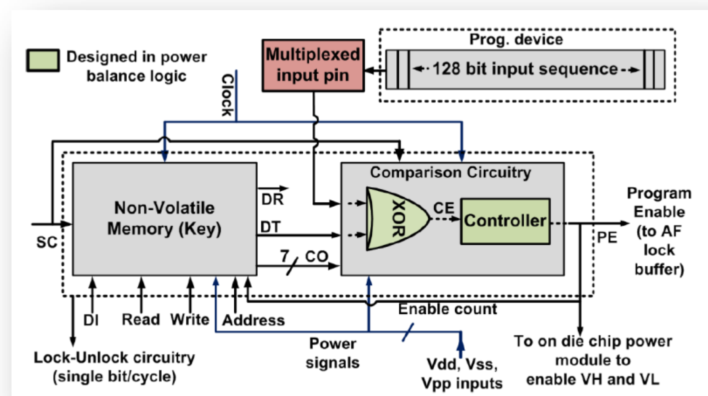
[5] F. Devic, B. Badrignans, and L. Torres. *Secure Protocol Implementation for Remote Bitstream Update Preventing Replay Attacks on FPGAs.* FPL 2010.

[6] L. Bossuet, V. Fischer, L. Gaspar, L. Torres, G. Gogniat. *Disposable Configuration of Remotely Reconfigurable Systems.* Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, *2015.*

IOB locking

- Using antifuse
  - Strong permanent lock
  - e-fuse for test
  - Hard to program without the key
  - One key par IC family
  - Dedicated to ASIC
  - Need an external programmer device
  - Only one final bit for the "program enable"

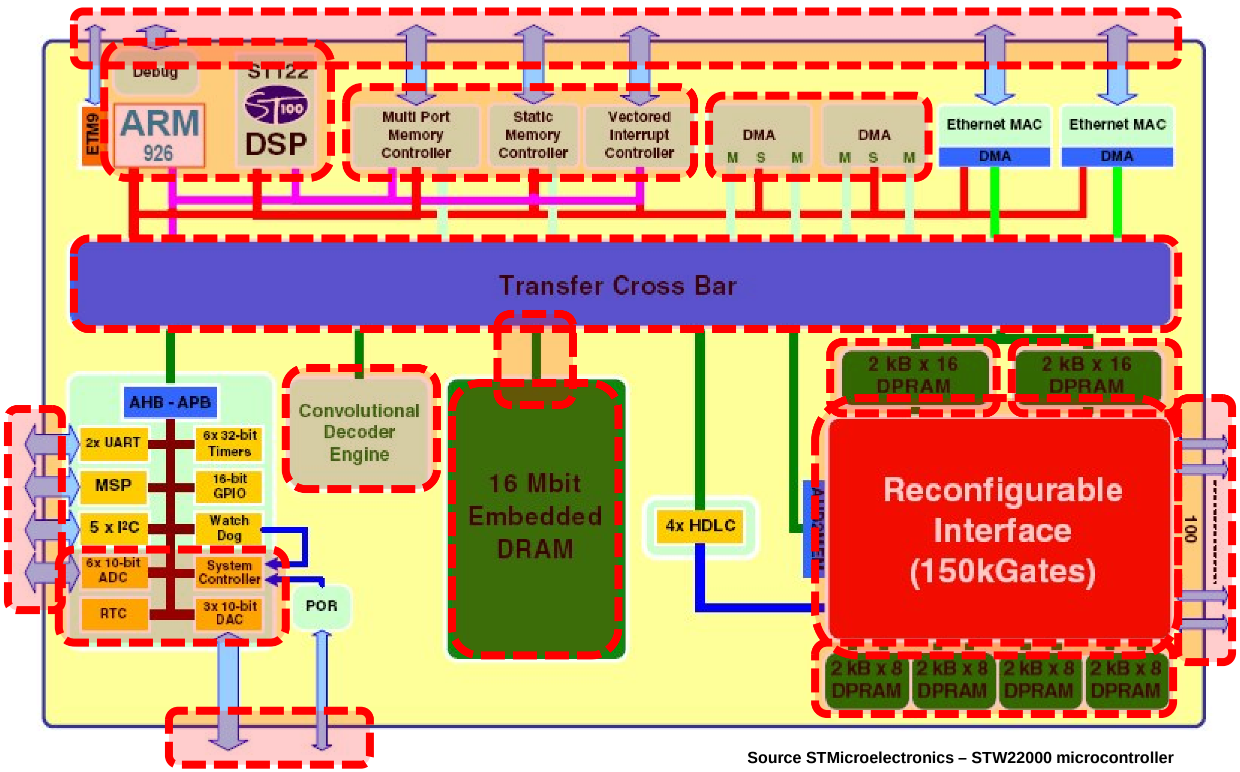




Z. Liu, Y. Li, R. Geiger, and D. Chen. *Active Defense against Counterfeiting Attacks through Robust Aantifuse-based On-Chip-Lock*. VLSI Test Symposium 2014

Locking of a System-on-Chip

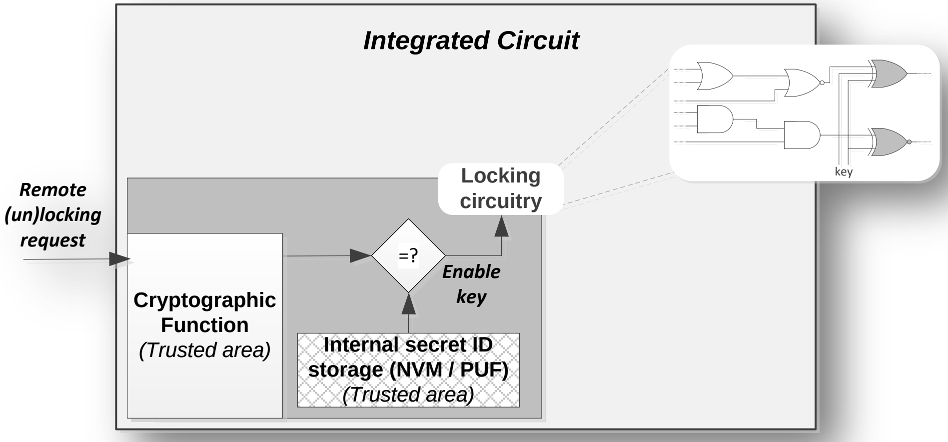
- What it is possible to lock in a SoC?
  - Control unit : FSM outputs masking/ FSM state registers masking / microprocessor obfuscation
  - Treatment unit: Logic masking/locking/obfuscation
  - Internal communication: bus encryption / Cross Bar routing masking/ NoC locking/encryption
  - Memory: DMA and bus encryption (bus @ / bus data), data encryption,
  - Configuration (eFPGA / multi-mode-IP): bitstream encryption
  - IOB: locking
  - Analog parts calibration (performance downgrading): ex. PLL, DAC, ADC …



Source STMicroelectronics – STW22000 microcontroller

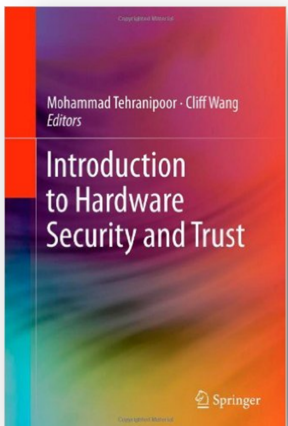
Active Salware Design

- Strong security
  - Use cryptographic functions to obtain the usual crypto services
    - Confidentially, integrity, authentication
  - Use protected hardware implementation
    - Protection against side-channel analysis and fault injection (trusted zone)
  - One activation key per device
    - Use device identification (PUF, NVM)
  - Many bits for activation
- Very low overhead
  - Locking system is rarely used
  - No system performance decrease
- Flexibility
  - Locking ⇔ unlocking
  - Test available
- Mutual actions
  - Different payload
  - Digital / Analog parts

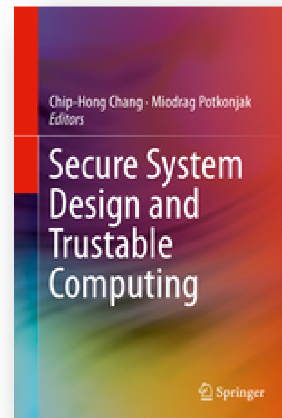


More information on active salware

- Springer 2012
  - M. Tehranipoor, Univ. Connecticut
  - C. Wang, US Army Research Office



- Springer 2016
  - C.H. Chang, Nanyang Tech. Univ.
  - M. Potkonjak, UCLA



- Springer fall 2016: Foundations of Hardware IP Protection
  - L. Bossuet, Univ. Lyon
  - L. Torres, Univ. Montpellier

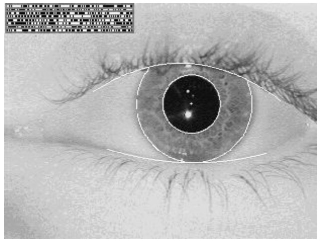
PASSIVE SALWARE

IC identification / authentication

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Fingerprint / Watermark

- Fingerprint
  - Measurement of a physical (or behavioral) characteristics



- Watermark
  - Additional (hidden) information (*steganography*)

- Silicon PUF (Physical Unclonable Function)

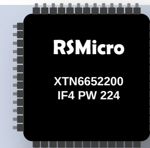
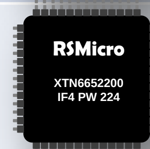
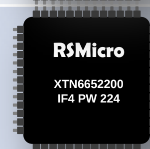
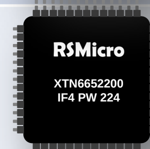
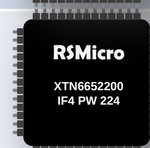
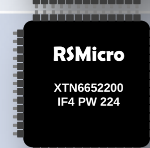
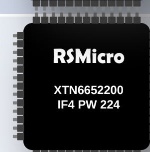
- Silicon Watermark

PUF

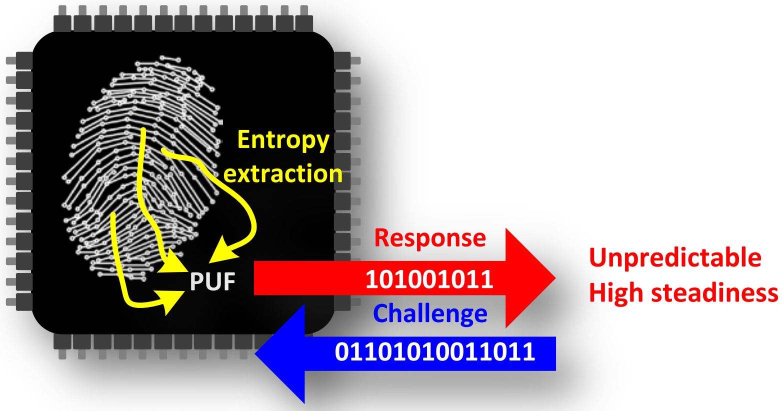
- Identification of IC
  - Set of ICs
  - Challenges / responses protocol
  - Extraction of entropy from CMOS process variations

PUF

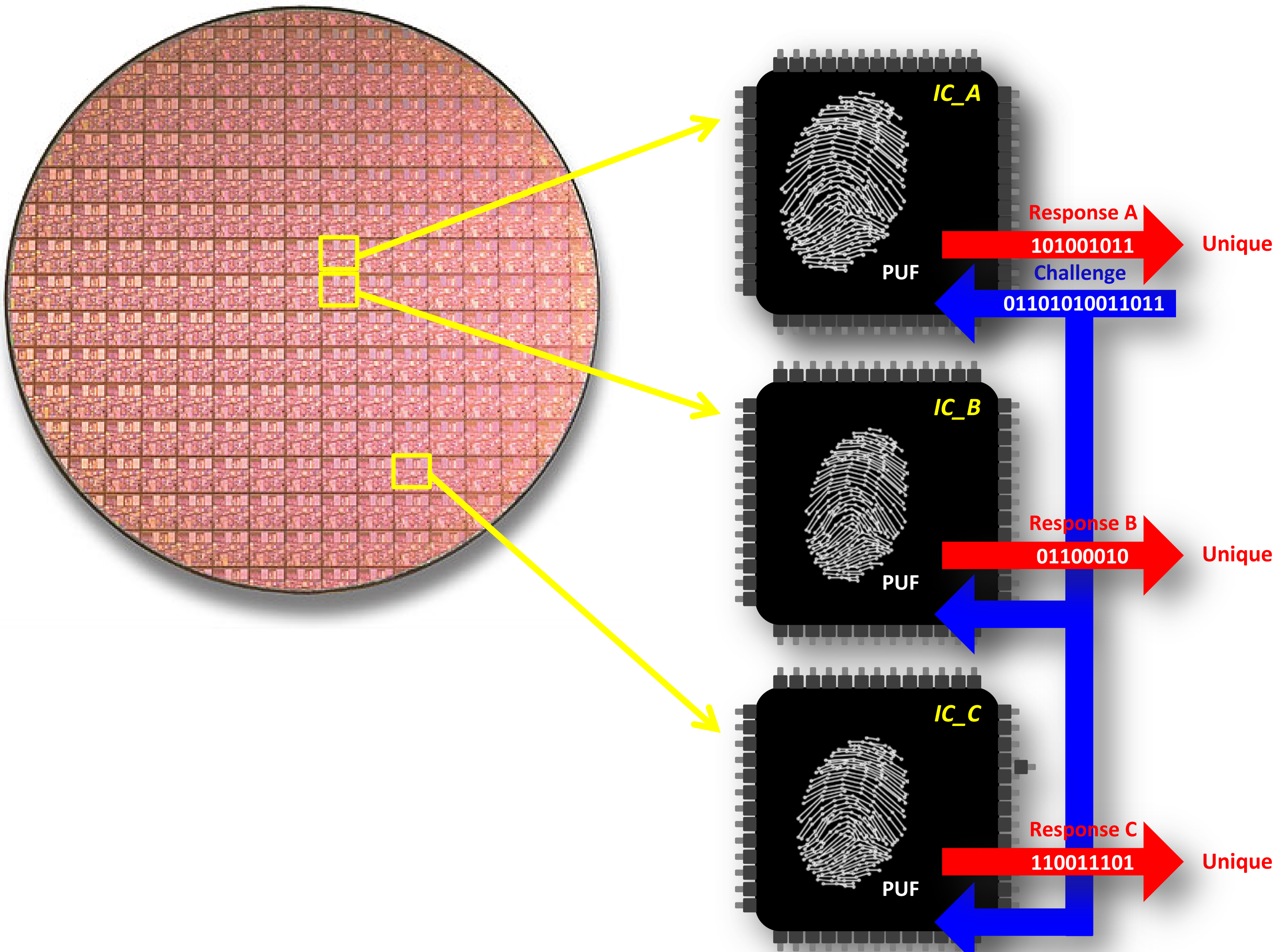
- Identification of IC
  - Set of ICs
  - Challenges / responses protocol
  - Extraction of entropy from CMOS process variations

ID	IC
AF30	
37B1	
8992	
FE72	
E90B	
5129	
8C9D	
253A	

Fingerprint of IC – Silicon PUF

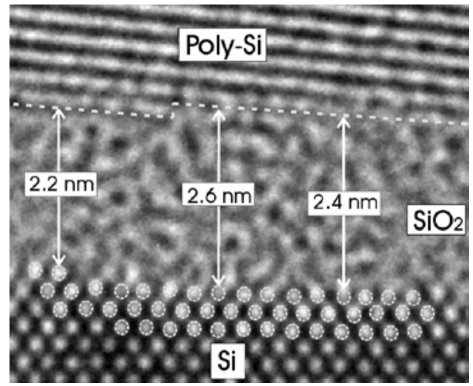


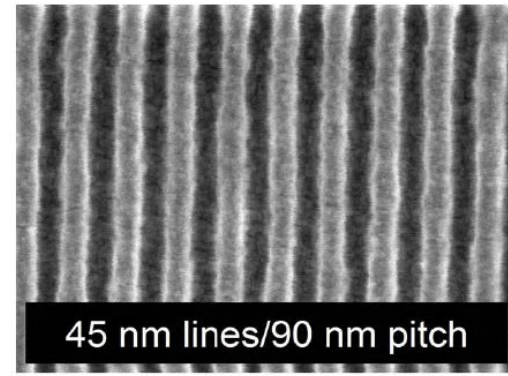
Fingerprint of IC – Silicon PUF



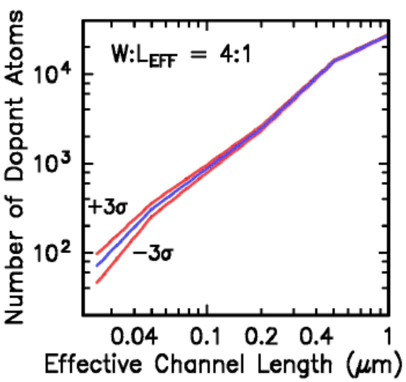
CMOS process variations

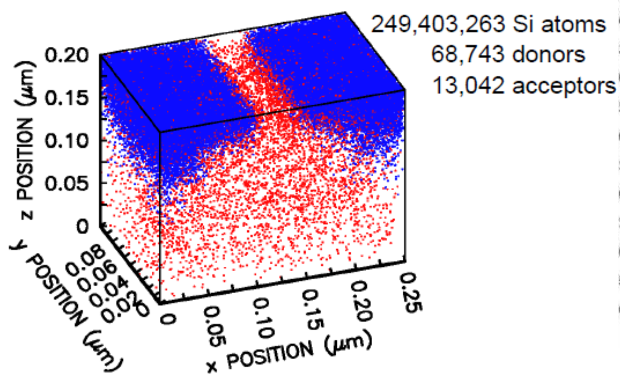
- Example
  - Oxide thickness
  - Metal line



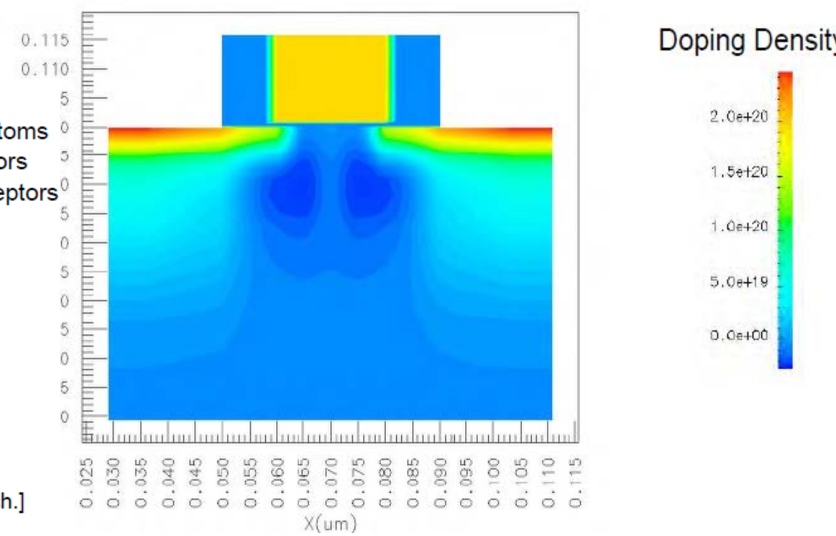


  - Number of dopant atoms
  - Position of dopants
  - Doping density



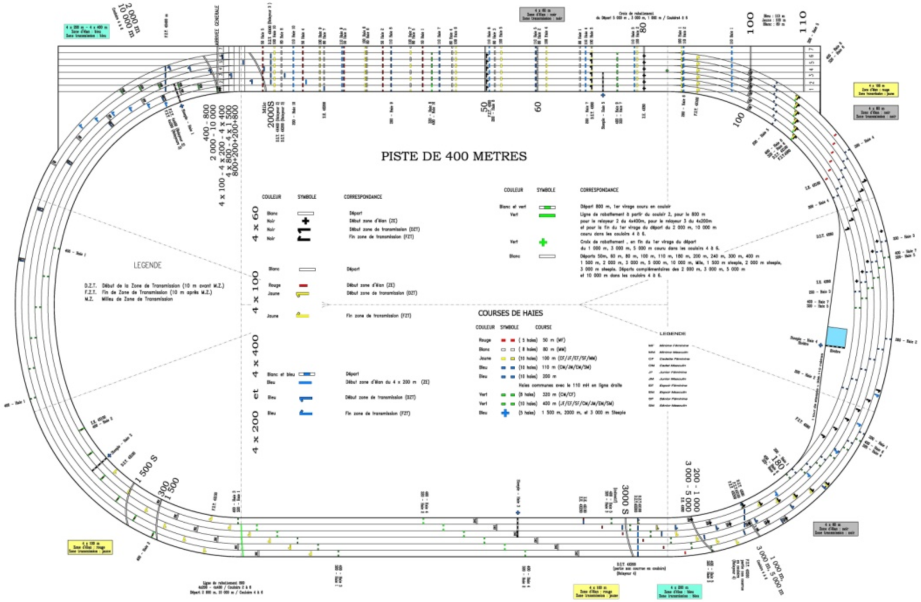


[D. J. Frank, et al., 1999 Symp. VLSI Tech.]



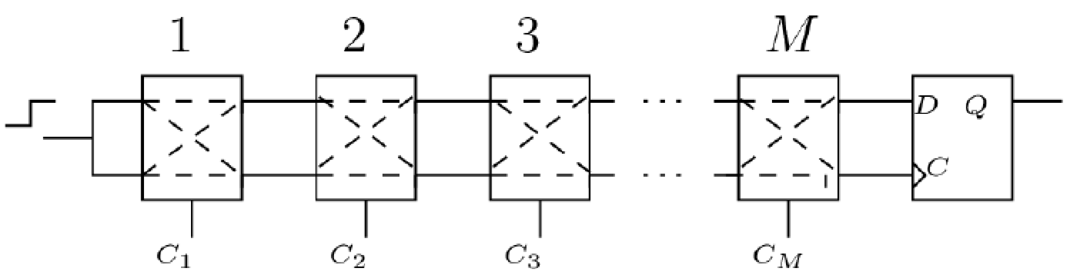
PUF principe: compare (theoretically) identical things !

- Example of an athletic race of clones
  - All the runners are identical (same doping)
  - Theoretically, all the lines on the stadium are the same
  - Lines length / runners speed mismatch measurement

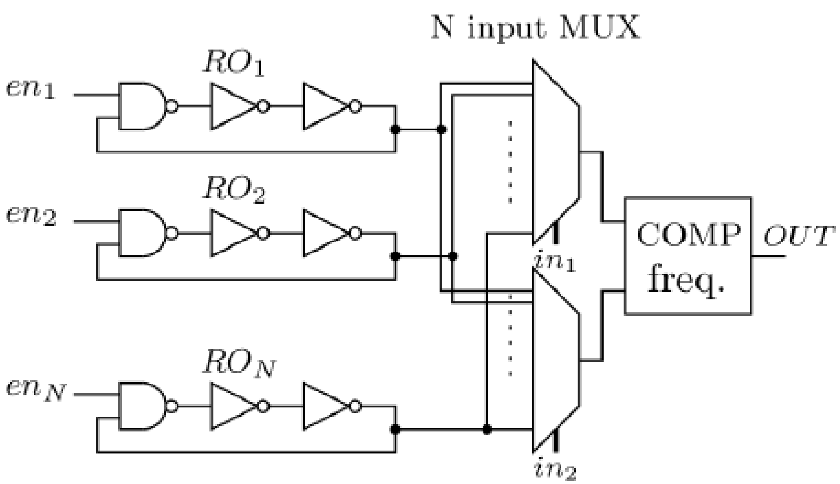


PUF Architectures

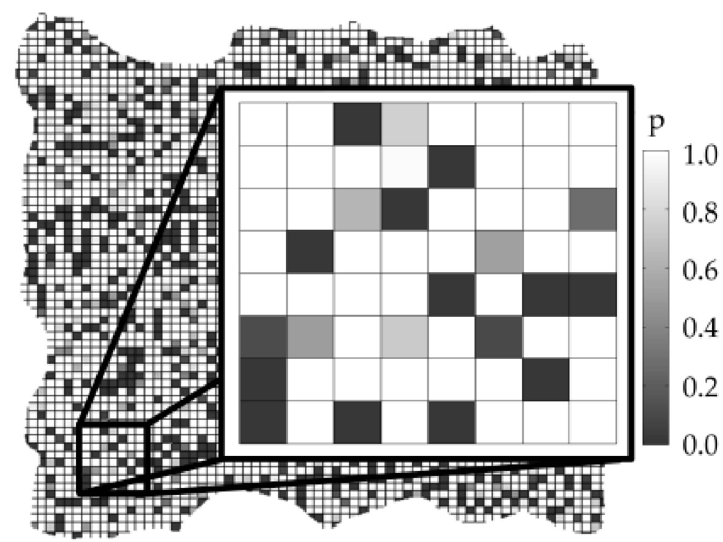
- Three main architectures
  - Race of delays between two symmetrical delay lines – Arbiter PUF
  - Frequency mismatch in multiple ring-oscillators – RO-PUF, loop-PUF
  - Metastability of a couple of cross-coupled elements – SRAM PUF, Butterfly



B. Gassend, D. Lim, D. Clarke, M. Van Dijk, S. Devadas. Identification and authentication of integrated circuits. Concurrency and Computation: Practice & Experience, 16(11):1077-1098, 2004.



G. Edward Suh, S. Devadas. Physical unclonable functions for device authentication and secret key generation. In DAC, pp. 9-14, 2007.



E. Holcomb, W. Burleson, K. Fu. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. IEEE Transations on Computers, Vol. 58, No. 9, 2009.

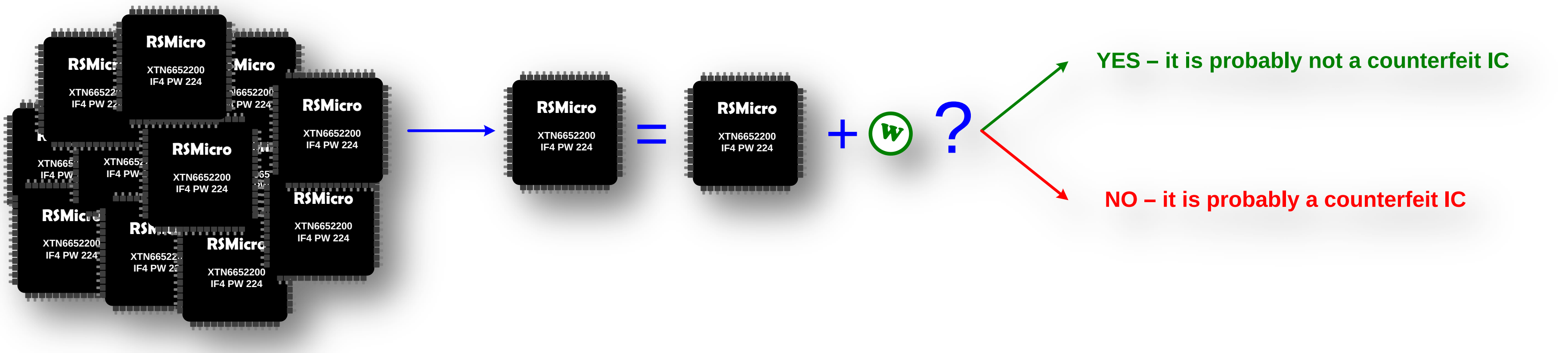
Some PUF challenges

- Future works
  - Experimental characterization of all PUF architectures in corner conditions on FPGA and ASIC
  - Aging compensation
  - Security analysis
    - Sensitivity to EM perturbation/analysis
    - Sensitivity to optical analysis
  - Construction of stochastic models of microelectronic process variations
  - Construction of physical model

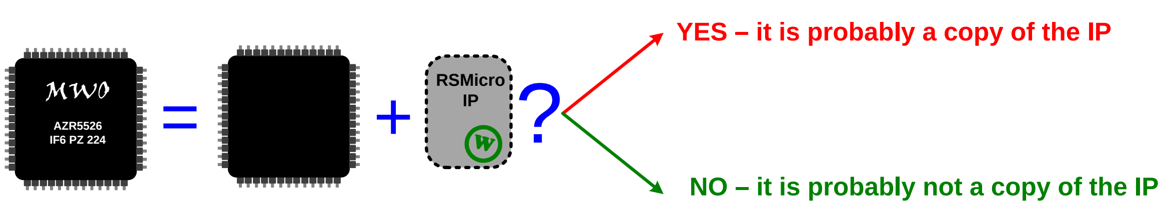
- Current project
  - European H2020 HECTOR project
  - http://www.hector-project.eu/
  - Technikon, KU Leuven, Univ. Jean Monnet, TU Graz, ThalesCommunications & Security SAS, STMicroelectronics Rousset SAS, STMicroelectronics SRL, Micronic AS, Brightsight

Watermark

- Detection of IC counterfeiting
  - Set of good referenced ICs

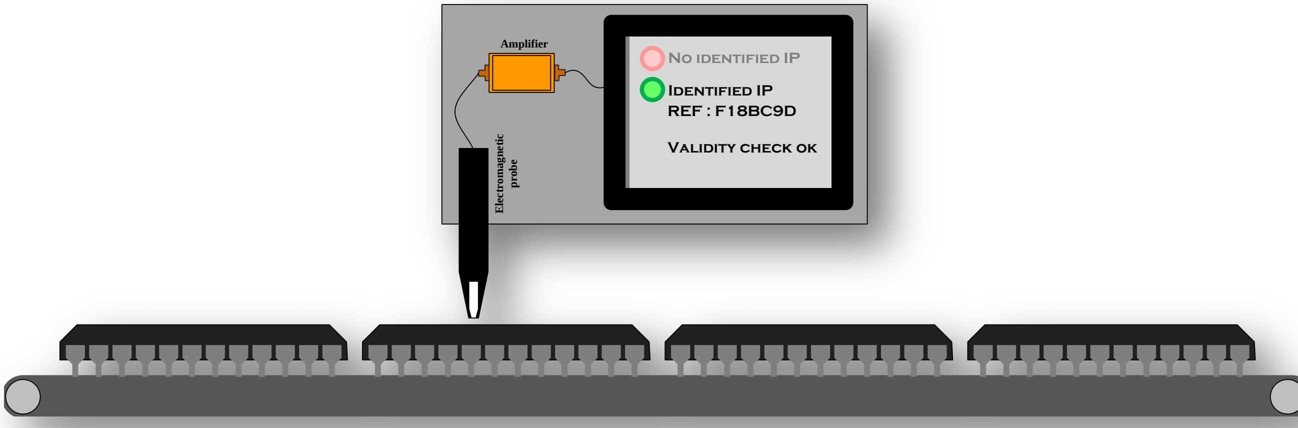


- Detection of IP theft (illegal copy/use)



Automatic detection of IC counterfeiting

- In the supply chain



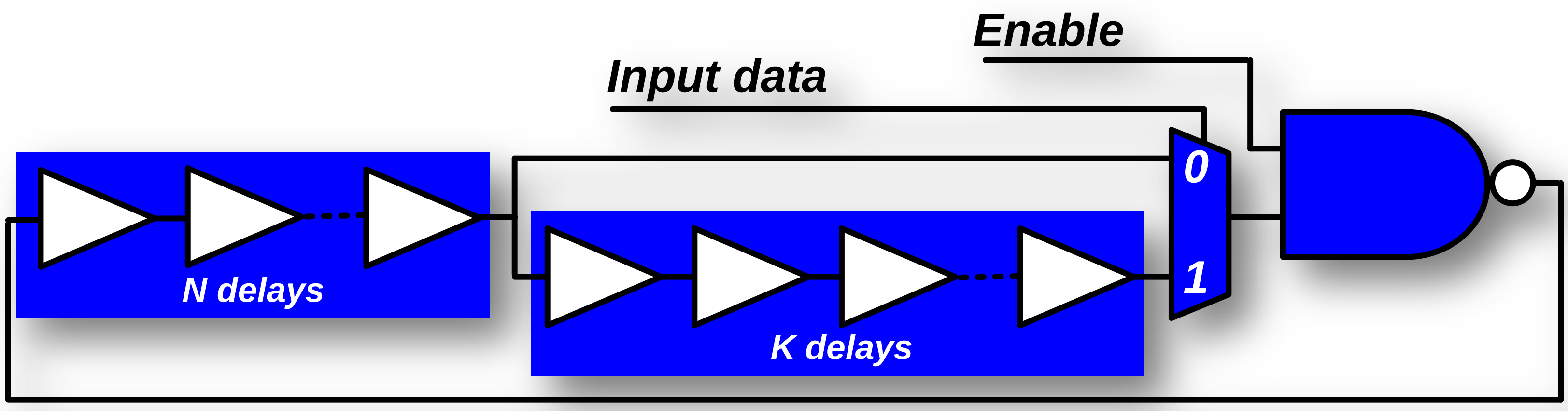
- **Contactless** => quick check
- **High data rate** => direct use in a supply chain (large set of ICs)
- **Very-low area overhead** => used few times only during the device life

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Ultra lightweight BFSK transmitter

- Transmission on the EM channel (contactless)
- Configurable ring-oscillator
  - Two frequencies generator $f_0 > f_1$
  - Two parameters *N* and *K*
  - *Size in number of LUT4 = 1+K+N*

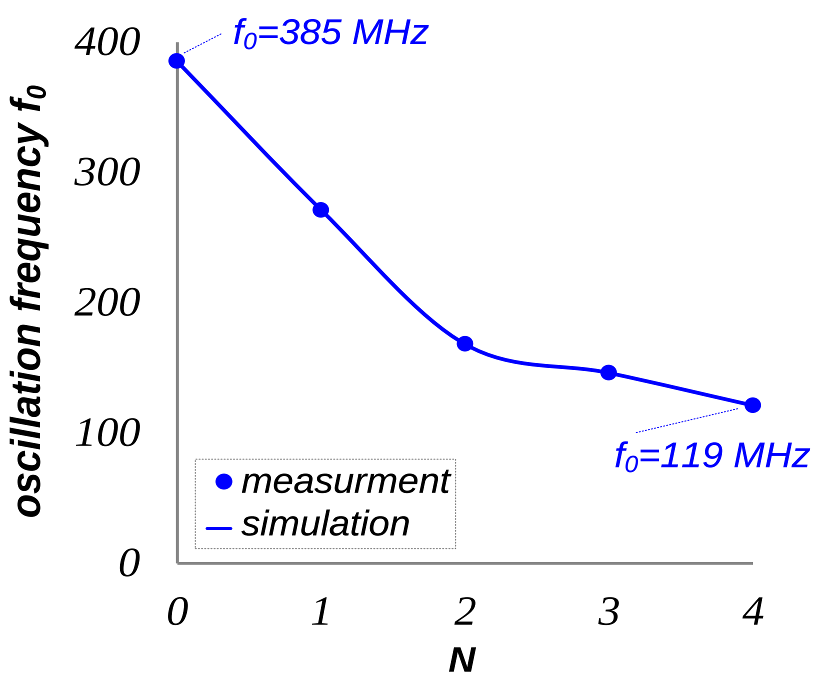
With Microsemi FUSION FPGA
(FLASH - 130 nm CMOS)

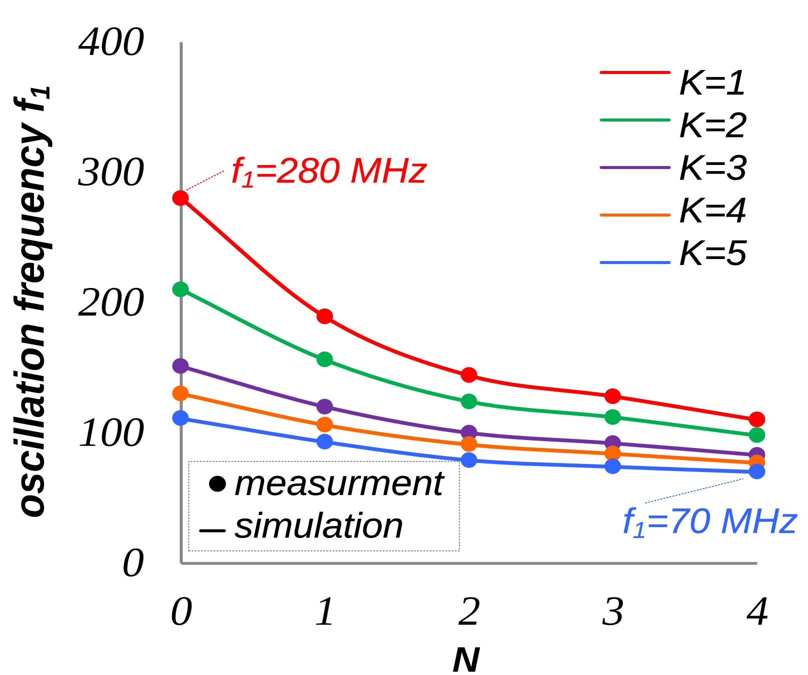


Ultra lightweight BFSK transmitter

- Transmission on the EM channel (contactless)
- Configurable ring-oscillator
  - Two frequencies generator $f_0 > f_1$
  - Two parameters *N* and *K*
  - *Size in number of LUT4 = 1+K+N*

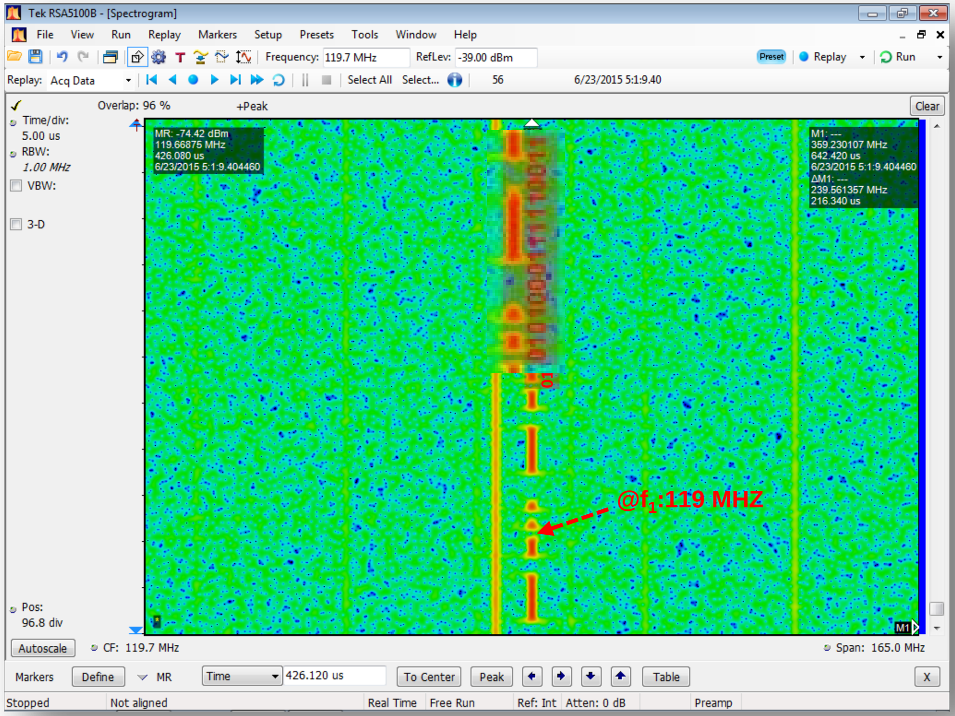
With Microsemi FUSION FPGA
(FLASH - 130 nm CMOS)

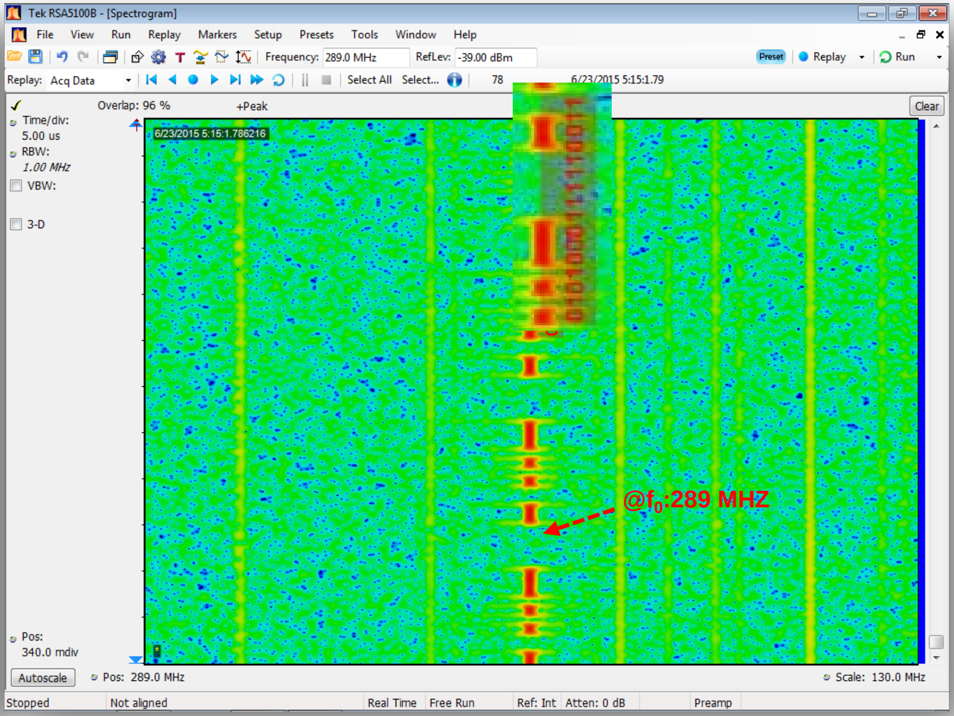




First experimentation – BFSK only

- Spectral cartography (amplitude vs time)
  - By using slippery window spectral analysis





Comparison with state-of-the art spy circuits

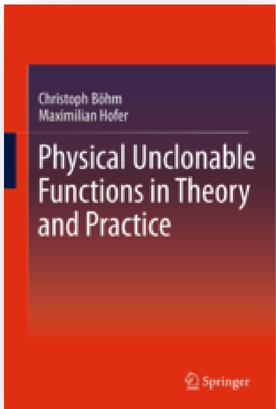
- Spy circuits in the literature
  - Applications: Hardware Trojan (malware) or IP Protection (salware)
  - Used side channel (SC): Thermal emanation (***TH***), Power consumption (***PC***) Electromagnetic emanation (***EM***)
  - Year of publication (YoP): since 2008

Ref	YoP	*SC*	Hardware resources	Bite rate
[5]	2008	*TH*	255 Spartan-3 Slices	7.10^{-3} bps
[6]	2008	*PC*	16*16 bit circular shift-register	200 bps
[9]	2009	*PC*	8 parallel Dff or 16 bit circular shift register	485 bps
[7]	2010	*PC*	16-bit circular shift register	500 bps
[10]	2013	*PC*	16-bit circular shift register per bit	976 bps
Our work	**2015**	***EM***	**1 configurable RO**	**1 Mbps**

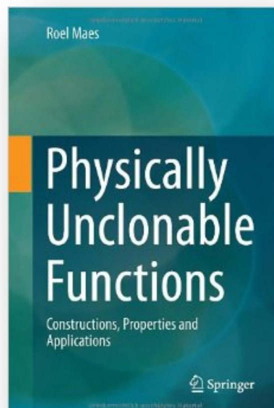
1024 times bigger data rate

More information on PUF and Watermarking

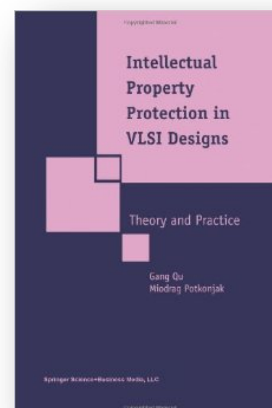
- Springer 2013, Graz University of Technology, Austria
  - eBook is provided DRM-free on the Springer web page



- Springer 2013, KU Leuven, Belgium



- Kluwer 2003, UCLA, USA



Conclusion

Synthesis

- Strategic issue for developed countries
  - Leadership on the semiconductor market
  - Limitation of illegal / malicious activities

- Many threats / many solutions
  - Filter out numerous publications (lot of publication noise)
  - Use a realistic threat model
  - Propose realistic and industrial solutions
  - Combine proposed solutions

- Need to develop specific skills
  - VLSI design / analog design
  - IC manufacturing
  - Hardware security
  - Applied cryptographic (need very-lightweight crypto)

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

This work was part of the SALWARE project

"The **SALWARE** project has received funding from the French ANR research and innovation programme under grant agreement number ANR-13-JS03-0003. It also supported by the French FRAE”

If you need further information, please contact the coordinator:
lilian.bossuet@univ-st-etienne.fr
Project web site: http://www.univ-st-etienne.fr/salware/

PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR

Fondation de Recherche pour l' Aeronautique & l' Espace

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

lilian.bossuet@univ-st-etienne.fr

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

For fun: are you sure to be free of counterfeit parts?

- Friday 27th February 2015, 2 p.m.
  - Fire alarm in my Laboratory
  - Localization: the office next door (opposite)

- Fire's origin
  - A "Xilinx" Platform Cable USB for FPGA configuration
  - Chinese label, unknown and untraceable provider: 306Studio.com