Salutary hardware – a state of the art

Lilian Bossuet

Associate Professor, CNRS Chair of Hardware Security

Jean Monnet University, Saint-Etienne

Protection of the intellectual property of the fabless designers

why ?

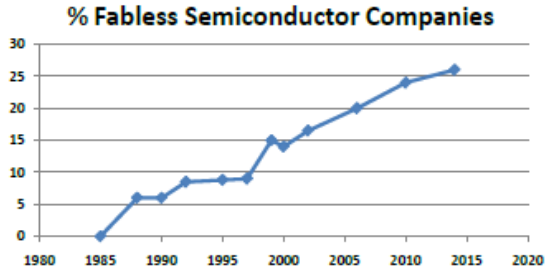
Semiconductor market

- Market increase
  - + 35% from 2009 to 2013 (305 billion of US $)
  - 2014 : expected to reach 316 billion of $
- 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]
  - G450c Investment: 4.4 billion of US $
- 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.

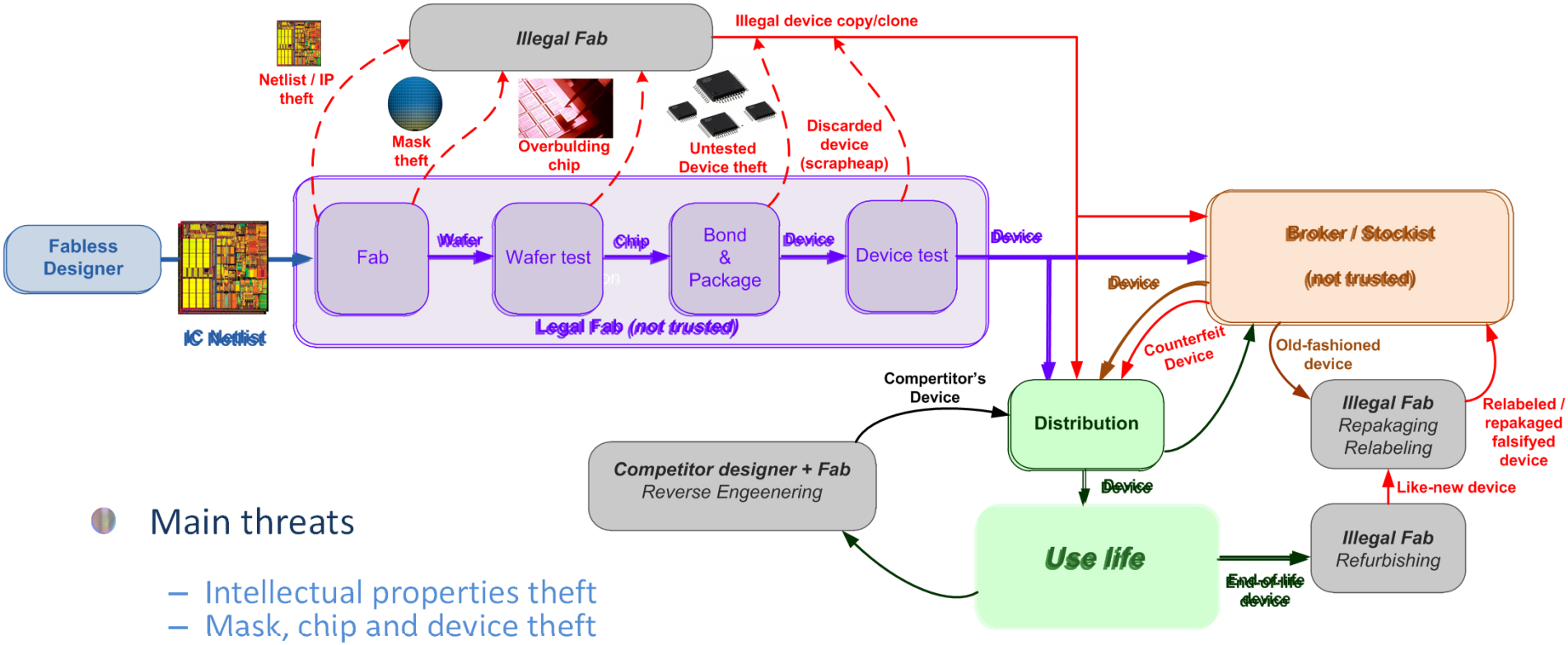
Tech.	Transistors	Manufacturing costs
130 nm	9 millions	9 millions €
90 nm	16 millions	18 millions €
65 nm	30 millions	46 millions €

Rapport Saunier, 2008



F. Koushanfar 2011

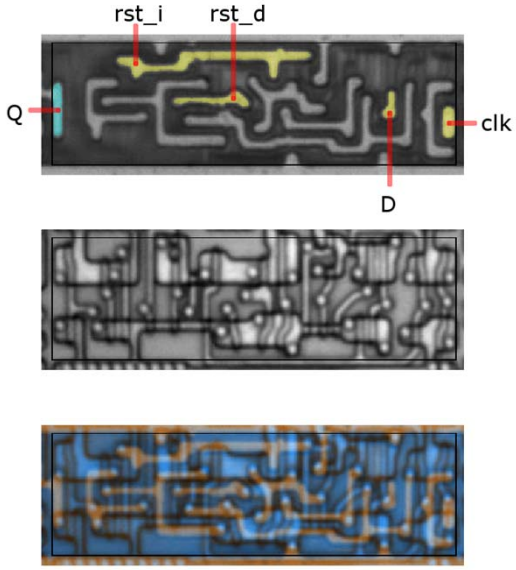
Threat model during manufacturing, supply chain and use life



- 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)

Typical Threats

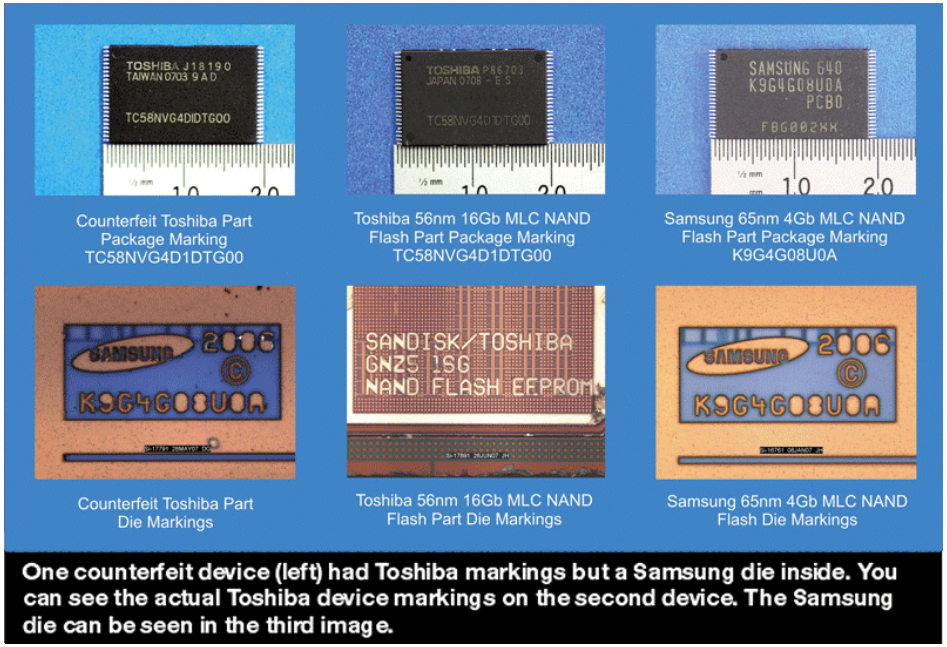
- Reverse engineering



Source: http://siliconzoo.org

- Chip salvaging / refurbishing

- Counterfeiting
  - Relabelling



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

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 EU's external border control secured 178 million of counterfeit items
  - Watch, leather goods, article of luxury, clothing, pharmaceuticals, tabacco, electronics products

- Estimation of counterfeiting of the word semiconductor market is between 7% and 10% [1]
  - Financial loss of 22 billion $ in 2014 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

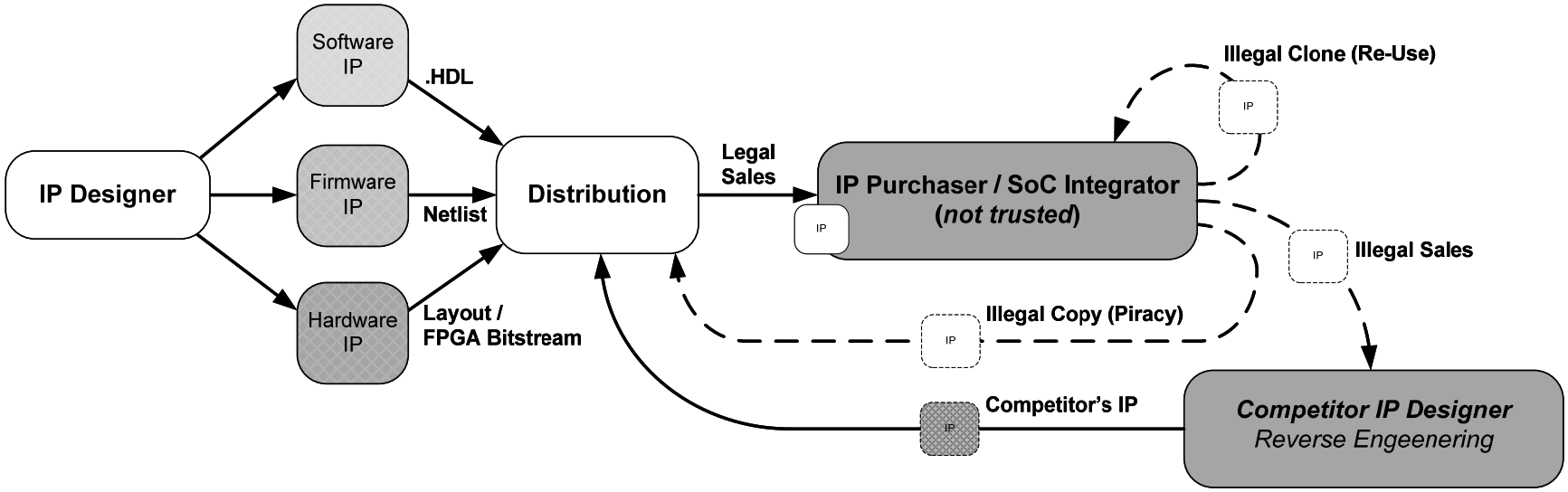
The rise of electronic device counteirfetings

[1] C. G… IEEE Spectrum, June 20…
[2] IHS-E… …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

Threat model for IP market



CURRENT INDUSTRIAL SOLUTIONS

Counterfeiting physical detection
Circuit camouflaging

Counterfeiting physical detection

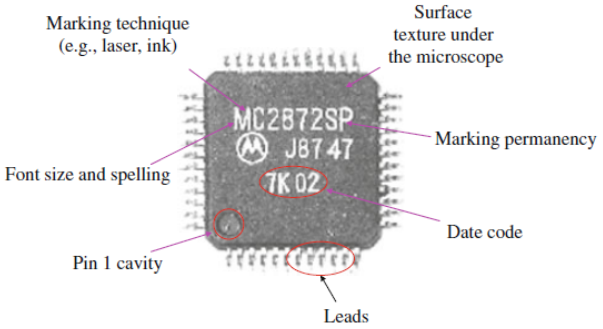
- Industrial means of detection
  - Marking permanency testing, visual inspection

Before

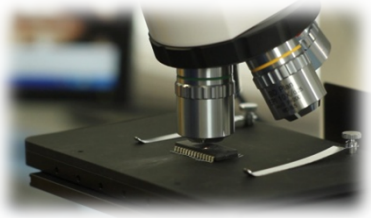
After

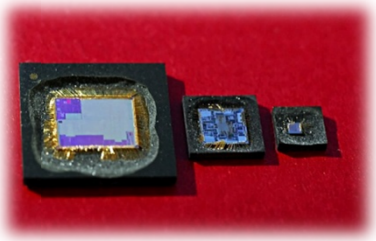
Fake Atmel

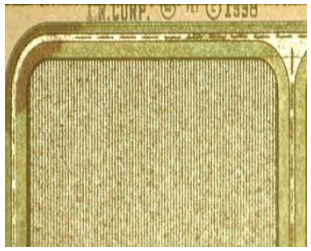

Fake Motorola

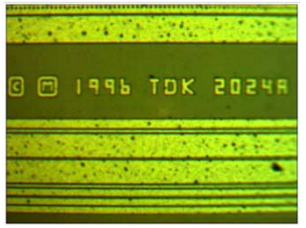


  - Decapsulation and high resolution optical inspection (reverse-engineering)

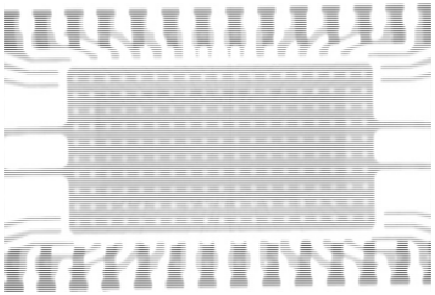


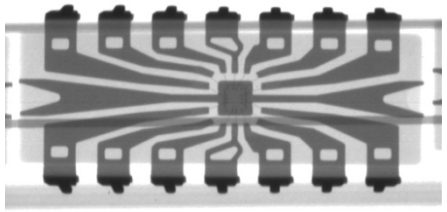






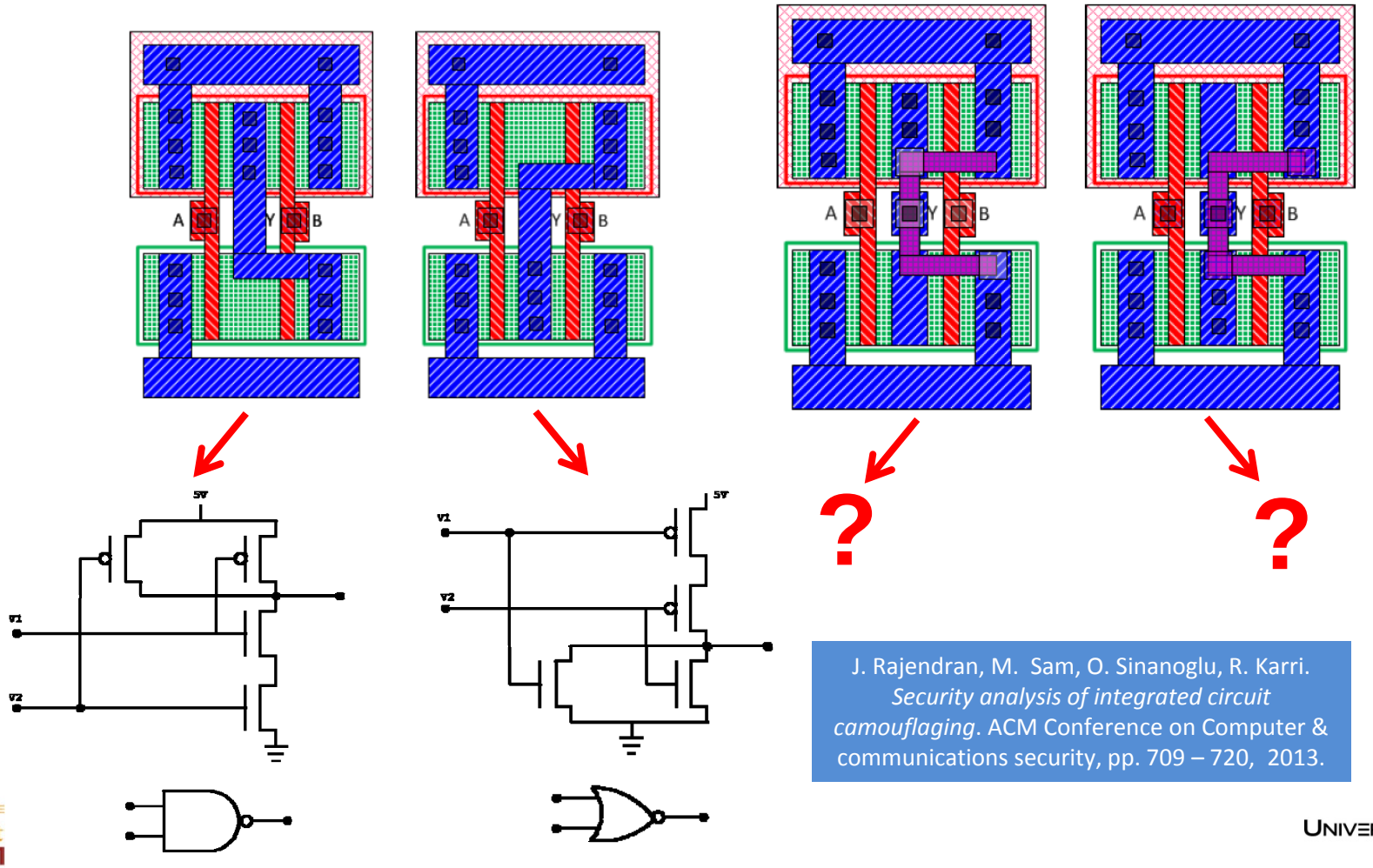
  - X-ray inspection





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

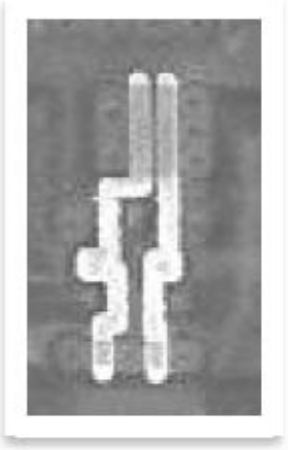


Figure 1: *Conventional 2 input NOR Gate*

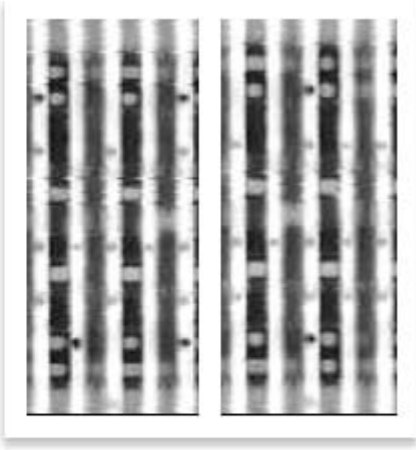


Figure 2: *SML 2-input NAND and NOR Gates*

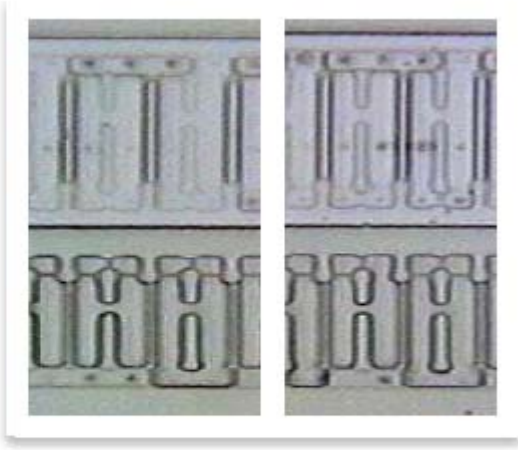


Figure 3: *SML 2-input NAND and NOR Gates without Metal*

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

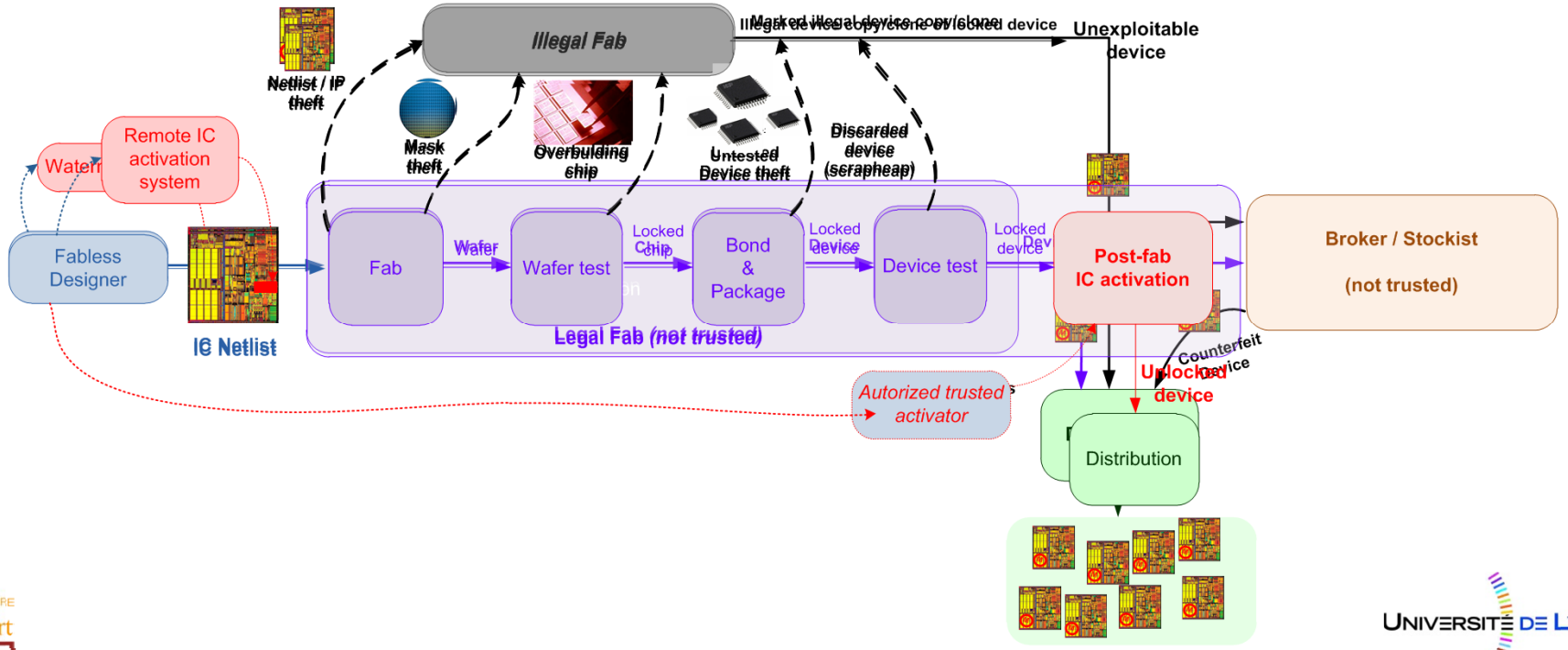
HARDWARE SOLUTION : SALWARE

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.

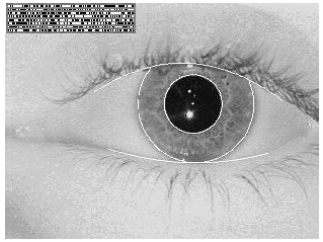


PASSIVE SALWARE

IC identification

Fingerprint / Watermark

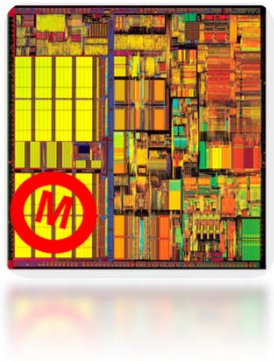
- Fingerprint
  - Measurement of a physical (or behavioral) characteristics



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

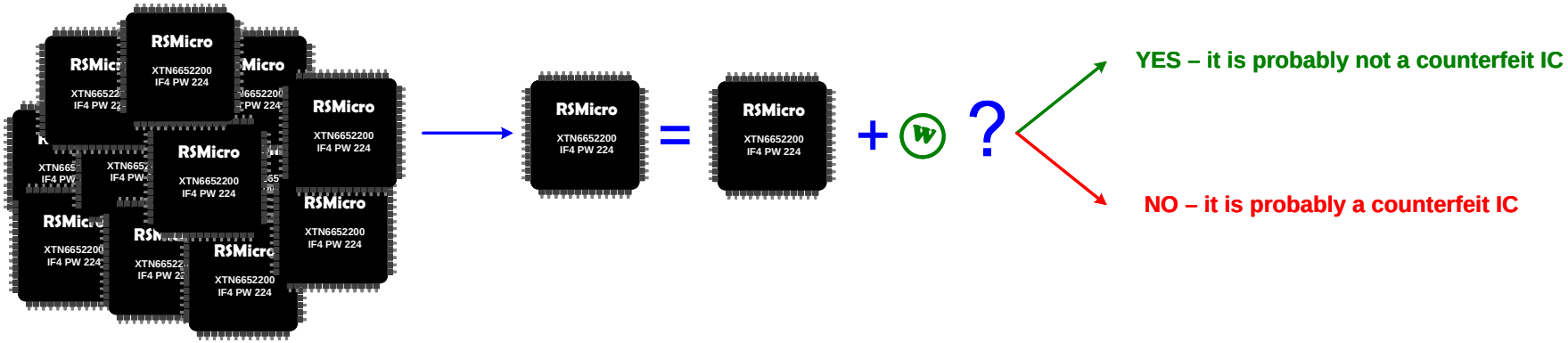
- Silicon PUF
  - Extraction of entropy from CMOS process variation

- Silicon Watermark

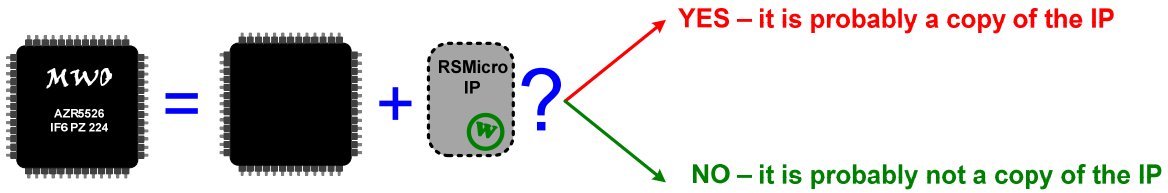


Watermark

- Detection of IC counterfeiting
  - Set of good referenced ICs



- Detection of IP theft (illegal copy/use)

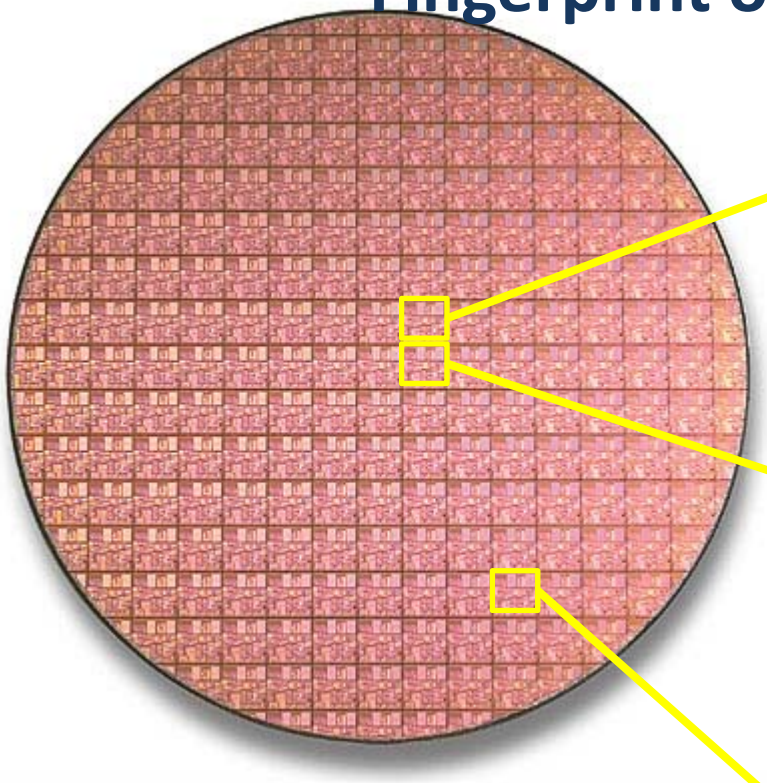


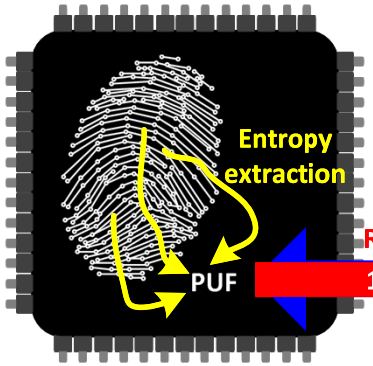
PUF

- Identification of IC
  - Used for active SALWARE
  - Cryptographic key generation
  - Set of ICs
  - Challenges / responses protocol

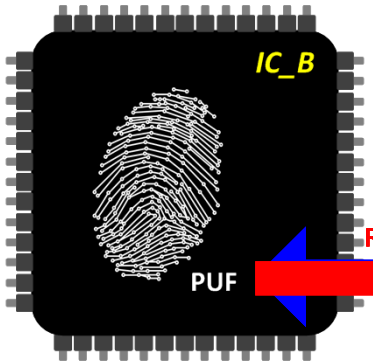
ID	IC
AF30	
37B1	
8992	
FE72	
E90B	
5129	
8C9D	
253A	

Fingerprint of IC – Silicon PUF

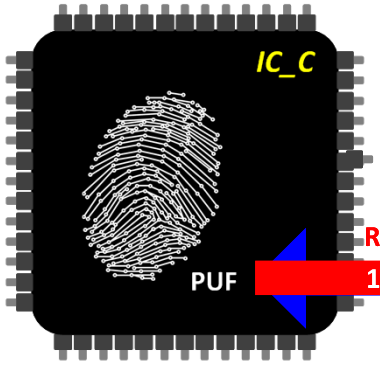




Response A
101001011
Unpredictable
Unique
High steadiness



Response B
01100010
Unique

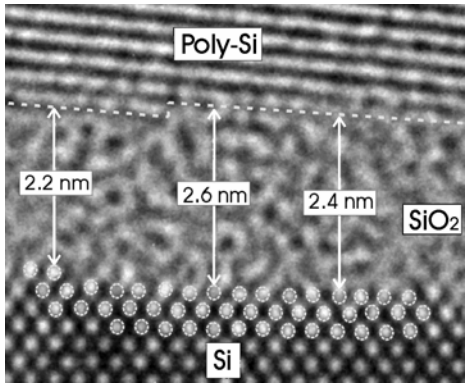


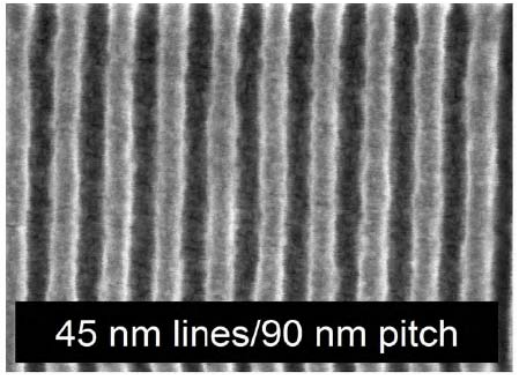
Response C
110011101
Unique

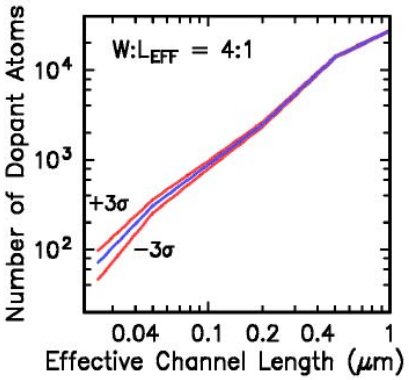
- Silicon PUF
  - Extraction of entropy from CMOS process variation

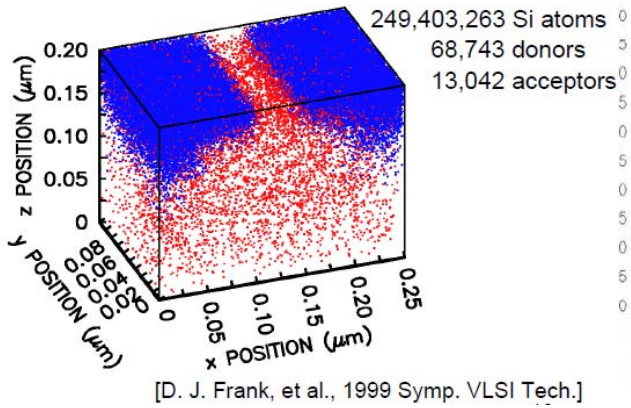
CMOS process variation

- Example
  - Oxide thickness
  - Metal line
  - Number of dopant atoms
  - Position of dopants
  - Doping density

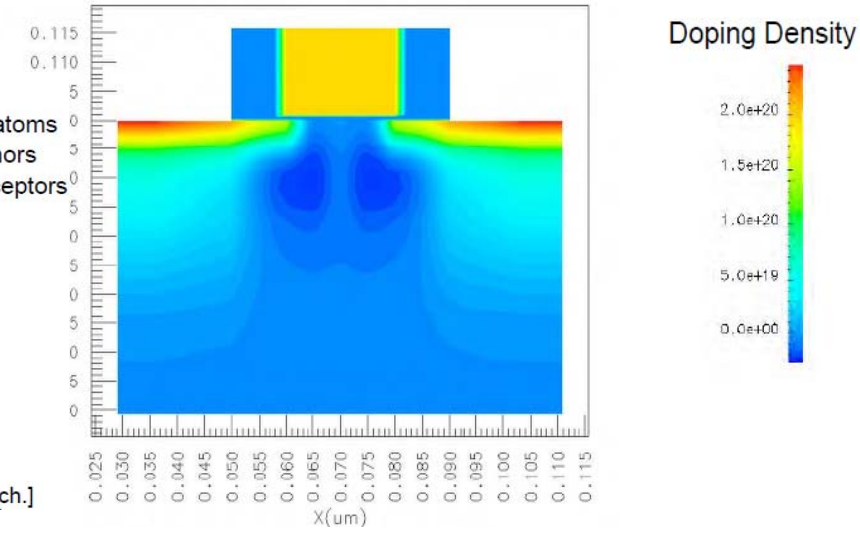






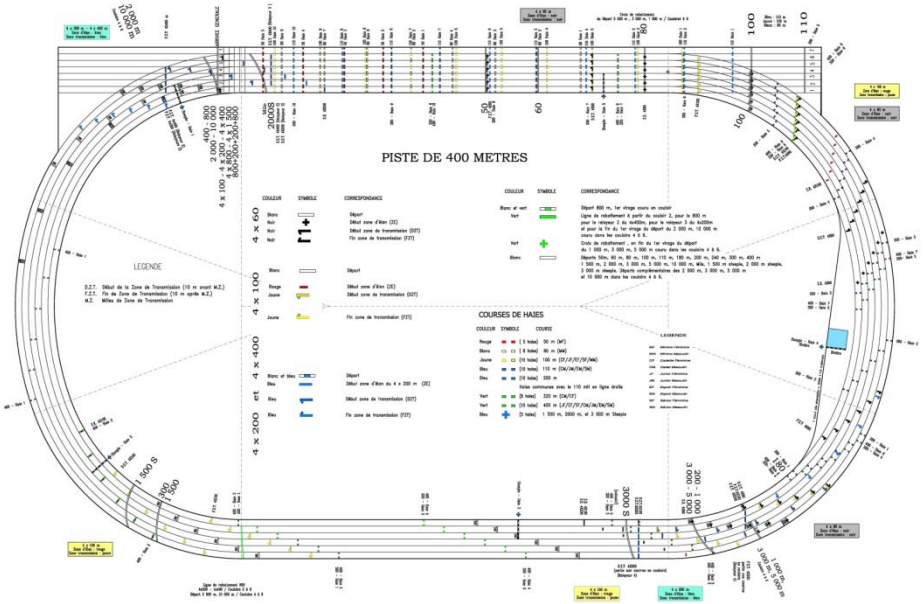


[D. J. Frank, et al., 1999 Symp. VLSI Tech.]



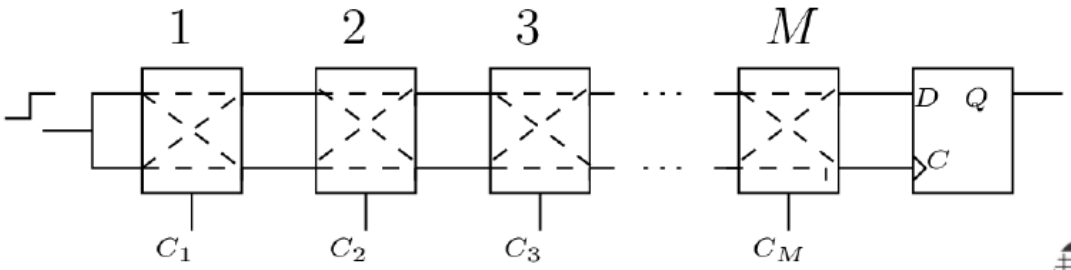
Principe: compare (theoretically) identical things !

- Example of an athletic race of clones
  - All the runners are identical (same doping)
  - Theoretically, all the lines on the stadium are the same
  - The winner have run on the shorter line!

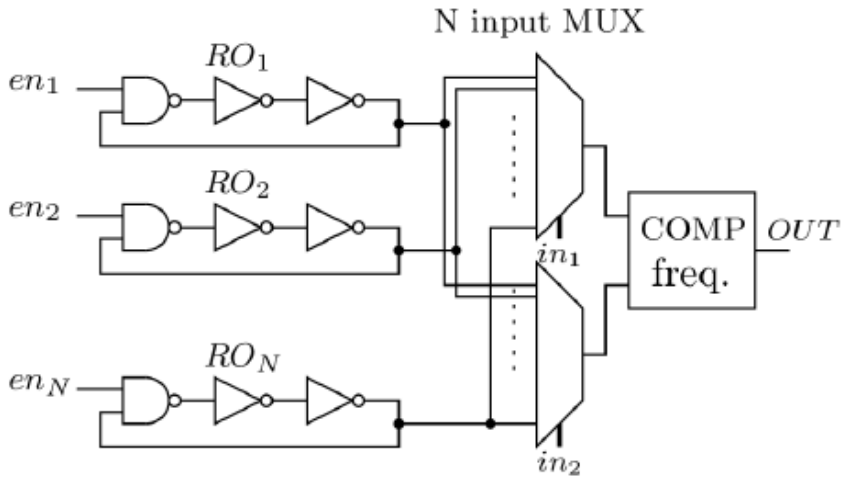


PUF Architectures

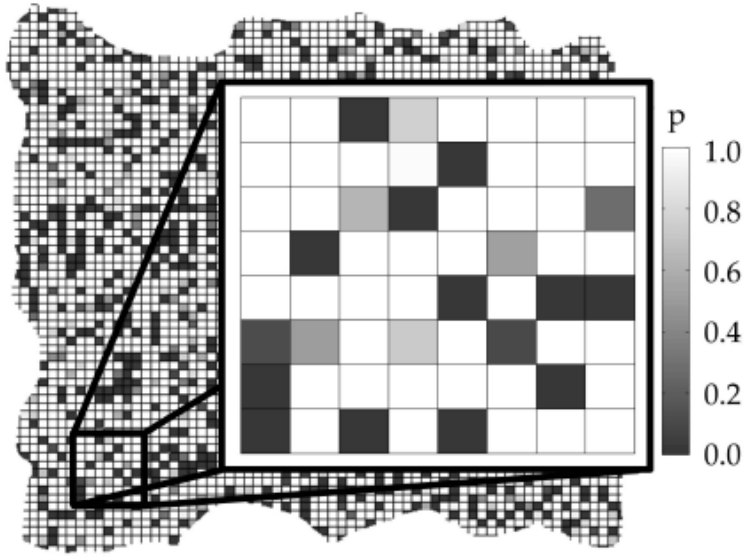
- Three main architectures
  - Race of delays between two symmetrical delay lines – Arbiter PUF
  - Frequency mismatch in multiple ring-oscillators – RO-PUF, loop-PUF
  - Metastability of a couple of cross-coupled elements – SRAM PUF, Butterfly



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.

Who are the best candidate for FPGA and ASIC implementation?

- Morozov et la., ARC 2010
  - Arbiter VS RO VS Butterfly
  - Target Xilinx Spartan-3E FPGA
  - ***"Symmetry requirements for Arbiter and Butterfly PUF cannot be satidfied using available FPGA routing schemes …. Such a RO based PUF can produce a working PUF"***

S. Morozov, A. Maiti, P. Schaumont, "A Comparative Analysis of Delay Based PUF Implementations on FPGA," 6th International Symposium on Applied Reconfigurable Computing, March 2010

- Maiti et al., HOST 2010
  - RO PUF
  - 125 Xilinx Spartan-3E FPGA, 512 RO/FPGA
  - ***"RO-PUF output signatures are fairly uniformly distributed with high rate of uniqueness in terms of inter-die Hamming distance"***

A. Maiti, J. Casarona, L. McHale and P. Schaumont, "A large scale characterization of RO-PUF," *in Proc. of Int. Sym. on Hardware-Oriented Security and Trust (HOST),* IEEE, 2010, pp.94-99.

- Maiti et al., NIST worshop 2011
  - Arbiter VS RO
  - 193 Xilinx Spartan-3E FPGA
  - ***"RO-PUF exhibited better performance compared to Arbiter PUF even if the former is implemented on a bigger device"***

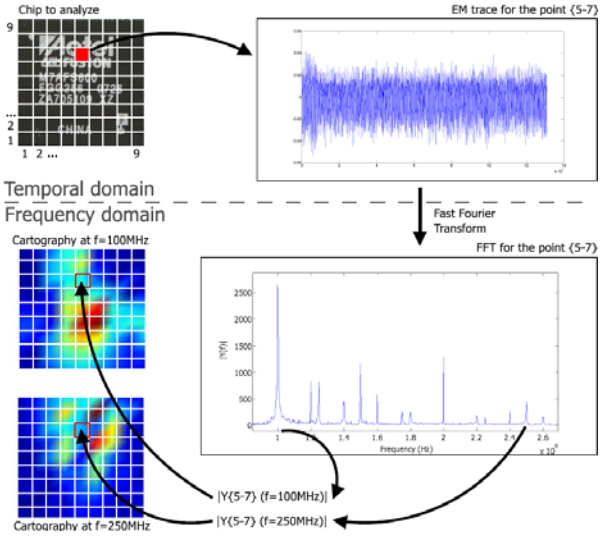
A. Maiti, J. Casarona, L. McHale and P. Schaumont, "A Framework for the Evaluation of Physical Unclonable Functions," *in Proc. of NIST Work. on Crypto. For Emerging Tech. and Appl.,* 2011.

- Katzenbeisser et al., CHES 2012
  - Arbiter VS RO VS SRAM VS FF and latch
  - Target: 96 ASIC TSMC 65 nm CMOS
  - ***"The SRAM and RO PUFs achieve almost all desired properties of a PUF"***

S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A.R. Sadeghi, I. Verbauwhede, C. Wachsmann. "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonalble Functions Cast in Silicon" *in Proc. of Int. Conf. on Cryptographic Hardware an Embedded Systems (CHES)*, Spinger, LNCS, vol. 7428, 2012, pp. 283-301.

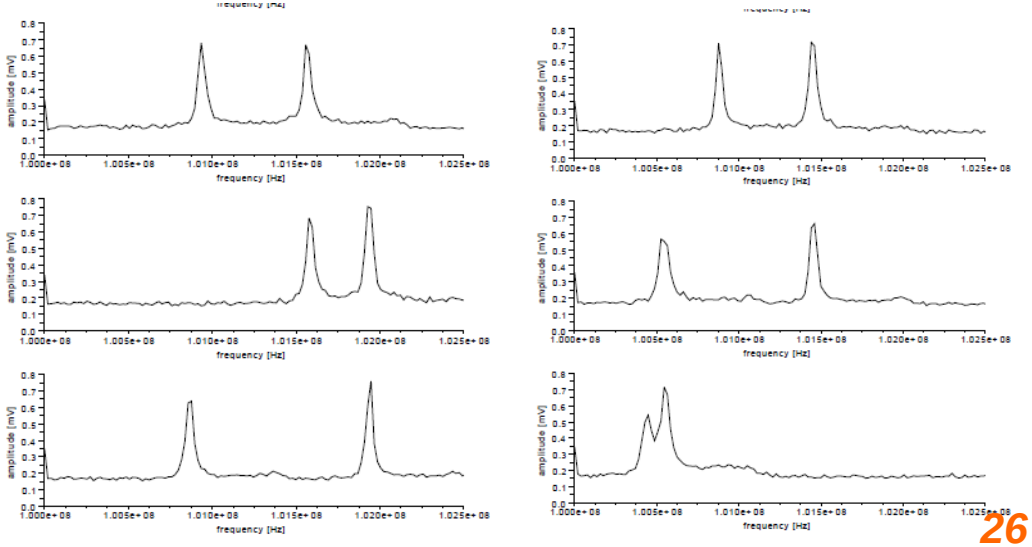
Bad news: *find the RO frequencies …*

- APEMC 2013: EM analysis on RO-TRNG
  - Method: using the electromagnetic radiation to analyze RO-TRNG
  - Finding : RO frequencies and physical localization
  - EM frequency cartographie
  - Differential frequency analysis (2 VDD)



P. Bayon, L. Bossuet, A. Aubert, V. Fischer. EM radiation analysis on true random number generators: Frequency and localization retrieval method. In Proceedings of the IEEE Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility (APEMC 2013),Melbourne, Australia, May 2013.

- Similar results with RO-PUF
  - Fraunhofer Institution AISEC
  - TU Müchen

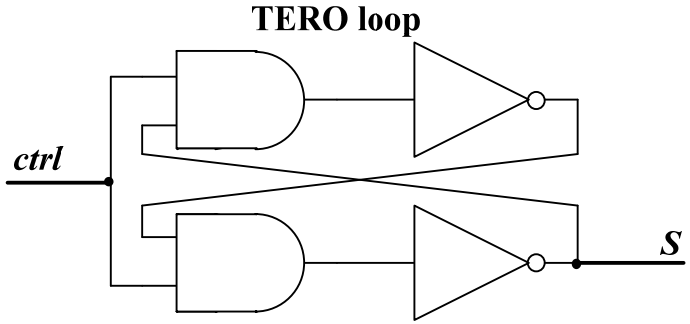


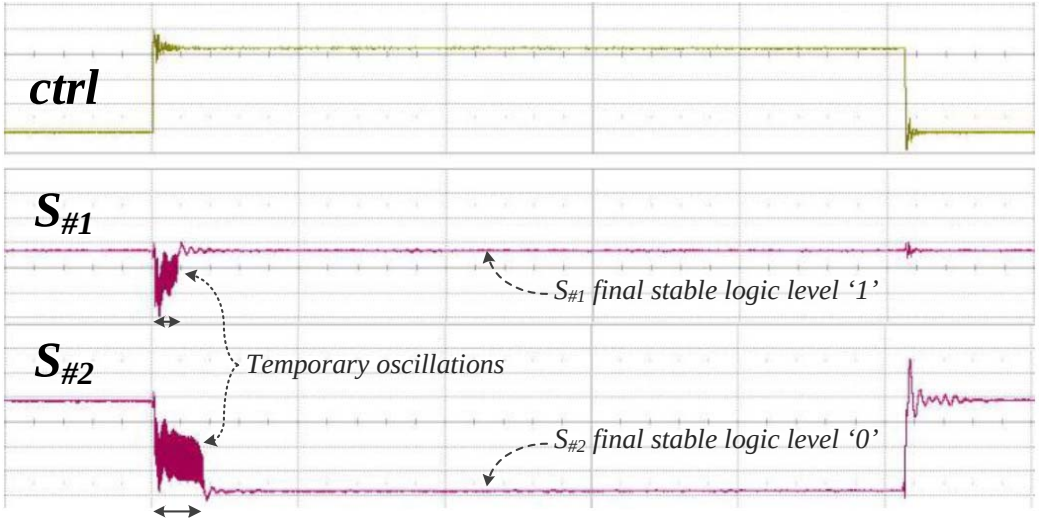
D. Merli, D. Schuster, G. Sigl, “Semi-invasive EM attack on FPGA RO PUFs and Countermeasures” In *Proc. of the Workshop on Embedded Systems Security (WESS)*. ACM, New York, NY, USA, 2011, Article 2, 9 pages.

These works challenge the use of RO for secure TRNG and PUF design

The TERO-PUF: a PUF based on transient effect ring oscillator

- Transient Effect Ring-Oscillator, the *TERO loop*
  - Composed of a SR flip-flop (one AND gate and a, even number of inverters)
  - TERO loop uses SR flip-flop with oscillatory metastability
    - S and R are connected to *ctrl* signal
  - Mixed structure between RO and Butterfly
    - Oscillatory mode
    - PUF and TRNG

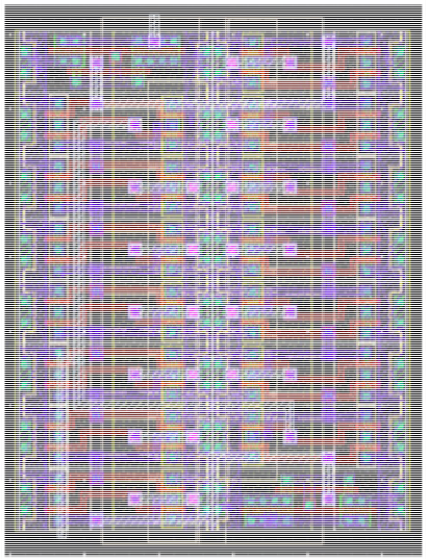


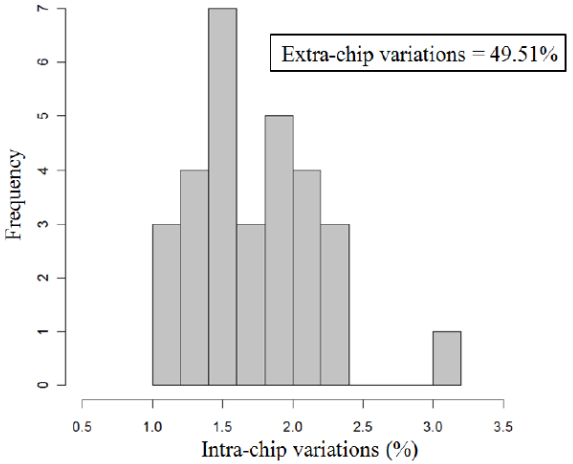


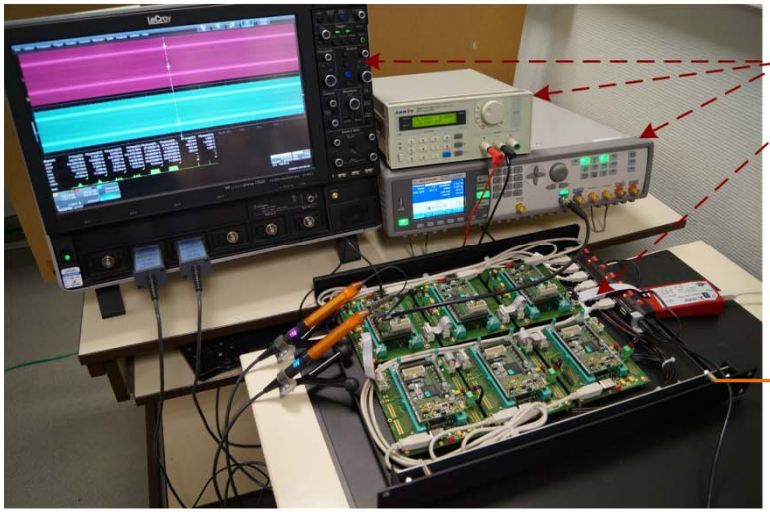
L. Bossuet, X. T. Ngo, Z. Cherif, V. Fischer. *A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon*. IEEE Transactions on Emerging Topics in Computing, Vol. 2, Issue 1, pp. 30-36, *2014*.

Hardware implementation and characterization

- Experimental setup
  - 30 ASIC (350 nm CMOS technology)
  - 30 FPGA Xilinx Spartan 6
  - 30 FPGA Altera Cyclone 5
  - 256 TEROs / chip
  - 7 inverter per TERO branch
  - 128-bit, 256-bit or 384-bit ID size
  - Temperature range -20°C / + 70°C
  - Vdd range 3V – 3.6V (*nom 3.3V*)

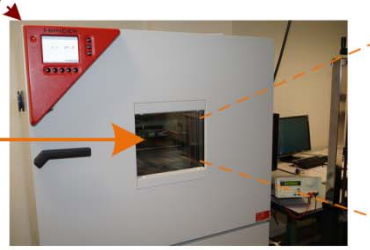






Automatic testbench for PUF charaterisation

- LeCroy oscilloscope, remote controlled power supply and clock generator
- Dedicated mother boards to 6 modules
  - LaHC 350nm ASIC (30 available modules)
  - Xilinx Spartan6 (30 available modules)
  - Altera Cyclone V (30 available modules)
- Binder drying oven -20°C / +180°C

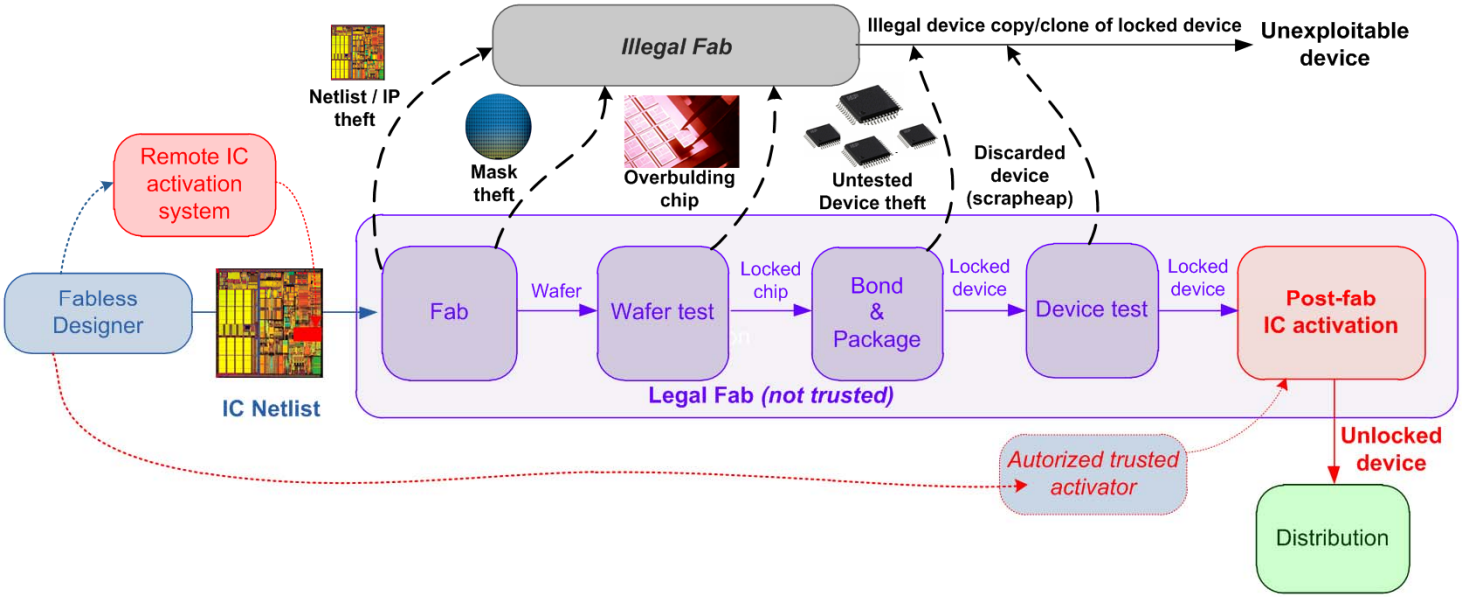


ACTIVE SALWARE

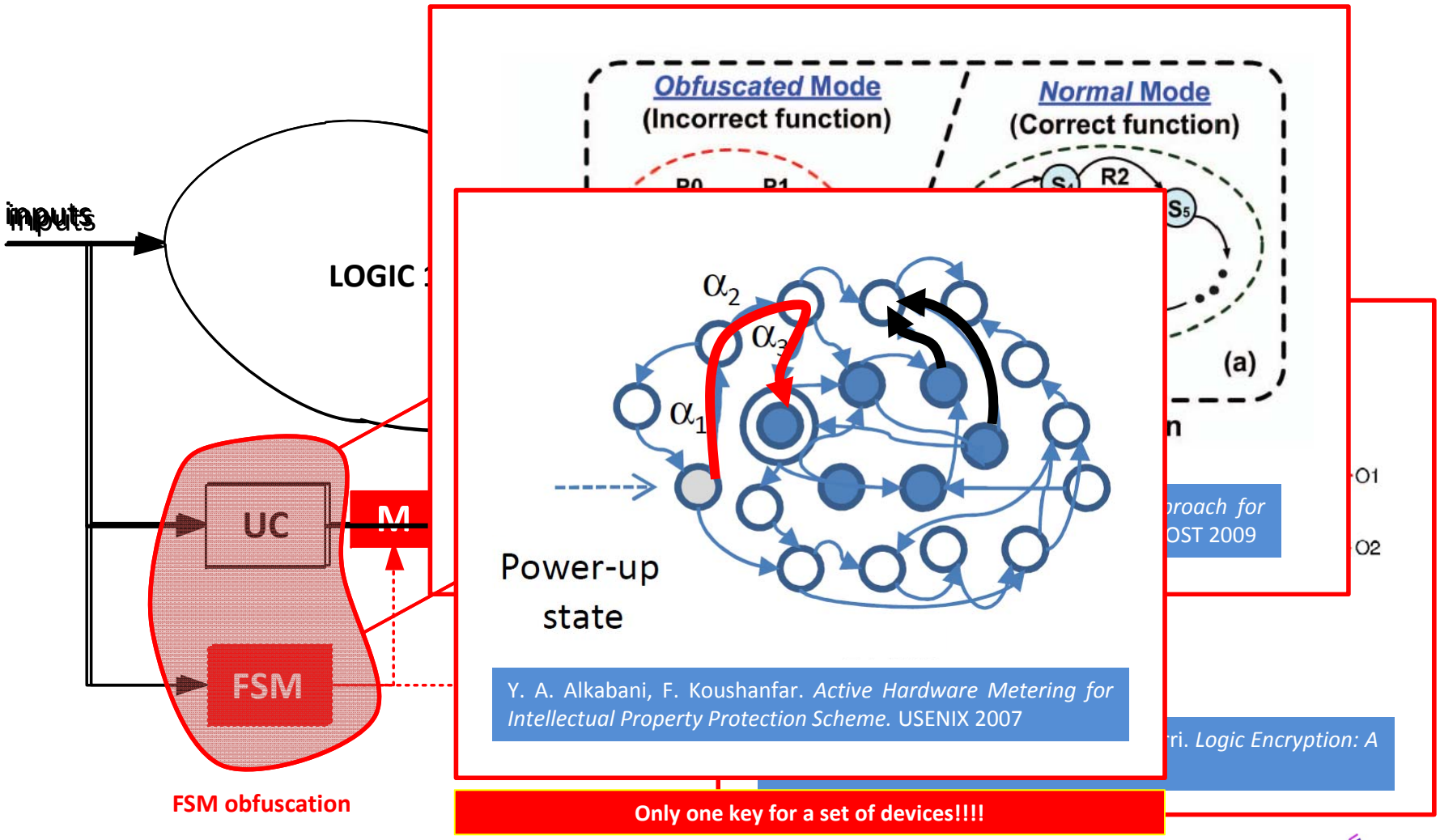
protection

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

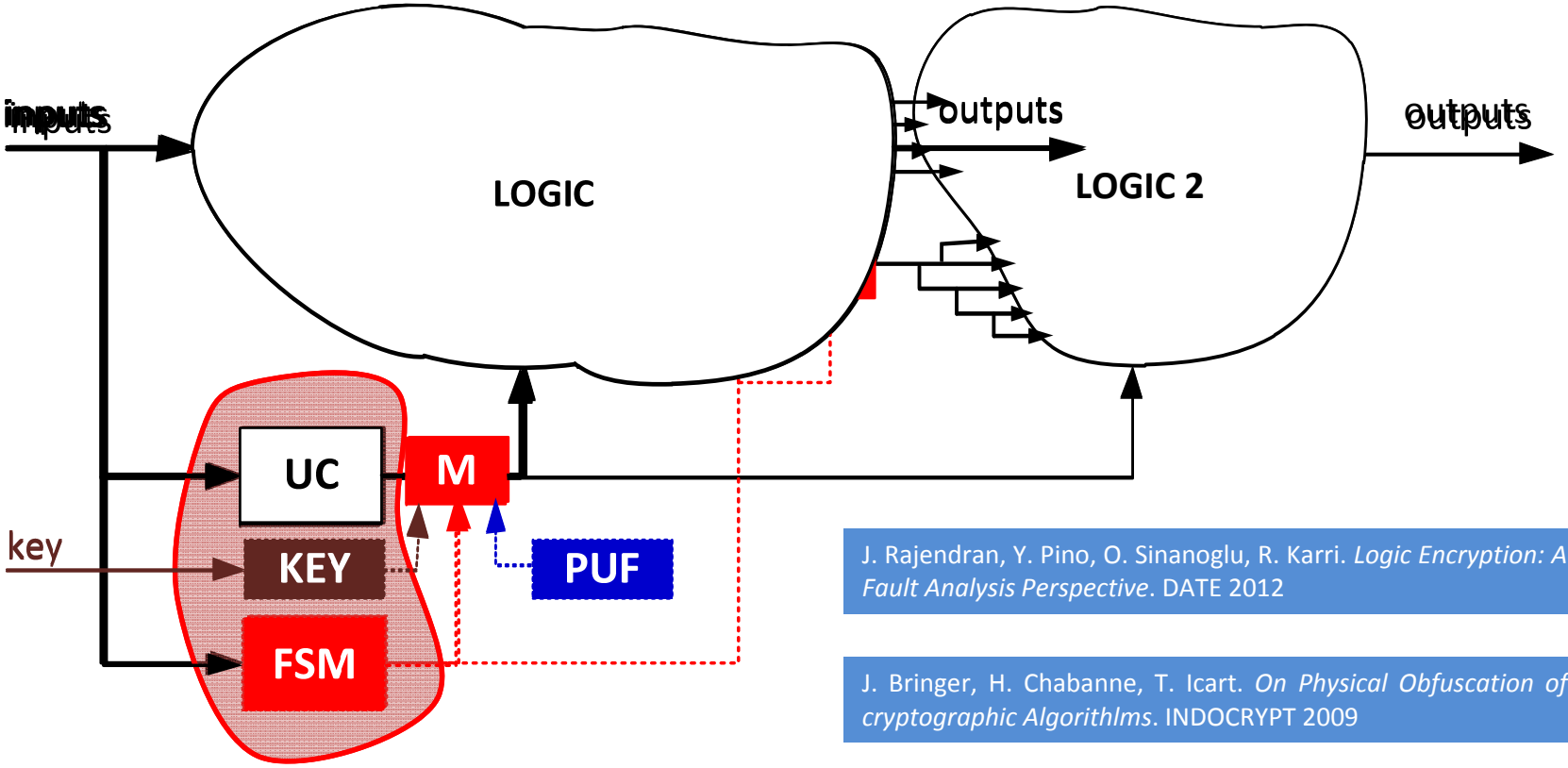


Logic *encryption* / FSM *obfuscation*



Logic *encryption* / FSM *obfuscation*

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



FSM obfuscation

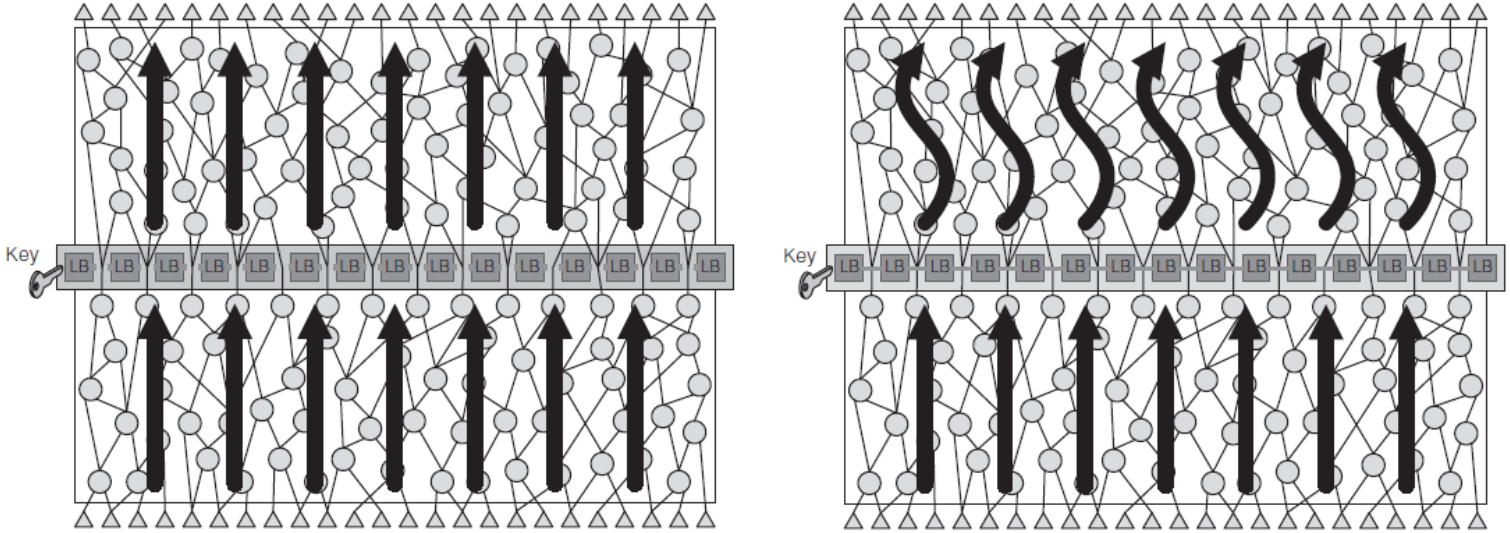
J. Rajendran, Y. Pino, O. Sinanoglu, R. Karri. *Logic Encryption: A Fault Analysis Perspective*. DATE 2012

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

Data-path *encryption*

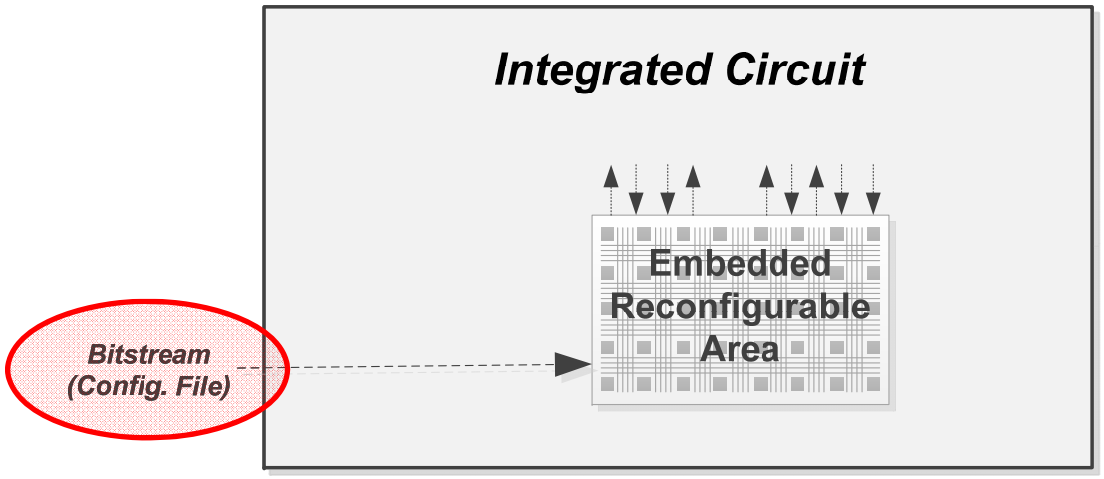
- Reconfigurable logic barriers
  - The barriers are implemented with LUT
  - Reconfigurable « firewall »
  - Need of an heuristic to place the logic barriers
    - Any increase of the critical path



A. Baumgarten, A. Tyagi, J. Zambreno. *Preventing IC Piracy Using Reconfigurable Logic Barriers*. IEEE Design & Test of Computers, January/February 2010

Design obfuscation

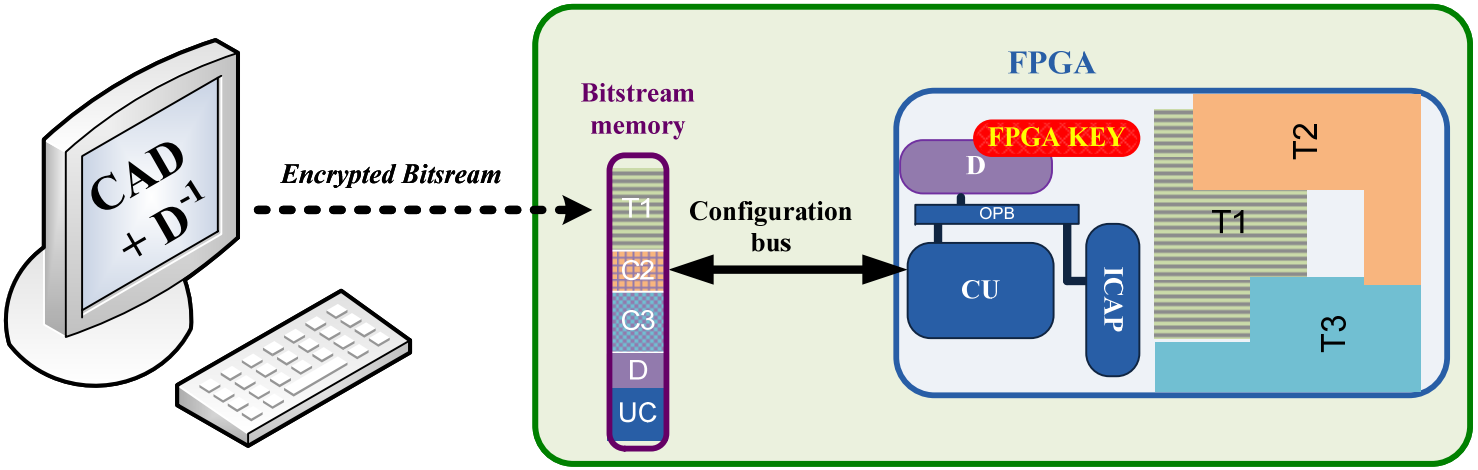
- Obfuscation by using reconfigurable area
  - Countermeasure to reverse-engineering
  - "High-information" parts have to be include in the reconfigurable area
    - Control Unit
    - Processor instruction decoder
  - Need encryption of the bitstream
    - Anti-cloning
    - One bitsream (encrypted)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



[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.

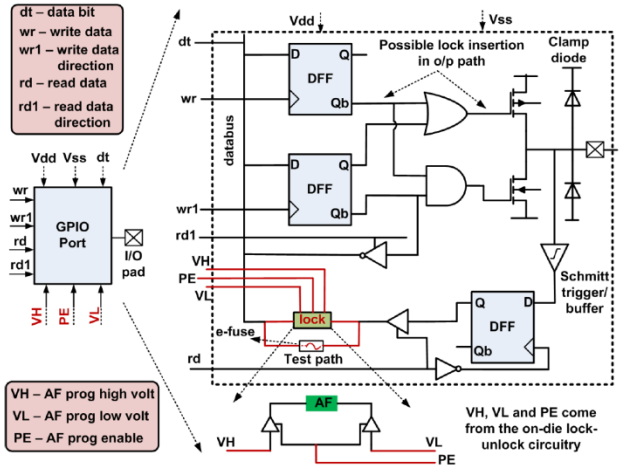
[3] Y. Hori, A. Satoh, H.Sakane, and K. Toda. *Bitstream encryption and authentication with AES-GCM in dynamically reconfigurable systems.* FPL 2008

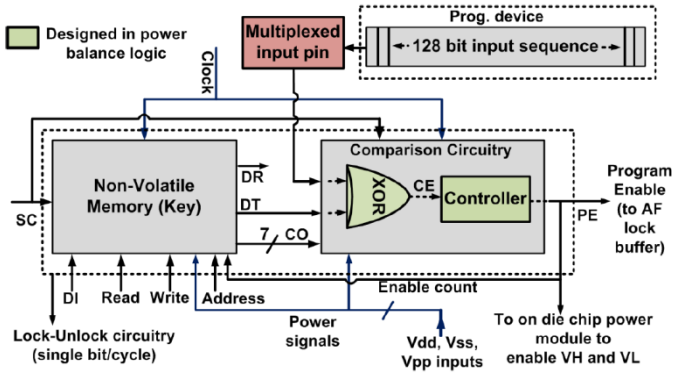
[4] S. Drimer and M. G. Kuhn. *A Protocol for Secure Remote Updates of FPGA Configurations.* ARC 2009.

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

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”

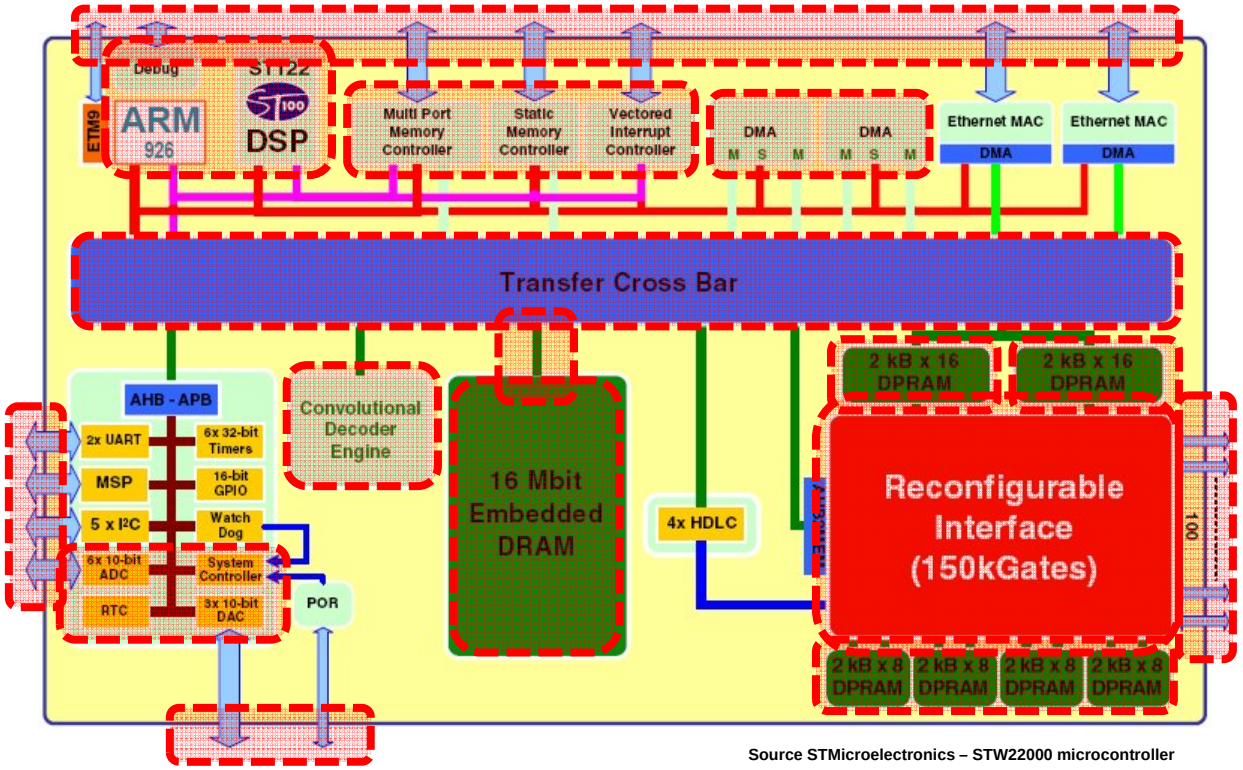




Z. Liu, Y. Li, R. Geiger, and D. Chen. *Active Defense against Counterfeiting Attacks through Robust Aantifuse-based On-Chip-Lock*. VLSI Test Symposium 2014

Locking of a System-on-Chip

- What it is possible to lock in a SoC?
  - Control unit : FSM obfuscation/ FSM register encryption/ microprocessor obfuscation
  - Treatment unit: Logic encryption/obfuscation
  - Internal communication: bus encryption / Cross Bar routing obfuscation / NoC locking
  - 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

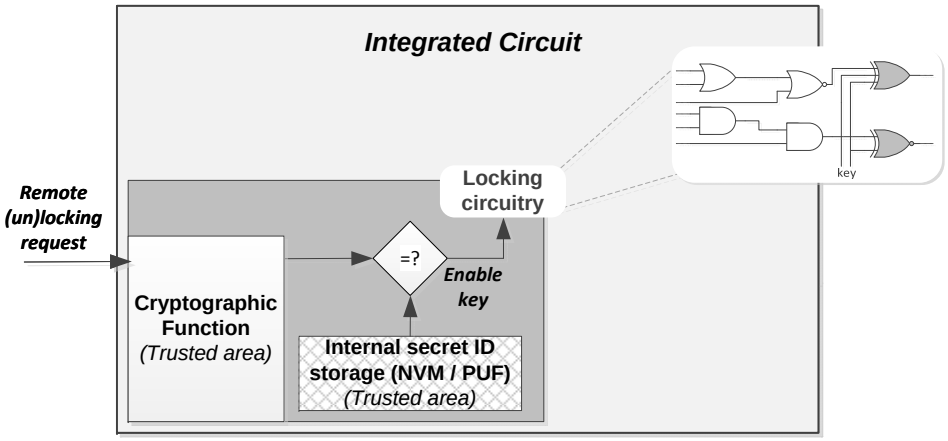
Active Salware Design

- 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

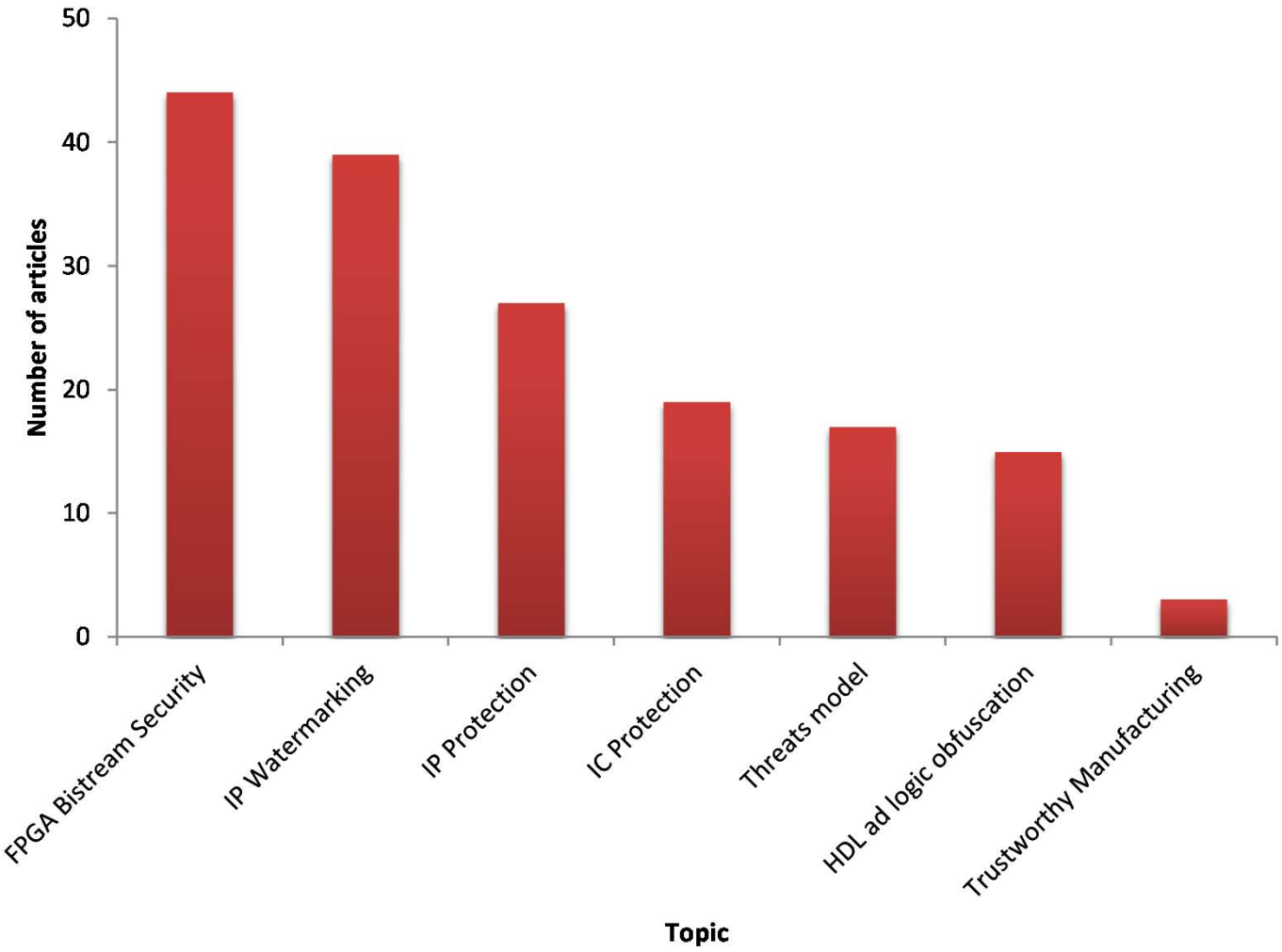


SALWARE

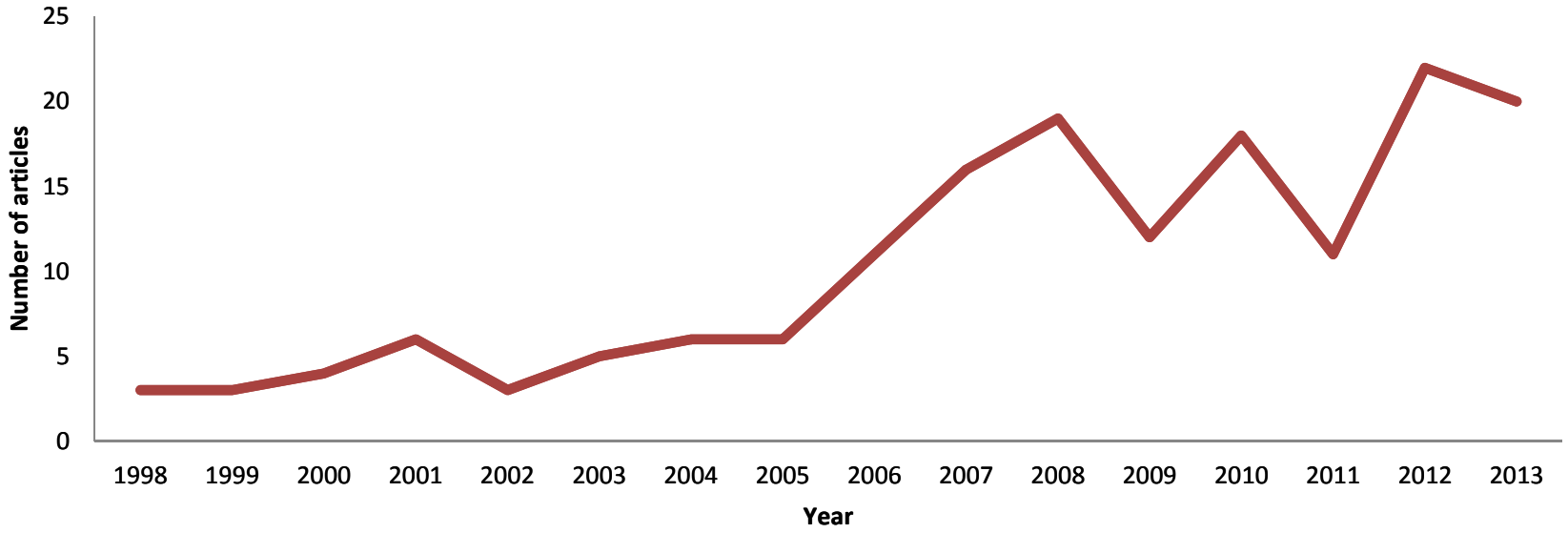
French ANR Project

- 42 month research project
  - Funding: ANR / FRAE
  - Additional funding: Région Rhône-Alpes
- Bibliography on the project's web site
  - More than 200 references (1999-2014)
  - http://www.univ-st-etienne.fr/salware/bibliography.html
    - Threats model
    - IC protection
    - IP protection
    - IP watermarking
    - FPGA bitstream security
    - HDL and logic obfuscation
    - Trustworthy manufacturing

Publications per topics

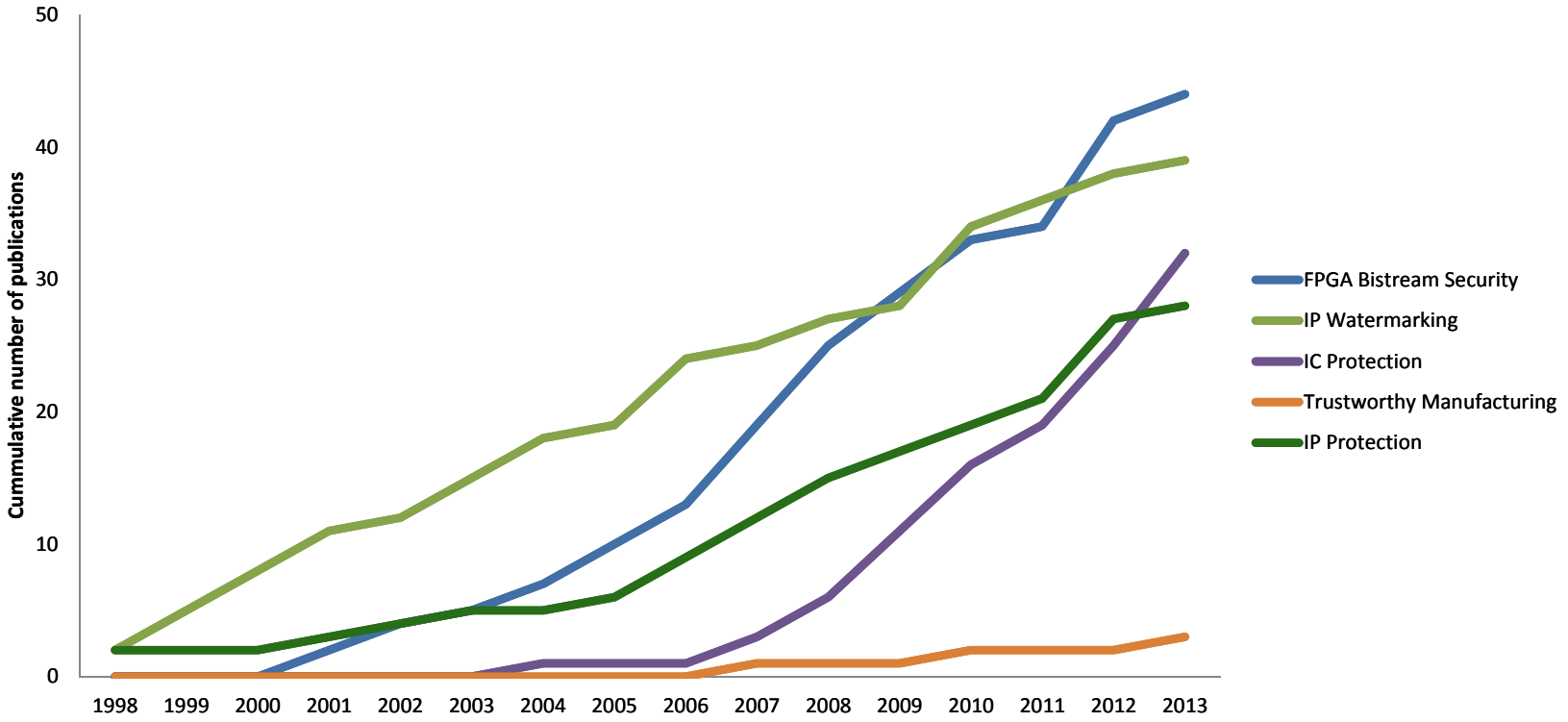


Publications per year

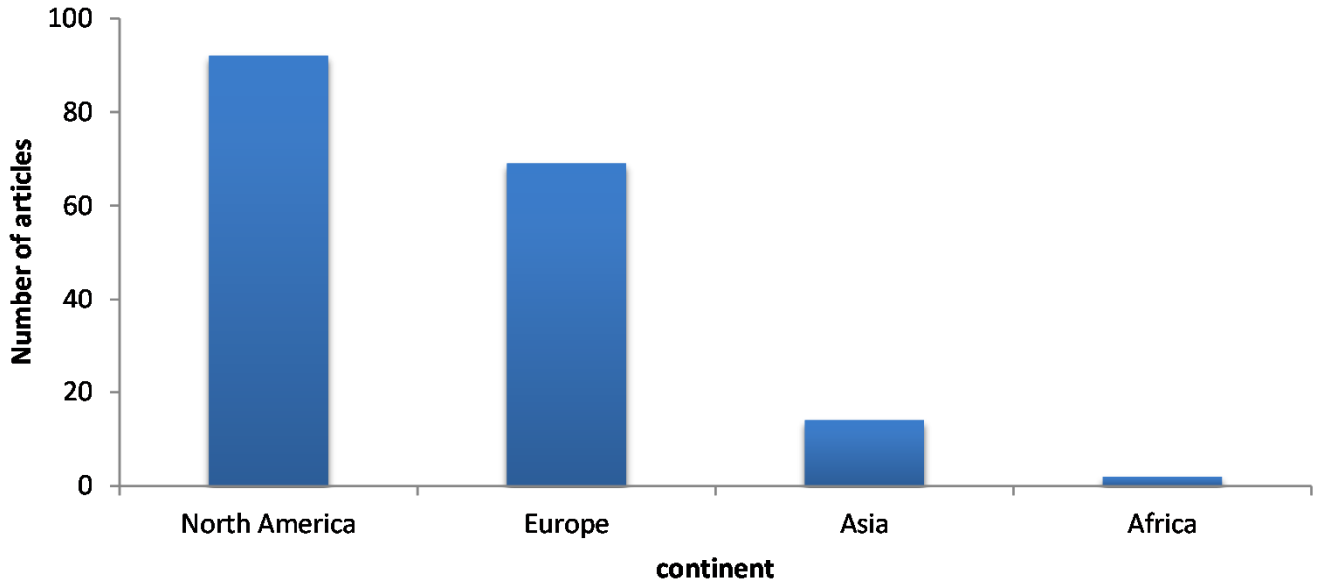


Evolution per research topics

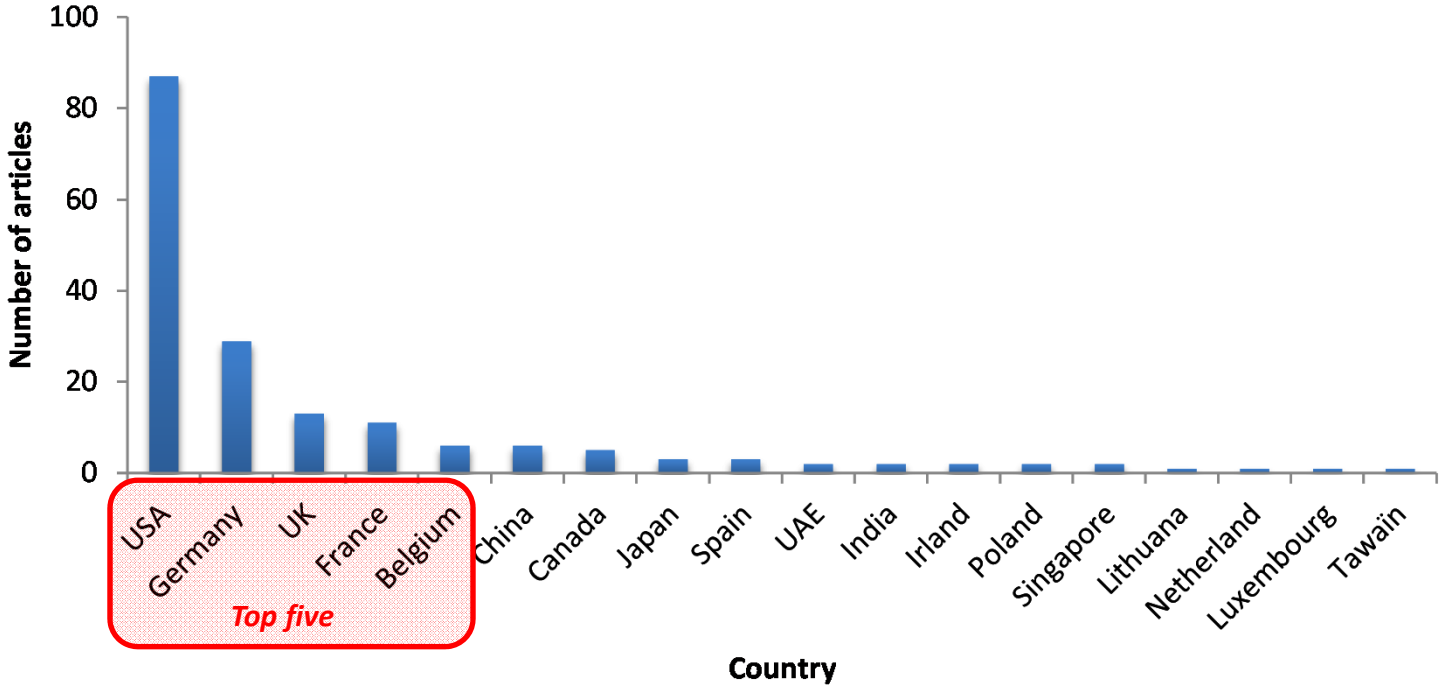
- Cumulative number of publications



Publication addresses (continents)



Publication addresses (countries)



Synthesis and future

- 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 European projects
  - More than only PUF/HT studies
  - Need strong skill in
    - VLSI design / analog design
    - IC manufacturing
    - Hardware security
    - Applied cryptographic (need very-lightweight crypto)

lilian.bossuet@univ-st-etienne.fr