Fighting against theft, cloning and counterfeiting of integrated circuits

Lilian Bossuet
Associate Professor, CNRS Chaire of Hardware Security

Jean Monnet University, Saint-Etienne

Training School on Trustworthy Manufacturing and Utilization of Secure Devices
15th July, 2014, Lisbon, Portugal

Fighting …

why ?

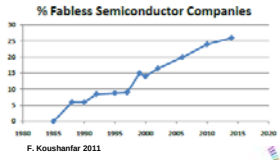
Semiconductor market

- 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.

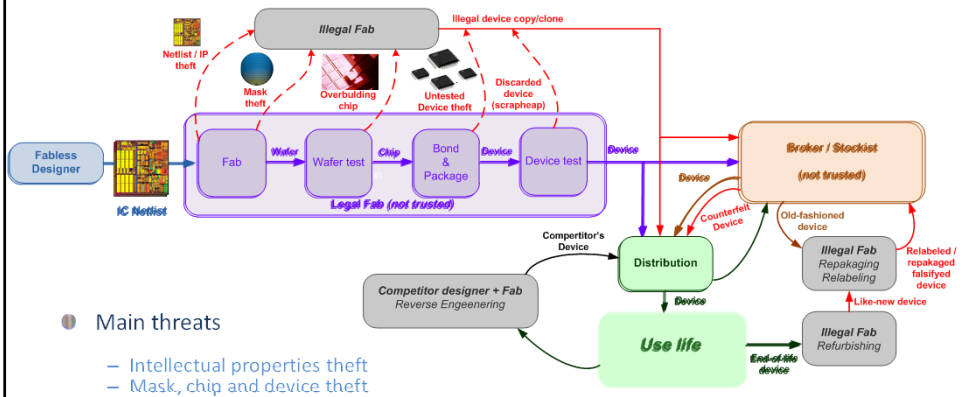
Tech.	Transistors	Manufacturing costs
130 nm	9 millions	9 millions €
90 nm	16 millions	18 millions €
65 nm	30 millions	46 millions €

Rapport Saunier, 2008



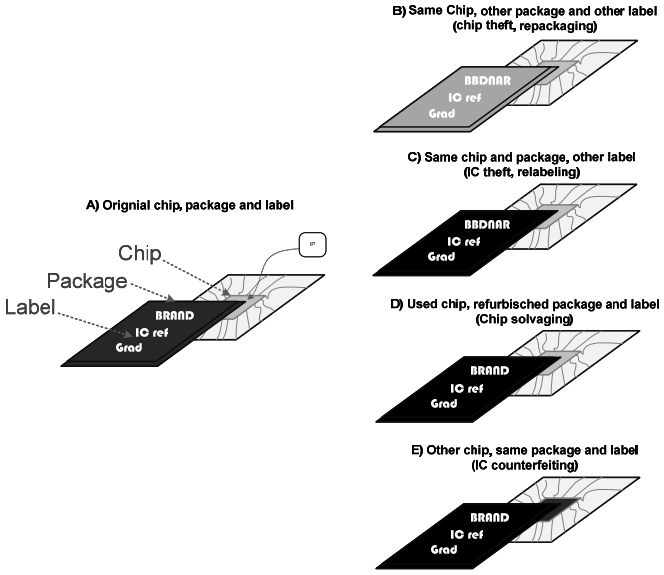
F. Koushanfar 2011

Threat model during manufacturing, supply chain and use life

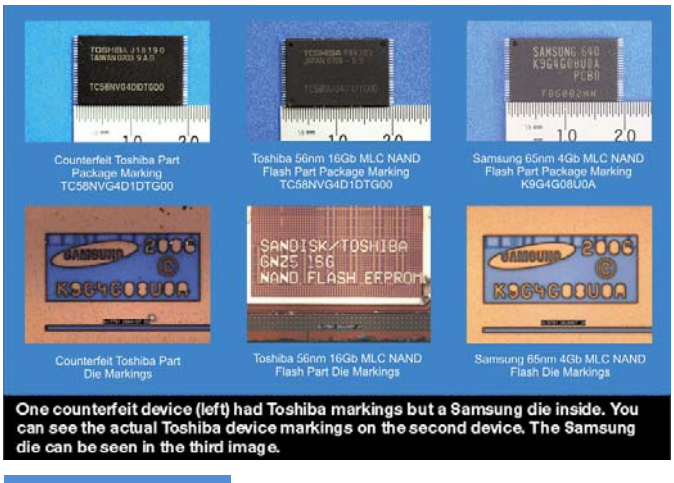


- Main threats
  - Intellectual properties theft
  - Mask, chip and device theft
  - Overbuilding
  - Illegal copy, cloning
  - Counterfeiting
  - Illegal refurbishing, repackaging, relabeling
  - Reverse engineering
  - Functional modifications (DRM violation, unlocking)

Definition



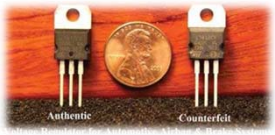
Example of counterfeiting flash memory



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

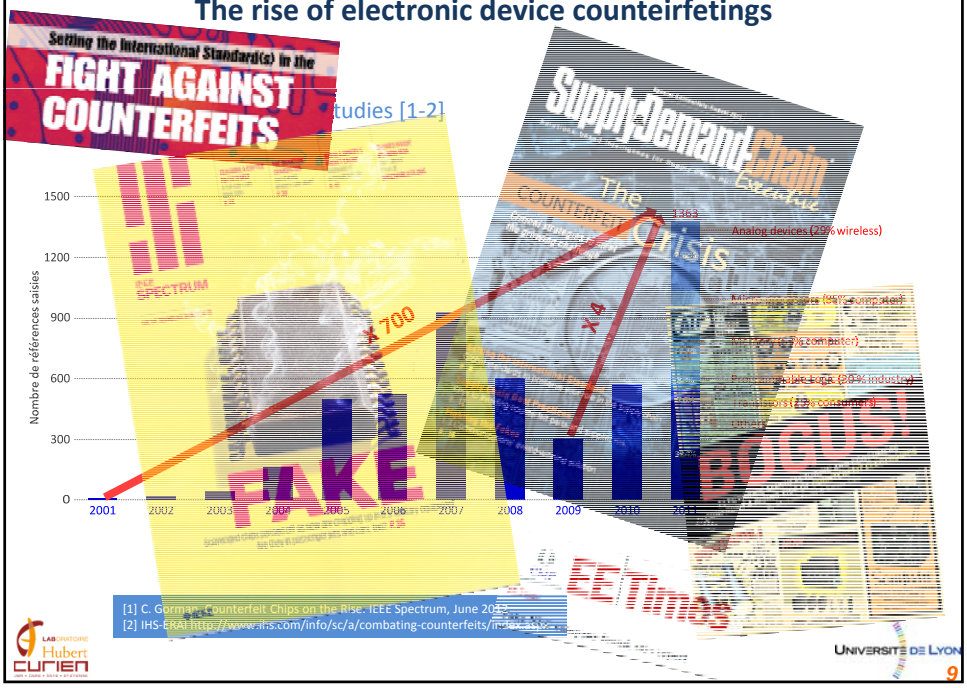
Amazing stories

- 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

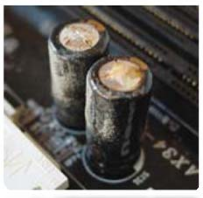
[1] Next Step for Counterfeiters: Faking the Whole Compagny, New York Times, May 2006 http://www.nytimes.com/2006/05/01/technology/01pirate.html?pagewanted=all
[2] Fake NEC compagny, says report, EE Times, April 2006 http://www.eetimes.com/electronics-news/4060352/Fake-NEC-company-found-says-report
[3]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

The rise of electronic device counteirfetings

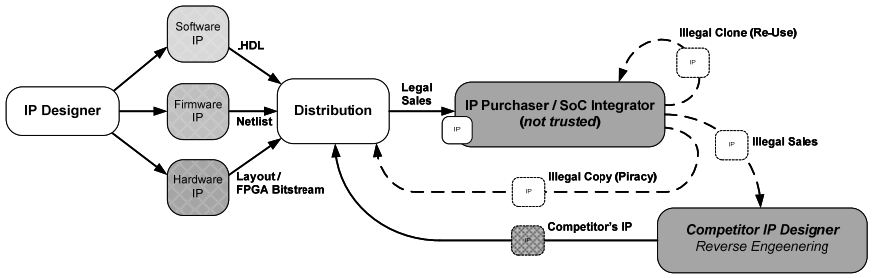


Consequences of electronic products counterfeiting

- 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

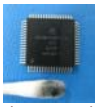
Counterfeiting physical detection

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

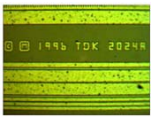

Before


After

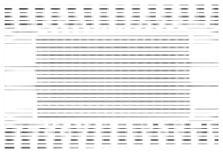

Fake Atmel

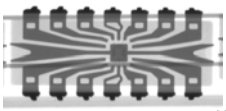

Fake Motorola

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



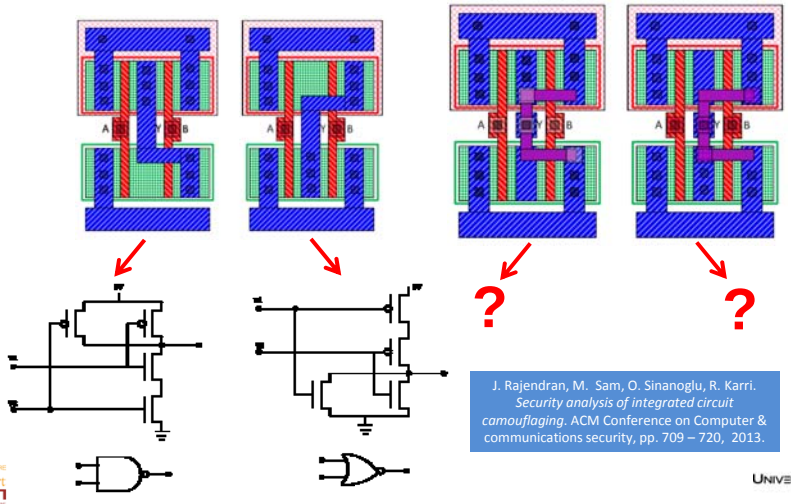
  - X-ray inspection





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 1/2

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

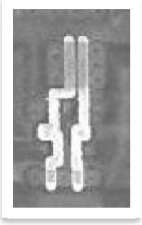


Figure 1: *Conventional 2 input NOR Gate*

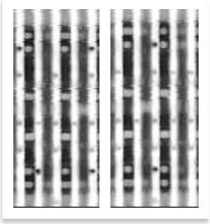


Figure 2: *SML 2-input NAND and NOR Gates*

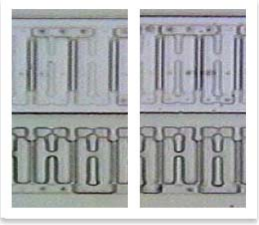


Figure 3: *SML 2-input NAND and NOR Gates without Metal*

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

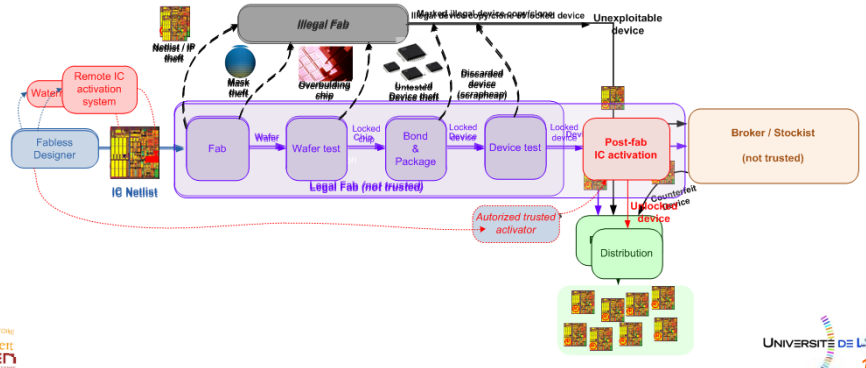
HARDWARE SOLUTION : SALWARE

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.

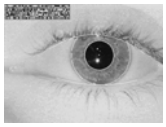


PASSIVE SALWARE

detection

Fingerprint / Watermarking

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



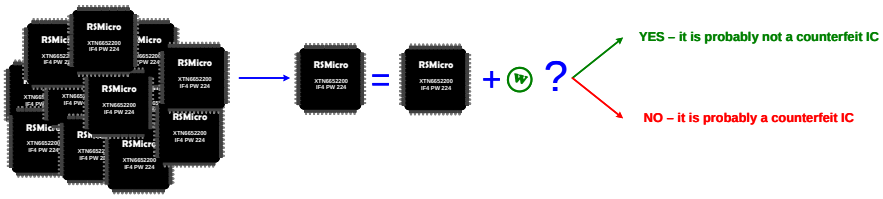
  - Silicon PUF

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

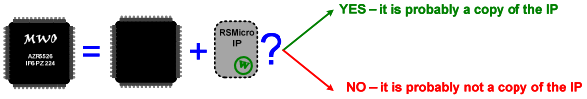
  - Silicon Watermark

Watermarking

- Detection of IC counterfeiting
  - Set of good referenced ICs

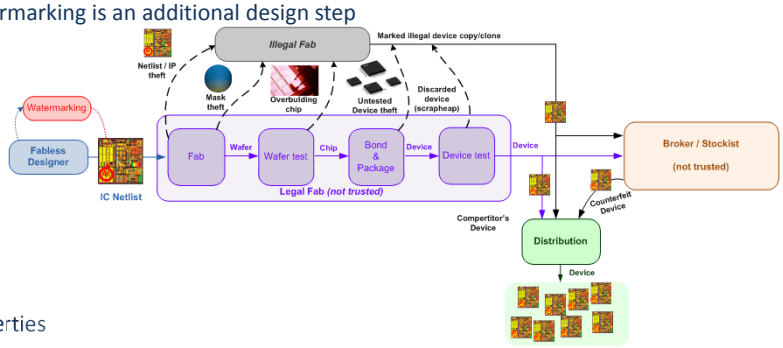


- Detection of IP theft (illegal copy/use)



Watermarking

- Watermarking is an additional design step



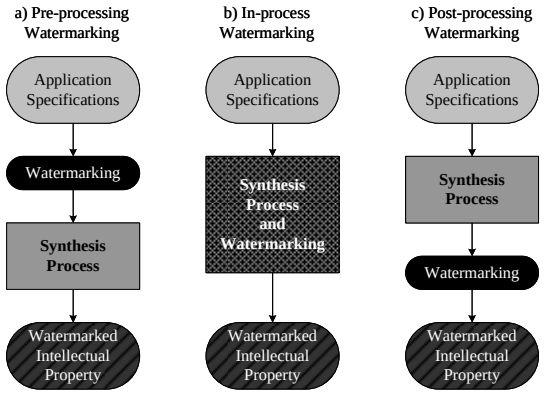
- Properties
  - The watermark does not affect the functionality and performances of the IP
  - The level of trust in the watermark and its detection is high
  - It is not possible to change, mask or remove the watermark
  - The amount of information contained in the watermark is sufficient
  - The cost of the watermark is (very) low
  - Detection of the watermark is easy (for the detection process)
  - Localization of the watermark is hard (for the attacker)

F. Petitcolas. *Watermarking schemes evaluation*. In IEEE Signal Processing Mag., vol. 17, no. 5, pp. 58-64, 2000

UNIVERSITÉ DE LYON 21

Watermarking and digital system design

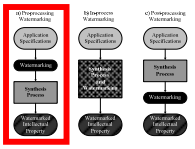
- Three different possible levels



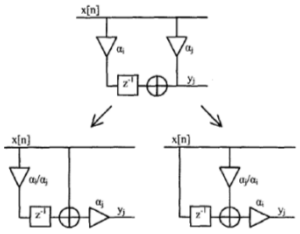
B. Le Gal, L. Bossuet. *Automatic low-cost IP watermarking technique based on output mark insertion*. Design Automation for Embedded System, Springer, 2012

UNIVERSITÉ DE LYON 22

At algorithm level



- The watermark is embedded in the filter coefficients
  - Modification of the magnitude response
  - Easy watermarking
  - Hard to insert a sufficient amount of information
  - IP performance modifications
- FIR filter structure transformation coding



A. Rashid, J. Asher, W.H. Mangione-Smith, M. Potkonjak. *Hierarchical Watermarking for Protection of DSP Filter Cores*. In Proc. IEEE custom Integrated Circuits Conference, 1999

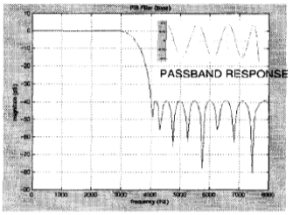


Fig. 4 31-tap non-watermarked filter

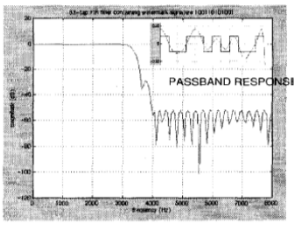
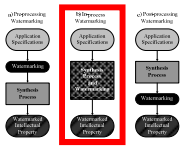
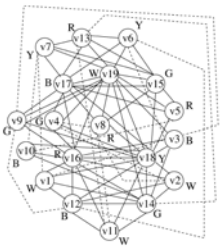


Fig. 5 63-tap watermarked filter

At synthesis level

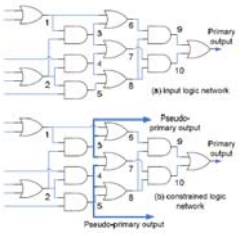


- Data flow graph modification before behavioral synthesis
  - Additional edge to the graph
  - Modification of the register allocation
  - FSM modification
  - Hard to locate
  - Reduction of the synthesis optimizations



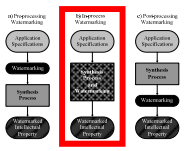
F. Koushanfar, I. Hong,M. Potkonjak, *Behavioral synthesis techniques for intellectual property protection", ACM Transactions on Design Automation of Electronic* Systems 10/3, 2005, 523–545.

- Data path modification after logical synthesis
  - Random selection of logic gate outputs
  - Additional dummy logic
  - Easy watermarking
  - Easy to locate
  - Logical overhead

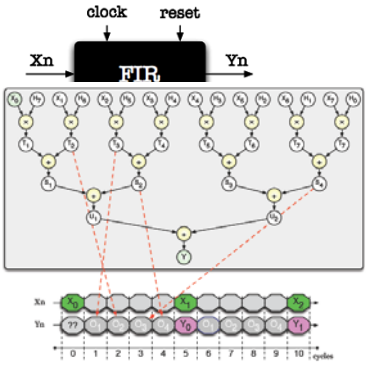


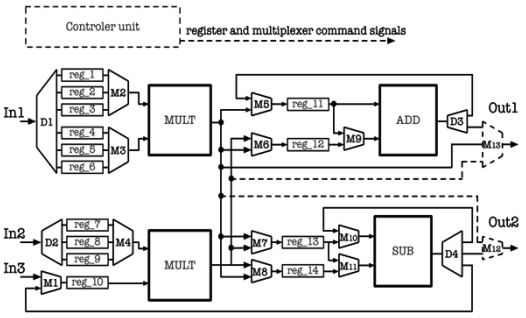
D. Kirovski, Y. Hwang, M. Potkonjak, J. Cong. *Intellectual property protection by watermarking conditional logic synthesis solutions*. In International Conference of Computer Aided Design, 1998,pp. 194-198,

At synthesis level



- Data path and FSM modification during High-Level Synthesis
  - Watermark = mathematical relationship between input and free output slots
  - Dedicated to DSP application
  - Very low cost watermark





B. Le Gal, L. Bossuet. *Automatic low-cost IP watermarking technique based on output mark insertion*. Design Automation for Embedded System, Springer, 2012 http://www.springerlink.com/content/100255/?Content+Status=Accepted

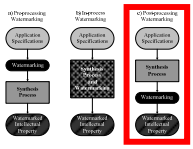
Synthesis level watermarking

- Performances comparison (based on published papers)
  - Application: DCT 2D

Work	System modifications	Watermark length (bits)	Area overhead	Throughput overhead	Watermark space size
1- Foushanfar et al. – 2005	*18 170 new edges on the DFG*	2047	-	-	2^{1E25}
2 - Kirovski et al. – 1998	*273 logical nets + glue*	256	4.40%	-	2^{1E637}
3 - Le Gal, Bossuet – 2012 (*cost-less*)	*Values of the output register of the FSM*	584	0.02%	0.2%	2^{584}
4 - Le Gal, Bossuet – 2012 (*low-cost*)	*Datapath*	584	1.02%	0.75%	$2^{1,5E3}$

- Main results
  - Tradeoff between watermark space size and overhead
  - Security => watermark diffusion (1 & 4)
  - Note : it is not necessary to add crypto-functions

At hardware (layout) level



- Use free LUT/memory block in FPGA
  - Direct storage of the watermark (LUT configuration/memory data)
  - Handmade *place and route* modification
  - Hard watermarking (handmade process)
  - Easy to detect / hard to locate

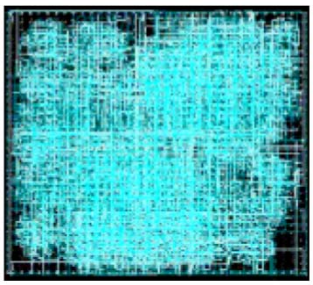


Figure 1. DES original layout

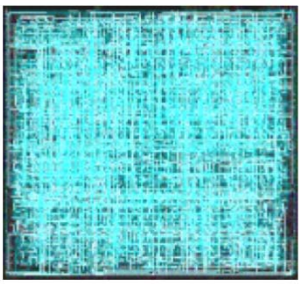


Figure 2. DES with 298 16-bit marks

J. Latch, W. Mangione-Smith, M. Potkonjak. *Robust FPGA intellectual property protection through multiple small watermarks*. In International DAC 1999

Watermarking

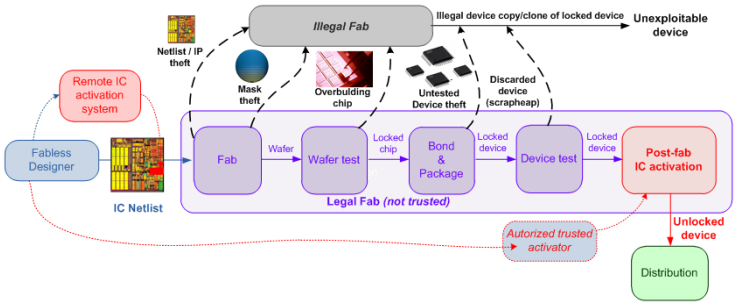
- Level of action ?
  - Pre-synthesis watermarking is too algorithm dependent (suitable only for some DSP applications), hard to use
  - In-synthesis watermarking benefits from automatic tools, with watermark diffusion, without significant overhead (power/area/time)
  - Post-synthesis watermarking uses the designer's knowledge, it is time consuming and design/device dependent
- Watermarking detection
  - Most of the time authors forget this point …
  - Some time it is not possible to perform detection directly
    - Ex: modification of FSM state-registers
  - Confidence level of the metrics used?

ACTIVE SALWARE

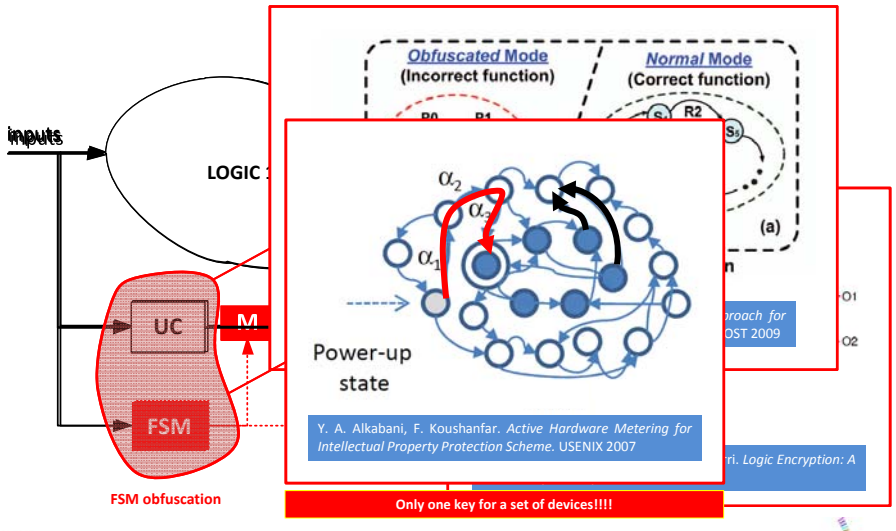
protection

IC Activation (locking/unlocking)

- (remote) activation atfer 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



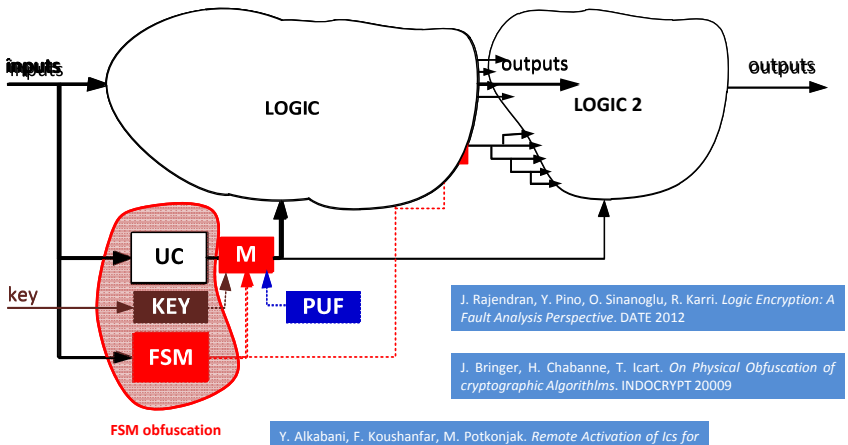
Logic *encryption* / FSM *obfuscation*



Y. A. Alkabani, F. Koushanfar. *Active Hardware Metering for Intellectual Property Protection Scheme.* USENIX 2007

Logic *encryption* / FSM *obfuscation*

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



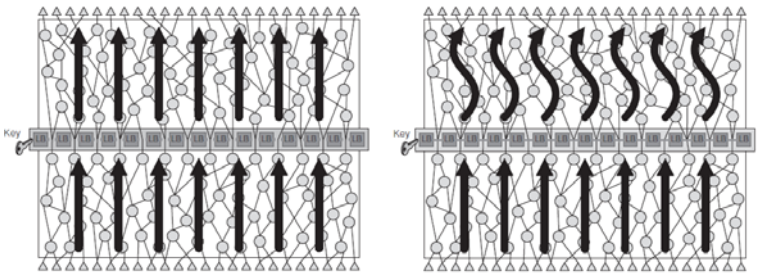
J. Rajendran, Y. Pino, O. Sinanoglu, R. Karri. *Logic Encryption: A Fault Analysis Perspective.* DATE 2012

J. Bringer, H. Chabanne, T. Icart. *On Physical Obfuscation of cryptographic Algorithlms.* INDOCRYPT 20009

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

Data-path *encryption*

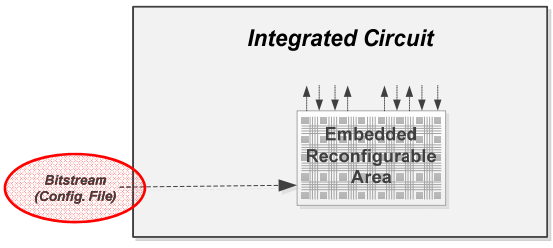
- Reconfigurable logic barriers
  - The barriers are implemented with LUT
  - Reconfigurable « firewall »
  - Need of an heuristic to place the logic barriers
    - Any increase of the critical path



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

Design obfuscation

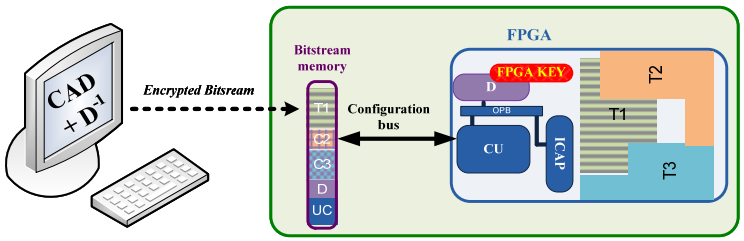
- Obfuscation by using reconfigurable area
  - Countermeasure to reverse-engineering
  - "High-information" parts have to be include in the reconfigurable area
    - Control Unit
    - Processor instruction decoder
  - Need encryption of the bitstream
    - Anti-cloning
    - One bitsream (encrypted)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

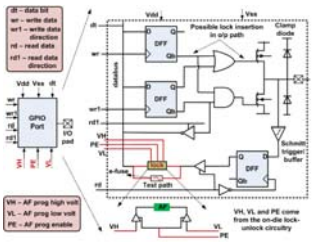
- Encryption of the FPGA bistream
  - Threats: probing /cloning/reverse-engineering/replay /denial
  - Solutions: partial and dynamic reconfiguration [1]-[2], embedded cipher with hash function [3], remote update protection [4], anti-replay [5] …

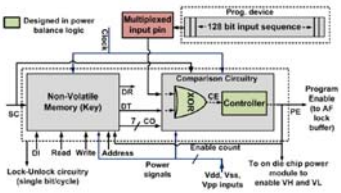


[1] L. Bossuet, G.Gogniat and W. Burleson. *Dynamically Configurable Security for SRAM FPGA Bitstreams.* RAW, IPDPS 2004
[2] A.S. Zeineddini, and K.Gaj. *Secure partial reconfiguration of FPGAs*. FPT 2005.
[3] Y. Hori, A. Satoh, H.Sakane, and K. Toda. *Bitstream encryption and authentication with AES-GCM 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"

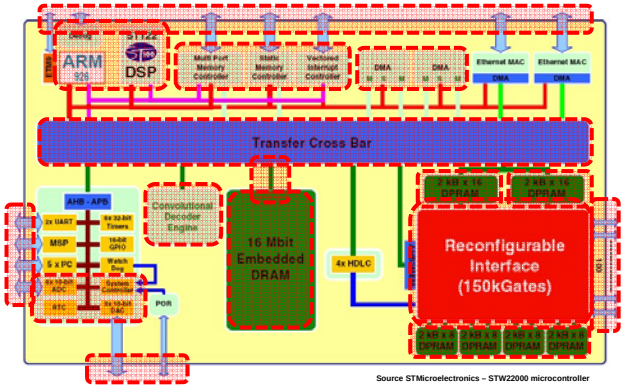




Z. Liu, Y. Li, R. Geiger, and D. Chen. *Active Defense against Counterfeiting Attacks through Robust Aantifuse-based On-Chip-Lock*. VLSI Test Symposium 2014

Locking of a System-on-Chip

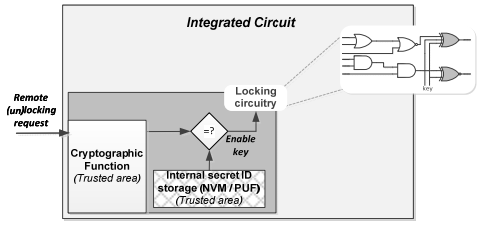
- What it is possible to lock in a SoC?
  - Control unit : FSM obfuscation/ FSM register encryption/ microprocessor obfuscation)
  - Treatment unit: Logic encryption/obfuscation
  - Internal communication: bus encryption / Cross Bar routing obfuscation / NoC locking
  - Memory: DMA and bus encryption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



EFFICIENT SALWARE DESIGN

how ?

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

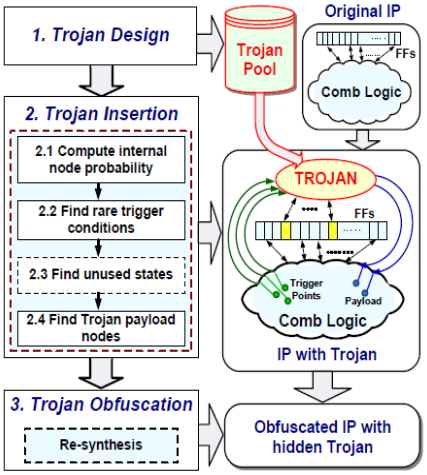
- MALWARE definition

  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

Example

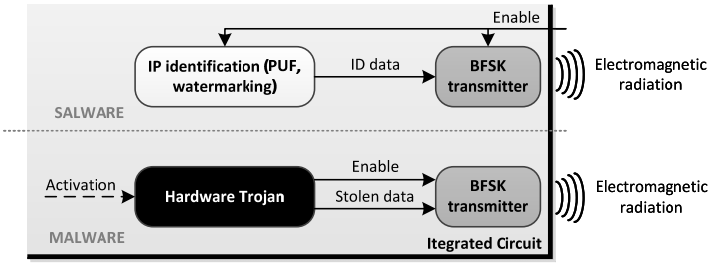
- Trojan insertion for IP protection during evaluation
  - Case Western Reserve University
  - Trojan insertion by IP's FSM modification
  - Re-synthesis of IP with Trojan
  - Time-activated Trojan
  - Trojan signature use as a digital watermarking (in case of illegal IP copy)



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

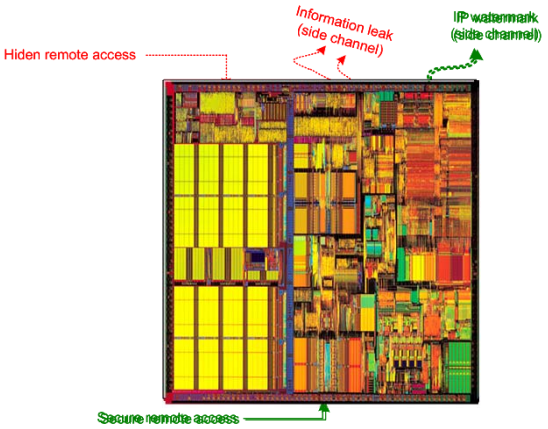
Example

- Side channel used to IP protection
  - IP information transmission
    - ID (from PUF)
    - Watermark
    - Fingerprinting
- Side channel to send IP watermarking
  - EM Channel (contactless, local)
  - BFSK transmitter
    - 200 / 300 Mhz
    - Max 50 Mbps
  - Adapted to FPGA and ASIC implementations
    - 2 LUT4 / 4,67 EG
    - 11µm² @90nm



Salware / Malware

- *Salutary Hardware* vs *Malicious Hardware*



- *Investigating MALWARE design and behavior as a opportunity to improve SALWARE*

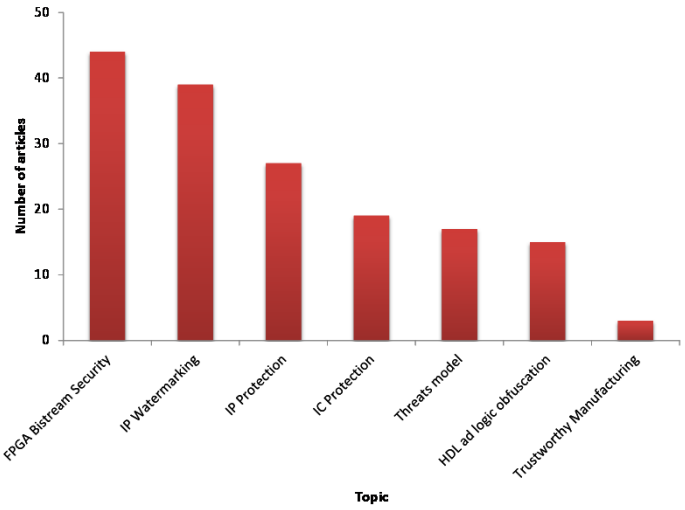
SALWARE
French ANR Project

- 42 month research project
  - Funding: ANR / FRAE

- Bibliography on the project's web site
  - More than 170 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

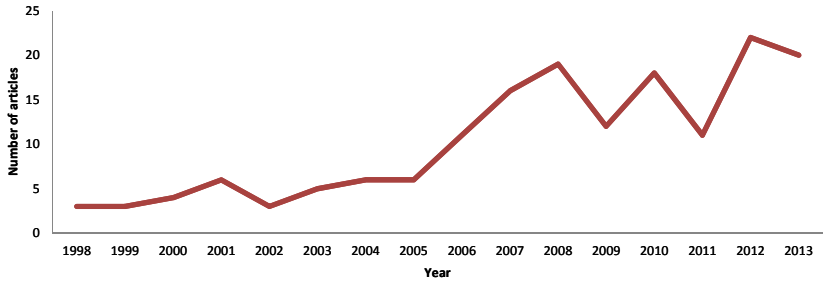
Université de Lyon
45

Publications per topics



Université de Lyon
46

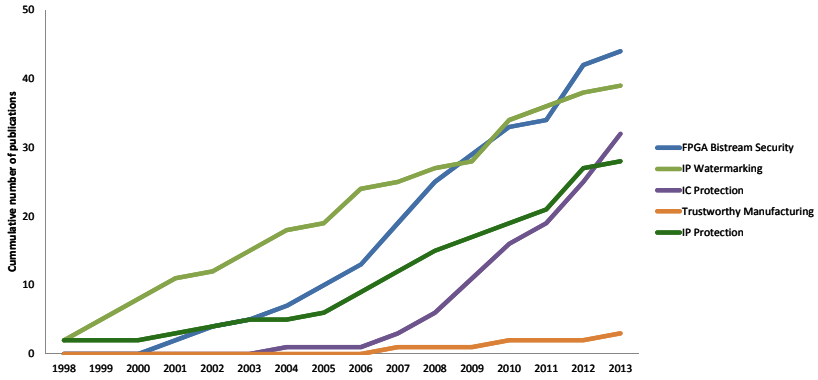
Publications per year



47

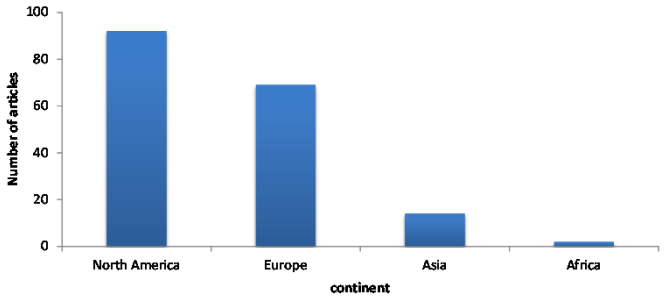
Evolution per research topics

- Cumulative number of publications

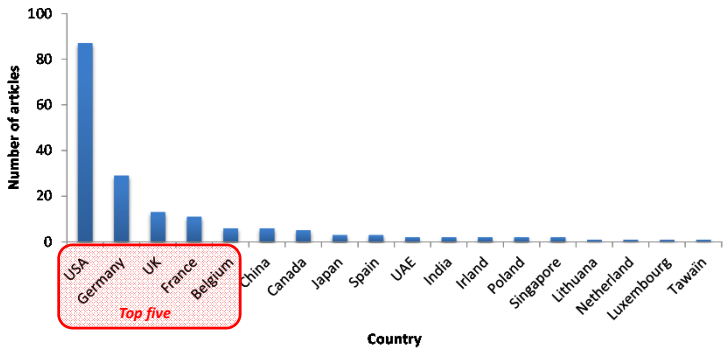


48

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)

51

lilian.bossuet@univ-st-etienne.fr