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
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€) => 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

<table>
<thead>
<tr>
<th>Tech.</th>
<th>Transistors</th>
<th>Manufacturing costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>130 nm</td>
<td>9 millions</td>
<td>9 millions €</td>
</tr>
<tr>
<td>90 nm</td>
<td>16 millions</td>
<td>18 millions €</td>
</tr>
<tr>
<td>65 nm</td>
<td>30 millions</td>
<td>46 millions €</td>
</tr>
</tbody>
</table>

Taiwan Semiconductor Manufacturing Co., Ltd.

Rapport Saunier, 2008

F. Koushanfar 2011
Threat model during manufacturing, supply chain and use life
Threat model during manufacturing, supply chain and use life

[Diagram showing the threat model with various stages including Fab, Wafer test, Bond & Package, Device test, Distribution, and End-of-life. Various threats such as Netlist/IP theft, Mask theft, Overbuilding chip, Untested Device theft, Discarded device (scrapheap), Illegal device copy/clone, and Counterfeit Device are depicted.]

Reverse engineering

Source: http://siliconzoo.org

Chip salvaging / refurbishing
Definition

A) Original 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, refurbished package and label (Chip salvaging)

E) Other chip, same package and label (IC counterfeiting)
Example of counterfeiting flash memory

Counterfeit Toshiba Part
Package Marking
TC58NVG4D1DTG00

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

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

Counterfeit Toshiba Part
Die Markings

Samsung 65nm 4Gb MLC NAND
Flash Part Die Markings

Toshiba 56nm 16Gb MLC NAND
Flash Part Die Markings

Samsung 65nm 4Gb MLC NAND
Flash Die Markings

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

Source: EE Times, August 2007
More examples ....
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, electronics products

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]

www.trustedfoundryprogram.or
Amazing stories

Fake NEC company
- 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 ...


<table>
<thead>
<tr>
<th>Company</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Micro Devices</td>
<td>$34,900.00</td>
</tr>
<tr>
<td>Altera</td>
<td>$7,611.00</td>
</tr>
<tr>
<td>Analog Devices</td>
<td>$75,580.66</td>
</tr>
<tr>
<td>Cypress Semiconductor</td>
<td>$33,446.00</td>
</tr>
<tr>
<td>Freescale</td>
<td>$40,021.00</td>
</tr>
<tr>
<td>Infineon Technologies</td>
<td>$10,036.00</td>
</tr>
<tr>
<td>Intel</td>
<td>$100,889.50</td>
</tr>
<tr>
<td>Intersil</td>
<td>$1,857.30</td>
</tr>
<tr>
<td>Linear Technology</td>
<td>$32,018.75</td>
</tr>
<tr>
<td>Maxim</td>
<td>$1,596.34</td>
</tr>
<tr>
<td>Mitel</td>
<td>$2,645.93</td>
</tr>
<tr>
<td>National Semiconductor</td>
<td>$5,943.80</td>
</tr>
<tr>
<td>NEC</td>
<td>$24,842.07</td>
</tr>
<tr>
<td>Peregrine Semiconductor</td>
<td>$2,640.00</td>
</tr>
<tr>
<td>Philips Electronics</td>
<td>$1,639.50</td>
</tr>
<tr>
<td>Renesas</td>
<td>$2,400.00</td>
</tr>
<tr>
<td>Samsung Electronics America</td>
<td>$77,165.00</td>
</tr>
<tr>
<td>STMicroelectronics</td>
<td>$18,619.21</td>
</tr>
<tr>
<td>Texas Instruments</td>
<td>$92,899.58</td>
</tr>
<tr>
<td>Toshiba</td>
<td>$2,424.00</td>
</tr>
<tr>
<td>Xilinx</td>
<td>$22,235.76</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$591,411.40</strong></td>
</tr>
</tbody>
</table>
The rise of electronic device counterfeiting

Target and evolution

- From US statistical studies [1-2]

The rise of electronic device counterfeiting

- Transistors (25% consumers)
- Programmable Logic (30% industry)
- Memory (53% computer)
- Micro-processors (85% computer)
- Analog devices (29% wireless)

From US statistical studies [1-2]


Fake NEC company found, says report
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
  - X-ray inspection
  - Unpackaging and high resolution optical inspection (reverse-engineering)
More information on counterfeit parts detection [TGF2015]

Springer, 2015 – University of Connecticut, USA
Taxonomy of defects in counterfeit components [TGF2015]
Taxonomy of counterfeit detection methods [TGF2015]
CURRENT INDUSTRIAL SOLUTIONS 2/2

Protection against the reverse engineering
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.*

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

HARDWARE SOLUTION : SALWARE

what ?
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

inputs

LOGIC 1

M1

UC

M2

LOGIC 2

outputs

FSM
Logic encryption

Logic locking

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

Benchmark ISCAS’85
  – 9-bit ALU
  – 2362 nodes
  – 178 inputs
  – 123 outputs
Comparison with logic “encryption”

**Area overhead** \(\approx 3\%\)
- 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

---


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

FSM obfuscation

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

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

FSM obfuscation

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


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 bitstream (encrypted) by device (one secret key by device)

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] ...

---

IOB locking

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

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 ...
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
- M. Potkonjak, UCLA

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

IC identification / authentication
Fingerprint / Watermark

Fingerprint
- Measurement of a physical (or behavioral) characteristics

Watermark
- Additional (hidden) information (steganography)

Silicon PUF (Physical Unclonable Function)

Silicon Watermark
Identification of IC

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

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

<table>
<thead>
<tr>
<th>PUF</th>
<th>ID</th>
<th>IC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AF30</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>37B1</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>8992</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>FE72</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>E90B</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>5129</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>8C9D</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
<tr>
<td></td>
<td>253A</td>
<td>RSMicro XTN6652200 IF4 PW 224</td>
</tr>
</tbody>
</table>
Fingerprint of IC – Silicon PUF

Unpredictable
High steadiness

Entropy extraction

Response
10100111
Challenge
01101010011011
Fingerprint of IC – Silicon PUF

IC_A
Response A
101001011
Unique
Challenge
01101010011011
IC_B
Response B
01100010
Unique
IC_C
Response C
110011101
Unique
CMOS process variations

Example

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

---


---


---

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/](http://www.hector-project.eu/)
Detection of IC counterfeiting
– Set of good referenced ICs

Detection of IP theft (illegal copy/use)

YES – it is probably not a counterfeit IC
NO – it is probably a counterfeit IC

YES – it is probably a copy of the IP
NO – it is probably not a copy of the IP
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
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)

![Graphs showing oscillation frequencies $f_0$ and $f_1$ vs. $N$.](image)
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

<table>
<thead>
<tr>
<th>Ref</th>
<th>YoP</th>
<th>SC</th>
<th>Hardware resources</th>
<th>Bite rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>[5]</td>
<td>2008</td>
<td>$TH$</td>
<td>255 Spartan-3 Slices</td>
<td>7.10^{-3} bps</td>
</tr>
<tr>
<td>[9]</td>
<td>2009</td>
<td>$PC$</td>
<td>8 parallel Dff or 16 bit circular shift register</td>
<td>485 bps</td>
</tr>
<tr>
<td>[10]</td>
<td>2013</td>
<td>$PC$</td>
<td>16-bit circular shift register per bit</td>
<td>976 bps</td>
</tr>
<tr>
<td>Our work</td>
<td>2015</td>
<td>$EM$</td>
<td>1 configurable RO</td>
<td>1 Mbps</td>
</tr>
</tbody>
</table>

Our work is 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)
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/
lilian.bossuet@univ-st-etienne.fr
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