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 US $

- **SoC manufacturing cost rise**
  - SoC complexity increase (add value increase)
  - +40% from 32nm (92 M€) => to 28nm (130 M€)
  - Reduction => 30% with 450nm 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

<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>

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**

A) Original chip, package and label

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

C) Same chip and package, other label (chip theft, relabelling)

D) Used chip, refurbished package and label (chip sourcings)

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

---

**Example of counterfeiting flash memory**

[Images of counterfeit and original flash memory devices]

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]


Amazing stories

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

- Visiotech (USA)
  - From 2006 to 2010, VisioTech sell more than 60 000 counterfeit integrated circuits [3]
  - Visiotech customers: US Navy, Raytheon

Advanced Micro Devices $24,900.00
Altera $7,611.00
Analog Devices $76,580.66
Cypress Semiconductor $25,446.00
Freescale $40,621.00
Infineon Technologies $100,636.00
Intel $100,885.50
Intersil $1,857.30
Linear Technology $32,618.75
Mitsubishi $1,596.34
Nvidia $3,645.93
National Semiconductor $8,543.80
Nec $2,184.07
Pentium Santa Barbara $2,640.00
Philips Electronics $1,639.50
Freescale $2,400.00
Samsung Electronics America $77,905.00
STMicroelectronics $18,619.91
Texas Instruments $92,899.58
Toshiba $2,424.00
Nokia $22,335.76
Total $99,313.80


©Lilian Bossuet 2014
The rise of electronic device counterfeiting

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
  - 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

---

Circuit Camouflaging 1/2

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

Figure 1: Conventional 2 input NOR Gate
Figure 2: SMIC 2-input NANO and NOR Gates
Figure 3: SMIC 2-input NANO and NOR Gates without Metal


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

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

- Silicon PUF
- Silicon Watermark

Watermarking

- **Detection of IC counterfeiting**
  - Set of good referenced ICs

- **Detection of IP theft (illegal copy/use)**

©Lilian Bossuet 2014
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)

Watermarking and digital system design

Three different possible levels

a) Pre-processing Watermarking
b) In-process Watermarking
c) Post-processing Watermarking

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

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

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

Synthesis level watermarking

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

<table>
<thead>
<tr>
<th>Work</th>
<th>System modifications</th>
<th>Watermark length (bits)</th>
<th>Area overhead</th>
<th>Throughput overhead</th>
<th>Watermark space size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Foushanfar et al. – 2005</td>
<td>18 170 new edges on the DFG</td>
<td>2047</td>
<td>-</td>
<td>-</td>
<td>(2^{2015})</td>
</tr>
<tr>
<td>2 - Kirovski et al. – 1998</td>
<td>273 logical nets + glue</td>
<td>256</td>
<td>4.40%</td>
<td>-</td>
<td>(2^{2187})</td>
</tr>
<tr>
<td>3 - Le Gal, Bossuet – 2012 (cost-less)</td>
<td>Values of the output register of the FSM</td>
<td>584</td>
<td>0.02%</td>
<td>0.2%</td>
<td>(2^{291})</td>
</tr>
<tr>
<td>4 - Le Gal, Bossuet – 2012 (low-cost)</td>
<td>Datapath</td>
<td>584</td>
<td>1.02%</td>
<td>0.75%</td>
<td>(2^{1305})</td>
</tr>
</tbody>
</table>

- 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

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 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

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


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

Security of FPGA bitstream (SRAM and FLASH)

- Encryption of the FPGA bitstream
  - 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] ...


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 Antifuse-based On-Chip Lock. VLSI Test Symposium 2014
Locking of a System-on-Chip

- What is it 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 ..

Active Salware Design

- Strong security
  - Use cryptographic functions to obtain the usual crypto services
    * Confidentiality, 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.
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)

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
  - Adaptable 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
42 month research project
– Funding: ANR / FRAE

Bibliography on the project’s web site
– More than 170 references (1999-2014)
  • Threats model
  • IC protection
  • IP protection
  • IP watermarking
  • FPGA bitstream security
  • HDL and logic obfuscation
  • Trustworthy manufacturing

Publications per topics

[Bar chart showing the number of publications per topic]

©Lilian Bossuet 2014
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