Hardware Counterfeiting

Paolo PRINETTO
Director
CINI Cybersecurity
National Laboratory

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

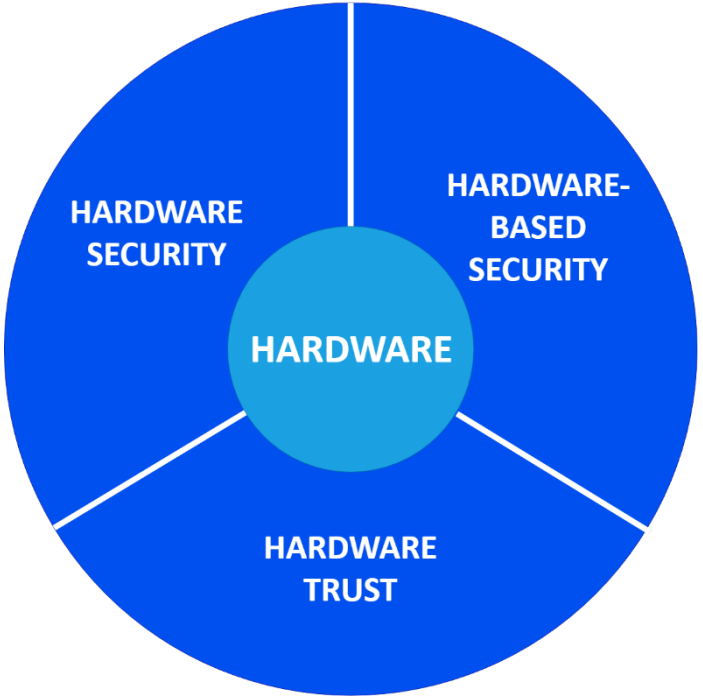
Acknowledgments

- The presentation includes material from
  - Giorgio DI NATALE
  - Nicolò MAUNERO
  - Gianluca ROASCIO

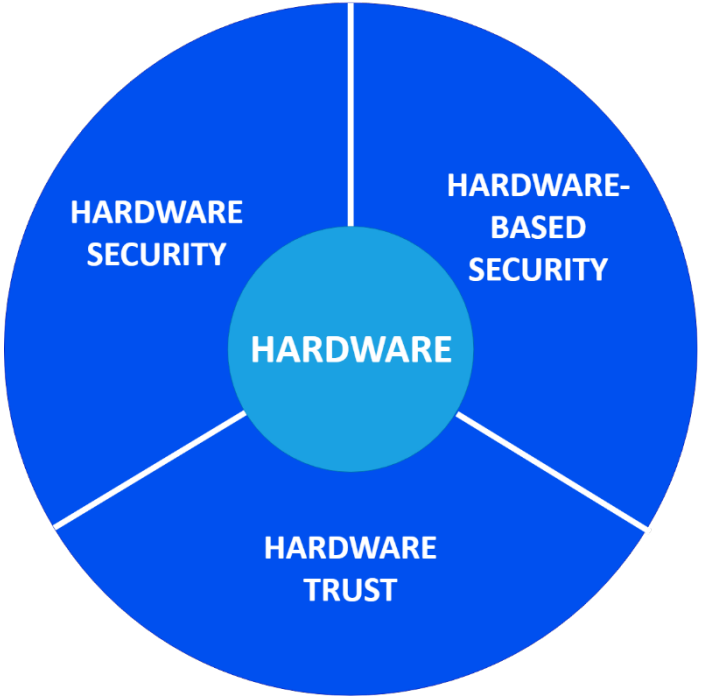
  whose valuable contribution is here acknowledged and highly appreciated

Goal

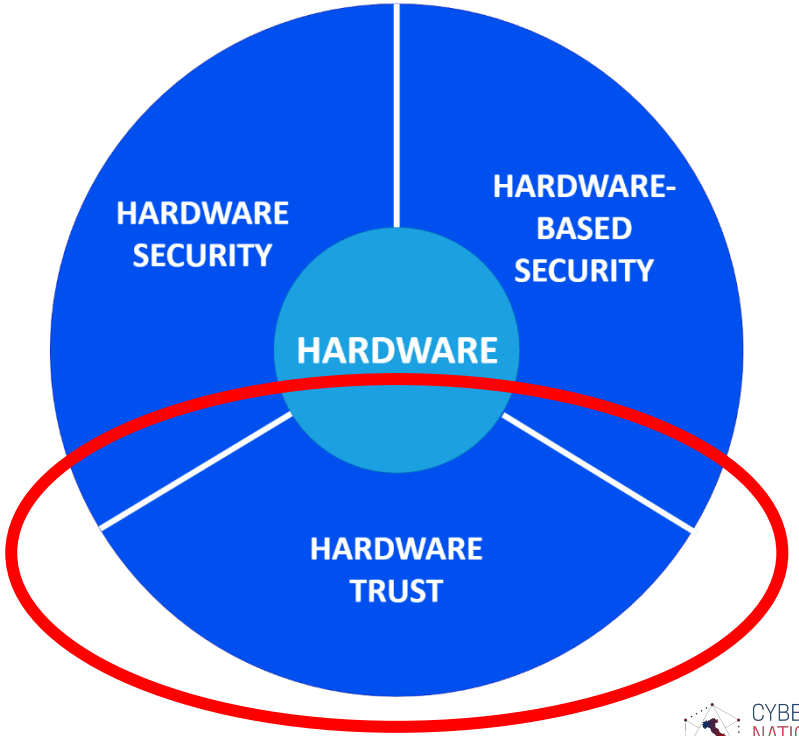
- Presenting the main issues related with *Hardware Trust*



The role of Hardware in Cybersecurity

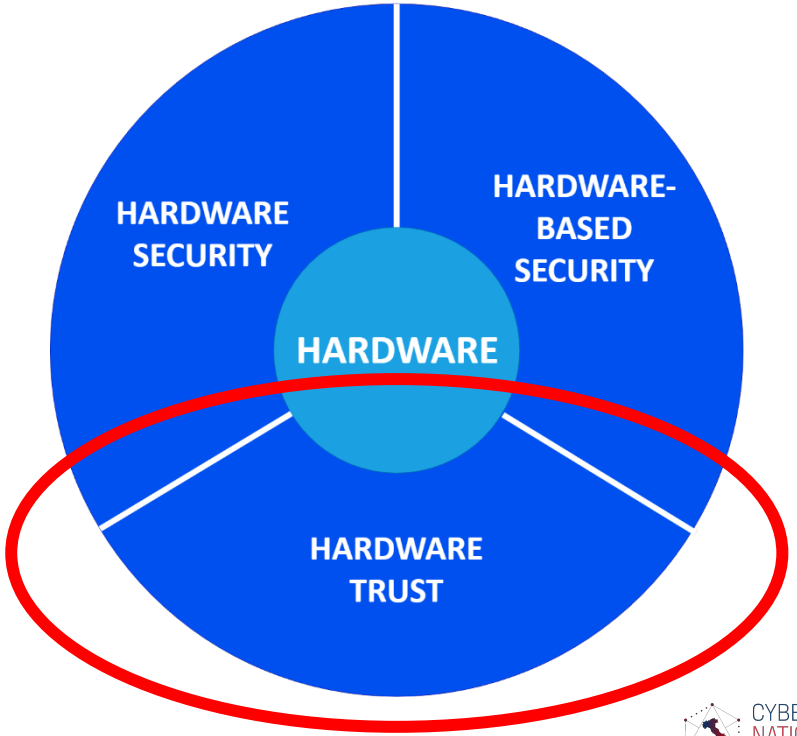


The role of Hardware in Cybersecurity

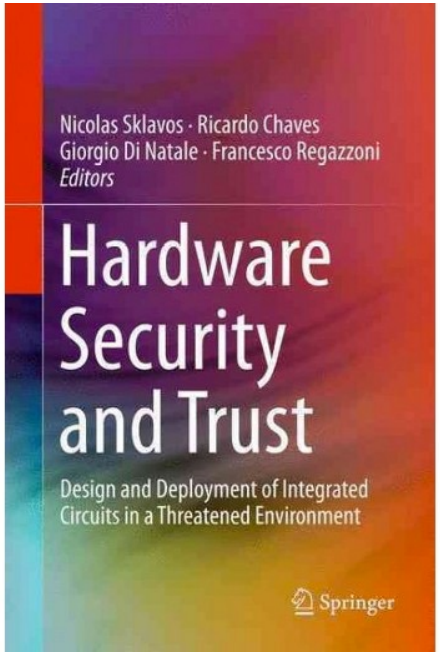


The role of Hardware in Cybersecurity

- Deals with the risks introduced by hardware counterfeiting
- Aims at guaranteeing the authenticity of the used hardware devices



Suggested references



- http://www.counterfeit-ic.org

Outline

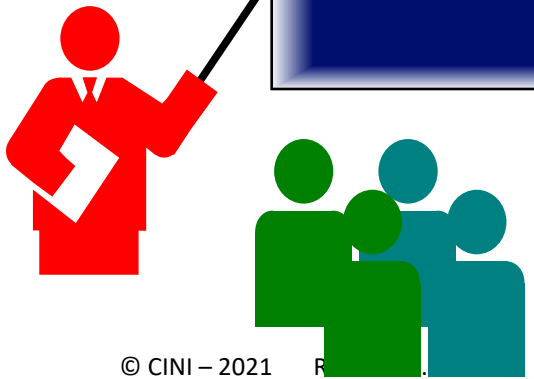
- Introduction
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Outline

- Introduction
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Alarm

Counterfeiting of integrated circuits has become a major challenge in almost ALL industrial sectors !!



Counterfeiting

Causes

- Complexity of the electronic systems significantly increased over the past few decades
- To reduce production cost, they are mostly fabricated and assembled globally

Counterfeiting

Causes

- Complexity of the electronic systems significantly increased over the past few decades
- To reduce production cost, they are mostly fabricated and assembled globally

Consequences

- This globalization has led to an illicit market willing to undercut the competition with counterfeit and fake parts

Counterfeiting

Today Lacks

- Deficiencies in the existing test solutions
- Lack of low-cost and effective avoidance mechanisms in place

Stories

- November 8, 2011, the US Committee on Armed Services held a hearing on an investigation of counterfeit electronic parts in the defense supply chain
- The investigation had revealed alarming facts: materials used to make counterfeit electronic (a.k.a. e-waste) parts are shipped from the US and other countries

http://www.industryweek.com/procurement/ticking-time-bomb-counterfeit-electronic-parts

Stories (cont'd)

- The e-waste is sent to cities like Shantou, China, where:
  - It is disassembled by hand, washed in dirty river water, and dried on the city sidewalk
  - It is sanded down to remove the existing part number or other markings that indicate its quality or performance
  - False markings are placed on the parts that lead the average person to believe they are new or high-quality parts

Stories (cont'd)

- In November 2011, Semiconductor Industry Association (SIA) President Brian Toohey said:

  …as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit

  …overall, we estimate that counterfeiting costs US companies more than $7.5 billion per year, which translates into nearly 11,000 lost American jobs

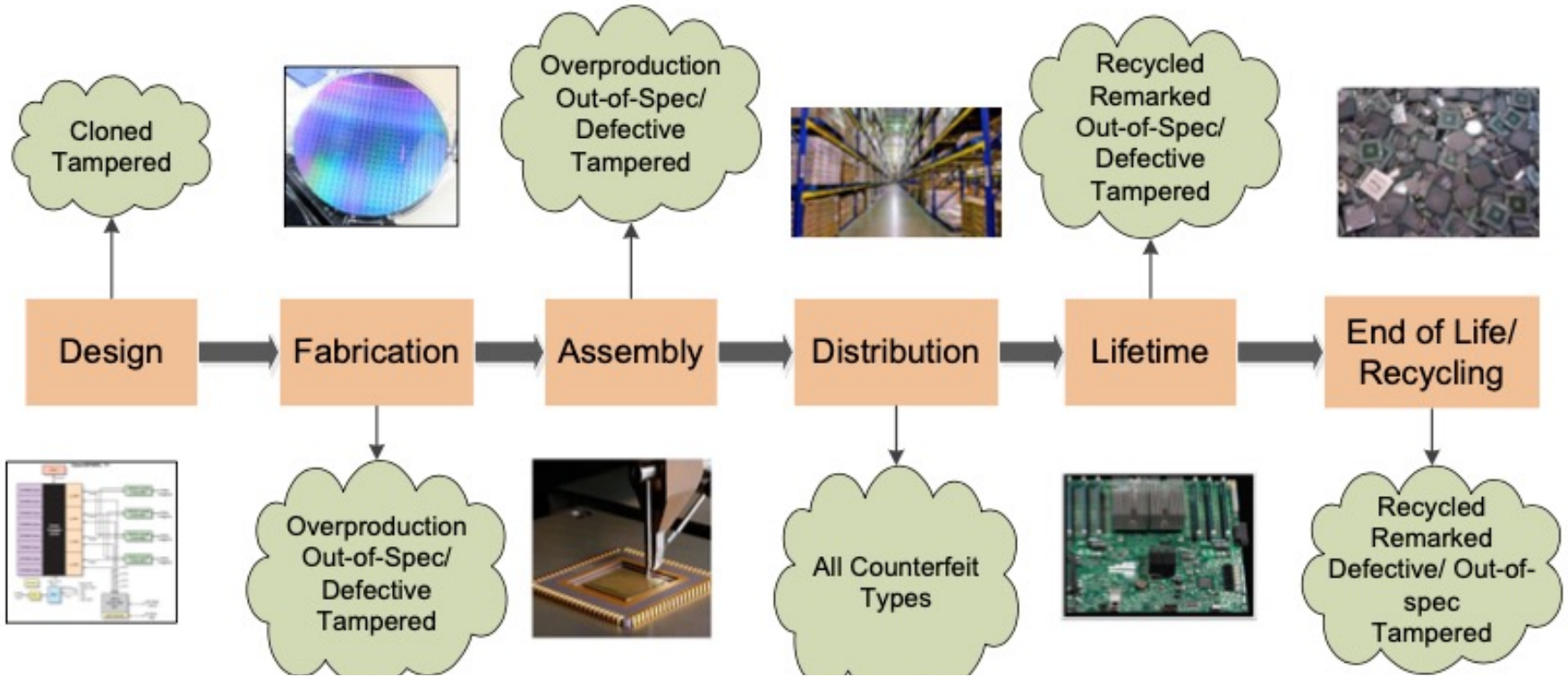
http://www.semiconductors.org/news/2011/11/08/news_2011/sia_president_testifies_at_senate_armed_services_committee_on_dangers_of_counterfeit_chips/

Stories (cont'd)

- Some Data:
  - $75 billion lost in 2013 (in semiconductors)
  - 186 million of fake mobile phones in 2013

http://www.havocscope.com/tag/counterfeit-electronics/

Electronic components supply chain vulnerabilities

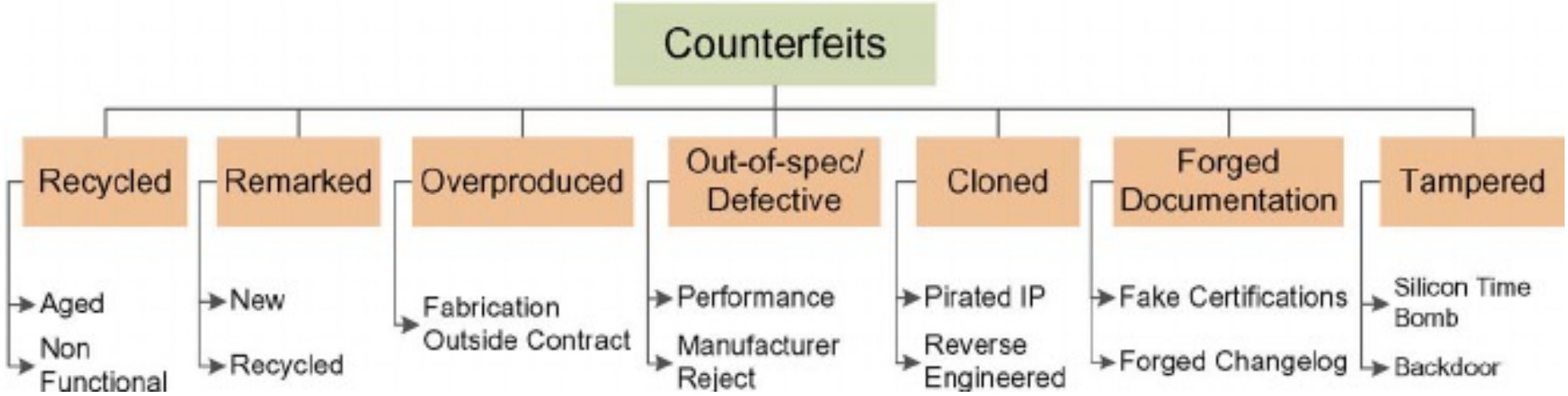


[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Outline

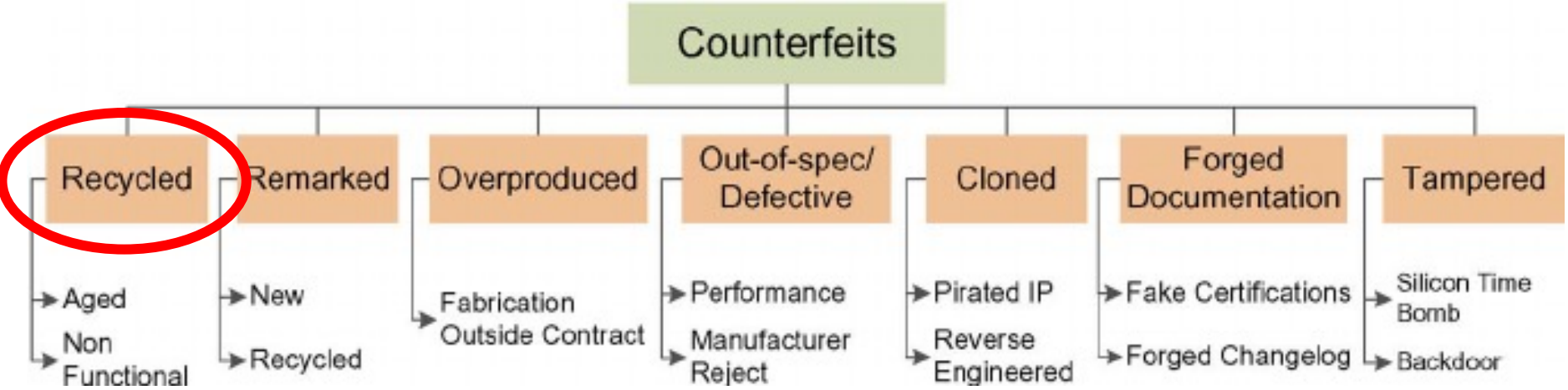
- Introduction
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Counterfeiting types



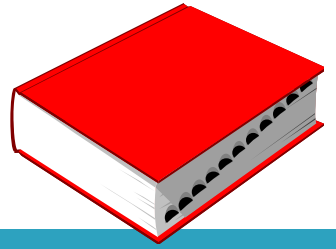
[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Counterfeiting types



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Recycled components



- Used ICs provided by untrustworthy suppliers, which are “recycled” from used or defective circuit boards

Recycled components

What

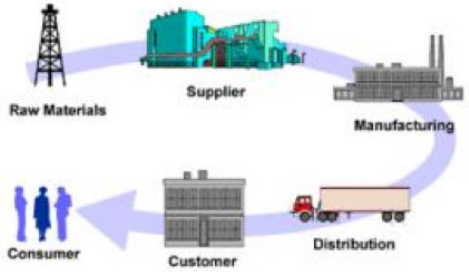
- Electronic component that is recovered from a system and then modified to be misrepresented as a new component

Most common forms of counterfeiting

Used or defective circuit boards

Malicious supplier

Recycled IC

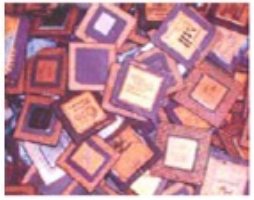


Electronic supply chain

Danger !!!

Millions of Scrap Boards

Component Removal



Sorted by size, similarity and lead count

Re-processed

Good vs. Bad

Clean facilities

Packaging

Testing

Marking

Good vs. Bad

Clean facilities

Packaging

Testing

Marking

De-soldering

De-packaging

Re-marking

Problems of Recycled ICs

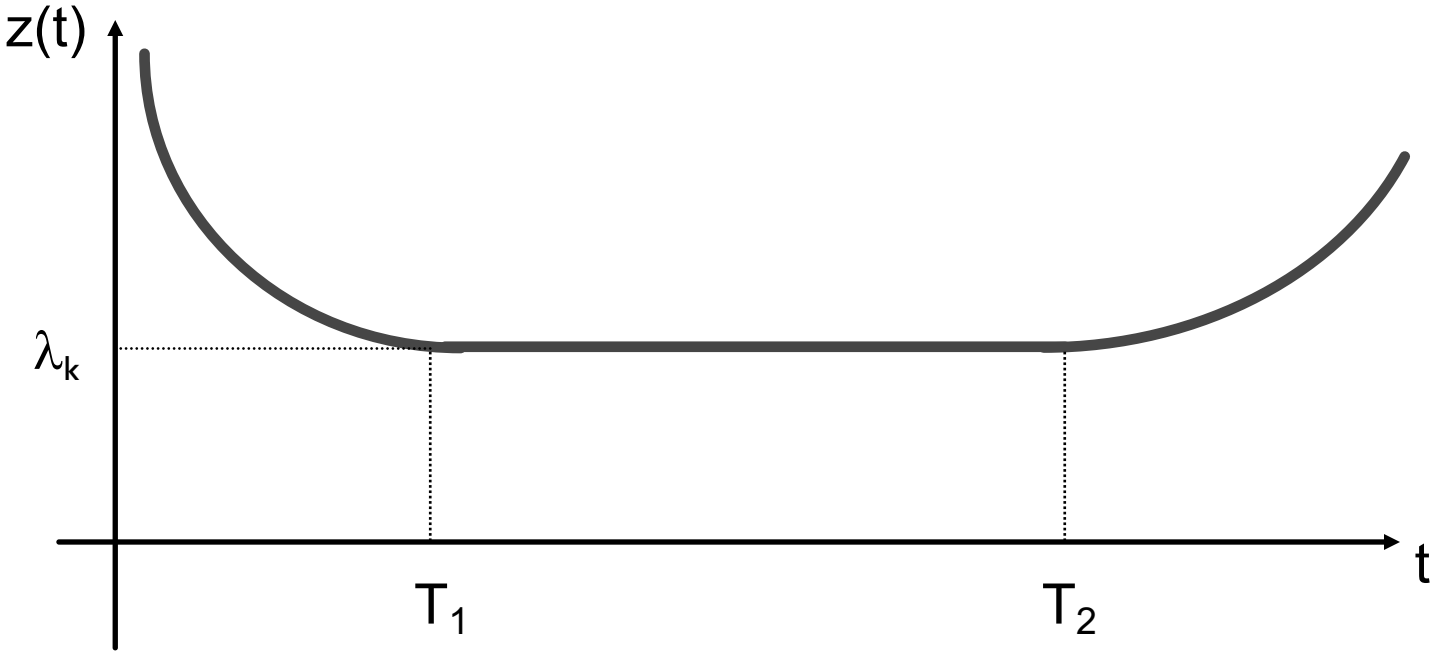
- Financial damage
- Safety
- Security

Problems of Recycled ICs

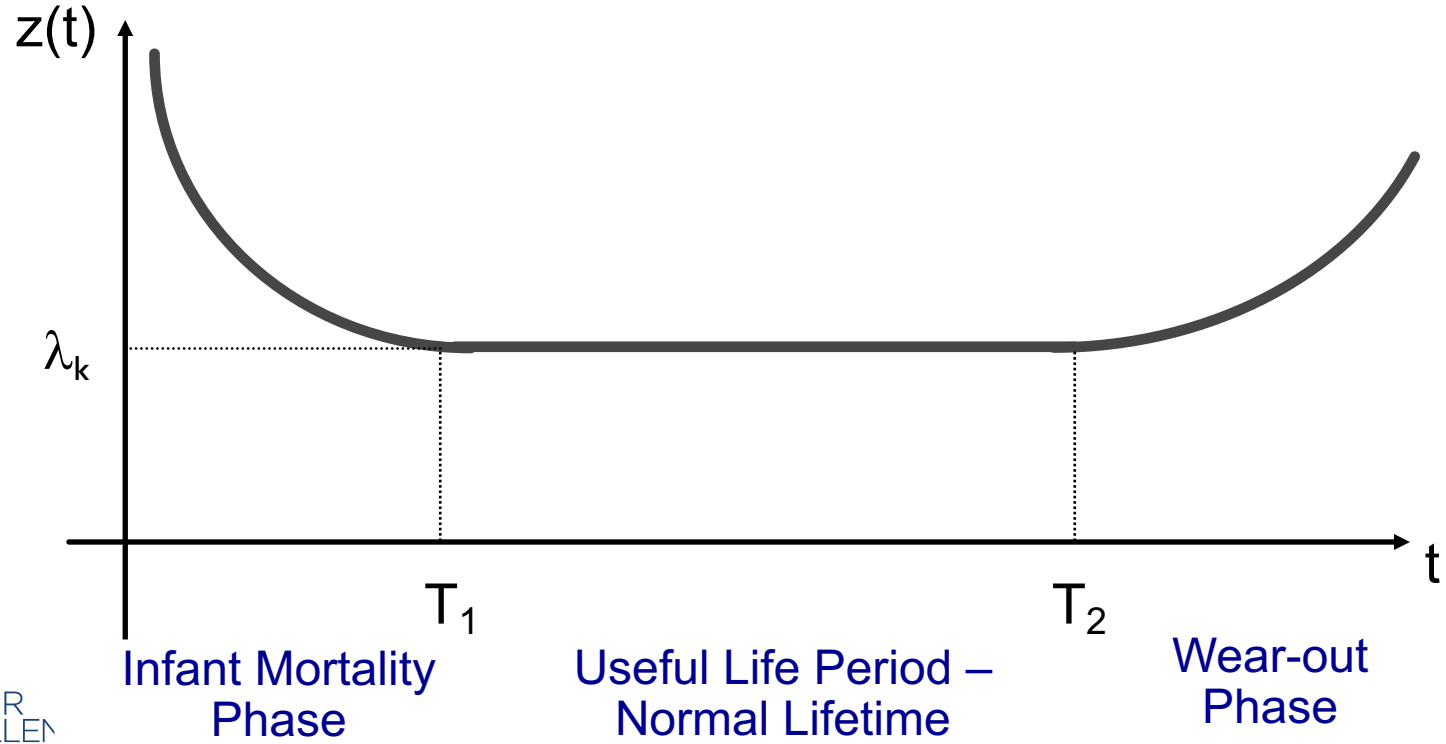
Safety

- Aging Phenomena (shorter lifetime)

Failure Rate Function
(Bathtub curve relationship)



Failure Rate Function
(Bathtub curve relationship)



Problems of Recycled ICs

Safety

- Aging Phenomena (shorter lifetime)
- Potential damage, due to the reclaiming process (removal under very high temperature, aggressive physical removal from boards, washing, sanding, repackaging, etc.)
- Lower performances

Problems of Recycled ICs

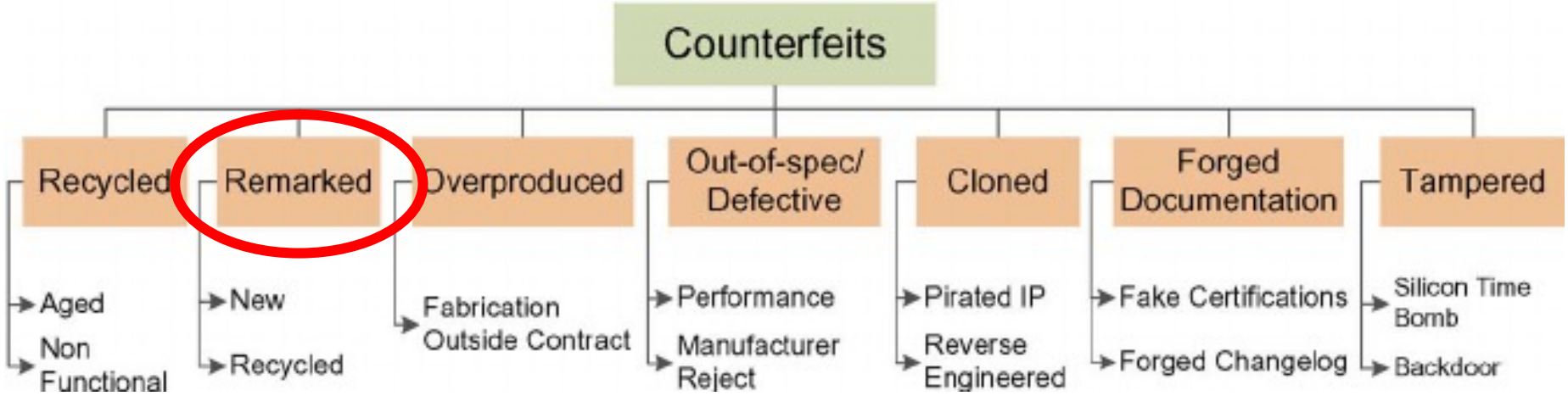
Safety

- Aging Phenomena (shorter lifetime)
- Potential damage, due to the reclaiming process (removal under very high temperature, aggressive physical removal from boards, washing, sanding, repackaging, etc.)
- Lower performances

Security

- Unpatched vulnerabilities

Counterfeiting types



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

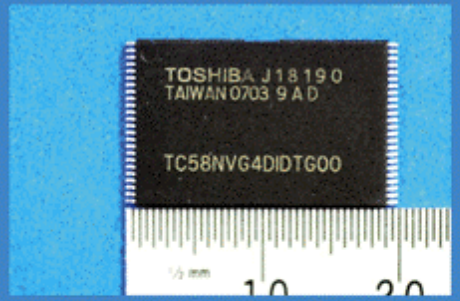
Remarked components

What

- Chemically or physically removing the original marking

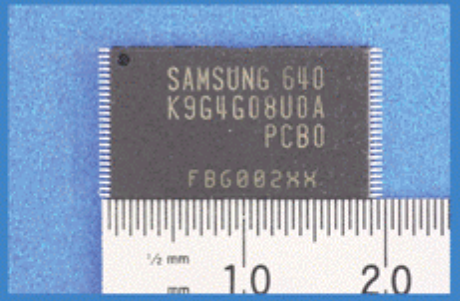
Goal

- Drive up a component's price on the open market
- Make a dissimilar lot fraudulently appear homogeneous

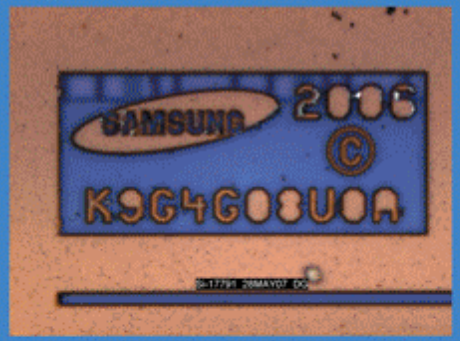


Counterfeit Toshiba Part Package Marking TC58NVG4D1DTG00

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

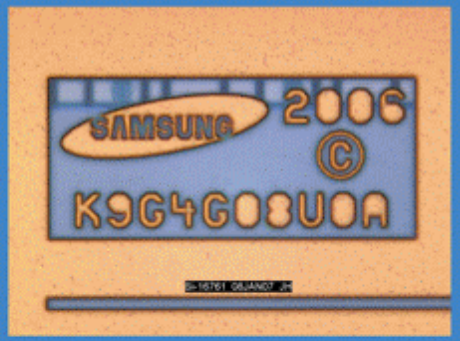


Samsung 65nm 4Gb MLC NAND Flash Part Package Marking K9G4G08U0A



Counterfeit Toshiba Part Die Markings

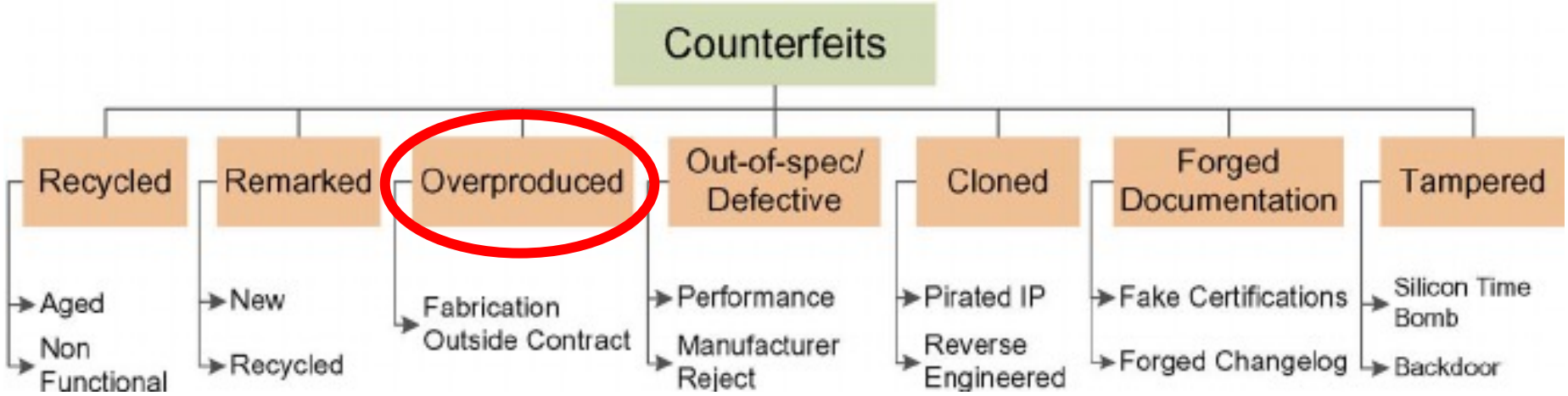
Toshiba 56nm 16Gb MLC NAND Flash Part Die Markings



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.

Counterfeiting types



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Overproduced components

What

- Overproduction occurs when foundries sell components outside of contract with the design houseparts

Overproduced components

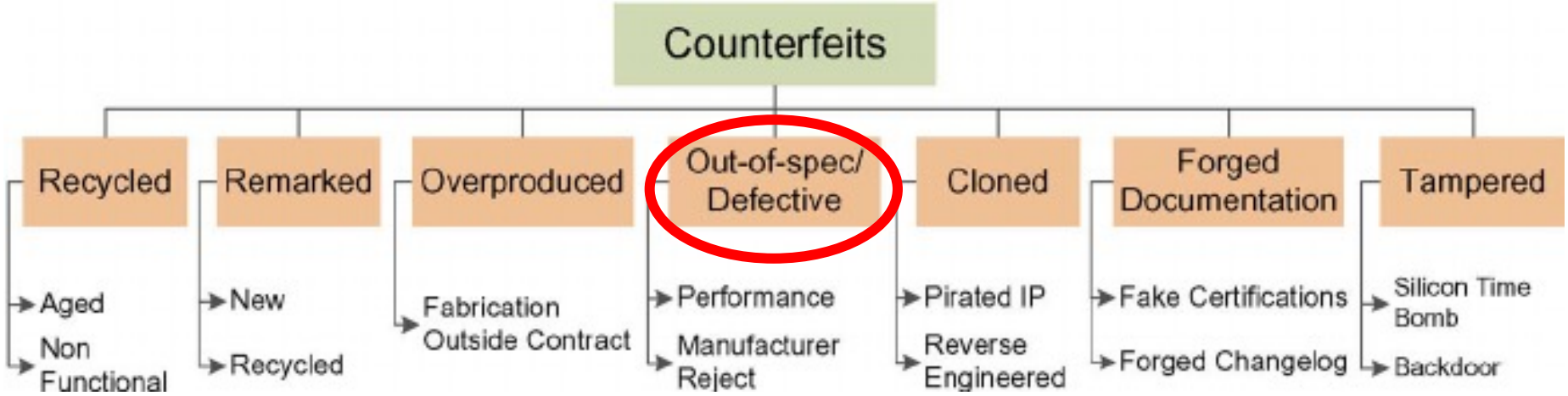
What

- Overproduction occurs when foundries sell components outside of contract with the design houseparts

Issues

- Loss in profits for the design and IP owner
- Reliability threats since they are often not subjected to the same rigorous testing as authentic parts

Counterfeiting types



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Defective components

What

- A part is considered defective if it produces an incorrect response to post-manufacturing tests

Defective components

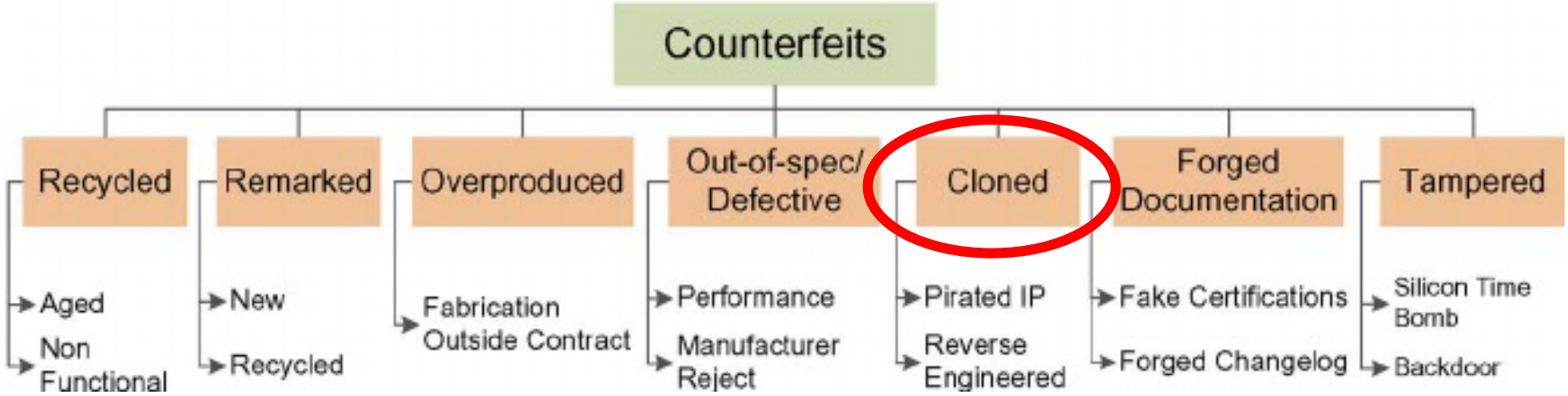
Actions to be taken

- These parts should be destroyed, downgraded, or otherwise properly disposed of

However…

- They are sold on the open markets:
  - knowingly by an untrusted entity
  - by a third party who has stolen them

Counterfeiting types



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Cloned components

What

- A copy of a design, in order to eliminate the large development cost of a part

Cloned components

What

- A copy of a design, in order to eliminate the large development cost of a part

How

- Reverse engineering
- By obtaining IP illegally (IP theft)
- With unauthorized knowledge transfer from a person with access to the part design

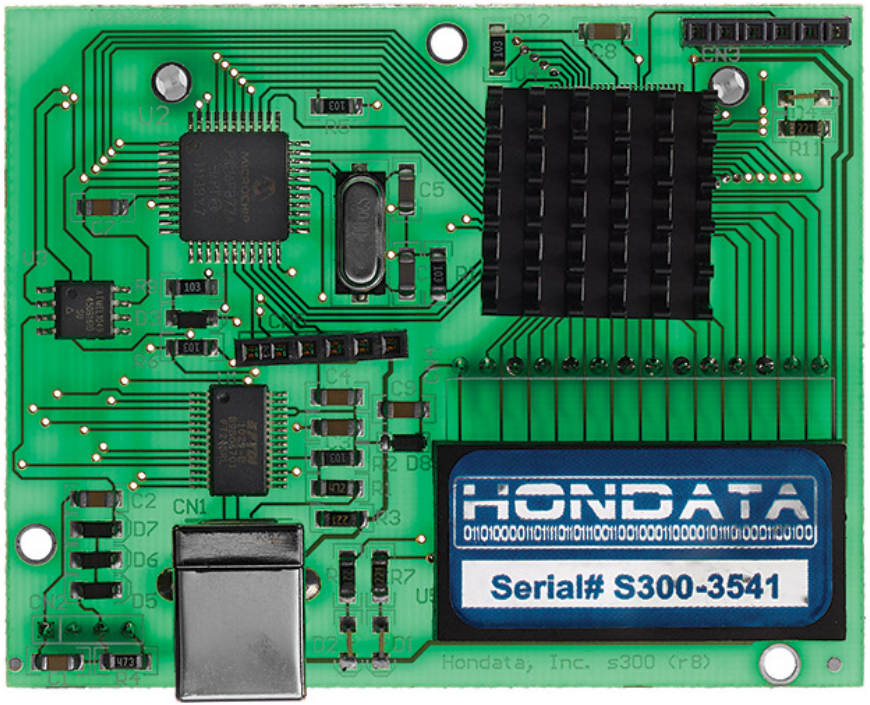
Risks

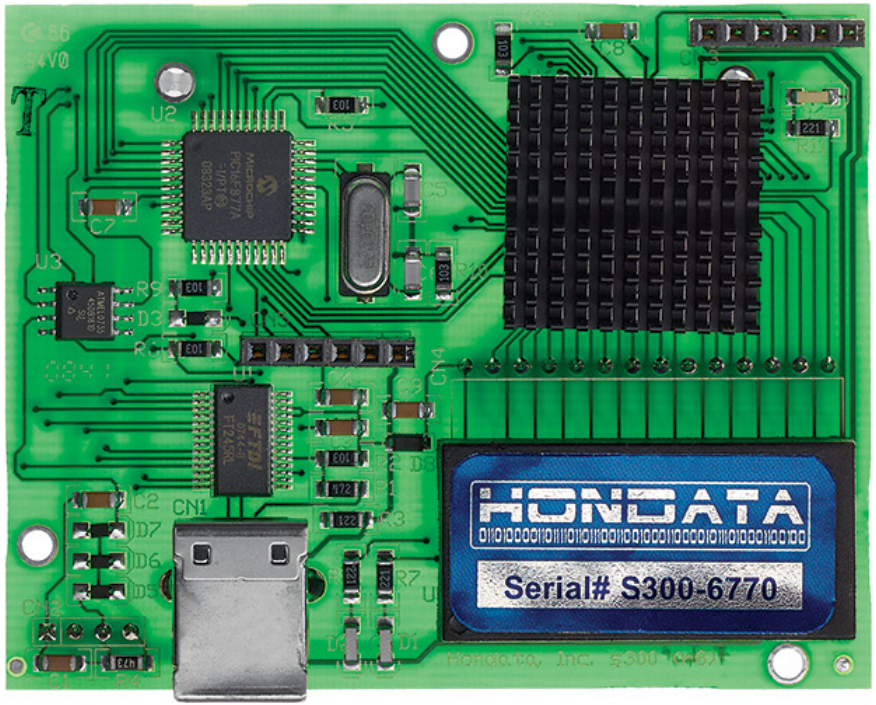
- Cloned electronics these days are potentially more nefarious: counterfeiters make their own components, boards, and systems from scratch and then package them into superficially similar products

Risks

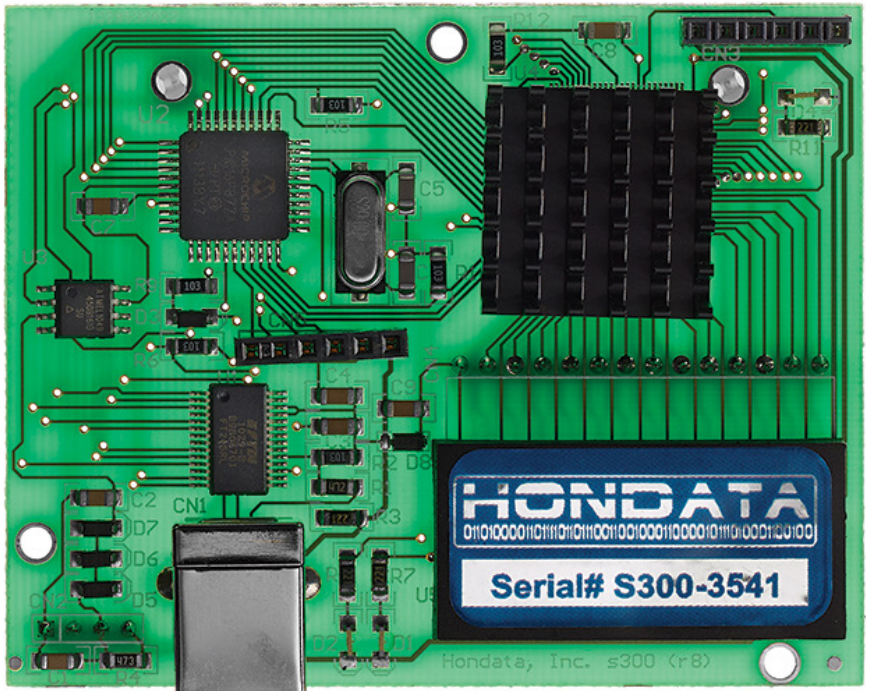
- The clones may be less reliable than the genuine product, having never undergone rigorous testing
- But they may also host unwanted or even malicious software, firmware, or hardware—and the buyer may not know the difference, or even know what to look for

Hondata s300 module

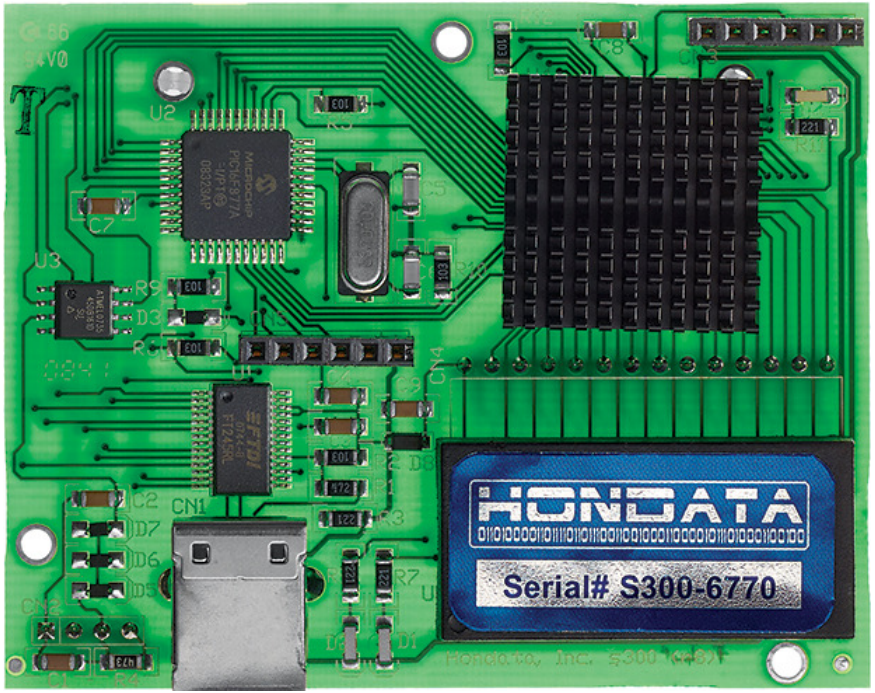




Hondata s300 module



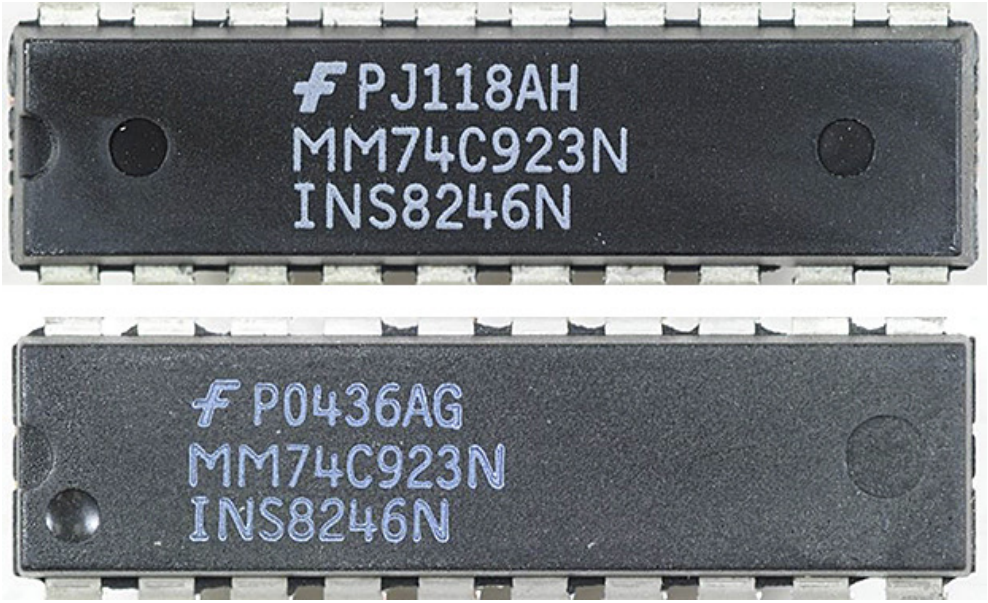
Cloned



Authentic

Encoder from Fairchild Semiconductor

Discontinued in 2011, but parts - real and fake - are still being sold



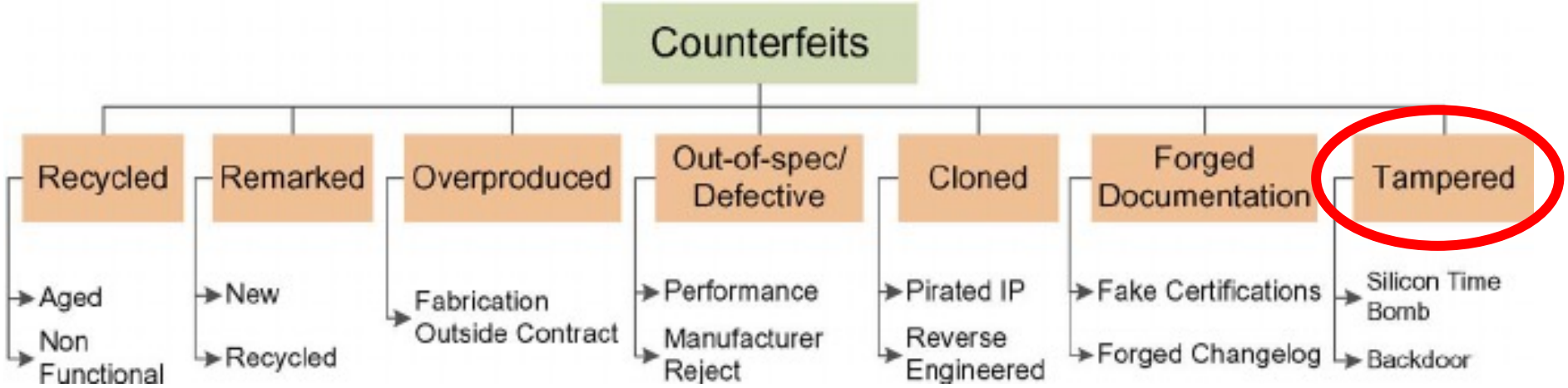
Encoder from Fairchild Semiconductor

Discontinued in 2011, but parts - real and fake - are still being sold

Cloned

Authentic

Counterfeiting types

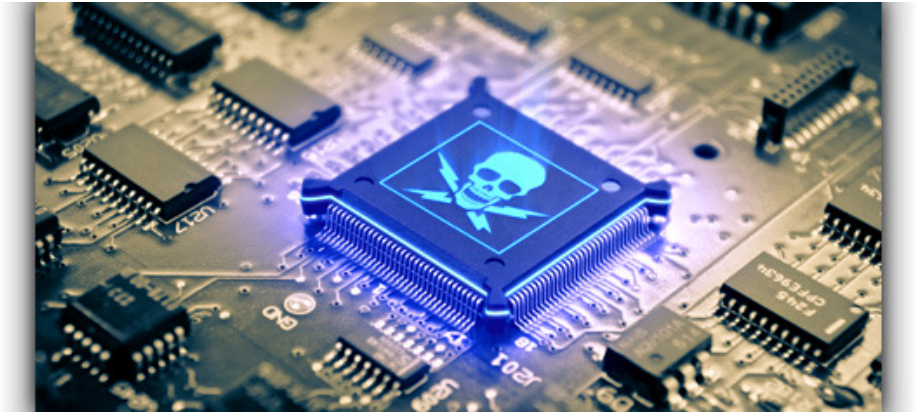


[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Tampered components

What

- Components modified in order to cause damage or make unauthorized alterations



Tampered components

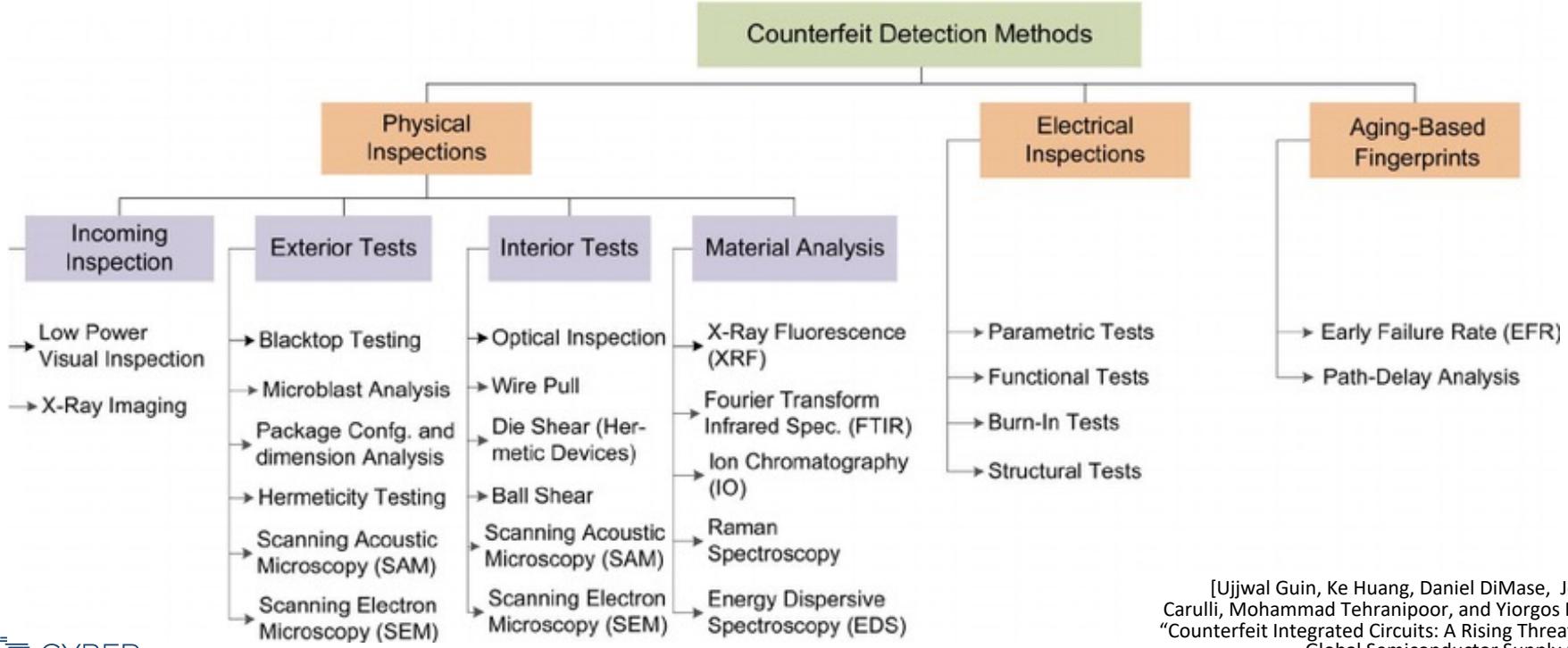
- They exploit *hardware Backdoors*

For a deeper analysis, please refer to the lecture:
CS_1.4 - Cybersecurity - Vulnerabilities

Outline

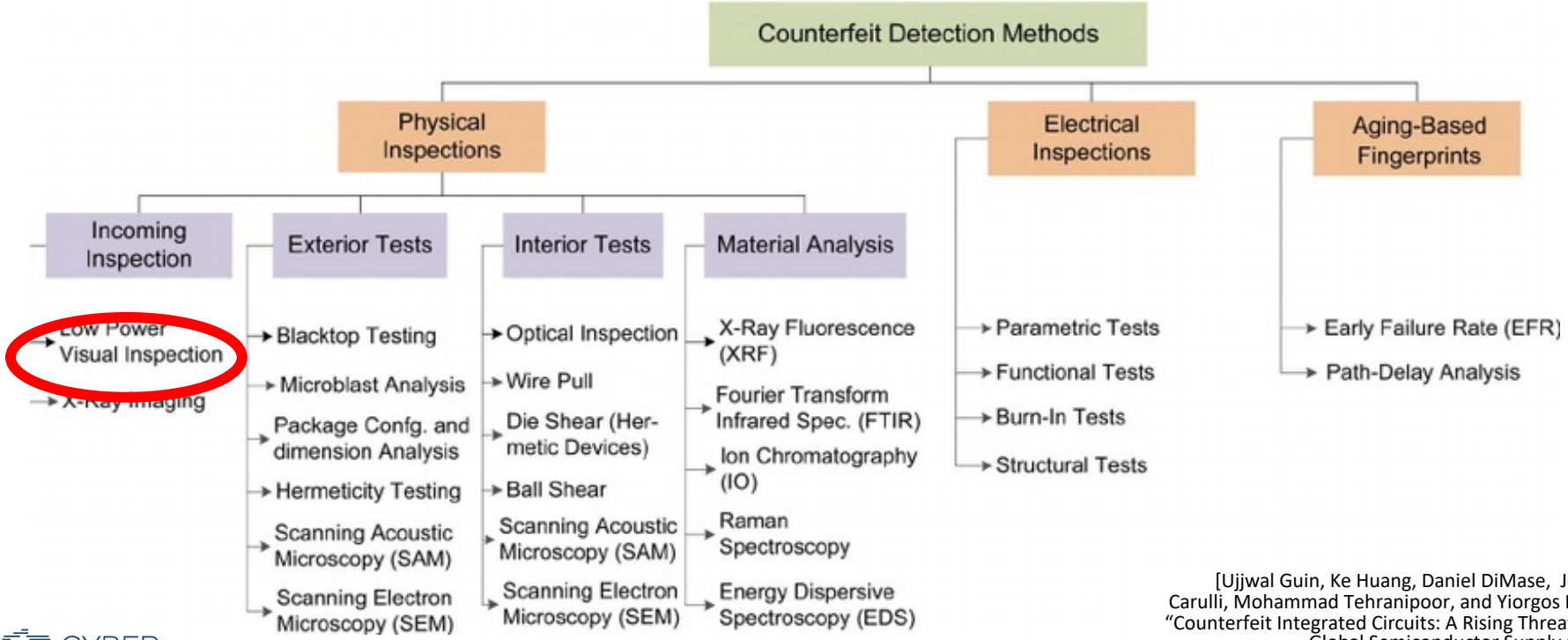
- Introduction
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Counterfeit Detection Methods



[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Counterfeit Detection Methods



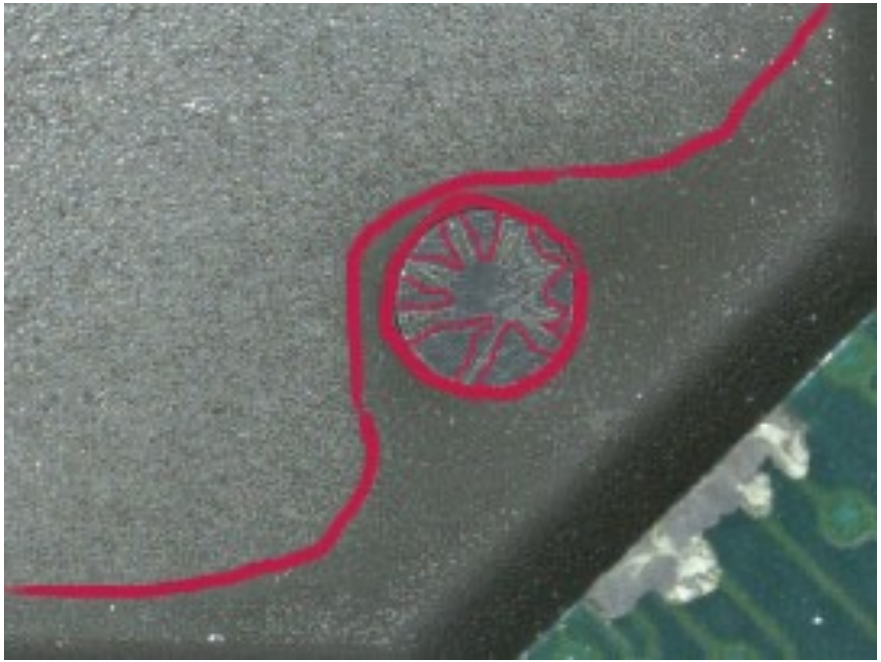
[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

Cleaning, visual inspection

- Aimed at identifying defects in the device packaging
- Some examples in the sequel

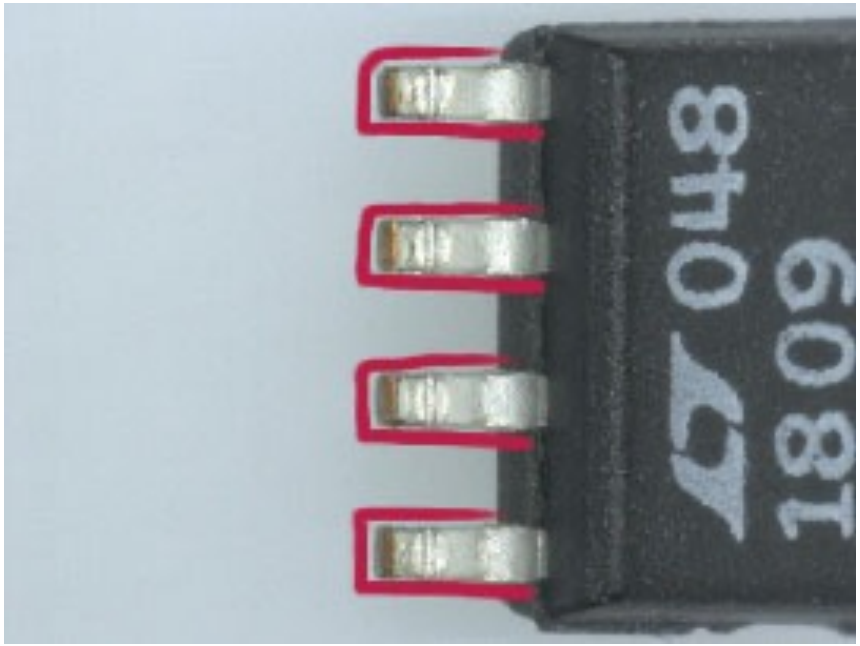
[http://www.counterfeit-ic.org]

Defect Description



- *Texture variation*
  is usually a consequence of sanding, remarking or resurfacing which are believed to be some of the most frequent but yet challenging to detect phenomena in counterfeit ICs

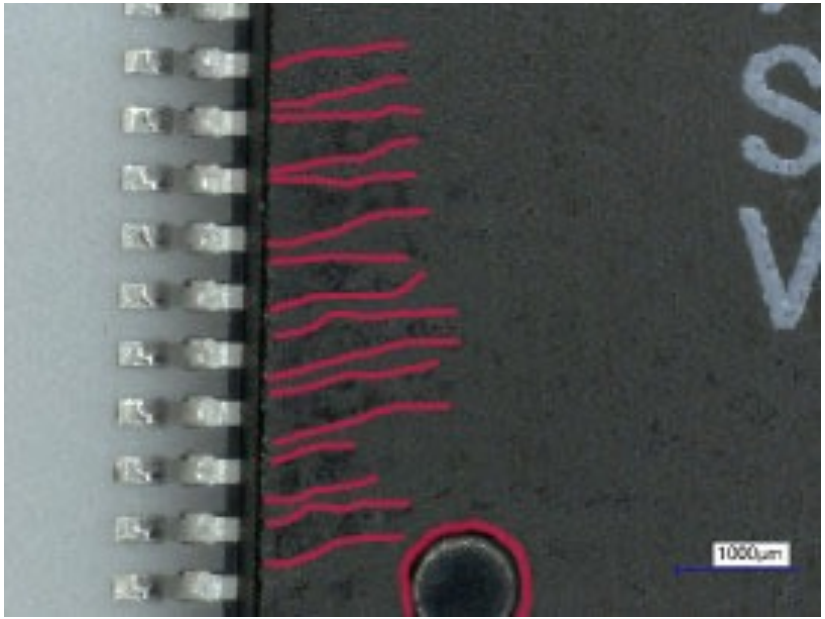
Defect Description



- *Oxidation*

  and corrosion on leads are caused when a part is kept for a long time without proper protection

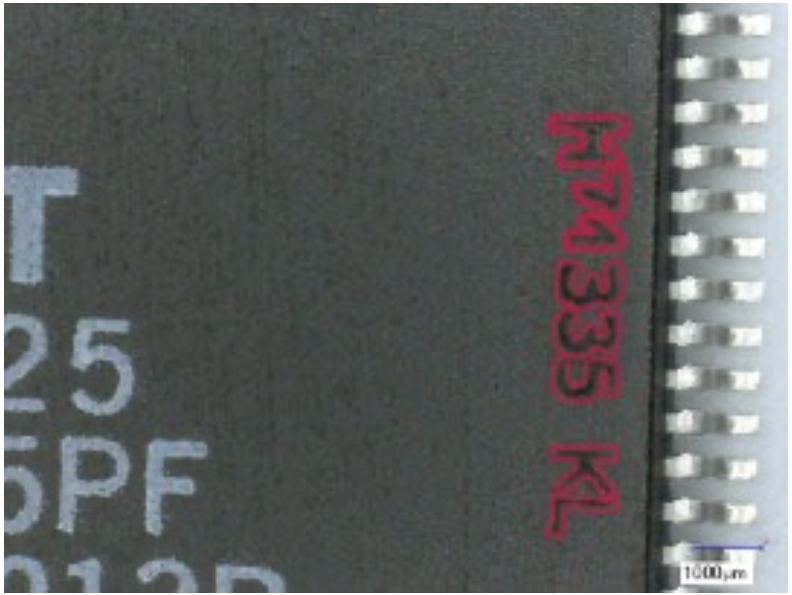
Defect Description



- *Contamination*

  indicates that the component could potentially be recycled

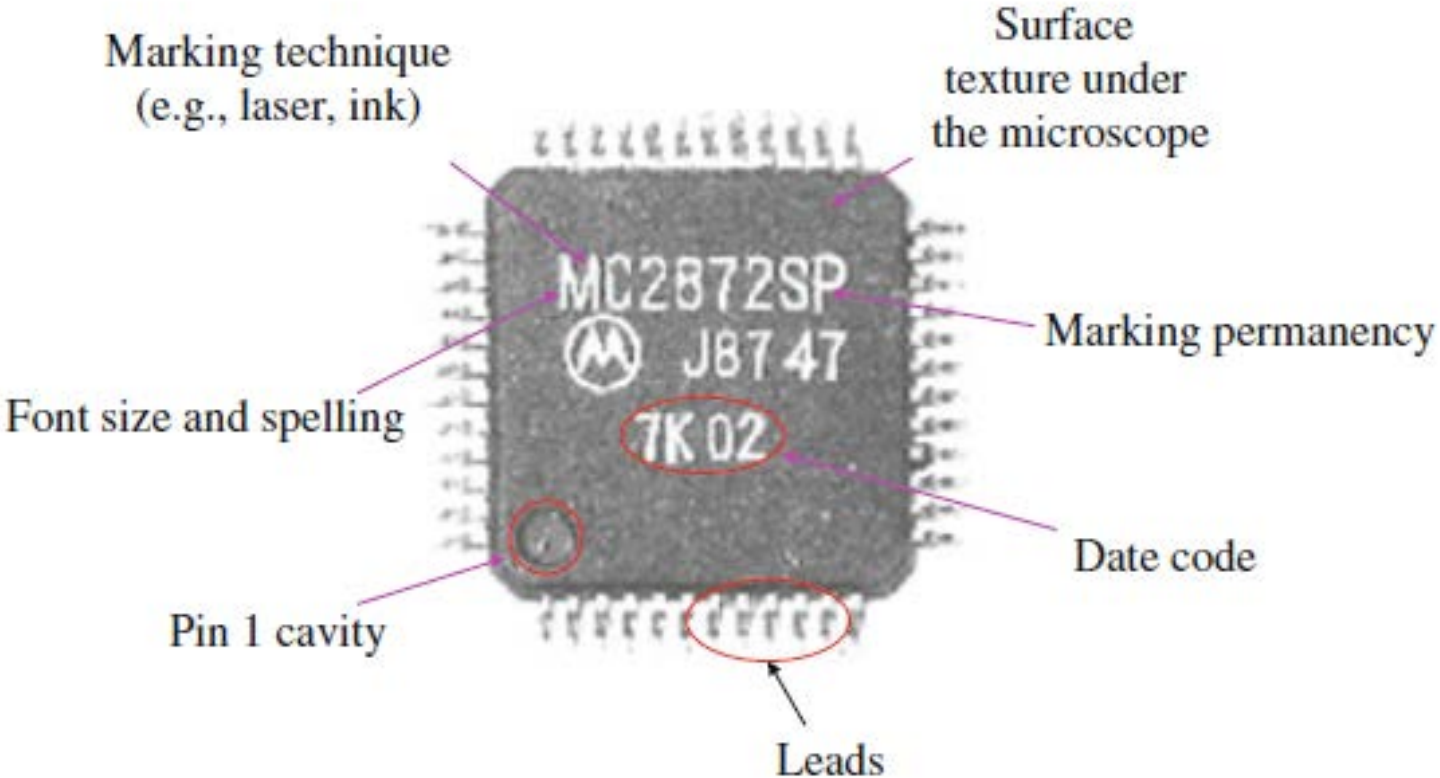
Defect Description



- *Ghost markings*

  appear when the counterfeiters do not remove entirely the original marking before printing the new one

What needs to be checked



Cleaning, visual inspection

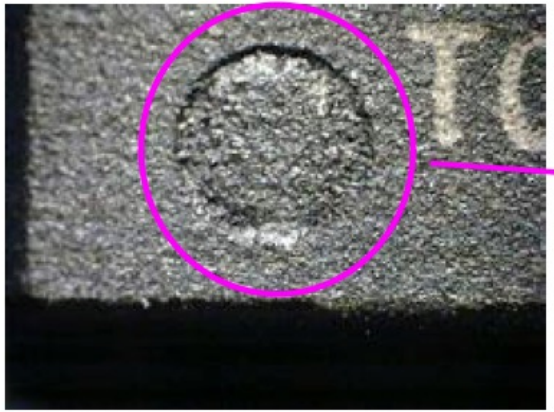
Cleaning, visual inspection

Real

Fake

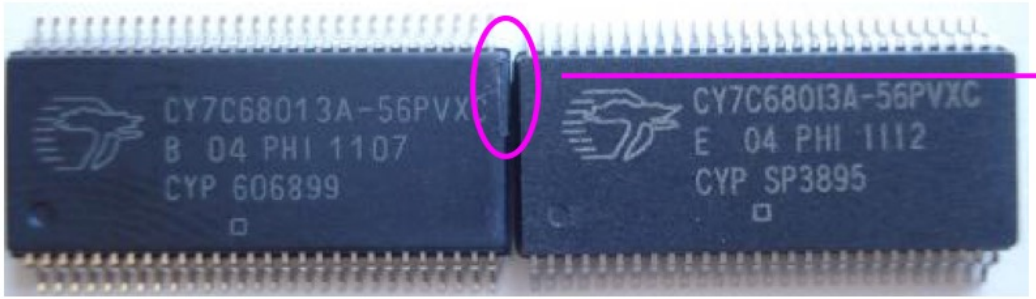
Cleaning, visual inspection

Cleaning, visual inspection



Indent filled in with the materials used to cover up the old surface

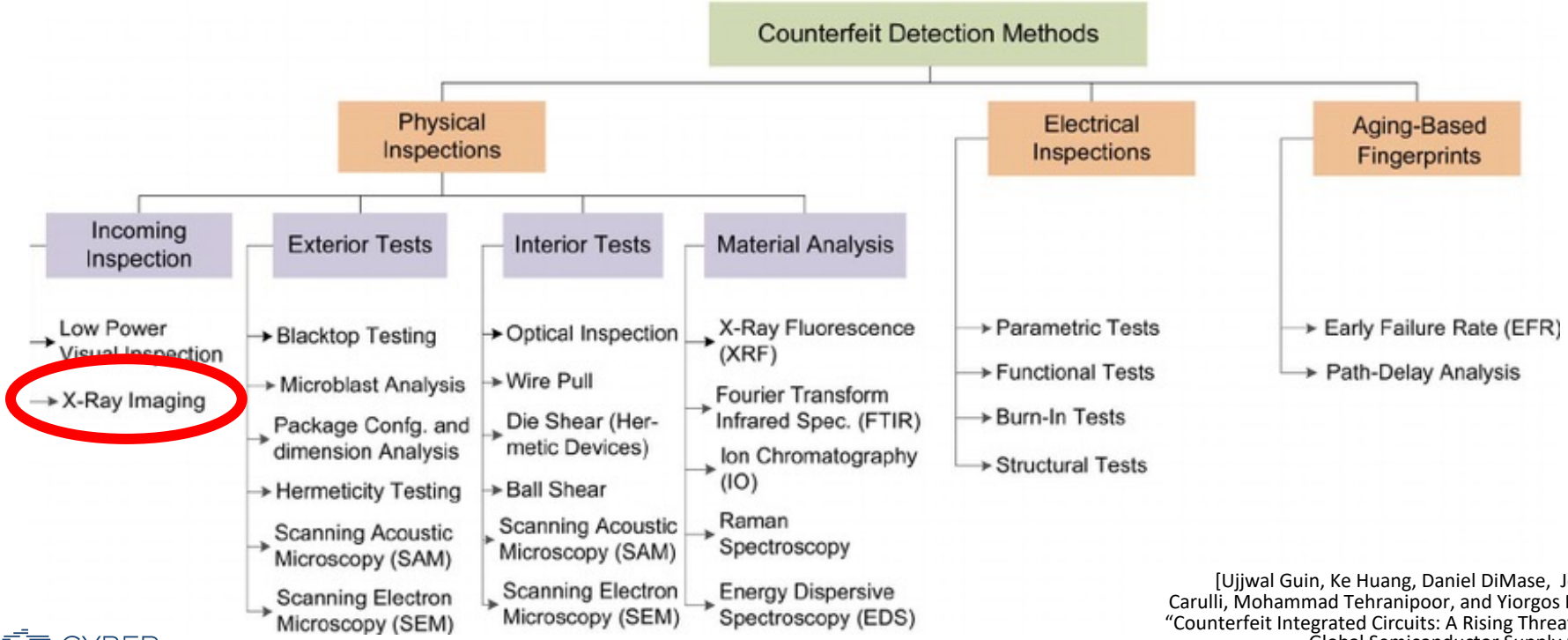
Cleaning, visual inspection



Brand new device has a sticker on its right side

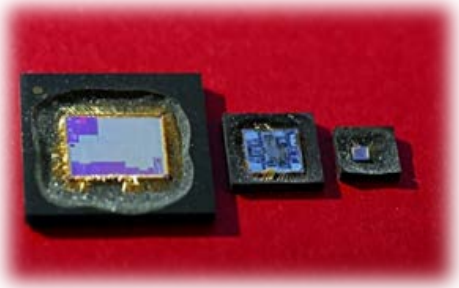
Brand new Counterfeit

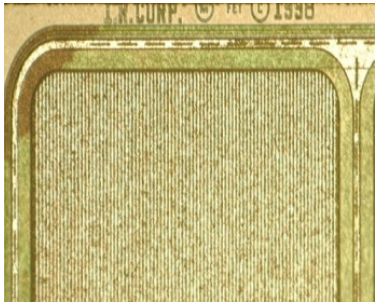
Counterfeit Detection Methods

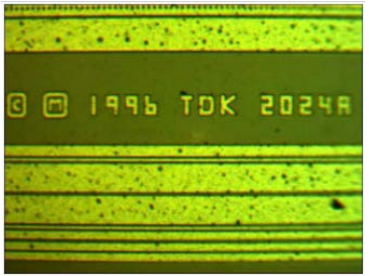


[Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, and Yiorgos Makris: "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", in Proceedings of the IEEE · August 2014 - DOI: 10.1109/JPROC.2014.2332291]

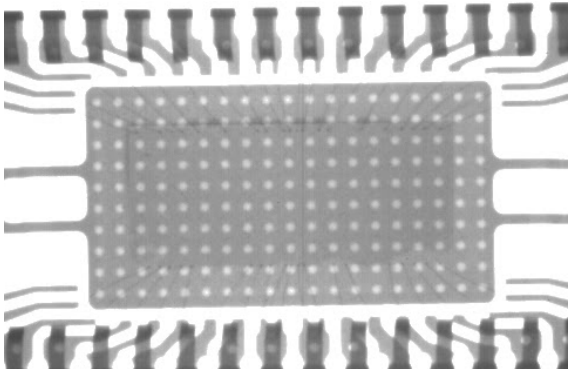
Inspection by microscopes

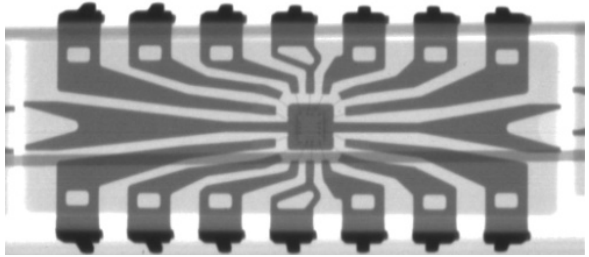






Inspection by X Ray





Outline

- Introduction
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Activation
- IP protection via Camouflage
- Physically Unclonable Functions (PUFs)

Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Activation
- IP protection via Camouflage
- Physically Unclonable Functions (PUFs)

Aging Detectors

- Sensors in the chip to capture the usage of the chip in the field
  - They rely on aging effects of MOSFETs to change a ring oscillator frequency in comparison with the golden one embedded in the chip
- Antifuse-based Technology for Recording Usage Time

Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Activation
- IP protection via Camouflage
- Physically Unclonable Functions (PUFs)

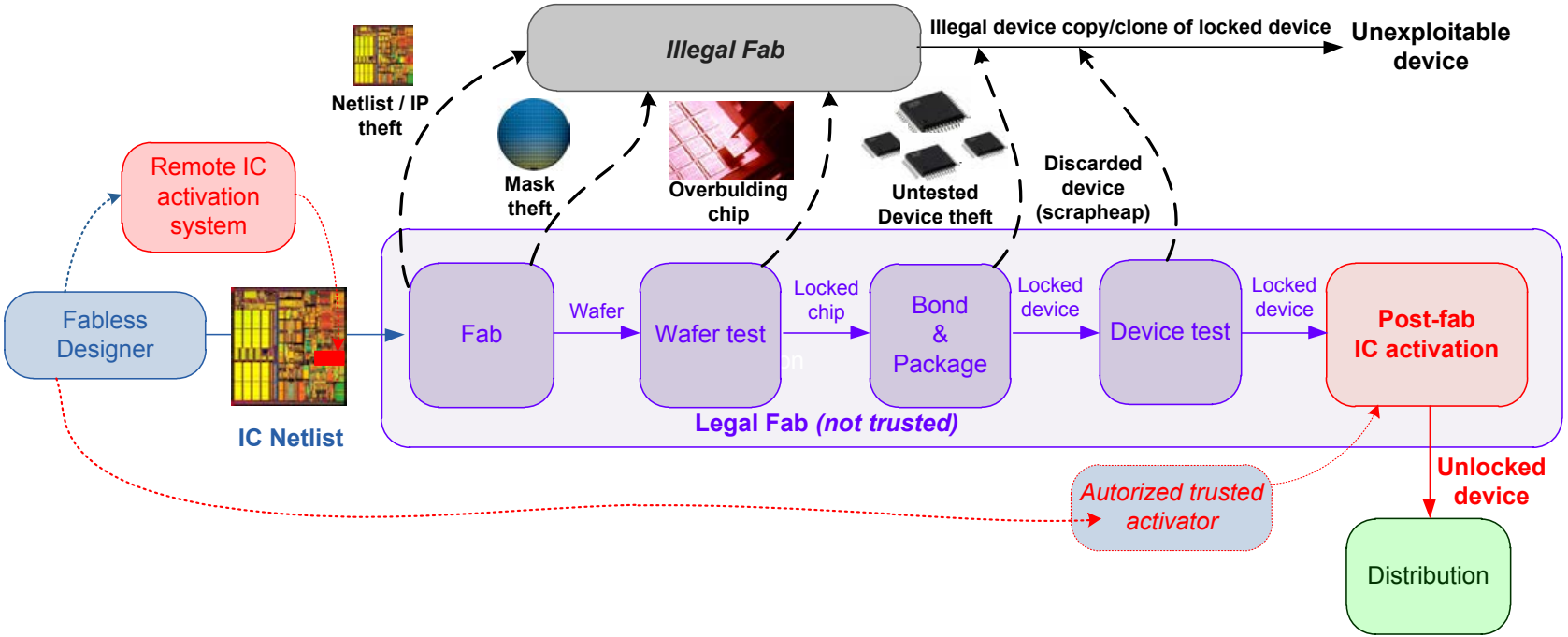
Hardware Metering

- A set of security protocols that enable the design house to achieve the post-fabrication control of the produced ICs to prevent overproduction
  - Post-Manufacturing Activation
  - Adding a Finite-State Machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs
  - Logic Encryption

Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Activation
- IP protection via Camouflage
- Physically Unclonable Functions (PUFs)

Integrated Circuits Activation

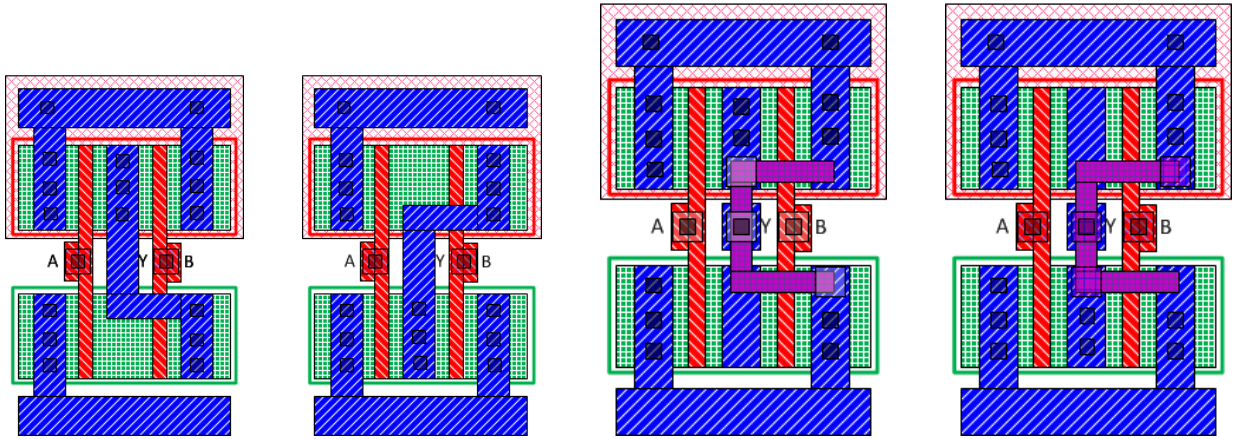


Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Activation
- IP protection via Camouflage
- Physically Unclonable Functions (PUFs)

IP protection via Camouflage

- Standard-cells are re-designed not to disclose their identity



NAND NOR Camouflaged NAND Camouflaged NOR

Advanced tools for Reverse Engineering

- A very interesting presentation on advanced tools for RE can be found here:
  - https://media.hardwear.io/integrated-circuit-offensive-security-olivier-thomas/

Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Activation
- IP protection via Camouflage
- Physically Unclonable Functions (PUFs)

PUFs - Physically Unclonable Functions

- A PUF (Physically Unclonable Function) is a built-in mechanism that generates one stable different ID for each identically-manufactured device, without the need of
  - programming the ID value
  - storing the value

PUFs - Physically Unclonable Functions

- Advan ges:
  - No re engineering can be applied
  - Even if cover an ID in one circuit, you cannot “clone” the dev *each* manufactured device has its own unclonab

For a deeper analysis, please refer to the lecture:
HS_2.5 - Physically Unclonable Functions - PUFs

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it