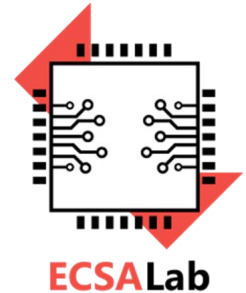


Integrated Circuit Security: The Hardware Trojan example

Paris Kitsos

Electronic Circuits, Systems and Applications Lab

E-mail: kitsos@uop.gr



<https://ecsalab.ece.uop.gr/>

Outline

- **ECE @ UoP profile presentation**
- **ECSA lab profile presentation**
- **Hardware Trojans (?)**

Department Profile

- **Department of Electrical and Computer Engineering was founded in MAY 2019 and belongs to the Engineering School in Patras**
- **Offer**
 - Undergraduate studies
 - Postgraduate studies
 - PhD studies
 - Post Doc studies
- **Personnel**
 - 32 Faculty Members
 - 5 Adjunct Teaching Staff with PhD
 - 6 Specialized Technical Laboratory Staff (ETEP)
 - 15 Teaching Assistants (Scholarships)

Studies

- **Undergraduate**

- 10 academic semesters (6 basic education and 4 specialism education)
 - Energy Systems
 - Signals, Telecommunications and Networks
 - Electronics, Computers and Systems
 - Informatics
- Integrated master



- **Postgraduate**

- Lasting 3 semesters
- Technologies and Services of Smart Information Systems and Communications



- **Doctoral**

- 58 Ph.D. students




- **Post – Doc**

- 3 post doc researcher (Electronics, Computer and Systems)

Electrical & Computer Engineering Department

Research and Development...

10 research labs operate in ECE department

Data & Media Lab (DM Lab) 

Data & Media Lab

Distributed Intelligent Systems and Data Lab (DISyD Lab) 

 **eBusiness and User Experience Lab (eBusiness Lab)**



ECSA Lab

Electronic Circuits, Systems and Applications Lab (ECSA Lab)

Embedded System Design and Applications Lab (ESDA Lab) 

ESDA
LAB

 **Interdisciplinary Semantic Interconnected Symbiotic Education
Environments Lab (InterSy Lab)**

Microelectronics & Communication Lab (MicroCom Lab) 

Nanotechnology & Advance Materials (NAM Lab) 

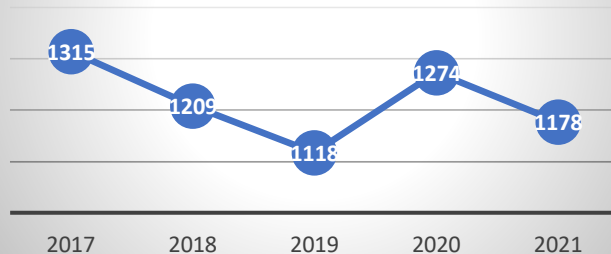
 **NeTDiT Network Technologies and Digital Transformation Lab (NeTDiT Lab)**

Power Systems Lab (PES Lab) 

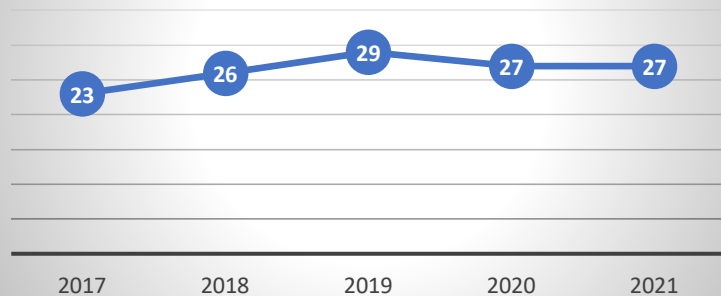
Power Energy Systems LAB

...Research and Development

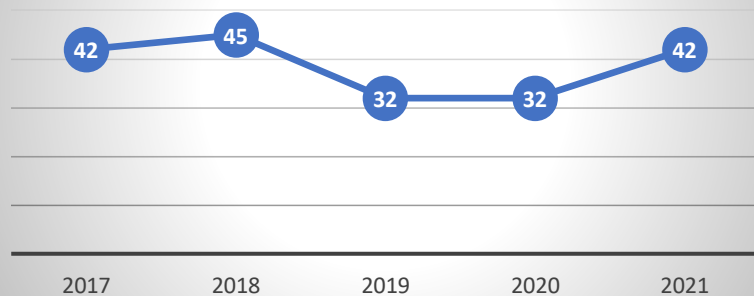
ECE dpt
Non-self Citations (Google Scholar)



ECE dpt
Journals

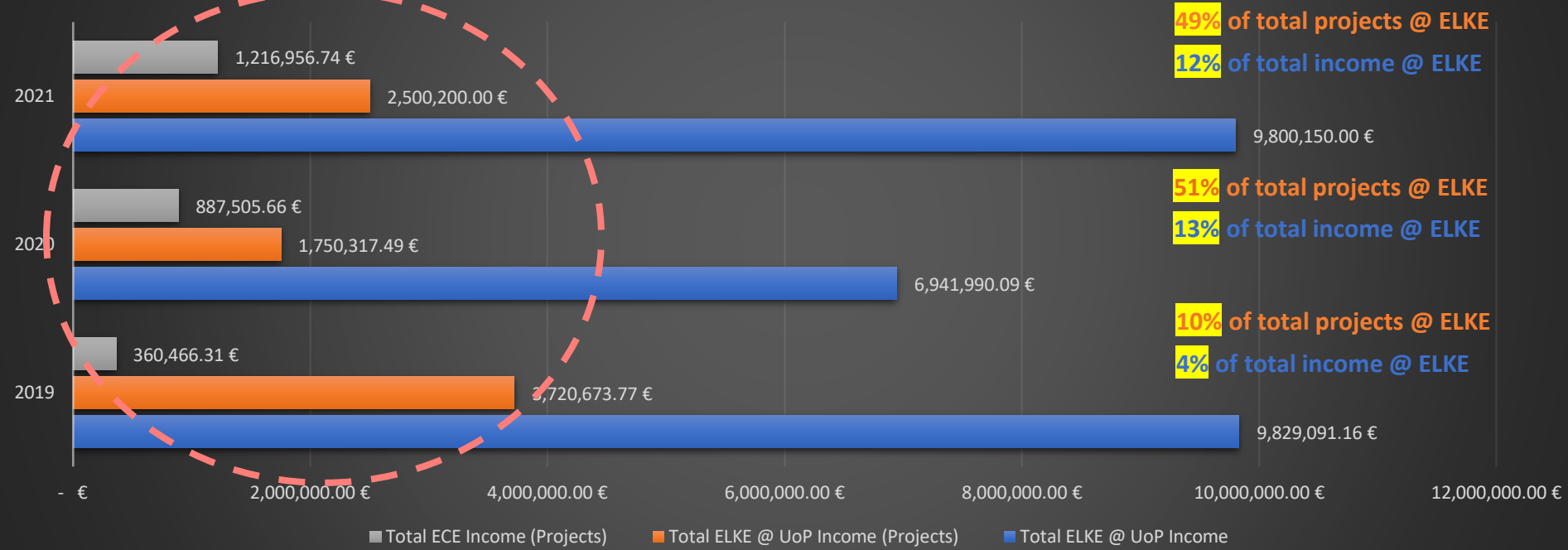


ECE dpt
Conferences



Participation in Research Projects

ECE contribution in total income of UoP ELKE (Special Account for Research Funding)



Electronic Circuits, Systems and Applications Lab...

- Founded in March 2020
- Focusing on education and research in the areas of Analog and Digital hardware design
- The major research subjects of the ECSA laboratory are:
 - HW design and prototyping for Security, Signal Processing and ML applications
 - FPGA and ASIC design
 - Analog and Mixed Signal Circuits
 - Analog nm IC design
 - Ultra Low Power Design
 - RF circuits
 - MOSFET modeling
 - ADCs
 - System-on-chip design
 - Microprocessor and microcontroller system design
 - Hardware – Software design

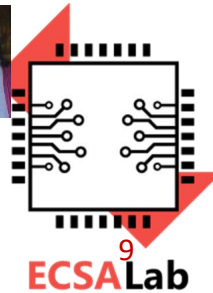
...Electronic Circuits, Systems and Applications Lab...

• Personnel

- 4 faculty members
- 2 Specialized Technical Laboratory Staff (ETEP)
- 1 Post-doc (in the field of Digital Signal Processing)
- 6 PhD students



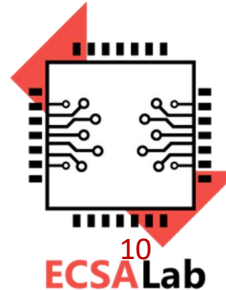
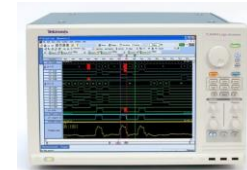
- Lampros Pyrgas, Hardware Implementations of Dictionary Learning Algorithms for Image Processing & Analysis
- Georgios Flamis, Efficient Hardware Architectures of Neural Networks
- Stavros Kalapothas, Hardware Design for Multi-modal Sensor Data Acquisition and Processing
- Marios Papadopoulos, Security of Cloud FPGAs
- Rafalia Malatesta, Analog Integrated Circuits for Low-consumption Systems
- Konstantinos Retsinas, Brain rhythm data retrieval system



...Electronic Circuits, Systems and Applications Lab...

- **Infrastructure**

- Educational platforms for Analog design
- Educational platforms for Digital design
- FPGA boards
- Oscilloscopes and Logic Analyzers
- PCB manufacturing equipment
- ASIC libraries
- Industrial equipment
- Power suppliers – waveform generators
- Europractice subscription



Research Projects (2019- today)

- 5 projects have been running in the lab or are running by the members of the laboratory
- 1 on-going (RIS3) dedicated to Smart Greenhouse (IoT Design and Data Processing)
- 4 finished
 - Smart health (Security)
 - Low-power IoT wireless protocol implementation
 - Industrial IoT (Security platform)
 - Smart farming (Video platform prototyping and implementation)
- We would like to confirm our interest to participate in preparation of project proposals

Research Publications

- **56 during the last years**
 - International journals (IEEE, MDPI, Elsevier, IET)
 - International conferences (IEEE, Euromicro)
 - Book chapters (Springer, CRC Press, IGI Global)
 - Edited books (Springer, Elsevier)
 - 2 books in Greek offered in Universities
 - 3 books offered in Hellenic Open University

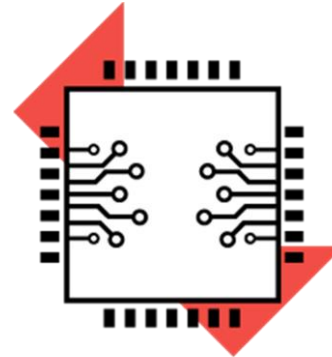
Thank you for your attention



Electrical & Computer
Engineering Department

**UNIVERSITY OF
PELOPONNESE**

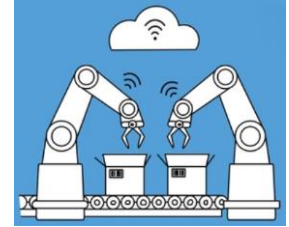
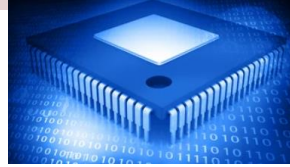
Questions??



ECSALab

Back-up Slides

Hardware Trojans - Introduction



- **Performing an action on a system (e.g. a cell phone calling, checking the root of a spaceship, etc.) is a combination of processes in software and hardware**
- **Software is the set of commands (programs) that perform operations in the system**
- **The hardware is the base (a circuit) in which the operation is performed based on the program that the software describes**



SW vs HW

- **SW can be replaced, updated, modified and downloaded from the Internet**
- **HW can not be modified after its manufacture**
- **SW Malware can be created and spread by anyone with a computer and Internet access**
- **HW Malware can only be imported by someone who can access, and change the circuit of an IC, during the design process**
 - **or during the programming of a FPGA**

#Fabless Design

- Fabless chip makers are companies that produce semiconductors for use in various types of electronics but does not manufacture the silicon wafers, or chips.

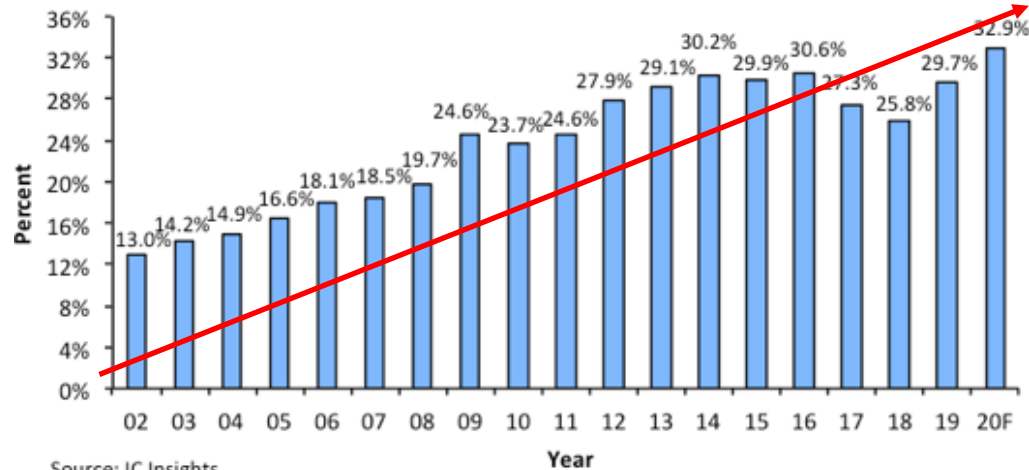
Rank	Company	3Q20 Revenue	3Q19 Revenue	YoY Change
1	Qualcomm	4,967	3,611	37.6%
2	Broadcom	4,626	4,486	3.1%
3	Nvidia	4,261	2,737	55.7%
4	MediaTek	3,300	2,154	53.2%
5	AMD	2,801	1,801	55.5%
6	Xilinx	767	833	-7.9%
7	Realtek	760	514	47.9%
8	Novatek	746	532	40.4%
9	Marvell	742	660	12.4%
10	Dialog	386	409	-5.6%

Notes:

1. This table shows only the top 10 IC design companies with publicly disclosed earnings.
2. NVIDIA's revenue excludes its OEM/IP businesses.
3. Qualcomm's revenue includes its QCT business only and not QTL; Broadcom's revenue includes its semiconductor business only.
4. 3Q20 USD/TWD=1:29.48; 3Q19 USD/TWD=1:31.21

Source: TrendForce, Dec. 2020

Fabless/System Company IC Sales as a Percent of Worldwide IC Sales (2002-2020)



Chip Manufacturing

- Different design phases of an Chip can be performed at geographically different locations
- An adversary has enough space to tamper the supply chain by a malicious hardware implementation of an extra logic
- This logic can be introduced in an IC at several points from the RTL source code to lithographic masks fabrication



Company A

Company B

Company D

The diagram features a central green rounded rectangle containing text. Above the rectangle, a dashed line connects three red boxes labeled 'Company A', 'Company B', and 'Company D'. Red lines also connect 'Company A' and 'Company B' to the top edge of the green box. 'Company D' is connected to the bottom edge of the green box. To the left of the green box, a red box labeled 'Company E' is partially visible.

Companies are located in different places in the world....

So, there is no EFFICIENT CONTROL what they sell!!!

Hardware Trojan

- A Hardware Trojan (HT) is a modification of the original IC design
 - Aiming to exploit hardware characteristics or access information stored/processed on the chip or downgrade the performance of the IC
- Consist of two main parts
 - Trigger part is used to activate the malicious payload when specific conditions are met
 - Payload part performs the malicious action(s) defined by its creator
- **Hardware Trojan has become one of the most critical threats to Chip production for commercial, consumer as well as military applications. (M. Tehranipoor and F. Koushanfar: "A survey of hardware Trojan taxonomy and detection", IEEE Des. Test. Comput., vol. 27, no. 1, January 2010)**

HT – An example

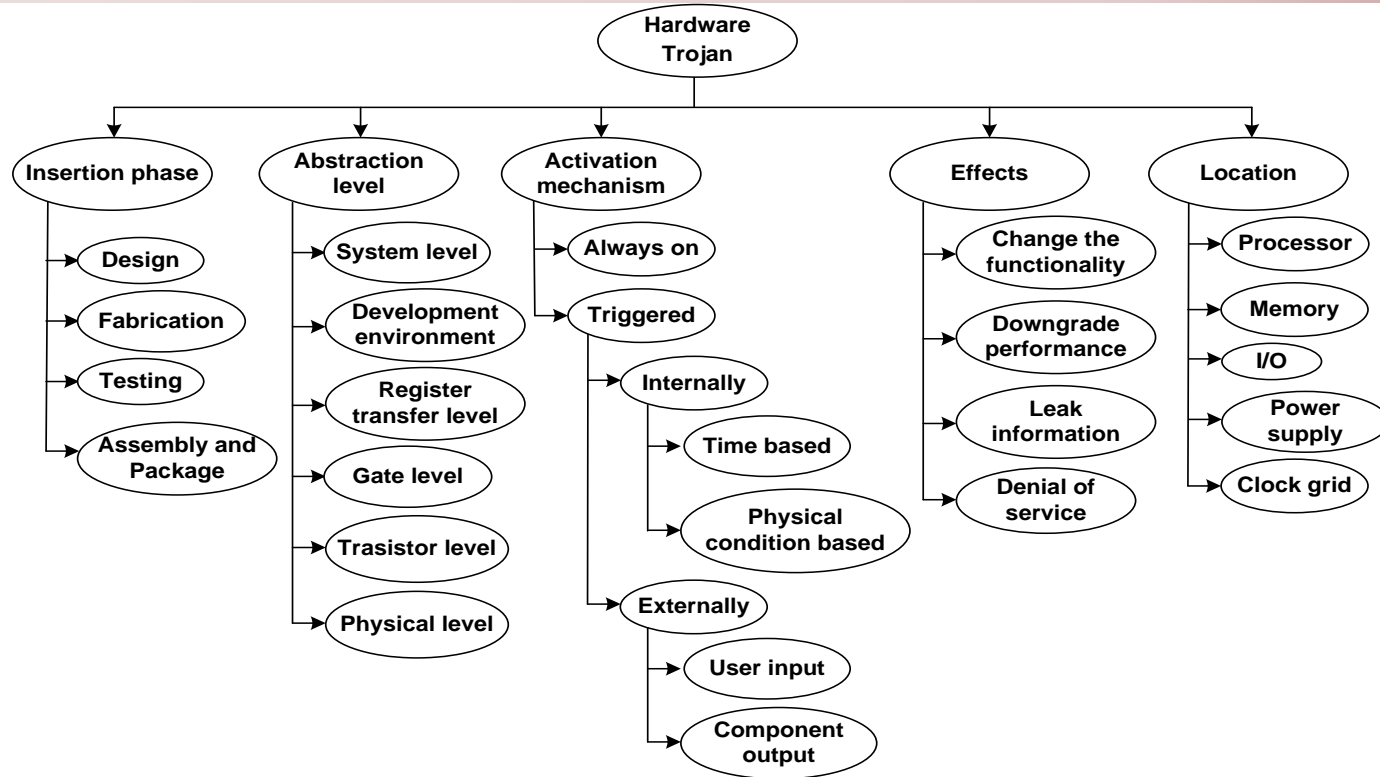
- In 2012, researchers announced for the first time that they had detected a backdoor in an FPGA that was commercially available for military use

«S. Skorobogatov and C. Woods, “Breakthrouhg Silicon Scanning Discovers Backdoor in Military Chip”. Cryptographic Hardware and Embedded Systems Workshop (CHES 2012), pp. 23-40, Springer, 2012»

HT Taxonomy...

- An approach to give an answer to the question: *“Are you sure that a Chip under test is free (or not free) of Hardware Trojan?”* is still missing.
- For an effective defense we **MUST** understand the design philosophy of HT design
- A framework that groups the Trojans types is required
 - This enables a systematic study of the Trojan characteristics
- Techniques for detection, mitigation and protection can be developed for each Trojan type along with some benchmarks for countermeasures' comparisons
- An efficient taxonomy that categorize the insertion, abstraction level, activation mechanism, effects, and location is needed

...HT Taxonomy



HT design...

- **Combinational circuit**

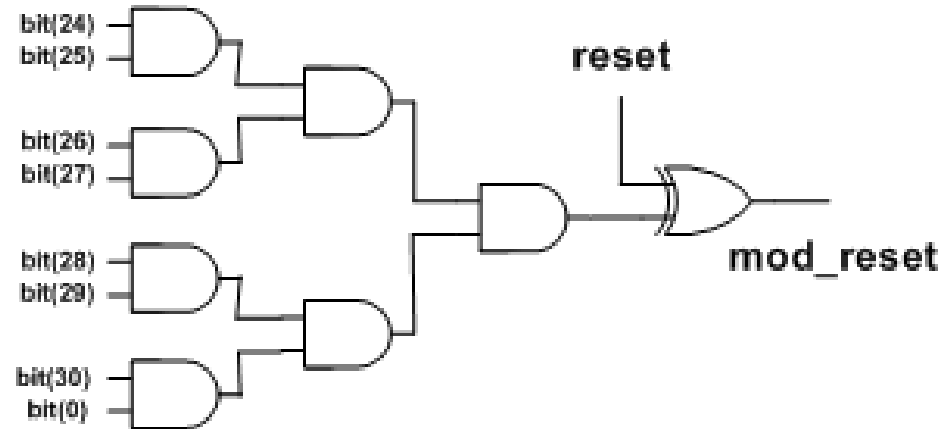
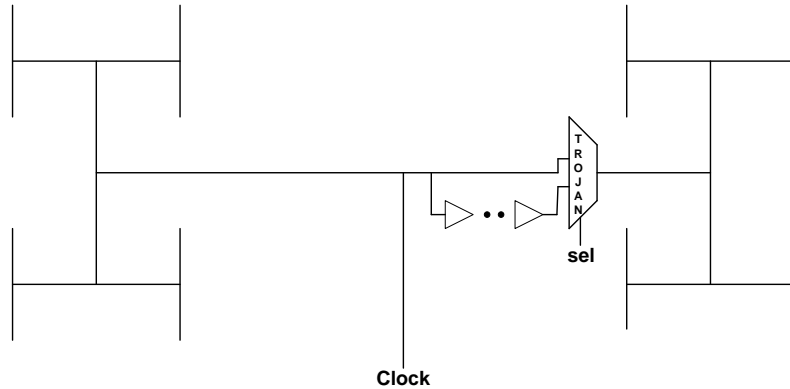
- **Small area and low overhead**
 - Sometimes as little as one gate
- **Simplistic design**
- **Limited effects**
 - Function---altering
 - Reliability degradation

- **Sequential circuit**

- **Larger and more Complex**
 - Logical datapath
 - Data storage registers
- **Wide range of effects**
- **High implementation cost**

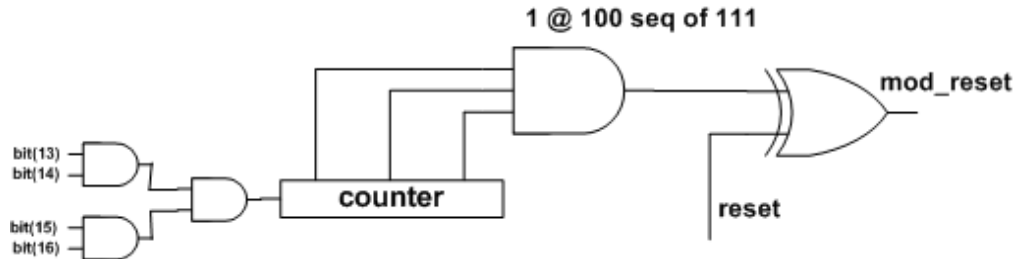
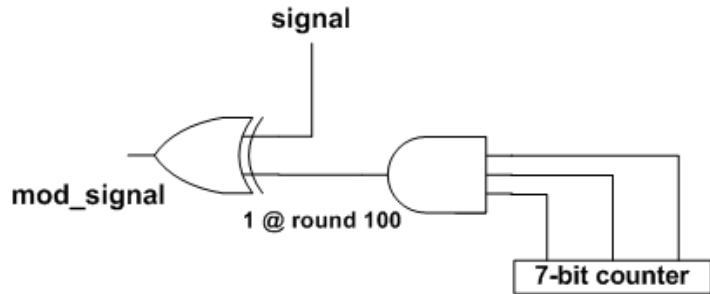
...HT design...

- Combinatorial circuits



HT design...

- Sequential circuits (Time bombs)



HT Detection Techniques

- **Destructive techniques**

- A demetallization process of the circuit under test extracts its layers, followed by image reconstruction and analysis for detecting modified transistors, gates, or routing elements
- Is an extremely expensive and time-consuming approach
- Impractical for all chips

- **Non destructive techniques**

- Run-time monitoring approach
- Test-time monitoring approach

Run-Time Approaches

- **These approaches are typically invasive approaches where some special circuits are involved in the chip**
- **These circuits can exploit pre-existing redundancy in the circuit to avoid an inflected part of the circuit**
- **All chips can integrate the monitoring circuits**
 - **However, significant performance and power consumption overheads are incurred**

Test-Time Approaches

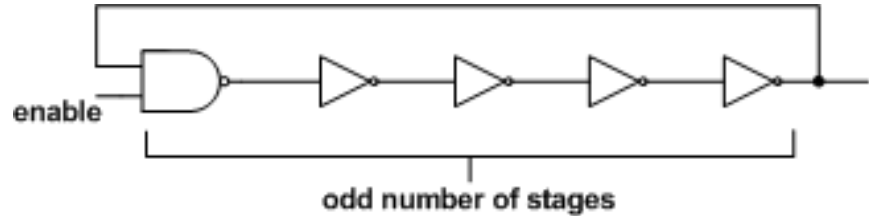
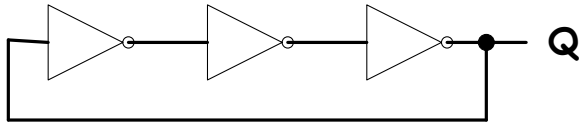
- **The test-time techniques can also be used by special circuits like scan-chains or sensors**
- **These circuits can enhance the detection sensitivity**
- **Test-time techniques can be classified into approaches based on circuit logic and on side-channel analysis**
 - **The circuit logic approaches apply carefully-crafted test vectors for activating the Trojan and observing the effects of the payload at the chip outputs**
 - **Large amount of test vectors are needed**

Side Channel Analysis

- **Any Trojan in the chip is reflected into one or more side-channel parameters**
 - Quiescent supply current; leakage current; dynamic power; electromagnetic radiation (EM) due to switching activity; and path-delay characteristic
- **Specialized and expensive testing equipment is necessary as to detect the weak side-channel signals produced by hardware Trojan horses**
- **Side-channel analysis does not need to activate the Trojan in order to detect it**
- **A golden chip is used for comparison**

Ring Oscillator (RO)

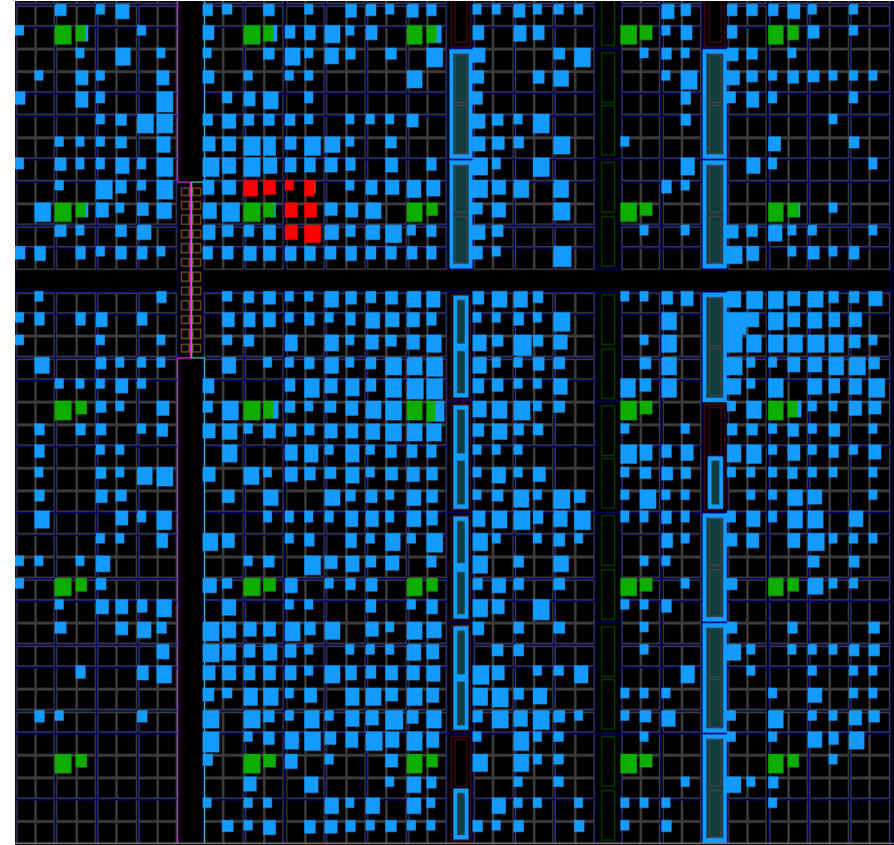
- On-chip digital sensor can be a helpful detection technique by focusing the test efforts on specific regions of an chip
- A Ring Oscillator (can be part of a digital sensor) is a digital component composed of an odd number of NOT gates whose output oscillates between the two logical levels, 0 and 1



RO-based HT Detection...

- **The Ring Oscillator (RO) oscillates due to its inherent logic**
- **The oscillation frequency depends on the exact components and size of a circuit**
 - The circuit around the RO
- **Modifications of the components, such as insertion of additional gates or different placement can change this frequency**

- AES block cipher has been implemented
- 25 sensors are placed in a 5x5 network structure (green)
- They have been placed several sensors so that at least one near an HT (red)



...RO-based HT Detection...

- **Measurement of the RO frequency in normal operating condition of the circuit (when HT is not activated)**
- **Force the circuit with suitable inputs (eg Combinatorial testing arrays^{# %}) so that there is a good chance of activating HT**
- **Measure the RO-frequency when HT is active**

[#]Paris Kitsos, Dimitris. E. Simos, Jose Torres-Jimenez, Artemios G. Voyiatzis, "Exciting FPGA Cryptographic Trojans using Combinatorial Testing", 26th IEEE International Symposium on Software Reliability Engineering (ISSRE 2015), Gaithersburg, MD, USA, November 2-5, 2015.

[%]Ludwig Kapmel, Paris Kitsos, Dimitris Simos, "Locating Hardware Trojans Using Combinatorial Testing for Cryptographic Circuits", IEEE Access, Vol. 10, pp: 18787 - 18806, 2022.

...RO-based HT Detection

- **Measurements with three types of ROs**

Ring Oscillator	# Registers	# LUTs	Count Difference
3-Stage RO	0	3	917
Latch RO	0	2	823
Flip-Flop RO	2	9	1488

L. Pyrgas, A. Panagiotarou and P. Kitsos, "Are ring oscillators without a combinatorial loop good enough for Hardware Trojan detection?", 23rd Euromicro Conference on Digital Systems (DSD'20), Slovenia, August 26 - August 28, 2020