COINS Summer School 2017 on Secure Implementation of Cryptographic Software

Metochi - Lesbos island, Greece

Detection of Hardware Trojans

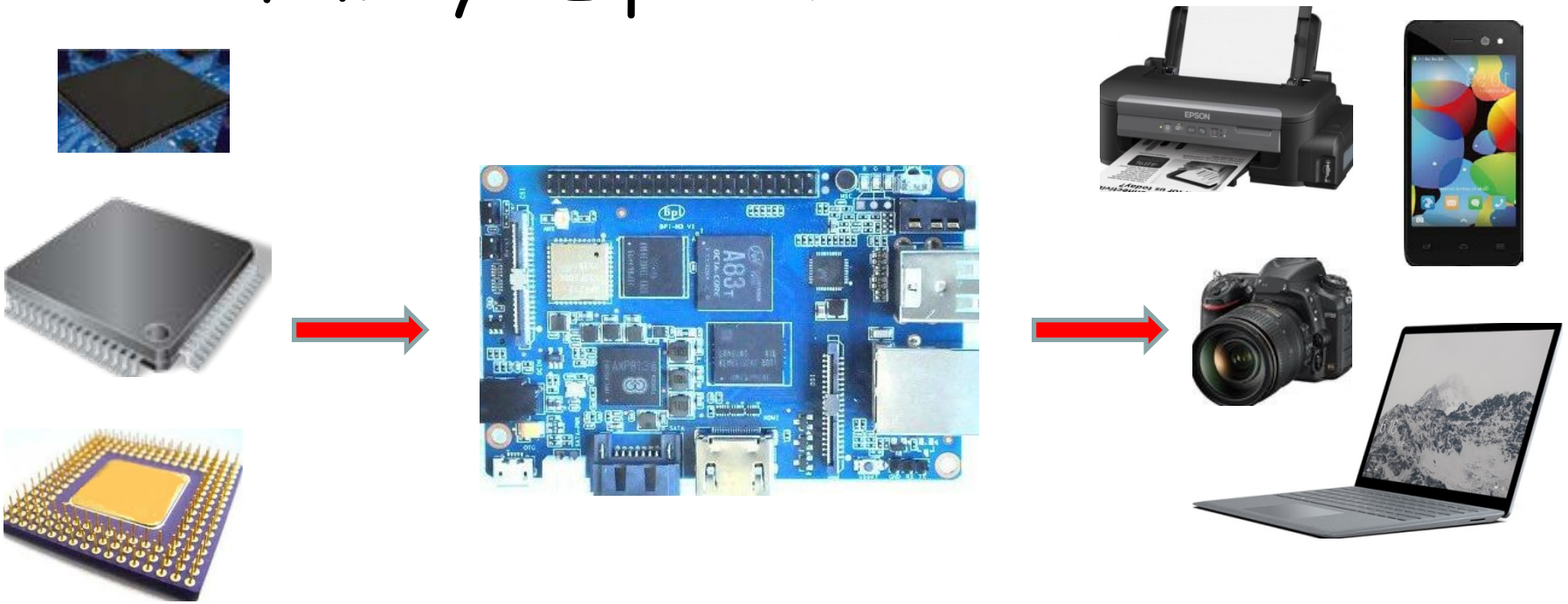
Paris Kitsos
Digital IC dEsign and Systems Lab (DICES Lab)
http://diceslab.cied.teiwest.gr
e-mail: pkitsos@teimes.gr

Agenda

- Introduction
- Hardware Trojans horses
- Detection techniques
- An example of a detection technique
- Case study: a Trojan on AES block cipher

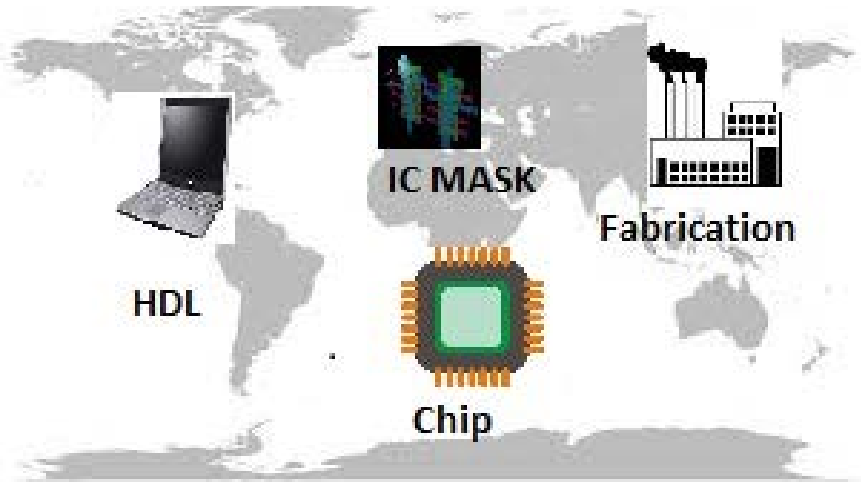
Introduction…

- VLSI chips (FPGAs and ASICs) are at the heart of many CE products!!!



…Introduction…

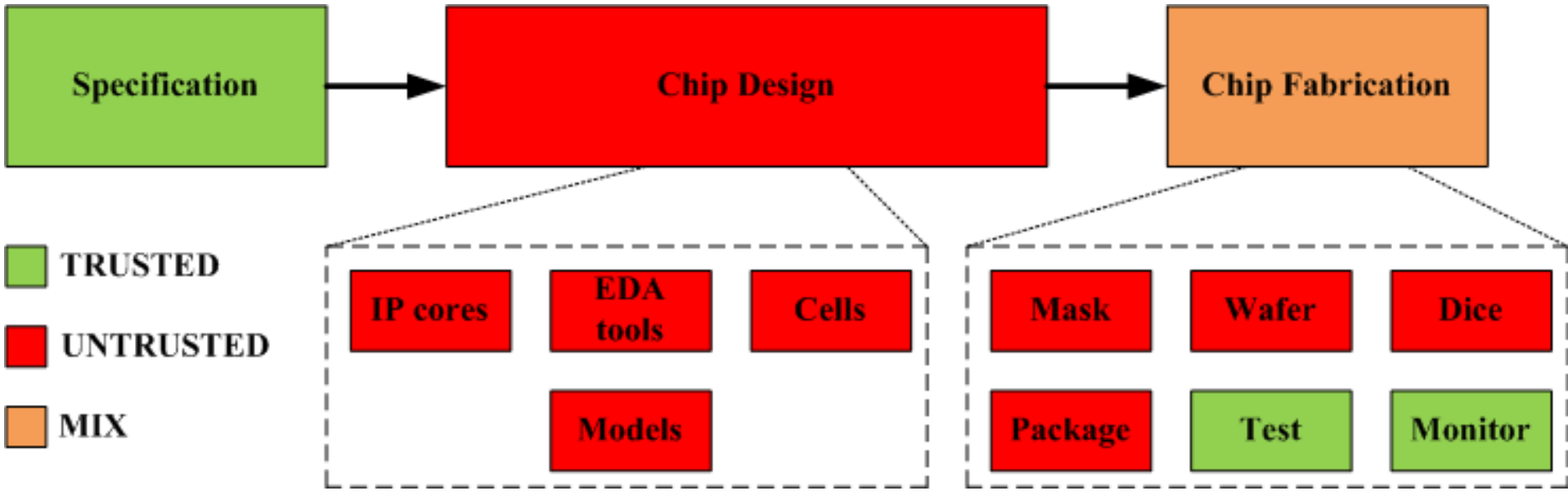
- Different design phases of a chip can be performed at geographically different locations
- An adversary has enough space to tamper the supply chain by a malicious hardware implementation of an extra logic
- This logic can be introduced in a chip at several points of design phases (from the RTL to fabrication)



Video

...Introduction

- The Life cycle of a chip



Sengupta A. (2017). Hardware Vulnerabilities and Their Effects on CE Devices: Design for Security Against Trojans [Hardware Matters]. IEEE Consumer Electronics Magazine.

Agenda

- Introduction
- Hardware Trojans horses
- Detection techniques
- An example of a detection technique
- Conclusion

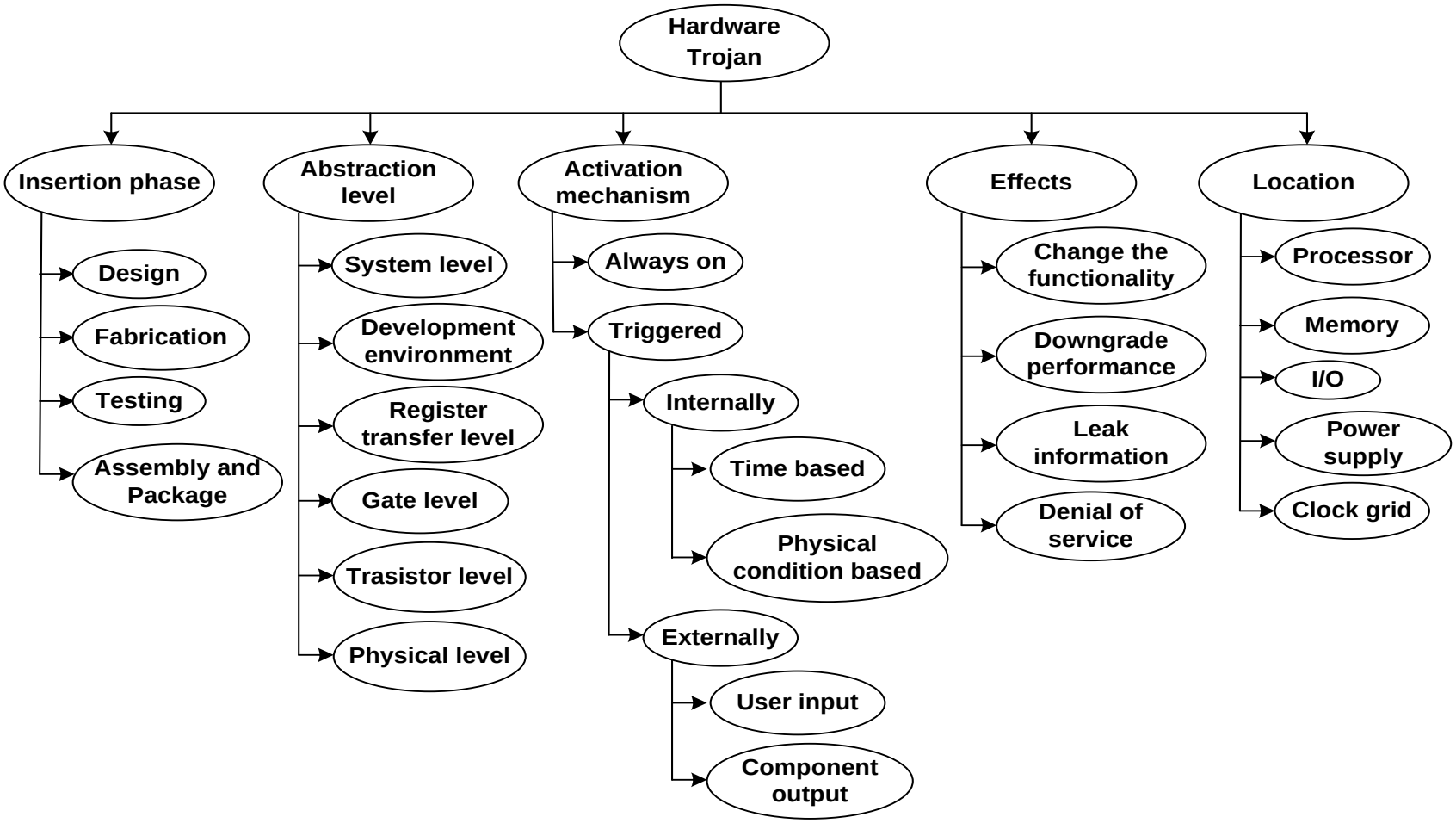
What is a hardware Trojan horse

- A Hardware Trojan Horse (HTH) is a modification of the original chip design
  - Aiming to exploit hardware characteristics or access information stored/processed on the chip or downgrade the performance of the chip
- Consist of two main parts
  - Trigger: is used to activate the malicious payload when specific conditions are met
  - Payload: performs the malicious action(s) defined by its creator

Hardware Trojan taxonomy…

- A methodological approach to address the question: "*Is a given chip under Test free of hardware Trojan horses?*" is still missing.
- For an effective defense we have to understand the design philosophy of HTH 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

…Hardware Trojan taxonomy



Rajendran, J., Gavas, E., Jimenez, J., Padman, V., & Karri, R. (2010). Towards a comprehensive and systematic classification of hardware Trojans. *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*

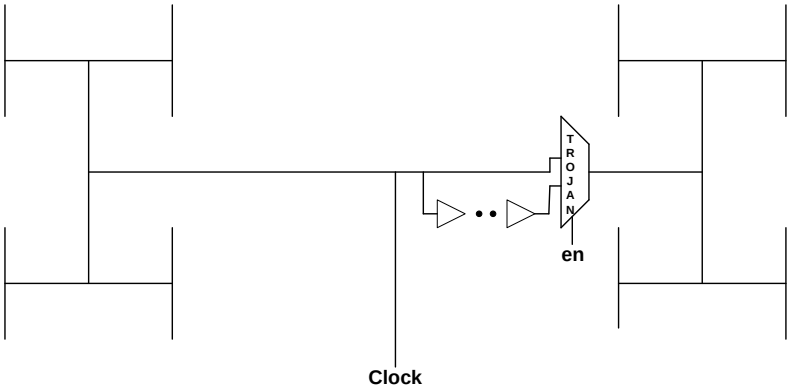
Hardware Trojan design…

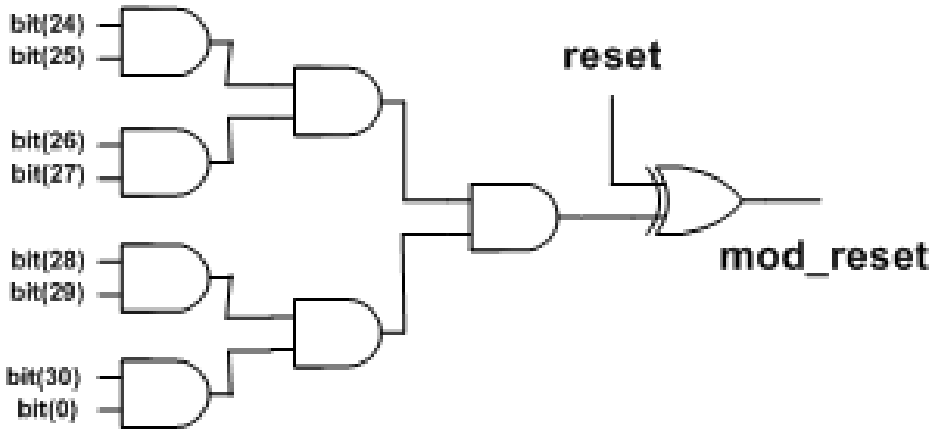
- Combinational circuit
- Small area and low overhead
  - Sometimes as little as one gate
- Simplistic design
- Limited effects
  - Function---altering
  - Reliability degradation

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

…Hardware Trojan design…

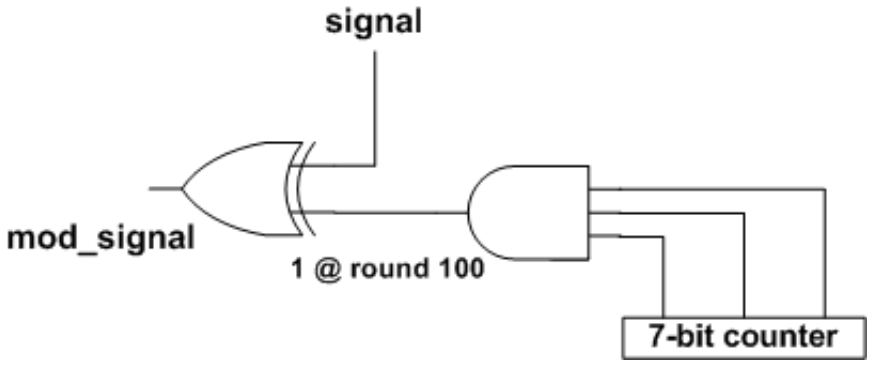
- Combinational circuits

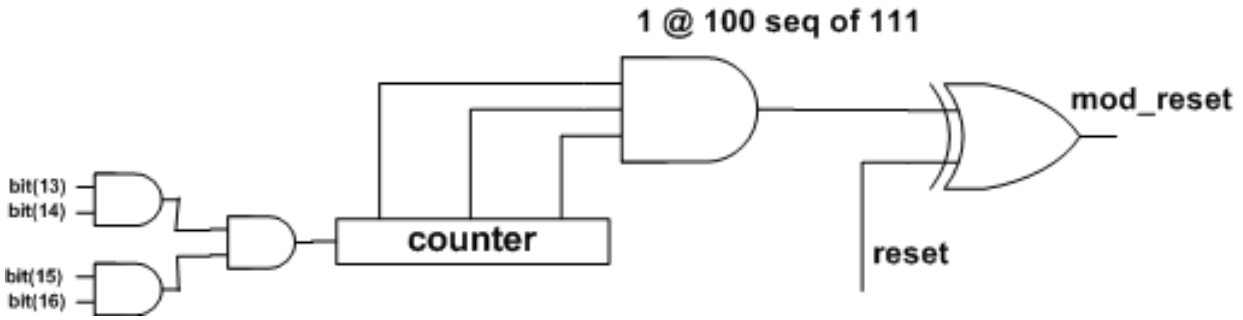




…Hardware Trojan design

- Sequential circuits (Time bombs)





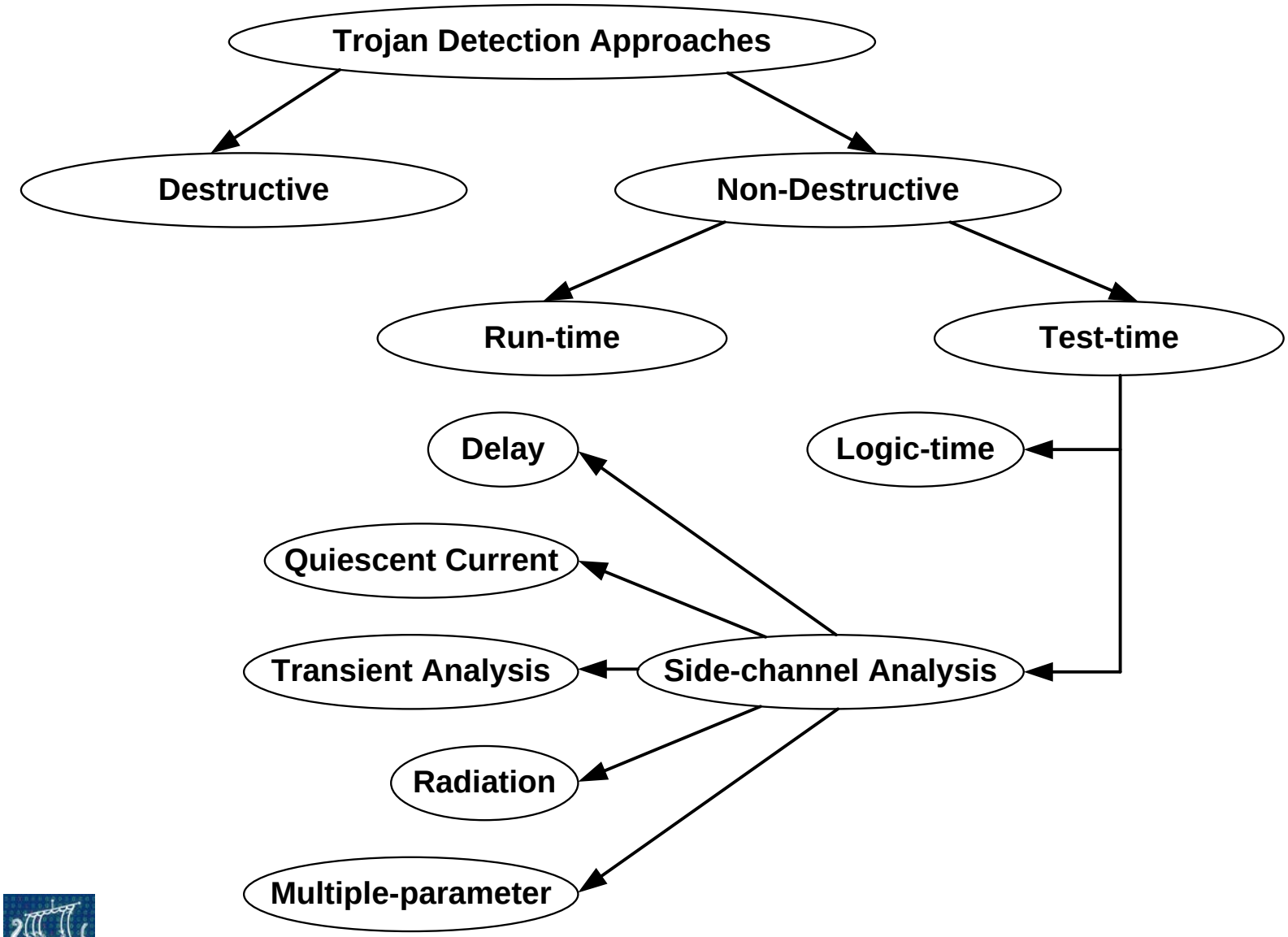
Agenda

- Introduction
- Hardware Trojans horses
- Detection techniques
- An example of a detection technique
- Conclusion

Golden CHIP

- Is an chip that is produced in a trusted fabrication plant
  - We are sure that is free of hardware Trojans
- This circuit can be used as a reference model for detecting behavior and performance deviations of circuit under test
- However, the existence of a golden chip is a topic of debate

…HTH detection techniques…



HTH 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
- A golden model is not required and 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 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
  - Large amount of test vectors are needed

Side channel analysis

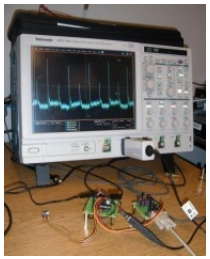
- Any Trojan in the chip is reflected into one or more side-channel parameters
  - Quiescent supply current; leakage current; dynamic power; electromagnetic radiation (EM) due to switching activity; etc
- Specialized and expensive testing equipment is necessary to detect the weak side-channel signals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

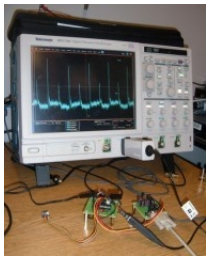
Side channel comparison

golden chip

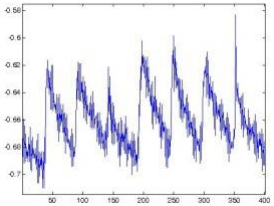
suspected chip

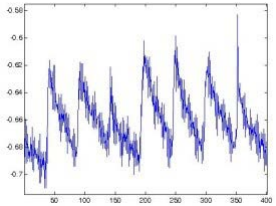
measured side-channel





compare





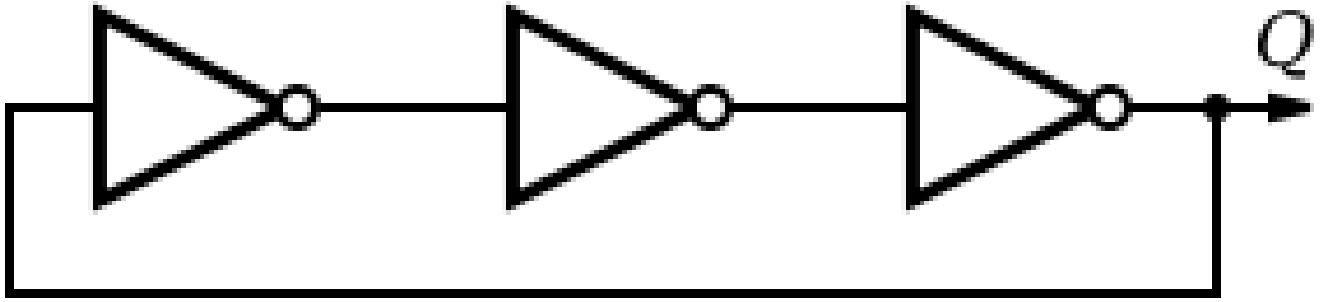
Agenda

- Introduction
- Hardware Trojans horses
- Detection techniques
- An example of a detection technique
- Case study: a Trojan on AES block cipher
- Conclusion

Ring Oscillator…

- 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
- The NOT gates are used in a close chain (ring)
- The output of the last NOT is fedback into the first NOT

…Ring Oscillator

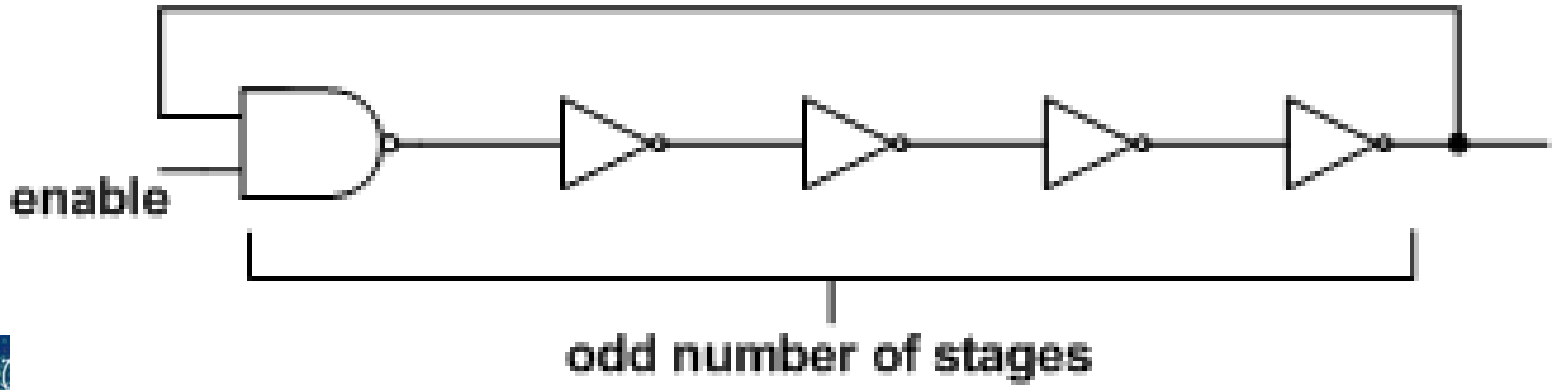


- The operating frequency is equal to $f = \frac{1}{2 * t * n}$
- t is the delay of NOT gate
- n is the number of NOT gate
- The frequency of oscillations decrease as the number of NOT gates in the oscillator increase

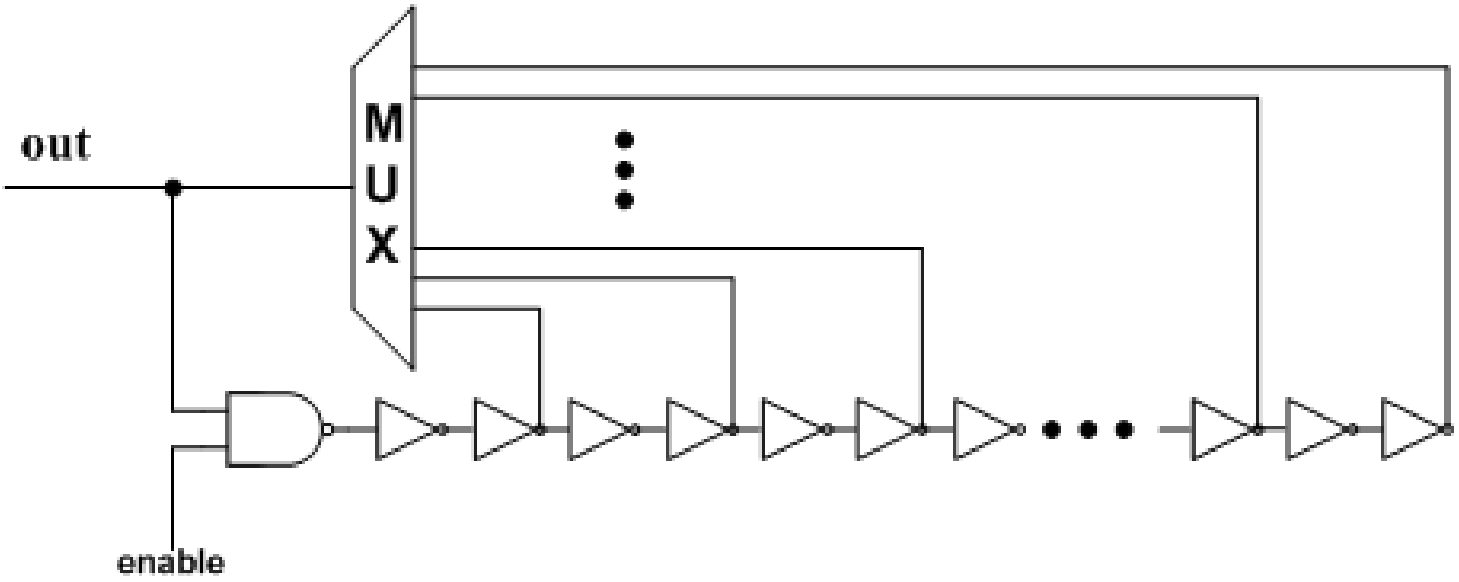
Gated Ring Oscillator

- Replacement one of the inverter with a NAND gate
- If the signal "Enable" is logic high the ring oscillator, oscillates
- If "Enable" is logic low the feedback is broken and the oscillation stops

A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0



Reconfigurable Ring Oscillator…



- A ring oscillator with a configurable-at-the-runtime length
- It comprises an even number of NOT gates and a NAND gate for enabling (activating)

…Reconfigurable Ring Oscillator

- The inputs of the multiplexer (MUX) control the number of the NOT gates taken into account for the operation of the RO
- The MUX output is fedback to the RO and is also used as the final output of the RO
- The oscillation frequency changes based on the input provided to the MUX

Detection with Ring Oscillators

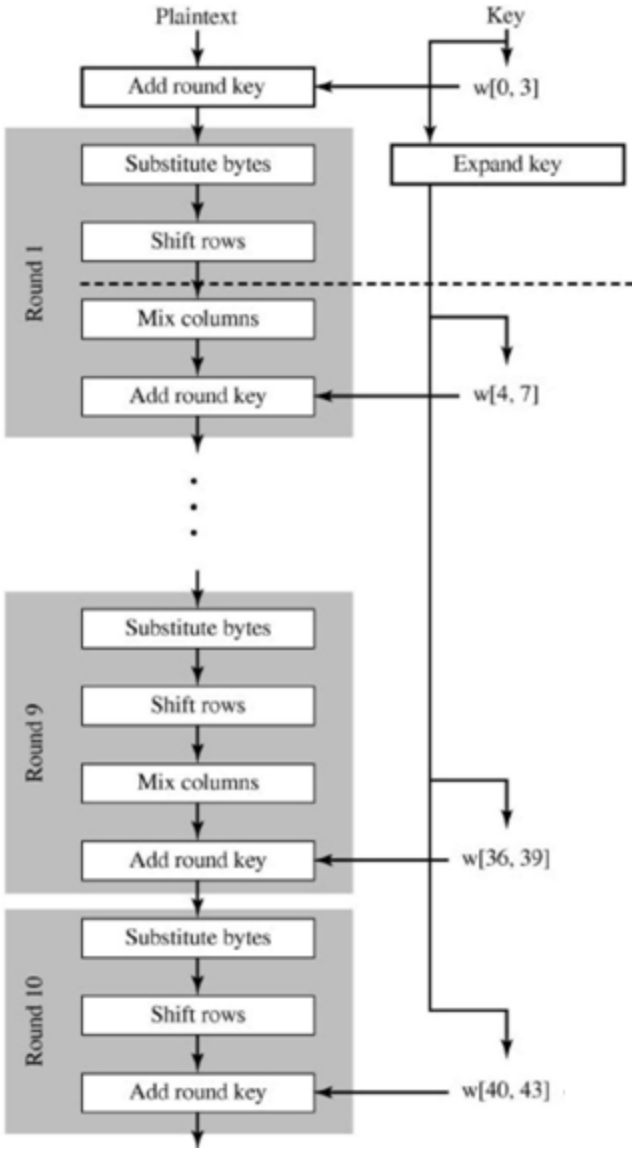
- The Ring Oscillator (RO) oscillates due to its inherent logic
- The oscillation frequency depends on the exact components and size of a circuit
  - The circuit around the RO
- Modifications of the components, such as insertion of additional gates or different placement can change this frequency
- Is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

Agenda

- Introduction
- Hardware Trojans horses
- Detection techniques
- An example of a detection technique
- Case study: a Trojan on AES block cipher
- Conclusion

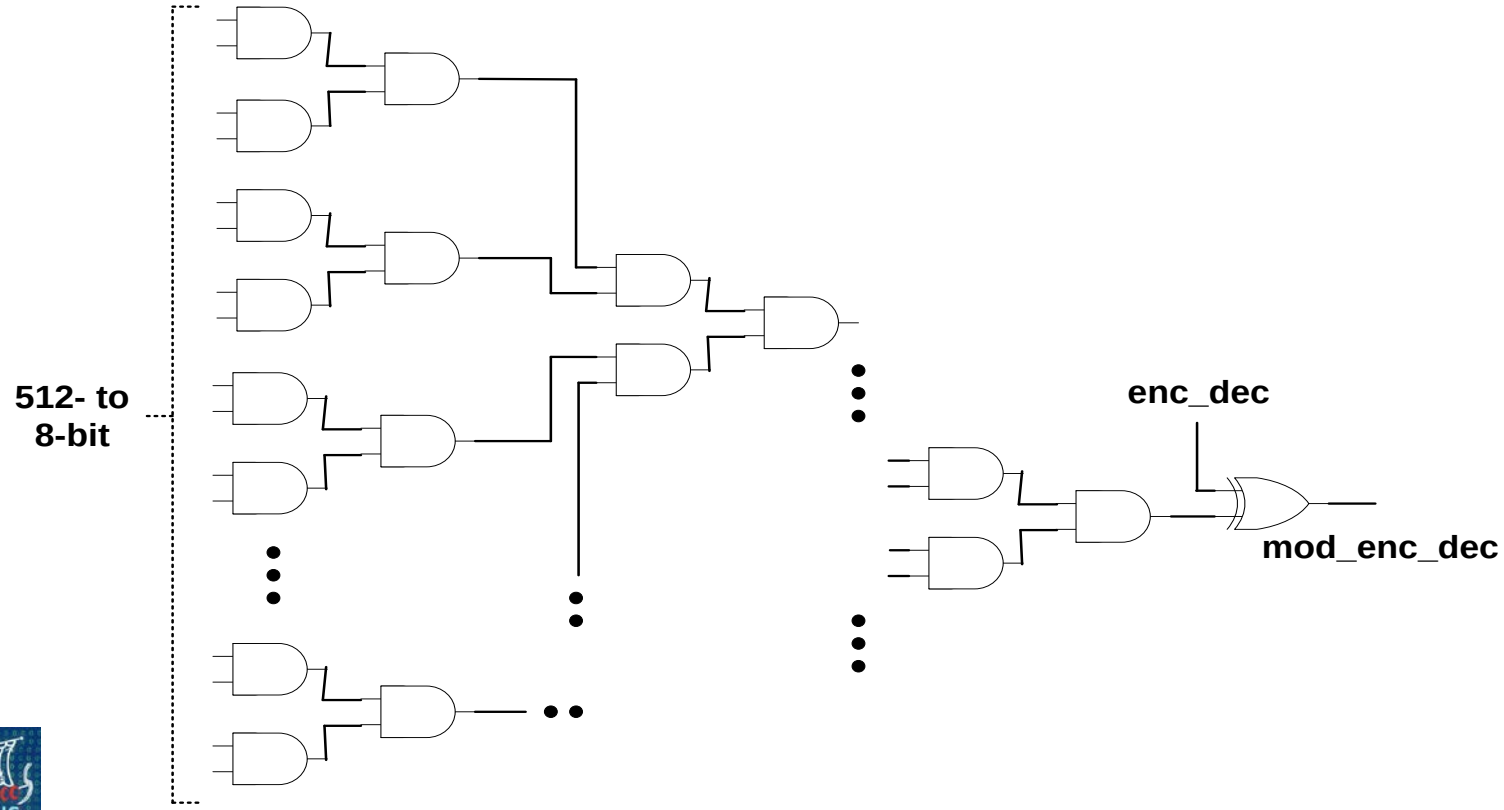
AES Block Cipher

- AES is a block cipher with a block length of 128 bits
- AES allows for three different key lengths: 128 bits (10 rounds), 192 bits (12 rounds)) or 256 bits (14 rounds)
- Each round consists of four transformations (Sub bytes, Shift rows, Mix columns and Add round key)
- Mix columns is missing in the last round



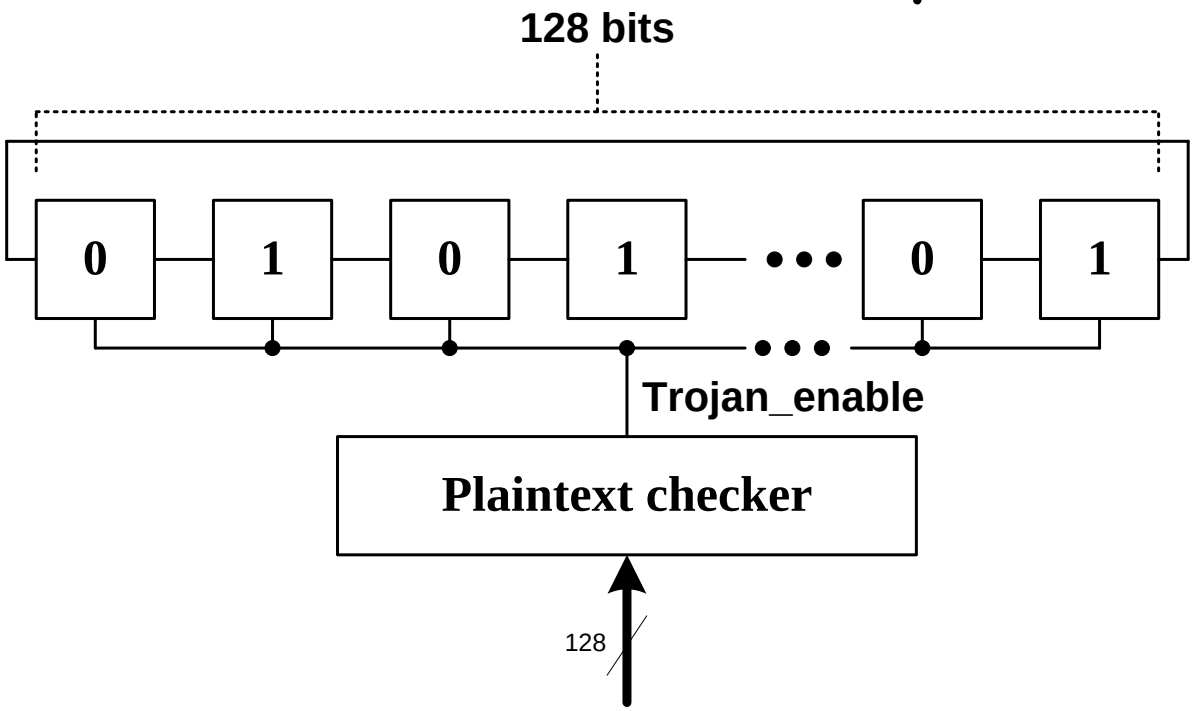
Hardware Trojans…

- Combinatorial Trojan
- Trigger: an AND gate with 512 to 8 inputs
- Payload: A XOR gate



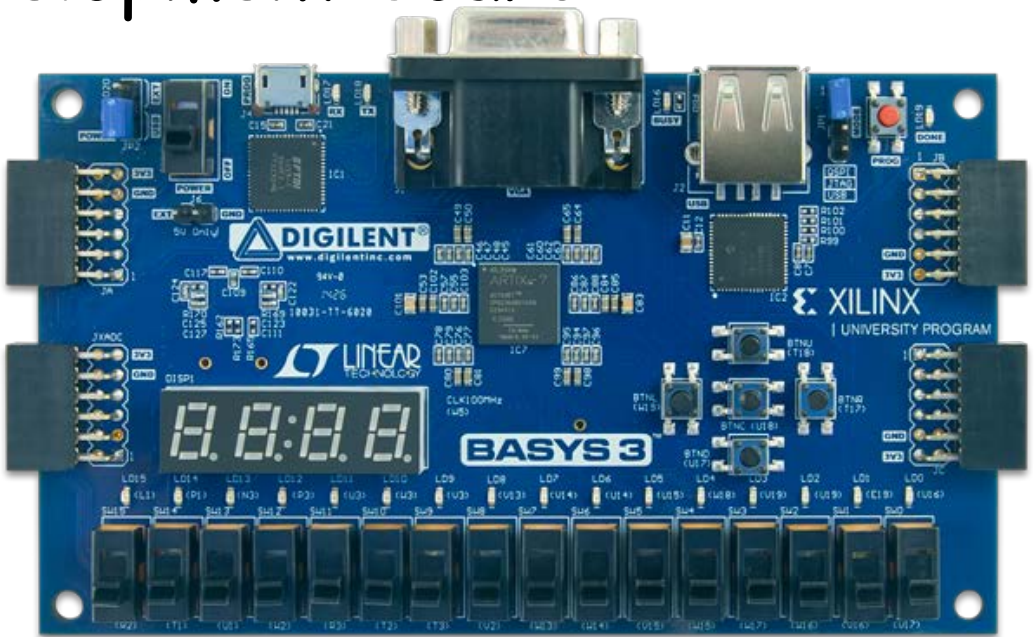
…Hardware Trojans

- Sequential Trojan
- Trigger: an plaintext checker
- Payload: A preloaded shift register (with zeroes and ones alternately)



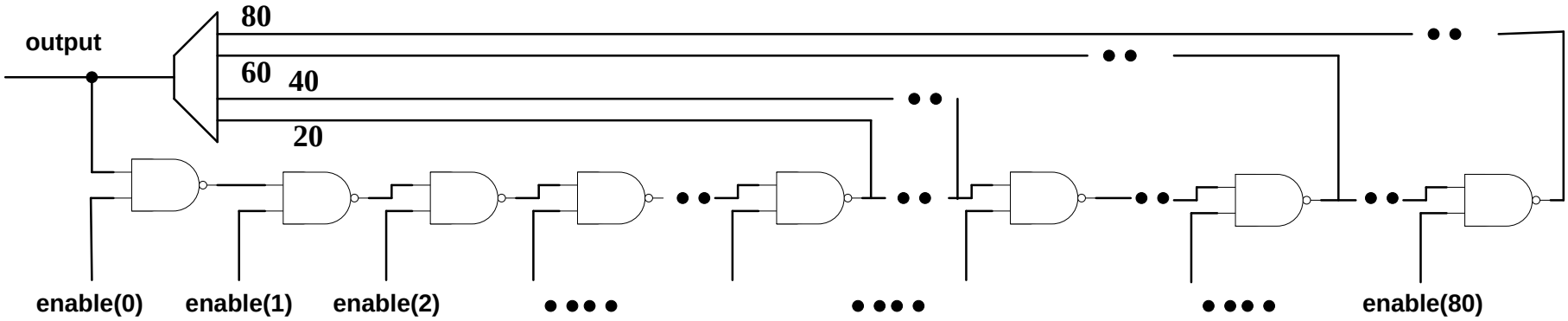
Experimental Setup…

- Setup consists of the design of AES block cipher* and the circuits of the hardware Trojans horse (combinatorial/sequential)
- We have used HDL code on a Digilent Basys 3 FPGA development board



* https://opencores.org/project,aes_core

…Experimental Setup…

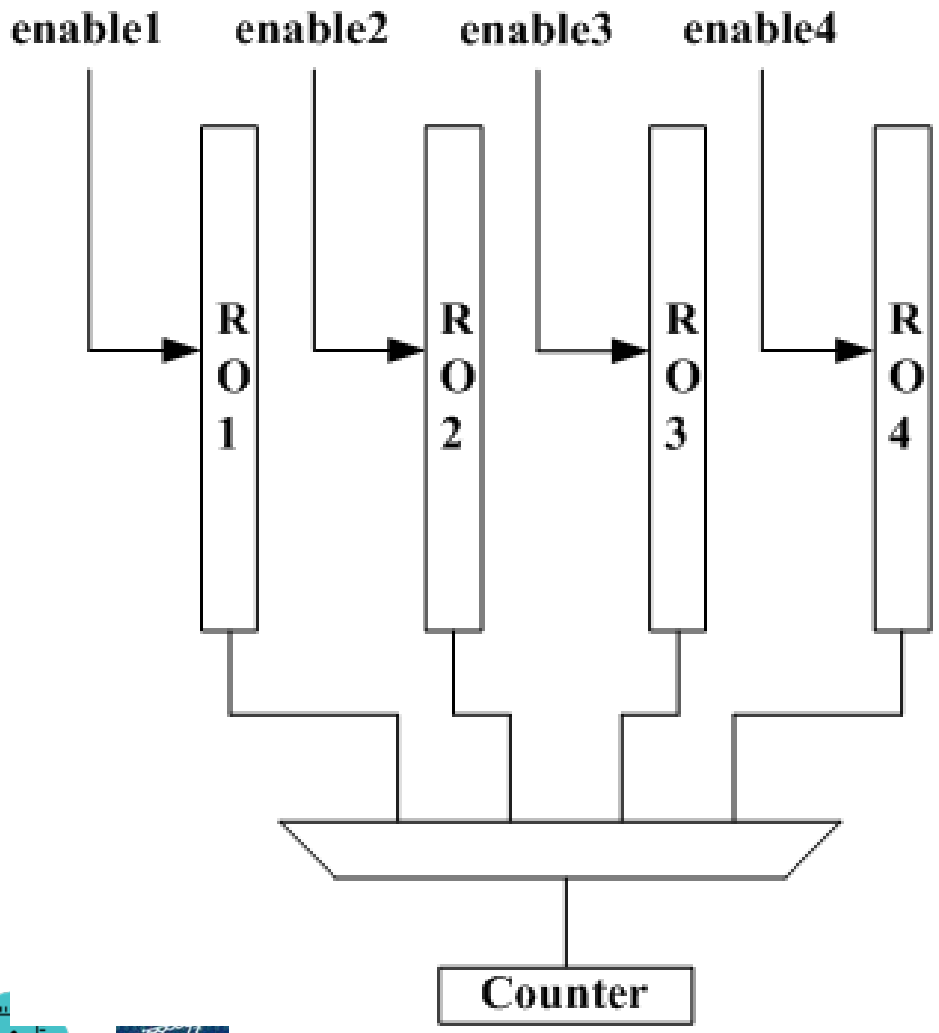


- It comprises of a series of NAND gates
  - The first one is for RO activation
- Each NAND is fed with the output of the previous one and one enable signal
- The basic design extends to a length of 80
- We can control the total length of the ring oscillator using the signal enable [0:80]

…Experimental Setup…

- For realizing a ring oscillator with length 60 out of it a signal of 60 ones followed by 20 zeroes is provided
- The same pattern is used for realizing any other length

…Experimental Setup…



- The activation of the ROs is controlled by the pushbuttons of the Basys3, using a multiplexer
- At each time, only one RO is active and its output is fed to the counter for logging

Continue…

…With a interesting exercise!!!