# A Side-Channel Hardware Trojan in 65nm CMOS with 2µW precision and Multi-bit Leakage Capability

Tiago D. Perez and Samuel Pagliarini
Dpt. of Computer Systems - School of IT
Tallinn University of Technology

# A Side-Channel Hardware Trojan in 65nm CMOS with 2µW precision and Multi-bit Leakage Capability

## Contents

- **Overview**
- **Side-Channel Trojan Design**
- **Trojan Insertion**
- **ASIC Prototype**
- **Conclusion**

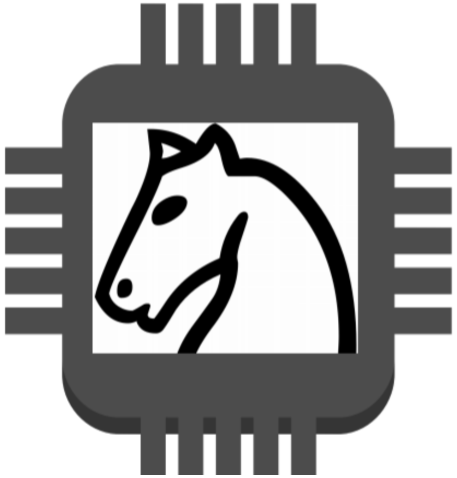
# Overview

❑**Goal**: demonstrate the capability of a rogue element inside an untrusted foundry

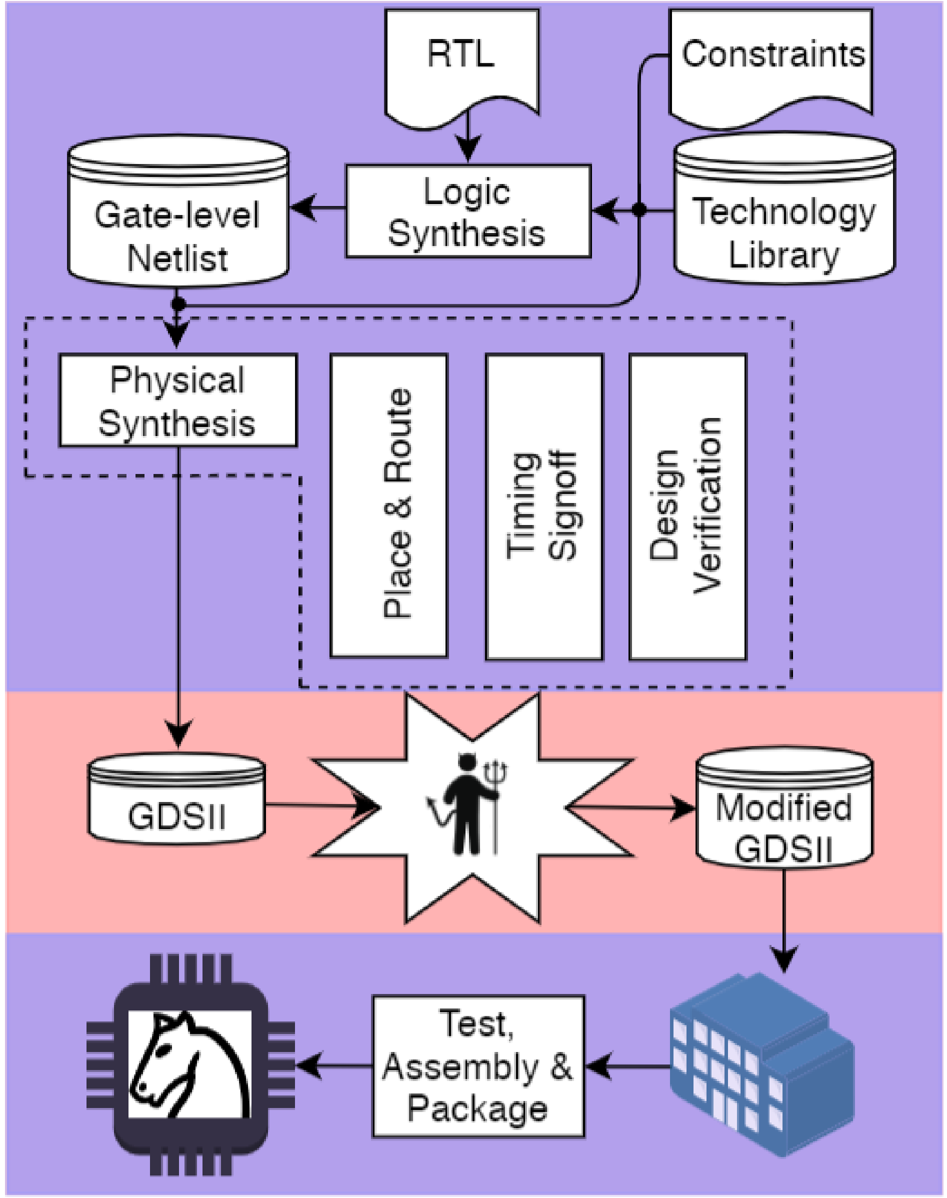
❑**Motivation**: feasibility of trojan insertion during fabrication-time

❑**Problem**: designing and insert such Hardware Trojan

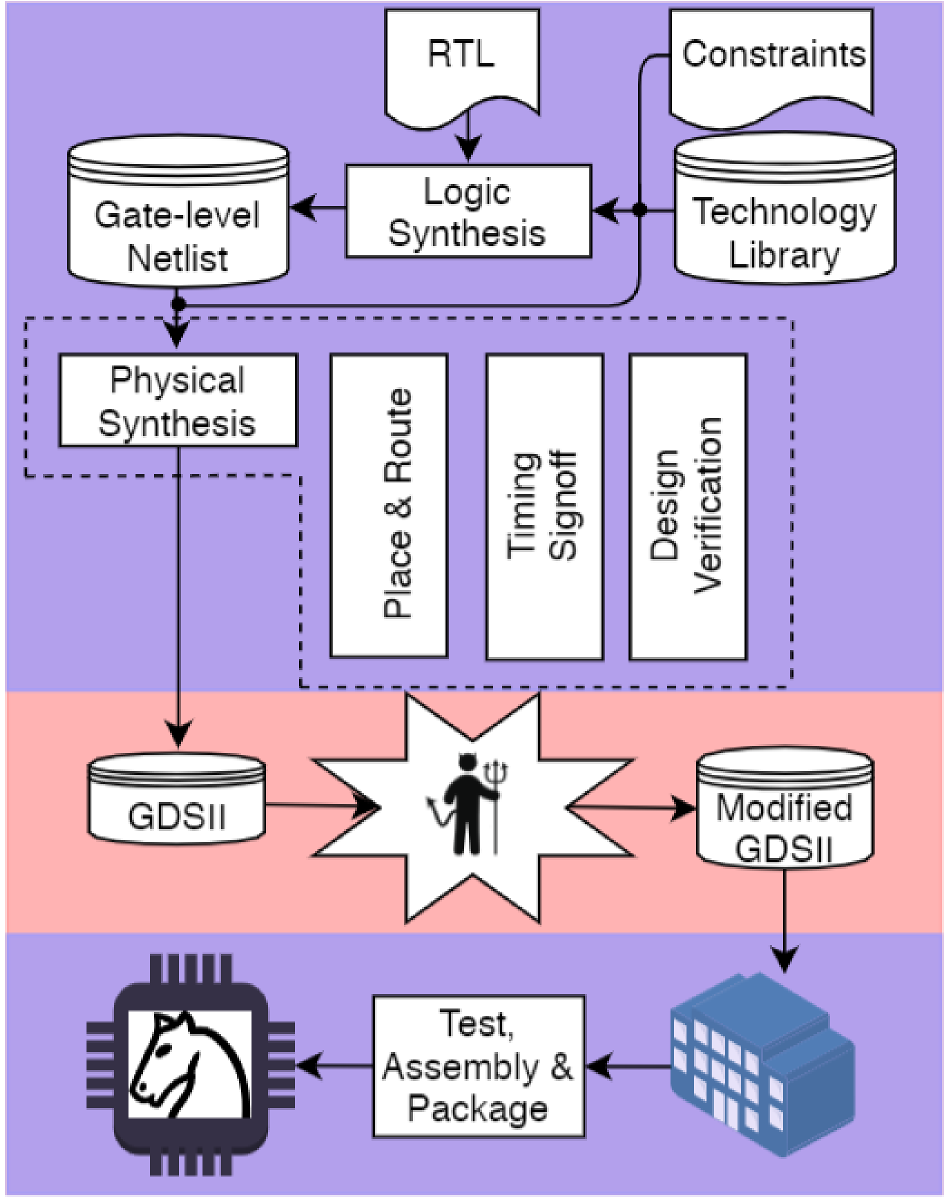
❑**Novelty**: using an Engineering Changing Order (ECO) for inserting the Hardware Trojan



# IC Design Process

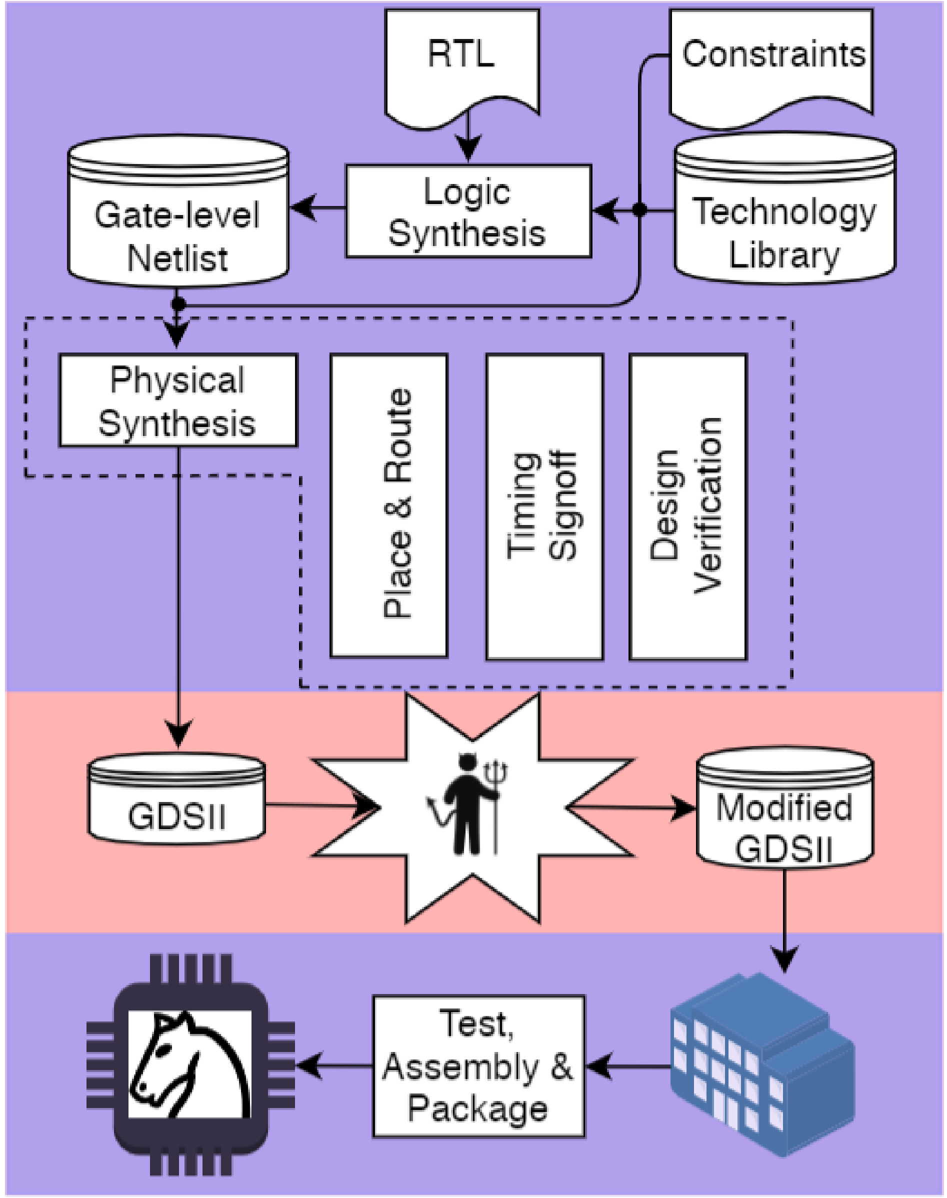


# IC Design Process



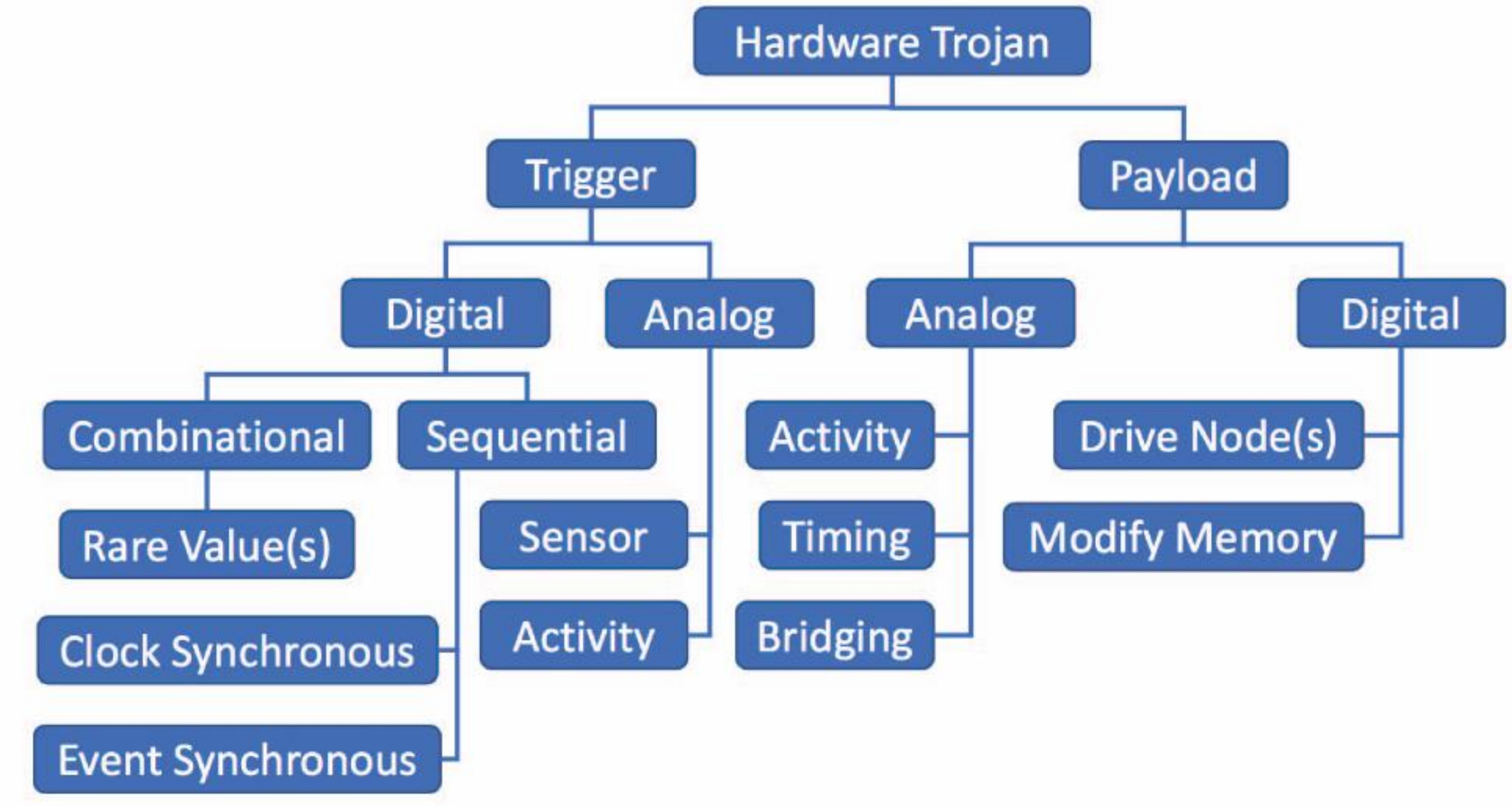
Manufacturing is outsourced

# IC Design Process



Fabrication-time attack!!

# Hardware Trojans



Source: ICAS: an Extensible Framework for Estimating the Susceptibility of IC Layouts to Additive Trojans Timothy, 2020, IEEE Symposium on Security and Privacy (SP).

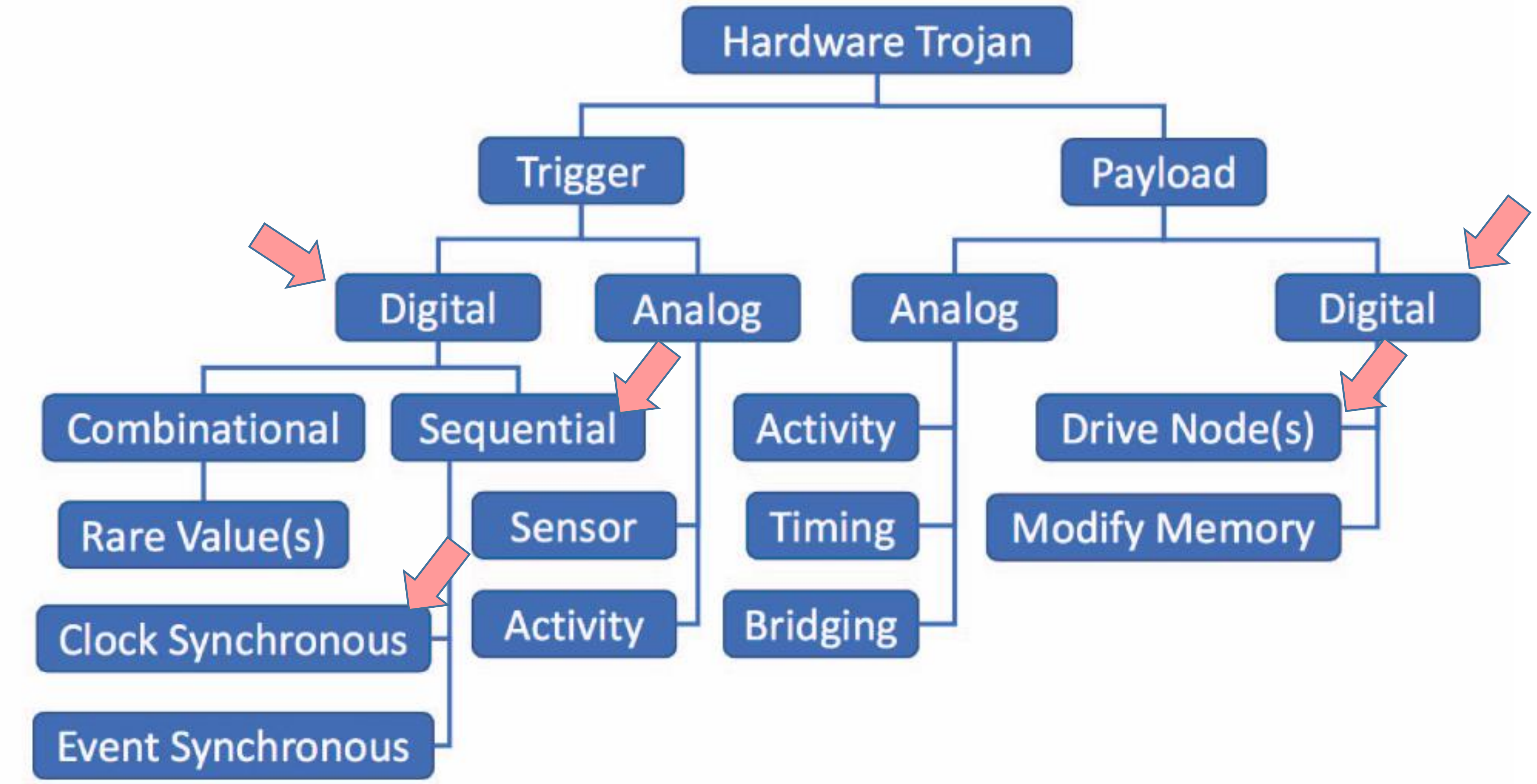
## Side-Channel Hardware Trojan

❑ Target: crypto cores

❑ Trigger: crypto core going idle. Specifically, when the “Done” signal is asserted

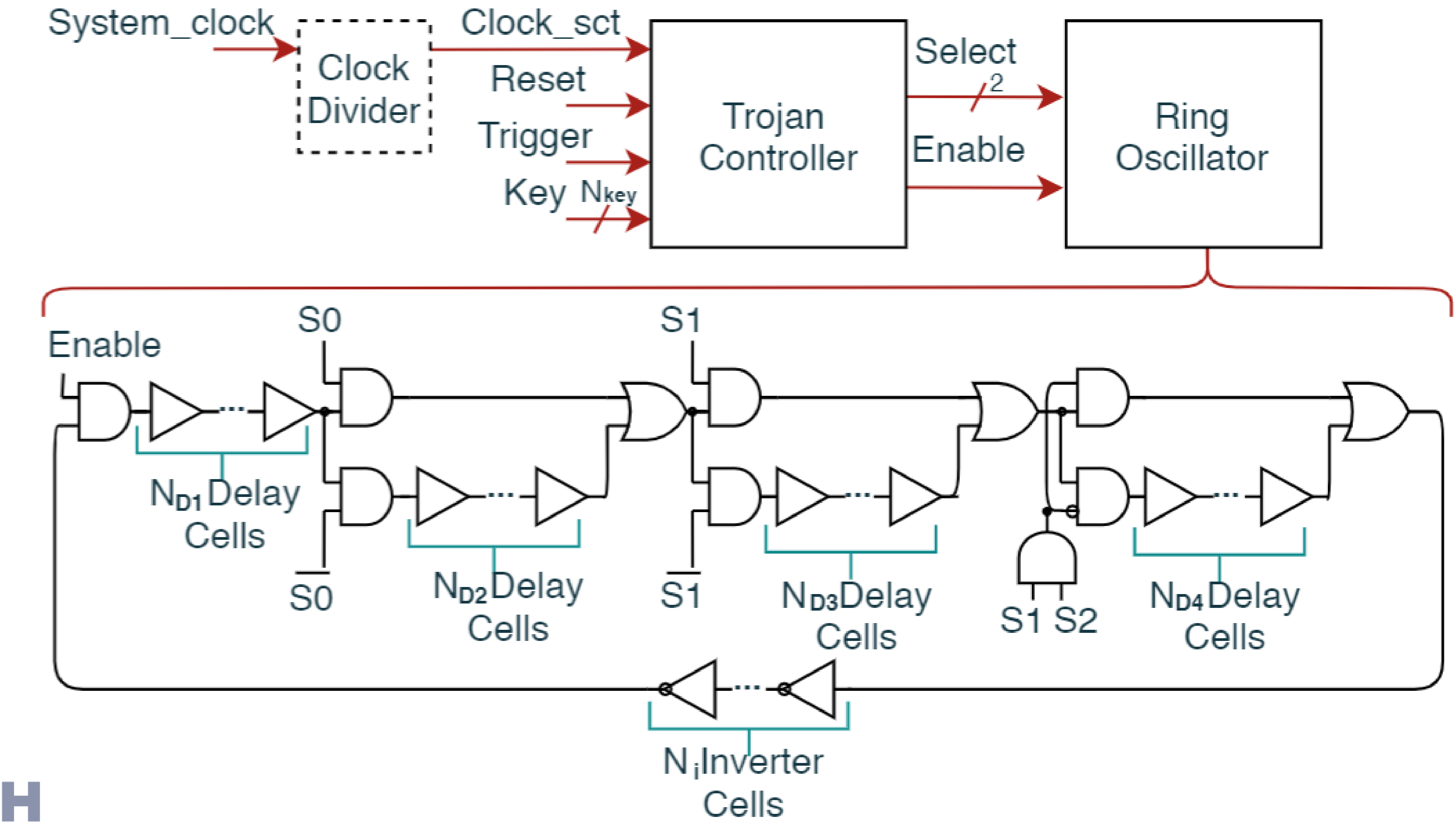
❑ Payload: induce extra power consumption in a controlled manner

# Hardware Trojans

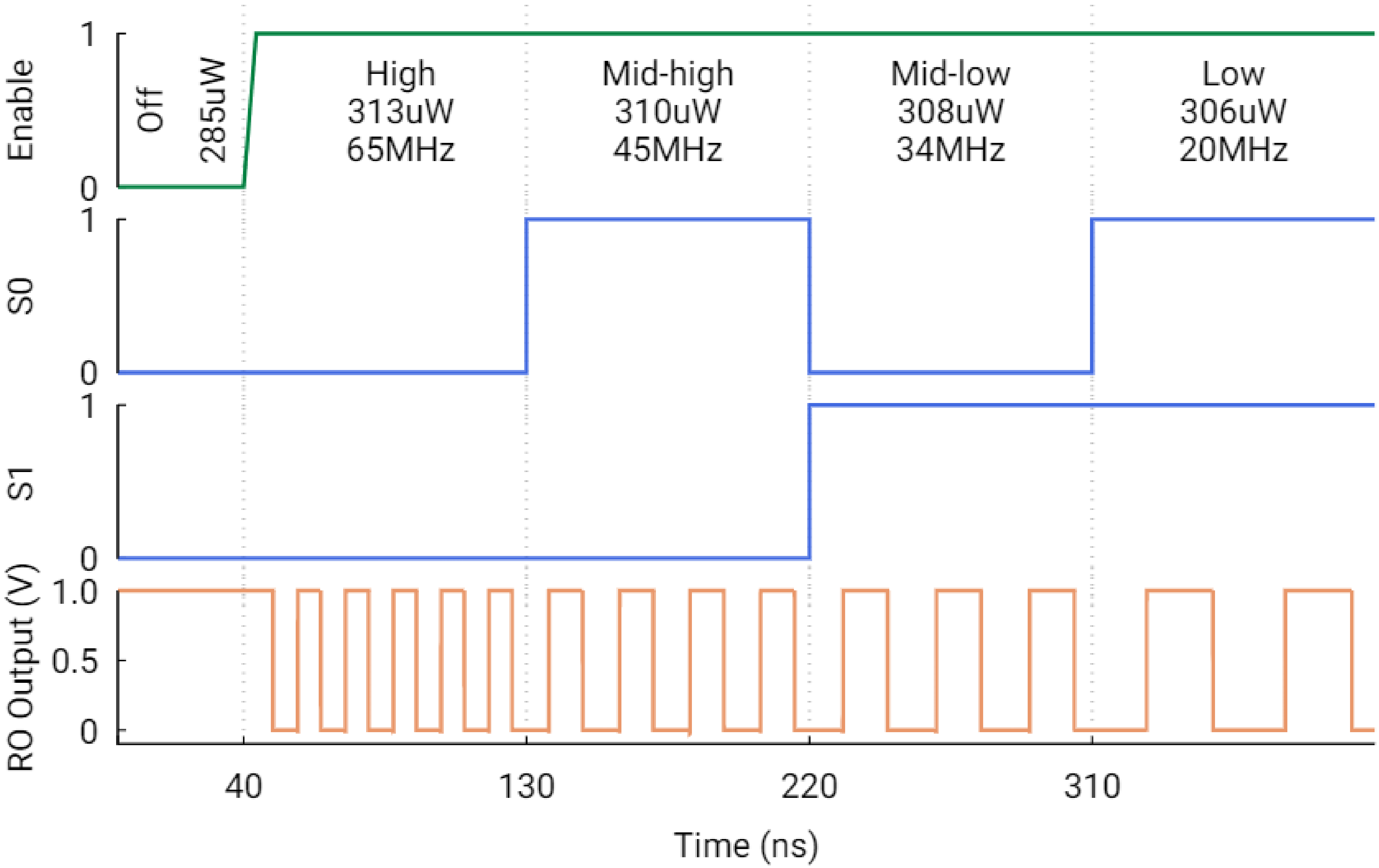


Source: ICAS: an Extensible Framework for Estimating the Susceptibility of IC Layouts to Additive Trojans
Timothy, 2020, IEEE Symposium on Security and Privacy (SP).

## Side-Channel Hardware Trojan – Architecture



# Side-Channel Hardware Trojan – Functionality Example



# How to insert a Hardware Trojan into a finalized layout?

## Hardware Trojan Insertion Options

- ❑A hardware trojan can be inserted manually

## Hardware Trojan Insertion Options

- ❑A hardware trojan can be inserted manually
  - ❑Time intensive task and prone to errors

## Hardware Trojan Insertion Options

- ❑A hardware trojan can be inserted manually
    - ❑Time intensive task and prone to errors

- ❑Re-implementing the entire design

# Hardware Trojan Insertion Options

- A hardware trojan can be inserted manually
  - Time intensive task and prone to errors

- Re-implementing the entire design
  - Requires time and power constraints
  - Very likely to hinder victim`s design performance

## Hardware Trojan Insertion Options

- □A hardware trojan can be inserted manually
  - □Time intensive task and prone to errors

- □Re-implementing the entire design
  - □Requires time and power constraints
  - □Very likely to hinder victim`s design performance

- □Utilizing the Engineering Change Order flow (ECO)

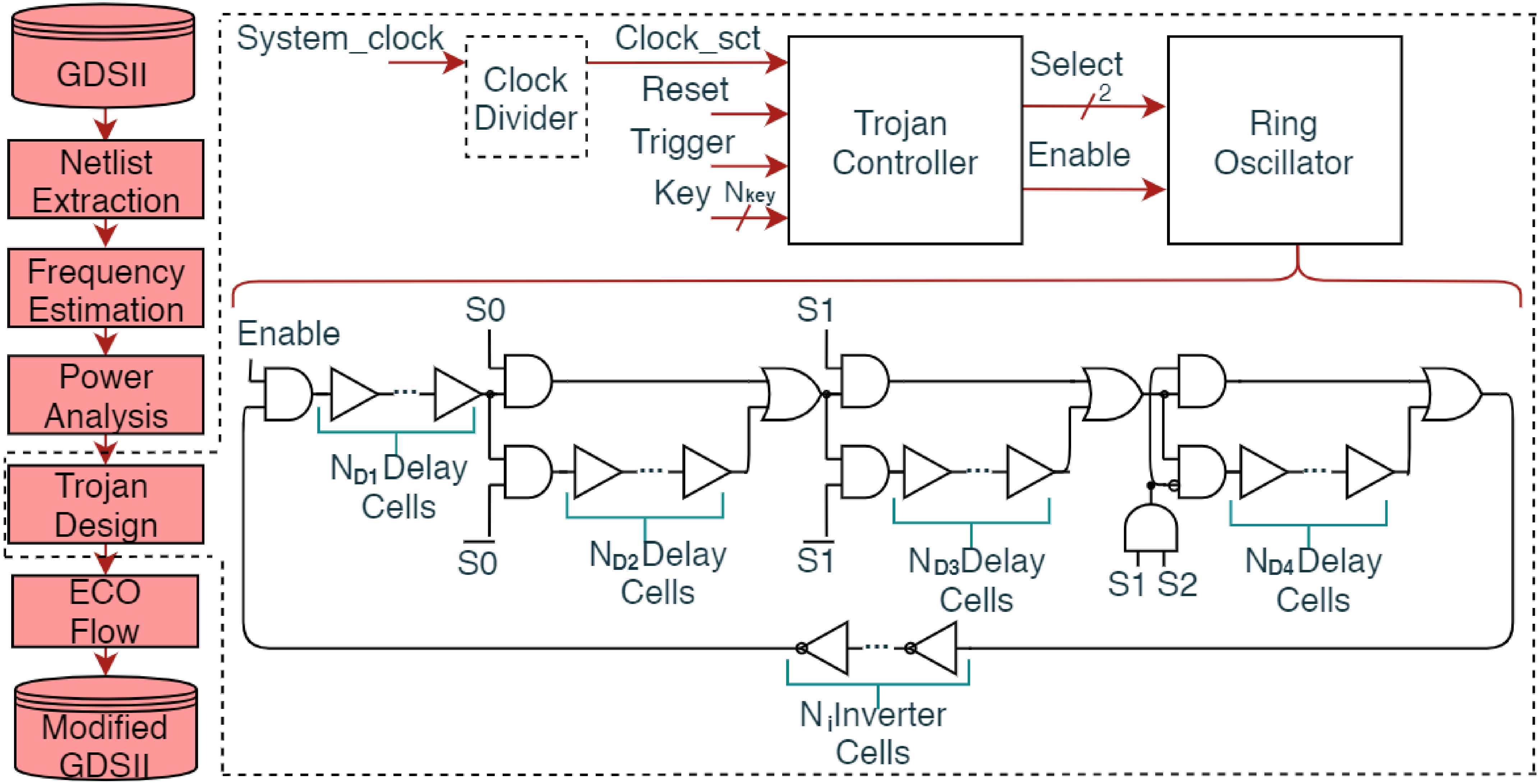
## Hardware Trojan Insertion Options

- A hardware trojan can be inserted manually
  - Time intensive task and prone to errors

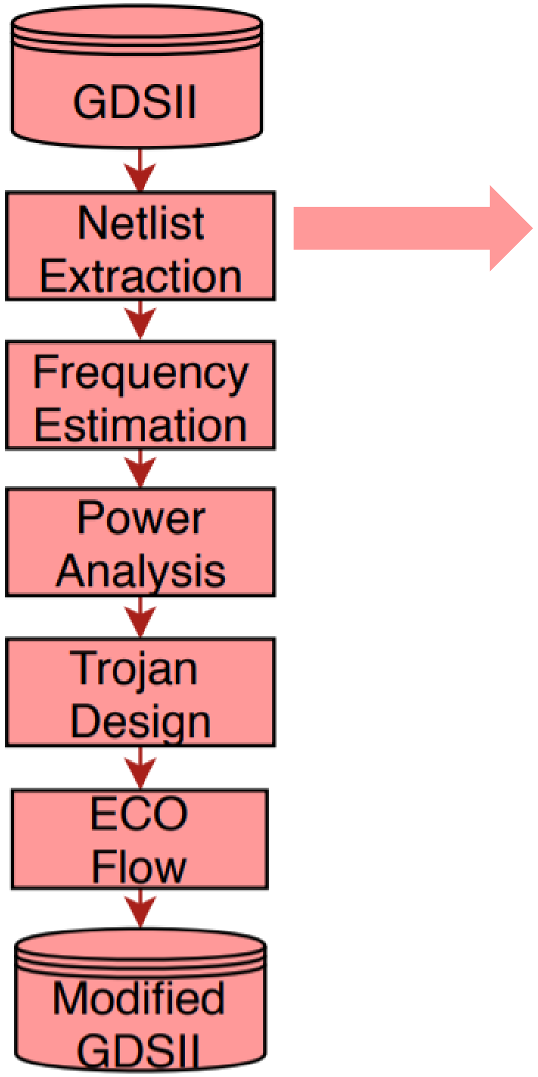
- Re-implementing the entire design
  - Requires time and power constraints
  - Very likely to hinder victim`s design performance

- Utilizing the Engineering Change Order flow (ECO)
  - Does not change the original circuit
  - Can be done with estimated constraints

# Side-Channel Hardware Trojan – Insertion

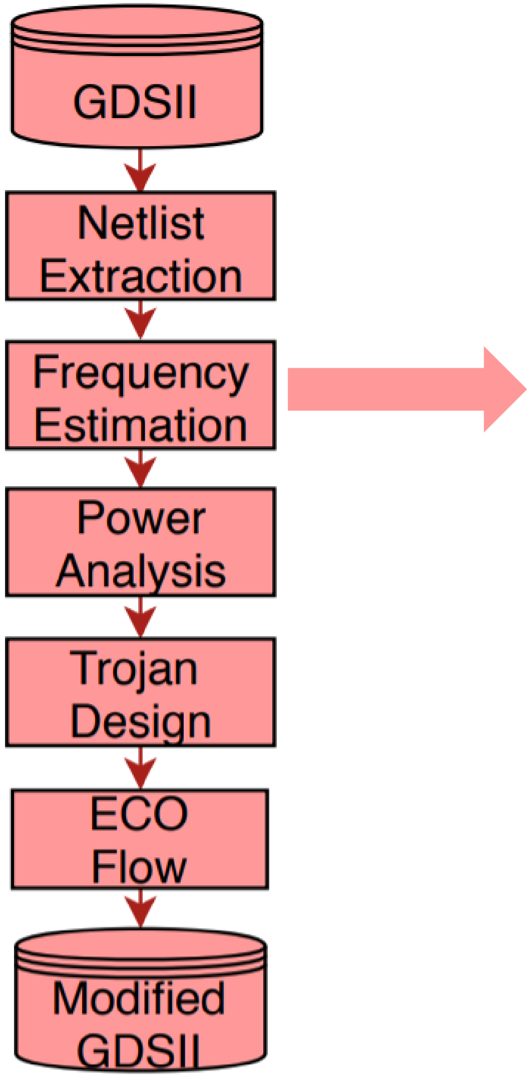


# Side-Channel Hardware Trojan – Insertion



Gate-level netlist can be extracted utilizing a CAD tool, e.g., Cadence Virtuoso

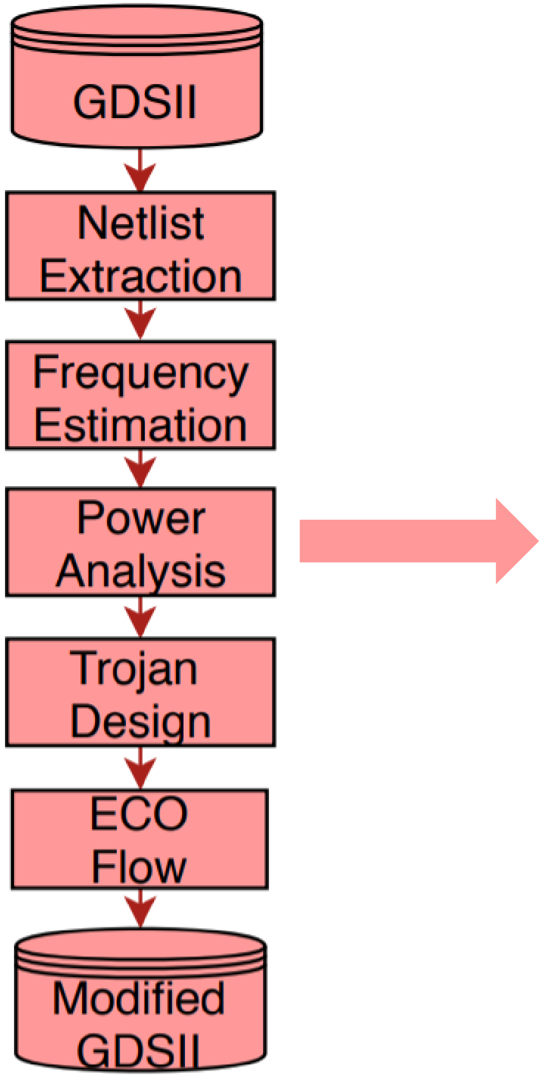
# Side-Channel Hardware Trojan – Insertion



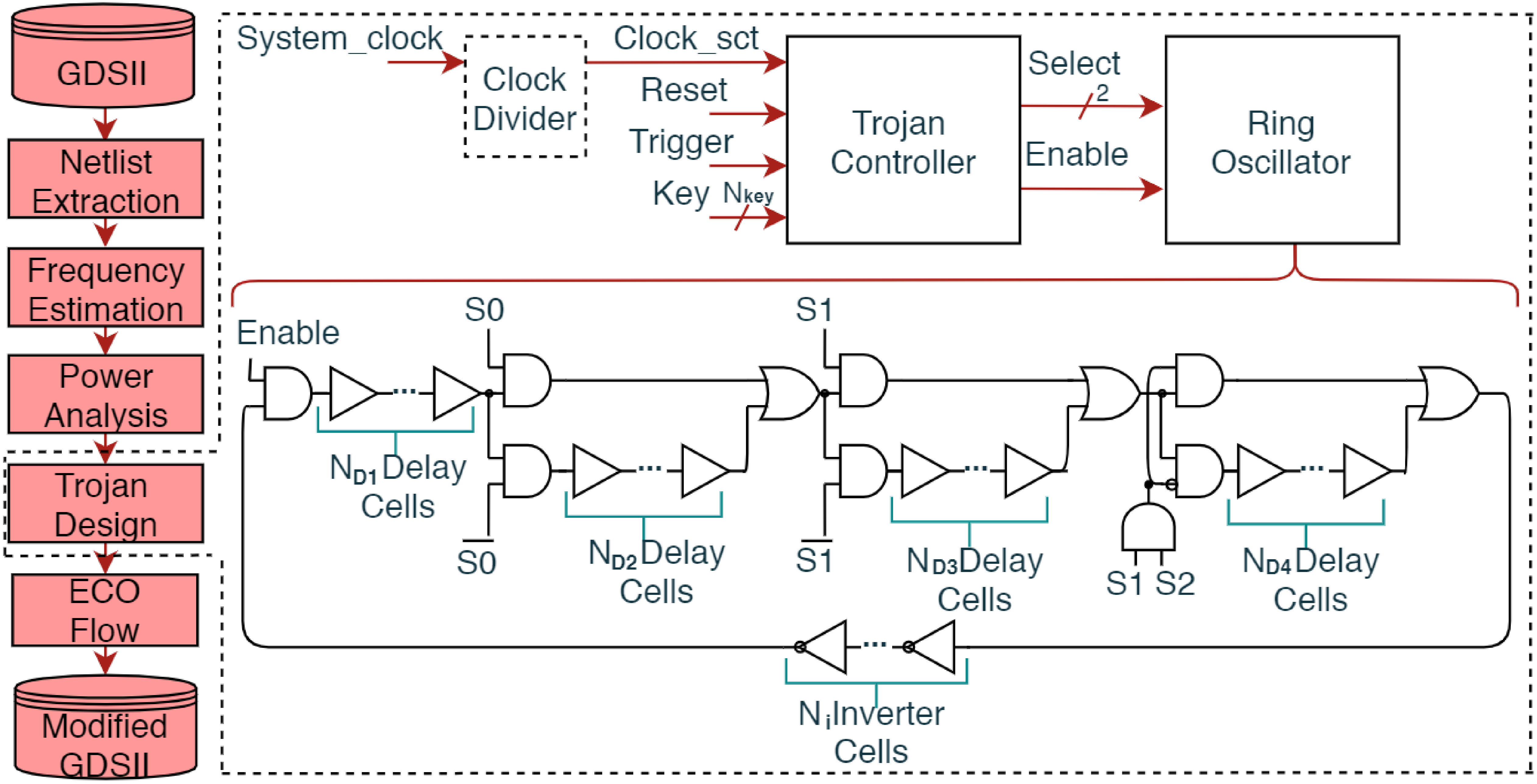
Operating frequency can be estimated by trial-and-error:

- ❑Educated guess a frequency value
- ❑Perform a timing analysis and observe the critical path
- ❑Repeat until the timing slack is near zero

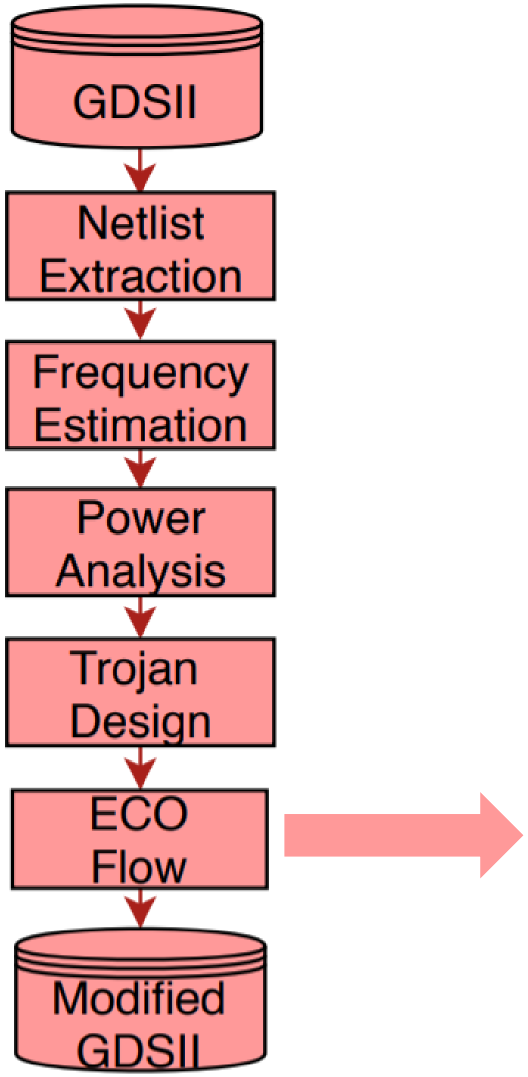
# Side-Channel Hardware Trojan – Insertion



Straightforward power analysis utilizing the extracted gate-level netlist and estimated frequency


GDSII
Netlist Extraction
Frequency Estimation
Power Analysis
Trojan Design
ECO Flow
Modified GDSII
System_clock
Clock Divider
Clock_sct
Reset
Trigger
Key
N_key
Trojan Controller
Select
2
Enable
Ring Oscillator
Enable
S0
N_D1 Delay Cells
S̄0
N_D2 Delay Cells
S1
S̄1
N_D3 Delay Cells
S1 S2
N_D4 Delay Cells
N_i Inverter Cells

# Side-Channel Hardware Trojan – Insertion



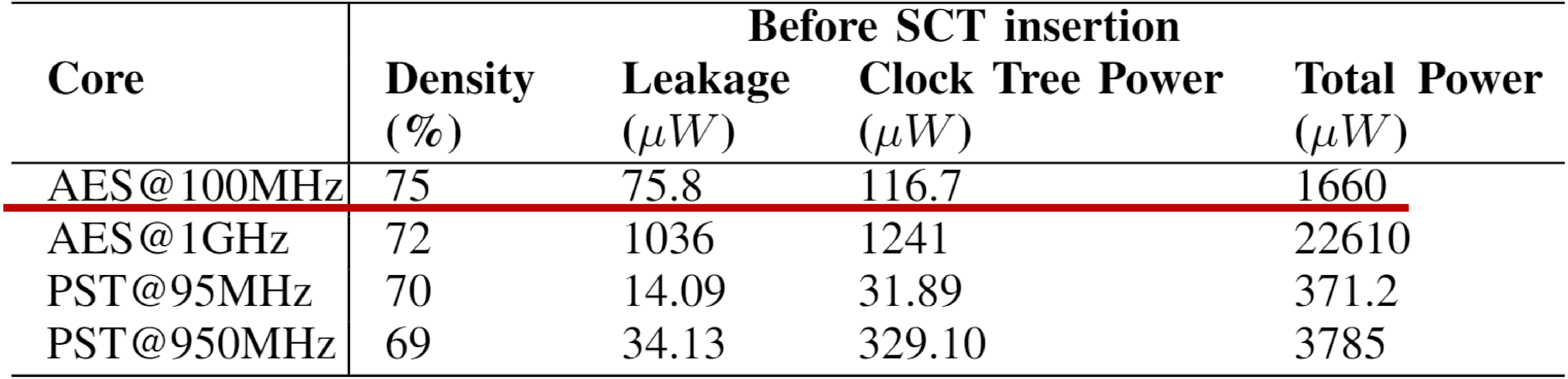
Typical ECO flow utilizing the modified gate-level netlist with the Trojan inserted.

## Experimental Investigation

❑Benchmark circuits: AES and Present cryptocores.

❑Implementation parameters:
  - ❑Higher density possible for minimizing empty spaces
  - ❑Very challenging frequency
  - ❑Low-frequency – 10% of high-frequency target

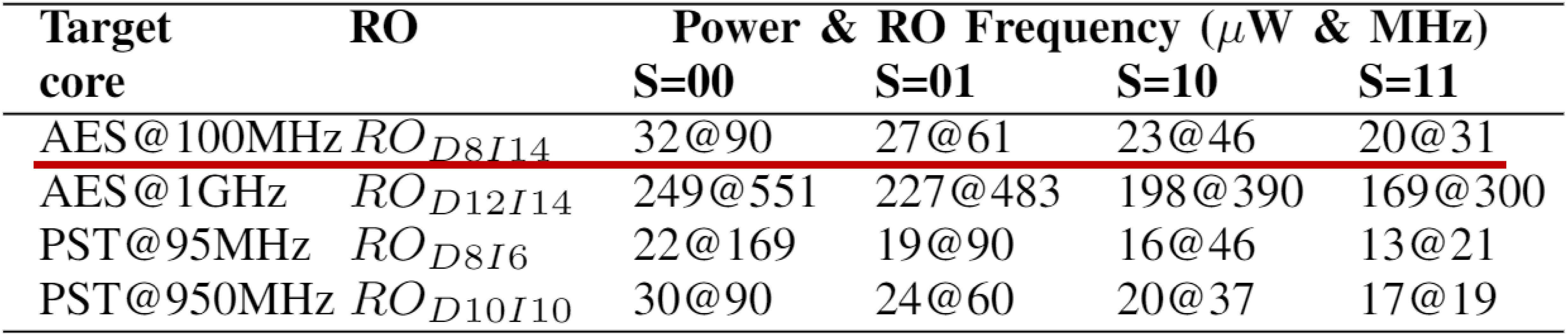
# Experimental Investigation – Cores implementation



| | Before SCT insertion | | | |
|---|---|---|---|---|
| Core | Density (%) | Leakage ($\mu W$) | Clock Tree Power ($\mu W$) | Total Power ($\mu W$) |
| AES@100MHz | 75 | 75.8 | 116.7 | 1660 |
| AES@1GHz | 72 | 1036 | 1241 | 22610 |
| PST@95MHz | 70 | 14.09 | 31.89 | 371.2 |
| PST@950MHz | 69 | 34.13 | 329.10 | 3785 |

Target Power → (Leakage + Clock Tree Power) x Designer Margin

# Experimental Investigation – RO Design



| Target core | RO | Power & RO Frequency ($\mu$W & MHz) | | | |
|---|---|---|---|---|---|
| | | S=00 | S=01 | S=10 | S=11 |
| AES@100MHz | $RO_{D8I14}$ | 32@90 | 27@61 | 23@46 | 20@31 |
| AES@1GHz | $RO_{D12I14}$ | 249@551 | 227@483 | 198@390 | 169@300 |
| PST@95MHz | $RO_{D8I6}$ | 22@169 | 19@90 | 16@46 | 13@21 |
| PST@950MHz | $RO_{D10I10}$ | 30@90 | 24@60 | 20@37 | 17@19 |

ND1 = 2
ND2 = 1
ND3 = 2
ND4 = 1

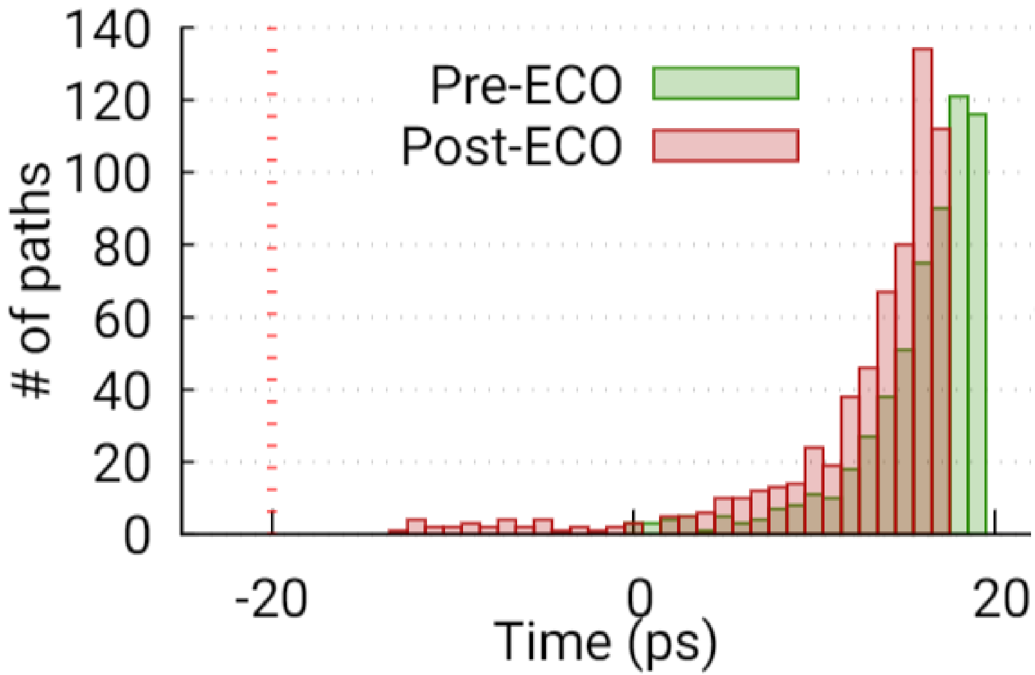
S=00 has 2 active delay cells

S=01 has 3 active delay cells

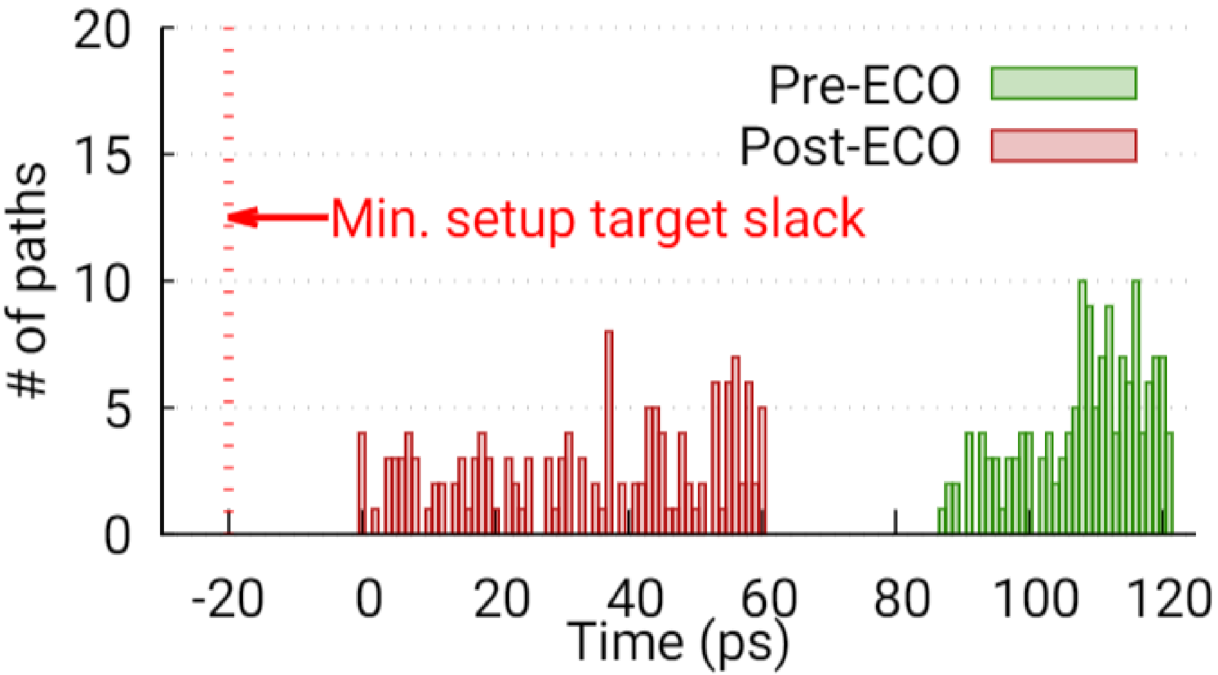
S=10 has 5 active delay cells

S=11 has 6 active delay cells

# Experimental Investigation – Post-ECO Timing Impact



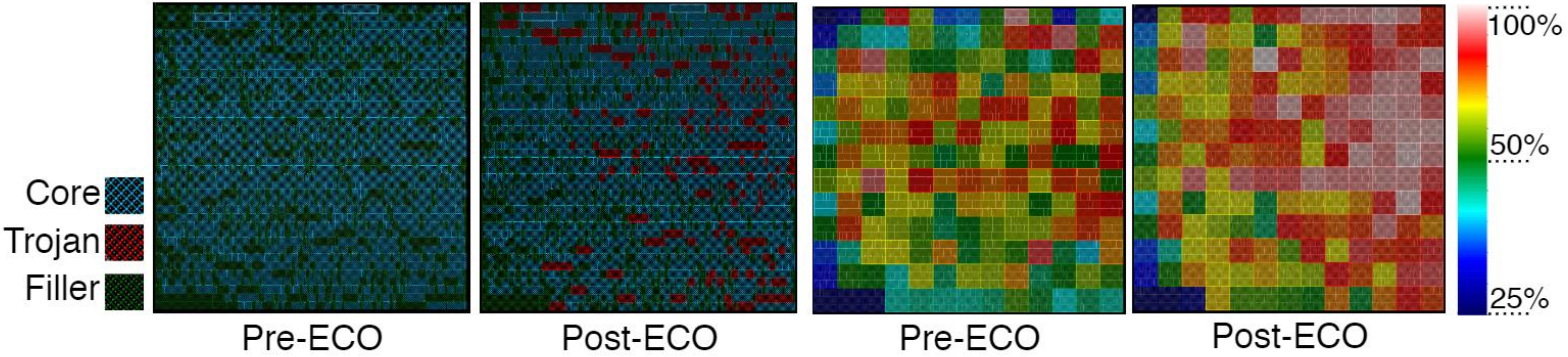
AES@1GHz



PST@950MHz

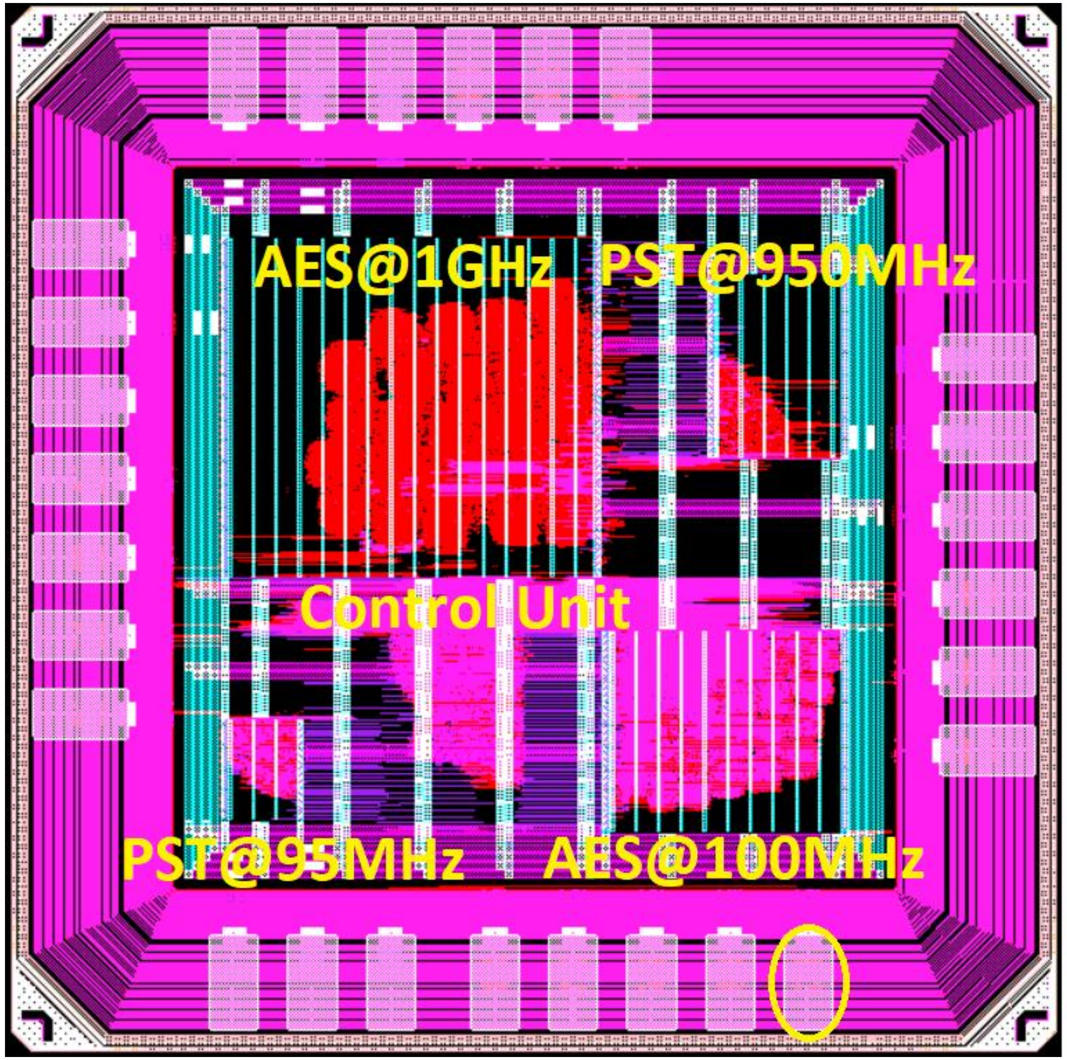
TAL TECH

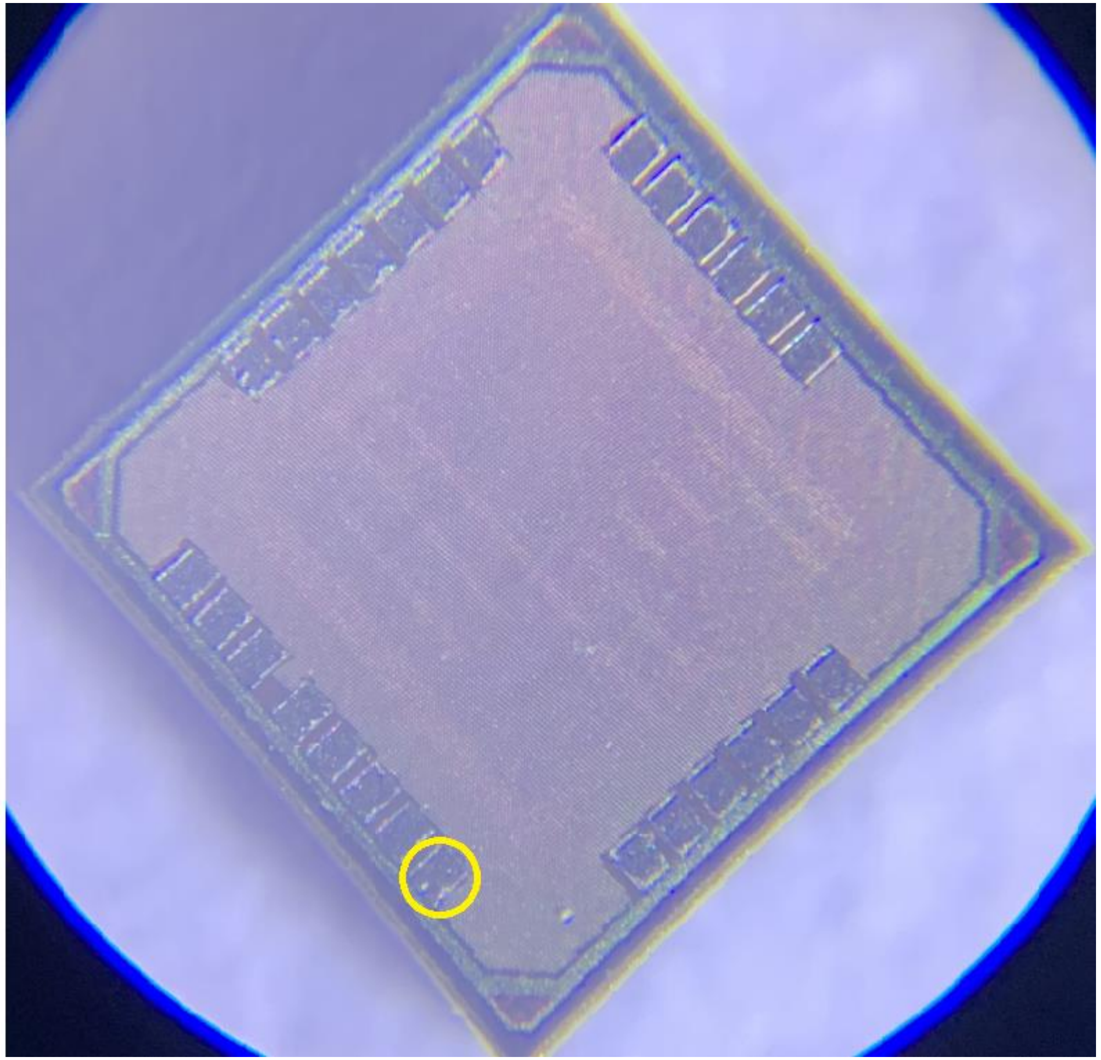
# Side-channel Trojan – Density Comparison



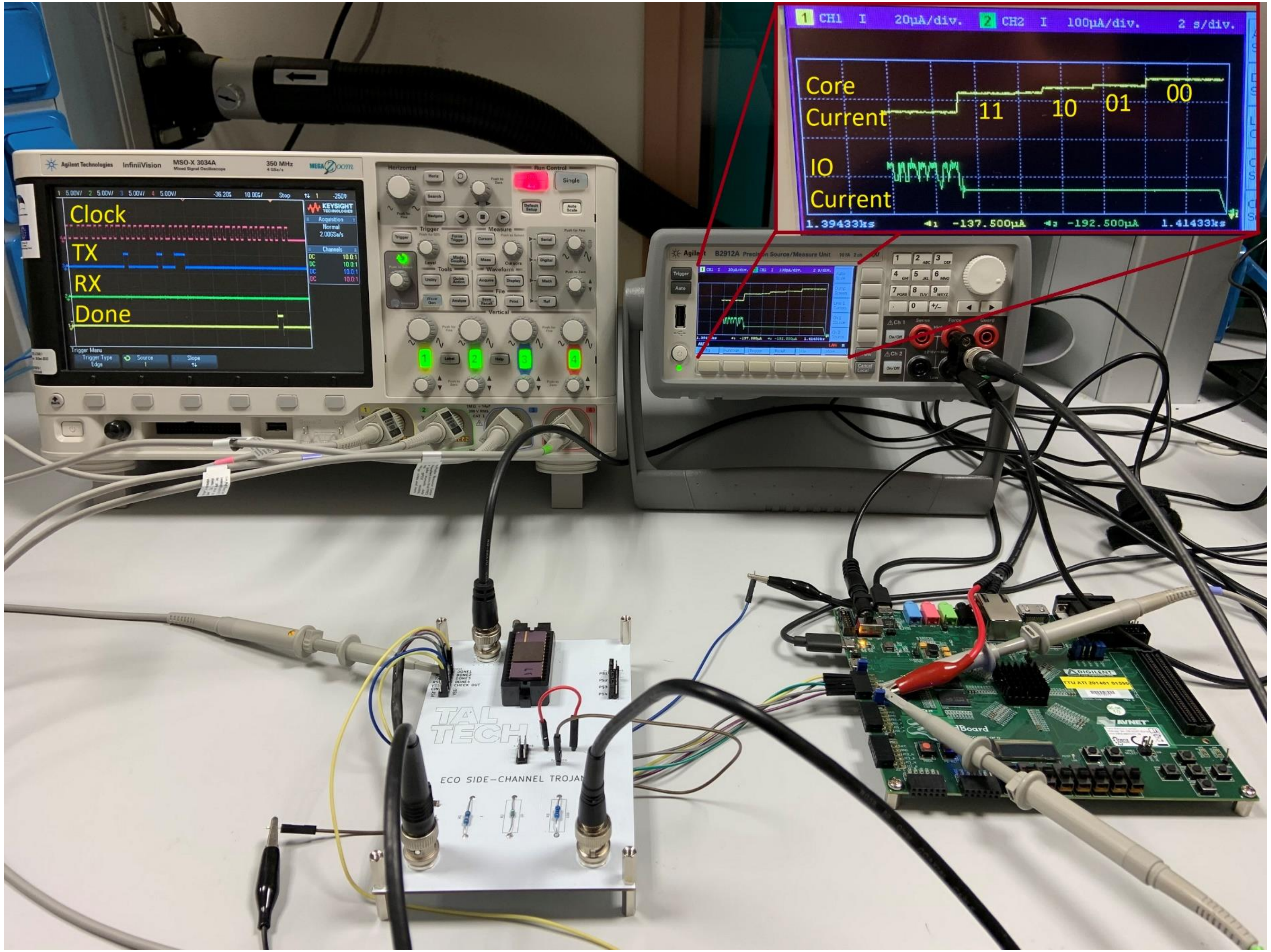
PST@950MHz

# ASIC Prototype



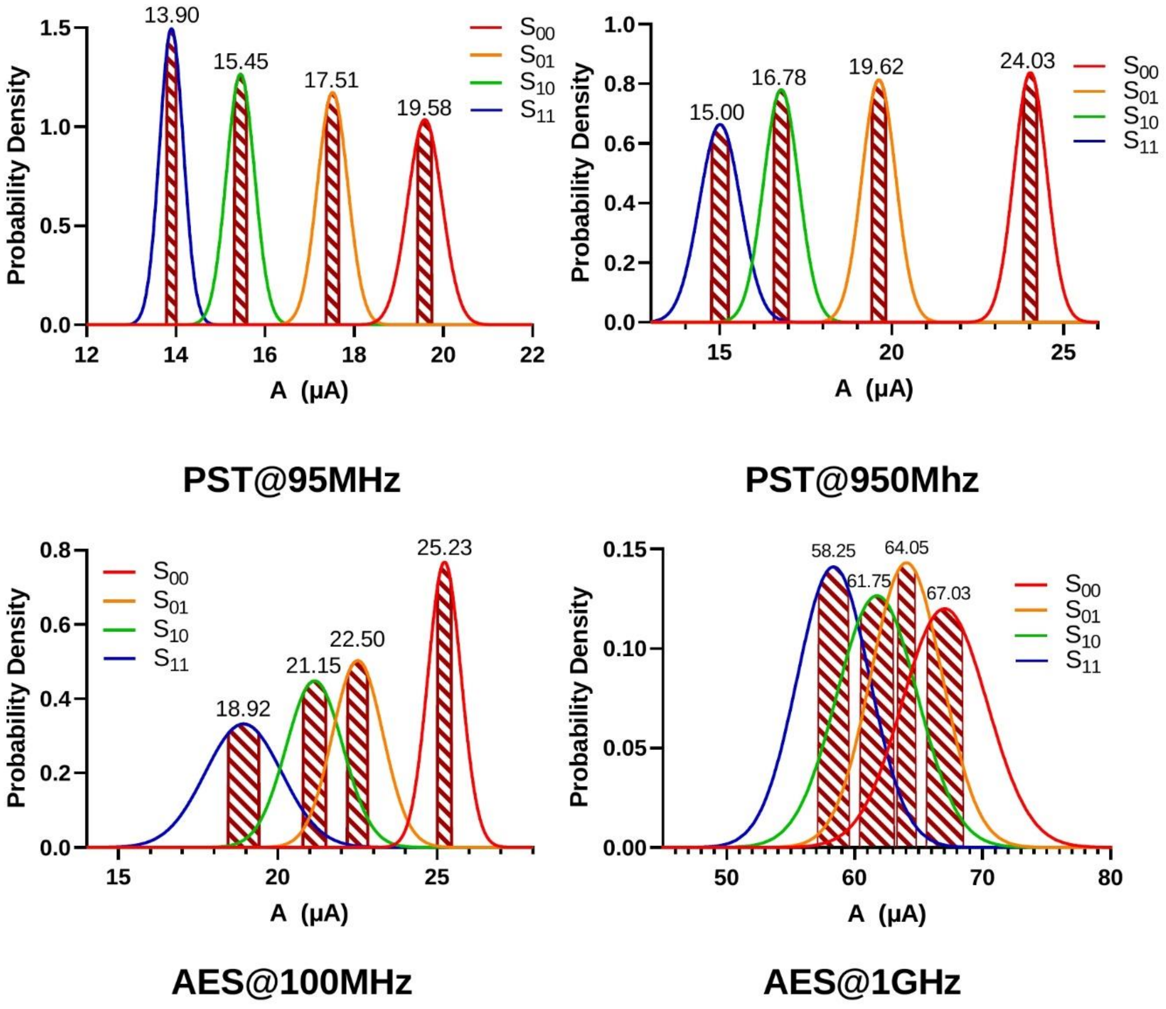


# Workbench Setup – AES@100MHz Example



# Hardware Validation Measures – 28 Samples Assessd

| Core | Total Power ($\mu$W) | Leakage ($\mu$W) |
|---|---|---|
| AES@1GHz | 101160±10781 | 743.79±108.07 |
| AES@100MHz | 3139.32±85.38 | 131.57±10.35 |
| PST@950MHz | 9661.3±758.52 | 80.75±7.82 |
| PST@95MHz | 868.56±57.90 | 74.35±6.84 |



PST@95MHz

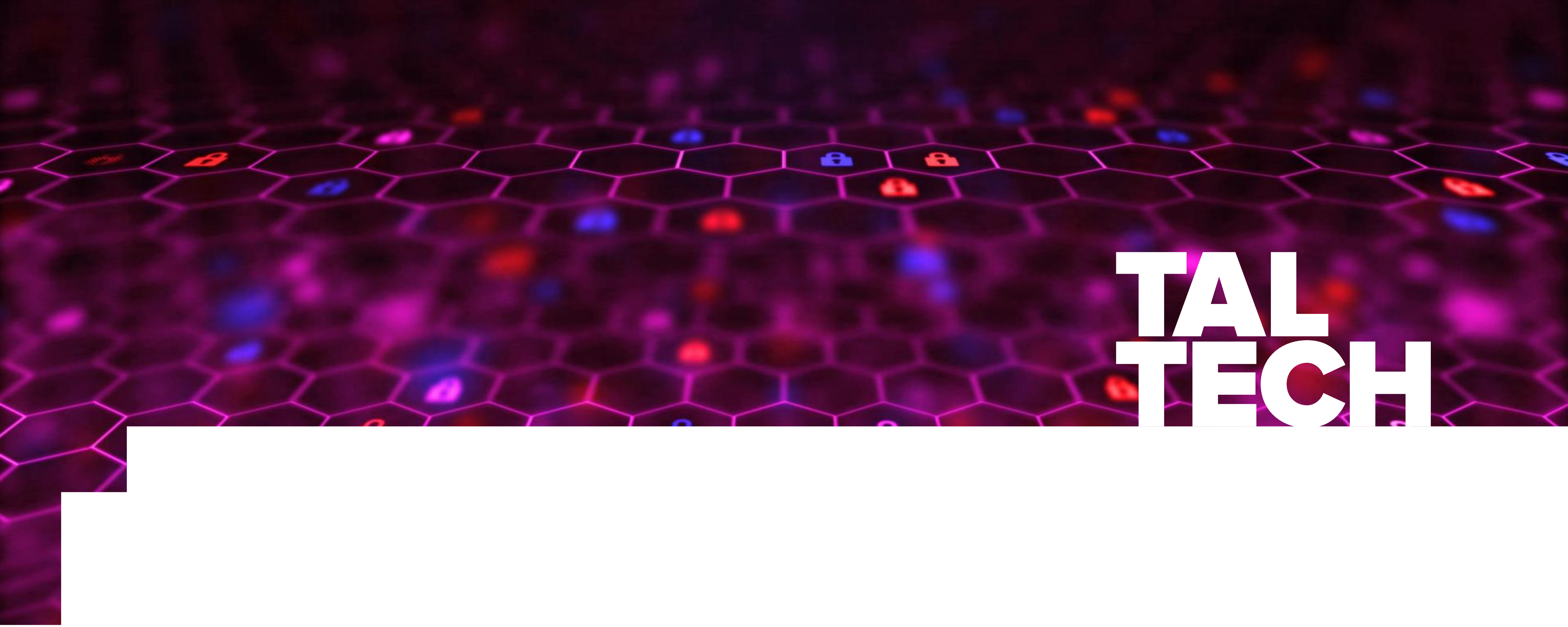
PST@950Mhz

AES@100MHz

AES@1GHz

## Conclusions

- ❑ECO flow can be used for malicious reasons.
- ❑A rogue element inside a foundry has all means necessary to modify a layout using ECO.
- ❑A very precise side-channel trojan can be built with only standard cells without the need of full custom design



THANK YOU!

CONTACT: TIAGO.PEREZ@TALTECH.EE