FABRICATION-TIME INSERTION OF HARDWARE TROJAN HORSES

Prof. Samuel Pagliarini
samuel.pagliarini@taltech.ee
Head of the Centre for Hardware Security
Tallinn University of Technology

Euroopa Liit
Euroopa Sotsiaalfond
Eesti tuleviku heaks
SAFEST

Outline

- Introduction
  - What is a hardware trojan?
  - Textbook example
- Fabrication-time insertion
  - Demonstration
- Final remarks

Source: https://www.eejournal.com/article/can-you-insert-hardware-trojan-spyware-ip-into-an-ic-at-the-fab-yes-you-can/

TAL TECH

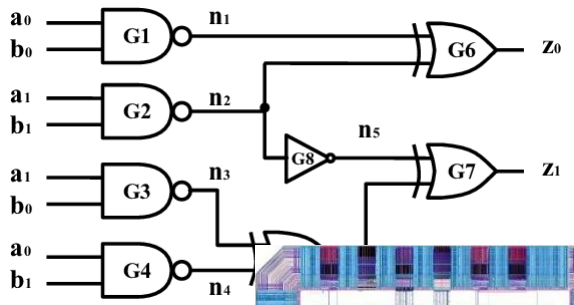
Outline

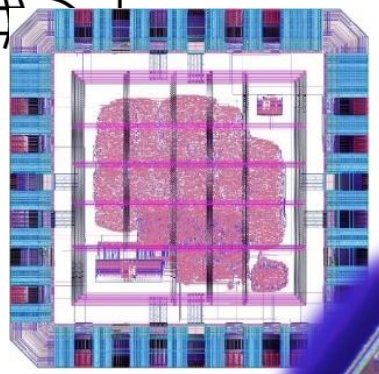
- **Introduction**
  - **What is a hardware trojan?**
  - Textbook example
- Fabrication-time insertion
  - Demonstration
- Final remarks

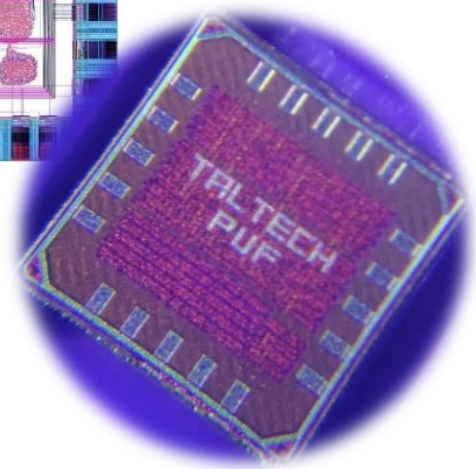
Source: https://www.eejournal.com/article/can-you-insert-hardware-trojan-spyware-ip-into-an-ic-at-the-fab-yes-you-can/

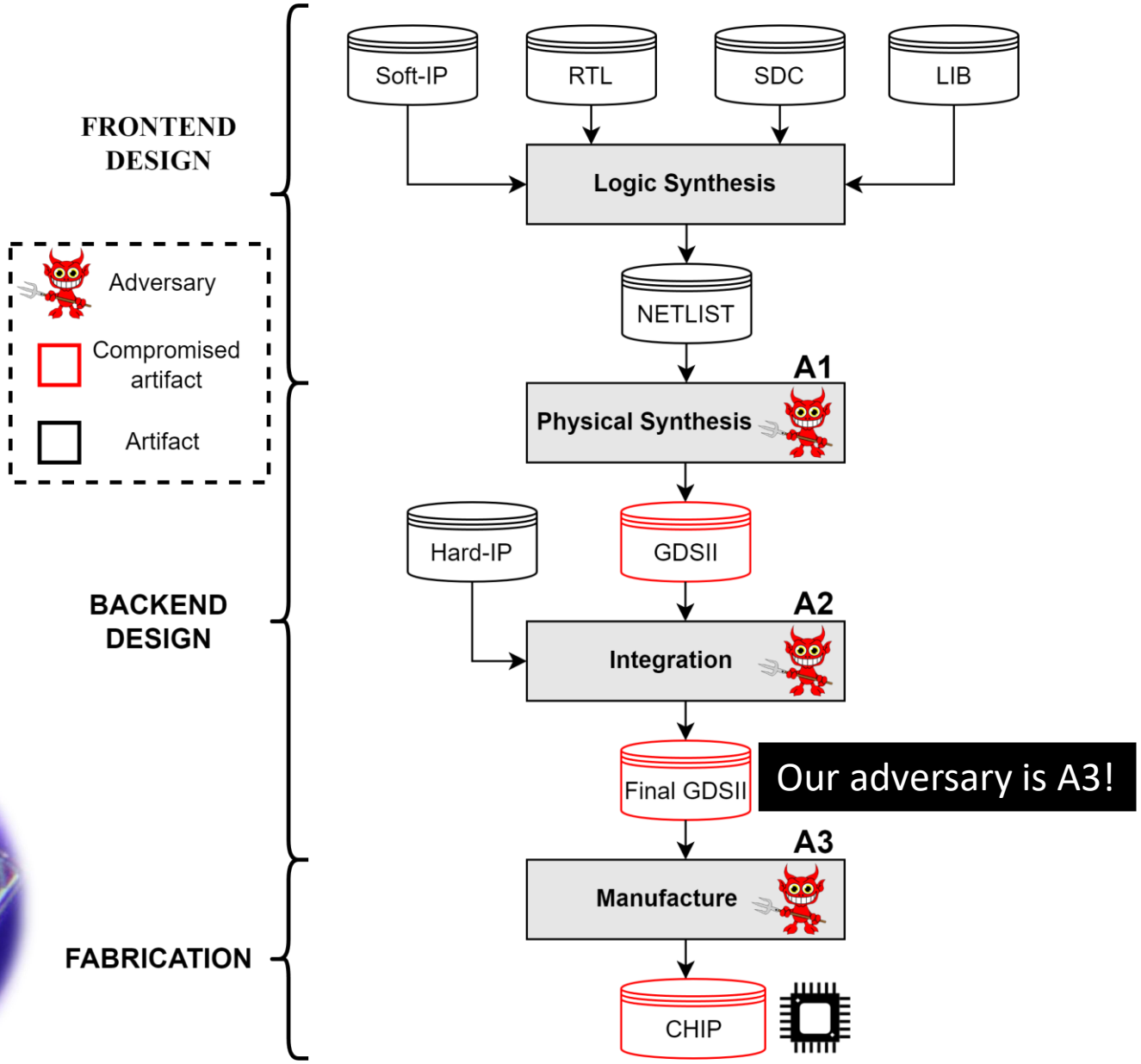
Threat models

```
1  module sample7(clk, a, b, c, avg);
2  input clk;
3  input [31:0] a, b, c;
4  output reg [31:0] avg;
5
6  always@(posedge clk) begin
7          avg <= (a + b + c) / 3;
8  end
9
10 endmodule
```

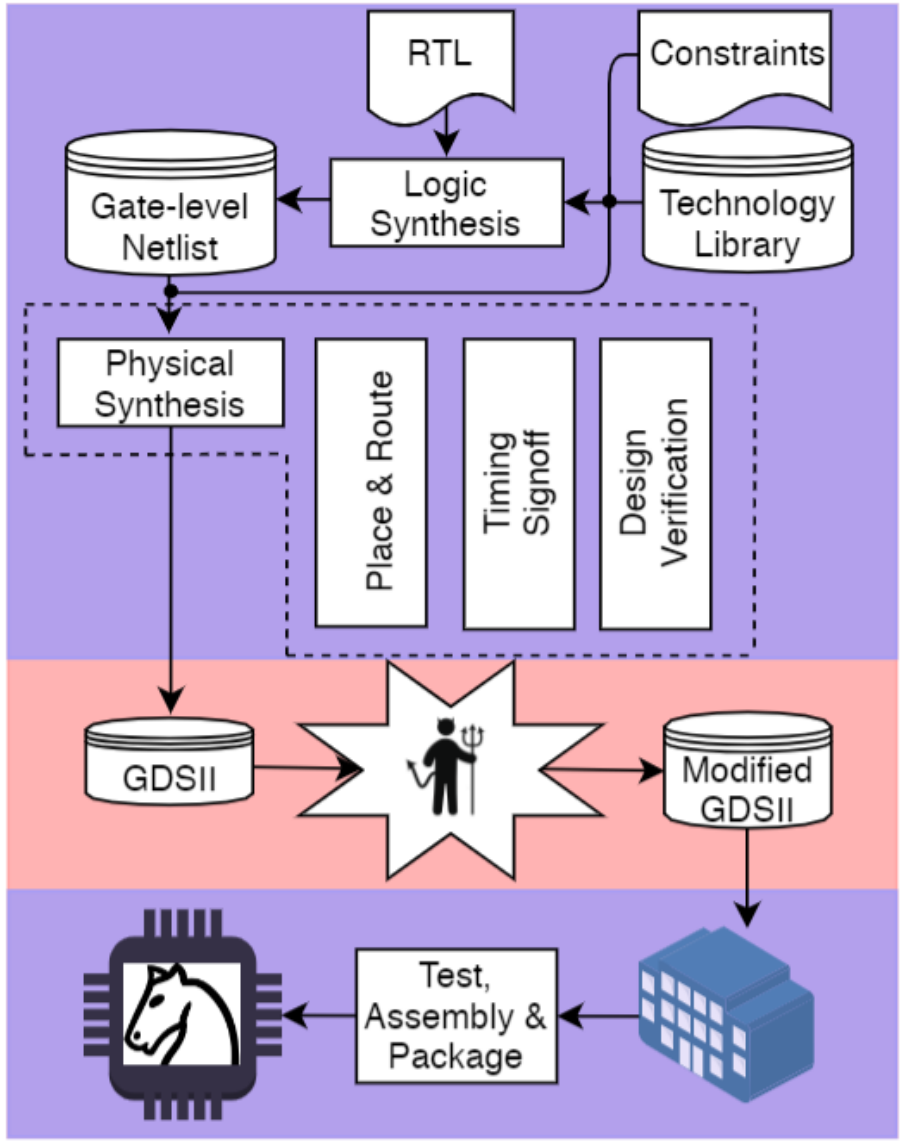








How are chips designed?



Let's have (another) look at the design flow…

Manufacturing is outsourced
Fabless model

Outline

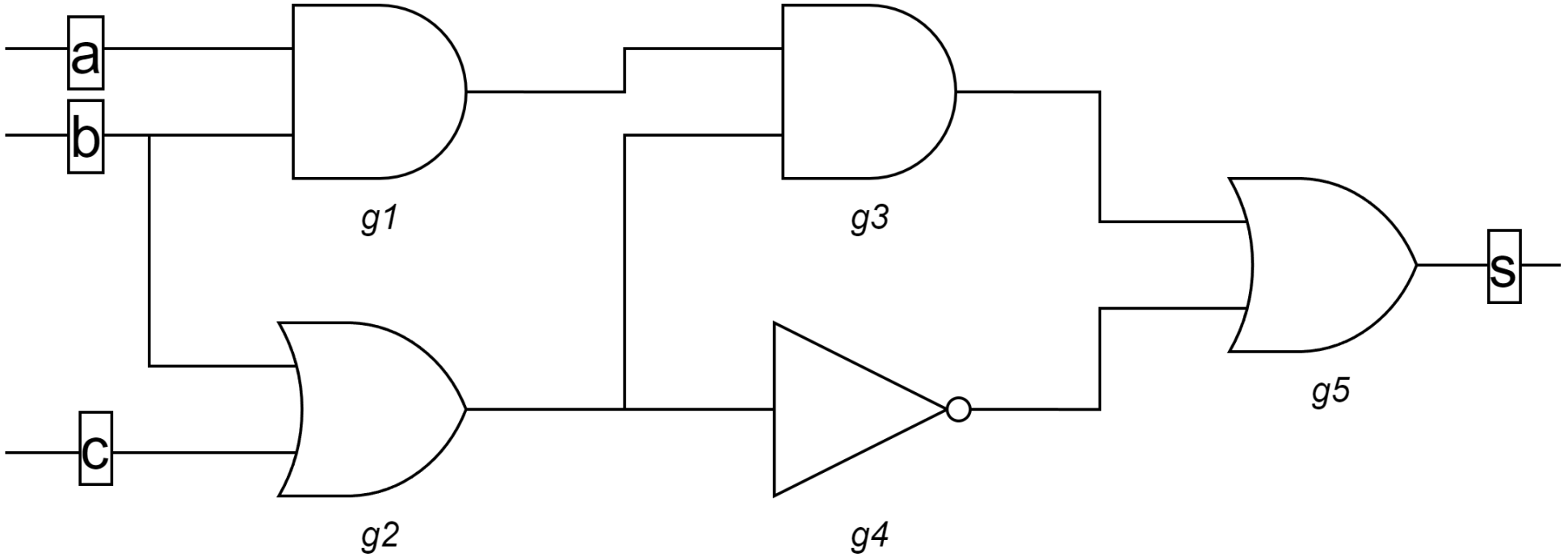
- **Introduction**
  - What is a hardware trojan?
  - **Textbook example**
- Fabrication-time insertion
  - Demonstration
- Final remarks

Source: https://www.eejournal.com/article/can-you-insert-hardware-trojan-spyware-ip-into-an-ic-at-the-fab-yes-you-can/

TAL TECH

Theory

- Let us consider the following logic as our “original circuit”

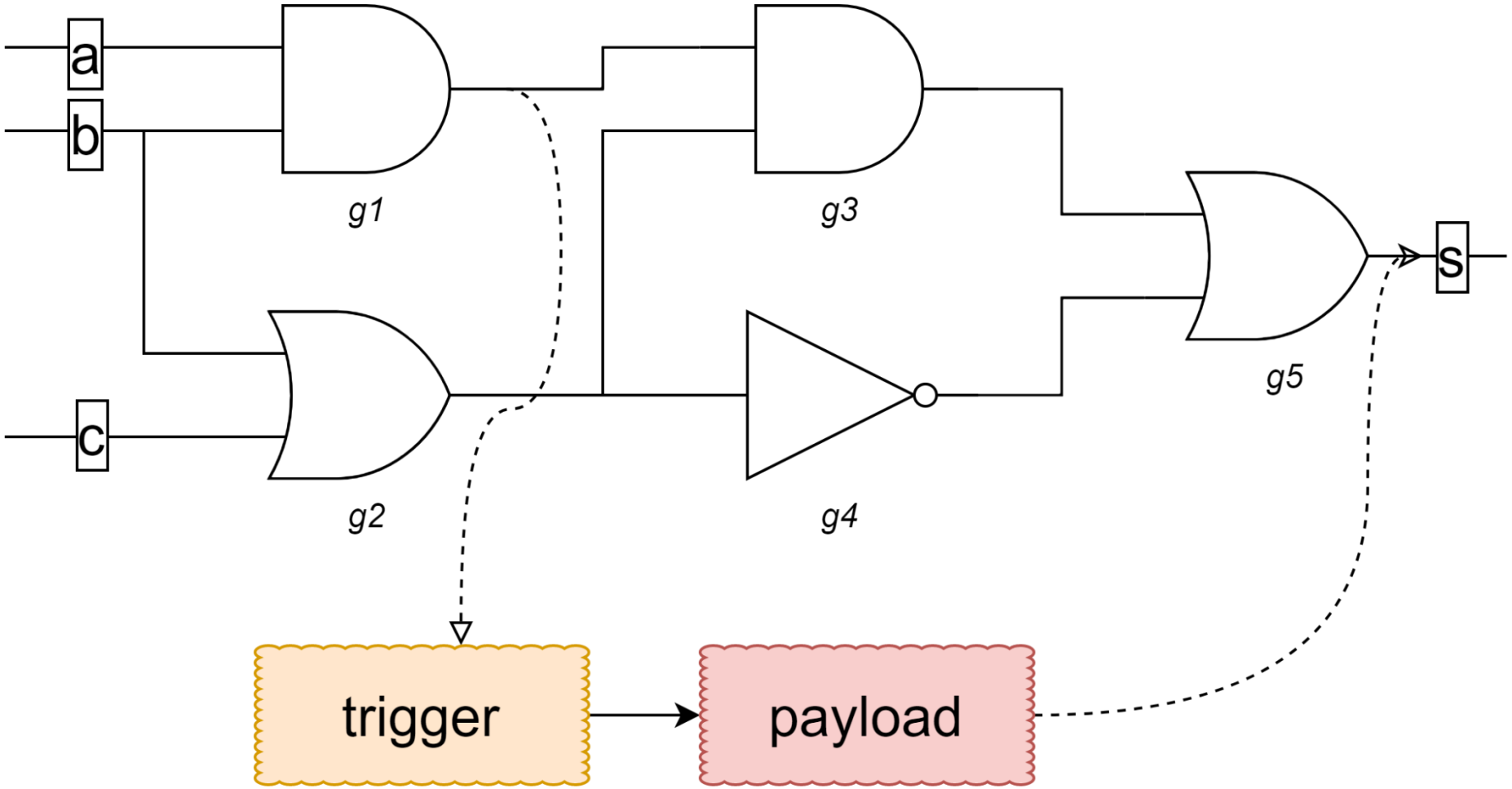


A	B	C	S
0	0	0	**1**
0	0	1	**0**
0	1	0	**0**
0	1	1	**0**
1	0	0	**1**
1	0	1	**0**
1	1	0	**1**
1	1	1	**1**

TAL TECH

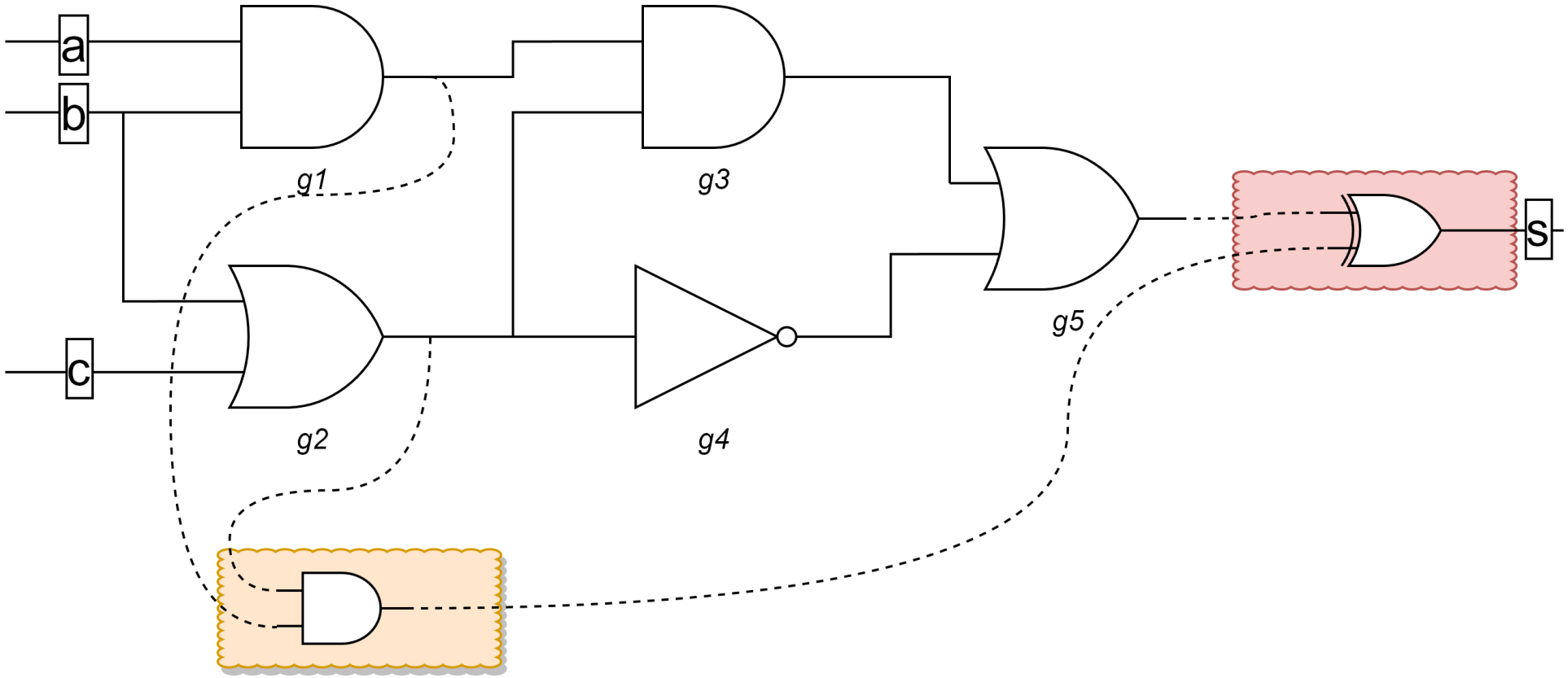
Theory

- A hardware trojan is composed of two parts, a **trigger** and a **payload**

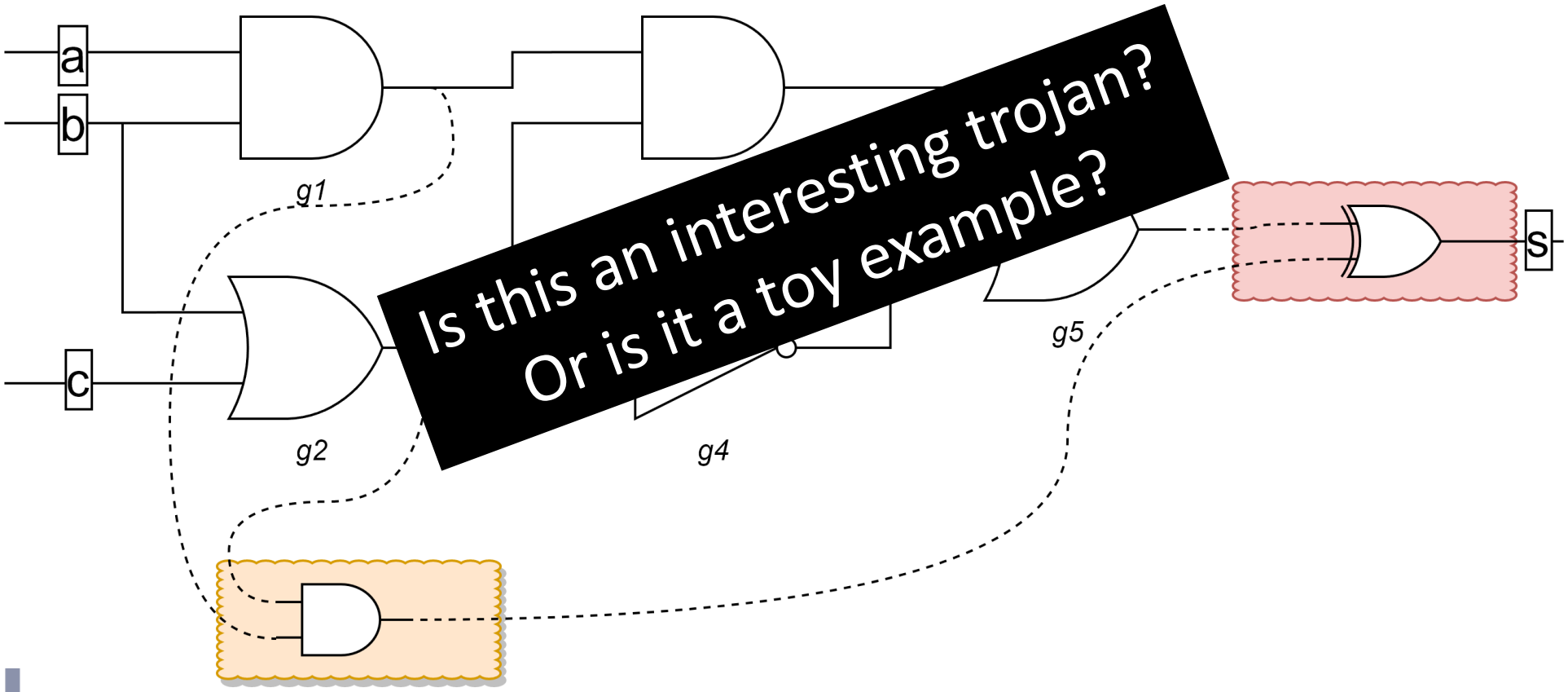


Textbook example

- Trigger: AND gate
- Payload: XOR gate



Textbook example



A	B	C	S	T	S*
0	0	0	1	N	S
0	0	1	0	N	S
0	1	0	0	N	S
0	1	1	0	N	S
1	0	0	1	N	S
1	0	1	0	N	S
1	**1**	**0**	**1**	**Y**	**!S**
1	**1**	**1**	**1**	**Y**	**!S**

TAL TECH

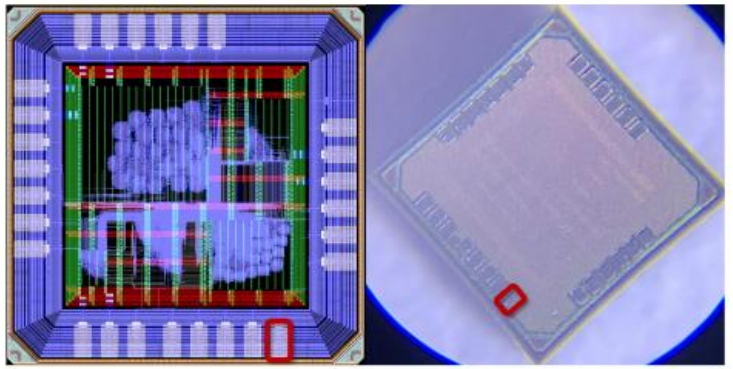
Textbook example

A	B	C	S	T	S*
0	0	0	1	N	S
0	0	1	0	N	S
0	1	0	0	N	S
0	1	1	0	N	S
1	0	0	1	N	S
1	0	1	0	N	S
1	**1**	**0**	**1**	**Y**	**!S**
1	**1**	**1**	**1**	**Y**	**!S**

Myths, inconsistencies, and threat models

- Research on hardware trojan horses is ongoing for ~20 years
- Threat models that are incoherent
- Trojans that lack precise goal
- Detection techniques that are meant for finding physical defects

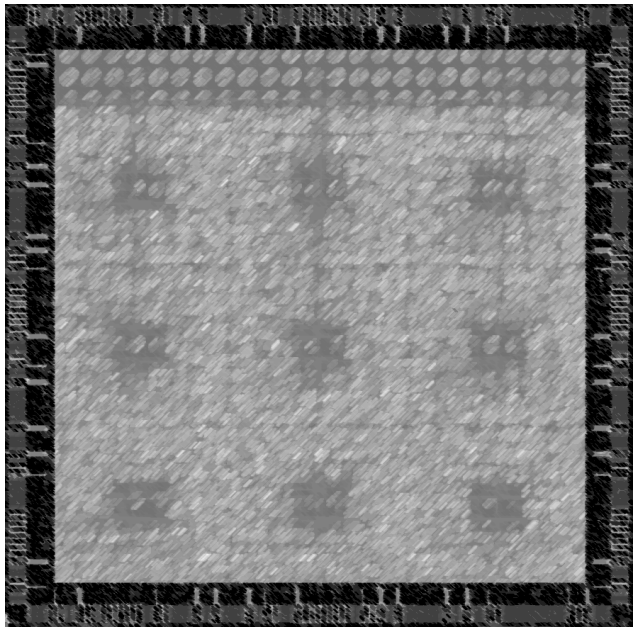
- This talk:
  - Attacker has **ambitious goals**
  - Attacker is **as capable** as a circuit designer
  - Has access to the **same CAD tools**
  - **Adversary + tools = problem!**



TAL TECH

Realistic execution times in chip design

- … for a 5mm x 5mm design w/ 0.5B transistors:
  - Placement + OPT takes **2 days**
  - CTS + OPT takes **3 days**
  - Routing takes **2-4 days**
  - Project load takes **1h**
  - Zoom-in to inspect a specific area takes **1 minute**
  - Exporting GDS takes **2-3h**
  - DRC takes **24h + 12h + 4h**



- Terrible scenario: last minute bug the day before a tapeout!
  - How to fix it without running the entire flow again?
  - **Pre-silicon ECO!**

TAL TECH

Outline

- Introduction
  - What is a hardware trojan?
  - Textbook example
- **Fabrication-time insertion**
  - **Demonstration**
- Final remarks

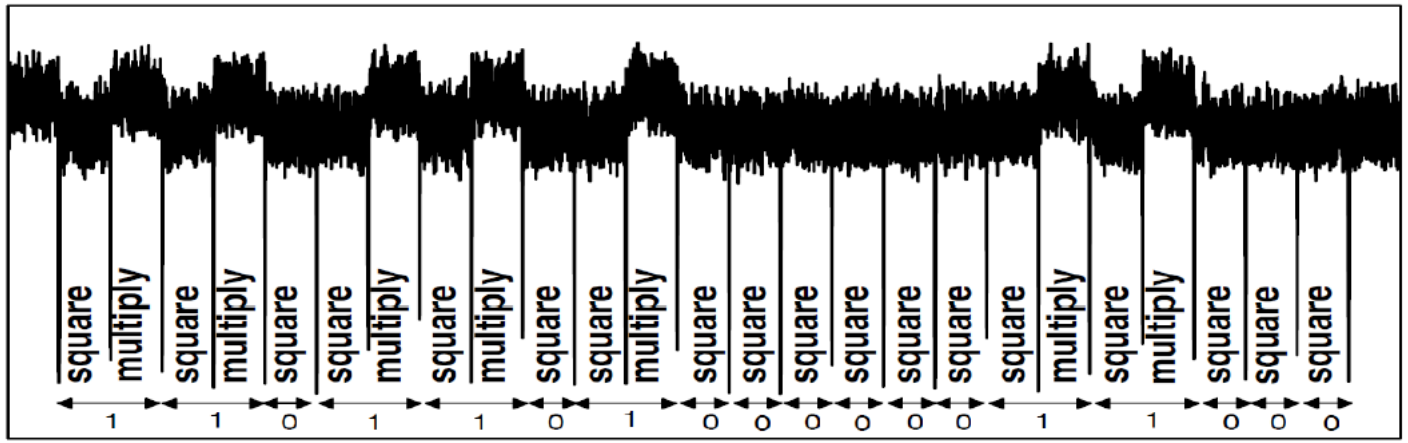
Source: https://www.eejournal.com/article/can-you-insert-hardware-trojan-spyware-ip-into-an-ic-at-the-fab-yes-you-can/

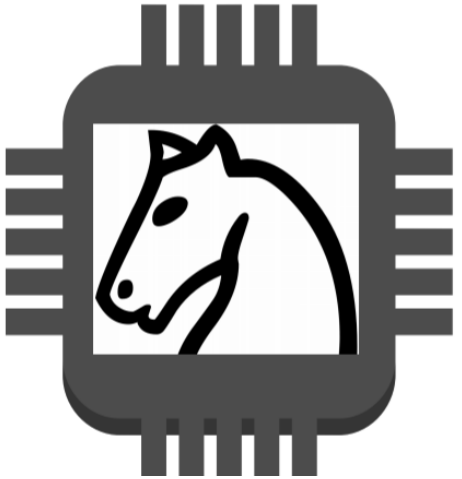
TAL TECH

Side-channel trojan

- **Goal**: create a hardware trojan that enables a power side-channel attack
- **Motivation**: SPA is great if you know what you are looking for
- **Challenge**: Designing and inserting a hardware trojan that modulates power

- **Novelty**: using an Engineering Changing Order (ECO) flow

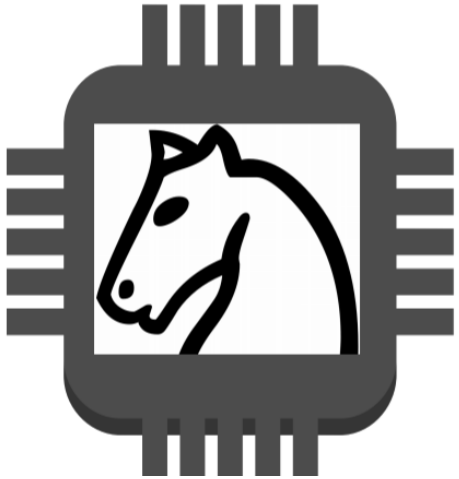




Side-channel trojan

- **Goal**: create a hardware trojan that enables a power side-channel attack
- **Motivation**: SPA is great if you know what you are looking for
- **Challenge**: Designing and inserting a hardware trojan that modulates power

- **Novelty**: using an Engineering Changing Order (ECO) flow



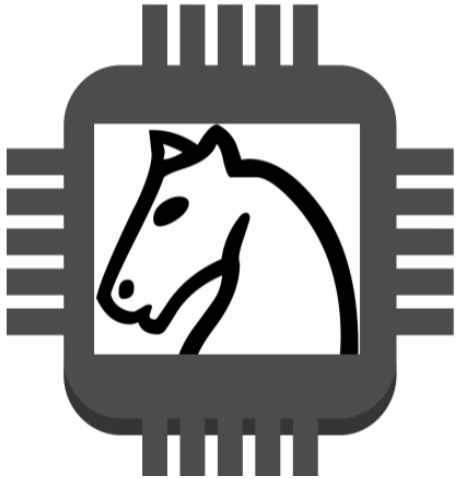
What circuit structure gives me controlled power consumption?

TAL TECH

Side-channel trojan

- **Goal**: create a hardware trojan that enables a power side-channel attack
- **Motivation**: SPA is great if you know what you are looking for
- **Challenge**: Designing and inserting a hardware trojan that modulates power

- **Novelty**: using an Engineering Changing Order (ECO) flow

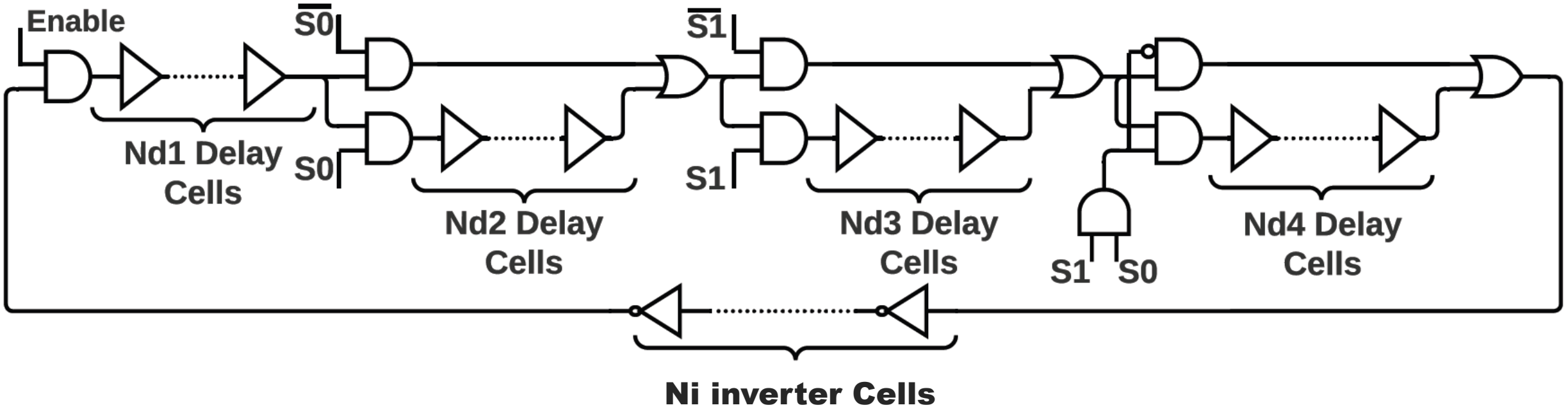


What circuit structure gives me controlled power consumption?
Ring oscillator

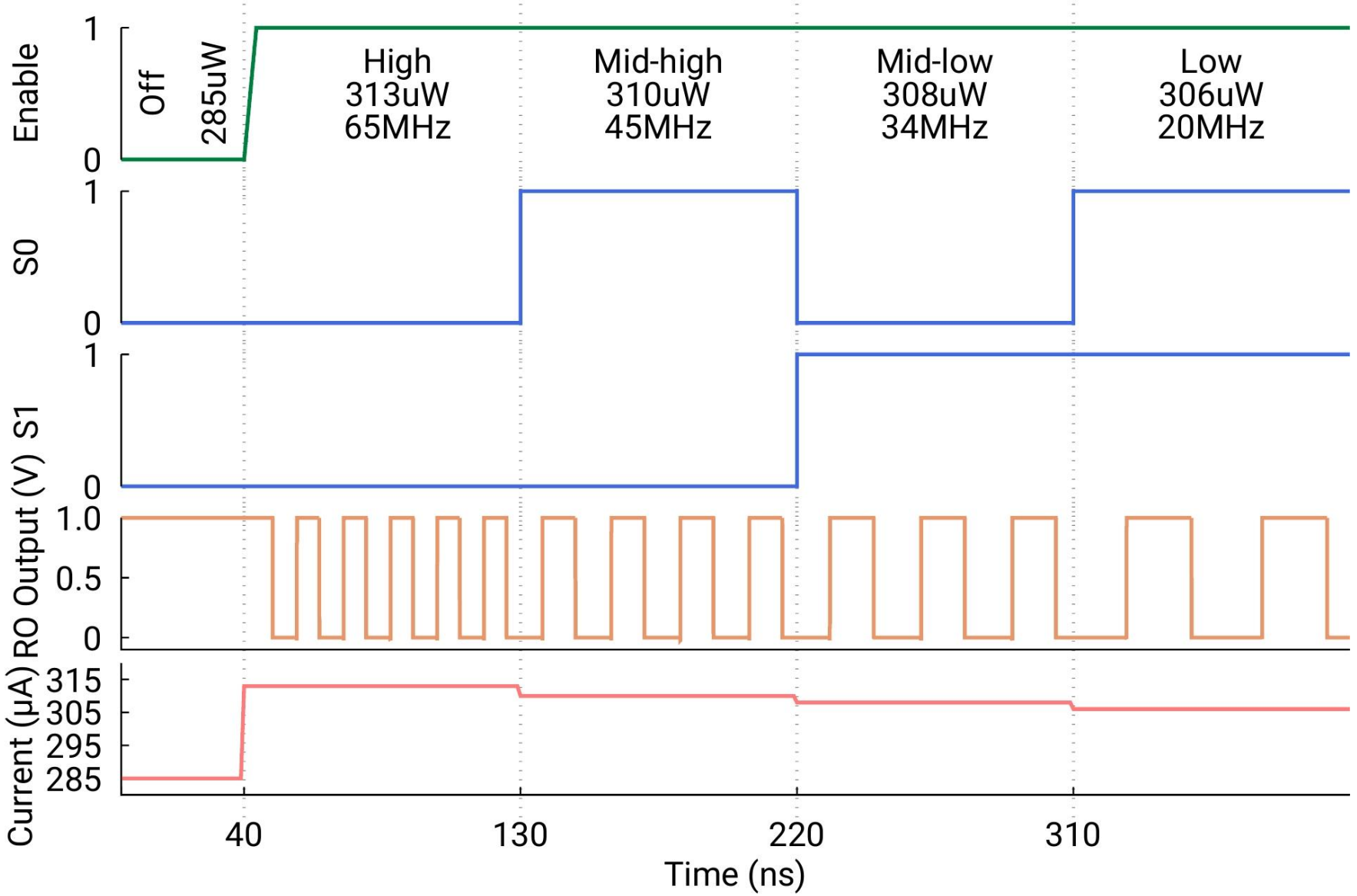
TAL TECH

Side-channel trojan

- S0 and S1 are select bits. They are the information I am trying to leak!

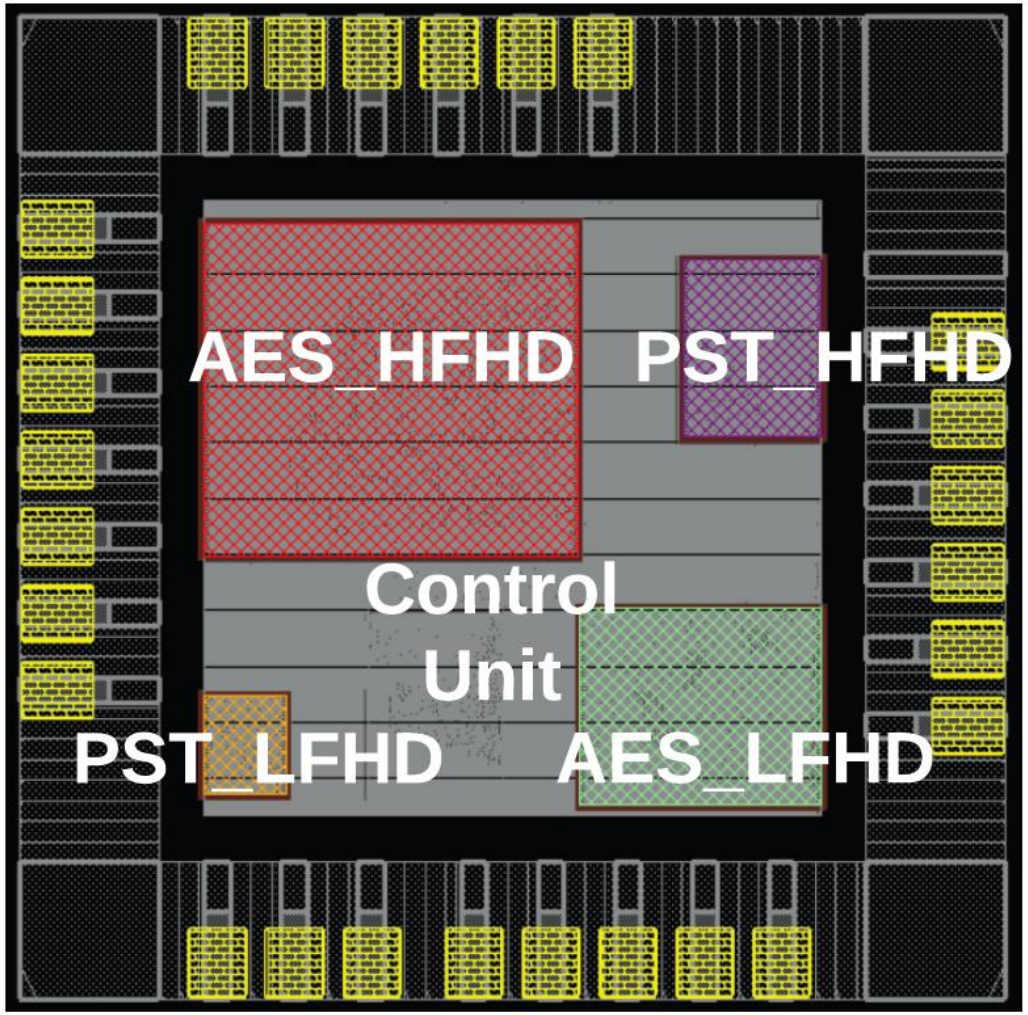


Side-channel trojan



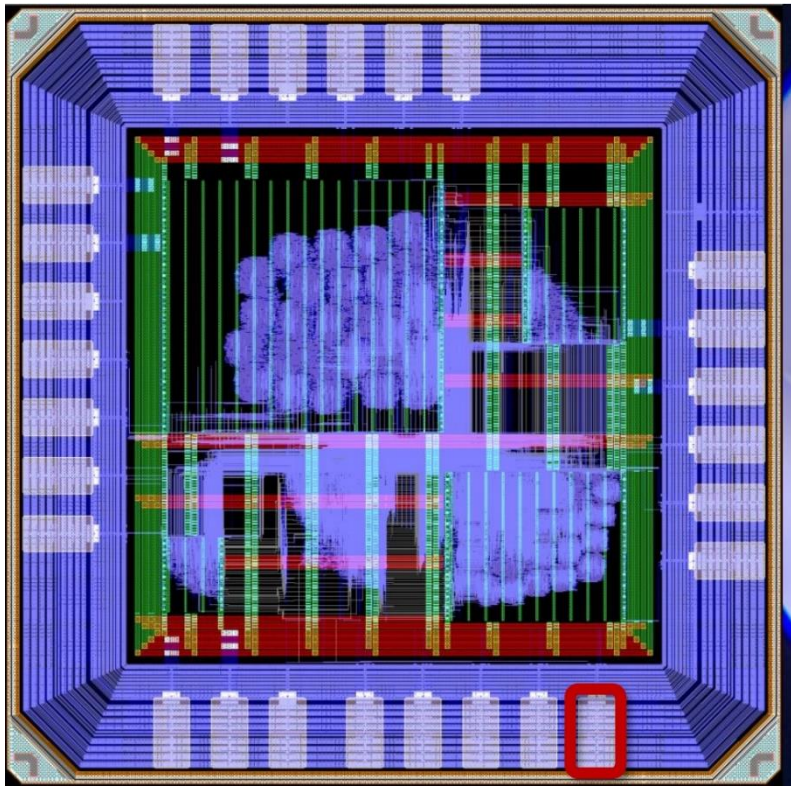
Our Prototype

- **Area:** 1mm^2
- **Technology:** 65nm
- **Architecture:** 4 crypto cores with one HT each
  - `HF = High frequency`
  - `LF = Low frequency`
  - `HD = High density`

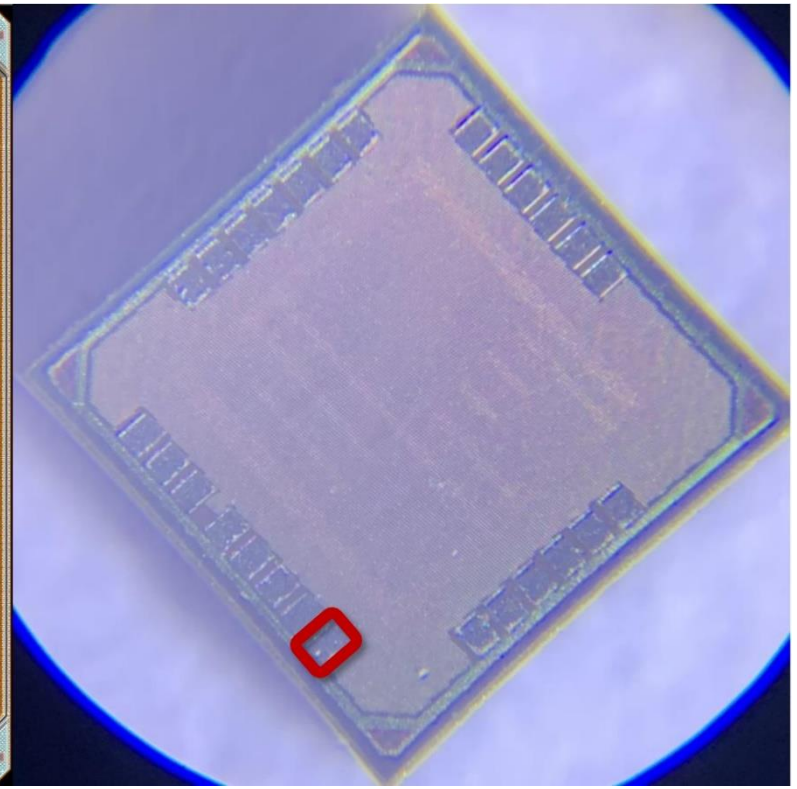


Our Prototype

- **Area:** 1mm^2
- **Technology:** 65nm
- **Trojan size**: 1000 xtors

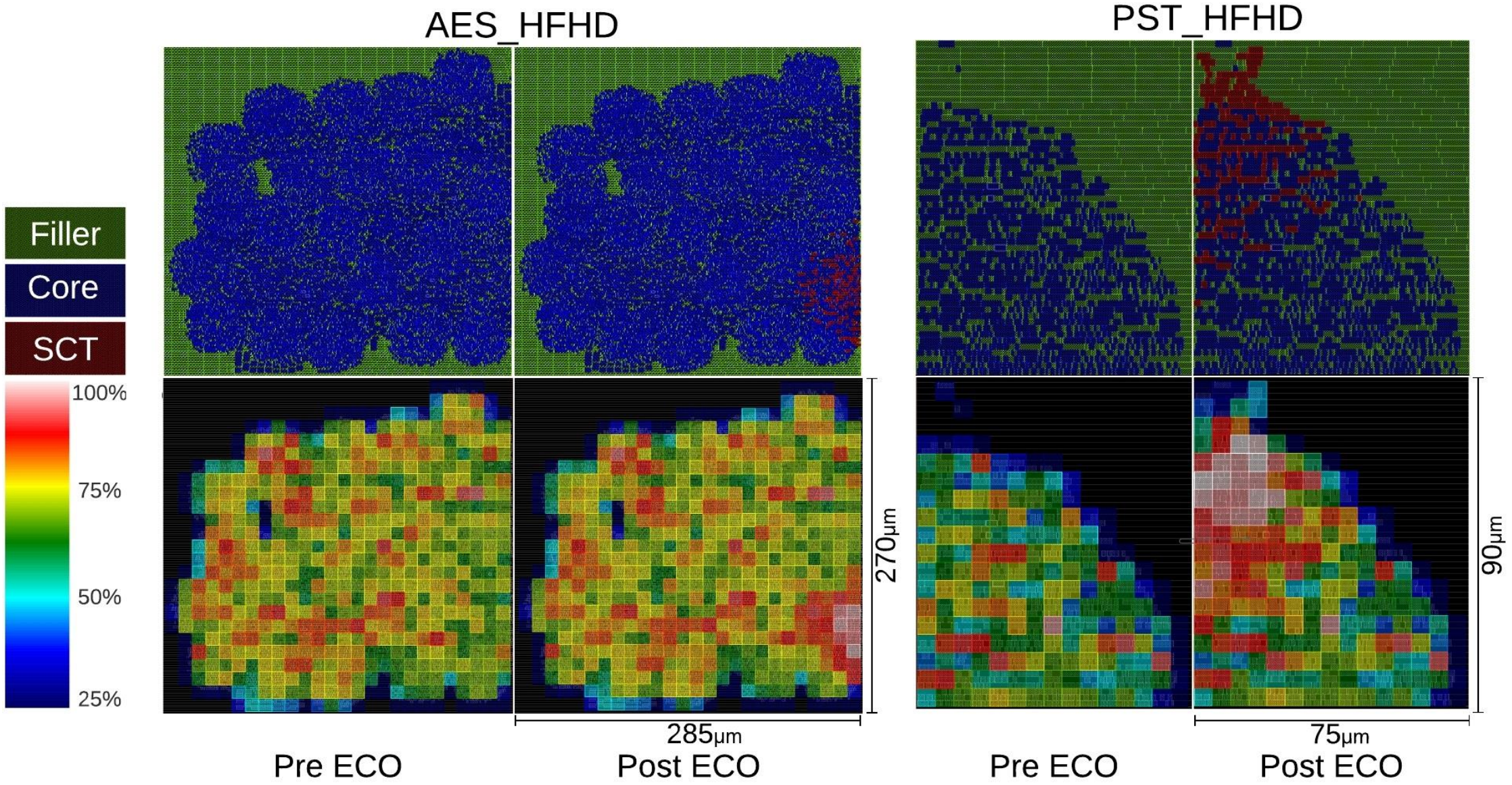


Layout



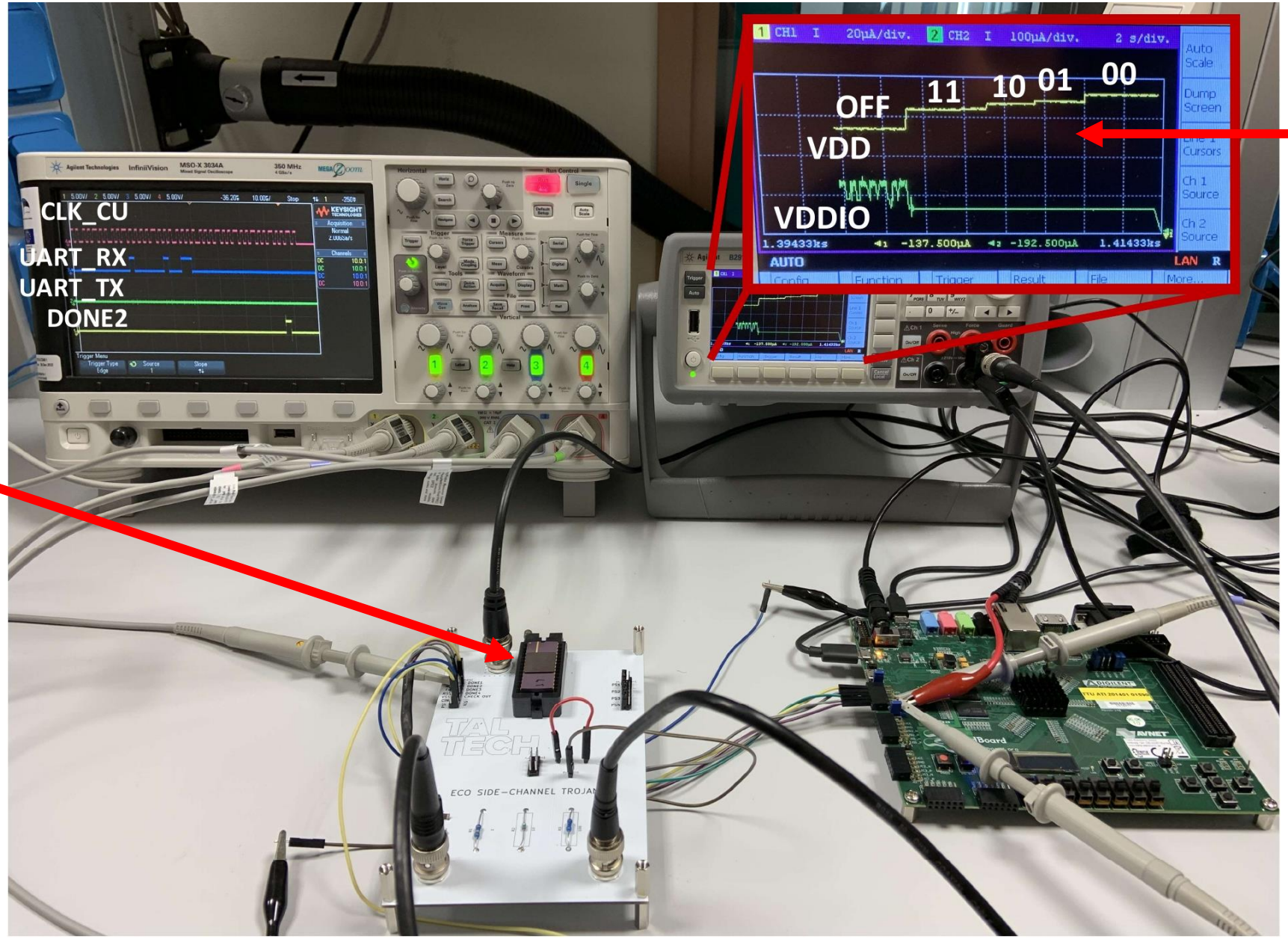
Die Shot

Side-channel trojan



TAL TECH

Testbench Setup



Outline

- Introduction
  - What is a hardware trojan?
- Theory
  - Textbook example
- Proposed approach
  - Demonstrations
- **Final remarks**

Source: https://www.eejournal.com/article/can-you-insert-hardware-trojan-spyware-ip-into-an-ic-at-the-fab-yes-you-can/

Final remarks

- HT insertion in finalized layouts is a realistic threat to today's globalized IC manufacturing and must **not** be taken lightly
- We still have a **long way** to go on trojan prevention
  - CAD support?

TAL TECH

ISPD'23 contest

- ISPD organizes a contest every year
- Now, in the 19th edition, the topic is Hardware Trojans!

- Open to students and postdocs!
- Registration closes on Feb 1st!

https://ispd.cc/

TAL TECH

References

- "Side-channel trojan insertion – a practical foundry-side attack via ECO," **ISCAS'21**
- "A Side-Channel Hardware Trojan in 65nm CMOS with 2uW precision and Multi-bit Leakage Capability," **ASPDAC'22**
- "Ransomware Attack as Hardware Trojan: A Feasibility and Demonstration Study," **IEEE Access**
- "Hardware Trojan Insertion in Finalized Layouts: a Silicon Demonstration," **TCAD**
- "A Pragmatic Methodology for Blind Hardware Trojan Insertion in Finalized Layouts," **ICCAD'22**

TAL TECH