Hardware Security: Investigation of Fingerprinting (Advanced CMOS and PCB level)

Matthias Ludwig, Vincent Krämer

2024-03-20

Table of contents

1	Introduction	3
2	SRAM	10
3	PCB	18
4	Conclusion	24

Table of contents

1	**Introduction**	**3**
2	SRAM	10
3	PCB	18
4	Conclusion	24

Introduction

Secured hardware is vital for system-critical applications

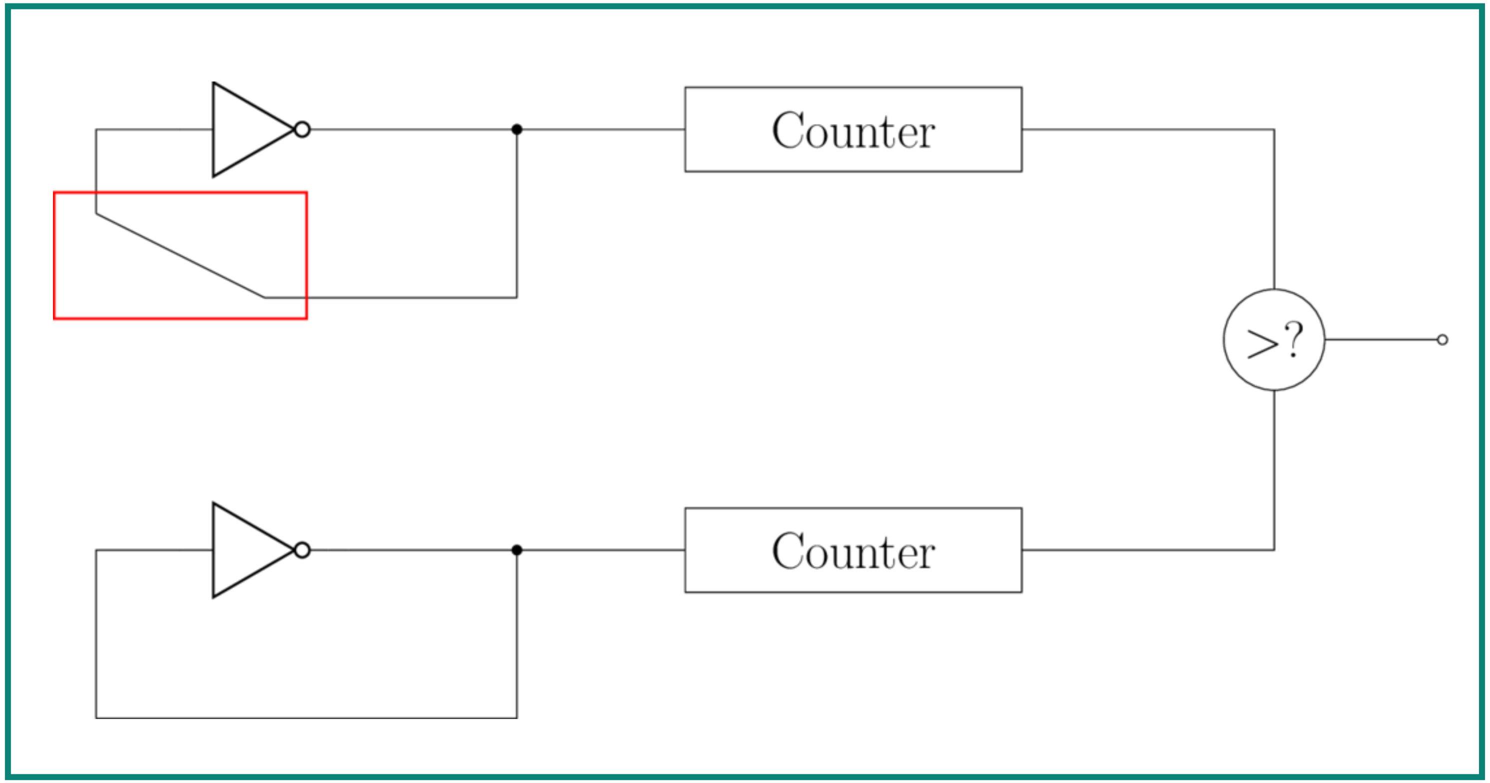
Hardware fingerprints claim to enable realizing security goals such as anti-counterfeiting, secured key storage, or authentication

Evaluating the **claimed property** that fingerprints are **protected from being reproduced** by direct physical characterization

Introduction: Fingerprinting

Example: Ring Oscillator

Equally designed and only influenced by randomly occurring **manufacturing variances**



Background & Research Question

Observing – Side-Channel

“Side-Channel Analysis of ‘PUFs’ and Fuzzy Extractors”

“Localized electromagnetic analysis of RO ‘PUFs’”

[1], [2]

Semi-Invasive – Optical

Attacks on ‘PUFs’ by photonic emission analysis

Identification of fingerprints by correlation optical images and emission fingerprints

[3], [4]

Invasive – FIB Modification

Demonstrated a Focused Ion Beam circuit edit with which they produced a physical clone of their Proof-of-Concept SRAM ‘PUF’ implementation

[5]

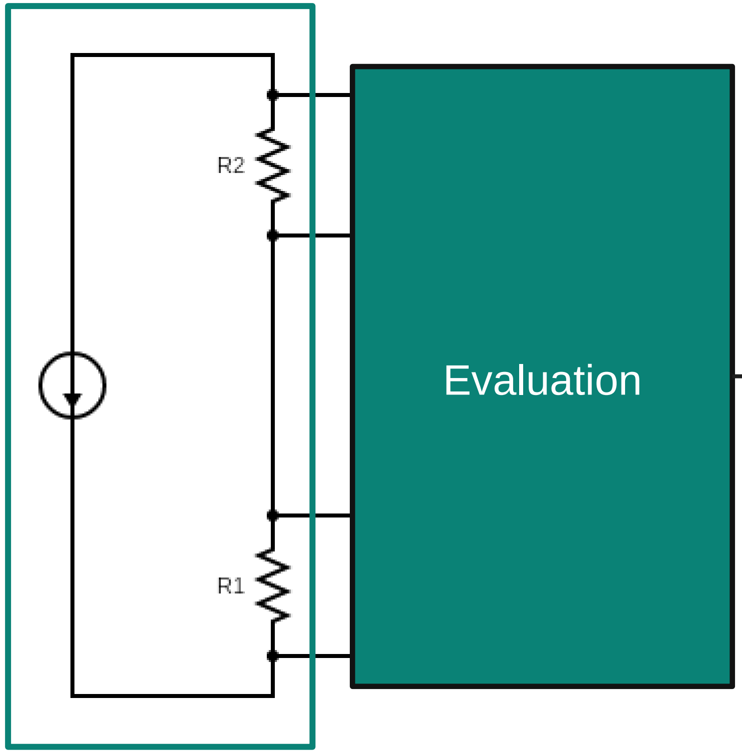
Research question: Can hardware fingerprints be effectively characterized by direct physical measurement methods?

Physical Model

To effectively characterize fingerprints, we need a **link between hardware and response**

R1 < R2 or

R1 > R2



0 or 1

Research Agenda

- **Ground Truth Generation**
- **Ground Truth Evaluation**
- **Model Generation**
- **Measurement**
- **Data Analysis**

Enrollment: Ground Truth Generation, Ground Truth Evaluation

Evaluation: Measurement, Data Analysis

Case Studies

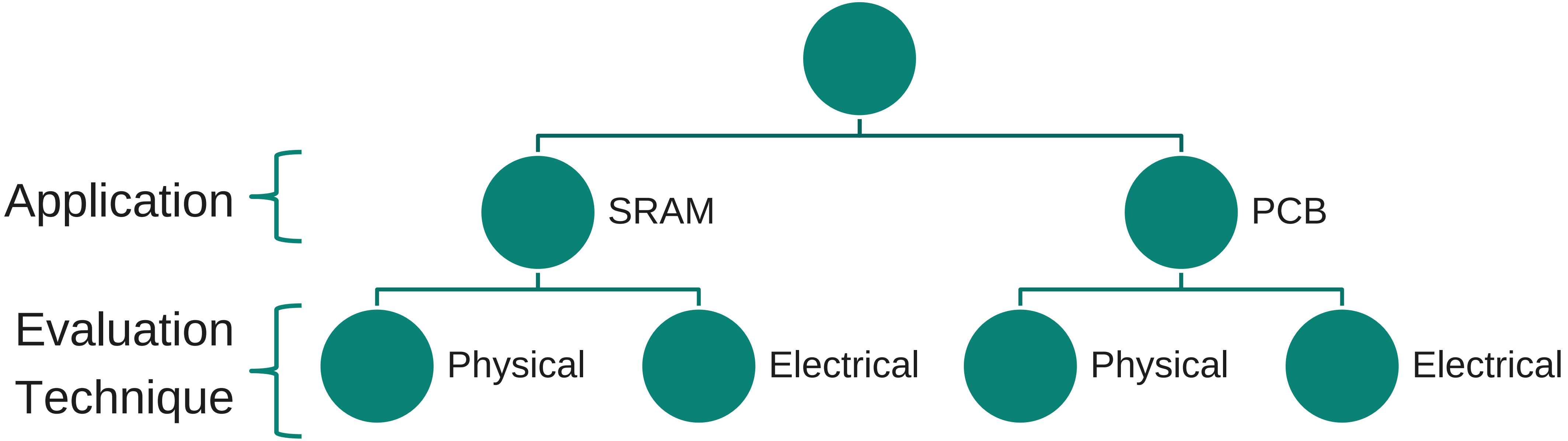
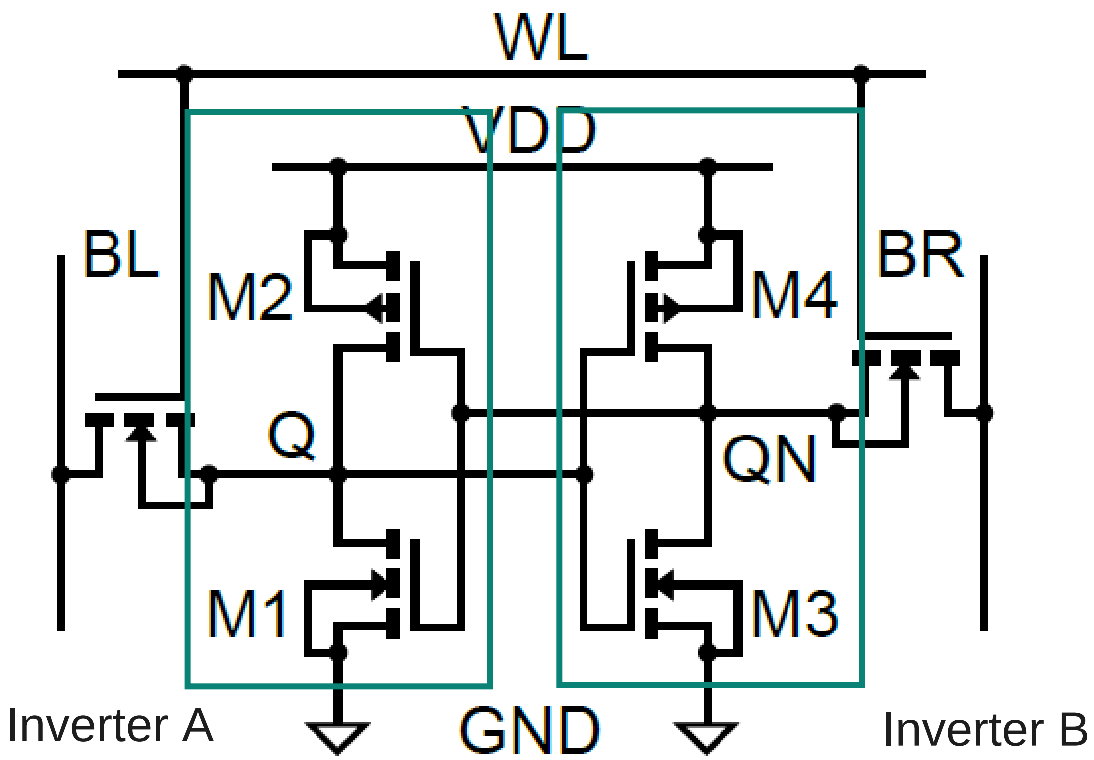


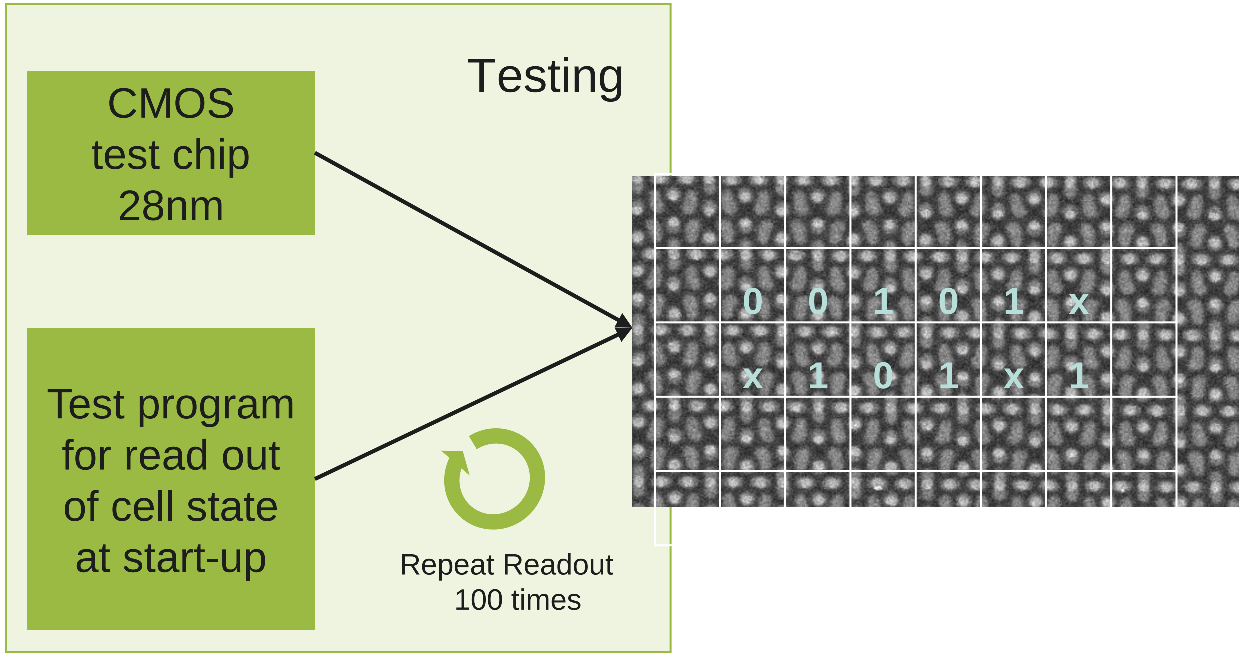
Table of contents

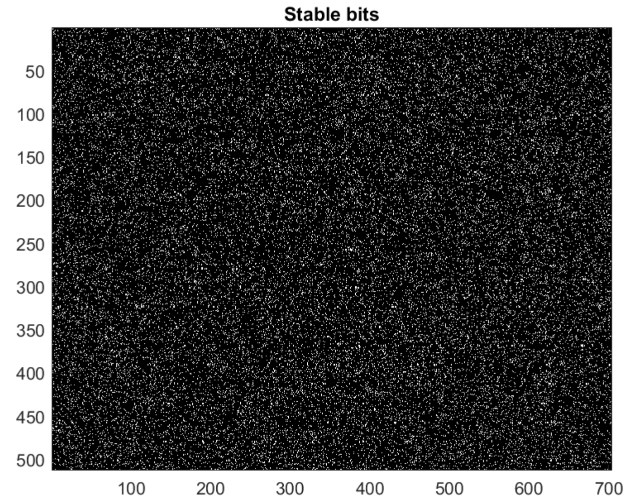
1	Introduction	3
2	**SRAM**	**10**
3	PCB	18
4	Conclusion	24

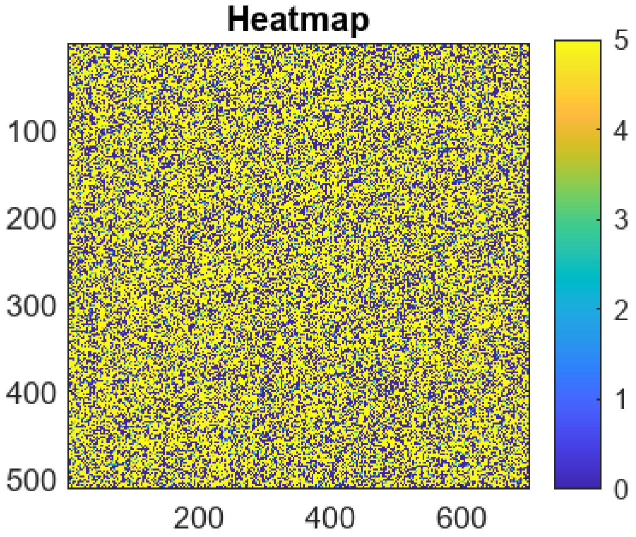
Recap: Start-Up SRAM Cell

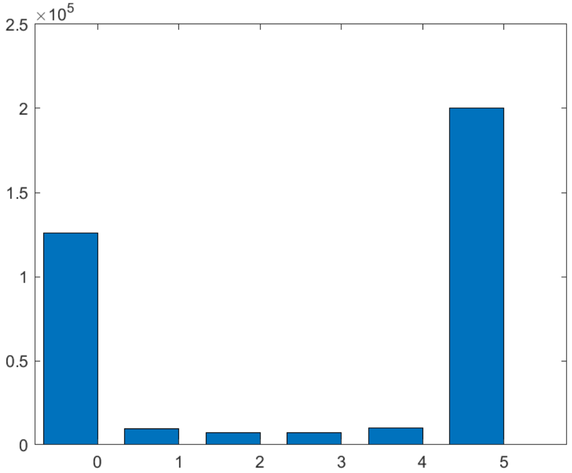


Ground Truth Generation & Evaluation

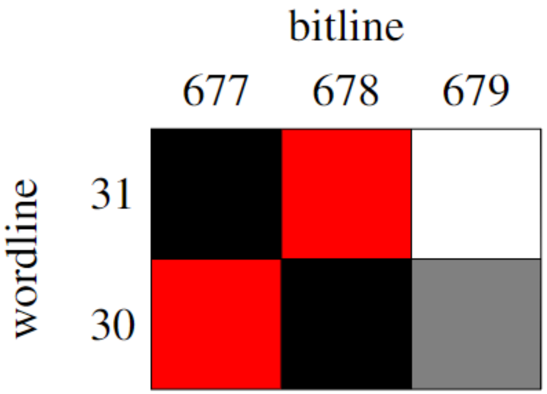


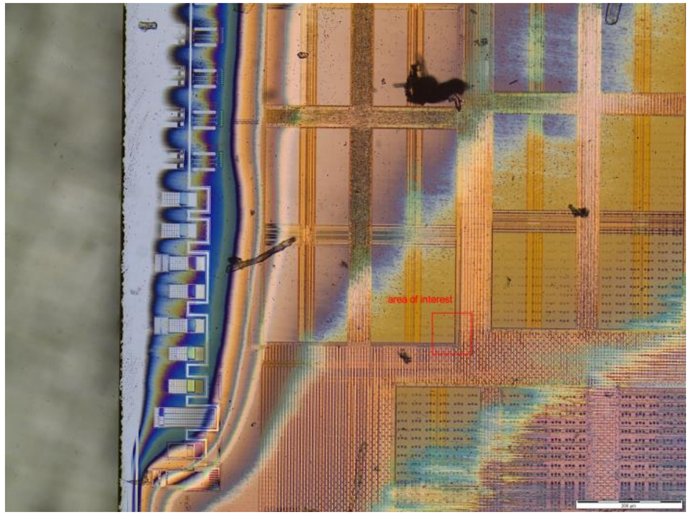


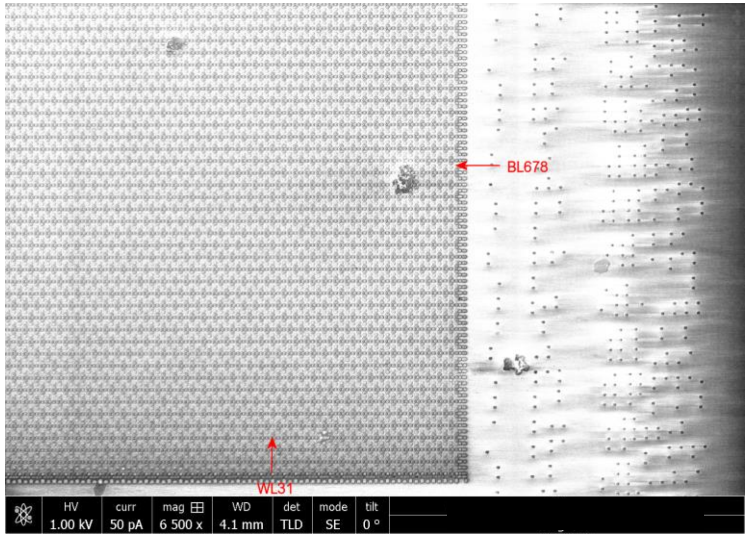


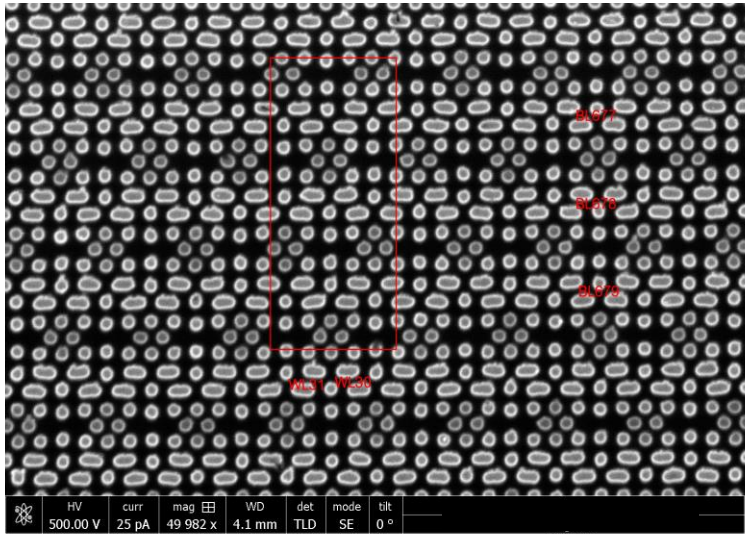


Delayering and Imaging (RE) of the ROI

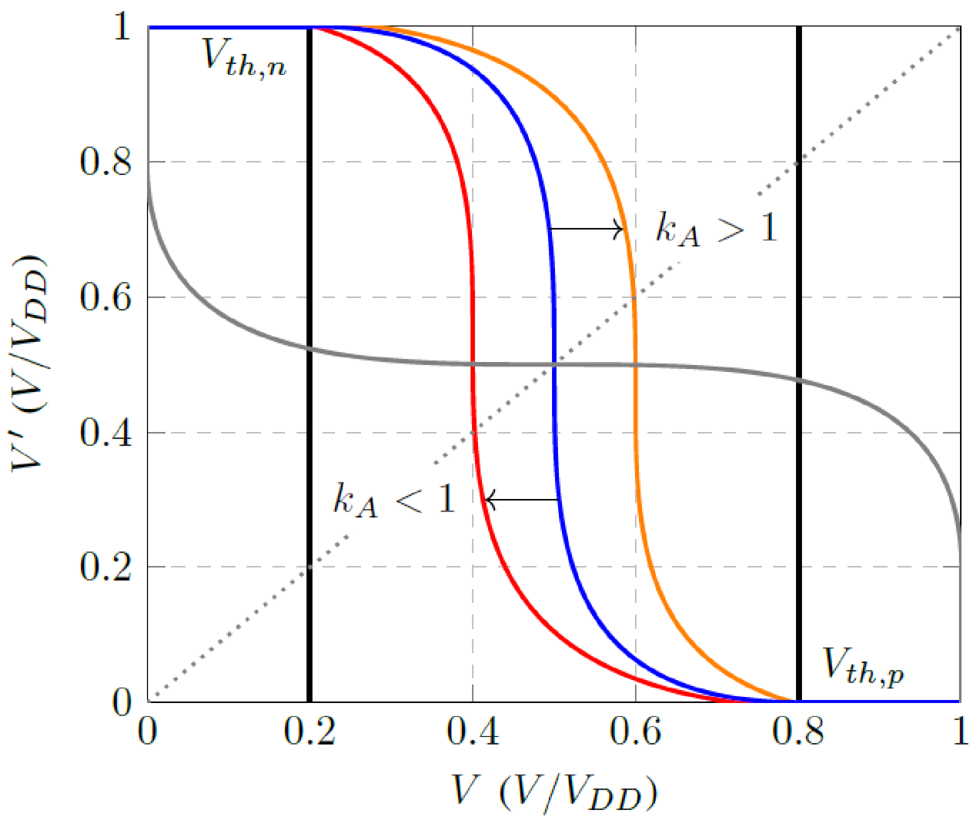








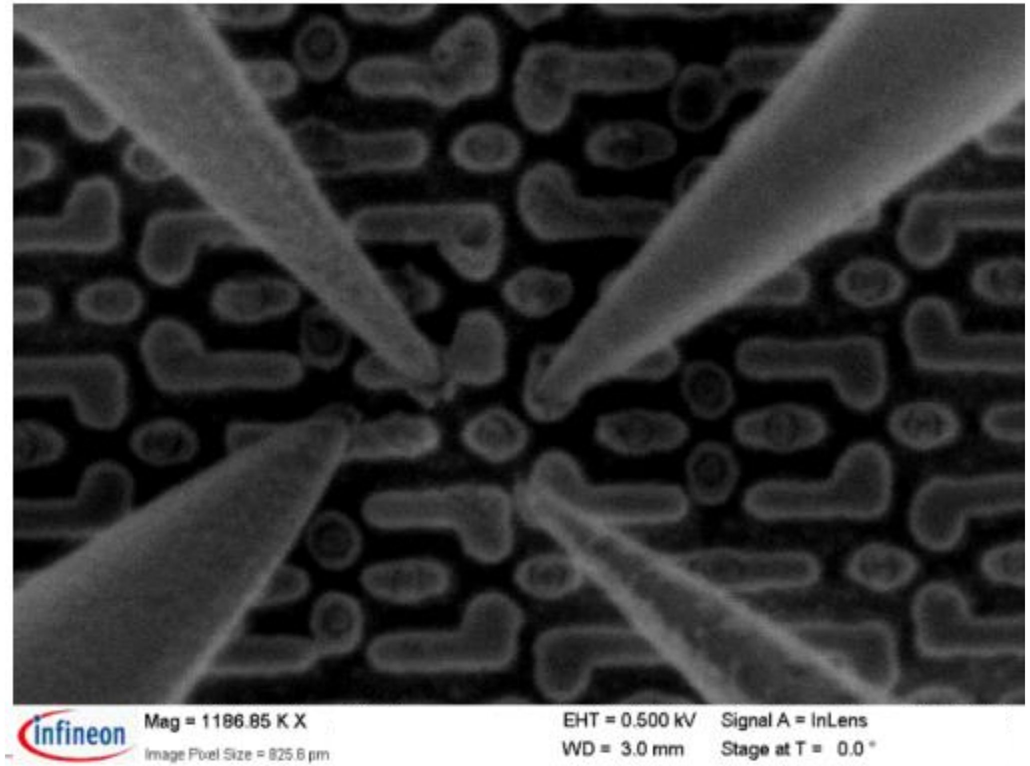
Physical Model Generation [7]



$$\beta_i = \frac{1}{2} \cdot \mu_i \cdot \frac{\varepsilon_0 \cdot \varepsilon_{r,ox}}{d_{ox}} \cdot \frac{W}{L} = c_i \cdot \frac{W}{L}; \quad k = \frac{\beta_n}{\beta_p}$$

Measurement and Data Analysis: Probing (WIP)

- **Place nanoprobes** on transistors
- **Output:** Voltage transfer characteristics
- Preferred cells is evaluated by equation from [6]
- **Does not scale** for many cells



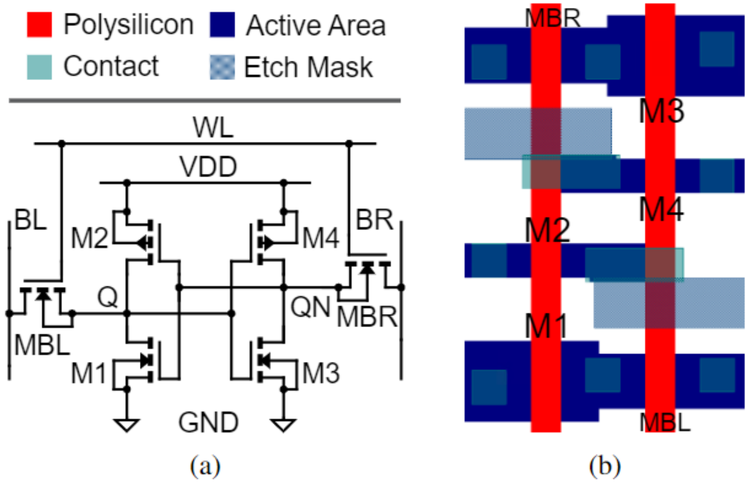
Measurement: Layout

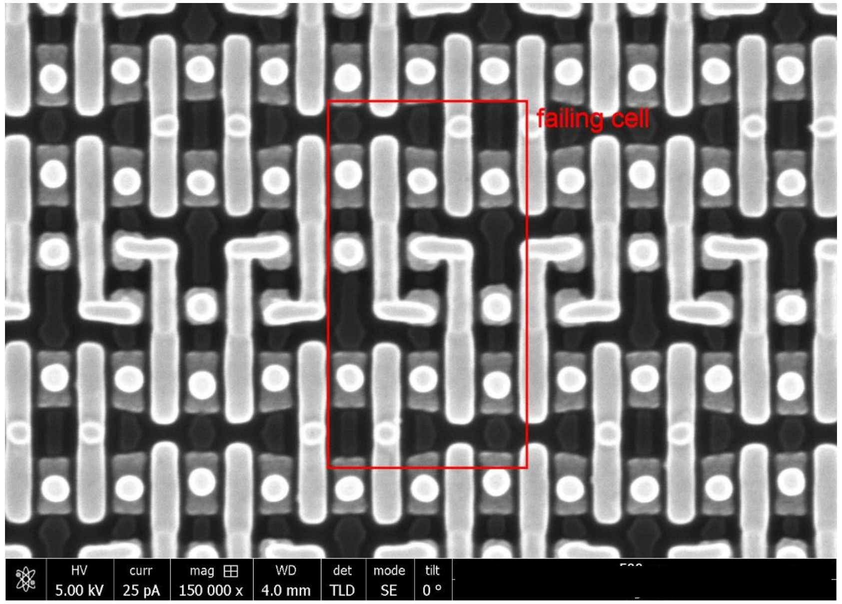
– Allows to measure length/width of transistors automatically

– Transconductance and, ultimately cell state depend on
  – Oxide thickness
  – Transistor geometry (L/W)
  – Doping parameters

– Only parameters length/width available in layout analysis

$$\beta_i = \frac{1}{2} \cdot \mu_i \cdot \frac{\varepsilon_0 \cdot \varepsilon_{r,ox}}{d_{ox}} \cdot \boxed{\frac{W}{L}}$$

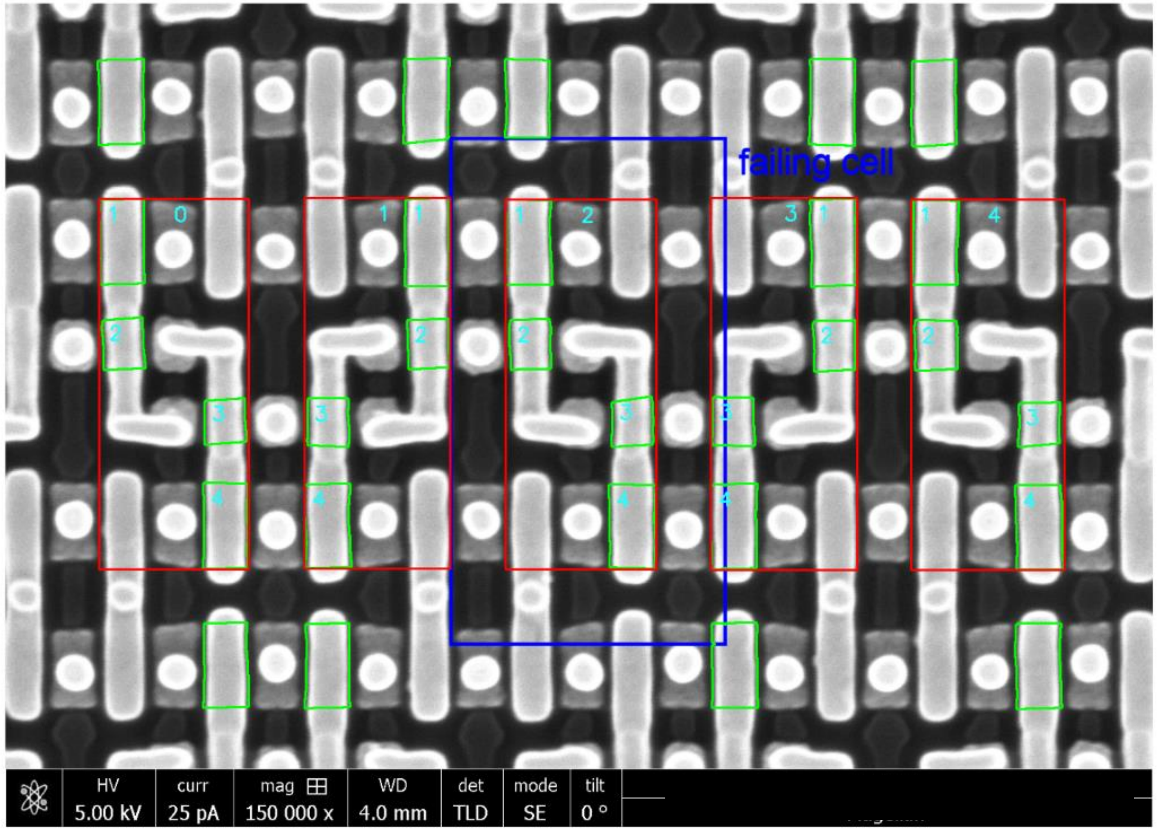




Data Analysis: Layout (WIP)

- Cells are detected by image processing (red)
- Width/length of transistors (green)

Cell	Transistor	L [nm]	W [nm]	Ground truth
C0	M1	62	116	1
	M2	60	71	
	M3	58	63	
	M4	61	116	
C1	M1	61	119	0
	M2	58	68	
	M3	58	66	
	M4	64	114	



- Find correlation between measurements and ground truth
- Preferred cells is evaluated by formula [7]

Table of contents

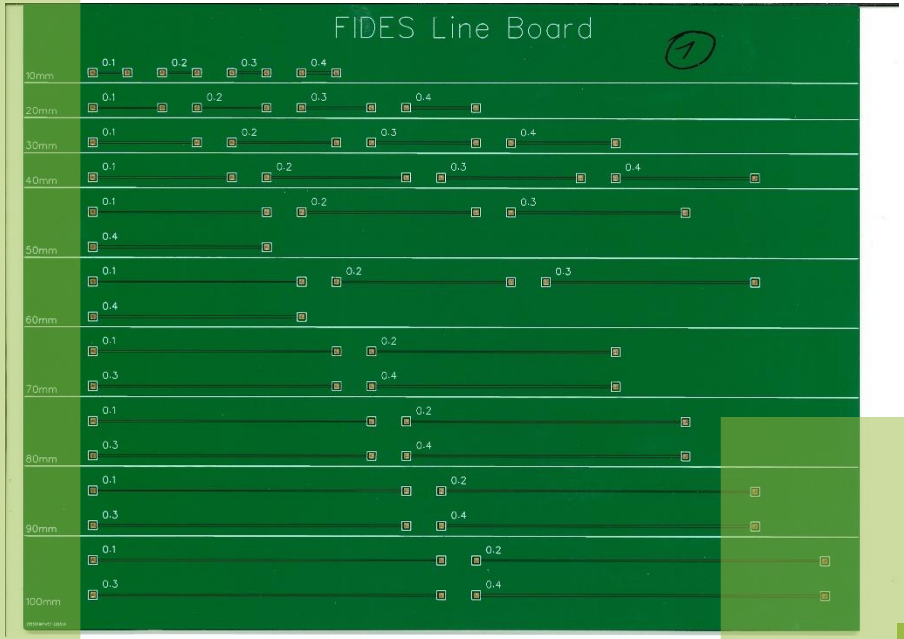
1	Introduction	3
2	SRAM	10
3	**PCB**	**18**
4	Conclusion	24

Overview

Measurement

Measure Resistances

Measure Capacitances



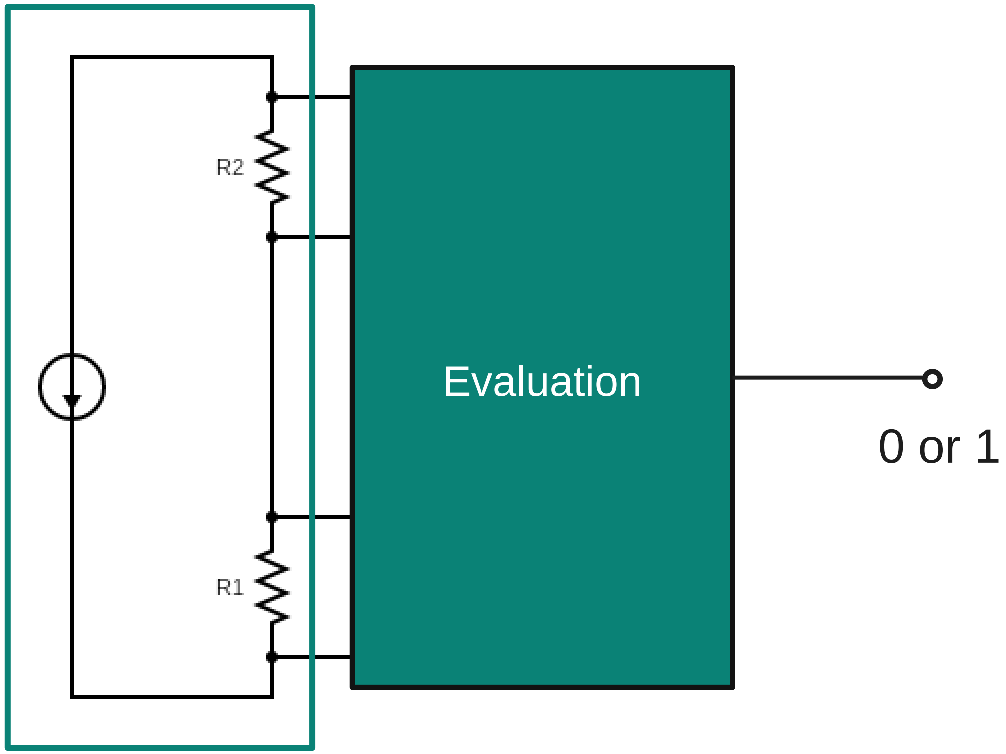
Data Analysis

Inspect Resistances

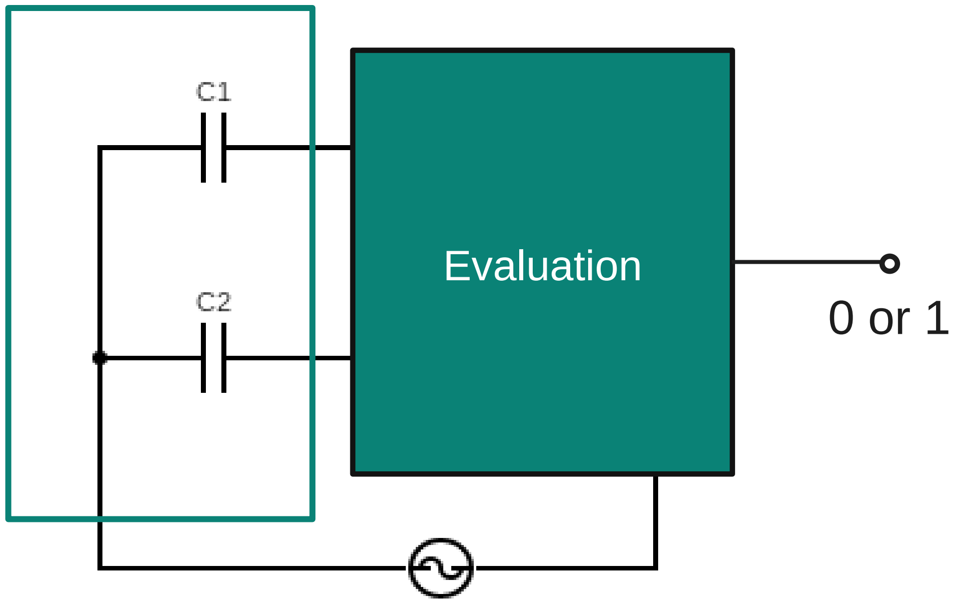
Inspect Capacitances

Physical Model Generation

R1 < R2 or
R1 > R2

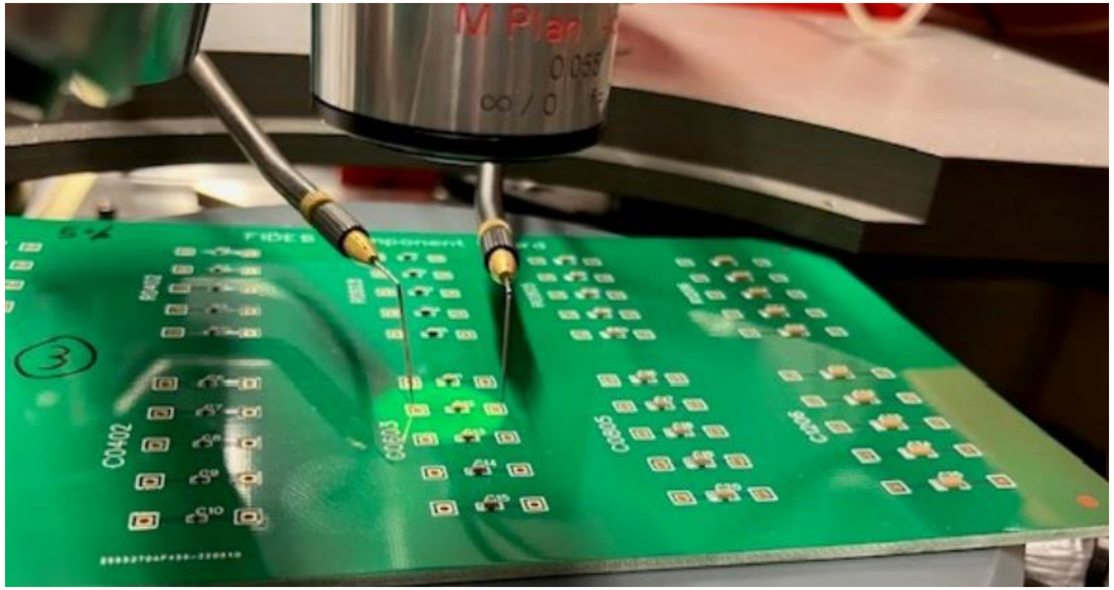


C1 < C2 or
C1 > C2



Resistance Measurement: Electrical

Method	Resolution	Cost
Laboratory set-up (resistance) (Keithley Model 4200, KS PM8, 407B simac tips)	0.1 µΩ, -	∼ 100 000€



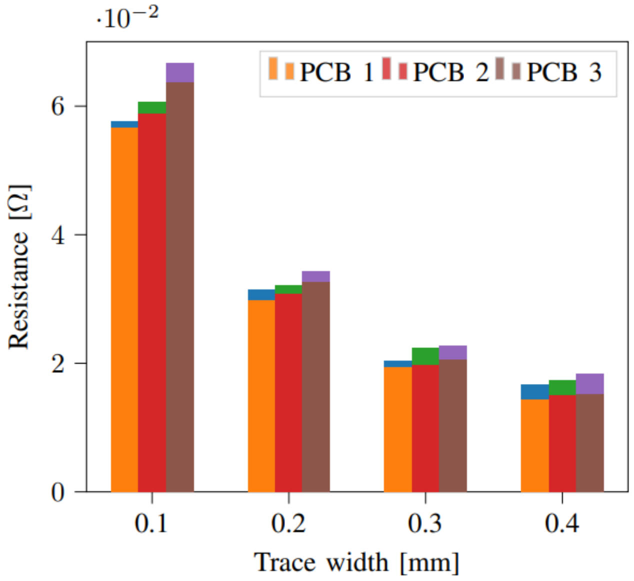
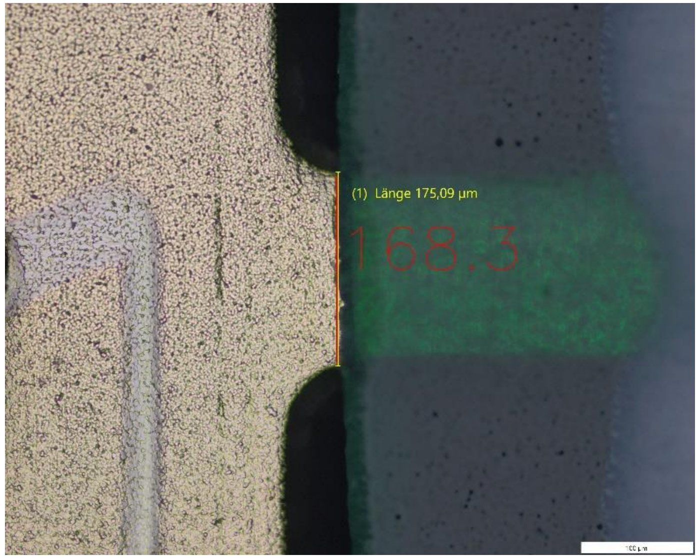
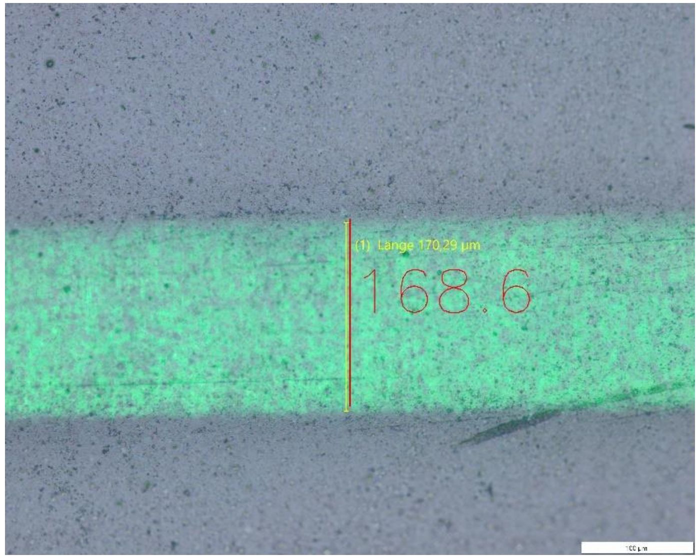
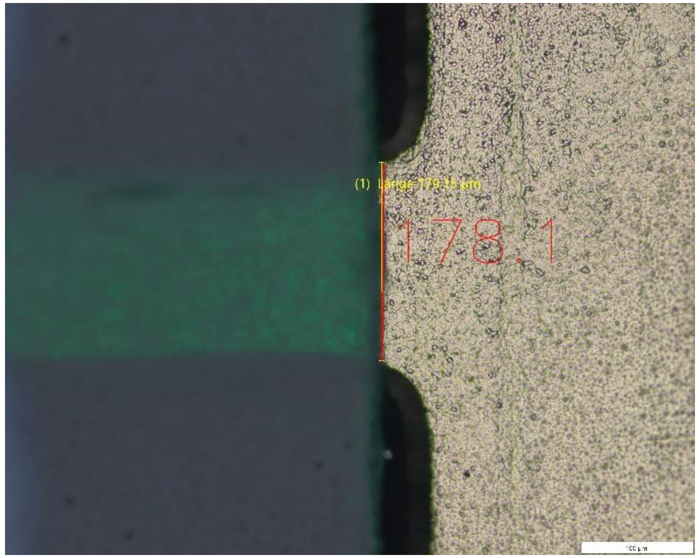


Fig. 14: Electrical resistance measurement results.

Resistance Measurement: Optical







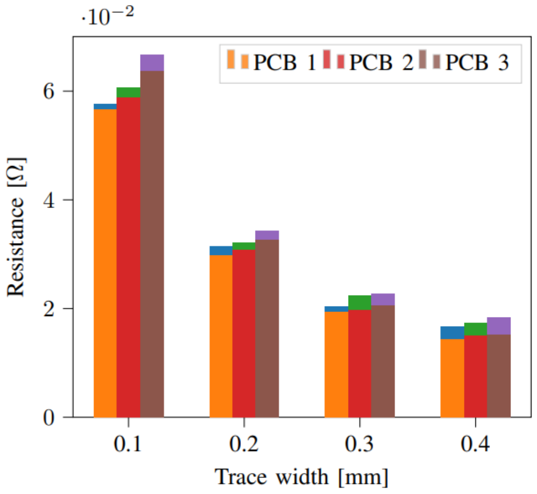


Fig. 14: Electrical resistance measurement results.

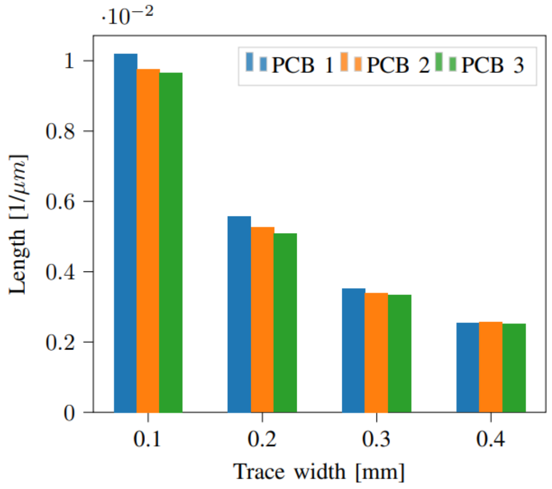
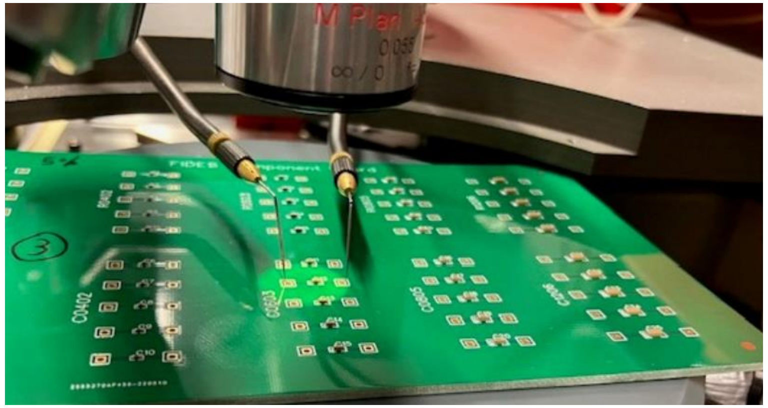


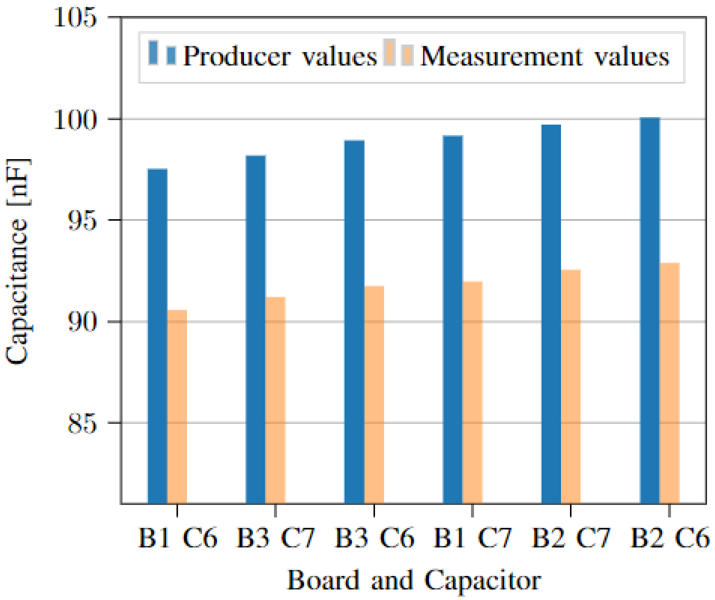
Fig. 15: Geometrical max width measurement results.

Both the **electrical** and the **optical** measurement **correlate** with the manufacturer values

Results of Capacitance Measurement: Electrical

Method	Resolution	Cost
Laboratory set-up (capacitance) (Andeen Hagerling 2700A, KS PM8, HM 7044, 407B simac tips)	-, 0.1 nF	∼ 80 000€





The measurement **correlates** with the manufacturer values

Table of contents

1	Introduction	3
2	SRAM	10
3	PCB	18
4	**Conclusion**	**24**

Conclusion

We propose a methodology to **transfer hardware physics and responses into a physical model**

Evaluation capability of hardware primitives' **correlates to financial expenditure**

Hardware design of fingerprints must take **reverse engineering / physical inspection** capabilities into account infineon

Literature

[1] Merli, Dominik / Schuster, Dieter / Stumpf, Frederic / Sigl, Georg; **Side-Channel Analysis of PUFs and Fuzzy Extractors**; 2011; Trust and Trustworthy Computing; Springer Berlin Heidelberg; p. 33-47

[2] Merli, Dominik / Heyszl, Johann / Heinz, Benedikt / Schuster, Dieter / Stumpf, Frederic / Sigl, Georg; **Localized electromagnetic analysis of RO PUFs**; 2013-06; 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)

[3] Tajik, Shahin / Dietz, Enrico / Frohmann, Sven / Seifert, Jean-Pierre / Nedospasov, Dmitry / Helfmeier, Clemens / Boit, Christian / Dittrich, Helmar; **Physical Characterization of Arbiter PUFs**; 2014; Advanced Information Systems Engineering

[4] Nedospasov, Dmitry / Seifert, Jean-Pierre / Helfmeier, Clemens / Boit, Christian; **Invasive PUF Analysis**; 2013-08; 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography; IEEE; p. 30-38

[5] Helfmeier, Clemens / Boit, Christian / Nedospasov, Dmitry / Seifert, Jean-Pierre; **Cloning Physically Unclonable Functions**; 2013-06; 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)

[6] Cortez, Mafalda / Dargar, Apurva / Hamdioui, Said / Schrijen, Geert-Jan; **Modeling SRAM start-up behavior for Physical Unclonable Functions**; 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT); IEEE

Reasons for Manufacturing Variations

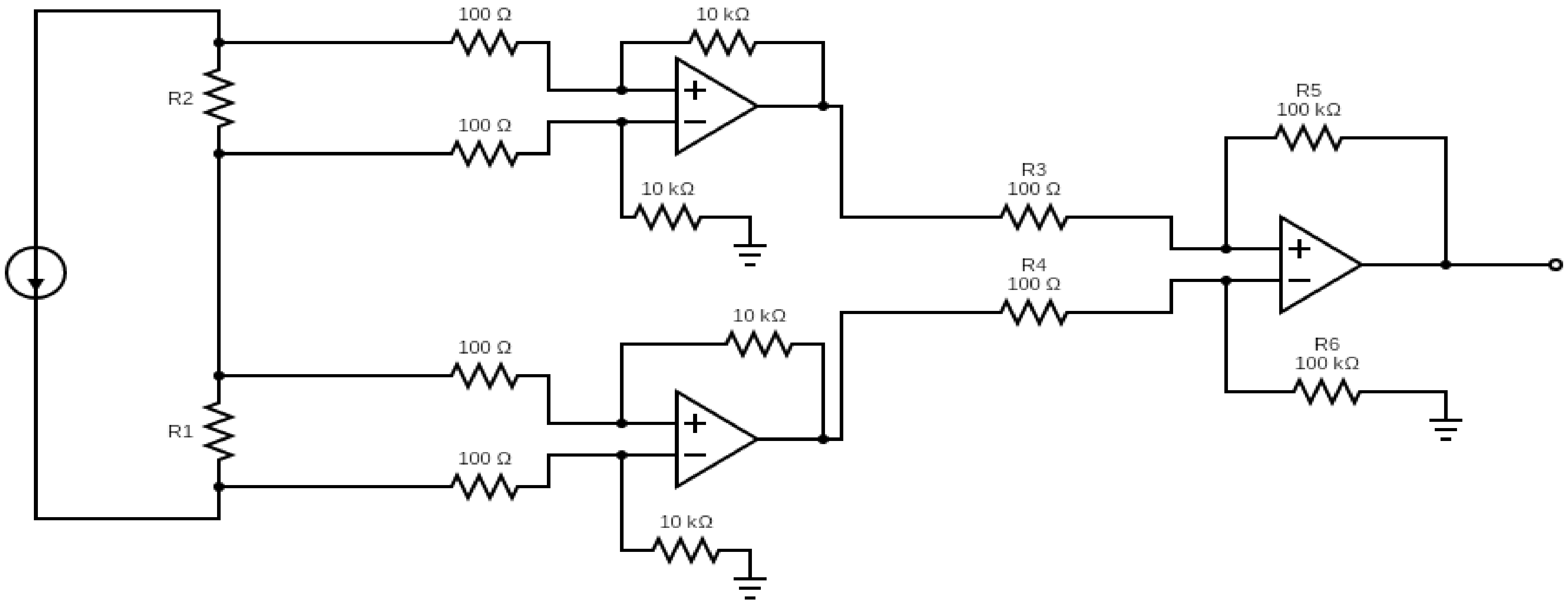
- Variations in Si0_2 Thickness
- Alignment of mask
- Variations in exposure / angle
- Variations due to distribution of etch liquid
- Variations in diffusion

→ Process Parameters affected by Variations (Drennan et al. 2003):

- Electron / Hole Mobility μn/ μp
- Flatband Voltage Vfb
- Substrate dopant concentration Nsub
- Gate oxide thickness tOx
- Length offset ΔL, Width offset ΔW, Short channel effect, Narrow width effect
- Source/drain sheet resistance

On-board measurement

- Evaluate the difference by operational amplifiers
- First differential amplifiers:
  - Put the voltage over R1/R2 to an single-ended output
- Second differential amplifier:
  - Amplify the difference to positive / negative value
- Gain is determined by R5/R3 (if R3=R4 and R5=R6)



On-board measurement

- Evaluate the difference by a schering bridge

- Difference of capacitance defines current flow through R1 resistor
- Operational amplifier increases this voltage
- Xor gate checks if signals are in phase
  - Produce stable 0/1 output