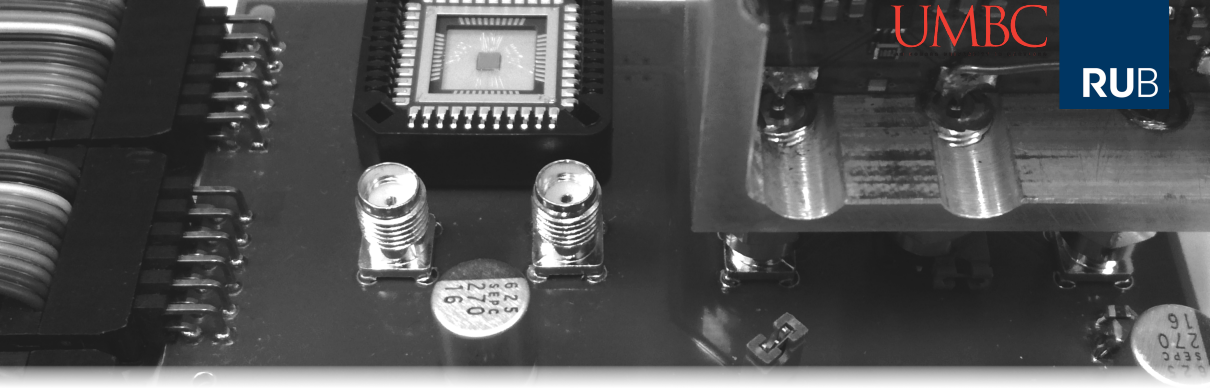


RUHR-UNIVERSITÄT BOCHUM

Exploring the Effect of Device Aging on Static Power Analysis Attacks

Naghmeh Karimi[1], Thorben Moos[2] and Amir Moradi[2]

[1] University of Maryland, Baltimore County, USA

[2] Ruhr University Bochum, Horst Görtz Institute for IT Security, Germany

28 August 2019

DFG Deutsche Forschungsgemeinschaft

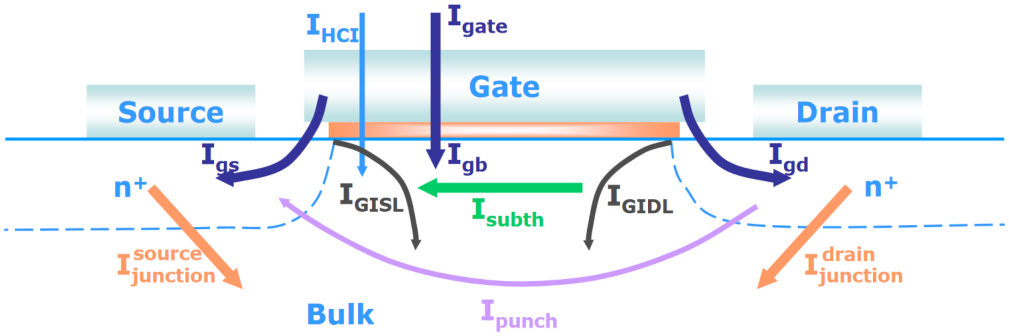
Outline

Section 1

Introduction

Static Leakage Currents

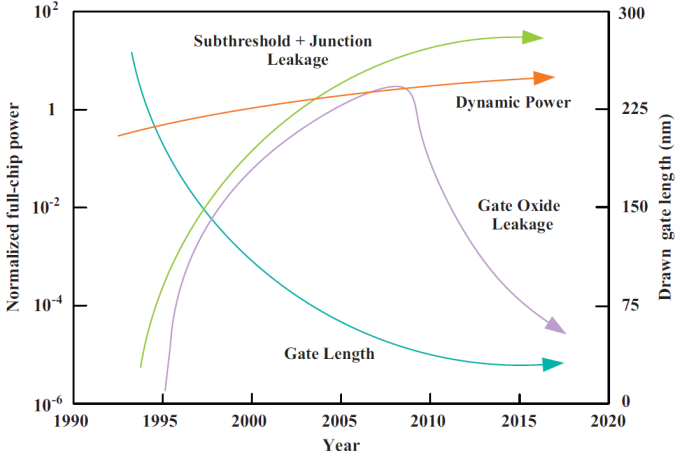
Introduction



Source: Leakage Models for High Level Power Estimation, Domenik Helms, PhD thesis, Carl von Ossietzky Universität Oldenburg, 2009

Static Leakage Development

Introduction

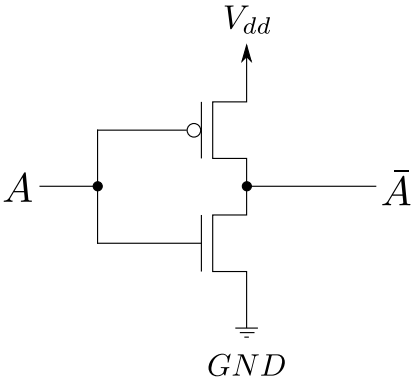


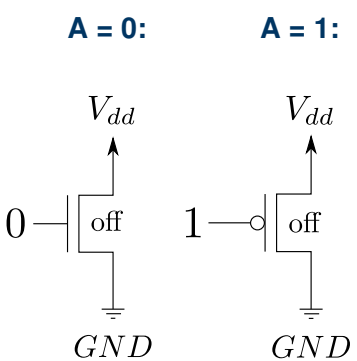
Source: Impact of technology scaling on leakage power in nano-scale bulk CMOS digital standard cells, Z. Abbas and M. Olivieri, Microelectronics Journal, Vol. 45 Issue 2, 2014

Data Dependency of CMOS Standard Cells: NOT Gate

Introduction

Formation of inactive transistors across power supply path for different inputs*:



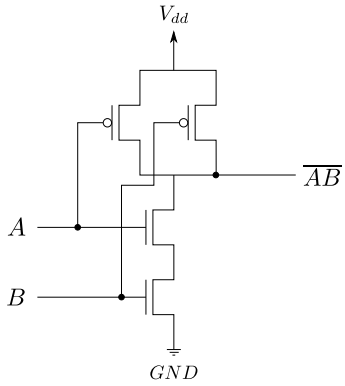


*Active (conducting) transistors are replaced by ideal wires in this simplification.

Data Dependency of CMOS Standard Cells: NAND Gate

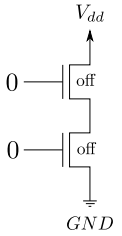
Introduction

Formation of inactive transistors across power supply path for different inputs*:

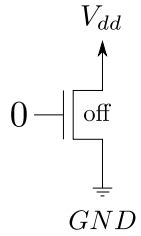


A = 0:

B = 0:



B = 1:

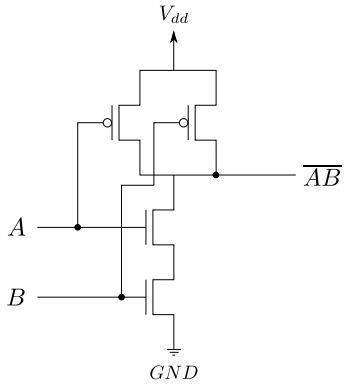


*Active (conducting) transistors are replaced by ideal wires in this simplification.

Data Dependency of CMOS Standard Cells: NAND Gate

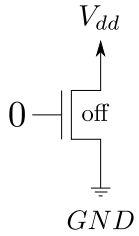
Introduction

Formation of inactive transistors across power supply path for different inputs*:

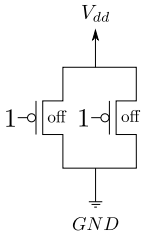


A = 1:

B = 0:



B = 1:



*Active (conducting) transistors are replaced by ideal wires in this simplification.

Device Aging

Introduction

- Device aging is an important failure mechanism in nanoscale designs that jeopardizes the *reliability* of electronic devices
- Performance of nanoscale CMOS circuits degrades over their lifetime

$\Rightarrow$ **Ultimate Failure**

Device Aging

Introduction

Circuit Aging Mechanisms

- Time dependent dielectric Breakdown (TDDB)

Device Aging

Introduction

Circuit Aging Mechanisms

- Time dependent dielectric Breakdown (TDDB)
- Electromigration (EM)

Device Aging

Introduction

Circuit Aging Mechanisms

- Time dependent dielectric Breakdown (TDDB)
- Electromigration (EM)
- Bias Temperature-Instability (BTI)

Device Aging

Introduction

Circuit Aging Mechanisms

- Time dependent dielectric Breakdown (TDDB)
- Electromigration (EM)
- Bias Temperature-Instability (BTI)
- Hot Carrier Injection (HCI)

Aging Mechanisms

Introduction

Negative Bias Temperature Instability (NBTI)

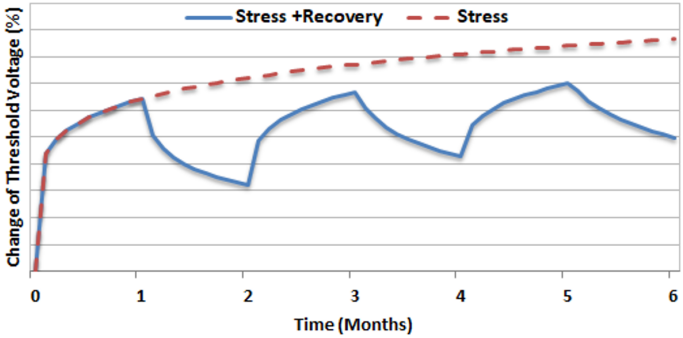
- **Cause:** Holes creating traps between Si-SiO2 and substrate
- **Impact:** **Vth increase**, especially for PMOS transistors

Hot Carrier Injection (HCI)

- **Cause:** Electrons colliding with the gate oxide (rather than going only to the conduction channel between source and drain)
- **Impact:** **Vth increase**, especially for NMOS transistors

Vth increase caused by NBTI

Introduction

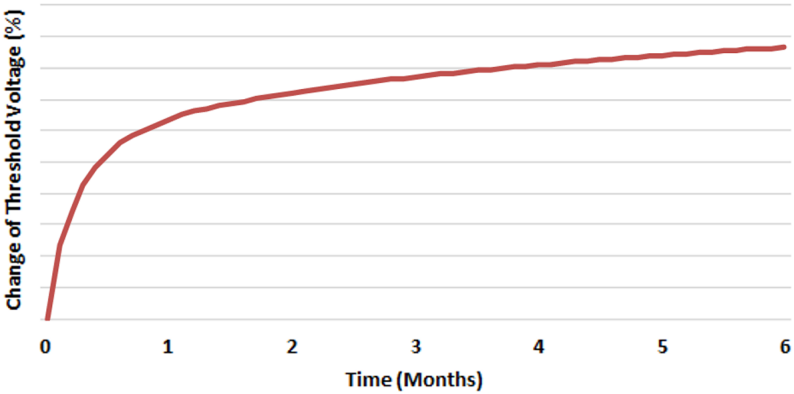


$$\Delta V_{th_{st}} = A_{NBTI} \cdot t_{ox} \cdot \sqrt{C_{ox}(V_{dd} - V_{th})} \cdot e^{\left(\frac{V_{dd}-V_{th}}{t_{ox} \times E_0} - \frac{E_a}{k \times T}\right)} \cdot t_{st}^{0.25}$$

$$\Delta V_{th_{NBTI}} = \Delta V_{th_{st}} \times \left(1 - \sqrt{\eta \frac{t_{rec}}{t_{rec} + t_{st}}}\right)$$

Vth increase caused by HCI

Introduction



$$\Delta V_{th_{HCI}} = A_{HCI} \cdot \alpha \cdot f \cdot e^{\frac{V_{dd}-V_{th}}{t_{ox} \cdot E_1}} \cdot t^{0.5}$$

Impact of Aging on Vth of MOSFETs

Introduction

- The threshold voltage of a MOSFET can be used as a parameter to regulate the trade-off between its propagation delay and its leakage current

Impact of Aging on Vth of MOSFETs

Introduction

- The threshold voltage of a MOSFET can be used as a parameter to regulate the trade-off between its propagation delay and its leakage current
- Devices with a high threshold voltage are slower and can be used where timing is not critical in order to reduce the leakage current

Impact of Aging on Vth of MOSFETs

Introduction

- The threshold voltage of a MOSFET can be used as a parameter to regulate the trade-off between its propagation delay and its leakage current
- Devices with a high threshold voltage are slower and can be used where timing is not critical in order to reduce the leakage current
- By aging a CMOS circuit the threshold voltage of devices increases and the design starts to fail timing

Impact of Aging on Vth of MOSFETs

Introduction

- The threshold voltage of a MOSFET can be used as a parameter to regulate the trade-off between its propagation delay and its leakage current
- Devices with a high threshold voltage are slower and can be used where timing is not critical in order to reduce the leakage current
- By aging a CMOS circuit the threshold voltage of devices increases and the design starts to fail timing
- The aging procedure can be accelerated by applying increased supply voltages and temperatures

Impact of Aging on Vth of MOSFETs

Introduction

- The threshold voltage of a MOSFET can be used as a parameter to regulate the trade-off between its propagation delay and its leakage current
- Devices with a high threshold voltage are slower and can be used where timing is not critical in order to reduce the leakage current
- By aging a CMOS circuit the threshold voltage of devices increases and the design starts to fail timing
- The aging procedure can be accelerated by applying increased supply voltages and temperatures
- The input-dependent leakage behavior of CMOS circuits changes non-linearly, also depending on the switching activity during aging (i.e., high vs. low activity)

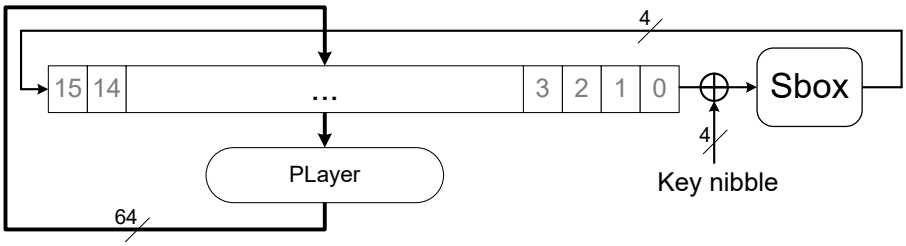
Section 2

Target

PRESENT Architecture

Target

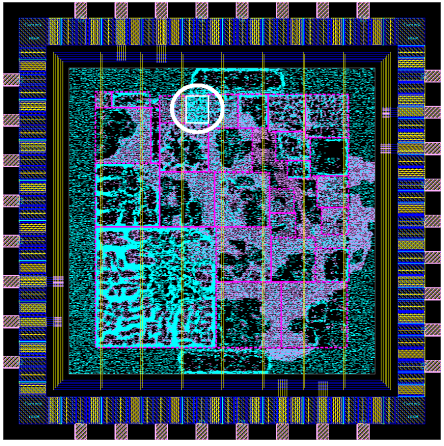
Nibble-serial PRESENT implementation with single Sbox instance:



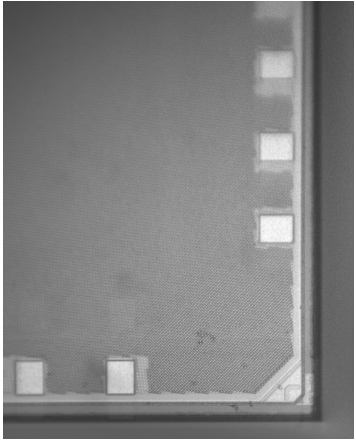
65 nm ASIC

Target

Chip Layout:



Corner of the Die:



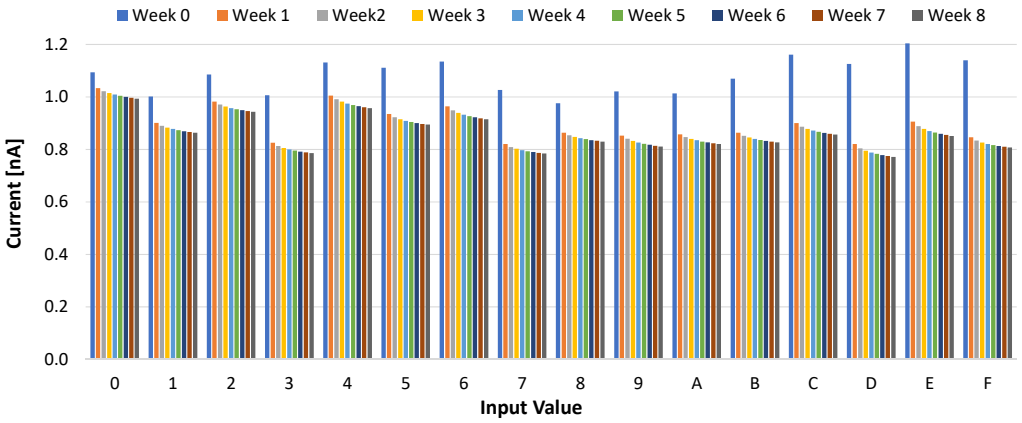
Section 3

Simulation Results

Simulated Input Dependency of Sbox Instance

Simulation Results

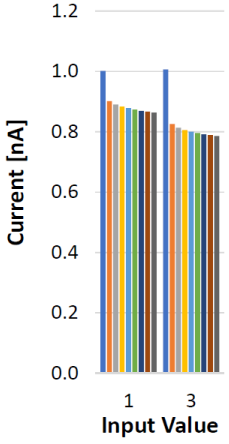
Accelerated aging at 90°C and 1.416 V for 8 weeks (acceleration factor ≈ 80):



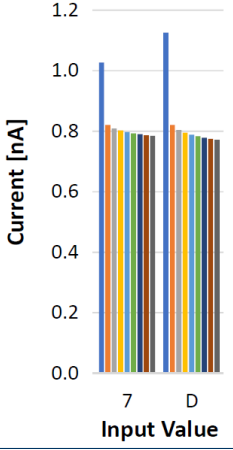
Simulated Input Dependency of Sbox Instance

Simulation Results

Increased distinguishability after aging:



Decreased distinguishability after aging:



Simulated Input Dependency of Sbox Instance

Simulation Results

- Input dependency of the Sbox instance changes completely during the aging process (already after the first week of accelerated aging)

Simulated Input Dependency of Sbox Instance

Simulation Results

- Input dependency of the Sbox instance changes completely during the aging process (already after the first week of accelerated aging)
- Absolute leakage currents decrease

Simulated Input Dependency of Sbox Instance

Simulation Results

- Input dependency of the Sbox instance changes completely during the aging process (already after the first week of accelerated aging)
- Absolute leakage currents decrease
- Input dependent variance between the leakage currents decreases as well

Simulated Input Dependency of Sbox Instance

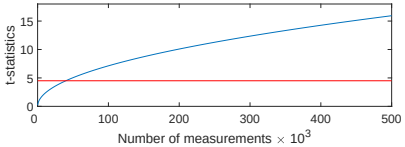
Simulation Results

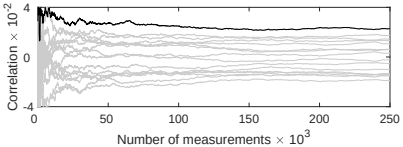
- Input dependency of the Sbox instance changes completely during the aging process (already after the first week of accelerated aging)
- Absolute leakage currents decrease
- Input dependent variance between the leakage currents decreases as well
- Static power side-channel attacks should become more difficult on aged devices

Simulation: T-test and CPA on HW of Sbox Output

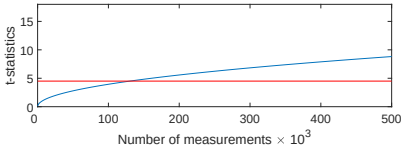
Simulation Results

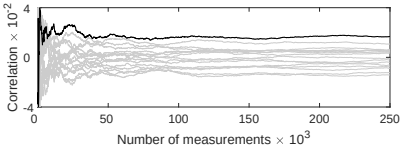
Original device:



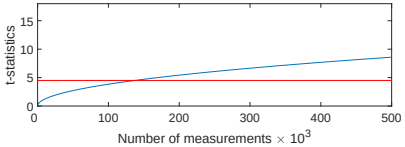


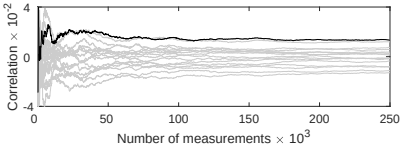
4 weeks aged:





8 weeks aged:



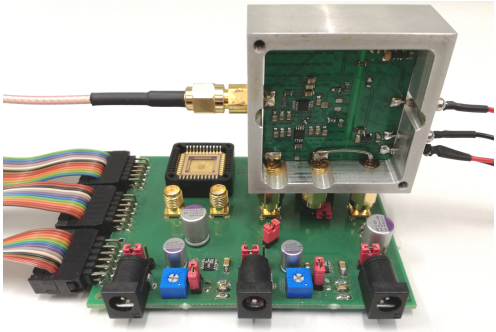


Section 4

Practical Results

Setup

Measurement Board:

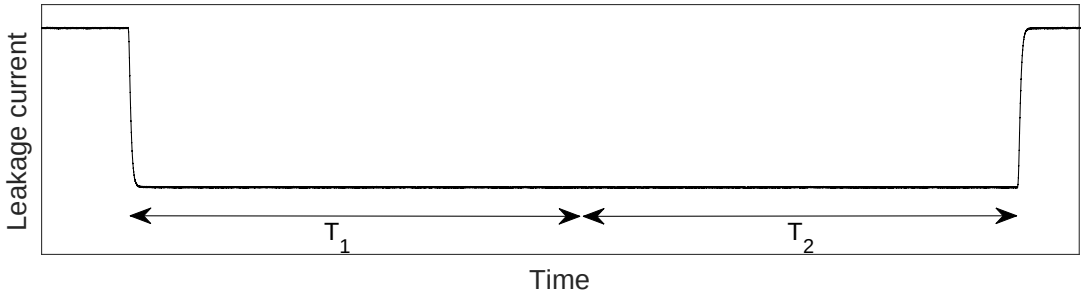


Climate Chamber and Scope:

Sample Measurement

Setup

Sample Measurement Procedure with Stopping the Clock Signal:



Experiments

Practical Results

- We have aged **two** distinct fresh samples of the 65 nm ASIC at 90°C and 1.416 V for 8 consecutive weeks

Experiments

Practical Results

- We have aged **two** distinct fresh samples of the 65 nm ASIC at 90°C and 1.416 V for 8 consecutive weeks
- At 0 (initial state), 4 and 8 weeks of aging we have measured the susceptibility of the PRESENT implementation to static power attacks (at 20°C and 1.2 V)

Experiments

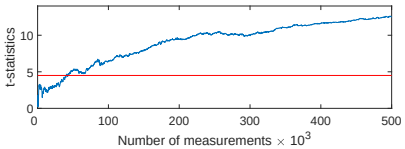
Practical Results

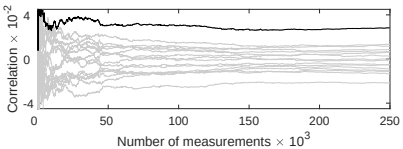
- We have aged **two** distinct fresh samples of the 65 nm ASIC at 90°C and 1.416 V for 8 consecutive weeks
- At 0 (initial state), 4 and 8 weeks of aging we have measured the susceptibility of the PRESENT implementation to static power attacks (at 20°C and 1.2 V)
- The setup (esp. the board) to operate the ASICs while aging was distinct from the one for measurements in order to avoid that setup aging influences the results

Sample 1: T-test and CPA on HW of Sbox Output

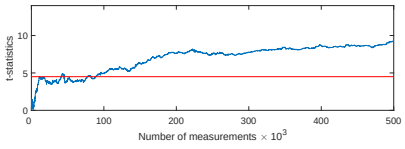
Practical Results

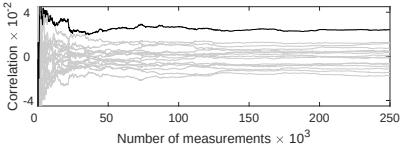
Original device:



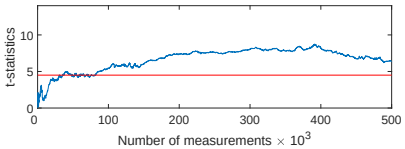


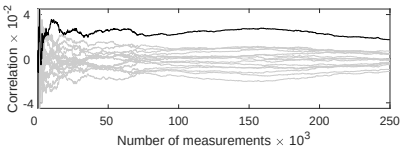
4 weeks aged:





8 weeks aged:

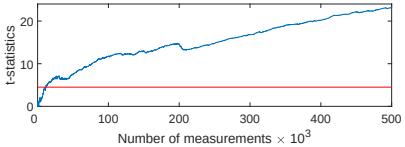


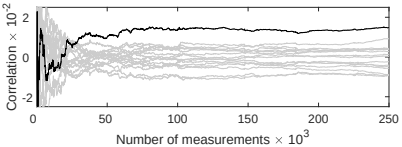


Sample 2: T-test and CPA on HW of Sbox Output

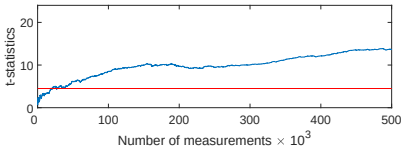
Practical Results

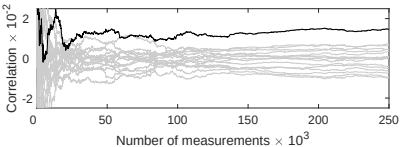
Original device:



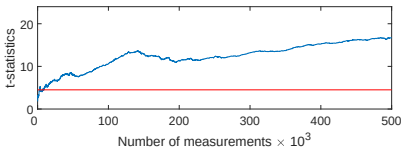


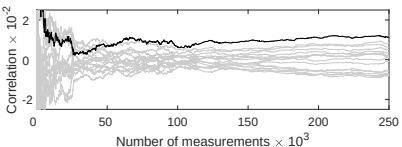
4 weeks aged:





8 weeks aged:





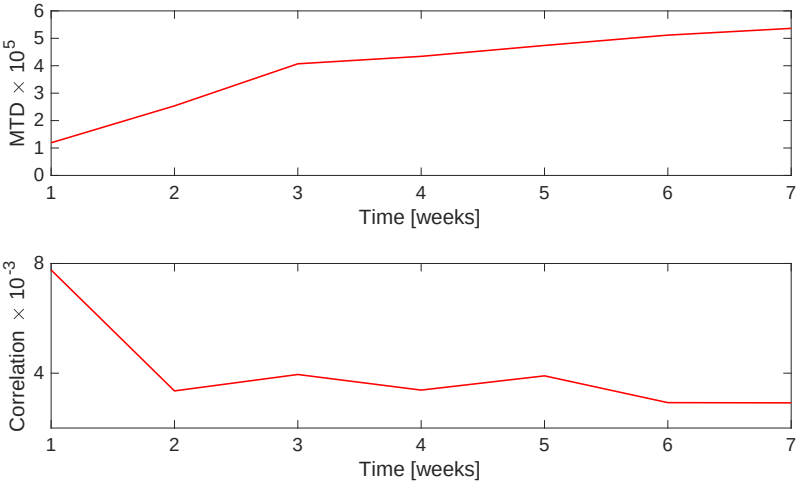
Comparison: Simulation vs. Experiments

Practical Results

Experiment	Stage of aging	t-stat.	Corr. coeff.	Avg. total curr.
Simulation	Original device	15.941	0.02283	-
Simulation	4 weeks aged	8.818	0.01682	-
Simulation	8 weeks aged	8.590	0.01340	-
Measurements sample 1	Original device	12.514	0.02801	8.6 µA
Measurements sample 1	4 weeks aged	9.299	0.02410	8.0 µA
Measurements sample 1	8 weeks aged	6.359	0.01718	7.5 µA
Measurements sample 2	Original device	23.251	0.01472	7.5 µA
Measurements sample 2	4 weeks aged	13.647	0.01465	7.2 µA
Measurements sample 2	8 weeks aged	16.710	0.01147	6.9 µA

Simultaneous Aging and Measuring - 150 nm Chip

Practical Results



Section 5

Conclusion

Conclusion

- Leakage currents of CMOS devices are reduced due to aging mechanisms

Conclusion

- Leakage currents of CMOS devices are reduced due to aging mechanisms
- Static power side-channel attacks require more traces to succeed

Conclusion

- Leakage currents of CMOS devices are reduced due to aging mechanisms
- Static power side-channel attacks require more traces to succeed
- The data dependency of combinatorial circuits changes completely

Conclusion

- Leakage currents of CMOS devices are reduced due to aging mechanisms
- Static power side-channel attacks require more traces to succeed
- The data dependency of combinatorial circuits changes completely
- Static power results taken from different phases of measurements do not correspond to each other

Conclusion

- Leakage currents of CMOS devices are reduced due to aging mechanisms
- Static power side-channel attacks require more traces to succeed
- The data dependency of combinatorial circuits changes completely
- Static power results taken from different phases of measurements do not correspond to each other
- Especially relevant when conducting attacks at increased temperatures and supply voltages, as it fuels device degradation significantly

Conclusion

- Leakage currents of CMOS devices are reduced due to aging mechanisms
- Static power side-channel attacks require more traces to succeed
- The data dependency of combinatorial circuits changes completely
- Static power results taken from different phases of measurements do not correspond to each other
- Especially relevant when conducting attacks at increased temperatures and supply voltages, as it fuels device degradation significantly
- Future static power experiments should state the age of devices at all stages

Thanks for your attention.

Any questions?