UCLouvain Institute of Information and Communication Technologies, Electronics and Applied Mathematics (ICTEAM)

Evolution of a Side Channel

Benchmarking the Static Power Vulnerability of Four CMOS Generations

Dr.-Ing. Thorben Moos

Crypto Group, ICTEAM Institute, UCLouvain, Louvain-la-Neuve, Belgium.

June 2nd, 2023

European Research Council

Acknowledgments

- Most of the work presented in this talk has been accomplished during my PhD at Ruhr-Universität Bochum (RUB) under supervision of Prof. Dr. Amir Moradi
- Funded by the German Research Foundation (Deutsche Forschungsgemeinschaft) through project "NaSCA: Nano-Scale Side-Channel Analysis - Physical Security for Next-Generation CMOS ICs" and through the Cluster of Excellence "CASA - Cyber Security in the Age of Large-Scale Adversaries".
- NaSCA: `https://gepris.dfg.de/gepris/projekt/271752544`
- CASA: `https://gepris.dfg.de/gepris/projekt/390781972`

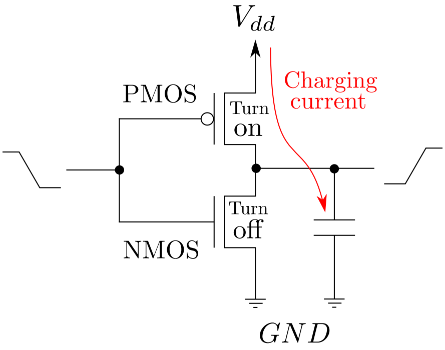
Section 1

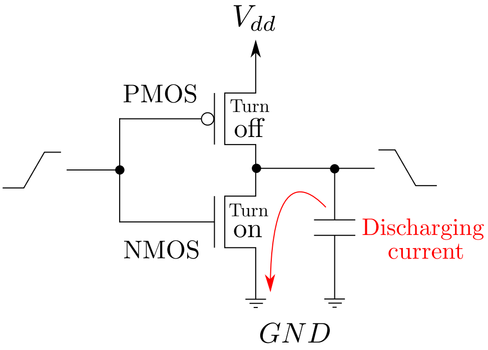
Introduction

Energy Consumption in Computing Hardware

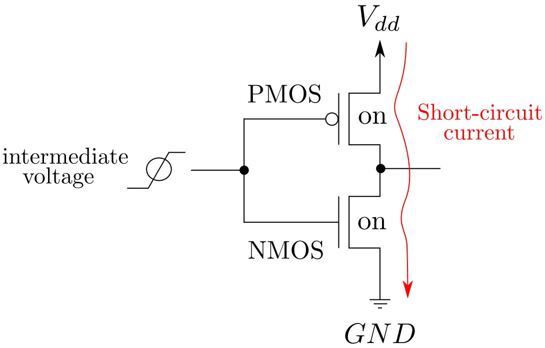
- Digital integrated circuits are typically modeled as state machines
- State transitions are triggered by events such as the edges of a clock signal
- Whenever a state transition occurs, energy is consumed as electric charges are moved
- The motion of electric charges creates an electromagnetic field

Charging/Discharging Currents in CMOS Gates





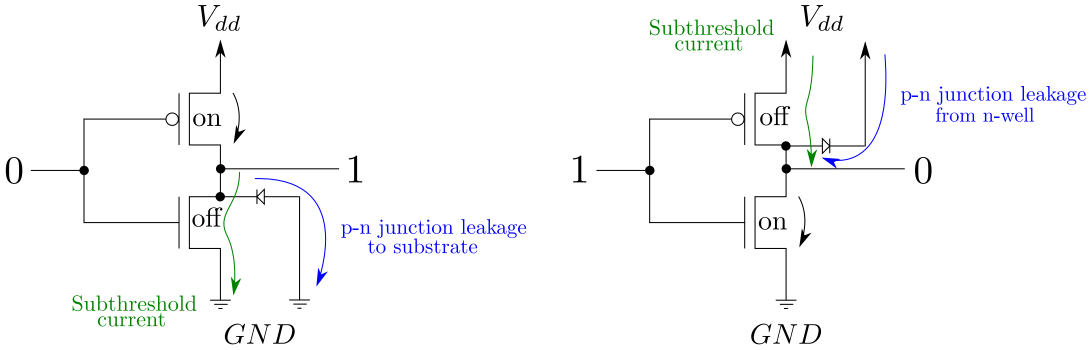
Short-Circuit Current in CMOS Gates



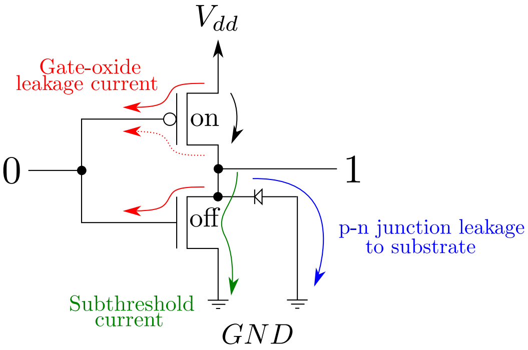
Energy Consumption in Computing Hardware

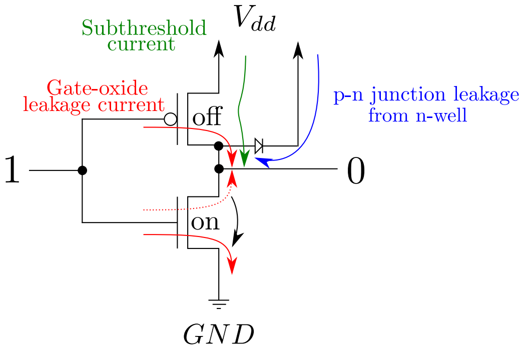
- Is that all?
- Is energy only consumed if state transitions (= active computations) occur?
- NO!

Leakage Currents in CMOS Gates

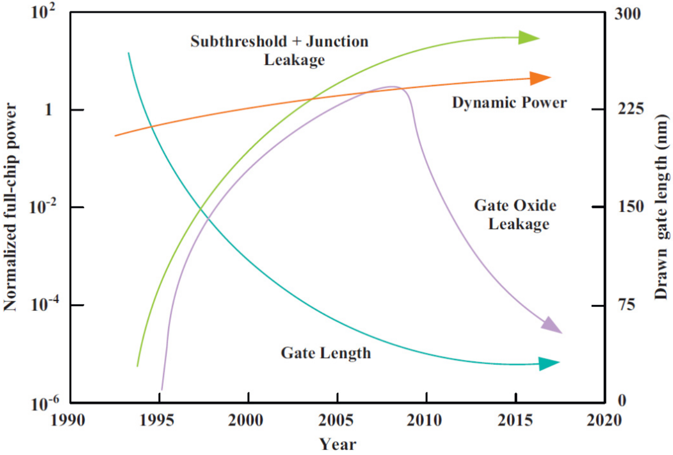


Leakage Currents in CMOS Gates





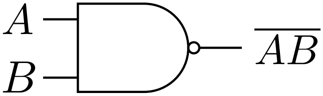
Leakage Development



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 Leakage Currents

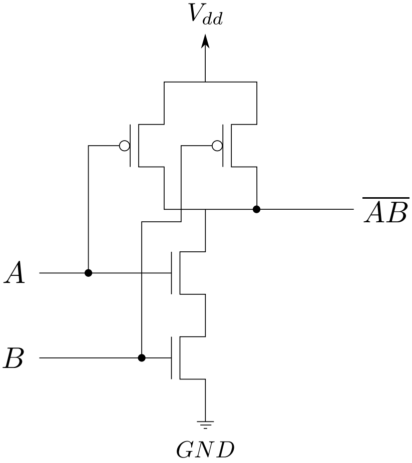
SPICE simulated leakage current of a 2-input `NAND` gate in 22 nm technology:

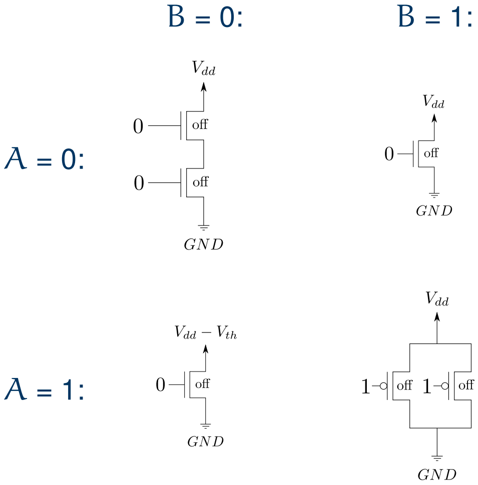


A	B	Leakage Current [nA]
0	0	72.09
0	1	96.93
1	0	46.87
1	1	144.01

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 Leakage Currents




B = 0:

B = 1:

A = 0:

A = 1:

Data-Dependency of Leakage Currents

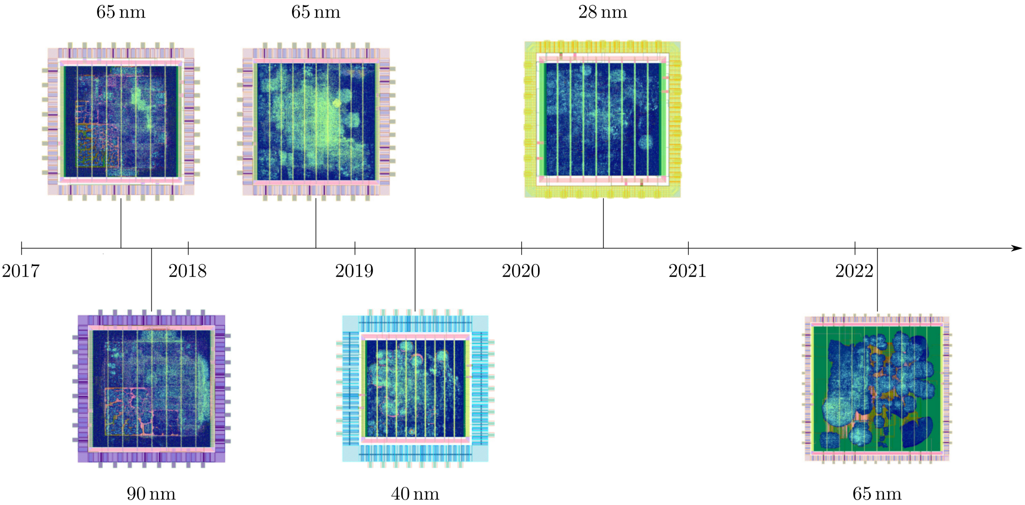
- The standby power of CMOS chips silently leaks information to potential adversaries about internally stored and processed data
- Again, even data that is not currently processed (=actively computed upon) is leaked
- Measuring a stable/static state allows lower noise measurements
- Operating conditions can be manipulated to increase these leakage currents
- Leakage currents are known to increase significantly as the physical feature size of transistors decreases

- Does this become dangerous at some point?

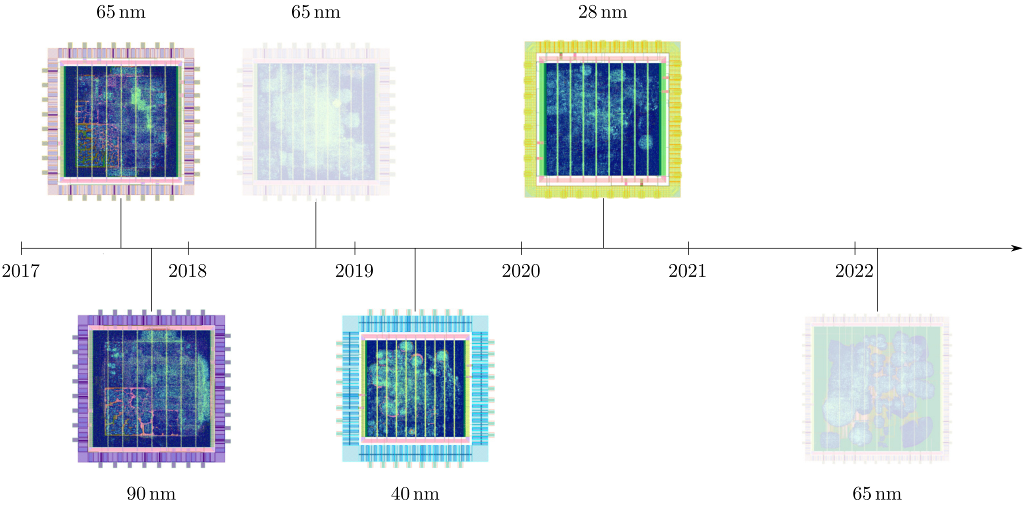
Section 2

Prototypes

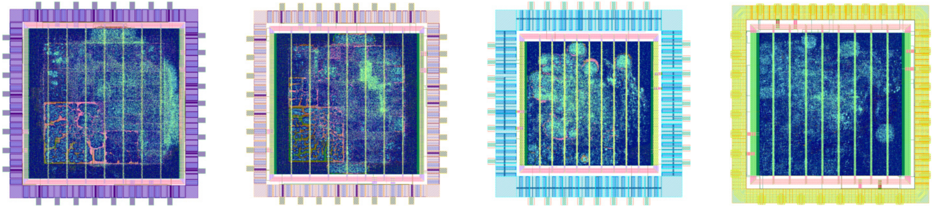
Digital IC Prototyping Timeline



Digital IC Prototyping Timeline



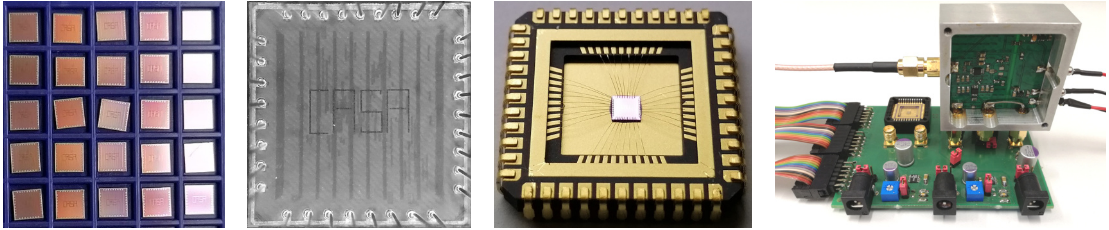
Selected ASIC Prototypes



	90 nm	65 nm	40 nm	28 nm	Sum
Area	3.834 mm^2	3.771 mm^2	2.826 mm^2	1.901 mm^2	12.332 mm^2
Standard Cell Area	2.089 mm^2	1.848 mm^2	1.052 mm^2	0.962 mm^2	5.951 mm^2
Number of Standard Cells	453 850	571 060	917 819	1 467 851	3 410 580
Unique Std. Cell Types	467	609	702	843	2621
IO voltage	2.5 V	2.5 V	2.5 V	1.8 V	-
Core voltage	1.2 V	1.2 V	1.1 V	0.9 V	-
Cost	12 100 €	13 220 €	17 640 €	18 270 €	61 230 €

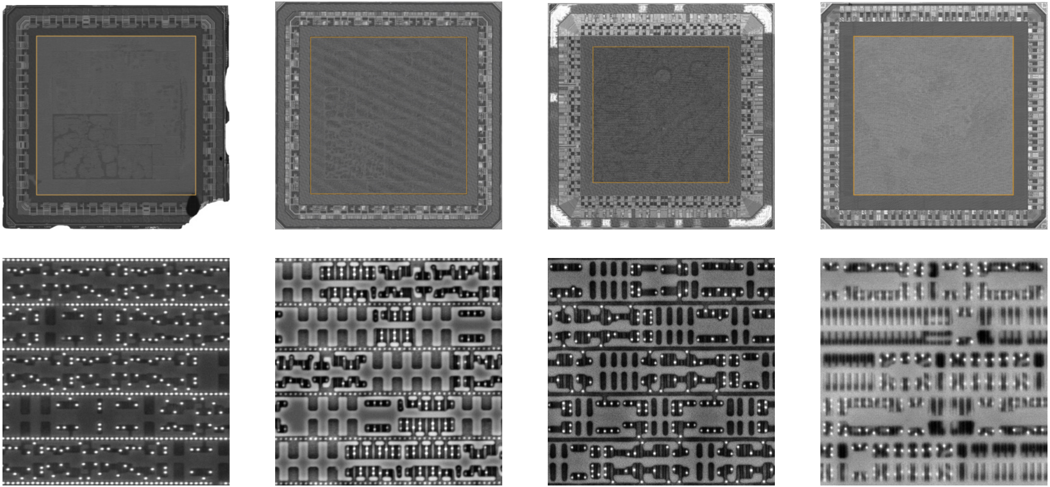
EUROPRACTICE low-cost MPW (mini@sic) fabrication prices

Chip Pictures



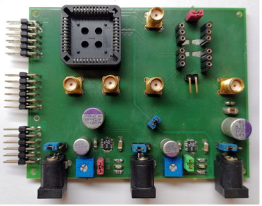
(a) Naked dies (b) Bonded die (c) Packaged die (d) Pack. die on PCB

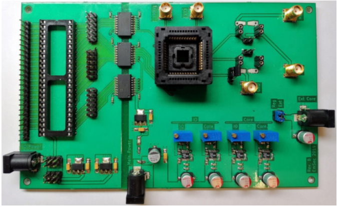
SEM Backside Images

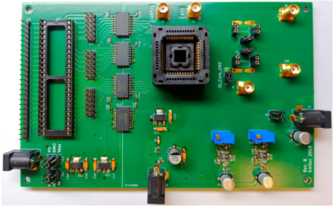


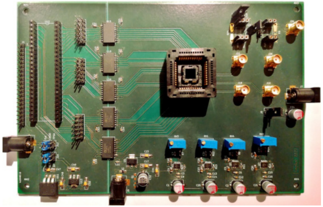
(a) 90 nm (b) 65 nm (c) 40 nm (d) 28 nm

Measurement Boards









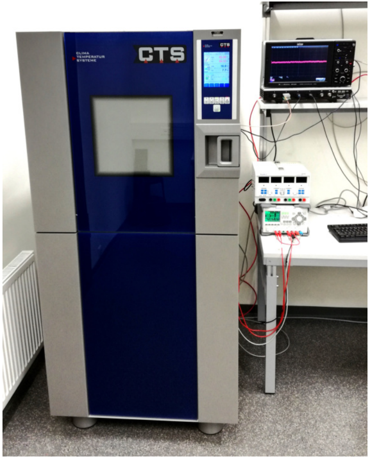
Section 3

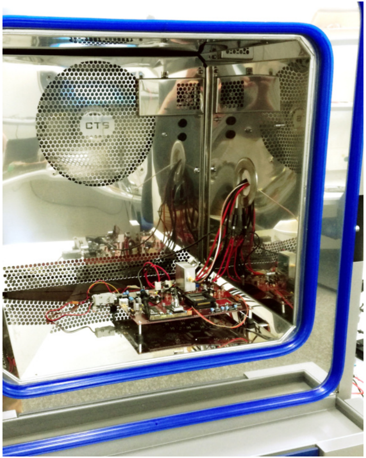
Setups

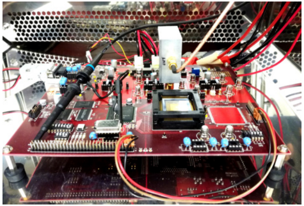
Challenges for a Static Power SCA Setup

- Low amplitude of the signal
- Very susceptible to temperature and voltage variations
- Targeted value needs to be stable for some time to accurately measure them (low clock frequency devices, devices with external clock, idling co-processors)
- Larger time consumption per measurement (milliseconds)

Static Power SCA Setup with Oscilloscope

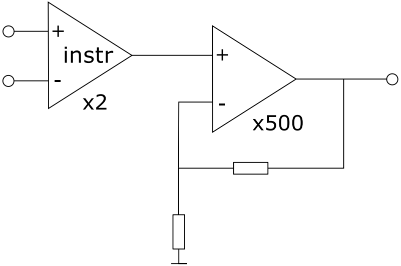


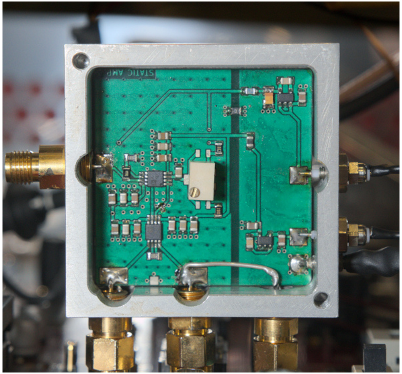




Static Power SCA Setup with Oscilloscope

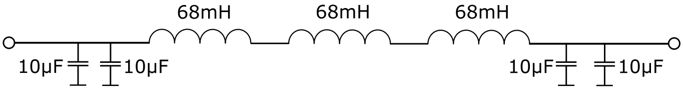
Custom Low-noise DC Amplifier with Gain of 1000:

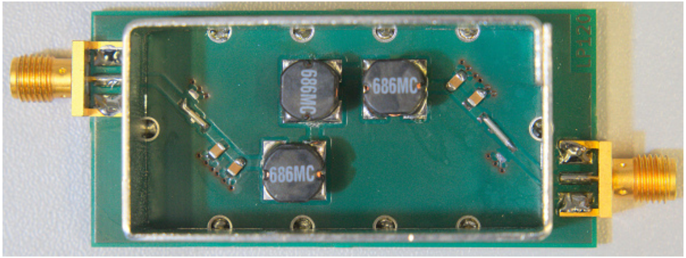




Static Power SCA Setup with Oscilloscope

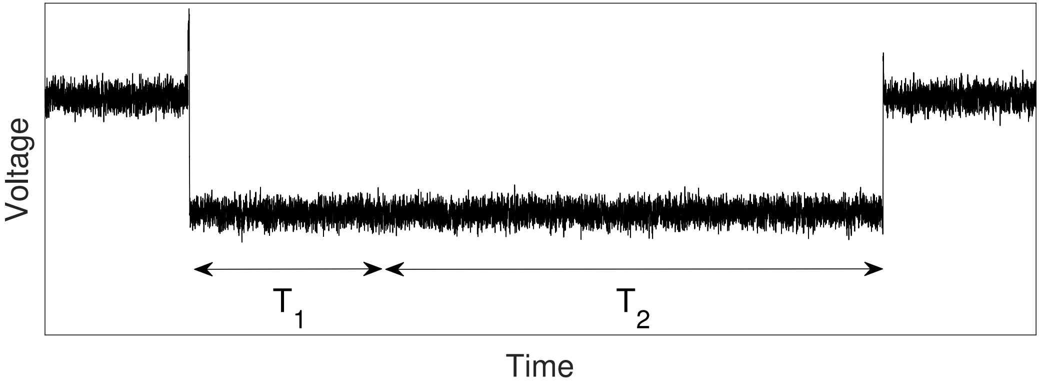
Third-order (Butterworth Pi) LC Low Pass Filter with Cutoff-Frequency of 100 Hz:





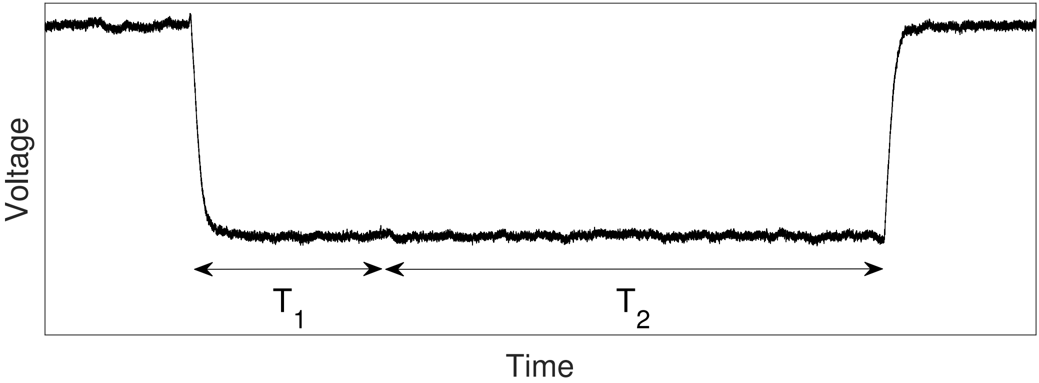
Static Power SCA Setup with Oscilloscope

Sample Trace without Low Pass Filter:

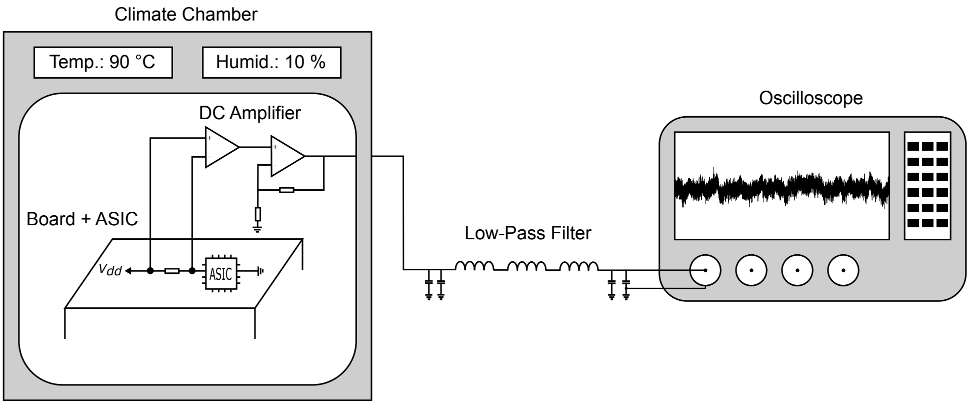


Static Power SCA Setup with Oscilloscope

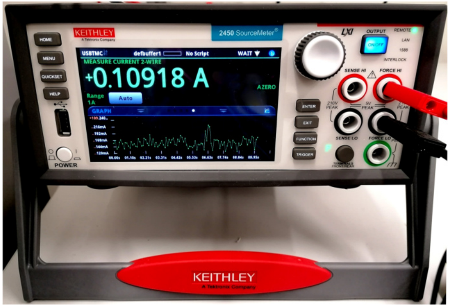
Sample Trace with Low Pass Filter:



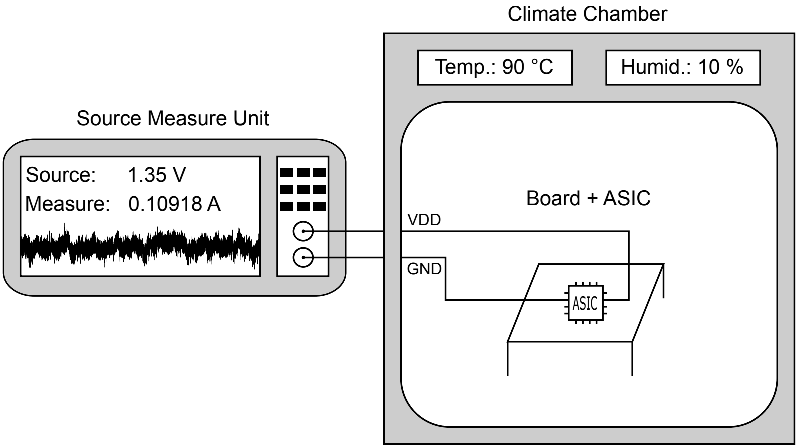
Static Power SCA Setup with Oscilloscope



Static Power SCA Setup with Sourcemeter

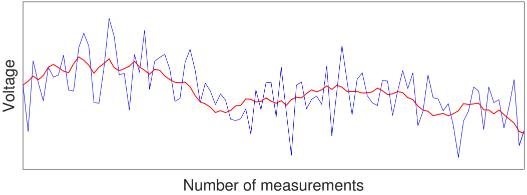


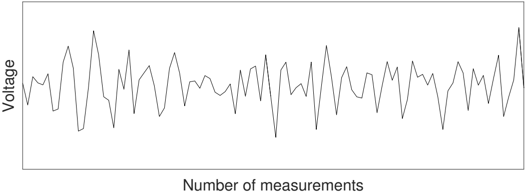
Static Power SCA Setup with Sourcemeter



Post-Processing in Both Cases

Moving Average Filter with adjustable Window Size:





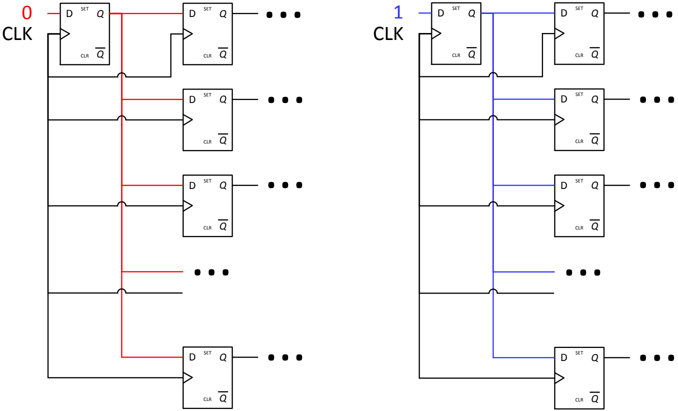
Section 4

Previous Inter-Chip Comparison

Target: 1024-bit HF Register

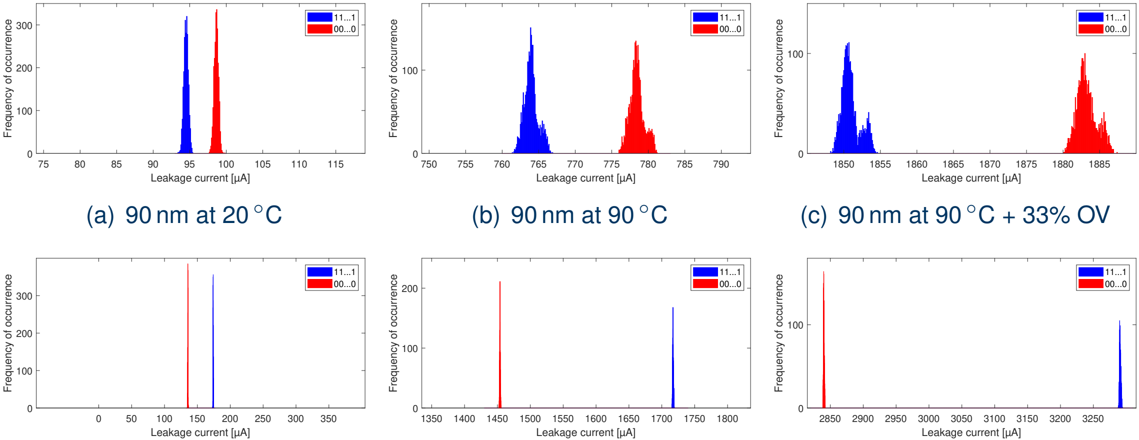
1024-bit HF Input Register

- filled either with 0s or 1s
- average fanout of 11



90 nm vs. 65 nm ASIC Comparison

Attention: x-axis scale is ×10 larger in the bottom row!



(a) 90 nm at 20 °C

(b) 90 nm at 90 °C

(c) 90 nm at 90 °C + 33% OV

(d) 65 nm at 20 °C

(e) 65 nm at 90 °C

(f) 65 nm at 90 °C + 33% OV

Data Dependency of HF-Register – 90 nm vs. 65 nm

Technology	Voltage	Temp.	Diff. of Means	Avg. Total Current
90 nm	1.2 V	20 °C	4.1353 µA	96.5 µA
90 nm	1.2 V	90 °C	14.4754 µA (×3.50)	771.1 µA (×7.99)
90 nm	1.6 V	90 °C	32.3217 µA (×7.82)	1,867.3 µA (×19.35)

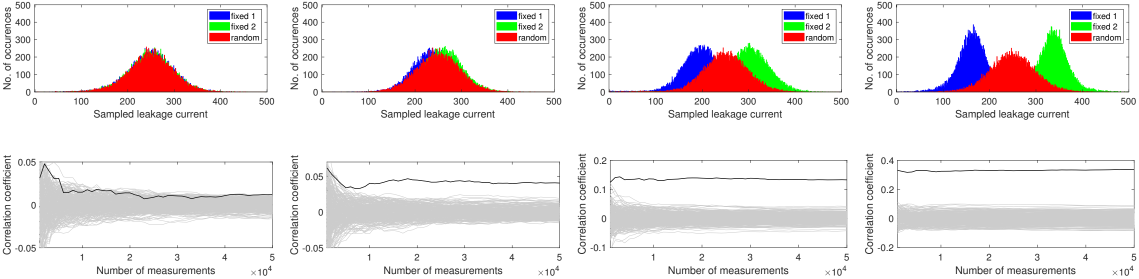
Technology	Voltage	Temp.	Diff. of Means	Avg. Total Current
65 nm	1.2 V	20 °C	38.4927 µA	154.9 µA
65 nm	1.2 V	90 °C	263.1579 µA (×6.84)	1,585.1 µA (×10.23)
65 nm	1.6 V	90 °C	450.6296 µA (×11.71)	3,067.2 µA (×19.80)

Section 5

New Results

Static Power SCA Results

Susceptibility of AES-128 Implementations at 20 °C:



(a) 90 nm

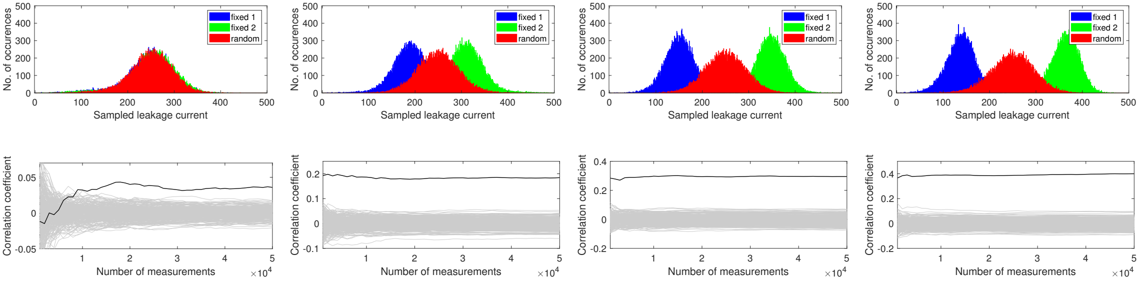
(b) 65 nm

(c) 40 nm

(d) 28 nm

Static Power SCA Results

Susceptibility of AES-128 Implementations at 90 °C:



(a) 90 nm

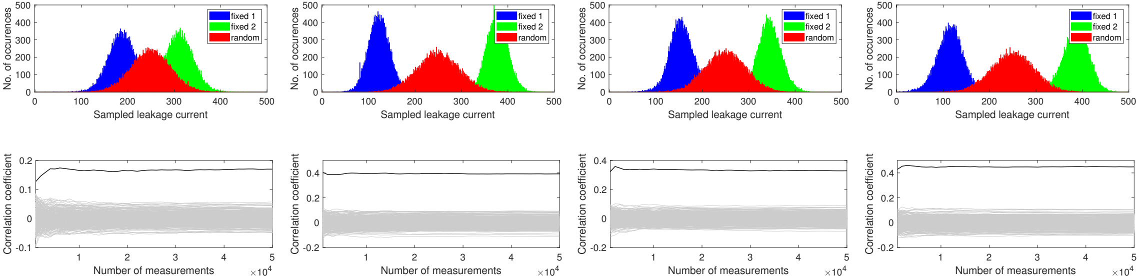
(b) 65 nm

(c) 40 nm

(d) 28 nm

Static Power SCA Results

Susceptibility of AES-128 Implementations at 90 °C and 50% over-voltage:



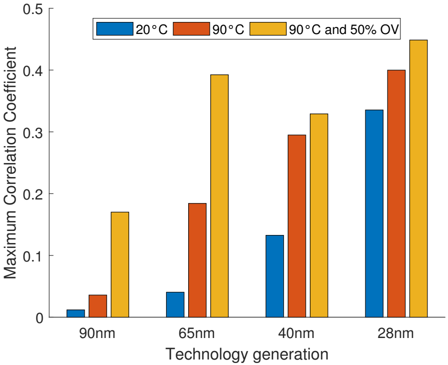
(a) 90 nm

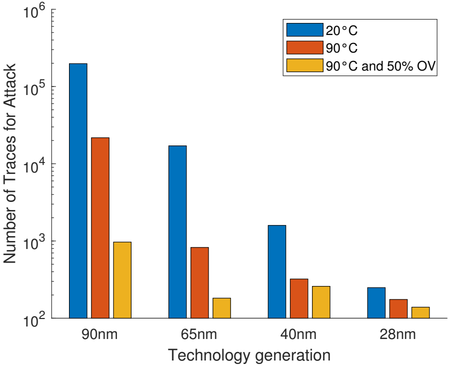
(b) 65 nm

(c) 40 nm

(d) 28 nm

Evolution of the Static Power Side Channel





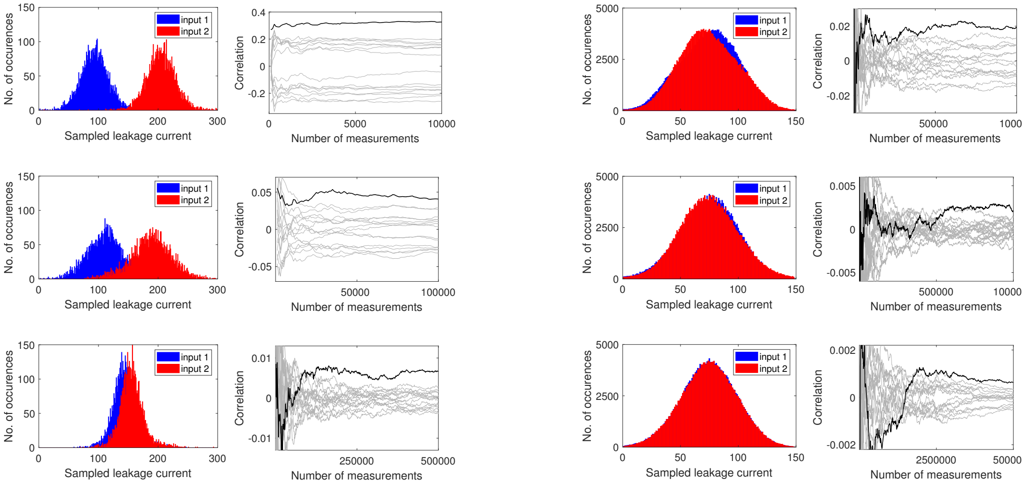
Section 6

Countermeasures

Selected Countermeasures on 28 nm ASIC

PRESENT Core	Area [GE]	Overhead factor
Unprotected	2 535.00	× 1.00
Shuffled	2 613.00	× 1.03
Balanced	20 207.00	× 7.97
Masked	7 233.33	× 2.85
Masked + Shuffled	9 856.33	× 3.89
Masked + Balanced	58 442.33	× 23.05

Selected Countermeasures on 28 nm ASIC

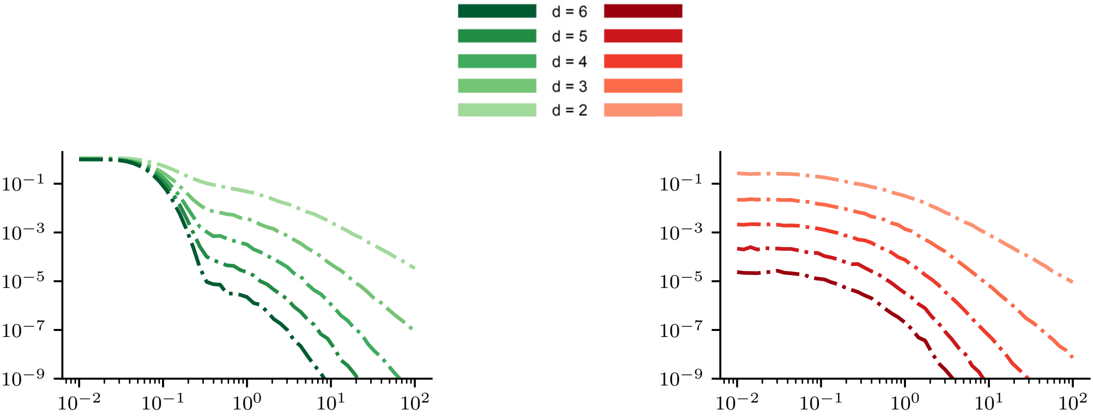


Selected Countermeasures on 28 nm ASIC

Data complexities as absolute values and per gate equivalents for all attacks:

PRESENT Core	Area [GE]	DC	DC / GE	Correlation Coefficient
Unprotected	2 535.00	< 100	< 0.039	0.3258
Shuffled	2 613.00	15 000	5.741	0.04069
Balanced	20 207.00	120 000	5.939	0.006618
Masked	7 233.33	23 600	3.263	0.01913
Masked + Shuffled	9 856.33	596 000	**60.469**	0.002144
Masked + Balanced	58 442.33	**2 930 000**	50.135	**0.0006170**

Inform. Theor. Approach: Prime-Field Masking



(a) MI(HW(shares)) vs Noise, $\mathbb{F}_{2^n}$

(b) MI(HW(shares)) vs Noise, $\mathbb{F}_p$

Conclusion

- There is a direct relationship between the feature size of the technology and the vulnerability of implementations to Static Power SCA Attacks
- Operating conditions can boost the exploitable information through this side-channel across all feature sizes
- Due to the low noise levels, Boolean masked implementations may be susceptible with comparably few traces
- It is dangerous to leave sensitive intermediates behind in a circuit and just wait for the next reset

- Leakage currents should not be neglected any longer when certifying the security of embedded devices

Open Problems and Future Directions

- Practical comparison to FD-SOI and FinFET technologies (below 28 nm)
- "Remote" static power analysis attacks
- Improved countermeasures against static power analysis attacks

Thank you very much for your attention.