RUHR-UNIVERSITÄT BOCHUM

Static Power SCA of Sub-100 nm CMOS ASICs

and the Insecurity of Masking Schemes in Low-Noise Environments

Thorben Moos

Ruhr University Bochum, Horst Görtz Institute for IT Security, Germany

August 28th, 2019

Deutsche Forschungsgemeinschaft

Section 1

Introduction

What’s known?

Introduction

- CMOS logic gates and memory elements have a data dependent static power consumption

What’s known?

Introduction

- CMOS logic gates and memory elements have a data dependent static power consumption
- Leakage currents increase significantly by down-scaling the physical feature size of transistors

What’s known?

Introduction

- CMOS logic gates and memory elements have a data dependent static power consumption
- Leakage currents increase significantly by down-scaling the physical feature size of transistors
- Attacks on crypto primitives exploiting this data dependency have been demonstrated in practice for FPGAs [CHES 2014] and ASICs [DATE 2015/2017]

What’s known?

Introduction

- CMOS logic gates and memory elements have a data dependent static power consumption
- Leakage currents increase significantly by down-scaling the physical feature size of transistors
- Attacks on crypto primitives exploiting this data dependency have been demonstrated in practice for FPGAs [CHES 2014] and ASICs [DATE 2015/2017]
- When clock control is obtained by an adversary, measurements with a very low noise influence can be recorded

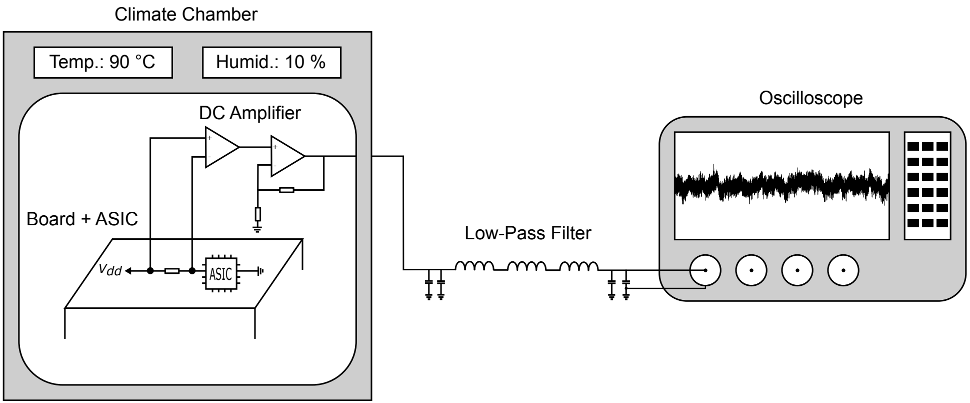
What’s known?

Introduction

- CMOS logic gates and memory elements have a data dependent static power consumption
- Leakage currents increase significantly by down-scaling the physical feature size of transistors
- Attacks on crypto primitives exploiting this data dependency have been demonstrated in practice for FPGAs [CHES 2014] and ASICs [DATE 2015/2017]
- When clock control is obtained by an adversary, measurements with a very low noise influence can be recorded
- Control over the operating conditions significantly enhances the ability to extract secrets, even though it accelerates device degradation

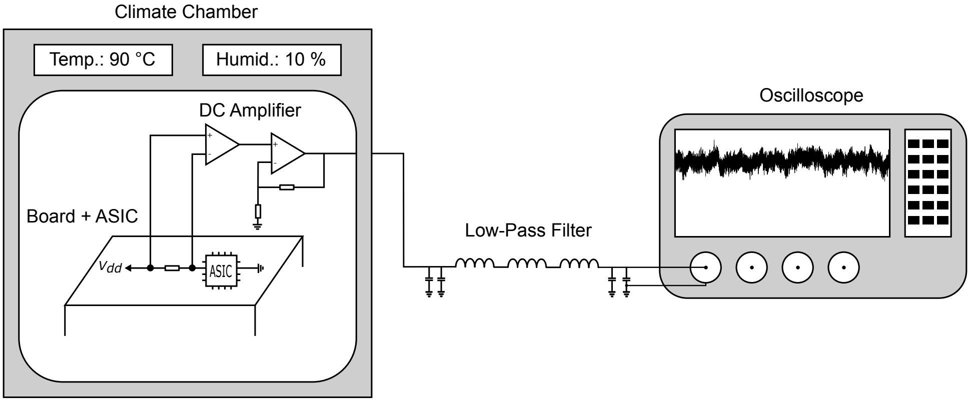
Setup

Introduction



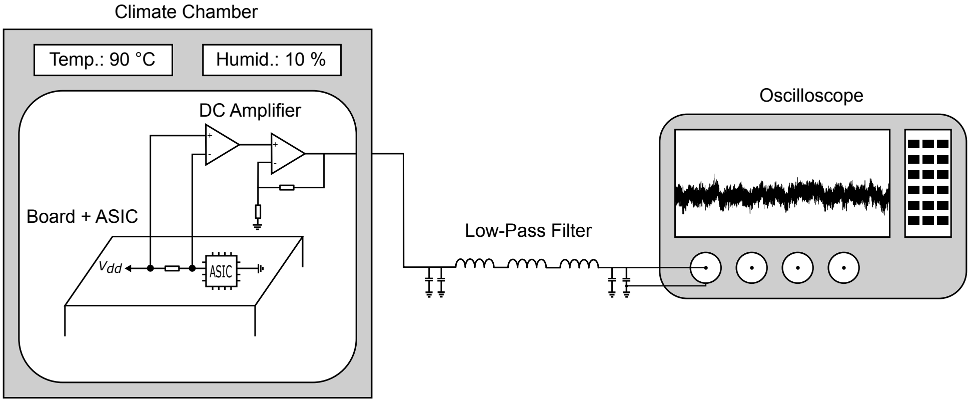
Setup

Introduction



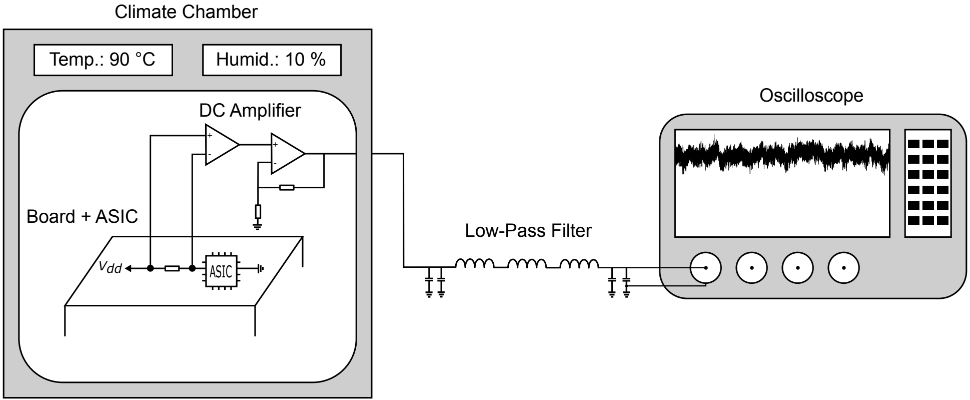
Setup

Introduction



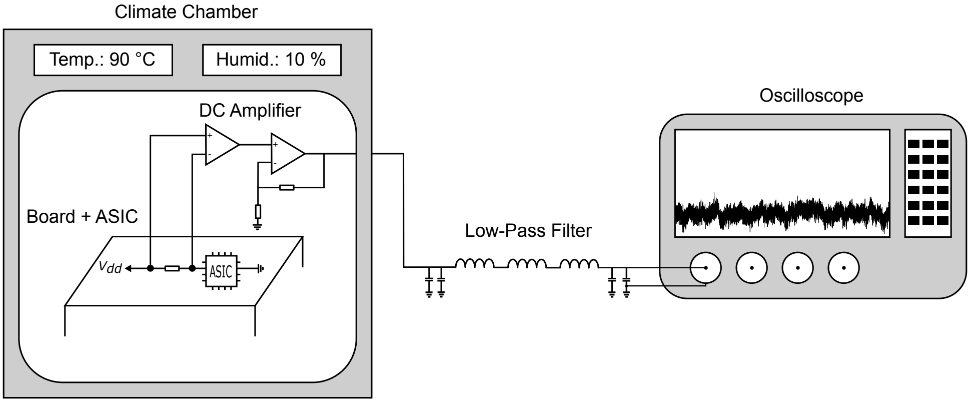
Setup

Introduction



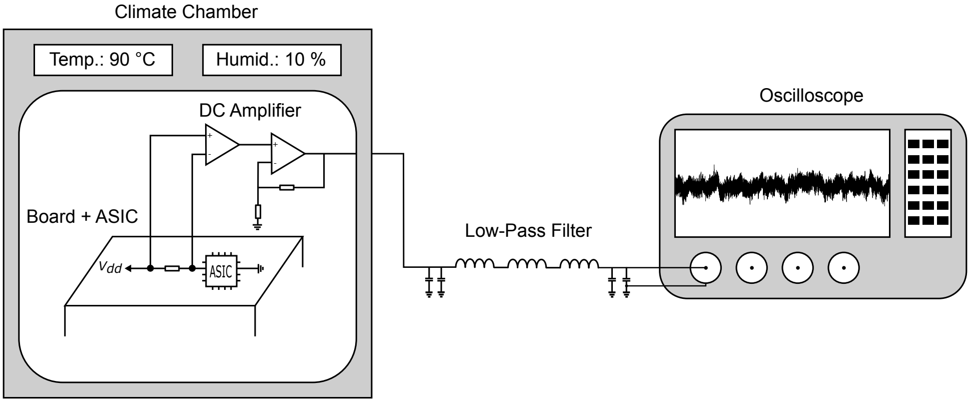
Setup

Introduction



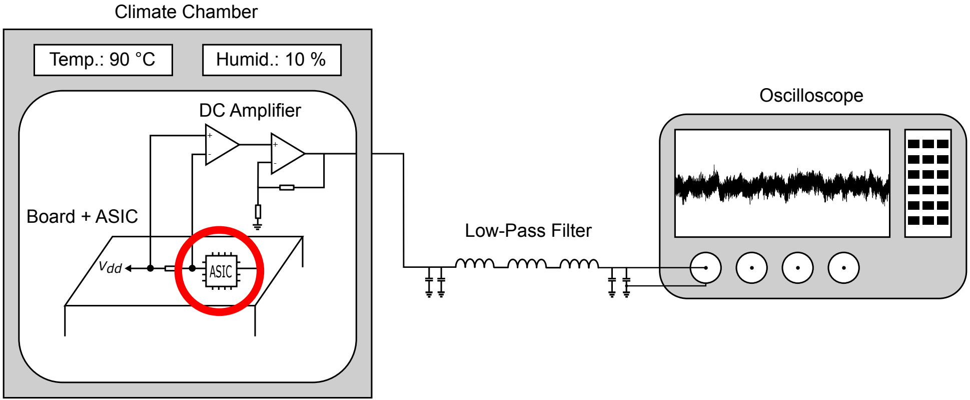
Setup

Introduction



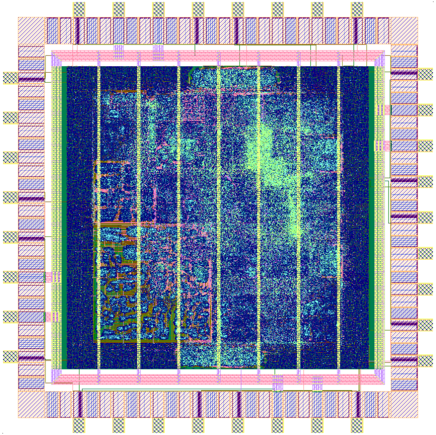
Setup

Introduction

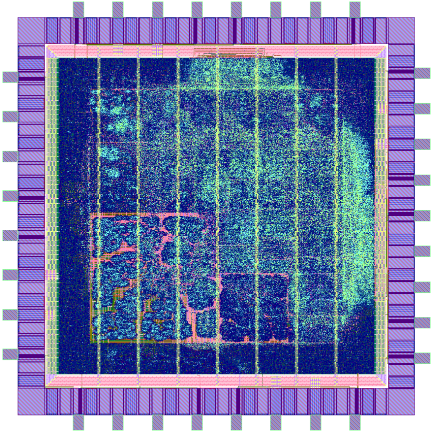


ASICs

Introduction



(a) 65nm ASIC layout



(b) 90nm ASIC layout

Section 2

Influence of Operating Conditions

Target

1024-bit HF Register

To evaluate the influence of operating conditions, choose an instance that leaks a lot:

Target

1024-bit HF Register

To evaluate the influence of operating conditions, choose an instance that leaks a lot:

1024-bit HF Input Register

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

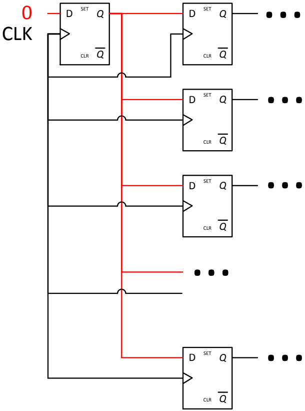
Target

1024-bit HF Register

To evaluate the influence of operating conditions, choose an instance that leaks a lot:

1024-bit HF Input Register

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



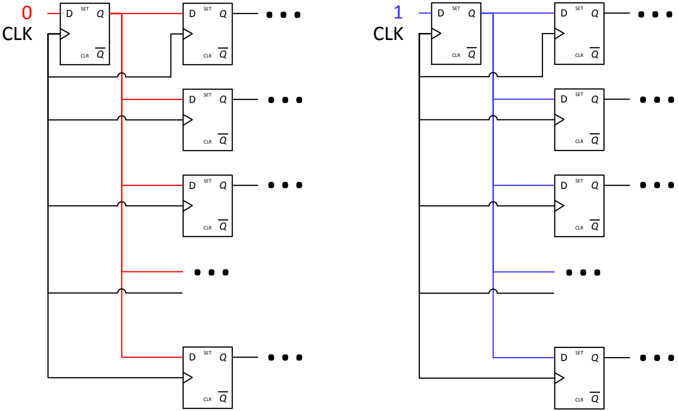
Target

1024-bit HF Register

To evaluate the influence of operating conditions, choose an instance that leaks a lot:

1024-bit HF Input Register

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

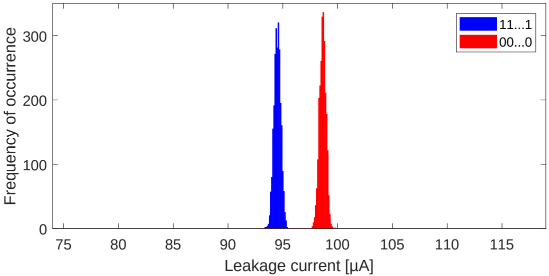


Subsection 1

90 nm ASIC

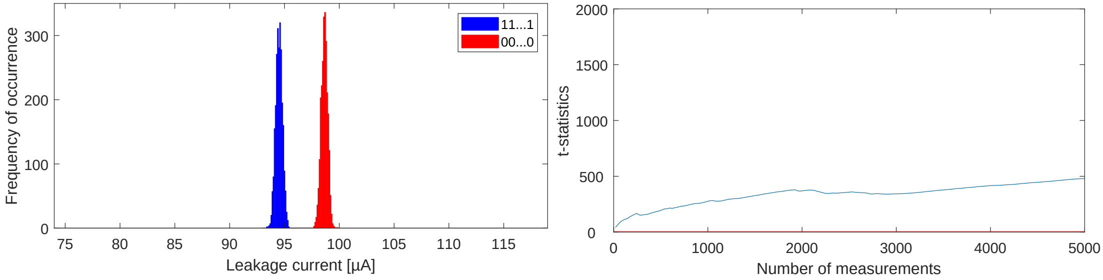
90 nm ASIC – Normal Operating Conditions

5,000 Measurements at 1.2 V and 20 °C



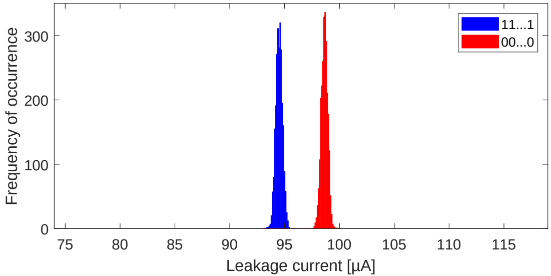
90 nm ASIC – Normal Operating Conditions

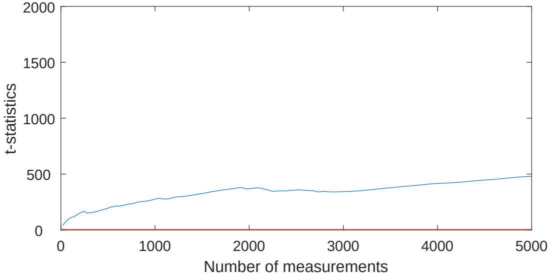
5,000 Measurements at 1.2 V and 20 °C



90 nm ASIC – Normal Operating Conditions

5,000 Measurements at 1.2 V and 20 °C

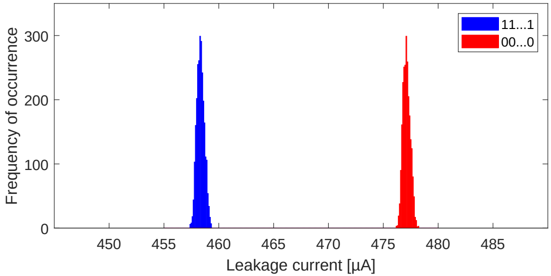


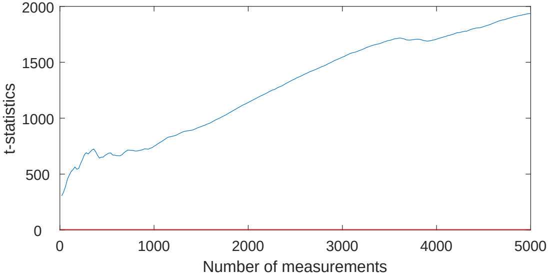


Difference of Means	4.1353 µA
Average Total Current	96.5 µA
t-value (after 5,000 Traces)	480

90 nm ASIC – Increased Supply Voltage

5,000 Measurements at 1.6 V and 20 °C

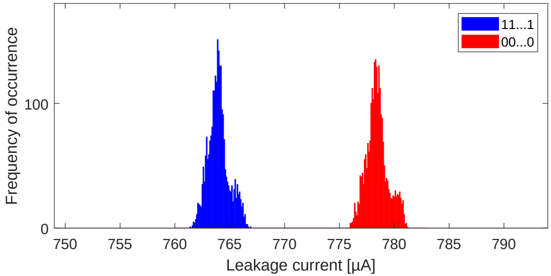


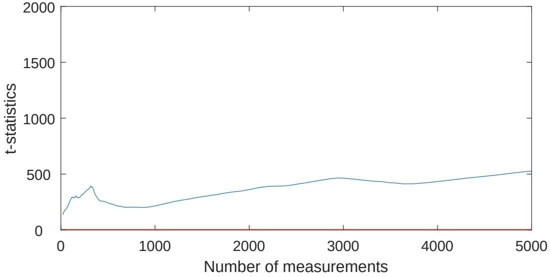


Difference of Means	18.7822 µA	×4.5419 gain
Average Total Current	467.3 µA	×4.8424 gain
t-value (after 5,000 Traces)	1938	×4.0375 gain

90 nm ASIC – Increased Temperature

5,000 Measurements at 1.2 V and 90 °C

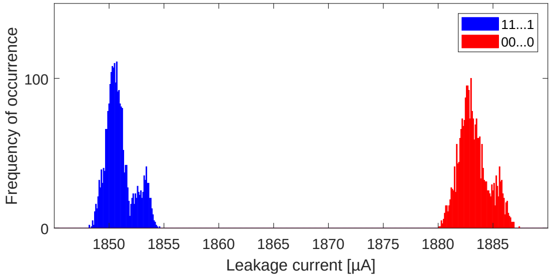


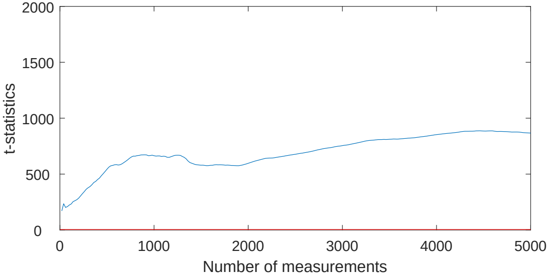


Difference of Means	14.4754 µA	×3.5004 gain
Average Total Current	771.1 µA	×7.9907 gain
t-value (after 5,000 Traces)	526	×1.0958 gain

90 nm ASIC – Increased Voltage and Temperature

5,000 Measurements at 1.6 V and 90 °C





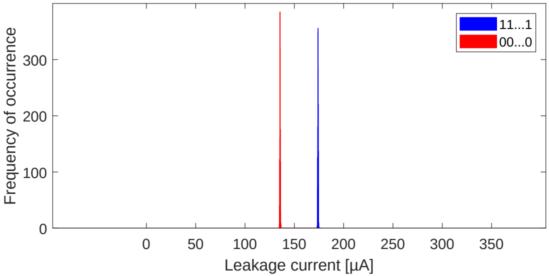
Difference of Means	32.3217 µA	×7.8160 gain
Average Total Current	1,867.3 µA	×19.3503 gain
t-value (after 5,000 Traces)	867	×1.8063 gain

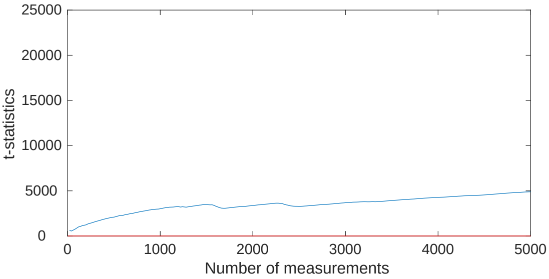
Subsection 2

65 nm ASIC

65 nm ASIC – Normal Operating Conditions

5,000 Measurements at 1.2 V and 20 °C

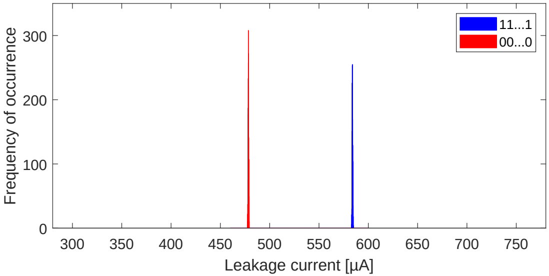


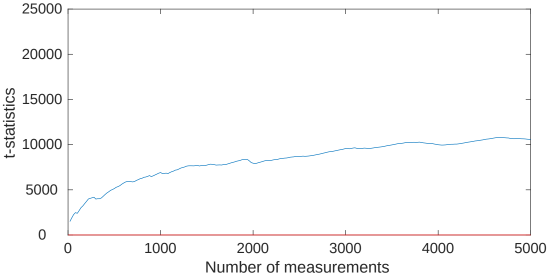


Difference of Means	38.4927 µA
Average Total Current	154.9 µA
t-value (after 5,000 Traces)	4890

65 nm ASIC – Increased Supply Voltage

5,000 Measurements at 1.6 V and 20 °C

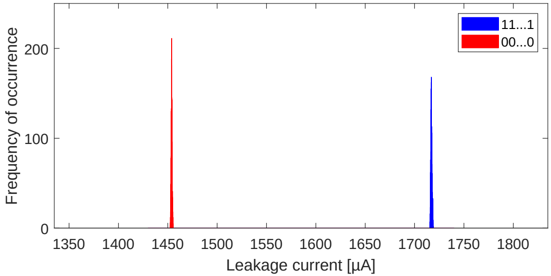


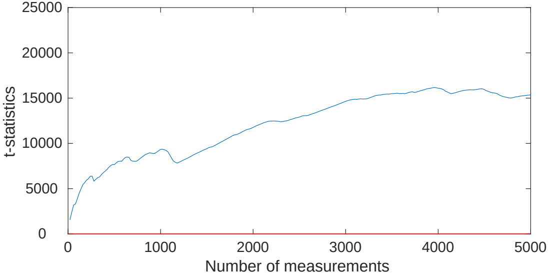


Difference of Means	105.5205 µA	×2.7413 gain
Average Total Current	529.9 µA	×3.4209 gain
t-value (after 5,000 Traces)	10570	×2.1616 gain

65 nm ASIC – Increased Temperature

5,000 Measurements at 1.2 V and 90 °C

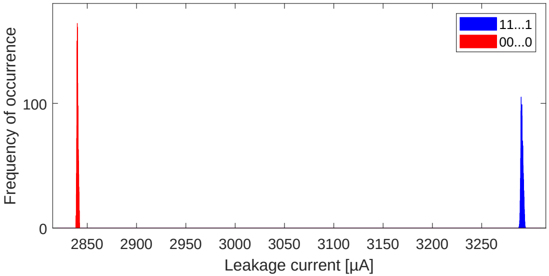


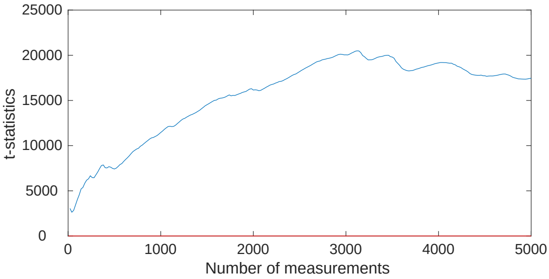


Difference of Means	263.1579 µA	×6.8366 gain
Average Total Current	1585.1 µA	×10.2331 gain
t-value (after 5,000 Traces)	15360	×3.1411 gain

65 nm ASIC – Increased Voltage and Temperature

5,000 Measurements at 1.6 V and 90 °C





Difference of Means	450.6296 µA	×11.7069 gain
Average Total Current	3067.2 µA	×19.8012 gain
t-value (after 5,000 Traces)	17460	×3.5706 gain

Section 3

Technology Comparison

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

5,000 Measurements

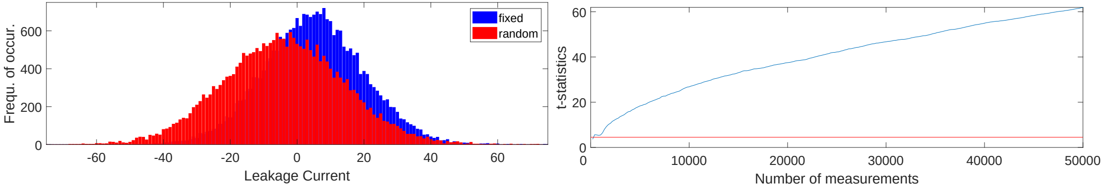
Technology	Voltage	Temp.	Diff. of Means	Avg. Total Current
90 nm	1.2 V	20 °C	4.1353 µA	96.5 µA
90 nm	1.6 V	20 °C	18.7822 µA (×4.54)	467.3 µA (×4.84)
90 nm	1.2 V	90 °C	14.4754 µA (×3.50)	771.1 µA (×7.99)
90 nm	1.6 V	90 °C	32.3217 µA (×7.82)	1,867.3 µA (×19.35)

Technology	Voltage	Temp.	Diff. of Means	Avg. Total Current
65 nm	1.2 V	20 °C	38.4927 µA	154.9 µA
65 nm	1.6 V	20 °C	105.5205 µA (×2.74)	529.9 µA (×3.42)
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)

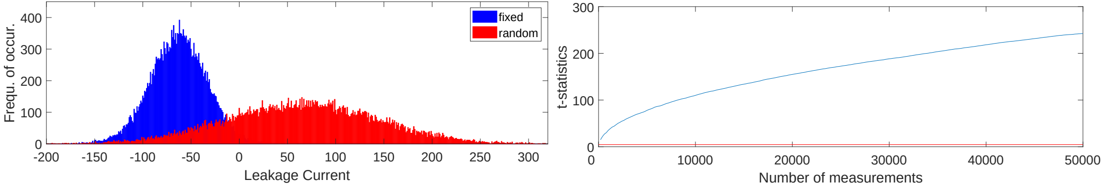
Data Dependency of PRESENT Core – 90 nm vs. 65 nm

50,000 Measurements at 1.6 V and 90 °C

90 nm ASIC:



65 nm ASIC:

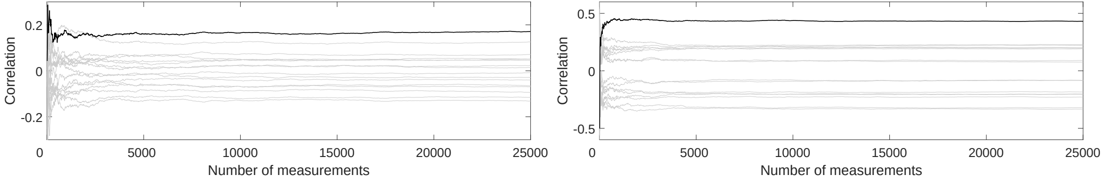


Data Dependency of PRESENT Core – 90 nm vs. 65 nm

50,000 Measurements at 1.6 V and 90 °C

90 nm ASIC:

65 nm ASIC:



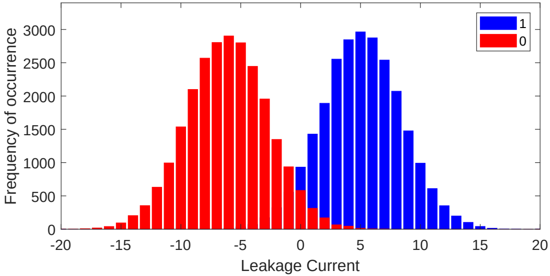
	90 nm	65 nm
Difference of Means	9.15 µA	128.46 µA
t-value (after 50,000 Traces)	61.96	242.50
Correlation	0.17	0.43
Measurements to Disclosure	2,180	100

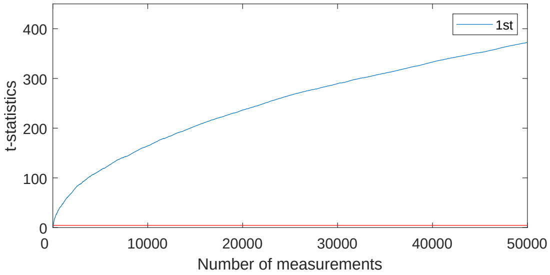
Section 4

Masking

65 nm ASIC – 1 Share in Register (1-bit)

50,000 Measurements at 1.6 V and 90 °C

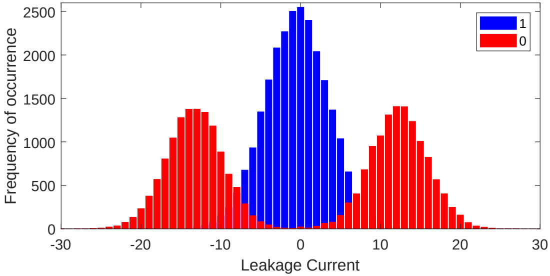


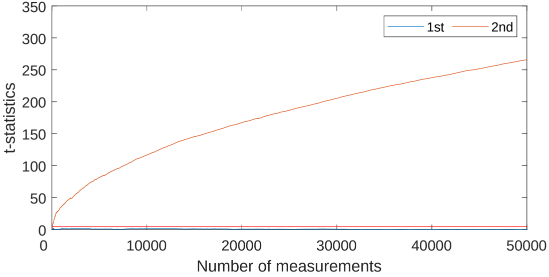


number of shares	1
detectable leakage at ...	1st-order
t-value (after 50,000 Traces)	372.4

65 nm ASIC – 2 Shares in Register (1-bit)

50,000 Measurements at 1.6 V and 90 °C

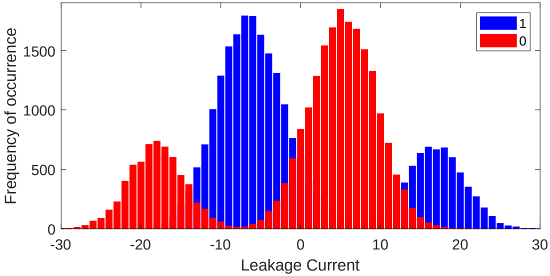


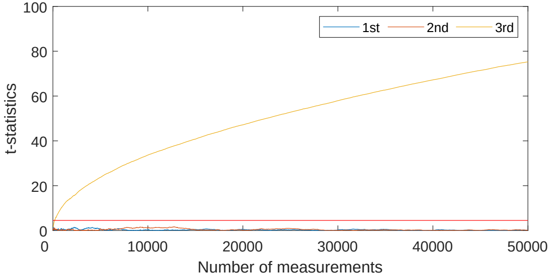


number of shares	1	2
detectable leakage at ...	1st-order	2nd-order
t-value (after 50,000 Traces)	372.4	265.7

65 nm ASIC – 3 Shares in Register (1-bit)

50,000 Measurements at 1.6 V and 90 °C

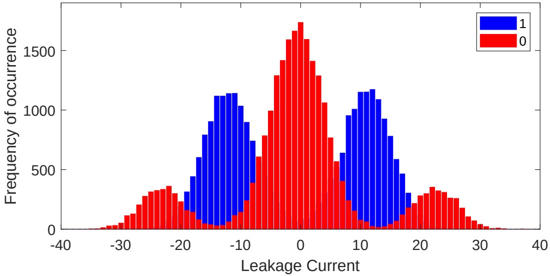


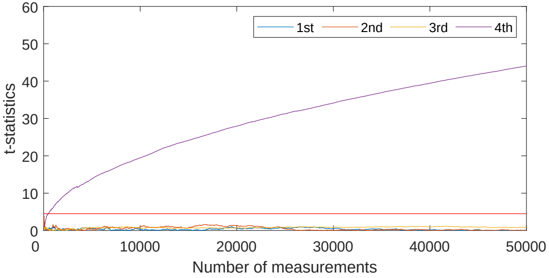


number of shares	1	2	3
detectable leakage at ...	1st-order	2nd-order	3rd-order
t-value (after 50,000 Traces)	372.4	265.7	75.25

65 nm ASIC – 4 Shares in Register (1-bit)

50,000 Measurements at 1.6 V and 90 °C

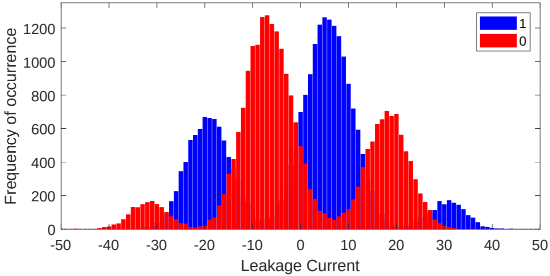


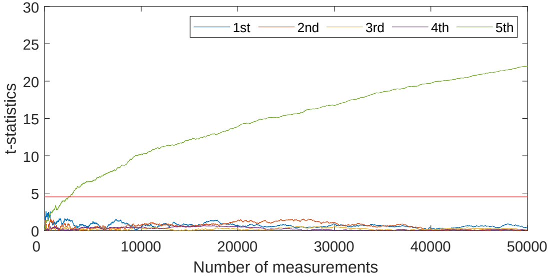


number of shares	1	2	3	4
detectable leakage at ...	1st-order	2nd-order	3rd-order	4th-order
t-value (after 50,000 Traces)	372.4	265.7	75.25	44.06

65 nm ASIC – 5 Shares in Register (1-bit)

50,000 Measurements at 1.6 V and 90 °C

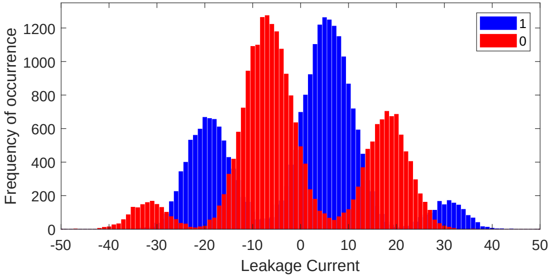


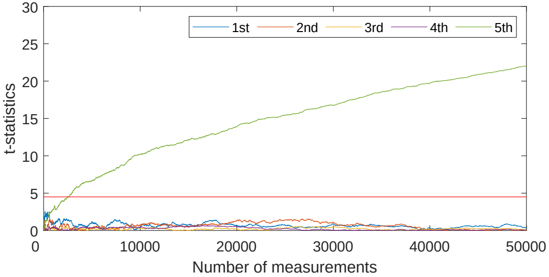


number of shares	1	2	3	4	5
detectable leakage at ...	1st-order	2nd-order	3rd-order	4th-order	5th-order
t-value (after 50,000 Traces)	372.4	265.7	75.25	44.06	22.00

65 nm ASIC – 5 Shares in Register (1-bit)

50,000 Measurements at 1.6 V and 90 °C



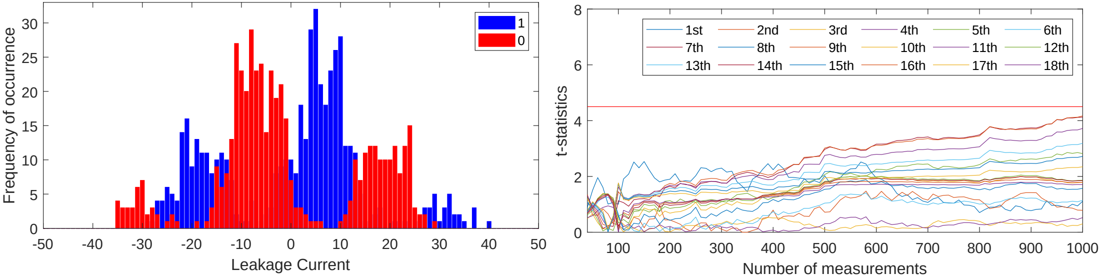


number of shares	1	2	3	4	5
detectable leakage at ...	1st-order	2nd-order	3rd-order	4th-order	5th-order
t-value (after 50,000 Traces)	372.4	265.7	75.25	44.06	22.00

65 nm ASIC – 5 Shares in Register (1-bit)

1,000 Measurements at 1.6 V and 90 °C

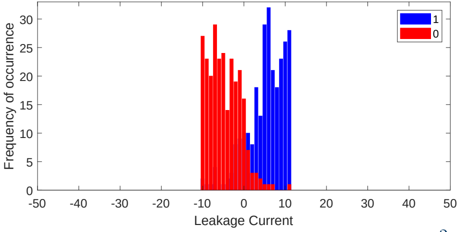
After the first 1,000 Traces the t-test does not indicate detectable leakage in any order (up to 18 shown) even though the distributions are clearly distinguishable:

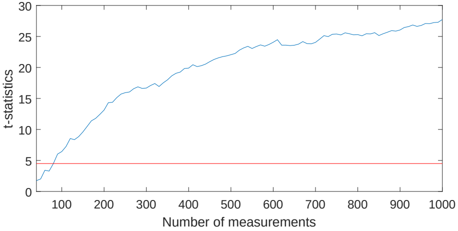


65 nm ASIC – 5 Shares in Register (1-bit)

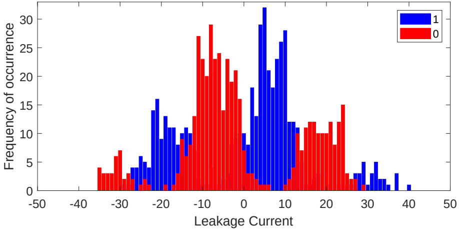
1,000 Measurements at 1.6 V and 90 °C

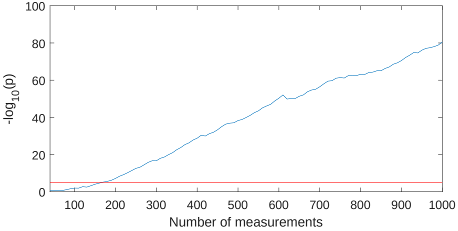
Order Conversion/Compression:





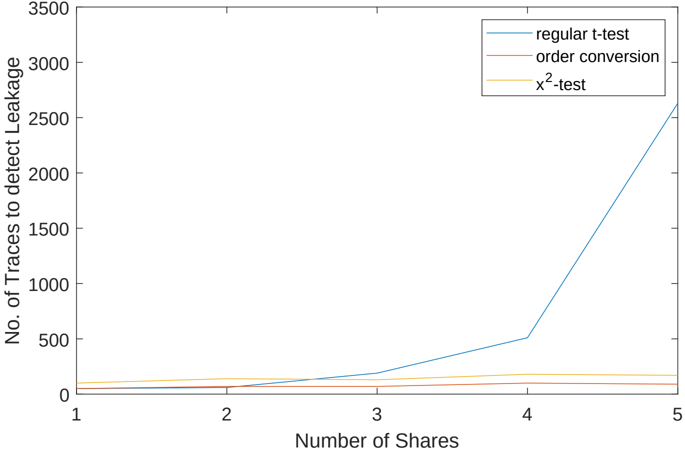
χ^2-Test:





65 nm ASIC – Detectability of the Leakage

50,000 Measurements at 1.6 V and 90 °C

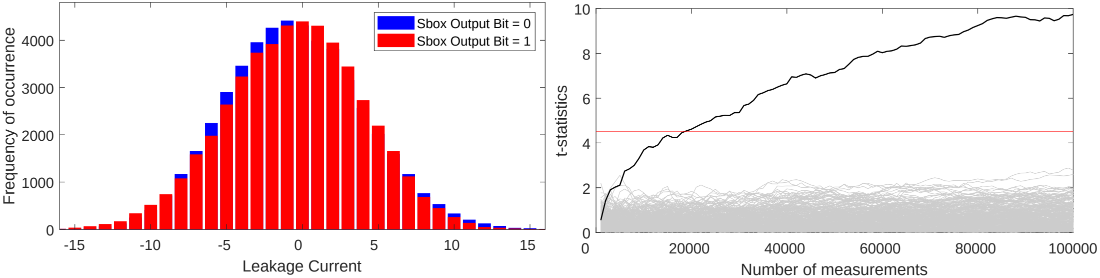


- Regular t-test indeed leads to false negatives at higher orders due to the low noise
- χ^2-test is pessimistic in low orders
- Order conversion, resp. compression, requires manual slicing of the distributions

65 nm ASIC – DPA on AES Threshold Implementation Core

100,000 Measurements at 1.6 V and 90 °C

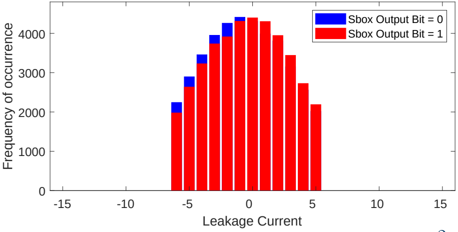
Third-order DPA using t-test:

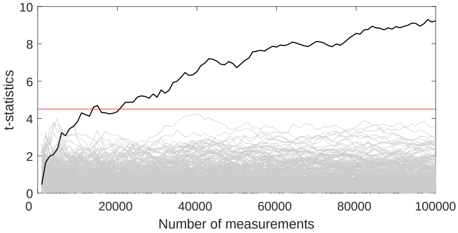


65 nm ASIC – DPA on AES Threshold Implementation Core

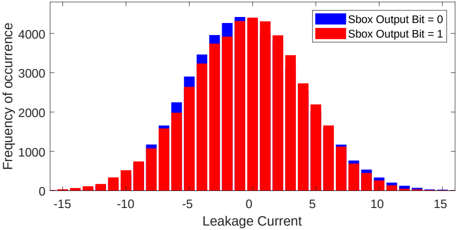
100,000 Measurements at 1.6 V and 90 °C

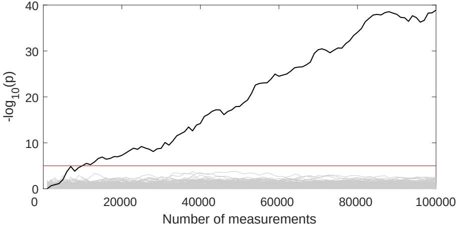
Order Conversion/Compression:





χ^2-Test:





65 nm ASIC – DPA on AES Threshold Implementation Core

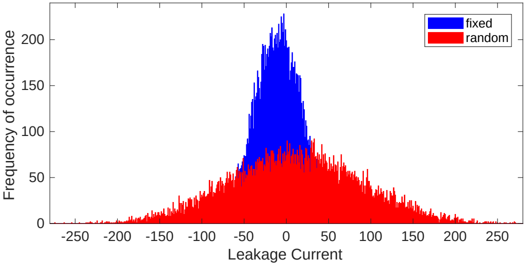
200,000 Measurements at 1.6 V and 90 °C

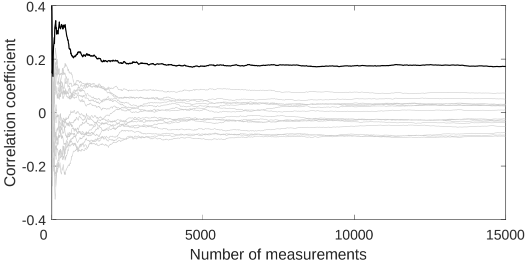
	No. of Traces for successful DPA
regular t-test	19,000
order conversion	21,000
χ^2-test	10,000

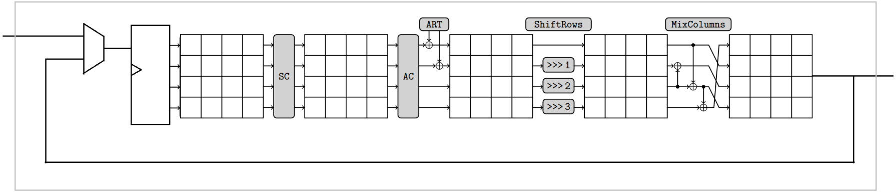
Section 5

Clock Control

SKINNY: Last Round State Remains in Circuit







Conclusion

- The potency of the static power side-channel increases significantly for smaller CMOS feature sizes

Conclusion

- The potency of the static power side-channel increases significantly for smaller CMOS feature sizes
- Operating conditions can significantly boost the available information through this side-channel

Conclusion

- The potency of the static power side-channel increases significantly for smaller CMOS feature sizes
- Operating conditions can significantly boost the available information through this side-channel
- Due to the low noise level masked implementations should not be analyzed with moment-based methods and are susceptible with comparably few traces

Conclusion

- The potency of the static power side-channel increases significantly for smaller CMOS feature sizes
- Operating conditions can significantly boost the available information through this side-channel
- Due to the low noise level masked implementations should not be analyzed with moment-based methods and are susceptible with comparably few traces
- If sensitive intermediates remain in a circuit after cryptographic operations, static power side-channel attacks without clock control may be performed

Thank you for your attention.

Any questions?