RUHR-UNIVERSITÄT BOCHUM

Side-Channel Leakage through Static Power

Should We Care about in Practice?

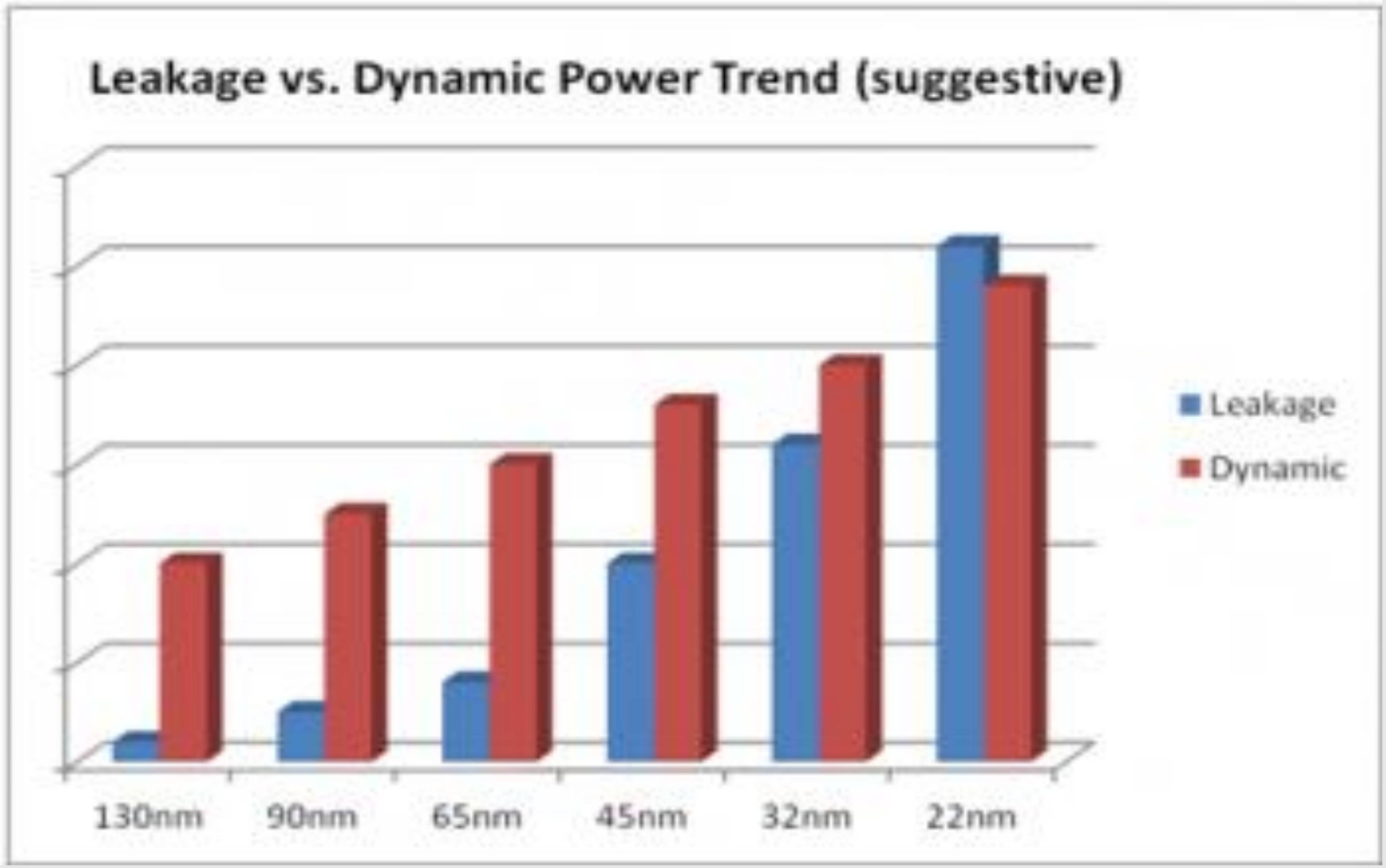
26. September 2014

Amir Moradi

Ruhr University Bochum

Horst Görtz Institute for IT-Security

Dynamic vs. Static Power

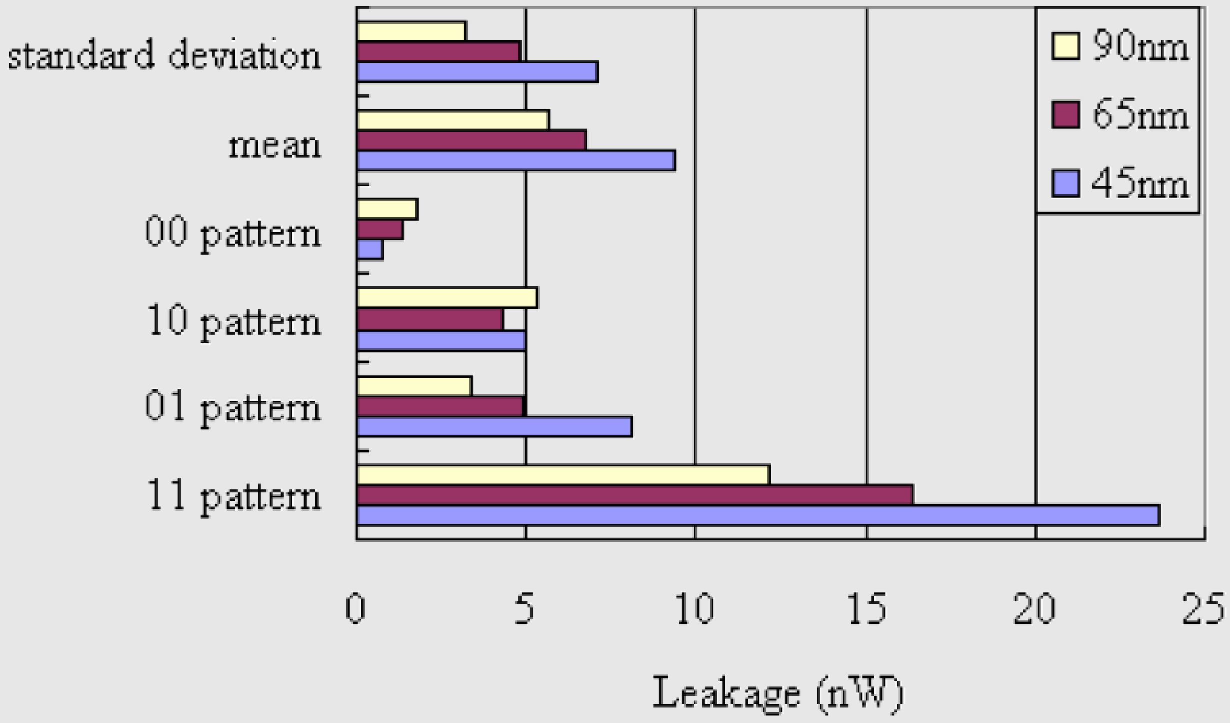


Dynamic vs. Static Power

- Dynamic power consumption
  - The main considered side channel (CMOS concept)
  - Easy to measure
  - Effective
  - …
- Static power consumption
  - becoming the major concern for VLSI community
  - introduced as a side channel by simulation results
  - also called *Leakage Power Analysis* (LPA)

What has been reported?

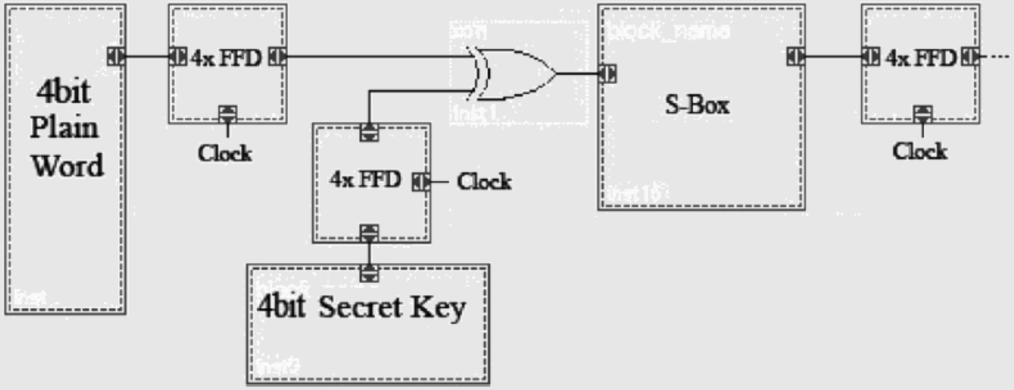
- Simulation results (2-input AND gate)

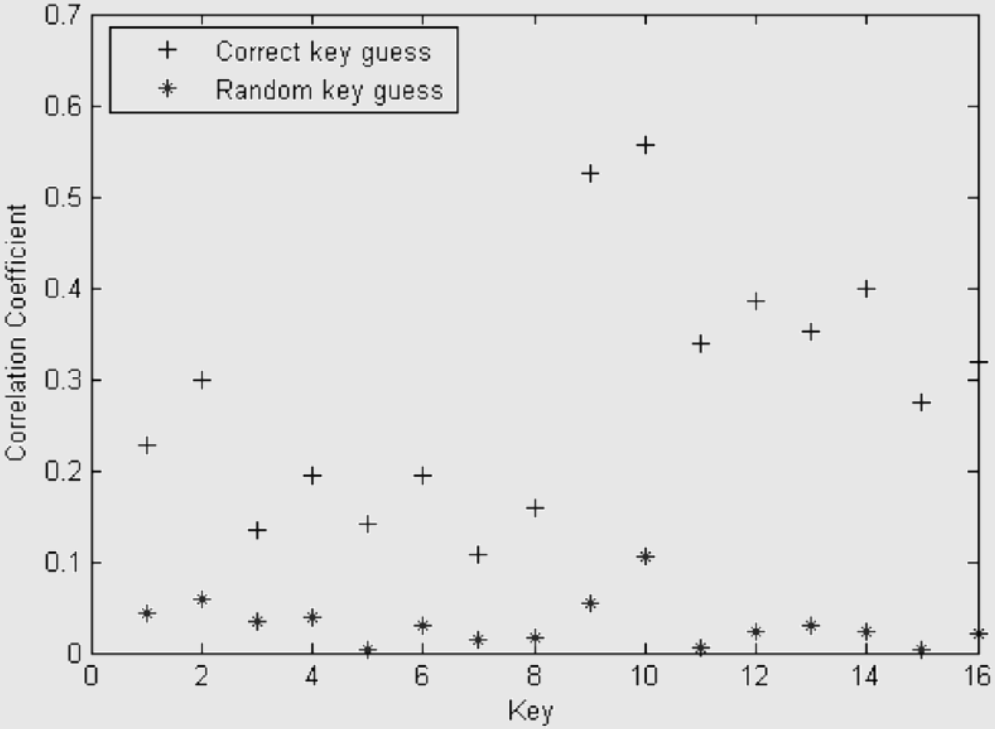


L. Lin and W. Burleson. Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems. ISCAS 2008.

What has been reported?

- Simulation results, Serpent Sbox

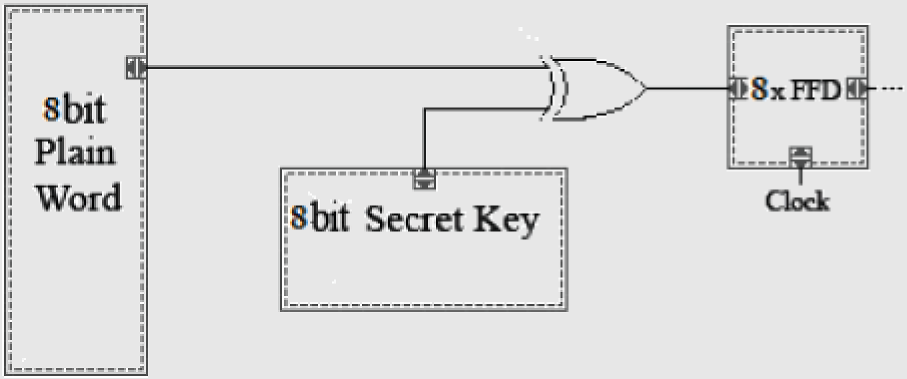


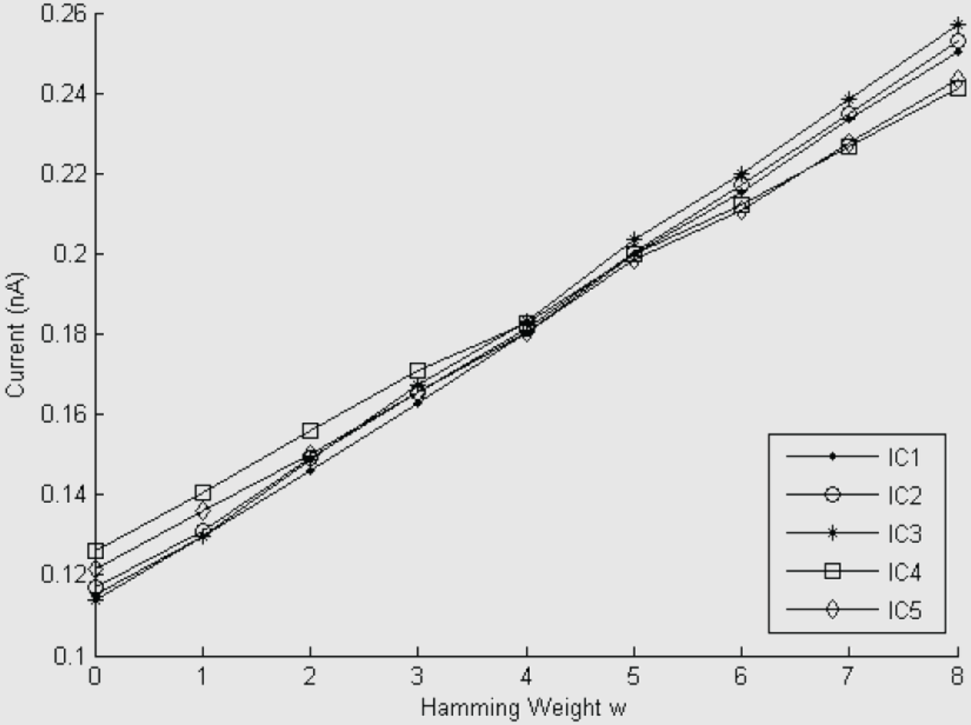


M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti. Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits. IEEE Trans. on Circuits and Systems, 2010.

What has been reported?

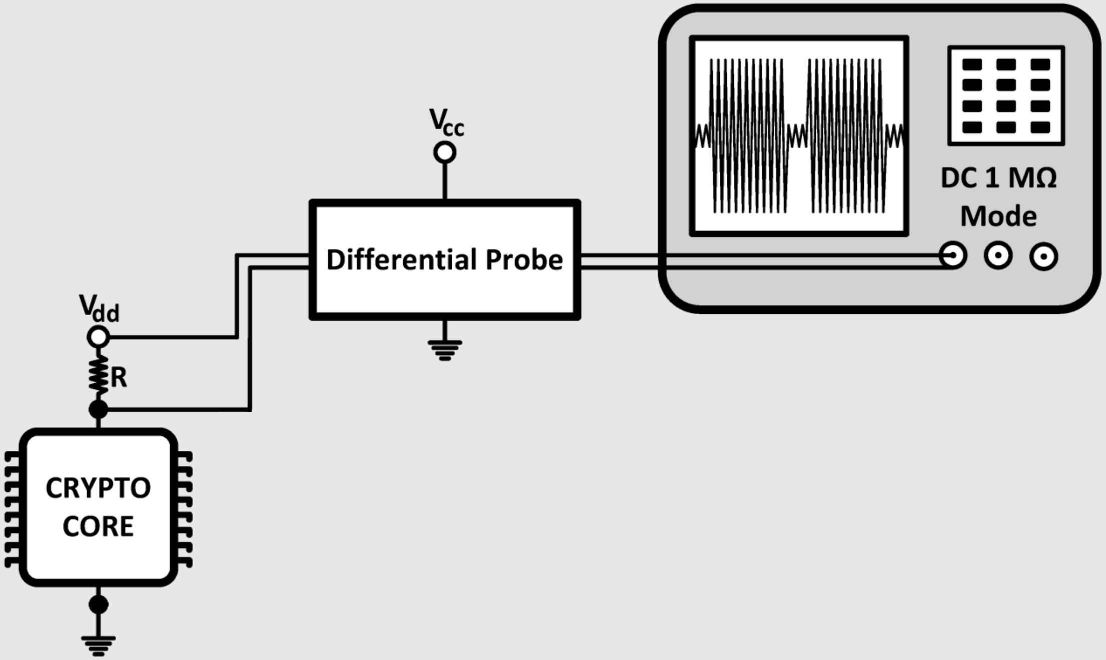
- Practical results (100 nm)



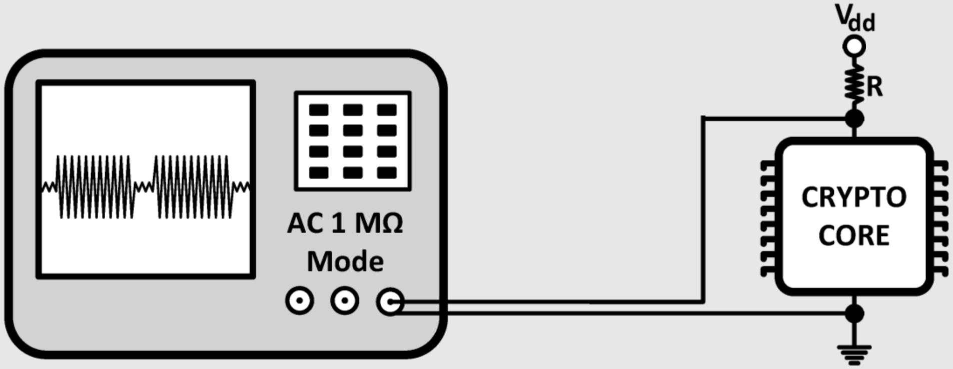


M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti. Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits. IEEE Trans. on Circuits and Systems, 2010.

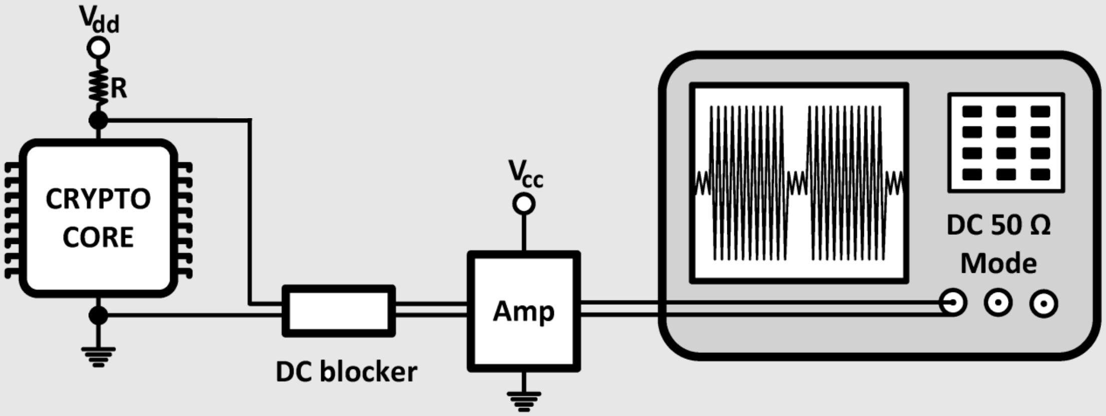
Measurement Setup (dynamic)



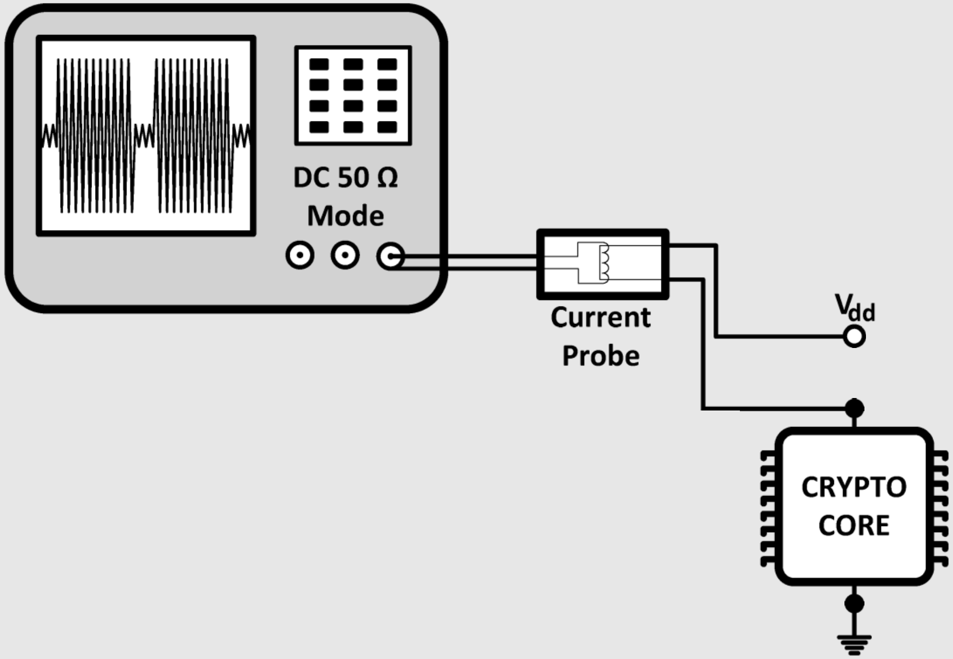
Measurement Setup (dynamic)



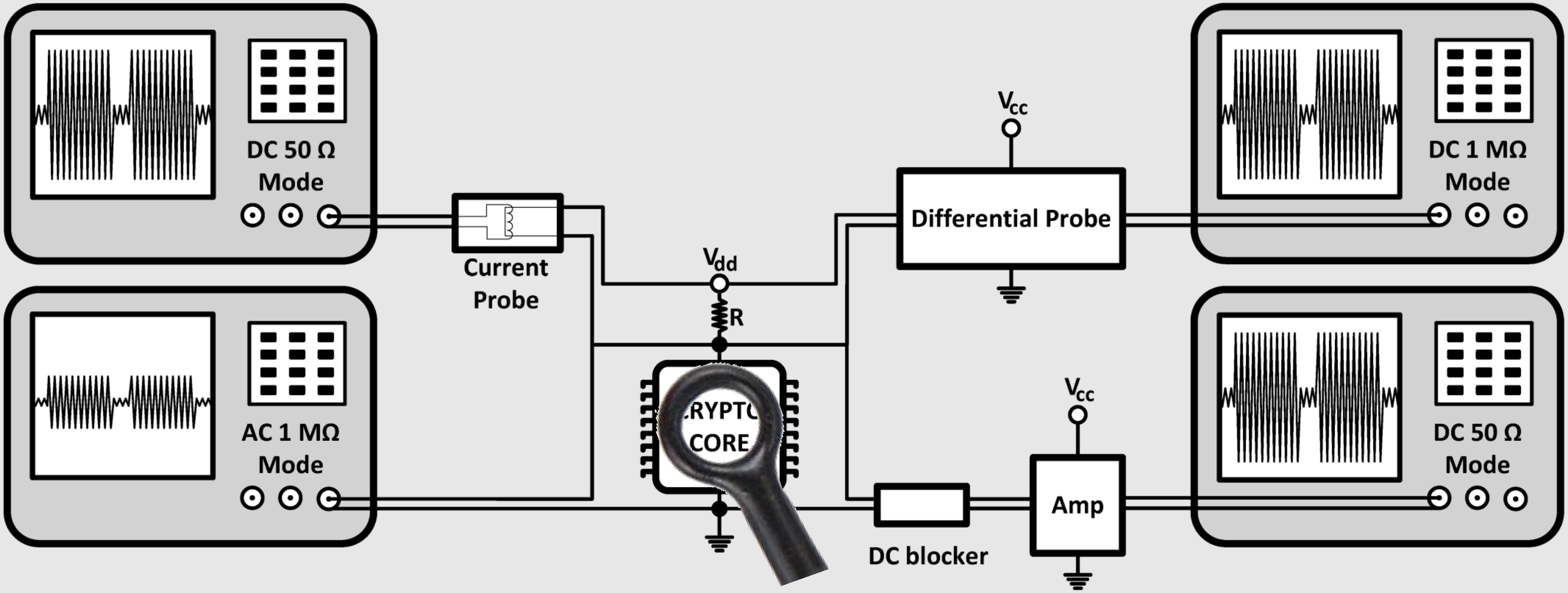
Measurement Setup (dynamic)



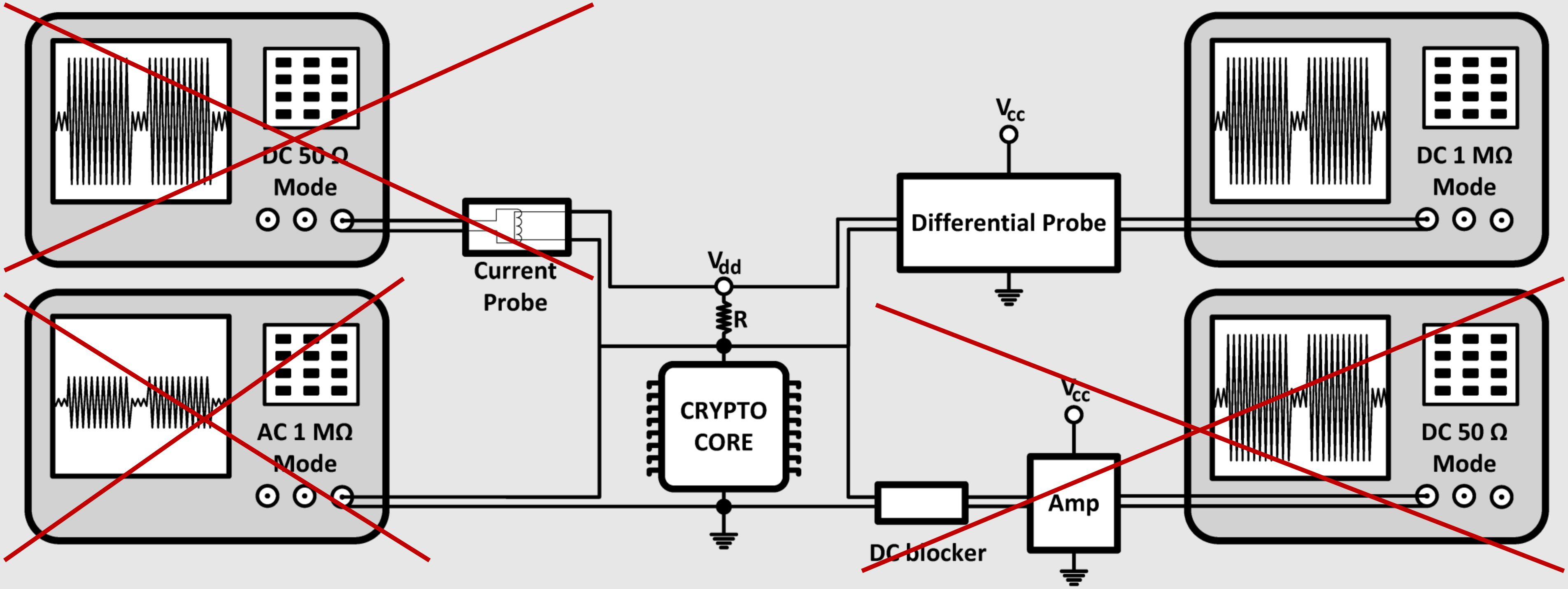
Measurement Setup (dynamic)



Measurement Setup (dynamic)



Measurement Setup (static)



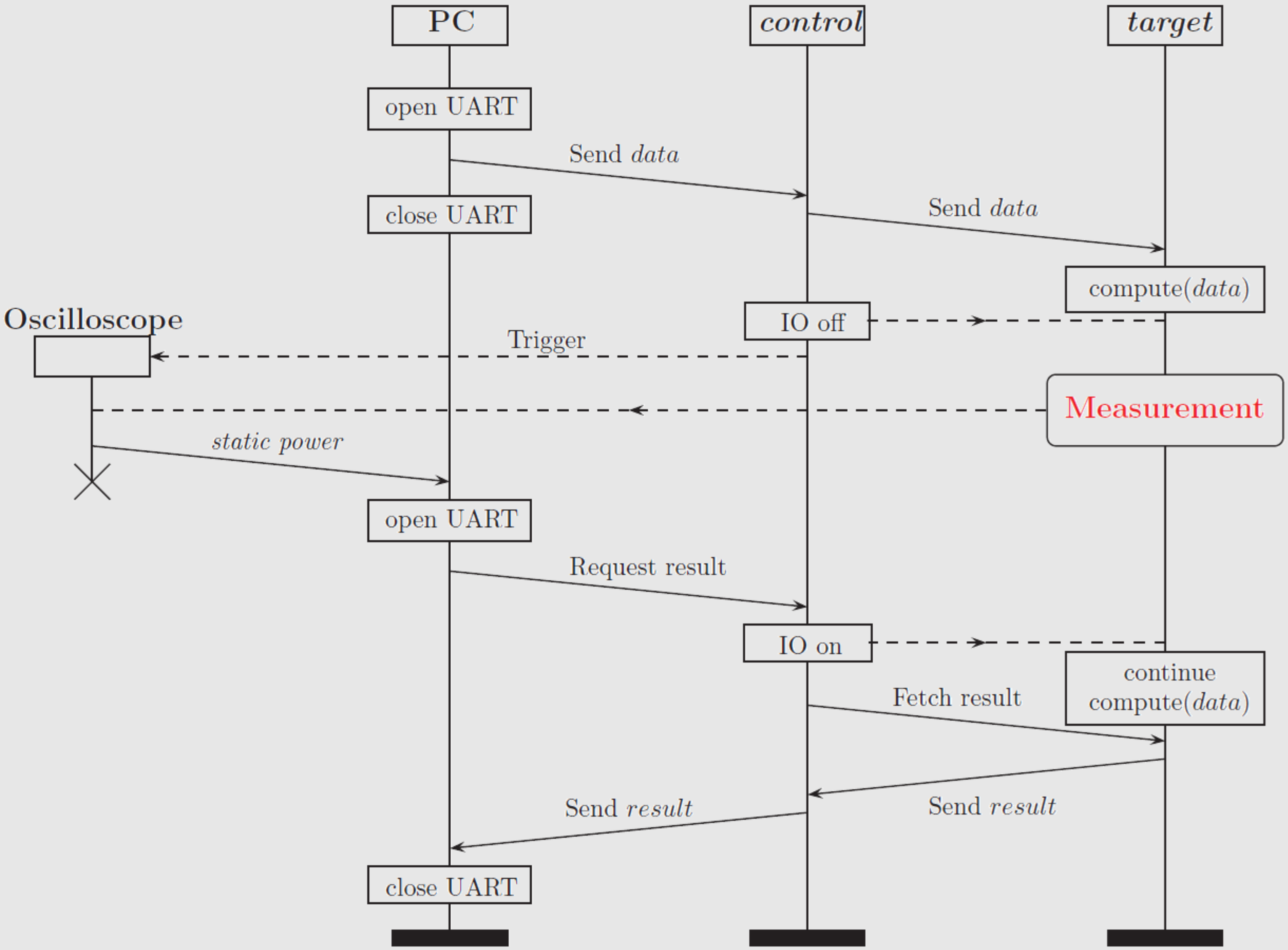
LeCroy AP 033

x10 internal amplifier

Targets

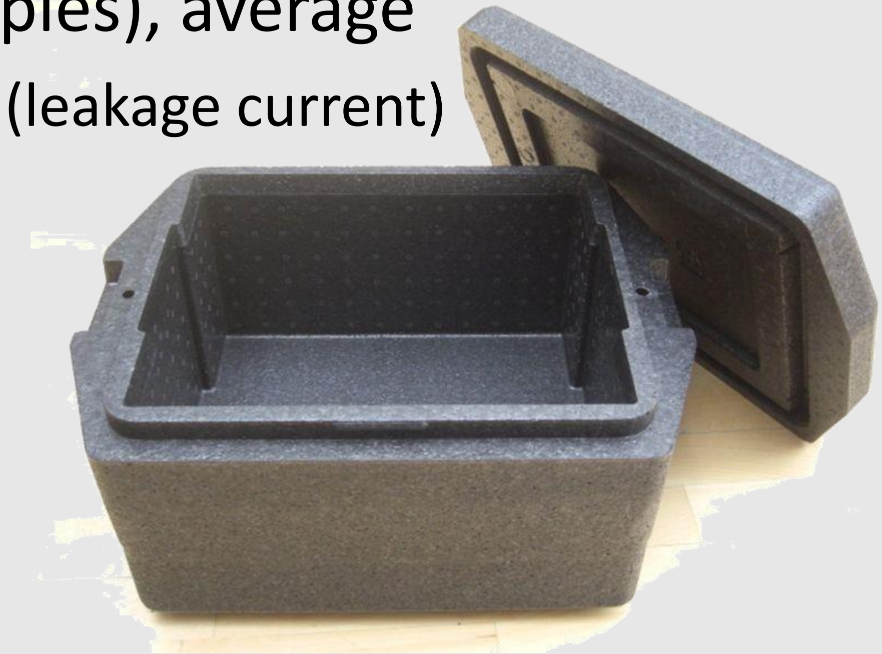
- SASEBO-GII, Virtex-5, 65nm
- SAKURA-G, Spartan-6, 45nm
- SAKURA-X, Kintex-7, 28nm

Measurement Methodology



Difficulties

- Highest vertical accuracy (200 µV/div)
- Noise
  - Sampling rate 1GS/s
  - 20MHz bandwidth limit
  - Long trace (10ms -> 10 M samples), average
    - A singular value as static power (leakage current)
- Super sensitive to temperature
  - Thermobox

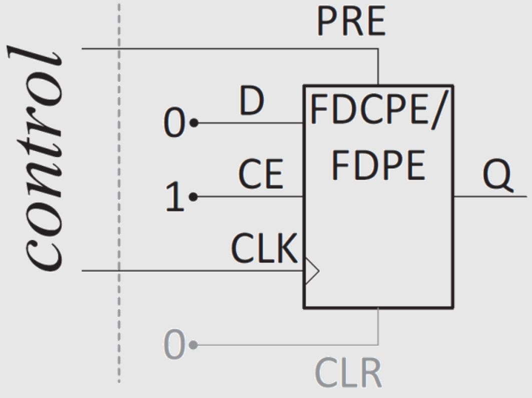


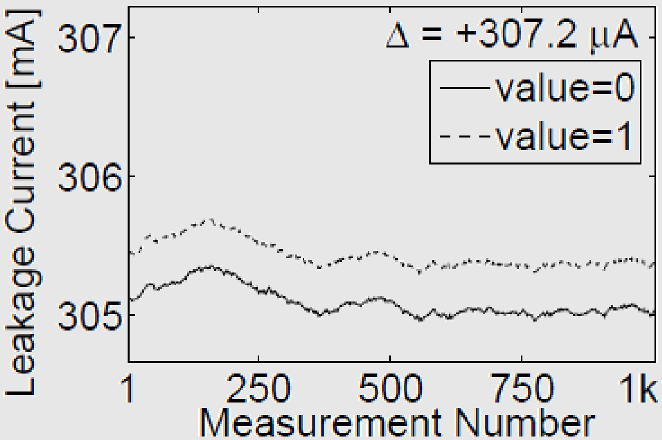
Preliminary Tests

- Contribution of Registers’ content
- Contribution of Connections (Switch Box)
- Contribution of Look-up tables (LUT)
- An AES Sbox
- A masked AES Sbox
- A masked shuffled AES encryption

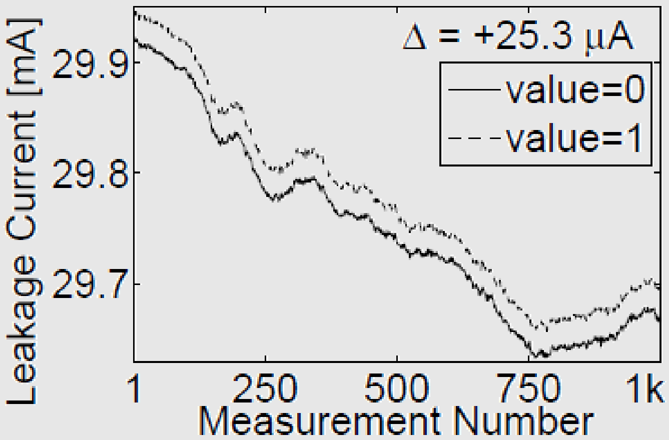
Preliminary Tests (Register)

- 14,400 registers
- The same measurement methodology for all targets

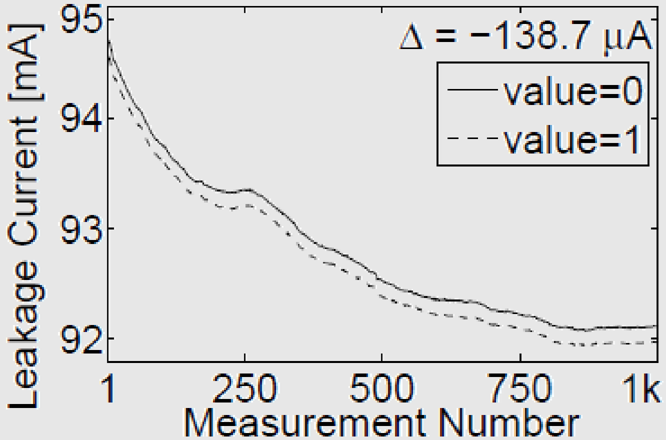




SASEBO-GII (Virtex-5)



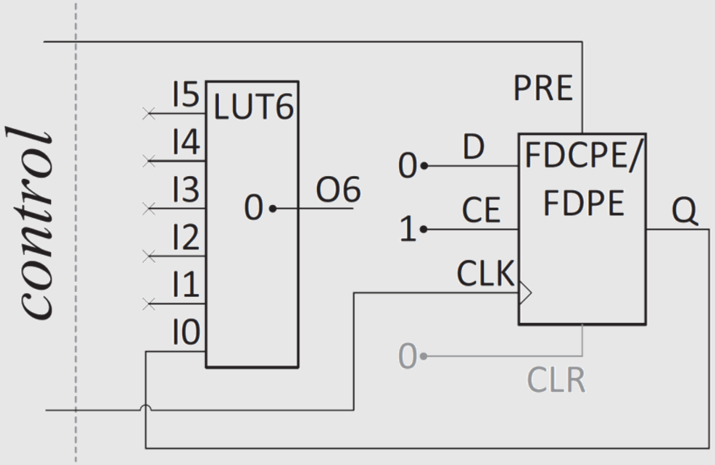
SAKURA-G (Spartan-6)

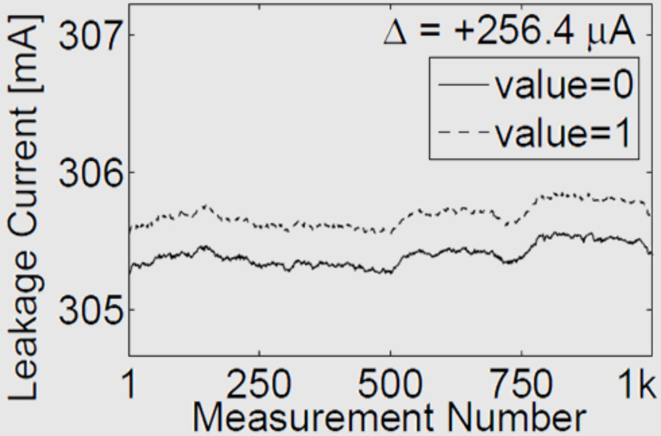


SAKURA-X (Kintex-7)

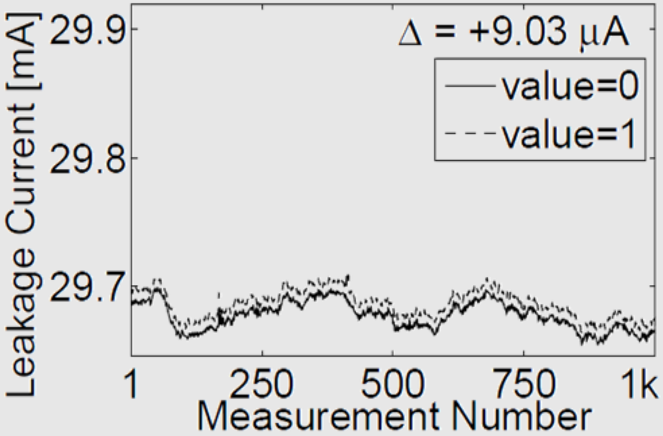
Preliminary Tests (Connection)

- 14,400 registers + Loop

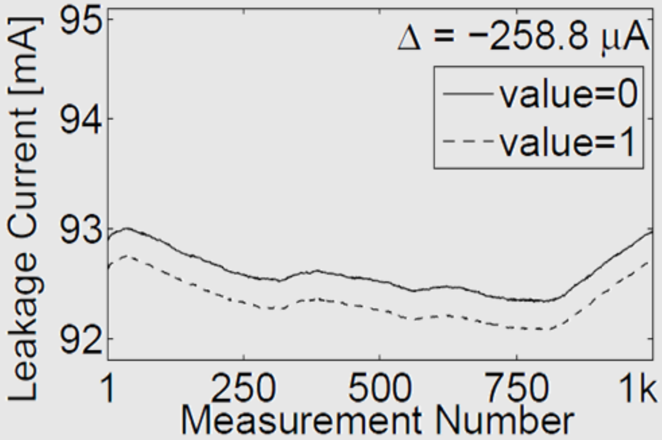




SASEBO-GII (Virtex-5)



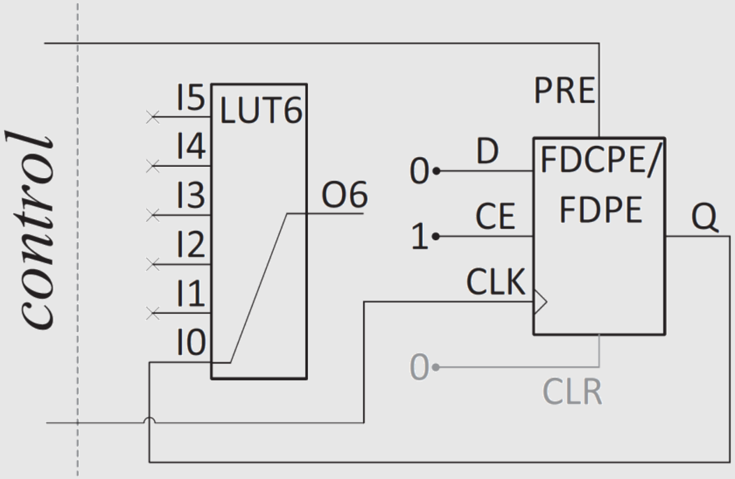
SAKURA-G (Spartan-6)

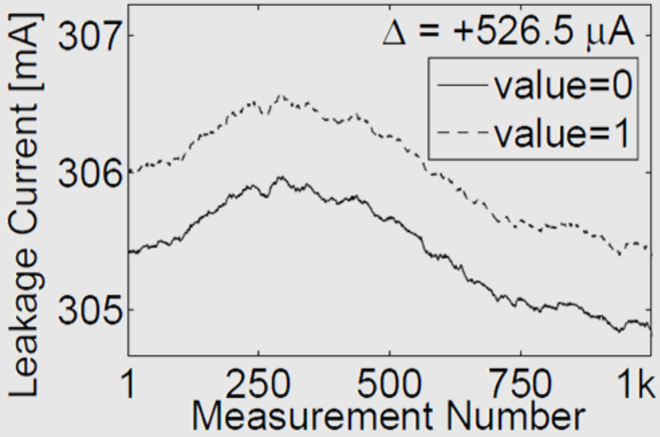


SAKURA-X (Kintex-7)

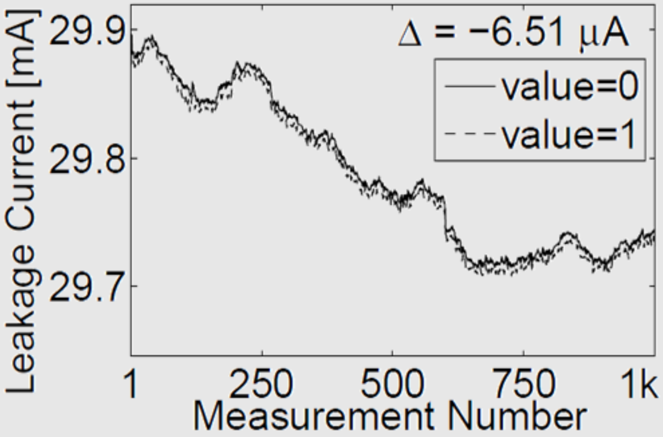
Preliminary Tests (LUT)

- 14,400 registers + Loop + LUT

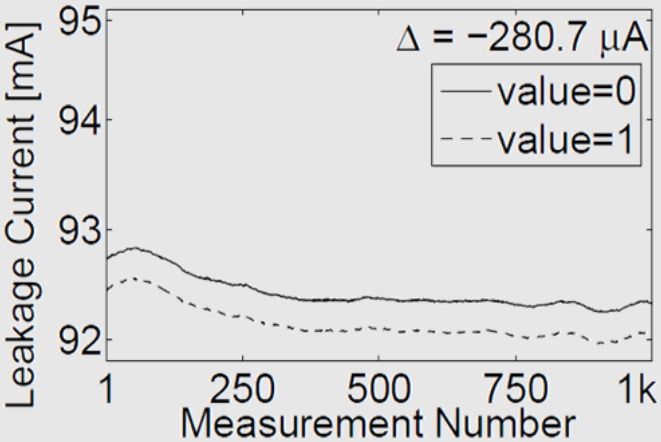




SASEBO-GII (Virtex-5)

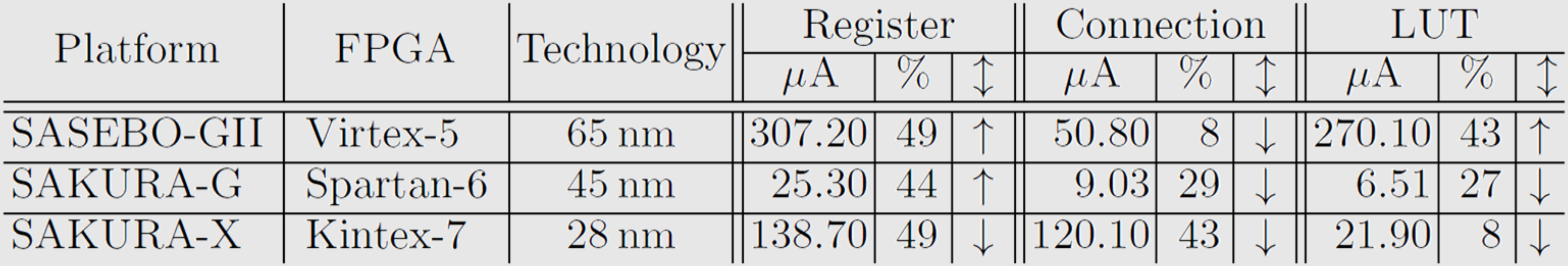


SAKURA-G (Spartan-6)



SAKURA-X (Kintex-7)

Preliminary Tests (summary)

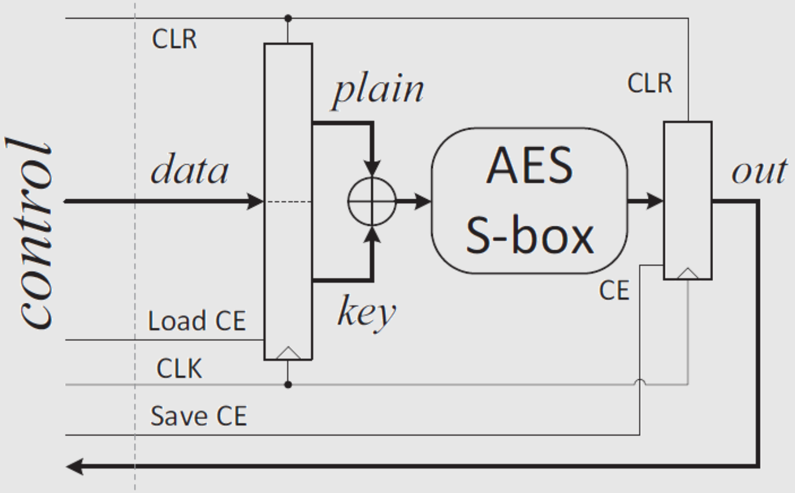


Platform	FPGA	Technology	Register			Connection			LUT		
			μA	%	↕	μA	%	↕	μA	%	↕
SASEBO-GII	Virtex-5	65 nm	307.20	49	↑	50.80	8	↓	270.10	43	↑
SAKURA-G	Spartan-6	45 nm	25.30	44	↑	9.03	29	↓	6.51	27	↓
SAKURA-X	Kintex-7	28 nm	138.70	49	↓	120.10	43	↓	21.90	8	↓

- Temperature of the tests/devices was not the same
  – results vary by slight temperature change

Preliminary Tests (Sbox)

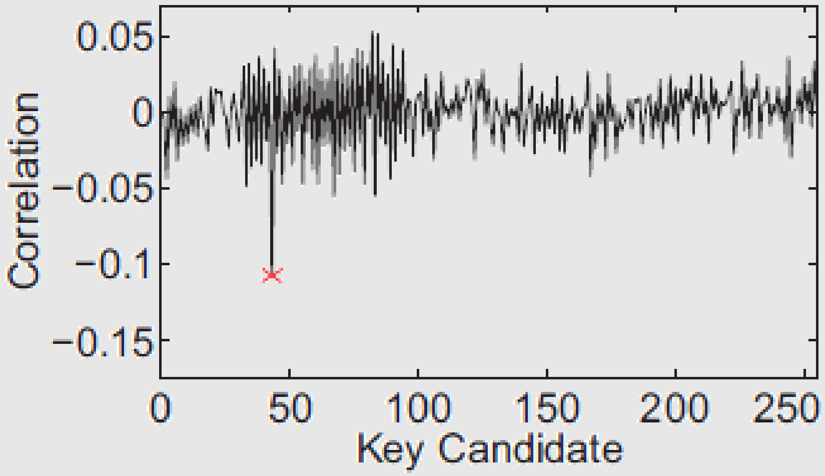
- Single Key XOR + AES Sbox
- Canright’s design
- SAKURA-X (Kintex-7)



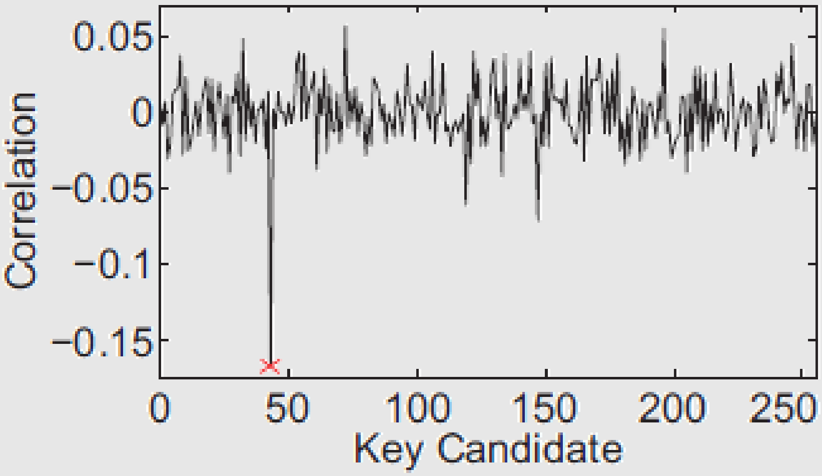
- Due to temperature change
  - Two consecutive measurements of RESET and DATA
  - L_{DATA}-L_{RESET} as the leakage corresponding to DATA
- Measure right before saving the Sbox output in register
- Two placements for Sbox and output registers distance

Preliminary Tests (Sbox)

- 10,000 measurements for a single key and random input
- CPA by Hamming weight model (Sbox output)
  - not a necessarily perfect model
    - depends on placement and routing
  - better model by e.g., profiling (moments-correlating DPA)



Normal Placement



Wide Placement

Issues

- Main energy-consuming component: connections in FPGAs
  - not the same in case of ASICs
- Dedicated measurement setup
  - low-noise ***DC*** amplifier
  - ability to control the CLOCK
    - Many other attacks, e.g., fault attacks, are possible
- Appropriate box to precisely control the temperature
  - not a thermobox
- Information about the device under attack is required
  - e.g., which clock cycle to stop the CLOCK and measure
- Longer measurement procedure vs. dynamic
- Lower SNR compared to dynamic

Final Message

- Static power side-channel analysis is possible, but
  - shown results are preliminary
  - more research in this area needed
    - dedicated measurement setup
    - in which scenarios it is favorable than dynamic one?
    - what is the behavior of the commonly-known countermeasures?
    - how well the results match with those of an ASIC?

Thanks!
Any questions?

amir.moradi@rub.de

Embedded Security Group, Ruhr University Bochum, Germany