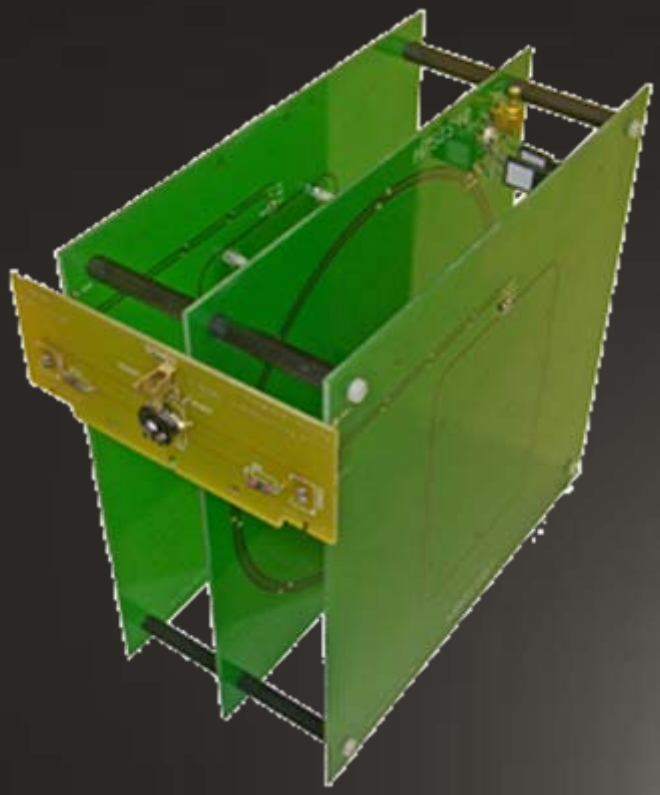
Test Apparatus for Side-Channel Resistance Compliance Testing

Michael Hutter, Mario Kirschbaum,
Thomas Plos, Jörn-Marc Schmidt

What is this talk about?

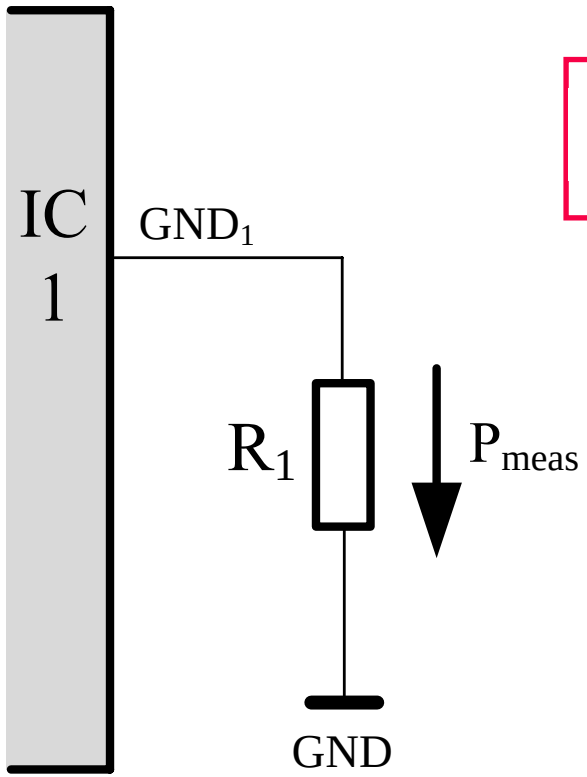
- Challenge
  - How to quantify side-channel resistance?
  - How to estimate the security level?
  - How to perform SCA compliance testing?

- Proposal
  - Non-invasive attack testing apparatus



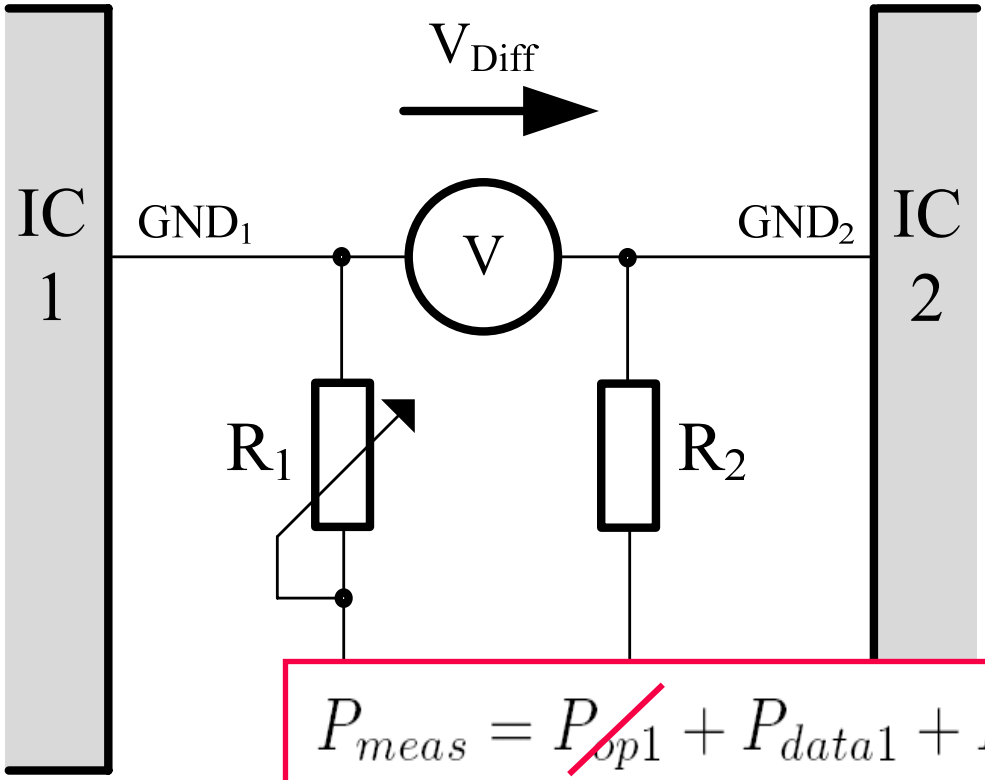
ISO/IEC 10373-6

The Classical SCA Setup



$$P_{meas} = P_{op} + P_{data} + P_{prox.noise} + P_{dev.noise}$$

The Proposed Apparatus



$$P_{meas} = \cancel{P_{op1}} + P_{data1} + \cancel{P_{prox.noise1}} + P_{dev.noise1} - \left(\cancel{P_{op2}} + P_{data2} + \cancel{P_{prox.noise2}} + P_{dev.noise2}\right)$$

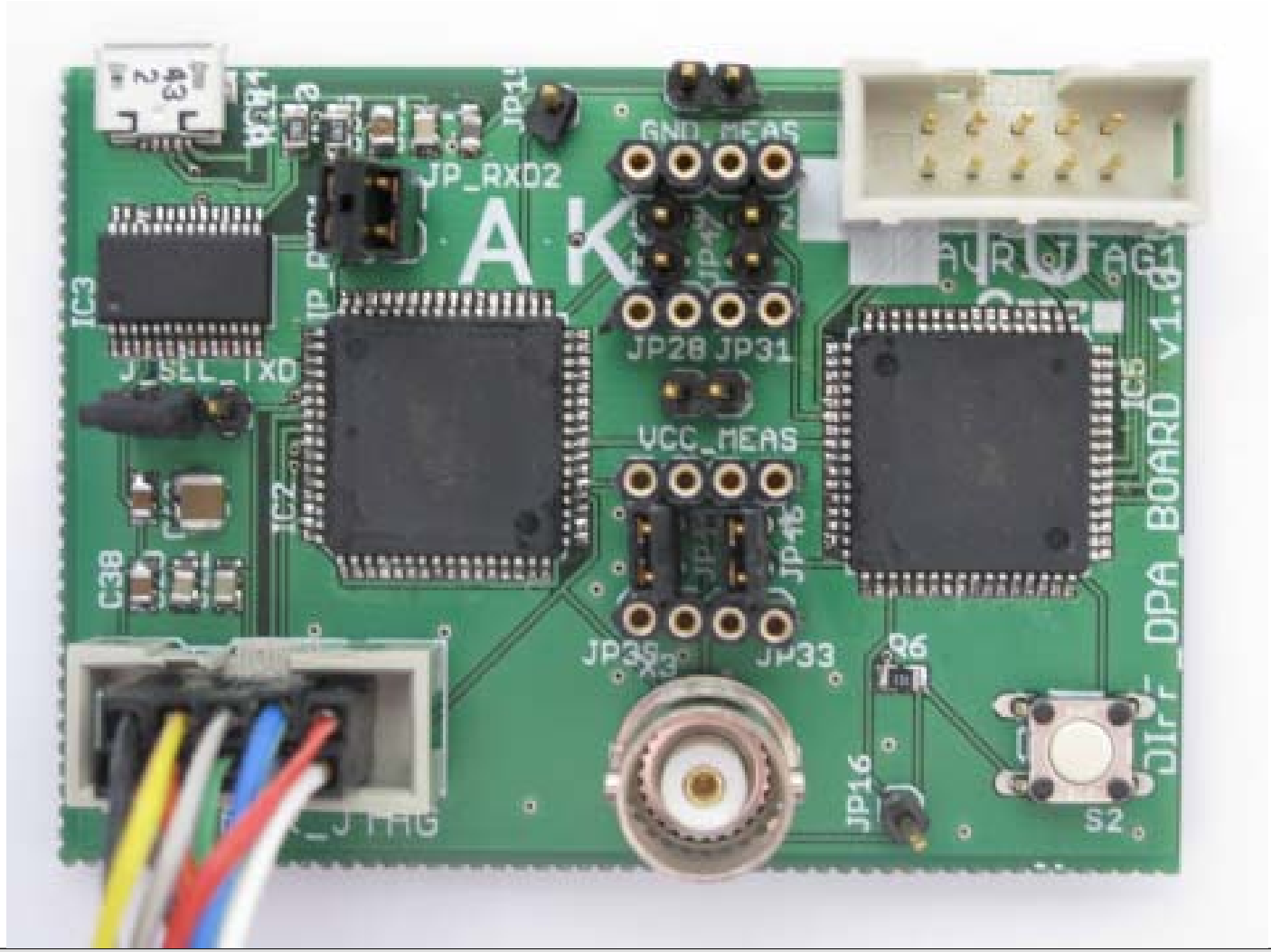
What are the Advantages?

1. Reduction of noise

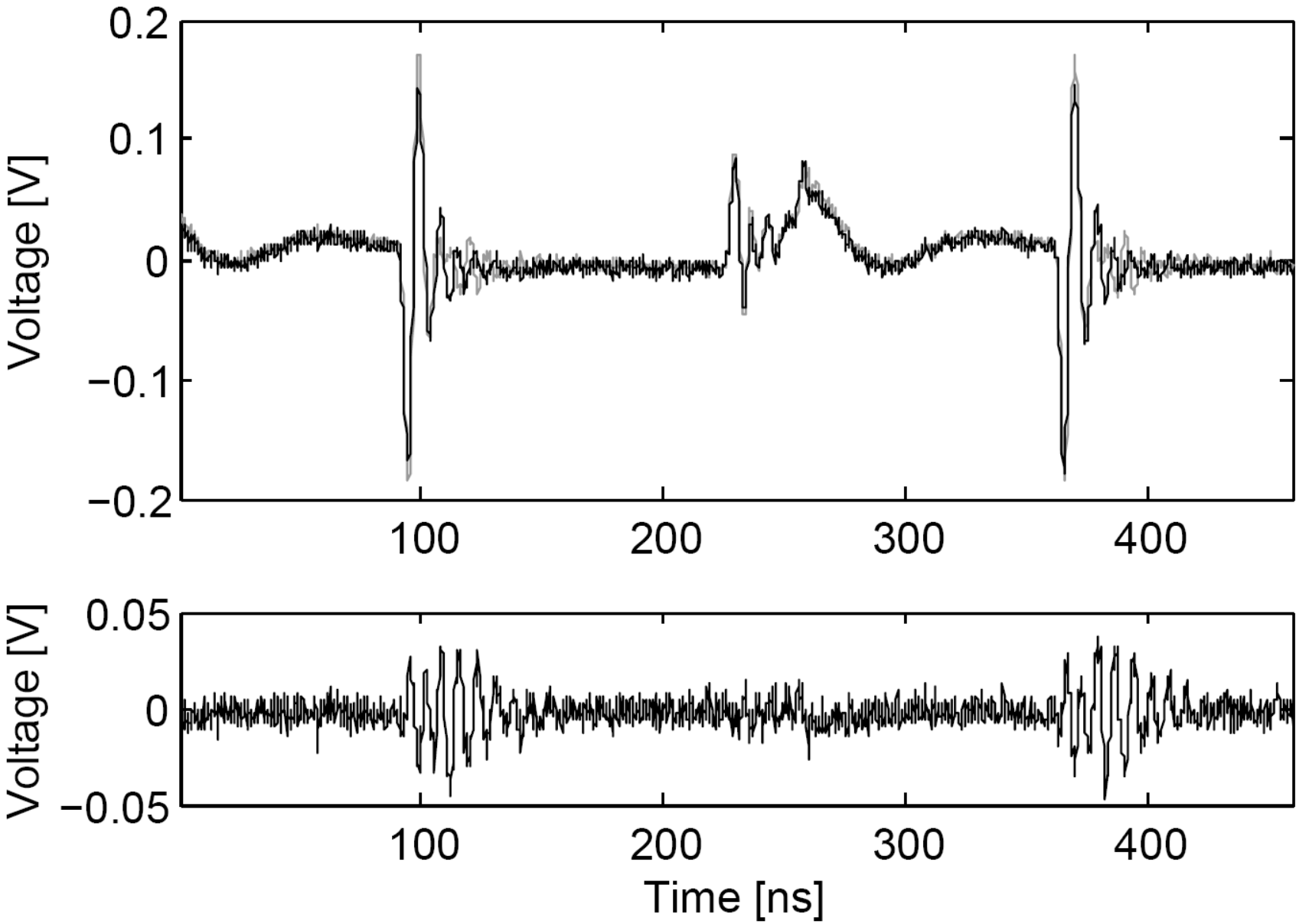
2. Higher measurement sensitivity

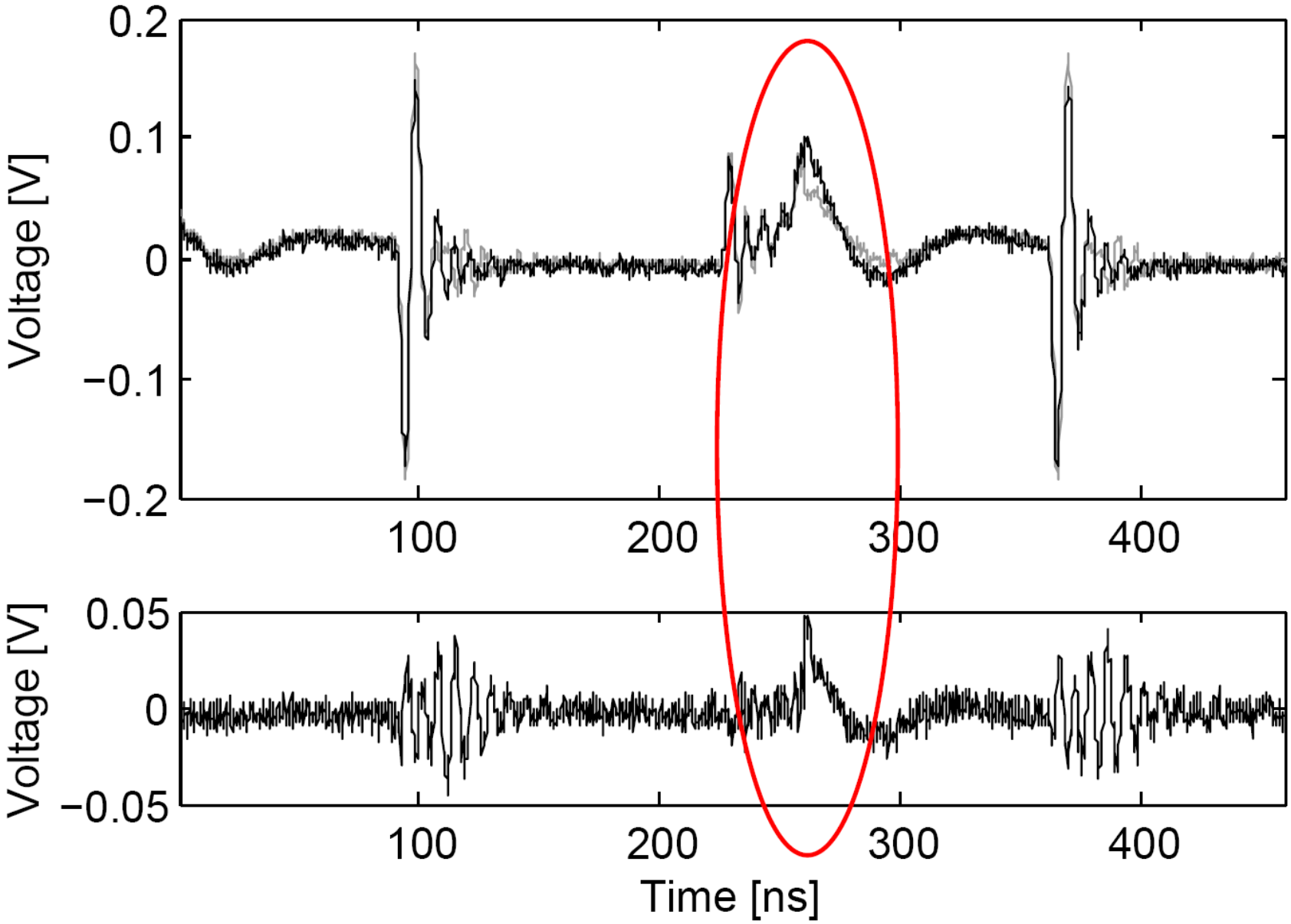
The AT89S8253 Apparatus

The ATmega128 Apparatus



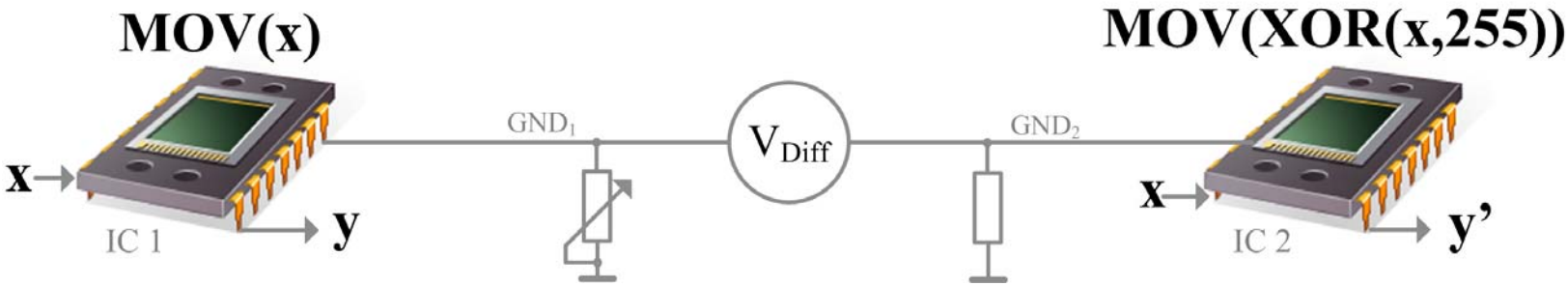
The GRANDESCA Apparatus


0.2
0.1
0
−0.1
−0.2
Voltage [V]
100
200
300
400
0.05
0
−0.05
Voltage [V]
100
200
300
400
Time [ns]


0.2
0.1
0
−0.1
−0.2
Voltage [V]
100
200
300
400
0.05
0
−0.05
Voltage [V]
100
200
300
400
Time [ns]

Attack Scenarios

1. White-box evaluation
   - Target: MOV operation

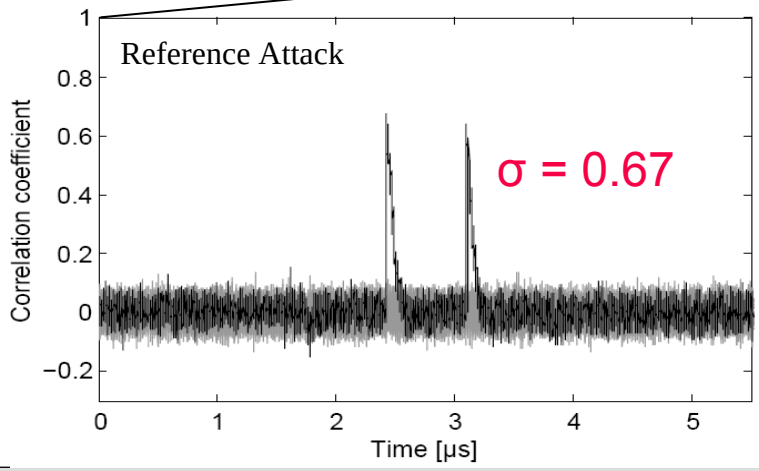


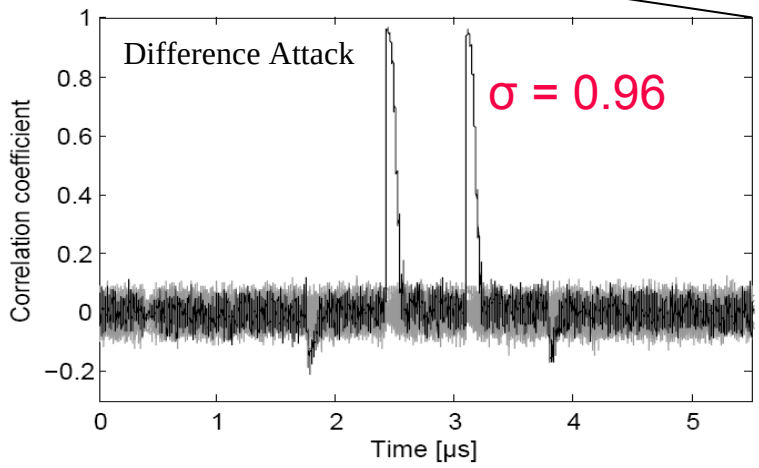
2. Black-box evaluation
   - Target: 1st S-box output of an AES-128 encryption (round 1)
     - IC_1: random input
     - IC_2: zero input

Results of Attacks



	AT89S8253	ATmega128	8051 GRANDESCA CMOS	8051 GRANDESCA iMDPL
Reference Attack	0.83	0.67	0.11	0.05
Difference Attack	0.99	0.96	0.22	0.16
Improvement	**0.16**	**0.29**	**0.11**	**0.11**
Improvement [%]	**20**	**43**	**100**	**220**





AES Results

	GRANDESCA AES COPROCESSOR CMOS							
Byte transition	$2 \rightarrow 1$	$3 \rightarrow 2$	$4 \rightarrow 3$	$16 \rightarrow 4$	$1 \rightarrow 5$	$11 \rightarrow 6$	$3 \rightarrow 7$	$4 \rightarrow 8$
Reference attack	0.0174	0.0163	0.0164	0.0315	0.0133	0.0170	0.0155	0.0292
Difference attack	0.0226	0.0239	0.0278	0.0436	0.0223	0.0293	0.0267	0.0466
Improvement	**0.0052**	**0.0076**	**0.0114**	**0.0121**	**0.009**	**0.0123**	**0.0112**	**0.0174**
Improvement [%]	**30**	**46**	**69**	**38**	**67**	**72**	**72**	**59**

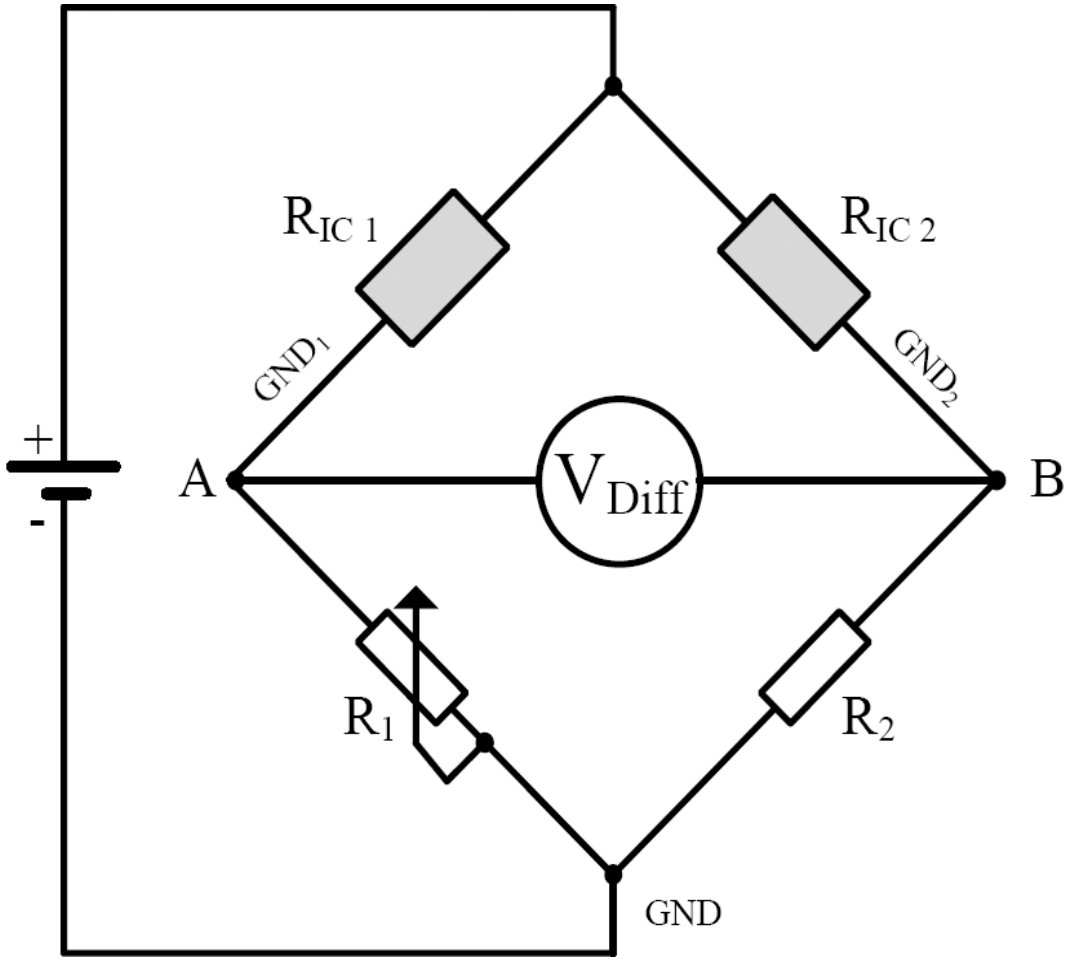
Summary

- Using two devices improves attack
- Less noise
- Better acquisition resolution
- Can be used for
  - Device characterization, profiling, countermeasure evaluation, SCA-resistance tests, compliance testing, attacks, …

SEnSE
Secure Entities for Smart Environments

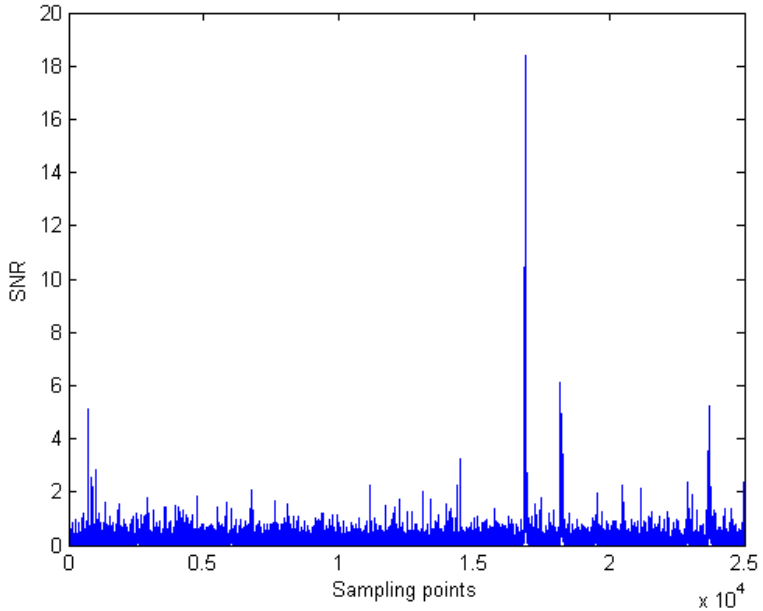
Michael Hutter
IAIK – Graz University of Technology
michael.hutter@iaik.tugraz.at
www.iaik.tugraz.at

The Wheatstone Bridge



Signal-to-Noise Ratio

Reference Attack



Difference Attack