Successfully Attacking Masked AES Hardware Implementations

Stefan Mangard, Norbert Pramstaller,

and Elisabeth Oswald

Side-Channel Analysis Lab

VLSI

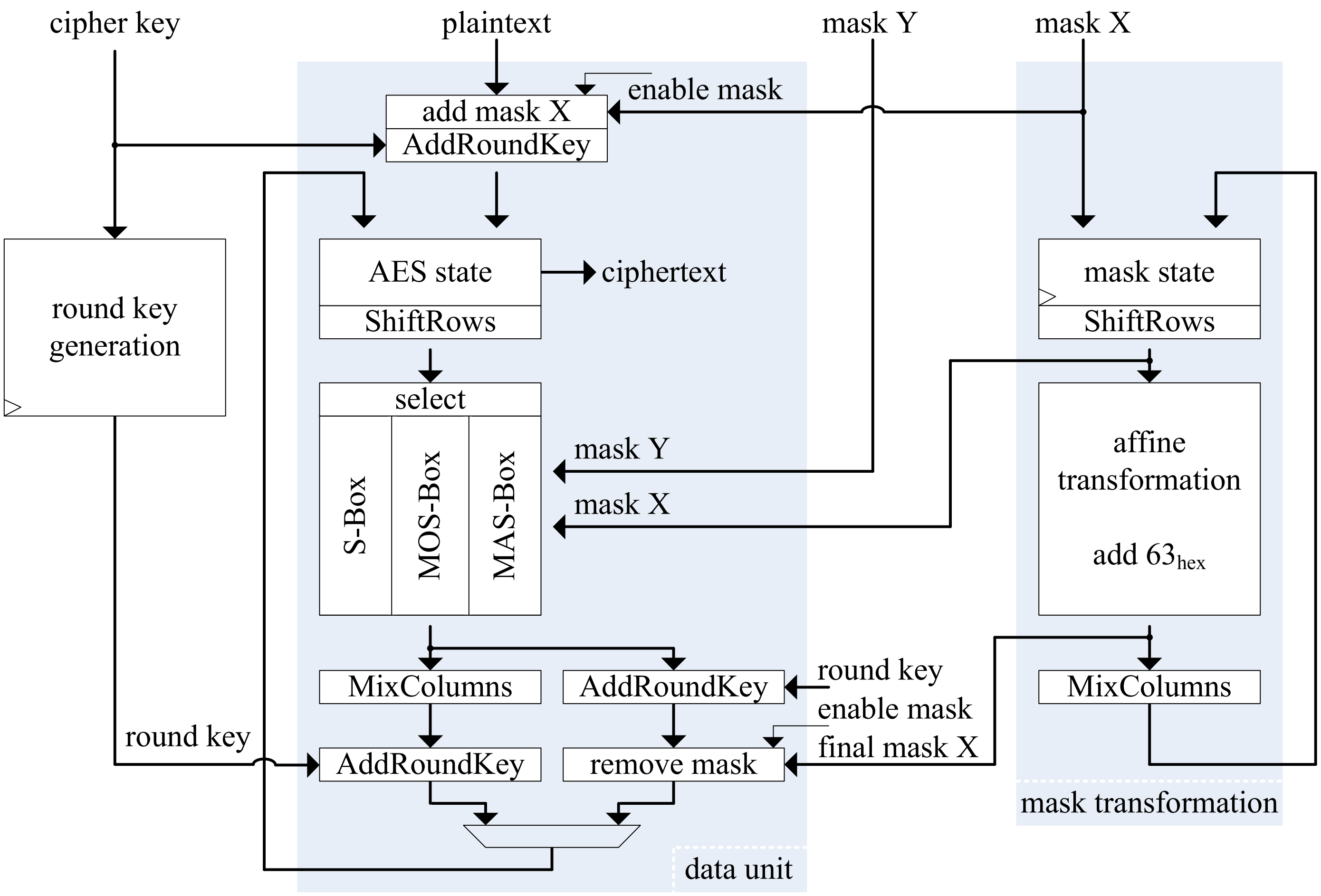
Presentation Outline

- Masking schemes for AES
- Implementation of masking schemes on a chip
- Results of attacks on the chip
- Conclusions and future work

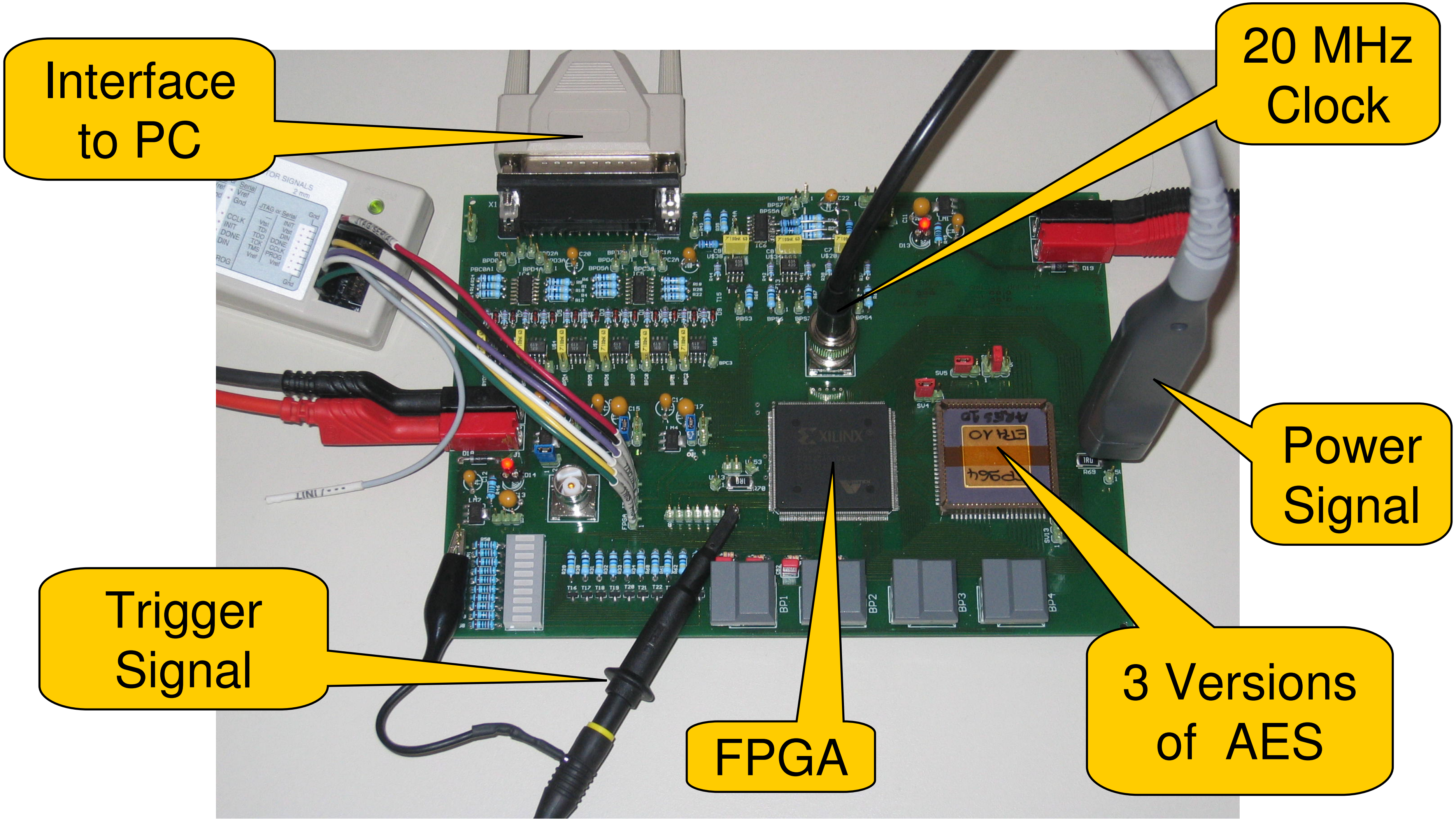
Masking Schemes for AES

- Multiplicative schemes having the “zero” problem
  - CHES 2001: Akkar, Giraud
  - CHES 2002: Trichina, De Seta, Germani
- Provably secure schemes:
  - SAC 2004: Blömer, Gerado, Krummel
  - FSE 2005: Oswald, Mangard, Pramstaller, Rijmen
- Other schemes:
  - CHES 2002: Golić, Tymen
  - AES 2004: Trichina, Korkishko

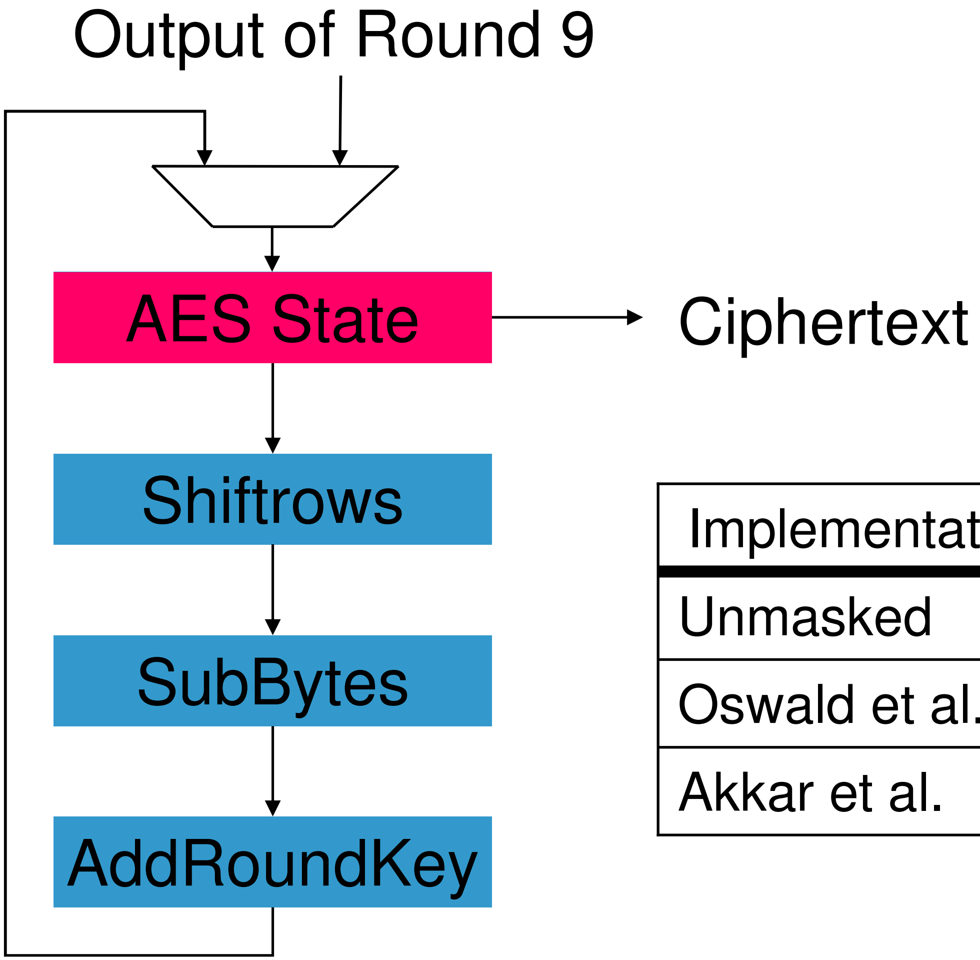
Block Diagram of the Chip



Measurement Setup

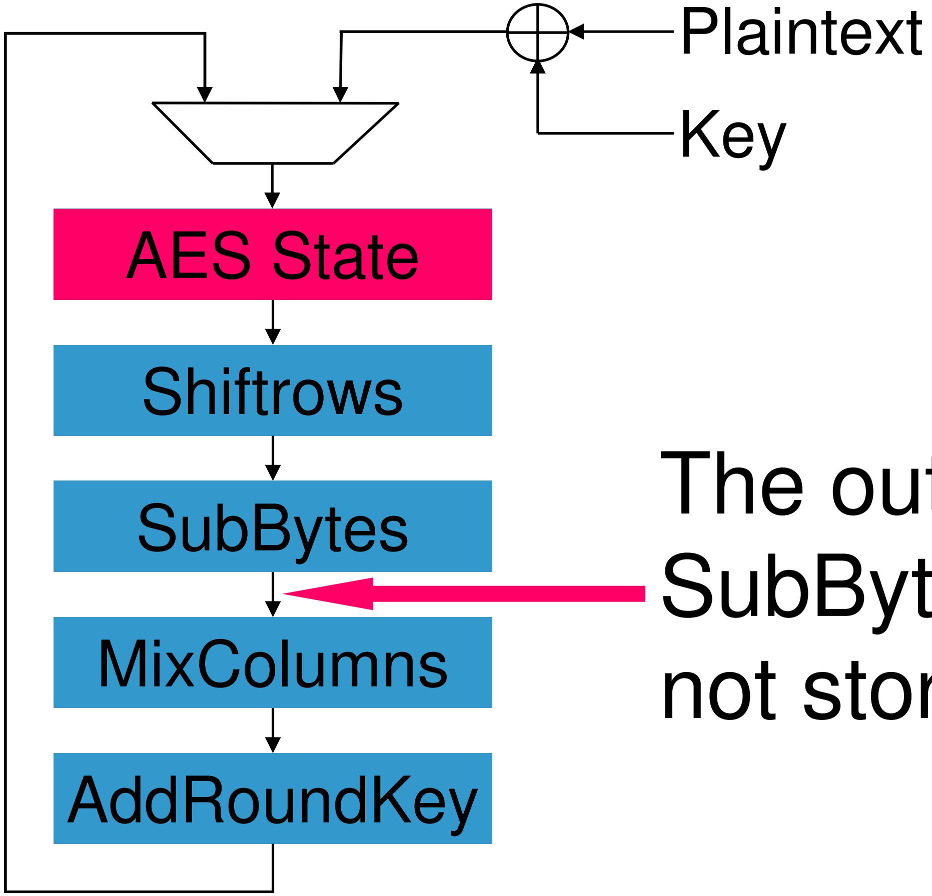


Attacking Registers in the Final Round



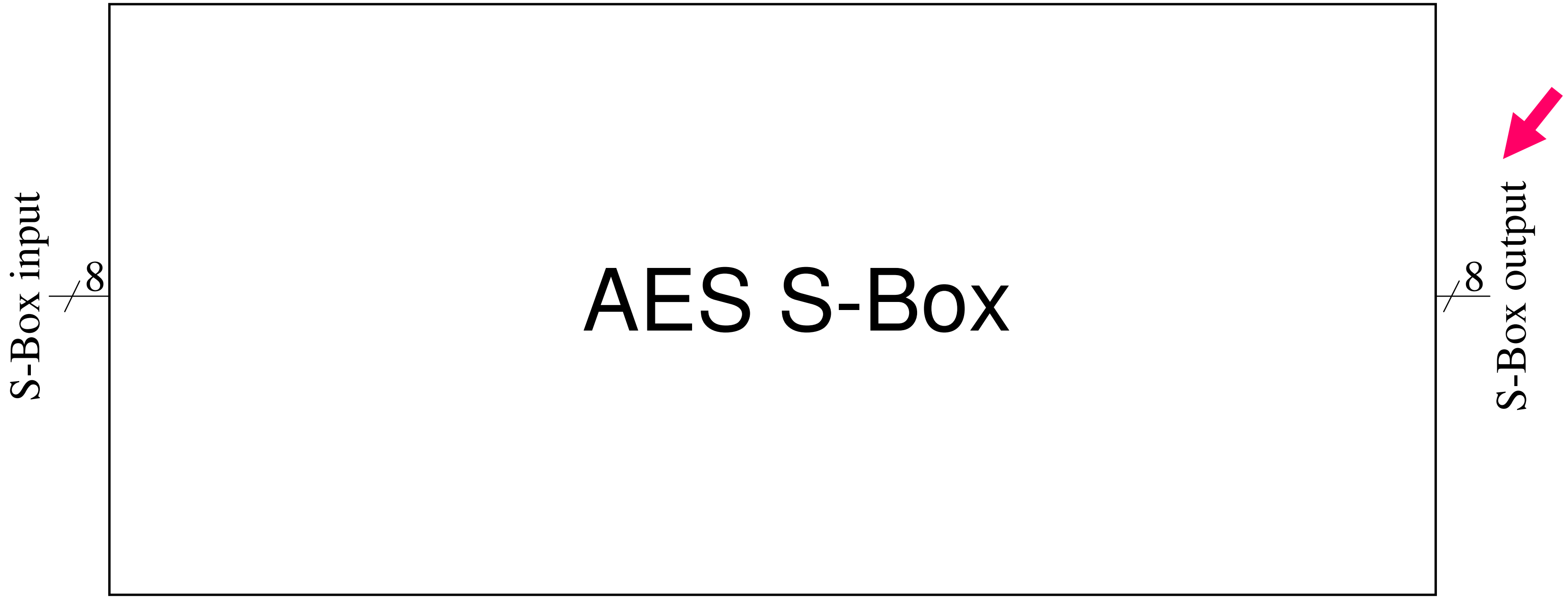
Implementation	Needed Measurements
Unmasked	120,000
Oswald et al.	1,000,000
Akkar et al.	1,000,000

Attacking the Output of SubBytes

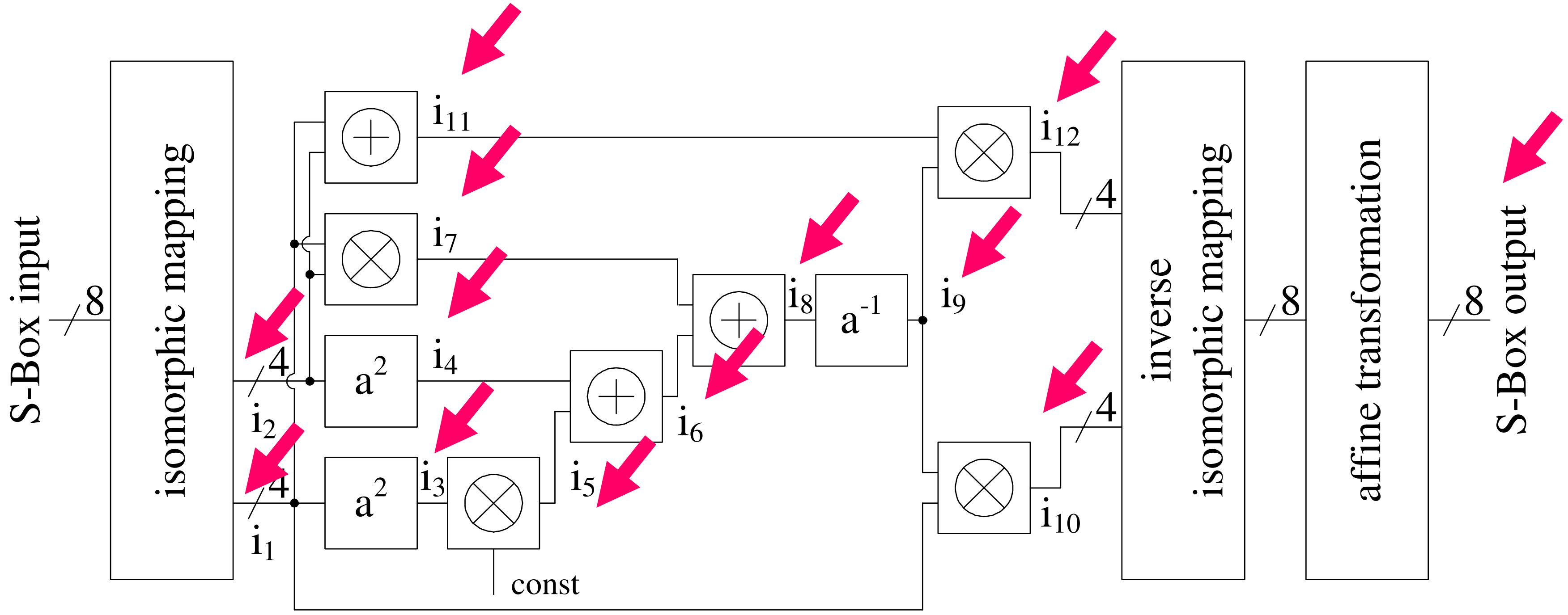


The output of the SubBytes transformation is not stored in registers!

Attacks on an Unmasked S-Box

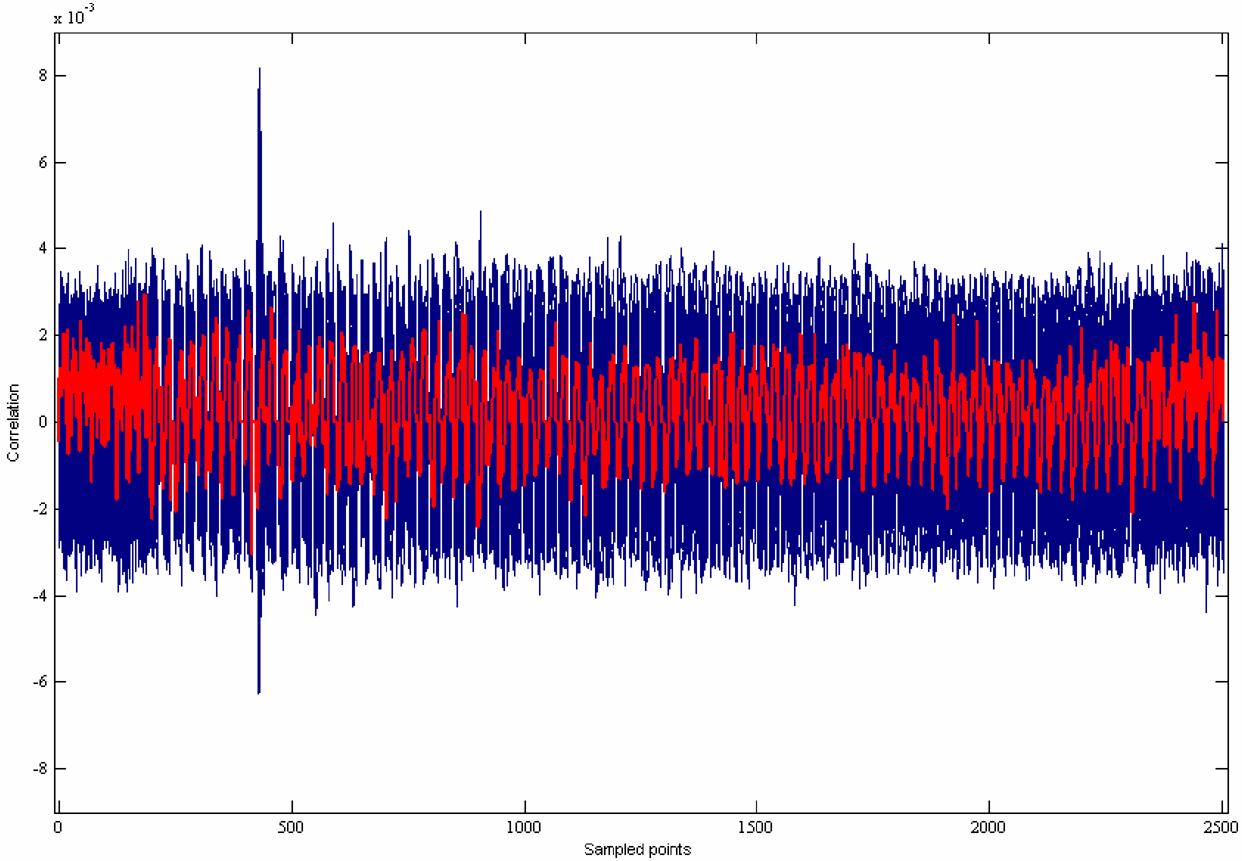


Attacks on an Unmasked S-Box



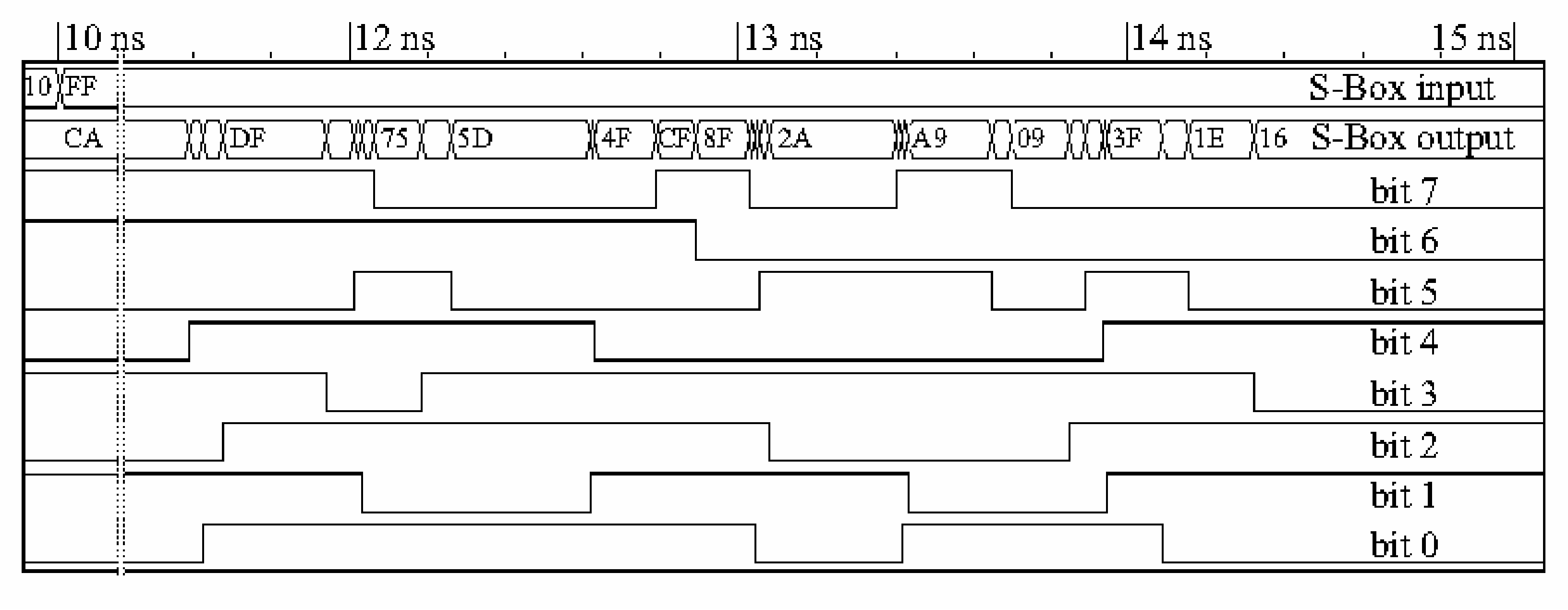
Attacks based on predicting the Hamming weight and individual bits have been performed

Results of Attacks on the Unmasked S-Box Implementations

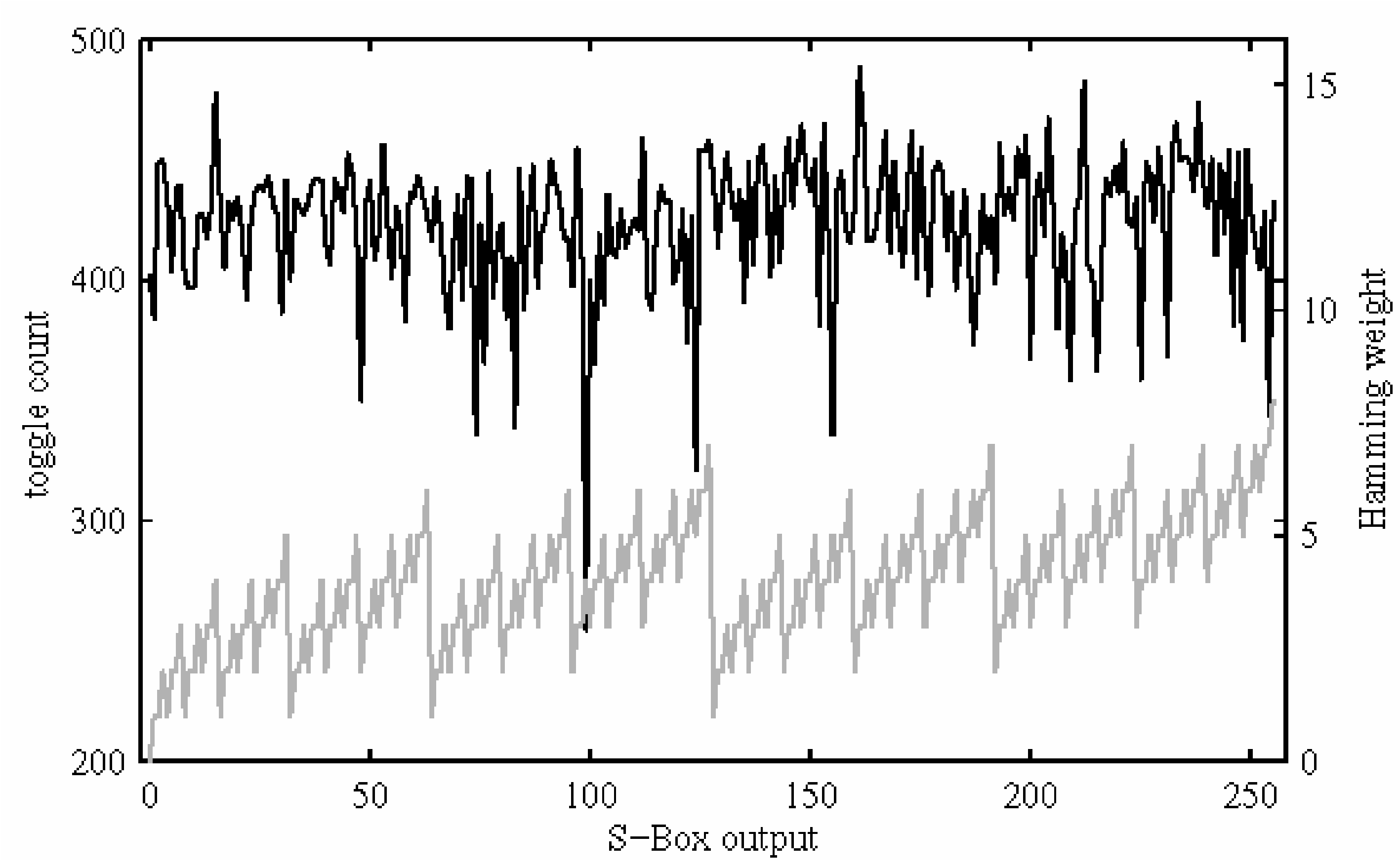


The correct key was not revealed (1 Mio Measurements)!

The Switching Activity of the Unmasked S-Box



The Switching Activity of the Unmasked S-Box



Average toggle count for the 256 possible outputs
(65536 simulations)

Results of Attacks Using the Simulated Power Model

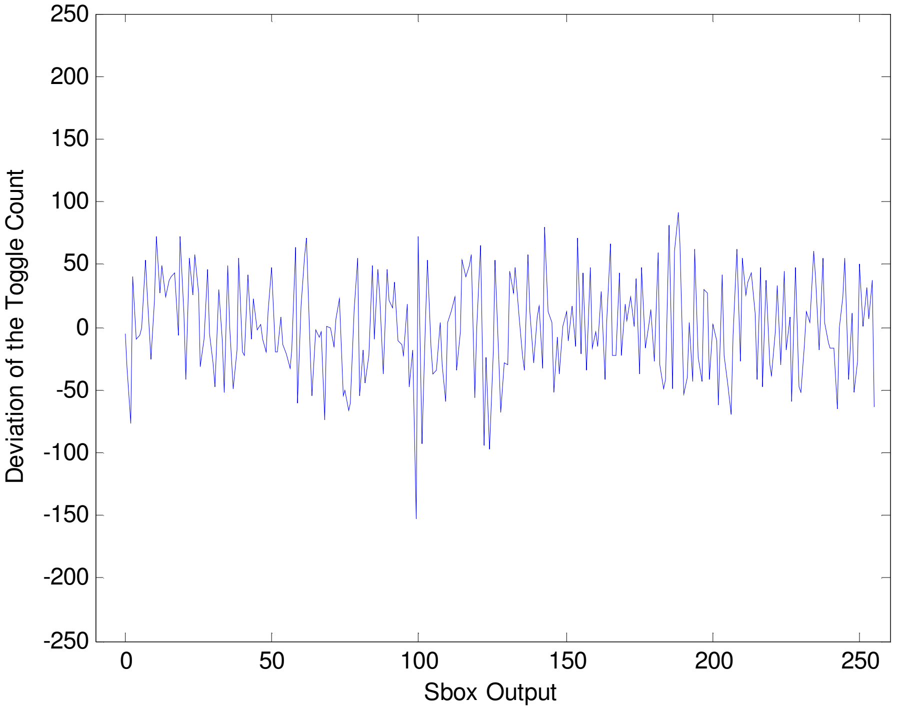
	Flip Flops	Sbox (simple power model)	Sbox (characterization)
Unmasked	120,000	220,000	25,000

Using the simulation result as power model, an attack was possible

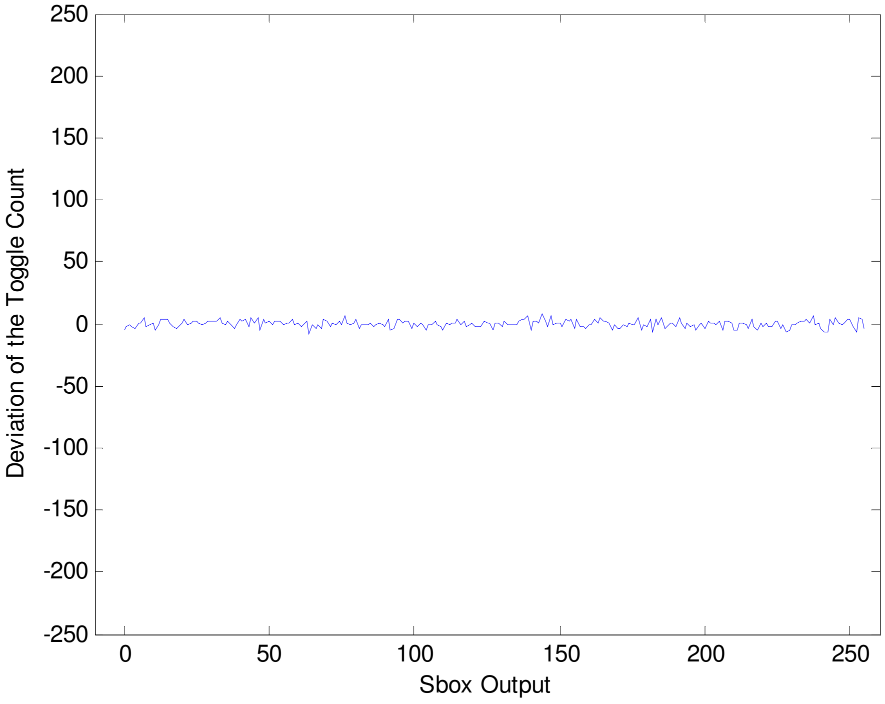
Results of Attacks with Simple Power Models

Implementation	Flip Flops	Sbox (simple power model)
Unmasked	120,000	220,000
Oswald et al.	1,000,000	250,000
Akkar et al.	1,000,000	900,000

The Switching Activity of the Masked Sbox (Oswald et al.)



Simulation based on the back-annotated netlist



Functional simulation based on the netlist (timing information is ignored)

Summary of all Attack Results

Implementation	Flip Flops	Sbox (simple power model)	Sbox (characterization)
Unmasked	120,000	220,000	25,000
Oswald et al.	1,000,000	250,000	30,000
Akkar et al.	1,000,000	900,000	130,000

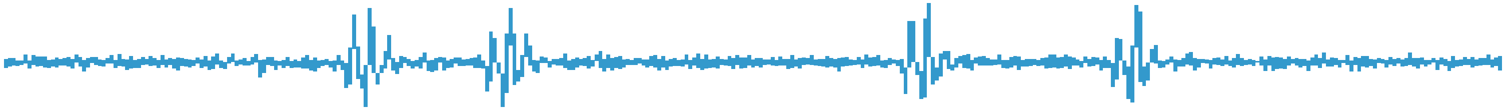
Conclusions and Future Work

- No significant difference in attacking masked and unmasked S-Box implementations, if implemented in static CMOS
- We are currently analyzing, if there are “general power models”
- Masking schemes need to consider glitches

The Team

The Side-Channel Analysis Lab

http://www.iaik.at/research/sca-lab



Stefan Mangard, Norbert Pramstaller,
and Elisabeth Oswald

Chip Design and Production in Cooperation With
Frank K. Gürkaynak (ETH Zürich) and
Simon Häne (ETH Zürich)