SCIENCE ▪ PASSION ▪ TECHNOLOGY

TU Graz

in collaboration with:

ETH zürich

CRYPTOGRAPHY RESEARCH

Towards Evaluating DPA Countermeasures for KECCAK on a Real ASIC

Michael Mühlberghuber — **ETH Zurich, IIS**
Thomas Korak — **TU Graz, IAIK**
Michael Hutter — **Cryptography Research**

14.04.2015

Contributions

- Taped-out ASIC named ZORRO
- Three distinct architectures of `SpongeWrap`-based AE algorithm
- Secured against DPA attacks
  - 3-Share (Bertoni et al. [1])
  - 3-Share* (re-masking, Bilgin et al. [2])
  - 4-Share (Bilgin et al. [2])
  - Additional hiding countermeasure
- Design goal: low area
- Smallest architecture: 14 kGE

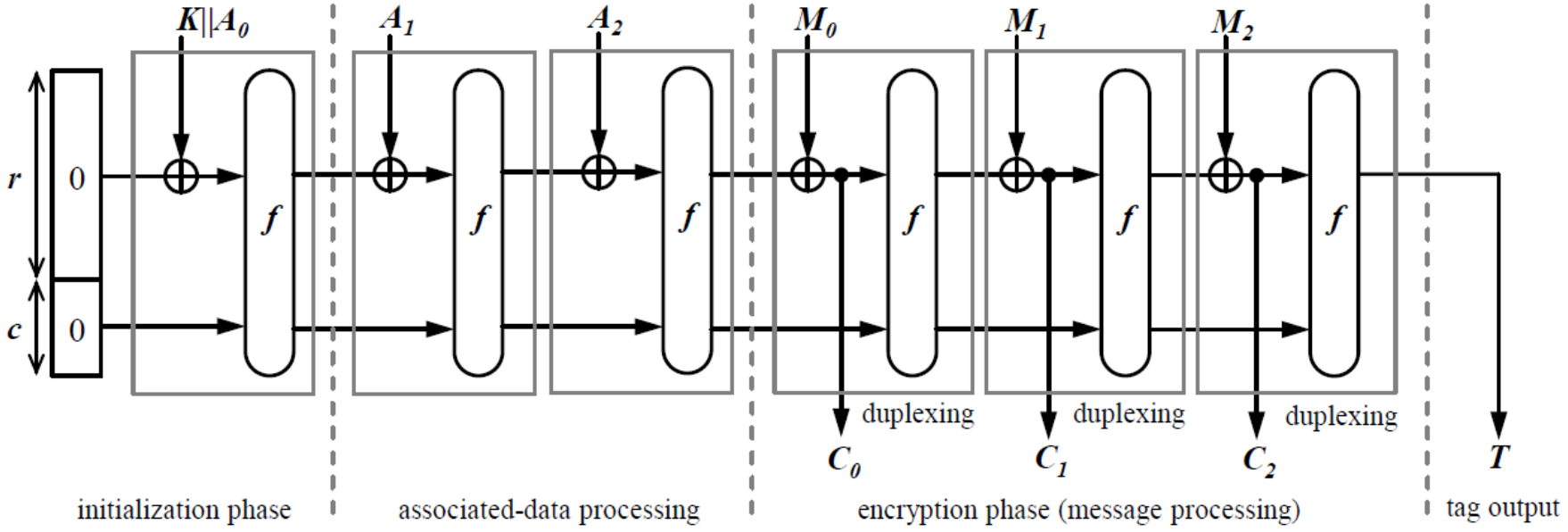
Contributions

- First DPA results
  - Unprotected < 100 measurements
  - Hiding 1 < 300 measurements
  - Hiding 15 < 5 000 measurements
  - 3-Share, HO-CPA ~ 70 000 measurements

Motivation

- Provide authenticity, integrity, and confidentiality services for resource-constrained devices
- Use well-analyzed algorithm (SHA3)
  - KECCAK-*f* permutation
  - `SpongeWrap` mode
- Protection against implementation attacks required
  - Secret Sharing
  - Hiding
- Develop an ASIC chip as an evaluation platform for DPA countermeasures: ZORRO

SpongeWrap Mode



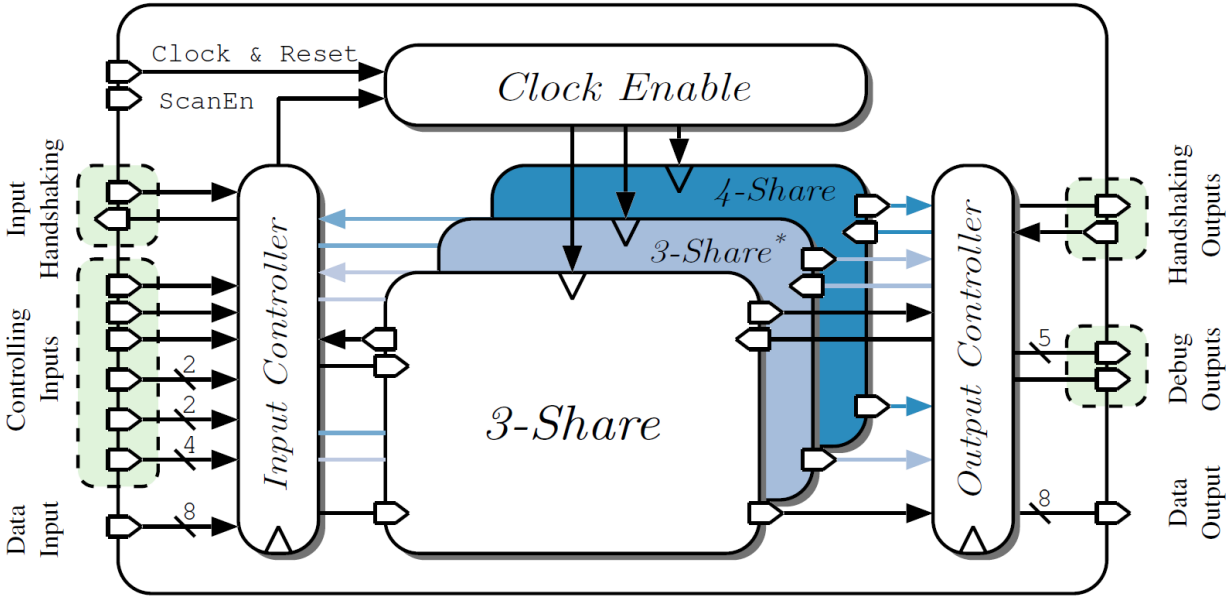
r = 1088 bits

c = 1600 - 1088 = 512 bits

|K| = 256 bits

$|A_0|$ = 1088 - 256 = 832 bits

Hardware Architecture of ZORRO



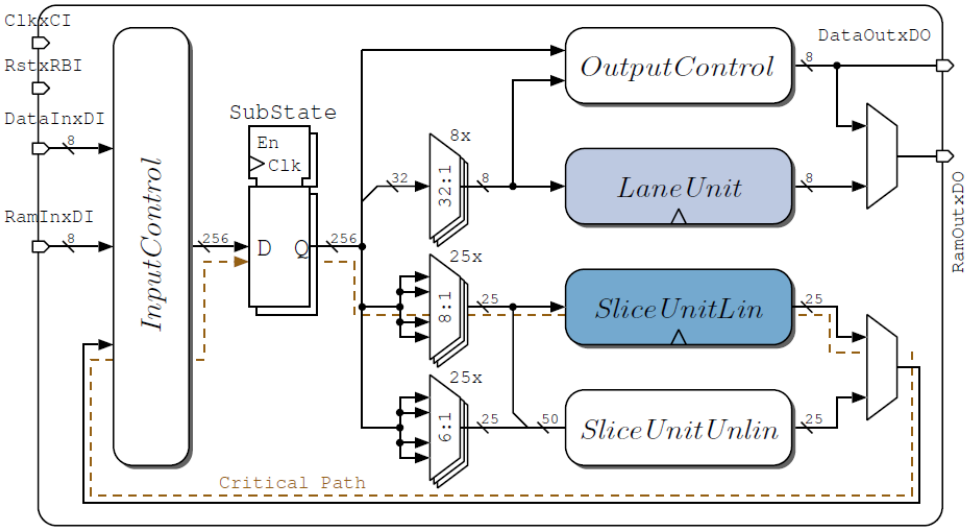
- AE algorithm based on KECCAK-*f*[1600]
- Evaluation platform for DPA countermeasures
- Three independent threshold implementations
- Random initialization values received from outside

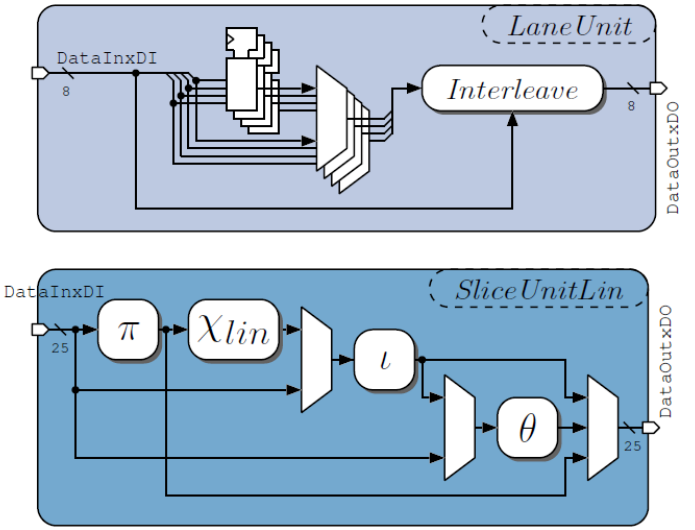
Hardware Architecture of Zorro

- RAM macro cell to store state
- Modified round schedule

$$R_1 = \theta \times \rho \qquad R_{2\ldots24} = \pi \times \chi \times \iota \times \theta \times \rho \qquad R_{25} = \pi \times \chi \times \iota$$

- Lane unit and slice unit





Results: Hardware Figures

- UMC 180nm CMOS technology
- Area breakdown after synthesis for 5ns

Component	Area [GE]	Area [%]
3-Share	13'370	30.5
Datapath & FSM	7'300	16.7
RAM	4'680	10.7
LFSR	300	0.7
SliceUnitLin	480	1.1
Others	610	1.3
*3-Share**	13'940	31.8
4-Share	16'190	37.0
I/O Interface	320	0.7
ZORRO Total	43'820	100.0

Results: Hardware Figures

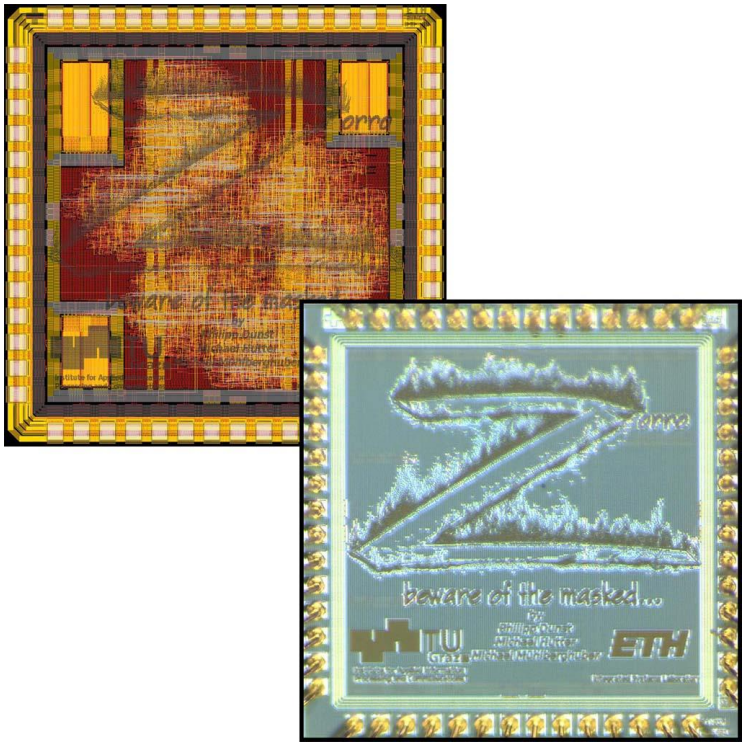
- Comparison with related work

Source	Techn. [nm]	Area [GE]	f_{max} [MHz]	Perf.† [Cycles]
Designs w/o DPA Countermeasures				
Pessl and Hutter [3]‡	130	5'522	61	22'570
Bilgin et al. [2]§	180	10'800	555	1'600
ZORRO in Normal Mode‡	180	13'370	200	21'888
3-Share-Secured Designs w/o Re-Masking				
Bertoni et al. [1]§	130	95'000	200	72
ZORRO *3-Share* Architecture‡	180	13'370	200	113'184
3-Share-Secured Designs w/ Re-Masking				
Bilgin et al. [2]§	180	33'100	553	1'625
ZORRO *3-Share** Architecture‡	180	13'940	200	113'184
4-Share-Secured Designs				
Bilgin et al. [2]§	180	43'100	572	1'600
ZORRO *4-Share* Architecture ‡	180	16'190	200	149'640

† KECCAK-f permutation ‡ Block size of 1088 bits § Block size of 1024 bits

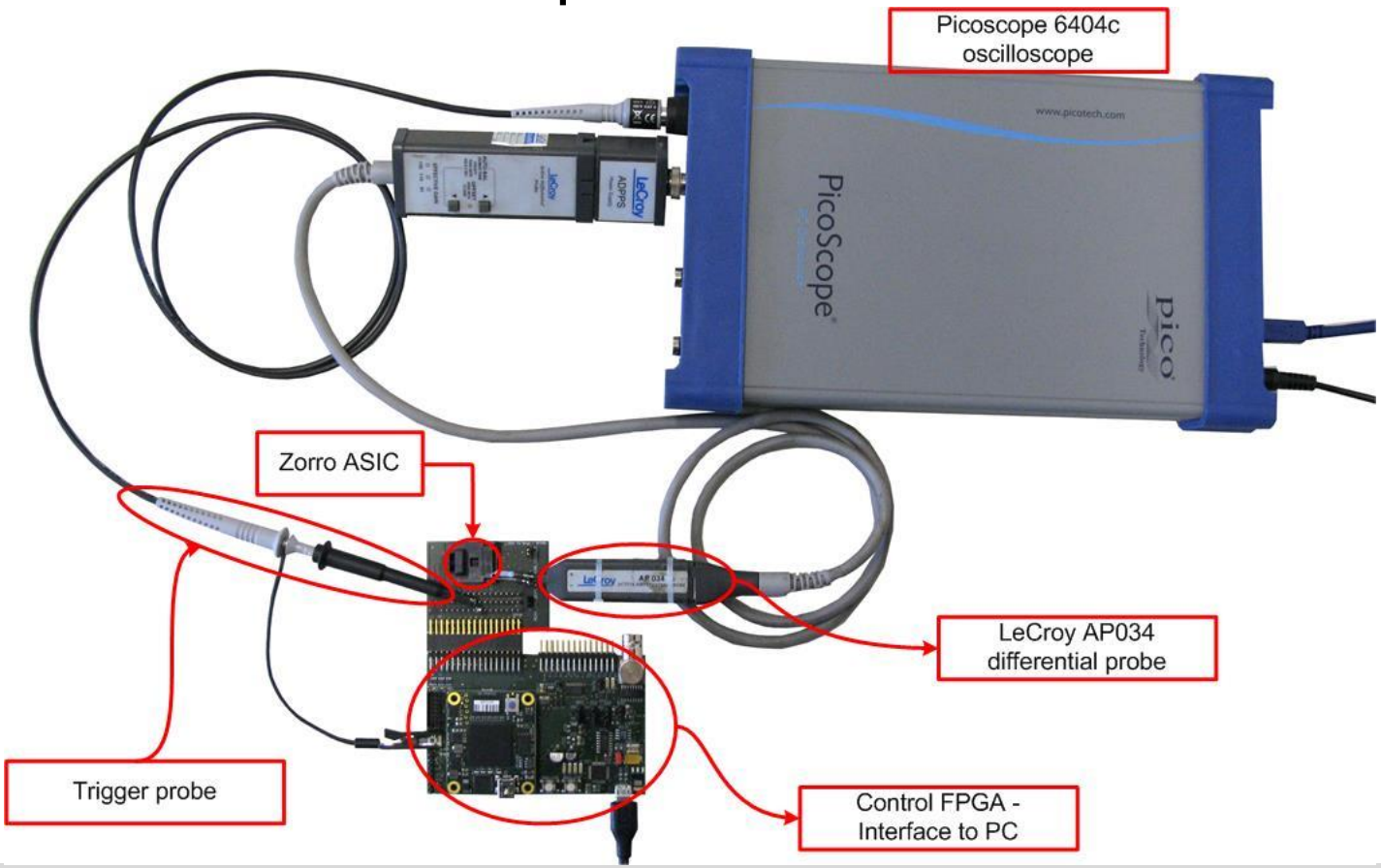
Results: Hardware Figures

- Tapeout version of ZORRO
  - DFT circuitries added
  - Area increase < 5%
    - 3-Share 14.0 kGE (+630 GE)
    - 3-Share* 14.5 kGE (+560 GE)
    - 4-Share 17.0 kGE (+810 GE)



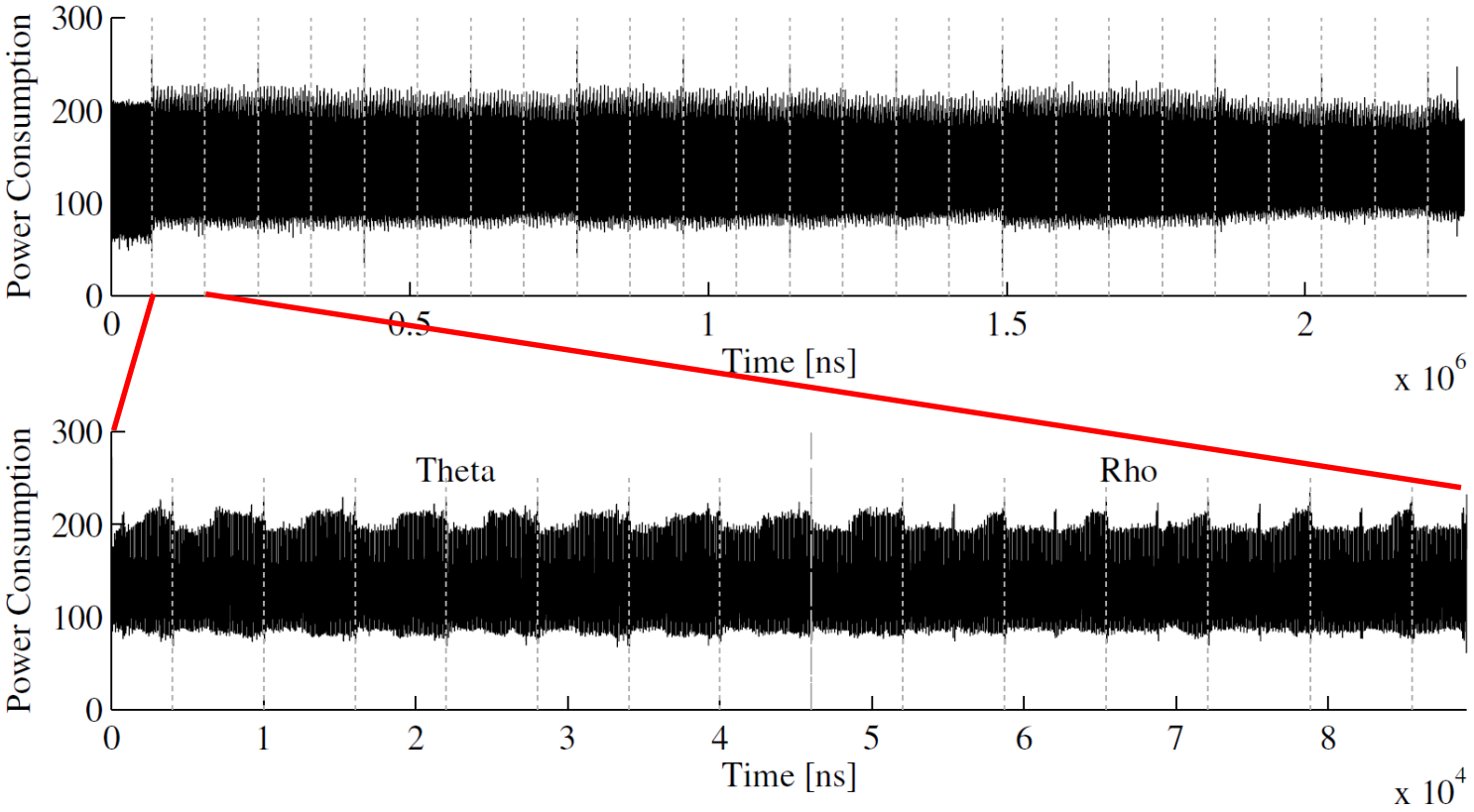
Results: Power Analysis

- Measurement setup



Results: Power Analysis

- First power trace (plain core)



Results: Power Analysis

- Target of the attacks: 1st θ step
- Initial state

$$S_{init} = K||A_0$$

- State after slice-based transform in round 1

$$S_1 = \theta(K||A_0)$$

- Power model

$$PM = HD(S_{init}, S_1)$$

Results: Power Analysis

Mode	ti	Win.	ρ_c	N_{tr}
Normal	1		0.700	<100
Hiding 1	16	N Y	0.049 0.237	285
Hiding 2	24	N Y	0.031 0.160	625
Hiding 15	128	N Y	-------- 0.057	4 925
MM 3-Share			0.016	70 000

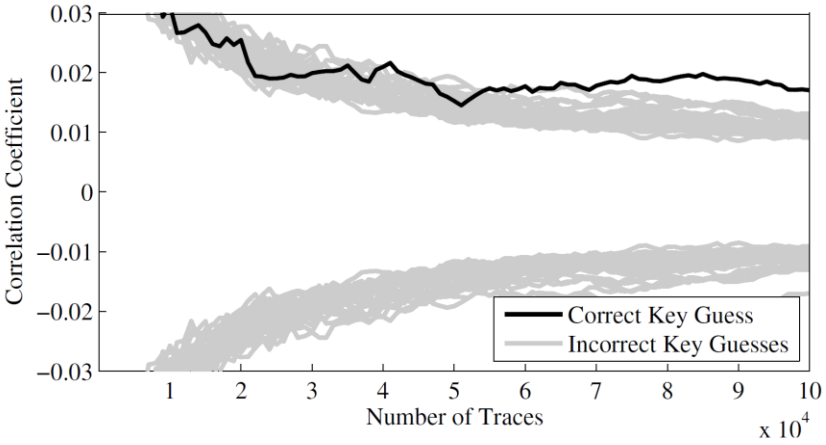
Results: Power Analysis

Mode	ti	Win.	ρ_c	N_{tr}
Normal	1		0.700	<100
Hiding 1	16	N Y	0.049 0.237	285
Hiding 2	24	N Y	0.031 0.160	625
Hiding 15	128	N Y	-------- 0.057	4 925
MM 3-Share			0.016	70 000

- 3rd order CPA
- Centralized product combining [4]
- Similar results for 3-Share*

Results: Power Analysis

Mode	ti	Win.	ρ_c	N_{tr}
Normal	1		0.700	<100
Hiding 1	16	N Y	0.049 0.237	285
Hiding 2	24	N Y	0.031 0.160	625
Hiding 15	128	N Y	-------- 0.057	4 925
MM 3-Share			0.016	70 000



- 3rd order CPA
- Centralized product combining [4]
- Similar results for 3-Share*

Conclusion & Future Work

- Taped-out ASIC named ZORRO
- DPA-countermeasure evaluation platform
- First DPA-attack results
  - 3rd order CPA – 70 000 measurements

- Analyze 4-Share architecture
- Target χ step – differences between 3-Share and 3-Share* architecture?
- Leakage assessment using fixed-vs-random t-test

References

[1] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Building Power Analysis Resistant Implementations of Keccak. In 2nd SHA-3 Candidate Conference, 2010.

[2] B. Bilgin, S. Nikova, V. Rijmen, V. Nikov, J. Daemen, and G. V. Assche. Efficient and First-Order DPA Resistant Implementations of KECCAK. In A. Francillon and P. Rohatgi, editors, CARDIS 2013, volume 8419 of LNCS. Springer, 2013.

[3] P. Pessl and M. Hutter. Pushing the Limits of SHA-3 Hardware Implementations to Fit on RFID. In CHES 2013, volume 8086, pages 126141. Springer, 2013.

[4] E. Prouff, M. Rivain, and R. Bévan. Statistical analysis of second order differential power analysis. Computers, IEEE Transactions on, 58(6):799811, 2009.

SCIENCE ▪ PASSION ▪ TECHNOLOGY

TU Graz

in collaboration with:

ETH zürich

CRYPTOGRAPHY RESEARCH

Towards Evaluating DPA Countermeasures for KECCAK on a Real ASIC

Michael Mühlberghuber — **ETH Zurich, IIS**
Thomas Korak — **TU Graz, IAIK**
Michael Hutter — **Cryptography Research**

14.04.2015