RUB

RUHR-UNIVERSITÄT BOCHUM

Side-Channel Countermeasures for Hardware: is There a Light at the End of the Tunnel?

11. Sep 2013

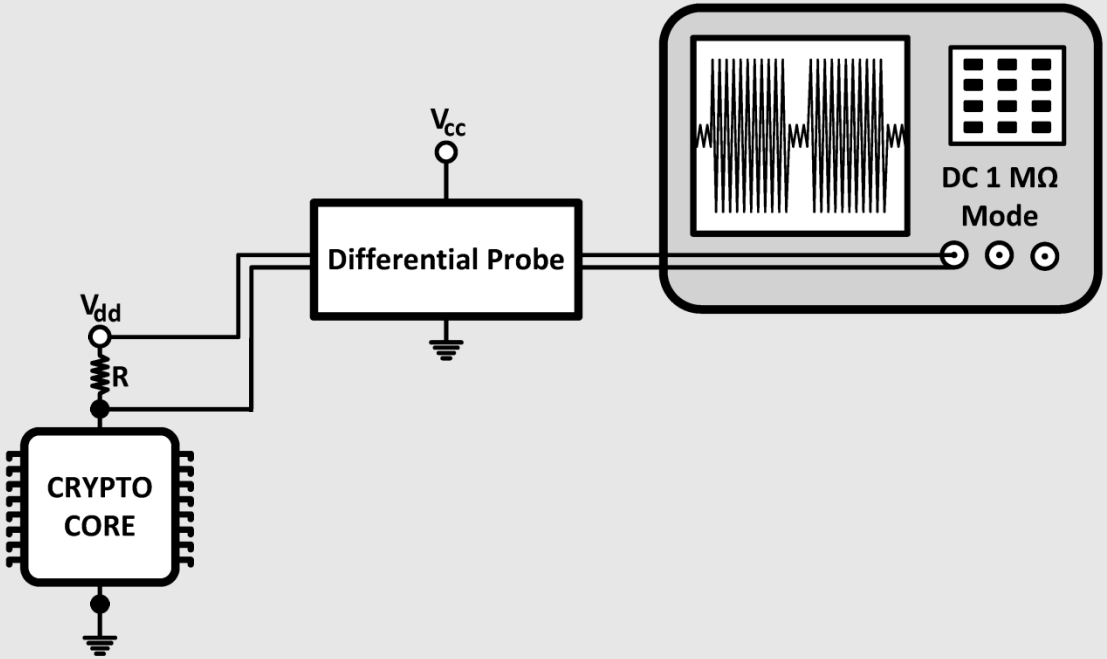
Amir Moradi
Ruhr University Bochum

hgi Horst Görtz Institute for IT-Security

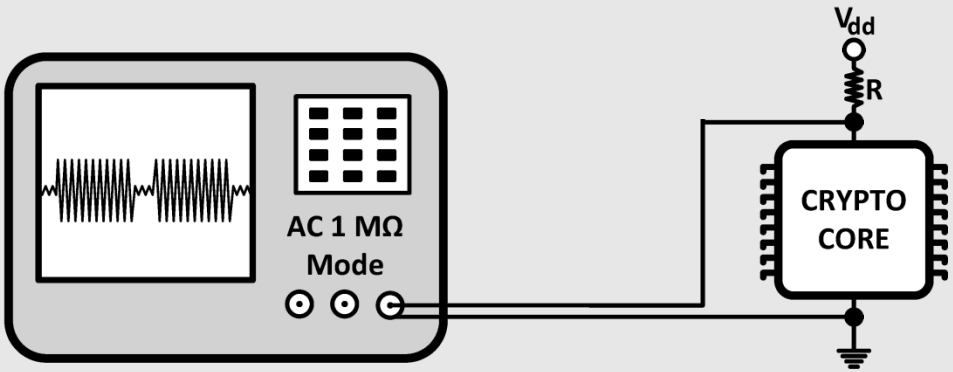
Outline

- Power Analysis Attack
- Masking
- Problems in hardware
- Possible approaches

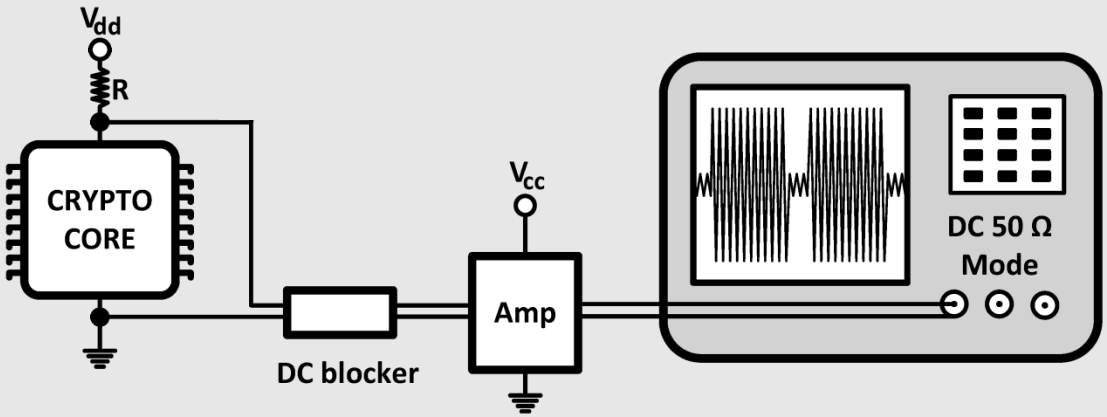
Measurement Setup



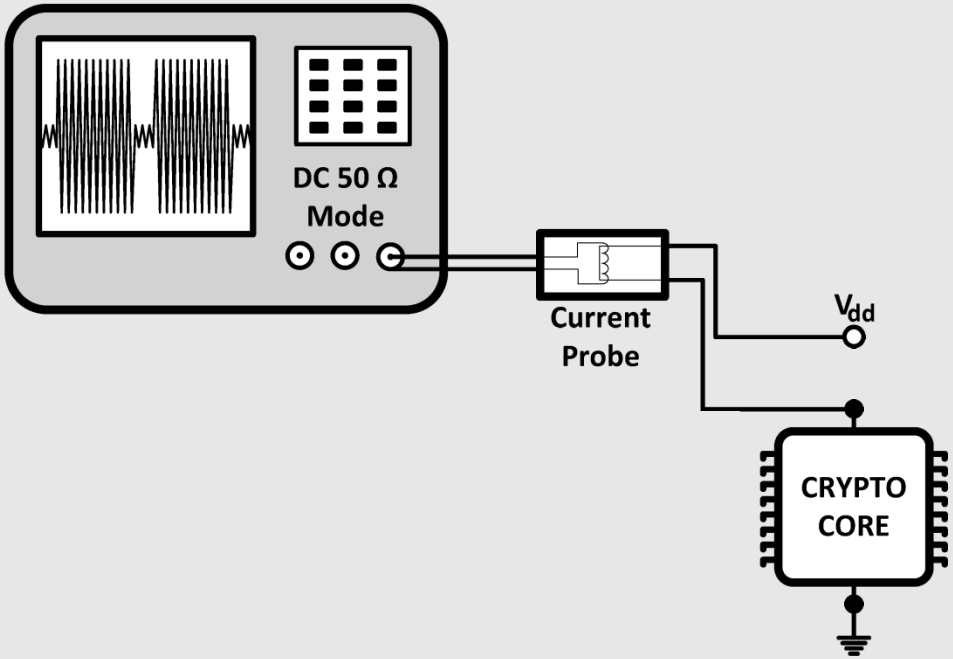
Measurement Setup



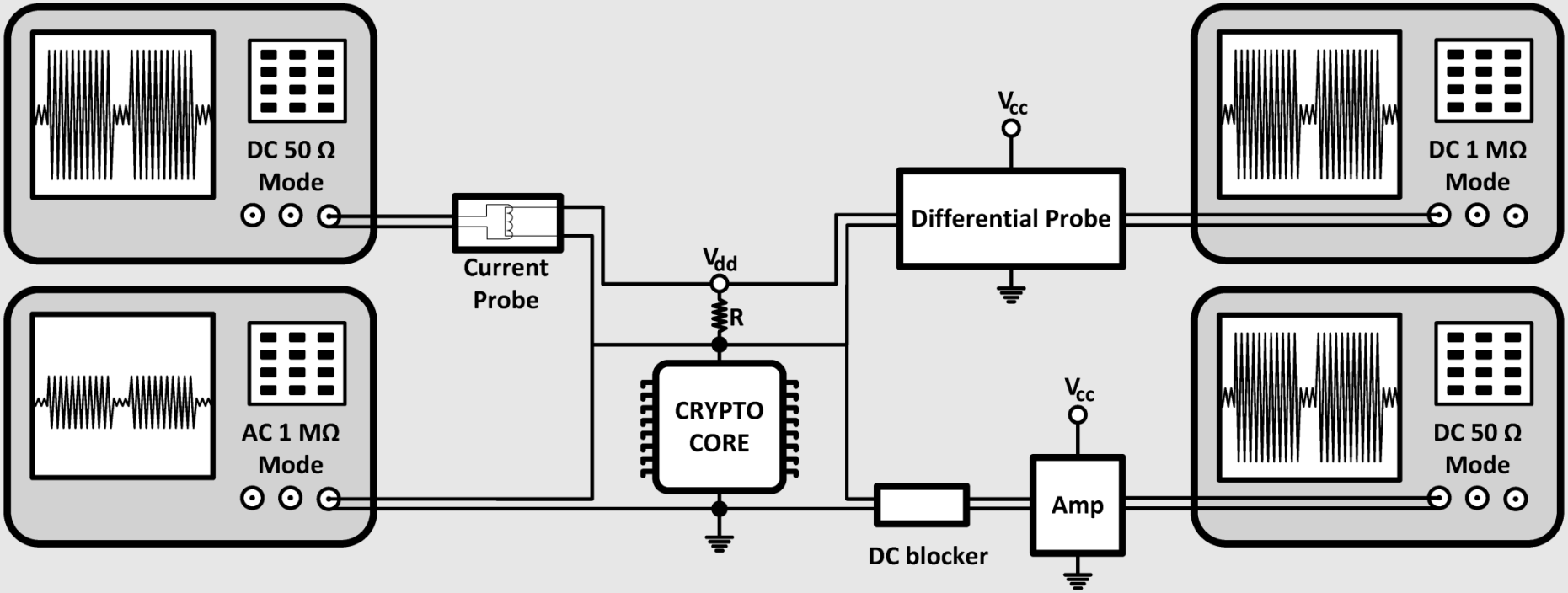
Measurement Setup



Measurement Setup

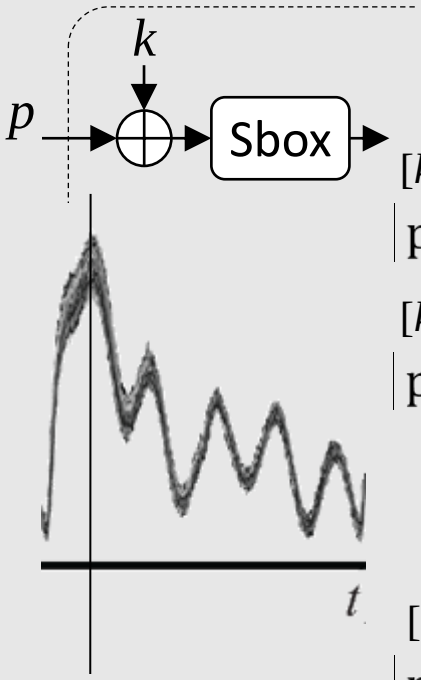


Measurement Setup



Power Analysis Attack

- Recovering the key of crypto devices
- Hypothetical model for power consumption
- Compare the model with side-channel leakage (power)
- How?



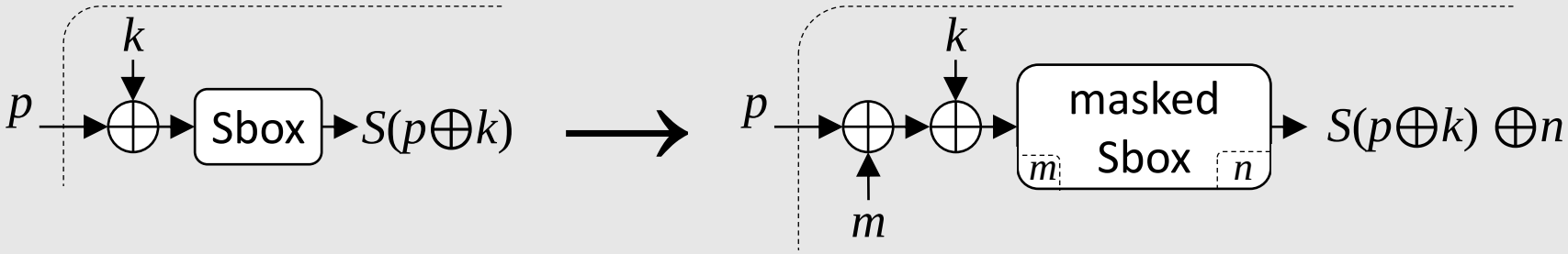
p	12	3d	78	…	f9	ab	3d
power	0.12	0.01	0.14	…	0.20	0.06	0.02
$[k{=}00]\ S$	c9	27	bc	…	99	62	27
$\widetilde{\text{power}}$	4	4	5	…	4	3	4
$[k{=}01]\ S$	7d	eb	b6	…	41	ac	eb
$\widetilde{\text{power}}$	6	6	5	…	2	4	6
⋮							
$[k{=}\text{ff}]\ S$	55	25	17	…	6f	20	25
$\widetilde{\text{power}}$	4	3	4	…	6	1	3

Correlation

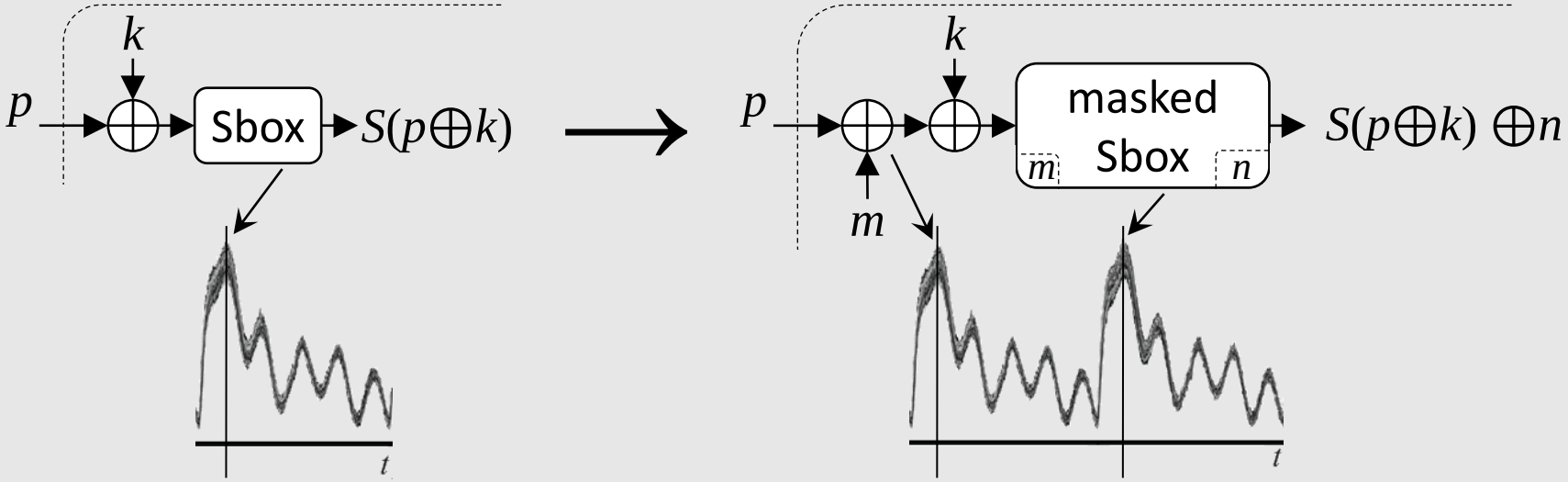
0.011
0.060
⋮
0.231
⋮
0.095

Masking

- Well-known SCA countermeasure
- to make the SC leakages independent of expected intermediate values
- Randomness is required
- Let's consider the most common one, Boolean Masking



Univariate vs. Multivariate Attacks



DPA/CPA/MIA

bivariate MIA

squaring: 2nd order univariate

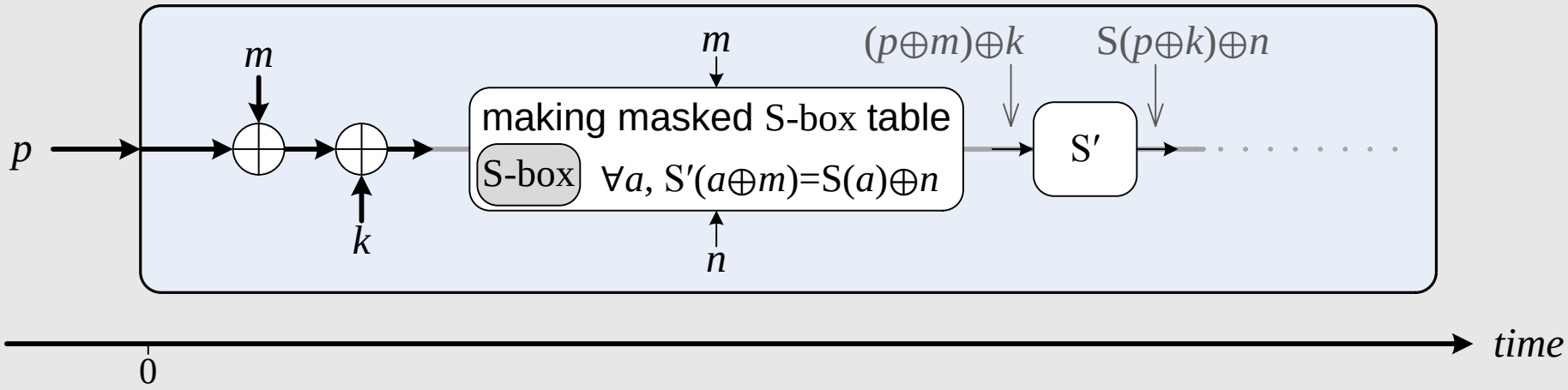
combining: DPA/CPA

multiply: 2nd order bivariate

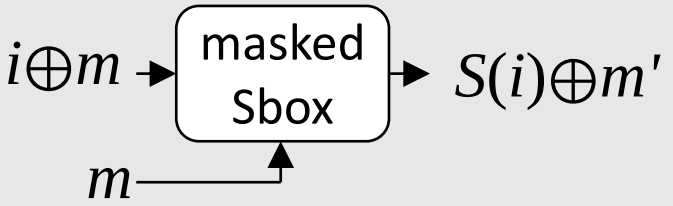
addition: 1st order bivariate

Masking (software case)

- Sequential operations
- First, generation of the “masked Sbox” having the mask(s)
- Second, feeding the masked input
- Time consuming
- Low efficiency
  - but feasible to counteract against univariate attacks

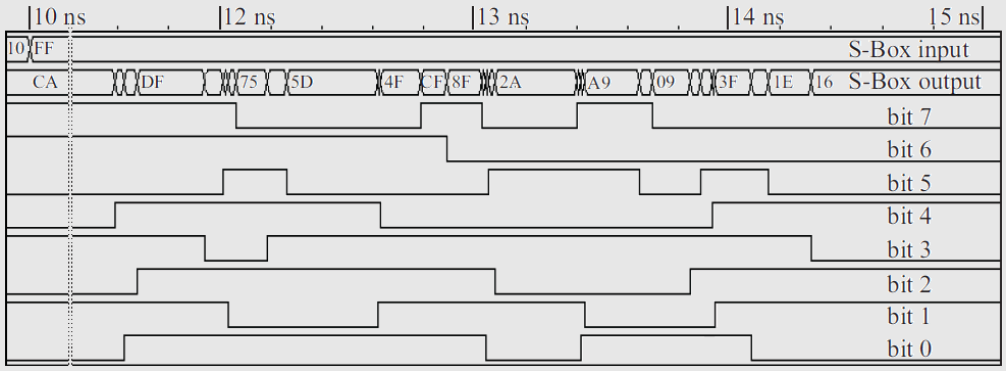


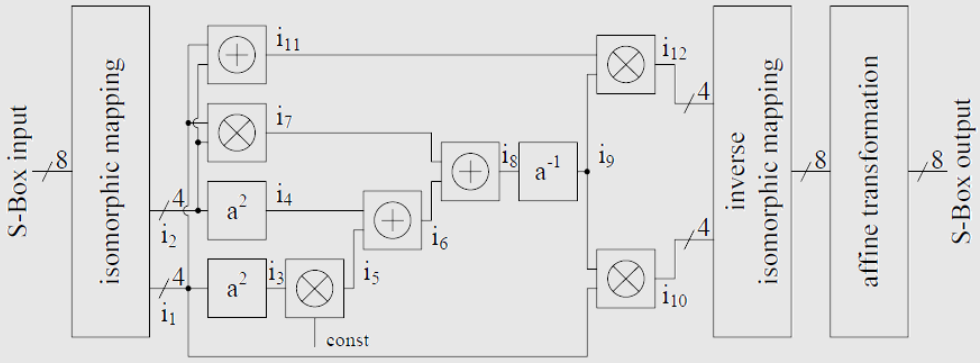
Masking (hardware case)

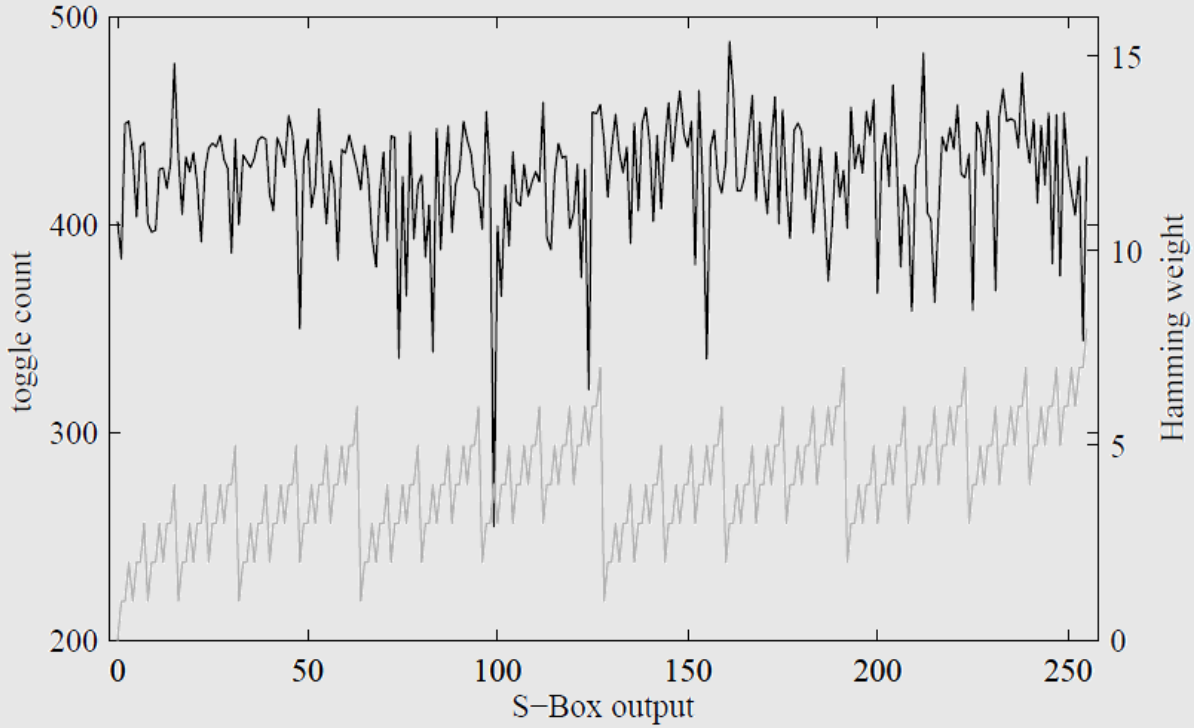


- High efficiency is desired
- ad-hoc/heuristic schemes
  - Oswald, et al: *A Side-Channel Analysis Resistant Description of the AES S-Box*. FSE 2005.
  - Canright, Batina: *A Very Compact "Perfectly Masked" S-Box for AES (corrected)*. ePrint 11 (2009), ACNS 2008.
- Processing the mask (m) and masked data ($i \oplus m$) simultaneously
  - joint distribution of SC leakages mainly because of GLITCHES
  - possible attacks
  - Mangard, et al: *Successfully Attacking Masked AES Hardware Implementations*. CHES 2005.
  - Moradi, et al: *Correlation-Enhanced Power Analysis Collision Attack*. CHES 2010.

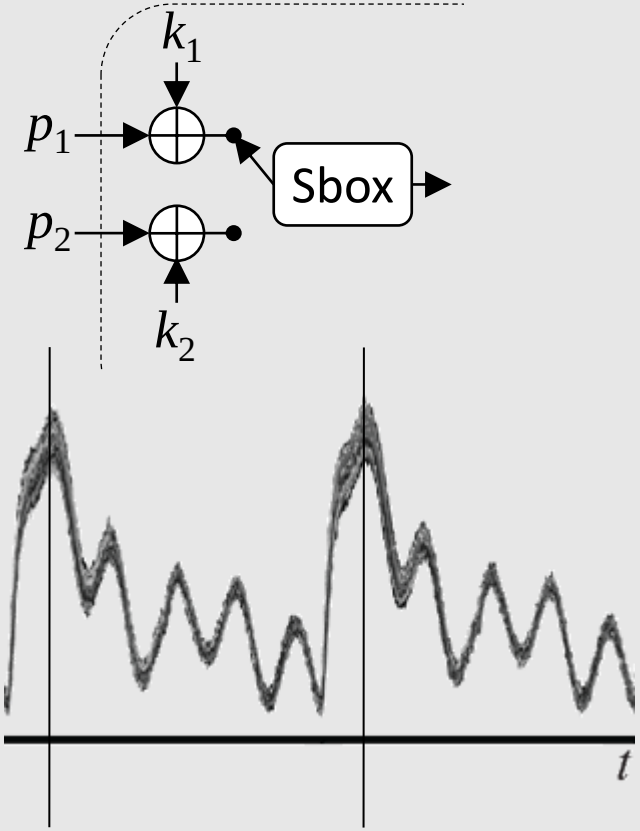
Successfully Attacking Masked AES Hardware …







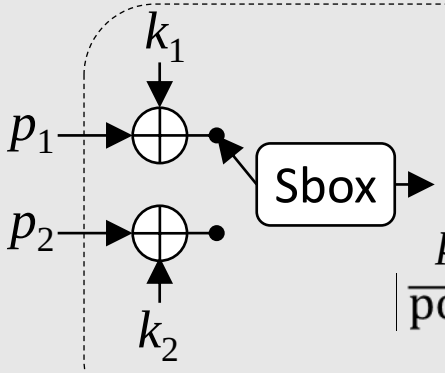
Our Solution at CHES 2010 (Correlation-Enhanced)



p_1	12	3d	78	…	f9	ab	3d
power	0.01	0.15	0.12	…	0.24	0.05	0.11

p_2	45	9a	cf	…	04	17	e2
power	0.32	0.20	0.05	…	0.19	0.27	0.26

Our Solution at CHES 2010 (Correlation-Enhanced)



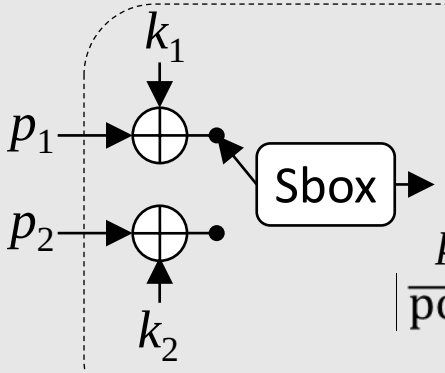
p_1	12	3d	78	…	f9	ab	3d
power	0.01	0.15	0.12	…	0.24	0.05	0.11

average

p_1	00	01	02	…	fd	fe	ff
power	0.23	0.12	0.21	…	0.06	0.09	0.14

p_2	45	9a	cf	…	04	17	e2
power	0.32	0.20	0.05	…	0.19	0.27	0.26

Our Solution at CHES 2010 (Correlation-Enhanced)



p_1	12	3d	78	…	f9	ab	3d
power	0.01	0.15	0.12	…	0.24	0.05	0.11

p_1	00	01	02	…	fd	fe	ff
power	0.23	0.12	0.21	…	0.06	0.09	0.14

average

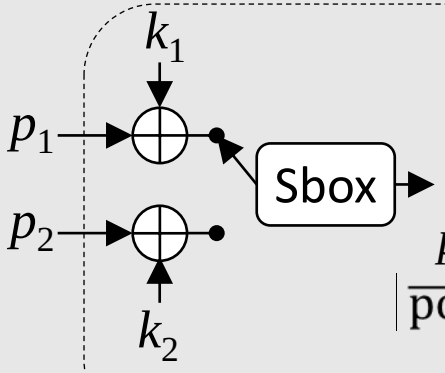
p_2	45	9a	cf	…	04	17	e2
power	0.32	0.20	0.05	…	0.19	0.27	0.26

$p_2 \oplus \Delta k$	00	01	02	…	fd	fe	ff
power	0.32	0.20	0.05	…	0.19	0.27	0.26

$\Delta k = 00$

average

Our Solution at CHES 2010 (Correlation-Enhanced)



p_1	12	3d	78	…	f9	ab	3d
power	0.01	0.15	0.12	…	0.24	0.05	0.11

p_1	00	01	02	…	fd	fe	ff
power	0.23	0.12	0.21	…	0.06	0.09	0.14

average

p_2	45	9a	cf	…	04	17	e2
power	0.32	0.20	0.05	…	0.19	0.27	0.26

$p_2 \oplus \Delta k$	00	01	02	…	fd	fe	ff	
power	0.32	0.20	0.05	…	0.19	0.27	0.26	$\Delta k = 00$

average

$p_2 \oplus \Delta k$	00	01	02	…	fd	fe	ff	
power	0.20	0.32	0.17	…	0.09	0.26	0.27	$\Delta k = 01$

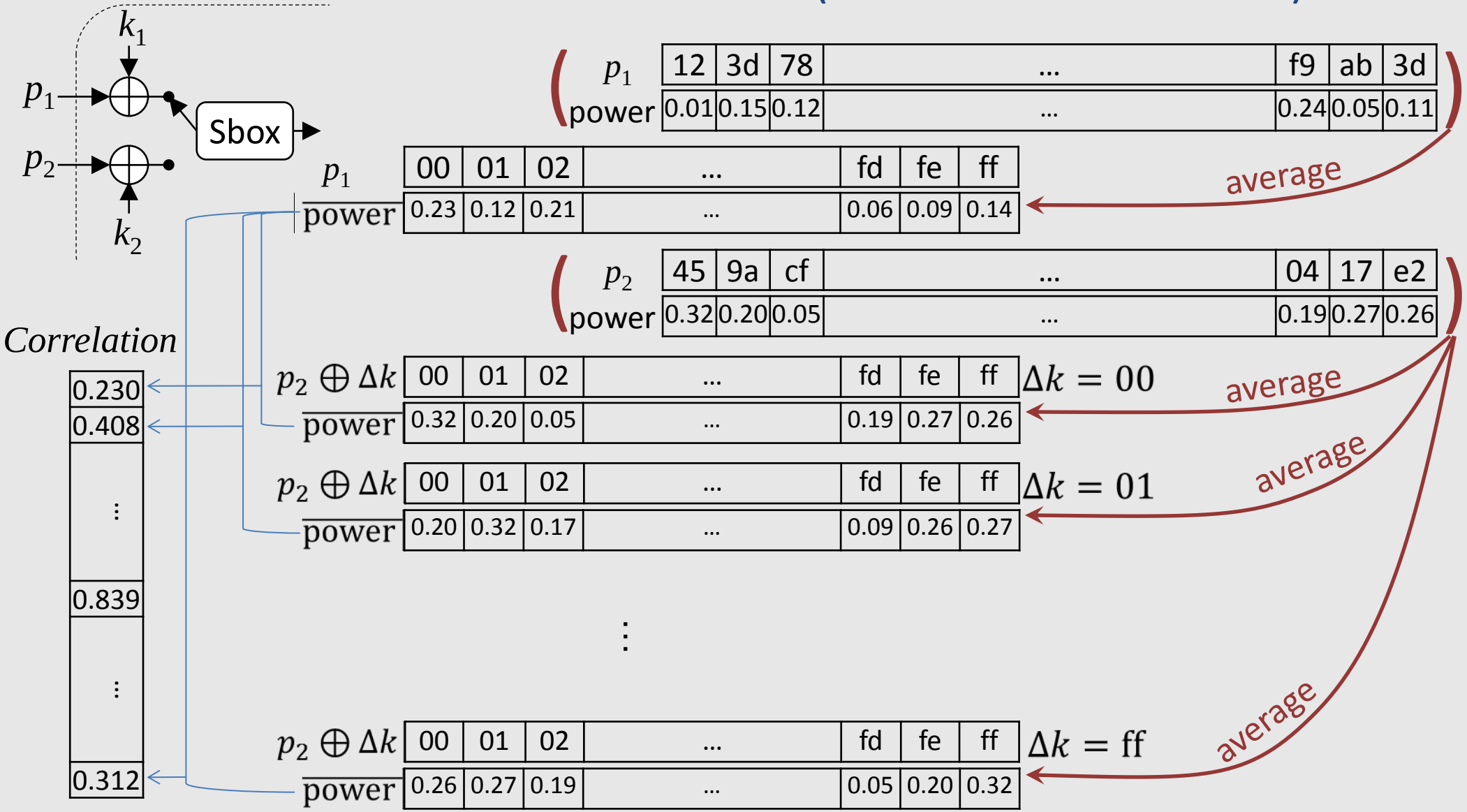
average

⋮

$p_2 \oplus \Delta k$	00	01	02	…	fd	fe	ff	
power	0.26	0.27	0.19	…	0.05	0.20	0.32	$\Delta k = ff$

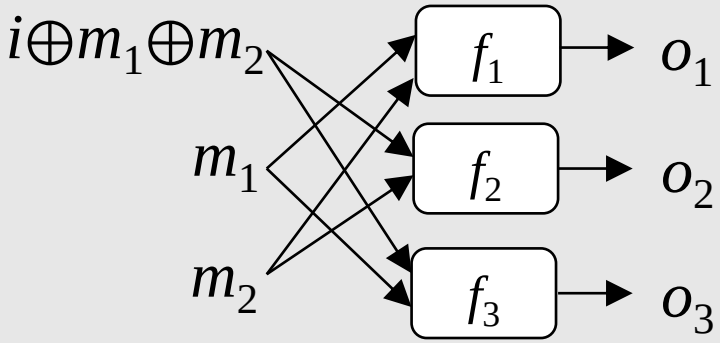
average

Our Solution at CHES 2010 (Correlation-Enhanced)



Masking (hardware case)

- Systematic schemes
  - Threshold Implementation
  - Nikova, et al: *Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches*. J. Cryptology 24(2):2011.

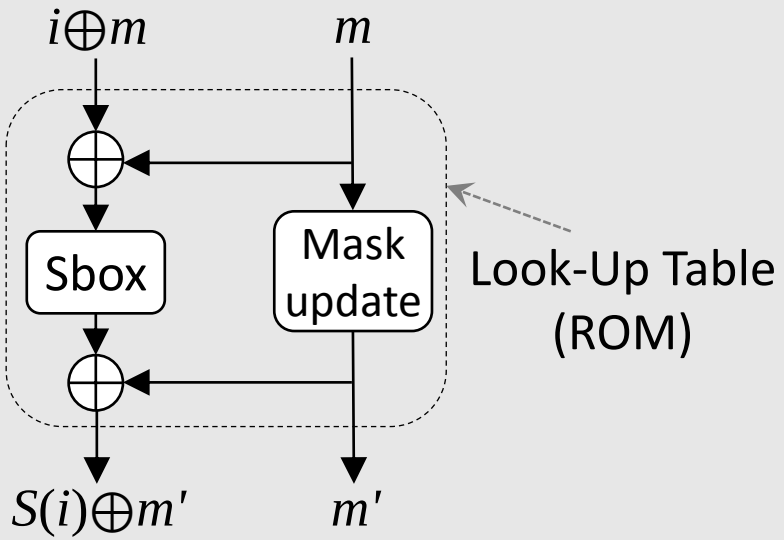


$$o_1 \oplus o_2 \oplus o_3 = S(i)$$

  - Independent leakage of f_1, f_2, f_3, no first-order leakage
  - Their joint distribution (f_1, f_2, f_3) still depends on i
    - a univariate attack still possible

Masking (hardware case)

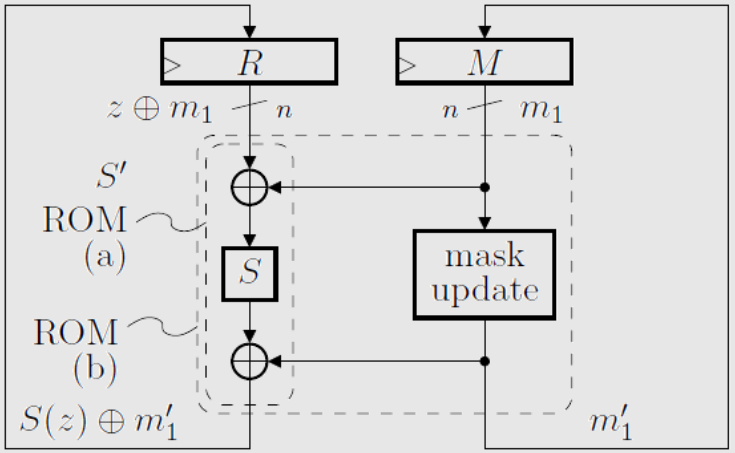
- Systematic schemes
  - Global Look-Up-Table (GLUT)
  - Prouff, Rivain: *A Generic Method for Secure SBox Implementation*. WISA 2007.
  - High area overhead
  - High performance
  - Still the same story
    - Processing the mask (m) and masked data ($i \oplus m$) simultaneously
    - a univariate leakage



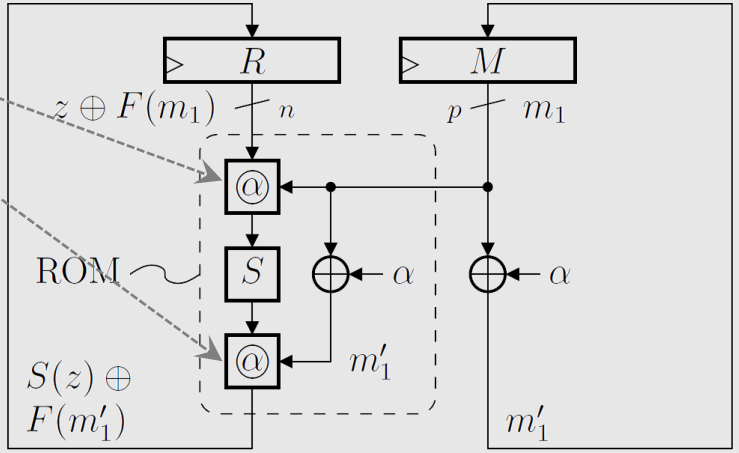
CT-RSA 2012 approach

A First-Order Leak-Free Masking Countermeasure

- GLUT
  - Register update model
    - HD model
  - Known leakage

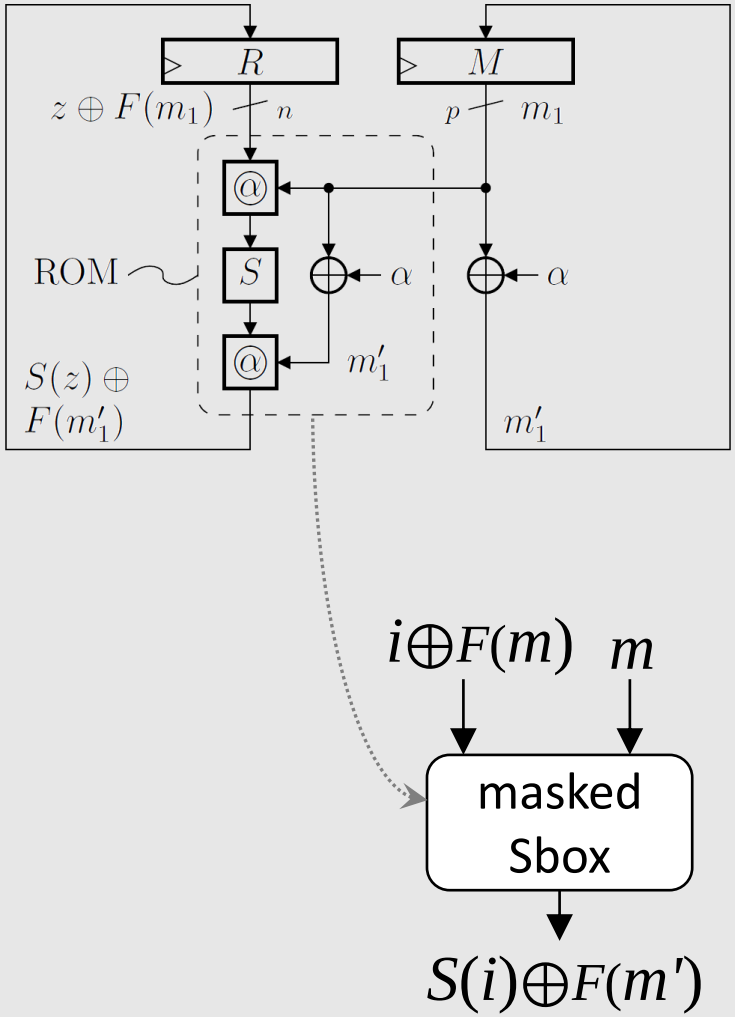


  - Specific value for α and f_α
  - Constant flipping bits of M register
  - Uniform distribution of ΔR
  - Two options for f_α
  - Satisfying desired protection
    - Having "Register Update Model"



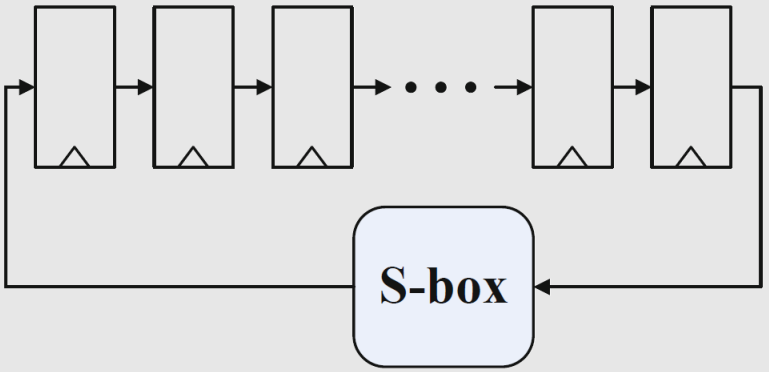
CT-RSA 2012 approach

- GLUT
  - The same story
  - Processing the mask (m) and masked data ($i \oplus F(m)$) simultaneously
  - a univariate leakage expected
    - no register update model!

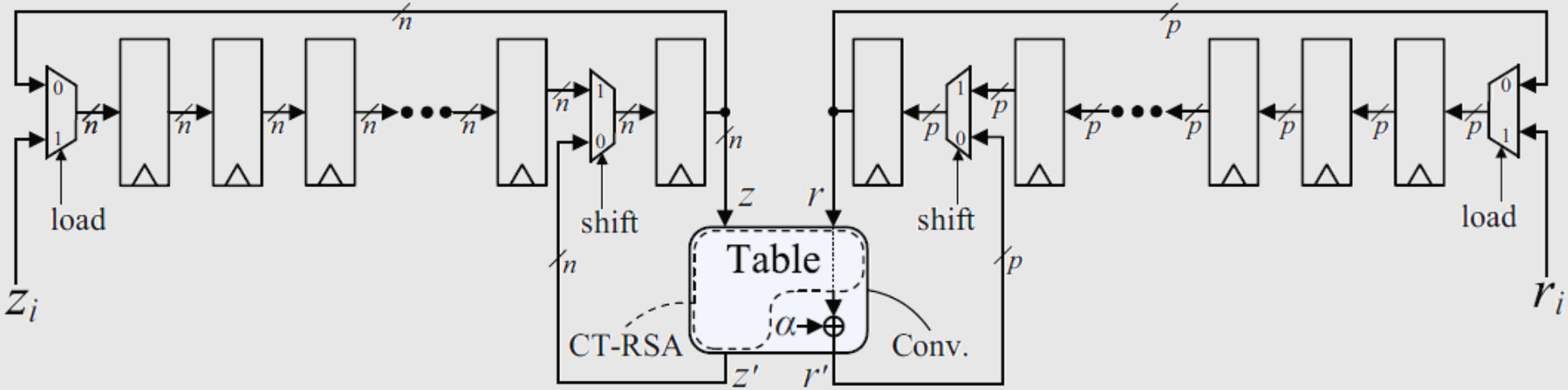


Implementation (case of AES)

- Xilinx Virtex-5 (LX50) FPGA
- Using (6 to 1) **LUT6** (or 16k-bit **BRAM)**
- Giant table
  - 1M bits for GLUT
    - 21840 LUT6 of all 28800
    - or 16 LUT6 + 64 BRAM of all 96
  - no way to have more than one GLUT in a design
- Common design architecture
  - Serialized (shift-register type)

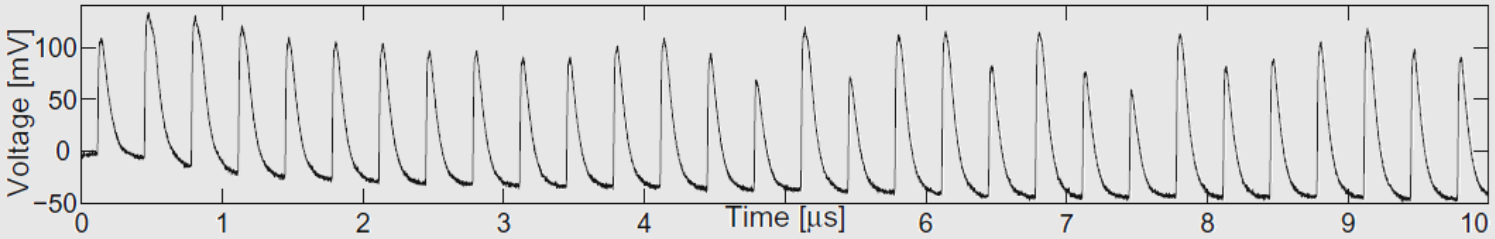


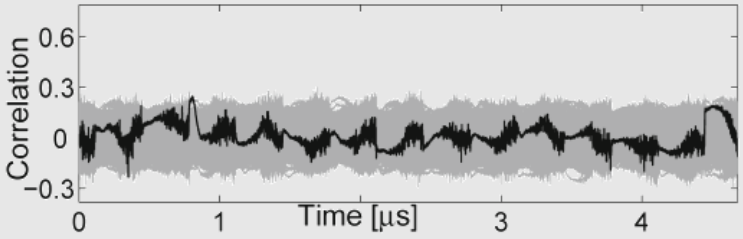
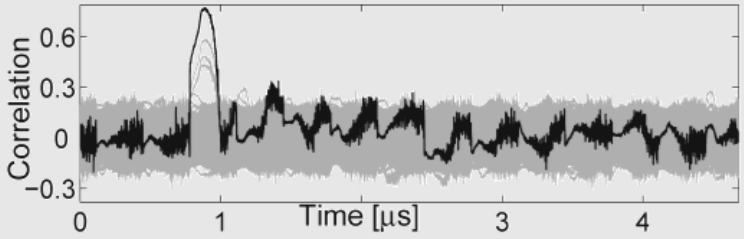
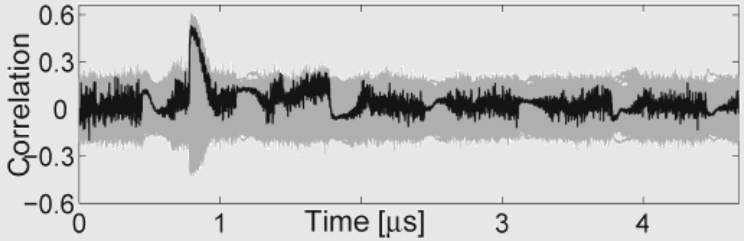
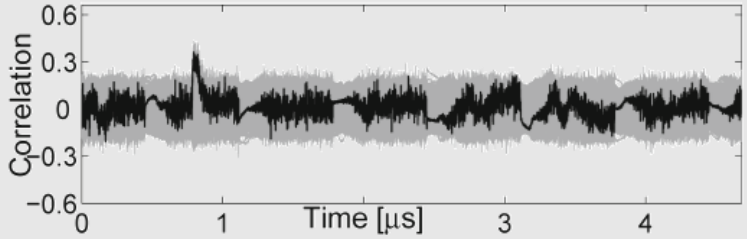
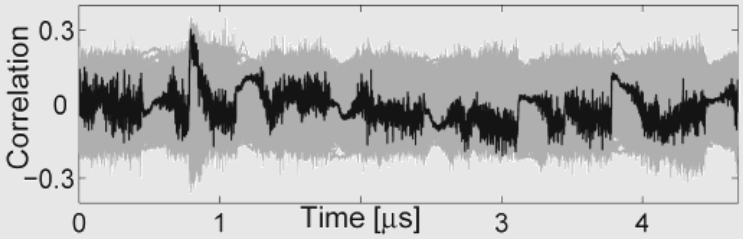
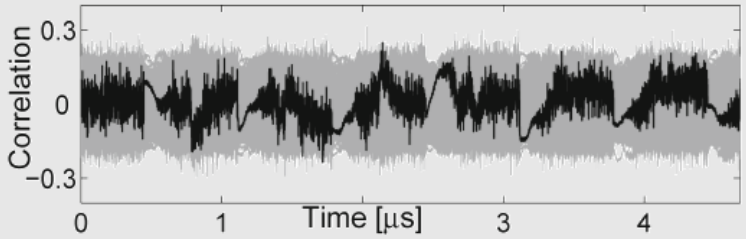
Practical Evaluation



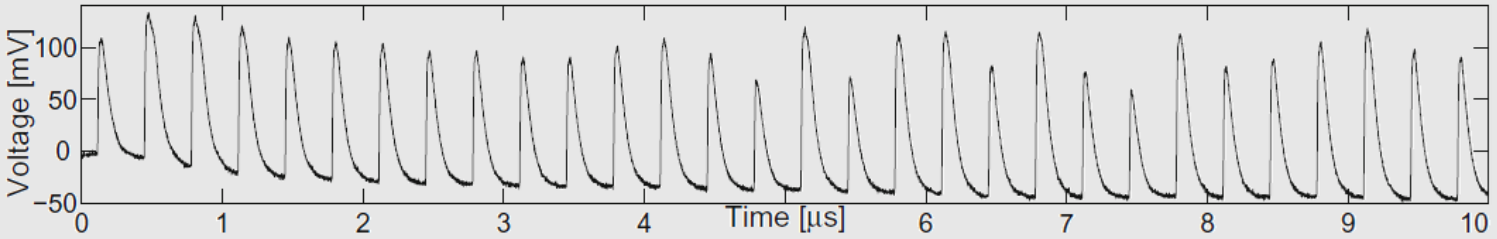
- SASEBO-GII
- 3 designs (Conventional, 1st CT-RSA, 2nd CT-RSA)
  - each by LUT6
- 3MHz clock, 1 GS/s, 20MHz bandwidth
- Fixed # of measurements 1 million
- Univariate correlation collision attack, 1st and 2nd order moments

Register Update Model



	1st order	2nd order
Conventional		
1st CT-RSA		
2nd CT-RSA		

Identity Model (Register Input/Output)



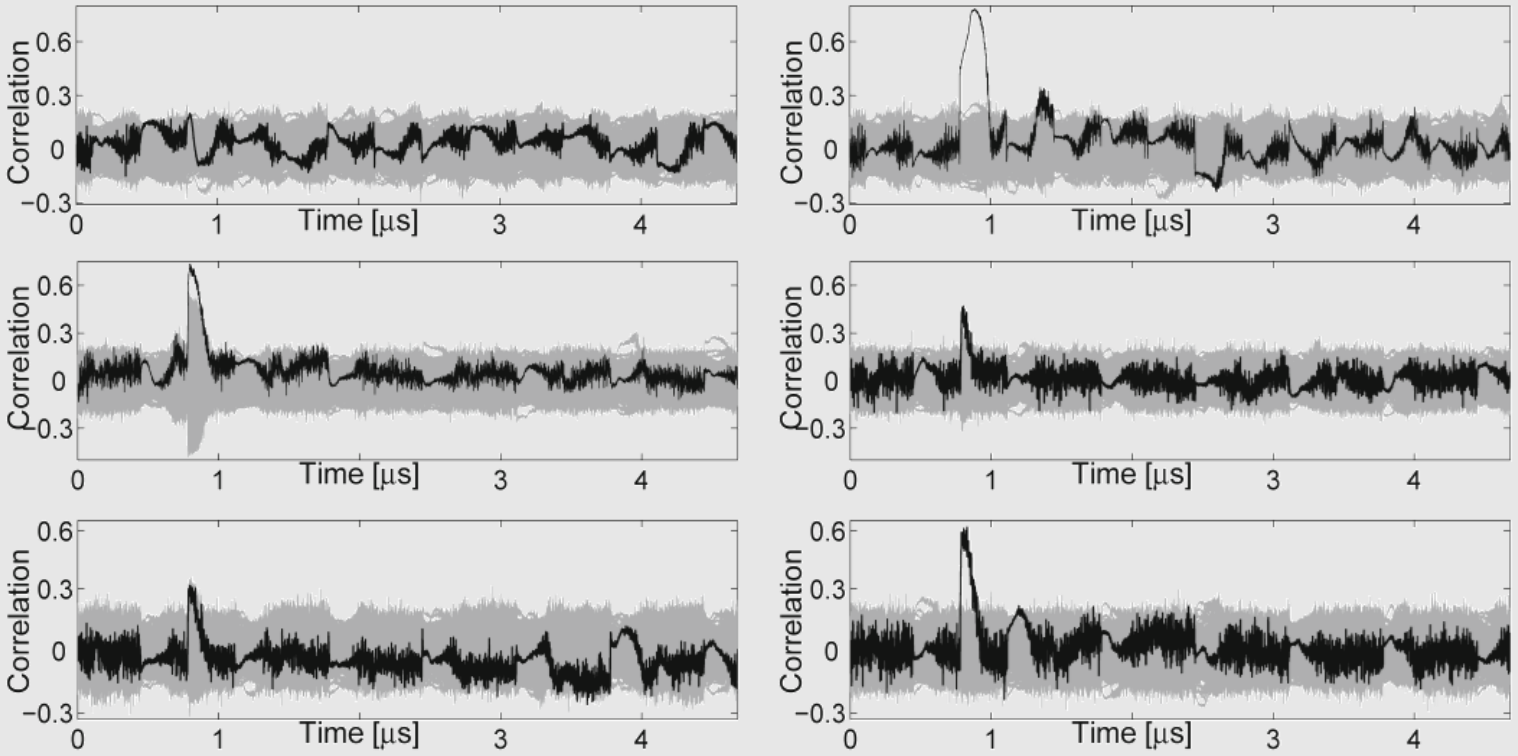
1st order

2nd order

Conventional

1st CT-RSA

2nd CT-RSA



Dual Cipher Concept

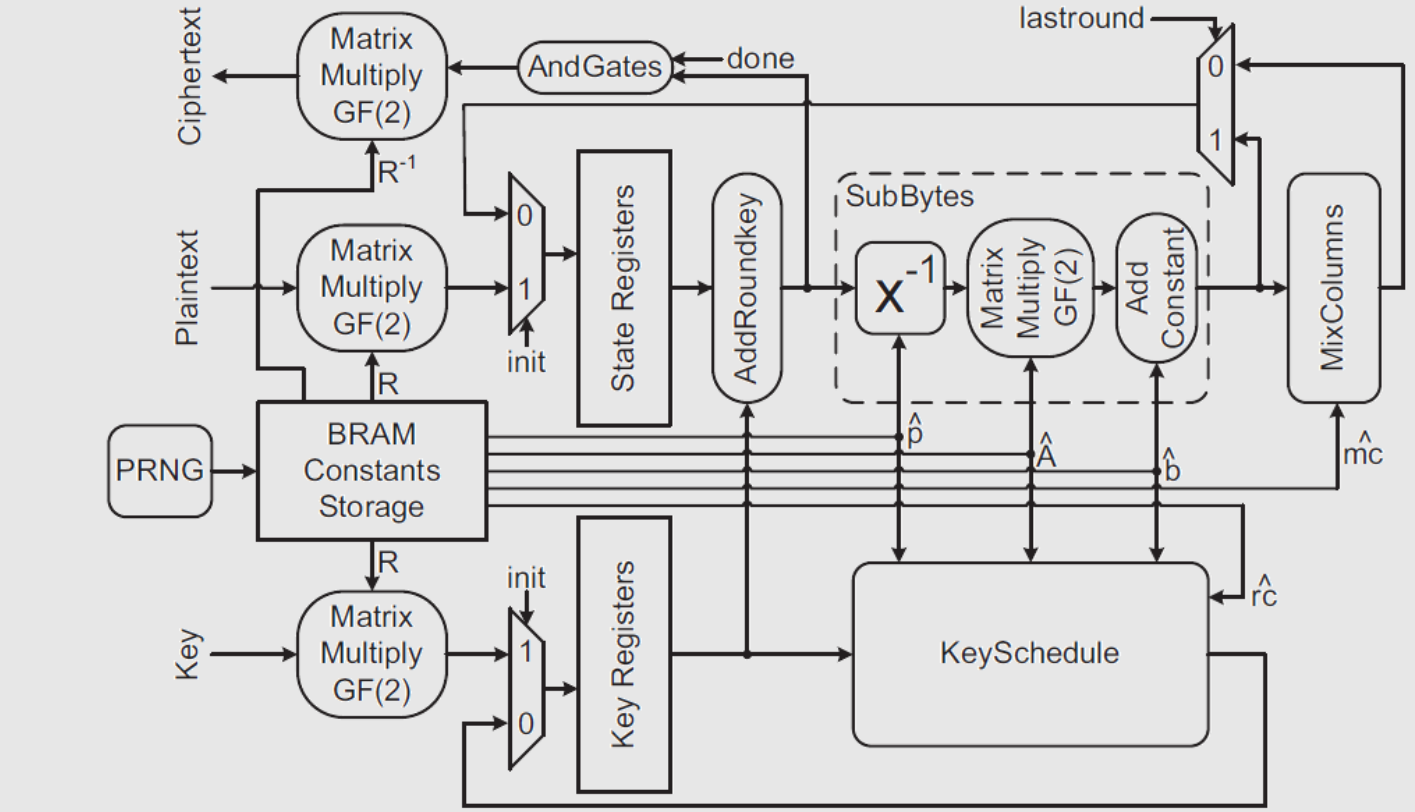
- AES dual ciphers by
  - Barkan and Biham. *In How Many Ways Can You Write Rijndael*? ASIACRYPT 2002.
- Two ciphers E and E' are called dual ciphers, if they are isomorphic, i.e., if there exist invertible transformations $f()$, $g()$ and $h()$ such that

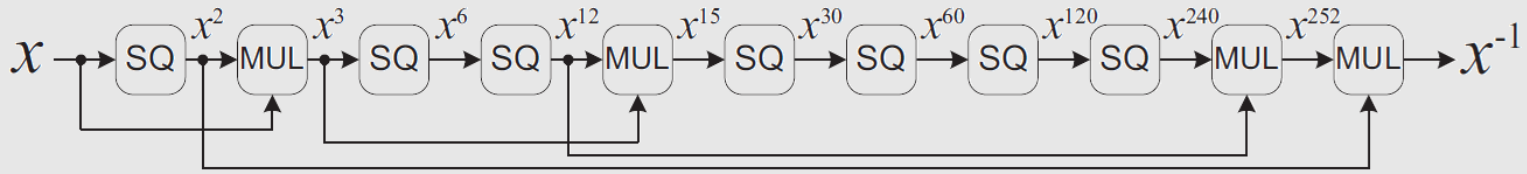
$$\forall P, K \quad E_K(P) = f(E'_{g(K)}(h(P)))$$

- If $f()$, $g()$ and $h()$ are restricted to linear functions (bitwsie matrix multiplication), square of AES can written easily
- The same for AES^4, AES^8, … AES^{128} 8 cases
- Irreducible polynomial also can be changed, 30 in $GF(2^8)$
- In sum 240 dual ciphers exist more by tower field approach (61200)

Dual Ciphers as SCA Countermeasure

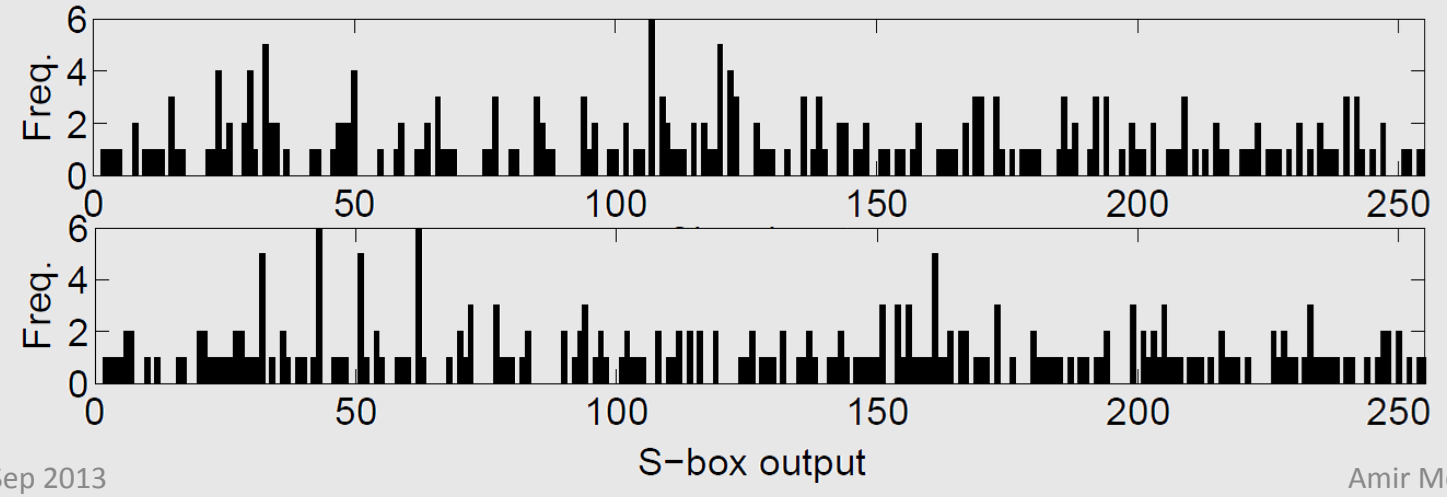
- claimed by the original authors, implemented by many





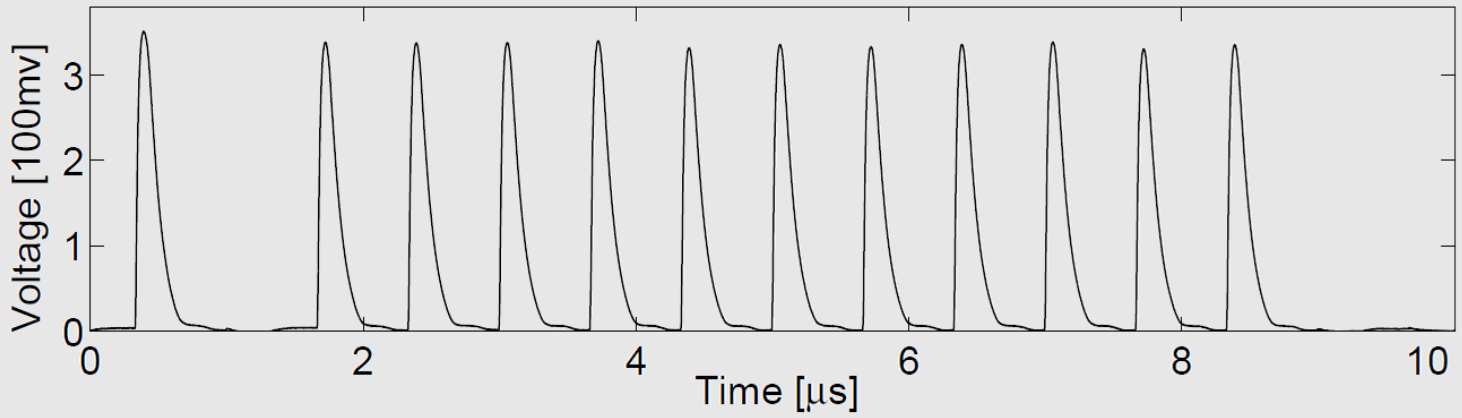
Evaluation

- found problems:
  - Mask Reuse
    - All plaintext bytes (Sboxes) share the same mask
  - Concurrent Processing
    - of Mask and the Masked Data
  - Unbalance (zero value)



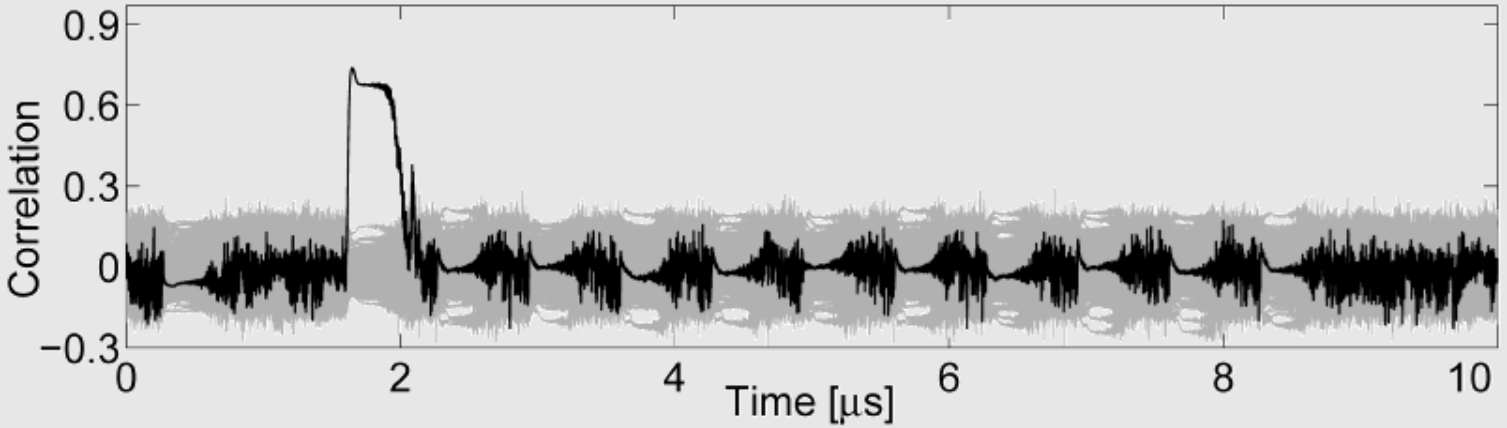
Practical Investigation

- As before (SASEBO-GII, 1GS/s, …)



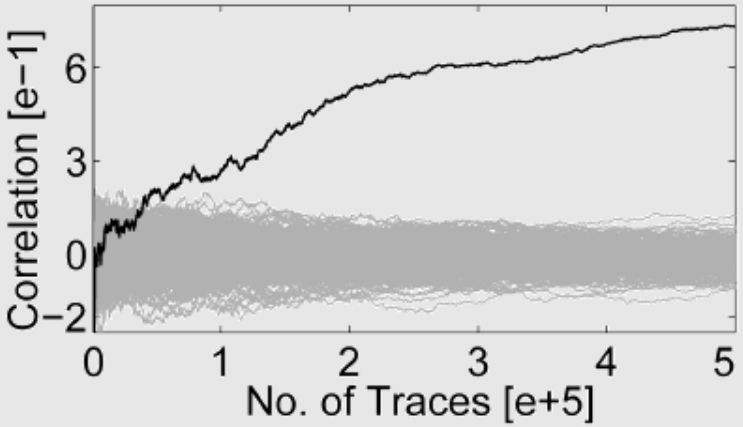
- Very high power consumption
- Very slow, maximum freq. of 21 MHz
- Very high area overhead, 26 times

Correlation Collision Attack (1st-Order)

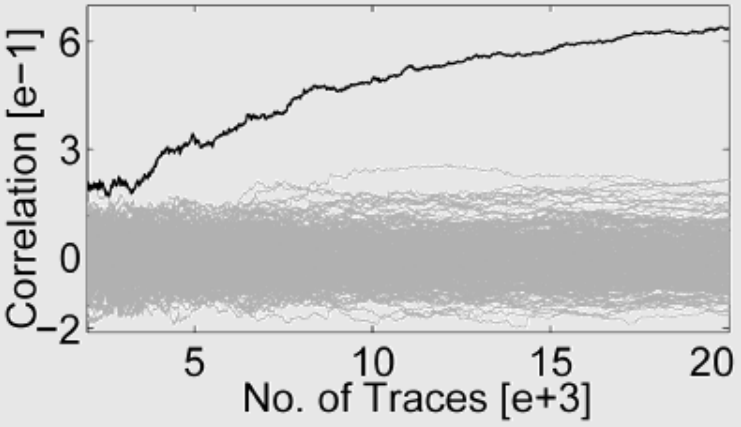


(a) PRNG ON

using 500k traces

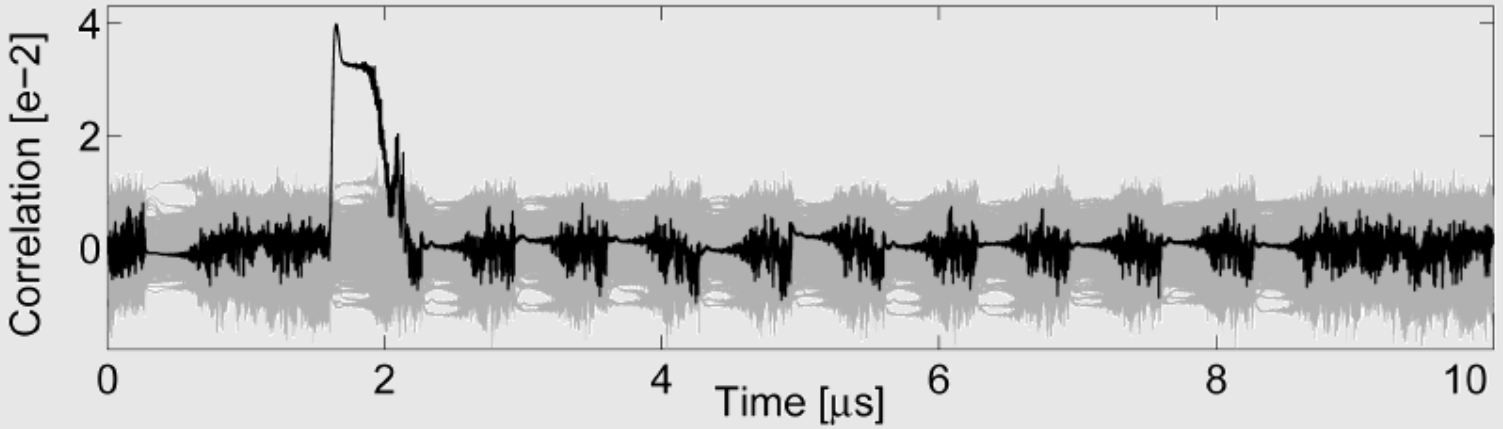


(b) PRNG ON



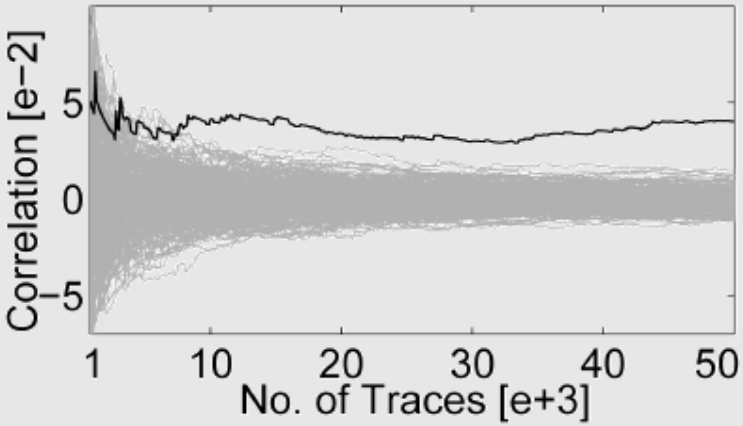
(c) PRNG OFF

Zero Value CPA

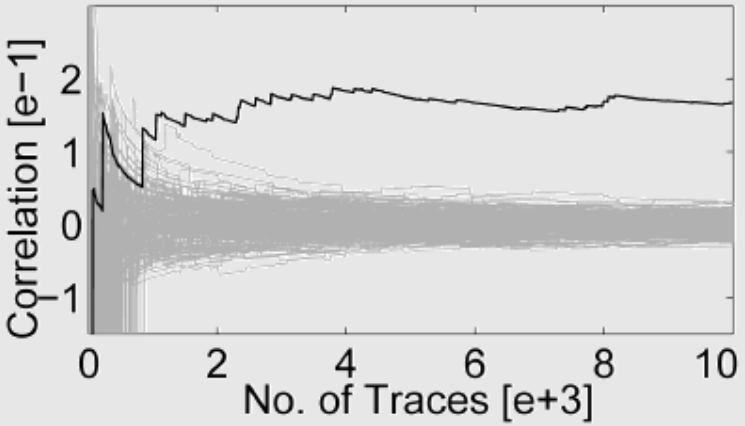


(a) PRNG ON

using 100k traces



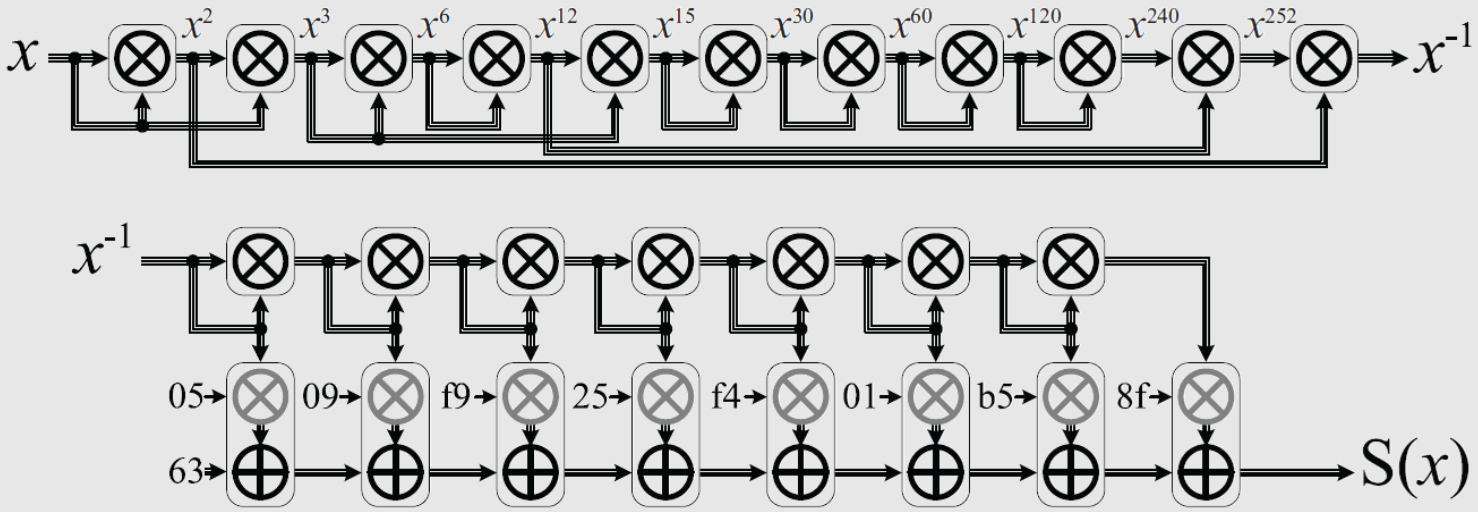
(b) PRNG ON



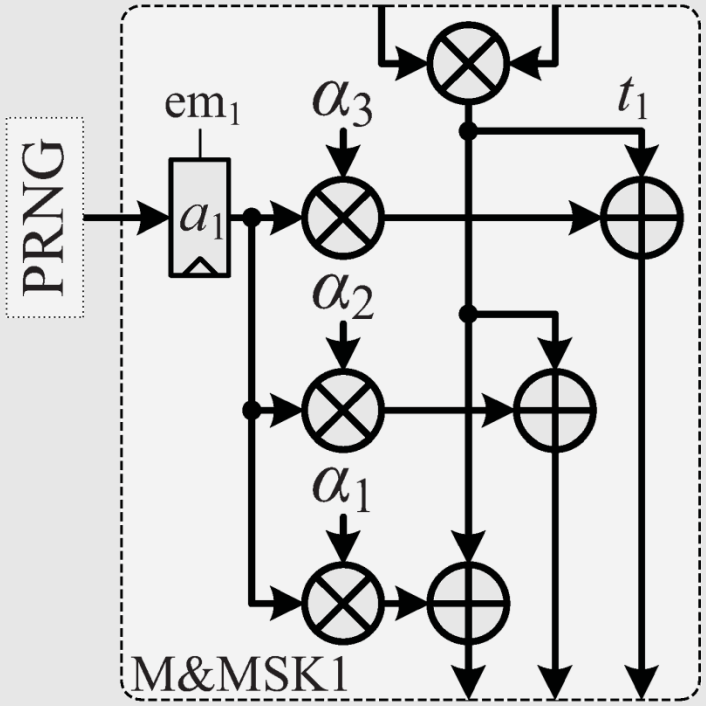
(c) PRNG OFF

Masking (hardware case)

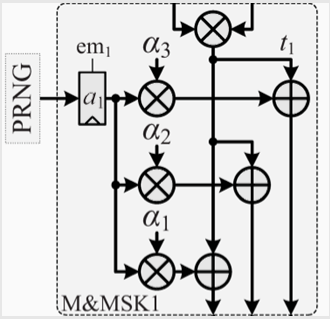
- One more systematic scheme
  - Multi-party computation + Shamir secret sharing
  - Prouff, Roche: *Higher-Order Glitches Free Implementation of the AES Using Secure Multi-party Computation Protocols*. CHES 2011.
- Basic GF(2^8) operations, e.g., addition is easy
  - Multiplication needs more effort
- An Sbox computation



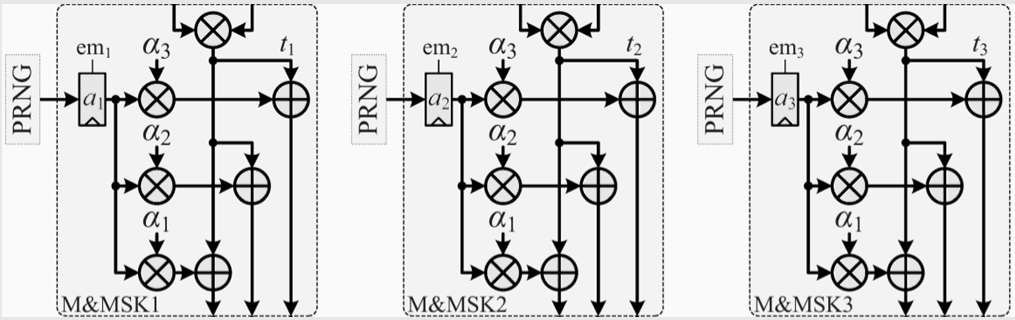
Target Scheme - Design



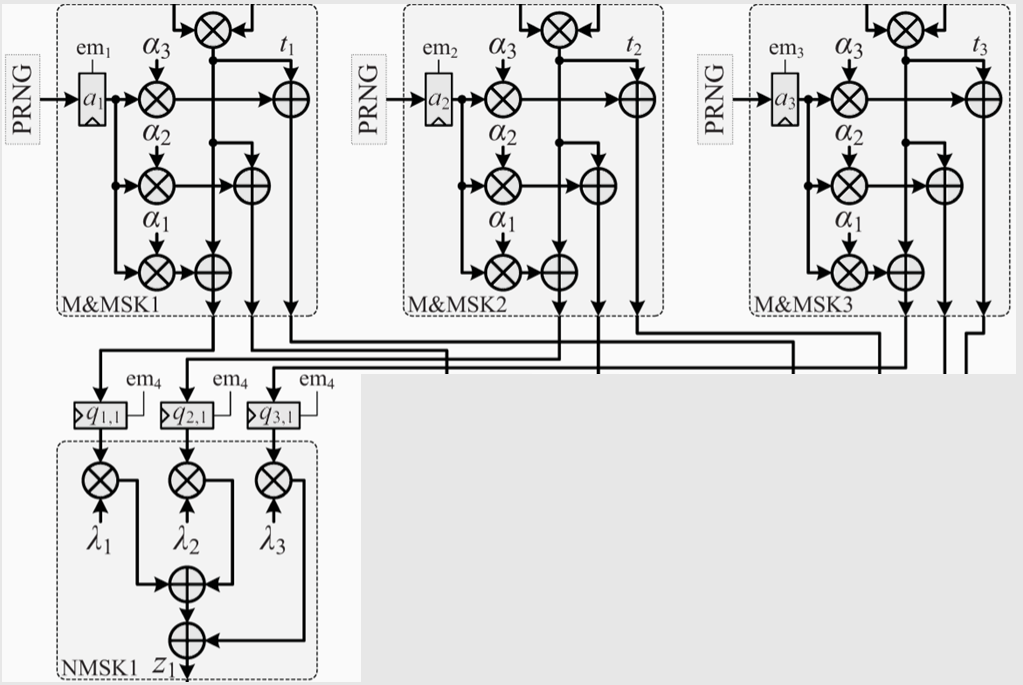
Target Scheme - Design



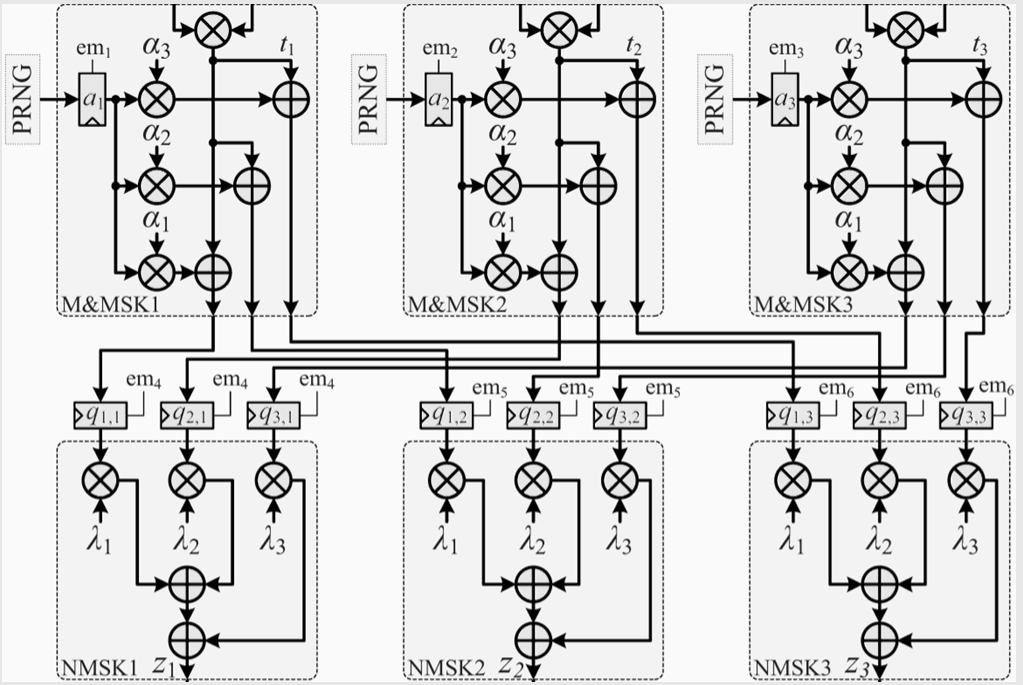
Target Scheme - Design



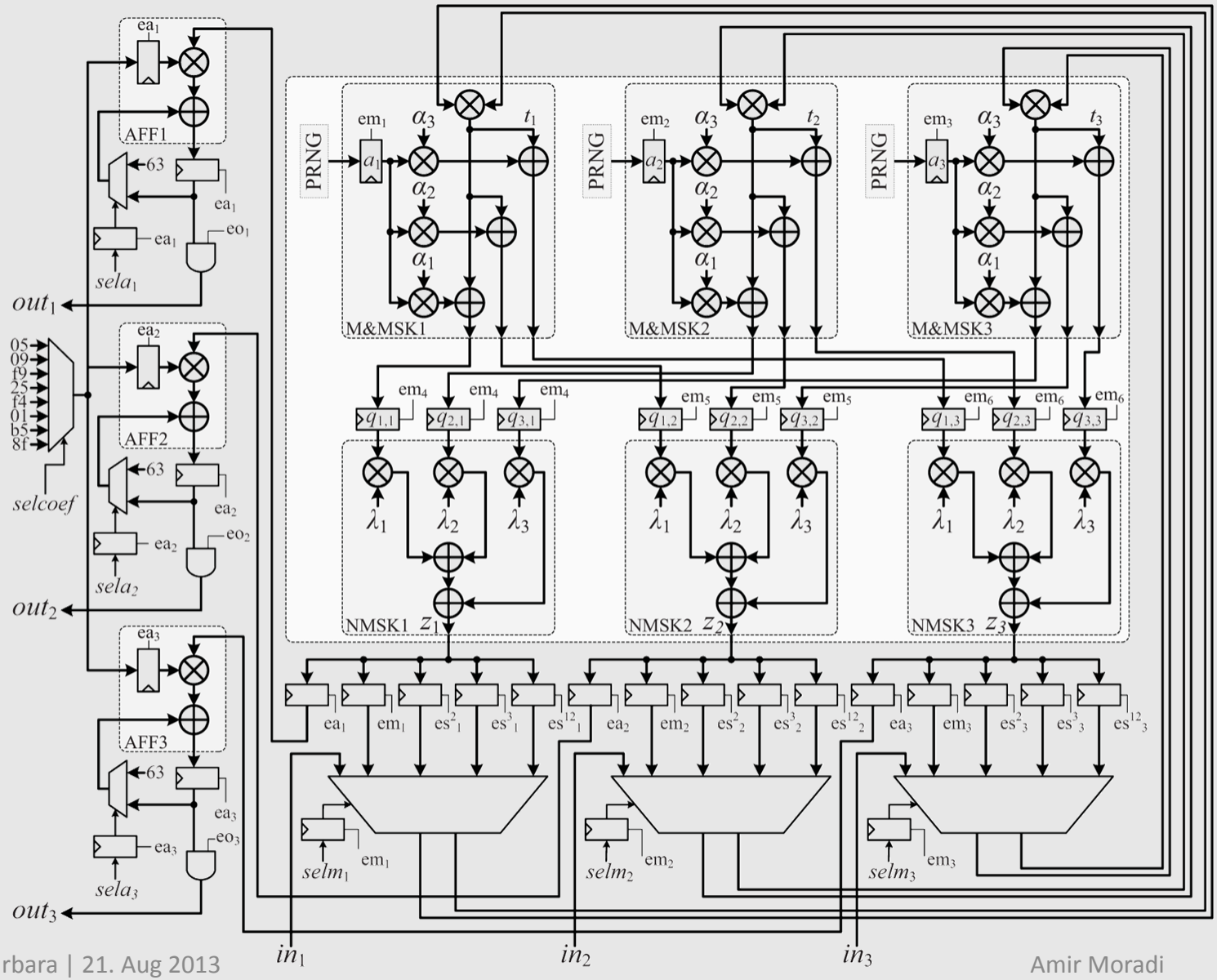
Target Scheme - Design



Target Scheme - Design



Target Scheme - Design

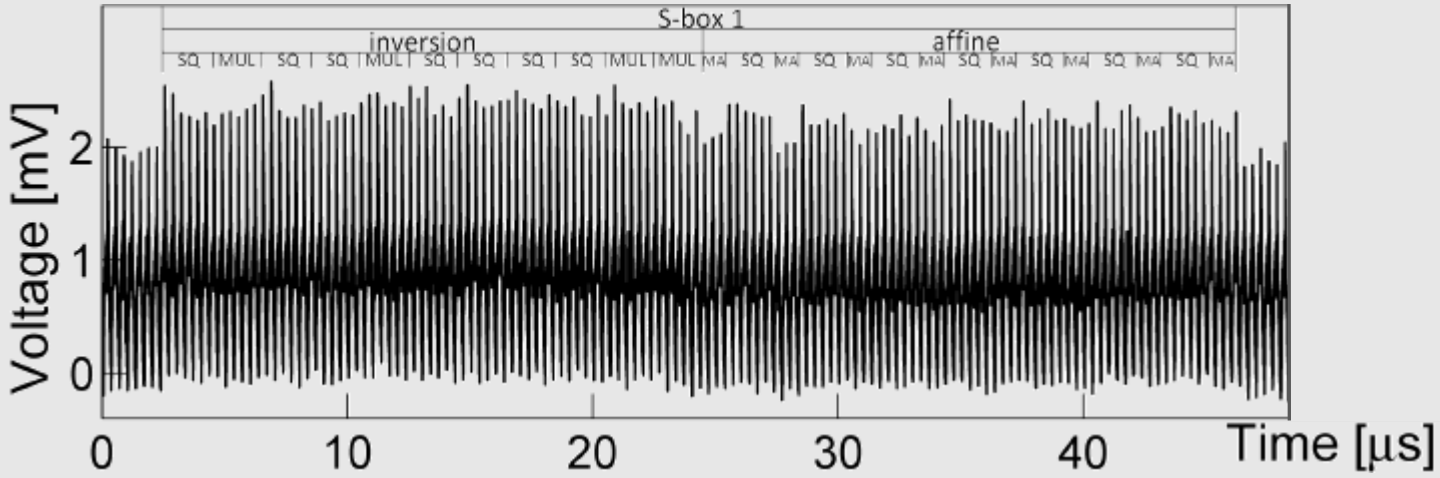


Our Evaluations

- FPGA-based platform (Virtex-5 LX50)

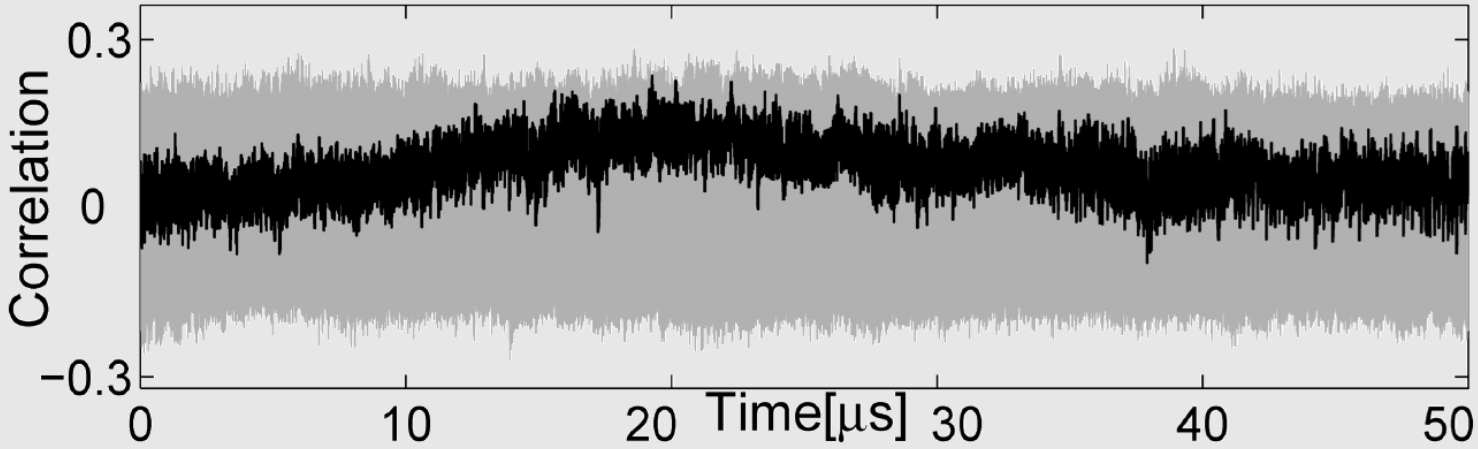
Design	FF		LUT		Slice		SB CLK	MC+ARK CLK	Encryption CLK
	#	%	#	%	#	%			
1 SB MC	315	1%	1387	5%	859	12%	2112	192	22 896
16 SB MC	4275	15%	21 328	74%	no fit		132	12	1431

- Moderate power consumption due to separation of different circuit stages (3Mhz)

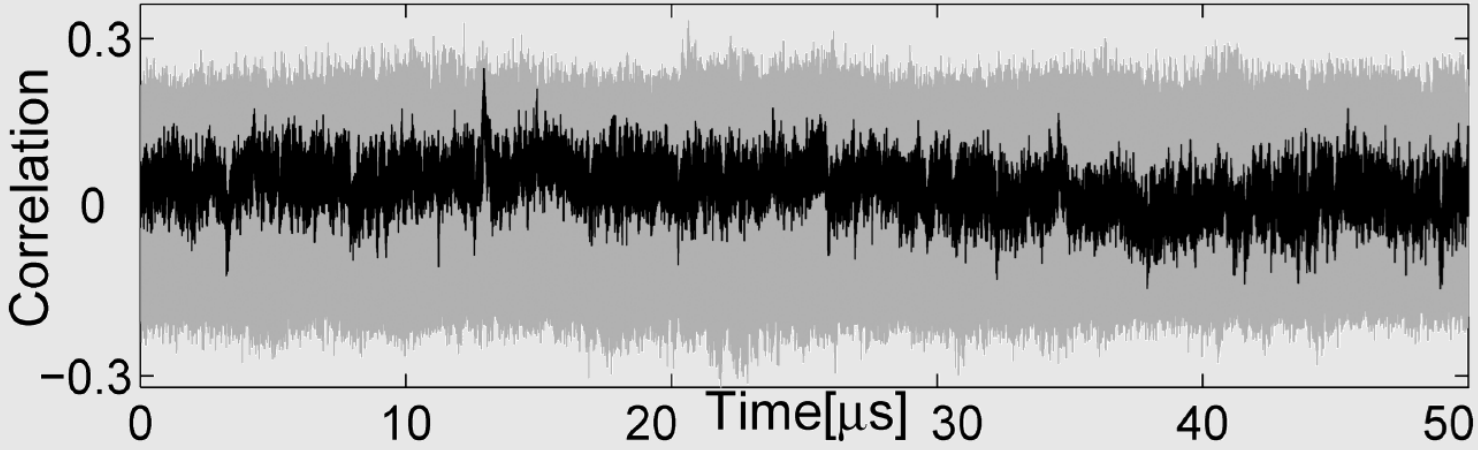


Attack Results, 10 million, 1st and 2nd orders

1st-order



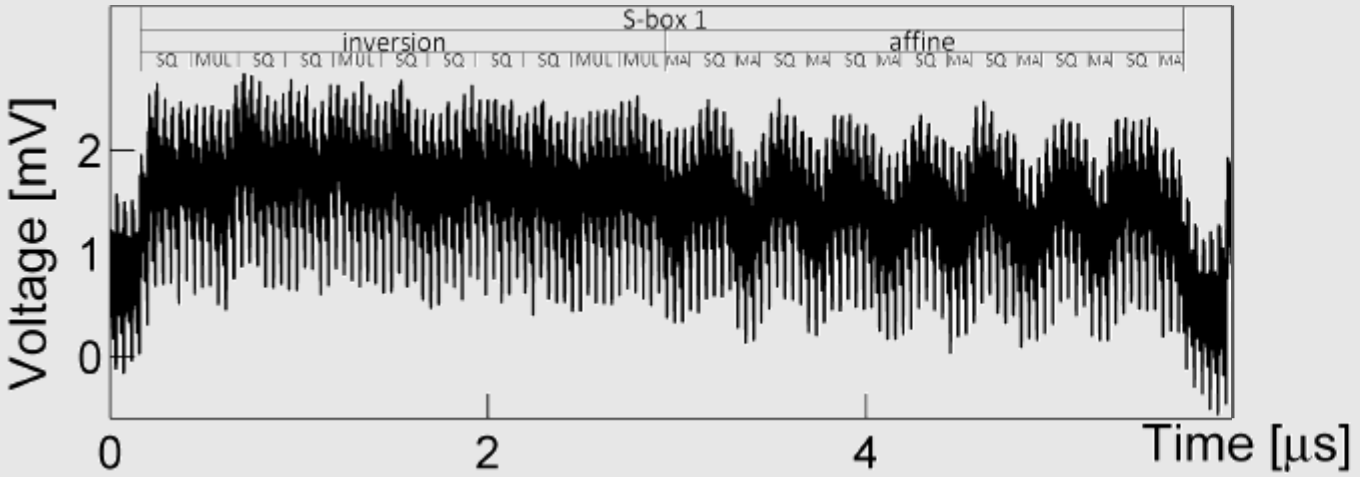
2nd-order



- The first known **univariate** resistant design in hardware

Danger?

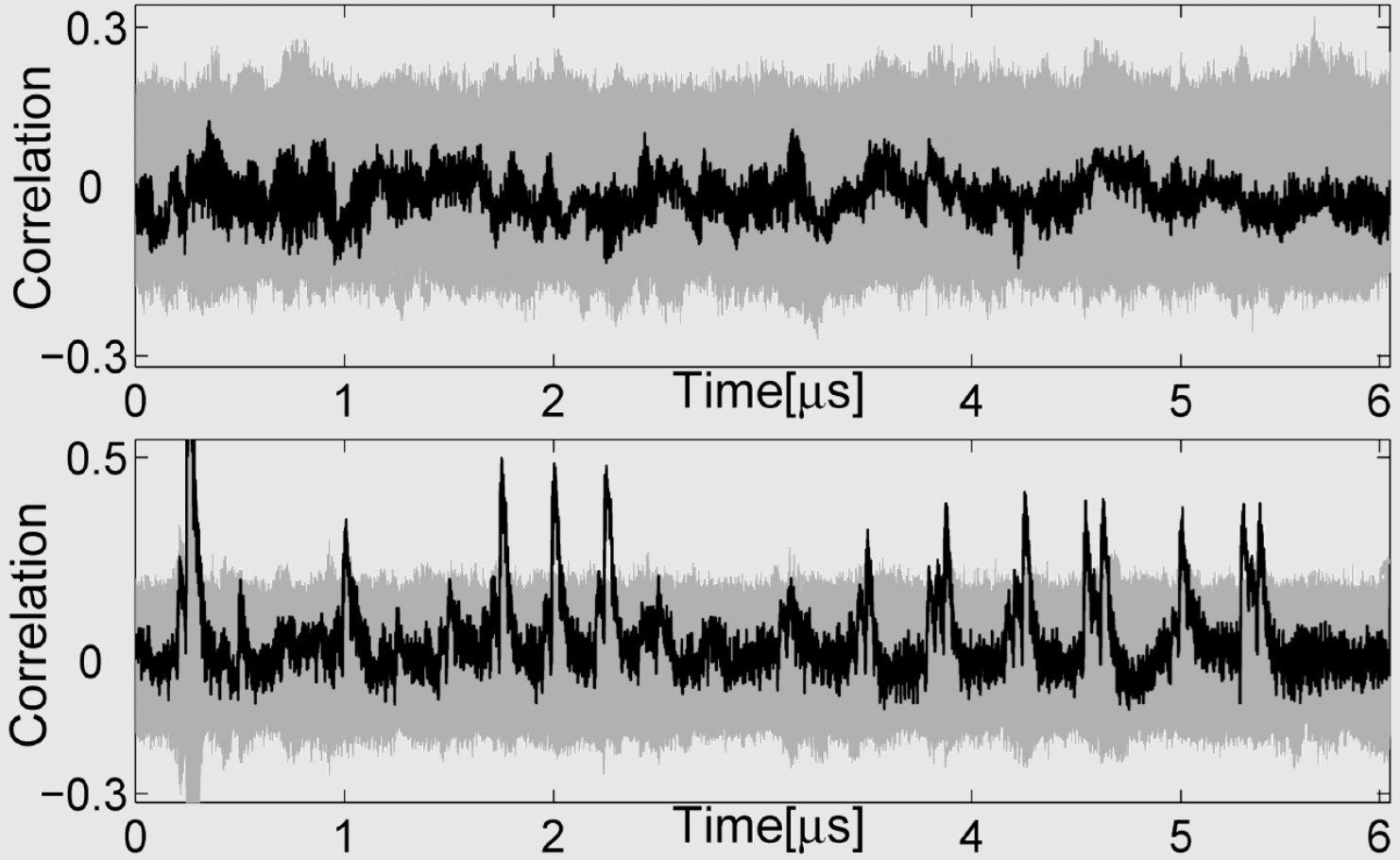
- Hardware platforms for performance
  - High throughput
    - which we did reach
  - High clock frequency
    - Power peaks may overlap
      - Problem? (@ 24Mhz)



Attack Results, 24MHz, 1 million

1st-order

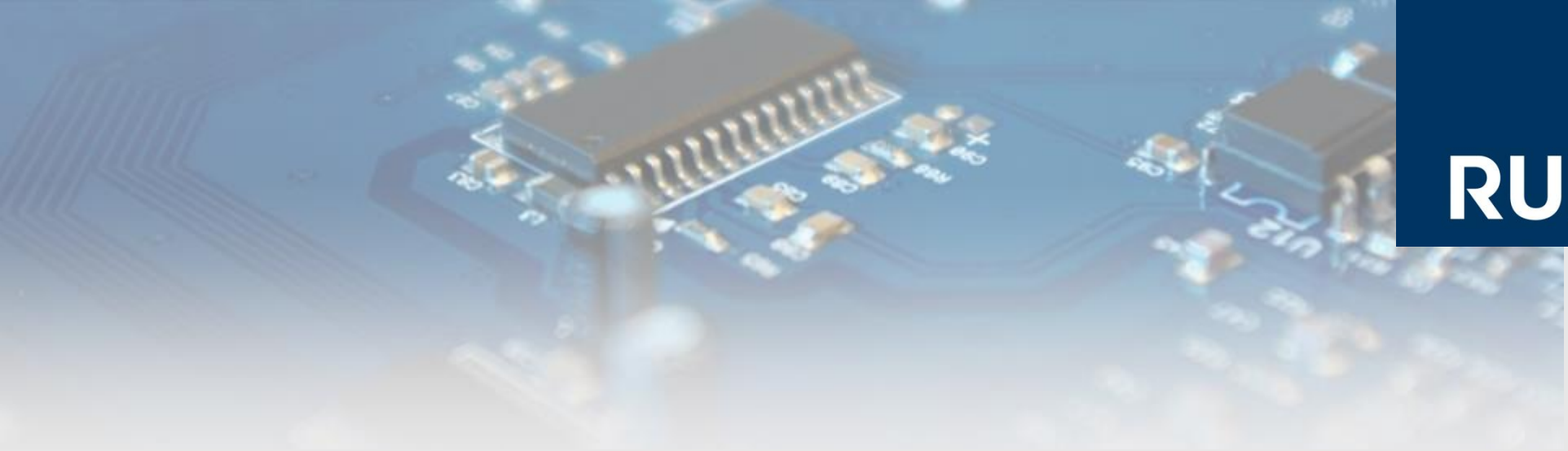
2nd-order



All because of processing the shares in consecutive clock cycles

Lesson Learned / Future Issues

- Design of a countermeasure based on a model
  - perfect protection
    - in theory and in practice?
  - more leakage sources and models in practice
- Exploiting leakage sources of the platform before design
- Cost of univariate resistance
  - security-performance tradeoff
- Processing the mask and masked data consecutively
  - slowly reaching the software performance?
    - making a processor by giant hardware?



Thanks!
Any questions?

amir.moradi@rub.de

Embedded Security Group, Ruhr University Bochum, Germany