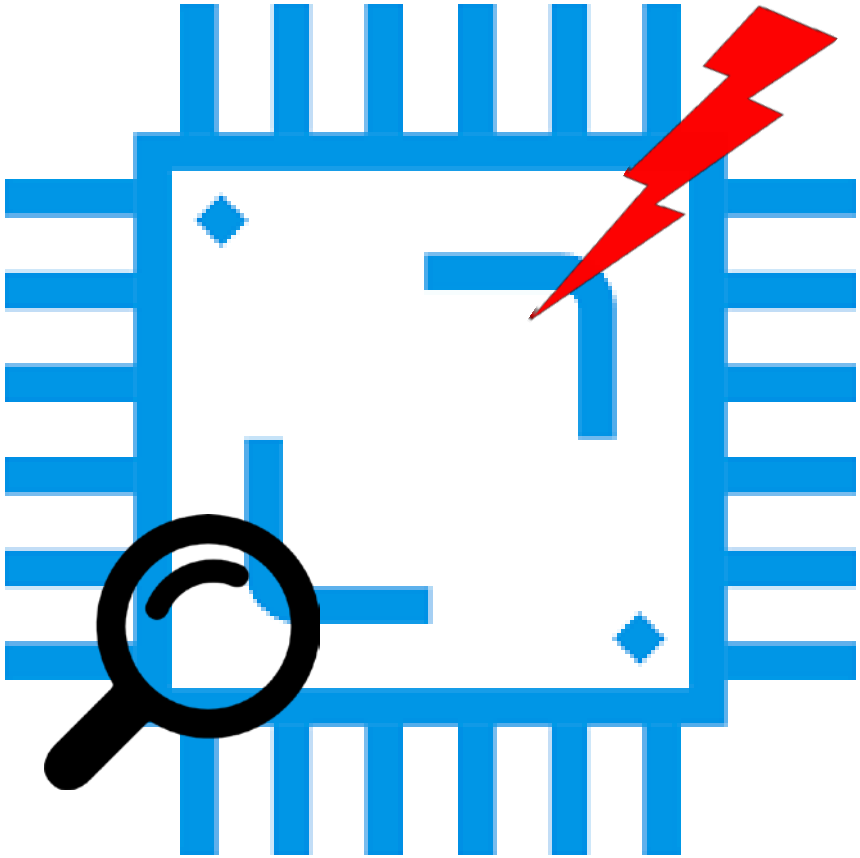
KU LEUVEN

COSIC

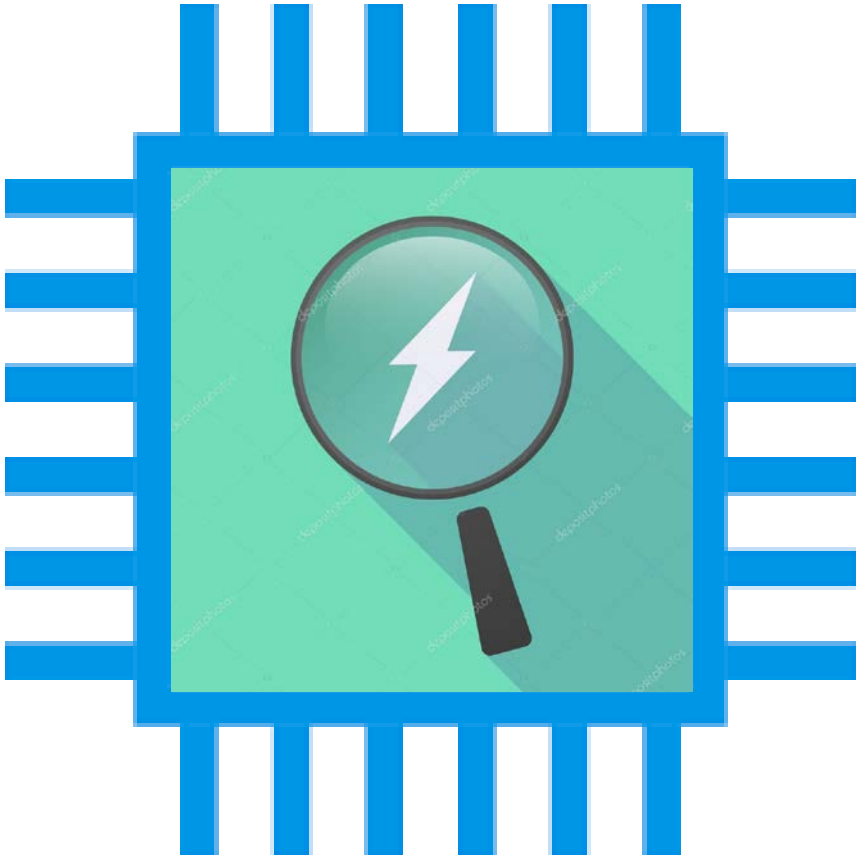
Glitch-Resistant Masking Schemes as Countermeasure Against Fault Sensitivity Analysis

Victor Arribas, Thomas De Cnudde, Danilo Šijačić

IoT security



IoT security



Outline

- FSA
- Threshold Implementations
- The power of SCA glitch-resistance
- Experiments
- Results

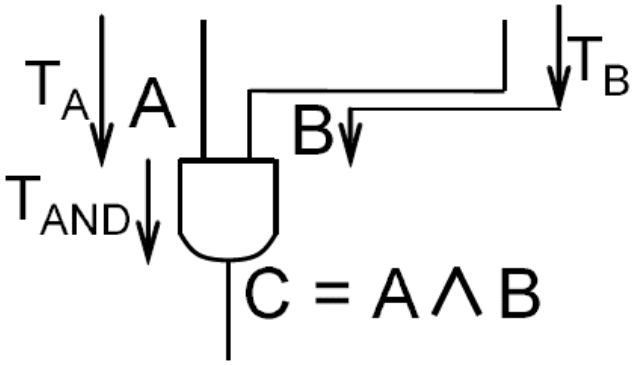
Outline

- FSA
- Threshold Implementations
- The power of SCA glitch-resistance
- Experiments
- Results

FSA

Actively triggered passive attack

Critical path depends on the data



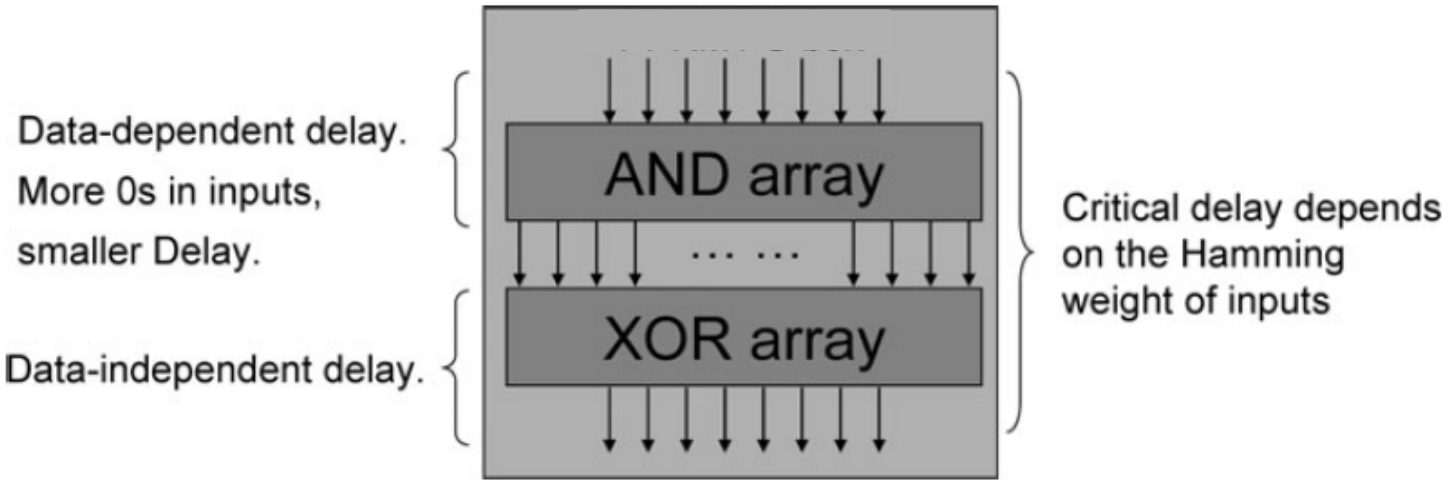
Source: ***[LSG+10]***

$$T_A < T_B \Rightarrow T_C = \begin{cases} T_A + T_{AND} & if\ A = 0 \\ T_B + T_{AND} & if\ A = 1 \end{cases}$$

XOR data-independent

[LSG+10] *Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in CHES 2010*

FSA



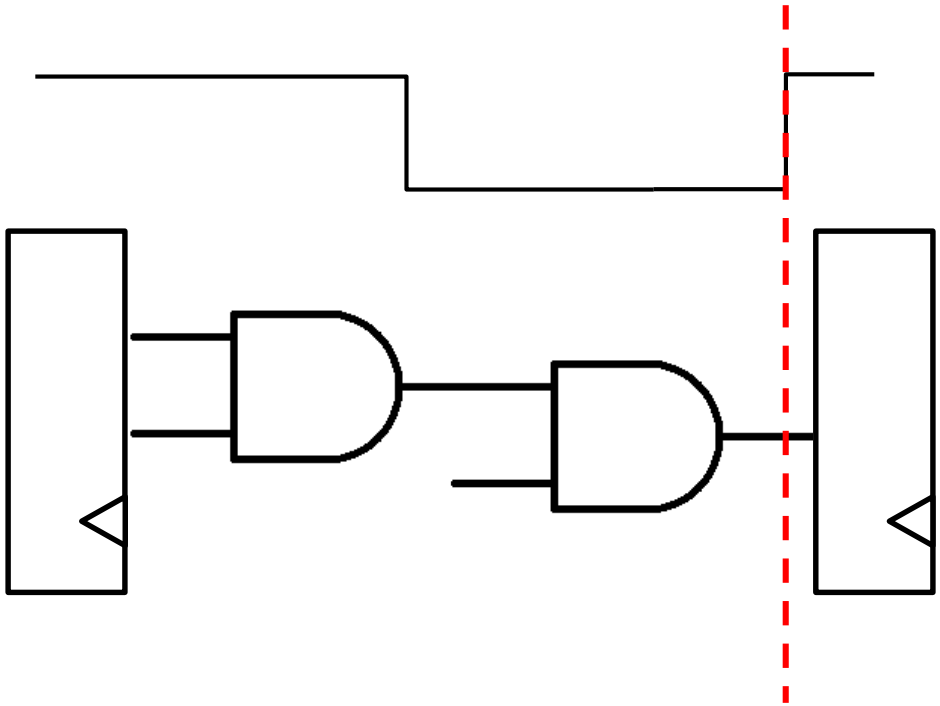
Source: ***[LSG+10]***

Critical timing delay ⇒ maximum timing delay

[LSG+10] *Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in CHES 2010*

FSA

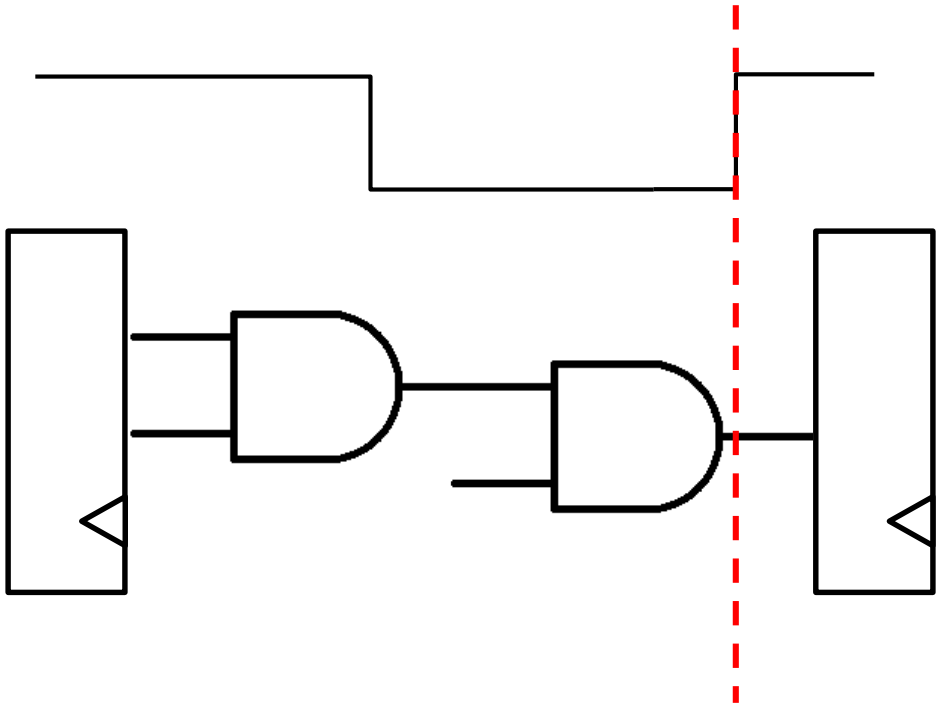
Fault sensitivity ⇒ Critical condition



[LSG+10] *Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in CHES 2010*

FSA

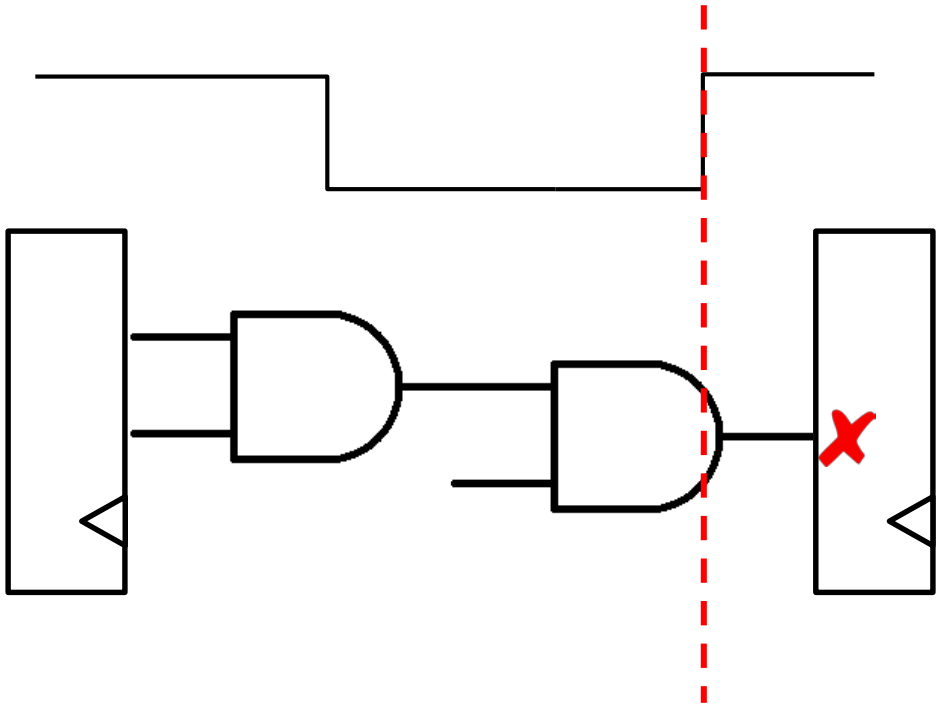
Fault sensitivity ⇒ Critical condition



[LSG+10] *Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in CHES 2010*

FSA

Fault sensitivity ⇒ Critical condition



Clock glitch

Our metric: propagation delay

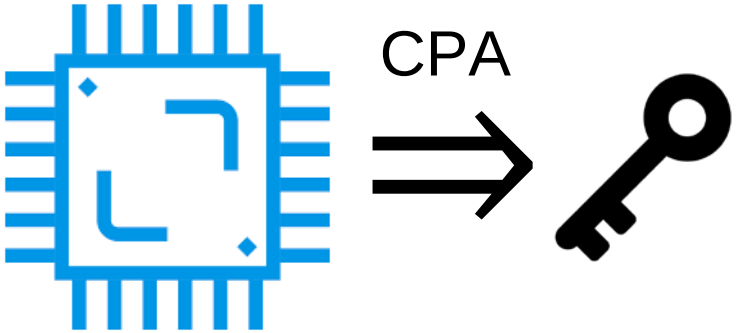
[LSG+10] *Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in CHES 2010*

FSA

Attack Implementation ⇒ Two phases

1. Profiling

2. Key recovery



Outline

- FSA
- Threshold Implementations
- The power of SCA glitch-resistance
- Experiments
- Results

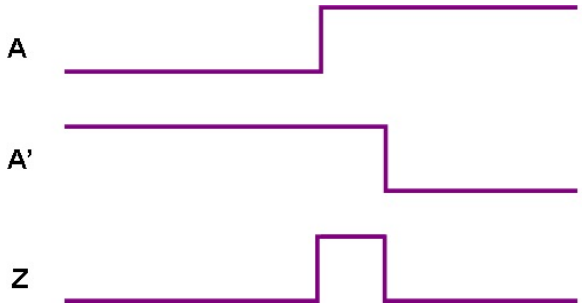
Threshold Implementations

Side-Channel Analysis (SCA) countermeasure

Provable security with minimal assumptions on the HW

Q.E.D.

Security in the presence of glitches



Threshold Implementations

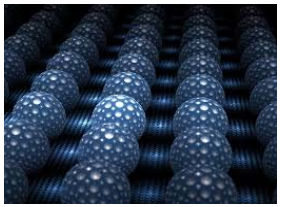
Boolean masking scheme

Secret sharing and multi party computation techniques

- Correctness

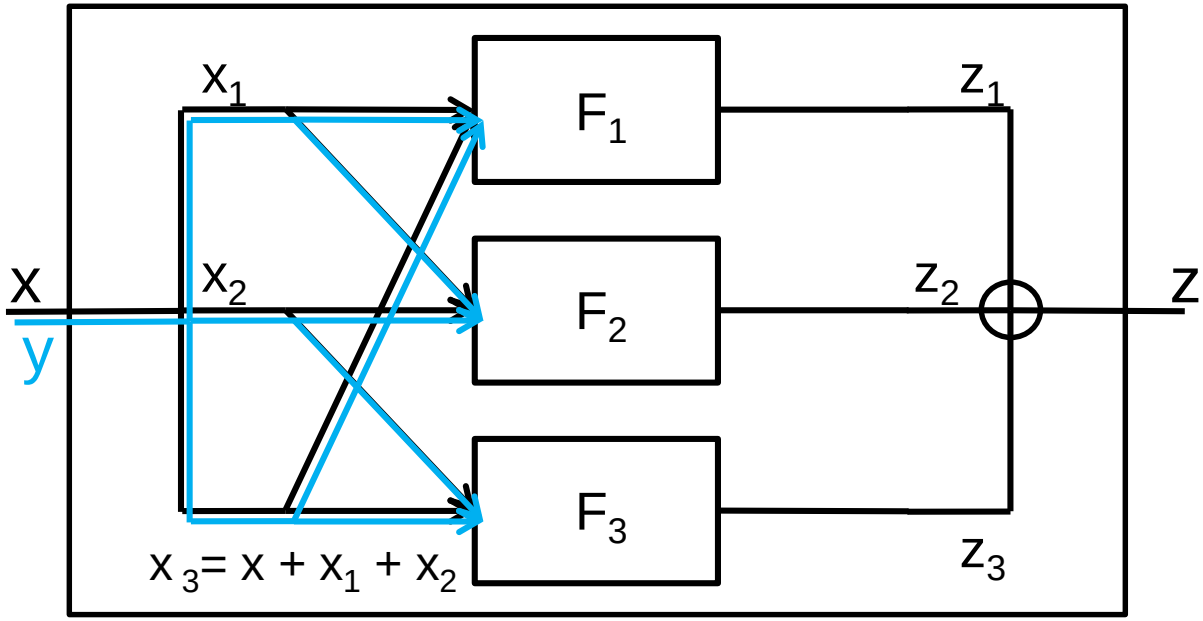
- Non-Completeness

- Uniformity



Threshold Implementations

Threshold Implementations (TI) [NRR06]

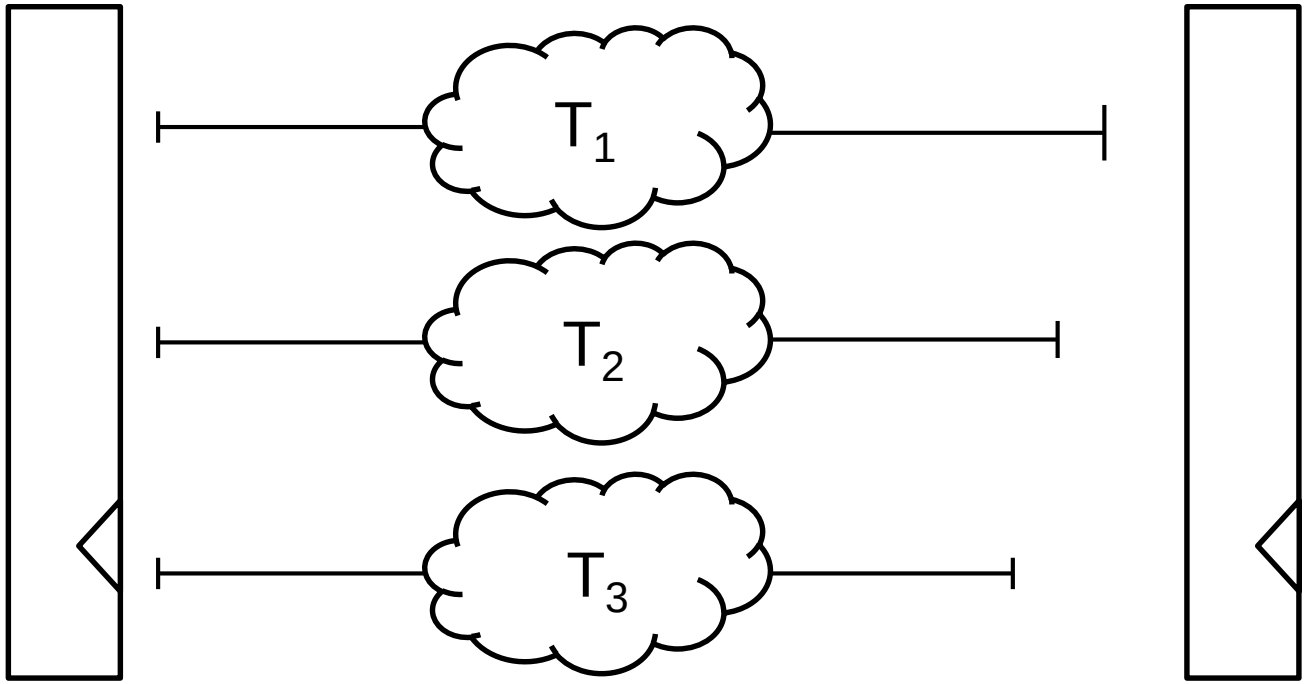


Outline

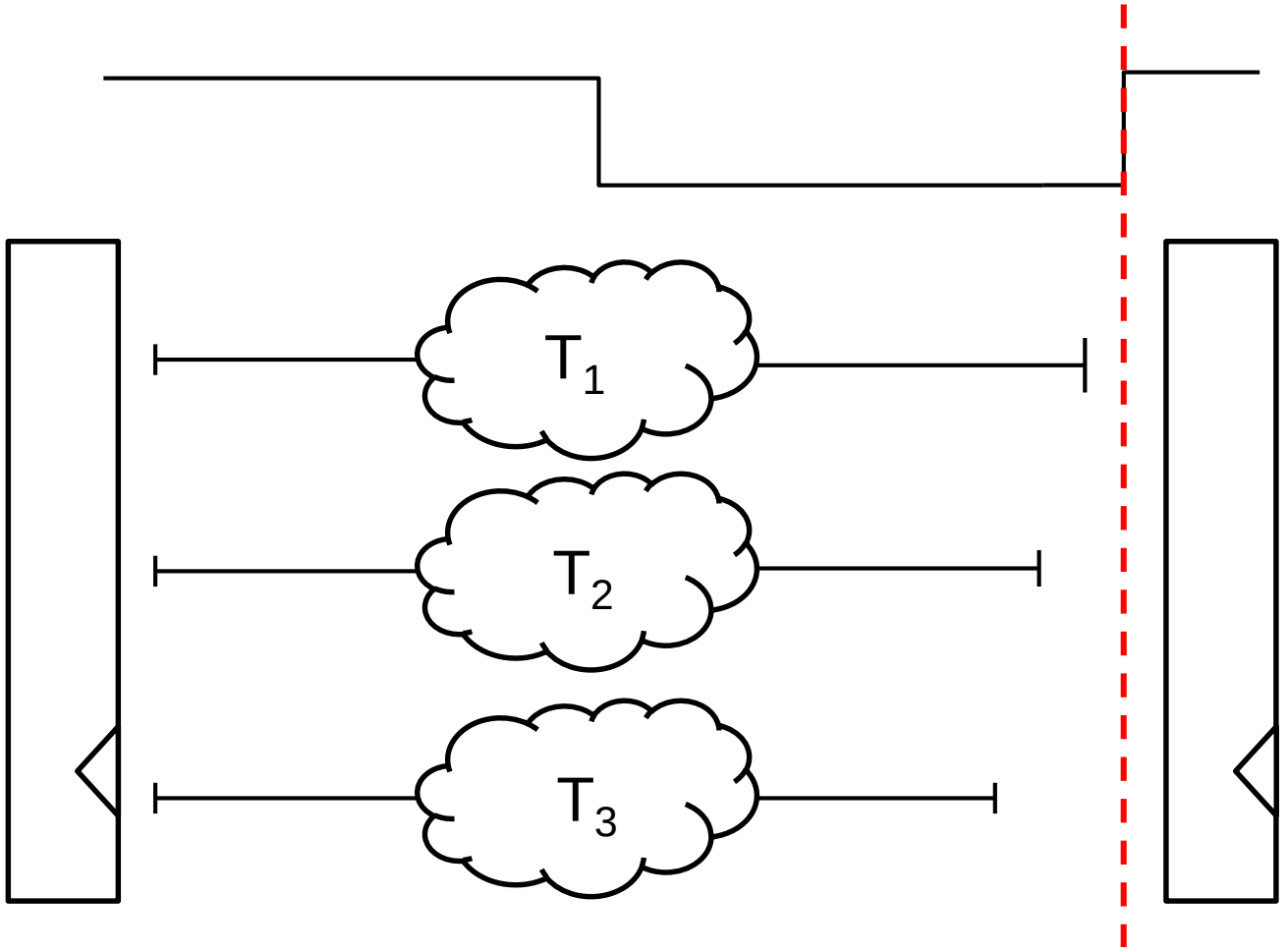
- FSA
- Threshold Implementations
- The power of SCA glitch-resistance
- Experiments
- Results

Glitch-Resistance

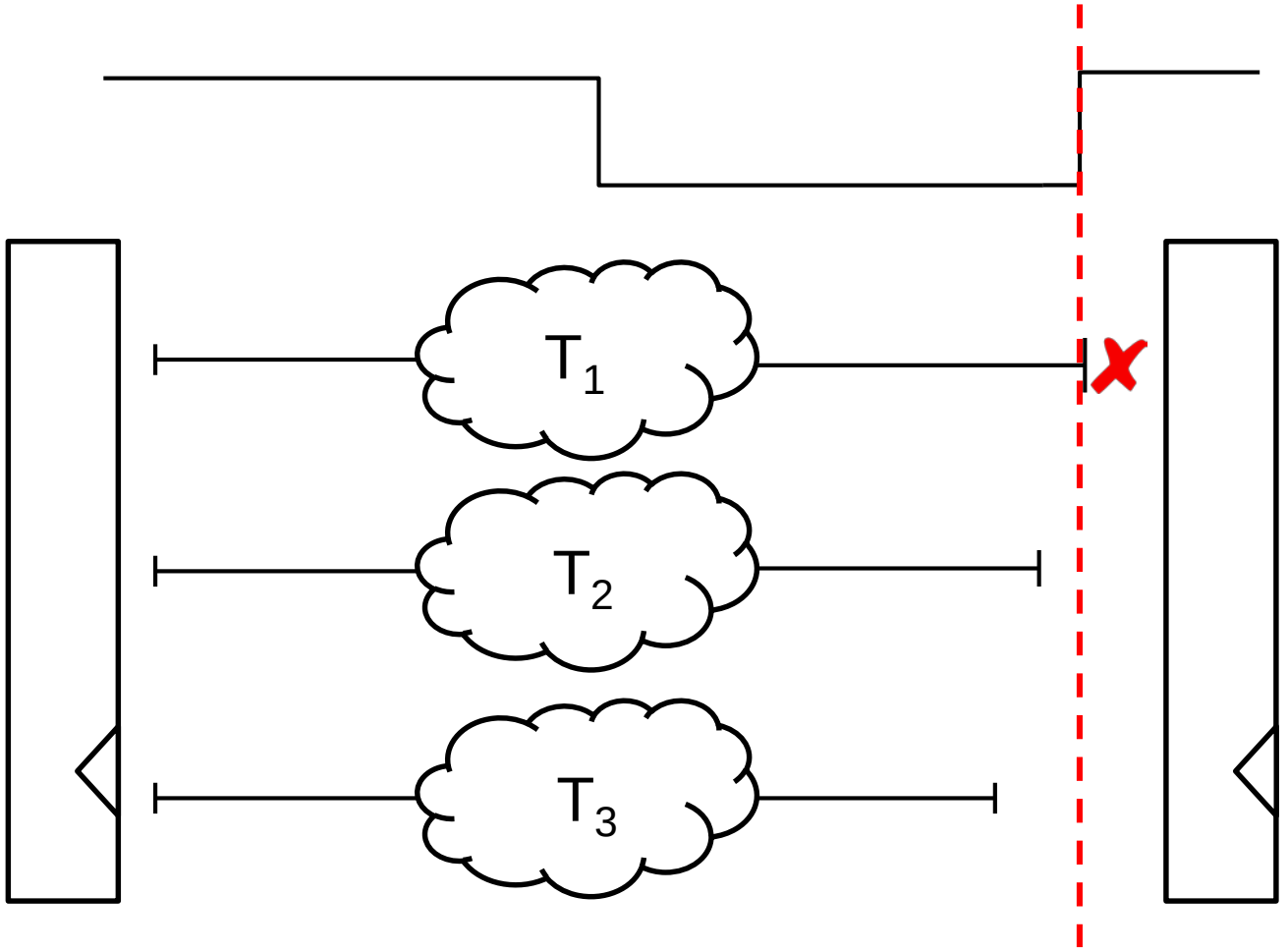
$$FS_1(x_{1,2}, y_1) \geq FS_2(x_{2,3}, y_2) \geq FS_3(x_{1,3}, y_1)$$



Glitch-Resistance

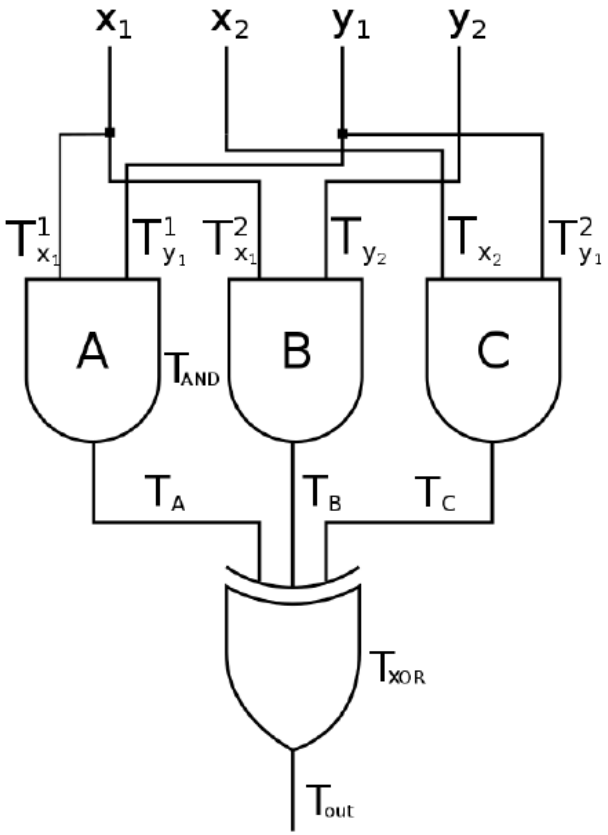


Glitch-Resistance



Glitch-Resistance

Share 1:



$$T_A = \begin{cases} T^1_{y_1} + T_{AND} & (\text{if } y_1 = \text{'0'}) \\ T^1_{x_1} + T_{AND} & (\text{if } y_1 = \text{'1'}) \end{cases}$$

$$T_B = \begin{cases} T_{y_2} + T_{AND} & (\text{if } y_2 = \text{'0'}) \\ T^2_{x_1} + T_{AND} & (\text{if } y_2 = \text{'1'}) \end{cases}$$

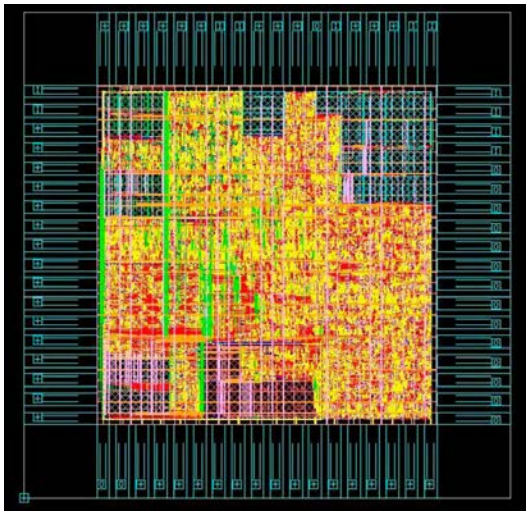
$$T_C = \begin{cases} T^2_{y_1} + T_{AND} & (\text{if } y_1 = \text{'0'}) \\ T_{x_2} + T_{AND} & (\text{if } y_1 = \text{'1'}) \end{cases}$$

Outline

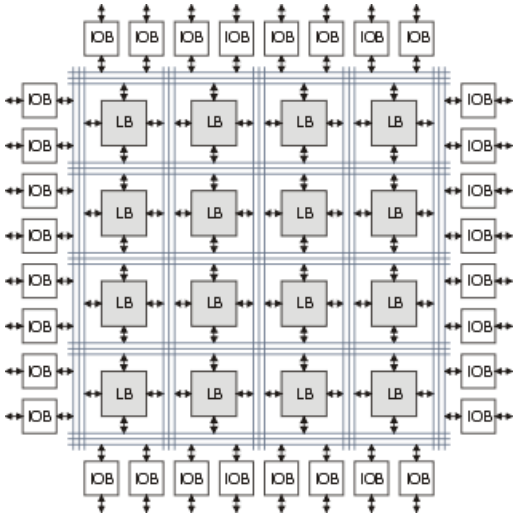
- FSA
- Threshold Implementations
- The power of SCA glitch-resistance
- Experiments
- Results

Experiments

ASIC



FPGA



CASCADE [SBY+18]

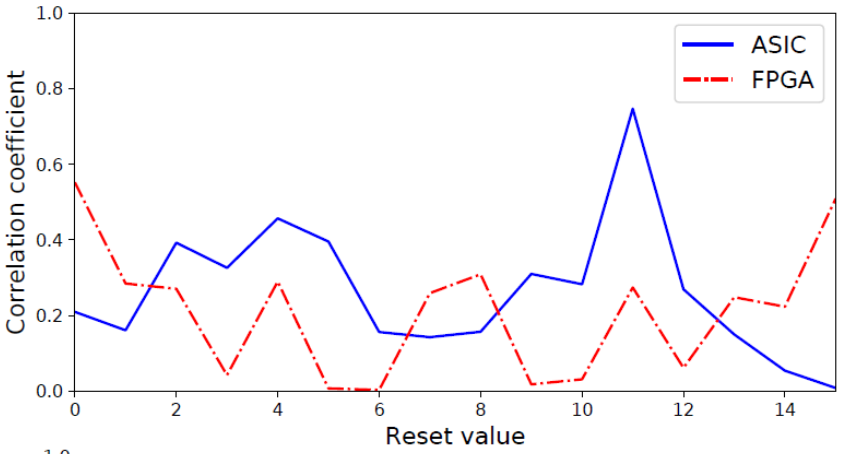
Xilinx tools

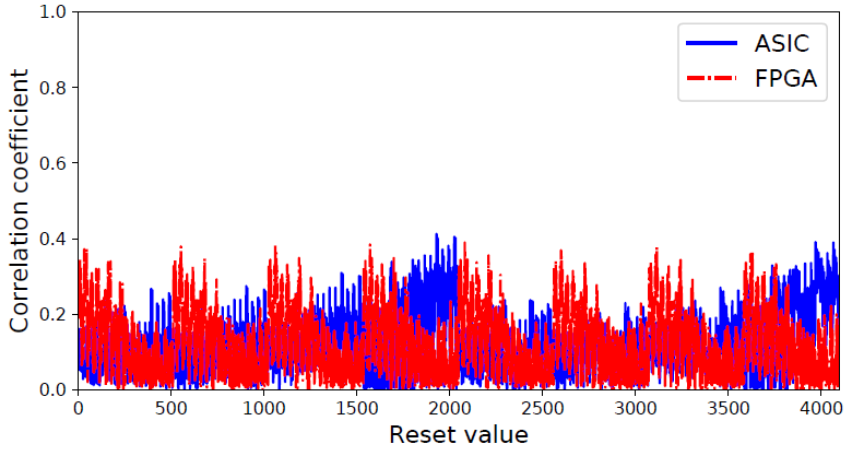
Targets: PRESENT and Keccak Sboxes

[SBY+18] *Danilo Šijačić, Josep Balasch, Bohan Yang, Santosh Ghosh and Ingrid Verbauwhede. Towards Efficient and Automated Side Channel Evaluations at Design Time. In PROOFS 2018*

Experiments

Profiling: initial value ⇒ $2^{2 \cdot N}$





PRESENT:

ASIC ⇒ 1011

FPGA ⇒ 0000

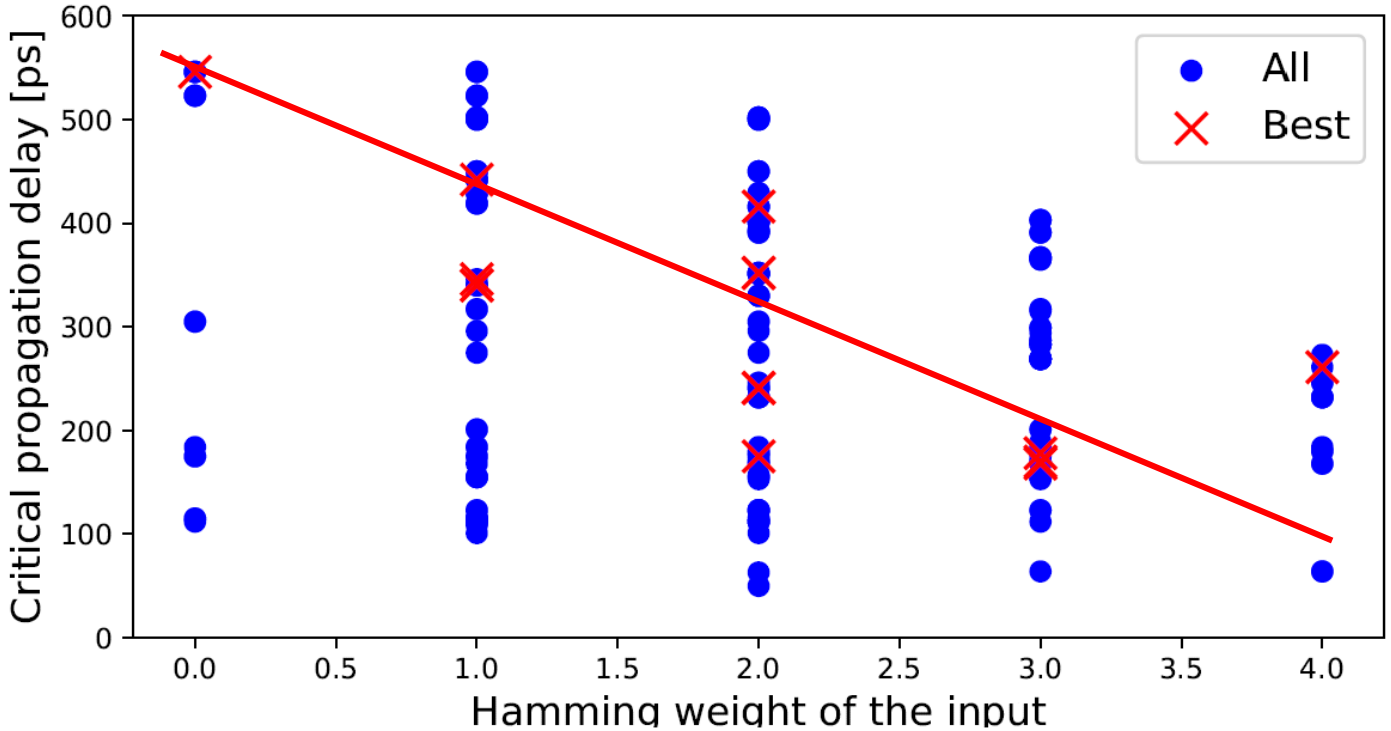
ASIC ⇒ 0x798

FPGA ⇒ 0x821

NOTE: correlation differences

Experiments

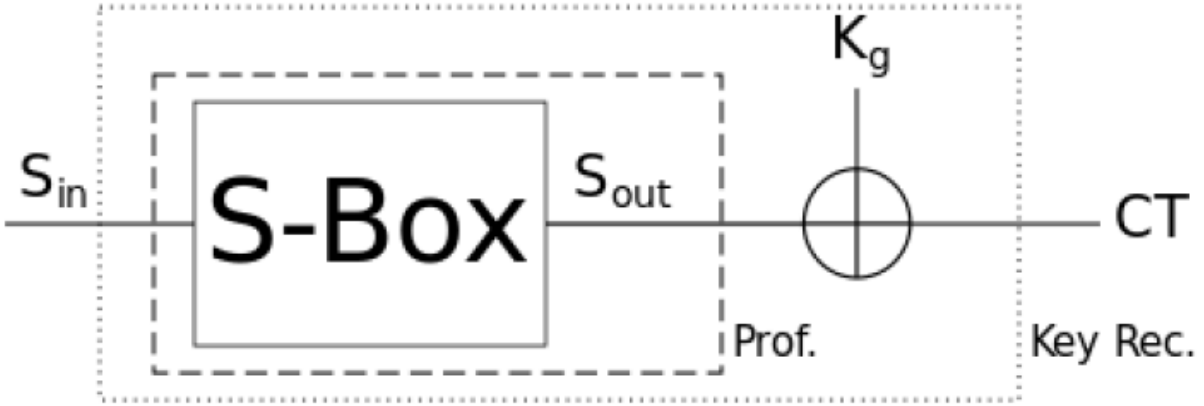
Profiling: One input reference profile



Pick the best correlation profile

Experiments

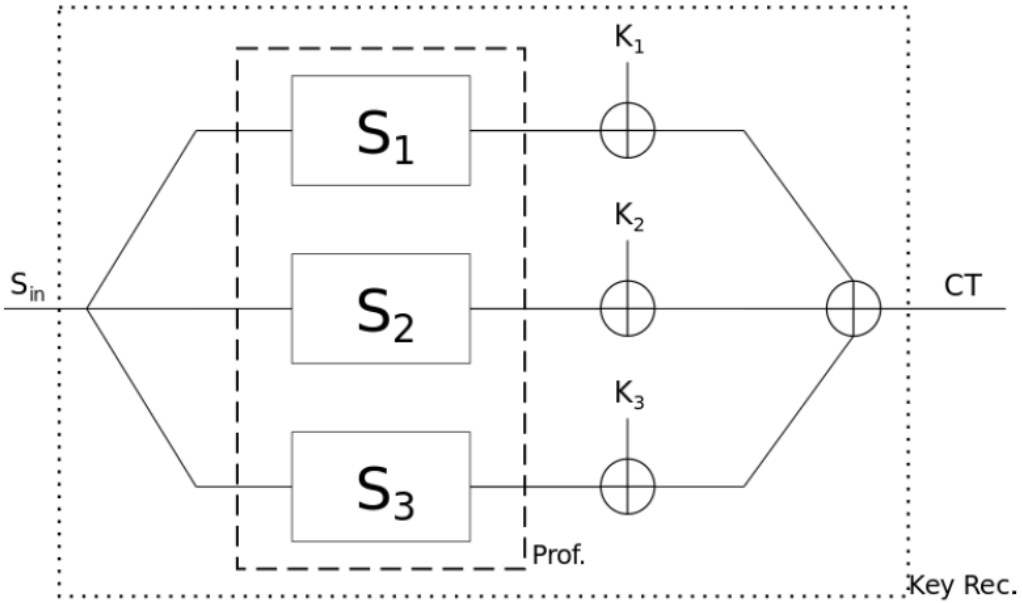
Test circuit



$$FS_g = HW(SBox^{-1}(CT \oplus K_g))$$

Experiments

Test circuit



Profiling ⇒ known sharing

Key recovery ⇒ unshared ptxt-ciph

Experiments

Unrealistically strong adversary

Detailed profiling

Straightforward circuit

Whole state of inputs covered

Highest correlation initial value

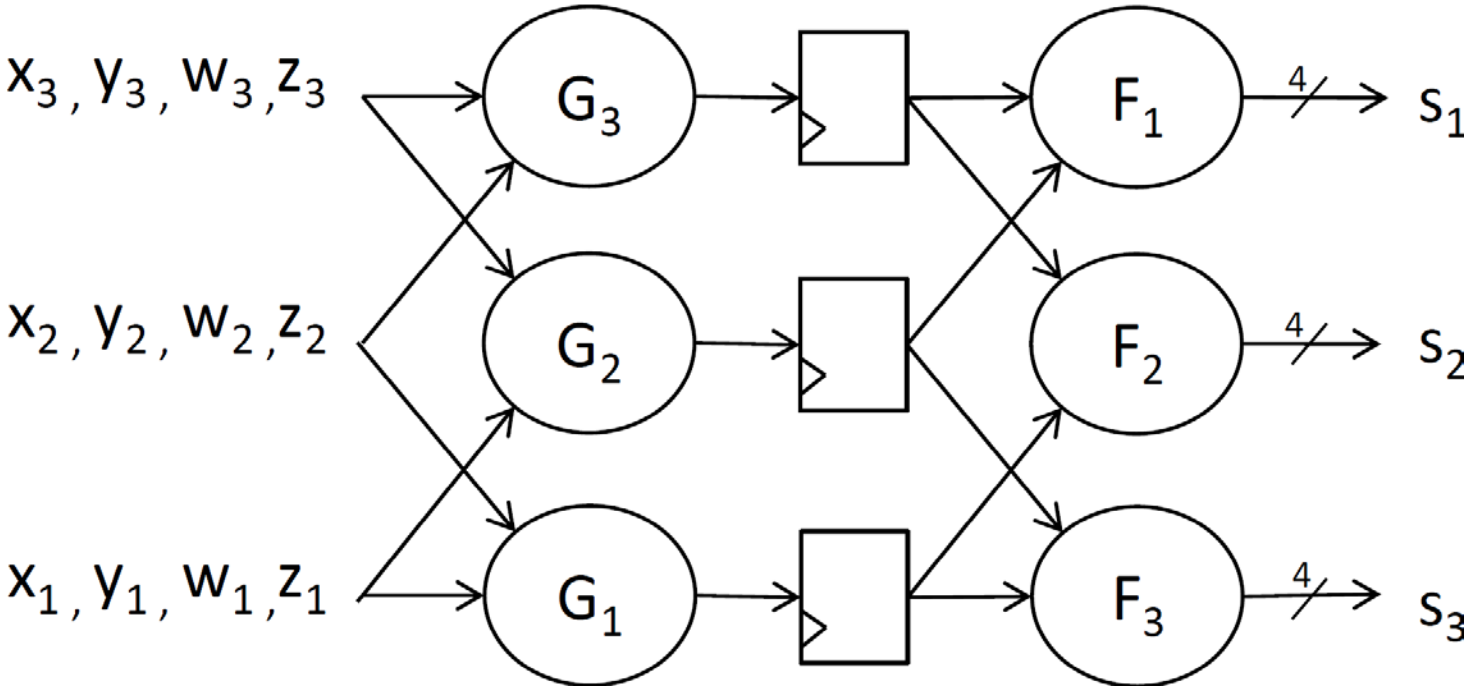
Unrealistic metric

Outline

- FSA
- Threshold Implementations
- The power of SCA glitch-resistance
- Experiments
- Results

Results

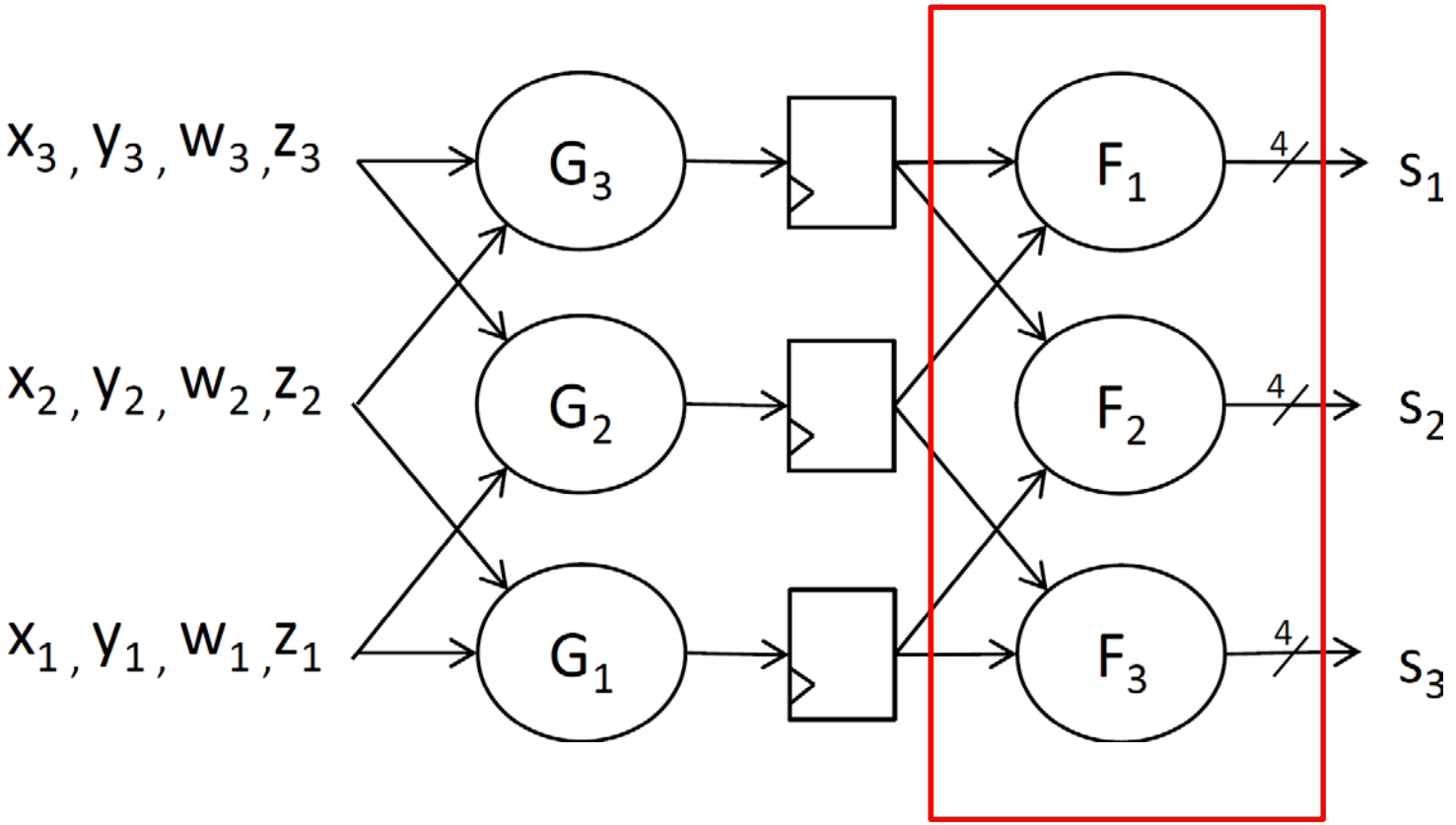
Poschmann et al. implementation of PRESENT [PMK+11]



[PMK+11] *Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-channel resistant crypto for less than 2, 300 GE. In J. Cryptology 2011.*

Results

Poschmann et al. implementation of PRESENT [PMK+11]

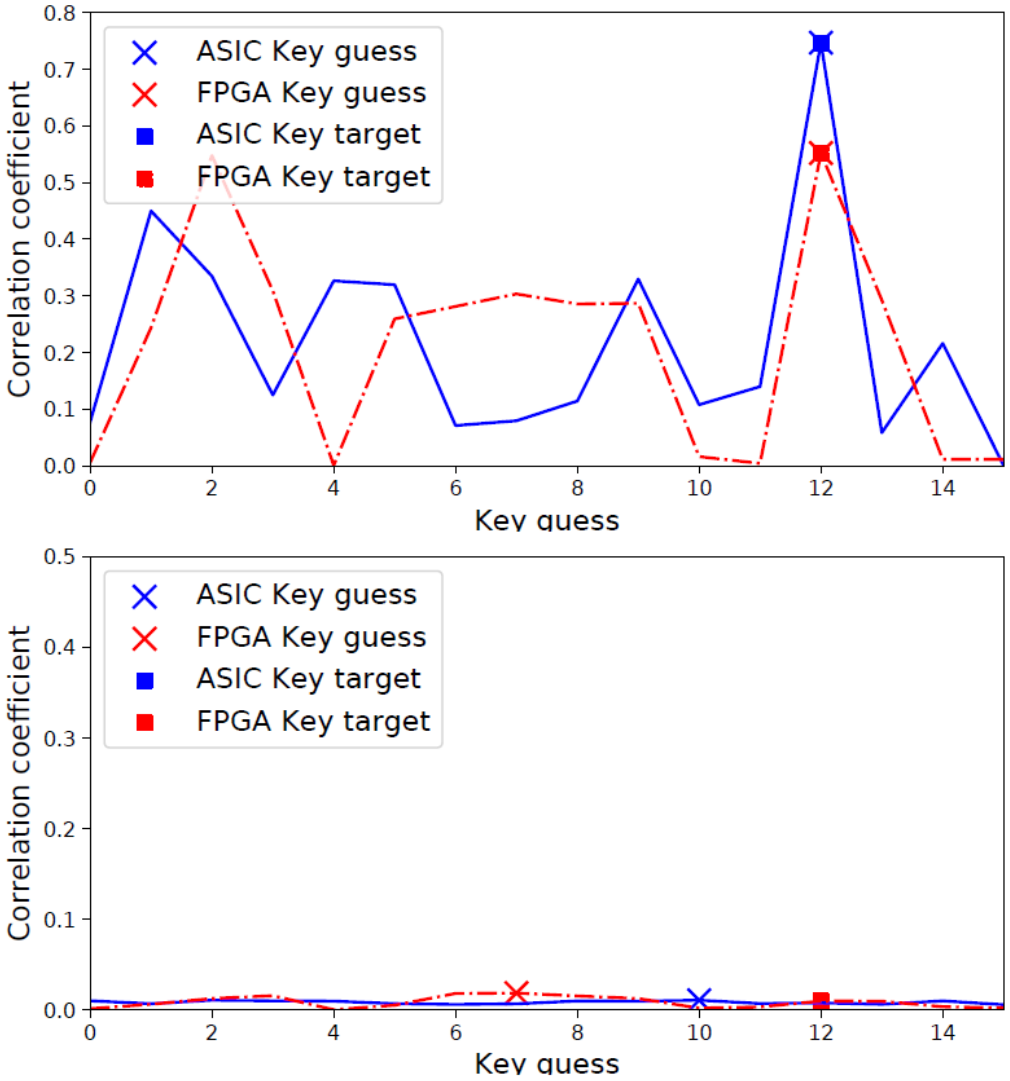


[PMK+11] *Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-channel resistant crypto for less than 2, 300 GE. In J. Cryptology 2011.*

Results

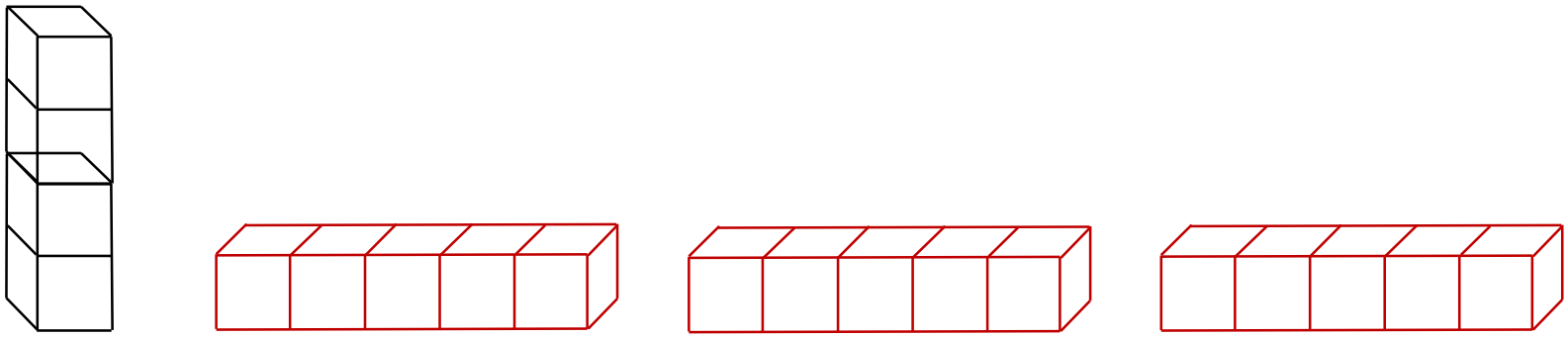
PRESENT:

Key = 12



Results

Keccak “Changing of the Guards” [Daemen17]



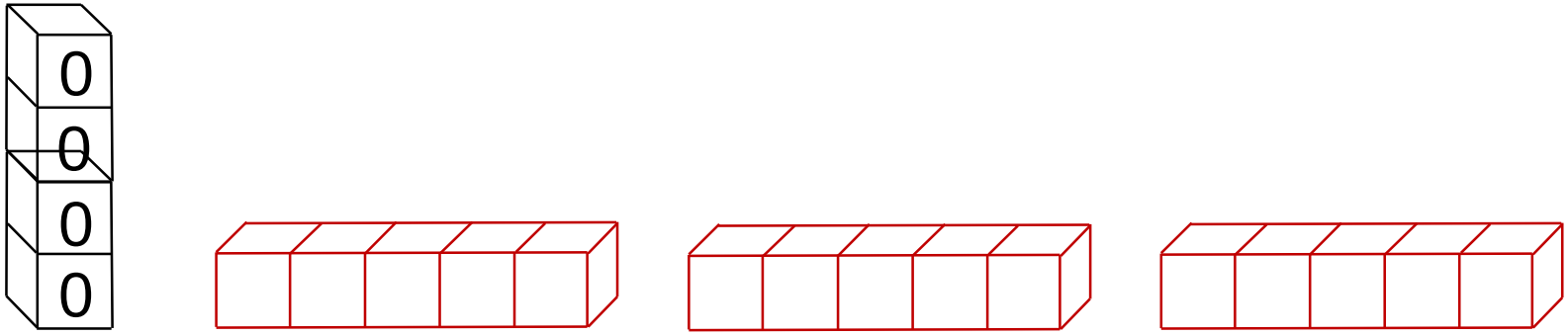
19 bits ⇒ 15 bits Sbox

Uniform

[Daemen17] *J. Daemen. Changing of the guards: A simple and efficient method for achieving uniformity in threshold sharing. In CHES 2017.*

Results

Keccak “Changing of the Guards”



15 bits ⇒ 15 bits Sbox

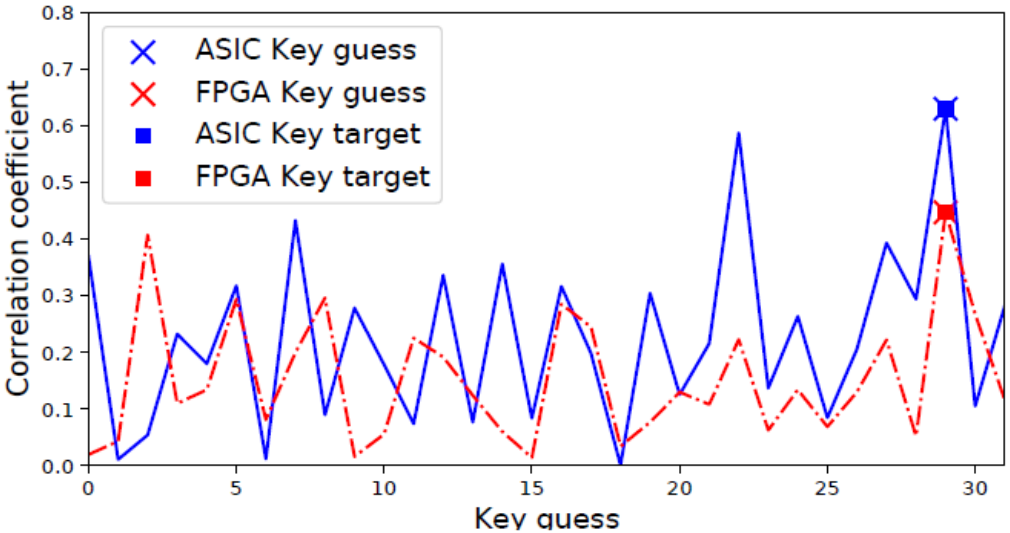
NOT Uniform

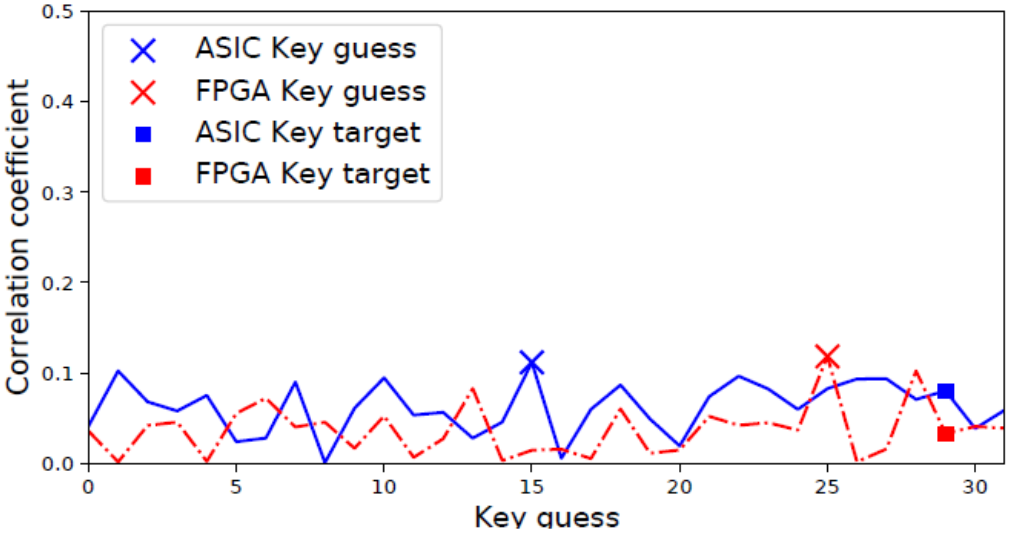
[Daemen17] *J. Daemen. Changing of the guards: A simple and efficient method for achieving uniformity in threshold sharing. In CHES 2017.*

Results

Keccak:

Key = 29





Conclusions

- Glitch-resistant masking schemes provide FSA protection
- This protection is ensured by Non-completeness
- Unreallistically powerfull attacker
- Tests over simulations in ASIC and FPGA

Thank you!