Constructive Side Channel Analysis

An Useful Tool for Secure Circuit Design

Marc Stöttinger

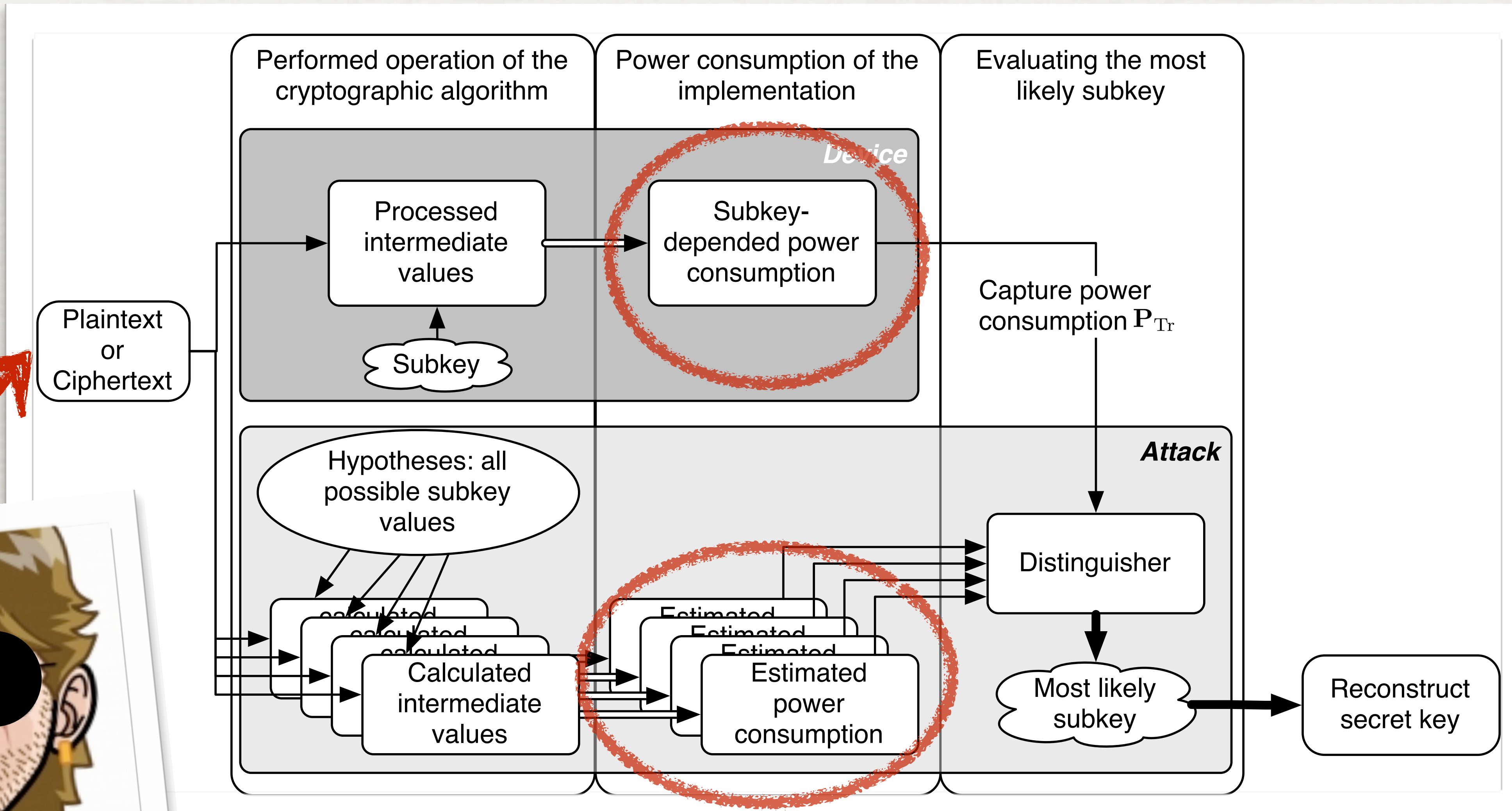
Technische Universität Darmstadt

Outline

- Assumptions of the Attacker
- Countermeasures
  - Masking
  - Hiding
- Constructive Side-Channel Analysis
  - Linear Regression based Modeling
  - Model Verification
  - Signal to Noise
- Summary
- Outlook

Assumptions of the Attacker

Power analysis attack

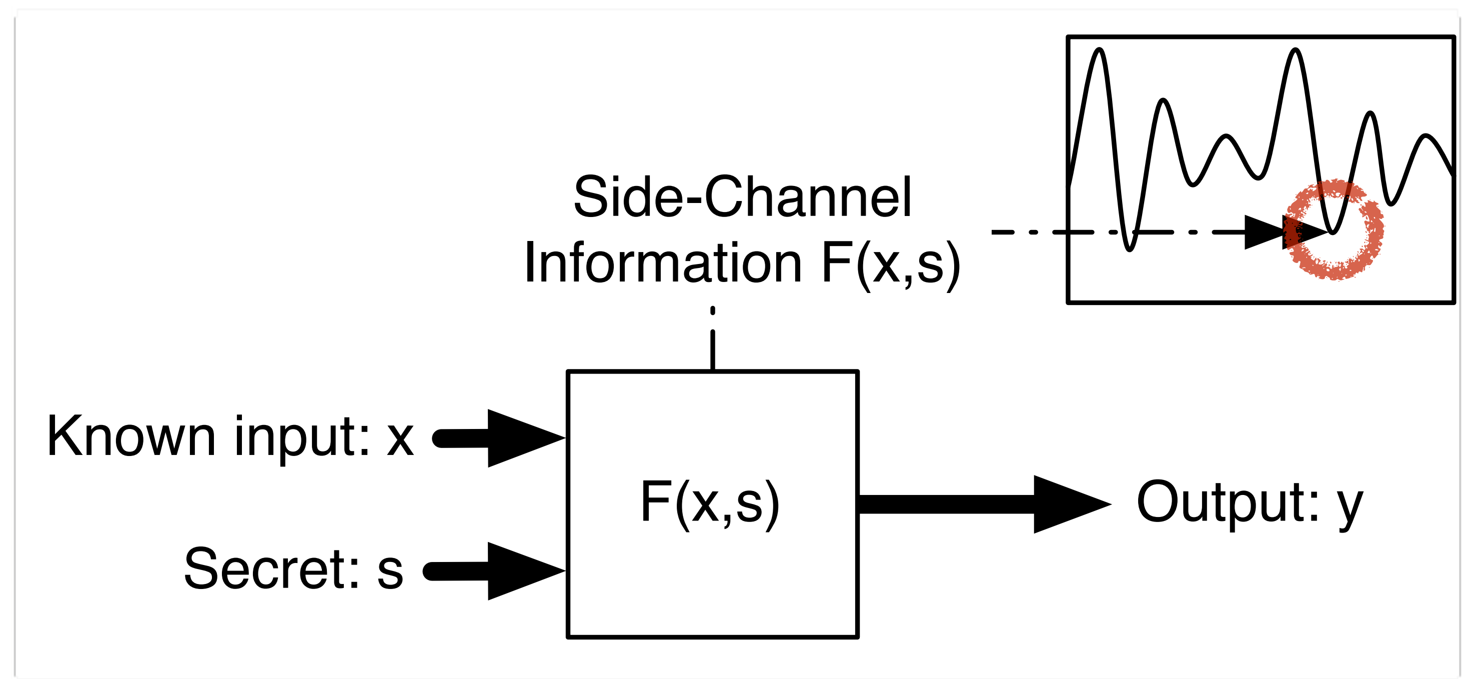


source: http://wikis.zum.de/rmg/Benutzer:Deininger_Matthias/Facharbeit/Alice_Bob_und_Mallory

Countermeasures

Introduction

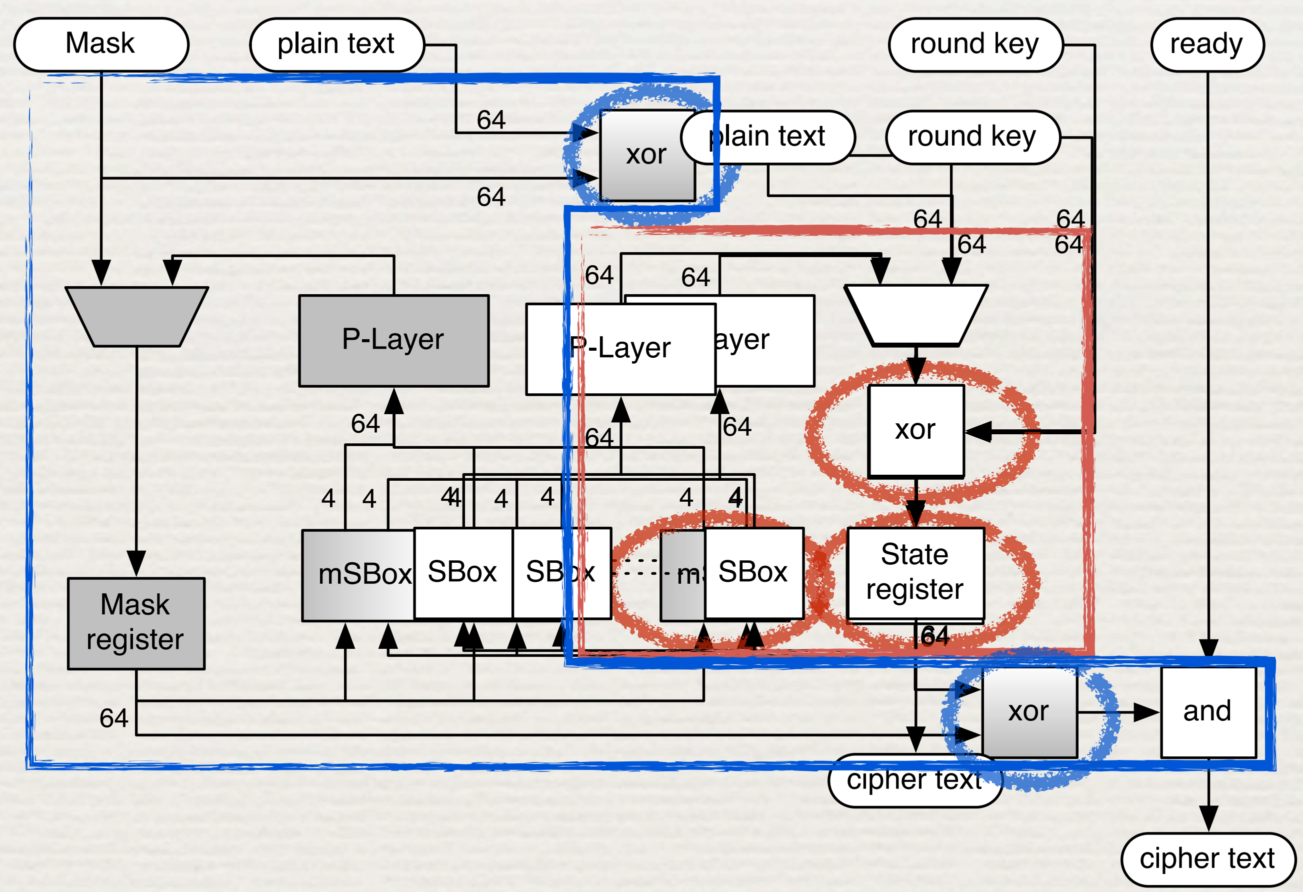
- **Protect** a specific operation or segment of the circuit
- Lower the information **leakage** at certain time instants
- Increase the **effort** to extract exploitable information from the observations



Countermeasures

Principle of masking

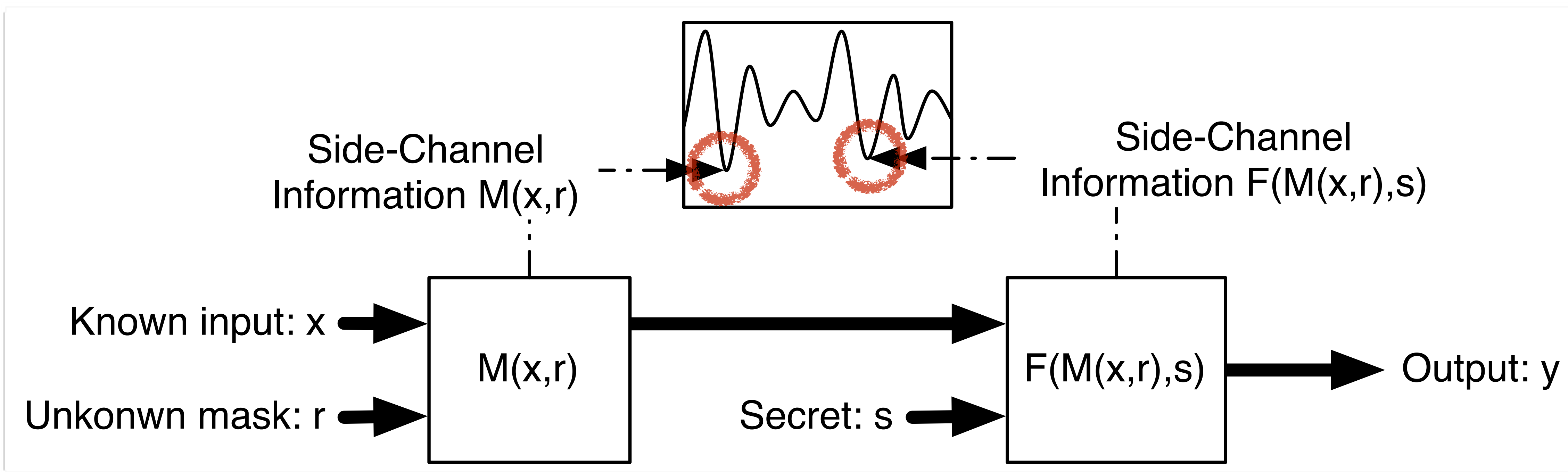
- **Randomize** intermediate values of the internal operation
- Use principle of secret sharing to **increase** the attack effort
- Attacker **cannot** properly estimate the power consumption per trace



Countermeasures

Principle of masking cond.

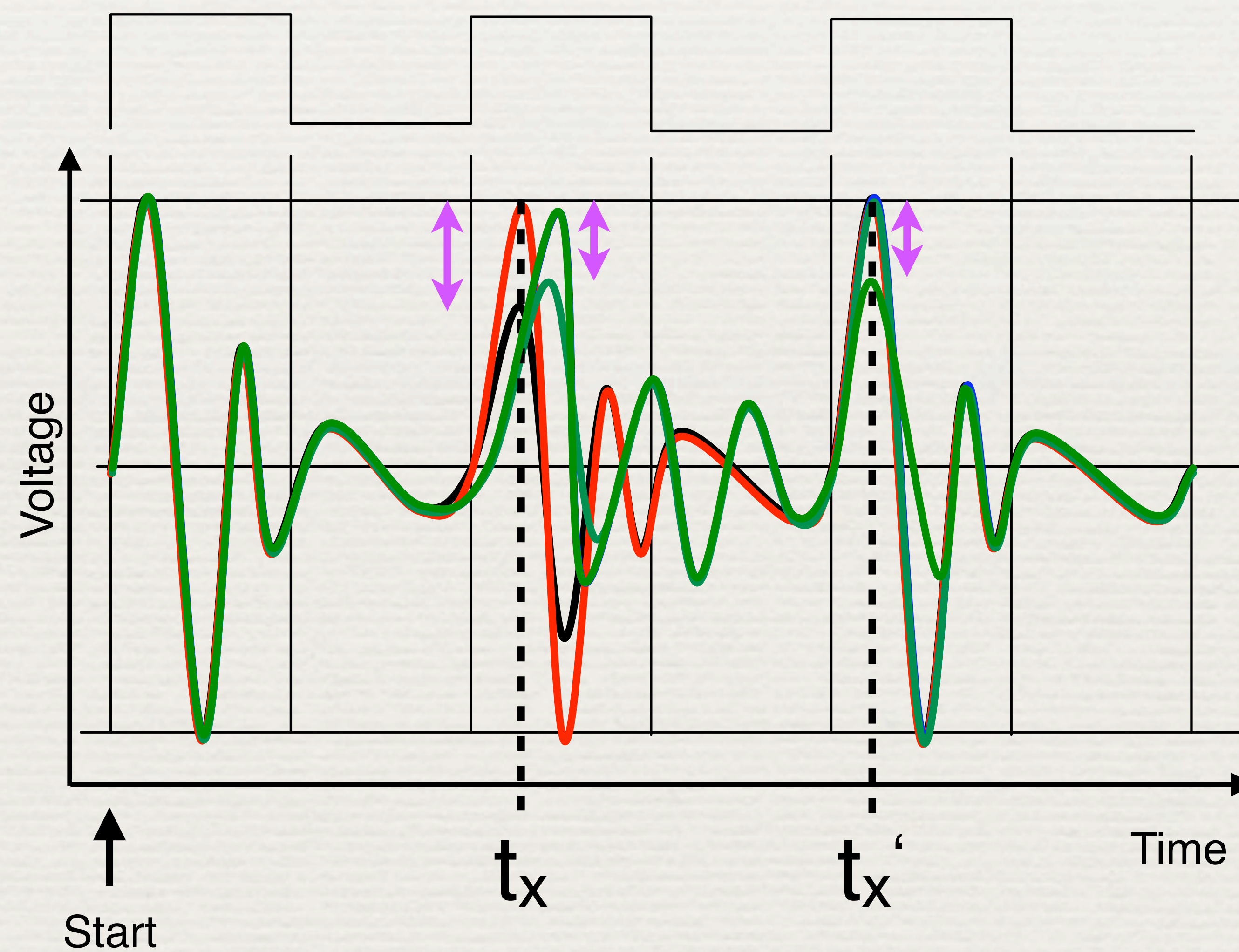
- Combine information from several points in time to extract exploitable informations -> **higher order** attacks



Countermeasures

Principle of hiding

- **Decoupling** the power consumption and the internal operation
- Randomizing or leveling the **overall** power consumption
- Hiding techniques can be applied on the **time**- and **amplitude**-domain

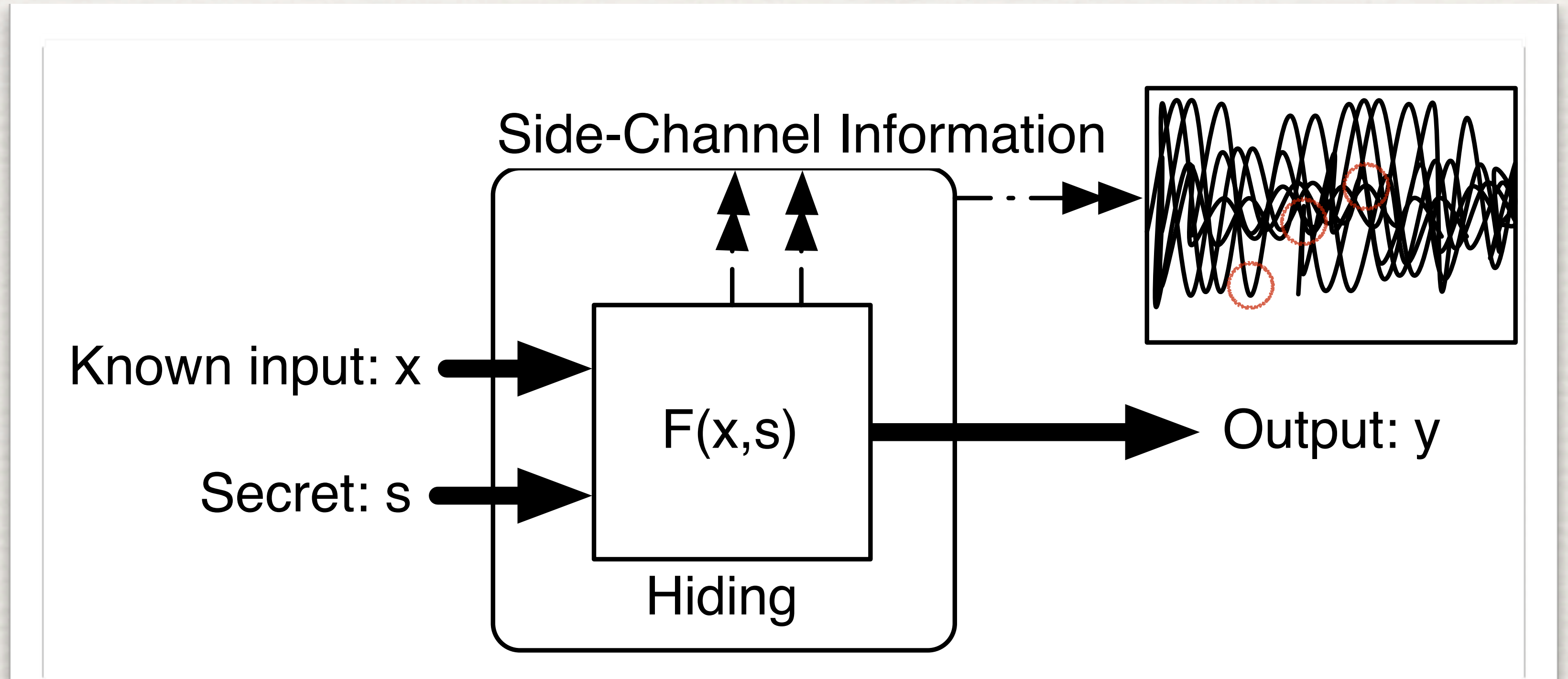


Mittwoch, 13. Juni 2012

Countermeasures

Principle of hiding cond.

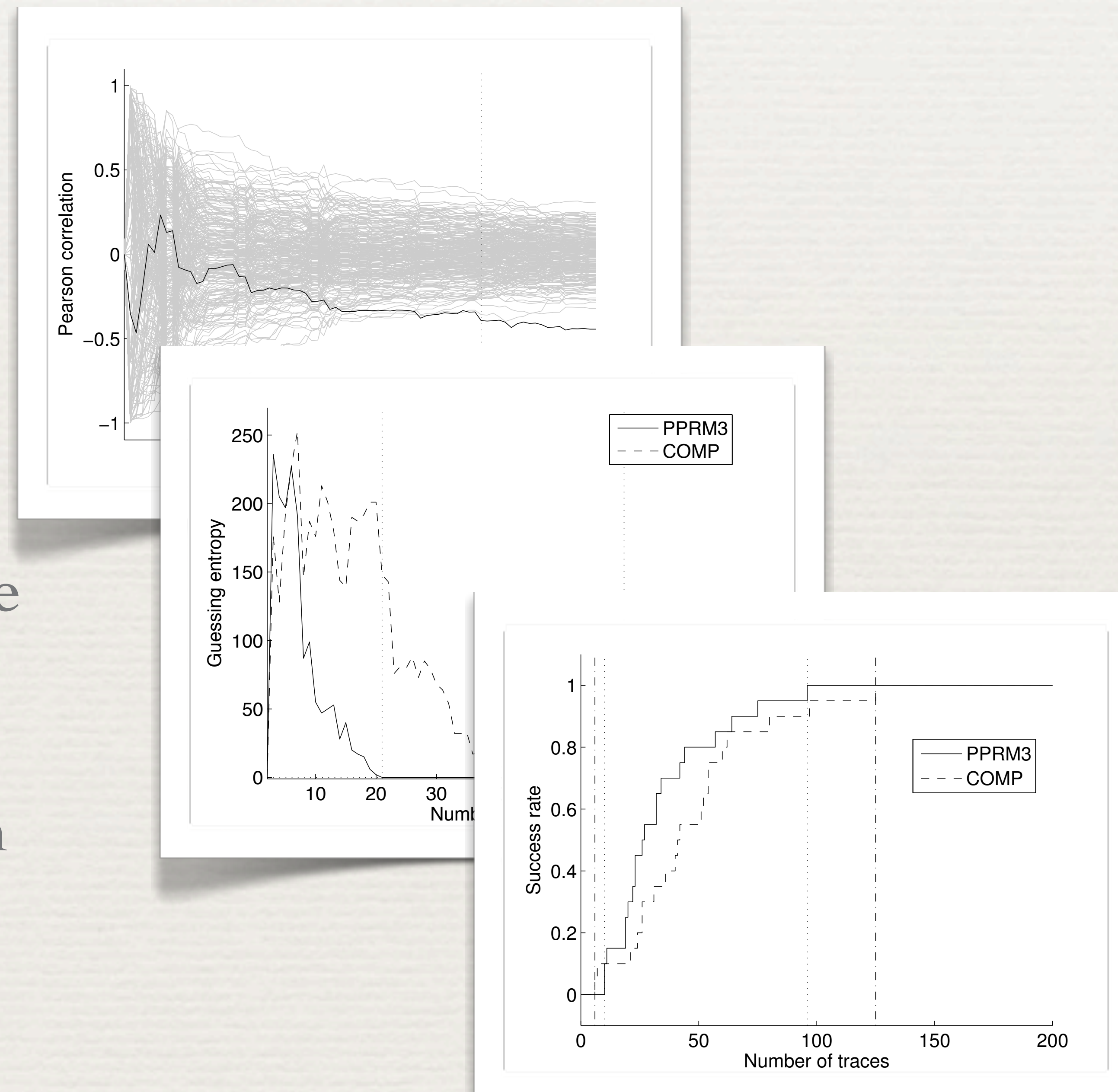
- More trace are required as well as preprocessing methods are needed in order to increase the information **extraction**
- Hiding techniques depends strongly on the **platform**



Countermeasures

Figure of merit

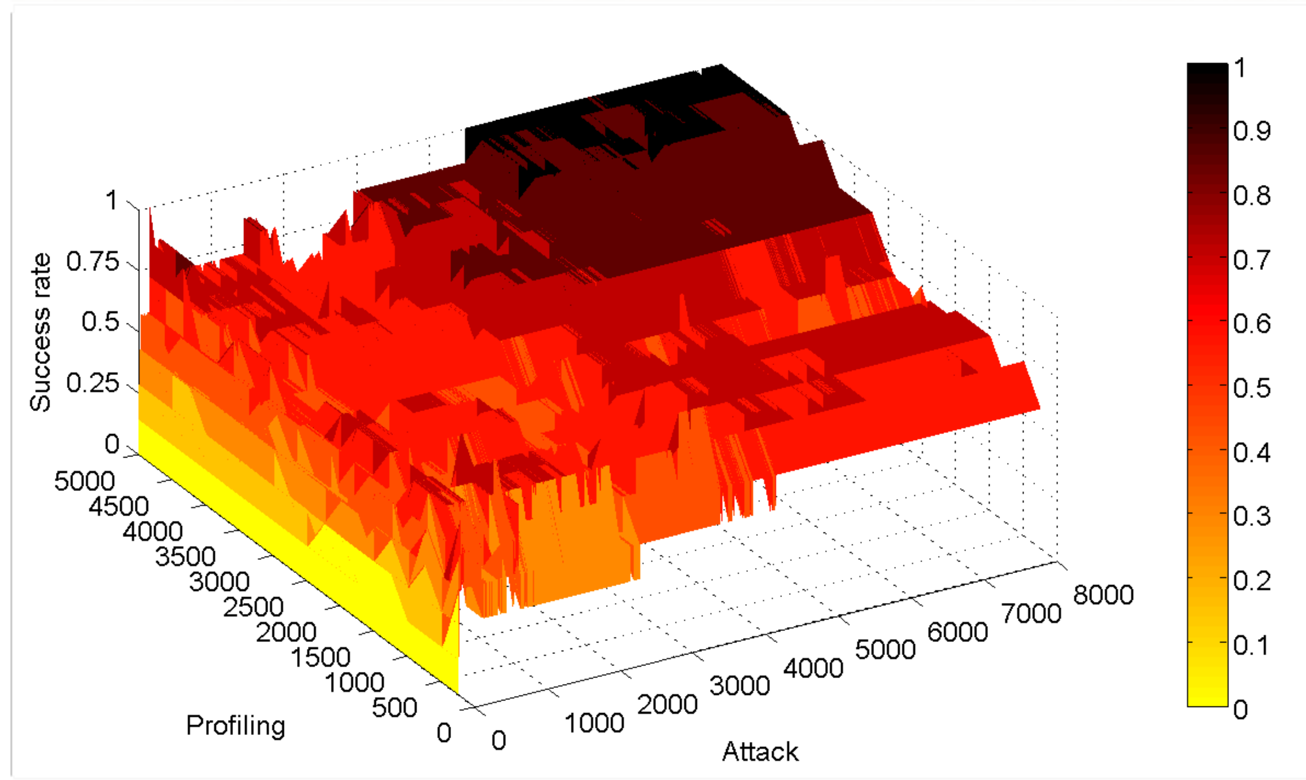
- Number of traces to successfully attack the design -> is **attackable** with a certain effort
- Guessing Entropy -> how much information an attacker **gains** per trace
- The success rate provides the attack success in **average** -> rough estimation of the general vulnerability



Countermeasures

What is the matter?

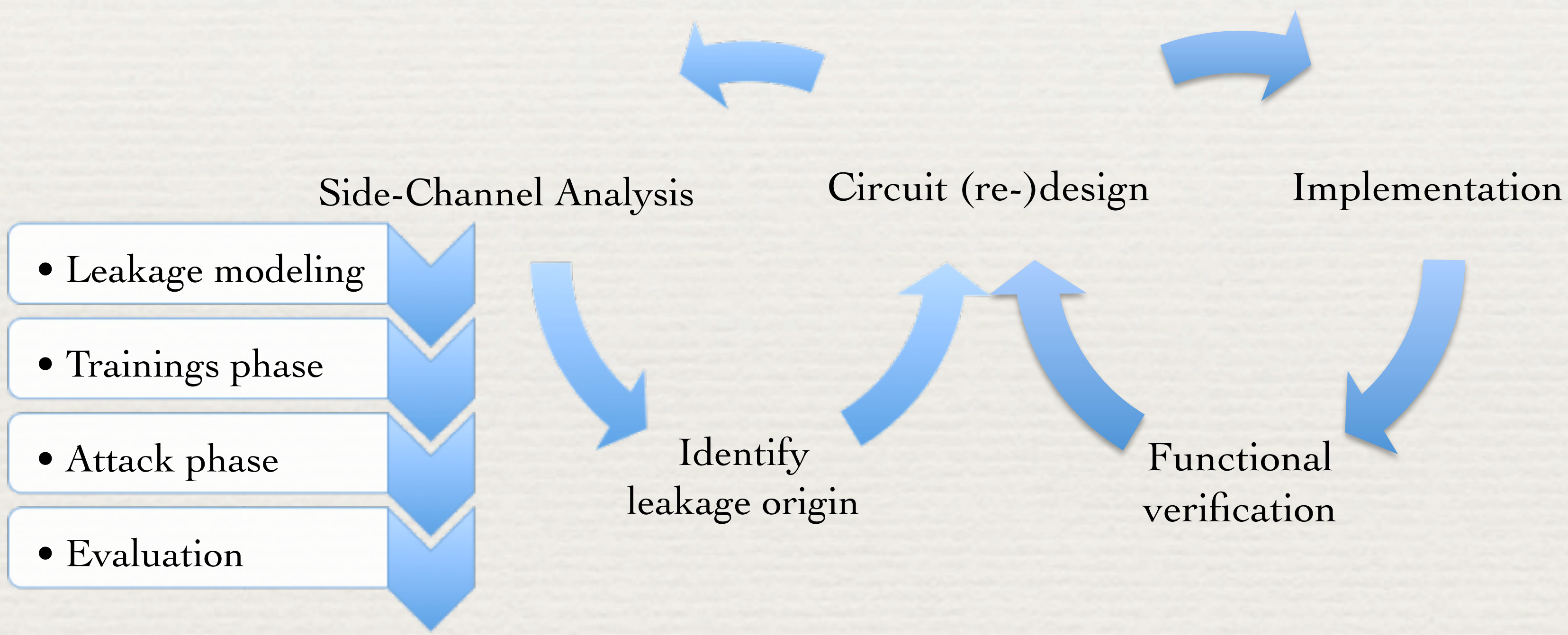
- In theory everything is clear



- **Iterative cycle** of designing, implementing and attacking
- Embedded devices have always resources and timing **constrains**!
- Multiple attacks are needed with different settings-> **time exhausting**

Confidence of Security

Correct model?



In the end a strong implementation?

source:http://coachchrisfore.wordpress.com/2012/05/06/the-importance-of-self-confidence-in-athletics-part-2/

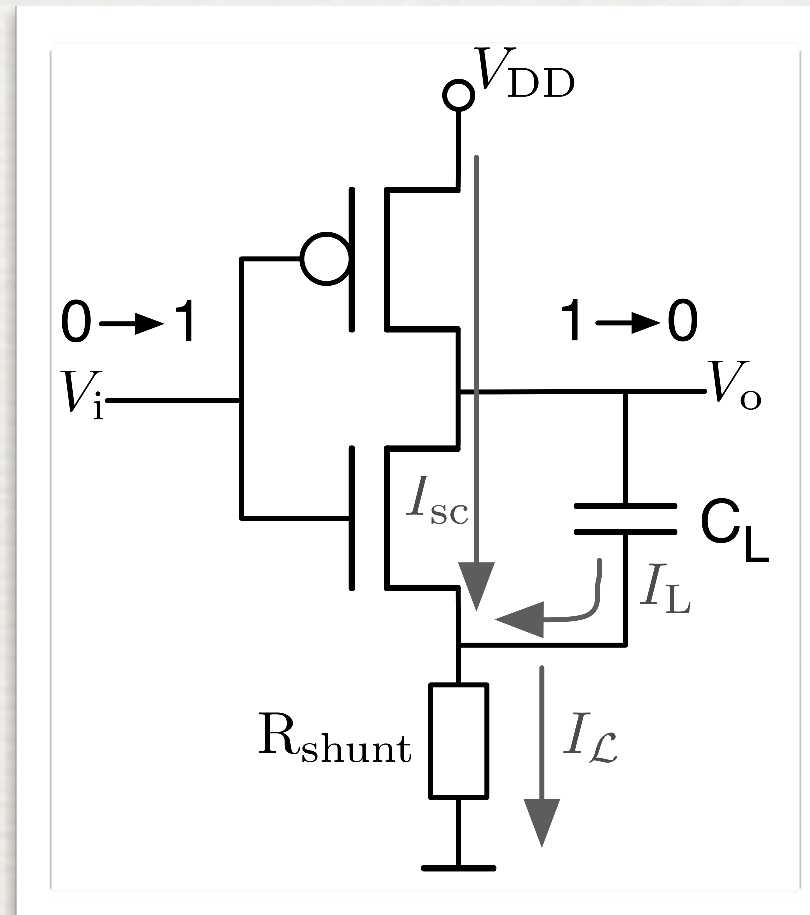
Better **understanding** of the circuit leads to:

- Better **leakage** models
- Better **countermeasures**
- There is a need to **check** the model

Constructive Side-Channel Analysis

What does we actually exploit in CMOS based circuits?

- **Short** circuit based power consumption
  $\mathcal{P}_{\text{sc}} = I_{\text{sc}} \cdot V_{\text{DD}}$



- Dynamic power consumption in **general**

$$\mathcal{P}_{dyn} = \mathcal{P}_{0\to1} + \mathcal{P}_{0\to1} = I_L \cdot V_{DD}$$
$$= \alpha \cdot C_L \cdot f \cdot V_{DD}^2$$

- Exploitable power consumption over measurement shunt in the **ground** line:

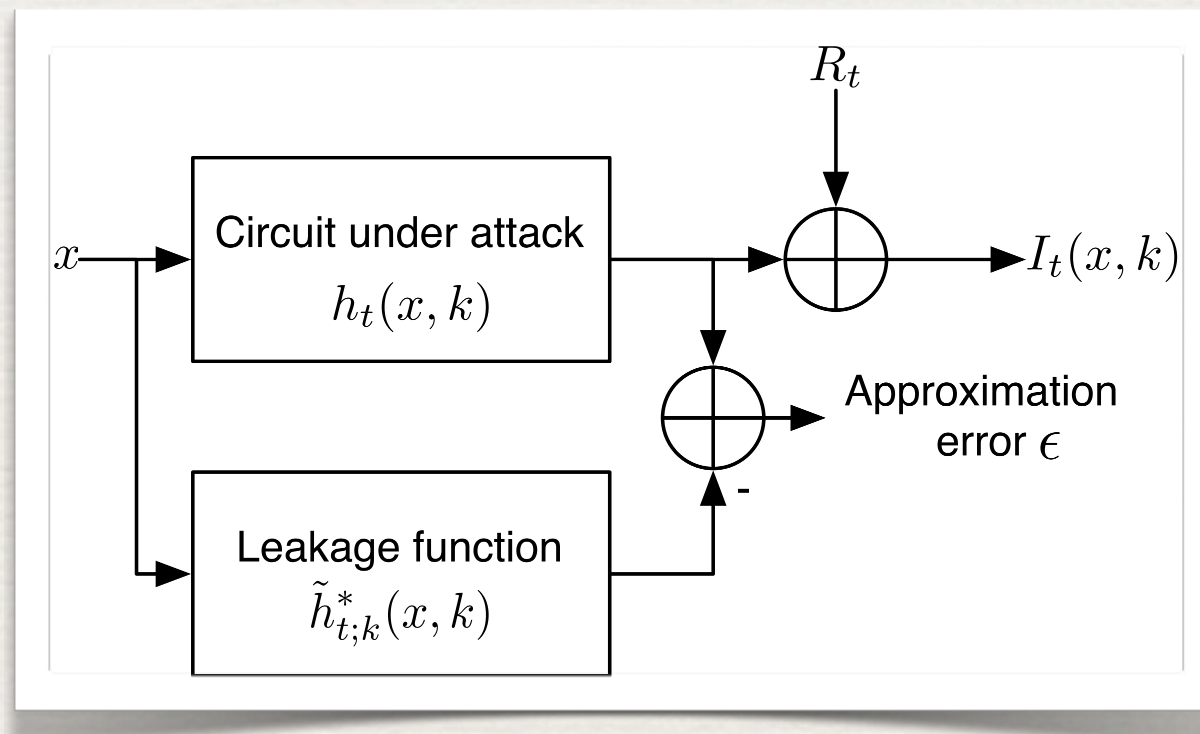
$$\mathcal{P}_{\mathcal{L}} = \begin{cases} \mathcal{P}_{\text{sc}} \approx \frac{V_{\mathcal{L}}^2}{\text{R}_{\text{shunt}}} = I_{\text{sc}}^2 \cdot \text{R}_{\text{shunt}} & 1 \to 0 \\ \mathcal{P}_{0\to1} + \mathcal{P}_{\text{sc}} \approx (I_{\text{sc}} + I_{\text{L}})^2 \cdot \text{R}_{\text{shunt}} & 0 \to 1 \end{cases}$$

Constructive Side-Channel Analysis

Phase one of the stochastic approach

- Basic model for the **current** consumption:

  $I_t(x,k) = h_t(x,k) + R_t$



- Exploitable current consumption is **approximated** by a weighted sum:

  $$\tilde{h}^*_{t;k}(\cdot,k) = \sum_{j=0}^{u-1} \tilde{\beta}^*_{j,f;k}(\cdot,k)\, g_{j,t;k}(\cdot)$$

- *Beta* coefficients are estimated with the **least squares** algorithm:

  $\tilde{\beta}^* = (A^T A)^{-1} A^T \vec{i}_t$

Constructive Side-Channel Analysis

Phase one of the stochastic approach cond.

- Basis functions $g_{j,t;k}(\cdot)$ span the **subspace** by exploiting the **switching activity** of the circuit and thus leading to the experimental matrix A:

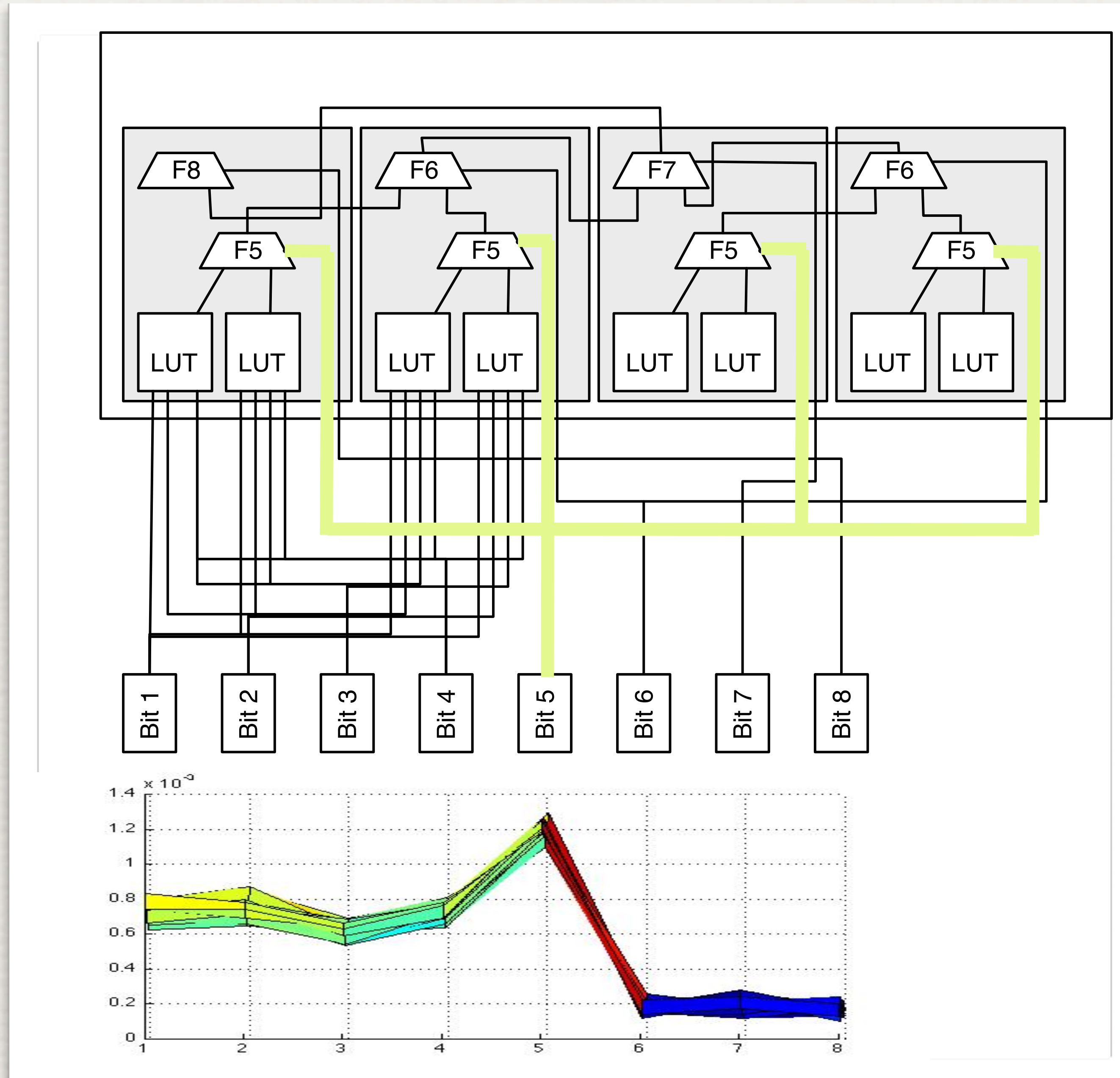
$$A := \begin{pmatrix} g_{0,t;k}(x_1, k) & \dots & g_{u-1,t;k}(x_1, k) \\ \vdots & \ddots & \vdots \\ g_{0,t;k}(x_{N_1}, k) & \dots & g_{u-1,t;k}(x_{N_1}, k) \end{pmatrix}$$

- *Beta* coefficients provides **quantitative** information about consumption of every bit line

Constructive Side-Channel Analysis

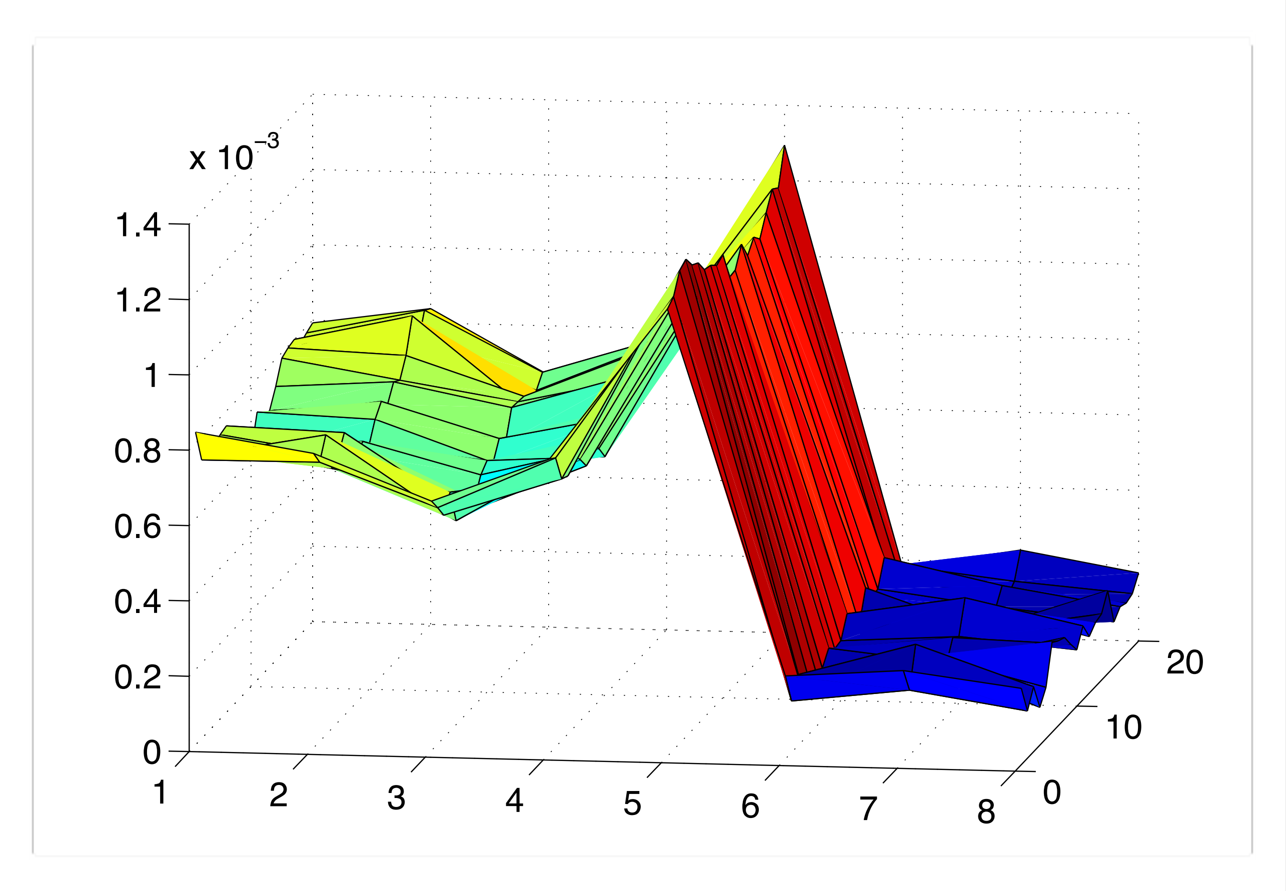
Benefits of *Beta* coefficients

- **Lookup**-table based FPGA implementation
- Strong **glitch** propagation based on the 5th bit
- Bit-specific information **leakage** feedback

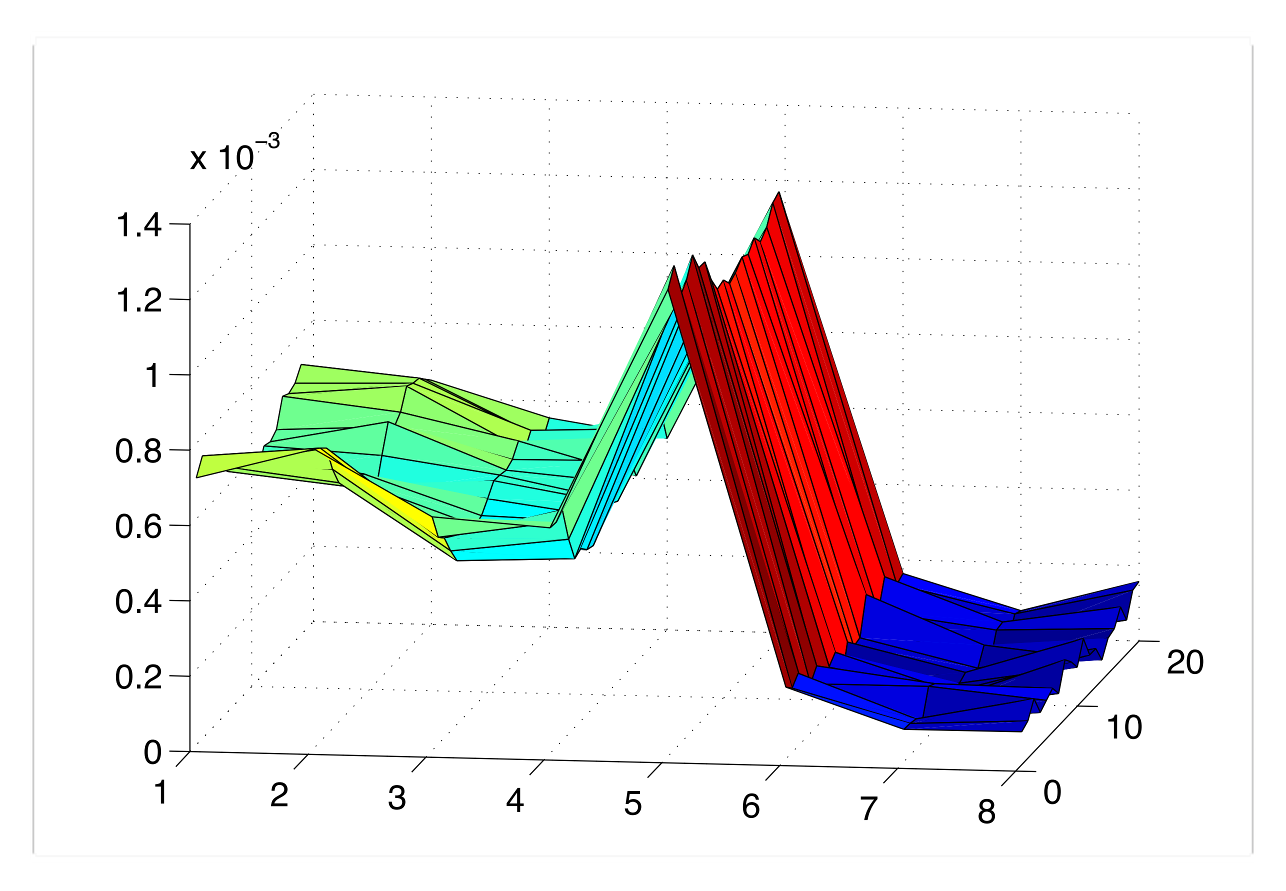


Constructive Side-Channel Analysis

Simple bit line oriented model



Beta characteristic for key value 19

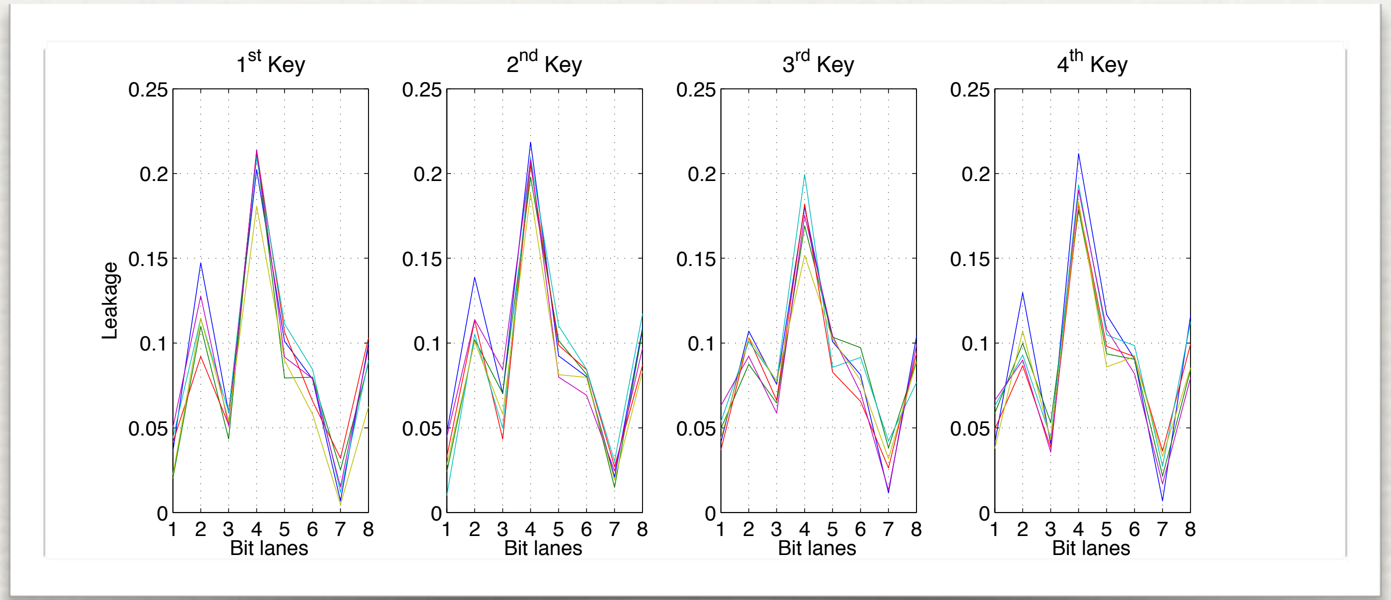


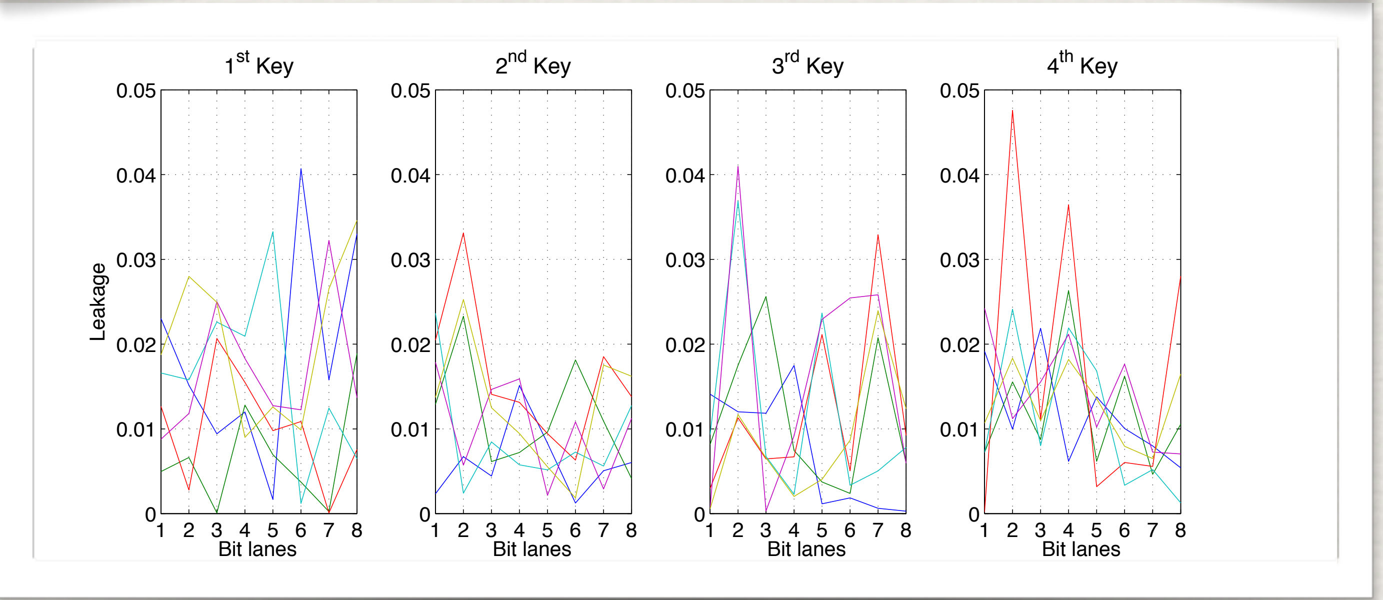
Beta characteristic for key value 220

Constructive Side-Channel Analysis

Symmetry effects

- Implementation issues are **deterministic** and **independent** of the subkey value
- The **image** contains the same elements apart from the secret key value
- Inappropriate models may lead to subkey **value-dependent** *Beta* coefficients





Constructive Side-Channel Analysis

Model check

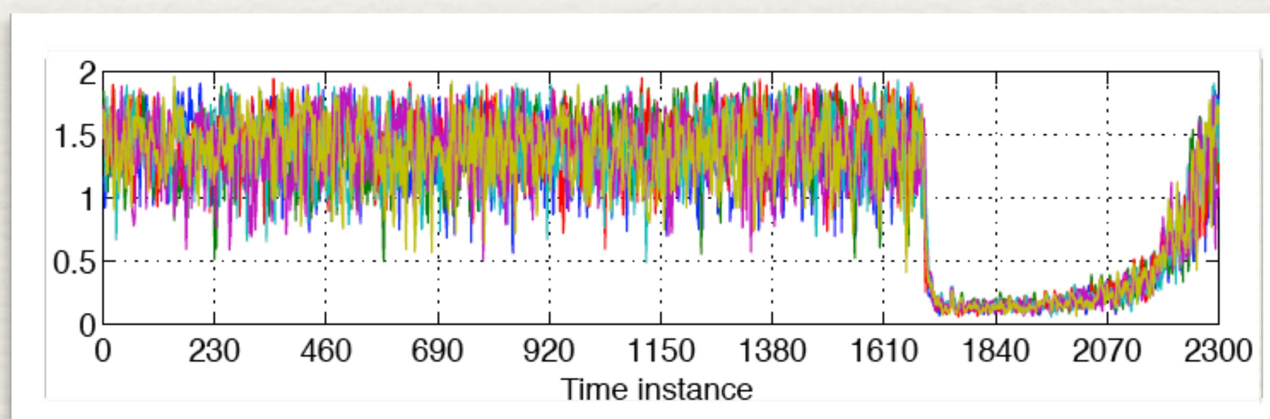
- Differences between the *Beta* coefficients of different subkey values are **directly** comparable:

$$\frac{2\sqrt{Var(\tilde{h}^*_{t;k'}) - Var(\tilde{h}^*_{t;k''})}}{\sqrt{Var(\tilde{h}^*_{t;k'})} + \sqrt{Var(\tilde{h}^*_{t;k''})}} \to$$

$$\frac{2\sqrt{\sum_{j=1}^{8}(\tilde{\beta}^*_{j,t;k'} - \tilde{\beta}^*_{j,t;k''})^2}}{\sqrt{\sum_{j=1}^{8}(\tilde{\beta}^*_{j,t;k'})^2} + \sqrt{\sum_{j=1}^{8}(\tilde{\beta}^*_{j,t;k'})^2}}$$

- A very **small** value and a **tight** grouping of different subkey values indicate symmetry properties

- In case of **high** symmetry not every subkey value has to be profiled in the trainings phase



Constructive Side-Channel Analysis

Signal-to-noise ratio

- Characterize the **quality** of the extractable information from the signal

$$SNR = \frac{Var(signal)}{Var(noise)}$$

- In case of an **orthonormal** subspace the *Beta* coefficients can directly be used for the SNR

$$SNR = \frac{Var_X(h_t(X,k))}{Var_X(I_t(X,k) - h_t(X,k))}$$

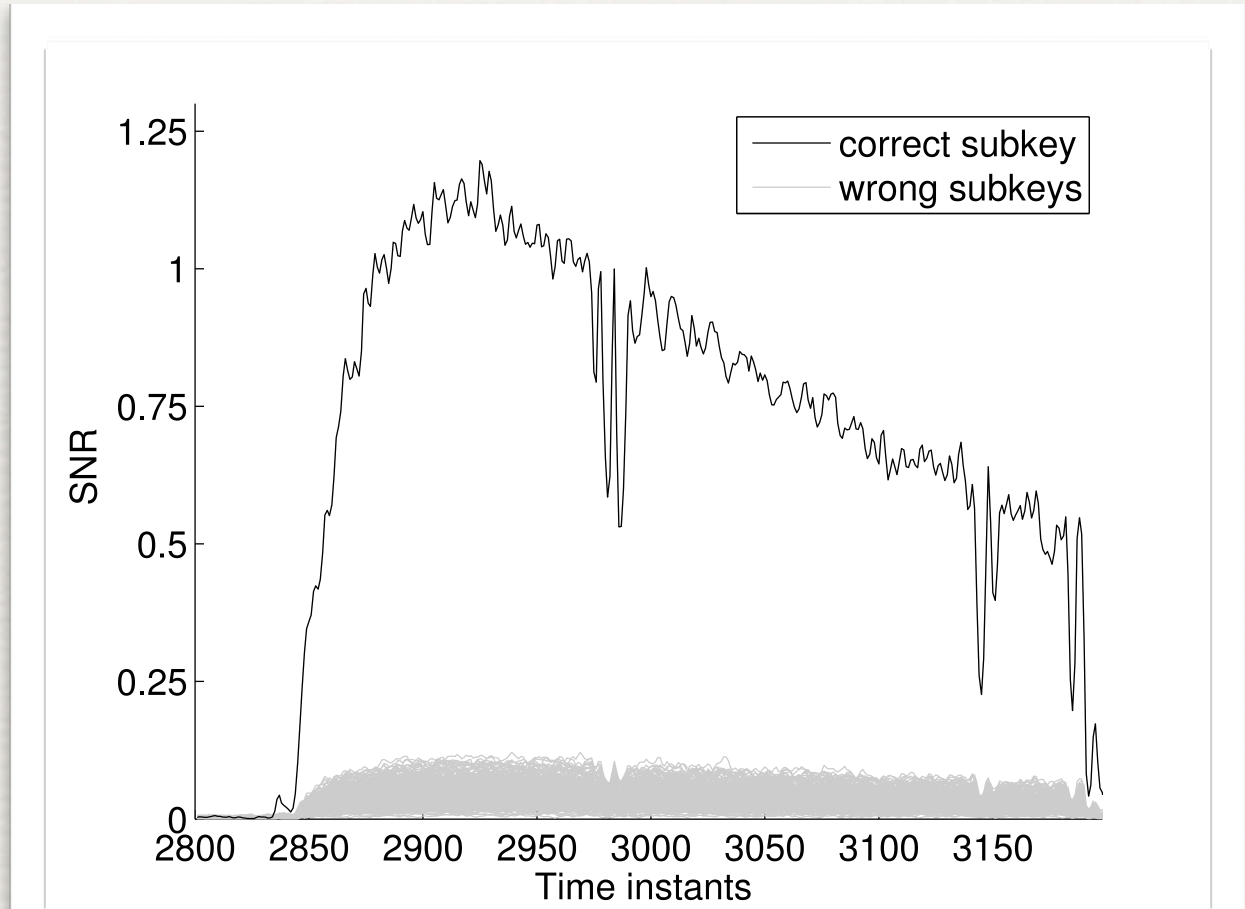
- SNR **depends** also on the quality or noise level of the measurement

$$\widetilde{SNR} = \frac{\sum_{j=1}^{u-1}(\tilde{\beta}^*_{j,t;k})^2}{Var_X(i_t(\vec{x},k) - \tilde{h}^*_t(\vec{x},k))}$$

Constructive Side-Channel Analysis

Signal-to-noise ratio cond.

- The **higher** the SNR value is the better the information is **distinguishable** from the noise
- Proposed SNR metric can be used to **evaluate** the side-channel leakage of **different** designs
- Together with the first phase of the stochastic approach the SNR metric is a non-profiling **attacking** tool



TECHNISCHE UNIVERSITÄT DARMSTADT

Summary

A useful tool for secure circuit design

- Linear regression based model design is a very powerful **tool** to approximate the physical behavior of the circuit

- Model **checking** is supported without conducting an attack during the design phase of the circuit

- Different **designs** and different measurement settings can be compared by the SNR metric

- Constructive side-channel analysis provides a more **quantitative** insight of the implementation vulnerabilities

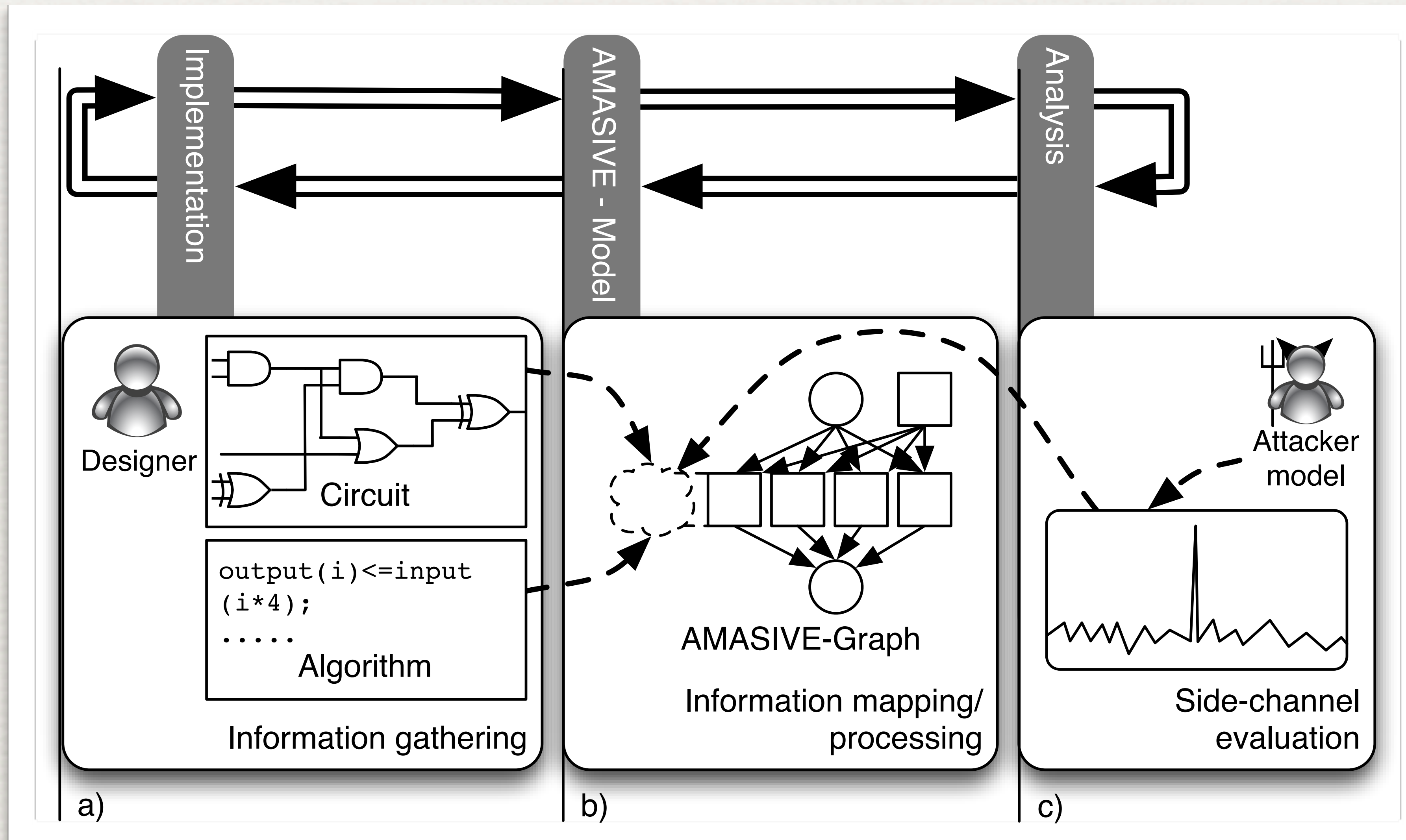
Outlook

Automated constructive side-channel analysis?

a) Gather information

b) Define and build internal models

c) Perform vulnerability analysis



Thank You!

source:http://www.geek.com/articles/mobile/the-mobile-patent-fight-visualized-20110829/

Questions?

Appendix

Variance of $\tilde{h}^*_{t;k}(\cdot, k)$ for orthonormal basis

$$Var_X(\tilde{h}^*_{t;k}(X,k)) = E_X(\tilde{h}^*_{t;k}(X,k)^2) - E_X^2(\tilde{h}^*_{t;k}(X,k))$$

$$= \sum_{j=0}^{u-1} (\tilde{\beta}^*_{j,t;k})^2 - (\tilde{\beta}^*_{0,t;k})^2$$

$$= \sum_{j=1}^{u-1} (\tilde{\beta}^*_{j,t;k})^2$$