Side Channel Analysis of Smart Cards

SRC Security Research & Consulting GmbH

Bonn - Wiesbaden

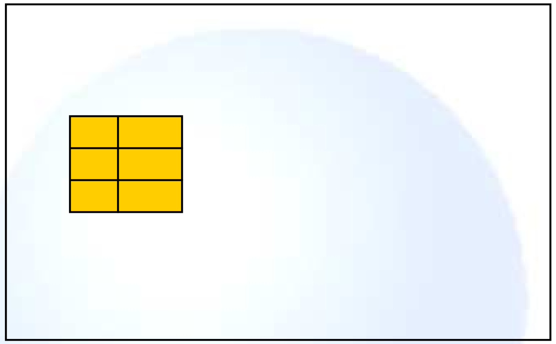
Agenda

- Evaluation of smart cards
- Measurement Setup
- General analysis characteristics
- Examples for a successful side channel analysis

© SRC Security Research & Consulting GmbH

Smart Cards: Applications

- Smart cards are not only used to store data.
- They can perform cryptographic operations.
  - Symmetric algorithms like Triple DES and AES and
  - asymmetric algorithms like RSA and ECC.
- The secret keys cannot be read out.



Smart Cards: Security

Smart cards can leak information through side channels like

- timing of an operation,
- power consumption while performing an operation,
- electromagnetic emanation.

For security applications, smart cards have to be resistant against such attacks.

© SRC Security Research & Consulting GmbH

Smart Cards: Requirements

Security requirements for smart cards including side channel resistance are e.g.

- ZKA Sicherheitskriterien,

  which provide the security criteria for the electronic banking systems in Germany,

- Common criteria for IT security evaluation (ISO 15408),

  mandatory by European law for

  - digital signature cards,
  - digital tachograph cards,
  - …

Equipment (1)

- Digital oscilloscope
  - 1 GHz band width
  - Up to 16 GS/s sample rate
- Probes
  - Standard probe 500 MHz
  - Active probe 1,5 GHz
- EM near field probes and self produced coils
- Analysis workstation
- Card reader (modified for analysis)
- Laboratory power supply unit

Equipment (2)

© SRC Security Research & Consulting GmbH

Evaluation of a smart card

- Execution of card commands
- Measurement of power consumption
- Preparing the traces
  - Finding the right time interval by cross correlation
  - Compression of measured data (identify cycles and their characteristics)
- Analysis of the traces
  - Arithmetic Mean, standard deviation
  - Correlation with hamming weight of intermediate values
- Evaluation of the results

Simple power analysis (SPA)

- Measuring power consumption of card during computation with secret data.
- Identifying the single computation steps of the algorithm.
- Identifying the time interval where the secret data are processed.
- Analysing the effect of the secret data on the power consumption.

SPA: Limitations

- Requires expertise in analysing traces
- Requires knowledge of the single computation steps of the implementation

But:

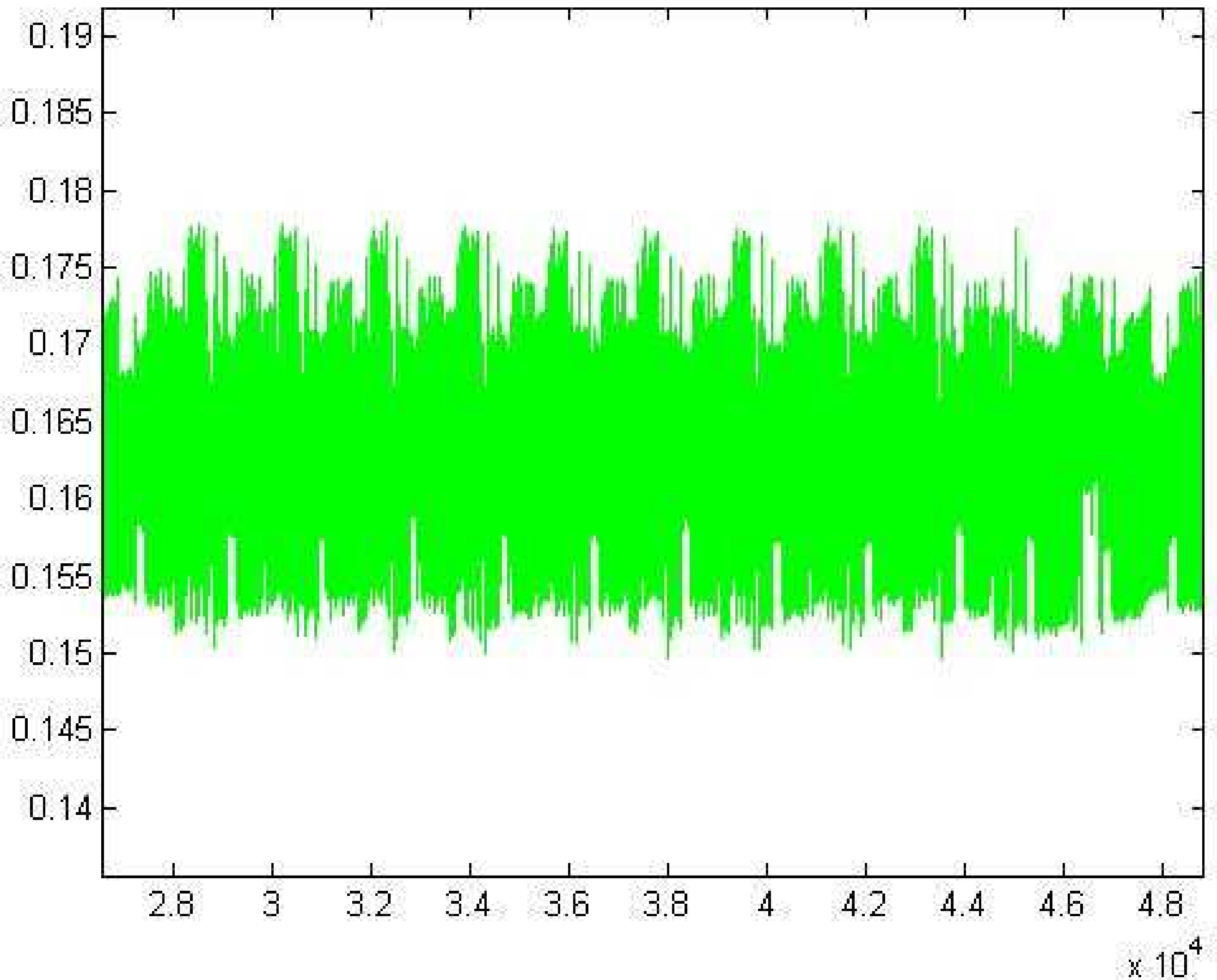
- Efficient, if possible
  (only a single trace required in the optimal case)
- First step for further analysis

Example: Rijndael

```
AddRoundKey(state, key)
for round = 1 step 1 to 9
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, keySchedule[round])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, keySchedule[10])
```

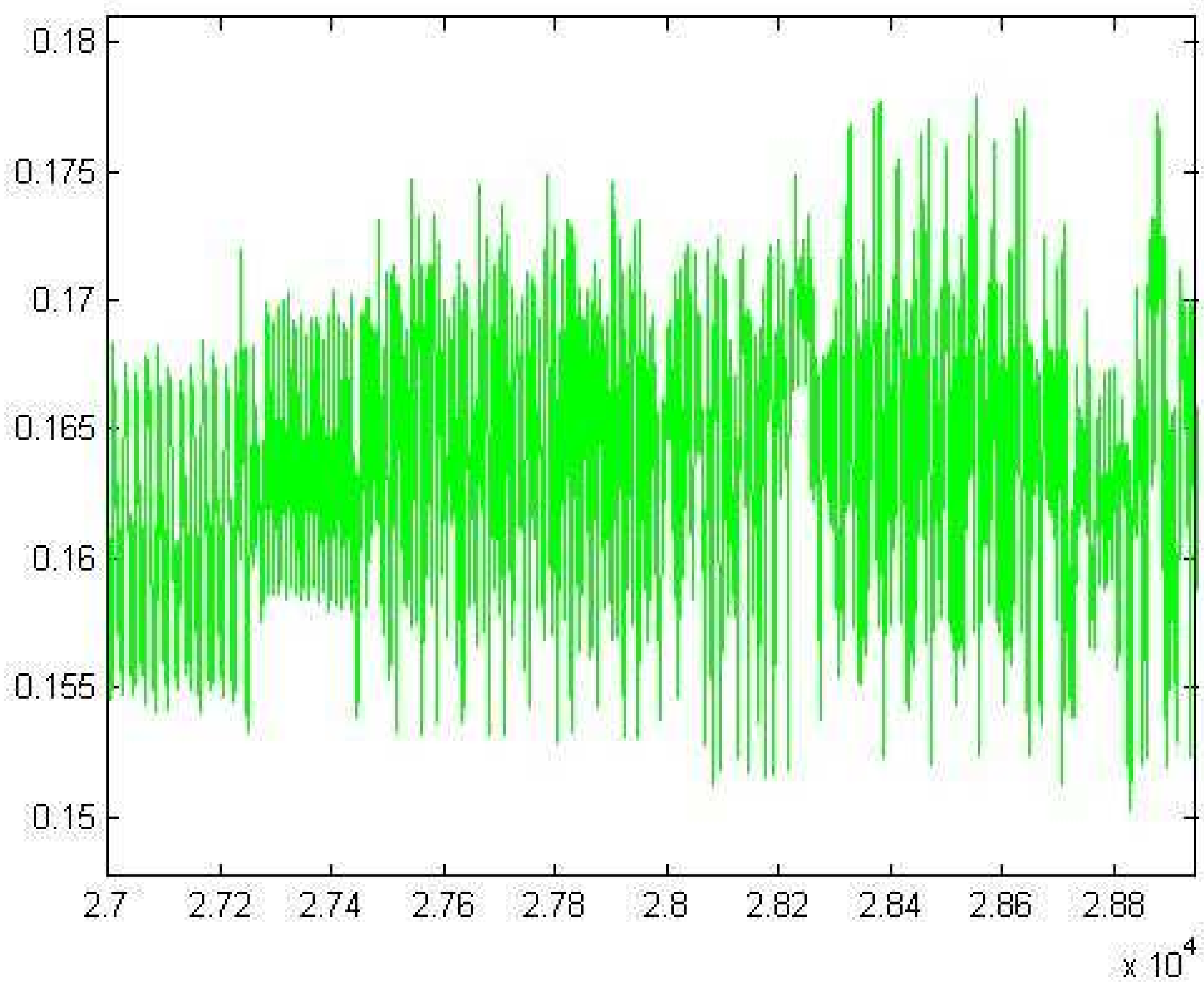

© SRC Security Research & Consulting GmbH

Example: Trace



© SRC Security Research & Consulting GmbH

Example: First Round



Differential power analysis

Statistical methods are applied

- The input data for the observed algorithm have to vary in a sufficient randomly manner
- Intermediate results of the computation are analysed, which depend only on a part of the secret data
- Different hypothesis for these secret data are tested as follows:

DPA: Testing of hypothesis

- a discriminant bit is chosen
- the value of this bit is computed, depending of a chosen key hypothesis
- the traces are divided in those with high and low power consumption and the two means are subtracted
- a peak indicates that the hypothesis is right

DPA: Limitations

- Many traces are needed

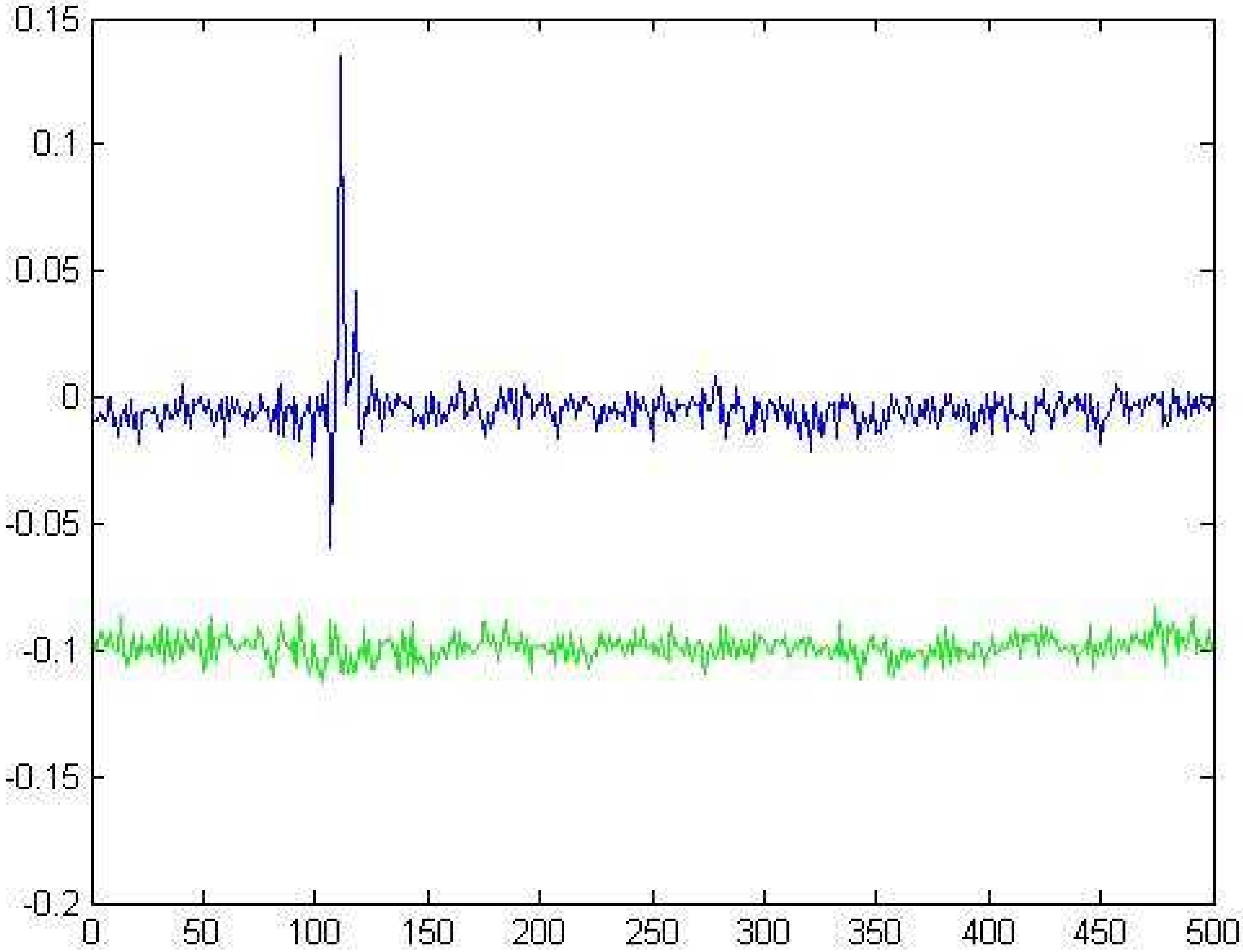
  some 100s at least, better up to some 10000s

- The input data have to vary

But:

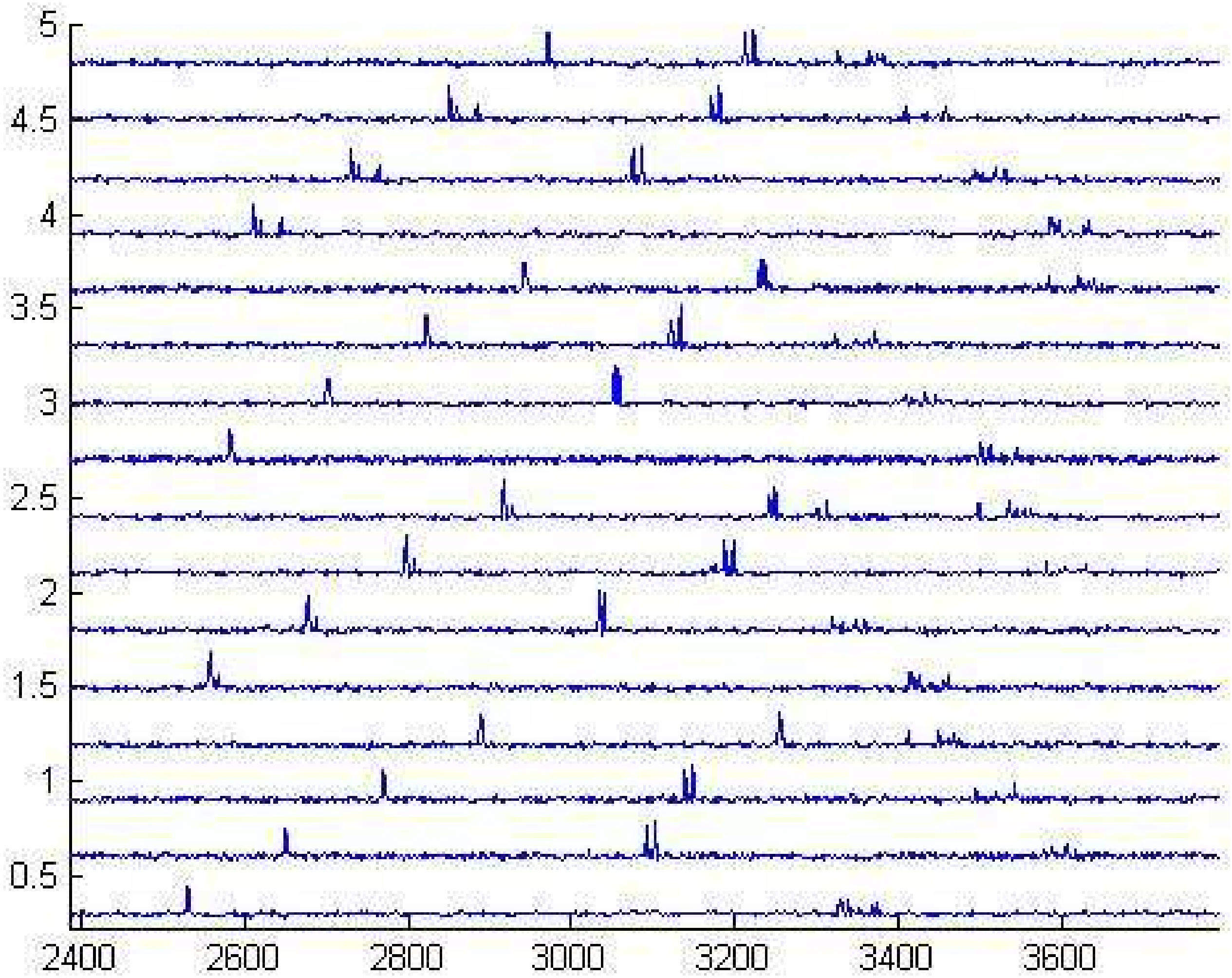
- Only a basic knowledge about the implementation is required
- If successful, also some information about the implementation is achieved

Example: Peak



© SRC Security Research & Consulting GmbH

Example: Implementation



Electromagnetic Analysis

Instead of the power consumption, the electromagnetic emanations of the card are measured.

The analysis of the measured data is similar to the analysis of power consumption traces.

EMA: Limitations

- The probe have to be positioned near the chip
- Expertise in positioning the probe is required

But:

- Counter measures which smooth the power consumption may not smooth the electromagnetic emanation
- The electromagnetic emanations also deliver some information which part of the chip is active

© SRC Security Research & Consulting GmbH

Contact

SRC
Security Research & Consulting GmbH
Graurheindorfer Str. 149a
53117 Bonn

Tel.	+49-(0)228-2806-0
Fax:	+49-(0)228-2806-199
E-mail:	info@src-gmbh.de
WWW:	www.src-gmbh.de