Side Channel Analysis of Smart Cards

SRC Security Research & Consulting GmbH

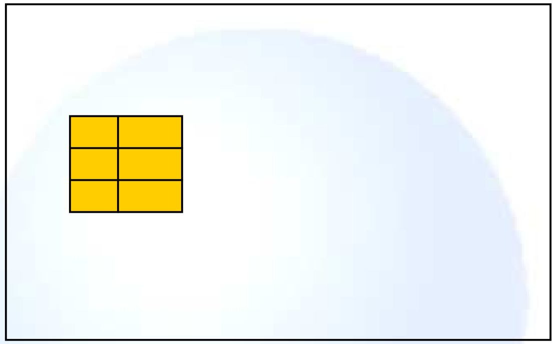
Bonn - Wiesbaden

Agenda

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

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.



© SRC Security Research & Consulting GmbH

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)

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:

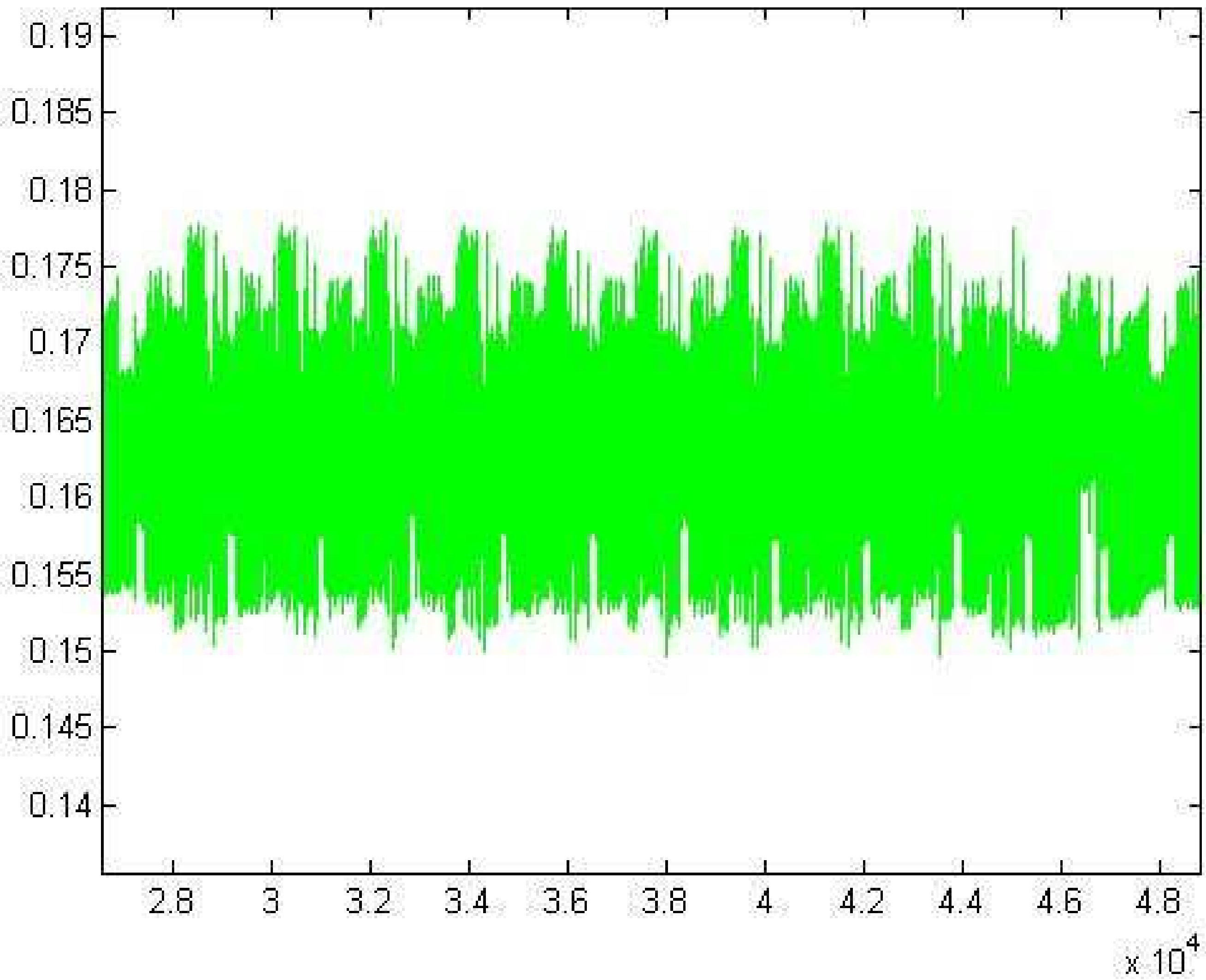
- Efficient, if possible
  (only a single trace required in the optimal case)
- First step for further analysis

Example: Rijndael

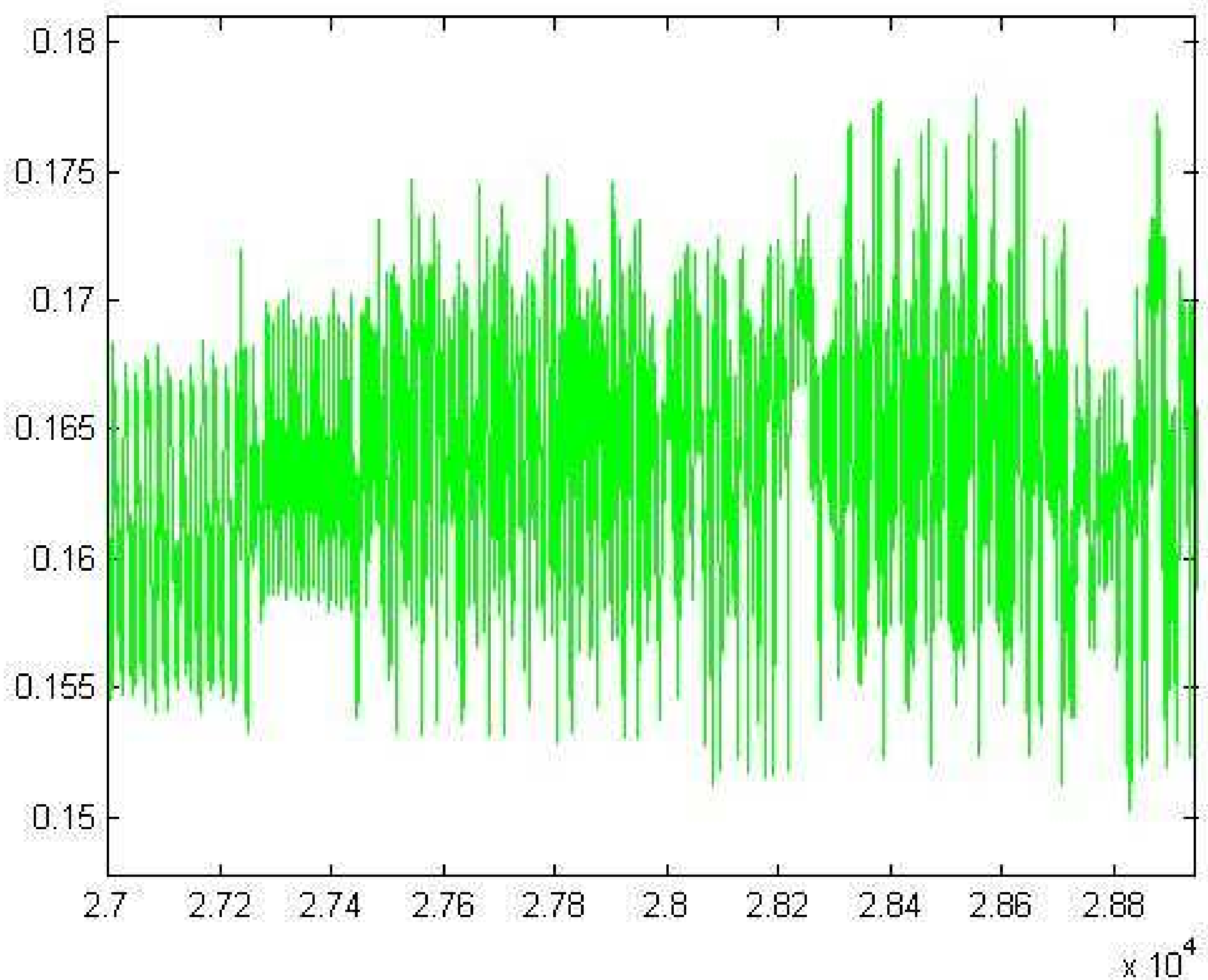
```
AddRoundKey(state, key)
for round = 1 step 1 to 9
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, keySchedule[round])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, keySchedule[10])
```


© SRC Security Research & Consulting GmbH

Example: Trace



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:

© SRC Security Research & Consulting GmbH

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

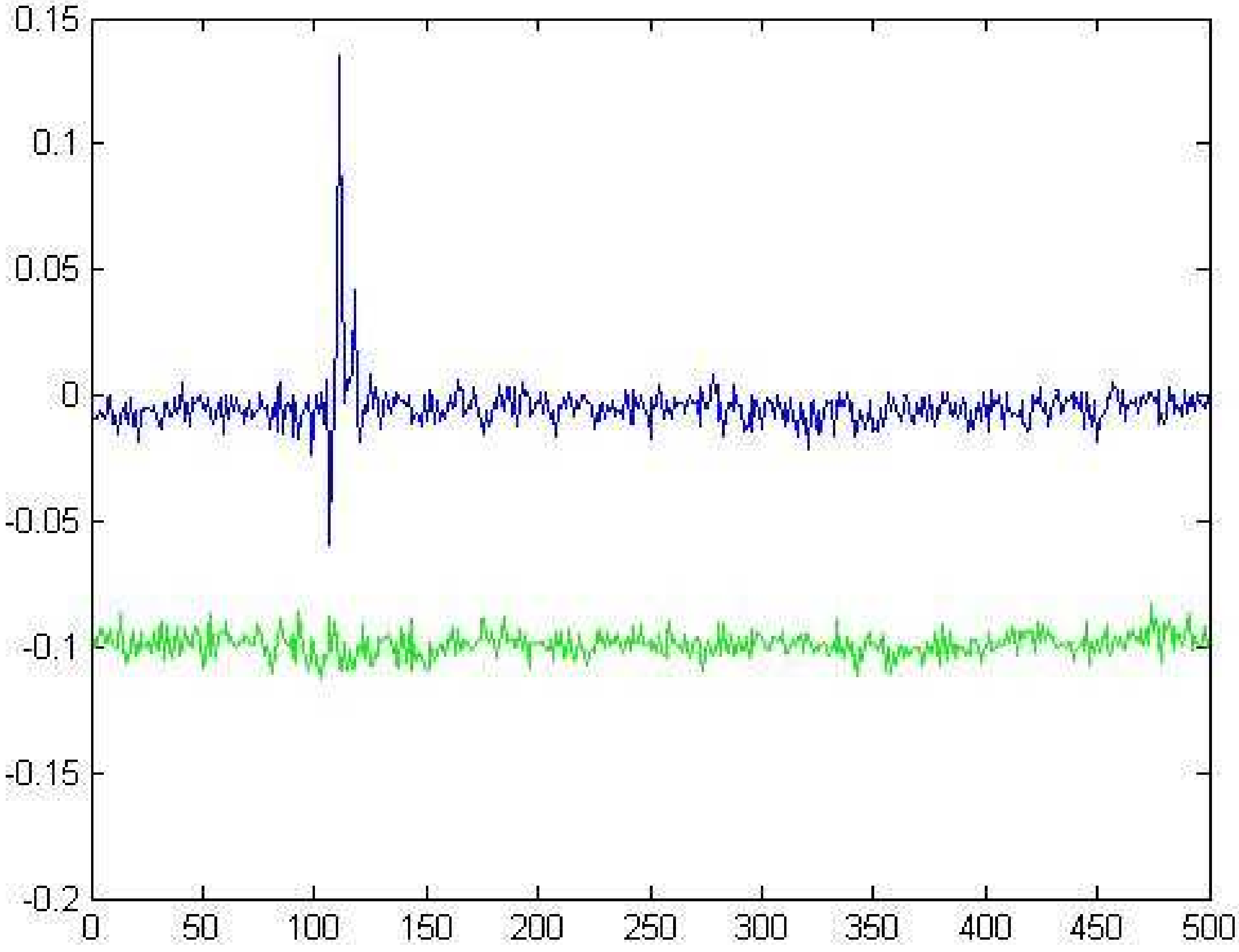
- Many traces are needed

  some 100s at least, better up to some 10000s
- The input data have to vary

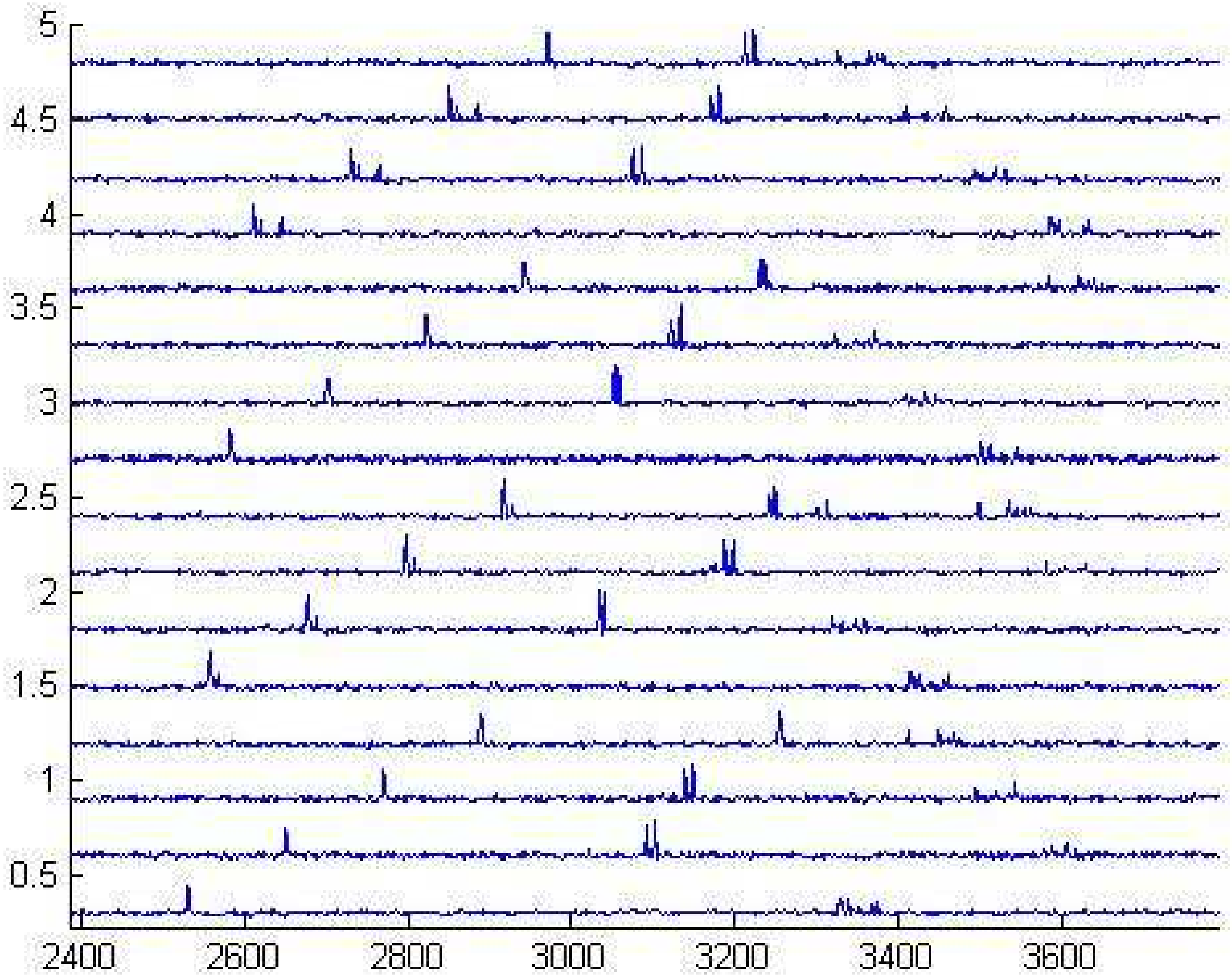
But:

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

Example: Peak



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.

© SRC Security Research & Consulting GmbH

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

© SRC Security Research & Consulting GmbH

Sidechannel-Analysis of RSA-Implementations in Smartcards

Matthias Heuft

21C3

Berlin, 27.12.2004

Overview

- RSA-Algorithm
- Sidechannel-Analysis
- Data-Analysis

RSA-Algorithm

The RSA-Algorithm

Steps in RSA-Algorithm

$\mathcal{A}$: Sender

$\mathcal{B}$: Receiver

- Key generation by $\mathcal{B}$, consisting of modulus n, public key component e and private (secret) key component d.
  $\langle e,\ n\rangle$ public, $\langle d,\ n\rangle$ private.

- Encryption of a message M by $\mathcal{A}$ via calculation of

$$C = M^e \mod n.$$

- Decrytion of C by $\mathcal{B}$ via calculation of

$$M = C^d \mod n.$$

Modular Exponentiation

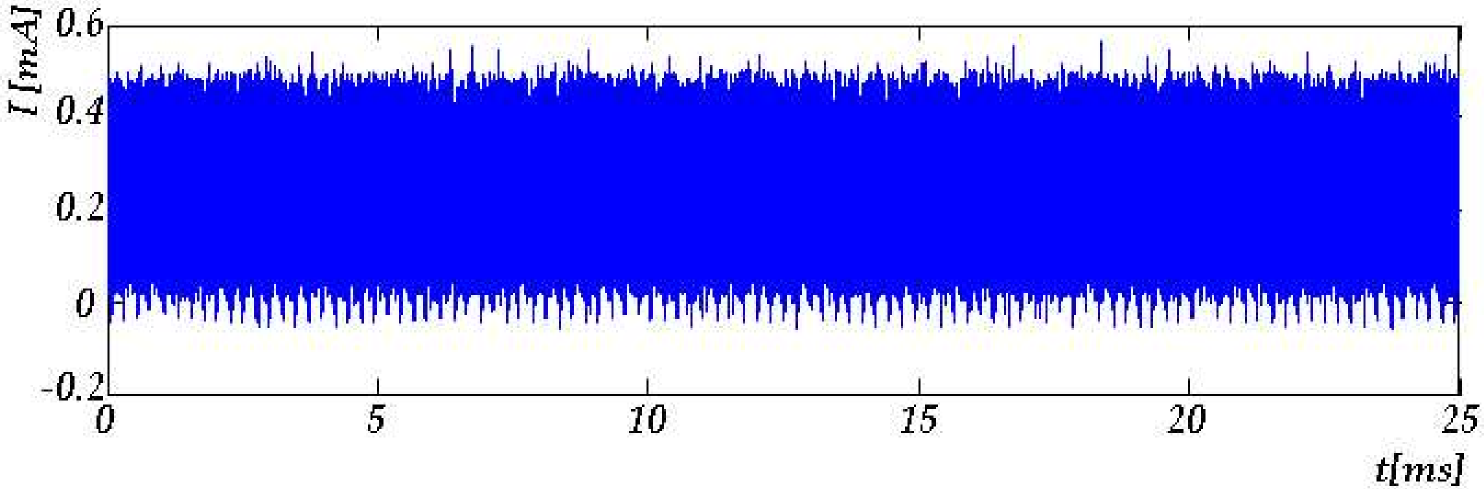
Square & Multiply algorithm for exponentiation of $p = a^e \bmod n$

1. Set $p \leftarrow a^{e_{n-1}}$ and $i = n - 2$.
2. Set $p \leftarrow p^2 \mod m$.
3. If $e_i = 1$, set $p \leftarrow p \cdot a \mod m$.
4. Set $i \leftarrow i - 1$; if $i \geq 0$, go to step 2.
5. Output p.

Sidechannel-Anaylsis

Power consumption of a smarcard

Profil of a trace.



Analysing the power consumption

DEFINITIONS

- The power consumption of a smartcard in a time interval is called *trace*.
  $X^i = (x^i_1, \ldots, x^i_l)$
- Addition and Subtraction are defined: For $X^1 = (x^1_1, \ldots, x^1_l)$ and $X^2 = (x^2_1, \ldots, x^2_l)$ is
  $$X^1 + X^2 = (x^1_1 + x^2_1, \ldots, x^1_l + x^2_l).$$
- X^i is the i-th Trace in a set $\mathfrak{X} = \{X^1, \ldots, X^m\}$ of traces. The *meantrace* $\overline{X}$ of $\mathfrak{X}$ ist given by
  $$\overline{X} := (\overline{X}_1, \ldots, \overline{X}_l) := \left(\frac{1}{m} \sum_{i=1}^{m} x^i_1, \ldots, \frac{1}{m} \sum_{i=1}^{m} x^i_l \right).$$

SEMD-Attack

SEMD: Single Exponent Multiple Data

Examine two traces:

- X^1 Trace of an encryption operation with public (known) exponent
- X^2 Trace of an encryption operation with private (unknown) exponent

Differencetrace: $D = (d_1, \cdots, d_l) = X^1 - X^2$

$$d_j \approx \begin{cases} 0, & \text{if j = data dependent point or exponentiantion operations agree} \\ \text{nonzero}, & \text{if j = point where the exponentiation operations differ} \end{cases}$$

SEMD-Attack

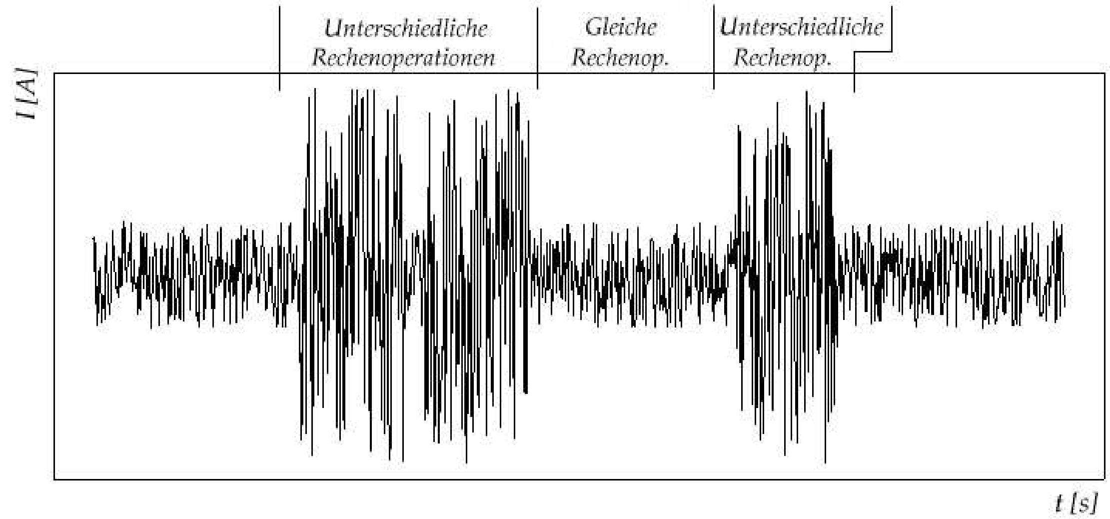


FIGURE 1: DIFFERENCE OF TWO TRACES.

MESD-Attack

MESD: Multiple Exponent Single Data.

Collect trace X^0 by performing RSA-operation with secret exponent.

ASSUMPTION: k Keybits $(e_{n-1} \ldots e_{n-k})$ already known.

Guess $e_{n-k-1} = 0$ and collect trace X^1 by performing RSA-operation with $(e_{n-1} \ldots e_{n-k} e_{n-k-1})$ as public exponent.

Guess $e_{n-k-1} = 1$ and collect trace X^2 by performing RSA-operation with $(e_{n-1} \ldots e_{n-k} e_{n-k-1})$ as public exponent.

Calculate $D^1 = X^0 - X^1$ and $D^2 = X^0 - X^2$.

Decide which guess was correct using DPA-result.

Update e.

MESD-Attack

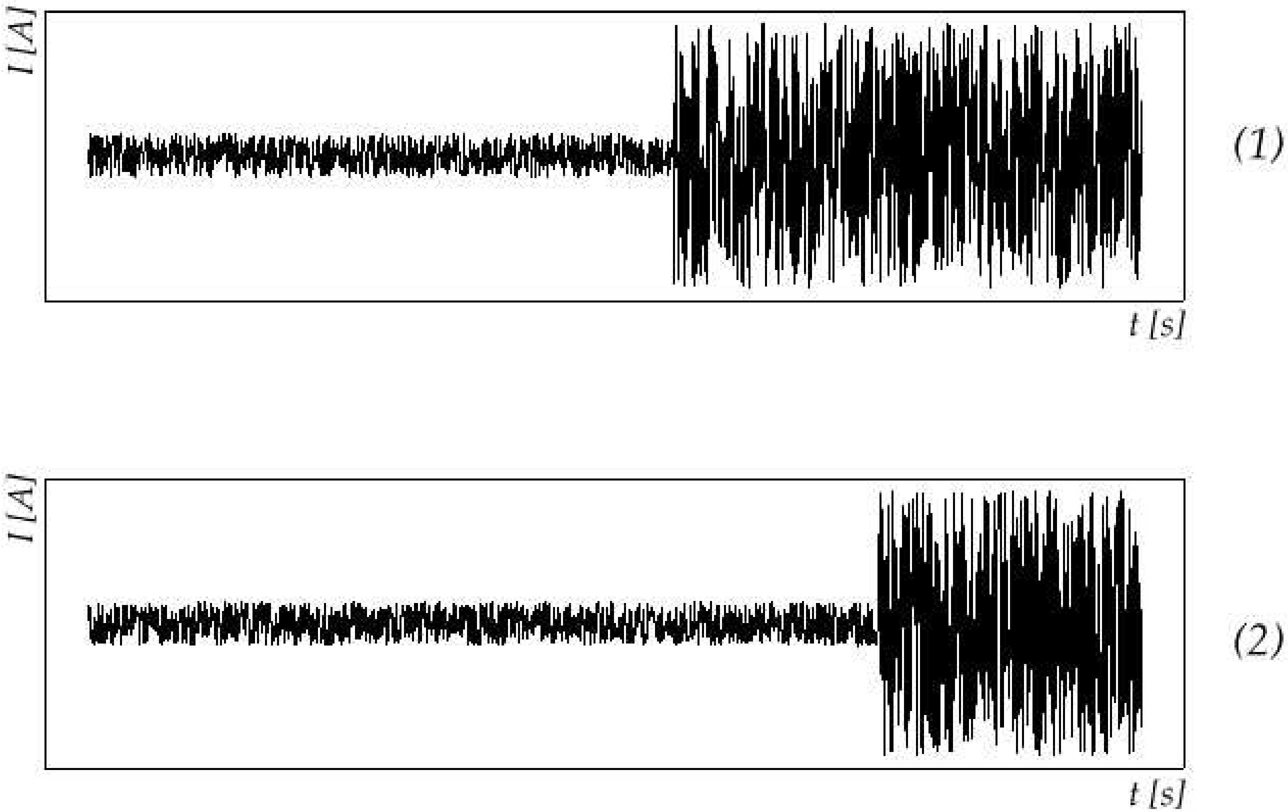


FIGURE 2: (1) DIFFERENCETRACE TO A FALSE GUESS,

(2) DIFFERENCETRACE TO A CORRECT GUESS.

Data-Analysis

Data value logging

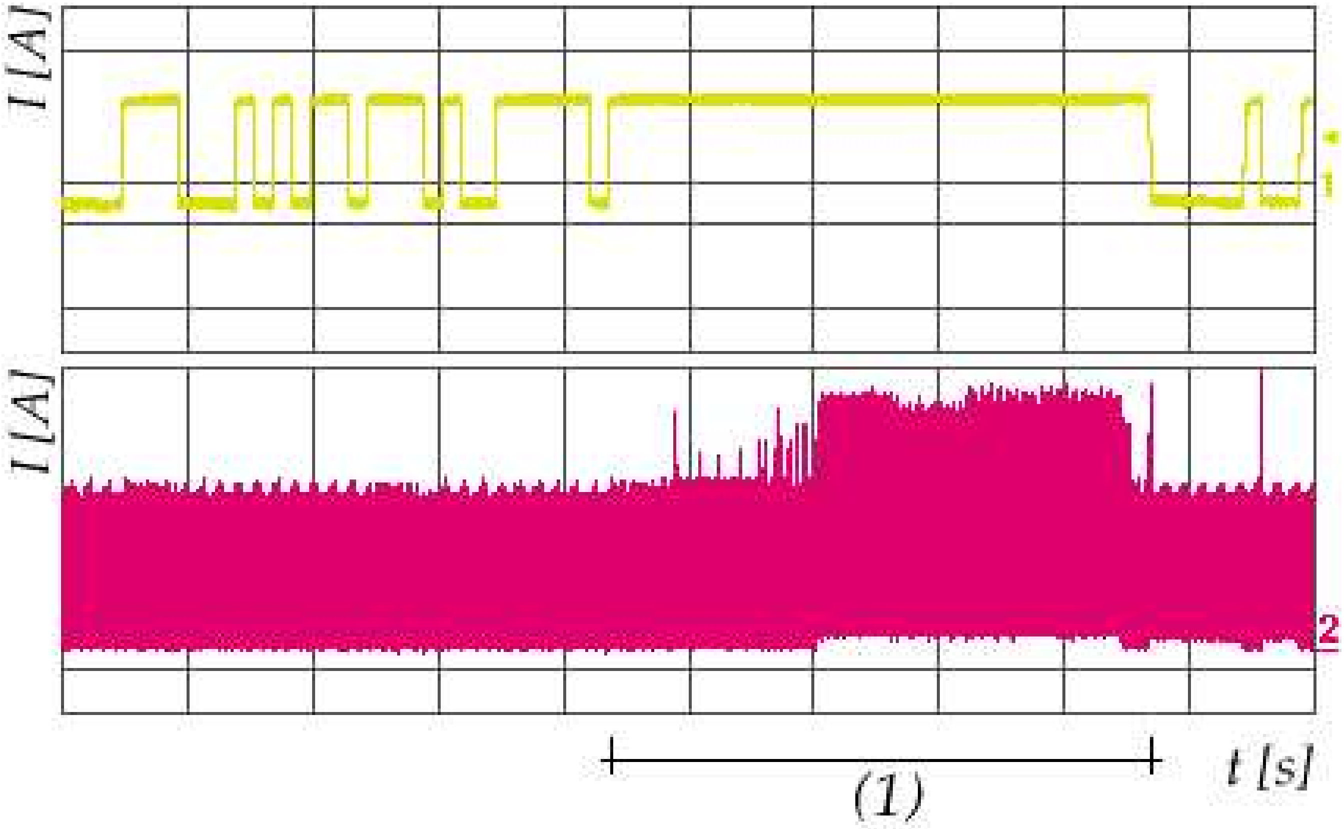


FIGURE 3: CHANNEL (1): TRANSMITION OF SMARDCARD-COMMANDS.

CHANNEL (2): POWER CONSUMPTION.

Data-Analysis - Preprocessing

- Synchronisation
  - Cross correlation
  - Minimal differences
- Compression

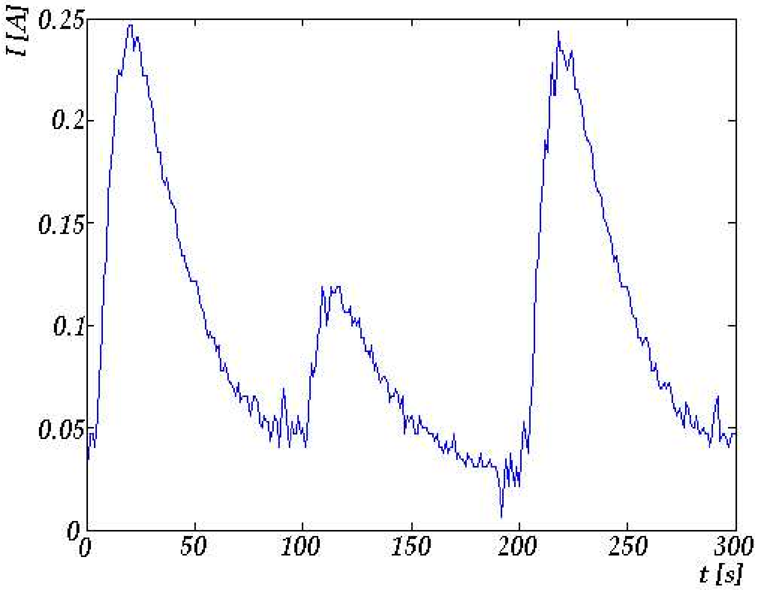


FIGURE 4: THREE CLOCK CYCLES. 100 MEASURE VALUES BUILD ONE CLOCK CYCLE.

Analysis Microcontroller

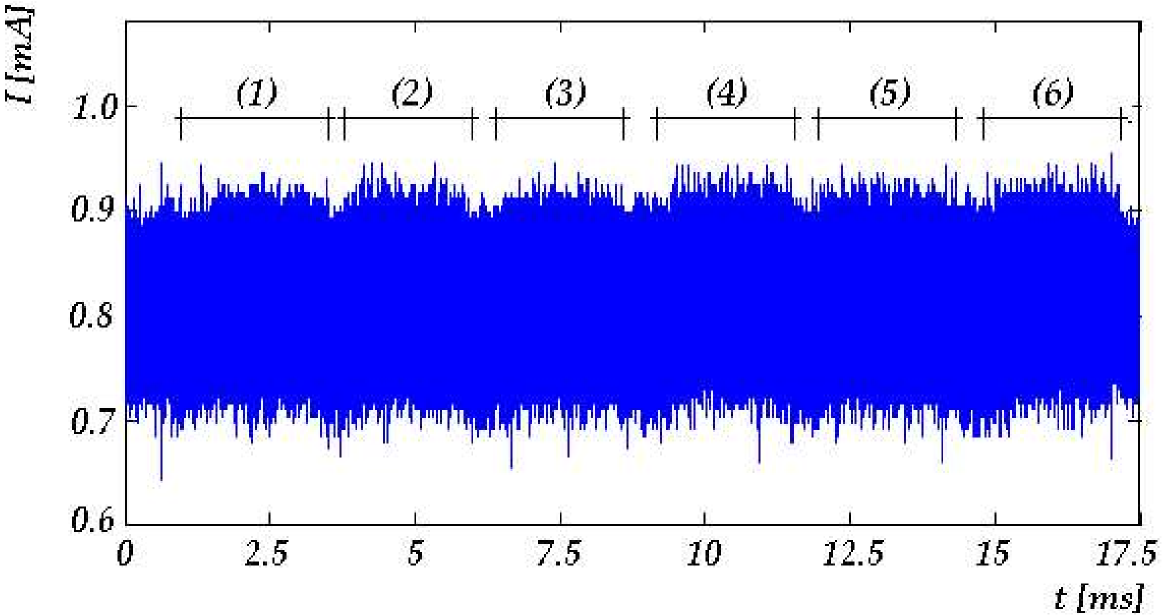


FIGURE 5: 6 INTERVALLS CONTAINING AN ARITHMETICAL OPERATION.

Analysis Microcontroller

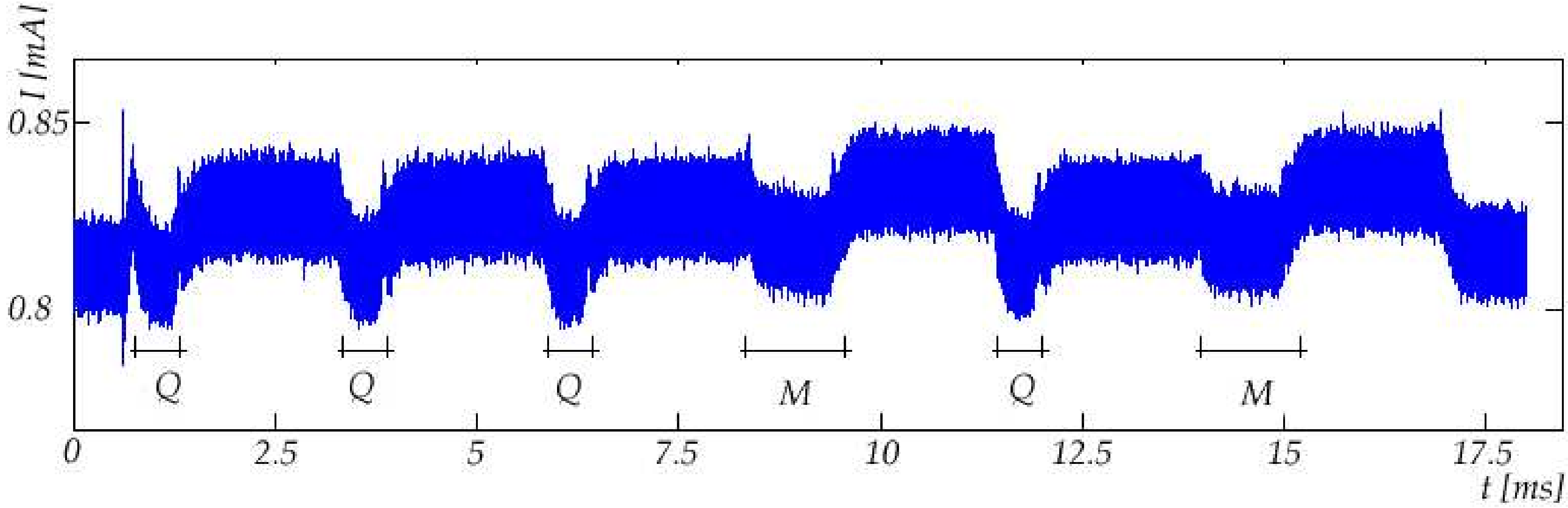


FIGURE 6: MEANTRACE FOR 100 TRACES. Q LABELS AN SECTION FOR A SQUARING DOWN, M LABELS A SECTION FOR A MULTIPLICATION.

EXPONENT: $e = (10011)$

Analysis Microcontroller

PROBLEM DPA: Execution time

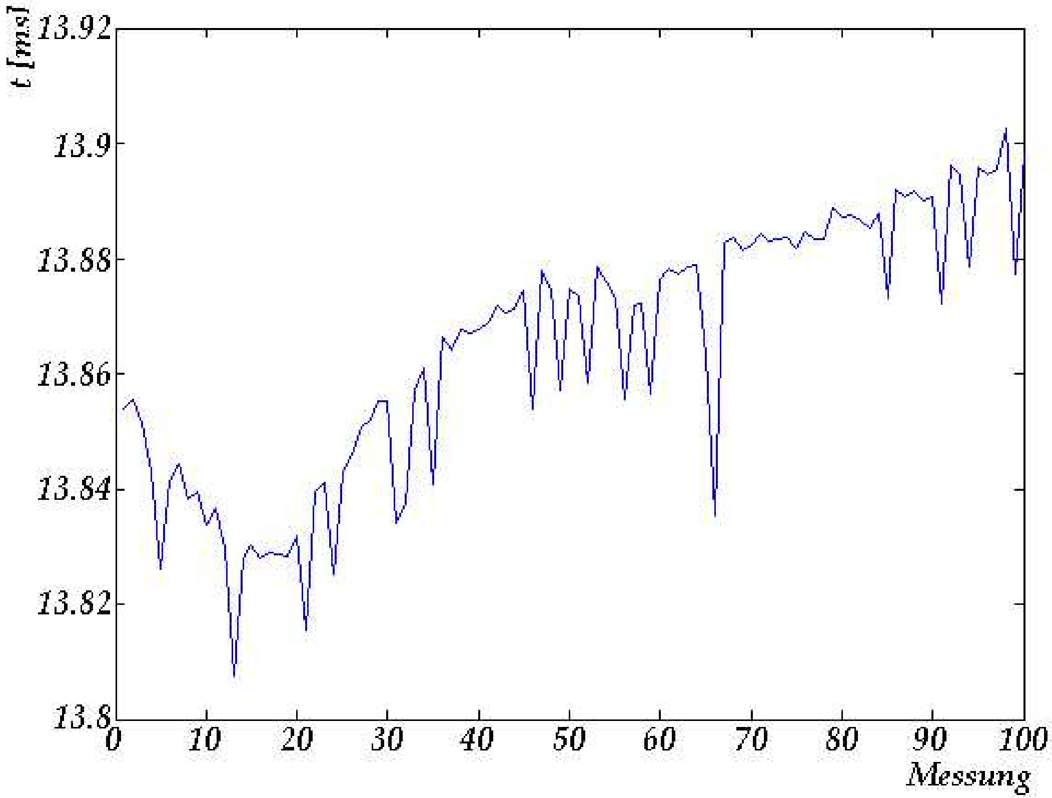


FIGURE 7: COHERENCE BETWEEN EXECUTION TIME FOR AN RSA-OPERATION AND RUNING TIME OF THE MICROCONTROLLER.

Identifying the algorithm and its position

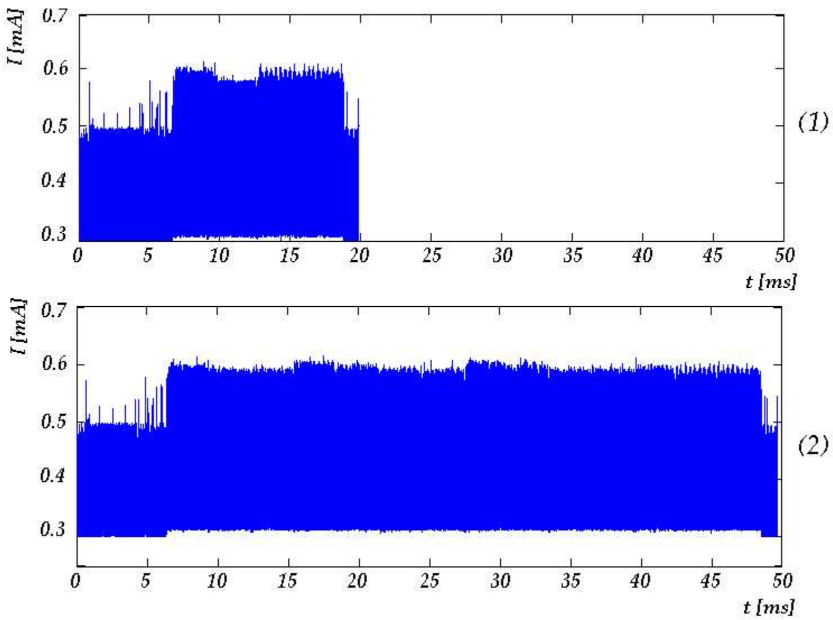


FIGURE 8: (1) ENCRYPTION OF MESSAGE M USING EXPONENT $e = (07)_{16}$.
(2) ENCRYPTION OF MESSAGE M USING EXPONENT $\hat{e} = (\mathsf{FF})_{16}$.

Analysis Smartcard

Algorithm: Square & Multiply

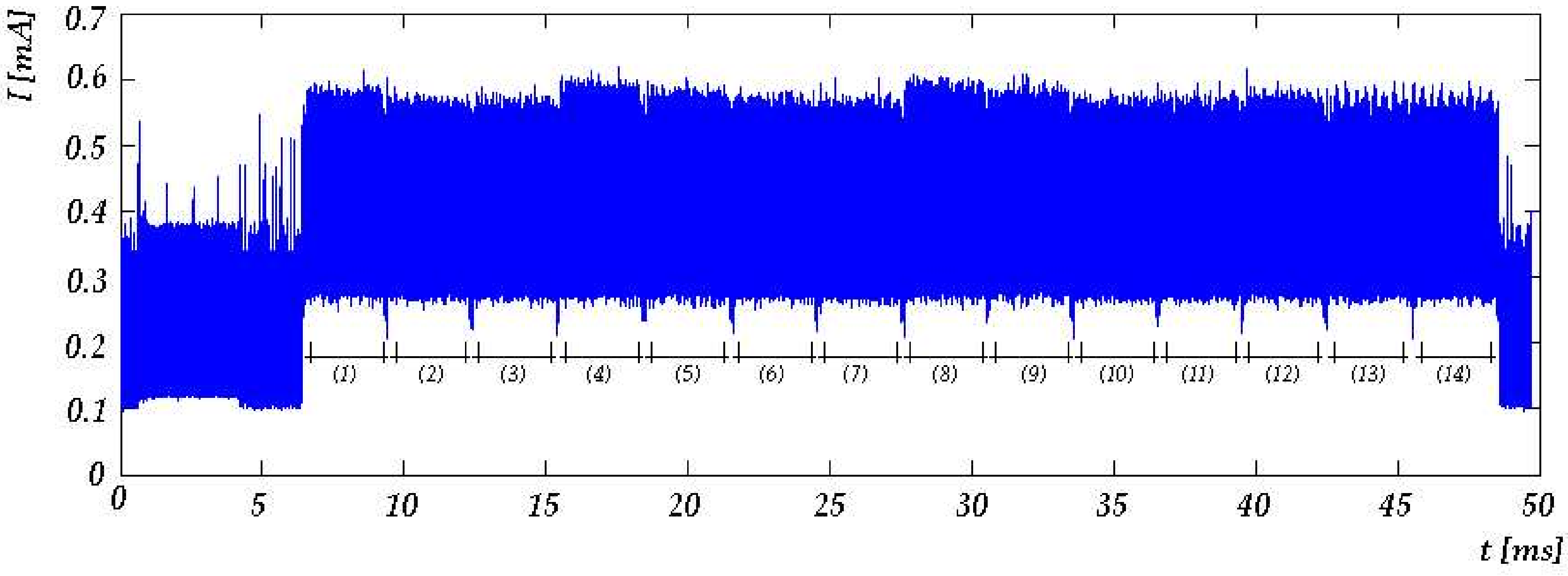


FIGURE 9: COMPRESSED MEANTRACE.

Analysis Smartcard

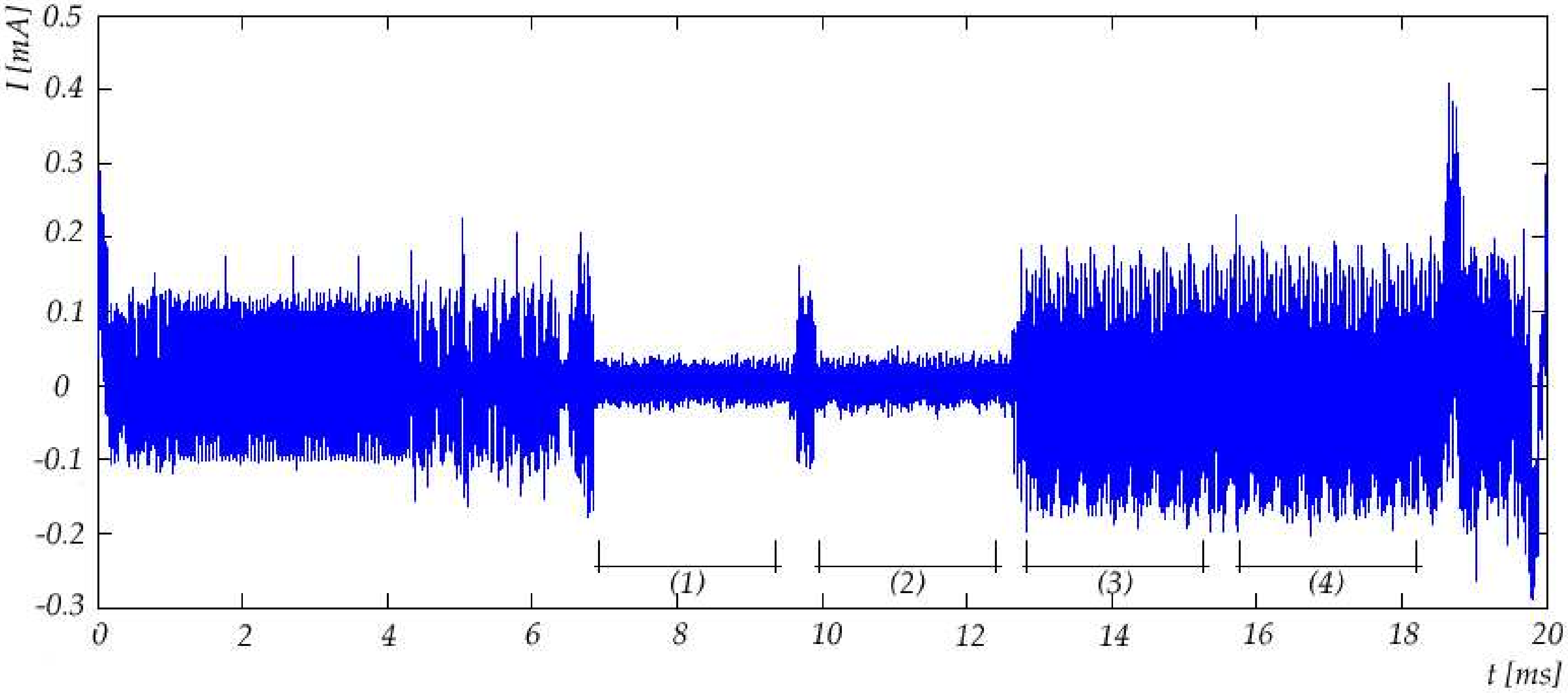


FIGURE 10: DIFFERENCETRACE OF TWO SETS.

Analysis Smartcard

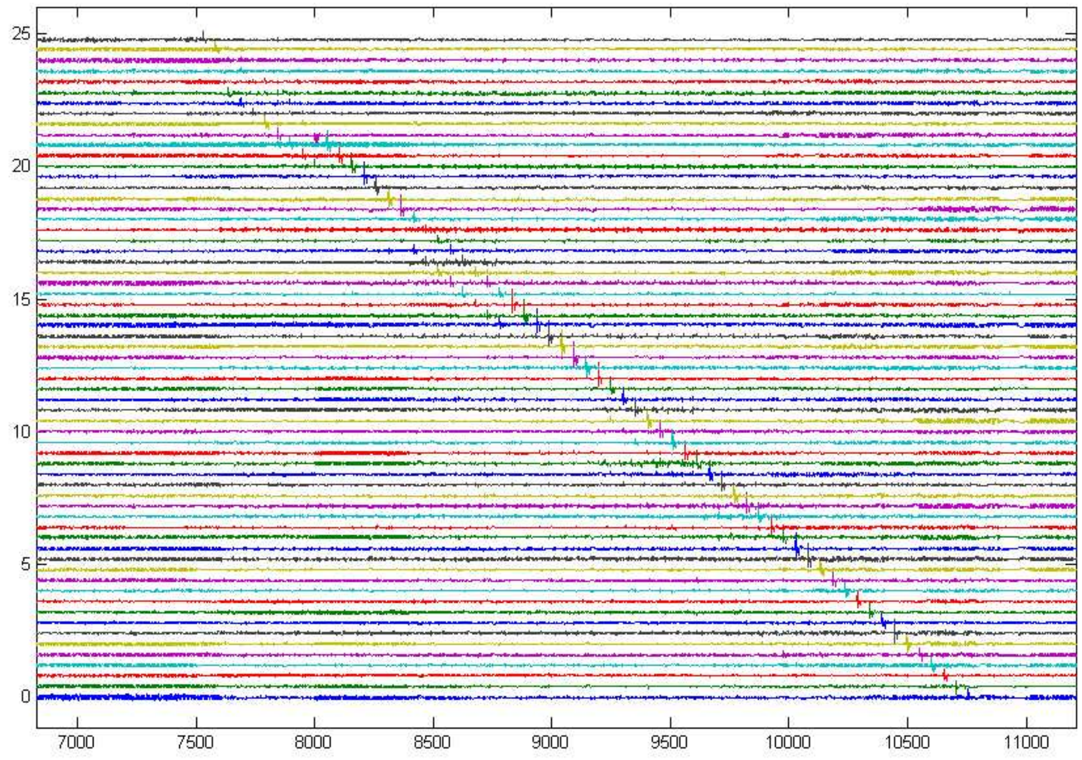


FIGURE 11: ANALYSIS OF THE PRECACULATION ON THE SMARTCARD

Questions