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

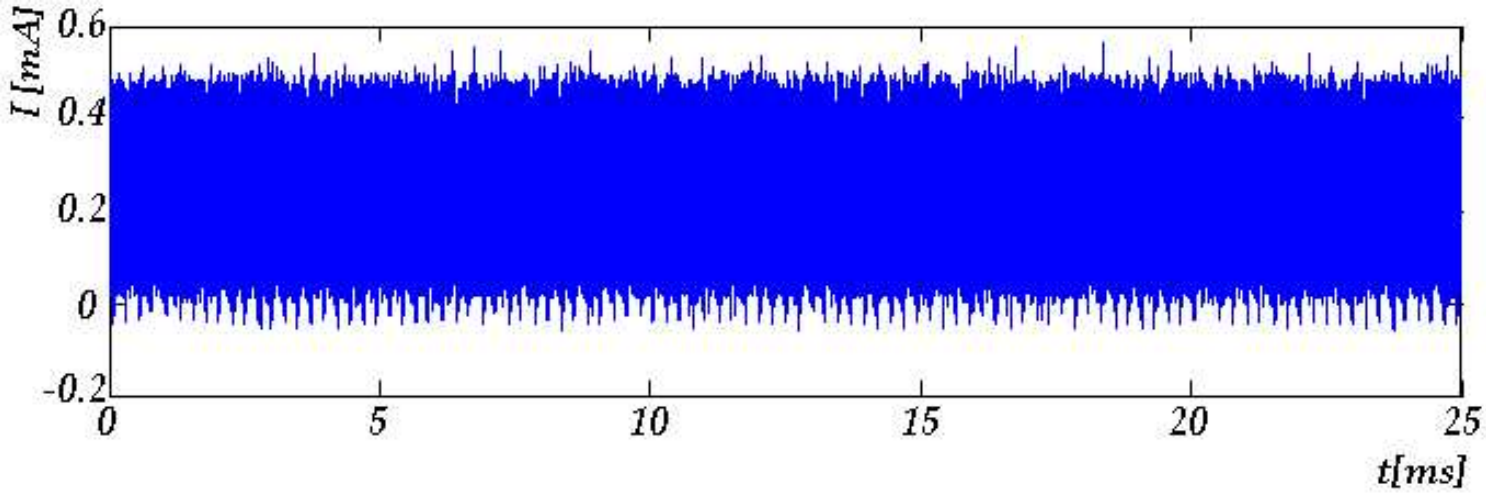
Square & Multiply algorithm for exponentiation of $p = a^e \bmod n$

1. Set $p \leftarrow a^{e_{n-1}}$ and $i = n - 2$.
2. Set $p \leftarrow p^2 \bmod m$.
3. If $e_i = 1$, set $p \leftarrow p \cdot a \bmod m$.
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*.
  $$X^i = (x_1^i, \ldots, x_l^i)$$
- Addition and Subtraction are defined: For $X^1 = (x_1^1, \ldots, x_l^1)$ and $X^2 = (x_1^2, \ldots, x_l^2)$ is
  $$X^1 + X^2 = (x_1^1 + x_1^2, \ldots, x_l^1 + x_l^2).$$
- 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
  $$\overline{X} := (\overline{X}_1, \ldots, \overline{X}_l) := \left(\frac{1}{m} \sum_{i=1}^{m} x_1^i, \ldots, \frac{1}{m} \sum_{i=1}^{m} x_l^i \right).$$

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

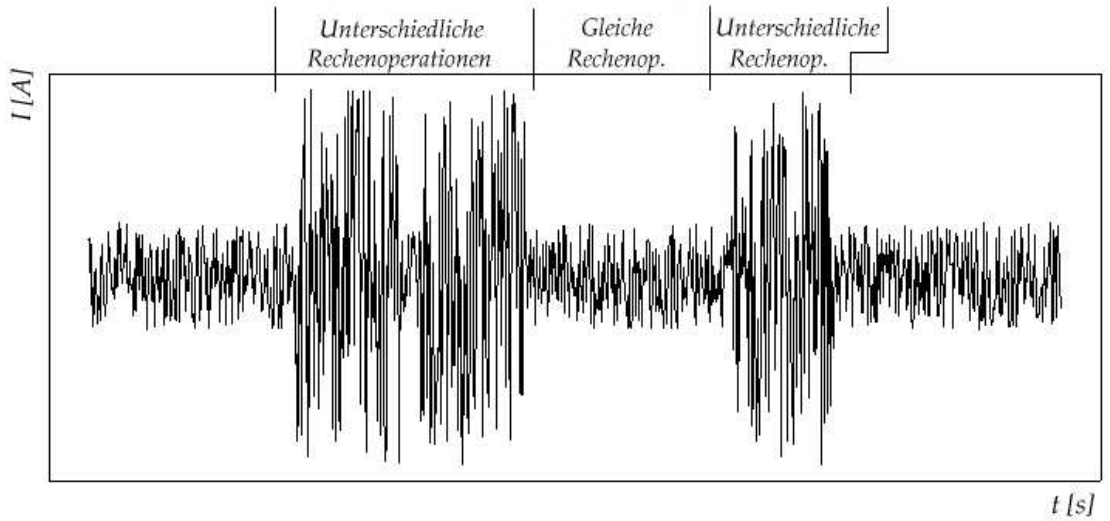


FIGURE 1: DIFFERENCE OF TWO TRACES.

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

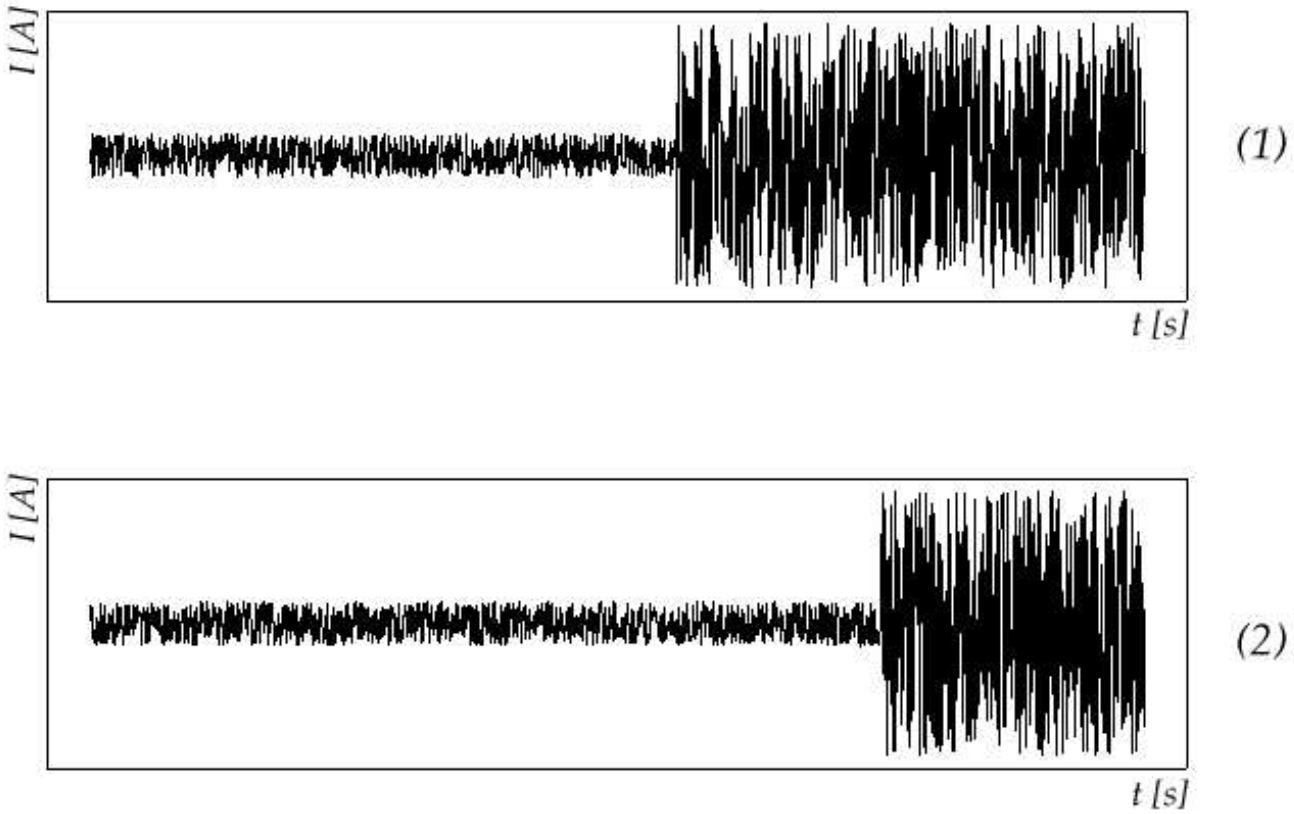


FIGURE 2: (1) DIFFERENCETRACE TO A FALSE GUESS,
(2) DIFFERENCETRACE TO A CORRECT GUESS.

Data-Analysis

Data value logging

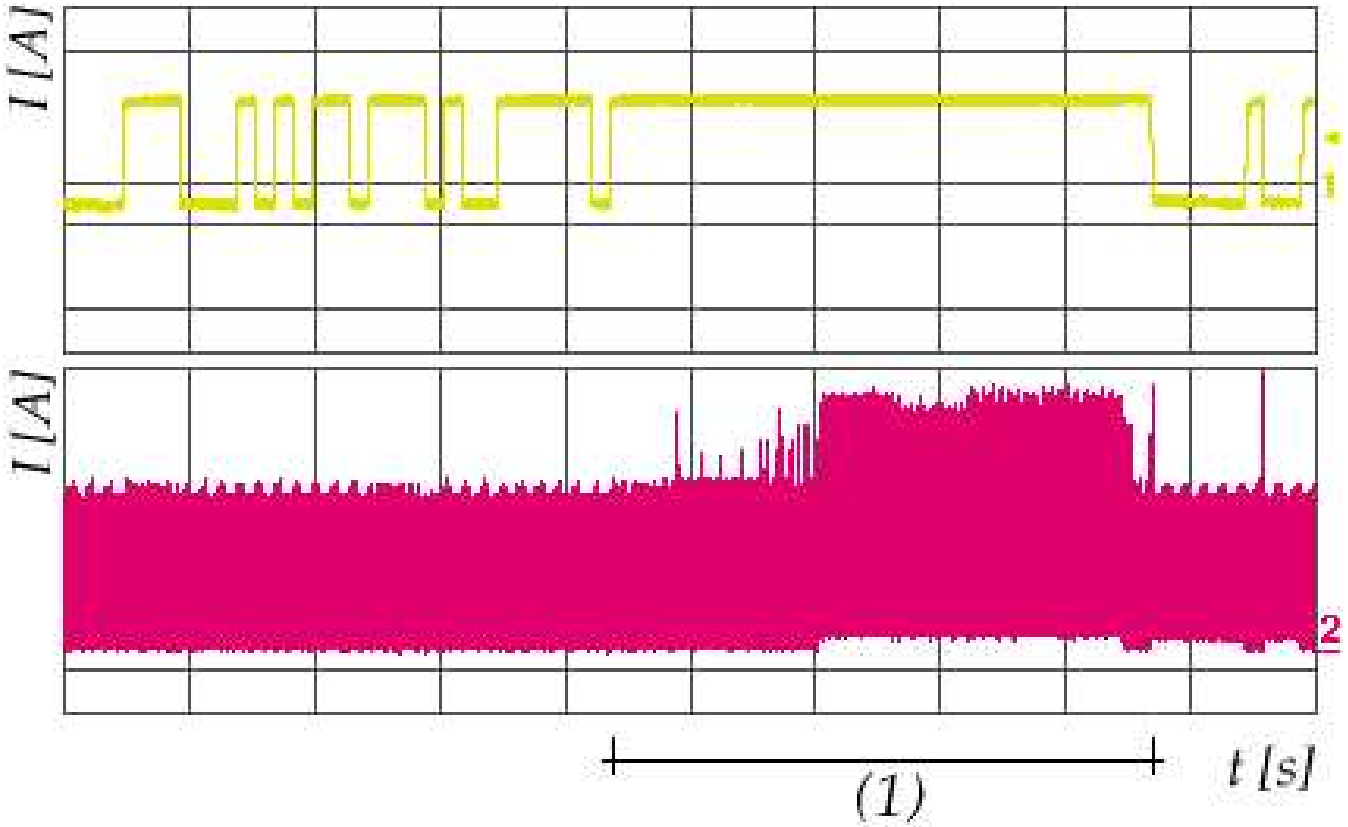


FIGURE 3: CHANNEL (1): TRANSMITION OF SMARDCARD-COMMANDS.

CHANNEL (2): POWER CONSUMPTION.

Data-Analysis - Preprocessing

- Synchronisation
  - Cross correlation
  - Minimal differences
- Compression

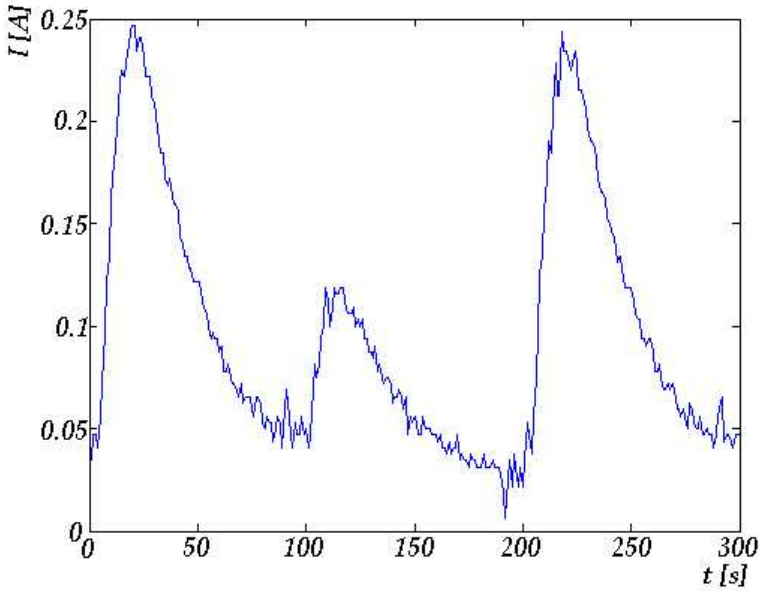


FIGURE 4: THREE CLOCK CYCLES. 100 MEASURE VALUES BUILD ONE CLOCK CYCLE.

Analysis Microcontroller

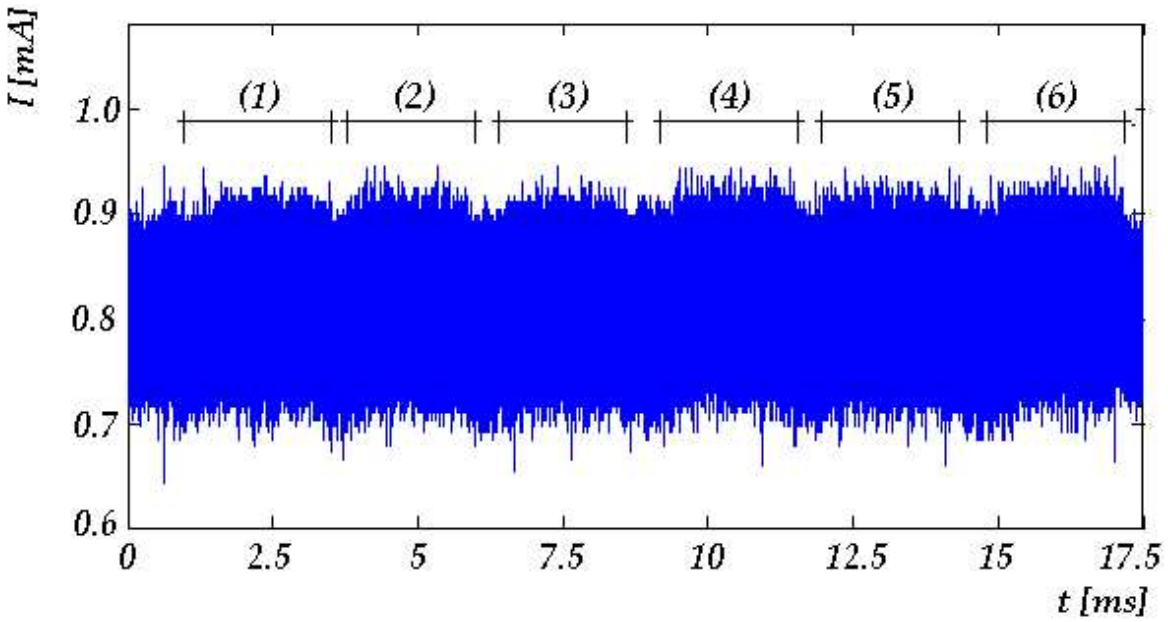


FIGURE 5: 6 INTERVALLS CONTAINING AN ARITHMETICAL OPERATION.

Analysis Microcontroller

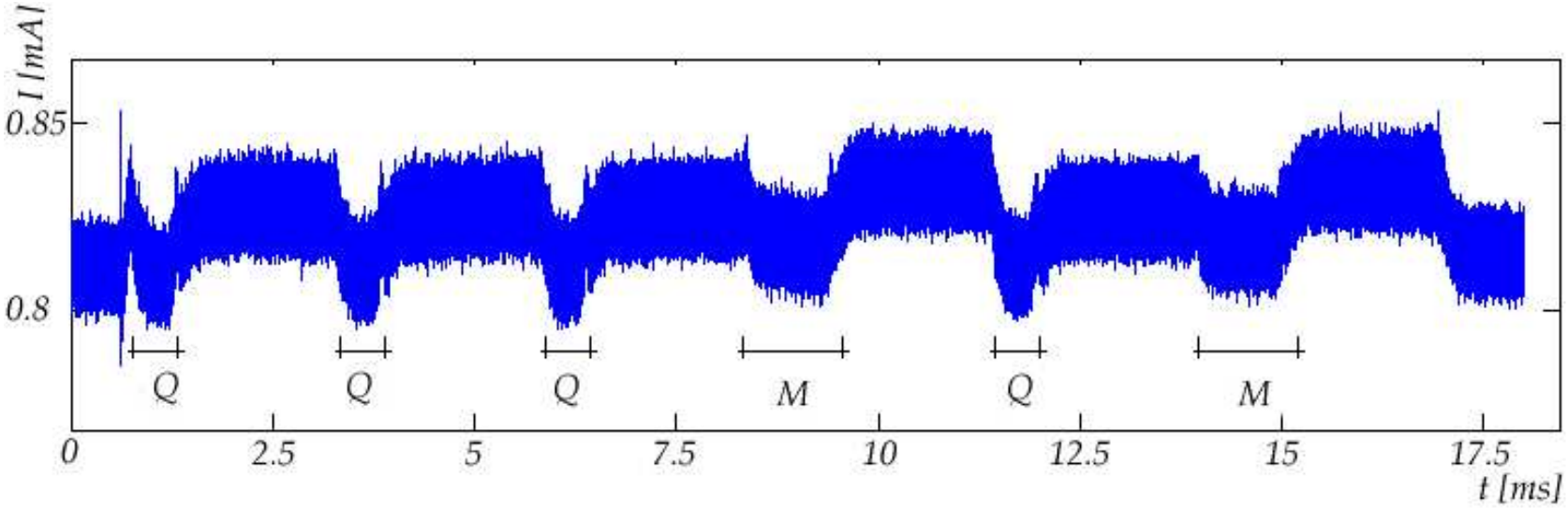


FIGURE 6: MEANTRACE FOR 100 TRACES. Q LABELS AN SECTION FOR A SQUARING DOWN, M LABELS A SECTION FOR A MULTIPLICATION.

EXPONENT: $e = (10011)$

Analysis Microcontroller

PROBLEM DPA: Execution time

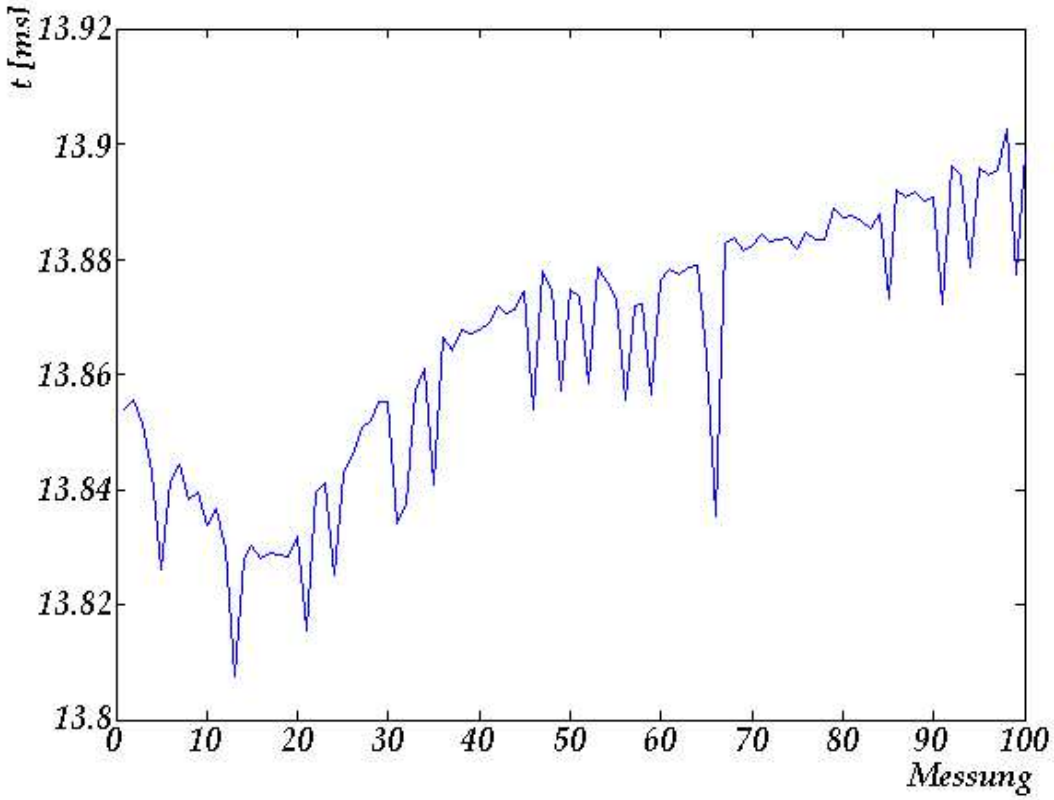


FIGURE 7: COHERENCE BETWEEN EXECUTION TIME FOR AN RSA-OPERATION AND RUNING TIME OF THE MICROCONTROLLER.

Analysis Smartcard

Identifying the algorithm and its position

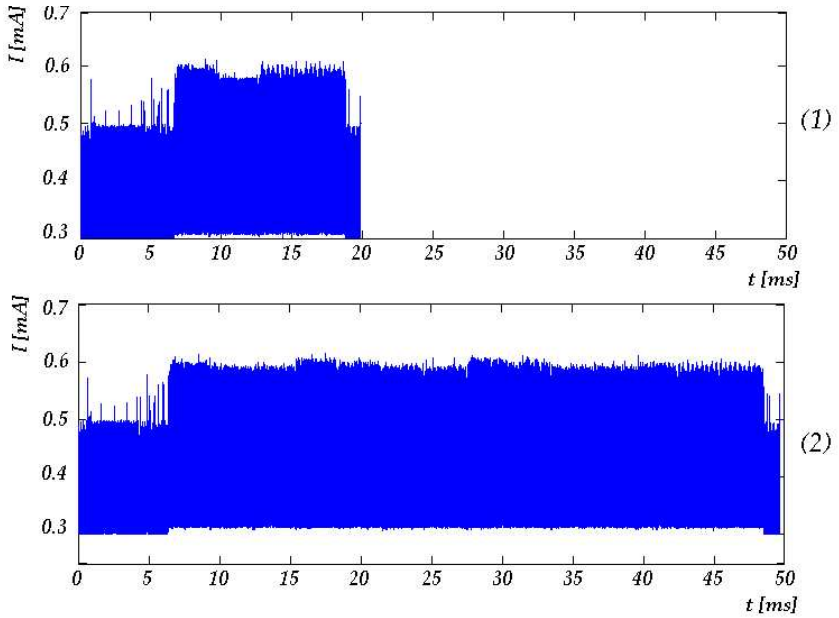


FIGURE 8: (1) ENCRYPTION OF MESSAGE M USING EXPONENT $e = (07)_{16}$.
(2) ENCRYPTION OF MESSAGE M USING EXPONENT $\hat{e} = (\mathrm{FF})_{16}$.

Analysis Smartcard

Algorithm: Square & Multiply

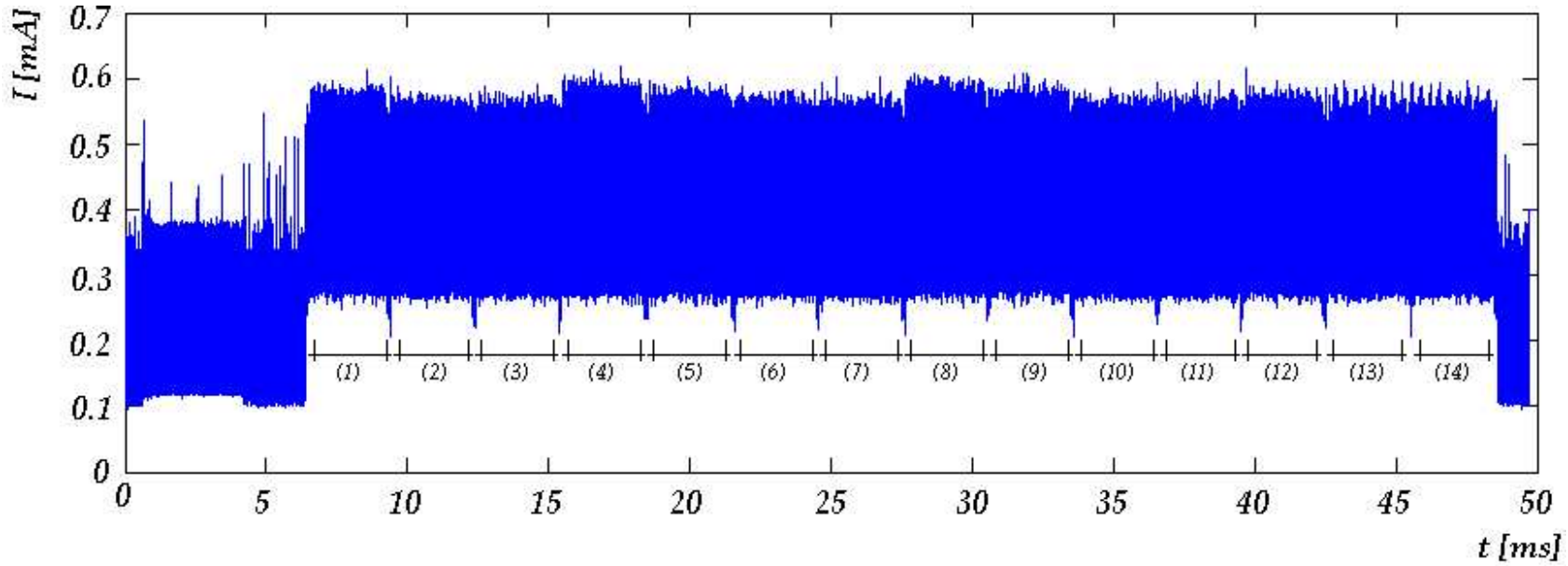


FIGURE 9: COMPRESSED MEANTRACE.

Analysis Smartcard

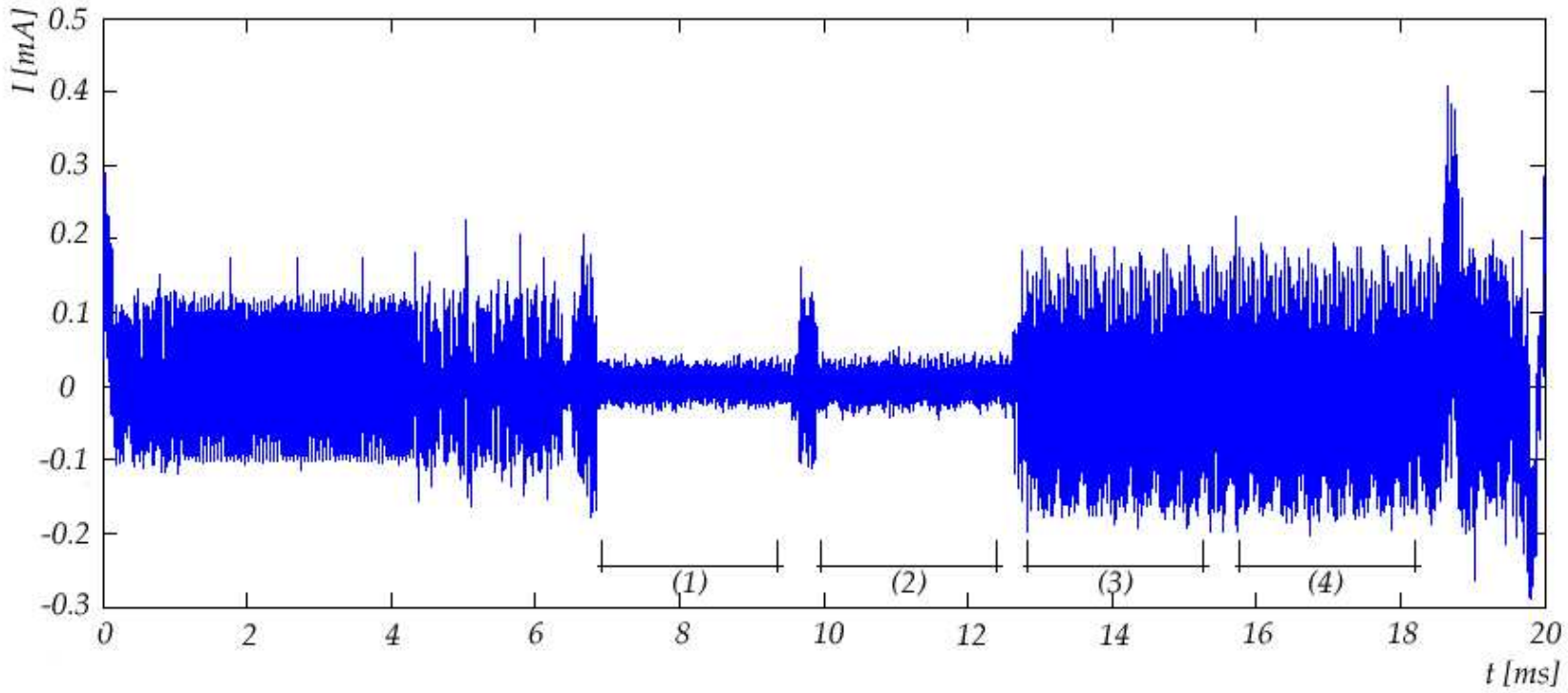


FIGURE 10: DIFFERENCETRACE OF TWO SETS.

Analysis Smartcard

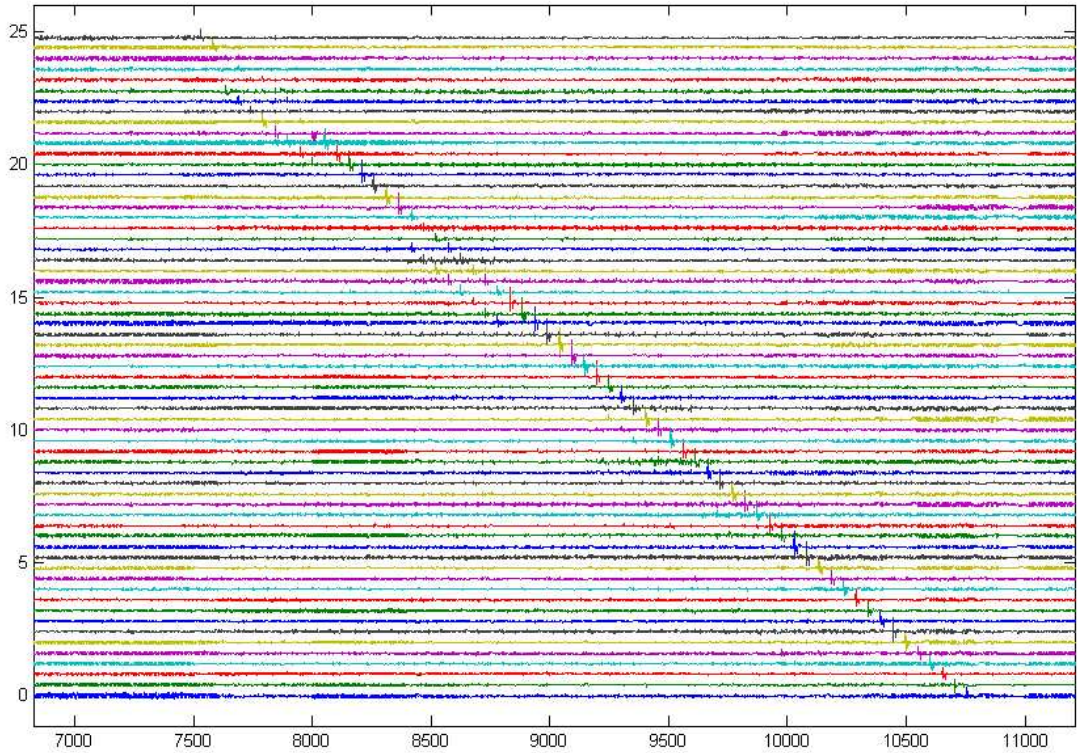


FIGURE 11: ANALYSIS OF THE PRECACULATION ON THE SMARTCARD

Questions