Applied Security

DPA on AES (8)

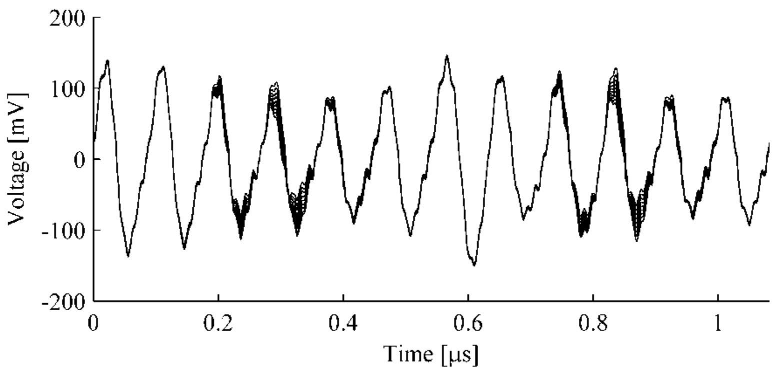
General Overview

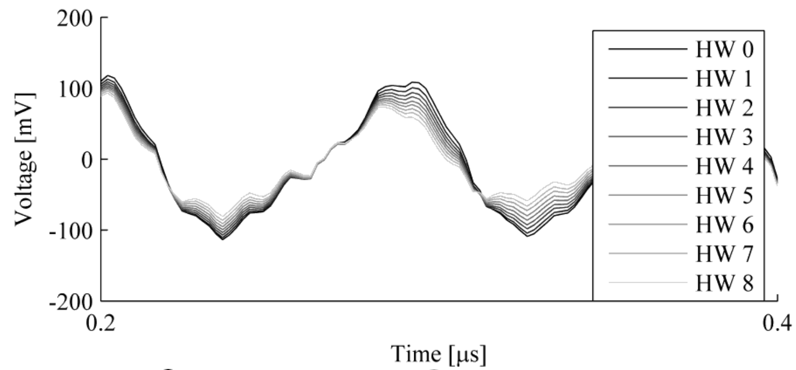
- We go through a DPA attack on AES step by step and think about the impact of choices we have in each step
- This will allow you to complete part of the coursework

Beware: in order to follow the lectures you NEED to be familiar with various cryptographic algorithms and implementation techniques!

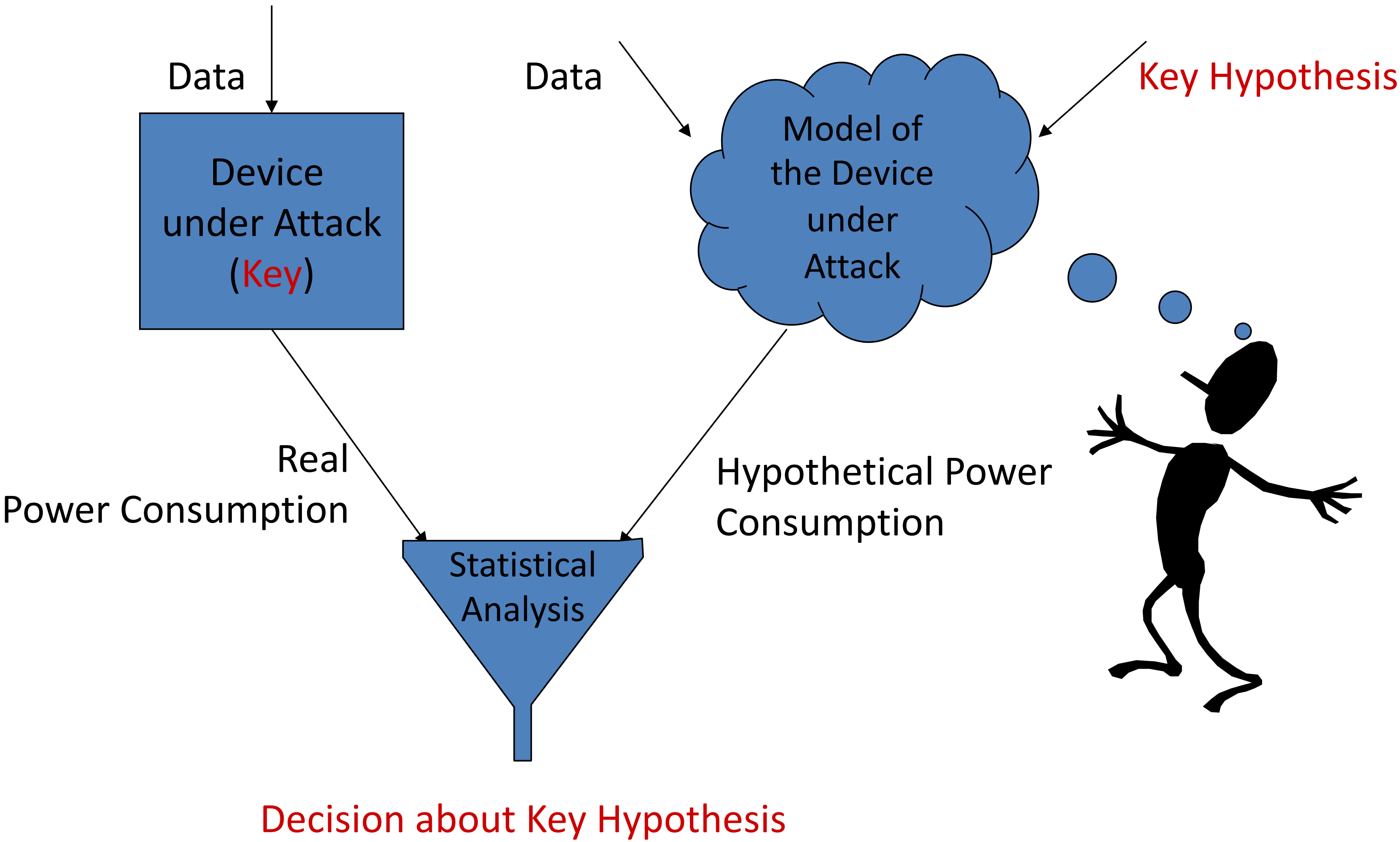
SPA vs DPA

- Typically SPA attacks exploit leakage that depends on the type of operation
- DPA attacks exploit the data depent leakage:
  - Example below shows MOV instructions on an 8-bit: the shape is the same but the height of the curves in some of the clock cycles depends on the data



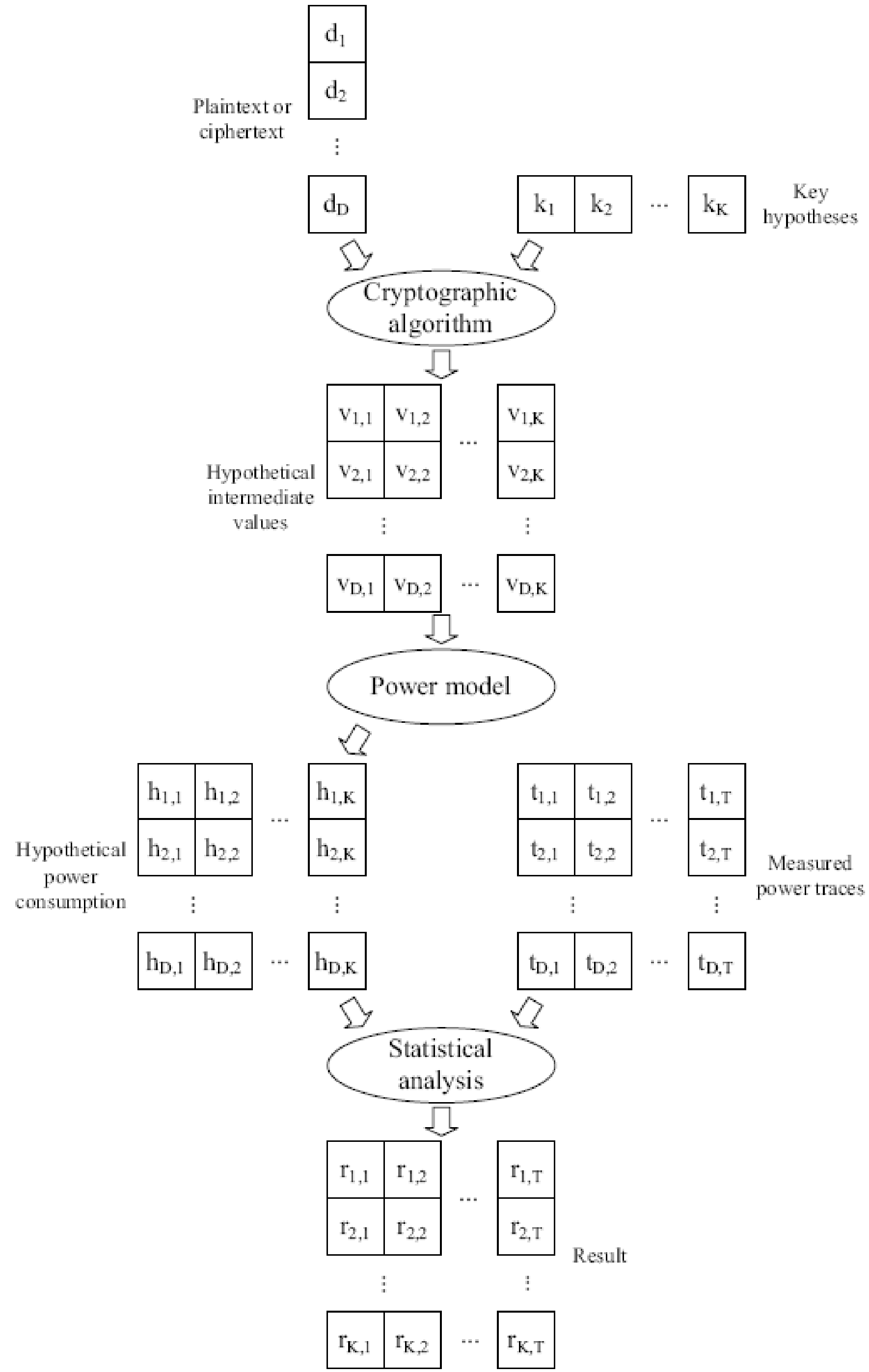


Principle of a differential power attack



5 Step Model of a DPA Attack

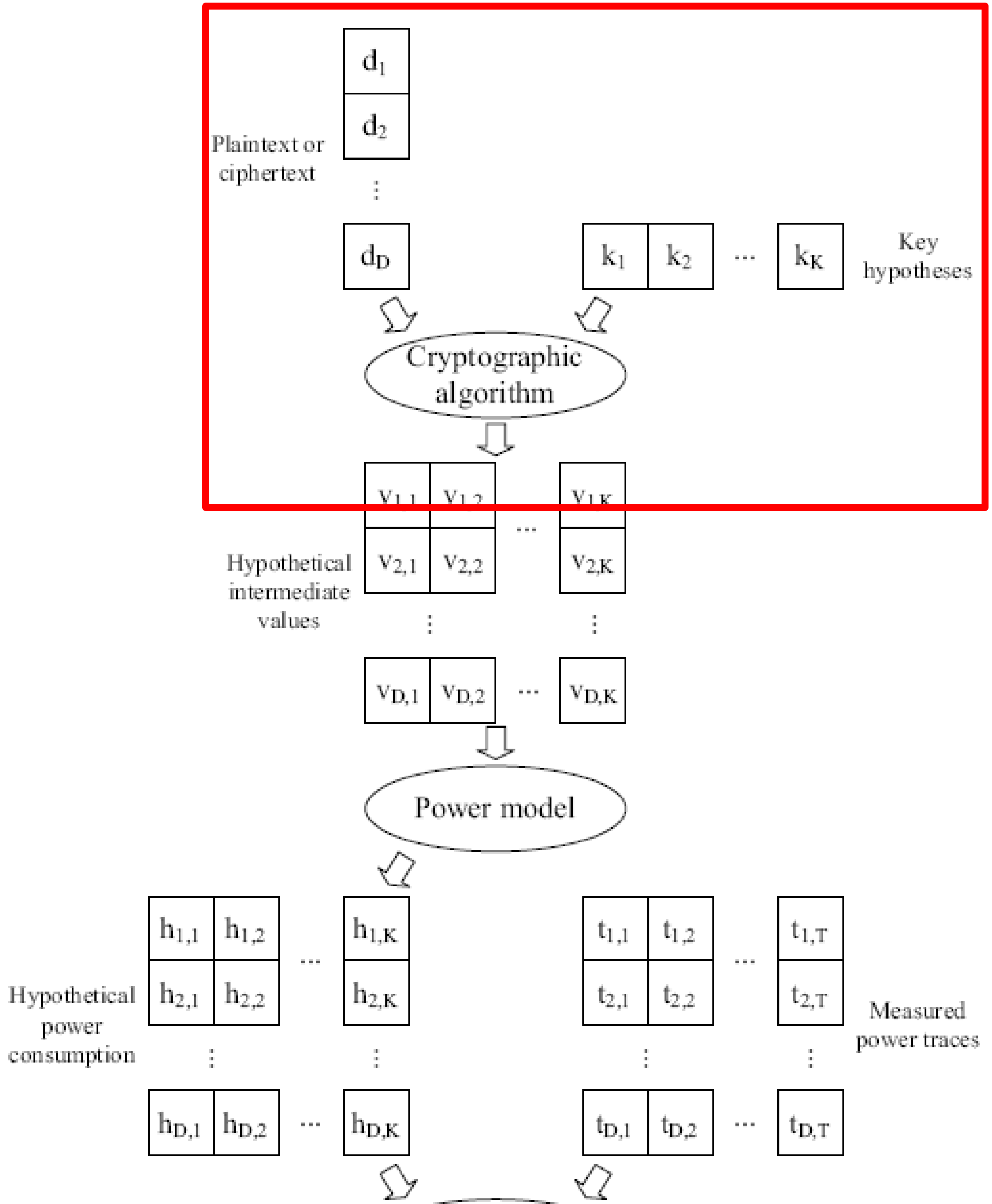
1) Selection of target intermediate variable
2) Measurement of the power consumption/EM
3) Calculation of the hypothetical intermediate values
4) Mapping of hypothetical values to predicted power consumption values
5) Statistical analysis using a distinguisher



5 Steps in detail

Step 1: Choosing an intermediate result of the executed cryptographic algorithm

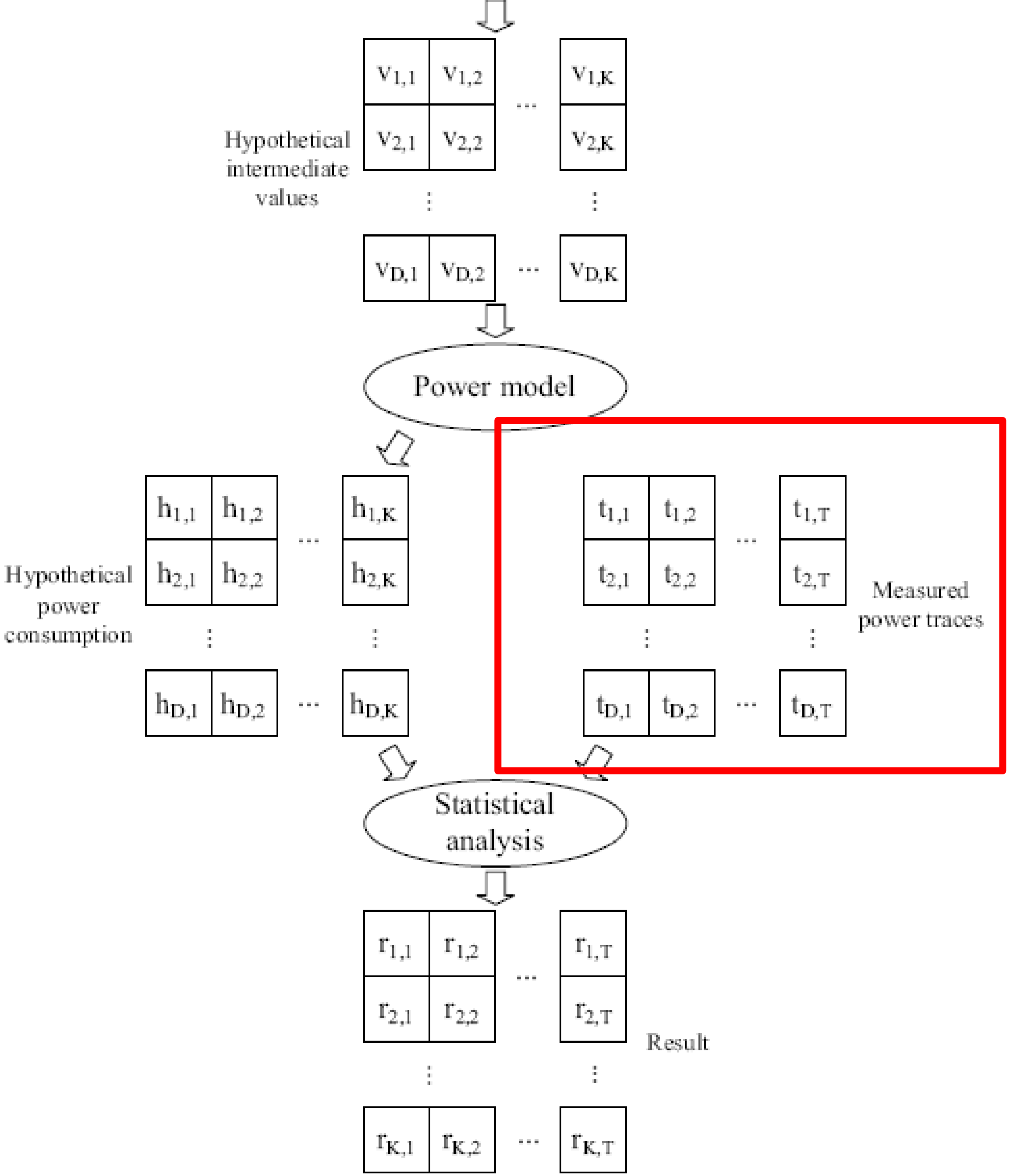
- Algorithm must be known
- Intermediate variable (the target) is function of key and data
- Good targets for DPA are functions which are highly non-linear as they facilitate distinguishability of the correct key hypothesis



5 Steps in detail

Step 2: Measuring the power consumption for D input values

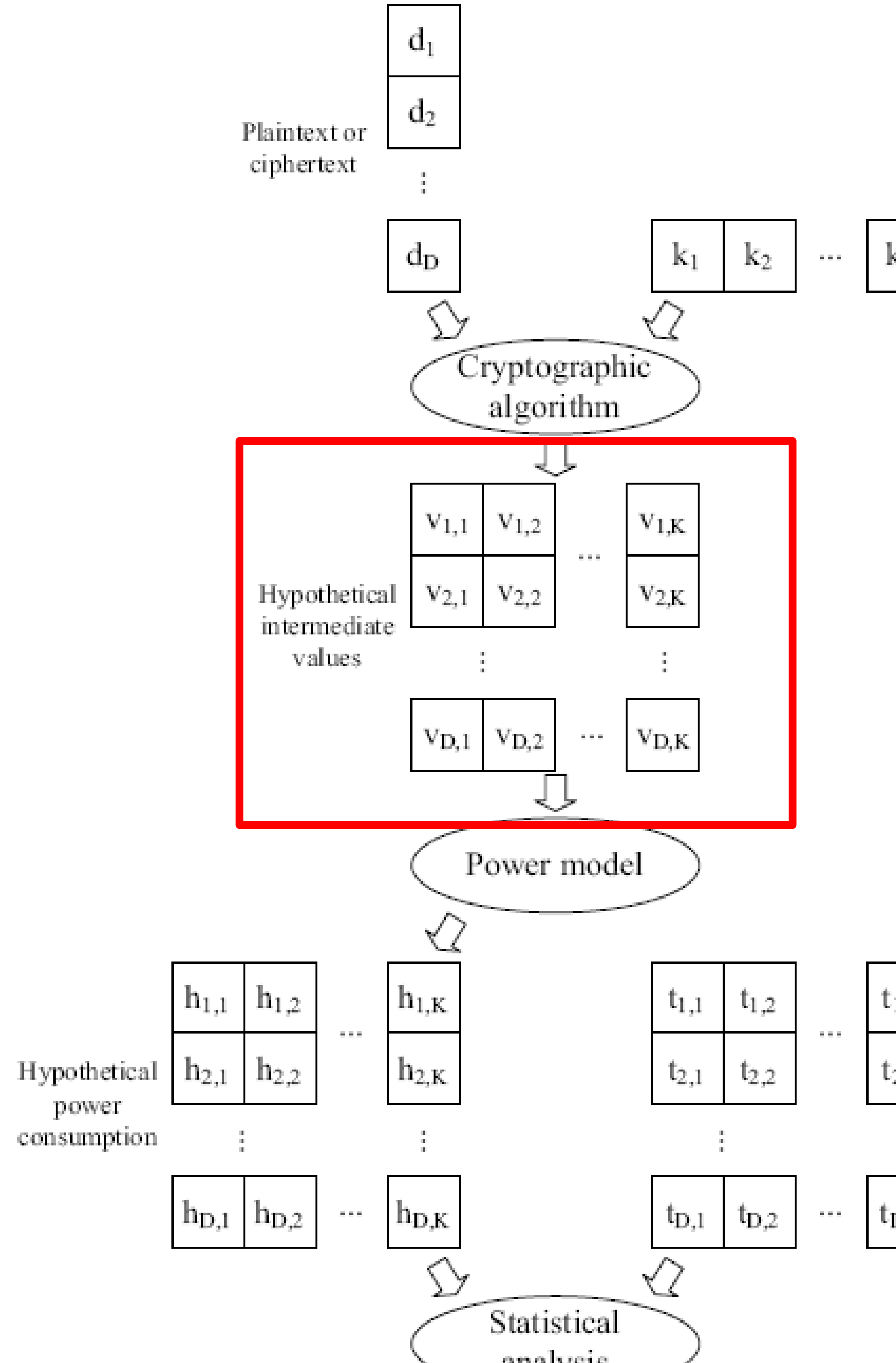
- If necessary process traces to reduce noise and strip away unnecessary information
- Result is a (D x T) matrix **t**
  - For each input we store a power trace consisting of T data points



5 Steps in detail

Step 3: Calculating hypothetical intermediate values

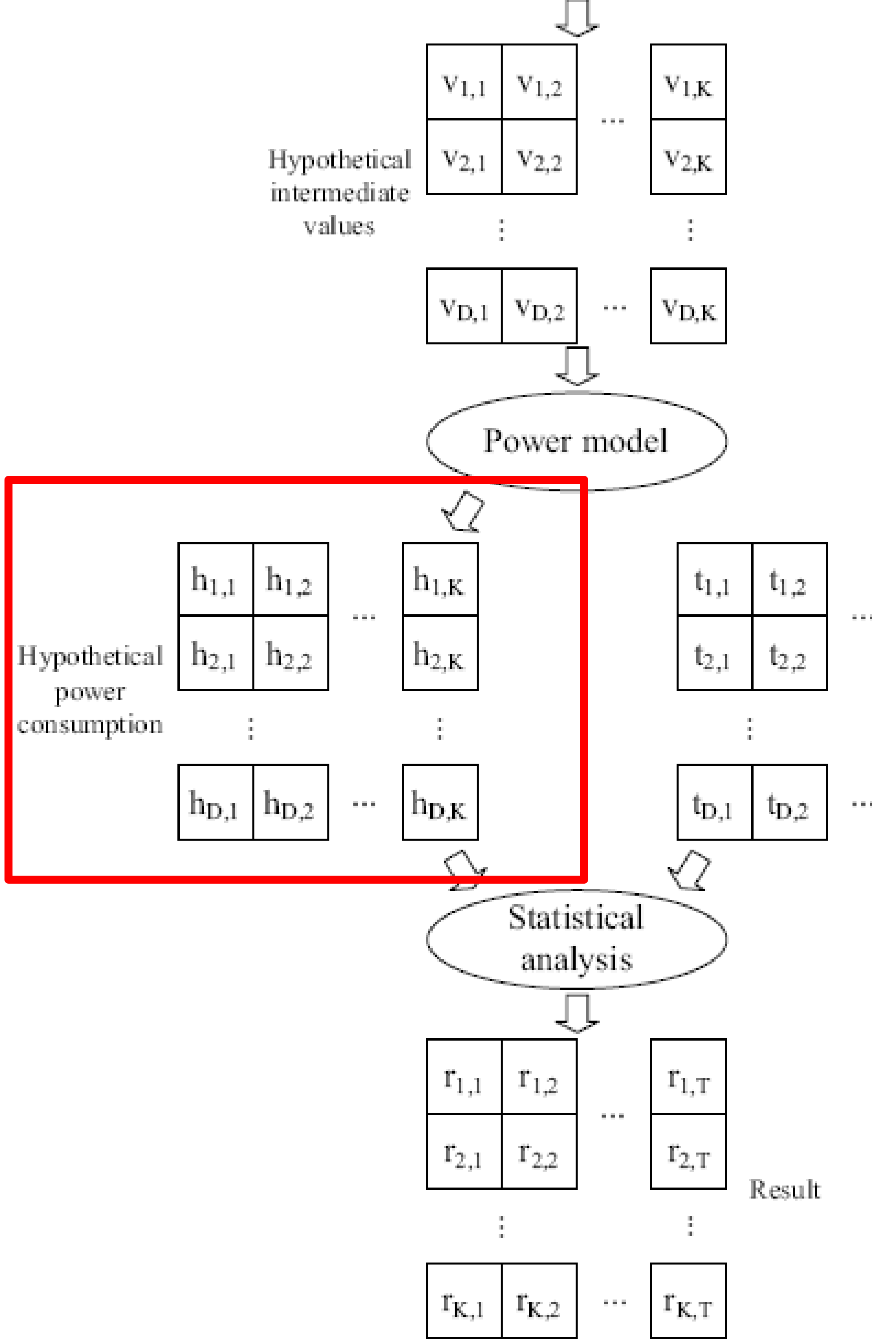
- For a K-bit guess we get 2^K key hypotheses: **k** = (k_1, …, k_{2^K})’
- Together with the D inputs we can calculate a (D x 2^K) Matrix containing the predicted intermediate values $v_{i,j} = f(d_i, k_j)$
  - We write the column corresponding to the correct key as `ck‘



5 Steps in detail

Step 4: Calculating hypothetical power values

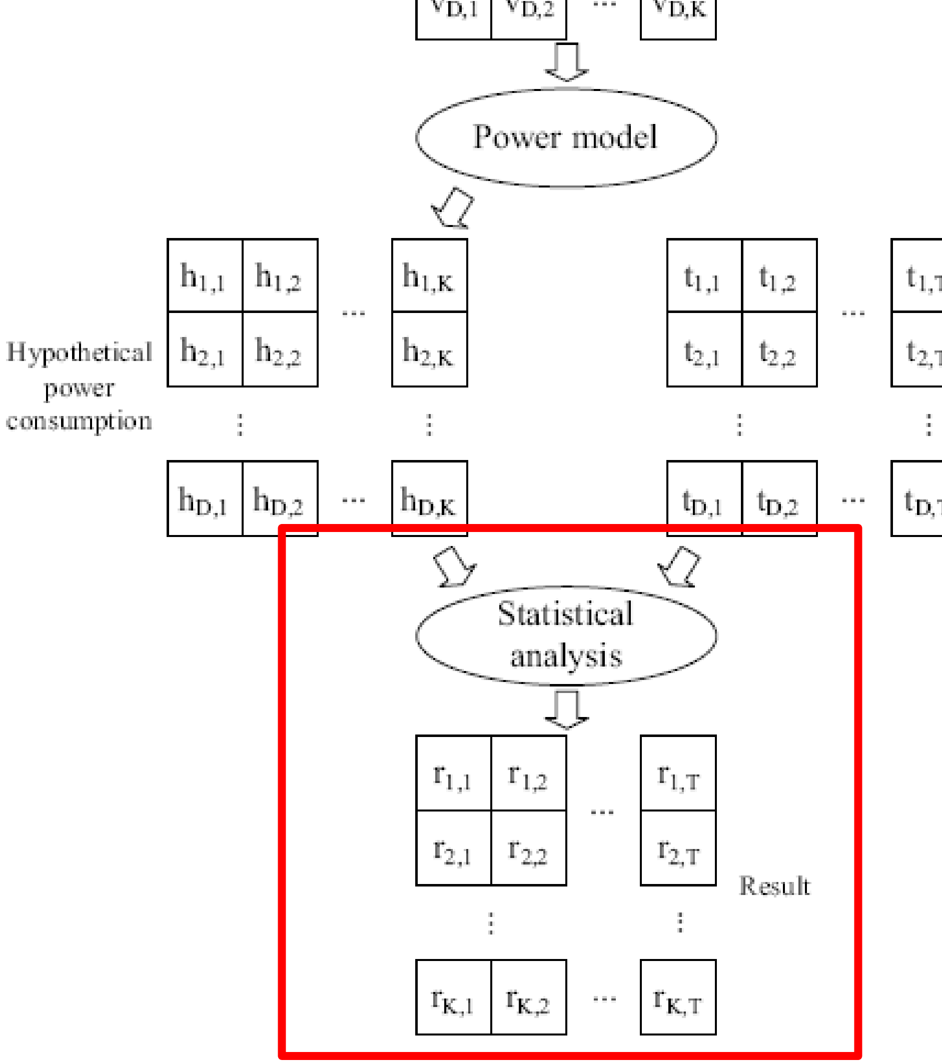
- We map the values in matrix V to matrix H using a power model
- Models requiring little knowledge:
  - Bit model
  - Zero-value model
- Models requiring moderate knowledge
  - Hamming Weight (HW)
  - Hamming Distance (HD)
- Models that require characterisation
  - Templates



5 Steps in detail

Step 5: statistical analysis

- Each column of **H** is compared with (column-wise)
  - Results in a (K x T) matrix
- The correct key hypothesis `stands o
  - How it stands out depends on the distinguisher
  - But the general principle is that the better the modelled traces resemb the real traces the more likely the associated key hypothesis is the correct key
  - We expect to see something `distinguishable‘ in **R** at index (ck, ct) (ct … time index when attacked intermediate variable is processed)

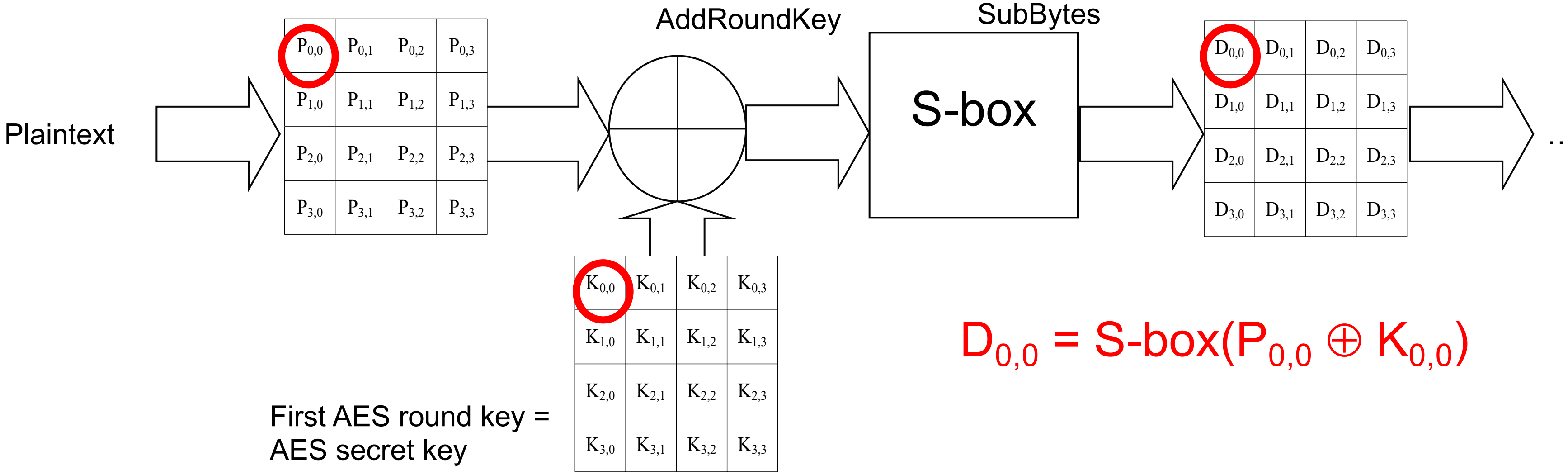


A DPA attack on an AES implementation

- We use traces that have been acquired using a simple microcontroller setup
  - Resemble traces one would get from a typical low-end DPA unprotected smart card
- AES has been implemented in software as described in the last lecture
  - ARK, SB, SR and the MC
- We assume the adversary has access to the plaintexts and aims to recover the key

Step 1: Intermediate variable

- **Choice:** output byte of the first AES S-box operation in round 1
  - Function of the first byte of the plaintext and the first byte of the key
- The first round of AES



$$D_{0,0} = \text{S-box}(P_{0,0} \oplus K_{0,0})$$

Steps 2-4

- **Step 2**: Measurement sample: 1000 traces → **T**
- **Step 3**: $v_{i,j}$ = S-box($d_i \oplus k_j$) → **V**
  - size of **V**: 1000x256
- **Step 4**: $h_{i,j}$ = LSB($v_{i,j}$) → **H**
  - size of **H**: 1000x256

Steps 2-4

Sample number i	Plaintext byte d_i	Key hypothesis k_1 (j=1)	Hyp. intermediate value $v_{i,1}$ = S-box($d_i \oplus k_1$)	Hyp. power consumption $h_{i,1}$ = LSB($v_{i,1}$)
1	0D	00	D7	1
2	95	00	2A	0
3	17	00	F0	0
4	C7	00	C6	0
5	9B	00	14	0
6	3B	00	E2	0
7	34	00	18	0

Steps 2-4

Sample number i	Plaintext byte d_i	Key hypothesis k_2 (j=2)	Hyp. intermediate value $v_{i,2}$ = S-box($d_i \oplus k_2$)	Hyp. power consumption $h_{i,2}$ = LSB($v_{i,2}$)
1	0D	01	FE	0
2	95	01	22	0
3	17	01	47	1
4	C7	01	B4	0
5	9B	01	B8	0
6	3B	01	80	0
7	34	01	96	0

Step 5

- **Step 5**: **R** = D(**H**, **T**), we choose D=correlation

Hypothetical power consumption (rows: Samples; columns: Key Hypotheses)

1	0	0
0	0	0
0	1	1
0	0	0

Measured power consumption (rows: Samples; columns: Time)

10	5	4	45	45
67	56	45	4	8
37	54	12	45	5
27	12	69	8	2

Correlation (rows: Key Hypotheses; columns: Time)

Step 5

Key Hypotheses →

Samples ↓

1	0	0
0	0	0
0	1	1
0	0	0

Hypothetical power consumption

Time →

Samples ↓

10	5	4	45	45
67	56	45	4	8
37	54	12	45	5
27	12	69	8	2

Measured power consumption

Time →

Key Hypotheses ↓

Correlation

Step 5

Key Hypotheses →

Samples ↓

1	0	0
0	0	0
0	1	1
0	0	0

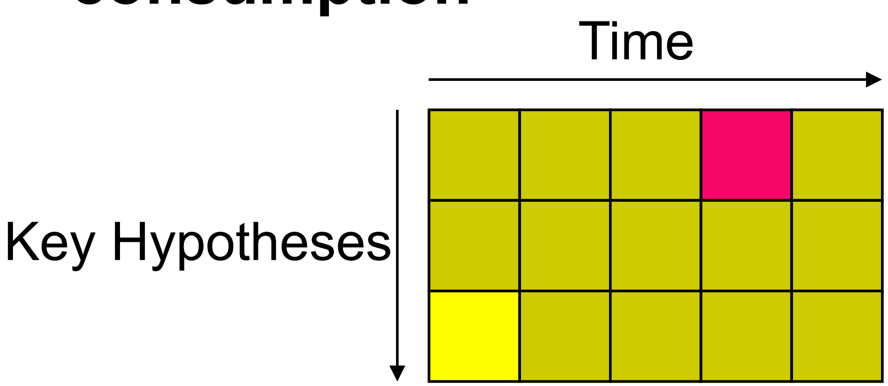
Hypothetical power consumption

Time →

Samples ↓

10	5	4	45	45
67	56	45	4	8
37	54	12	45	5
27	12	69	8	2

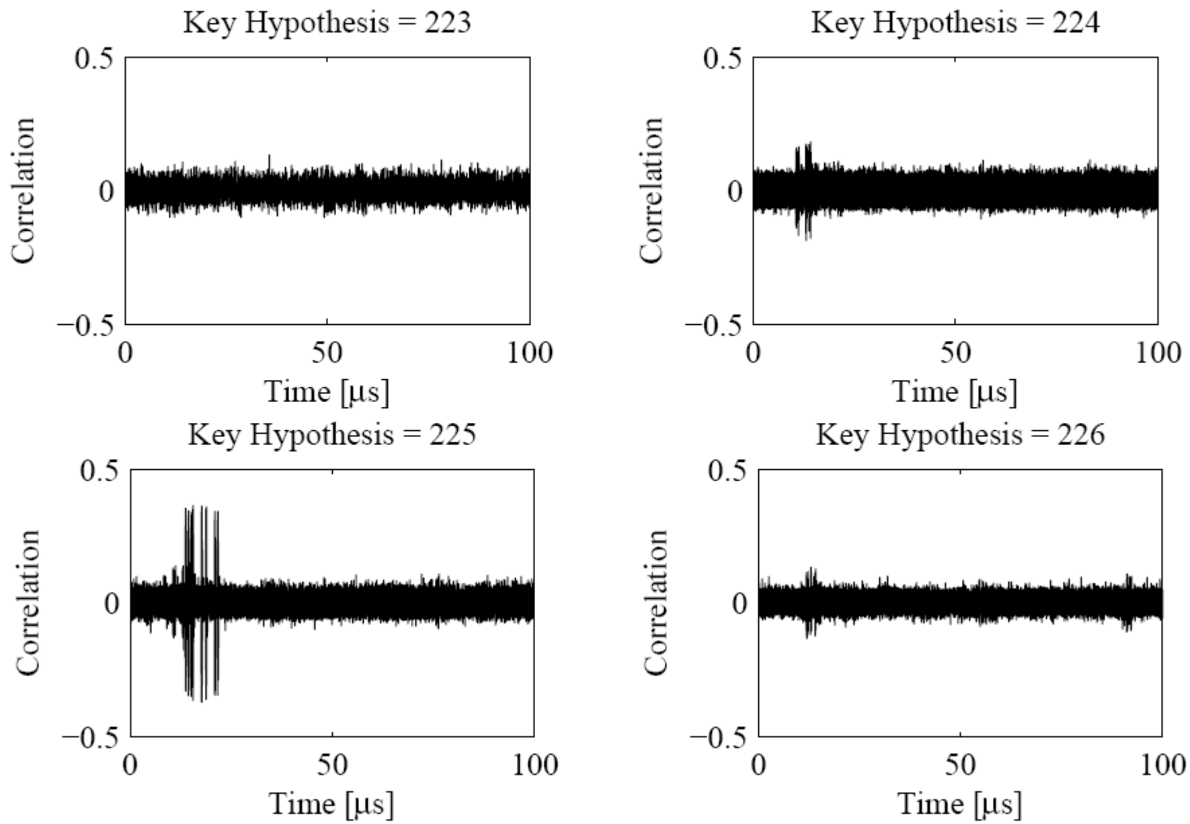
Measured power consumption



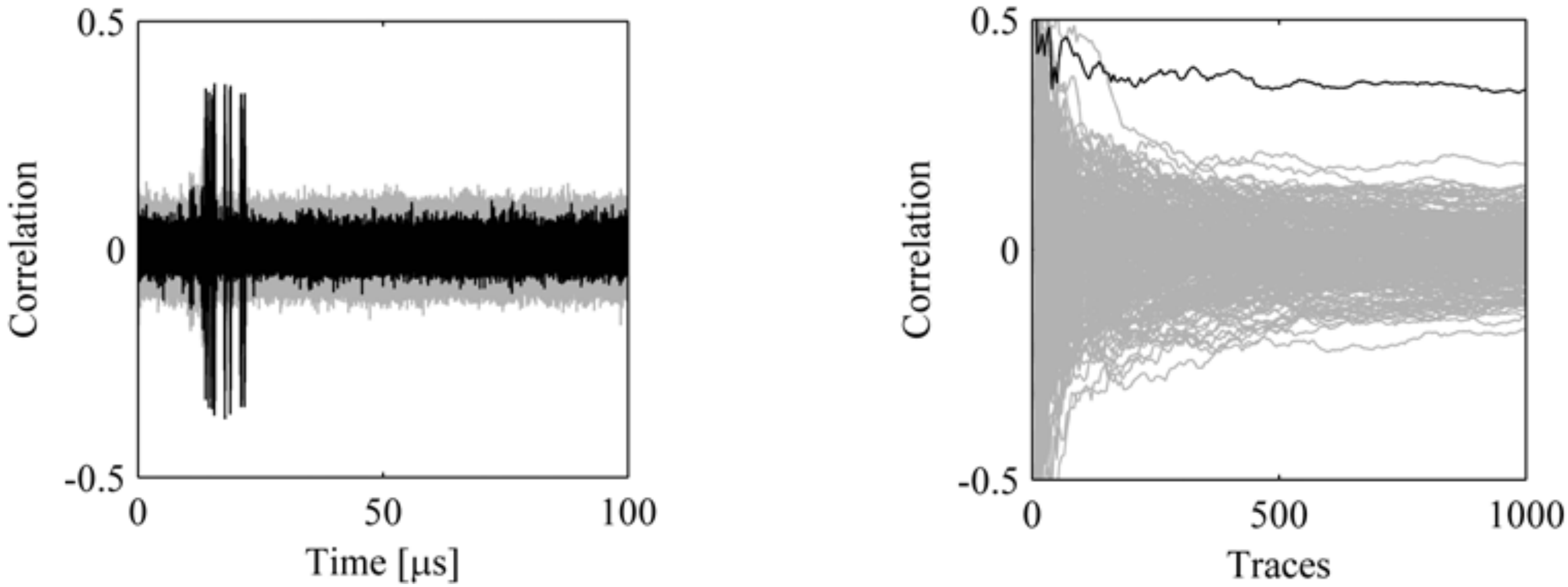
Correlation

Step 5: Result

- Inspect the resulting 256 traces
- We used correlation hence we expect the correct key hypothesis to lead to the highest correlation
- Key ck = 226



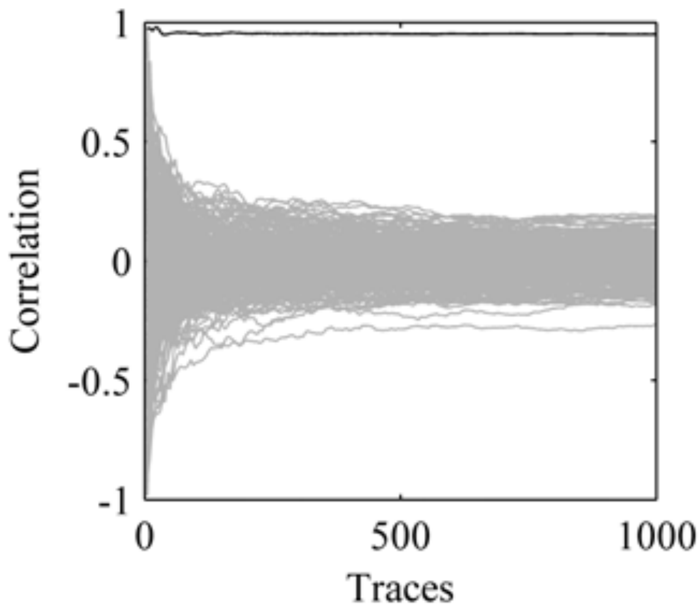
A closer look at the result

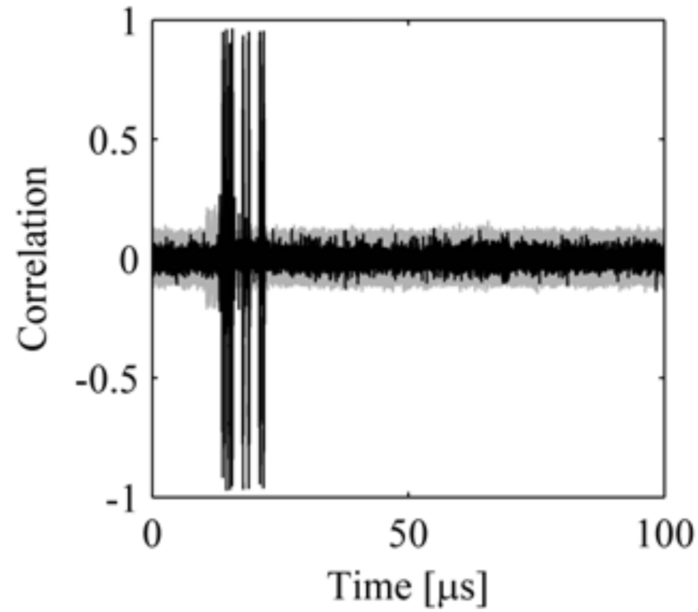


- The correct key hypothesis leads to peaks in the correlation trace that are significantly higher than the peaks that come from incorrect key hypotheses

- About 200 power traces suffice to determine the key

Improving the result

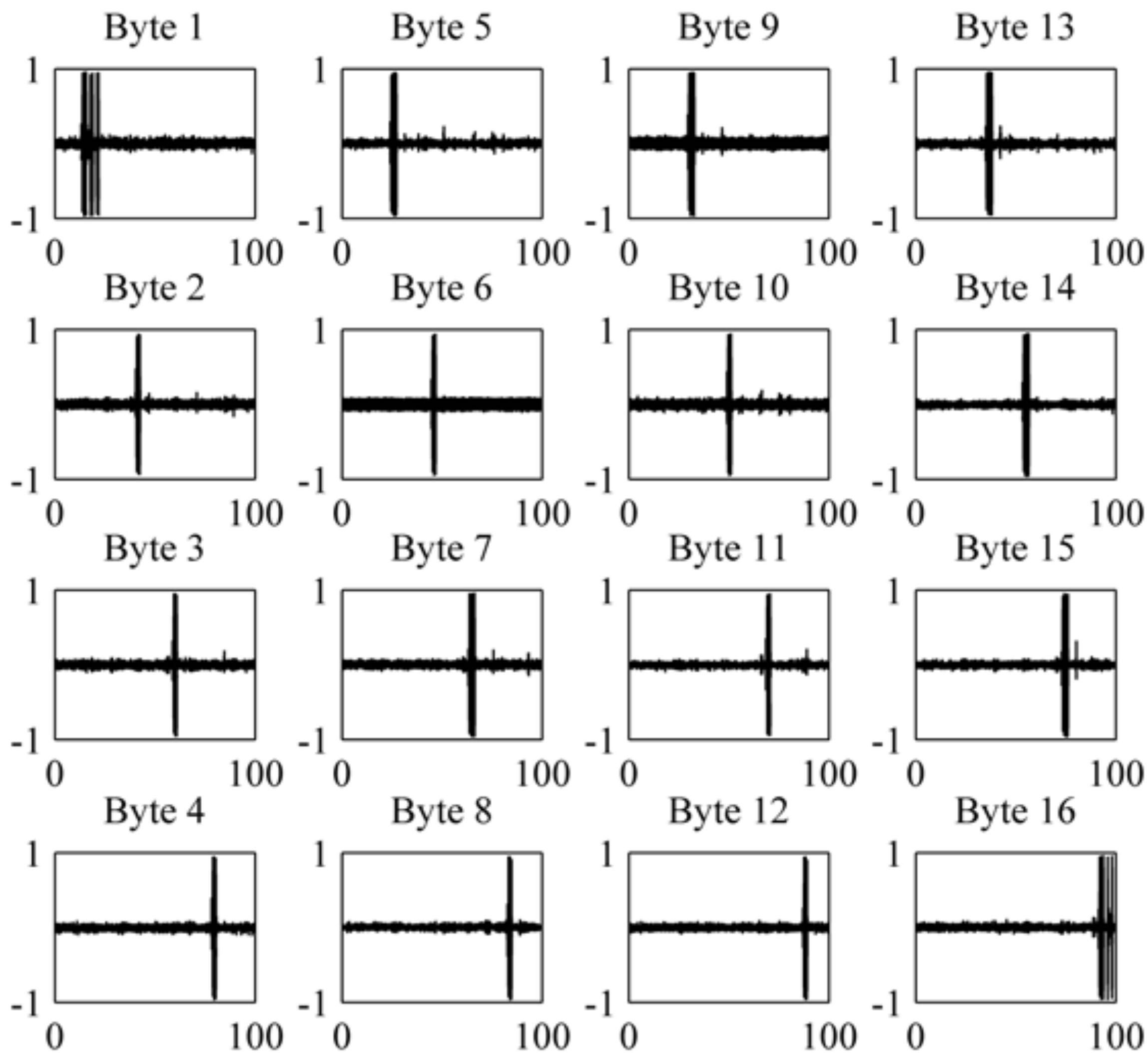




- Using a better power model improves the result of a DPA attack:
  - The correlation coefficient goes up to almost 1 if we compare the Hamming weight of the hypothetical intermediate values with the power traces

Peaks reveal information about implementation too

- High correlation coefficients indicate correct key byte
- Correlation coefficients in this example are almost maximal
- About 30 traces are sufficient to reliably determine the key
- Positions of DPA peaks reveal the points in time when attacked intermediate result is computed.



5 Step Model of a DPA Attack

1) Selection of target intermediate variable
2) Measurement of the power consumption/EM
3) Calculation of the hypothetical intermediate values
4) Mapping of hypothetical values to predicted power consumption values
5) Statistical analysis using a distinguisher

1. Linear vs. Non-linear transformation on combination of input and key
2. Signal vs. Noise
3. Computational resources depending on size of key hypothesis
4. Quality of model
5. Ability of distinguisher to use power model

DPA Demo

- www.dpabook.org

A summary

- DPA attacks involve a number of steps which include choices that will influence the results
- A good power model is crucial for a correlation based attack to succeed (with few traces)
- Clearly the more distinguishable key hypotheses are the less traces are needed

- Note: you are now able to do the DPA assignment in your coursework!