# Securizarea avansata a sistemelor de calcul

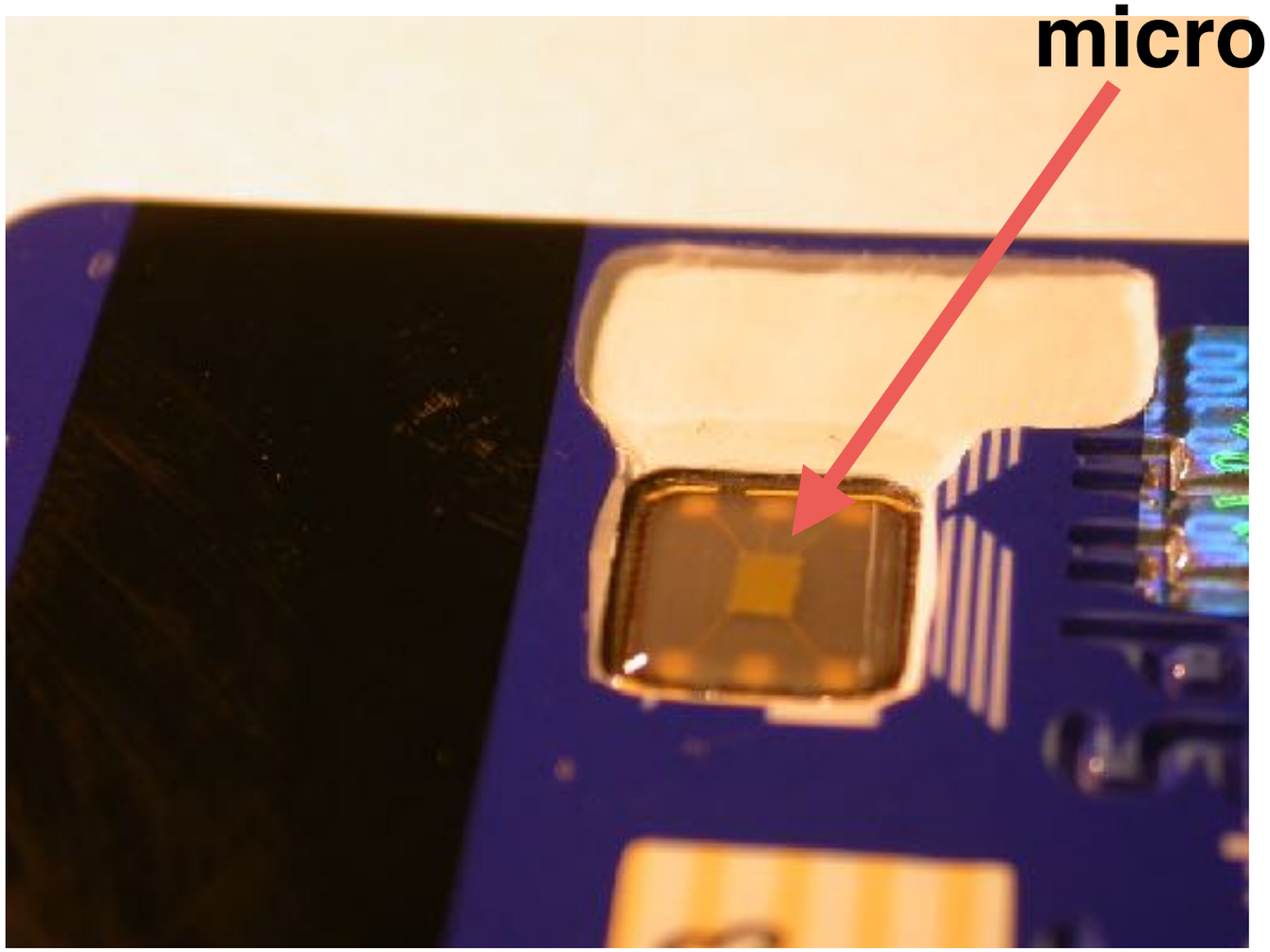
## Side-channel attacks

Marios Choudary
UPB

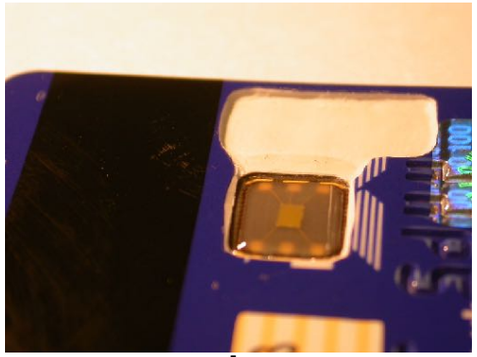
# Smartcards used in many applications (e.g. banking)

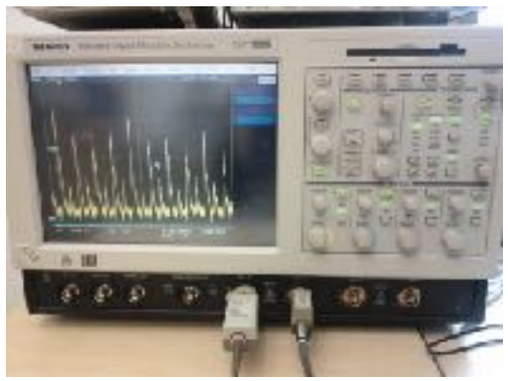

Other examples: Pay-TV, transport

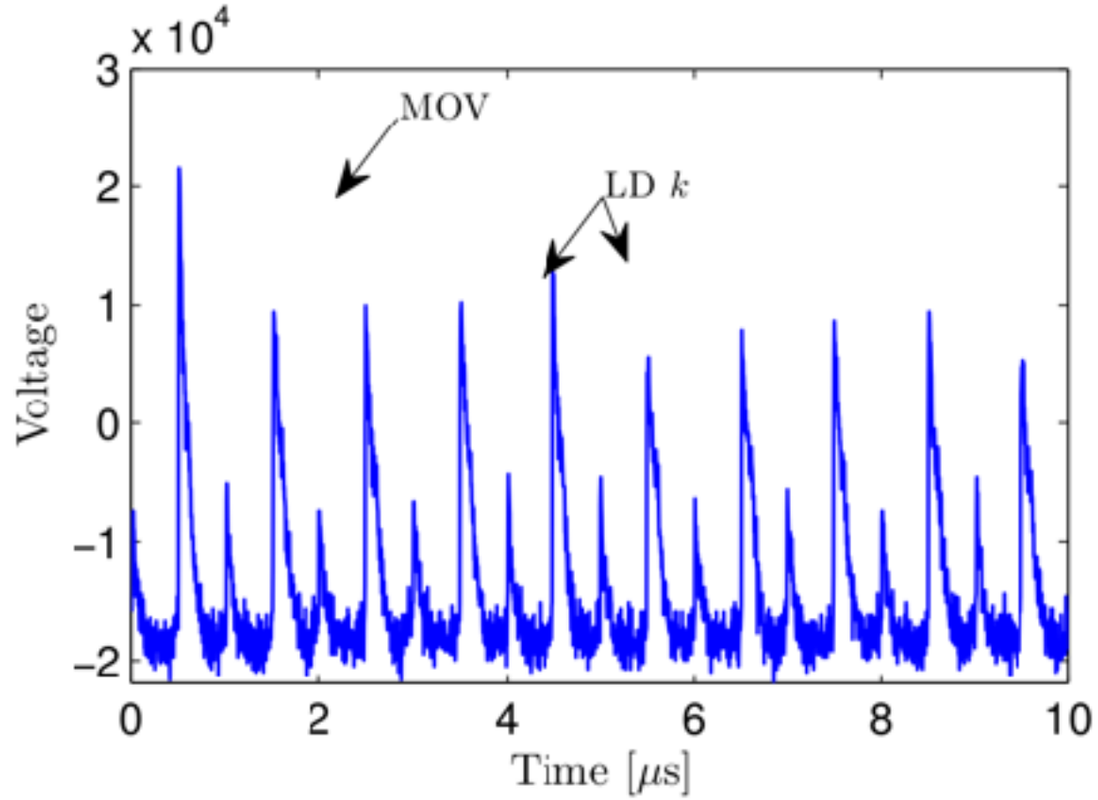
# Microcontroller in smartcards



# Microcontrollers “leak” information via physical side-channel







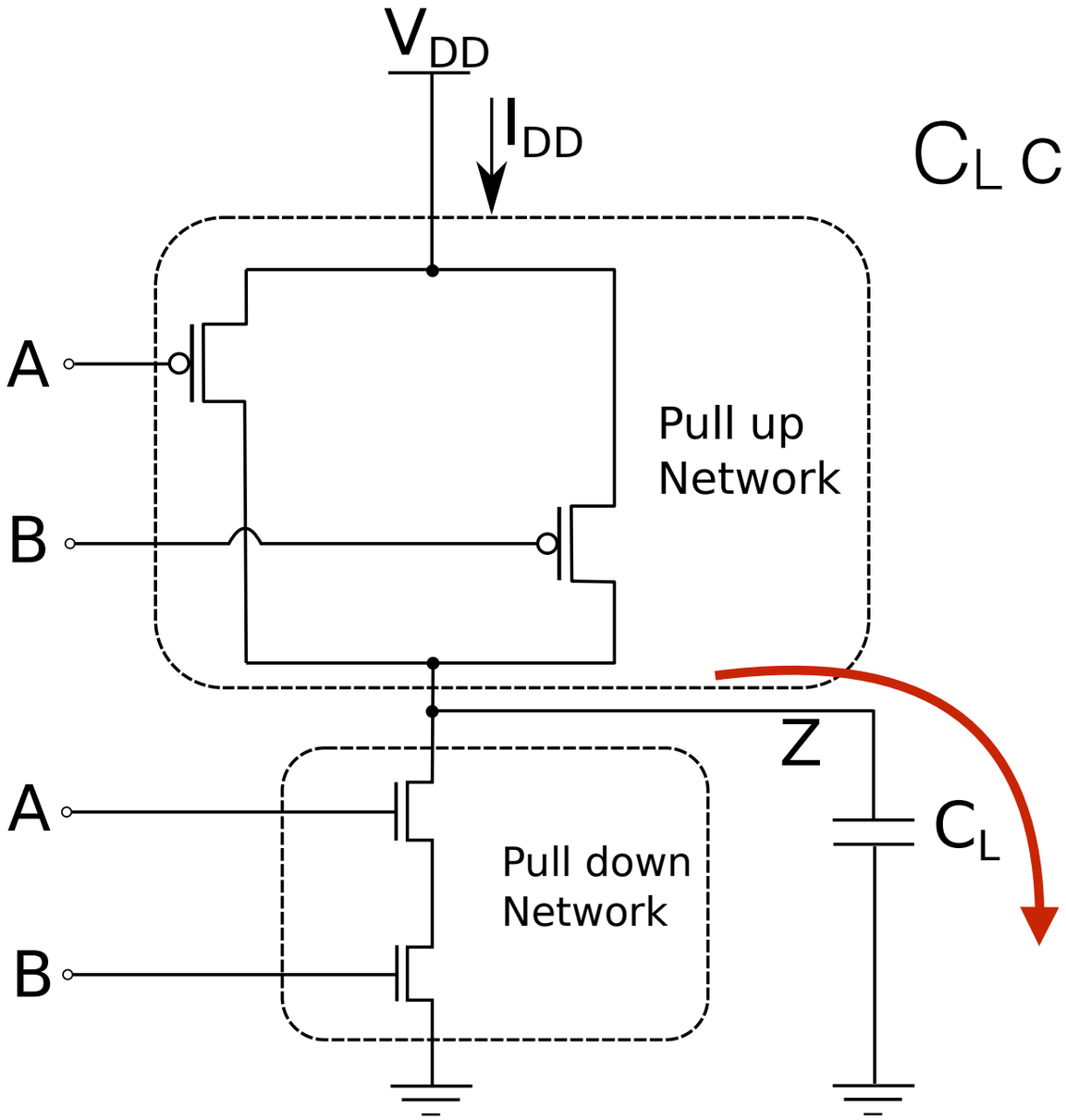

example of leakage: EM, power

# Microcontrollers “leak” information via physical side-channel

- We may target:
  - cryptographic algorithms (secret keys)
  - instructions (reverse engineering)
  - data (bus eavesdropping)

# CMOS leakage

Typical NAND gate

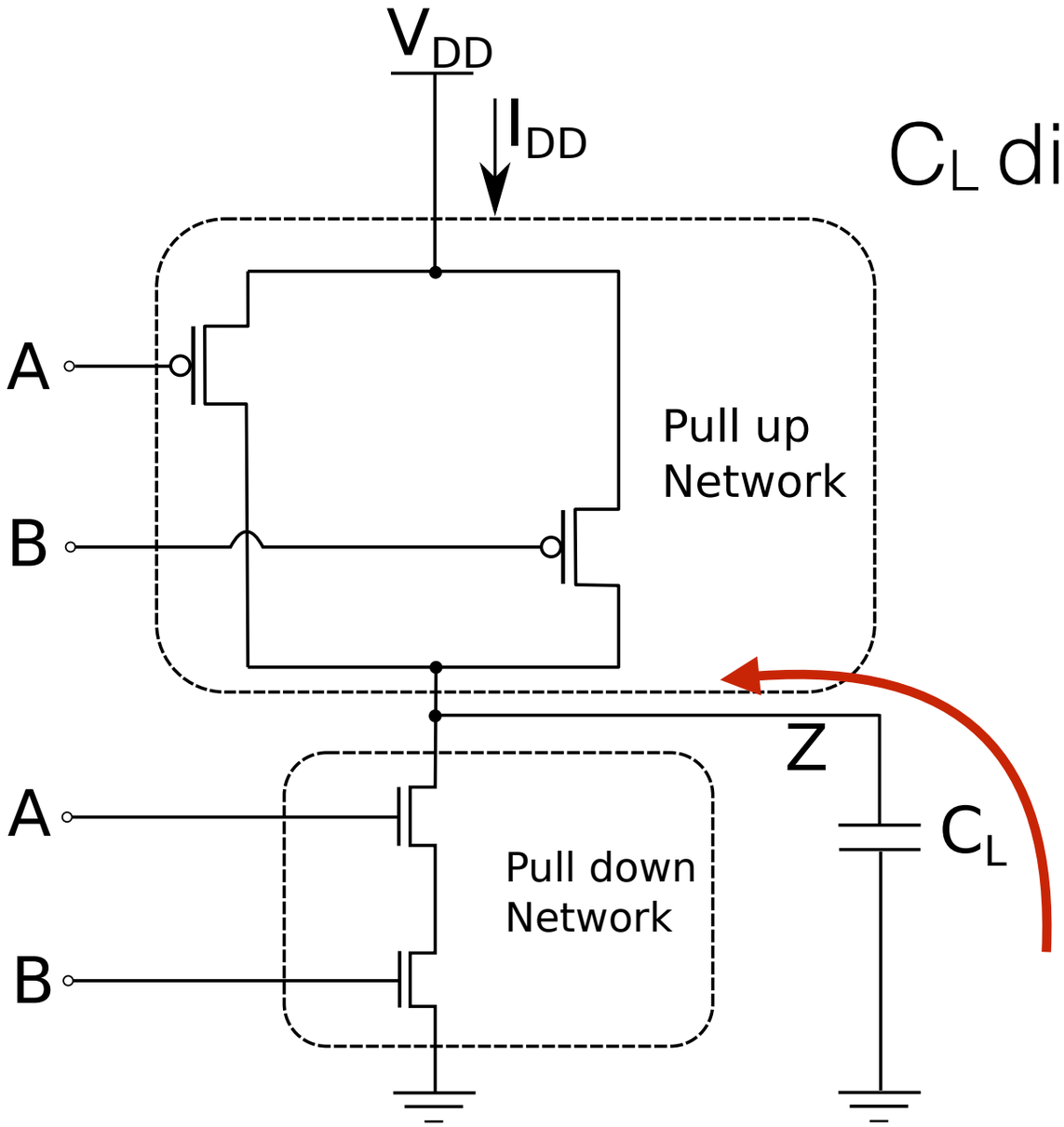



A = 0 or B = 0:

$C_L$ charges => current flows out

# CMOS leakage

Typical NAND gate

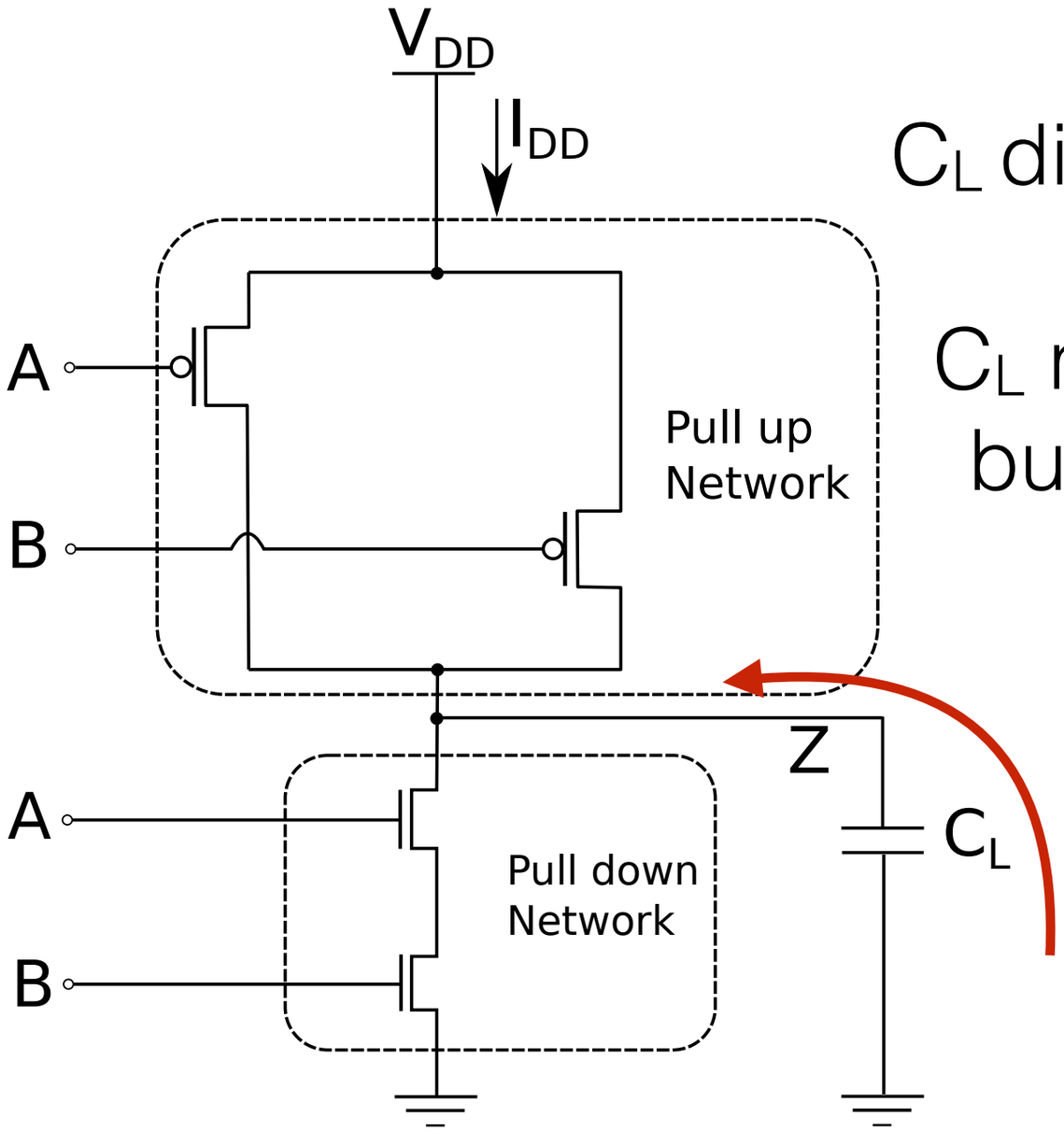



A = B = 1:

$C_L$ discharges => current flows in

# CMOS leakage

Typical NAND gate

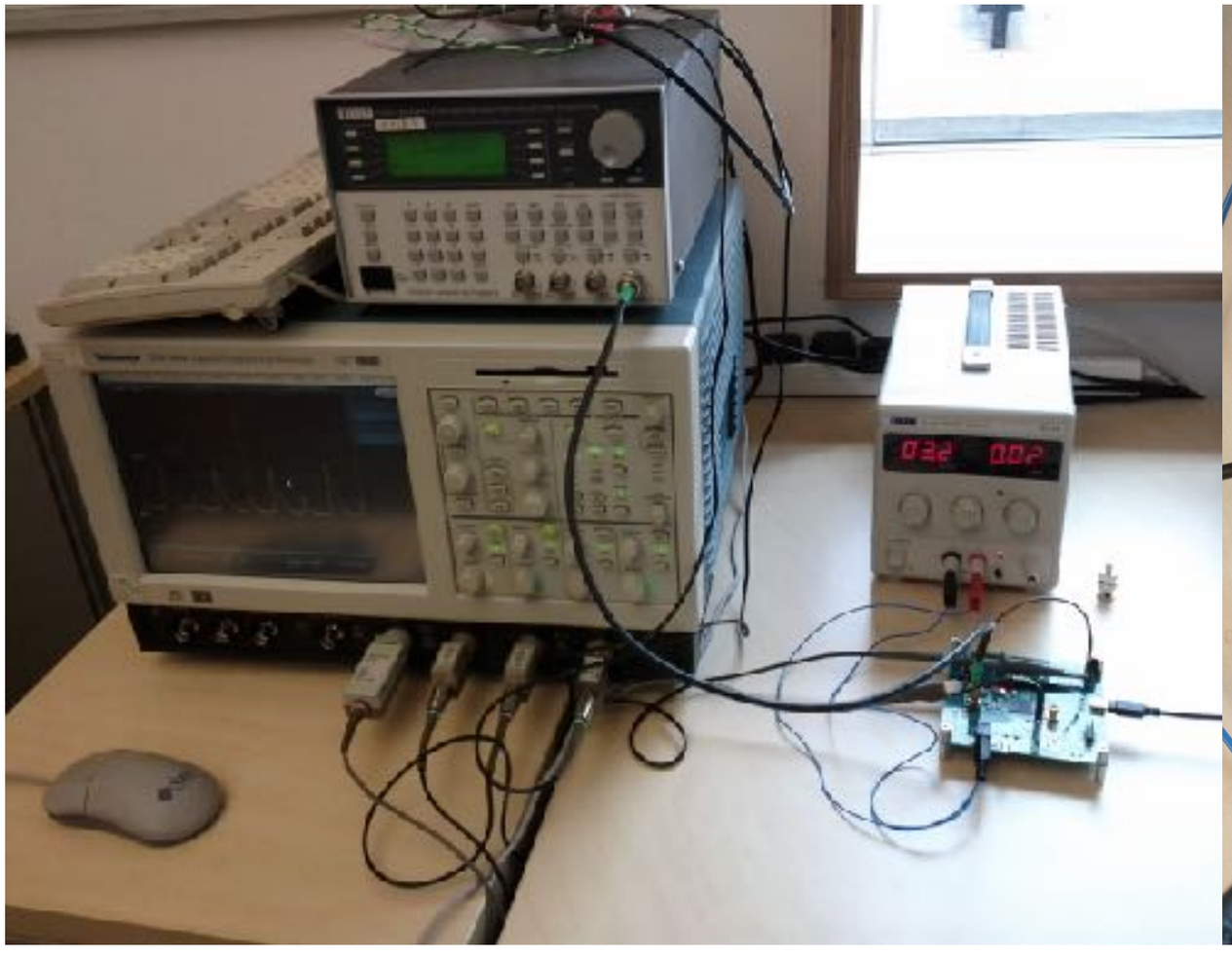


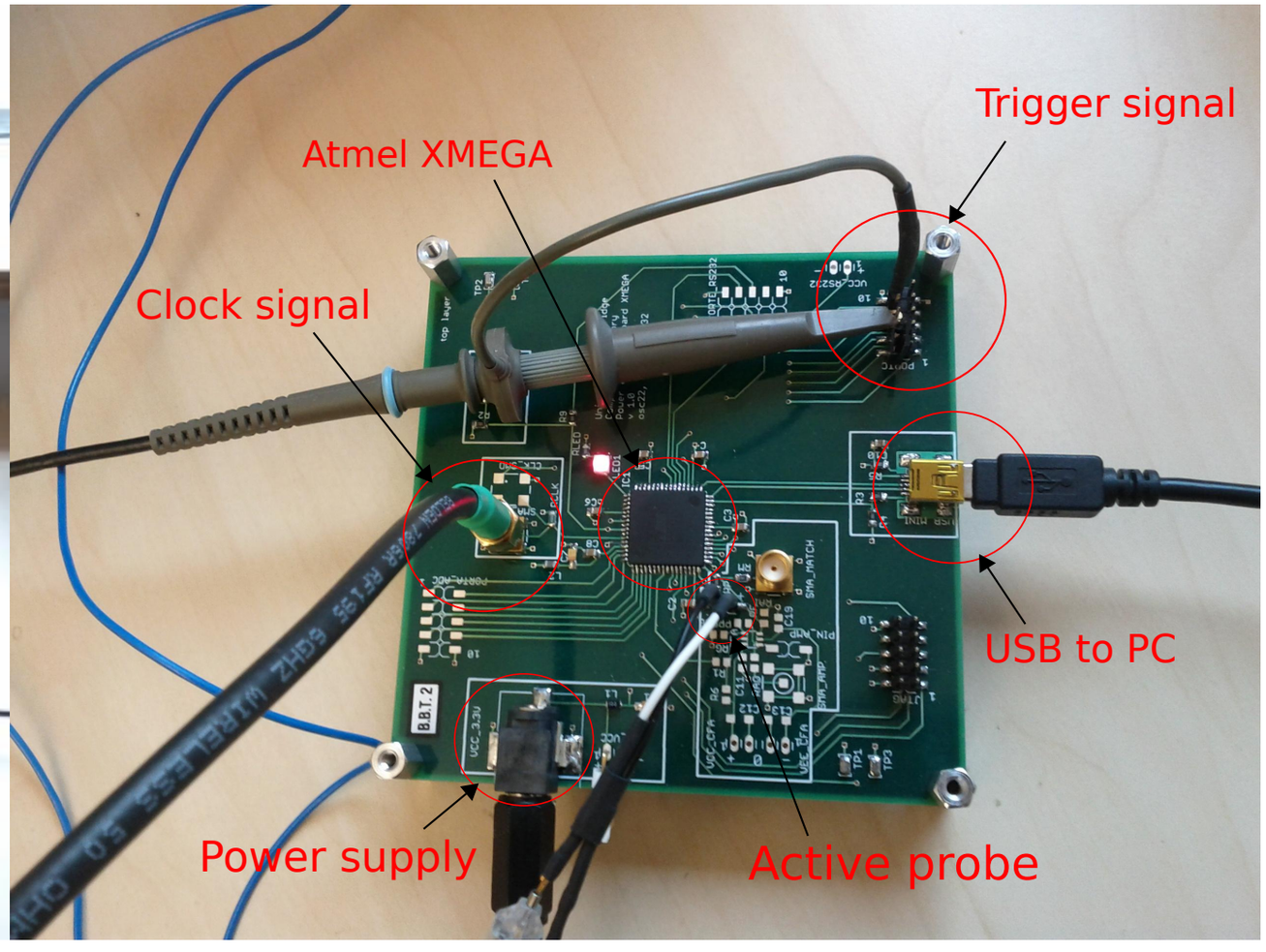

A = B = 1:

$C_L$ discharges => current flows in

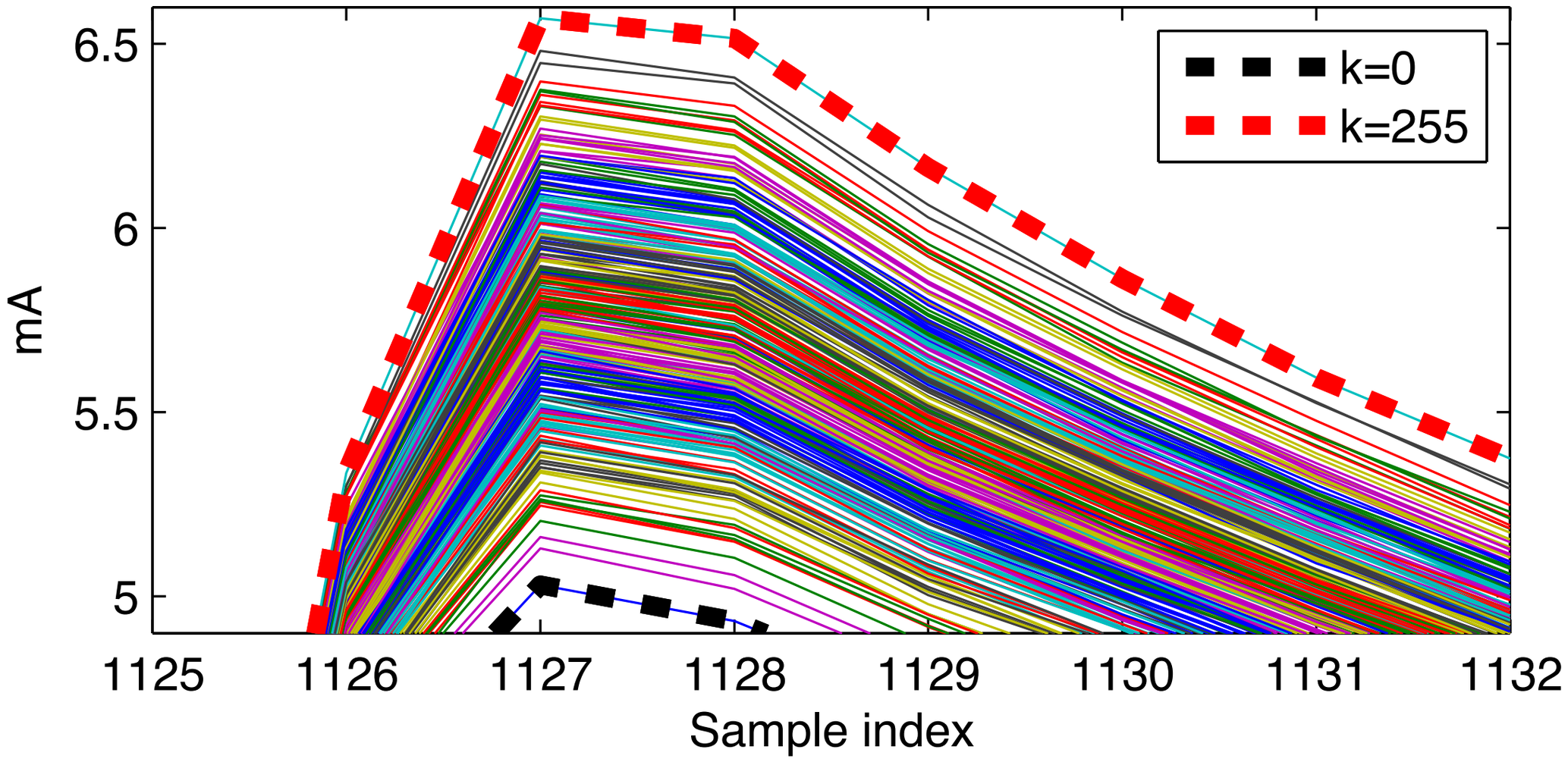
$C_L$ may be input of next gate or bus lines (large capacitance)

# Use an oscilloscope to measure power consumption of a microcontroller



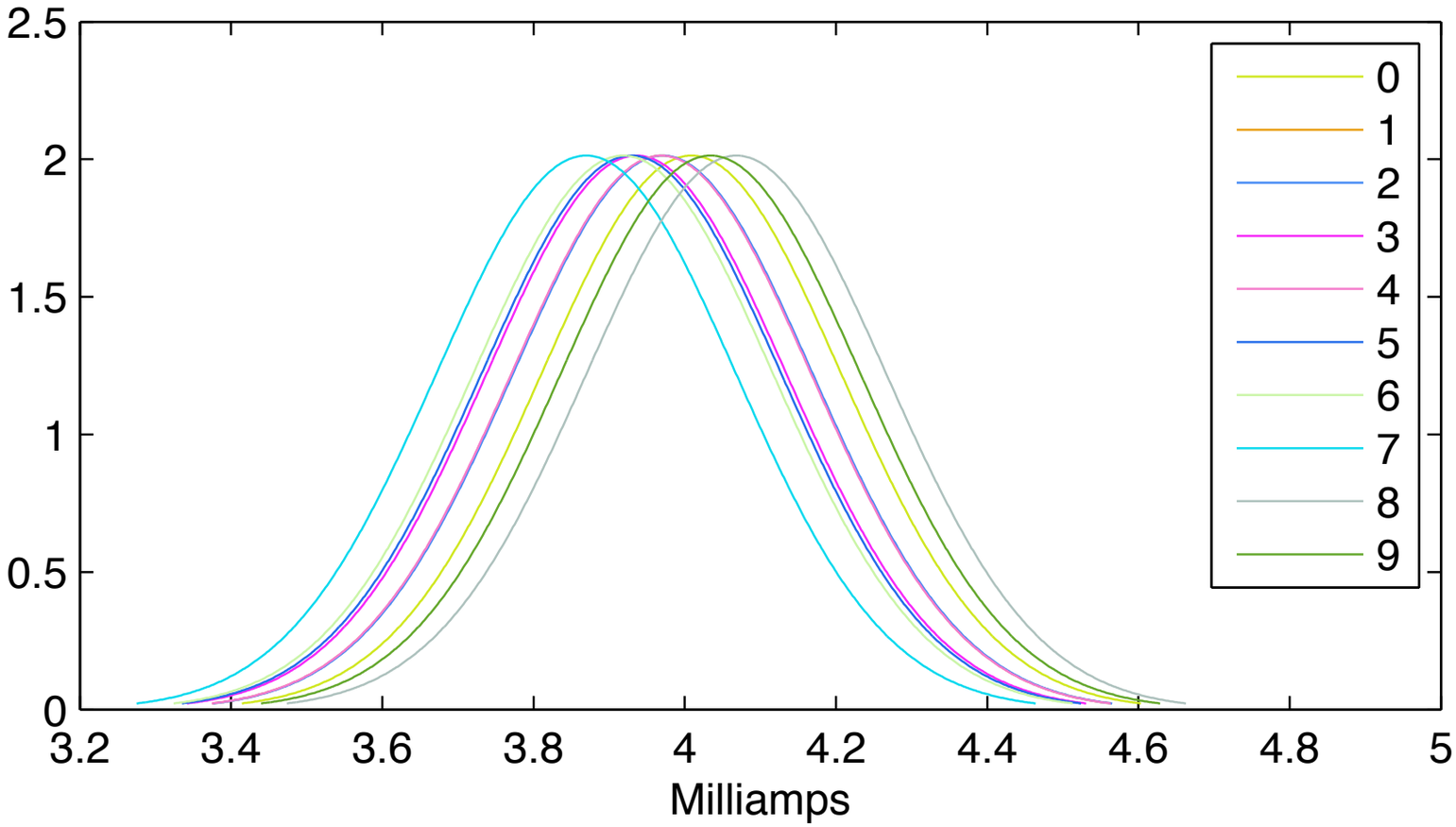


# Transition of all CMOS gates affect overall power consumption




(loading a value into a register, when the previous value on the bus was 0)

# Power consumption of loading one byte with different values




k = 0, 1, …, 9

Leakage for one sample

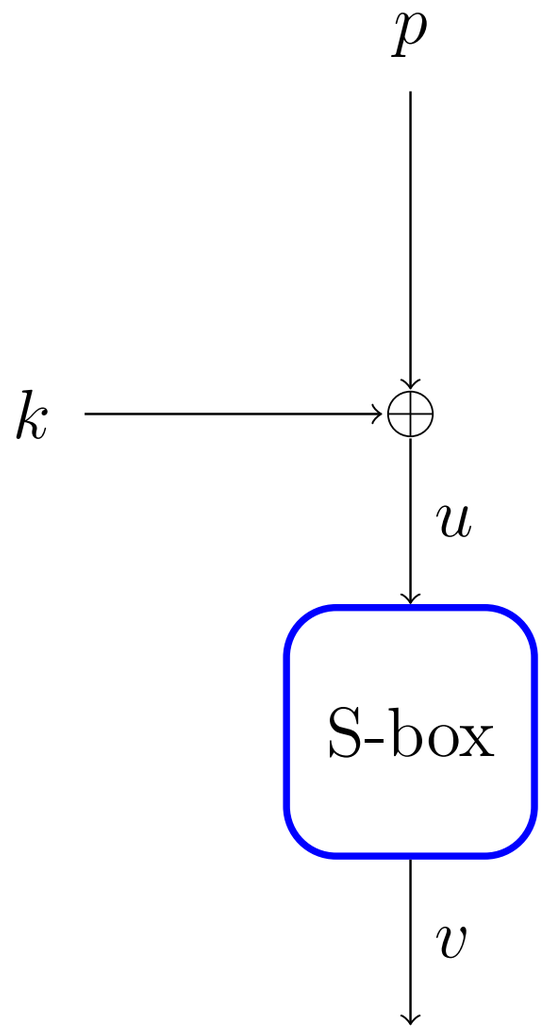
# Beginnings of power analysis

Paul Kocher, 1997

(see “Differential Power Analysis”, Kocher et al., CRYPTO ’98)

# Differential power analysis

1. Select target computation: typically the S-box lookup in a block cipher (DES, AES)

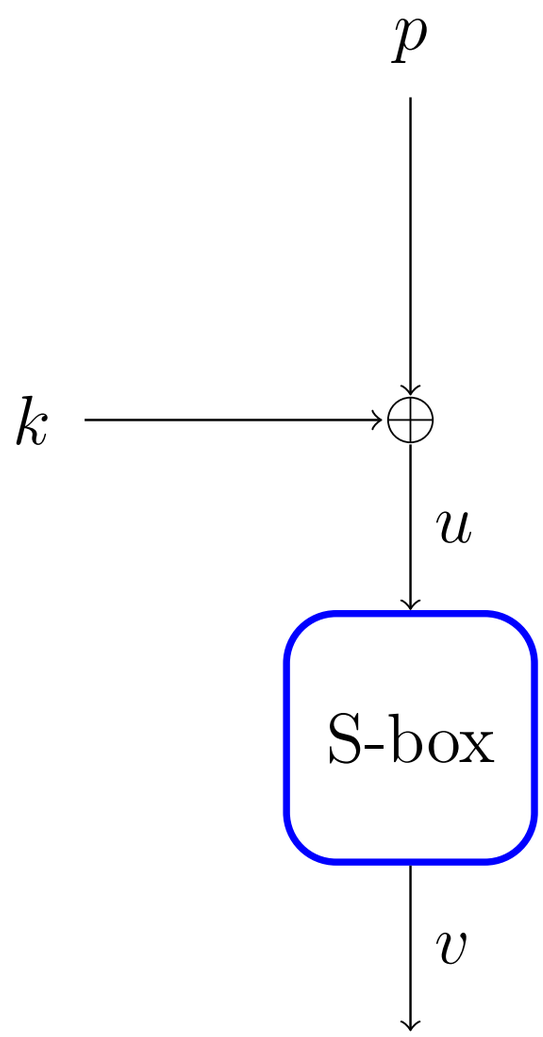


# Differential power analysis

2. Apply “divide et impera”:

a good block cipher cannot be brute-forced due to large key size: $(AES \geq 128\ bits)$

=> we target one byte at a time: reduce brute-force from $2^{128}$ to $16*2^8$ (in best case)



# Differential power analysis

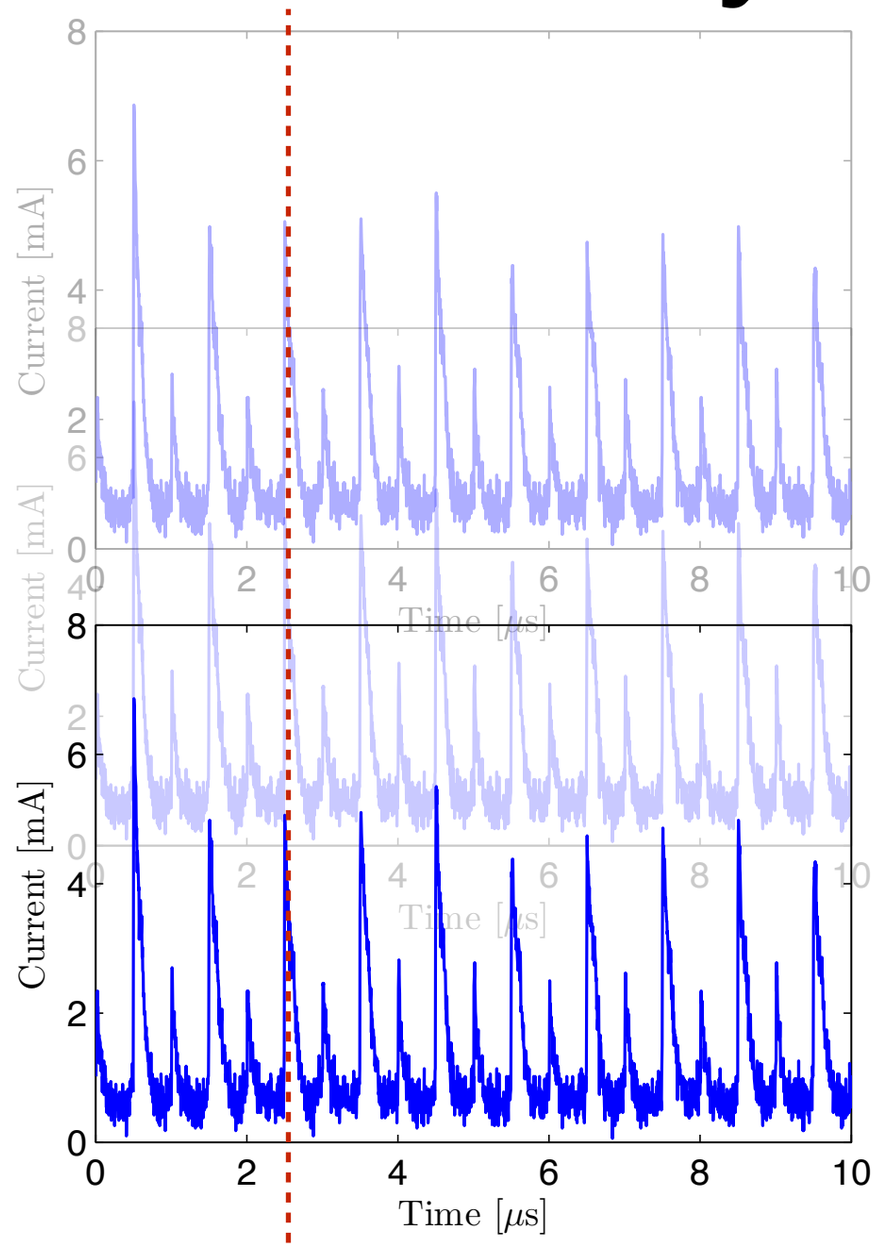
3. Take a large number (thousands, millions) of leakage traces

$x_1$

$x_2$

...

$x_N$




Typically interested in a single sample

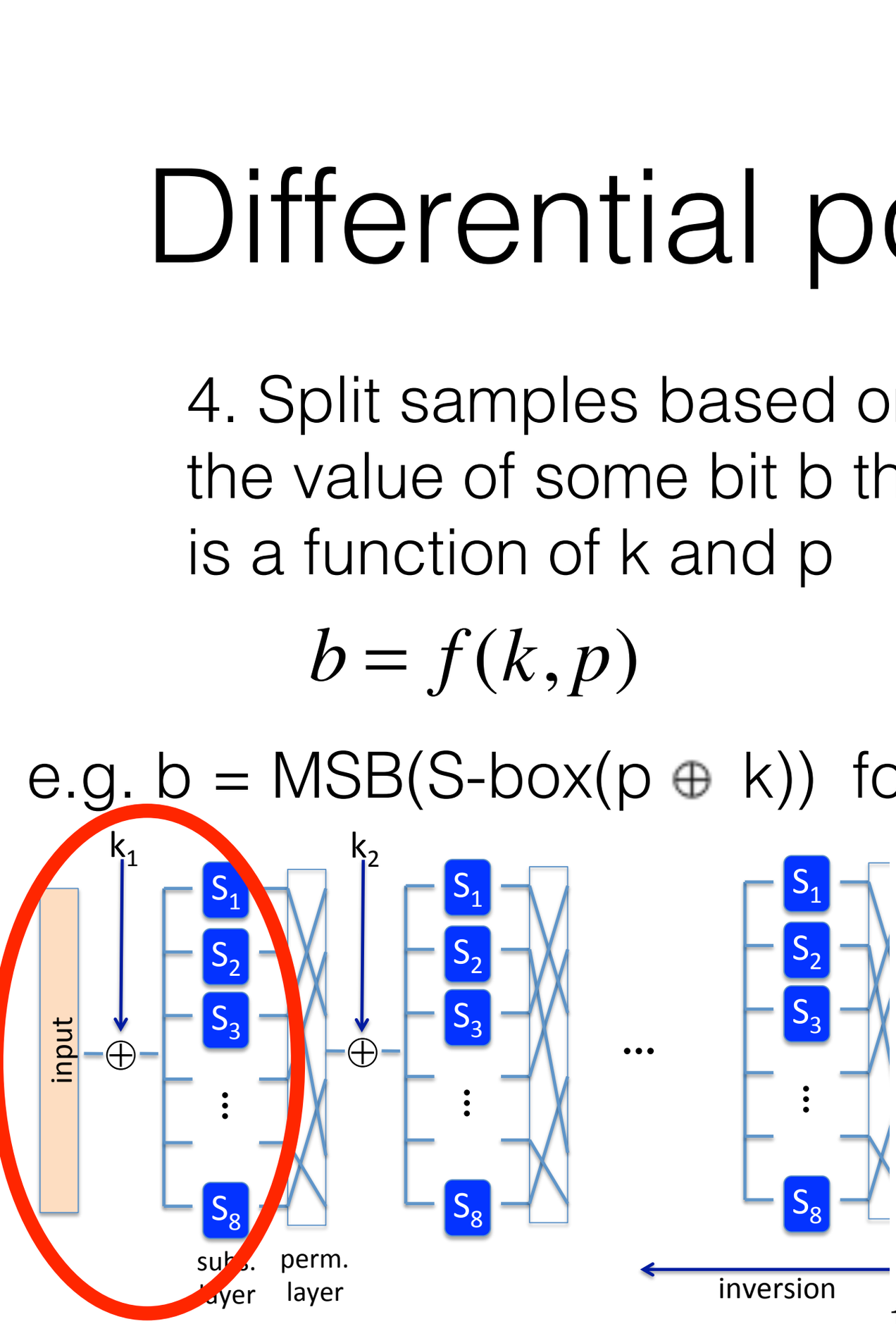
$t_i$

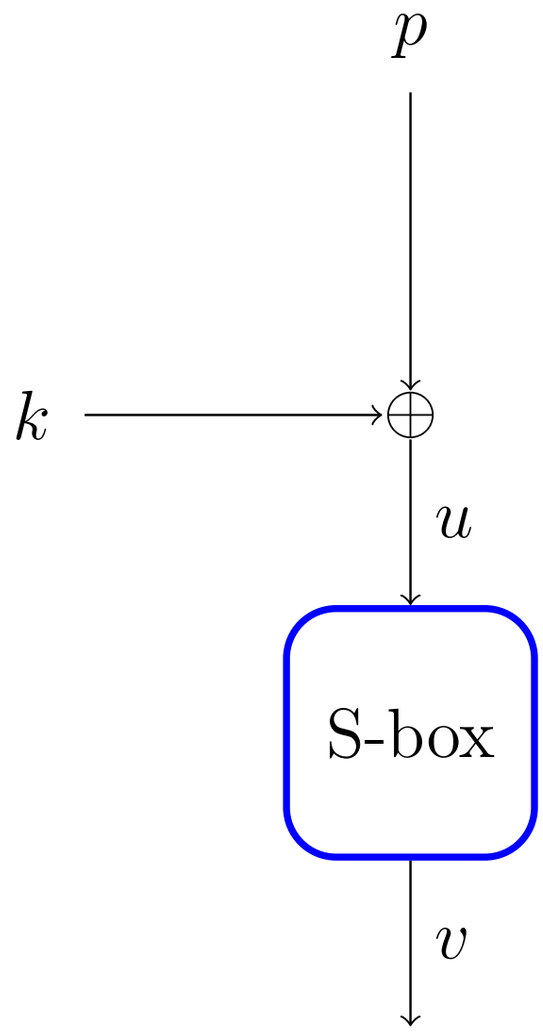
# Differential power analysis

4. Split samples based on the value of some bit b that is a function of k and p

$$b = f(k, p)$$

e.g. b = MSB(S-box(p ⊕ k)) for AES

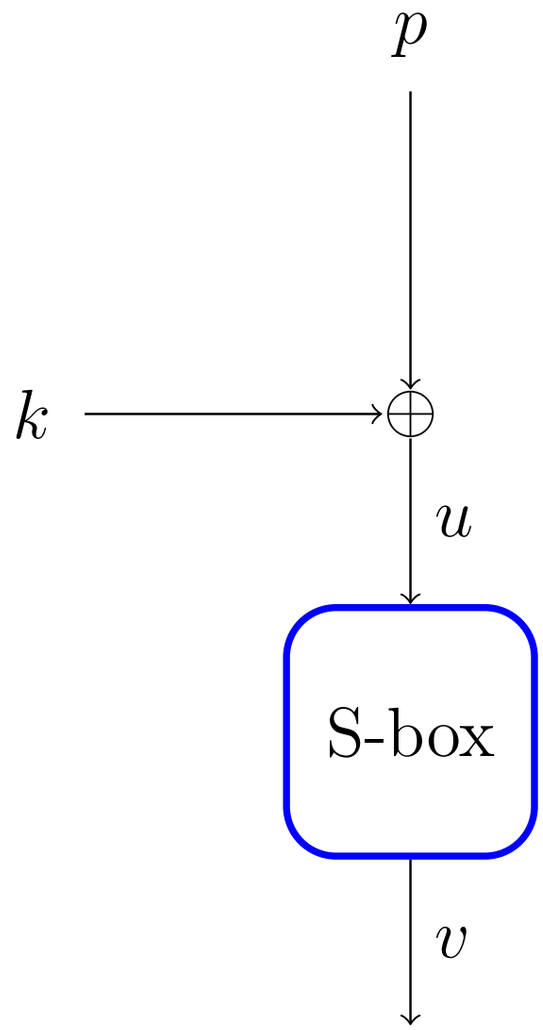


# Differential power analysis

5. Find k for which difference between average power consumption in the two groups is largest:

$$\Delta_k = (\overline{\text{power}}_{b=0} - \overline{\text{power}}_{b=1})$$



# Differential power analysis

5. Find k for which difference between average power consumption in the two groups is largest:

$$b = f(k, p)$$

★ b==0

★ b==1

k=0


$\Delta_k =$ avg(★) - avg(★) ≈0

# Differential power analysis

5. Find k for which difference between average power consumption in the two groups is largest:

$$b = f(k, p)$$

★ b==0

★ b==1

k=1


$\Delta_k =$ avg(★) - avg(★) ≈0

# Differential power analysis

5. Find k for which difference between average power consumption in the two groups is largest:

$$b = f(k, p)$$

★ b==0

★ b==1

k=42 (correct)


$\Delta_k =$ avg(★) - avg(★) =max

# Differential power analysis

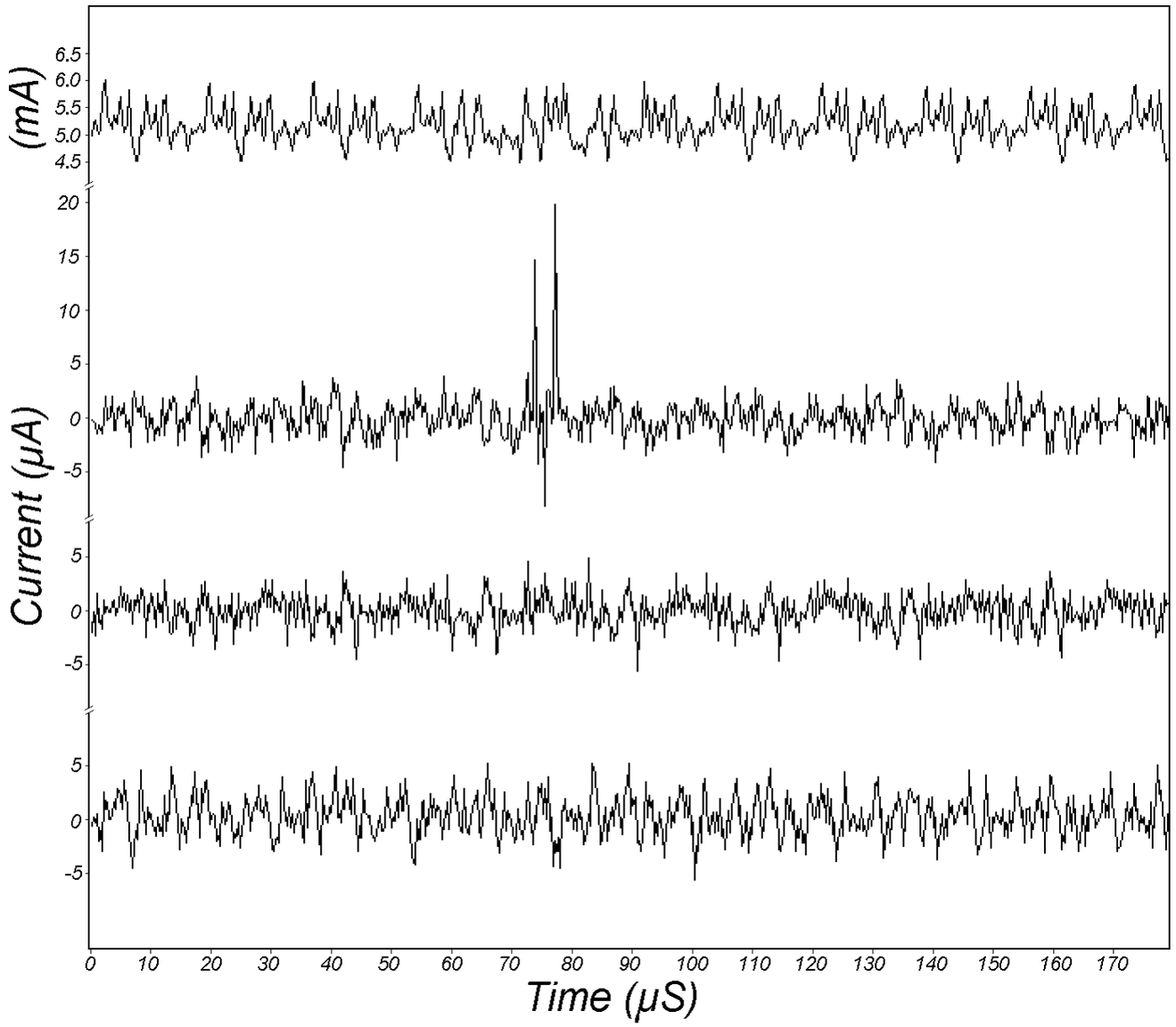



**Figure 4:** DPA traces, one correct and two incorrect, with power reference.

[Kocher et al. ]

# Correlation Power Analysis

- Test correlation between actual leakage samples (e.g. obtained with an oscilloscope) and hypothetical leakage (e.g. with Hamming Weight model and key candidate)

- Most common candidate: HW(S-box(p $\oplus$ k))

# Correlation Power Analysis

- Pearson's correlation for 2 variables X, Y:

$$\rho_{XY} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2} \cdot \sqrt{\sum_{i=1}^{N}(y_i - \bar{y})^2}}$$

- When X, Y are correlated, then $\rho_{XY}$ is high

- Idea for side-channel attacks:
  - Use actual leakage for X
  - Use expected leakage from HW model with candidate k for Y:
    Y = HW(S-box(p $\oplus$ k))
  - Compute $\rho_{XY}$ for all possible byte values k and choose k with highest $\rho_{XY}$

# Correlation Power Analysis

Example from attack on real cryptographic ASIC

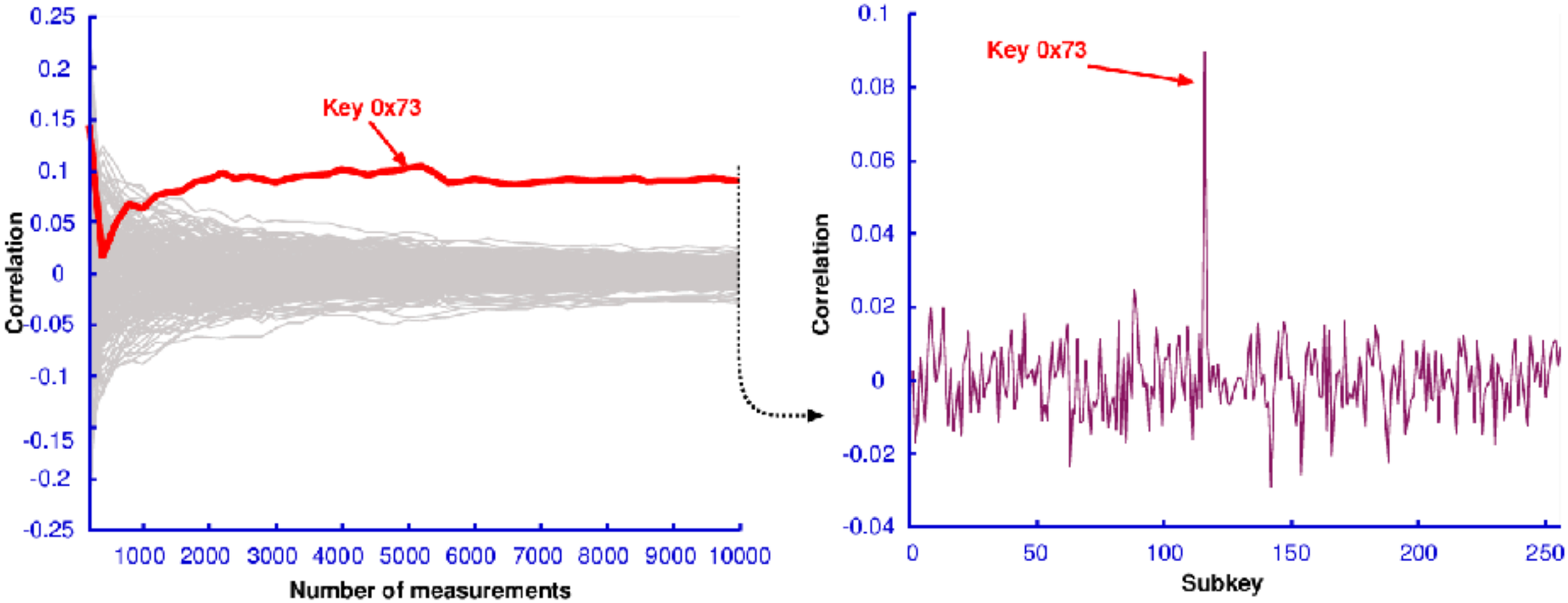



Figure from https://iis-people.ee.ethz.ch/~kgf/acacia/c3.html

Left: correlation with good key as function of number of traces (N)
Right: correlation as a function of key candidate for fixed N

# Defences and Secure IC industry

# Countermeasures

- Noise generation: try to keep the data-dependent signal below the noise floor
- Randomise computations: make it hard to align traces
- Masking: split data into several shares and compute on those such that leakage does not depend on key/data but on random values
- Dual rail and other special hardware architectures

# Industrial impact

- Development of countermeasures (hardware, software) - see Infineon, Gemalto, NXP, etc.
- Common Criteria evaluation
- Evaluation and certification laboratories
- National security evaluations
- One evaluation may cost > 100.000 EUR