Implementation attacks and countermeasures

Lejla Batina

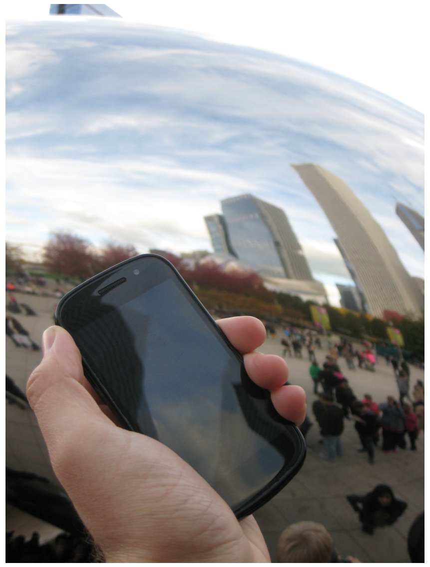
Digital Security Group,
Institute for Computing and Information Sciences (iCIS)
Radboud University, The Netherlands

Summer school on real-world crypto and privacy,
June 1, 2015
Solaris, Croatia

OUTLINE

- Implementation of security vs secure implementations
- Side-channel analysis basics
- Power analysis attacks
- EM analysis
- Countermeasures
- Fault analysis
- SCA on PKC
- Recent and future challenges
- Conclusions

EMBEDDED CRYPTOGRAPHIC DEVICES



Embedded security:
- resource limitation
- physical accessibility

THE GOALS OF THE ATTACKERS

- Secret keys/data
- Unauthorized access
- IP/piracy
- (Location) privacy
- (Theoretical) cryptanalysis [RS01]
- Reverse engineering
- Finding backdoors in chips [SW12]
- …

iCIS | Digital Security
Radboud University

PHYSICAL SECURITY BEFORE

- **Tempest** – known since early 1960s that computers generate EM radiation that leaks info about the data being processed
- In 1965, MI5: microphone near the rotor-cipher machine used by the Egyptian Embassy the click-sound the machine produced was analyzed to deduce the core position of the machines rotors
- 1979: effect of cosmic rays on memories (NASA & Boeing)
- First academic publications on SCA by Paul Kocher: 1996 (timing) and 1999 (power)
- Faults - Bellcore attack in 1997 by Boneh, DeMillo and Lipton

PHYSICAL SECURITY TODAY

- As a research area took off in the late 90's
- CHES workshop since 1999
- Many successful attacks published on various platforms and **real products** e.g. KeeLoq [EK+08], CryptoMemory [BG+12], Simon Voss (2013)
- Security evaluation labs e.g. Riscure

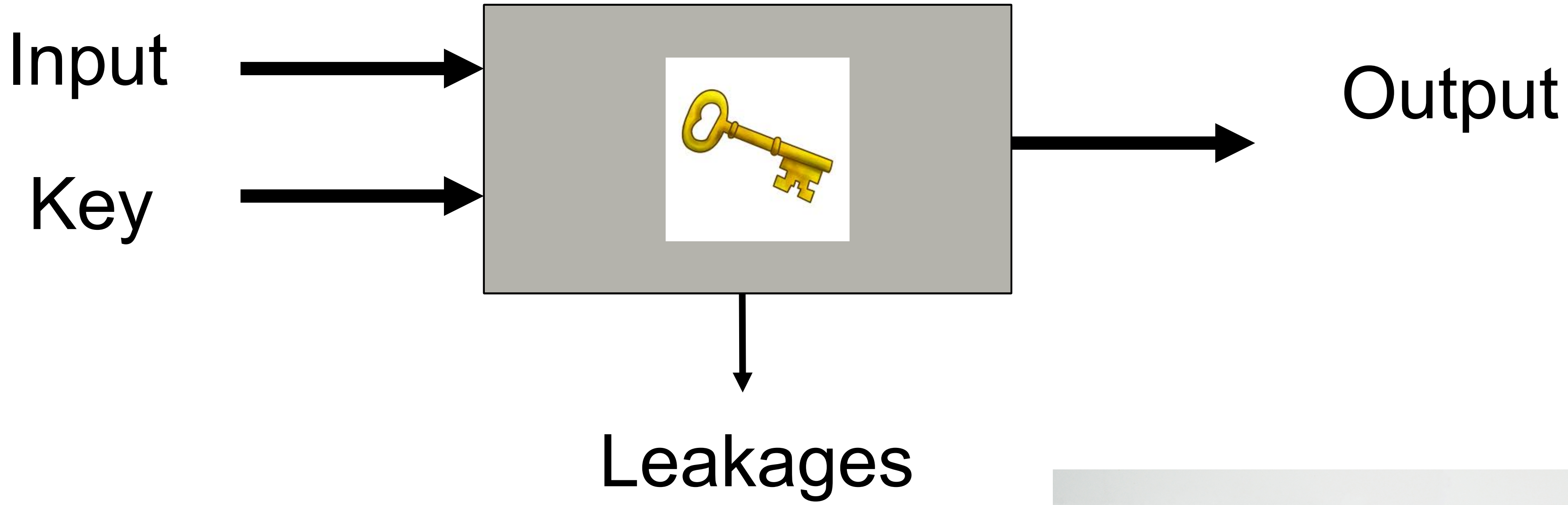
CONCEPTS OF SIDE-CHANNEL LEAKAGE

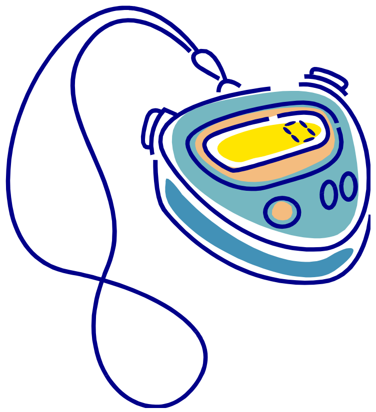
- Side-channel leakage is based on (non-intentional) physical information that enables new kind of attack
- Closely tied to implementations
- Often, **optimizations** enable leakages
  - Cache: faster memory access
  - Special tricks to boost performance
  - Square vs multiply (for PK)

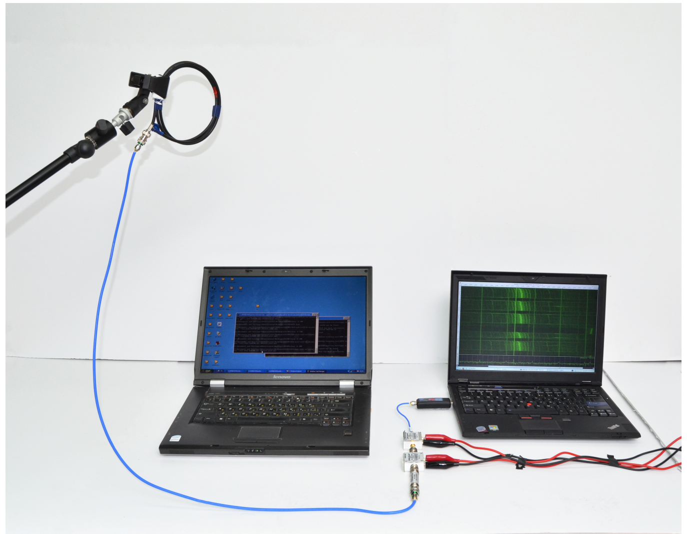
iCIS | Digital Security
Radboud University

SIDE-CHANNEL ATTACKS BASICS

SIDE-CHANNEL LEAKAGE



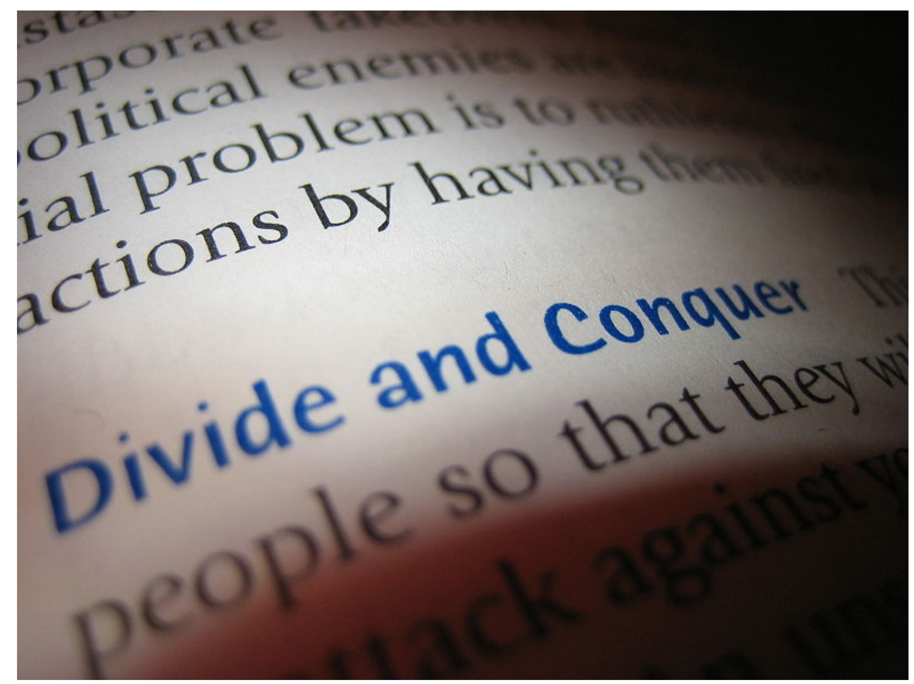




- Timing, Power, EM, Sound, Temperature, Light, …
- Observe physical quantities in the device's vicinity and use this information for secret data (key) recovery

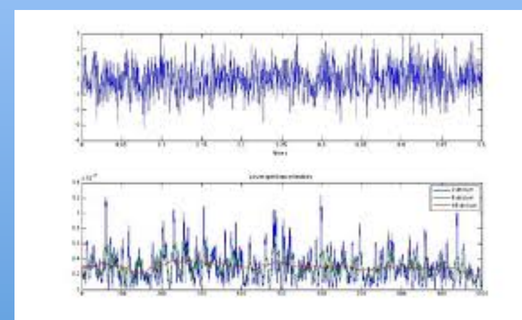
LEAKAGE IS OFTEN EXPLOITABLE

1. Due to the (dependency of leakages on) **sequences** of instructions executed
2. Due to the **data** (also sensitive!) being processed in pieces

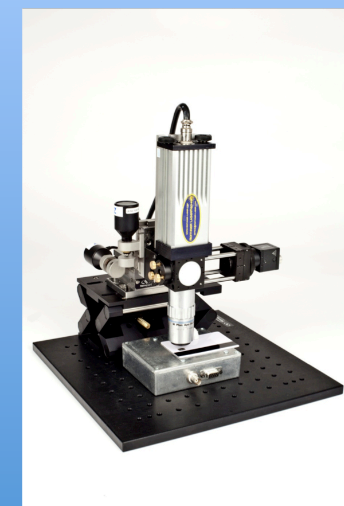


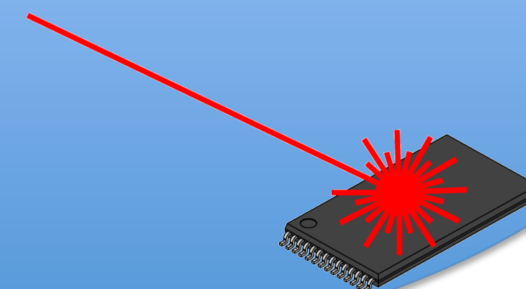
ATTACK CATEGORIES

Side-channel attacks

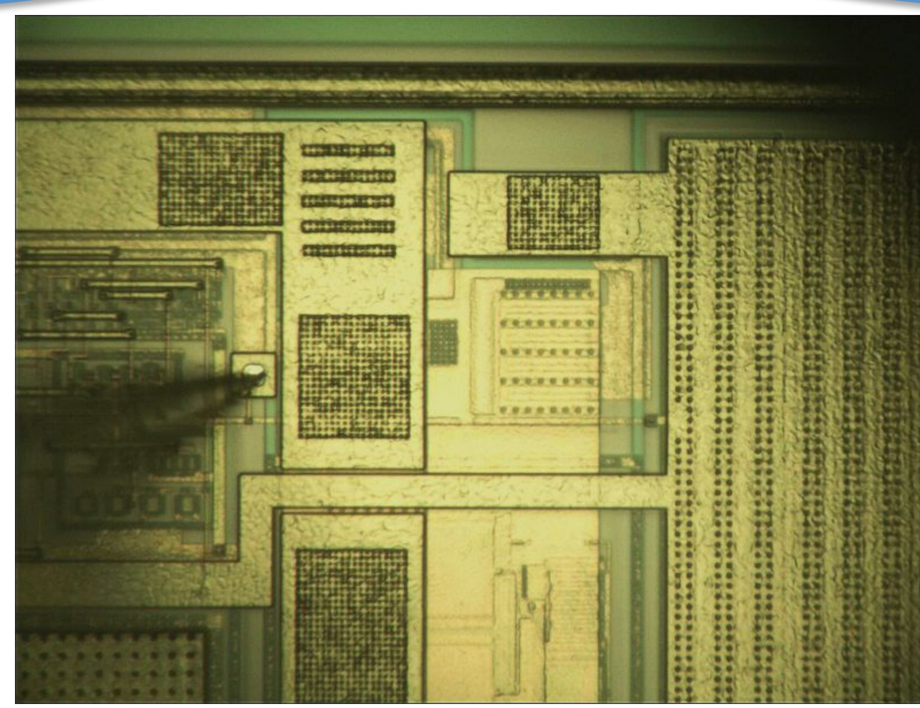


Fault attacks





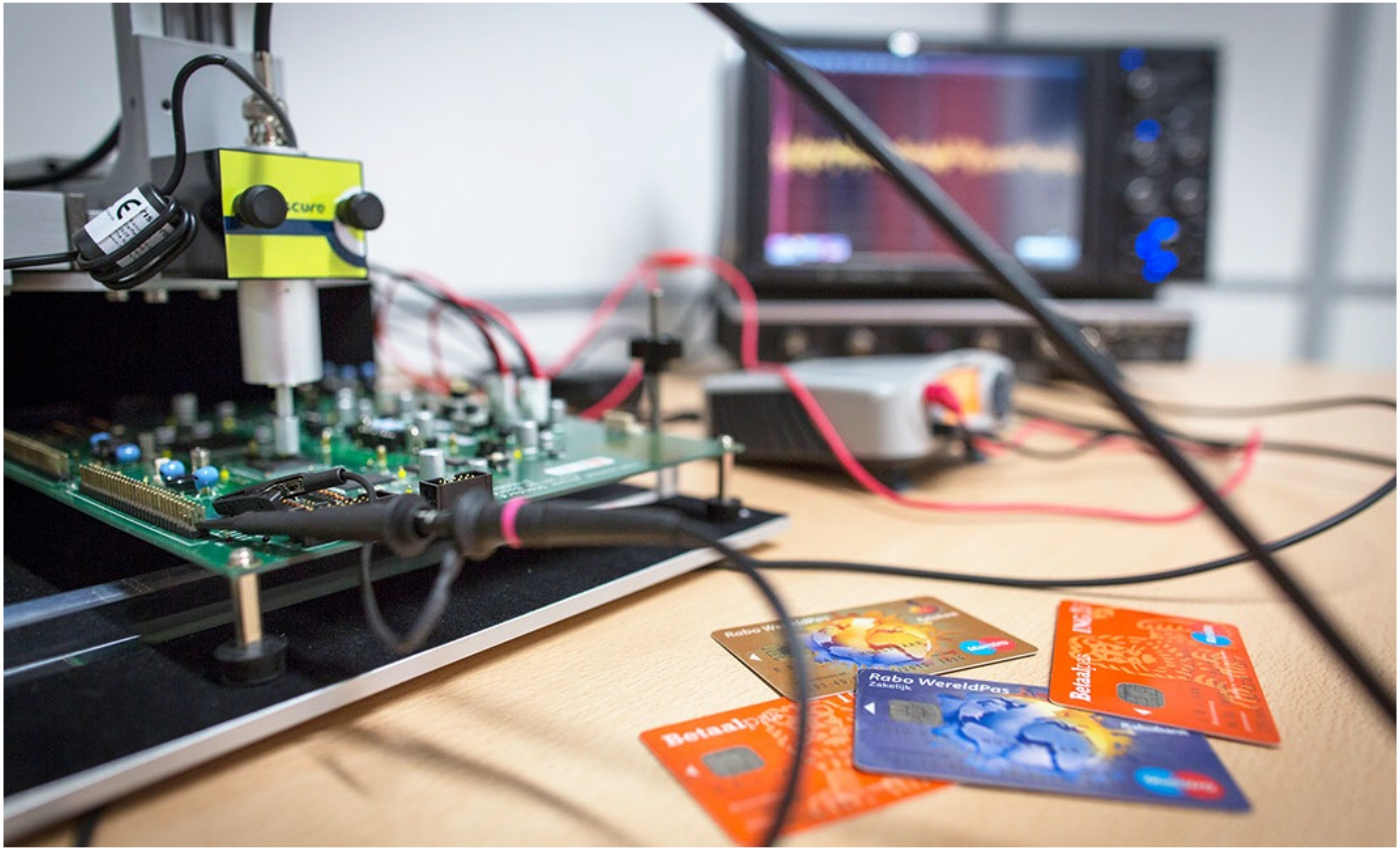
Microprobing



ATTACKERS CAPABILITIES

- "Simple" attacks: one or a few measurements - visual inspection
- Differential attacks: multiple (sometimes millions of) measurements
  - Use of statistics, signal processing, etc.
- Higher order attacks: n-th order is using n different samples
- Combining two or more side-channels
- Combining side-channel attacks with theoretical cryptanalysis

IMPLEMENTATION ATTACKS - EQUIPMENT



POWER ANALYSIS ATTACKS

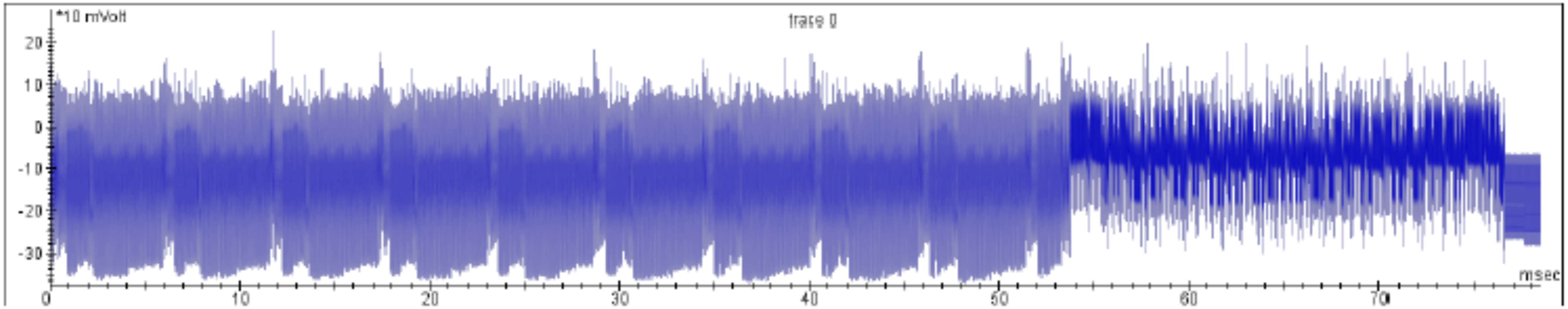
SIMPLE POWER ANALYSIS (SPA)

- Based on one or a few measurements
- Mostly discovery of data-(in)dependent but instruction-dependent properties e.g.
  - Symmetric:
    - Number of rounds (resp. key length)
    - Memory accesses (usually higher power consumption)
  - Asymmetric:
    - The key (if badly implemented, e.g. RSA / ECC)
    - Key length
    - Implementation details: for example RSA w/wo CRT
- Search for repetitive patterns

conditional operation

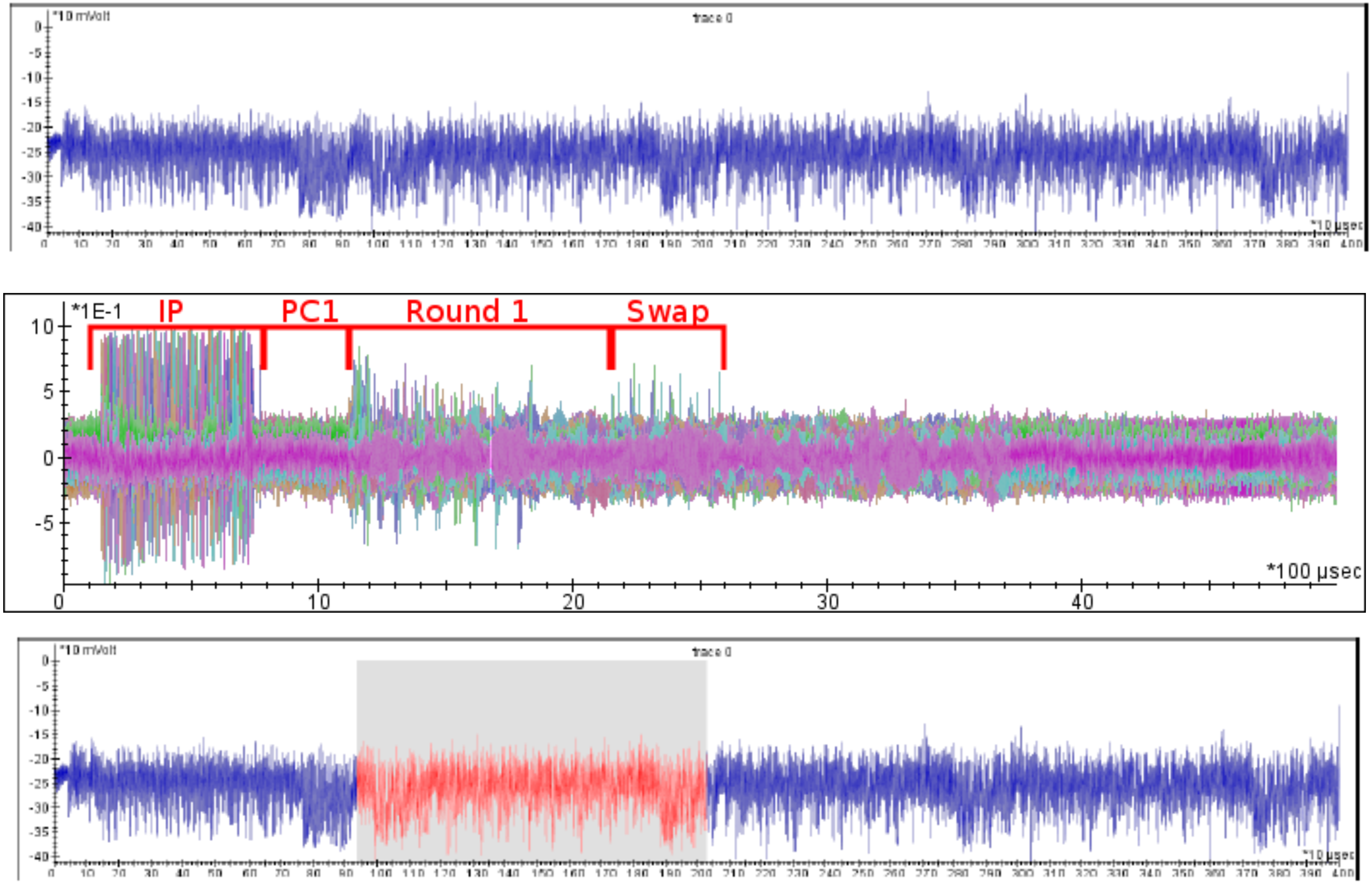
EXAMPLE

This is a power consumption trace of …

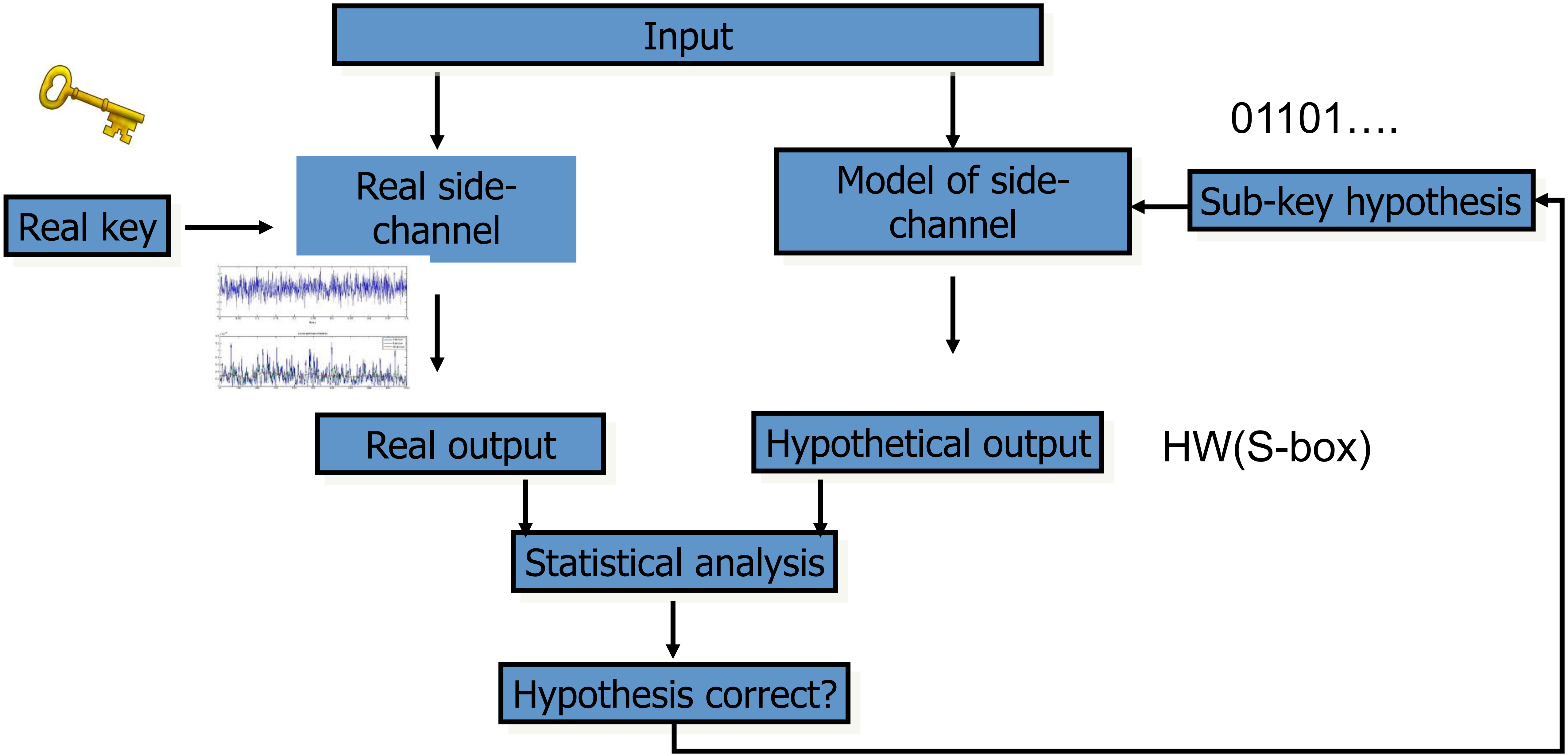


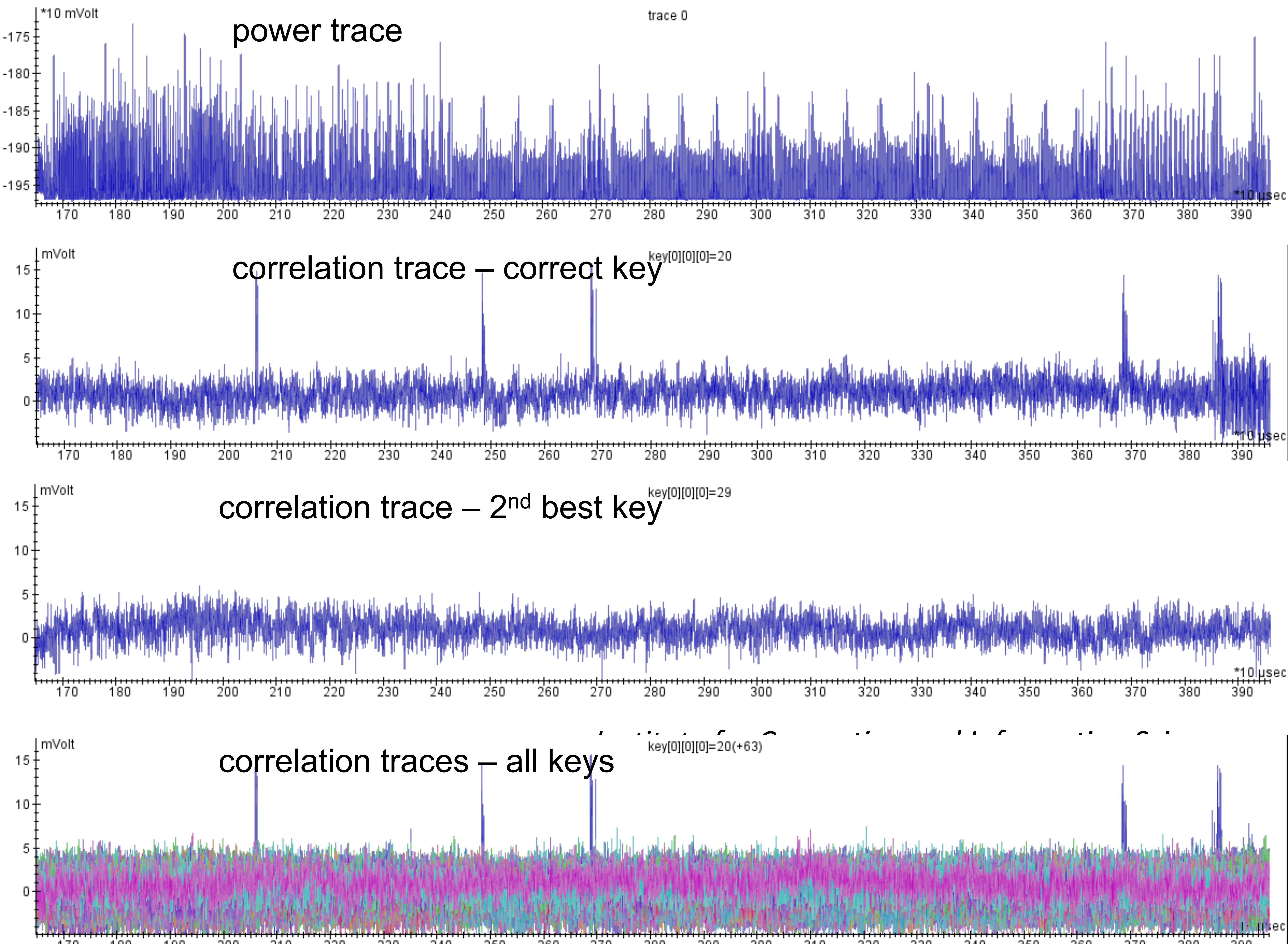
time axis

LEARNING FROM SPA– DES EXAMPLE



DIFFERENTIAL POWER ANALYSIS (DPA)



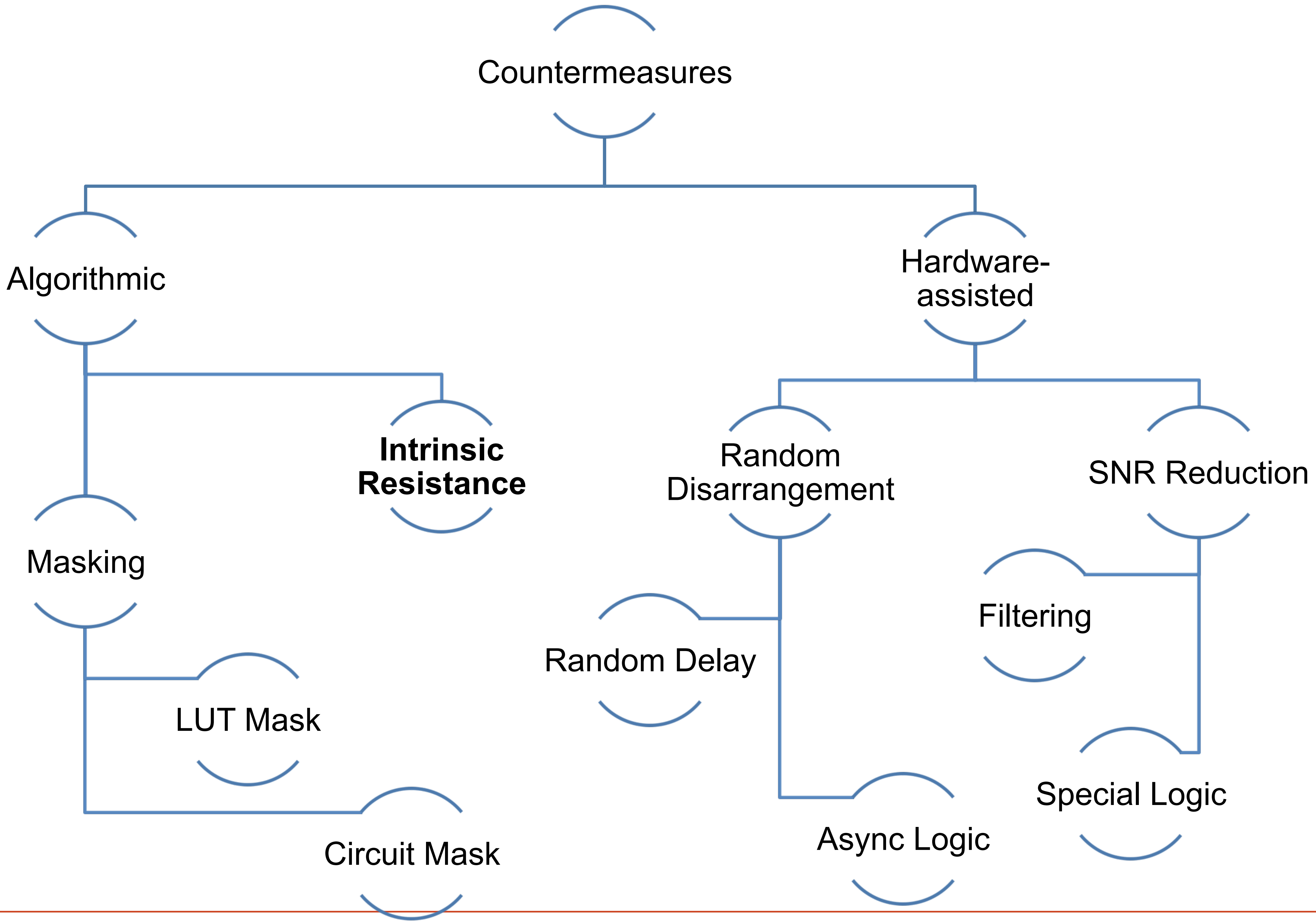

*10 mVolt
trace 0
power trace
*10 µsec
mVolt
key[0][0][0]=20
correlation trace – correct key
*10 µsec
mVolt
key[0][0][0]=29
correlation trace – 2nd best key
*10 µsec
mVolt
key[0][0][0]=20(+63)
correlation traces – all keys

LEAKAGE MODELS

- Transition = Hamming distance model
  - Counts number of 0->1 and 1->0 transitions
  - Assuming same power consumed for both, ignores static power consumption
  - Typically for register outputs in ASIC's
  - HD(v_0, v_1)=HW(v_0 xor v_1)
  - Requires knowledge of preceding or succeeding v_i
- Hamming weight model
  - Typical for pre-charged busses
- Weighted Hamming weight/distance model
- Signed Hamming distance (0->1 neq 1->0)
- Dedicated models for combinational circuits

SIDE-CHANNEL ATTACKS: COUNTERMEASURES

SIDE-CHANNEL ATTACKS COUNTERMEASURES



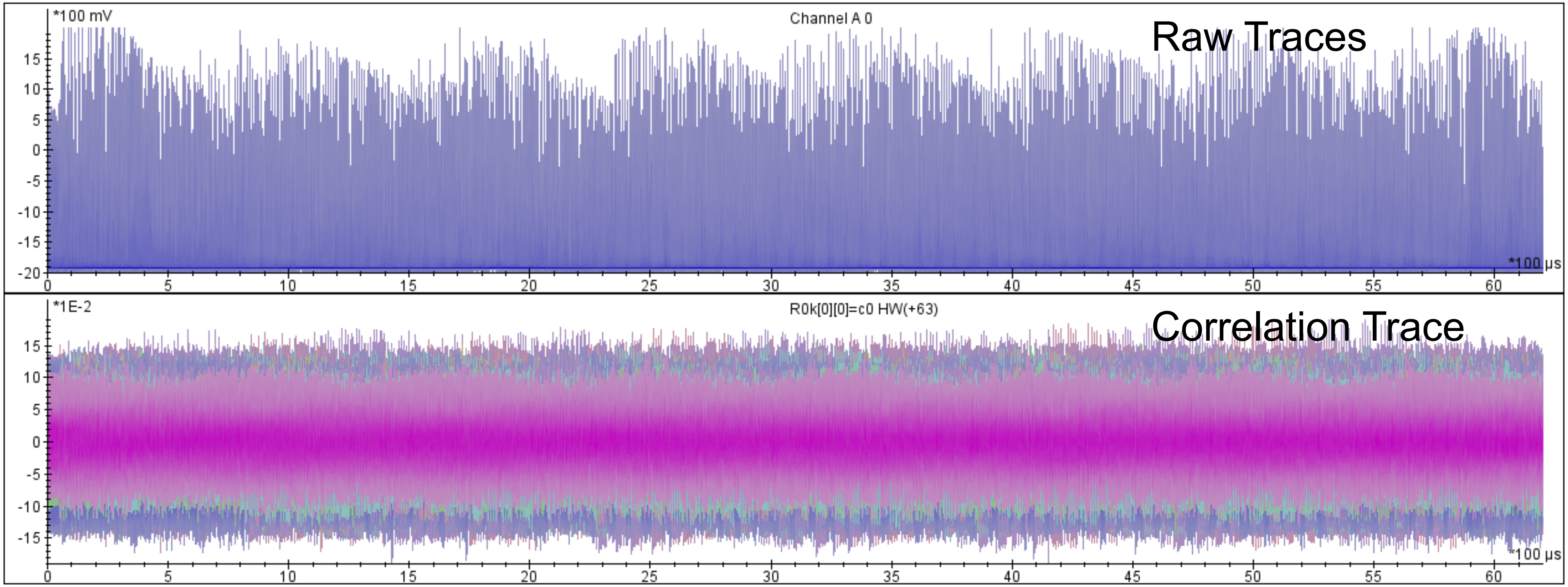
SOFTWARE COUNTERMEASURES

- Time randomization: the operations are randomly shifted in time
  - use of NOP operations
  - add random delays
  - use of dummy variables and instructions (sequence scrambling)
  - data balancing (a data element is represented redundantly to make H.w. constant)
- Permuted execution
  - rearranged instructions e.g. S-boxes
- Masking techniques

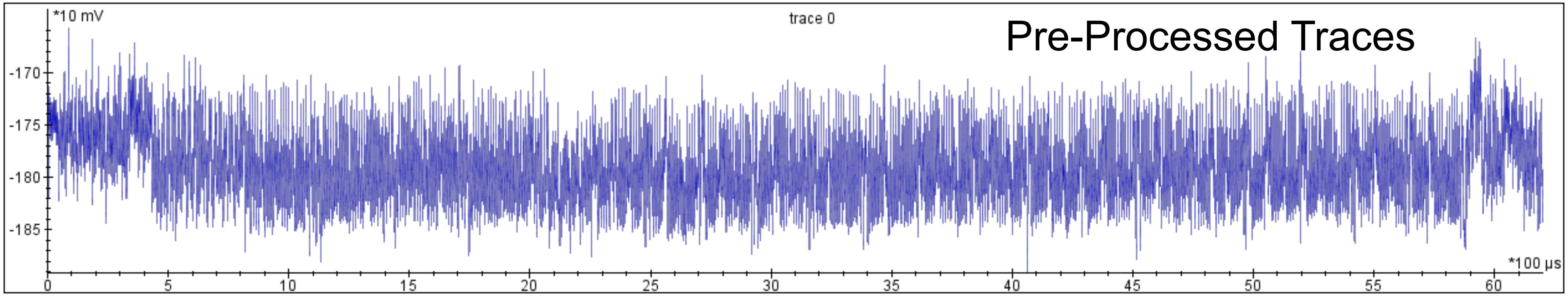
HARDWARE COUNTERMEASURES

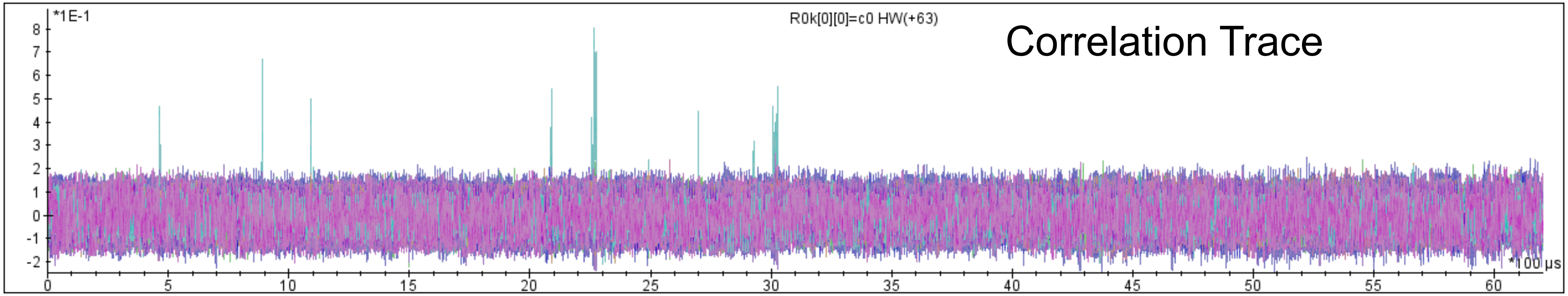
- Noise generation
  - HW noise generator requires the use of RNG
  - total power is increased (problem for handheld devices)
- Power signal filtering
  - ex.: RLC filter (R-resistor, C-capacitor, L-inductor) smoothing the pow. cons. signal by removing high frequency components
  - one should use active comp. (transistors) in order to keep power cons. relatively constant - problem for mob. phones
- Novel circuit designs
  - special logic styles

THE IMPACT OF NOISE



PREPROCESSING





EM SIDE CHANNELS

EM HISTORY

- Compromising emanations discovered many years ago – TEMPEST
- Not exclusive to crypto devices – e.g. vulnerability to EM analysis was found in some voting machines in 2006 in The Netherlands:
- Van Eck in 1985: video display units generate EM that can be reconstructed up to 1 km
- Markus Kuhn. Compromising emanations: eavesdropping risks of computer displays

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf

EM AS SIDE-CHANNEL

- Each current-carrying component produces EM field
- EM is a 3-dim vector field as a function of time
- Probe can act as a coil:
  - a small magnetic coil is used allowing precise positioning
- SEMA and DEMA
- Focusing also on frequency analysis
- Usually more difficult than PA – the issue of antenna positioning, etc.
- **More leakage available: locally-based leakage**

CLASSICAL VS SIDE-CHANNEL CRYPTANALYSIS

- Knowledge:
  - Input/output pairs
  - Input/output pairs + some leakage
- Applicability
  - Generally applicable
  - Limited to certain implementation

Combining both could be beneficial when access to side-channel info is restricted!

EM COUNTERMEASURES

- Faraday cage
  - A Faraday Cage (shield) can be described as an enclosure created by conducting materials that blocks external electric fields (both static and non-static)
- Design for low power => reducing EM signals
- Asynchronous design
- Dual rail logic

ADVANCED ATTACKS

TEMPLATE ATTACKS [CRR02]

- Strongest form of SC attacks in an information theoretic sense
- Assumption that the same device (as the one under attack) is available
- Precisely modeling noise instead of eliminating it – similarly to techniques in signal detection and estimation
- Suitable when only a few samples or measurements are available i.e. adversary has to work with far fewer signals
  - Stream ciphers
  - Fast hardware crypto modules
  - EM measurements
- Consist of 2 phases:
  - Characterization or profiling phase (building templates)
  - Template matching or Key recovery

TEMPLATE ATTACKS: ASSUMPTIONS

- Strong assumptions on adversary
- Find templates for certain sequences of instructions or execute the same code for different values of key bits:
  - Templates consist of the mean signal and noise probability distribution (noise characterization) for that particular case
  - Templates are created for all sub-key values (e.g. bytes) consisting of a vector of means and the noise covariance matrix
- Maximum-likelihood rule finds the right key

HIGHER-ORDER DPA: THE IDEA

- As mentioned in the original DPA paper:

"Of particular importance are high-order DPA functions that combine multiple samples from within a trace."

- 2nd order DPA attack: Messerges in 2000 [Mes00b]

```
W1 (PTI)
{
A: Result = PTI xor SecretKey
…
return CTO
}
```

1st order DPA applies

```
W2 (PTI)
{
B: RandomMask = rand()
mPTI = PTI xor RandomMask
C: Result = mPTI xor SecretKey
…
return CTO
}
```

2nd order DPA applies

FAULT ANALYSIS

HISTORY

- 1978: one of the first examples fault injection was unintentional, discovered by May and Woods (radioactive particles)
- 1979: effect of cosmic rays on memories (NASA & Boeing)
- 1992: use of laser beam to charge particles on microprocessors, discovered by Habing
- 1997: 1st academic pub. by Boneh, DeMillo, and Lipton showing what's possible with a single fault [BDL97]
- 1997: differential fault analysis on secret-key cryptosystems by Biham and Shamir [BS97]
- 2002: 1st pub. implementing Bellcore attack [AB+12]
- 2003: 1st FDTC workshop

ATTACKER GOALS

- Insert computational fault
  - Null key
  - Wrong crypto result (Differential Fault Analysis - DFA)
- Change software decision
  - Force approval of false PIN
  - Reverse life cycle state
  - Enforce access rights
- …

COUNTERMEASURES

Generic

- Correctness check: encrypt twice
- Random delays: limits the precision
- Masking:
  - Linear secret sharing complicates probing wires of the device
  - Adversary cannot predict the effect of the injected fault

Hardware

- Supply voltage, frequency detectors
- Active shields
- Redundancy: duplication of hardware blocks
- Dual rail implementations
- *(m-of-n) encoding:* each bit is represented by *n* wires, from which exactly *m* carry a 1

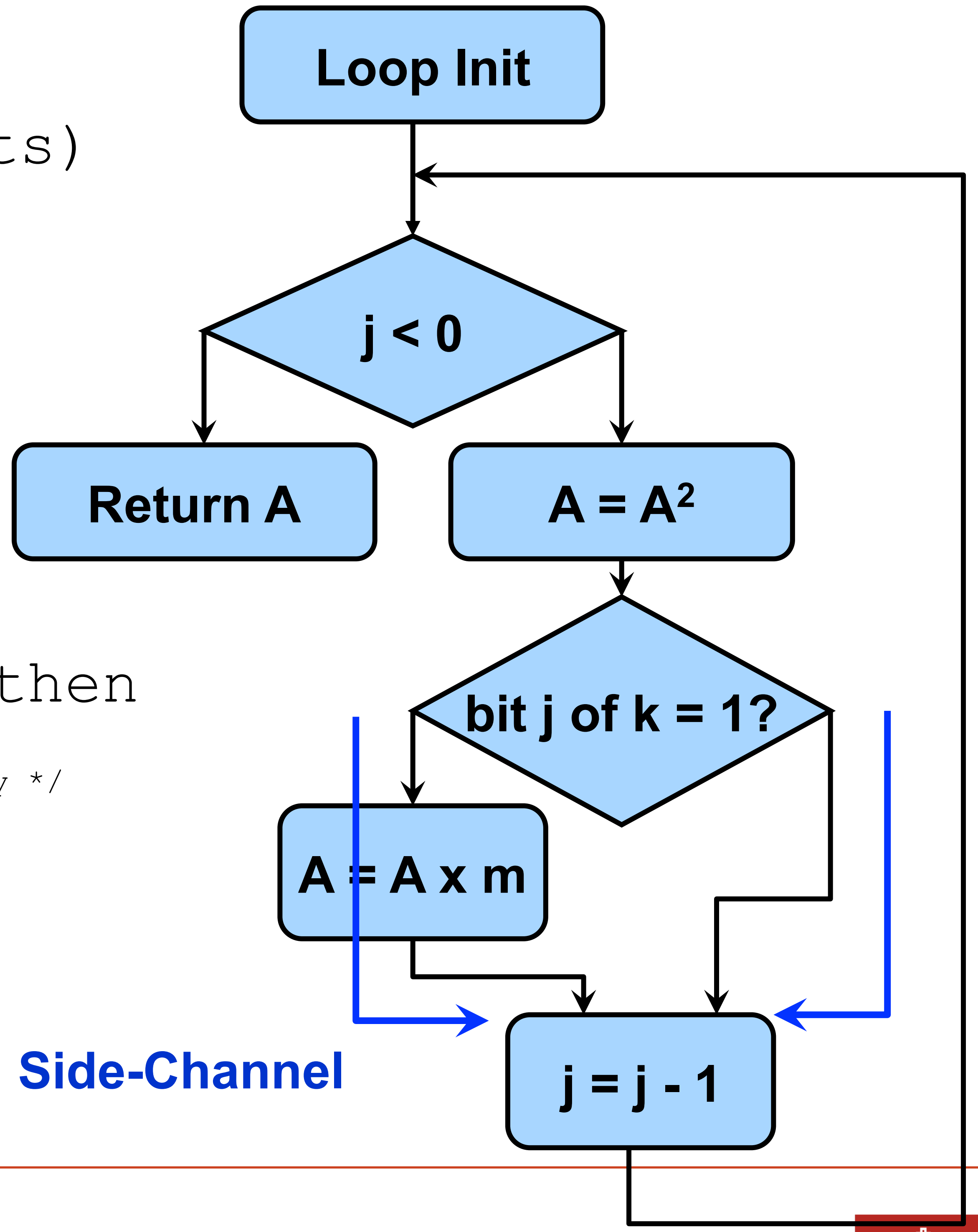
SIDE-CHANNEL ANALYSIS ON PKC

INSECURE RSA IMPLEMENTATION

RSA modular exponentiation

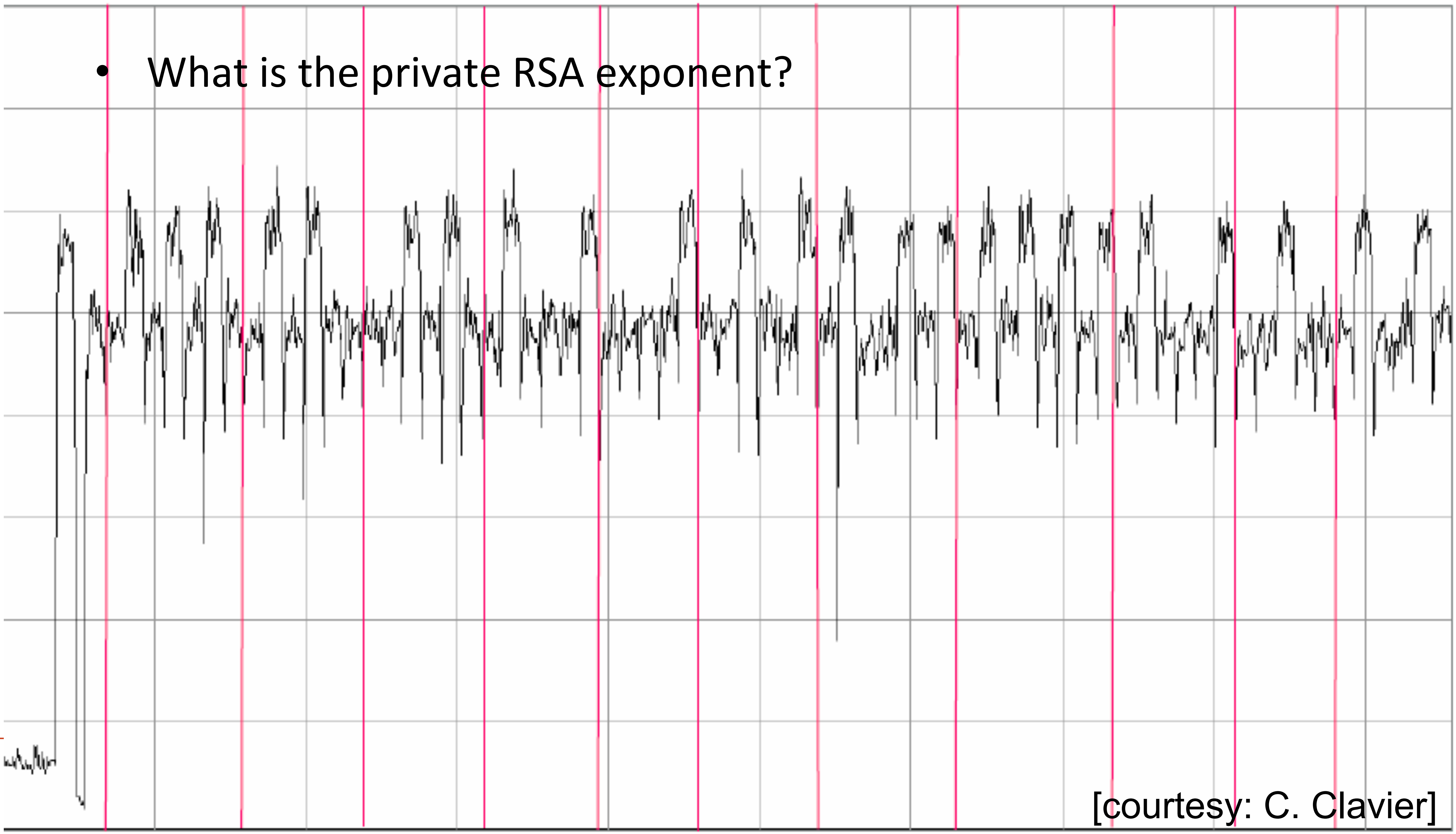
```
In: message m,key e(l bits)
Output: mᵉ mod n

A = 1
for j = l − 1 to 0
    A = A² mod n /* square */
    if (bit j of k) is 1 then
    A = A x m mod n /* multiply */
Return A
```



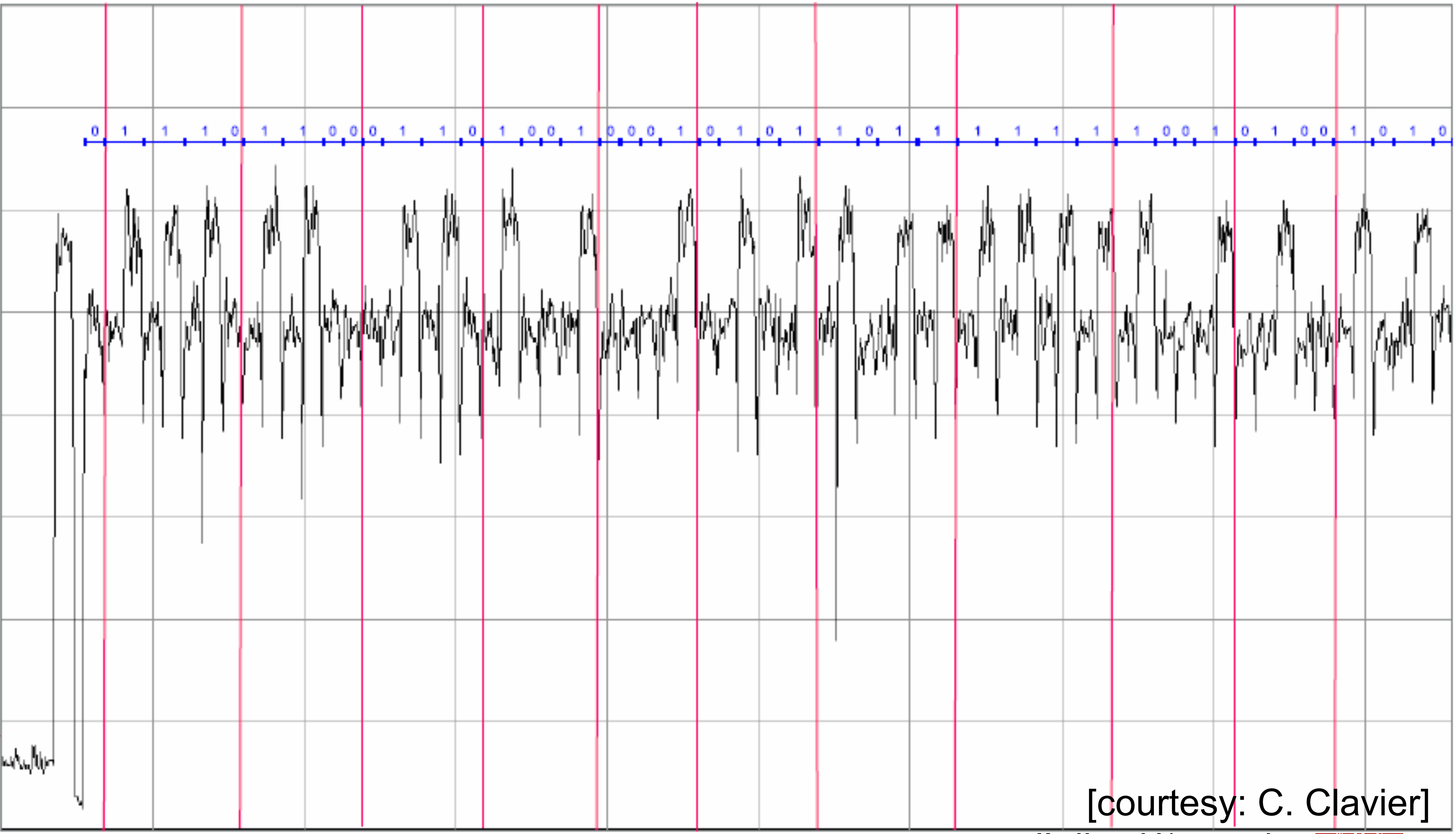
Simple Power Analysis (RSA)

- What is the private RSA exponent?



[courtesy: C. Clavier]

SIMPLE POWER ANALYSIS (RSA)



[courtesy: C. Clavier]

PROTECTING RSA FROM SPA

Left-to-right binary method
Input: N, m and e.
Output: $c = m^e \bmod N$.
1. Let $e = [e_t, e_{t-1}, \ldots, e_1, e_0]_2$;
2. $c := 1$;
3. For $i:=t$ downto 0 do
4. $c := c^2 \bmod N$;
5. if $e_i == 1$ then
6. $c := cm \bmod N$;
Return c.

Montgomery Powering Ladder
Input: N, m and e.
Output: $c = m^e \bmod N$.
1. Let $e = [1, e_{t-1}, \ldots, e_1, e_0]_2$;
2. $R[0] := m$; $R[1] = m^2 \bmod N$;
3. For $i:=t-1$ downto 0 do
4. $R[1-e_i] := R[0]R[1] \bmod N$;
5. $R[e_i] := R[e_i]R[e_i] \bmod N$;
Return $R[0]$.

PROTECTING RSA FROM DPA - RANDOMIZATION

Randomized m

Input: N, m and e.
Output: $c = m^e \bmod N$.

1. r = Random(); //r <N
2. $m_s := rm$;
3. $v = m_s^e \bmod N$;
4. $u := r^e \bmod N$;
5. $c := v/u \bmod N$;

Return c.

Randomized d

Input: N, m, $\varphi(N)$ and d.
Output: $s = m^d \bmod N$.

1. r = Random();
2. $d' = d + r\,\varphi(N)$;
3. $s := m^{d'} \bmod N$;

Return s.

PROTECTING ECC FROM DPA - RANDOMIZATION

Randomized scalar

Input: k, **P**.
Output: **Q** = k**P**.

1. r = Random(); //r < order(**P**)
2. k' := k + r *order(**P**);
3. **Q**= k' **P**;

// [order(**P**)] **P** = O.

Return **Q**.

Base point blinding

Input: k, **P**.
Output: **Q** = k**P**.
precomputed: **R**, **S**=k**R**.

1. **T** := **P** + **R**;
2. **Q'** = k **T**;
3. **Q** = **Q'** – **S**
4. r = Random(); //r < 2^{32}
5. **R** = rR, **S** = rS; //update R, S

Return **Q**.

SCA: RECENT DEVELOPMENTS

- Theory
  - Metrics for side-channel analysis
  - Leakage resilient crypto
- Theory and Practice
  - More advances in attacks: algorithm specific (combined with cryptanalysis)
  - SCA and faults combined
  - Machine learning methods for analysis
  - New countermeasures
  - New models

CONCLUSIONS AND OPEN PROBLEMS

- Physical access allows many attack paths
- Trade-offs between assumptions and computational complexity
- Requires knowledge in many different areas
- Combining SCA with theoretical cryptanalysis
- "Cheap" and effective countermeasures are still to be found

THANK YOU FOR YOUR ATTENTION

REFERENCES

- [KJJ99] P. Kocher, J. Jaffe, B. Jun. “Differential Power Analysis”. CRYPTO 1999.
- [QS01] J. -J. Quisquater and D. Samyde. “ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards”mart 2001.
- [GMO01] K. Gandolfi et al. “Electromagnetic Analysis: Concrete Results”. CHES’01.
- [Koc96] P. Kocher. “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”. CRYPTO 1996
- [RS01] T. Romer and J.-P. Seifert. “Information Leakage Attacks against Smart Card Implementations of the Elliptic Curve Digital Signature Algorithm”. E=Smart 2001
- [CRR03] Chari, Rao and Rohatgi. Template attacks. CHES 2002.
- [AA+02] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side-channel(s). CHES 2002.
- [Mess00b] T. S. Messerges: Using Second-Order Power Analysis to Attack DPA Resistant Software. CHES 2000.
- [Cor99] Jean-Sébastien Coron: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. CHES 1999.
- [BG+12] J. Balasch et al. “Power Analysis of Atmel CryptoMemory - Recovering Keys from Secure EEPROMs.” CT-RSA 2012.
- [EK+08] T. Eisenbarth et al. “On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoqCode Hopping Scheme”, CRYPTO 2008.