Spectral Incoherence: a tool for EM Side Channel Analysis

A. Dehbaoui, S. Tiran, V. Lomne, T. Ordas, F. X. Standaert, N. Veyrat Charmillon,
L. Torres, M. Robert, **P. Maurine**

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

Agence Nationale de la Recherche
ANR

SOLUTIONS COMMUNICANTES SECURISEES
PÔLE DE COMPÉTITIVITÉ MONDIAL

Agenda

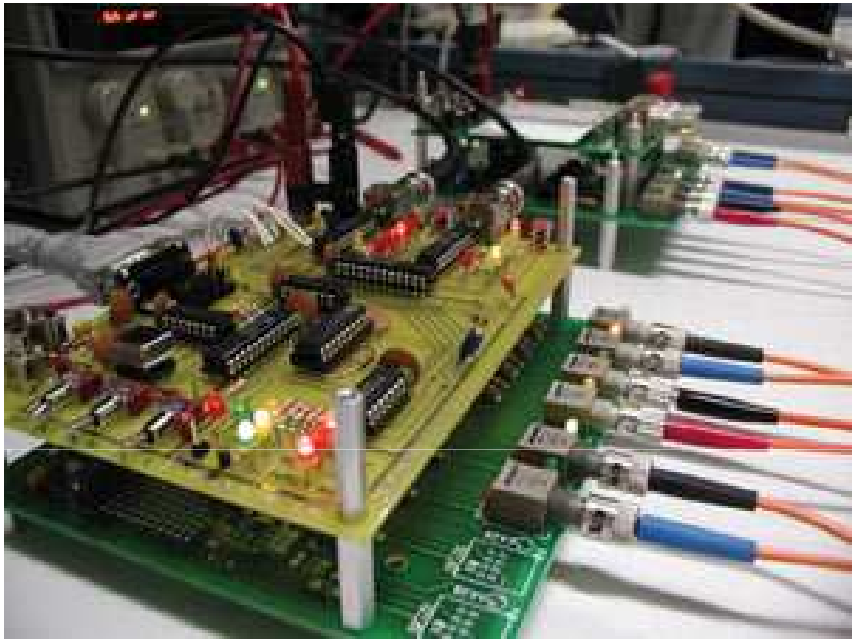
EM Analysis : some advantages … for attackers

Magnitude Squared Incoherence Analysis

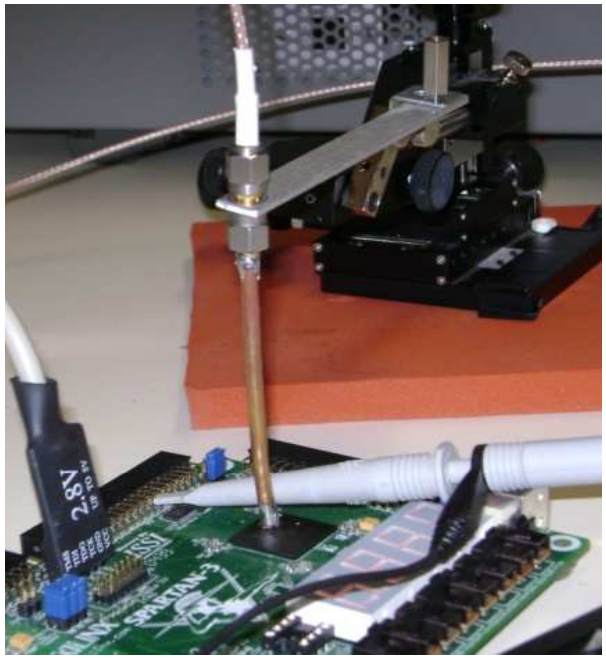
- to localize of hot spots
- as a standard distinguisher

Toward new attacks ?

EM Analysis advantages … for attackers

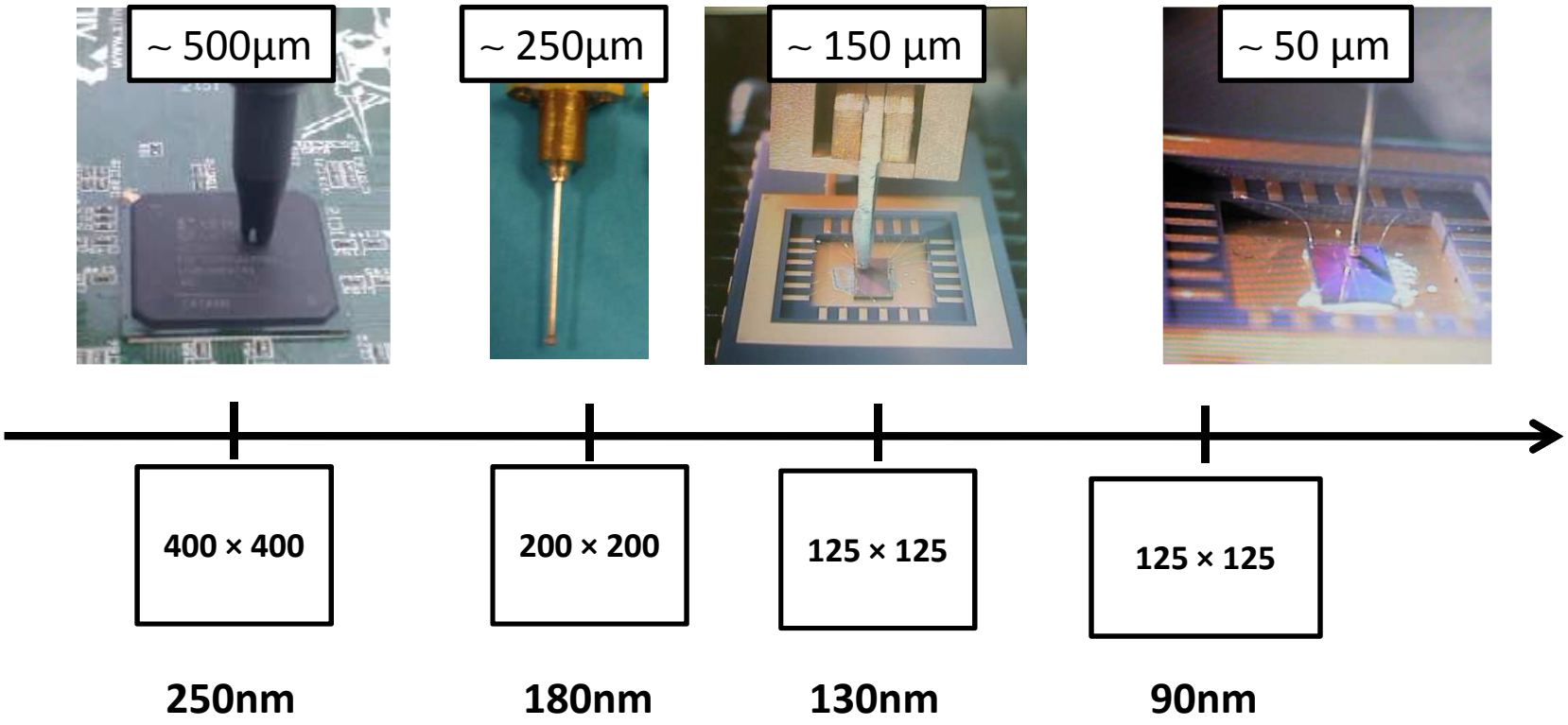


VS



- No specific board
- low cost
- Contactless
- Undetectable

EM Analysis advantages … for attackers

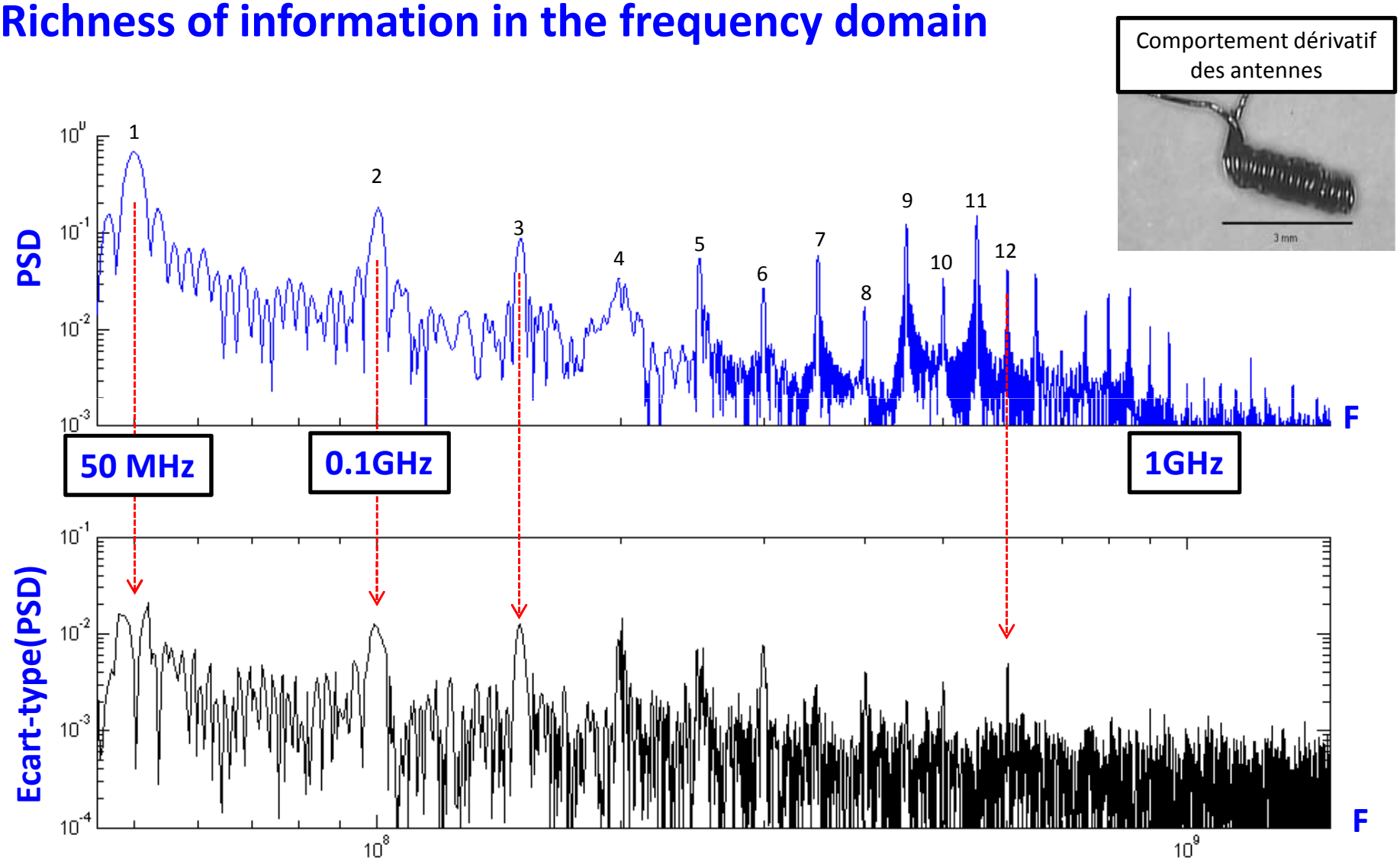


Adaptability wrt the targets

- FPGA vs ASIC
- Scaling with technology (Area and Frequency)
- Manage the SNR

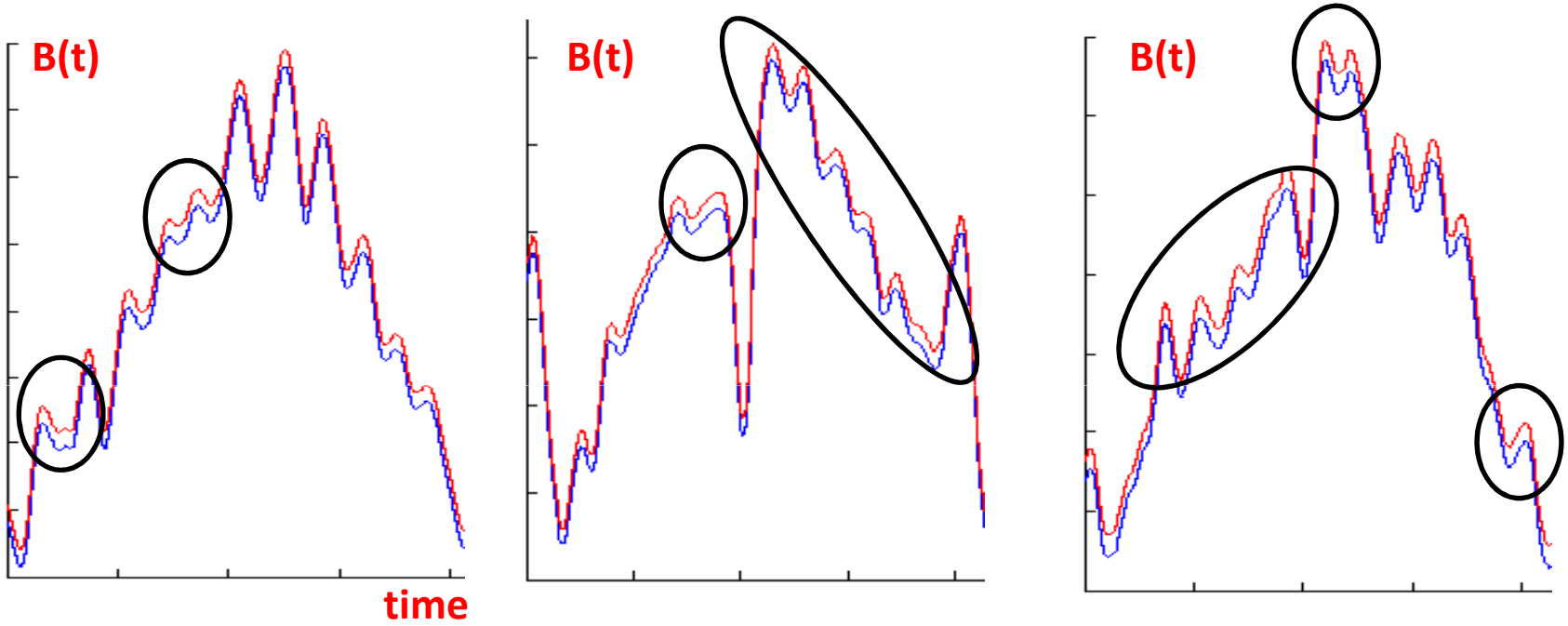
EM Analysis advantages … for attackers

Richness of information in the frequency domain



EM Analysis advantages … for attackers

Richness of information in the time domain



Leakage spread over time

Leakage does not necessarily appear on extrema

The way the signal is captured modifies the leakage

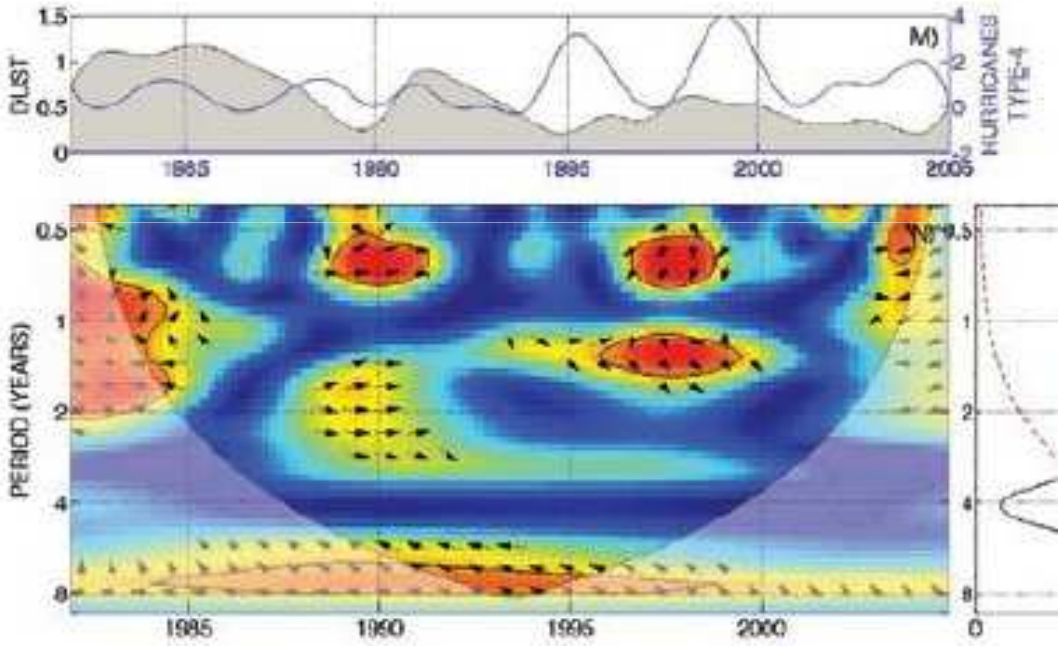
Is the waveforms of B(t) are the real / complete leakage ?

If yes, how to interpret waveforms rather than samples ?

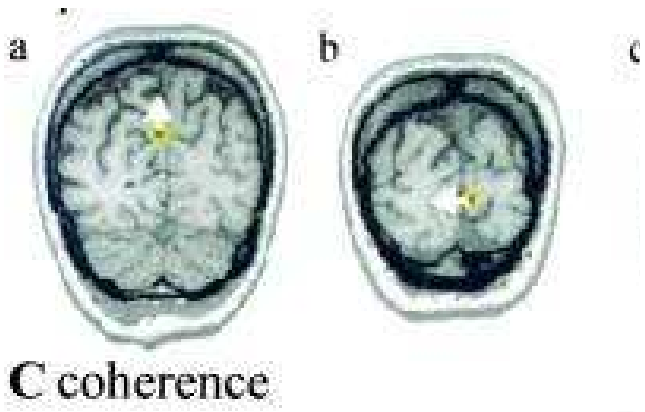
Magnitude Squared Coherence

Basics

Taux de similitude (Coherence) de 2 comportements temporels



Coherence Dust Hurricane type 4



Magnitude Squared Coherence / Incoherence

Basics

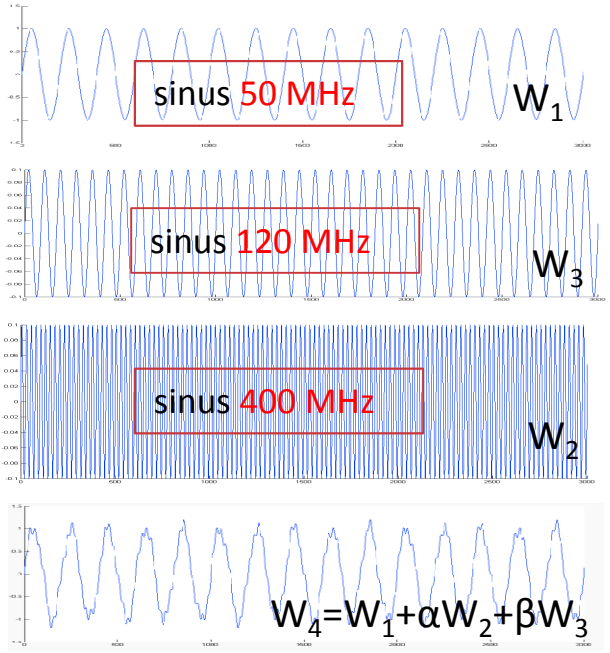
$$MSC_{w_1,w_2}(f) = \frac{\left|P_{w_1,w_2}(f)\right|^2}{P_{w_1,w_1}(f)\,.P_{w_2,w_2}(f)}$$

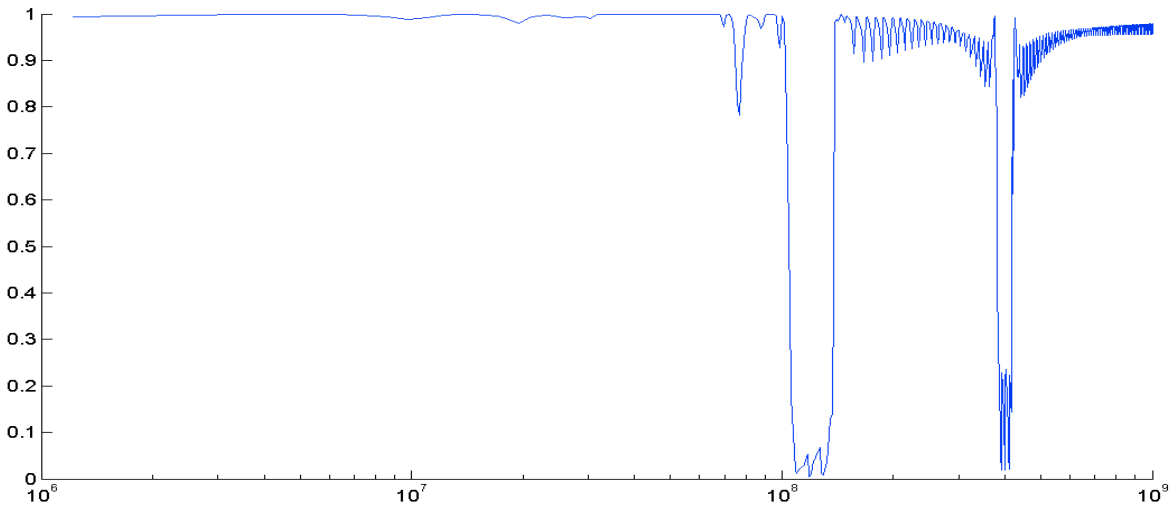
$$0 \le MSC_{w_1,w_2}(f) \le 1$$

$$MSI_{w_1,w_2}(f) = 1 - MSC_{w_1,w_2}(f)$$

$$0 \le MSI_{w_1,w_2}(f) \le 1$$

- $P_{W1,W1}(f)$ et $P_{W2,W2}(f)$ les densités spectrales de Puissance de $w_1(t)$ et $w_2(t)$
- $P_{W1,W2}(f)$ la densité spectrale croisée de Puissance de $w_1(t)$ et $w_2(t)$

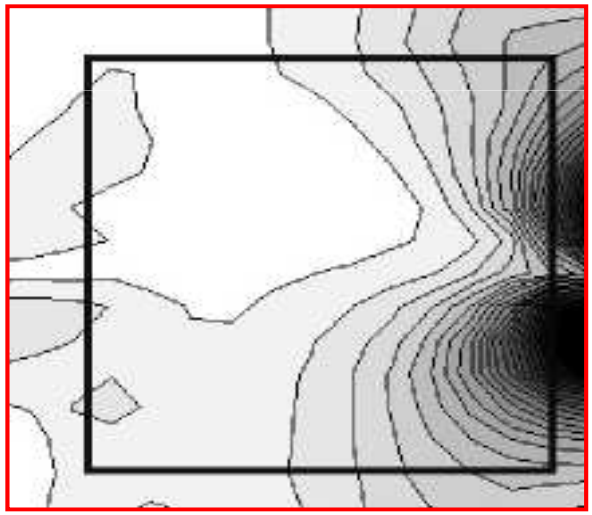


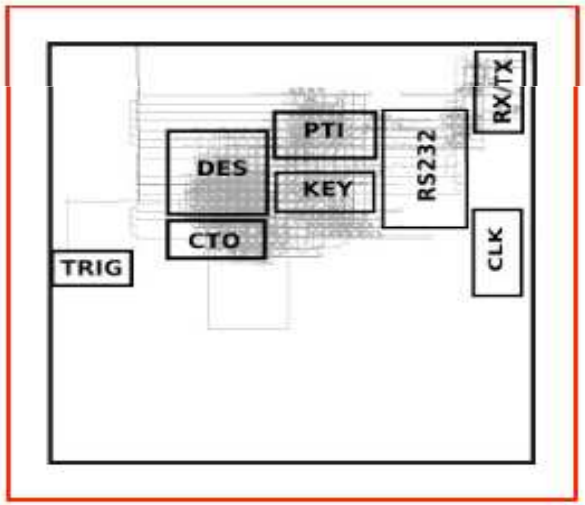


Magnitude Squared Incoherence

To localize hot spots

$$WGMSI_{w_1,w_2} = \sum_{f \in BW} \frac{MSI_{w_1,w_2}(f)}{N_f} \times \frac{A_{w_2}(f)}{\max_{f \in BW}(A_{w_2}(f))}$$





Magnitude Squared Incoherence

To localize hot spots

Normalized WGMSI (100%)
Cartography (5 PTI)

Y/X	1	2	3	4	5	6	7	8
8	9	12	14	9	4	1	1	1
7	8	12	23	22	9	1	1	2
6	11	11	26	27	27	1	2	14
5	30	12	33	38	41	6	100	32
4	39	10	21	20	22	2	4	8
3	57	30	8	11	4	4	1	4
2	36	21	5	6	8	6	2	1
1	27	5	1	2	2	3	5	3

Correlation de 30 à 50%

MTD (%)
CEMA Pearson 5k PTI

Y/X	1	2	3	4	5	6	7	8
8	F	36	38	40	F	F	F	F
7	50	35	35	32	39	F	41	F
6	31	38	19	20	38	F	23	35
5	36	F	21	9	38	29	25	12
4	28	F	13	15	41	35	34	21
3	7	40	18	18	16	18	F	32
2	49	43	F	17	22	24	33	F
1	23	F	F	69	30	32	39	F

Agenda

EM Analysis advantages … for attackers

Magnitude Squared Incoherence Analysis

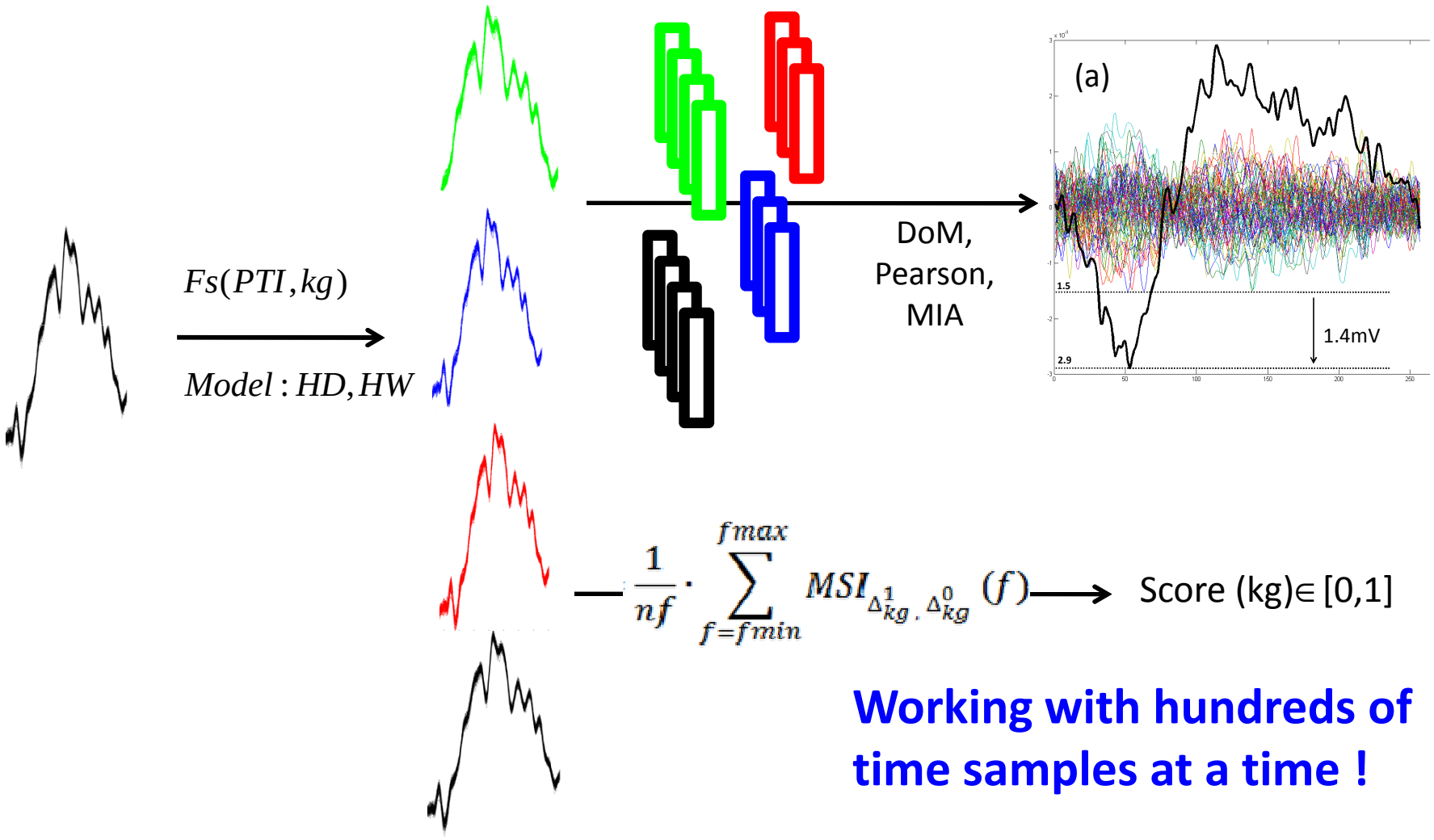
- basics
- to localize of hot spots
- as a standard distinguisher

Towards new attacks ?

Magnitude Squared Incoherence

As a distinguisher

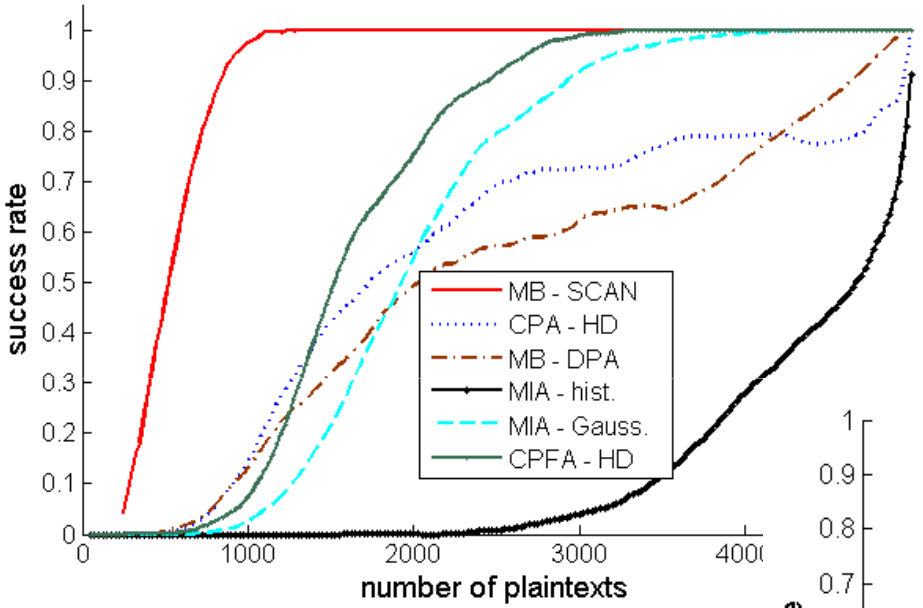
Working with a sample serie !



Working with hundreds of time samples at a time !

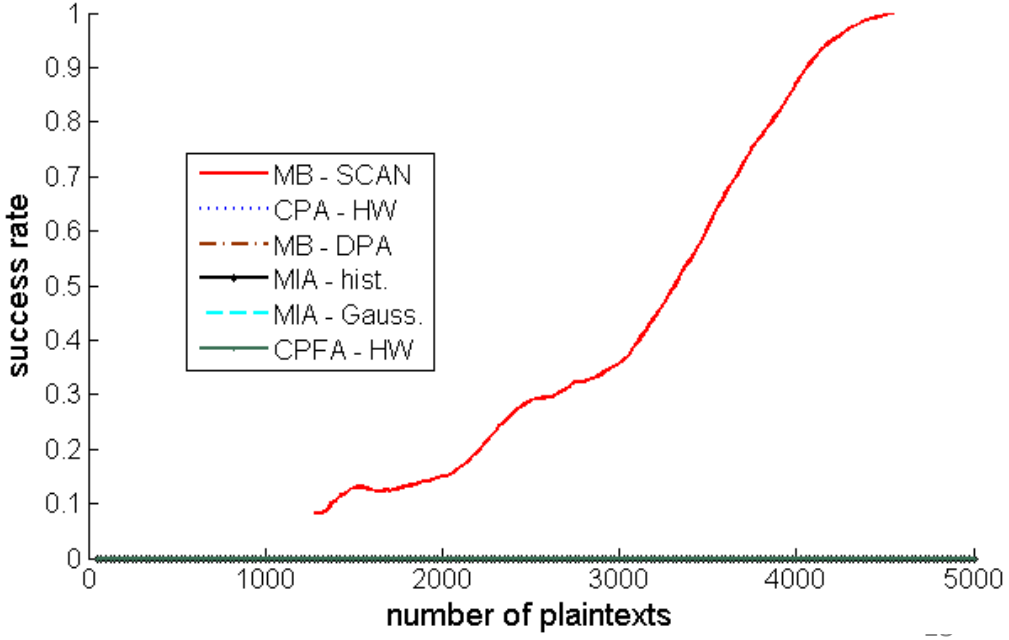
Magnitude Squared Incoherence

As a distinguisher



Hamming Distance

Hamming Weight



Agenda

EM Analysis advantages … for attackers

Magnitude Squared Incoherence Analysis

- basics
- to localize of hot spots
- as a standard distinguisher

Toward new attacks ?

Magnitude Squared Coherence

Comparing EM waveforms ...

n waveforms -----> ½ · n·(n-1) comparisons

n traces	# of comparisons	
100	5 000	
500	125 000	
1 000	500 000	
1 500	1 120 000	→ ~1 Million
4 500	10 000 000	
20 000	200 000 000	→ DPA Contest 2
45 000	1 000 000 000	
1 000 000	500 000 000 000	

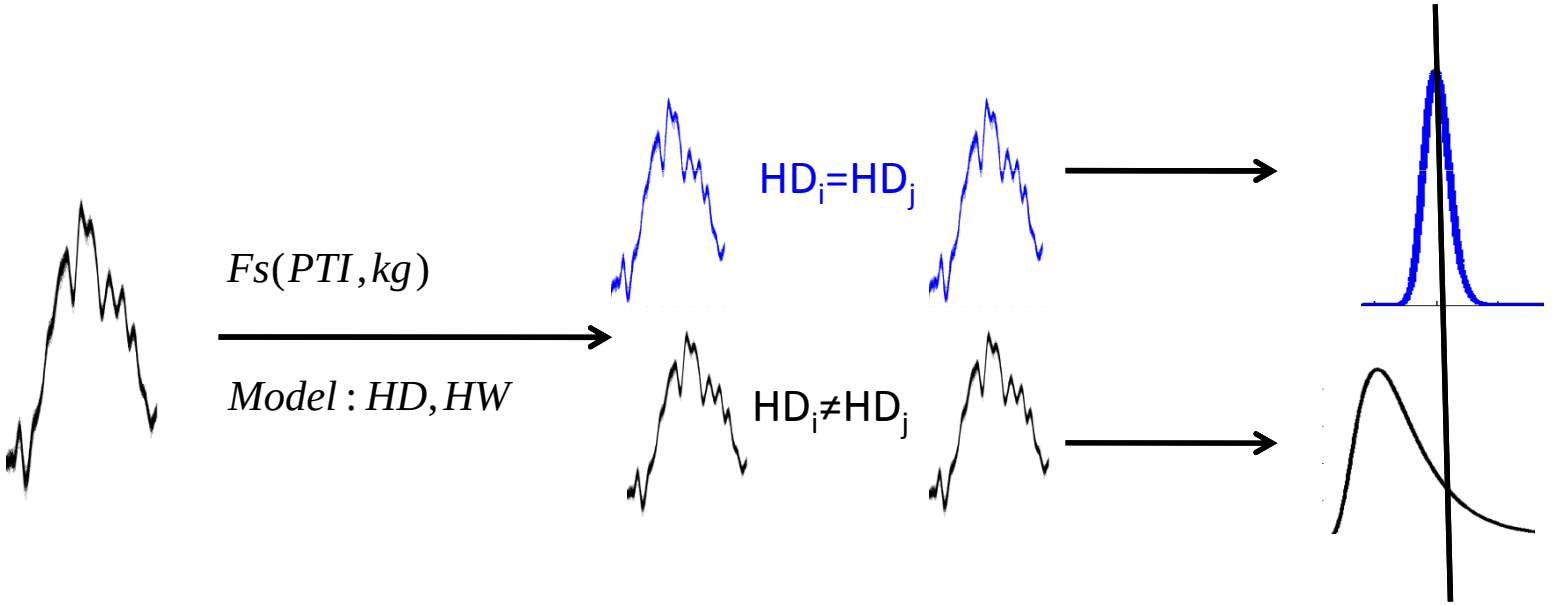
Magnitude Squared Coherence

Comparing EM waveforms ...

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

GROUPE CRYPTO

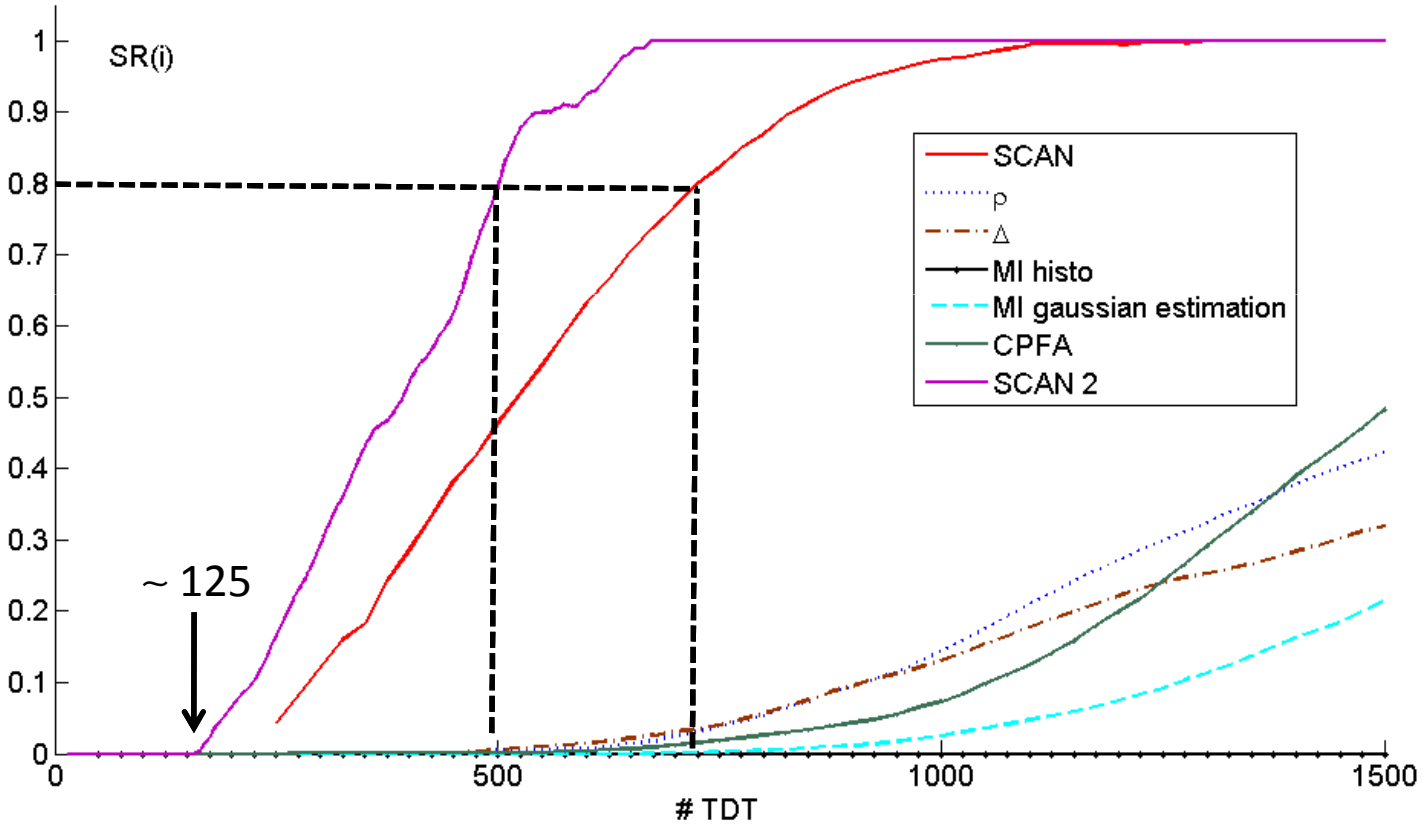
Coherence between all pairs of EM traces



Mean, Median, Variance, Variance IQ, Skewness, Curtosis

Magnitude Squared Coherence

Statistical analysis : mean and variance



Conclusions

EM traces contain different leakages

EM waveforms is a main threat

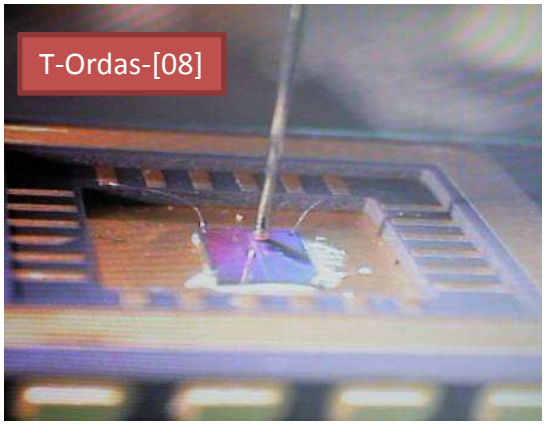
Magnitude Squared Coherence may be applied to…

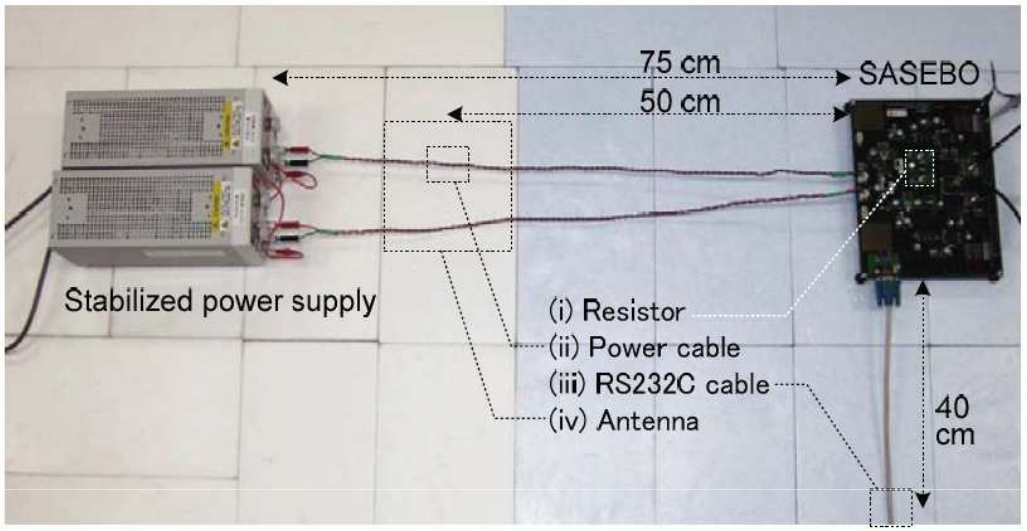
- localize of hot spots
- define new SCA attacks on private key algorithms (undergoing)
- enhance collision attacks on public key algorithms (undergoing)
- re-think template attacks (tbd)

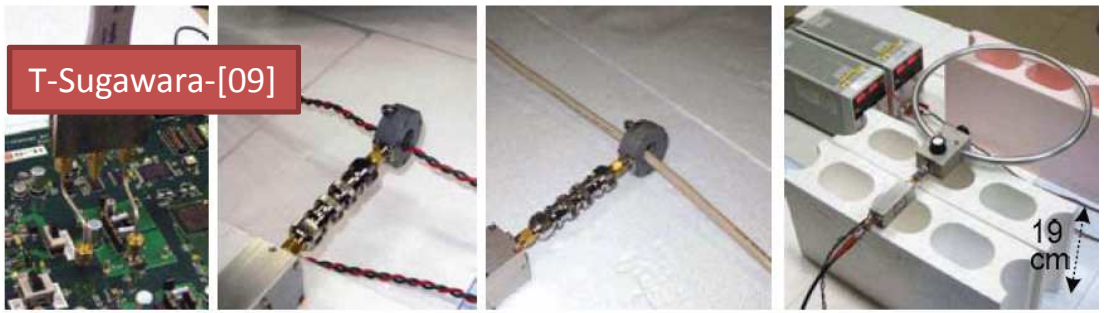
…

by comparing EM waveforms !

EM Analysis advantages … for attackers







Exchanging data ---> EM leakage due to several antennas and different EM coupling mechanisms

Agenda

EM Analysis advantages … for attackers

Magnitude Squared Incoherence Analysis

- basics
- to localize of hot spots
- as a standard distinguisher

Toward new attacks ?