DE LA RECHERCHE À L'INDUSTRIE

Ecole Nationale Supérieure des Mines SAINT-ETIENNE

www.cea.fr

THE BAD AND THE GOOD OF PHYSICAL FUNCTIONS

Cryptarchi 2013, Fréjus

Bruno Robisson, Ingrid Exurville, Jean-Yves Zie, Hélène Le Bouder, Jean-Max Dutertre, Jacques Fournier, Jean-Baptiste Rigaud

24 JUNE 2013

SCHEDULE

Physical function

- Intuitive definition
- Mathematical definition : function
- Mathematical definition revisited : probability mass function (**pmf**)

Examples of probability mass functions

- Leakage function
  - Model based
  - Measures
- Error function
  - Model based
  - Measures

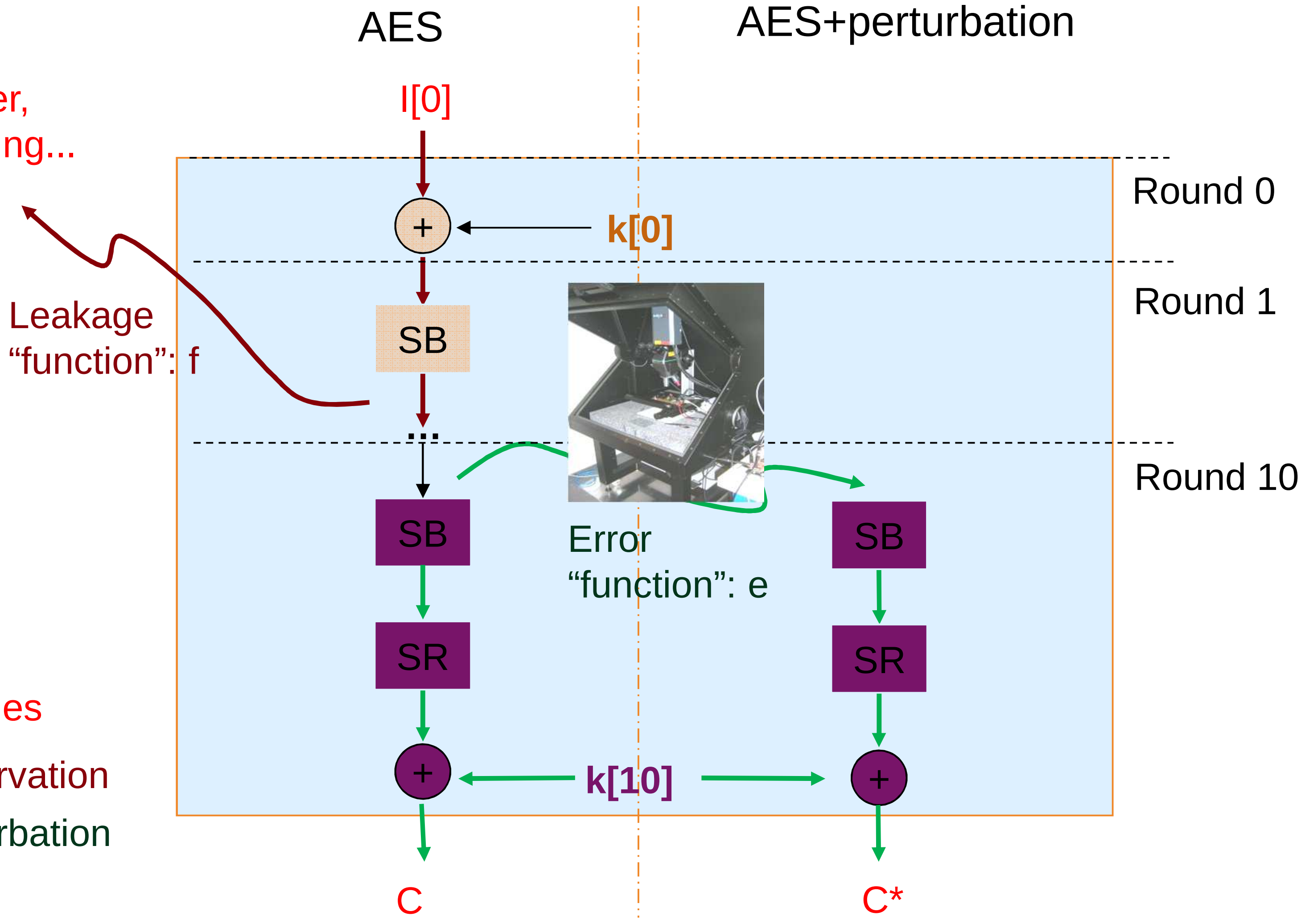
The bad of pmf : Model-free perturbation attack

The good of pmf : Hardware Trojan detection

Conclusion and perspectives

PHYSICAL FUNCTION : INTUITION

EM,
power,
probing...



Observables

→ Observation

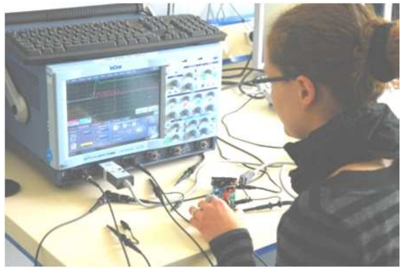
→ Perturbation

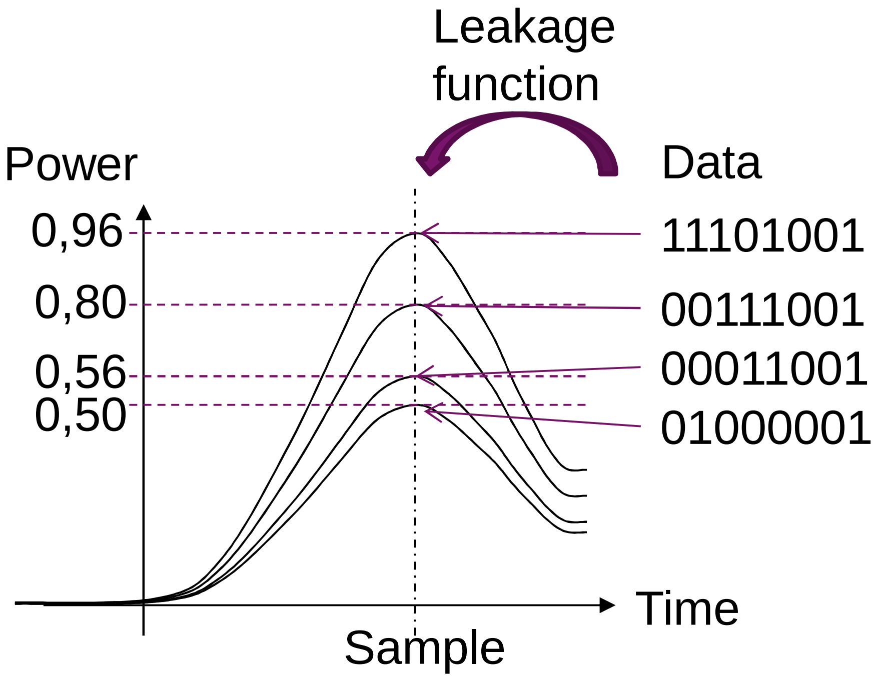
⇨ No analytical expression of physical functions

PHYSICAL FUNCTION : MATH DEFINITION

Leakage function: DATA → MEASURE

Example 1: power measurment





DATA = 1 octet
MEASURE = Output of the acquisition chain (power probe+ampli+oscilloscope) at one instant = power

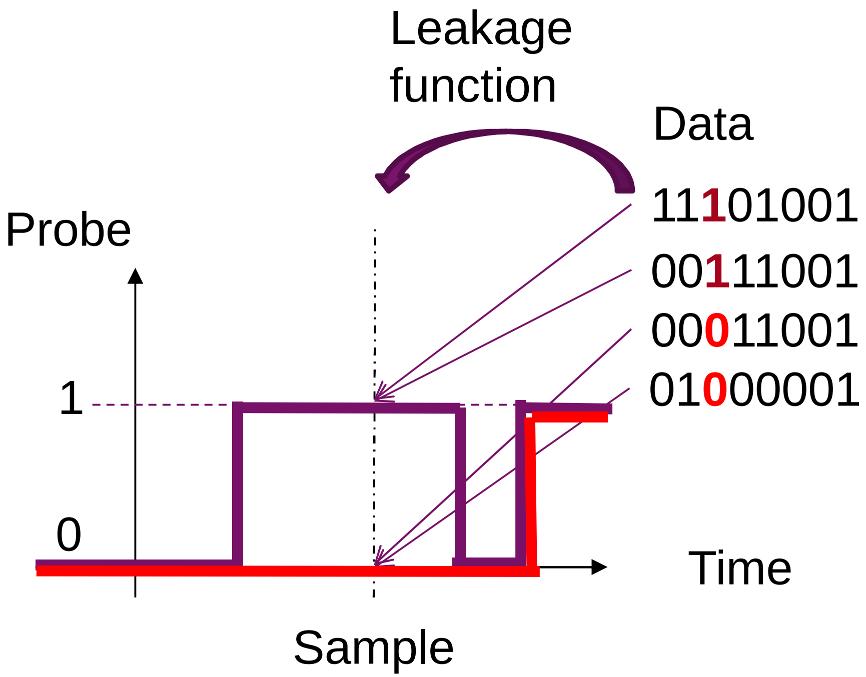
$\{0 ; 2^{M}-1\} \rightarrow \{0;2^{N}-1\}$

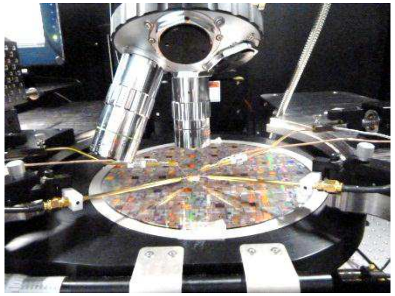
M=# of bits of the data
N=vertical resolution of the oscilloscope

PHYSICAL FUNCTION : MATH DEFINITION

Leakage function: DATA → MEASURE

Example 2: micro-probing





DATA = 1 octet
MEASURE = Output of the acquisition chain (micro-probe+ampli+oscilloscope) at one instant = « Probe »

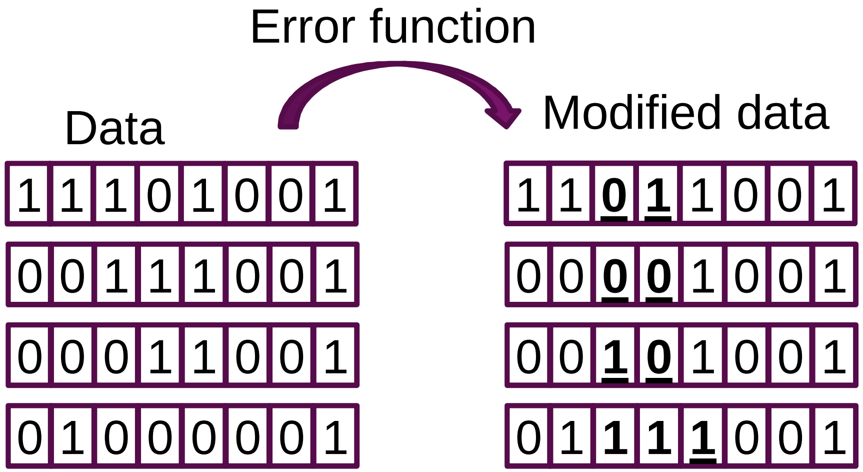
$\{0 ; 2^M-1\} \rightarrow \{0;1\}$

M=# of bits of the data

PHYSICAL FUNCTION : MATH DEFINITION

Error function : DATA → DATA

Example: laser bench



Error function

Data	Modified data
1 1 1 0 1 0 0 1	1 1 **0** **1** 1 0 0 1
0 0 1 1 1 0 0 1	0 0 **0** **0** 1 0 0 1
0 0 0 1 1 0 0 1	0 0 **1** **0** 1 0 0 1
0 1 0 0 0 0 0 1	0 1 **1** **1** **1** 0 0 1

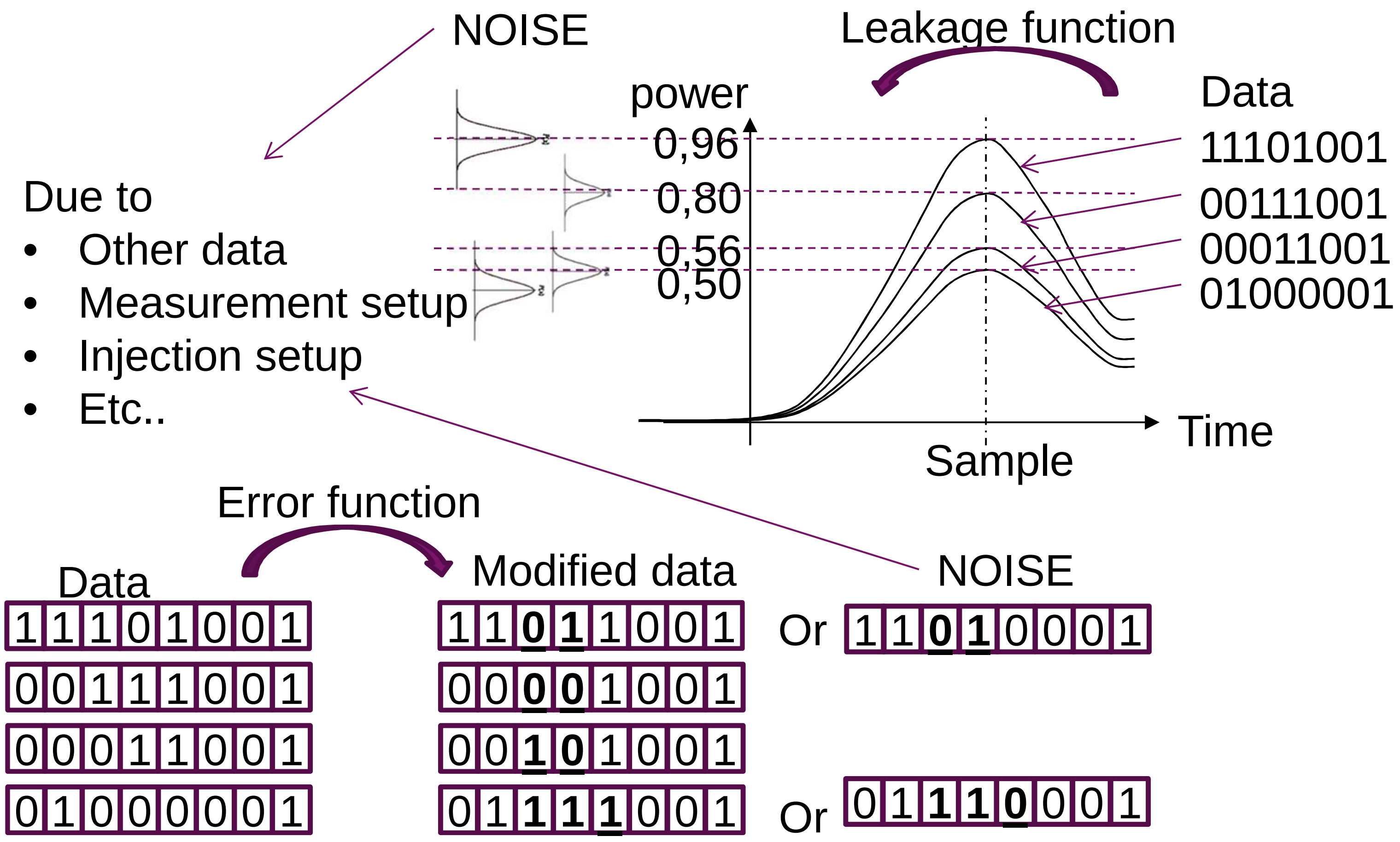
DATA = 1 octet
DATA = DATA modified by the pertubation mean = 1 octet (of hidden data)

$\{0 ; 2^{M}-1\} \rightarrow \{0 ; 2^{M}-1\}$

M=# of bits of the data

PHYSICAL FUNCTION : LIMITS OF THE MATH DEFINITION

- Classical math definition : linked with models used to perform model based attacks (DPA, DFA, DBA, FSA, etc.)
- Limitation : definition has to take NOISE into account



NOISE

Due to
- Other data
- Measurement setup
- Injection setup
- Etc..

NOISE

Error function

Data

1 1 1 0 1 0 0 1

0 0 1 1 1 0 0 1

0 0 0 1 1 0 0 1

0 1 0 0 0 0 0 1

Modified data

1 1 **0** **1** 1 0 0 1 Or 1 1 **0** **1** 0 0 0 1

0 0 **0** **0** 1 0 0 1

0 0 **1** **0** 1 0 0 1

0 1 **1** **1** **1** 0 0 1 Or 0 1 **1** **1** **0** 0 0 1

PHYSICAL FUNCTION : PROPOSAL OF A NEW MATH DEFINITION

Our proposal :

« Noisy » physical function
=
Joint probability mass function (pmf)

Example 1:
DATA: D → R and
MEASURE: M → R

DATA and MEASURE are considered as two discrete random variables with sample spaces
$D=\{0 ; 2^{M}-1\}$ and
$M=\{0;2^{N} -1\}$

The joint pmf of the discrete variables DATA*MEASURE is
$f_{DATA*MEASURE}: R^{2} \rightarrow [0;1]$ defined such that
$f_{DATA*MEASURE}(x,y)=Pr(DATA=x,MEASURE=y)$ whatever x and $y \in R$

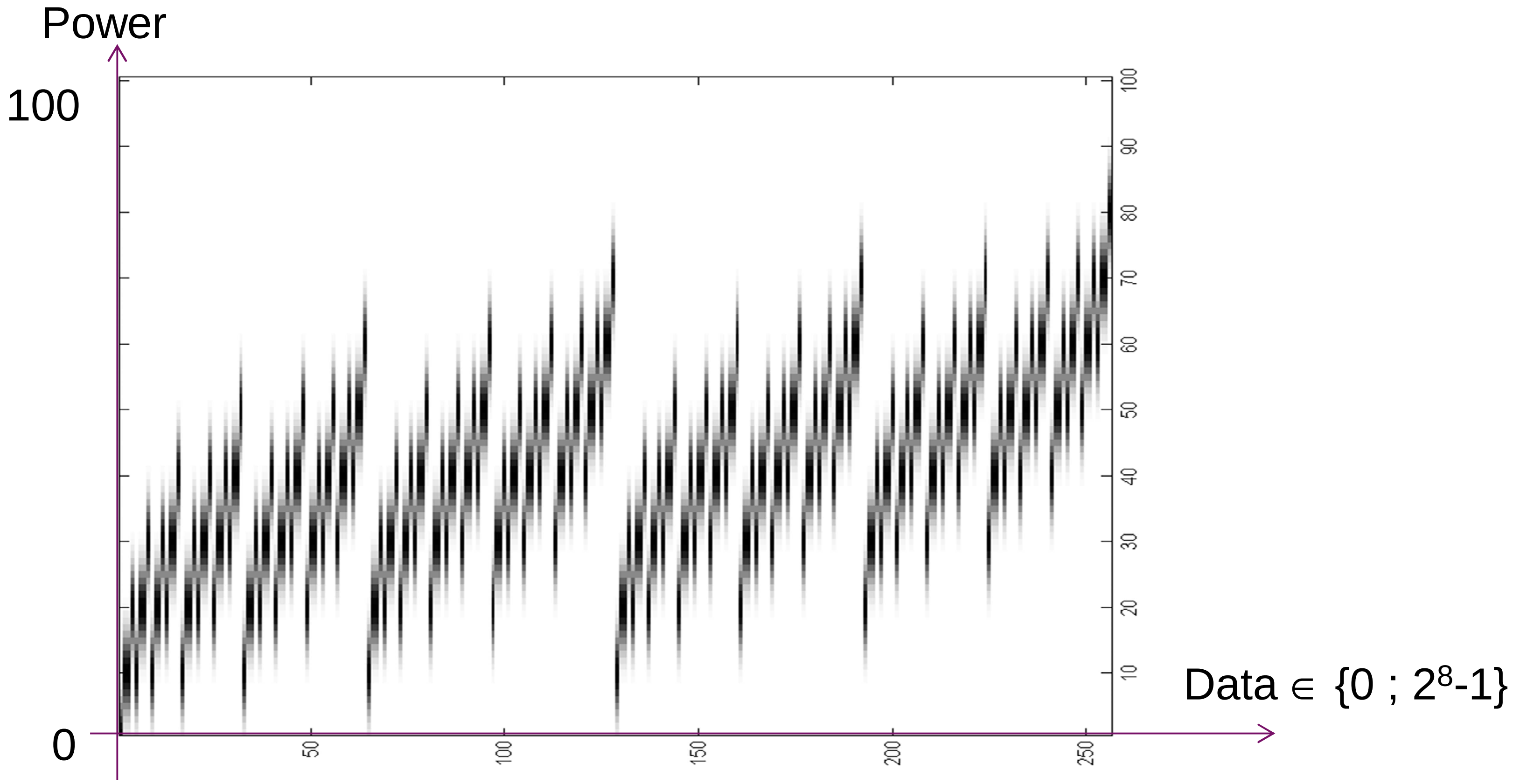
EXAMPLES OF PMF: MODEL-BASED LEAKAGE FUNCTION

Leakage function: Power(x)= Gauss(10*HW(x) , 4) with $x \in \{0 ; 2^8-1\}$

Mean

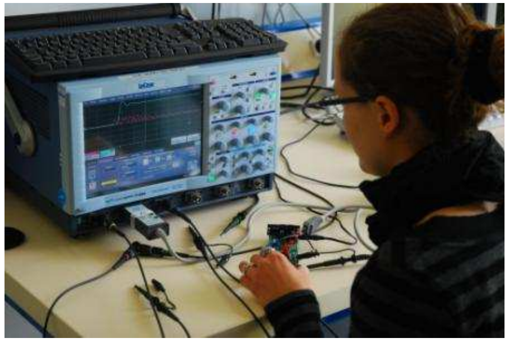
Standard deviation

Associated pmf:



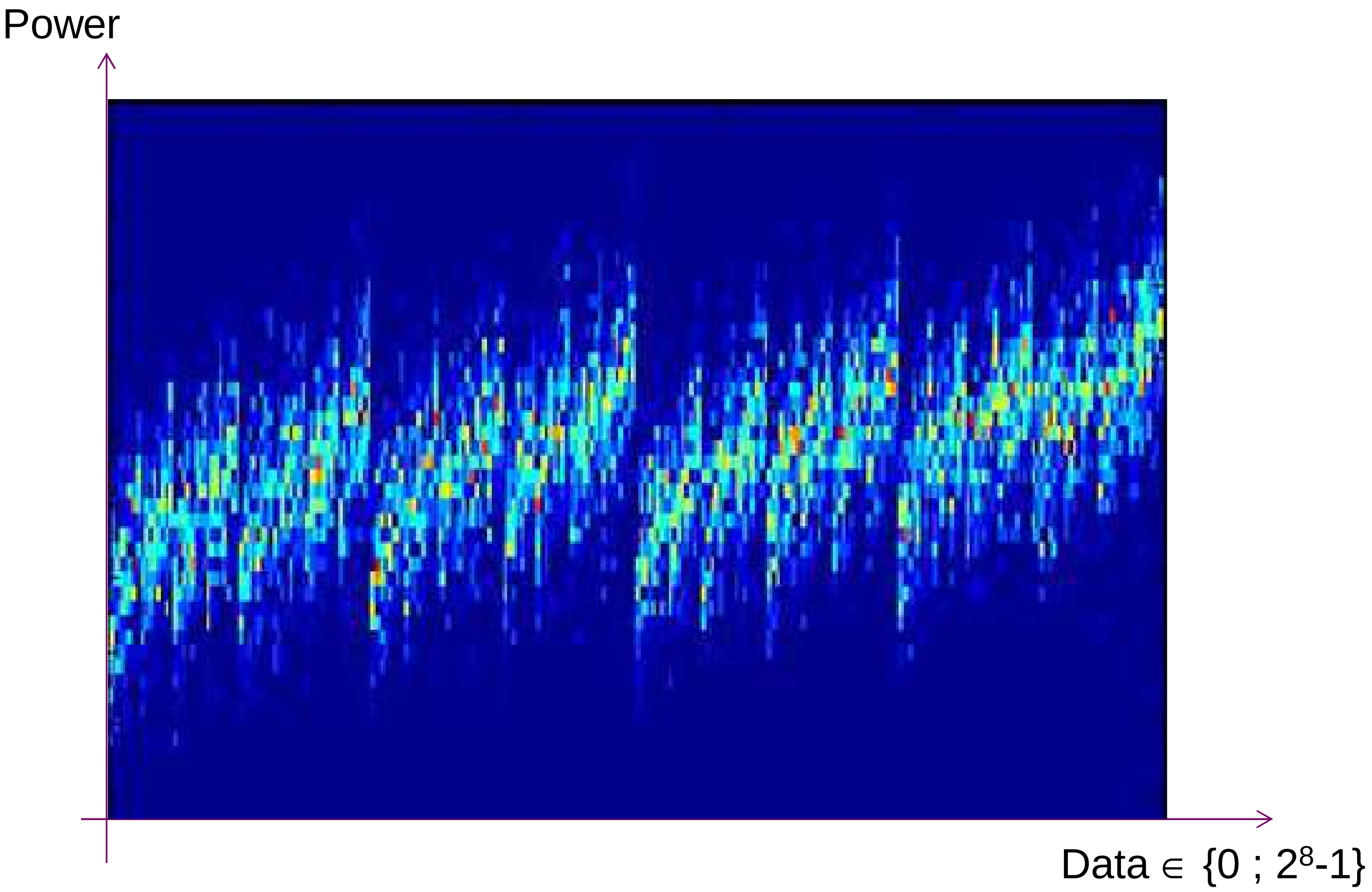
EXAMPLES OF PMF: MEASURE OF LEAKAGE FUNCTION

- 32-bit microcontroler evaluation board (without countermeasure)
- Software implementation of the AES-128
- Oscilloscope Tektronix DPO 7104 (1 GHz)
- Plain texts (known) : XX 00 00 00 00 00 00 00 (XX ∊ [0:255])
- Key (known) : 43 00 00 …. 00 00
- Measure = power consumption during round 1
- Data = output of Sbox 1

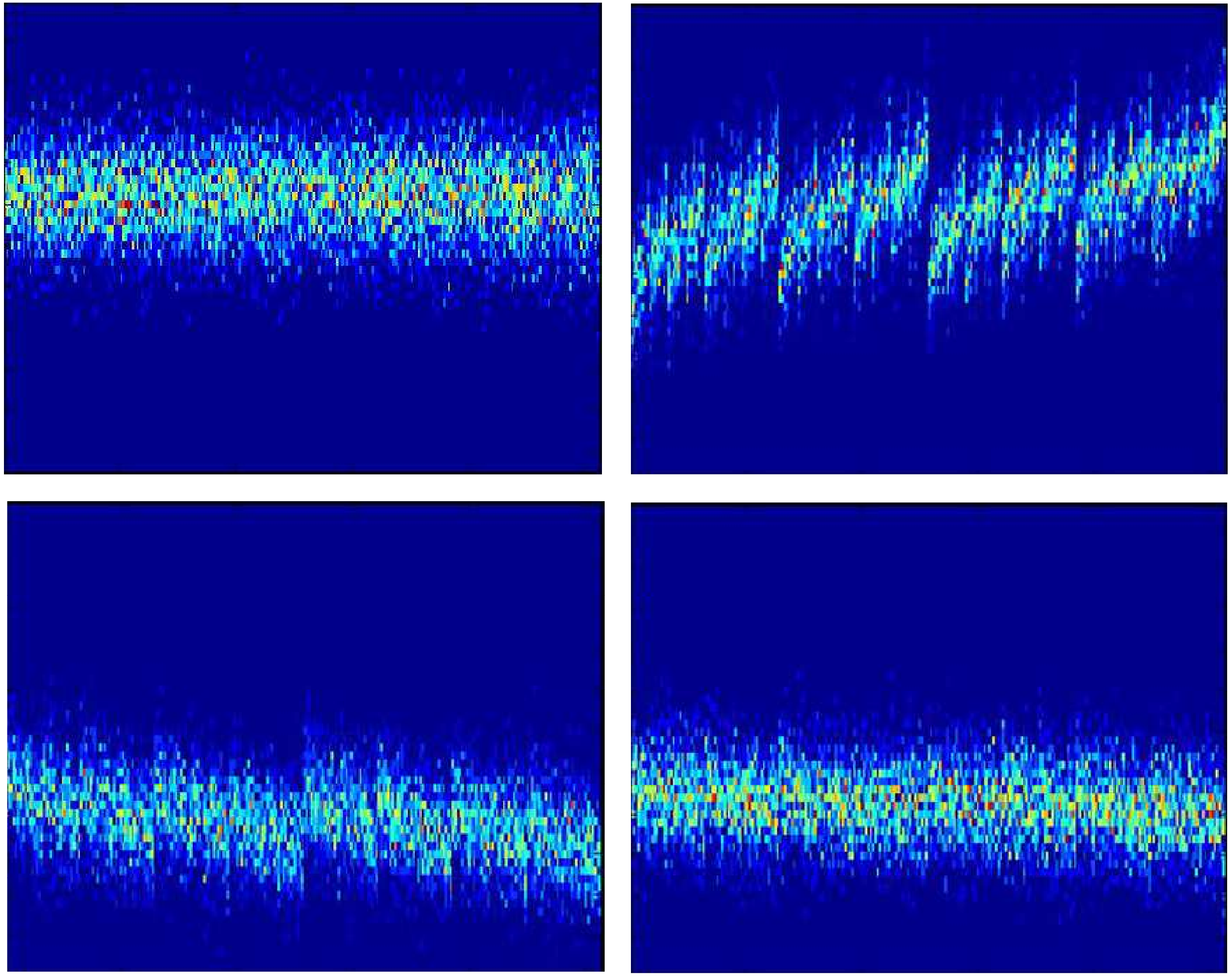


EXAMPLES OF PMF: MEASURE OF LEAKAGE FUNCTION

Measured pmf on a 32 bit microcontroller (S Box1) :



EXAMPLES OF PMF: MEASURE OF LEAKAGE FUNCTION



Start of round

« Start of middle round »

« End of middle round »

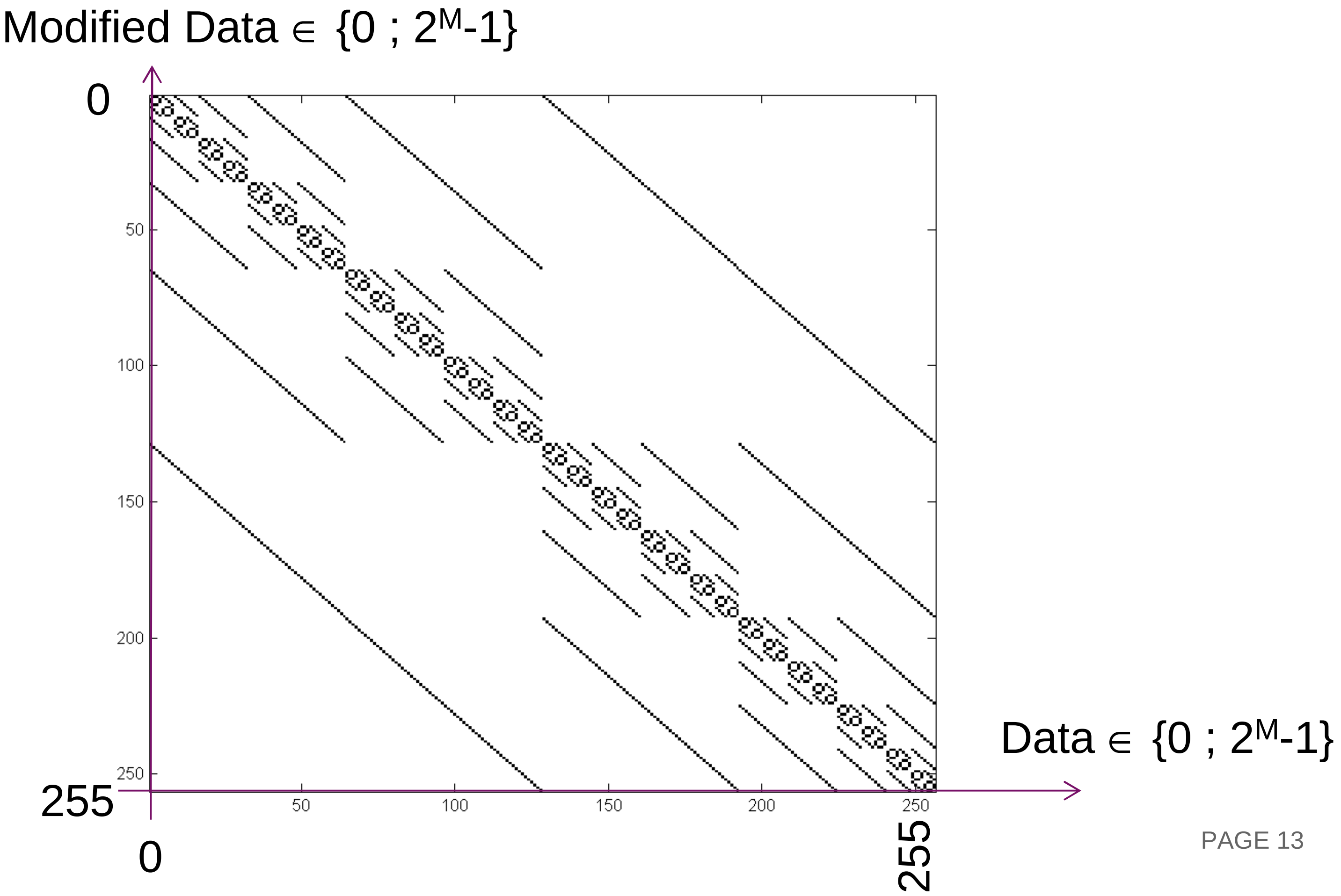
End of round

Impact of sample instant

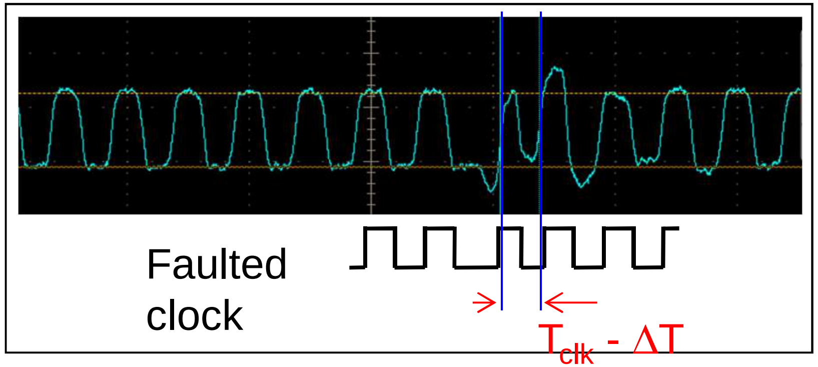
EXAMPLES OF PMF: MODEL-BASED ERROR FUNCTION

Error function: Modified_Data(x)= x + e_i with x ∈ {0 ; 2^8-1} and $e_i=2^i$ with $p(e_i)=1/8$ and i ∈{0,7} i.e « random monobit fault »

Associated pmf



EXAMPLES OF PMF: MEASURE OF ERROR FUNCTION

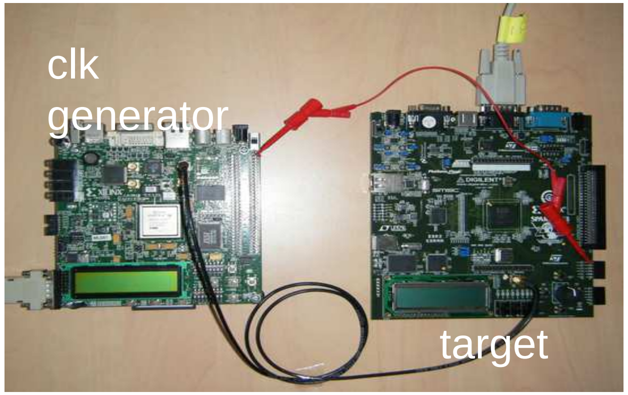


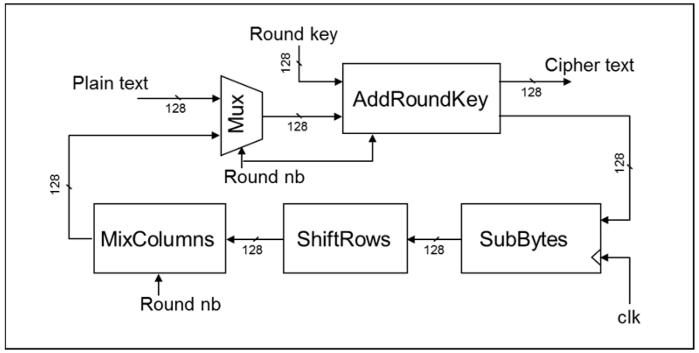
Fault injection principle :

- reduction of one period of the clock (ΔT) ,
- fault injection by clock set-up time

Characteristics of clk generator :

- resolution of ΔT : ~ 35 ps à 100 MHz,
- low cost platform (FPGA Xilinx),
- easy set-up.

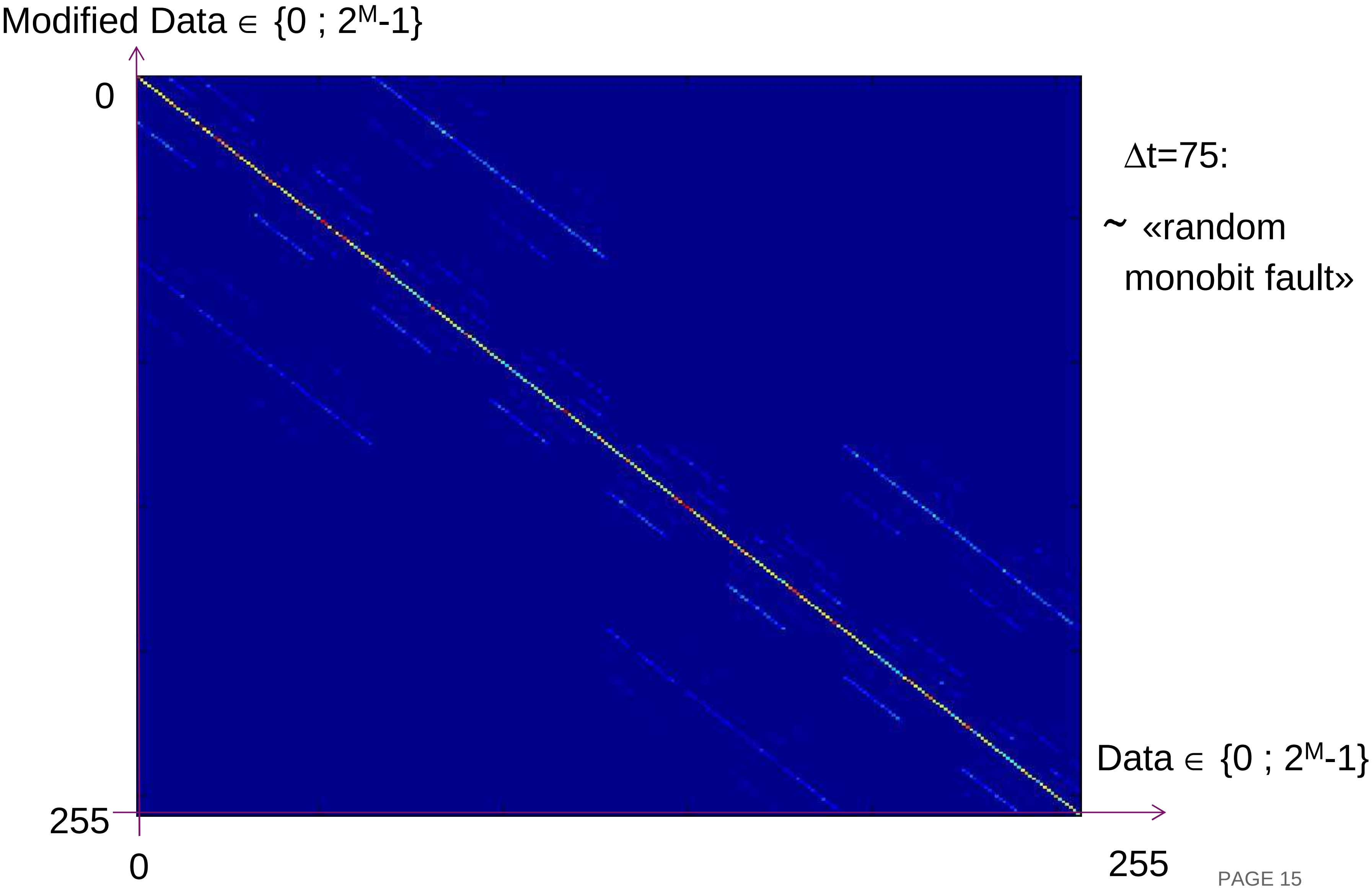




Target

- AES-128 on FPGA (virtex 3 board)
- Fault during the computation of round 9, i.e fault on round[10].start
- Δt from 50 to 130 (*35ps) by step of 1

EXAMPLES OF PMF: MEASURE OF ERROR FUNCTION



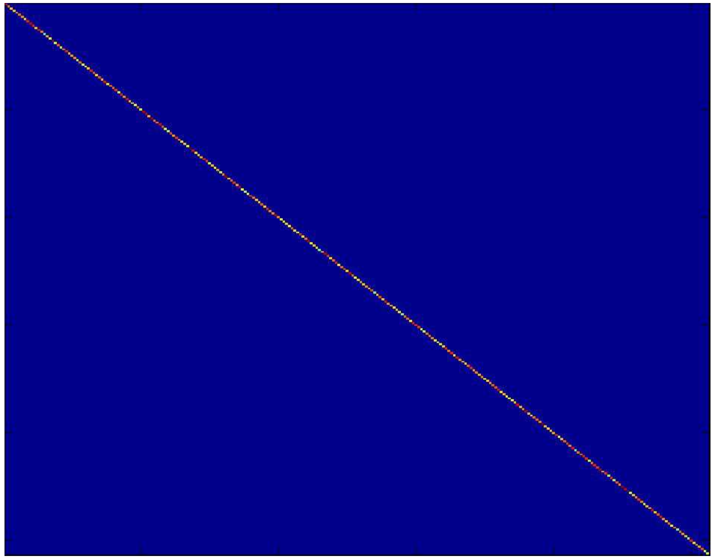
Δt=75:

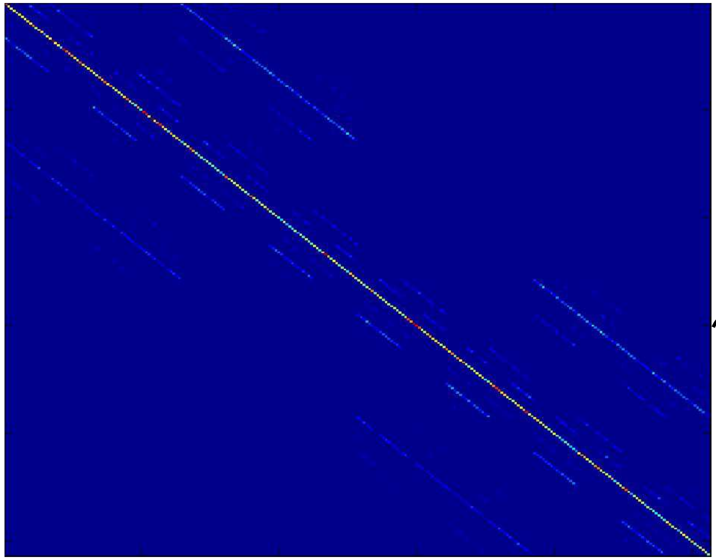
~ «random monobit fault»

EXAMPLES OF PMF: MEASURE OF ERROR FUNCTION

Octet 13

Δt=50:
No fault

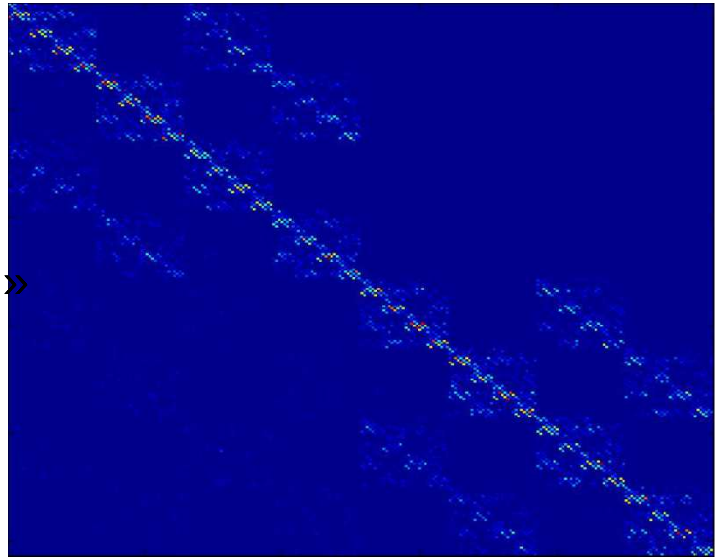


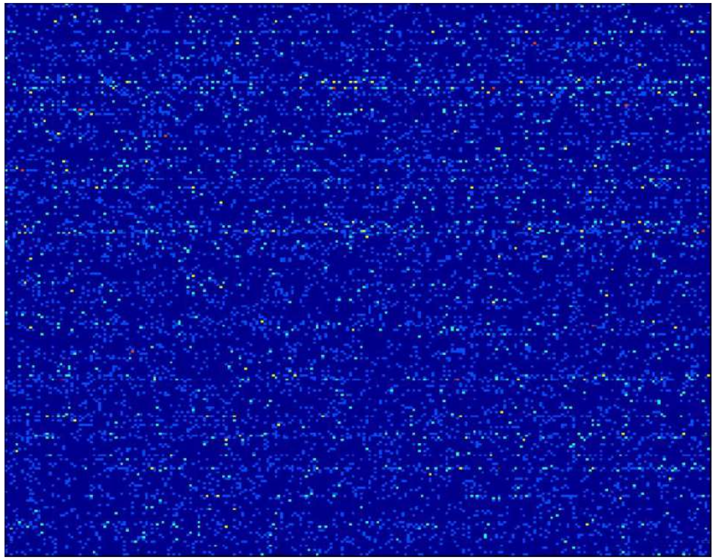


Δt=75:

~ random-monobit

Δt=90
« strange »





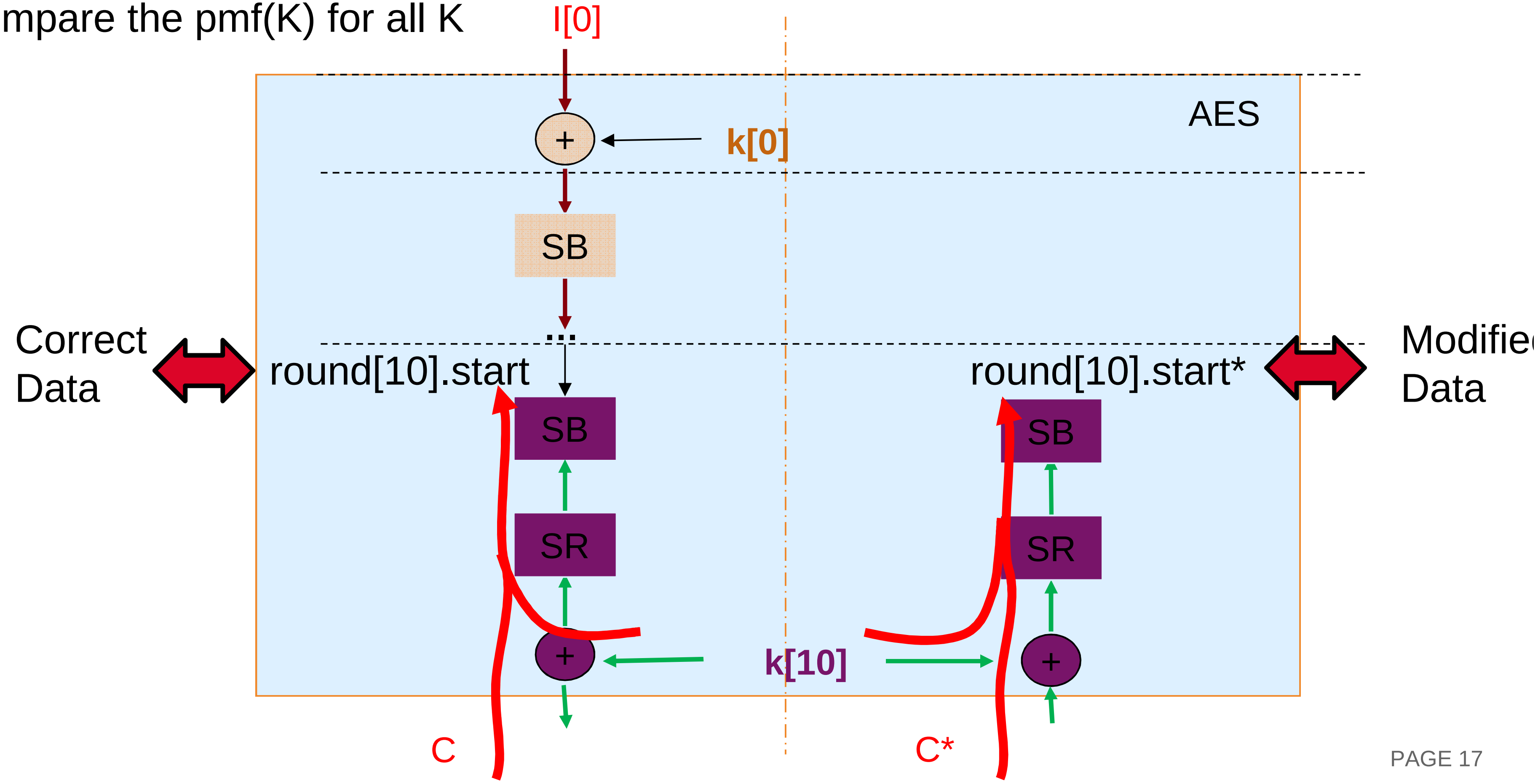
Δt=130
random

THE BAD OF PHYSICAL FUNCTION: ATTACK

For all hypothesis K on k[10]

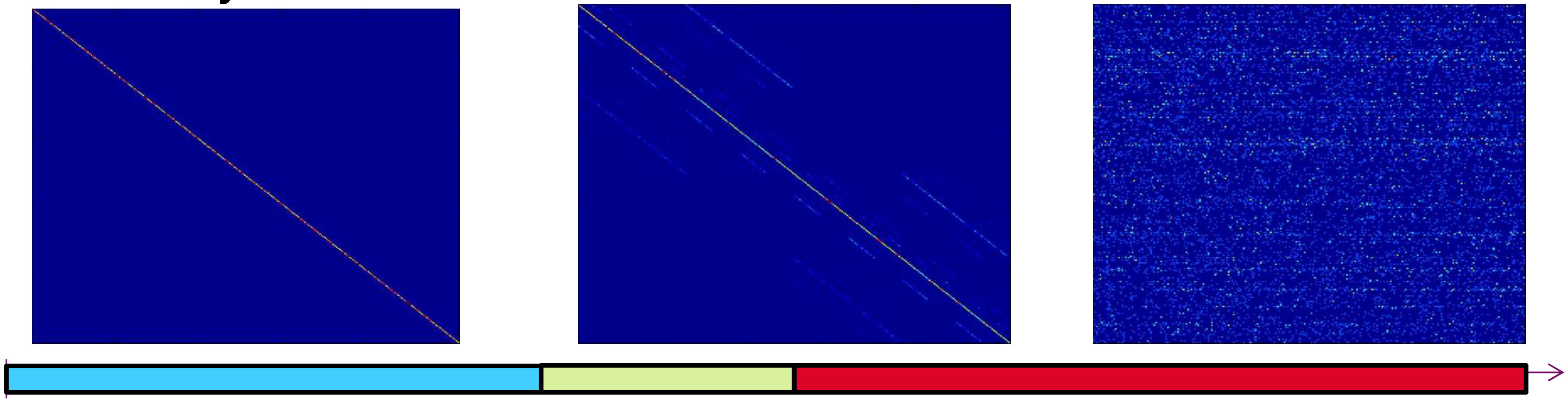
- Compute round[10].start from C and K
- Compute round[10].start* from C* and K
- Display pmf(K)

Compare the pmf(K) for all K



THE BAD OF PHYSICAL FUNCTION: ATTACK DISPLAY STEP

Correct key :



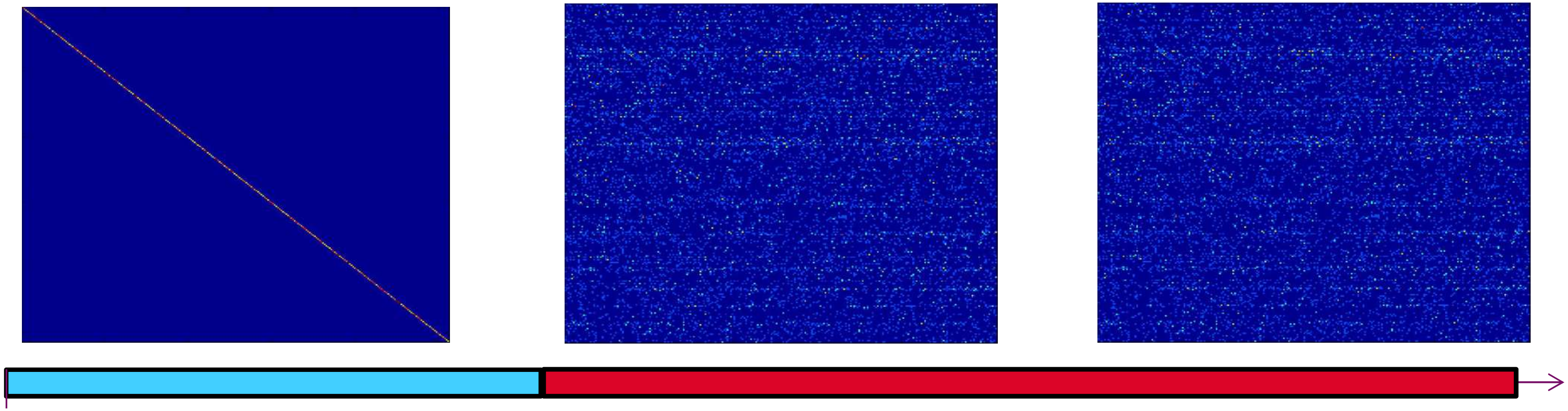
No fault

Fault but « not too random »

Random

Δt

Uncorrect key :



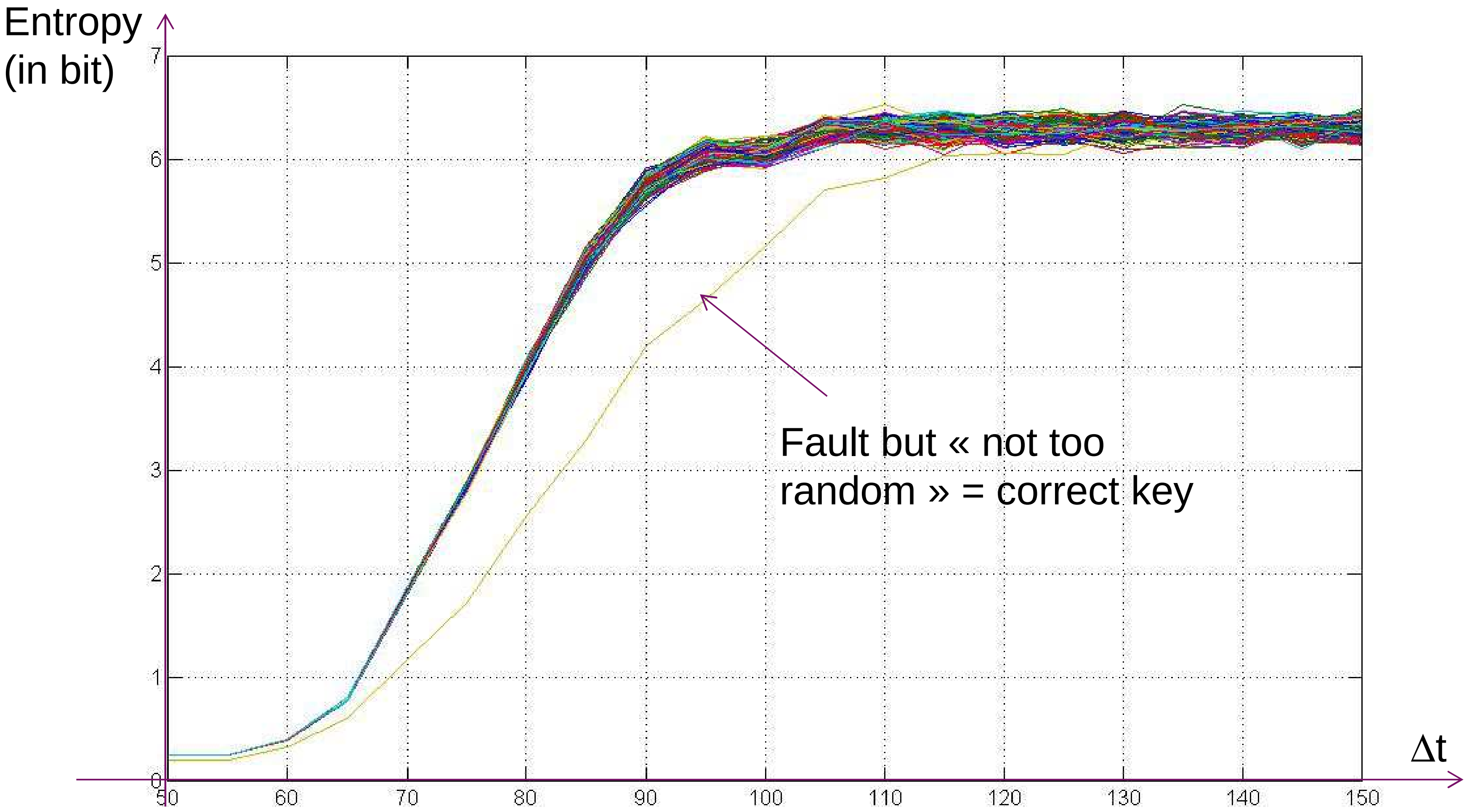
No fault

Random

Δt

THE BAD OF PHYSICAL FUNCTION: ATTACK COMPARISON STEP

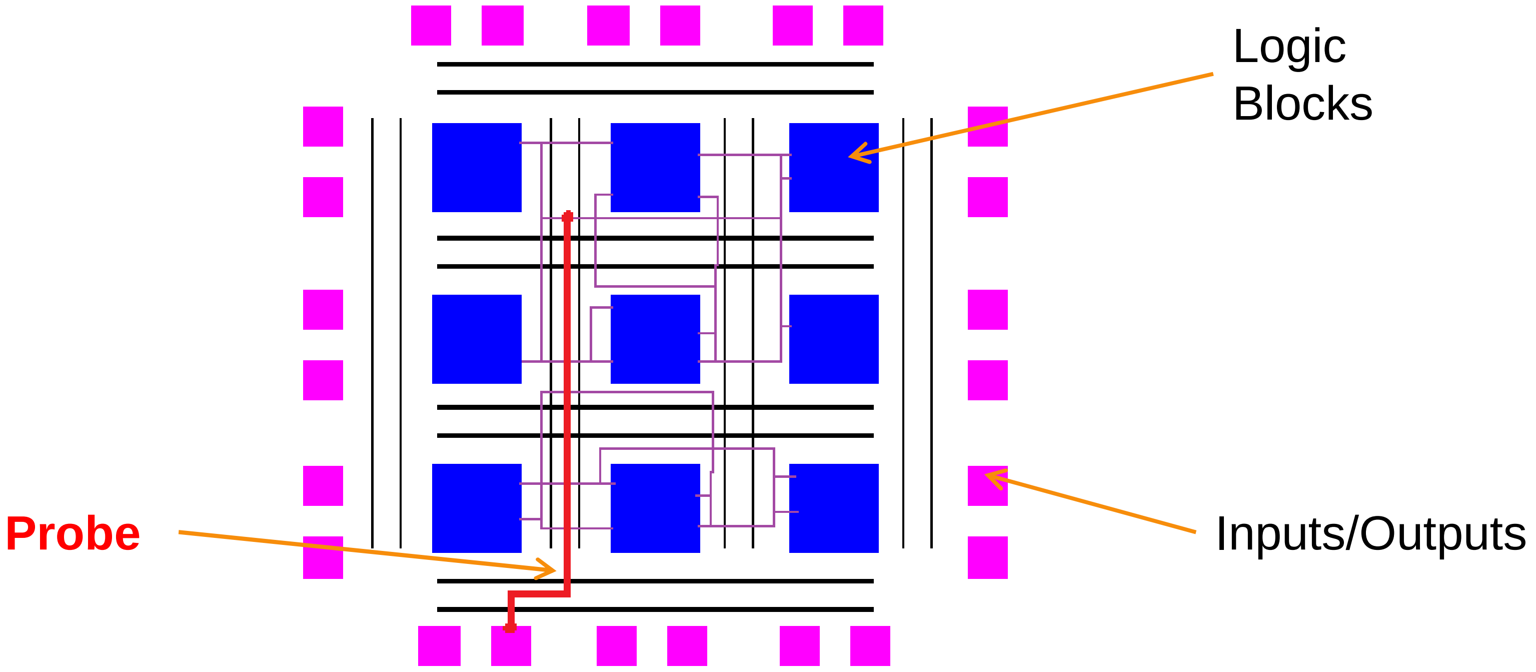
Entropy of the pmf with 100 pairs of correct and uncorrect cipher texts for every key hypothesis:



Fault but « not too random » = correct key

THE GOOD OF PHYSICAL FUNCTION: HW TROJAN DETECTION

HW Trojan: Add « probes » (i.e. additional wires from an internal signal to an I/O) in the design

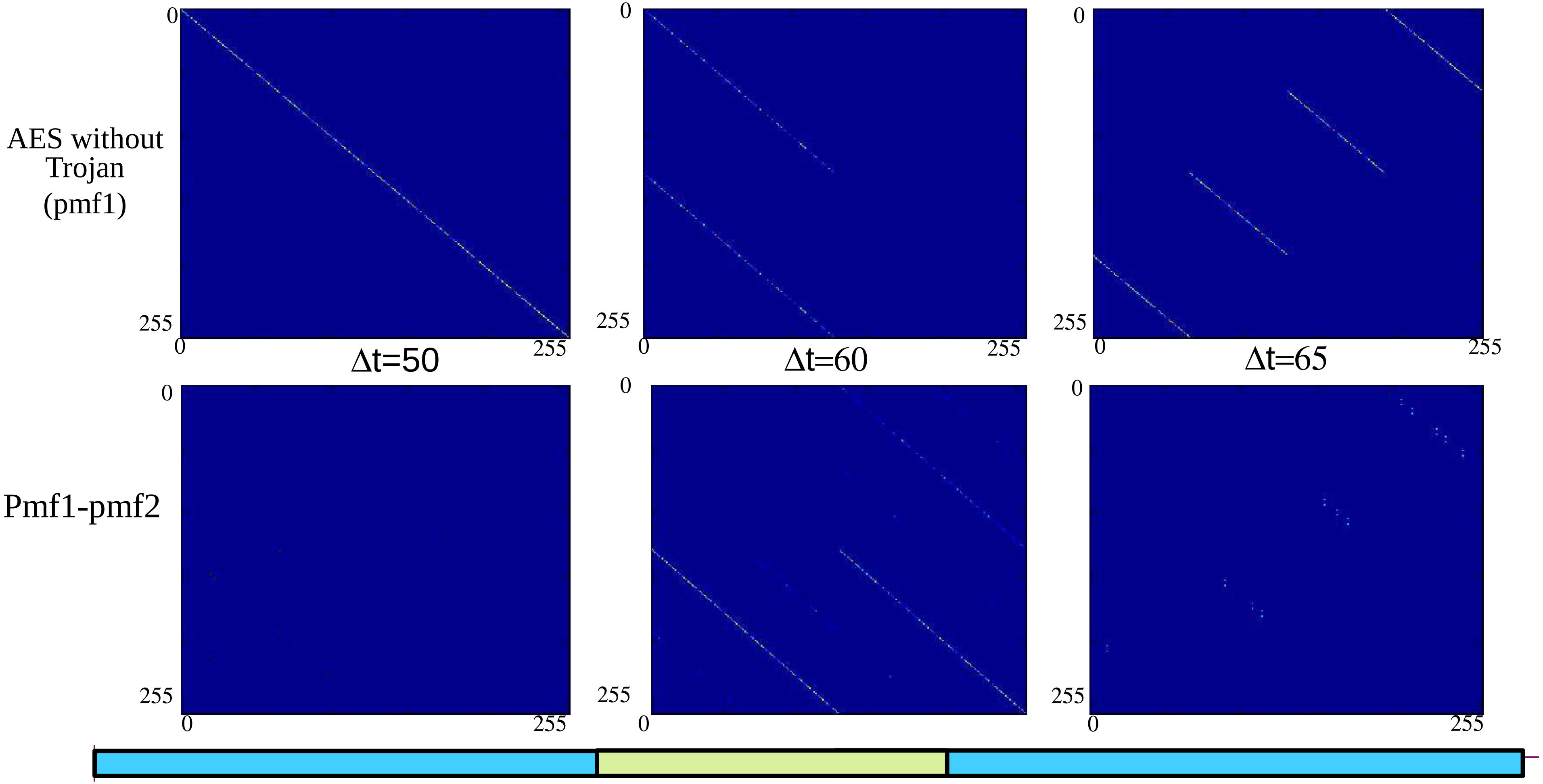


AES-128 on an FPGA

➡ Fundamental hypothesis: the HW Trojan modifies the PMF

THE GOOD OF PHYSICAL FUNCTIONS: HW TROJAN DETECTION

Measure pmf for circuit without (pmf1) and with Trojan (pmf2) and compute pmf1-pmf2



No difference

Difference= TROJAN

Small difference

CONCLUSION AND PERSPECTIVES

Conclusion

- Proposal of a definition of « physical functions » : pmf
- Link with “classical” models and measurments
- Examples of the use of such a definition
  - Model-free attack with error pmf
  - Detection of HW Trojan with error pmf

Perspectives

- Model-free attack with leakage pmf
- Detection of HW Trojan with error pmf
- Combination of error and leakage pmf

Thanks to Driss Aboulkassimi, Ronan Lashermes and Amine Dehbaoui for their help on this work.

Commissariat à l’énergie atomique et aux énergies alternatives
Centre de Saclay | 91191 Gif-sur-Yvette Cedex

Etablissement public à caractère industriel et commercial | R.C.S Paris B 775 685 019

DRT
Institut CEA Tech en Région
Département PACA
Laboratoire SAS