DE LA RECHERCHE À L'INDUSTRIE

cea

MINES Saint-Étienne

www.cea.fr

PHYSICAL FUNCTIONS : THE COMMON FACTOR OF SIDE-CHANNEL AND FAULT ATTACKS ?

Proofs 2014, Busan, Korea

Bruno Robisson, Hélène Le Bouder

Secure Architecture and Systems Laboratory
Joint team between CEA and Ecole des Mines de Saint-Etienne
Gardanne, France

27 SEPT 2014

INTRODUCTION

Intensive research on fault and side-channel attacks (i.e. physical attacks) since late 90's.

Several works for unifying side-channel attacks

+ Several publications on combined attacks

Unify both fault and side channel attacks (except obviously experimental setup) ?

Demonstrate on the AES-128 algorithm

SCHEDULE

Relationships

Models of physical functions

Generic key retrieving algorithms

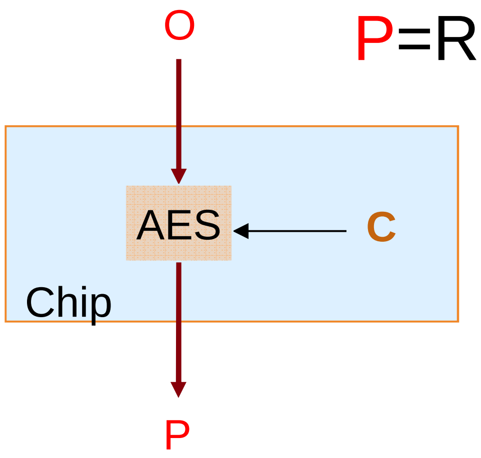
Giraud’s DFA revisited

Conclusion

RELATIONSHIPS : DEFINITION

Mathematical relationship REL
O,P : observables
C: internal data
G: known mathematical functions

P=REL(C,G,O)



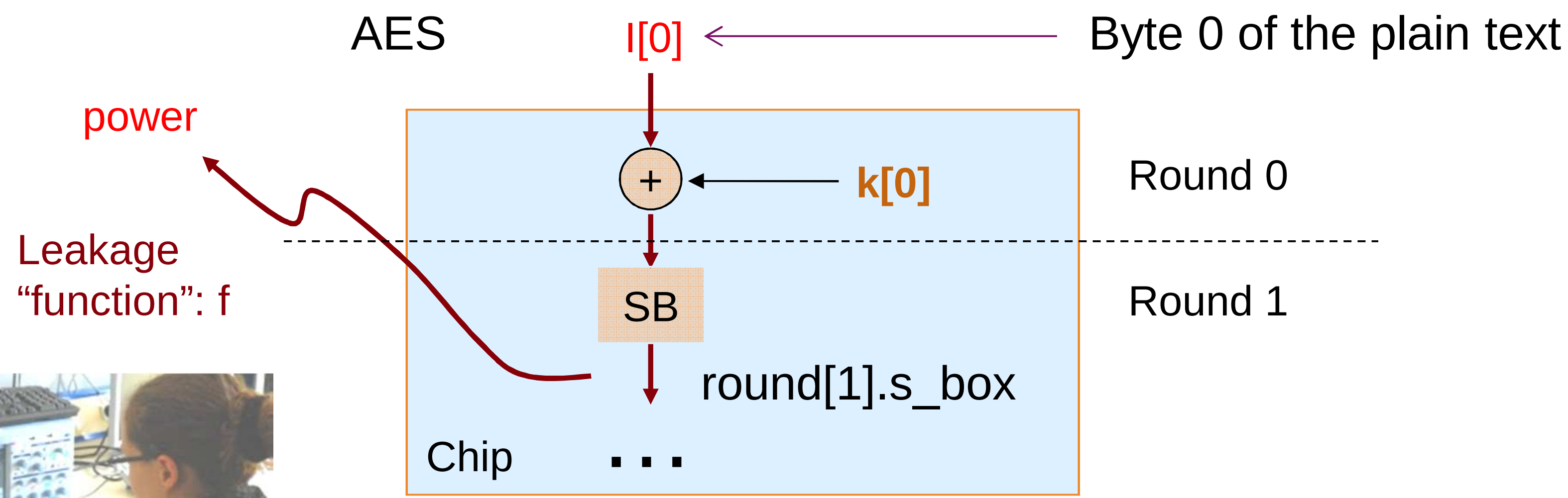
P=AES(O,C)

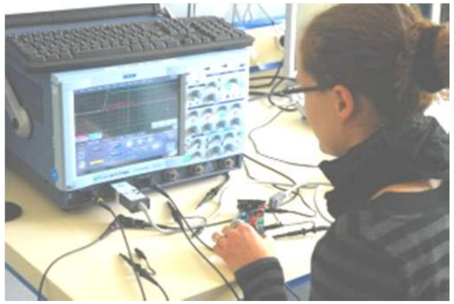
Such mathematical relationships are used for traditional cryptanalysis.
Thanks to ad-hoc experimental setup, the attacker goes « **inside the circuit** ».
This indirect access to the internal data that enables **divide and conquer** approach.

Mathematical and physical relationships REL
O,P : observables
C: internal data
G: mathematical functions
F: **physical functions**

P=REL(C,F,G,O)

RELATIONSHIPS: EXAMPLE 1





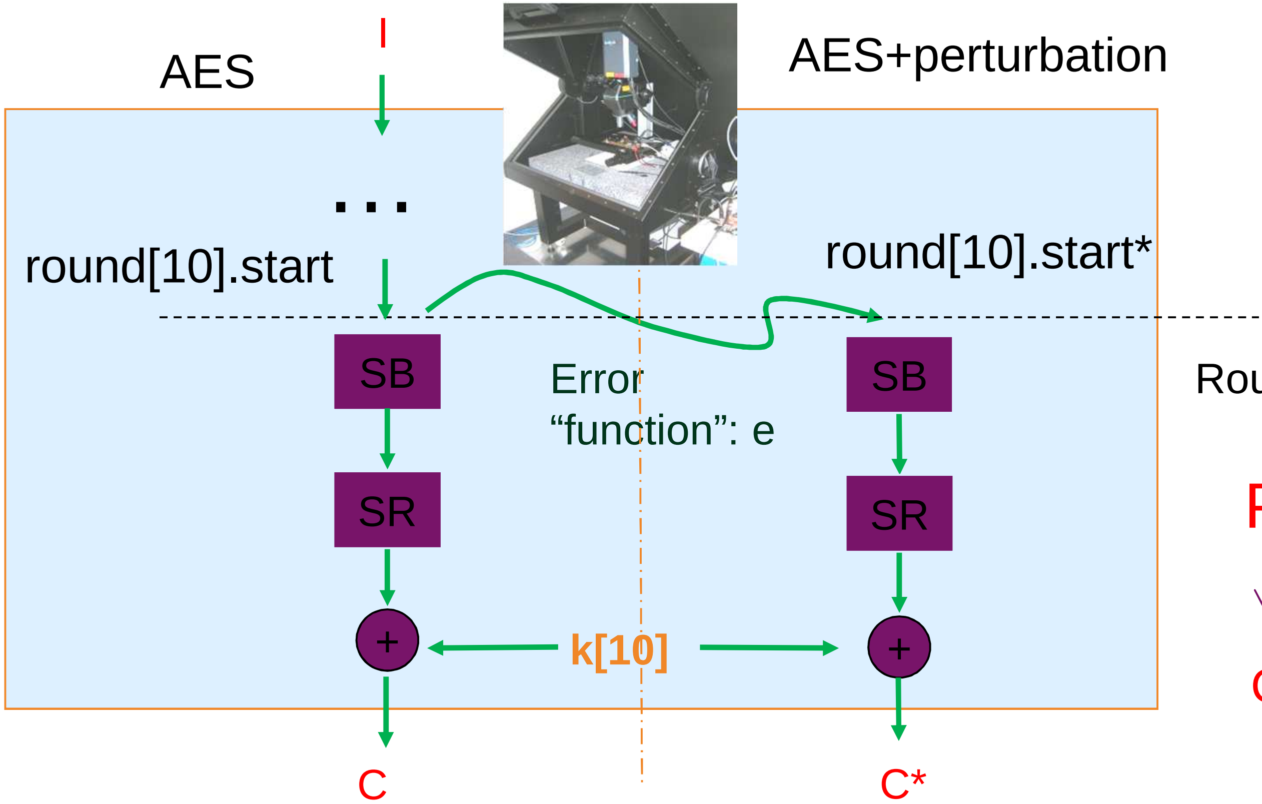
P=REL(C,F,G,O)

Power — k[0] — f — SB, + — I[0]

power= f1 (SB(I[0] + k[0]))

round[1].s_box

RELATIONSHIPS: EXAMPLE 2



$P = REL(C, F, G, O)$

C*

k[10]

e

C

SR
SB
SB^{-1}
SR^{-1}

round[10].start*

$C^* = SR(SB(\ e(\ \ SB^{-1}(SR^{-1}(\ C + k[10]\ ))\ \ )\ ))+k[10]$

round[10].start

RELATIONSHIPS

Mathematical and physical relationships REL
C: internal data
F: (unknown) **physical functions**
G: (known) mathematical functions
O,P : (known) observables

$$P=REL(C,F,G,O)$$

There is no analytical expression of physical functions
ONLY MODELS of physical functions

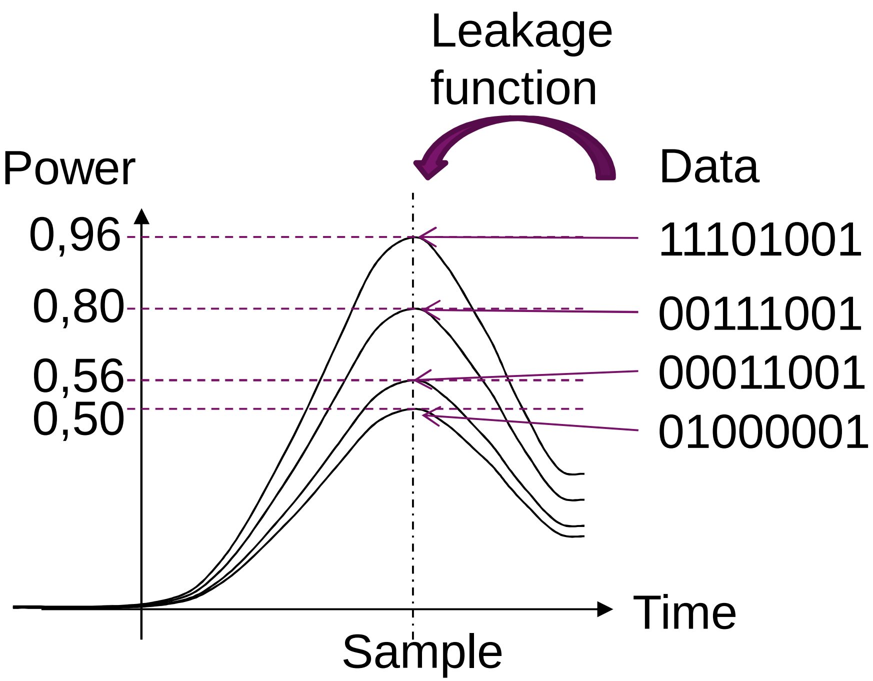
2 kinds of models of physical functions:

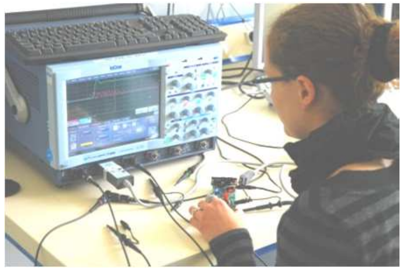
- Deterministic (one input $\rightarrow$ one output)
- Probabilistic (one input $\rightarrow$ probability for one or several outputs)

DETERMINISTIC MODELS OF LEAKAGE FUNCTIONS

Leakage function: DATA → MEASURE

Example 1: power measurement





DATA = 1 byte
MEASURE = Output of the acquisition chain (power probe+amplifier+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

HW, HD, weighted HD or HW are also examples of deterministic leakage functions

DETERMINISTIC MODELS OF ERROR FUNCTIONS

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 byte
DATA = DATA modified by the pertubation mean = 1 byte

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

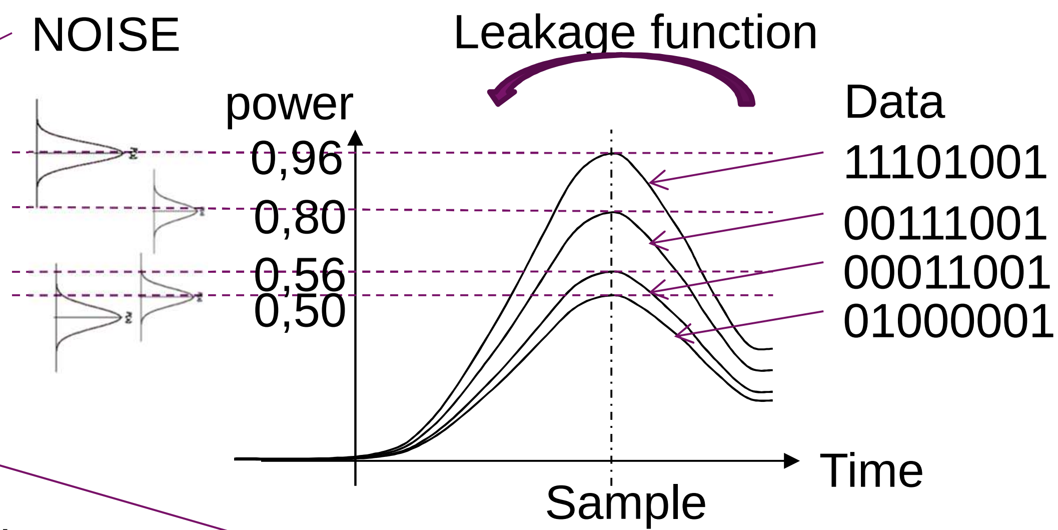
M=# of bits of the data

➡ Bit flip, set, reset, stuck-at, etc. are also examples of deterministic error functions

NEED FOR PROBABILISTIC PHYSICAL FUNCTIONS

- Deterministic physical functions are used for DPA, DBA, FSA, etc.
- Limitation : experimental setup and other data introduce NOISE → has to taken into account in the models

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



MODEL OF PROBABILISTIC PHYSICAL FUNCTIONS

Our proposal :

Probabilistic physical function = Joint probability mass function (pmf)

Example 1:
DATA: $D \rightarrow R$ and
MEASURE: $M \rightarrow R$

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

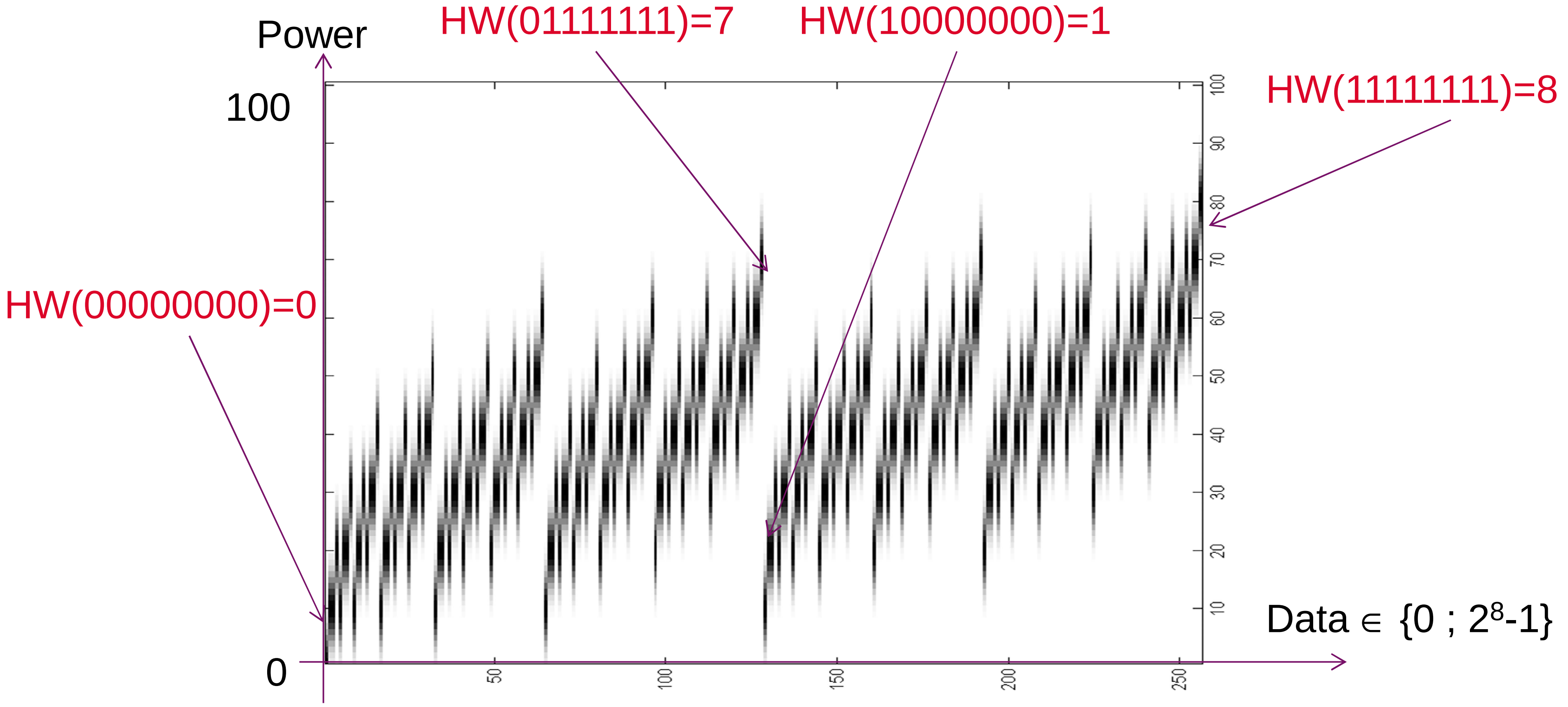
The joint pmf of the discrete variables DATA*MEASURE is
$f_{DATA*MEASURE}: R^2 \rightarrow [0;1]$ defined such that
$f_{DATA*MEASURE}(x,y)=Pr(DATA=x,MEASURE=y)$ whatever x and $y \in R$

EXAMPLE 1 : THEORITICAL LEAKAGE FUNCTION

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

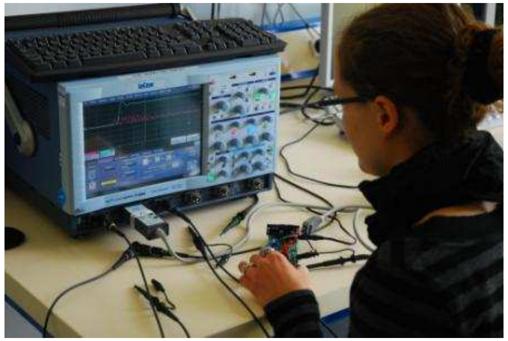
Mean — Standard deviation

Associated pmf:



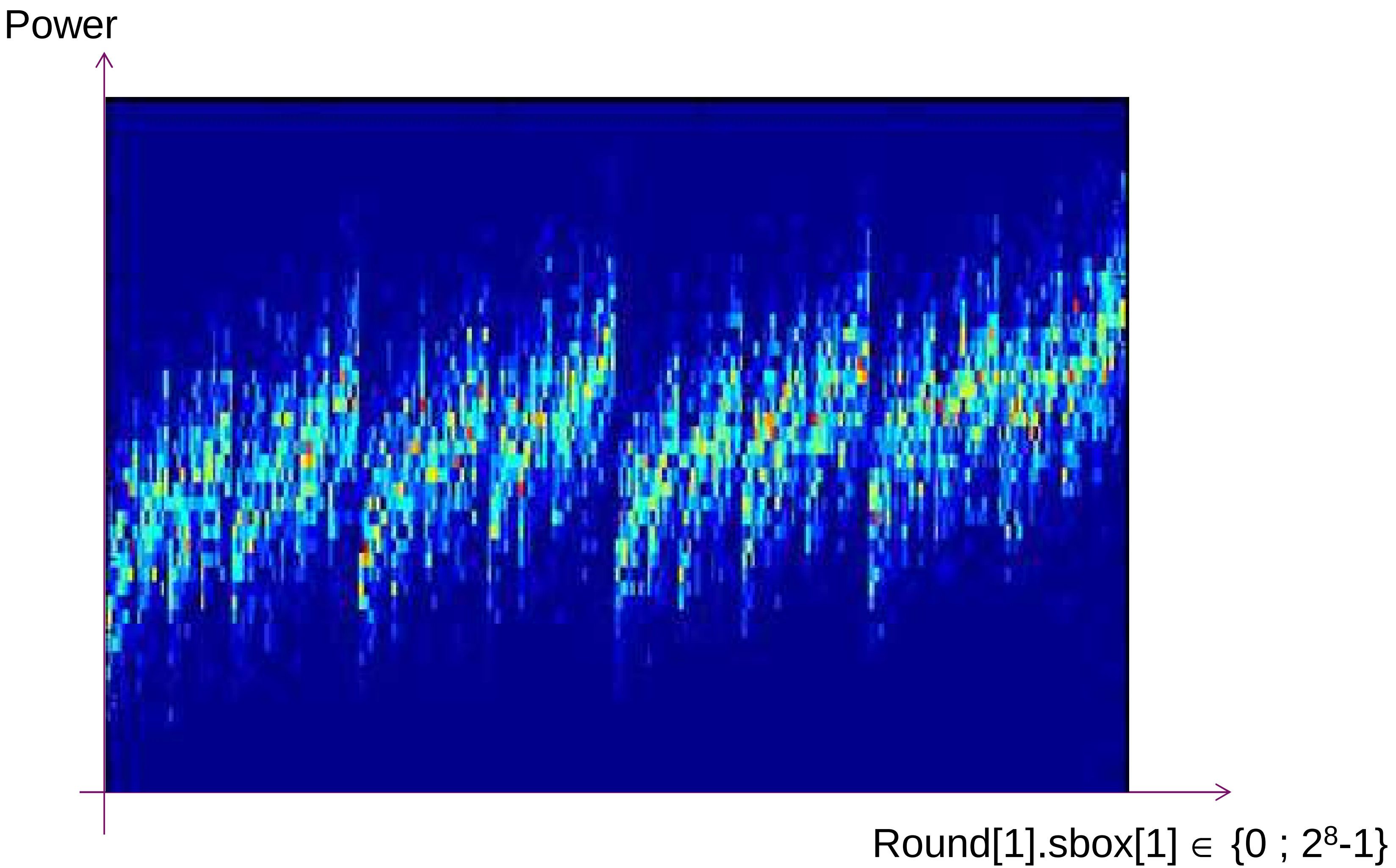
EXAMPLE 2 : REAL LEAKAGE FUNCTION

- 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 $\in$ [0:255])
- Key (known) : 43 00 00 …. 00 00
- Measure = power consumption during round 1
- Data = output of Sbox 1



EXAMPLE 2: REAL LEAKAGE FUNCTION

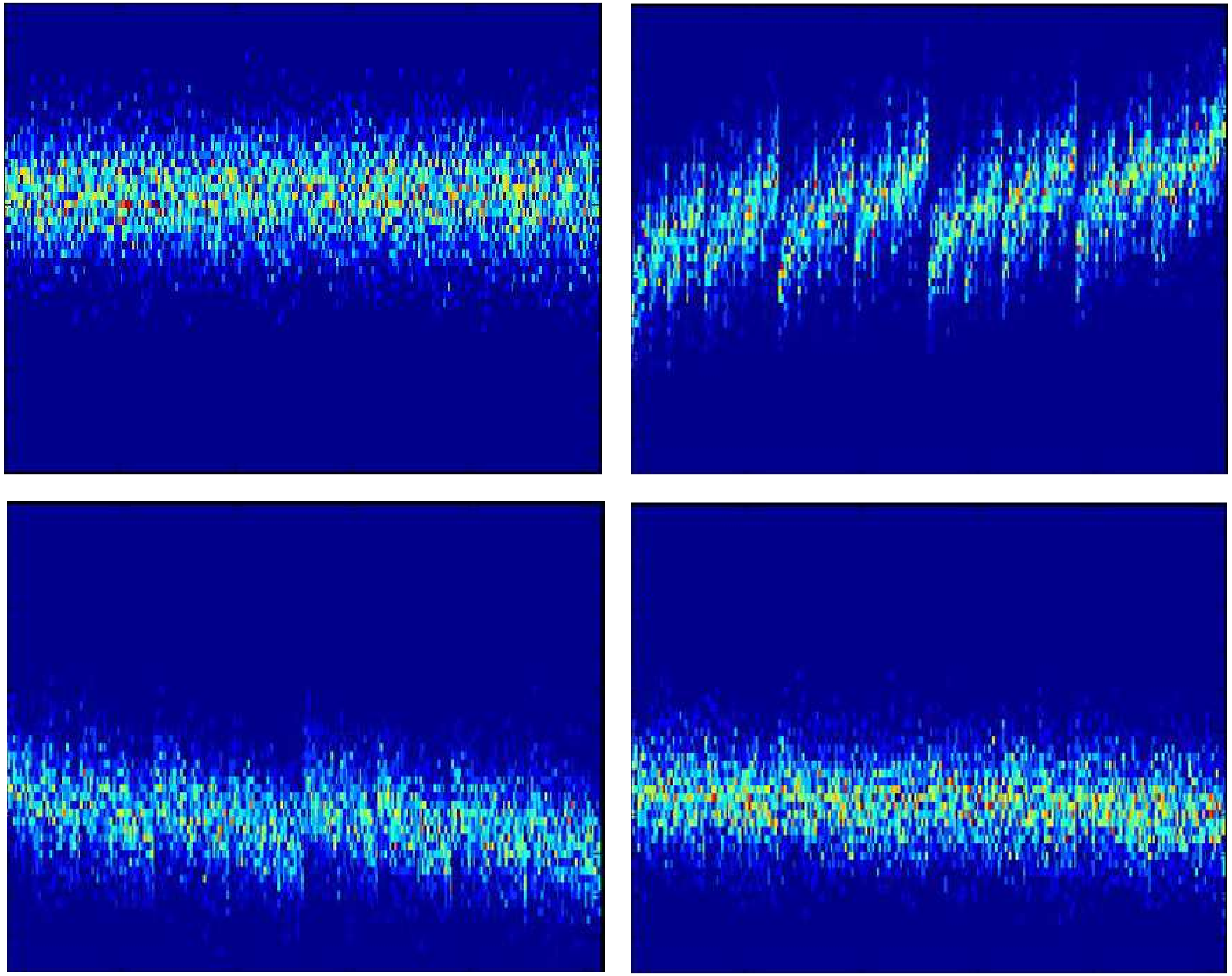
Pmf of a power consumption measured on a 32 bit microcontroller (S Box1, round 1) :



EXAMPLES OF PMF: MEASURE OF LEAKAGE FUNCTION

Start of round

« Start of middle round »



« End of middle round »

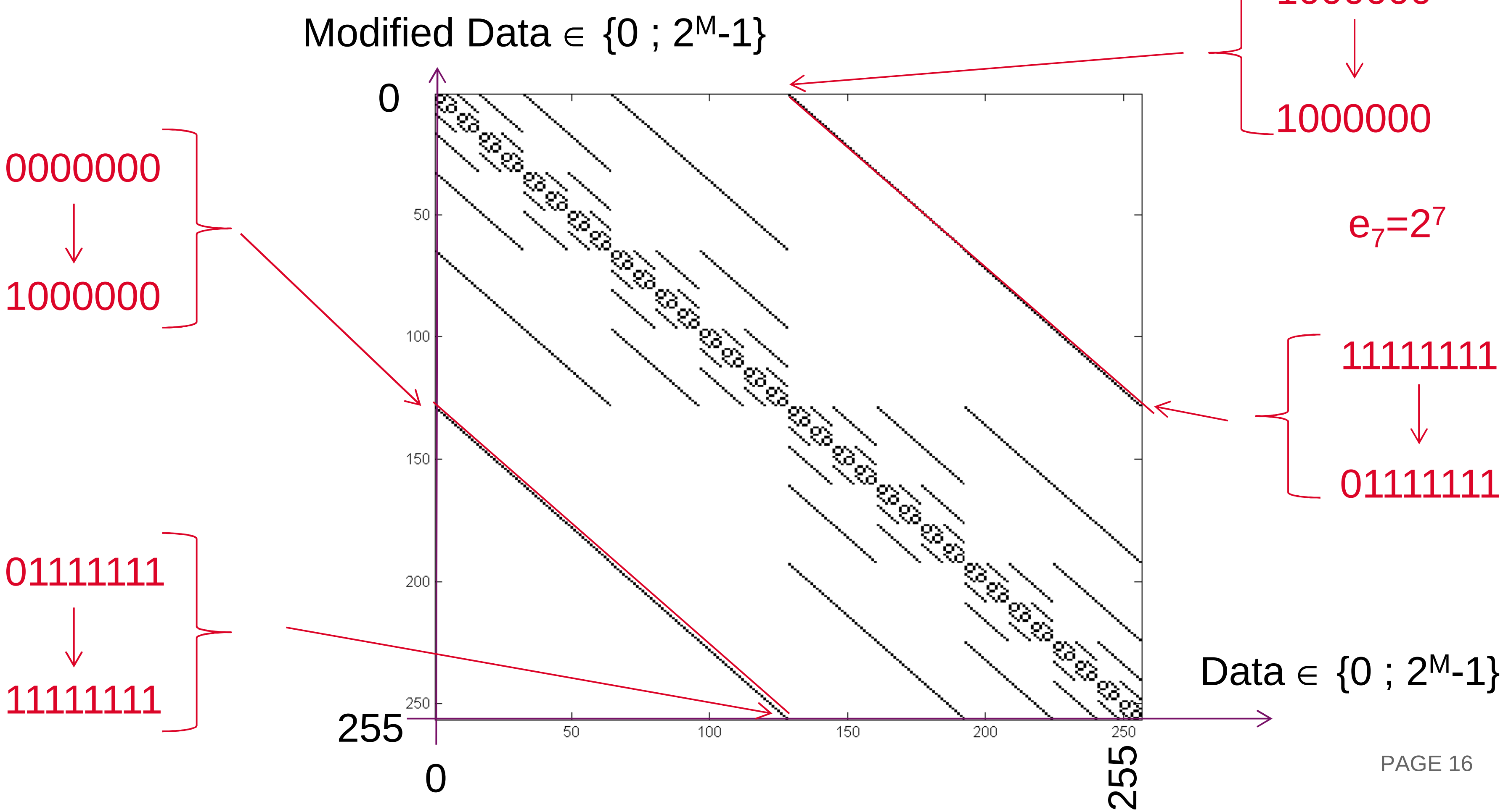
End of round

Impact of sample instant

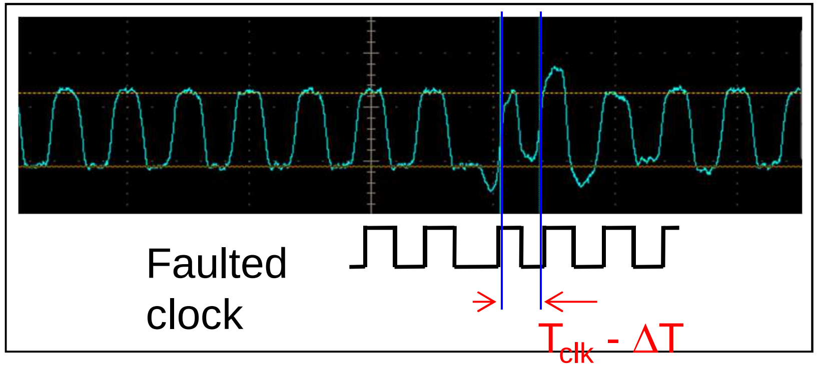
EXAMPLE 3: THEORETICAL ERROR FUNCTION

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:

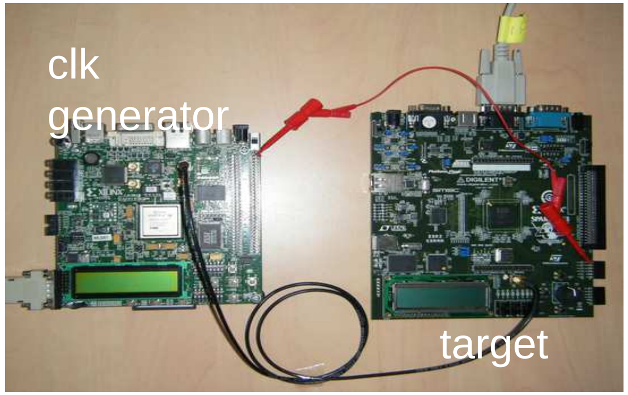


EXAMPLE 4 : REAL ERROR FUNCTION



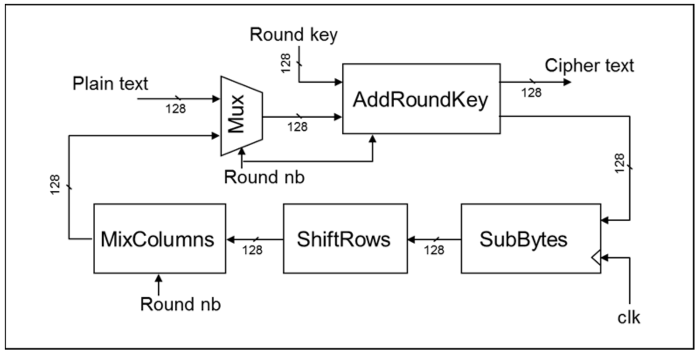
Fault injection principle :

- 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.



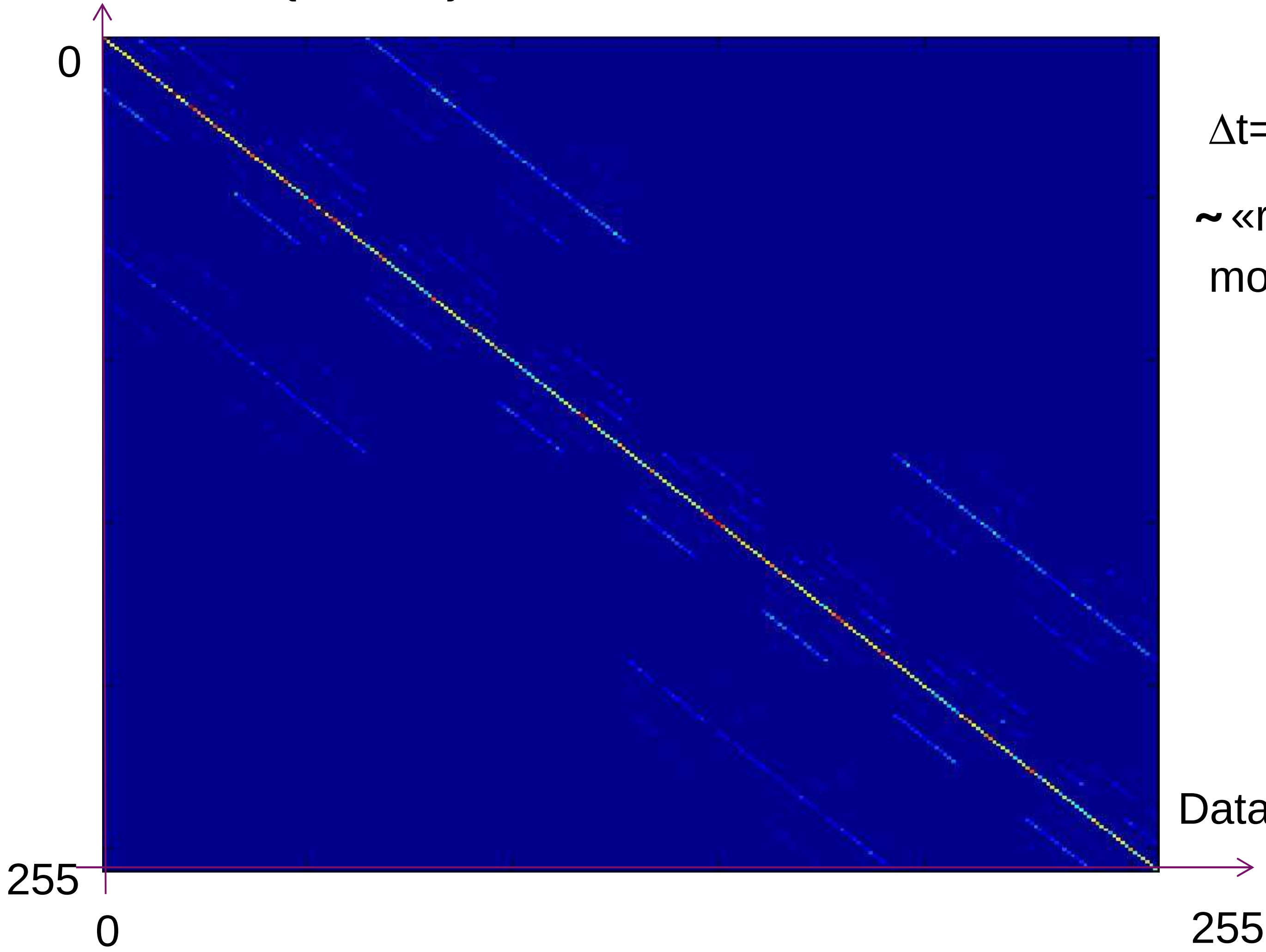
Target

- 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

EXAMPLE 4: REAL ERROR FUNCTION

Pmf of an error function measured on an FPGA implementation of the AES (start, round 10) faulted by using clock glitch :

Modified Data $\in \{0 ; 2^M-1\}$



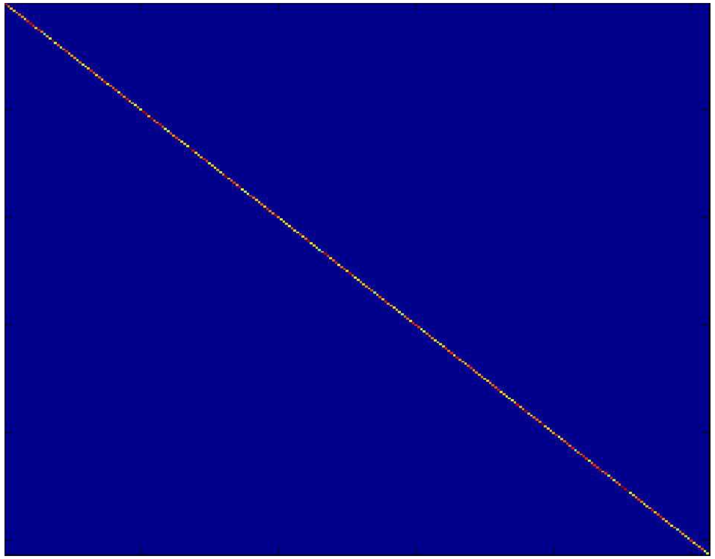
Δt=75:

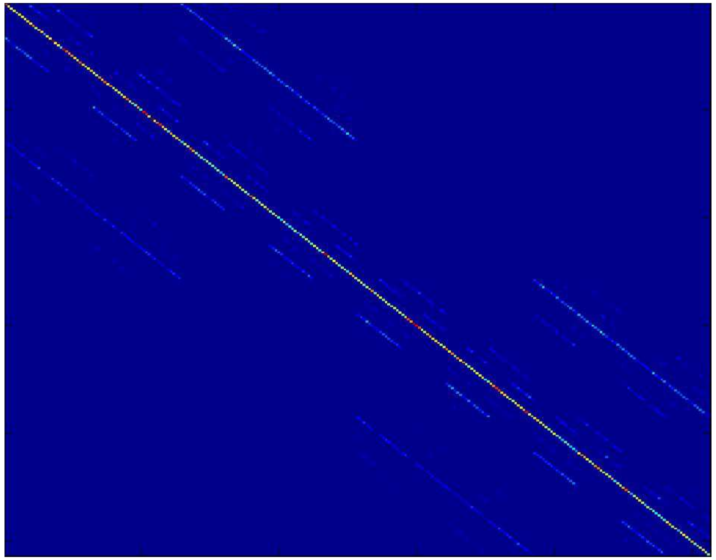
~ «random monobit fault»

EXAMPLE 4: REAL ERROR FUNCTION

Octet 13

Δt=50:
No fault

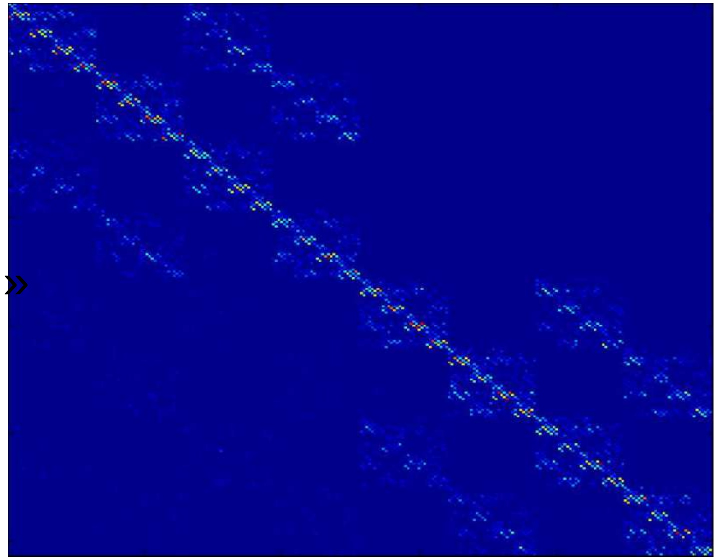


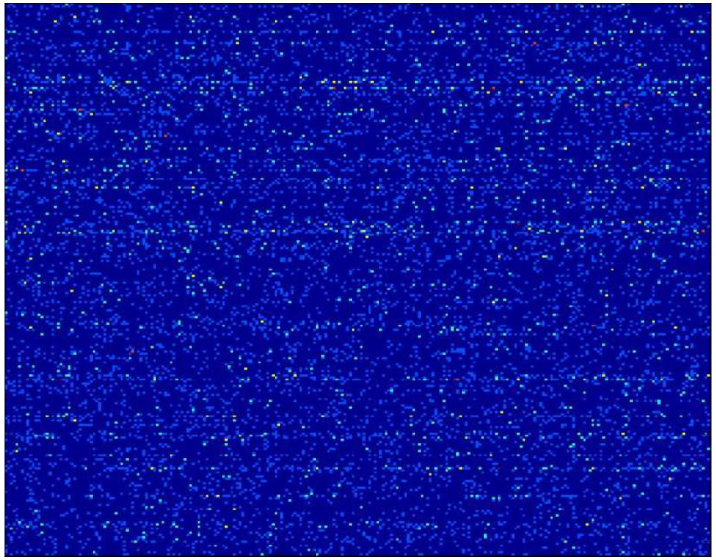


Δt=75:

~ random-
monobit

Δt=90
« strange »





Δt=130
random

PHYSICAL ATTACKS: MAIN PRINCIPLE

Measures

Observables

$$P=REL(C,F,G,O)$$

Internal data

Physical function

Predictions

Hypothesis on internal data

Hypothesis on models physical functions

$$P_{Mod(i,j)}=REL(c_i,f_i,G,O)$$

Predictions of observables

Observables

Compare Measures and Predictions

$P \sim P_{Mod(i,j)}$ when i and j / $c_j = C$ and $f_j \sim F$

Deterministic physical functions $\subset$ Probabilistic physical functions

Described with probabilistic physical functions

KEY RETRIEVING ALGORITHM

Measure P for several values O

$$P = REL(C, F, O) \longrightarrow Pr(P, O)$$

Compute the pmf

For all the models of indexes i and j, predict $Pr(P_{Mod(j,i)})$ from the same values of O

Compute the pmfs

$$P_{Mod(j,i)} = REL(c_i, f_i, O) \longrightarrow Pr(P_{Mod(i,j)}, O)$$

COMPARISON WITH DISTINGUISHERS

$Pr(P,O)$ versus $Pr(P_{Mod(i,j)},O)$

Any measure of « similarity » between the 2 pmf (see [Cha])

$Pr(P,O)$ and $Pr(P_{Mod(i,j)},O)$ ⟶ $Pr(P_{Mod(i,j)}, P)$

Any measure of « dependancy » between $P_{Mod(i,j)}$ and P

Ad Hoc : Sieve, count, distance of means,

Statistical : mutual information, correlation, etc…

$Pr(P_{Mod(i,j)})$ versus $Pr(P)$

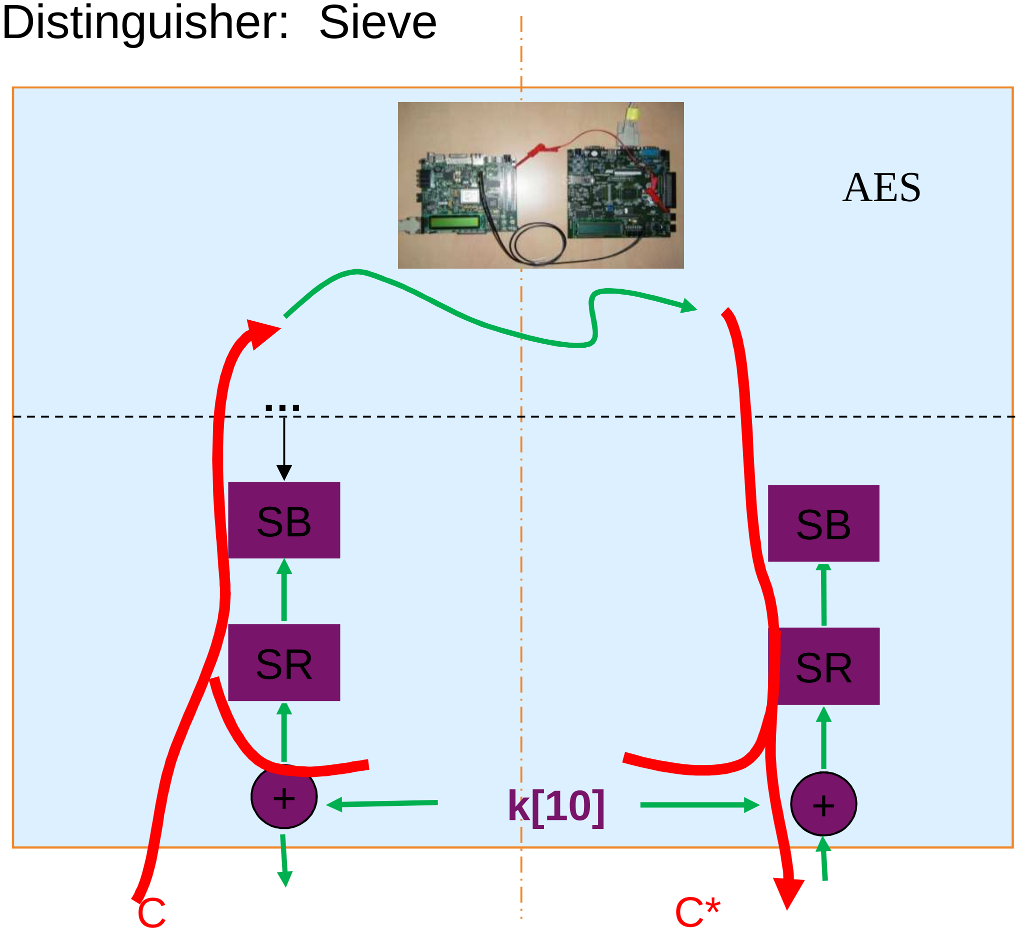
Any measure of « similarity » between these two pmf (see [Cha])

GIRAUD MONOBIT

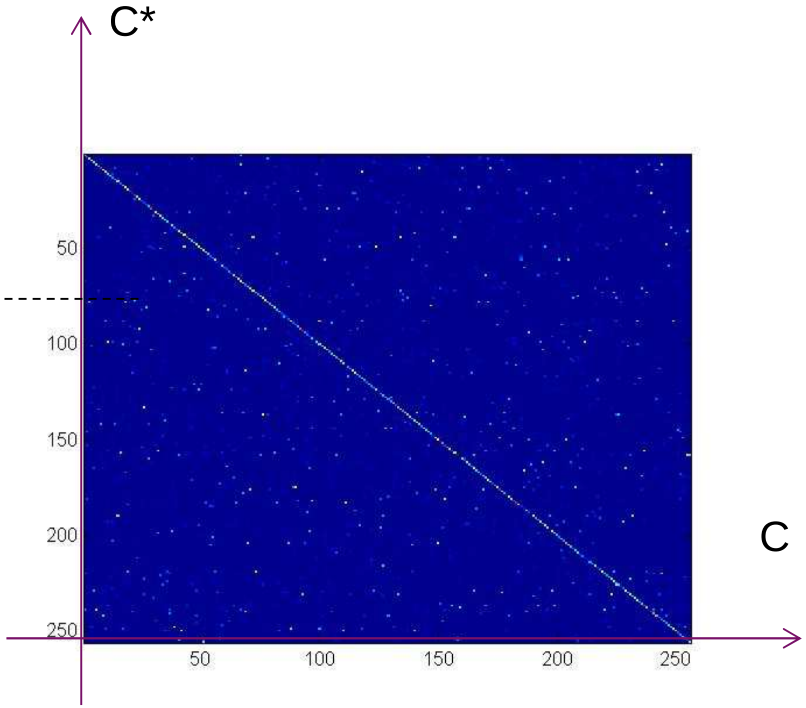
Relationship : $C^* = SR(SB(\, e(\, \underbrace{SB^{-1}(SR^{-1}(\, C + k[10]\,))}\,))) + k[10]$

Hypothesis : Random monobit on round[10].start ;

Distinguisher: Sieve



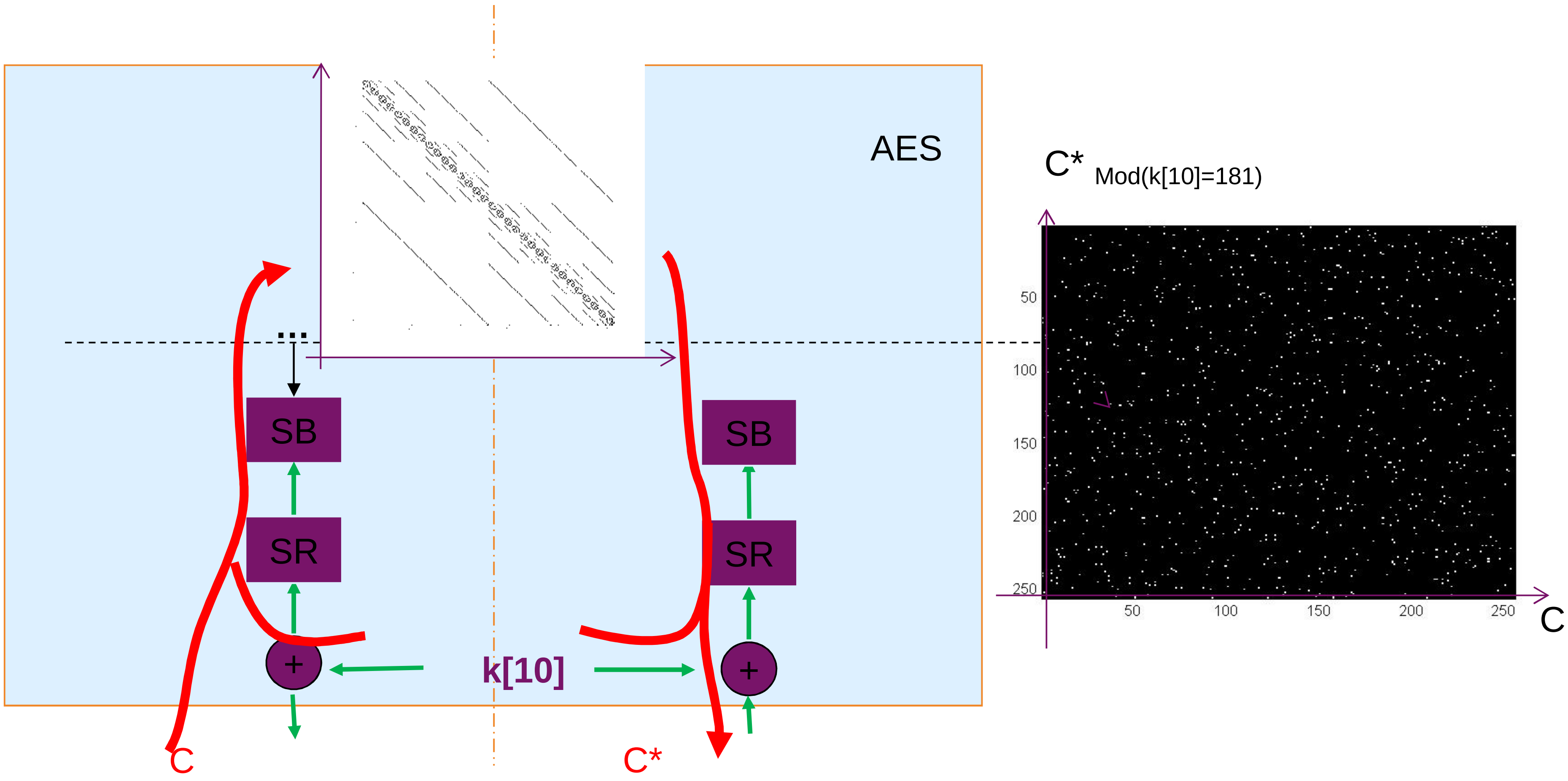
Measure with clock glitch:



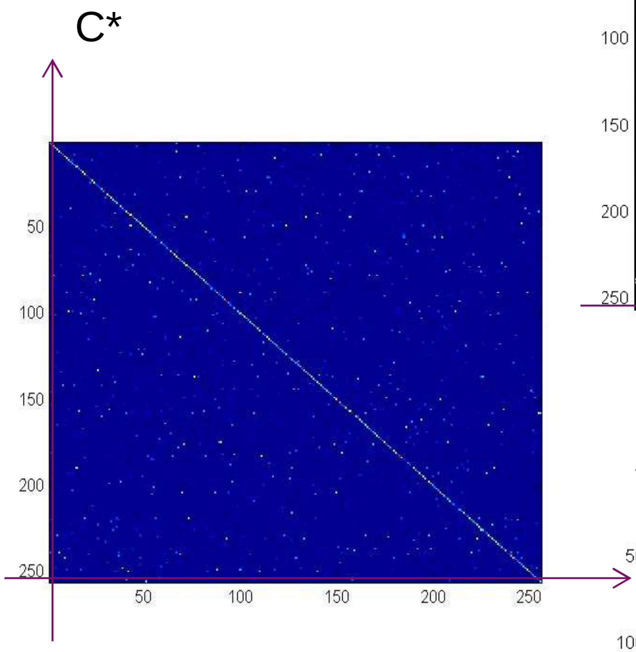
GIRAUD MONOBIT REVISITED

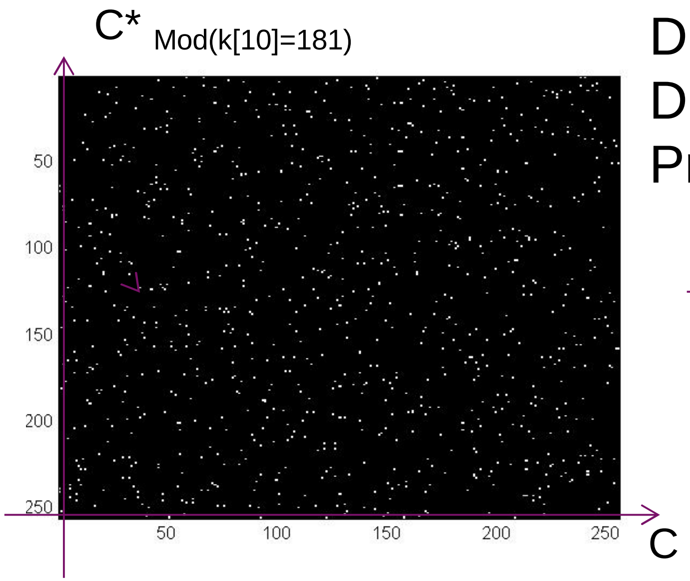
Relationship : $C^* = SR(SB(e(SB^{-1}(SR^{-1}(C + k[10]))))) + k[10]$

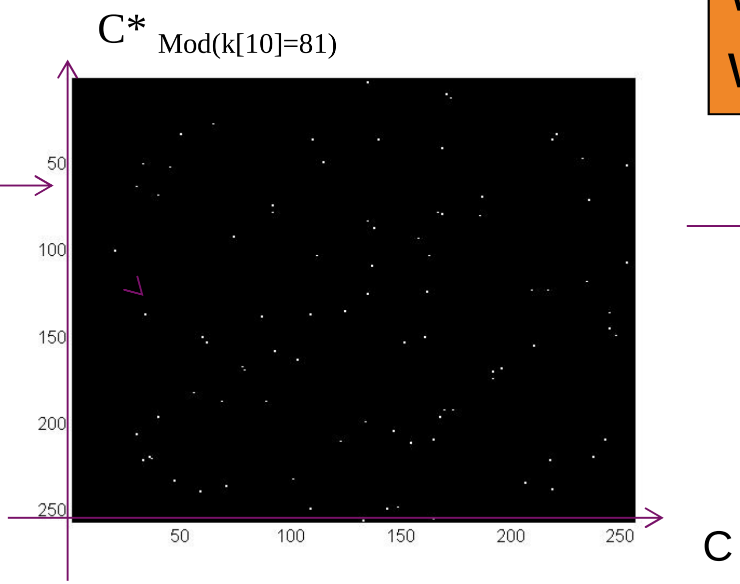
Hypothesis : Random monobit on round[10].start



GIRAUD MONOBIT REVISITED







Distinguisher :
D=ΣΣ Pmf(C,C*)≠0 and
Pmf(C,C**) ≠0

→ d=937
(1000 experiments)

CPA on
Pr($C^*_{Mod(k[10]}$, C*)
works also very
well

→ d=87
(1000 experiments)

RESULTS

A long list of physical attacks are covered by this formalism:

Attack	Relationships	Physical function	Kind of physical functions	Similarity and distance tools
Semi-exhaustive (on octet j)	R_0 $O = \{plain\}$ $P = \{cipher\}$ $C = \{k\_sch[0]\}$	$f(x) = x$ if x is the j^{th} octet $f(x) = 0$ else	Determ.	All
μ-probing	R_1 $O = \{plain^j\}$ $P = \{probe\}$ $C = \{k\_sch[0]^j\}$	$f(x) = R_\Omega(x)$ with $\Omega \in \{1, 2, 4, \ldots, 128\}$	Determ.	All
DPA [8]	R_2 $O = \{cipher^j\}$ $P = \{Power\}$ $C = \{k\_sch[10]^j\}$	$f(x) = R_\Omega(x)$ with $\Omega \in \{1, 2, 4, \ldots, 128\}$	Determ.	DoM or Pearson correlation
CPA [3]	R_1 $O = \{plain^j\}$ $P = \{power\}$ $C = \{k\_sch[0]^j\}$	$f(x) = HW(x \oplus \Omega)$ with $\Omega \in [\![1, 255]\!]$	Determ.	Pearson correlation
MIA [18]	R_1 $O = \{plain^j\}$ $P = \{power\}$ $C = \{k\_sch[0]^j\}$	$f(x) = HW(x) + N$ with N a Gaussian noise	Probab.	Mutual information
DFA1 [7]	R_3 $O = \{cipher^j\}$ $P = \{faulted^j\}$ $C = \{k\_sch[10]^j\}$	$f(x) = x \oplus \Omega$ with $\Omega \in \{1, 2, 4, \ldots, 128\}$ and $(Pr(\Omega) = 1/8)\ \forall \Omega$	Probab.	Sieve
DFA2 [16]	R_4 $O = \{cipher^j\}$ $P = \{faulted^j\}$ $C = \{k\_sch[10]^j,$ $round[9].m\_col^j\}$	$h(x) = x$ and $g(x, \Omega) = x \oplus \Omega$ with $\Omega \in [\![1, 255]\!]$ $f(y, \Gamma) = y \oplus \Gamma$ with $\Gamma \in [\![1, 255]\!]$	Determ.	Count
DFA+ [16]	R_4 $O = \{cipher^j\}$ $P = \{power\}$ $C = \{k\_sch[10]^j,$ $round[9].m\_col^j\}$	$h(x) = HW(x)$ f and g as above	Determ.	Pearson correlation
DBA [15]	R_1 $O = \{plain^j\}$ $P = \{behavior\}$ $C = \{k\_sch[0]^j\}$	$f(x) = (R_\Omega(x) == 0)$ with $\Omega \in [\![1, 255]\!]$	Determ.	Pearson correlation
FSA [12]	R_2 $O = \{cipher^j\}$ $P = \{intensity^j\}$ $C = \{k\_sch[10]^j\}$	$f(x) = HW(x)$ or $f(x) = R_\Omega(x)$ with $\Omega \in \{1, 2, 4, \ldots, 128\}$	Determ.	Pearson correlation

Table 2. Examples of physical attacks and associated parameters

Described by only three main parameters

- -Relationships
- -Models of physical function
- -Distinguisher

CONCLUSION AND PERSPECTIVES

Conclusions

- Proposal of a model of physical functions
- Create a formal link between a wide class of fault and side-channel attacks
- Choice of the model more important than the choice of the distinguisher

Perspectives

- Extend to other attacks (for example on public key algorithms)
- Determine new relationships and combine existing attacks
- Analyze the impact on protections
- Answer many open questions, among them
  - How to find the physical function which leaks the most?

Thanks to D. Aboulkassimi, J.-M Dutertre, I. Exurville, J. Fournier, R. Lashermes, J.-B. Rigaud, A. Tria and Jean-Yves Zie 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