

« Differential Behavioral Analysis »

Bruno ROBISSON
Pascal MANET

CEA-LETI

SESAM Laboratory (joint R&D team CEA-LETI/EMSE),
Centre Microélectronique de Provence
Avenue des Anémones, 13541 Gardanne, France

© CEA 2006. Tous droits réservés.

Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA
All rights reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA

Introduction

Differential Behavioral Analysis

- Hypothesis

- Description

- Result interpretation

- Simple case study on AES-128

Relaxing fault hypothesis

- Minimum number of faulty text

- Wrong injection

- Fault multiplicity

Comparison with existing fault attacks

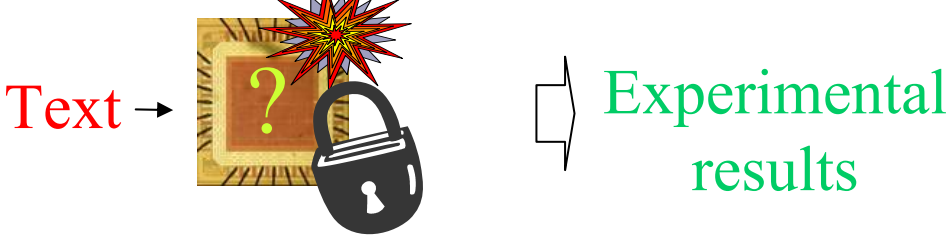


Fault attacks

Leti

Fault injection

Vcc, clk, T, flash, laser, etc...



Attack inputs

Cipher texts

Side Channels

Behavior

Methods

Differential Fault Analysis (DFA)

Fault based Collision

Safe-error (SEA)

#faulty executions

few

few

many

Fault constraints

light

strong

~~Very strong~~ **medium**

Safe-error Key bits leak only through the information whether the device has a normal **behavior** or not in presence of fault

+ DPA **Correlating** a power model parameterized by the value of a small number of bits of the key (the partial key) to power measurements

Differential Behavioral Analysis

Correlating a functional model parameterized by the value of a partial key to **behaviors** of the device in presence of faults

➤ DPA-like hypothesis

- Known cryptographic algorithms,
- Known plain texts (or cipher texts)
- There must exist intermediate variables (attack bits) that can be expressed as functions depending on the plain texts and on only a small number of key bits

➤ Fault injection

- Location : On nodes and instants corresponding to the computation of the attack bits
- Type : « Stuck-at » possibly of unknown value but identical for each impacted bits
- Focalization: Must impact only small number of bits (typically less than 8)
- Repetitivity : Same error for different plaintexts

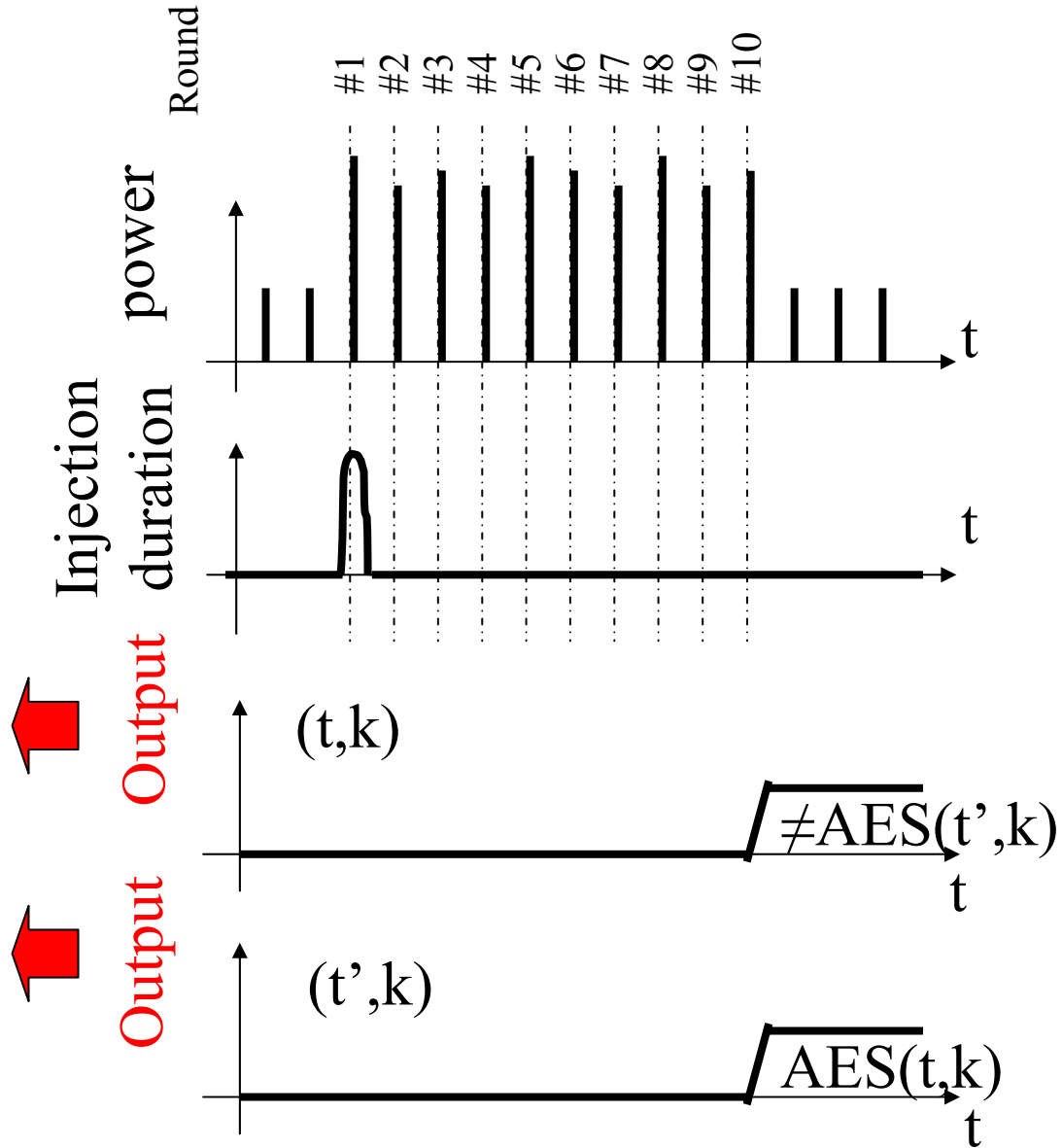
➤ Distinguish faults which create an error during round one or during another round

- Synchronous AES hardware without DFA countermeasure
- Precise control on the fault occurrence time
- Cipher texts

Input for DBA

Fault created an error during round 1

Fault did not create an error during round 1

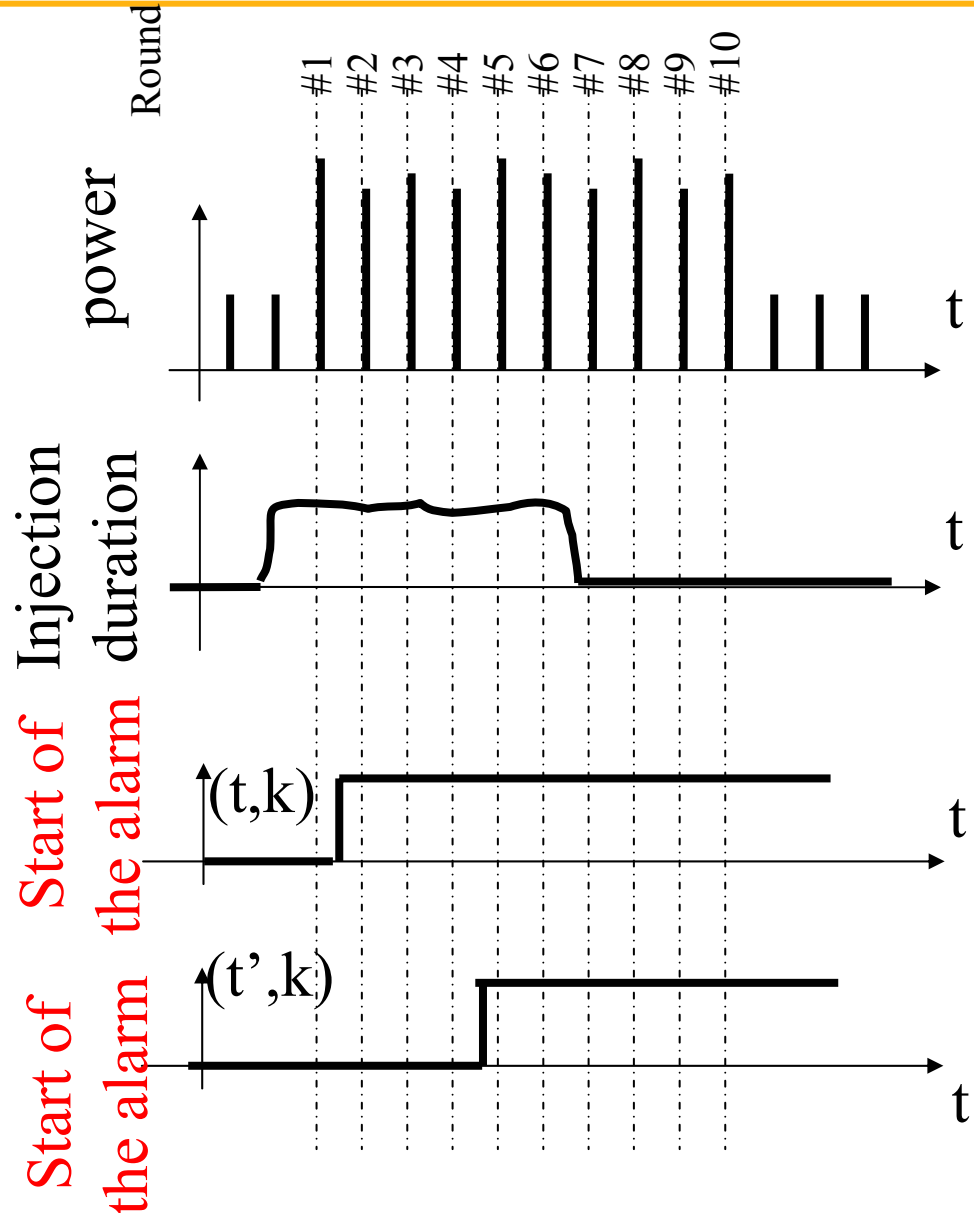


- Synchronous AES hardware with DFA countermeasure (EDC-based)
- Raw control on the fault occurrence time
- Alarm signal

Input for DBA

Fault created an error during round 1

Fault did not create an error during round 1 (but in round 4)

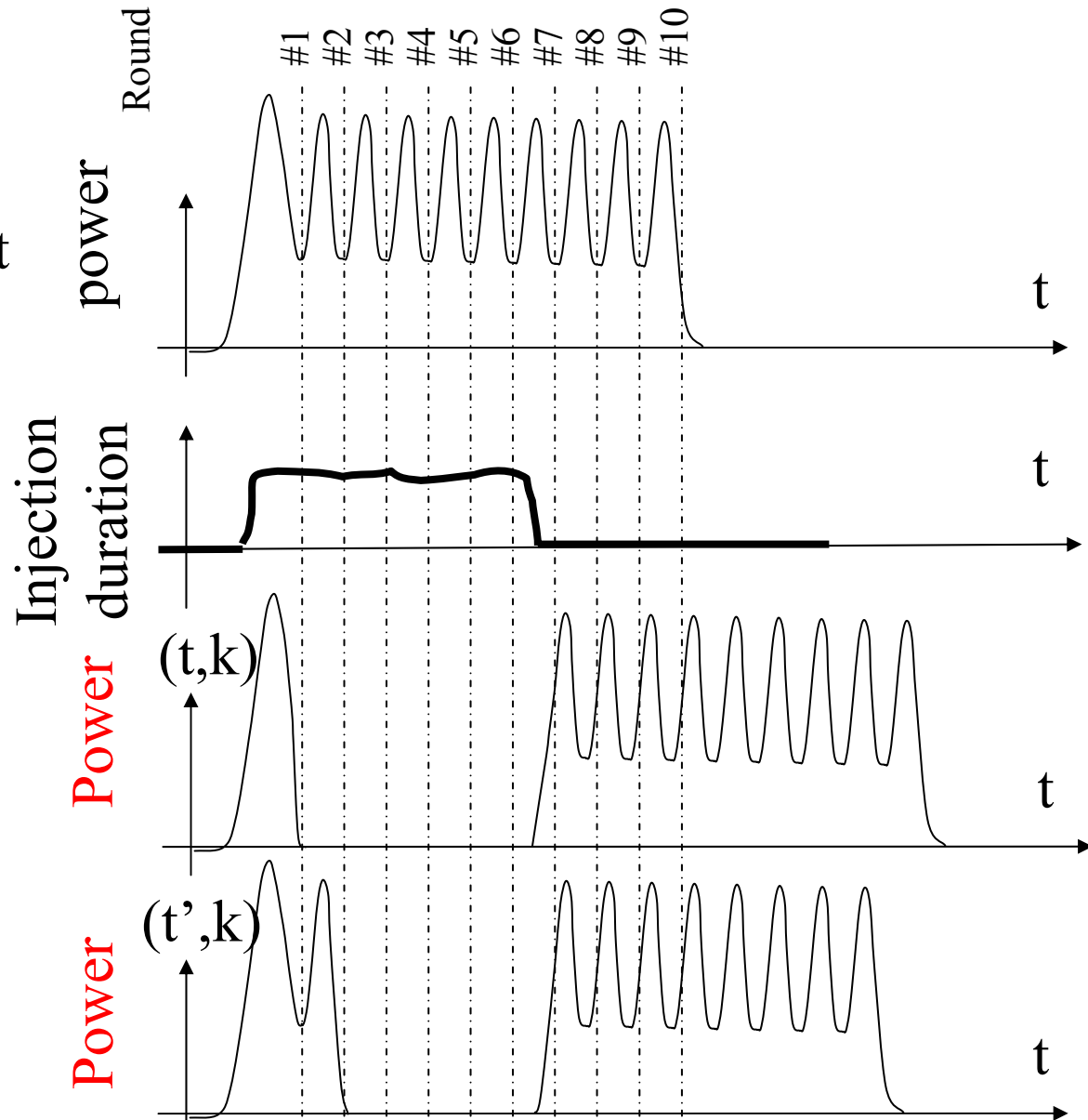


- Asynchronous AES hardware
- Raw control on the fault occurrence time
- Power consumption

**Input
for
DBA**

Fault created
an error during
round 1

Fault did not
create an error
during round 1
(but in round 2)



Modeling

(predicting the value of the attack bits for different guess keys)

Experimentations



Correlation

Value of the partial key

K : set of guess keys

T : set of plaintexts

B : set of attack bits

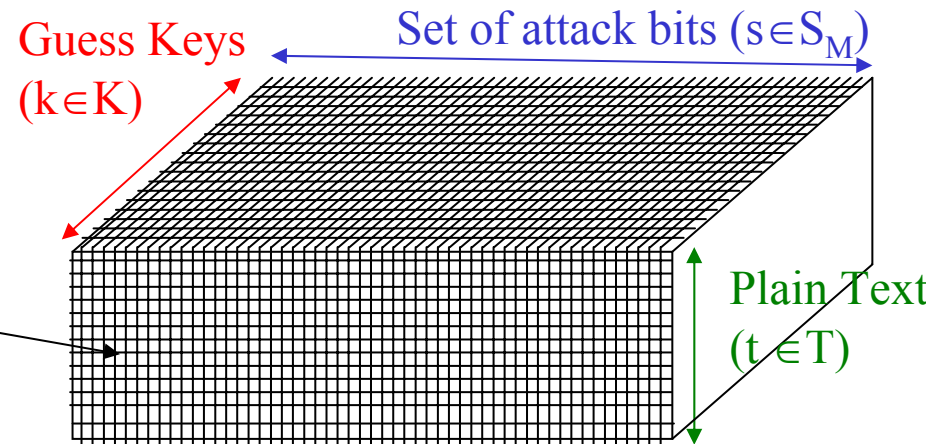
M : number of bits in **B** which are supposed to be faulty ($M < |B|$)

S_M : all the possible partial sets from **B** with at most M elements and at least one

f (optional) : value of the “stuck-at” fault (in $\{0;1\}$)

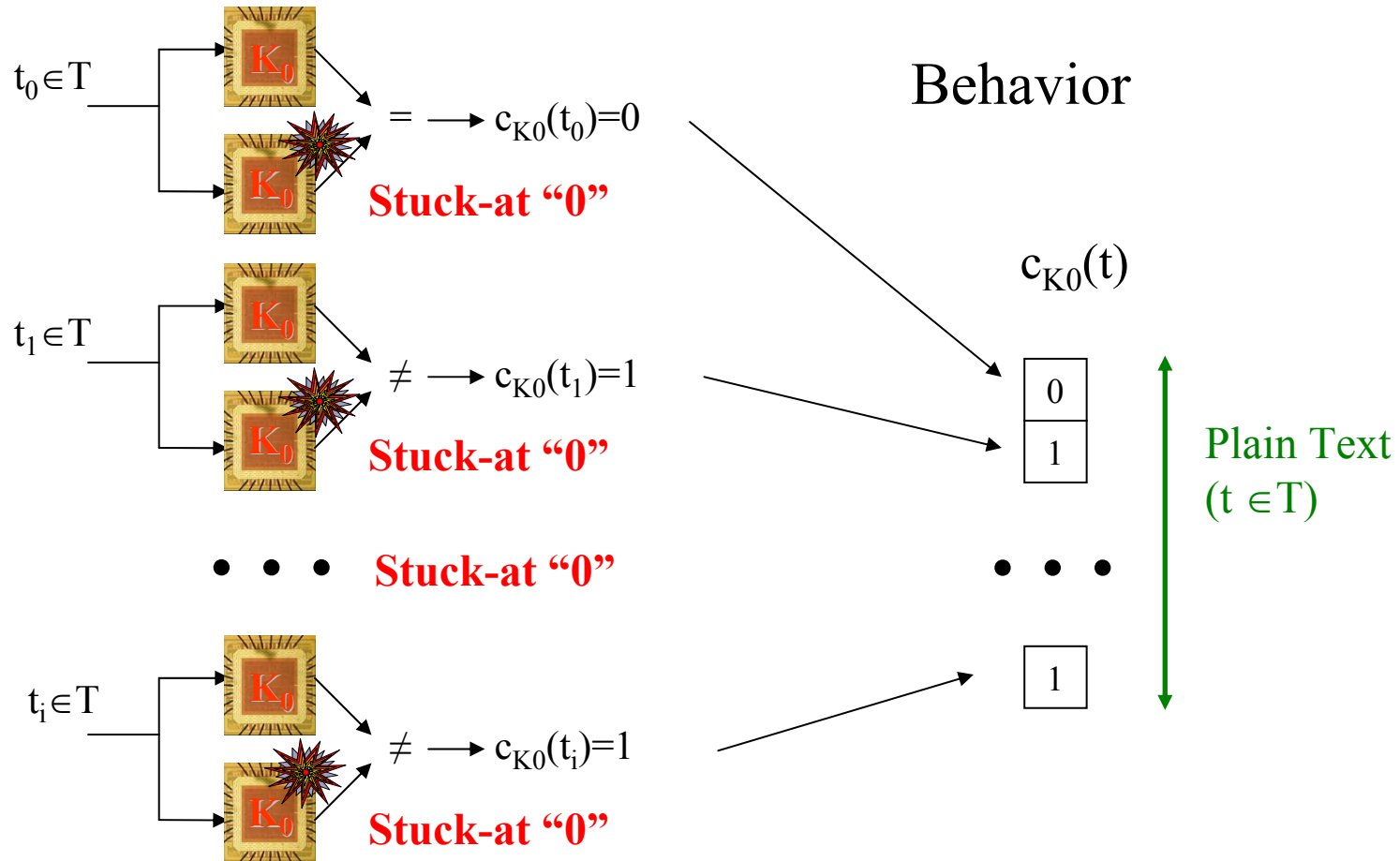
Given M and f , compute $r^f(s,k,t)$ for all $k \in K$, $t \in T$ and $s \in S_M$

$r^f(s,k,t)$: 0 if all the bits of s
are equal to f
1 otherwise

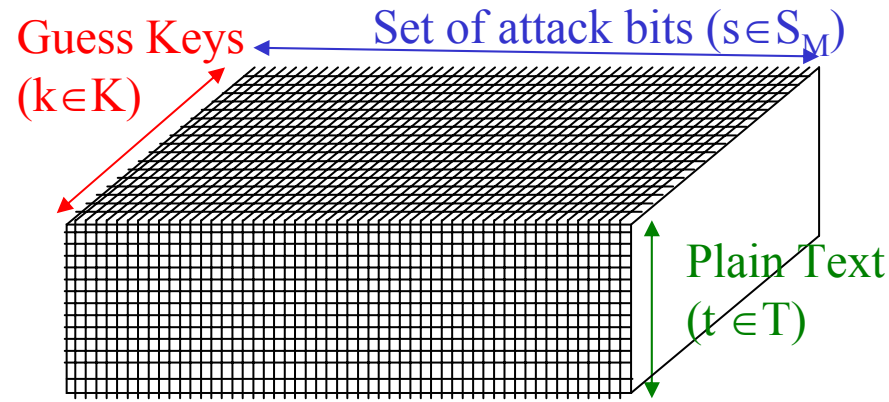


DBA : experimentations

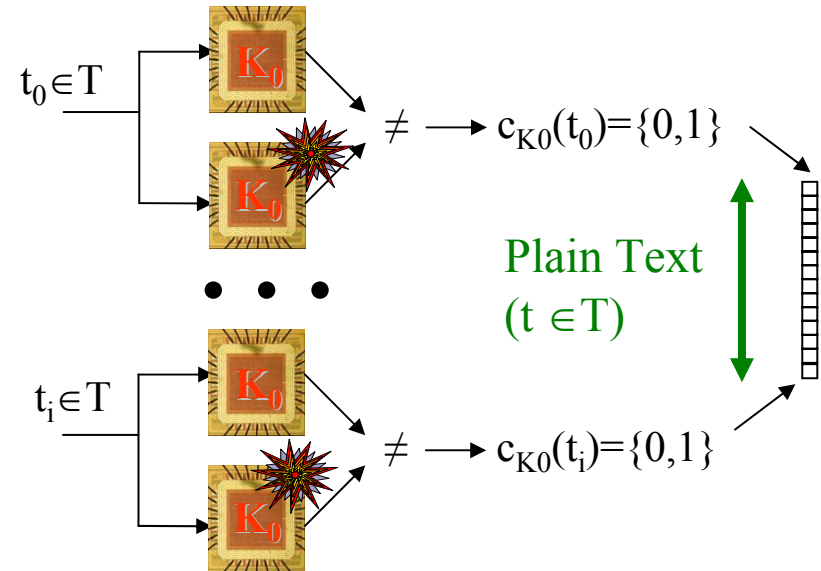
0: fault create an error during round 1
 1: otherwise



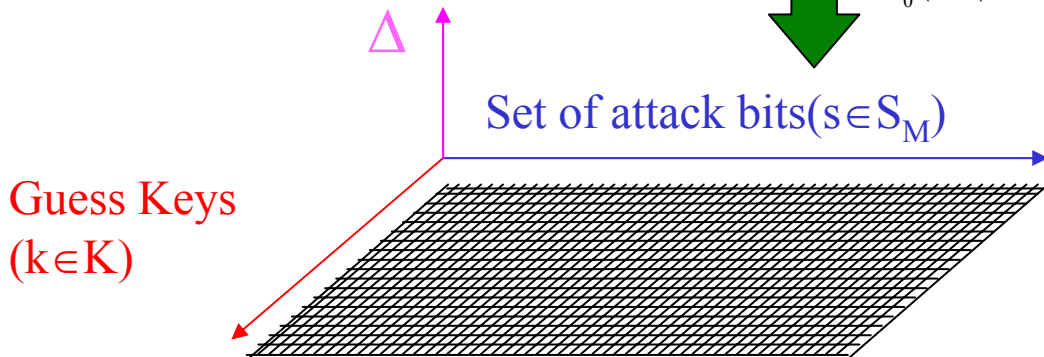
Parameterized modeling



Experimentations



$$\Delta_{K_0}^T(s, k) = \frac{\sum_{t \in T} (r^f(s, k, t) * c_{K_0}(t) + (1 - r^f(s, k, t)) * (1 - c_{K_0}(t)))}{|T|}$$




- Value of the partial key
- Set of the faulty bits
- Value of the stuck at fault
- Repetitivity of the fault injection


Parameterized modeling

- T : set of the 256 plain texts which exhaust the S-box 0 entries
- K : set of the 256 guess keys which exhaust the S-box 0 entries
- B : the 8 bits at the output of S-box 0 during first round
- M=1 (so $S_1 = \{ \{SB_0(t \oplus k)\}, \{SB_1(t \oplus k)\}, \dots, \{SB_7(t \oplus k)\} \}$)
- f=0

Simulated experimentations

- Standardized algorithmic description of the AES_{128}
- Modified algorithmic description of the $AES_{128} \rightarrow$ Stuck-at zero, during first round, on **one** bit at the output of S-box 0
- Encryption of each element of T with the unknown key K0 with AES_{128} and with the modified one AES'_{128}

 $r^0(s, k, t) \quad \forall (s \in S_1, t \in T, k \in K)$

 $c_{K0}(t) = (AES_{128}(t, K0) = = AES'_{128}(t, K0))$

Monobit DBA on AES-128

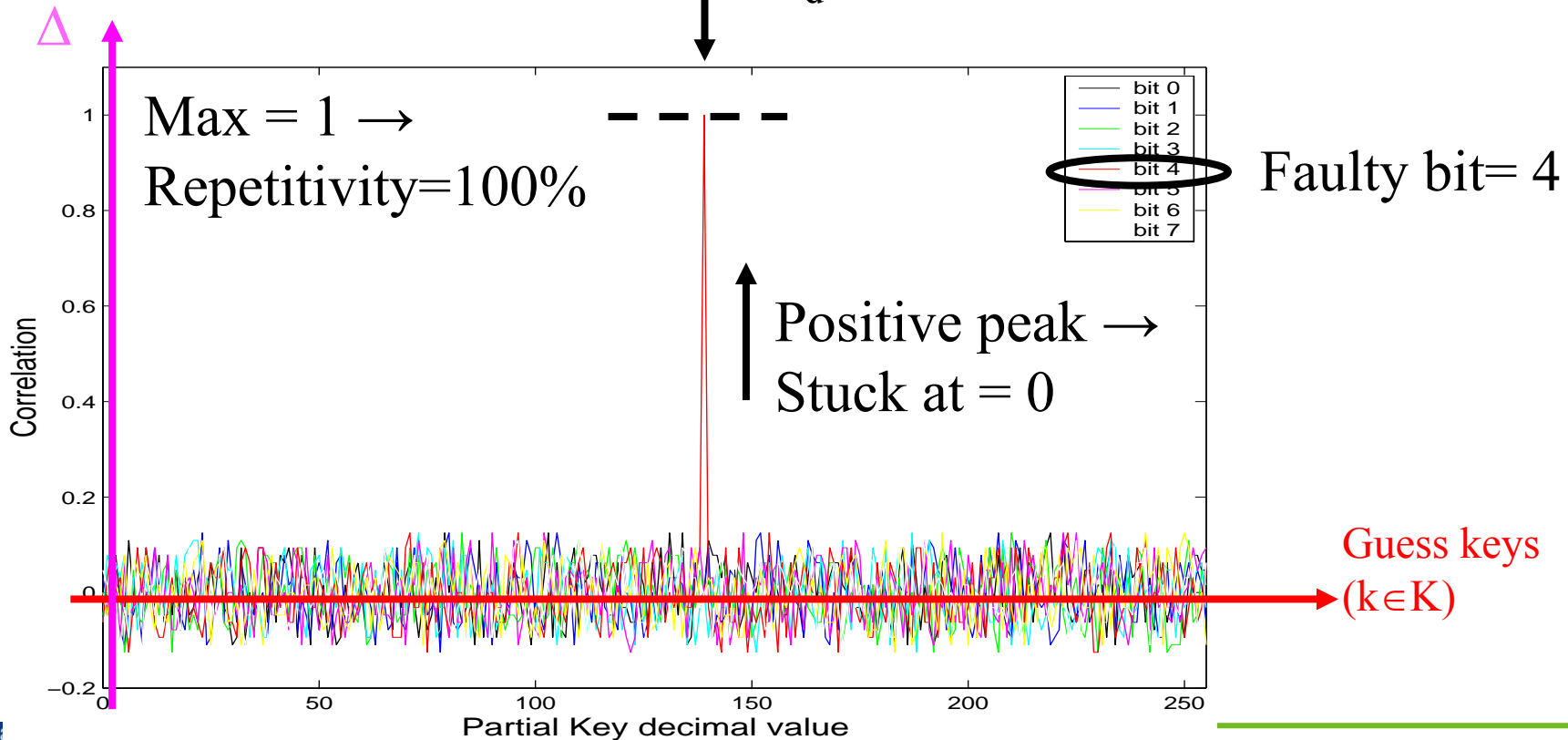
Parameterized modeling

Simulated experimentations



Computation of $\Delta^T_{K0}(s,k)$ and projection on (Δ, K)

$K0=139_d$



Introduction

Differential Behavioral Analysis

- Hypothesis

- Description

- Result interpretation

- Simple case study on AES-128

Relaxing fault hypothesis

- Minimum number of faulty text

- Wrong injection

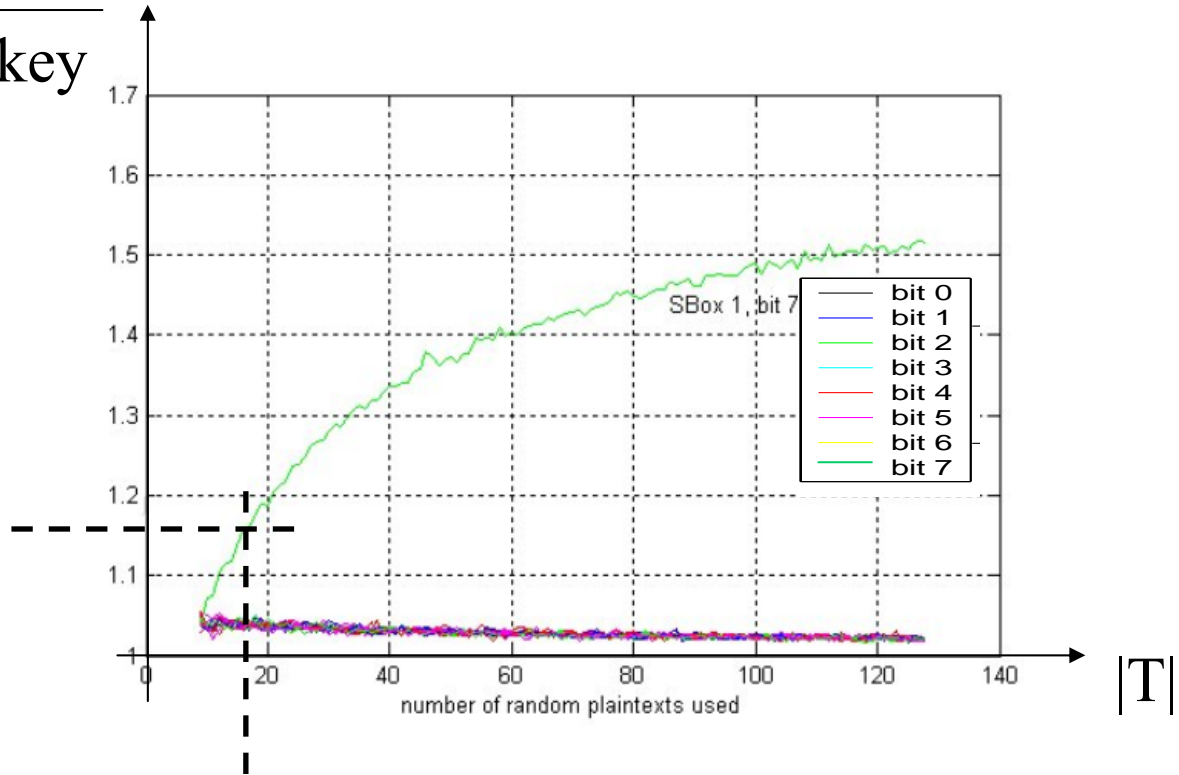
- Fault multiplicity

Comparison with previous works

Minimum number of faulty realization

Good key
Best false key

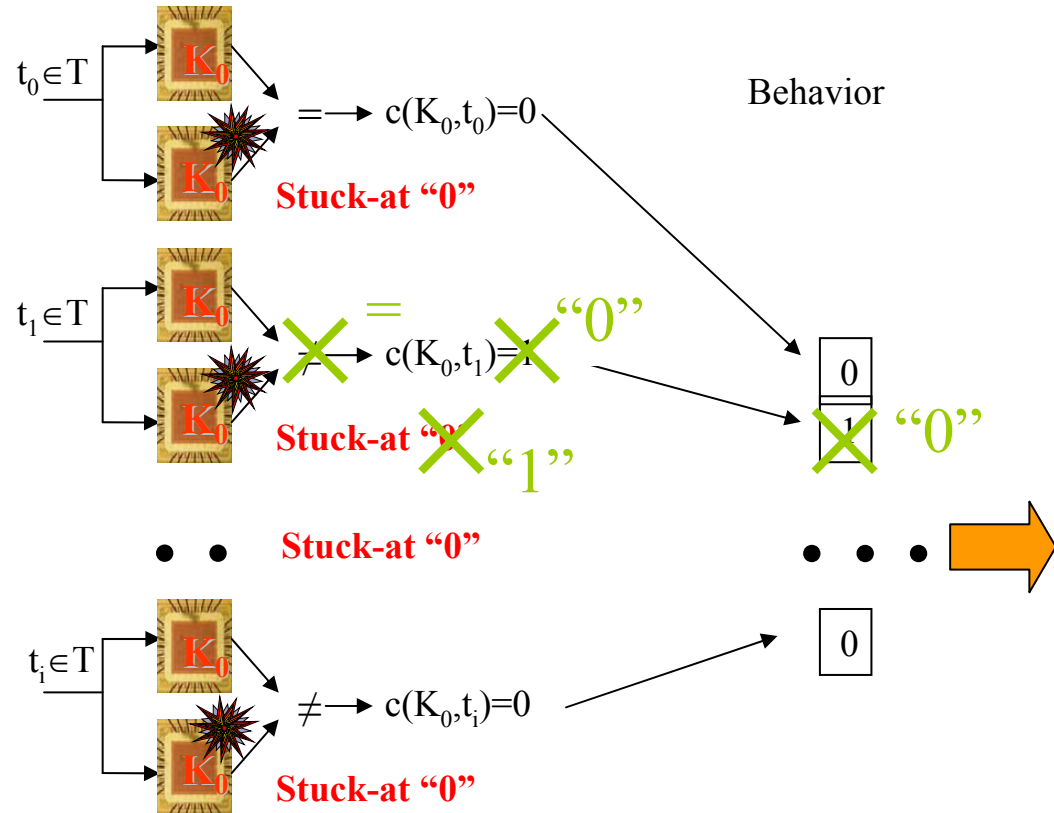
Chosen threshold
15%



16 faulty executions to
recover a byte

➔ The more faulty realizations, the best S/N

Wrong injection



DBA still successful for low wrong fault injection (WFI) rate

But need for more faulty experiments :

16 with perfect injection

~ 25 with 10% WFI

~ 60 with 20% WFI

And smaller correlation value:

1 with perfect injection


~ 0,90 with 10% WFI

~ 0,80 with 20% WFI

➔ The more repetitive experimentations are, the best S/N is


Parameterized modeling

- T : set of the 256 plain texts which exhaust the S-box 0 entries
- K : set of the 256 guess keys which exhaust the S-box 0 entries
- B : the 8 bits at the output of S-box 0 during first round
- **M=8** ($S_8 = \{$
 $\{SB_0\}, \{SB_1\}, \dots, \{SB_7\},$
 $\{SB_0, SB_1\}, \dots, \{SB_6, SB_7\},$
 \dots
 $\{SB_0, SB_1, SB_2, SB_3, SB_4, SB_5, SB_6, SB_7\}, \dots \}$)
- $f=0$

 $r^0(s, k, t)$

Simulated experimentations

- Standardized algorithmic description of the AES_{128}
- Modified algorithmic description of the $AES_{128} \rightarrow$ Stuck-at 0, during first round, on **q bits** at the output of S-box 0
- Encryption of each element of T with the unknown key K0 with AES_{128} and with the modified one AES'_{128}

 $c_{K0}(t) = (AES_{128}(t, K0) = = AES'_{128}(t, K0))$

Parameterized modeling



Exp with
($q=1, p=0$)

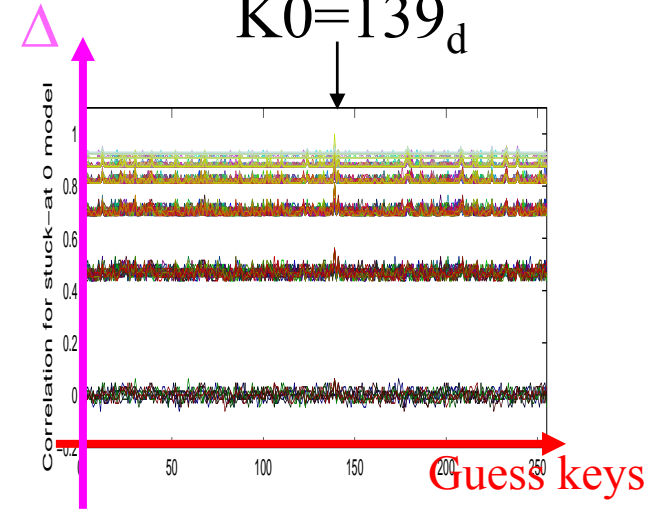
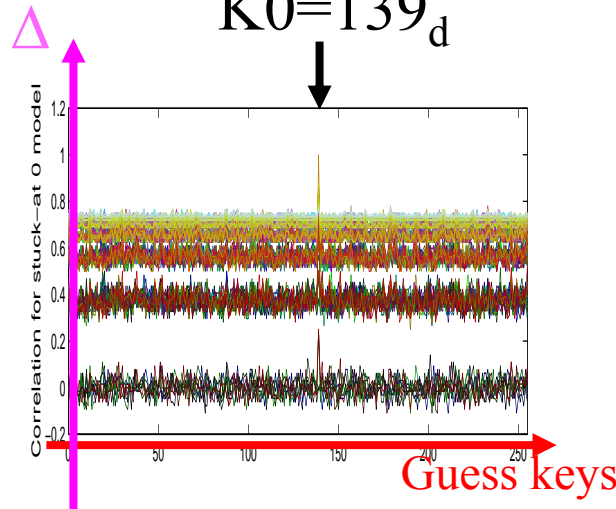
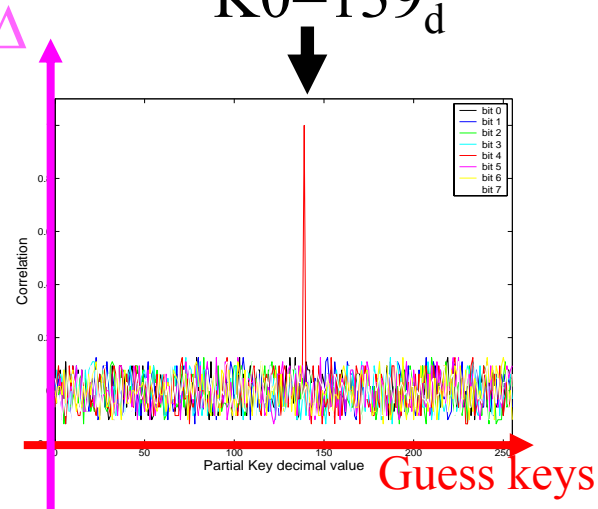
Exp with
($q=3, p=0$)

Exp with
($q=5, p=0$)

$K0=139_d$

$K0=139_d$

$K0=139_d$



➔ The less bits stuck are, the best S/N is

Introduction

Differential Behavioral Analysis

- Hypothesis

- Description

- Result interpretation

- Simple case study on AES-128

Relaxing fault hypothesis

- Minimum number of faulty text

- Wrong injection

- Fault multiplicity

Comparison with previous work

Comparison with previous work

Type	Attack inputs	Fault hypothesis		Experimental constraints		Fault oriented countermeasure			Side Channel oriented countermeasure	
		Type of fault	Multiplicity	# distinct location	# faulty realizations	Error checking + alarm	Fault tolerance	Chip sensors	Path balancing	Data randomizing
DFA	Cipher text	Random	Byte	4 or 1	"+8 or +2"	X	X	X		
Collision	Side	Inversion	Bit	16	approx. 32		X	X	X	X
SEA	Behavior	Stuck-at	Bit	128	128		X	X		X

Relax fault and experimental constraints



SEA	Behavior	Stuck-at	Bit to Byte	16	approx. 256 to 4096		X	X		X
-----	----------	----------	-------------	----	---------------------	--	---	---	--	---

N-order DBA?



SEA	Behavior	Stuck-at	Bit to Byte	16	approx. 256 to 4096		X	X		
-----	----------	----------	-------------	----	---------------------	--	---	---	--	--

Efficiency of a new safe-error attack demonstrated on AES and DES algorithms

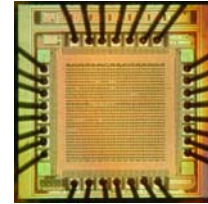
Realistic attack scenario (robust / EDC and path balancing) but...
Define N-order DBA to overcome data-randomizing

Realistic fault hypothesis (repetitive stuck at on a byte) but...
Relax again constraints on fault injection hypothesis

Validated in simulation but...

Validation on a real circuit in progress

✓ Choice of the test chips

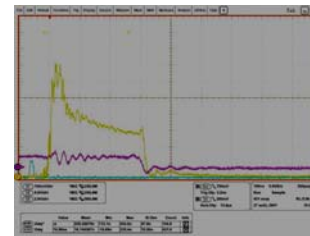


✓ Choice of the injection method

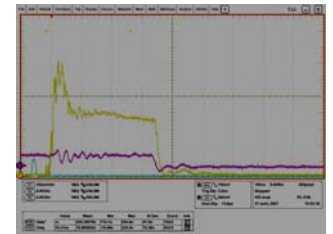


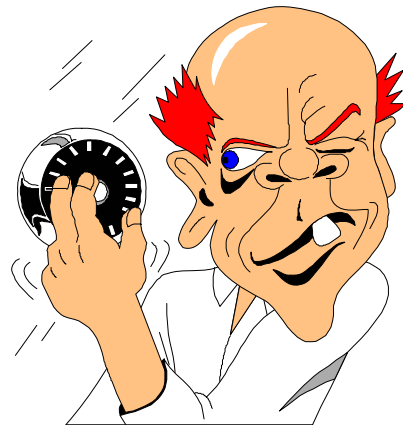
✓ Preparation of the chips

Promising preliminary results on fault injection on a DES asynchronous circuit



≠





This work has been realized in the frame of the CIMPACA/Micro-PackS BTRS Project cofunded by the “Fonds Social Européen” (FSE) and the “Direction Générale des Entreprises” (DGE).

- [AES97]** Federal Information Processing Standards. Advanced Encryption Standard (AES). FIPS publication 197.
- [Blomer03]** J. Blomer and J.-P. Seifert. Fault Based Cryptanalysis of the Advanced Encryption Standard (AES). In Rebecca N. Wright, editor, *Financial Cryptography, 7th International Conference, FC 2003, Guadeloupe, January 27-30, 2003*, Lecture Notes in Computer Science, pages 162-181. Springer-Verlag, 2003.
- [Chen03]** C.-N. Chen and S.-M. Yen. Differential Fault Analysis on AES Key Schedule and Some Countermeasures. In R. Safavi-Naini and J. Seberry, editors, *Information Security and Privacy, 8th Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11, 2003*, volume 2727 of *Lecture Notes in Computer Science*, pages 118-129. Springer-Verlag, 2003.
- [Choukri05]** Round Reduction Using Faults Hamid Choukri and Michael Tunstall, In L. Breveglieri and I. Koren, Eds., *Workshop on Fault Diagnosis and Tolerance in Cryptography 2005 – FDTC 2005*, pp. 13–24, 2005.
- [Dusart03]** P. Dusart, G. Letourneux, and O. Vivolo. Differential Fault Analysis on A.E.S. In J. Zhou, M. Yung, and Y. Han, editors, *Applied Cryptography and Network Security, First International Conference, ACNS 2003, Kunming, China, October 16-19, 2003*, volume 2846 of *Lecture Notes in Computer Science*, pages 293-306. Springer-Verlag, 2003.
- [Giraud03]** C. Giraud. DFA on AES. Technical Report 2003/008, IACR eprint archive, 2003. Available at <http://eprint.iacr.org/2003/008.ps>.
- [Monnet06]** Yannick Monnet, Marc Renaudin, Regis Leveugle, Christophe Clavier, Pascal Moitrel, *Case study of a fault attack on asynchronous DES crypto-processors*, *Workshop on Fault Diagnosis and Tolerance in Cryptography 2006 – FDTC 2006*, LNCS 4236, pp. 88-97
- [Piret03]** G. Piret and J. J. Quisquater. A differential fault attack technique against SPN structures, with application to the AES and Khazad. *Cryptographic Hardware and Embedded Systems Workshop (CHES-2003)*, pages 77-88, 2003. *Lecture Notes in Computer Science No. 2779*.
- [Blomer06]** J. Blömer, V. Krummel, *Fault Based Collision Attacks on AES*, *Workshop on Fault Diagnosis and Tolerance in Cryptography 2006 – FDTC 2006*, LNCS 4236, pp. 106-120
- [Skorobogatov02]** S. Skorobogatov and R. Anderson. Optical fault induction attacks. *Cryptographic Hardware and Embedded Systems Workshop (CHES-2002)*, pages 2-12, 2002. *Lecture Notes in Computer Science No. 2523*.