Ecole Nationale Supérieure des Mines
SAINT-ETIENNE
Site Georges Charpak

Crypto'Puces 2009

leti
cea

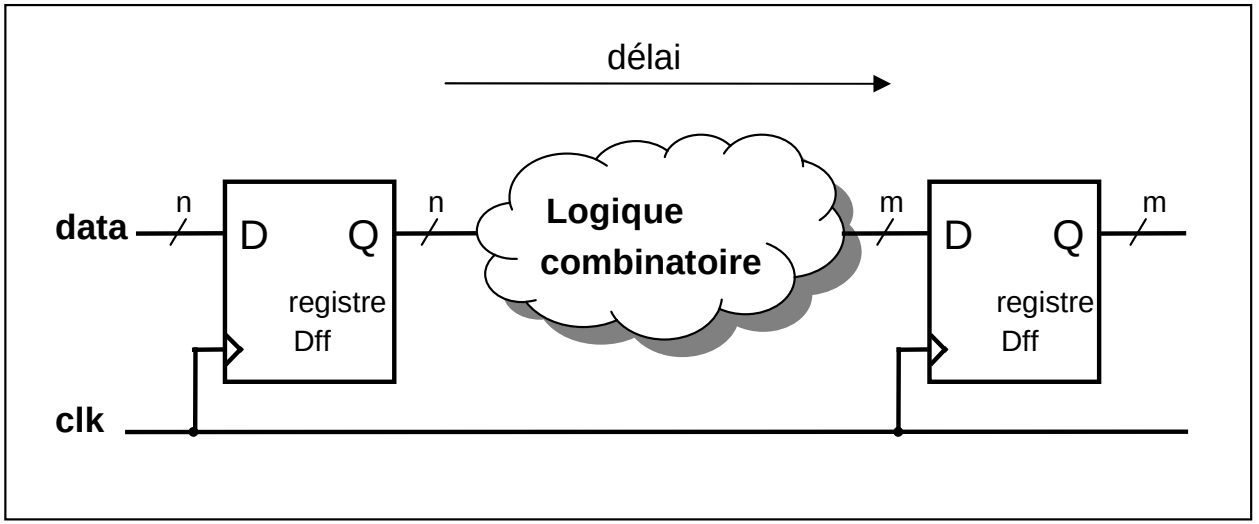
Injection de fautes par modification de l'horloge, application à l'AES

Jean-Max Dutertre – ENSME
Assia Tria – CEA-LETI
Bruno Robisson – CEA-LETI
Michel Agoyan – CEA-LETI

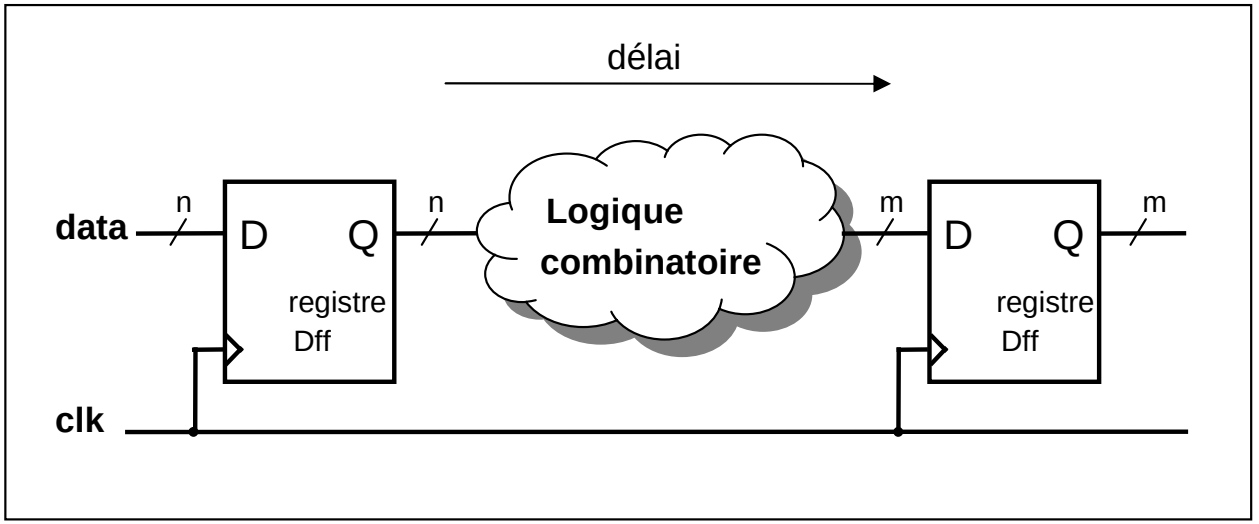
Département SAS
Équipe mixte CEA-LETI/ENSMSE
Site Georges Charpak
Centre Microélectronique de Provence
880, route de Mimet
13541 Gardanne

- Une nouvelle technique d'injection de fautes
  - Principe de fonctionnement synchrone
  - Injection de fautes de délai
  - Nouvelle technique d'injection
- Validation expérimentale
  - DFA sur AES (Giraud monobit)
  - Circuit de test
  - Mise en œuvre de l'attaque
- Conclusion

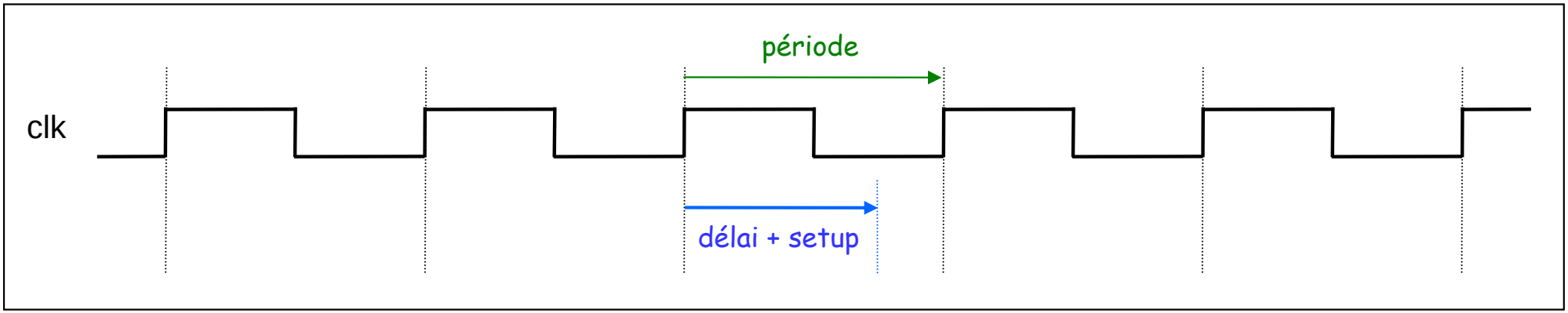
- Principe de fonctionnement synchrone



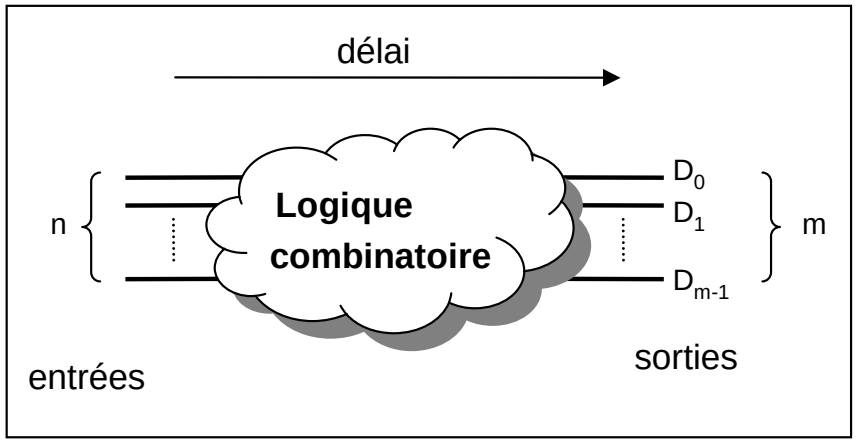
- Principe de fonctionnement synchrone



période > délai maximal + temps setup des bascules D



Temps de propagation – Chemin critique



sorties = f (entrées)

f fonction logique

temps de propagation à travers la logique différent pour chaque D_i

Chemin critique = délai de propagation maximale

Les temps de propagation varient :

- avec les niveaux logiques (0 / 1)

→ pour un vecteur d'entrée différent le temps de propagation est modifié (le chemin critique est susceptible de changer)

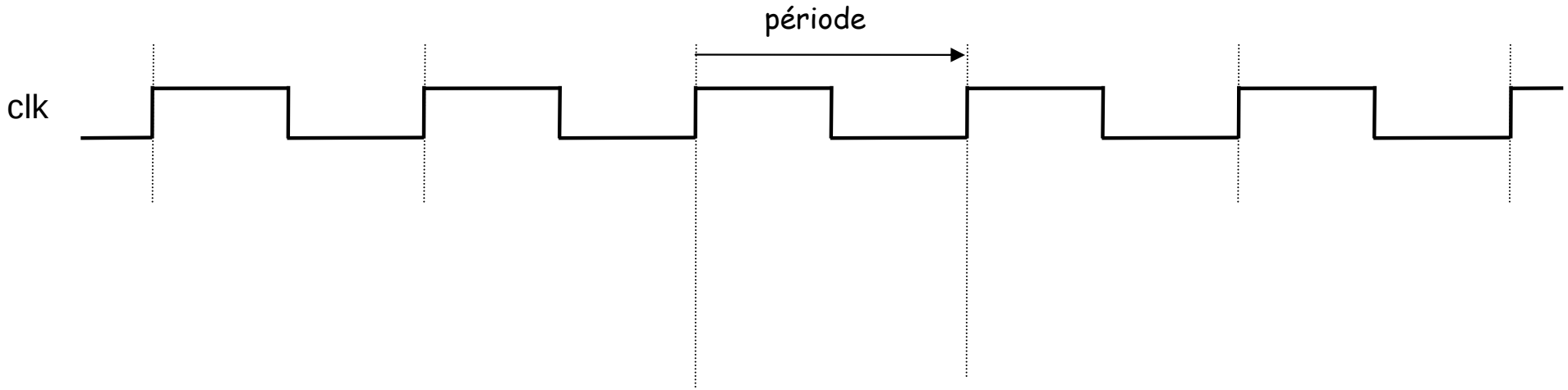
- avec la tension d'alimentation
- avec la température

- Injection de fautes de délai

Une approche classique : diminution de la période d'horloge

⇨ apparition de fautes par violation des temps de setup

$période_{faute}$ < délai critique + tps setup

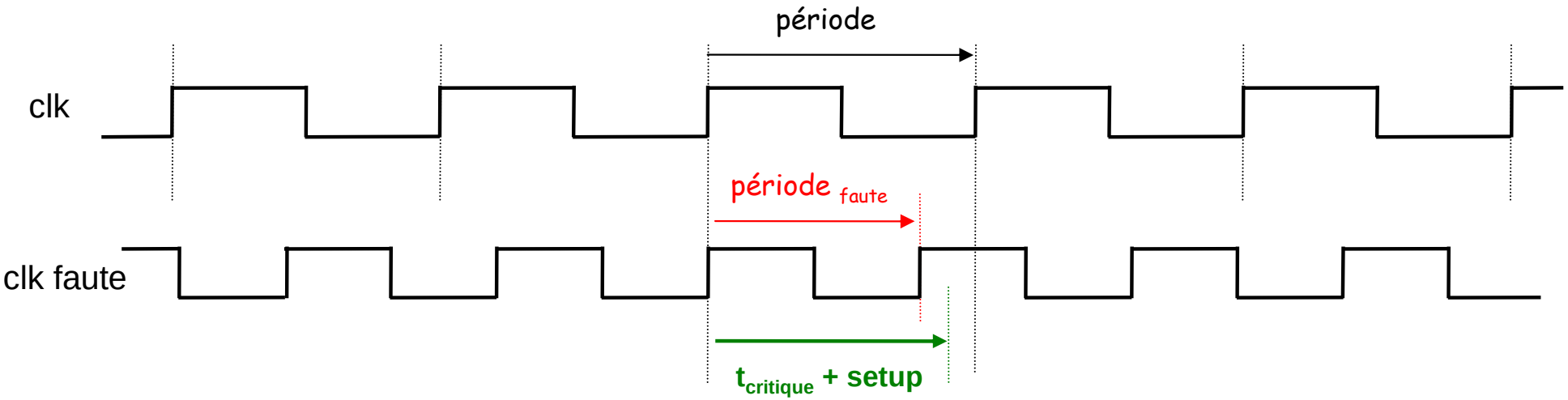


- Injection de fautes de délai

Une approche classique : diminution de la période d'horloge

⇨ apparition de fautes par violation des temps de setup

$période_{faute}$ < délai critique + tps setup

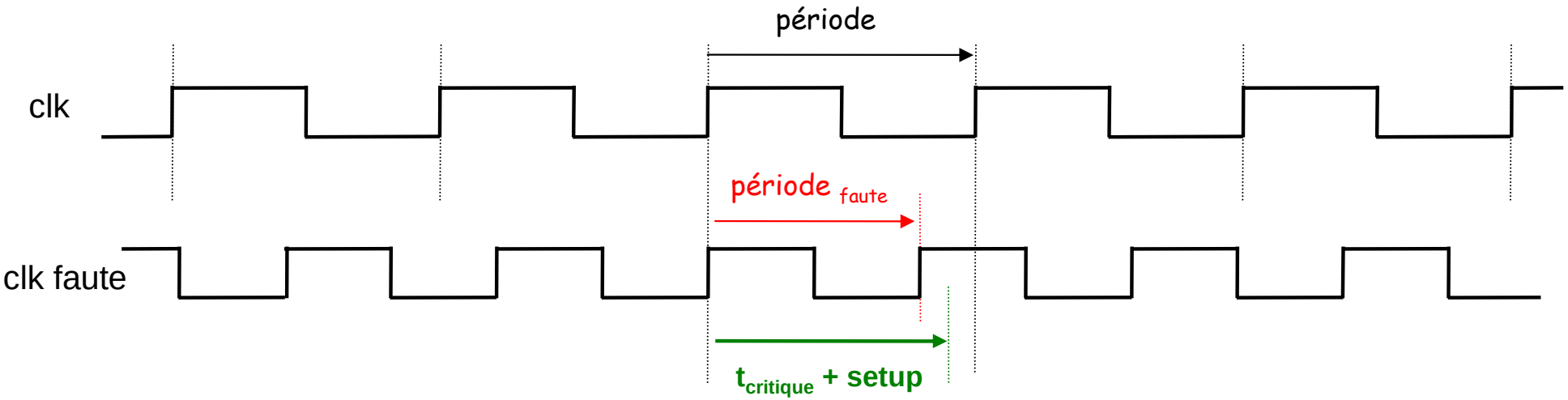


- Injection de fautes de délai

Une approche classique : diminution de la période d'horloge

⇨ apparition de fautes par violation des temps de setup

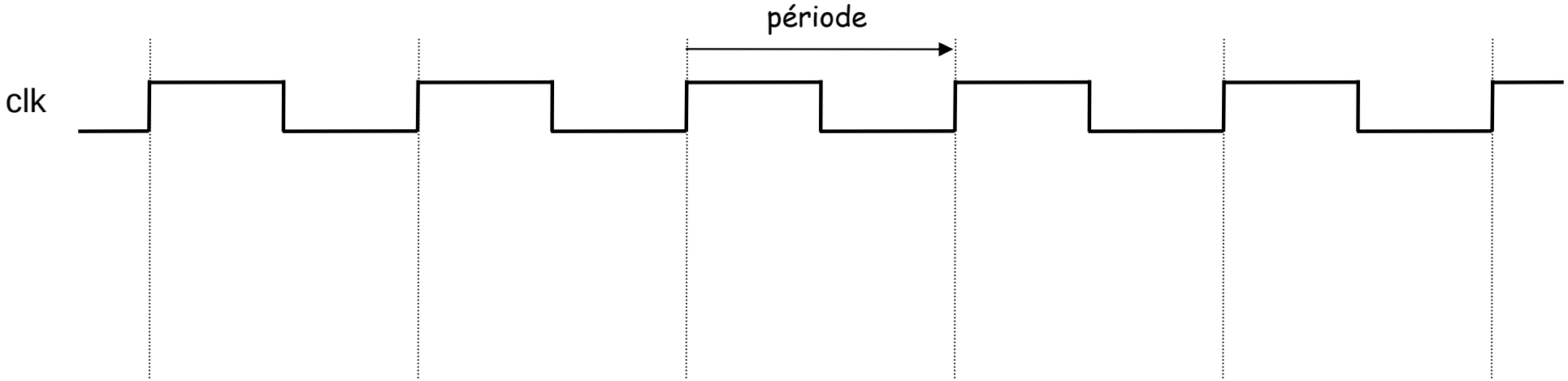
$période_{faute}$ < délai critique + tps setup



⇨ défaut : injection de fautes à chaque cycle d'horloge

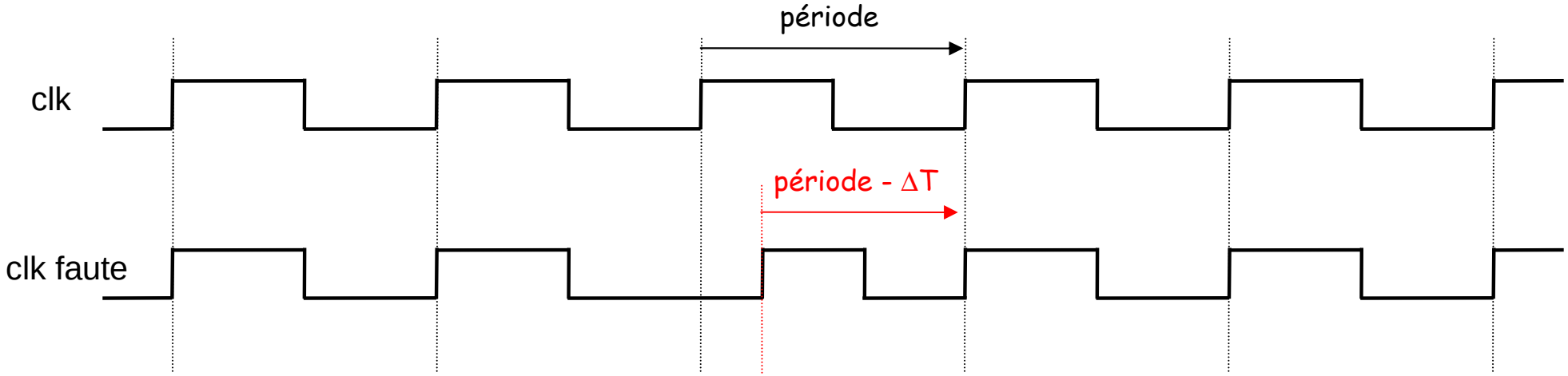
- Nouvelle technique d'injection

Injection de faute par modification du signal d'horloge sur une <u>seule</u> période



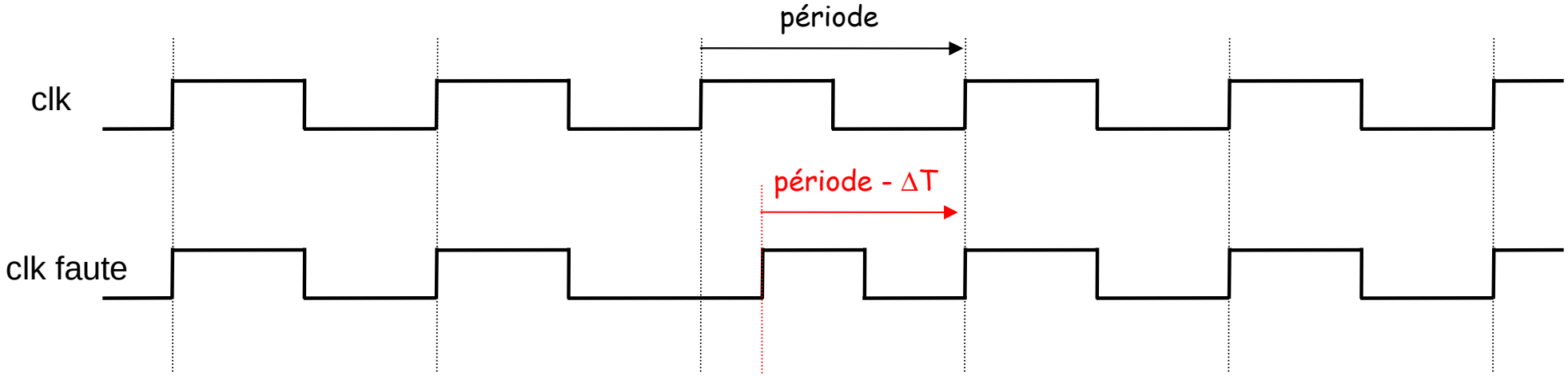
- Nouvelle technique d'injection

Injection de faute par modification du signal d'horloge sur une <u>seule</u> période



- Nouvelle technique d'injection

Injection de faute par modification du signal d'horloge sur une <u>seule</u> période



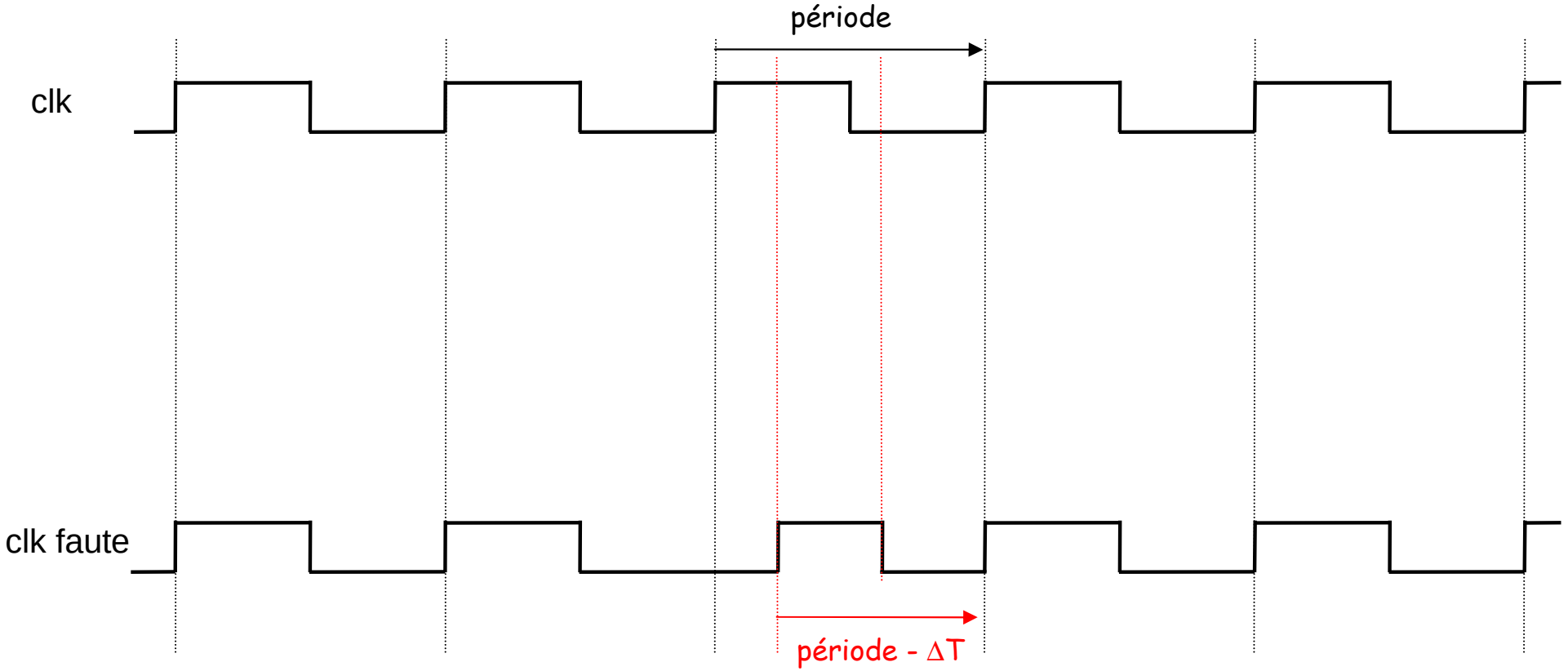
⇨ choix du cycle d'injection

⇨ réglage fin de ΔT afin de contrôler précisément la nature des fautes injectées

Contrôle de ΔT avec un pas de 35 ps.

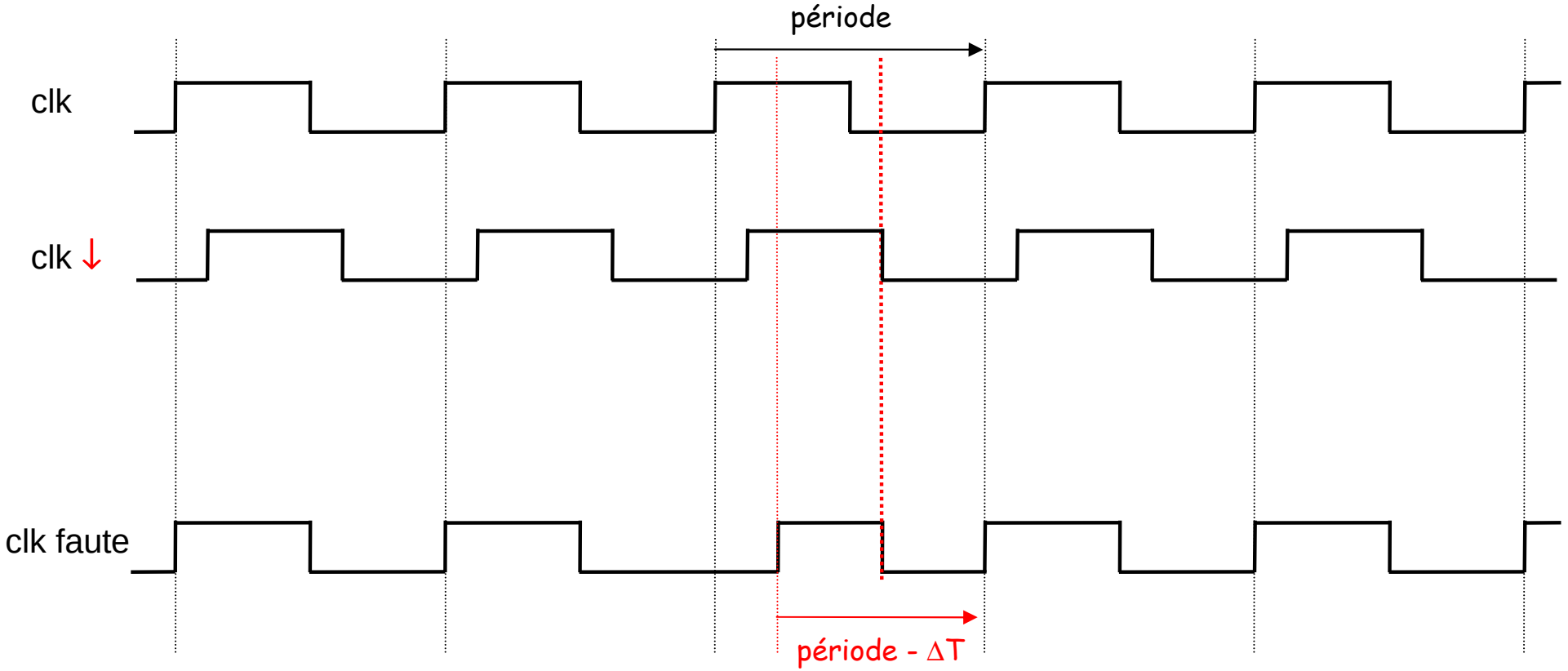
- Nouvelle technique d'injection

Performances obtenues grâce à l'utilisation d'une boucle à verrouillage de délais – DLL (Xilinx Virtex-5).



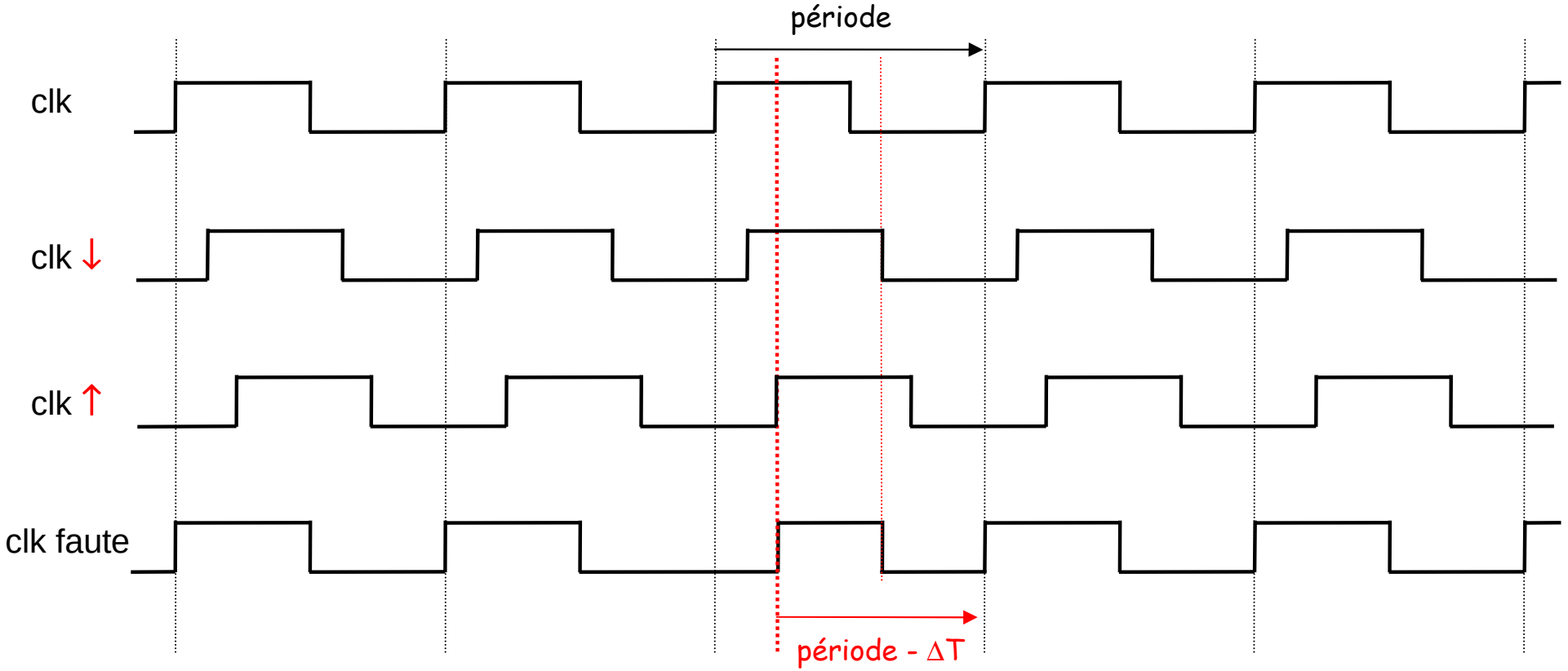
- Nouvelle technique d'injection

Performances obtenues grâce à l'utilisation d'une boucle à verrouillage de délais (Xilinx Virtex-5).

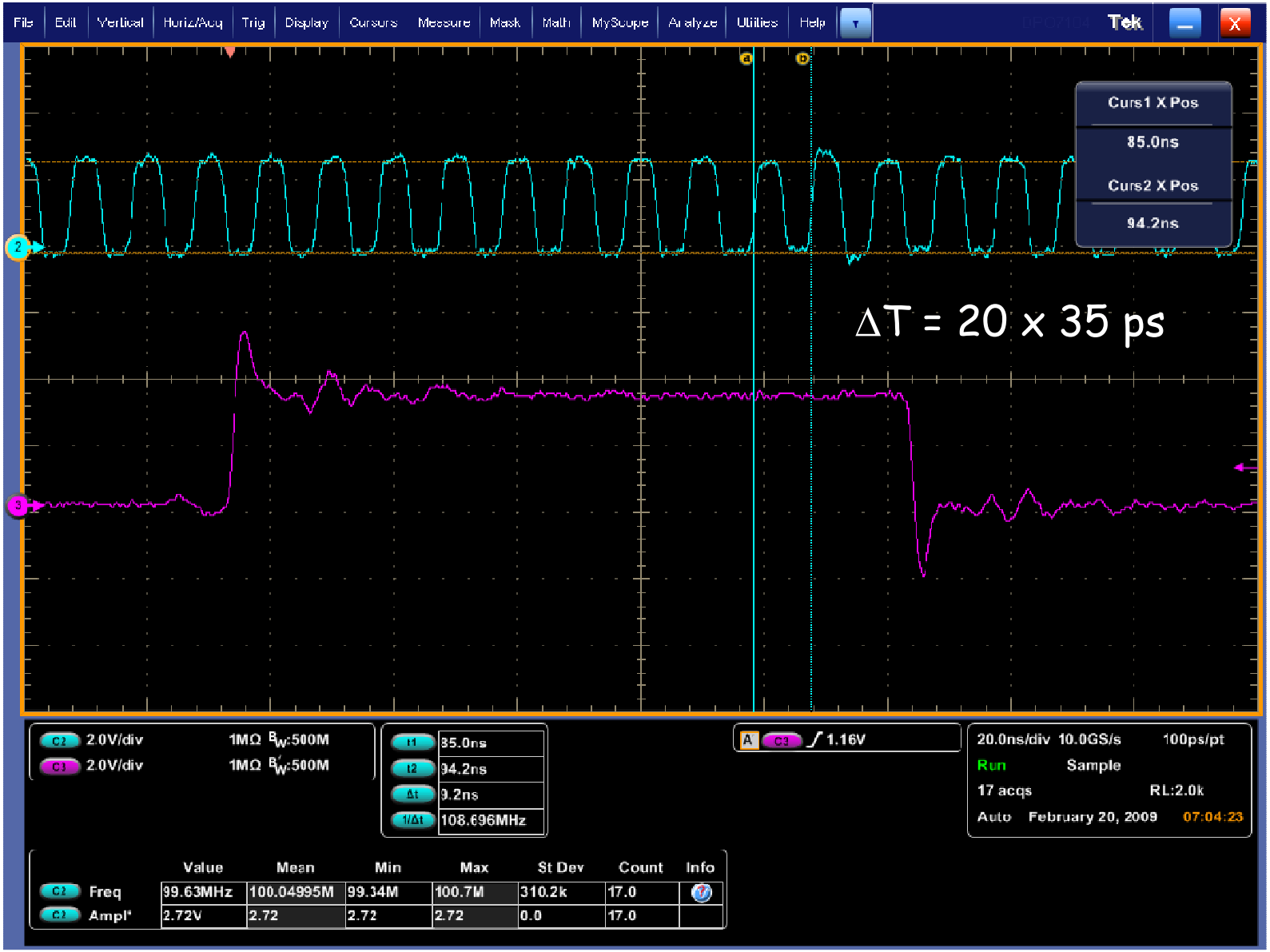


- Nouvelle technique d'injection

Performances obtenues grâce à l'utilisation d'une boucle à verrouillage de délais (Xilinx Virtex-5).



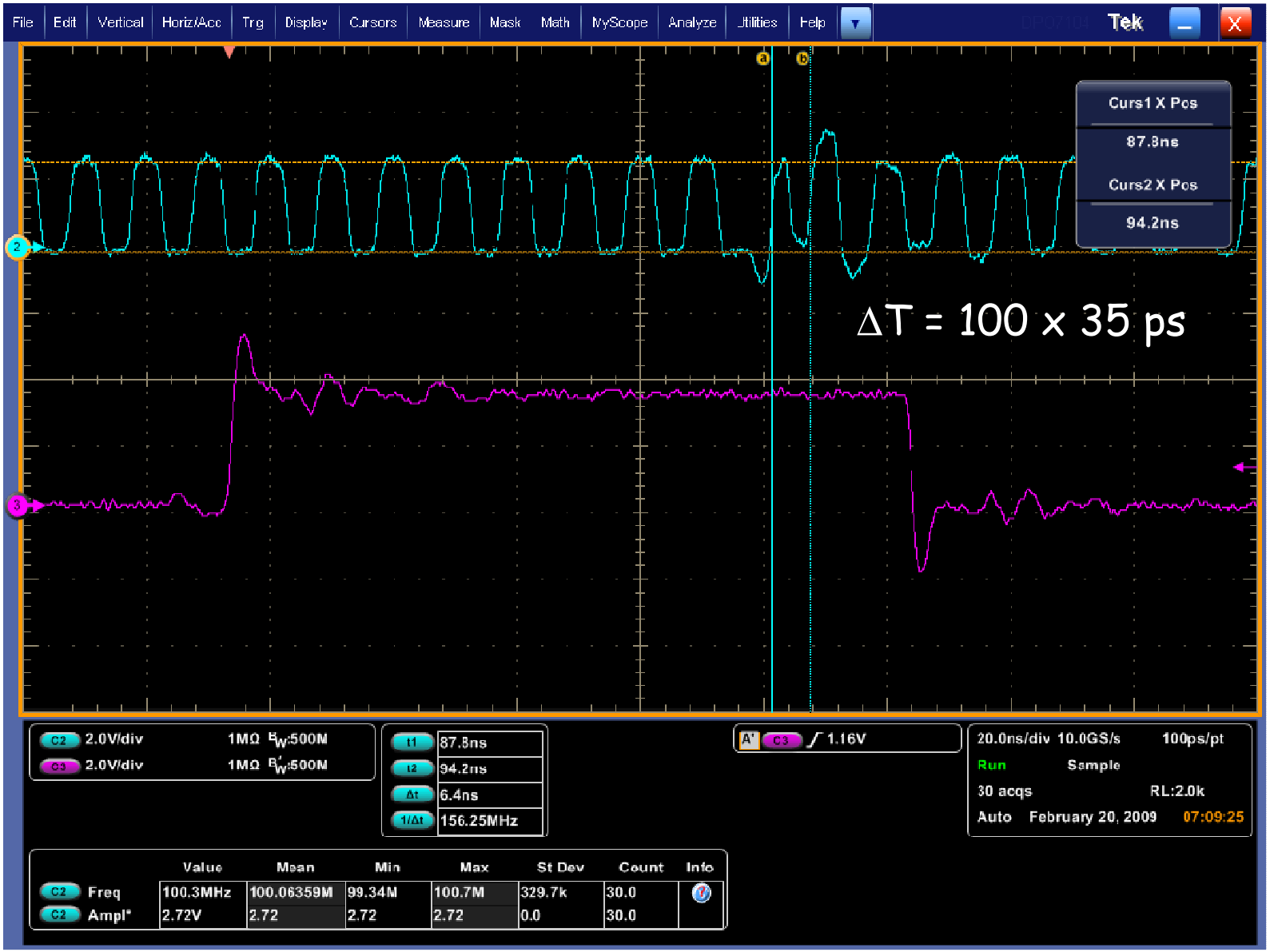

File
Edit
Vertical
Horiz/Acq
Trig
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
84.2ns
Curs2 X Pos
94.2ns
ΔT = 0
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 84.2ns
t2 94.2ns
Δt 10.0ns
1/Δt 100.0MHz
C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
15 acqs RL:2.0k
Auto February 20, 2009 07:03:46
Value Mean Min Max St Dev Count Info
C2 Freq 100.3MHz 100.03429M 99.34M 100.7M 308.7k 15.0
C2 Ampl* 2.72V 2.72 2.72 2.72 0.0 15.0


File
Edit
Vertical
Horiz/Acq
Trig
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
85.0ns
Curs2 X Pos
94.2ns
ΔT = 20 x 35 ps
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 85.0ns
t2 94.2ns
Δt 9.2ns
1/Δt 108.696MHz
A C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
17 acqs RL:2.0k
Auto February 20, 2009 07:04:23
Value Mean Min Max St Dev Count Info
C2 Freq 99.63MHz 100.04995M 99.34M 100.7M 310.2k 17.0
C2 Ampl 2.72V 2.72 2.72 2.72 0.0 17.0

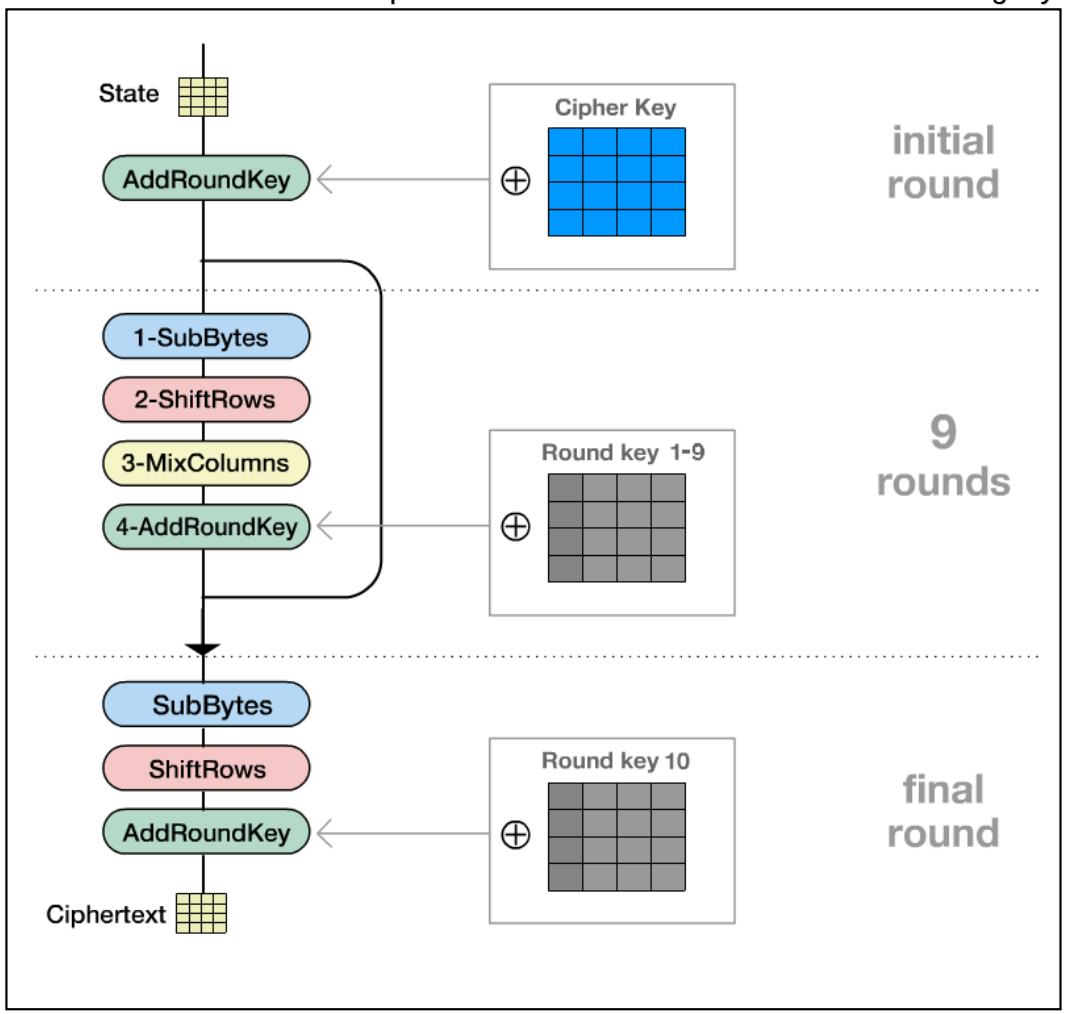

File
Edit
Vertical
Horiz/Acc
Trg
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
85.5ns
Curs2 X Pos
94.2ns
ΔT = 40 x 35 ps
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 85.5ns
t2 94.2ns
Δt 8.6ns
1/Δt 116.279MHz
A' C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
21 acqs RL:2.0k
Auto February 20, 2009 07:05:25
Value Mean Min Max St Dev Count Info
C2 Freq 100.3MHz 100.09428M 99.34M 100.7M 314.1k 21.0
C2 Ampl* 2.72V 2.72 2.72 2.72 0.0 21.0


File
Edit
Vertical
Horiz/Acc
Trg
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
86.2ns
Curs2 X Pos
94.2ns
ΔT = 60 x 35 ps
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 86.2ns
t2 94.2ns
Δt 8.0ns
1/Δt 125MHz
A' C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
24 acqs RL:2.0k
Auto February 20, 2009 07:06:06
Value Mean Min Max St Dev Count Info
C2 Freq 99.34MHz 100.05838M 99.34M 100.7M 331.3k 24.0
C2 Ampl 2.72V 2.72 2.72 2.72 0.0 24.0


File
Edit
Vertical
Horiz/Acq
Trig
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
87.0ns
Curs2 X Pos
94.2ns
ΔT = 80 x 35 ps
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 87.0ns
t2 94.2ns
Δt 7.2ns
1/Δt 138.889MHz
C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
26 acqs RL:2.0k
Auto February 20, 2009 07:07:47
Value Mean Min Max St Dev Count Info
C2 Freq 99.75MHz 100.0475M 99.34M 100.7M 323.5k 26.0
C2 Ampl 2.72V 2.72 2.72 2.72 0.0 26.0


File
Edit
Vertical
Horiz/Acc
Trg
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
87.3ns
Curs2 X Pos
94.2ns
ΔT = 100 x 35 ps
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 87.3ns
t2 94.2ns
Δt 6.4ns
1/Δt 156.25MHz
A' C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
30 acqs RL:2.0k
Auto February 20, 2009 07:09:25
Value Mean Min Max St Dev Count Info
C2 Freq 100.3MHz 100.06359M 99.34M 100.7M 329.7k 30.0
C2 Ampl 2.72V 2.72 2.72 2.72 0.0 30.0

- DFA sur AES (Giraud monobit)



AES 128 bits (Rijndael)

FIPS - 197

Algorithme de chiffrement à clef secrète

Implémentation non sécurisée sur un FPGA avec un chemin de données de 128 bits.

(Xilinx – Spartan 3)

- DFA sur AES (Giraud monobit)

DFA on AES, Christophe Giraud, Advanced Encryption Standard AES, 4th International Conference, AES 2004

DFA = Attaque en faute différentielle

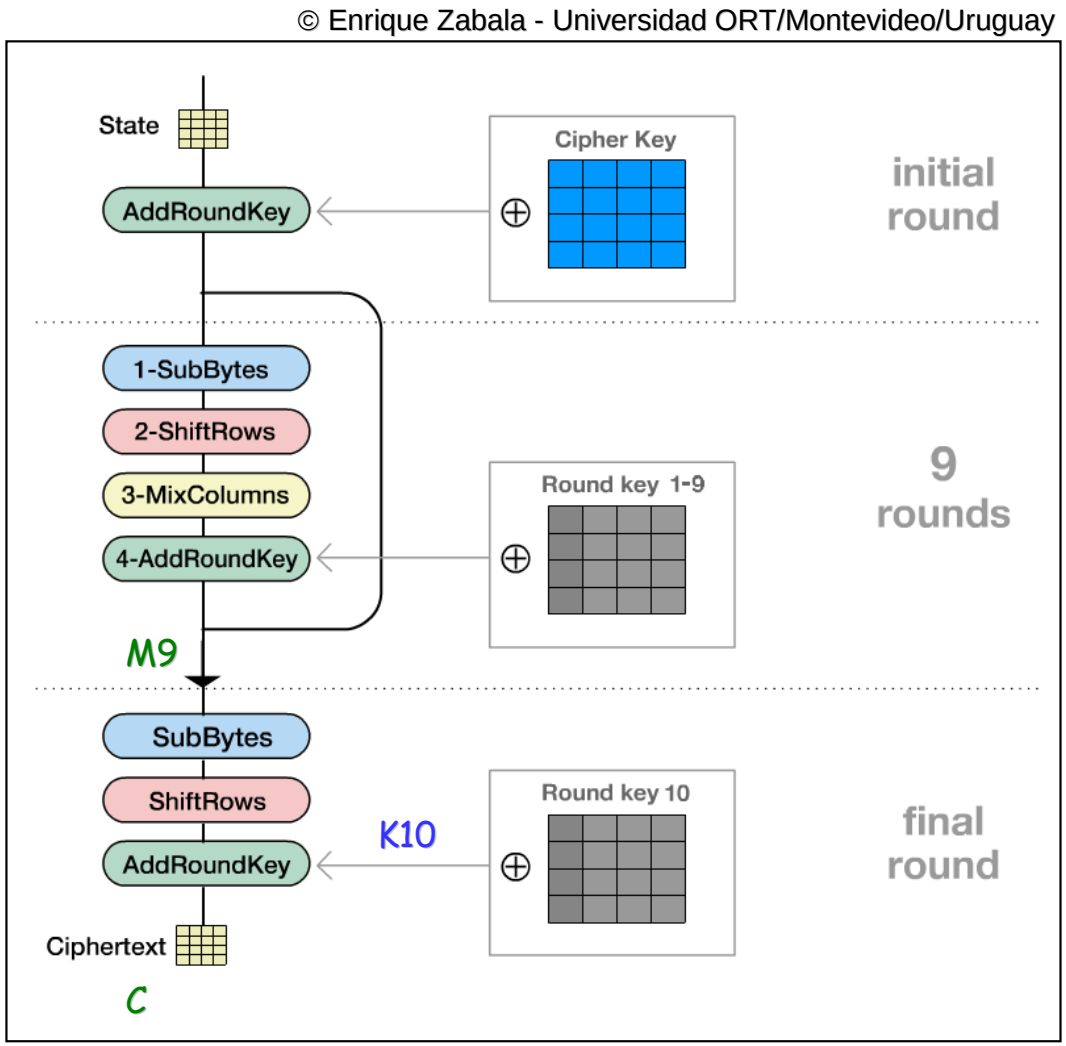
⇨ chiffrement perturbé par injection de faute(s)

⇨ récupération d'informations secrètes par comparaison des chiffrés correct et fauté

Attaque Giraud monobit :

- Exploitation des propriétés des Sbox
- Faute : un bit sur un octet avant le dernier SubBytes (hypothèse fondamentale)

- DFA sur AES (Giraud monobit)

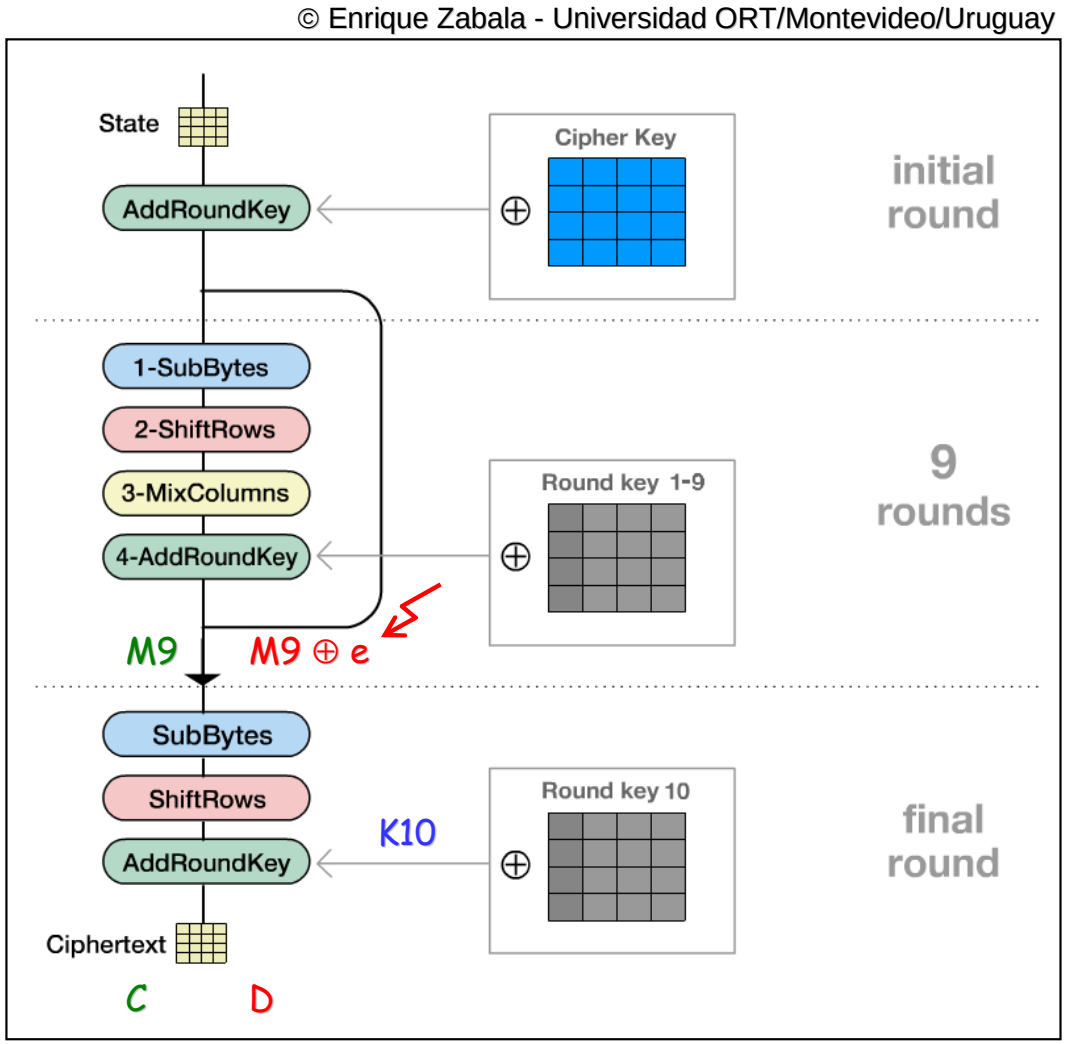


Exécution non fautée :

$C = SB(M9) \oplus K10$

(raisonnement sur octets)

- DFA sur AES (Giraud monobit)



Exécution non fautée :

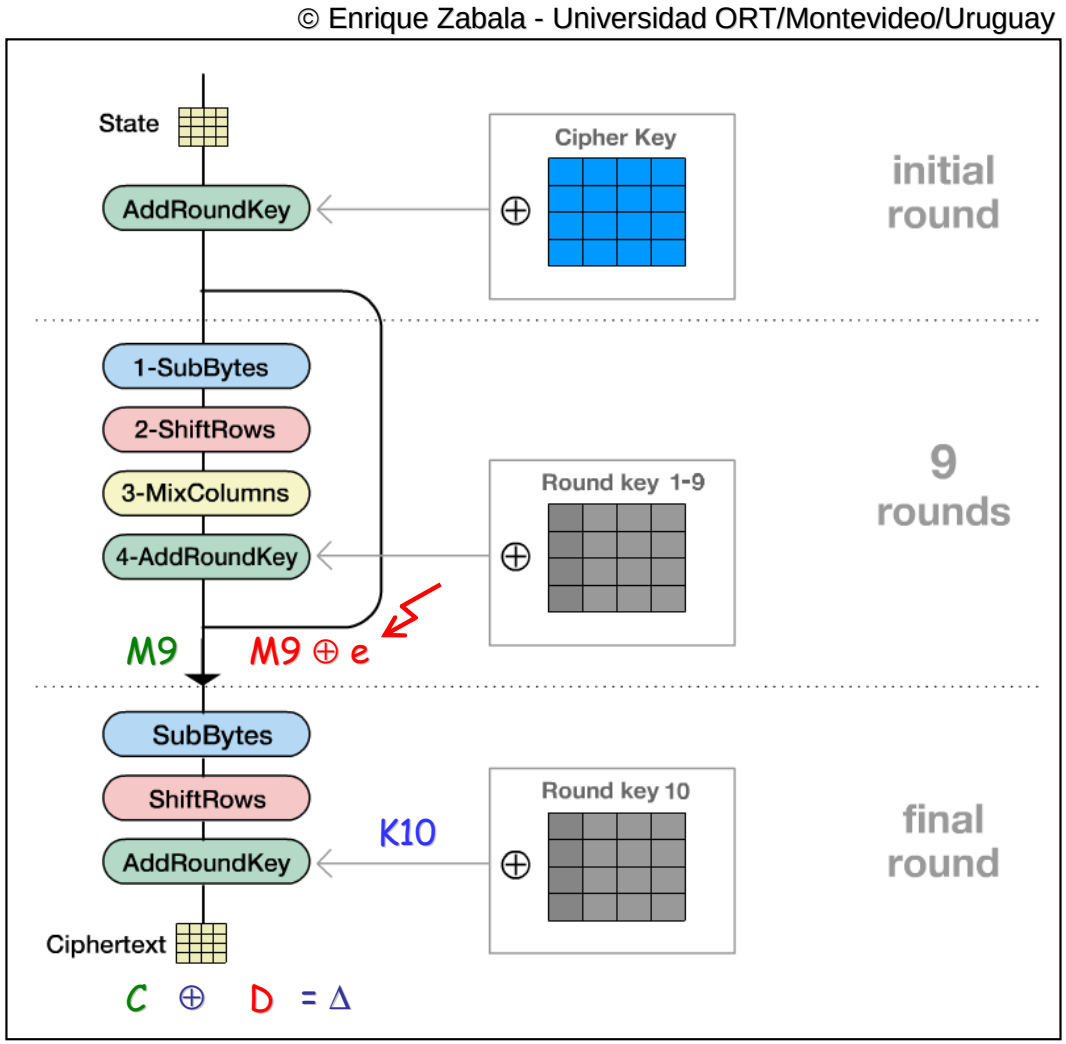
$C = SB(M9) \oplus K10$

Exécution fautée :

$D = SB(M9 \oplus e) \oplus K10$

e faute monobit

- DFA sur AES (Giraud monobit)



Exécution non fautée :

$C = SB(M9) \oplus K10$

Exécution fautée :

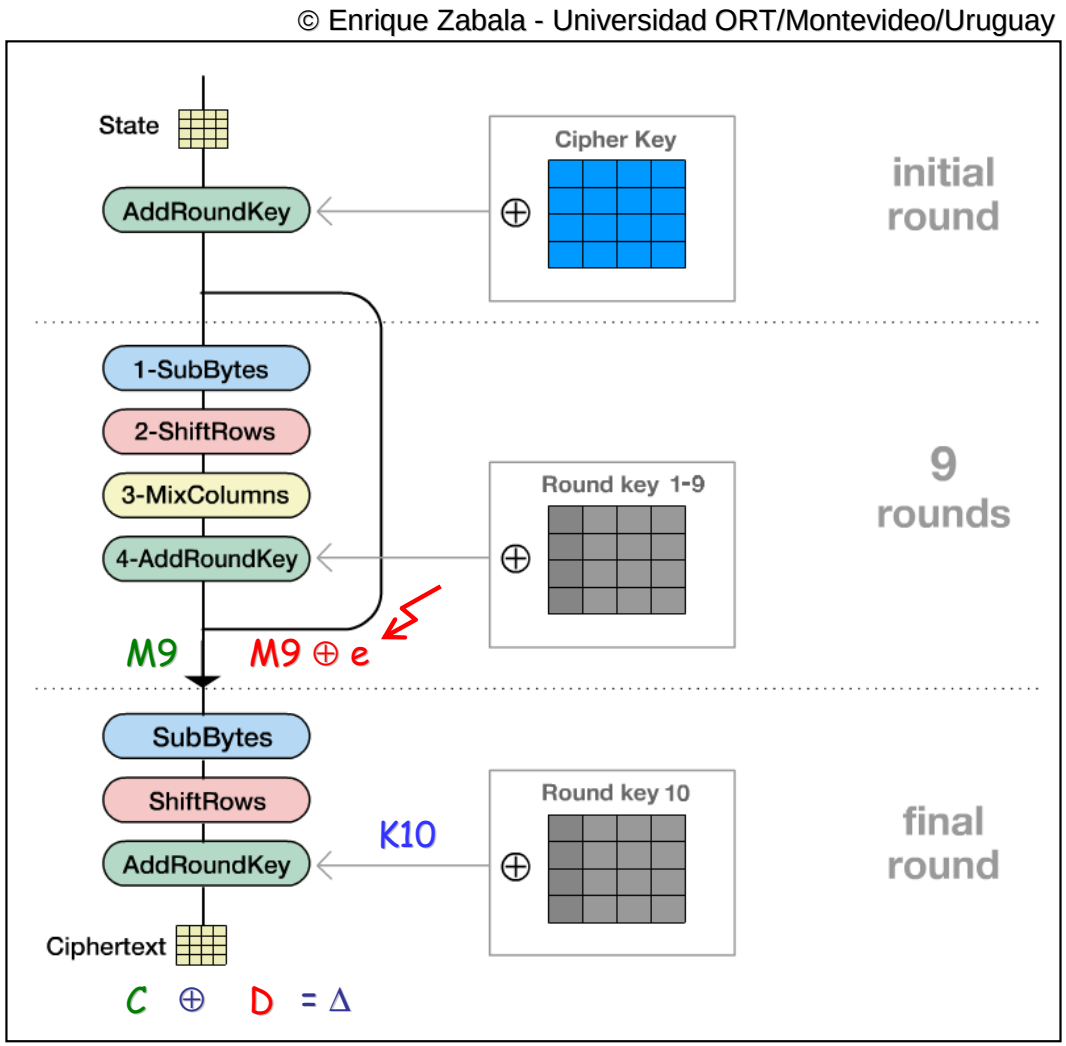
$D = SB(M9 \oplus e) \oplus K10$

Différentiation :

$\Delta = SB(M9 \oplus e) \oplus SB(M9)$

En l'absence de faute $\Delta = 0$

- DFA sur AES (Giraud monobit)



Exécution non fautée :

$C = SB(M9) \oplus K10$

Exécution fautée :

$D = SB(M9 \oplus e) \oplus K10$

Différentiation :

$\Delta = SB(M9 \oplus e) \oplus SB(M9)$

⟹ ensemble d'hypothèses sur M9 et e

- DFA sur AES (Giraud monobit)

Puis enfin d'après :

$$K10 = C \oplus SB(M9)$$

on obtient un ensemble d'hypothèses sur l'octet de clef considéré K10

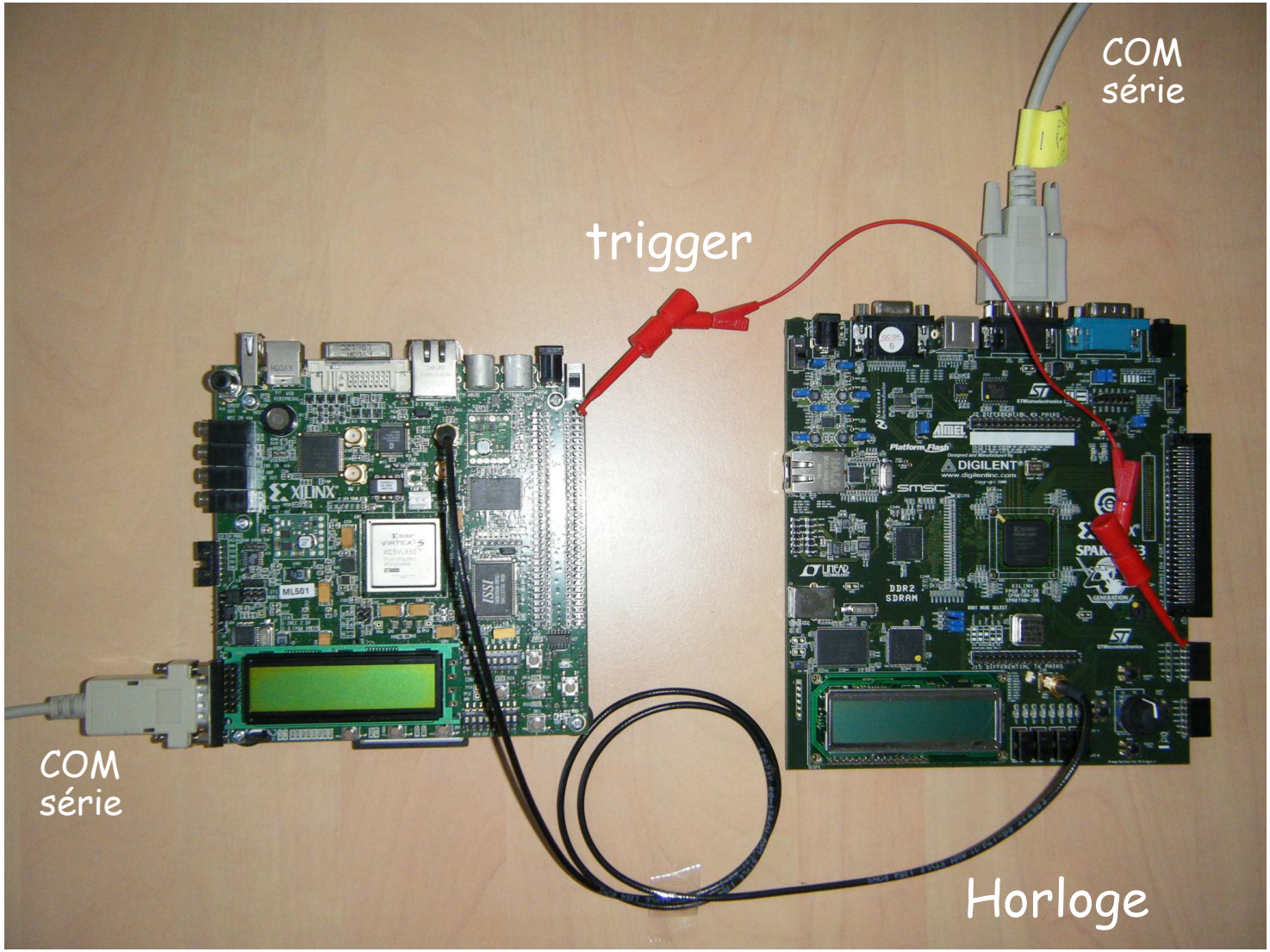
La taille de cet ensemble est réduit à 1 progressivement en répétant cette analyse pour une faute monobit différente et/ou un texte clair différent.

Par itérations successives sur chacun de ses octets, la $10^{ième}$ clef de ronde est extraite par l'attaquant.

Attaque pouvant être mener simultanément sur plusieurs octets.

- Mise en œuvre de l'attaque

Maquette génération horloge



Maquette AES

- Mise en œuvre de l'attaque

Scénario de test :

- Envoi texte clair à l'AES
- Envoi clef de chiffrement à l'AES
- Initialisation du déphasage du cycle d'horloge *fautant* $\Delta T = 0$
- Tant que (période - ΔT) > 0 :
  - Chiffrement
  - Récupération du chiffré
  - Recherche de faute
  - Incrément de ΔT ($\Delta T = \Delta T + 35$ ps)

Analyse des résultats :

- Hypothèse : sur chaque octet la première occurrence d'une faute correspond à une faute monobit
- Calcul de la dernière clef de ronde (Matlab)

Résultat du scénario de test :

Texte clair 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
Clef 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

			calc	39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32	
ph=68	ERROR	00 00 00 00 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 1d 02 0e 09 fb dc 11 85 97 19 6a 0b 32	
ph=69	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32	
ph=70	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32	
ph=71	ERROR	00 00 00 00 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 1d 02 0e 09 fb dc 11 85 97 19 6a 0b 32	
ph=72	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32	
ph=73	ERROR	00 00 00 D3 00 D2 36 00 00 00 00 00 00 00 00 82	AES	39 25 84 ce 02 0e 3f fb dc 11 85 97 19 6a 0b b0	
ph=74	ERROR	00 00 00 D3 00 D2 36 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 3f fb dc 11 85 97 19 6a 0b 32	
ph=75	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0	
ph=76	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0	
ph=77	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0	
ph=78	ERROR	00 00 00 D3 00 7B 36 00 00 00 00 00 00 00 87 82	AES	39 25 84 ce 02 a7 3f fb dc 11 85 97 19 6a 8c b0	
ph=79	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0	
ph=80	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 84 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 9d 31 8c b0	
ph=81	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0	
ph=82	ERROR	00 00 B4 D3 00 76 36 00 00 00 00 00 00 5B 87 82	AES	39 25 30 ce 02 aa 3f fb dc 11 85 97 19 31 8c b0	
ph=83	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0	
ph=84	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0	
ph=85	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 00 00 5B 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 97 19 31 8c b0	
ph=86	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0	
ph=87	ERROR	00 00 B4 34 1A 76 C3 00 16 00 00 46 6F 68 87 2F	AES	39 25 30 29 18 aa ca fb ca 11 85 d1 76 02 8c 1d	
ph=88	ERROR	00 00 B4 D3 1A 76 36 00 16 00 00 1B 6F 63 87 82	AES	39 25 30 ce 18 aa 3f fb ca 11 85 8c 76 09 8c b0	
ph=89	ERROR	00 00 B4 8B 1A 76 36 00 16 00 00 46 6F 63 E2 2F	AES	39 25 30 96 18 aa 3f fb ca 11 85 d1 76 09 e9 1d	
ph=90	ERROR	00 00 0A 34 1A 76 C3 00 16 00 00 46 6F 68 87 2F	AES	39 25 8e 29 18 aa ca fb ca 11 85 d1 76 02 8c 1d	
ph=91	ERROR	00 00 0A 34 1A 76 C3 00 16 00 00 46 6F 68 E2 2F	AES	39 25 8e 29 18 aa ca fb ca 11 85 d1 76 02 e9 1d	
ph=92	ERROR	00 00 B4 34 1A 76 AF 00 16 00 00 46 6F 68 E2 2F	AES	39 25 30 29 18 aa a6 fb ca 11 85 d1 76 02 e9 1d	
ph=93	ERROR	F8 40 0A 78 37 76 61 D9 92 3F 00 46 6F 4F 87 2F	AES	c1 65 8e 65 35 aa 68 22 4e 2e 85 d1 76 25 8c 1d	
ph=94	ERROR	00 40 0A 78 37 76 61 D9 92 3F 00 46 6F 4F 87 2F	AES	39 65 8e 65 35 aa 68 22 4e 2e 85 d1 76 25 8c 1d	
ph=95	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 0D CC 30 2F	AES	c7 65 8e 65 33 aa 68 22 48 2e 85 d1 14 a6 3b 1d	
ph=96	ERROR	FE 0E 6E 78 38 76 61 D9 94 23 00 46 0D CC 30 2F	AES	c7 2b ea 65 3a aa 68 22 48 32 85 d1 14 a6 3b 1d	
ph=97	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 69 4E 24 2F	AES	c7 65 8e 65 33 aa 68 22 48 2e 85 d1 70 24 2f 1d	
ph=98	ERROR	FE 0E 6E 78 38 76 61 D9 94 23 00 46 0D CC 8E B9	AES	c7 2b ea 65 3a aa 68 22 48 32 85 d1 14 a6 85 8b	
ph=99	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 0D CC 30 2F	AES	c7 65 8e 65 33 aa 68 22 48 2e 85 d1 14 a6 3b 1d	
ph=100	ERROR	FE 0E 6E 78 F5 16 F5 43 02 23 C9 54 0D CC 8E B9	AES	c7 2b ea 65 f7 ca fc b8 de 32 4c c3 14 a6 85 8b	
ph=101	ERROR	FE 0E 6E D5 F5 16 F5 43 B4 23 53 54 0D CC 8E B9	AES	c7 2b ea c8 f7 ca fc b8 68 32 d6 c3 14 a6 85 8b	
ph=102	ERROR	FE 0E 6E 78 F5 16 F5 43 02 23 C9 54 0D CC 8E B9	AES	c7 2b ea 65 f7 ca fc b8 de 32 4c c3 14 a6 85 8b	
ph=103	ERROR	FE 0E 6E 63 F5 7C F5 F5 7B 8D 53 E2 09 AF B2 0F	AES	c7 2b ea 7e f7 a0 fc 0e a7 9c d6 75 10 c5 b9 3d	
ph=104	ERROR	FE 0E 6E 63 F5 7C F5 F5 7B 98 53 E2 7A AF B2 0F	AES	c7 2b ea 7e f7 a0 fc 0e a7 89 d6 75 63 c5 b9 3d	

Mise en œuvre de l'attaque

Texte clair **32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34**
Clef **2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c**

calc 39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32

Chiffré correct (calcul software)

ph=68	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=69	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=70	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=71	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=72	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=73	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	6a	0b	b0
ph=74	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	6a	0b	32
ph=75	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=76	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=77	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=78	ERROR	00	00	00	D3	00	7B	36	00	00	00	00	00	00	00	87	82	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
ph=79	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=80	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	84	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	9d	31	8c	b0
ph=81	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=82	ERROR	00	00	B4	D3	00	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	02	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=83	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=84	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=85	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=86	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=87	ERROR	00	00	B4	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=88	ERROR	00	00	B4	D3	1A	76	36	00	16	00	00	1B	6F	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
ph=89	ERROR	00	00	B4	8B	1A	76	36	00	16	00	00	46	6F	63	E2	2F	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
ph=90	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=91	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	E2	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
ph=92	ERROR	00	00	B4	34	1A	76	AF	00	16	00	00	46	6F	68	E2	2F	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
ph=93	ERROR	F8	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=94	ERROR	00	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=95	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=96	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	30	2F	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
ph=97	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	69	4E	24	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
ph=98	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	8E	B9	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
ph=99	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=100	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=101	ERROR	FE	0E	6E	D5	F5	16	F5	43	B4	23	53	54	0D	CC	8E	B9	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
ph=102	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=103	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	8D	53	E2	09	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
ph=104	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	98	53	E2	7A	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d

Mise en œuvre de l'attaque

Texte clair **32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34**
Clef **2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c**

Chiffrés *fautés* (calcul hardware)

	calc	39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32
ph=68	ERROR	00 00 00 00 00 D2 00 00 00 00 00 00 00 00 00 00	AES 39 25 84 1d 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=69	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES 39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=70	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES 39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=71	ERROR	0 00 00 00	AES 39 25 84 1d 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=72	ERROR	0 00 00 00	AES 39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=73	ERROR	00 00 00 D3 00 D2 36 00 00 00 00 00 00 00 00 82	AES 39 25 84 ce 02 0e 3f fb dc 11 85 97 19 6a 0b b0
ph=74	ERROR	00 00 00 D3 00 D2 36 00 00 00 00 00 00 00 00 00	AES 39 25 84 ce 02 0e 3f fb dc 11 85 97 19 6a 0b 32
ph=75	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES 39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=76	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES 39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=77	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES 39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=78	ERROR	00 00 00 D3 00 7B 36 00 00 00 00 00 00 00 87 82	AES 39 25 84 ce 02 a7 3f fb dc 11 85 97 19 6a 8c b0
ph=79	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES 39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=80	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 84 5B 87 82	AES 39 25 84 ce 02 b1 3f fb dc 11 85 97 9d 31 8c b0
ph=81	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES 39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=82	ERROR	00 00 B4 D3 00 76 36 00 00 00 00 00 00 5B 87 82	AES 39 25 30 ce 02 aa 3f fb dc 11 85 97 19 31 8c b0
ph=83	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES 39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0
ph=84	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES 39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0
ph=85	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 00 00 5B 87 82	AES 39 25 30 ce 18 aa 3f fb dc 11 85 97 19 31 8c b0
ph=86	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES 39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0
ph=87	ERROR	00 00 B4 34 1A 76 C3 00 16 00 00 46 6F 68 87 2F	AES 39 25 30 29 18 aa ca fb ca 11 85 d1 76 02 8c 1d
ph=88	ERROR	00 00 B4 D3 1A 76 36 00 16 00 00 1B 6F 63 87 82	AES 39 25 30 ce 18 aa 3f fb ca 11 85 8c 76 09 8c b0
ph=89	ERROR	00 00 B4 8B 1A 76 36 00 16 00 00 46 6F 63 E2 2F	AES 39 25 30 96 18 aa 3f fb ca 11 85 d1 76 09 e9 1d
ph=90	ERROR	00 00 0A 34 1A 76 C3 00 16 00 00 46 6F 68 87 2F	AES 39 25 8e 29 18 aa ca fb ca 11 85 d1 76 02 8c 1d
ph=91	ERROR	00 00 0A 34 1A 76 C3 00 16 00 00 46 6F 68 E2 2F	AES 39 25 8e 29 18 aa ca fb ca 11 85 d1 76 02 e9 1d
ph=92	ERROR	00 00 B4 34 1A 76 AF 00 16 00 00 46 6F 68 E2 2F	AES 39 25 30 29 18 aa a6 fb ca 11 85 d1 76 02 e9 1d
ph=93	ERROR	F8 40 0A 78 37 76 61 D9 92 3F 00 46 6F 4F 87 2F	AES c1 65 8e 65 35 aa 68 22 4e 2e 85 d1 76 25 8c 1d
ph=94	ERROR	00 40 0A 78 37 76 61 D9 92 3F 00 46 6F 4F 87 2F	AES 39 65 8e 65 35 aa 68 22 4e 2e 85 d1 76 25 8c 1d
ph=95	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 0D CC 30 2F	AES c7 65 8e 65 33 aa 68 22 48 2e 85 d1 14 a6 3b 1d
ph=96	ERROR	FE 0E 6E 78 38 76 61 D9 94 23 00 46 0D CC 30 2F	AES c7 2b ea 65 3a aa 68 22 48 32 85 d1 14 a6 3b 1d
ph=97	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 69 4E 24 2F	AES c7 65 8e 65 33 aa 68 22 48 2e 85 d1 70 24 2f 1d
ph=98	ERROR	FE 0E 6E 78 38 76 61 D9 94 23 00 46 0D CC 8E B9	AES c7 2b ea 65 3a aa 68 22 48 32 85 d1 14 a6 85 8b
ph=99	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 0D CC 30 2F	AES c7 65 8e 65 33 aa 68 22 48 2e 85 d1 14 a6 3b 1d
ph=100	ERROR	FE 0E 6E 78 F5 16 F5 43 02 23 C9 54 0D CC 8E B9	AES c7 2b ea 65 f7 ca fc b8 de 32 4c c3 14 a6 85 8b
ph=101	ERROR	FE 0E 6E D5 F5 16 F5 43 B4 23 53 54 0D CC 8E B9	AES c7 2b ea c8 f7 ca fc b8 68 32 d6 c3 14 a6 85 8b
ph=102	ERROR	FE 0E 6E 78 F5 16 F5 43 02 23 C9 54 0D CC 8E B9	AES c7 2b ea 65 f7 ca fc b8 de 32 4c c3 14 a6 85 8b
ph=103	ERROR	FE 0E 6E 63 F5 7C F5 F5 7B 8D 53 E2 09 AF B2 0F	AES c7 2b ea 7e f7 a0 fc 0e a7 9c d6 75 10 c5 b9 3d
ph=104	ERROR	FE 0E 6E 63 F5 7C F5 F5 7B 98 53 E2 7A AF B2 0F	AES c7 2b ea 7e f7 a0 fc 0e a7 89 d6 75 63 c5 b9 3d

Texte clair **32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34**
Clef **2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c**

1ère occurrence d'une faute

Chiffrés *fautés* (calcul hardware)

ph = nombre de pas élémentaires retirés à la période

ΔT = ph x 35 ps

	calc	39	25	84	1d	02	dc	09	fb	dc	11	85	97	19	6a	0b	32
ph=68	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	00
ph=69	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	00
ph=70	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	00
ph=71	ERROR	0												00	00	00	00
ph=72	ERROR	0												00	00	00	00
ph=73	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	82
ph=74	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	00
ph=75	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82
ph=76	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82
ph=77	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82
ph=78	ERROR	00	00	00	D3	00	7B	36	00	00	00	00	00	00	00	87	82
ph=79	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82
ph=80	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	84	5B	87	82
ph=81	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82
ph=82	ERROR	00	00	B4	D3	00	76	36	00	00	00	00	00	00	5B	87	82
ph=83	ERROR	00														87	82
ph=84	ERROR	00														87	82
ph=85	ERROR	00														87	82
ph=86	ERROR	00														87	82
ph=87	ERROR	00														87	2F
ph=88	ERROR	00	00	B4	D3	1A	76	36	00	16	00	00	1B	6F	63	87	82
ph=89	ERROR	00	00	B4	8B	1A	76	36	00	16	00	00	46	6F	63	E2	2F
ph=90	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F
ph=91	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	E2	2F
ph=92	ERROR	00	00	B4	34	1A	76	AF	00	16	00	00	46	6F	68	E2	2F
ph=93	ERROR	F8	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F
ph=94	ERROR	00	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F
ph=95	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F
ph=96	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	30	2F
ph=97	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	69	4E	24	2F
ph=98	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	8E	B9
ph=99	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F
ph=100	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9
ph=101	ERROR	FE	0E	6E	D5	F5	16	F5	43	B4	23	53	54	0D	CC	8E	B9
ph=102	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9
ph=103	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	8D	53	E2	09	AF	B2	0F
ph=104	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	98	53	E2	7A	AF	B2	0F
	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	b0
	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	32
	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	9d	31	8c	b0
	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	30	ce	02	aa	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d

1ère occurrence d'une faute

		Texte clair	32	43	f6	a8	88	5a	30	8d	31	31	98	a2	e0	37	07	34
		Clef	2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c
		calc	39	25	84	1d	02	dc	09	fb	dc	11	85	97	19	6a	0b	32
ph=68	ERROR	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=69	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=70	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=71	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=72	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=73	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	82	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	b0
ph=74	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	32
ph=75	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=76	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=77	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=78	ERROR	00	00	00	D3	00	7B	36	00	00	00	00	00	00	00	87	82	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
ph=79	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=80	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	84	5B	87	82	AES	39	25										7	9d	31	8c	b0
ph=81	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25										7	19	31	8c	b0
ph=82	ERROR	00	00	B4	D3	00	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25										7	19	31	8c	b0
ph=83	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25										c	19	09	8c	b0
ph=84	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=85	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=86	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=87	ERROR	00	00	B4	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=88	ERROR	00	00	B4	D3	1A	76	36	00	16	00	00	1B	6F	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
ph=89	ERROR	00	00	B4	8B	1A	76	36	00	16	00	00	46	6F	63	E2	2F	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
ph=90	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=91	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	E2	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
ph=92	ERROR	00	00	B4	34	1A	76	AF	00	16	00	00	46	6F	68	E2	2F	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
ph=93	ERROR	F8	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=94	ERROR	00	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=95	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=96	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	30	2F	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
ph=97	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	69	4E	24	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
ph=98	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	8E	B9	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
ph=99	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=100	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=101	ERROR	FE	0E	6E	D5	F5	16	F5	43	B4	23	53	54	0D	CC	8E	B9	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
ph=102	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=103	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	8D	53	E2	09	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
ph=104	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	98	53	E2	7A	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d

ERROR = calc ⊕ AES

Visualisation de l'erreur

1ère occurrence d'une faute

		Texte clair	**32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34**	
		Clef	**2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c**	
		calc	39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32	
ph=68	ERROR	00 00 00 00 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 1d 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=69	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=70	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=71	ERROR	00 00 00 00 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 1d 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=72	ERROR	00 00 00 D3 00 D2 00 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 09 fb dc 11 85 97 19 6a 0b 32
ph=73	ERROR	00 00 00 D3 00 D2 36 00 00 00 00 00 00 00 00 82	AES	39 25 84 ce 02 0e 3f fb dc 11 85 97 19 6a 0b b0
ph=74	ERROR	00 00 00 D3 00 D2 36 00 00 00 00 00 00 00 00 00	AES	39 25 84 ce 02 0e 3f fb dc 11 85 97 19 6a 0b 32
ph=75	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=76	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=77	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=78	ERROR	00 00 00 D3 00 7B 36 00 00 00 00 00 00 00 87 82	AES	39 25 84 ce 02 a7 3f fb dc 11 85 97 19 6a 8c b0
ph=79	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=80	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 84 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 9d 31 8c b0
ph=81	ERROR	00 00 00 D3 00 6D 36 00 00 00 00 00 00 5B 87 82	AES	39 25 84 ce 02 b1 3f fb dc 11 85 97 19 31 8c b0
ph=82	ERROR	00 00 B4 D3 00 76 36 00 00 00 00 00 00 5B 87 82	AES	39 25 30 ce 02 aa 3f fb dc 11 85 97 19 31 8c b0
ph=83	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0
ph=84	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0
ph=85	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 00 00 5B 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 97 19 31 8c b0
ph=86	ERROR	00 00 B4 D3 1A 76 36 00 00 00 00 1B 00 63 87 82	AES	39 25 30 ce 18 aa 3f fb dc 11 85 8c 19 09 8c b0
ph=87	ERROR	00 00 B4 34 1A 76 C3 00 16 00 00 46 6F 68 87 2F	AES	39 25 30 29 18 aa ca fb ca 11 85 d1 76 02 8c 1d
ph=88	ERROR	00 00 B4 D3 1A 76 36 00 16 00 00 1B 6F 63 87 82	AES	39 25 30 ce 18 aa 3f fb ca 11 85 8c 76 09 8c b0
ph=89	ERROR	00 00 B4 8B 1A 76 36 00 16 00 00 46 6F 63 E2 2F	AES	39 25 30 96 18 aa 3f fb ca 11 85 d1 76 09 e9 1d
ph=90	ERROR	00 00 0A 34 1A 76 C3 00 16 00 00 46 6F 68 87 2F	AES	39 25 8e 29 18 aa ca fb ca 11 85 d1 76 02 8c 1d
ph=91	ERROR	00 00 0A 34 1A 76 C3 00 16 00 00 46 6F 68 E2 2F	AES	39 25 8e 29 18 aa ca fb ca 11 85 d1 76 02 e9 1d
ph=92	ERROR	00 00 B4 34 1A 76 AF 00 16 00 00 46 6F 68 E2 2F	AES	39 25 30 29 18 aa a6 fb ca 11 85 d1 76 02 e9 1d
ph=93	ERROR	F8 40 0A 78 37 76 61 D9 92 3F 00 46 6F 4F 87 2F	AES	c1 65 8e 65 35 aa 68 22 4e 2e 85 d1 76 25 8c 1d
ph=94	ERROR	00 40 0A 78 37 76 61 D9 92 3F 00 46 6F 4F 87 2F	AES	39 65 8e 65 35 aa 68 22 4e 2e 85 d1 76 25 8c 1d
ph=95	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 0D CC 30 2F	AES	c7 65 8e 65 33 aa 68 22 48 2e 85 d1 14 a6 3b 1d
ph=96	ERROR	FE 0E 6E 78 38 76 61 D9 94 23 00 46 0D CC 30 2F	AES	c7 2b ea 65 3a aa 68 22 48 32 85 d1 14 a6 3b 1d
ph=97	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 69 4E 24 2F	AES	c7 65 8e 65 33 aa 68 22 48 2e 85 d1 70 24 2f 1d
ph=98	ERROR	FE 0E 6E 78 38 76 61 D9 94 23 00 46 0D CC 8E B9	AES	c7 2b ea 65 3a aa 68 22 48 32 85 d1 14 a6 85 8b
ph=99	ERROR	FE 40 0A 78 31 76 61 D9 94 3F 00 46 0D CC 30 2F	AES	c7 65 8e 65 33 aa 68 22 48 2e 85 d1 14 a6 3b 1d
ph=100	ERROR	FE 0E 6E 78 F5 16 F5 43 02 23 C9 54 0D CC 8E B9	AES	c7 2b ea 65 f7 ca fc b8 de 32 4c c3 14 a6 85 8b
ph=101	ERROR	FE 0E 6E D5 F5 16 F5 43 B4 23 53 54 0D CC 8E B9	AES	c7 2b ea c8 f7 ca fc b8 68 32 d6 c3 14 a6 85 8b
ph=102	ERROR	FE 0E 6E 78 F5 16 F5 43 02 23 C9 54 0D CC 8E B9	AES	c7 2b ea 65 f7 ca fc b8 de 32 4c c3 14 a6 85 8b
ph=103	ERROR	FE 0E 6E 63 F5 7C F5 F5 7B 8D 53 E2 09 AF B2 0F	AES	c7 2b ea 7e f7 a0 fc 0e a7 9c d6 75 10 c5 b9 3d
ph=104	ERROR	FE 0E 6E 63 F5 7C F5 F5 7B 98 53 E2 7A AF B2 0F	AES	c7 2b ea 7e f7 a0 fc 0e a7 89 d6 75 63 c5 b9 3d

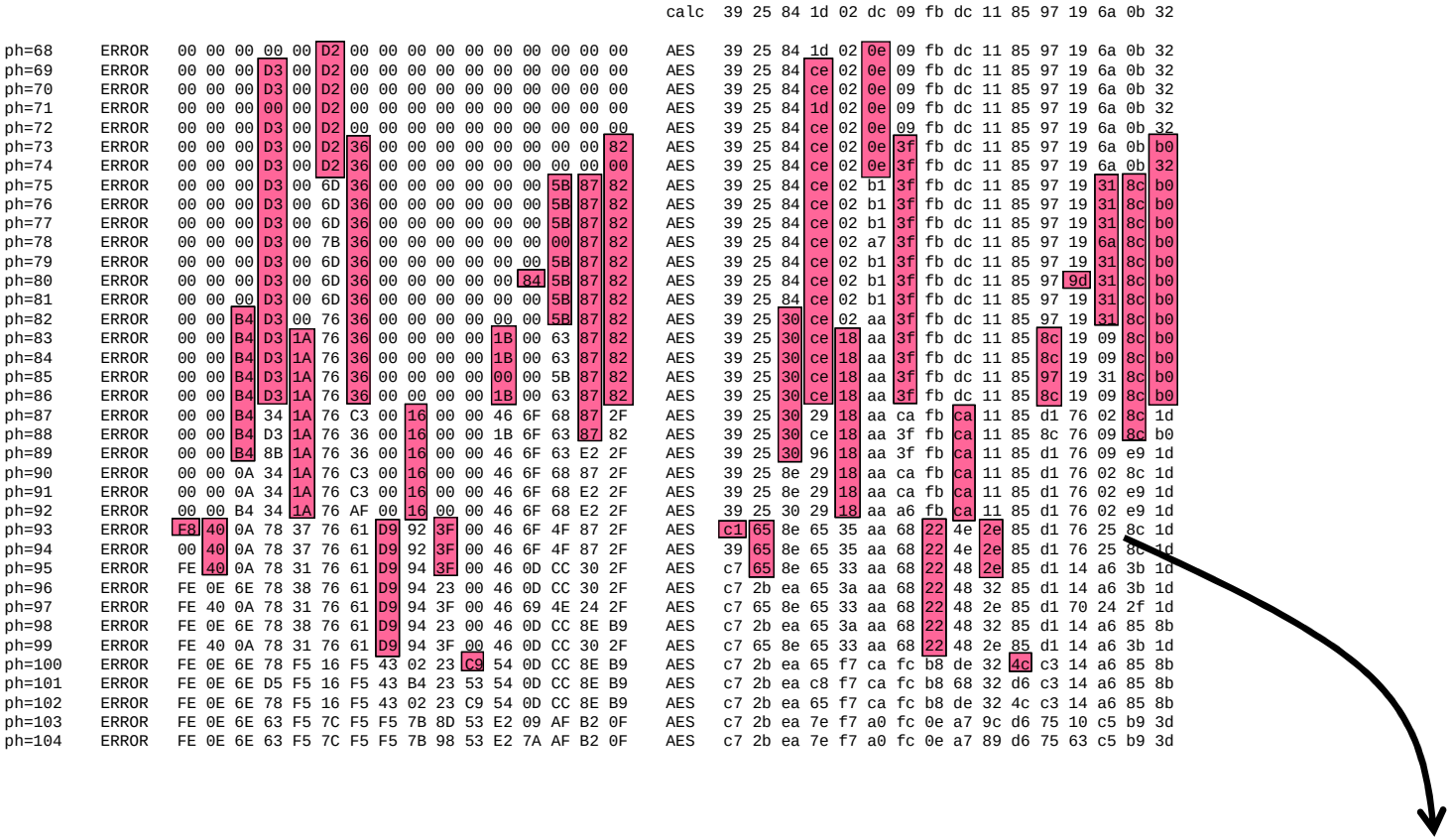
																Texte clair	**32**	**43**	**f6**	**a8**	**88**	**5a**	**30**	**8d**	**31**	**31**	**98**	**a2**	**e0**	**37**	**07**	**34**
																Clef	**2b**	**7e**	**15**	**16**	**28**	**ae**	**d2**	**a6**	**ab**	**f7**	**15**	**88**	**09**	**cf**	**4f**	**3c**
																calc	39	25	84	1d	02	dc	09	fb	dc	11	85	97	19	6a	0b	32
ph=68	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=69	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=70	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=71	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=72	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=73	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	82	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	b0
ph=74	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	32
ph=75	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=76	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=77	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=78	ERROR	00	00	00	D3	00	7B	36	00	00	00	00	00	00	00	87	82	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
ph=79	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=80	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	84	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	9d	31	8c	b0
ph=81	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=82	ERROR	00	00	B4	D3	00	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	02	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=83	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=84	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=85	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=86	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=87	ERROR	00	00	B4	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=88	ERROR	00	00	B4	D3	1A	76	36	00	16	00	00	1B	6F	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
ph=89	ERROR	00	00	B4	8B	1A	76	36	00	16	00	00	46	6F	63	E2	2F	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
ph=90	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=91	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	E2	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
ph=92	ERROR	00	00	B4	34	1A	76	AF	00	16	00	00	46	6F	68	E2	2F	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
ph=93	ERROR	F8	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=94	ERROR	00	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=95	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=96	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	30	2F	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
ph=97	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	69	4E	24	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
ph=98	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	8E	B9	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
ph=99	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=100	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=101	ERROR	FE	0E	6E	D5	F5	16	F5	43	B4	23	53	54	0D	CC	8E	B9	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
ph=102	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=103	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	8D	53	E2	09	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
ph=104	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	98	53	E2	7A	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d

Hypothèse : faute monobit

																	Texte clair	**32**	**43**	**f6**	**a8**	**88**	**5a**	**30**	**8d**	**31**	**31**	**98**	**a2**	**e0**	**37**	**07**	**34**
																	Clef	**2b**	**7e**	**15**	**16**	**28**	**ae**	**d2**	**a6**	**ab**	**f7**	**15**	**88**	**09**	**cf**	**4f**	**3c**
																	calc	39	25	84	1d	02	dc	09	fb	dc	11	85	97	19	6a	0b	32
ph=68	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=69	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=70	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=71	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=72	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=73	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	82	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	b0
ph=74	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	32
ph=75	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=76	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=77	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=78	ERROR	00	00	00	D3	00	7B	36	00	00	00	00	00	00	00	87	82	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
ph=79	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=80	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	84	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	9d	31	8c	b0
ph=81	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=82	ERROR	00	00	B4	D3	00	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	02	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=83	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=84	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=85	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=86	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=87	ERROR	00	00	B4	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=88	ERROR	00	00	B4	D3	1A	76	36	00	16	00	00	1B	6F	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
ph=89	ERROR	00	00	B4	8B	1A	76	36	00	16	00	00	46	6F	63	E2	2F	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
ph=90	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=91	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	E2	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
ph=92	ERROR	00	00	B4	34	1A	76	AF	00	16	00	00	46	6F	68	E2	2F	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
ph=93	ERROR	F8	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=94	ERROR	00	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=95	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=96	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	30	2F	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
ph=97	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	69	4E	24	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
ph=98	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	8E	B9	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
ph=99	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=100	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=101	ERROR	FE	0E	6E	D5	F5	16	F5	43	B4	23	53	54	0D	CC	8E	B9	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
ph=102	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=103	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	8D	53	E2	09	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
ph=104	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	98	53	E2	7A	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d

Mise en œuvre de l'attaque

																	Texte clair	**32**	**43**	**f6**	**a8**	**88**	**5a**	**30**	**8d**	**31**	**31**	**98**	**a2**	**e0**	**37**	**07**	**34**
																	Clef	**2b**	**7e**	**15**	**16**	**28**	**ae**	**d2**	**a6**	**ab**	**f7**	**15**	**88**	**09**	**cf**	**4f**	**3c**
																	calc	39	25	84	1d	02	dc	09	fb	dc	11	85	97	19	6a	0b	32
ph=68	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=69	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=70	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=71	ERROR	00	00	00	00	00	D2	00	00	00	00	00	00	00	00	00	00	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=72	ERROR	00	00	00	D3	00	D2	00	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=73	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	82	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	b0
ph=74	ERROR	00	00	00	D3	00	D2	36	00	00	00	00	00	00	00	00	00	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	32
ph=75	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=76	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=77	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=78	ERROR	00	00	00	D3	00	7B	36	00	00	00	00	00	00	00	87	82	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
ph=79	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=80	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	84	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	9d	31	8c	b0
ph=81	ERROR	00	00	00	D3	00	6D	36	00	00	00	00	00	00	5B	87	82	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=82	ERROR	00	00	B4	D3	00	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	02	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=83	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=84	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=85	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	00	00	5B	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=86	ERROR	00	00	B4	D3	1A	76	36	00	00	00	00	1B	00	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=87	ERROR	00	00	B4	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=88	ERROR	00	00	B4	D3	1A	76	36	00	16	00	00	1B	6F	63	87	82	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
ph=89	ERROR	00	00	B4	8B	1A	76	36	00	16	00	00	46	6F	63	E2	2F	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
ph=90	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	87	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=91	ERROR	00	00	0A	34	1A	76	C3	00	16	00	00	46	6F	68	E2	2F	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
ph=92	ERROR	00	00	B4	34	1A	76	AF	00	16	00	00	46	6F	68	E2	2F	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
ph=93	ERROR	F8	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=94	ERROR	00	40	0A	78	37	76	61	D9	92	3F	00	46	6F	4F	87	2F	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=95	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=96	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	30	2F	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
ph=97	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	69	4E	24	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
ph=98	ERROR	FE	0E	6E	78	38	76	61	D9	94	23	00	46	0D	CC	8E	B9	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
ph=99	ERROR	FE	40	0A	78	31	76	61	D9	94	3F	00	46	0D	CC	30	2F	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=100	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=101	ERROR	FE	0E	6E	D5	F5	16	F5	43	B4	23	53	54	0D	CC	8E	B9	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
ph=102	ERROR	FE	0E	6E	78	F5	16	F5	43	02	23	C9	54	0D	CC	8E	B9	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=103	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	8D	53	E2	09	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
ph=104	ERROR	FE	0E	6E	63	F5	7C	F5	F5	7B	98	53	E2	7A	AF	B2	0F	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d



		calc	39	25	84	1d	02	dc	09	fb	dc	11	85	97	19	6a	0b	32
ph=68	ERROR	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=69	ERROR	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=70	ERROR	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=71	ERROR	AES	39	25	84	1d	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=72	ERROR	AES	39	25	84	ce	02	0e	09	fb	dc	11	85	97	19	6a	0b	32
ph=73	ERROR	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	b0
ph=74	ERROR	AES	39	25	84	ce	02	0e	3f	fb	dc	11	85	97	19	6a	0b	32
ph=75	ERROR	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=76	ERROR	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=77	ERROR	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=78	ERROR	AES	39	25	84	ce	02	a7	3f	fb	dc	11	85	97	19	6a	8c	b0
ph=79	ERROR	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=80	ERROR	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	9d	31	8c	b0
ph=81	ERROR	AES	39	25	84	ce	02	b1	3f	fb	dc	11	85	97	19	31	8c	b0
ph=82	ERROR	AES	39	25	30	ce	02	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=83	ERROR	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=84	ERROR	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=85	ERROR	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	97	19	31	8c	b0
ph=86	ERROR	AES	39	25	30	ce	18	aa	3f	fb	dc	11	85	8c	19	09	8c	b0
ph=87	ERROR	AES	39	25	30	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=88	ERROR	AES	39	25	30	ce	18	aa	3f	fb	ca	11	85	8c	76	09	8c	b0
ph=89	ERROR	AES	39	25	30	96	18	aa	3f	fb	ca	11	85	d1	76	09	e9	1d
ph=90	ERROR	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	8c	1d
ph=91	ERROR	AES	39	25	8e	29	18	aa	ca	fb	ca	11	85	d1	76	02	e9	1d
ph=92	ERROR	AES	39	25	30	29	18	aa	a6	fb	ca	11	85	d1	76	02	e9	1d
ph=93	ERROR	AES	c1	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=94	ERROR	AES	39	65	8e	65	35	aa	68	22	4e	2e	85	d1	76	25	8c	1d
ph=95	ERROR	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=96	ERROR	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	3b	1d
ph=97	ERROR	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	70	24	2f	1d
ph=98	ERROR	AES	c7	2b	ea	65	3a	aa	68	22	48	32	85	d1	14	a6	85	8b
ph=99	ERROR	AES	c7	65	8e	65	33	aa	68	22	48	2e	85	d1	14	a6	3b	1d
ph=100	ERROR	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=101	ERROR	AES	c7	2b	ea	c8	f7	ca	fc	b8	68	32	d6	c3	14	a6	85	8b
ph=102	ERROR	AES	c7	2b	ea	65	f7	ca	fc	b8	de	32	4c	c3	14	a6	85	8b
ph=103	ERROR	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	9c	d6	75	10	c5	b9	3d
ph=104	ERROR	AES	c7	2b	ea	7e	f7	a0	fc	0e	a7	89	d6	75	63	c5	b9	3d

monobit C1 65 30 CE 18 0E 3F 22 CA 2E 4C 8C 9D 31 8C B0

Chiffré fauté reconstitué à partir des fautes monobits supposées sur chacun des octets

Lecture du couple de mots cryptés correct et faux N°1

Valeur de C : **39 02 dc 19**
25 dc 11 6a
84 09 85 0b
1d fb 97 32

Valeur de D : **c7 18 ca 9d**
65 0e 2e 31
30 3f 4c 8c
ce 22 8c b0

Hypothèses sur K10 :

K10(1) : 7f 81 45 bb 2d d3 f2 0c

K10(2) : 54 14 75 35 25 65

K10(3) : 4d f9 72 c6

K10(4) : a8 7b 1b c8 c6 15 ea 39

K10(5) : 8c 96 d3 c9 a0 ba

K10(6) : 3c ee a1 73 a2 70 19 cb

K10(7) : 25 13 68 5e e0 d6 8f b9 1a 2c

K10(8) : 37 ee 50 89 f2 2b 0f d6

K10(9) : 44 52 33 25 83 95 d7 c1 f7 e1

K10(10) : c1 fe a5 9a c8 f7 3f 00

K10(11) : 5a 93 4c 85 c5 0c

K10(12) : c8 d3 f5 ee 31 2a 9d 86 57 4c

K10(13) : 90 14 4b cf e2 66 32 b6 b2 36

K10(14) : 63 38 d0 8b 1d 46

K10(15) : b5 32 0c 8b c0 47 66 e1 15 92 6b ec

K10(16) : 61 e3 a0 22 f6 74 55 d7 bd 3f

Lecture du couple de mots cryptés correct et faux N°2

Valeur de C :	**95 f6 da e8**	**Valeur de D :**	**6c 11 52 58**
	ef 25 7d e1		**91 58 57 b7**
	73 6e c9 f2		**e4 98 7a a7**
	2e eb 05 41		**76 78 97 2b**

Hypothèses sur K10 :

K10(1) : 0c 1f 29 2d 2e 43 45 7f 81 ba bb d0 d3 d7 e6 f2

K10(2) : 14

K10(3) : 06 08 2b 4d 52 72 91 9f bc c5 c6 f9

K10(4) : a8

K10(5) : c9

K10(6) : 3c ee

K10(7) : 25

K10(8) : 37 50 89

K10(9) : 44 e1

K10(10) : 3f

K10(11) : 0c 85

K10(12) : c8

K10(13) : 14 b6

K10(14) : 63

K10(15) : 0c

K10(16) : 22 61

Lecture du couple de mots cryptés correct et faux N°3

Valeur de C :	**4c 67 df 90**	**Valeur de D :**	**9a 2d 87 75**
	71 a2 65 47		**6e c7 9f 27**
	61 49 43 5e		**77 73 b4 6f**
	a7 f1 06 22		**11 54 78 69**

Hypothèses sur K10 :

K10(1) : d0

K10(2) : 14

K10(3) : f9

K10(4) : a8

K10(5) : c9

K10(6) : 02 11 22 3c 47 67 74 af ca ee

K10(7) : 25

K10(8) : 89

K10(9) : e1

K10(10) : 3f

K10(11) : 0c

K10(12) : c8

K10(13) : b6

K10(14) : 63

K10(15) : 0c

K10(16) : 21 22 27 35 3c 61 6a 6c 77 7e a6 b6 ed fd

Lecture du couple de mots cryptés correct et faux N°4

Valeur de C :	**b5 e3 1e cb**	**Valeur de D :**	**5d 41 c6 46**
	77 54 2f e2		**e6 0f ad 8d**
	ed 32 6e 71		**41 56 75 77**
	00 95 82 77		**7a c2 e1 f5**

Hypothèses sur K10 :

K10(1) : d0

K10(2) : 14

K10(3) : f9

K10(4) : a8

K10(5) : c9

K10(6) : ee

K10(7) : 25

K10(8) : 89

K10(9) : e1

K10(10) : 3f

K10(11) : 0c

K10(12) : c8

K10(13) : b6

K10(14) : 63

K10(15) : 0c

K10(16) : a6

❑ Conclusion

- Présentation d'une nouvelle technique d'injection de faute via le signal d'horloge
  - Choix du cycle d'injection - Contrôle fin de la période "fautante" (35 ps)
  - Attaque bas coût – Comparaison / glitch
- Validation expérimentale
- Mise en évidence de la vulnérabilité inhérente au signal d'horloge

⇨ Développement de contre-mesures adaptées