Ecole Nationale Supérieure des Mines
SAINT-ETIENNE
Site Georges Charpak

leti
cea

Revue expérimentale des techniques d'injection de fautes

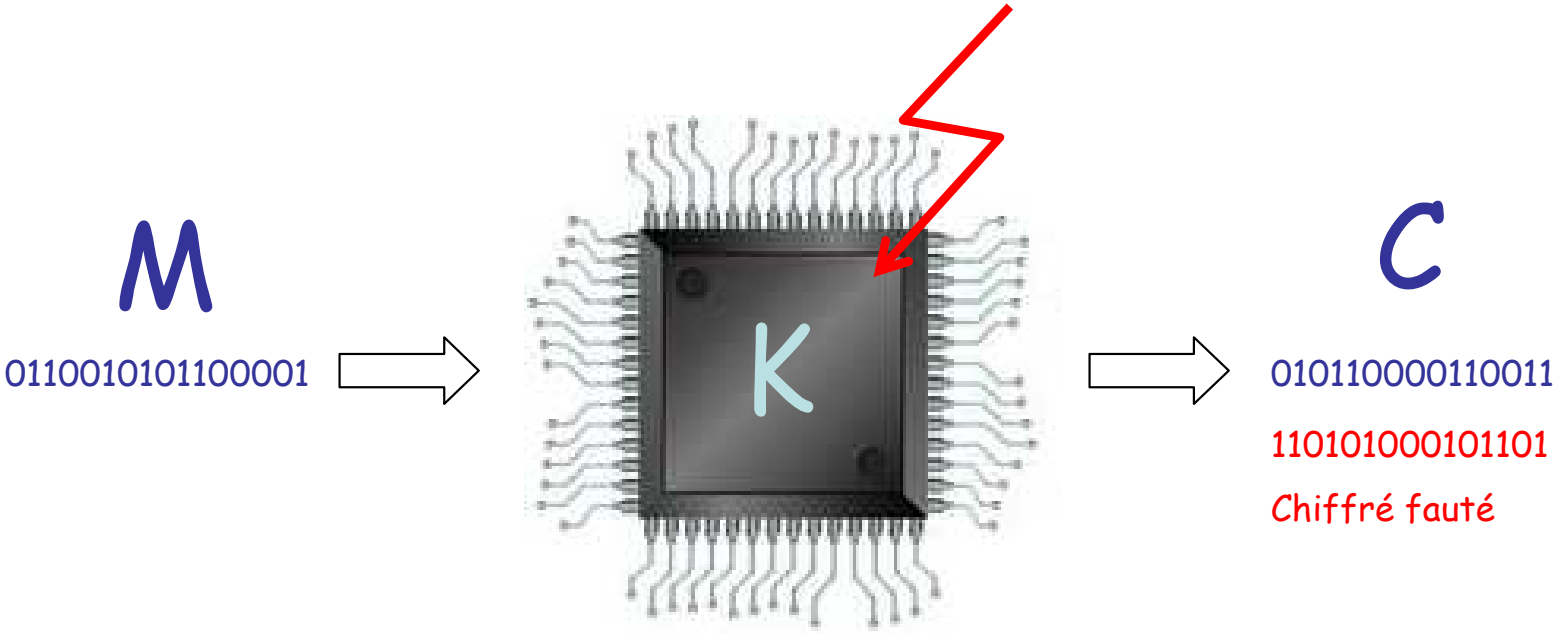
Journée sécurité – 31 mars 2010 – GDR SoC-SiP

Jean-Max Dutertre – ENSMSE
Amir-Pasha Mirbaha - ENSMSE
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

- Introduction.
  - Mise en perspective - Problématique
- Techniques d'injection de fautes non invasives.
  - Théorie (violations de setup et de délai)
  - Réalisations expérimentales
- Techniques d'injection de fautes semi-invasives.
  - L'injection laser (effet photoélectrique)
  - Injection mono octet
- Conclusion

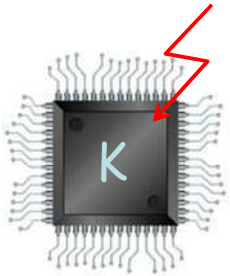
- Attaques par injection de fautes



Technique d'attaque active, visant l'implémentation physique d'un algorithme de chiffrement.

Perturbation de l'environnement du circuit lors du chiffrement.

Partie expérimentale



Technique d'injection

Chiffrés fautés, side channels, comportement, etc.

Extraction informations

Méthodes

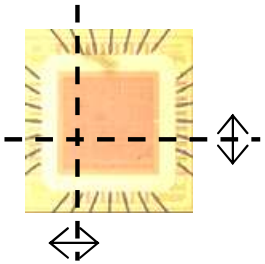
- Réduction nb. rondes
- Analyse différentielle de fautes
- Safe error

Modèle de faute

- Instant d'injection
- Bit /Octet
- Random / Given value

La technique d'injection employée doit permettre l'injection de fautes respectant le modèle de faute requis.

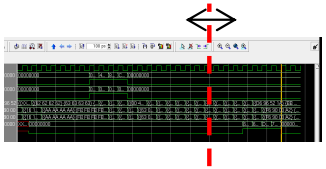
- Caractéristiques principales des techniques d'injection de fautes.



Contrôle de la localisation (x, y, z)

+

Contrôle de l'instant d'injection

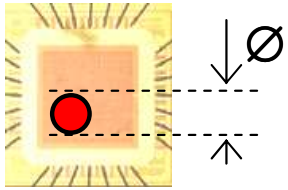


+

Type de faute (collage, inversion, aléatoire, etc.)

+

Contrôle de la focalisation (nb. bits fautés)



+

Reproductibilité

+

Coût

+

Facilité d'emploi

Du point de vue d'un attaquant / de la caractérisation sécuritaire.

- Principaux modèles de faute.

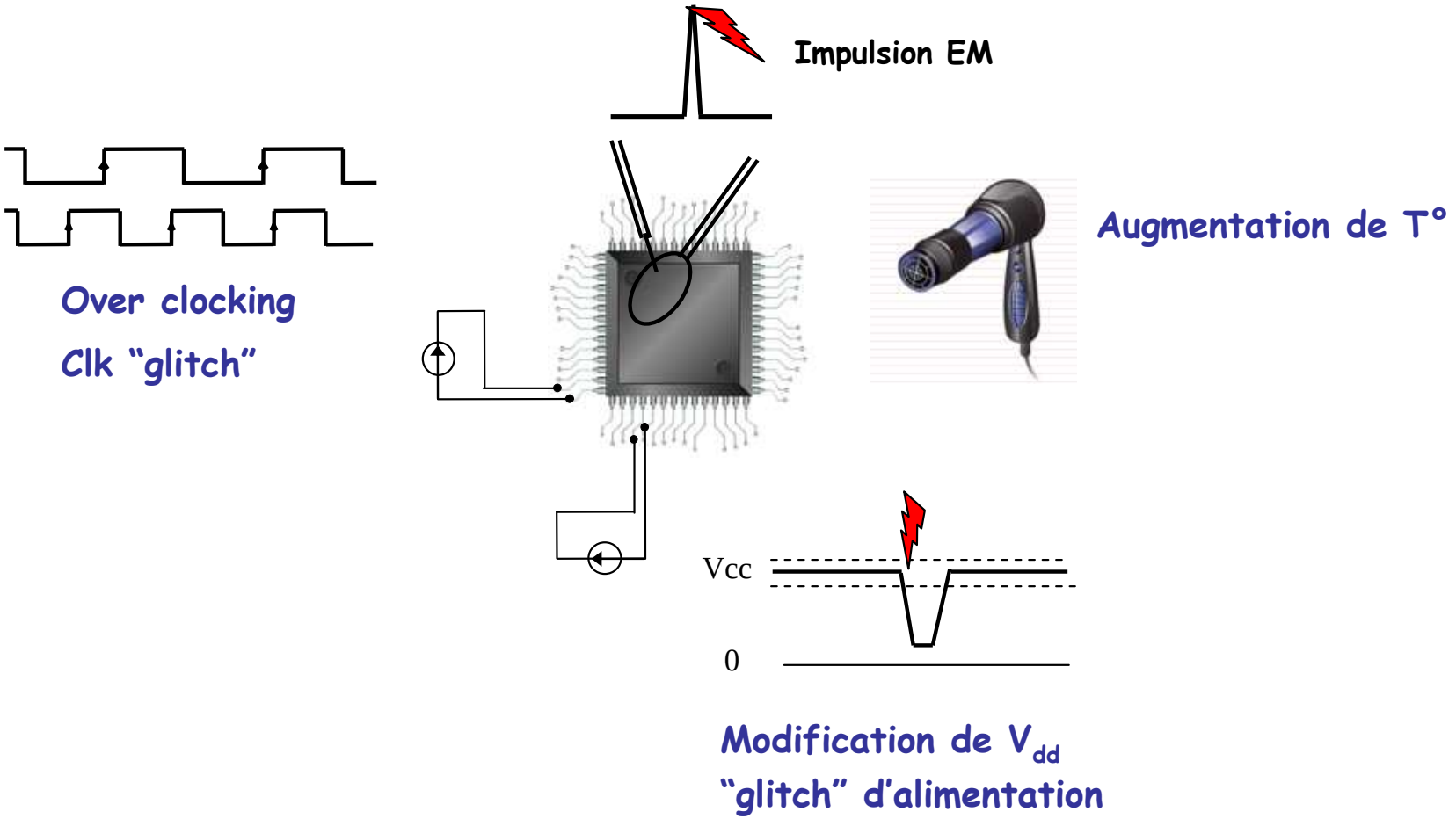
Ref	Type	Localisation	Type de faute	Focalisation	Nb. localisations distinctes	Nb. Réalisations
[Giraud03]	DFA	Data (16*start[9])	Inversion	Bit	16	approx. 50
[Giraud03]	DFA	Key (4*w[9] and 4*w[8]) Data (4*m[8])	Random	Byte	12	250 (for 14 bytes)
[Chen03]	DFA	Key (4*w[9]) Data 7*w[8]	Random	Byte	11	32 (for 13 bytes)
[Piret03]	DFA	Data (4*(anywhere between the 2 last mixcolumns) ou 1*m[8])	Random	Byte	4 or 1	"+8 or +2"
[Dusart03]	DFA	Data (4*(anywhere between the 2 last mixcolumns))	Random	Byte	4	8
[Blomer03]	SEA	Data (start[0])	Collage	Bit	128	128
[Rob07]	SEA	Data (between sbox[0] and start[1])	Collage	Bit	16	approx. 256
[Rob07]	SEA	Data (sbox[0])	Collage	Bit to Byte	16	approx. 256 to 4096
[Choukri05]	RR	Round counter	Depending	Depending	1	3
[Monnet06]	RR	Round counter	bit-flip	1 or 2 bits	depends	depends

- Principales techniques d'injection de fautes.

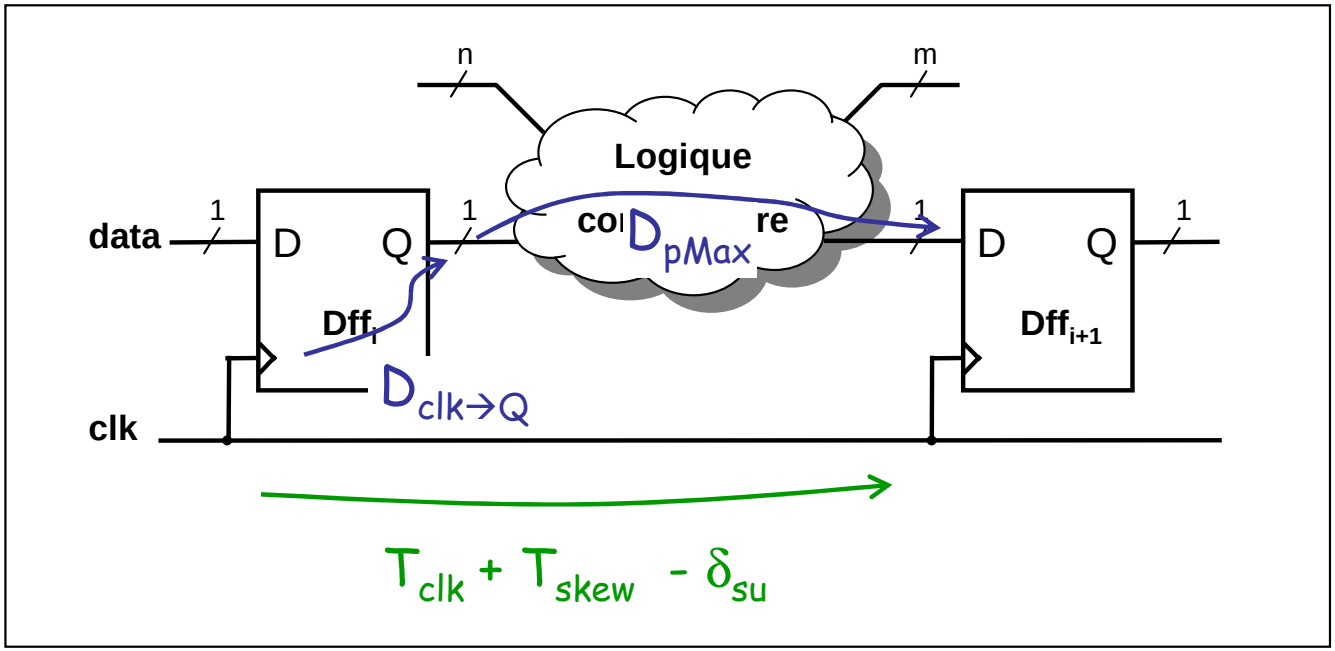
  Attaques non invasives.

  Attaques semi-invasives.

- Attaques non invasives : ne requérant pas l'ouverture du boîtier.



- Contrainte temporelle des circuits synchrones.



data arrival time = $D_{clk \rightarrow Q} + D_{pMax}$

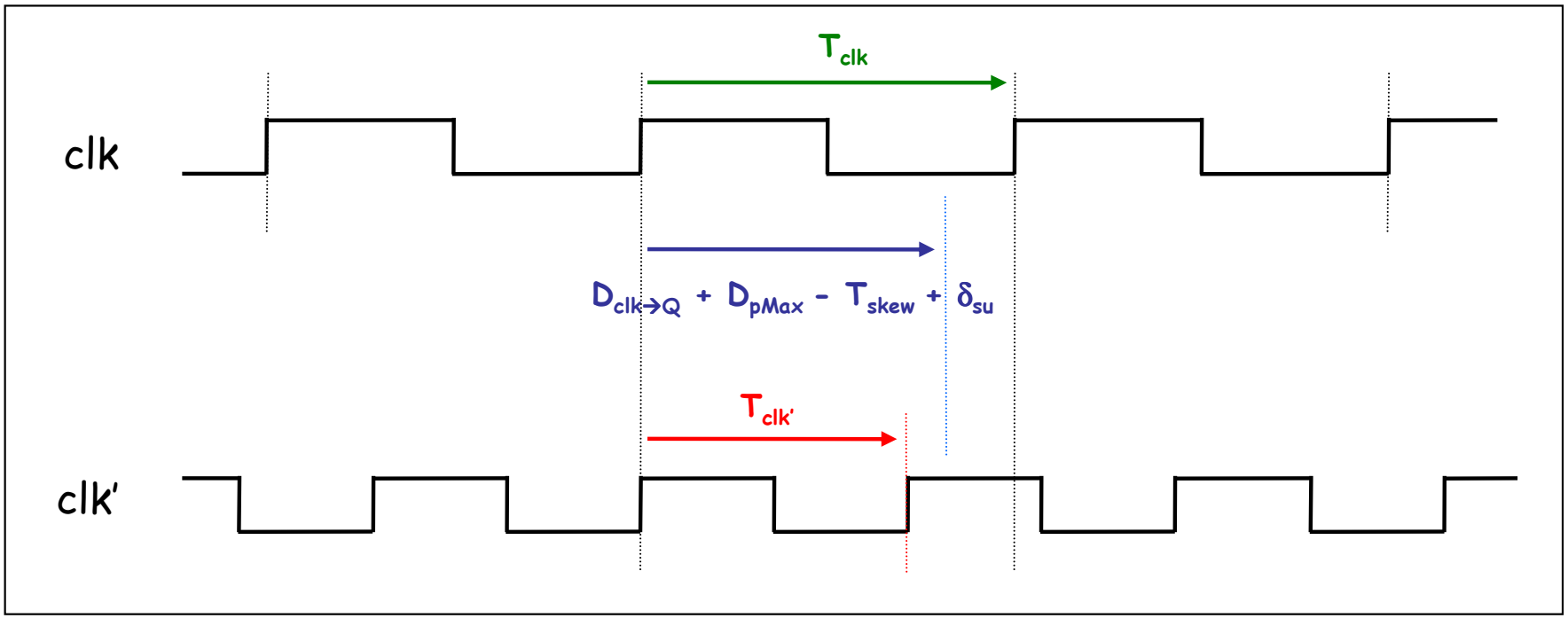
data required time = $T_{clk} + T_{skew} - \delta_{su}$

$\Rightarrow$ $T_{clk} > D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su}$

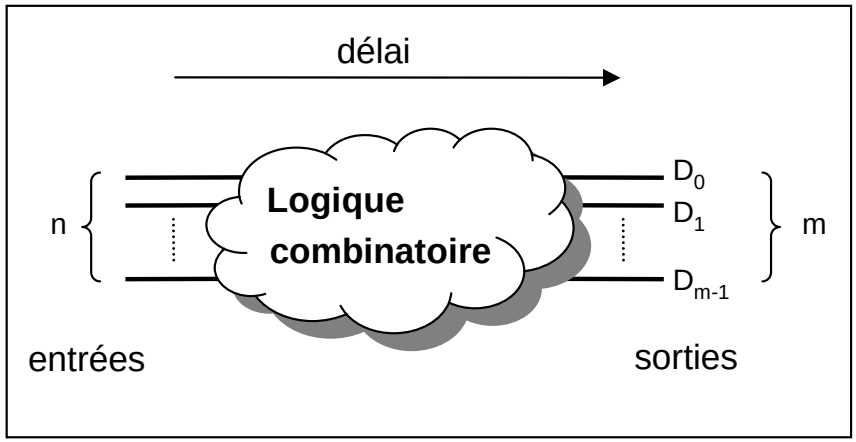
- Overclocking.

  Approche classique : décroissance progressive de T_{clk} jusqu'à obtenir une violation de temps de setup.

$$T_{clk'} < D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su} < T_{clk}$$



- Temps de propagation – Chemin critique



sorties = f(entrées)

f fonction logique

chaque D_i possède son propre temps de propagation

Localisation des fautes :

délai > $T_{clk'}$ – setup time – $D_{clk \to Q}$ + T_{skew}

Chemin critique = max des tps de propagation

Le temps de propagation dépend :

- **des niveaux logiques (0 / 1)**
  → le temps de propagation change avec les entrées

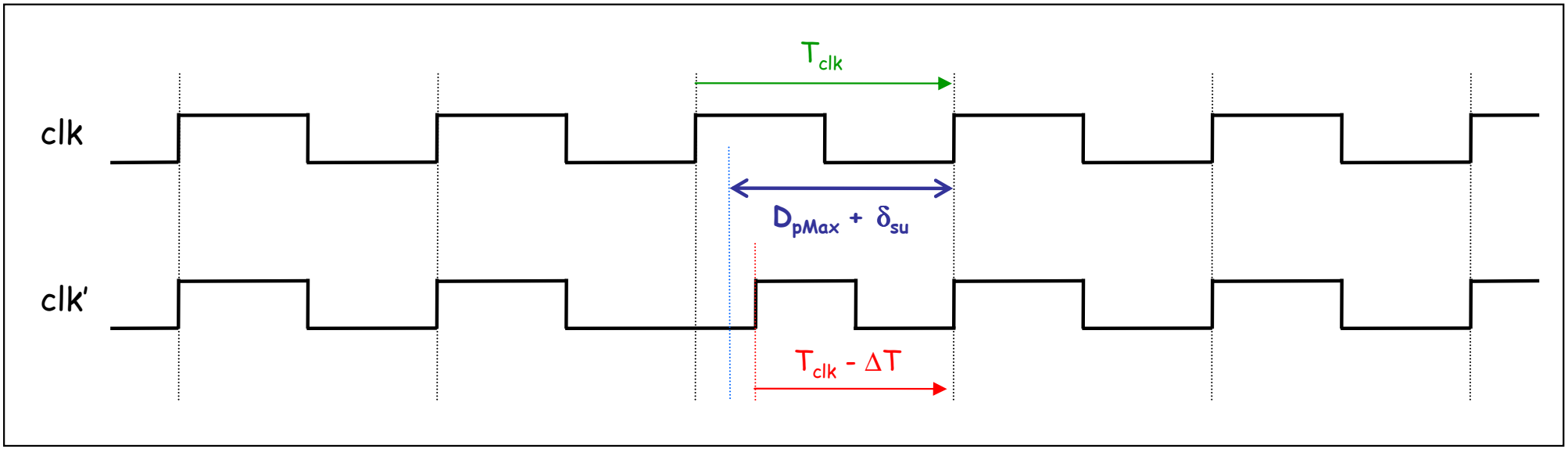
permet de modifier l'endroit d'injection

- de la tension d'alimentation
- de la température

- Overclocking (suite).

⇨ limitation : injection de fautes potentiellement à chaque cycle d'horloge.

- *Glitch* d'horloge – Modification locale d'une période.

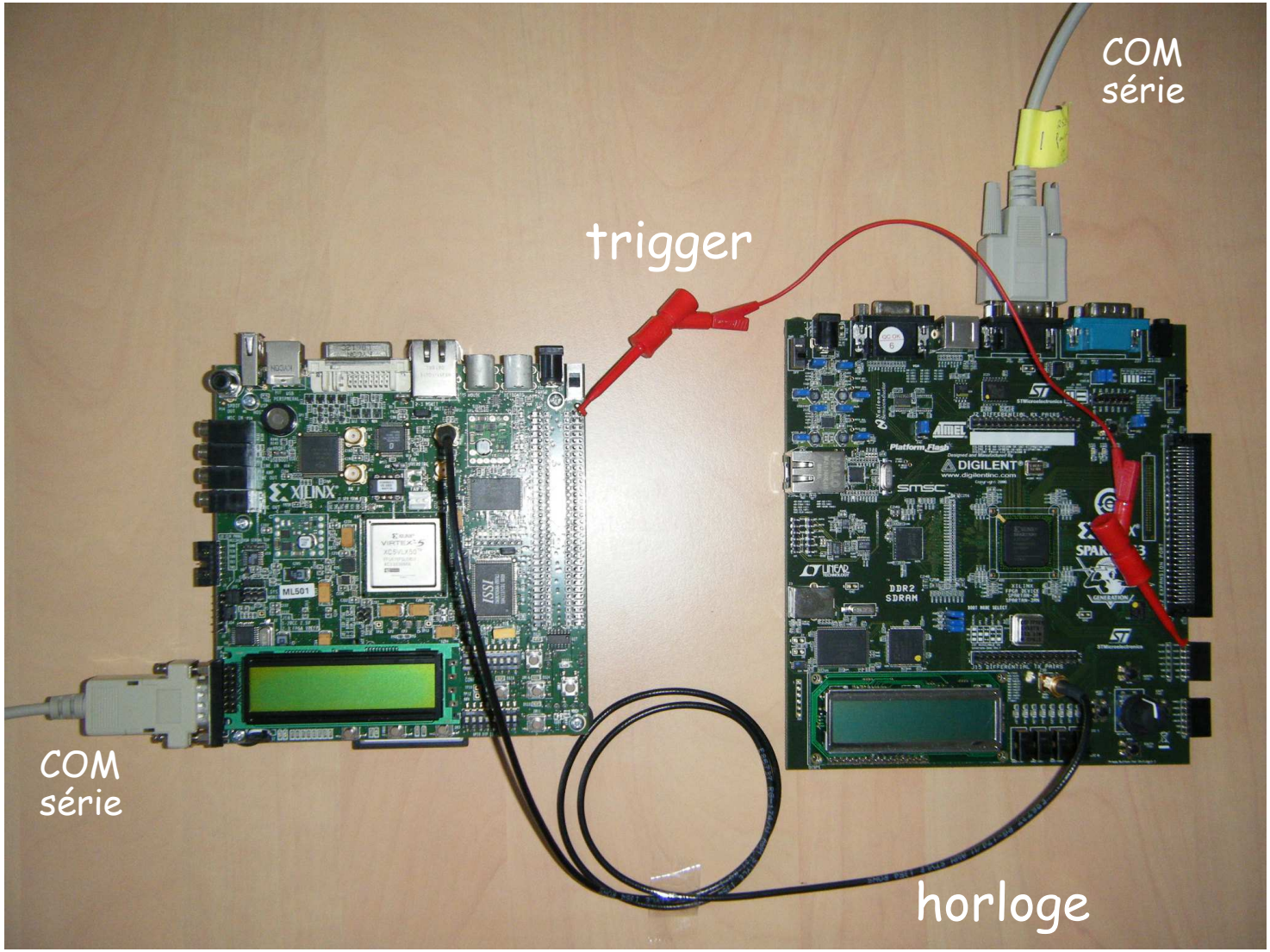


⇨ Choix du cycle d'injection.

⇨ Contrôle fin de la nature des fautes injectées ($\Delta T = 35$ ps).

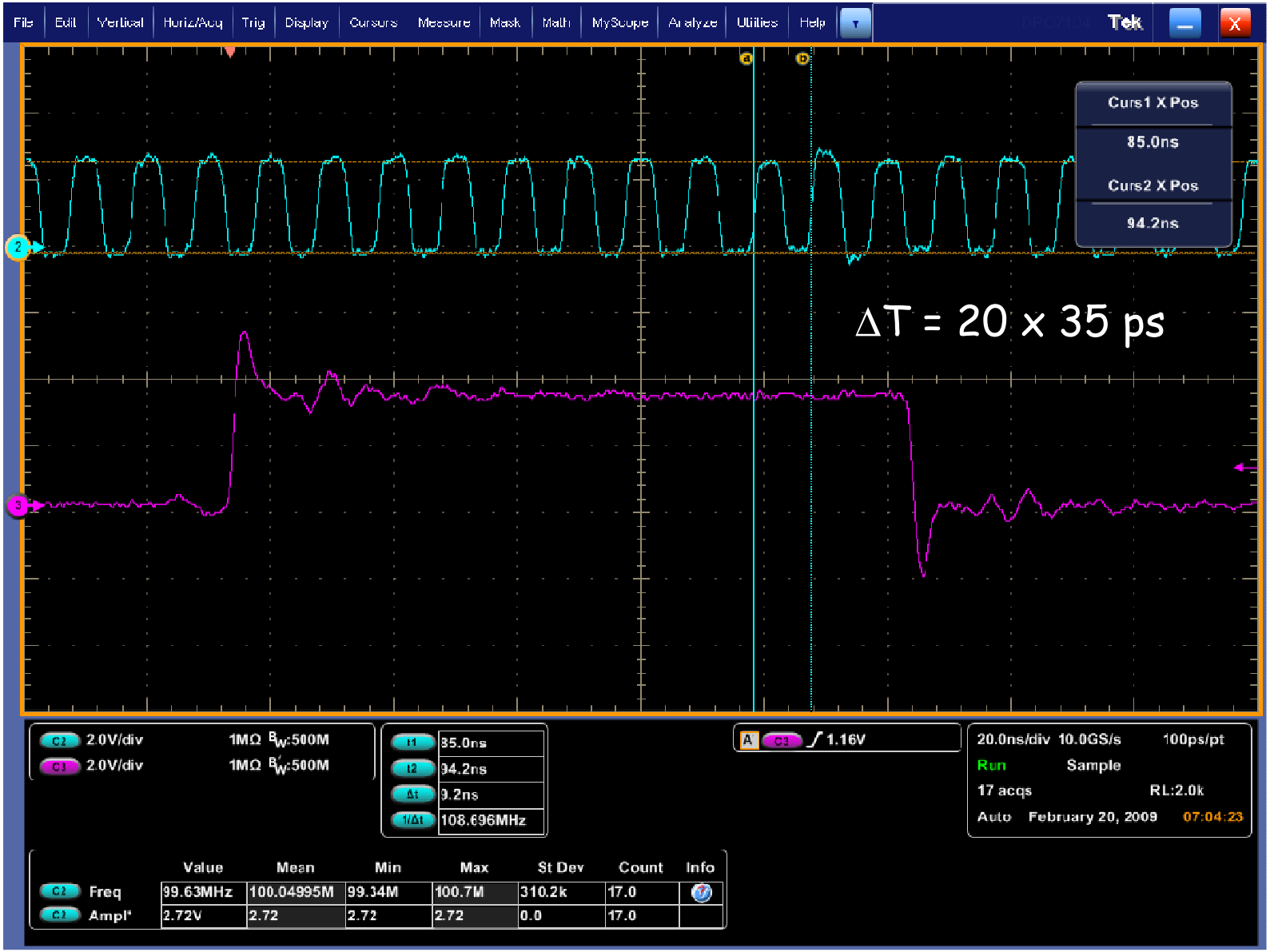
- Dispositif expérimental

maquette génération horloge



maquette AES

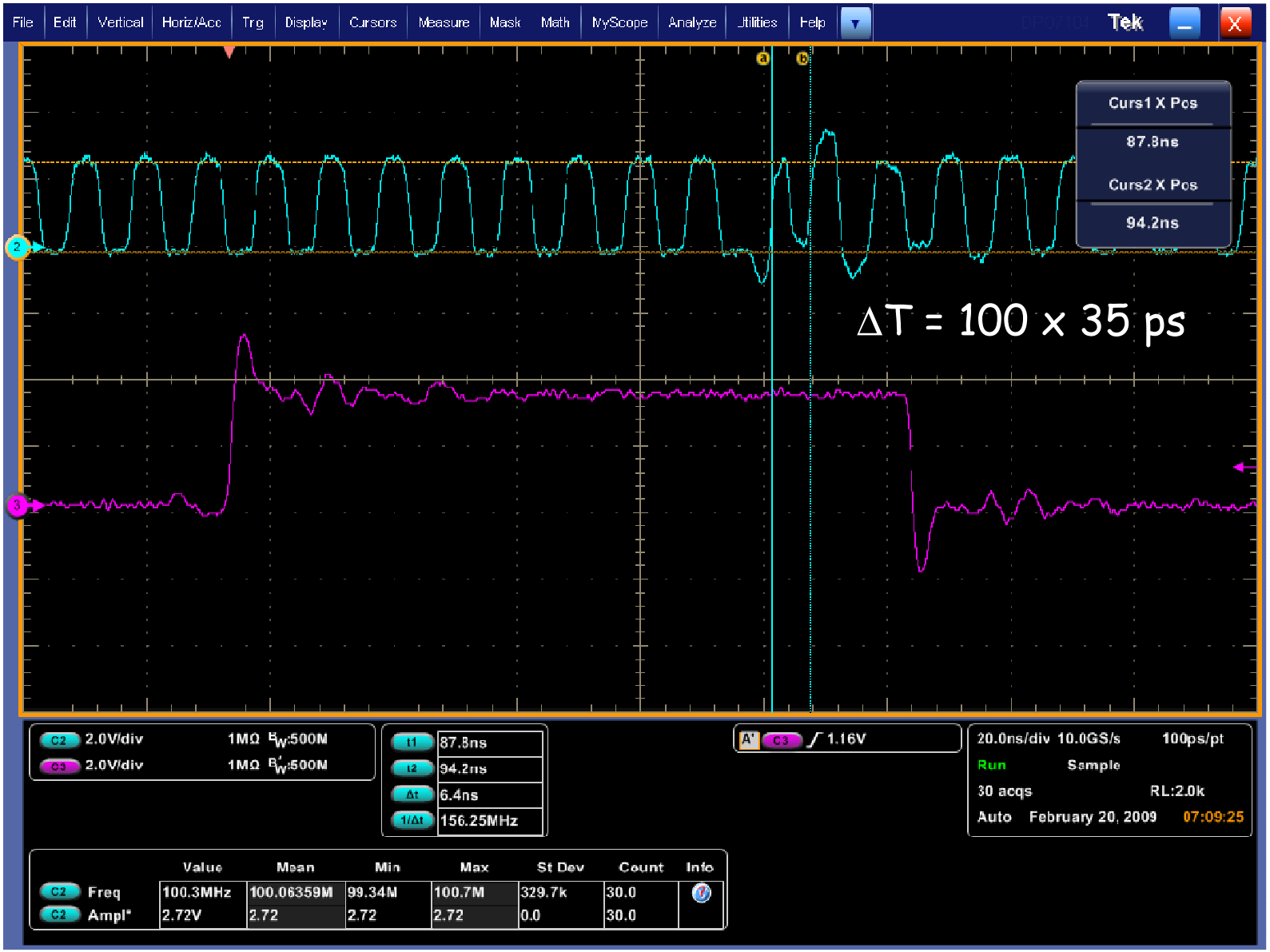

File
Edit
Vertical
Horiz/Acq
Trig
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
84.2ns
Curs2 X Pos
94.2ns
ΔT = 0
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 84.2ns
t2 94.2ns
Δt 10.0ns
1/Δt 100.0MHz
C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
15 acqs RL:2.0k
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

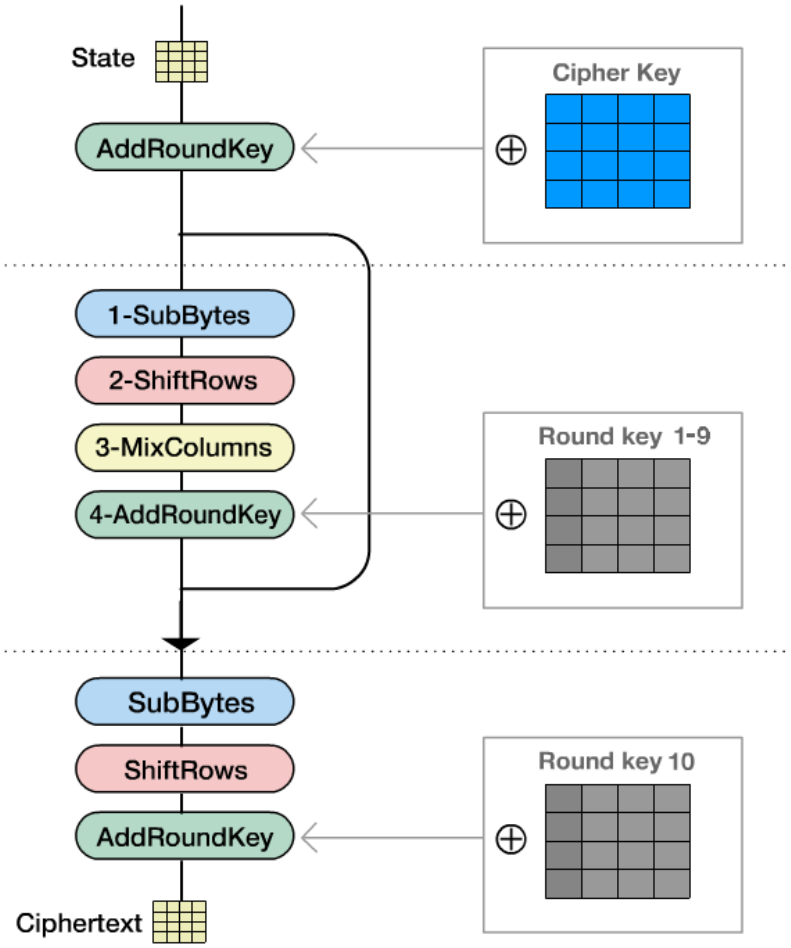

File
Edit
Vertical
Horiz/Acc
Trg
Display
Cursors
Measure
Mask
Math
MyScope
Analyze
Utilities
Help
Tek
Curs1 X Pos
85.5ns
Curs2 X Pos
94.2ns
ΔT = 40 x 35 ps
C2 2.0V/div 1MΩ BW:500M
C3 2.0V/div 1MΩ BW:500M
t1 85.5ns
t2 94.2ns
Δt 8.6ns
1/Δt 116.279MHz
A' C3 1.16V
20.0ns/div 10.0GS/s 100ps/pt
Run Sample
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

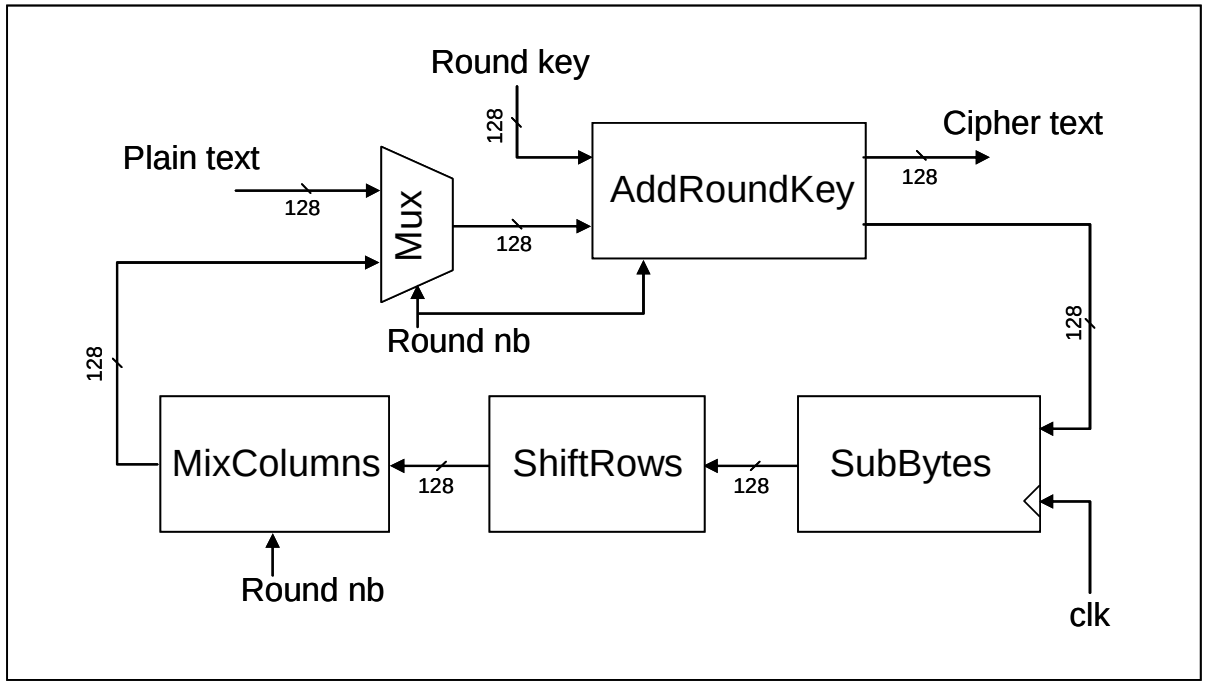
Glitch d'horloge – Capture d'écrans


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

- Cible : AES matériel.



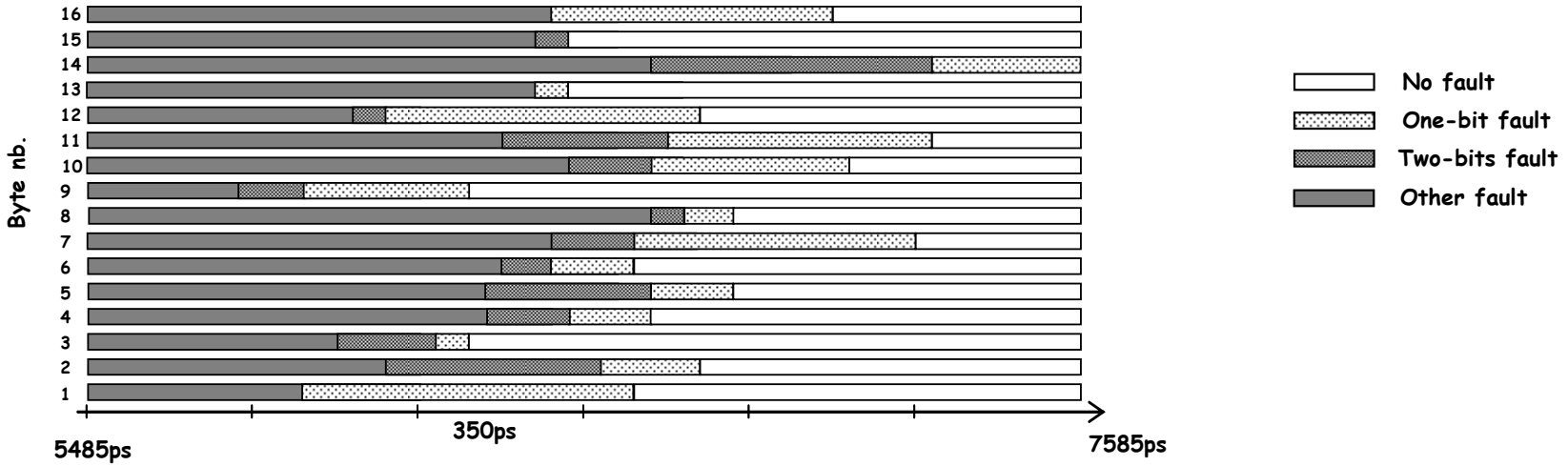
© Enrique Zabala - Universidad ORT/Montevideo/Uruguay



- Registre en entrée du SubBytes
- Architecture en boucle (i.e. chemin critique)

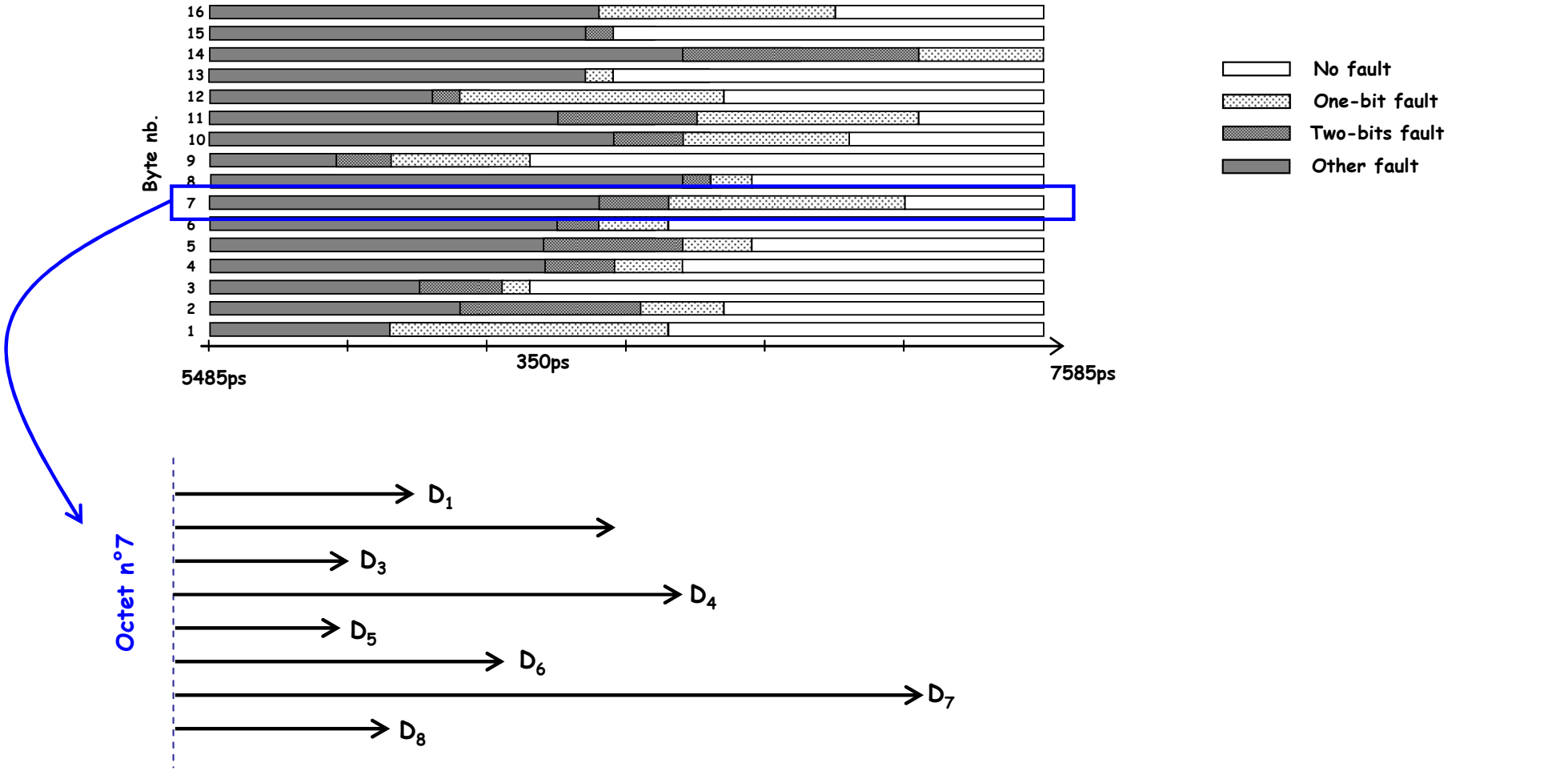
Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

Diminution progressive de T_{clk} (ΔT = 35 ps)



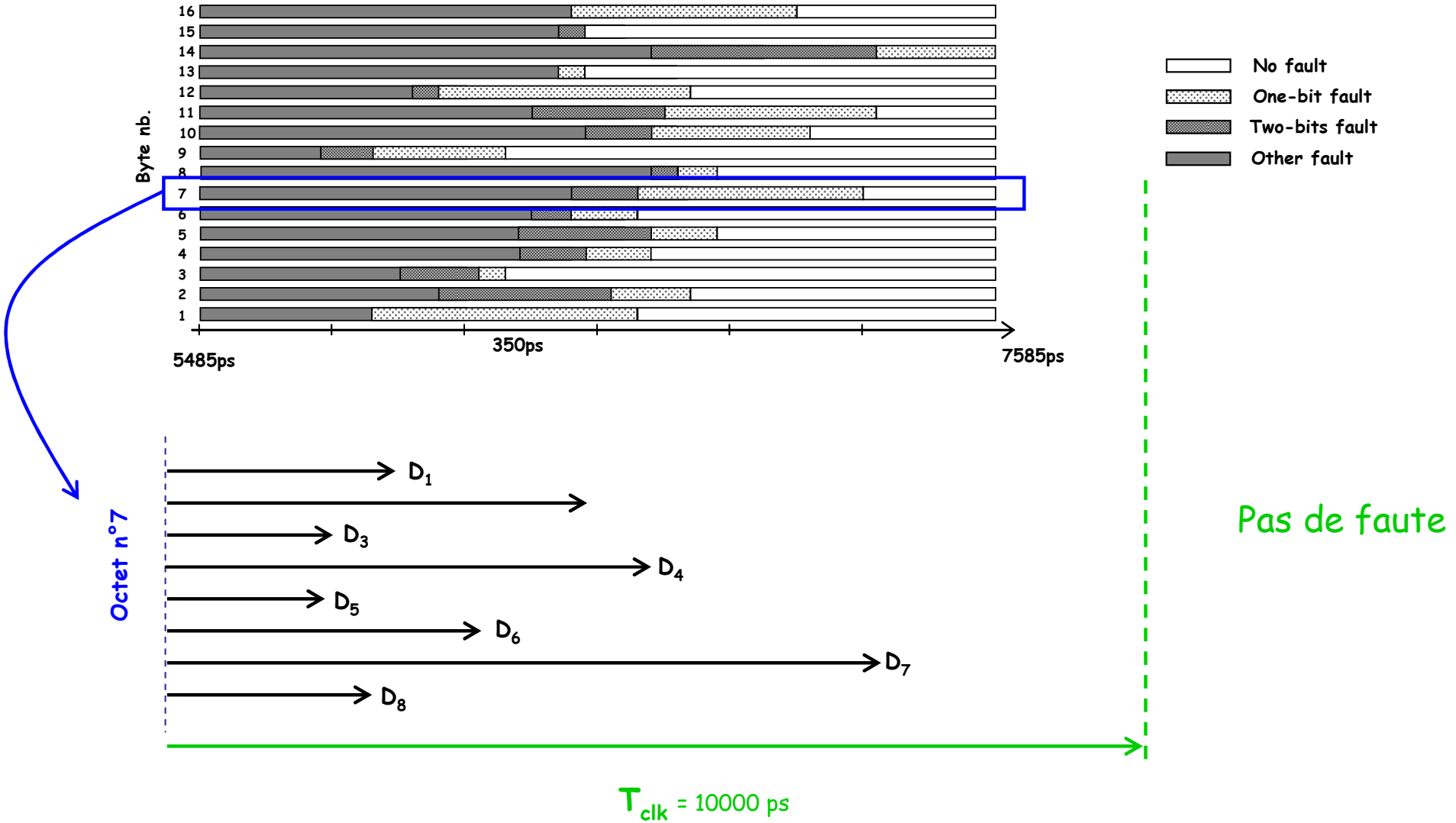
Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

Diminution progressive de T_{clk} (ΔT = 35 ps)



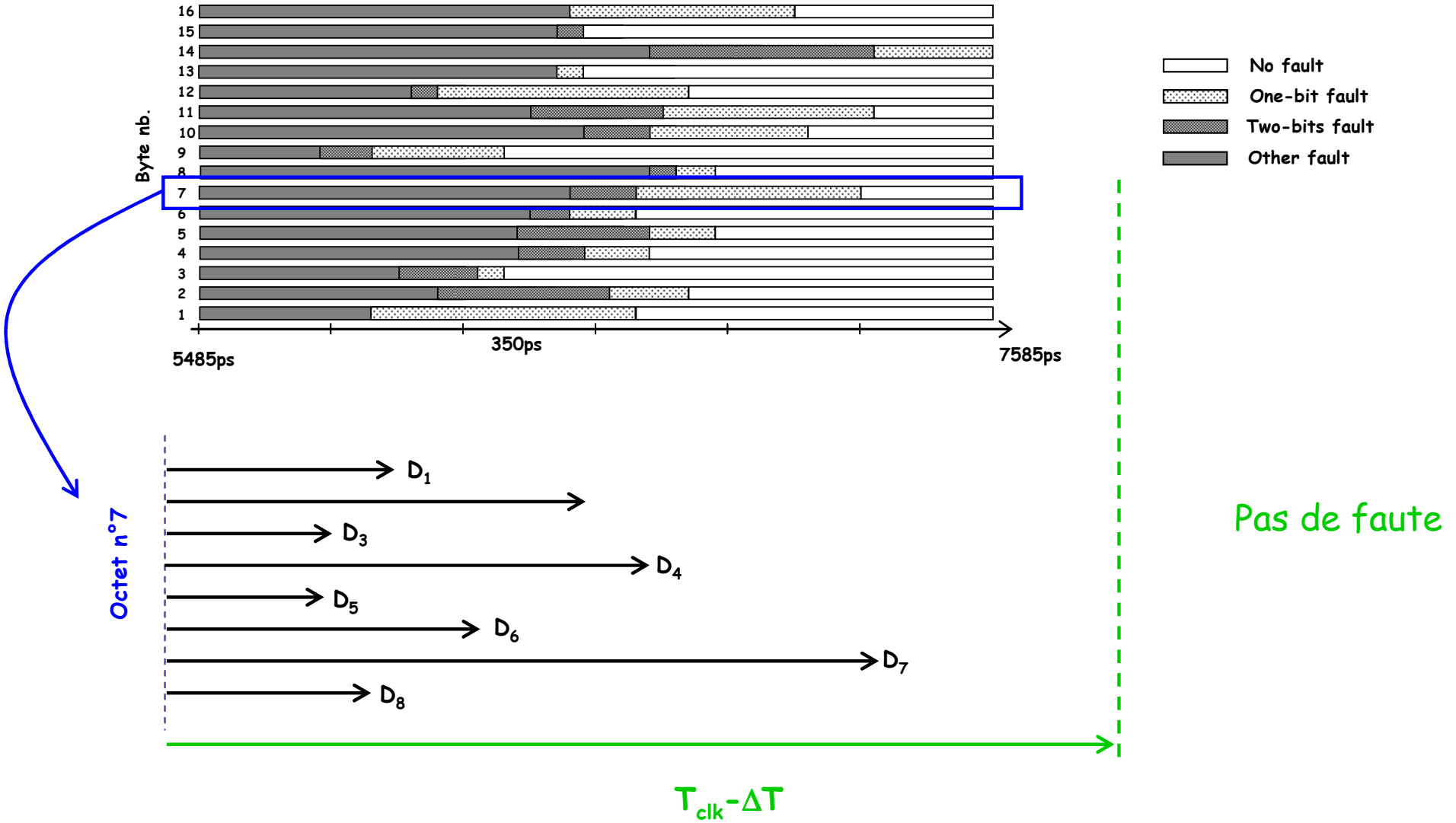
Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

Diminution progressive de T_{clk} (ΔT = 35 ps)



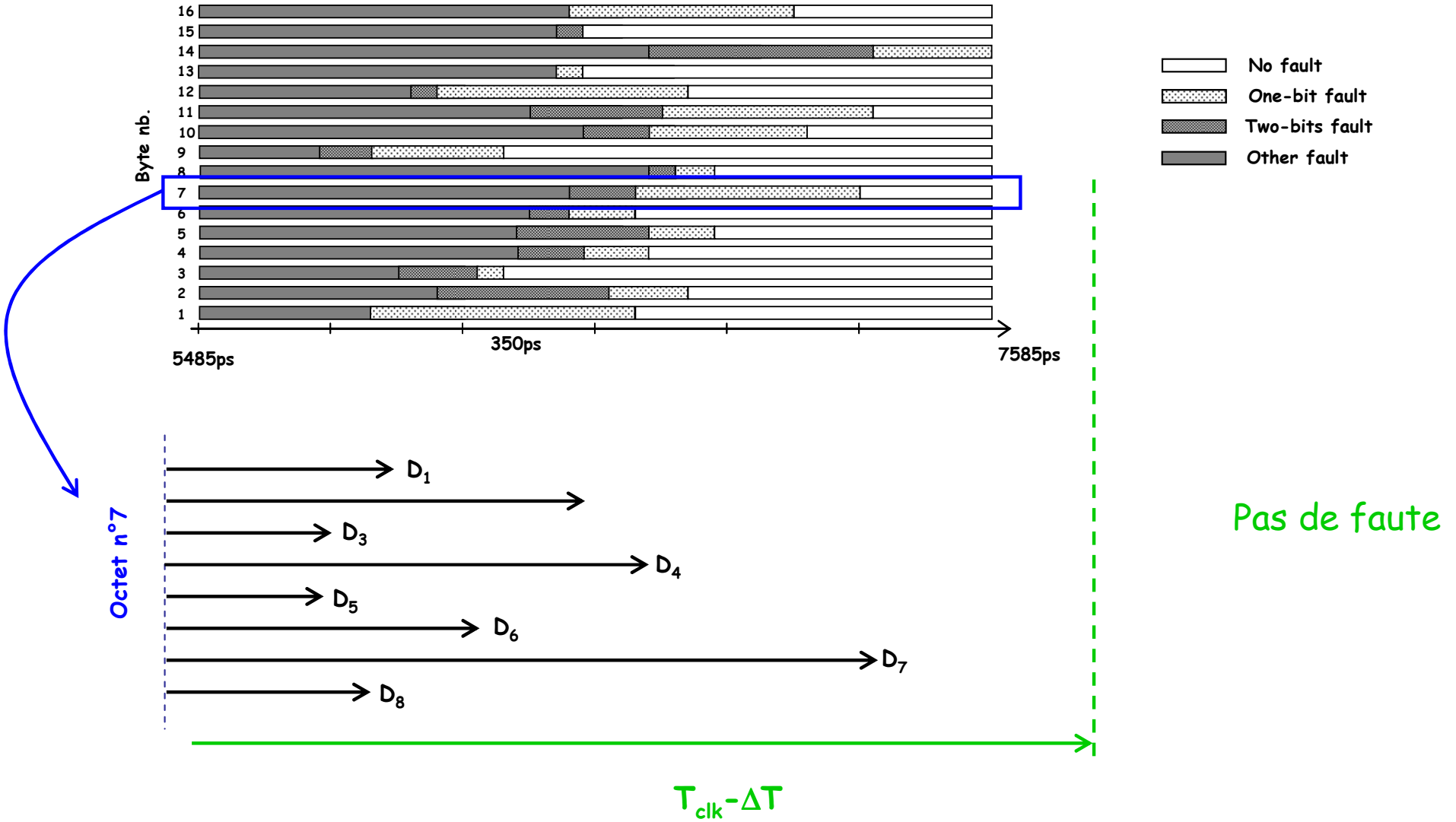
Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

Diminution progressive de T_{clk} (ΔT = 35 ps)



Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

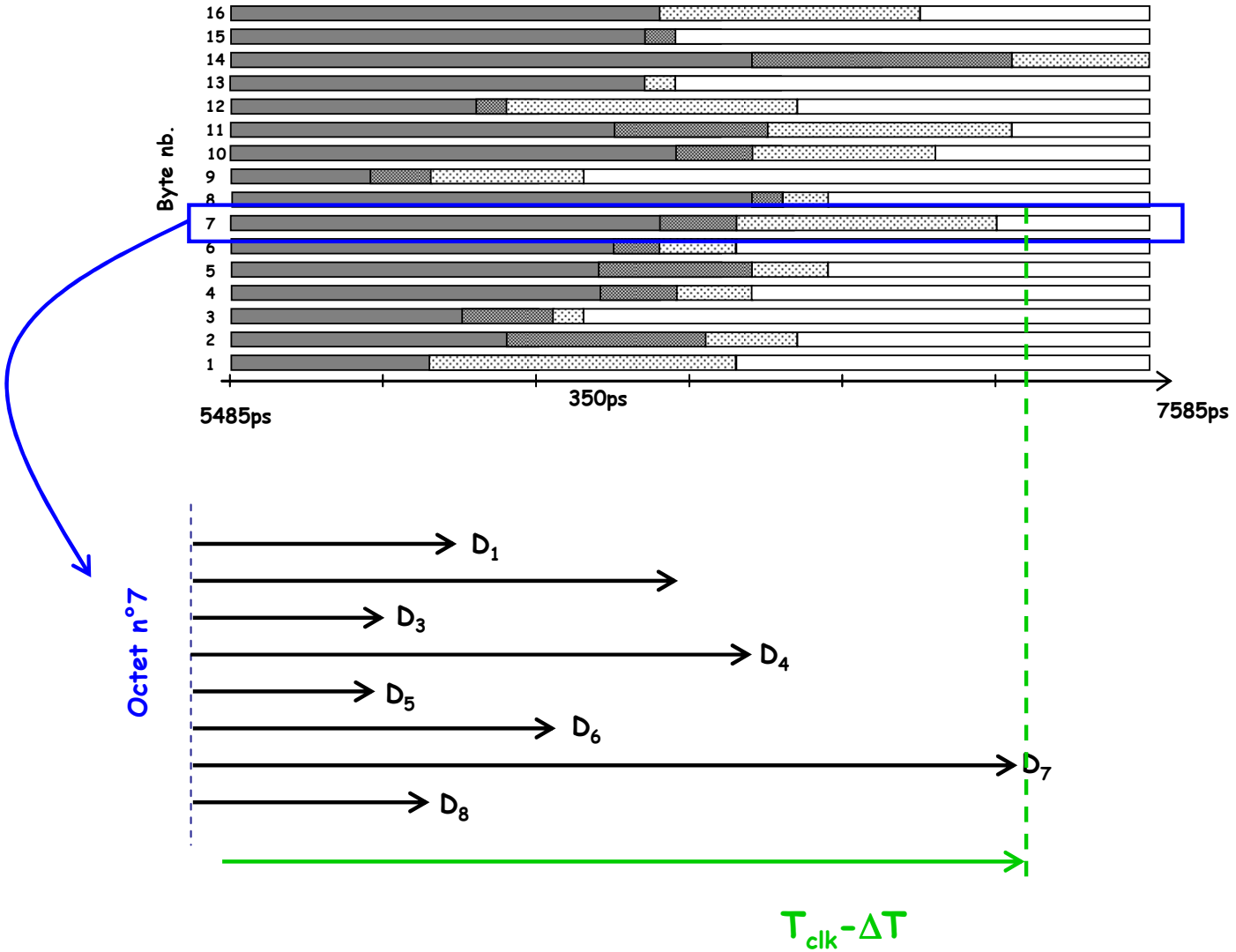
Diminution progressive de T_{clk} (ΔT = 35 ps)



Pas de faute

Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

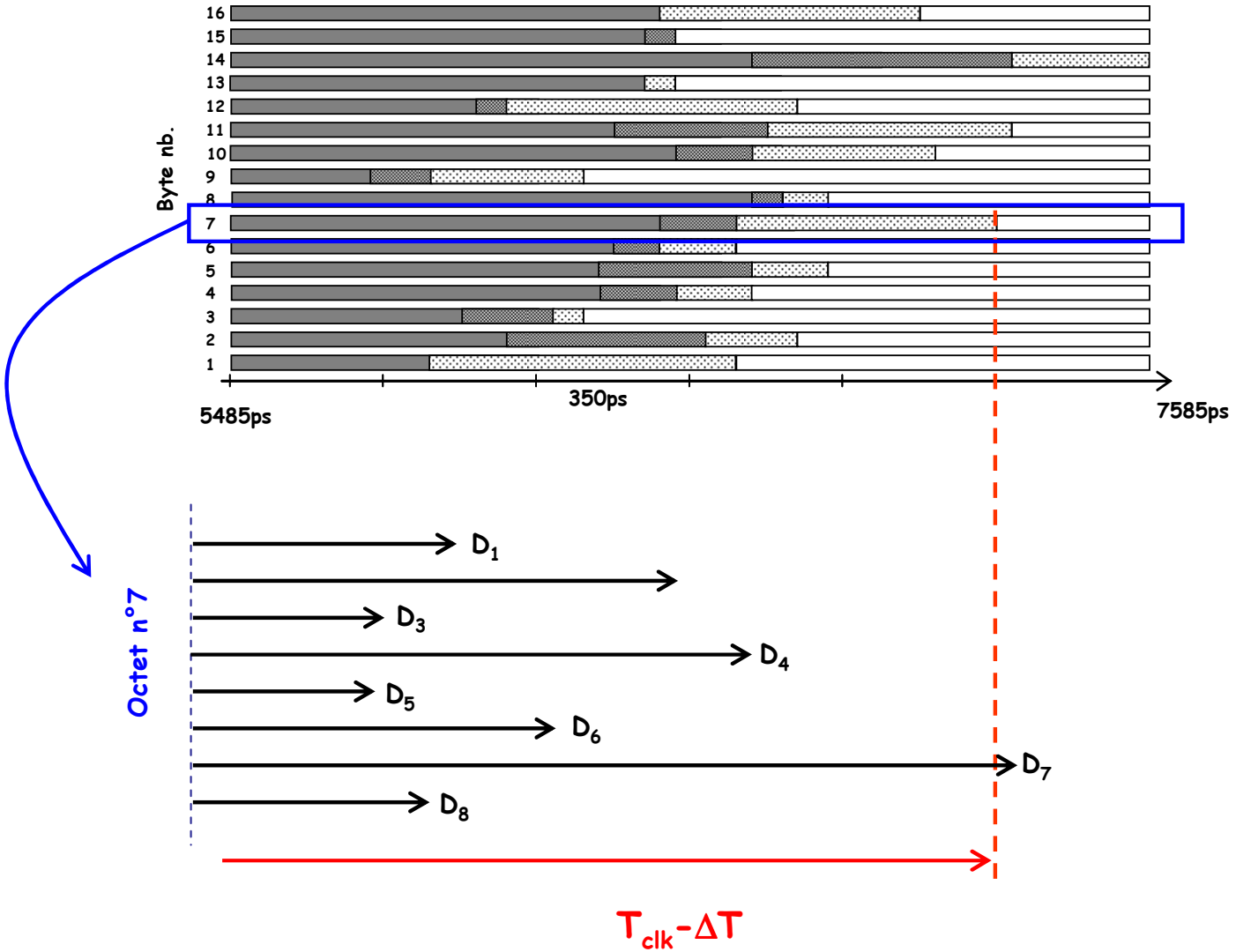
Diminution progressive de T_{clk} (ΔT = 35 ps)



Pas de faute

Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

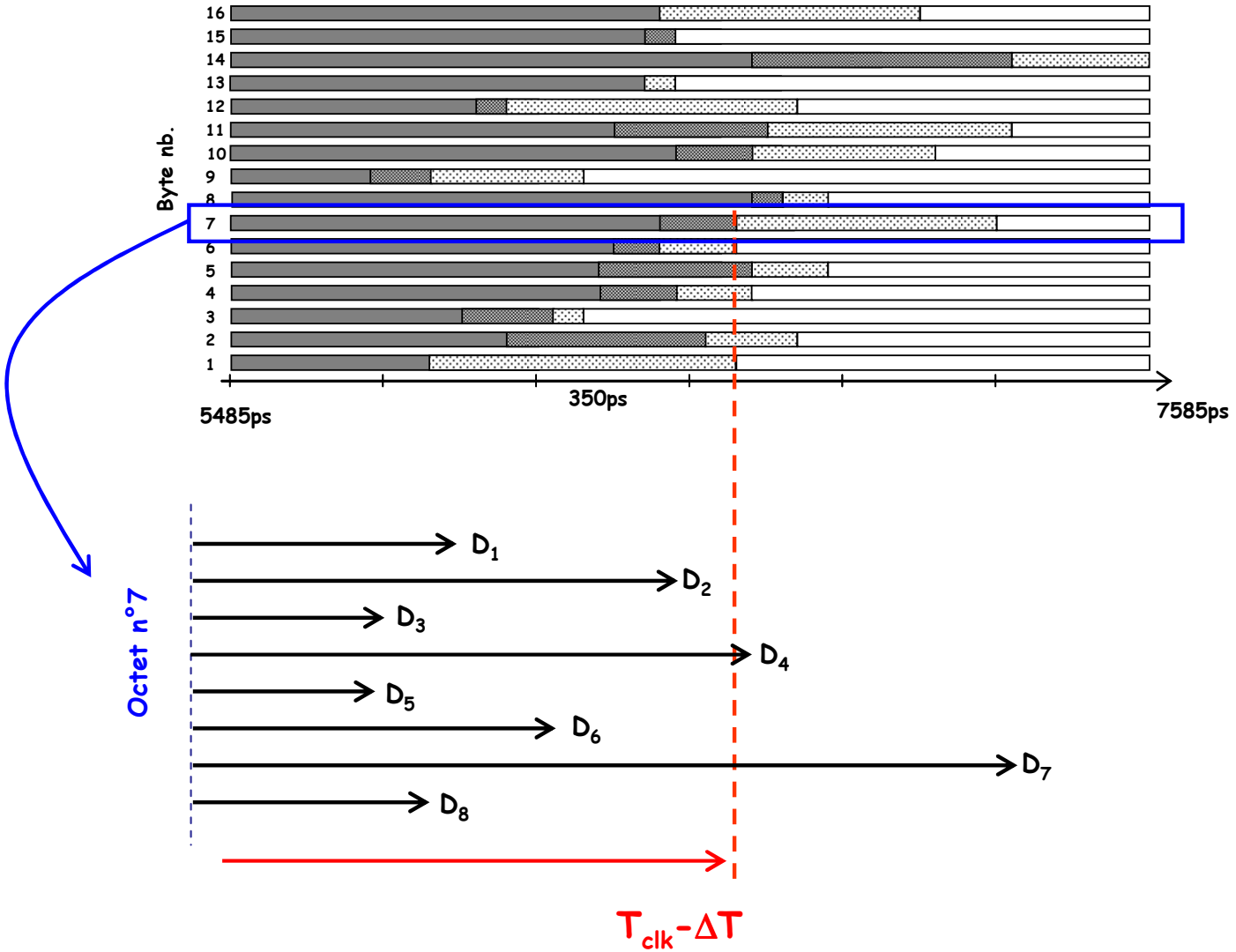
Diminution progressive de T_{clk} (ΔT = 35 ps)



1 bit fauté

Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

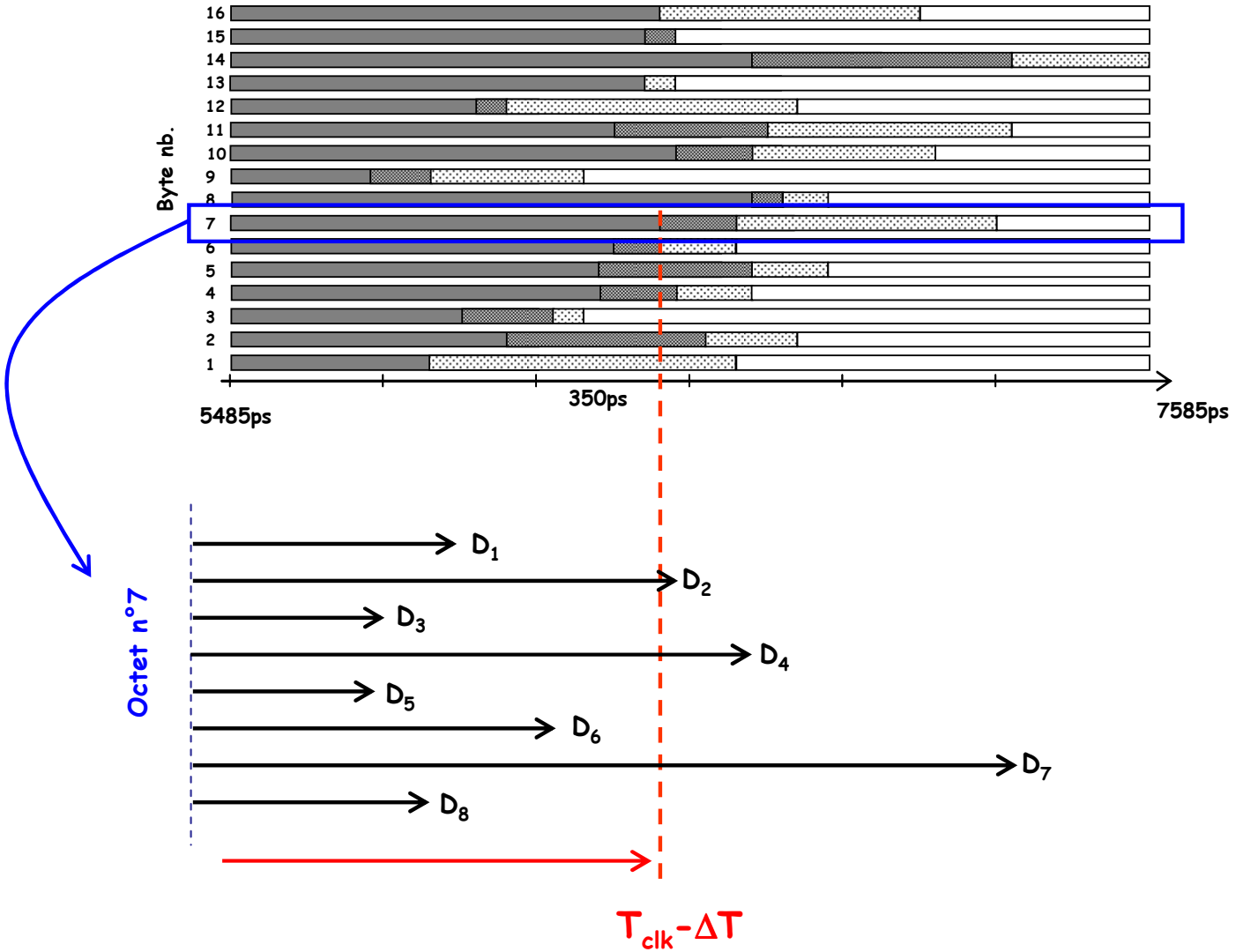
Diminution progressive de T_{clk} (ΔT = 35 ps)



2 bits fautés

Injection en ronde finale ($f_{clk, nom}$ = 100 MHz)

Diminution progressive de T_{clk} (ΔT = 35 ps)



3 bits fautés

- Glitch d'horloge.

Accès CLK requis

Contrôle de la focalisation : excellent

Faute mono-bit	> 90%
Fautes 1 puis 2 bits	> 70%
Fautes 1,2 puis 3 bits	> 50%

Contrôle de l'instant d'injection : total (choix du cycle)

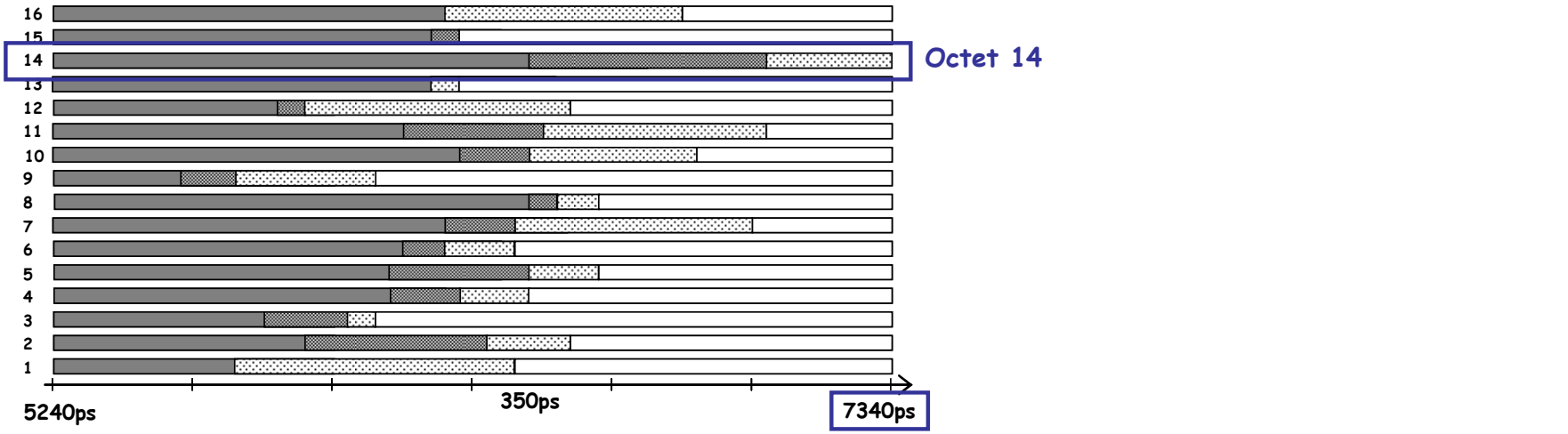
Type de fautes : aléatoire

Facilité d'emploi : aisée (plateforme numérique)

Coût : faible (<1000 €)

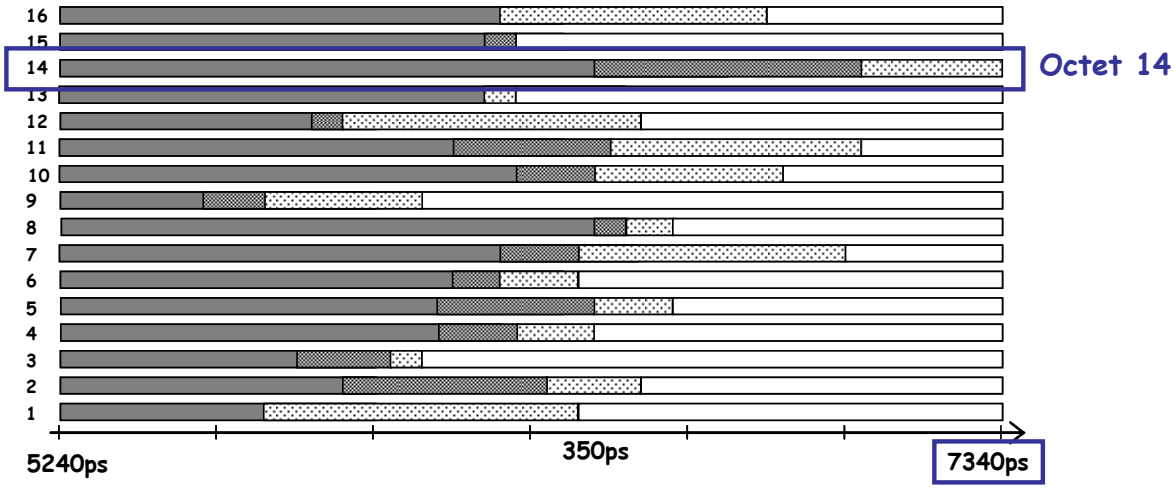
- Glitch d'horloge.

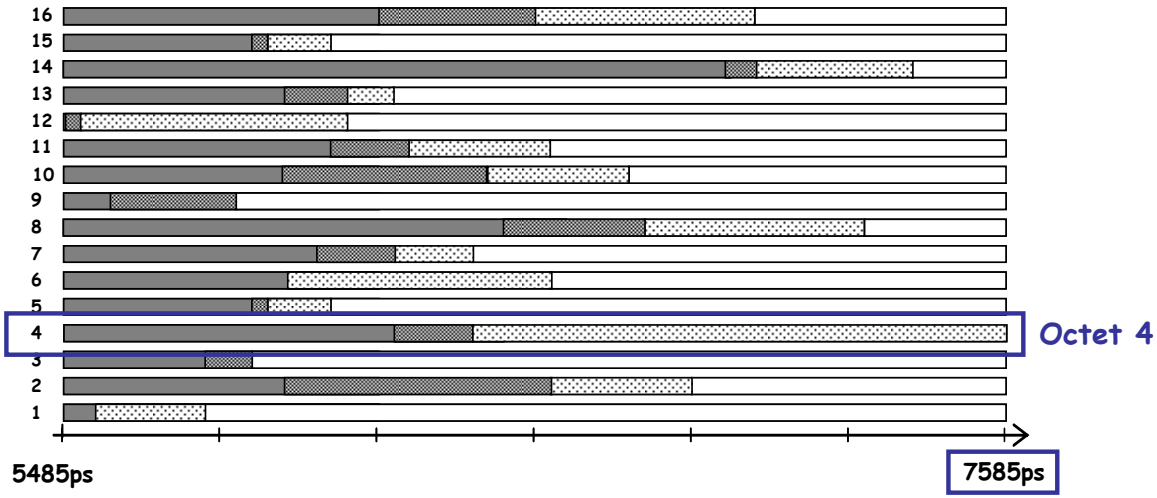
Contrôle de la localisation : par variation du texte clair



- Glitch d'horloge.

Contrôle de la localisation : par variation du texte clair





Même clef

Texte clair différent

- Glitch d'horloge.

Résultats obtenus pour 12000 essais :

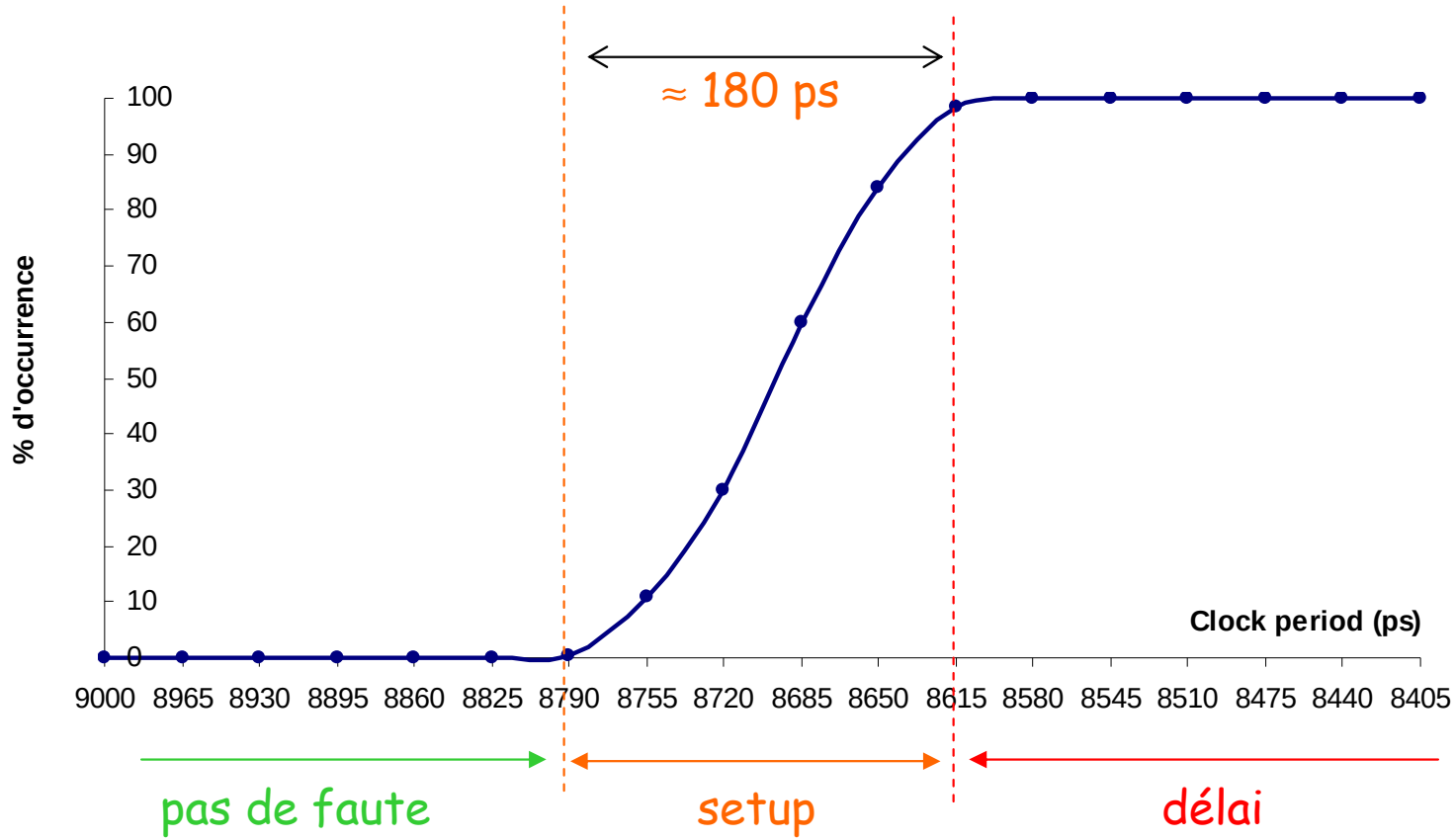
	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
bit0	0	0	77	893	0	0	56	1	6	0	1402	0	438	746	22	0
bit1	0	9	1554	11	17	0	1	176	0	0	13	0	0	1	0	7
bit2	0	216	0	0	0	0	0	107	1	11	2	2	0	10	10	21
bit3	0	0	0	629	2	0	1	0	0	1	0	56	0	0	0	663
bit4	0	32	0	275	33	0	0	3	0	0	0	0	222	147	0	29
bit5	0	0	312	33	23	0	0	1290	22	0	0	2	368	9	0	406
bit6	225	690	0	69	83	5	0	0	0	486	1	0	0	0	5	3
bit7	0	10	0	3	95	0	0	62	12	43	0	0	0	0	0	0
Total	225	957	1943	1913	253	5	58	1639	41	541	1418	60	1028	913	37	1129

< 10
< 100
≥ 100

<u>Contrôle de la localisation</u> : possible (dépendant de l'implémentation)

- Glitch d'horloge.

Reproductibilité : bonne (mais non absolue)



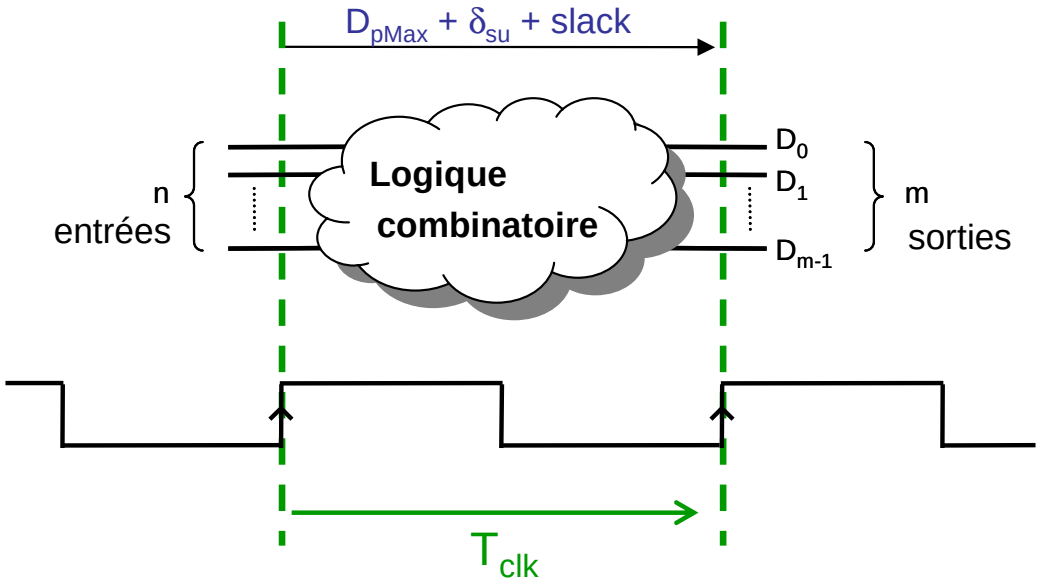
- Injection de faute par diminution de la tension d'alimentation.
  (à fréquence nominale)

Tension d'alimentation ↘

⇨ D_{pMax} ↗ ($D_{clk \rightarrow Q}$, δ_{su}, $|T_{skew}|$ ↗)

$T_{clk} < D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su}$

Injection de fautes à chaque cycle d'horloge



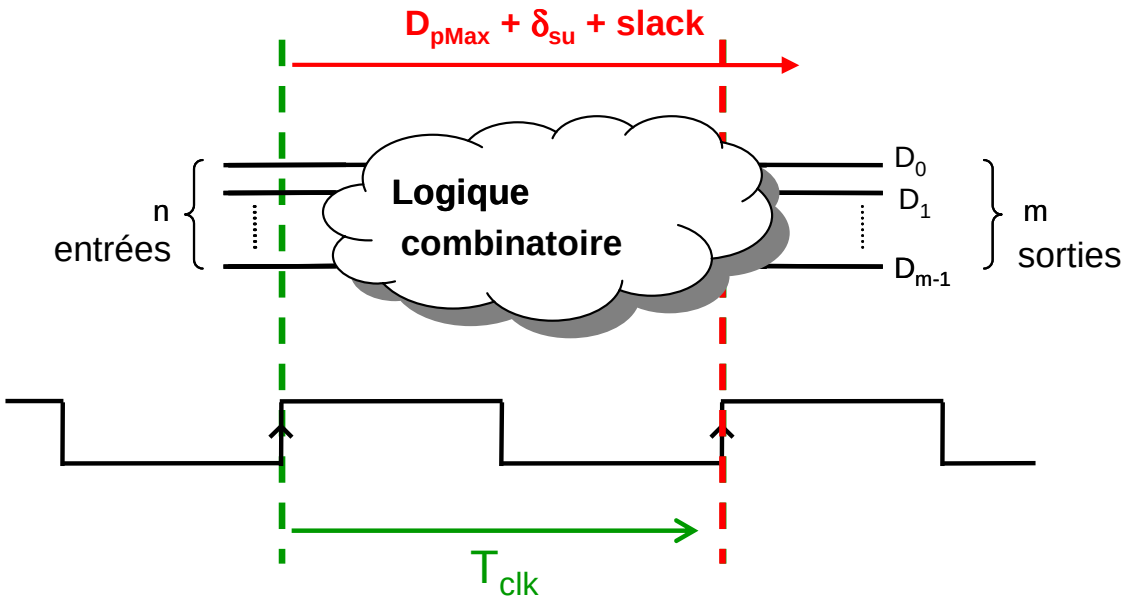
- Injection de faute par diminution de la tension d'alimentation.
  (à fréquence nominale)

Tension d'alimentation ↘

⇨ D_{pMax} ↗ ($D_{clk \rightarrow Q}$, δ_{su}, $|T_{skew}|$ ↗)

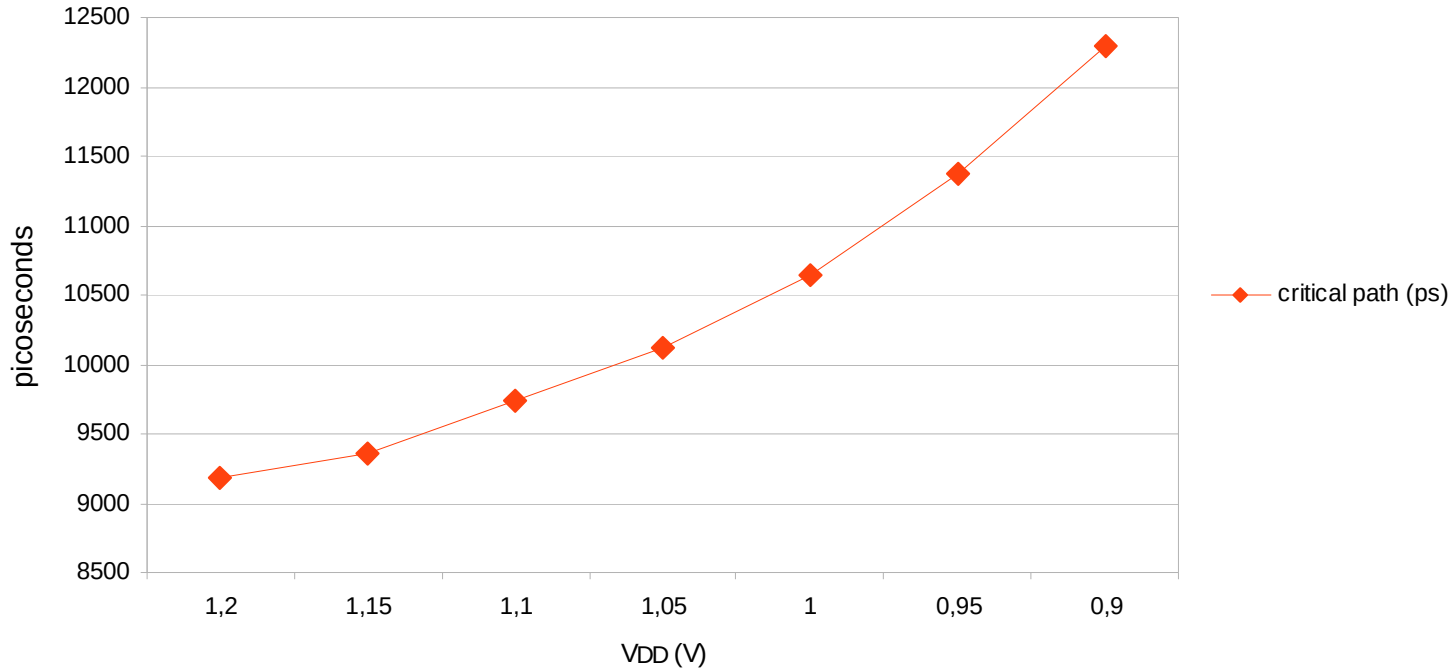
$T_{clk} < D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su}$

Injection de fautes à chaque cycle d'horloge



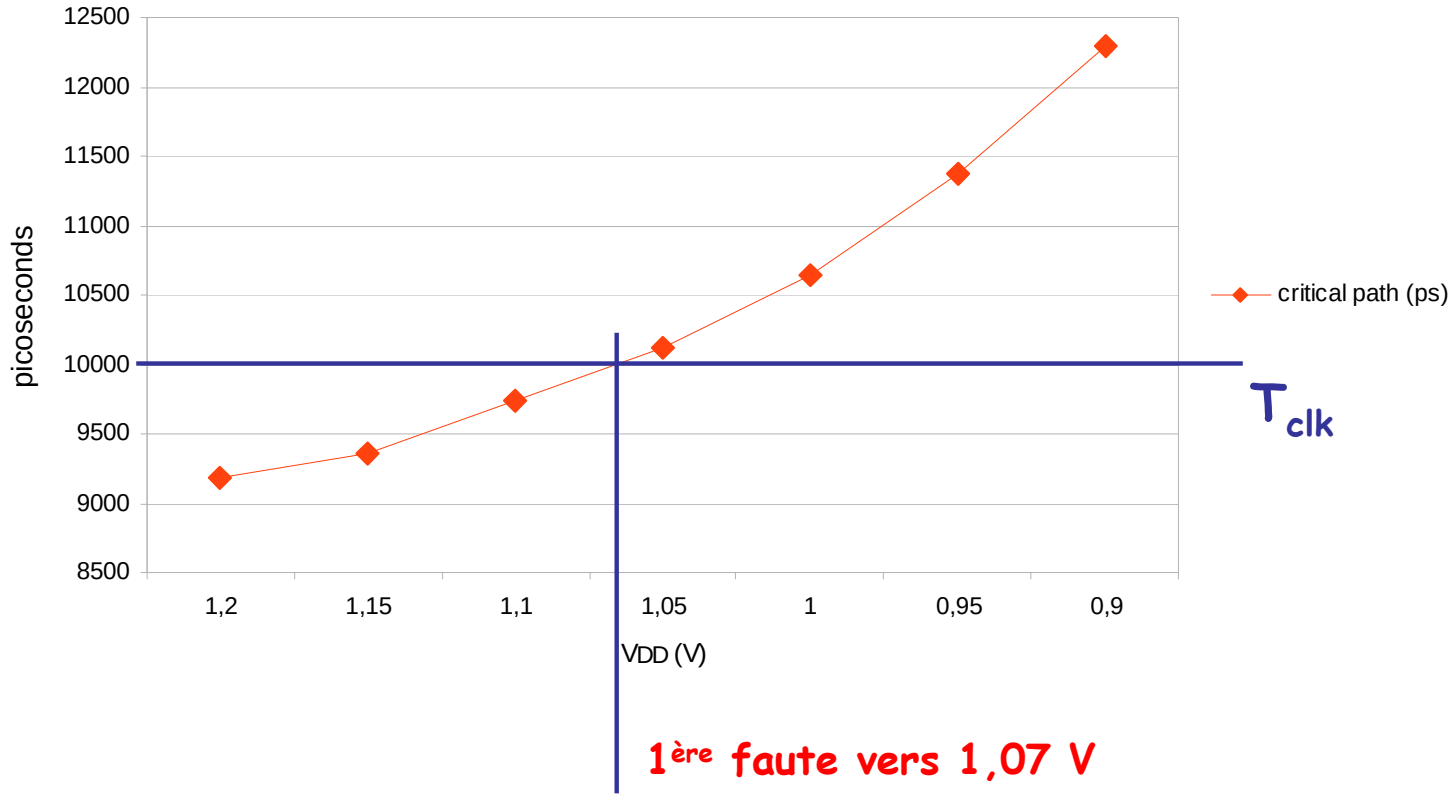
- Injection de faute par diminution de la tension d'alimentation.

Evolution du temps critique avec la tension d'alimentation :

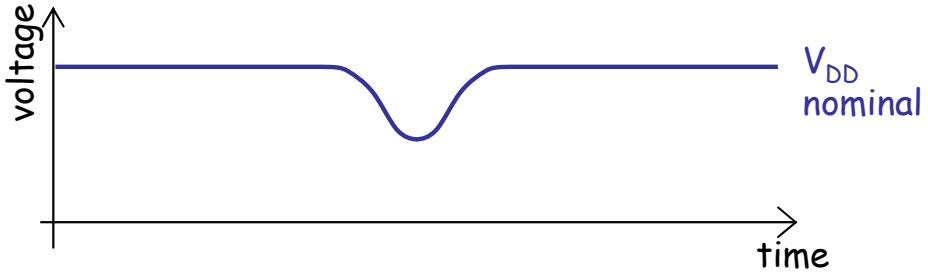


- Injection de faute par diminution de la tension d'alimentation.

Evolution du temps critique avec la tension d'alimentation :

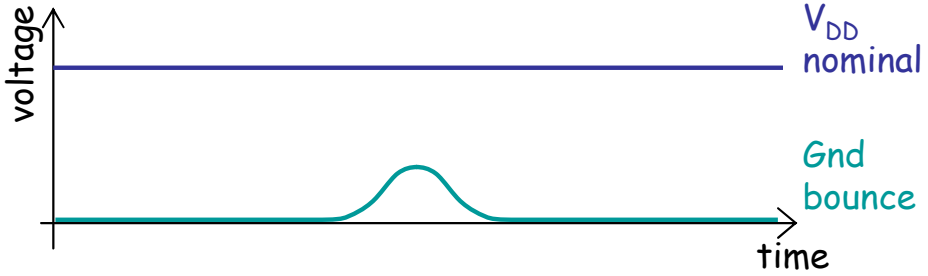


- Glitch d'alimentation (à fréquence nominale)



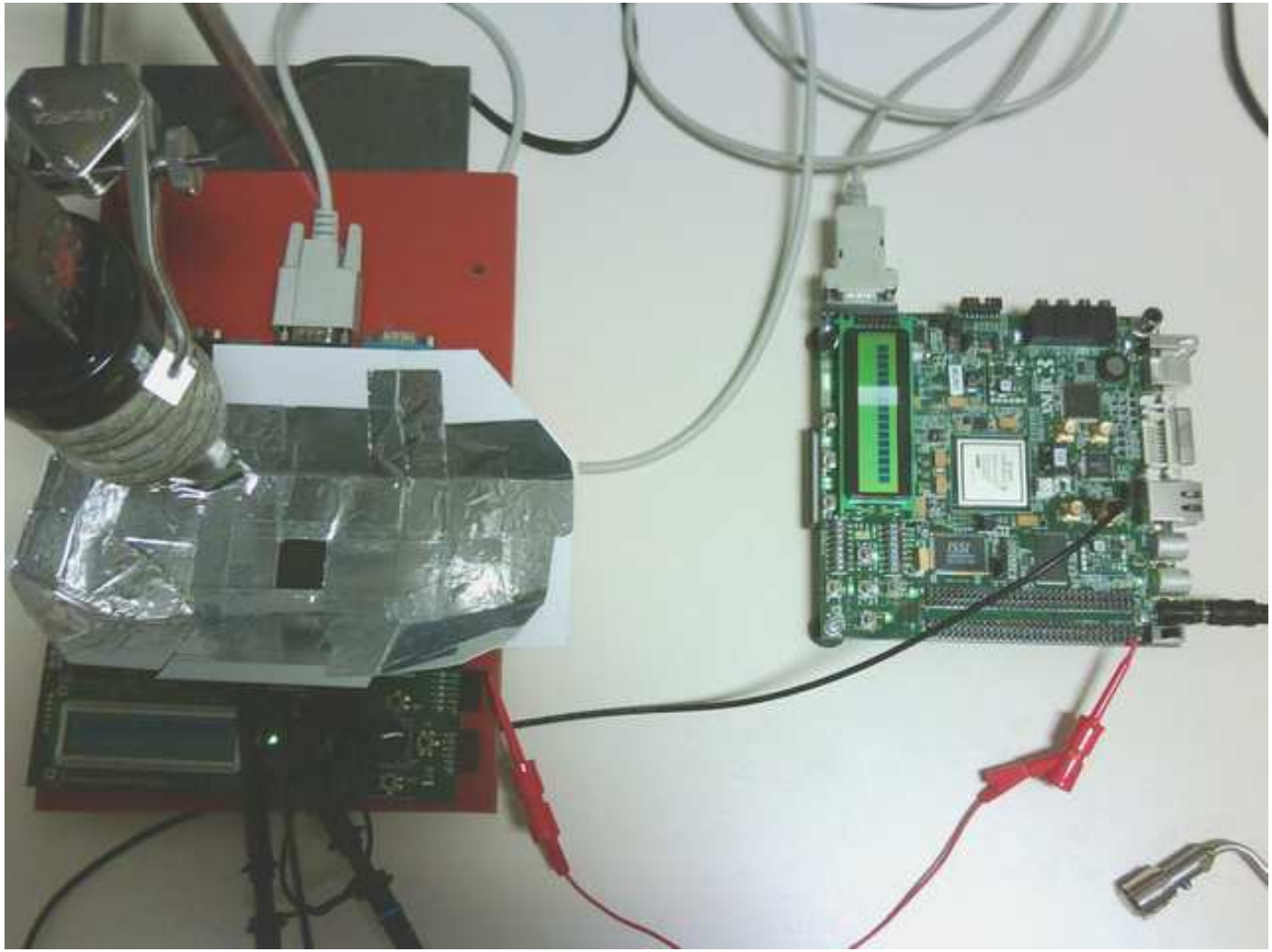
Injection de faute durant le glitch

⇨ choix du cycle d'injection



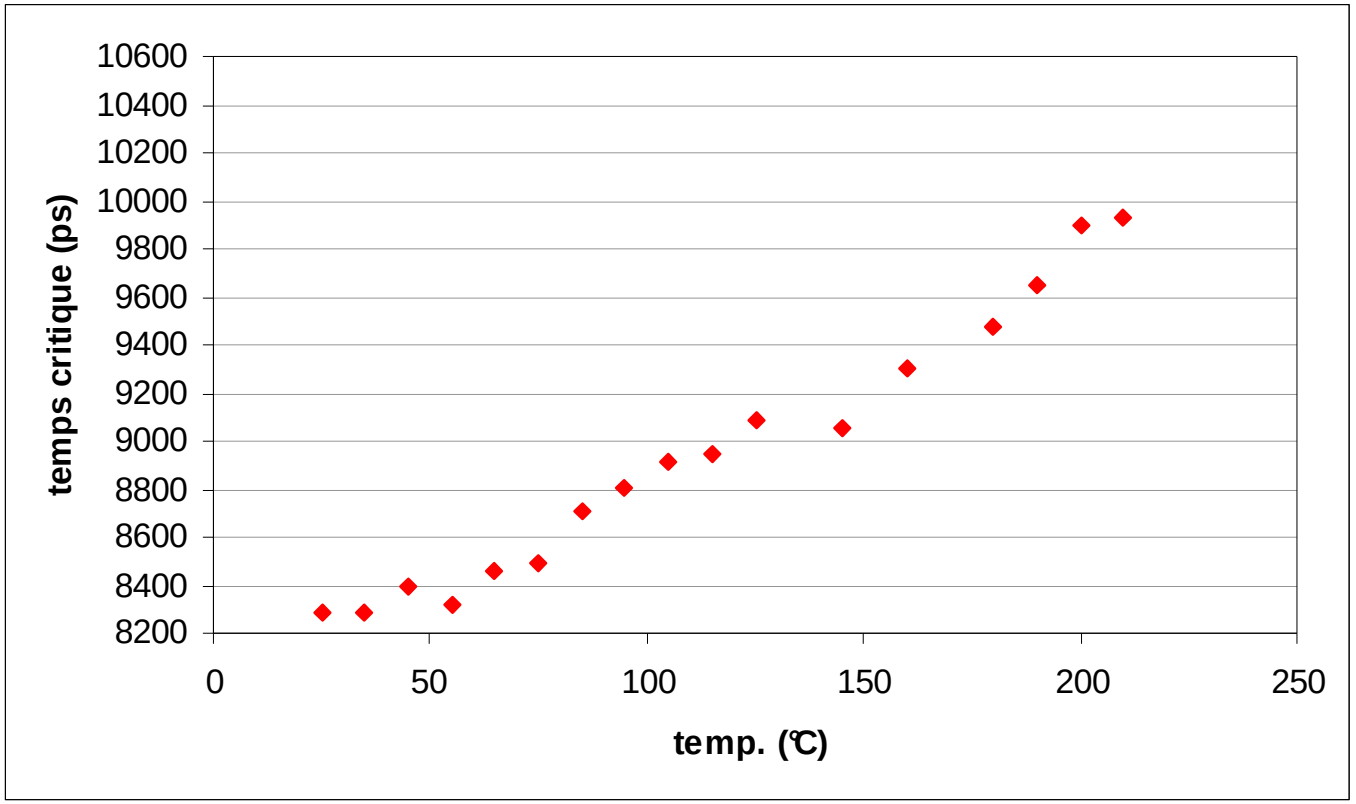
Même mécanisme pour un glitch sur la masse (ground bounce)

- Augmentation de la température (à fréquence nominale)



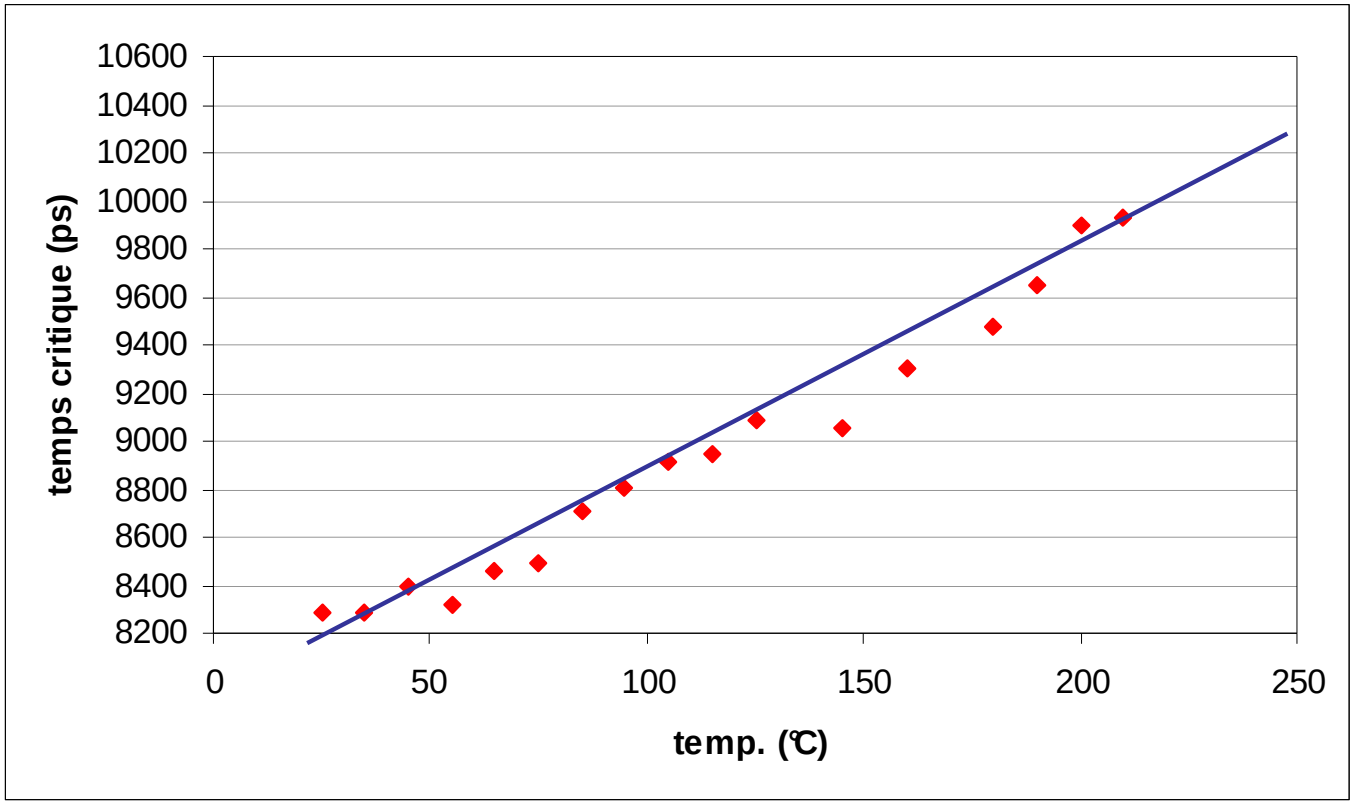
- Augmentation de la température (à fréquence nominale)

$\Rightarrow \quad D_{pMax} \nearrow \qquad (D_{clk \rightarrow Q}, \delta_{su}, |T_{skew}| \nearrow)$



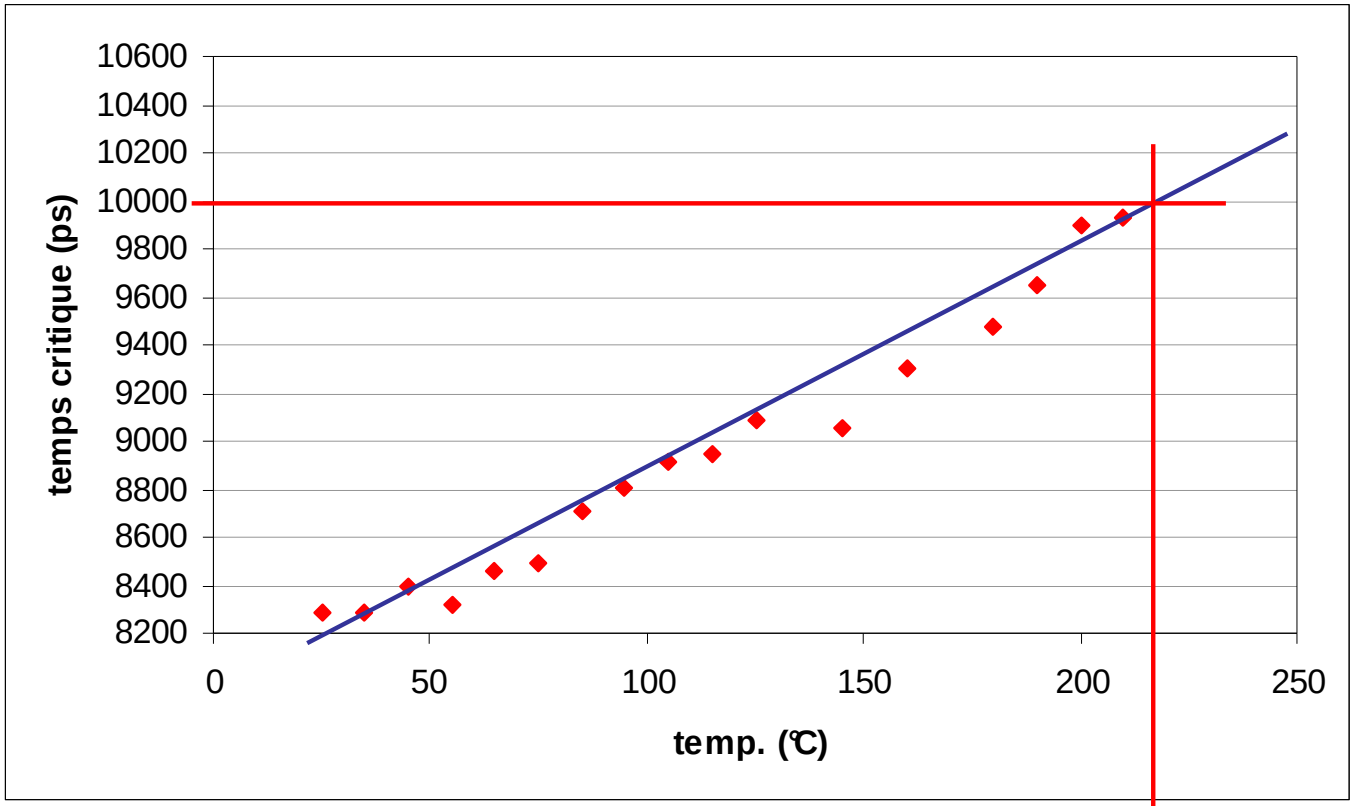
- Augmentation de la température (à fréquence nominale)

$\Rightarrow$ D_{pMax} ↗ ($D_{clk \rightarrow Q}$, δ_{su}, $|T_{skew}|$ ↗)



- Augmentation de la température (à fréquence nominale)

$\Rightarrow \quad D_{pMax} \nearrow \qquad (D_{clk \rightarrow Q}, \delta_{su}, |T_{skew}| \nearrow)$

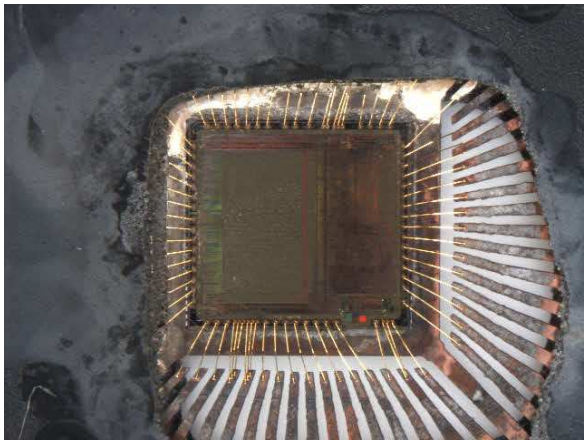


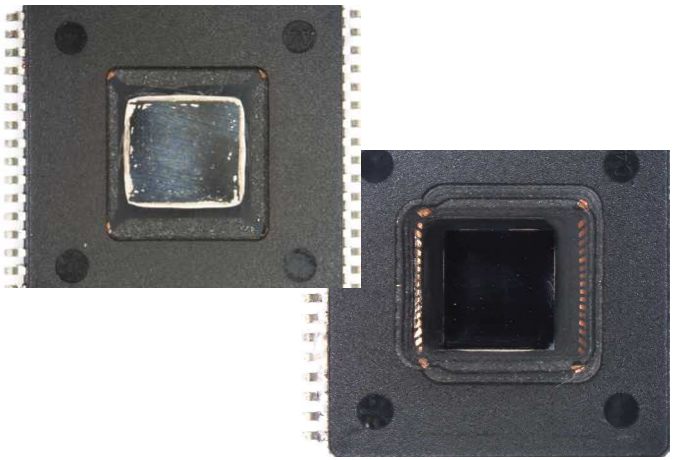
- Injection de faute par violation de temps de setup / délai :
  - Overclocking.
  - Glitch d'horloge.
  - Injection de faute par diminution de la tension d'alimentation.
  - Glitch d'alimentation.
  - Augmentation de la température.

⇨ Mécanisme d'injection similaire.

Validation expérimentale de l'identité des fautes injectées.

- Attaques semi-invasives : ouverture chimique/mécanique du boîtier.

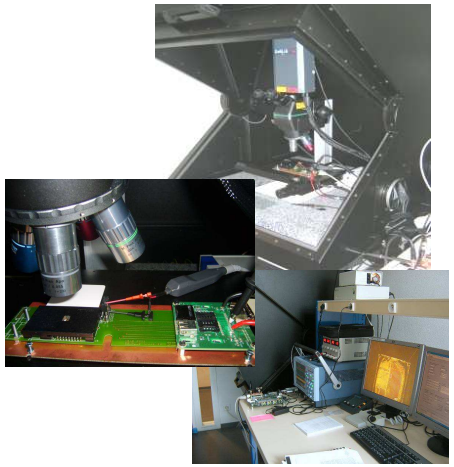


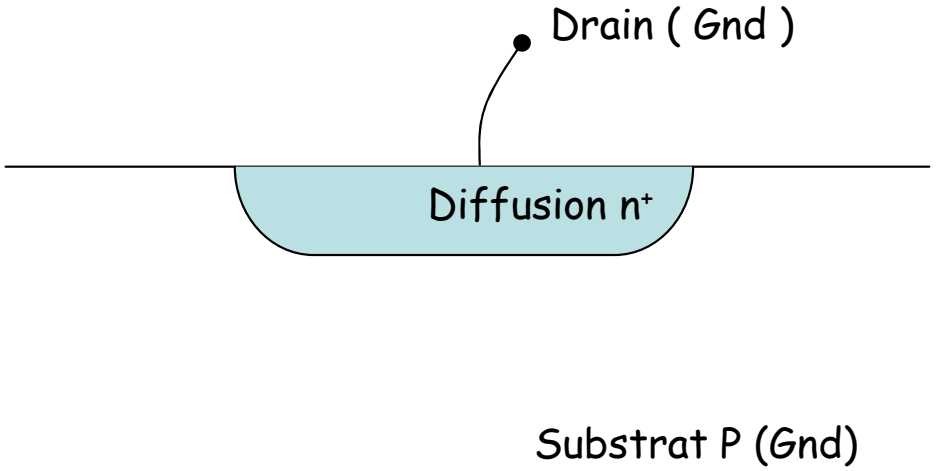


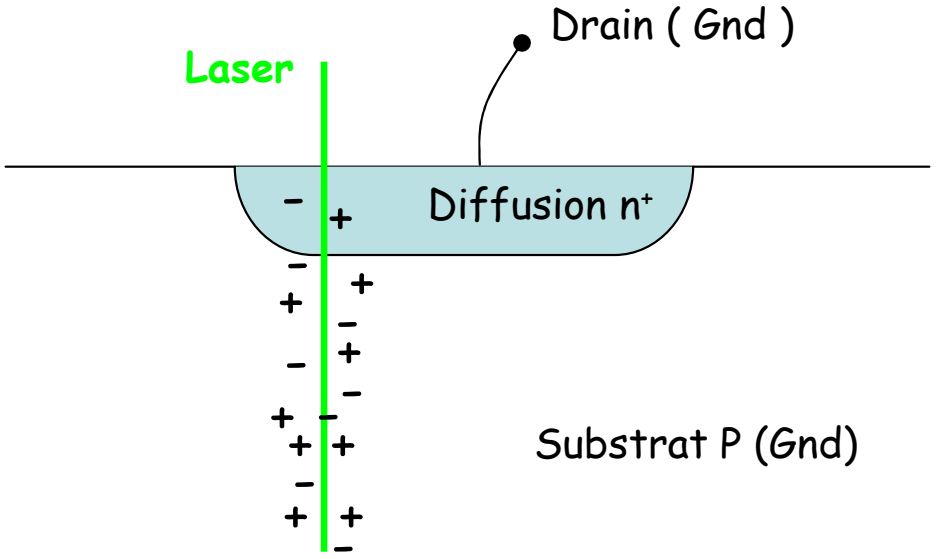
Techniques d'injection optique [Sko02] :

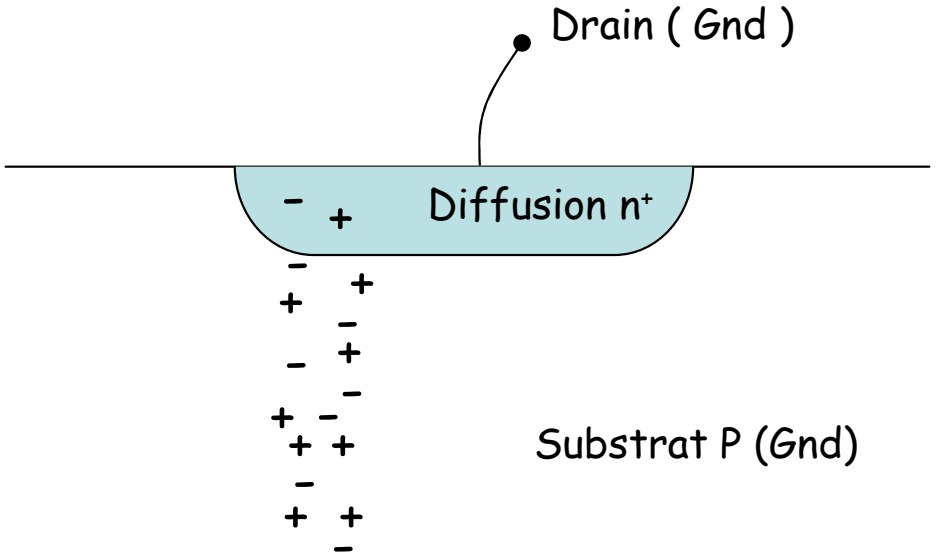
- flash,
- Laser.

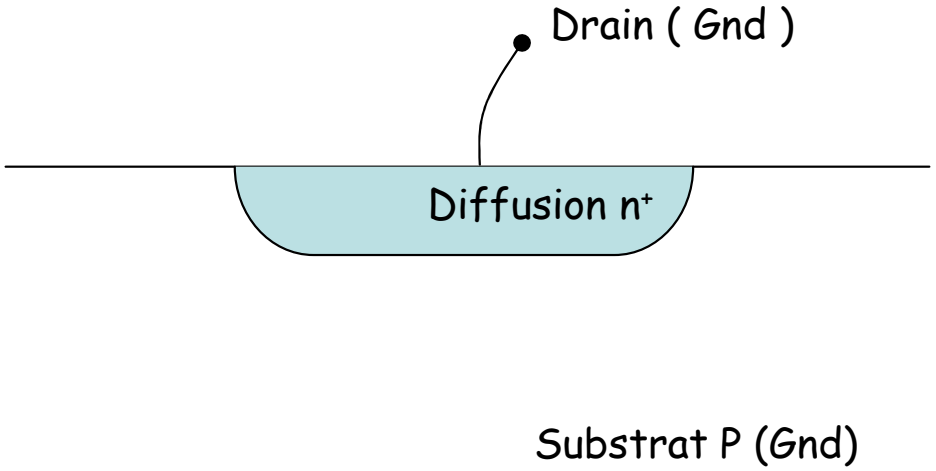
[Sko02]

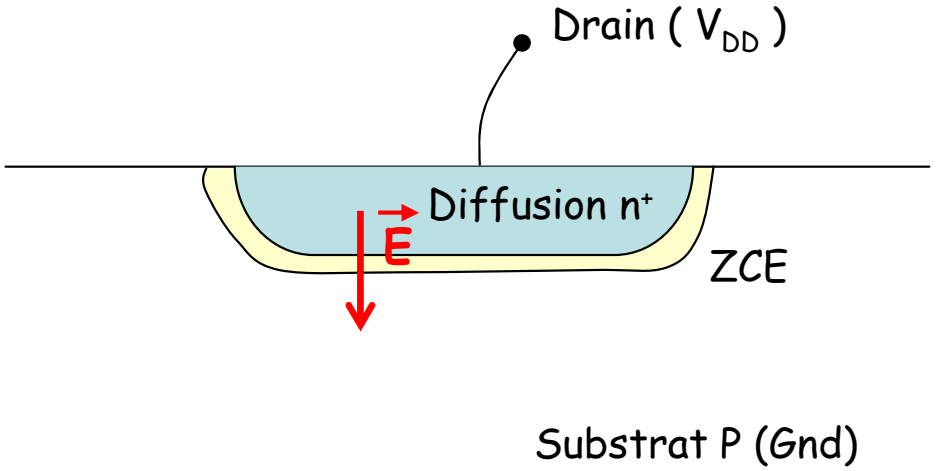


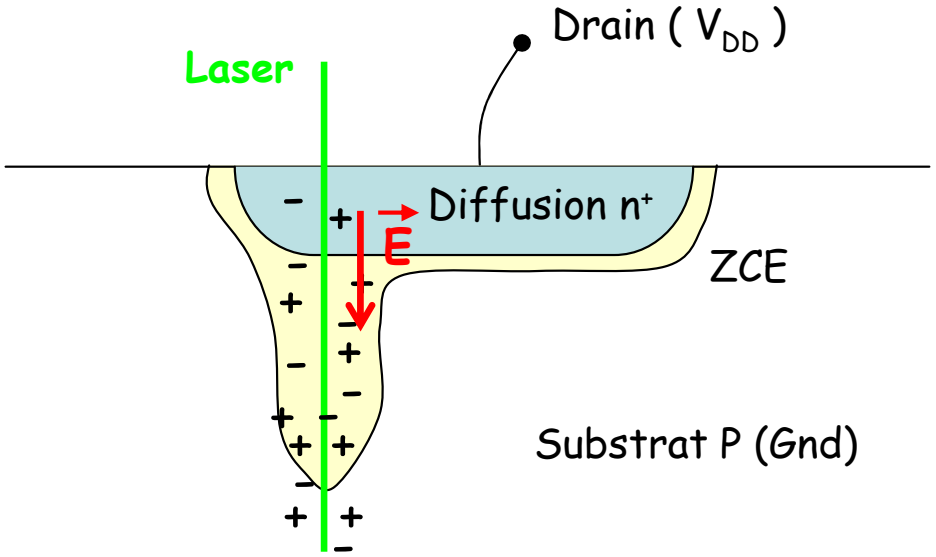

Drain (Gnd)
Diffusion n+
Substrat P (Gnd)

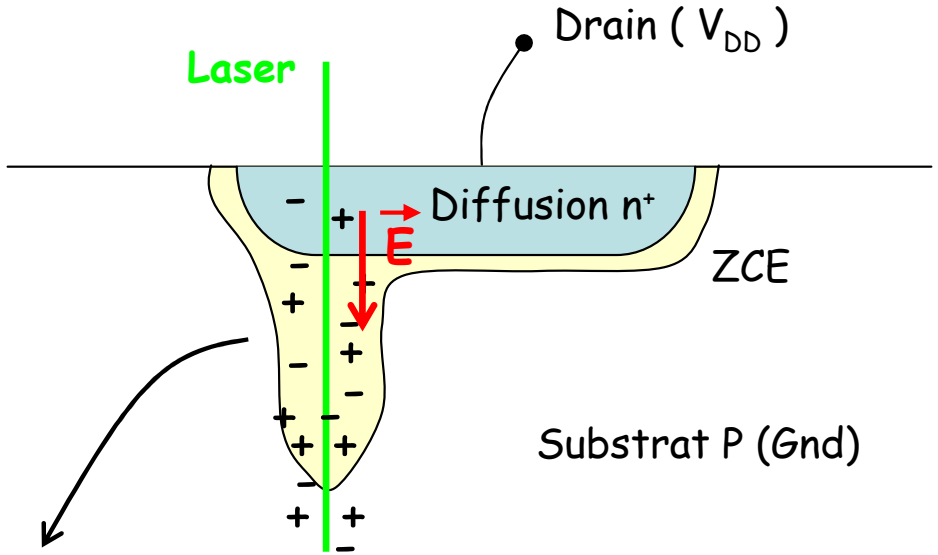

Drain (Gnd)
Laser
Diffusion n+
Substrat P (Gnd)

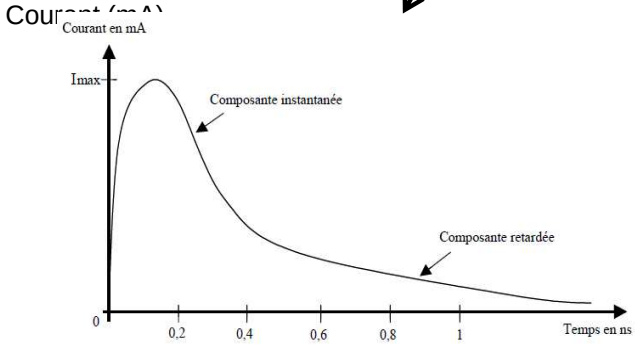

Drain (Gnd)
Diffusion n+
Substrat P (Gnd)

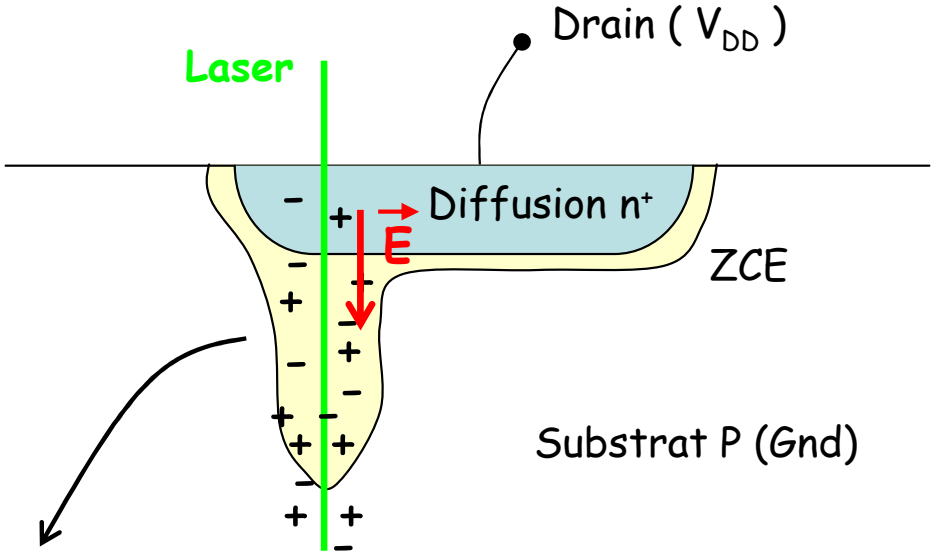

Drain (Gnd)
Diffusion n+
Substrat P (Gnd)

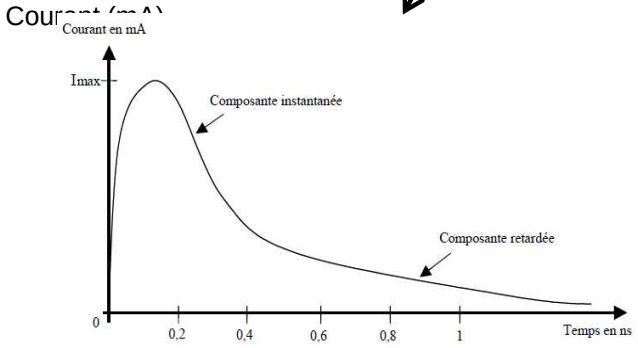

Drain (V_{DD})
Diffusion n+
E
ZCE
Substrat P (Gnd)


Drain (V_{DD})
Laser
Diffusion n+
E
ZCE
Substrat P (Gnd)


Drain (V_{DD})
Laser
Diffusion n+
E
ZCE
Substrat P (Gnd)


Courant en mA
Imax
Composante instantanée
Composante retardée
0
0,2
0,4
0,6
0,8
1
Temps en ns





Transitoire de courant

- énergie du faisceau
- durée

⇨ transitoire de tension

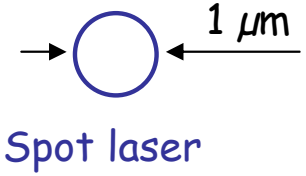
Attention à l'amorçage d'une structure thyristor parasite potentiellement destructif (Latchup)

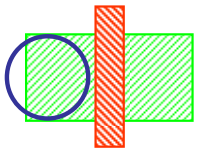
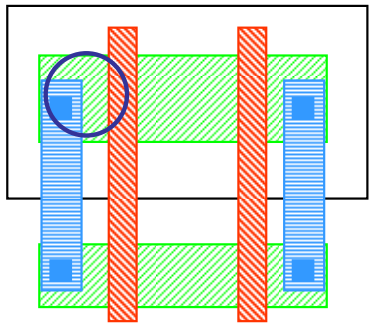
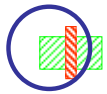
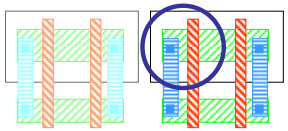
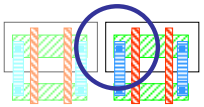
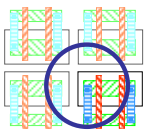
- Effet du transitoire de tension :
  - propagation dans la logique sans mémorisation,
  - propagation dans la logique avec mémorisation,
  - inversion de l'état d'un point mémoire (registre, SRAM).

  ⇨ injection de faute

- Paramètres de réglage d'un laser :
  - longueur d'onde,
  - énergie,
  - taille du faisceau, (état de l'art 1 µm min.)
  - durée de l'impulsion,
  - gigue.

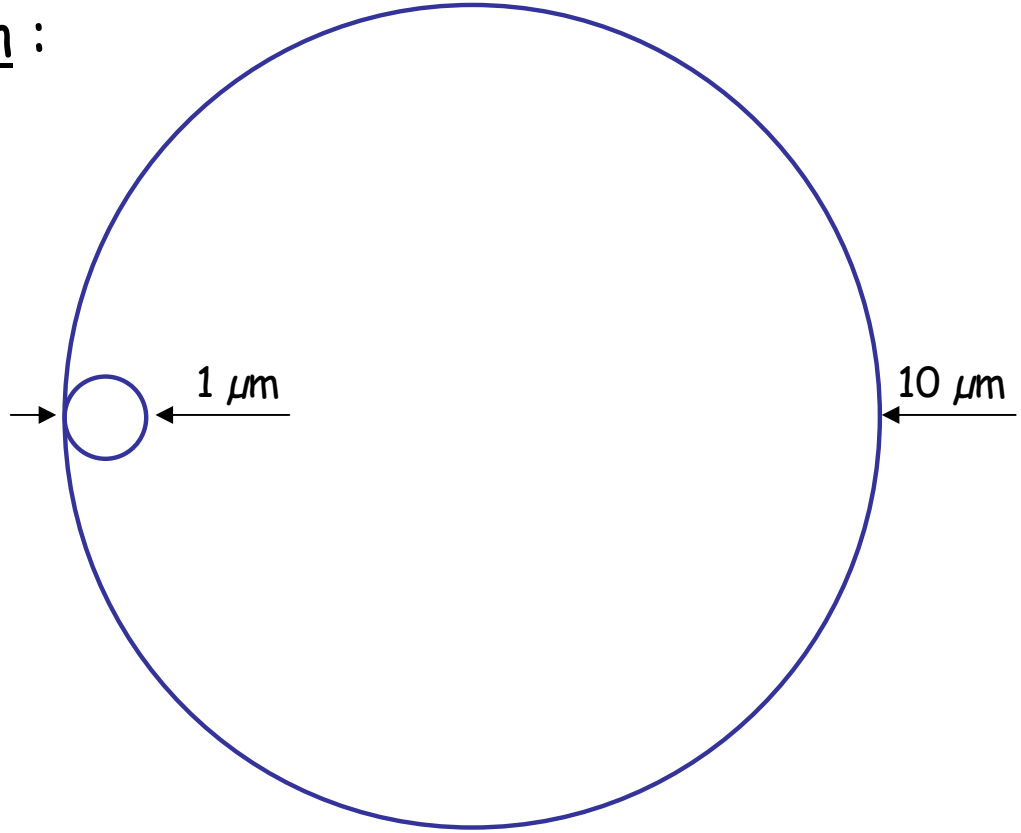
Contrôle de la focalisation :



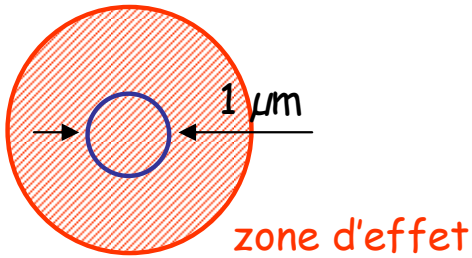
Technologie	Transistor MOS	SRAM
0.35 µm		
130 nm		
90 nm		
65 nm		

Contrôle de la focalisation :

- Taille du spot



- Zone d'effet
  Energie déposée



Contrôle de la localisation : lié au contrôle de la focalisation
platine (x,y,z)

Contrôle de l'instant d'injection : selon électronique de commande
et technologie (gigue).

Coût : élevé à très élevé (qqs 10^{aine} k€ à qqs 100^{aines} k€)

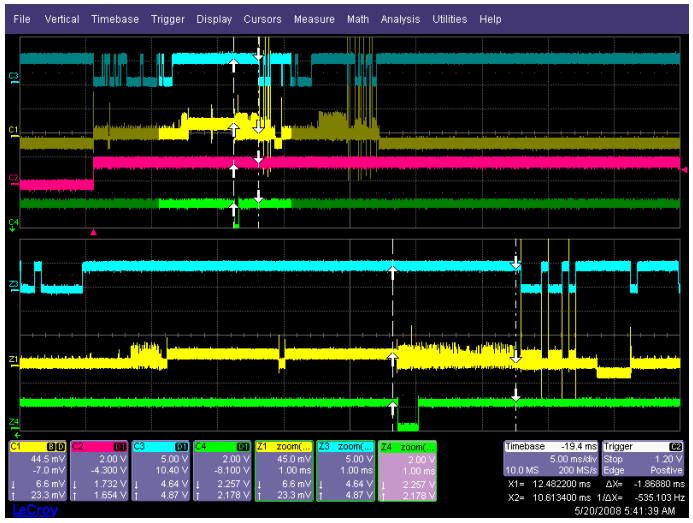
- Instrument de caractérisation sécuritaire (pour les plus chers)
  Multinationales, gouvernements, etc.

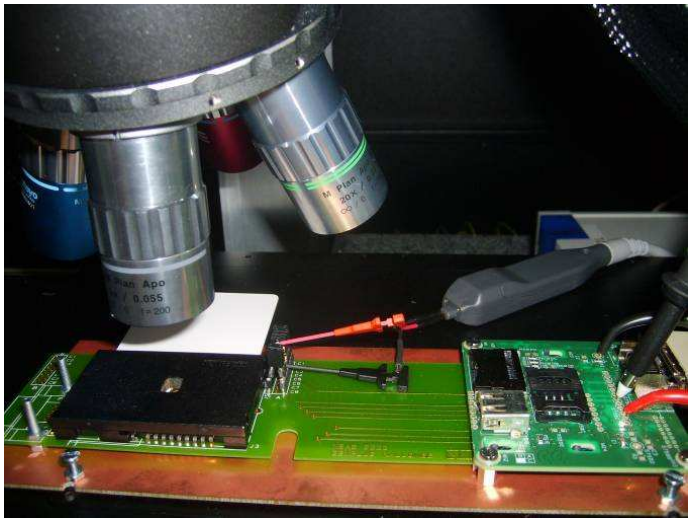
  Intérêt : reproductibilité, contrôle de la localisation/focalisation.

- Outil d'attaque pratique (pour les moins chers)
  Performances limitées (optiques inadaptées, pointeur laser, expertise, etc.).

  Interrogation : possibilité de satisfaire aux modèles de faute (DFA) ?

- Laser (IR, Green, UV)
- XY stage
- Camera
- Oscilloscope
- Synchronization board
- ISO Reader (optional)



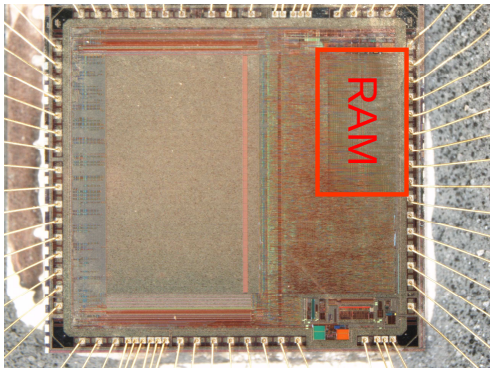


- Amélioration de la focalisation (injection mono-octet).

  Cadre : banc d'injection rudimentaire ($\varnothing_{spot}$ > 20 µm).

  ⟹ Gain en résolution spatiale dû au contrôle de l'instant d'injection

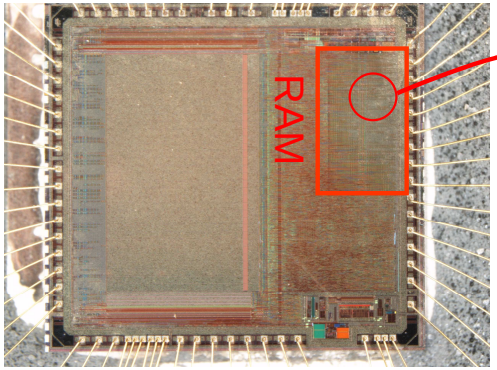
  Cible : implémentation AES sur microcontrôleur

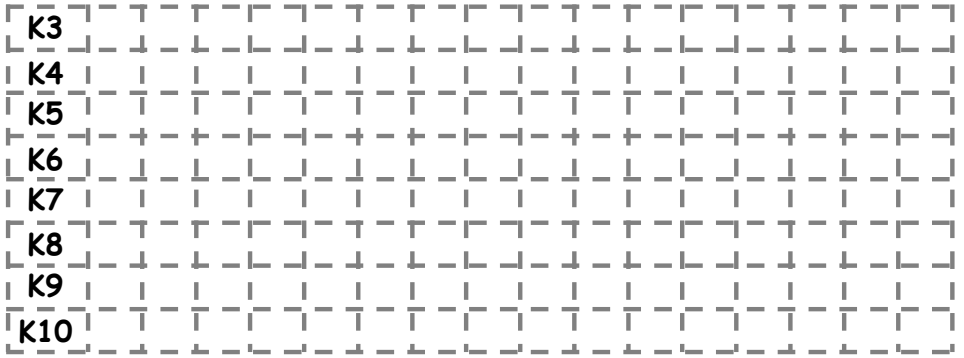


Attaque Piret – Quisquater :

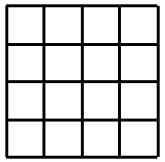
fauter un octet avant le MixColumn de la ronde 9

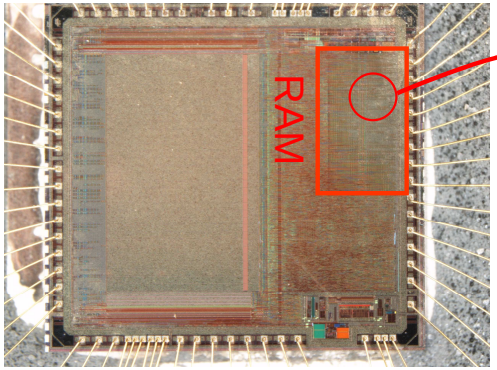
⟹ fauter un octet de K8

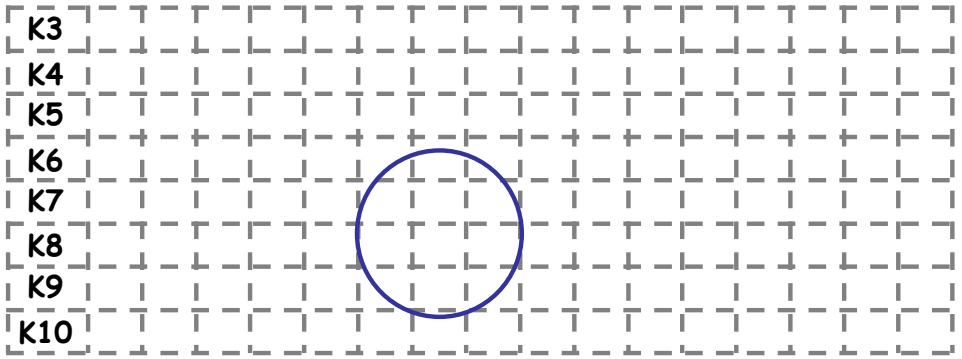




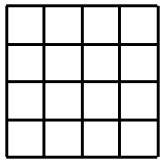
Chiffré

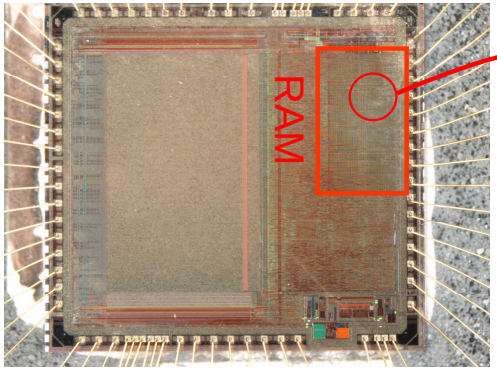


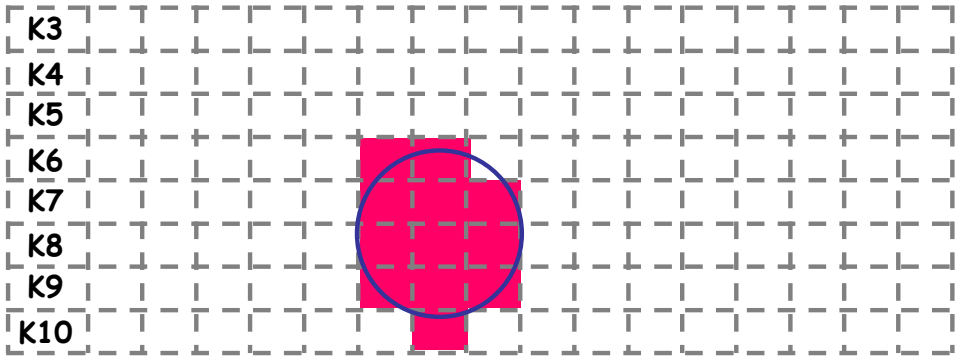




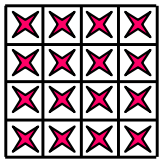
Chiffré

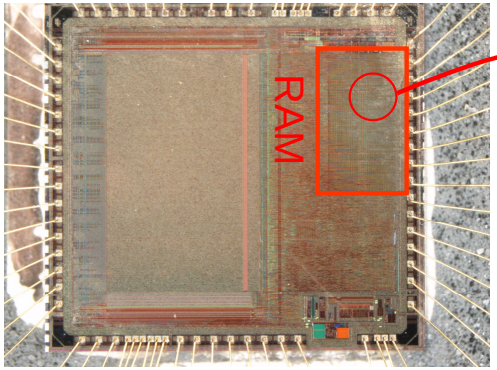


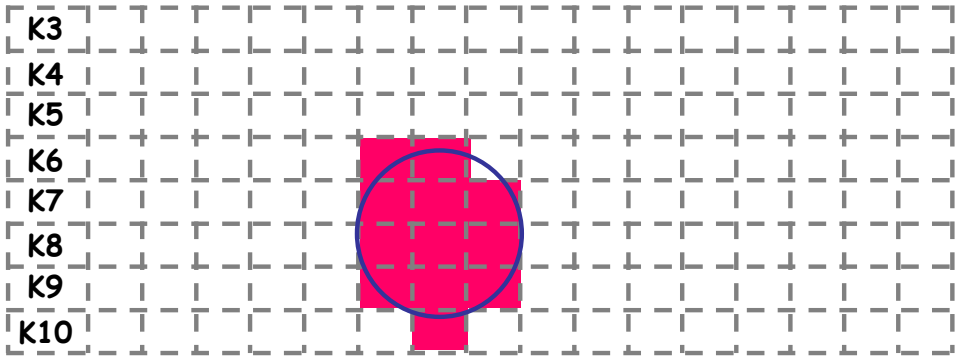




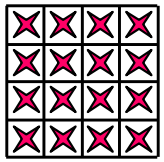
Chiffré



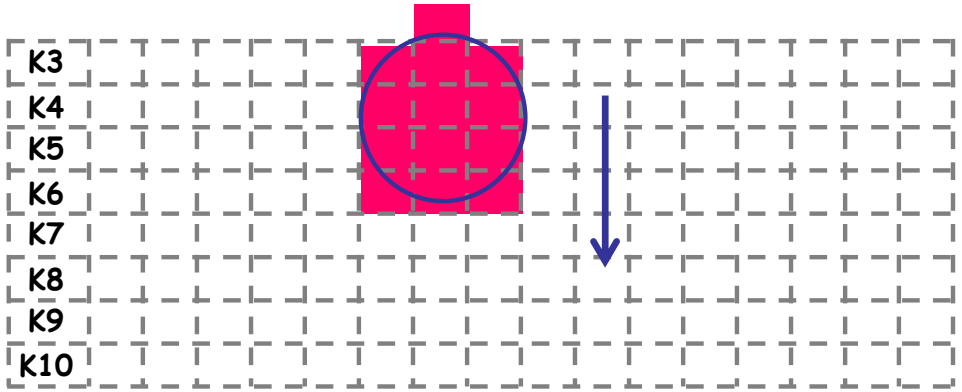




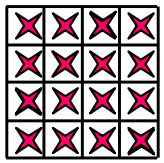
Chiffré

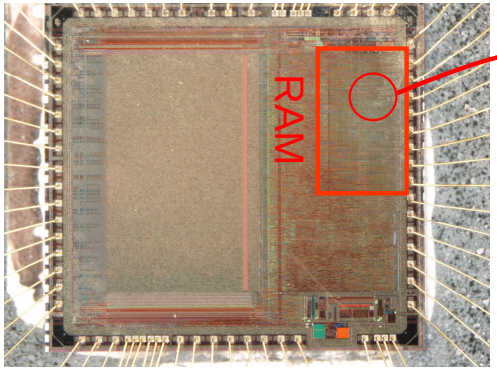


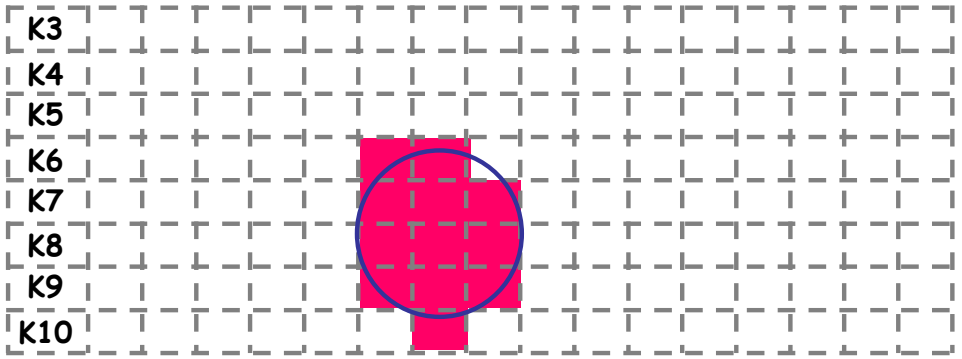
Pas de déplacement : 0,1 µm



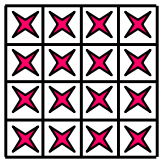
Chiffré



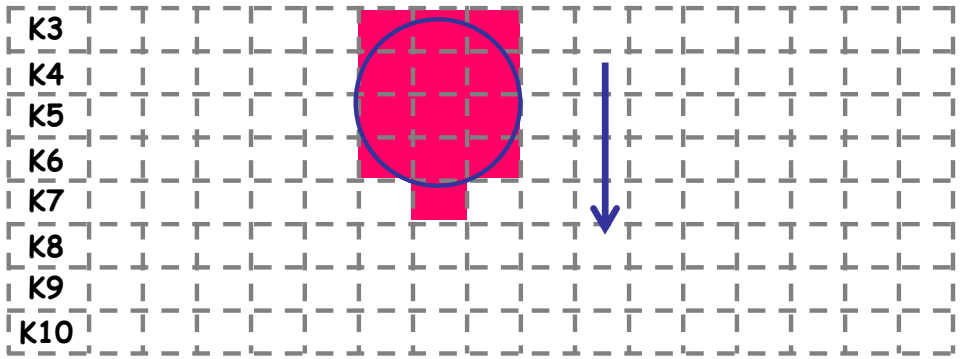




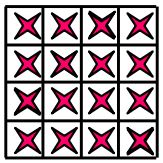
Chiffré

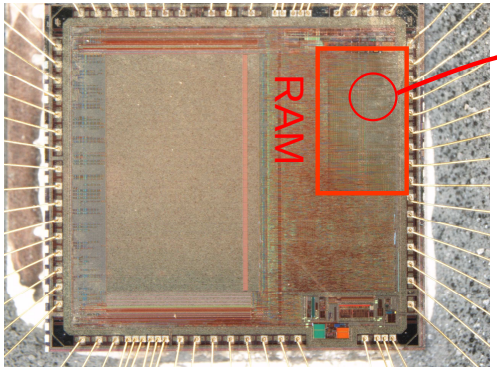


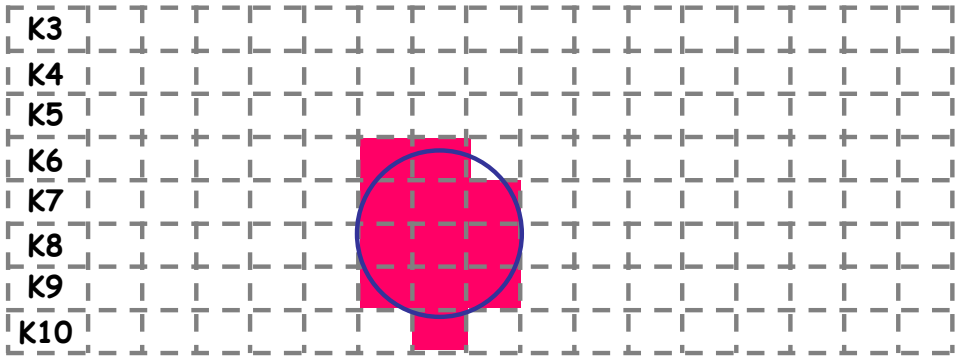
Pas de déplacement : 0,1 µm



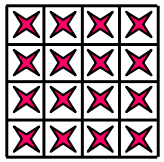
Chiffré



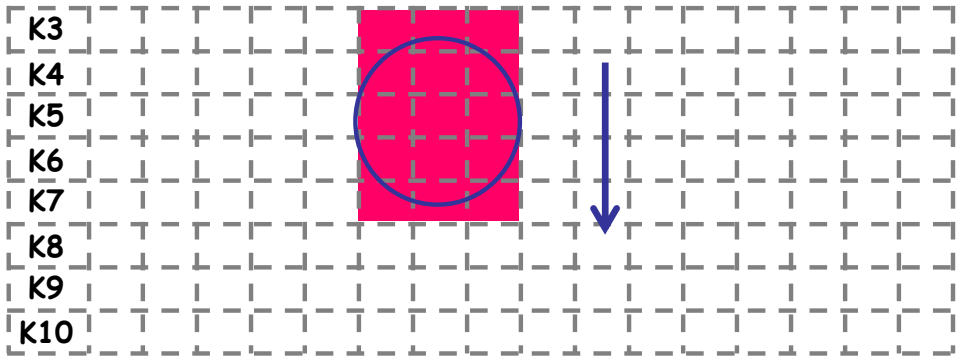




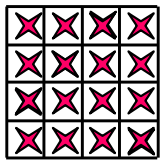
Chiffré

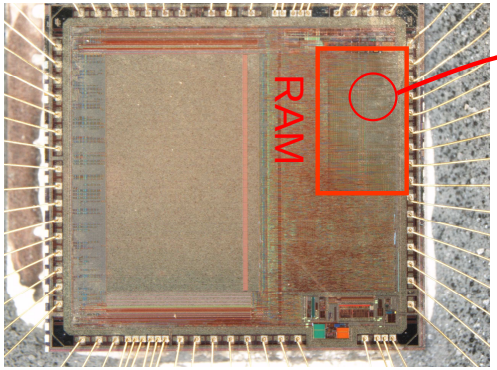


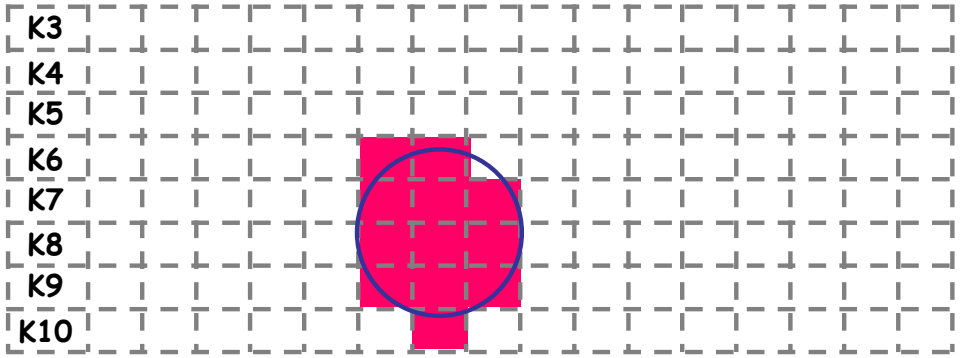
Pas de déplacement : 0,1 µm



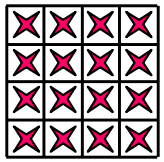
Chiffré



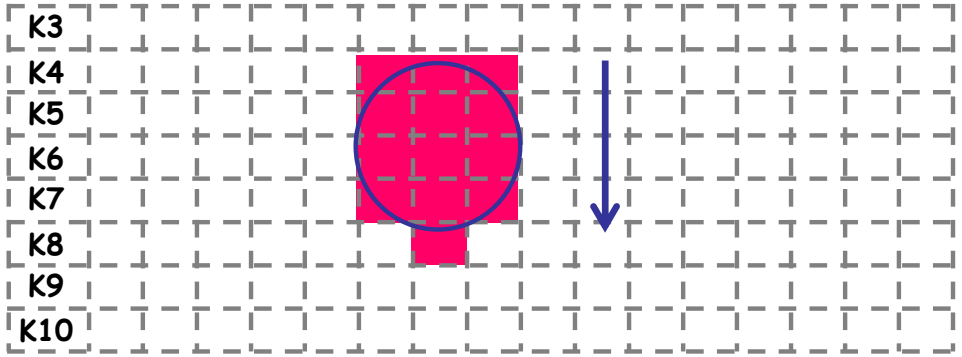




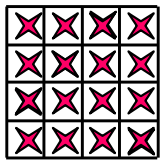
Chiffré

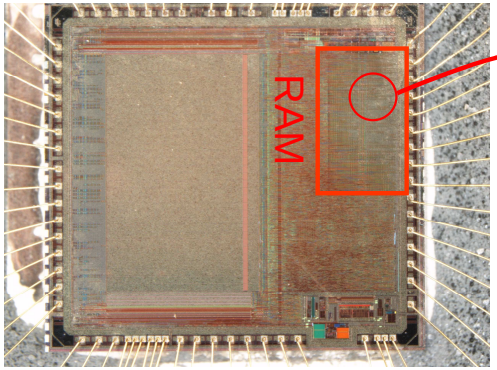


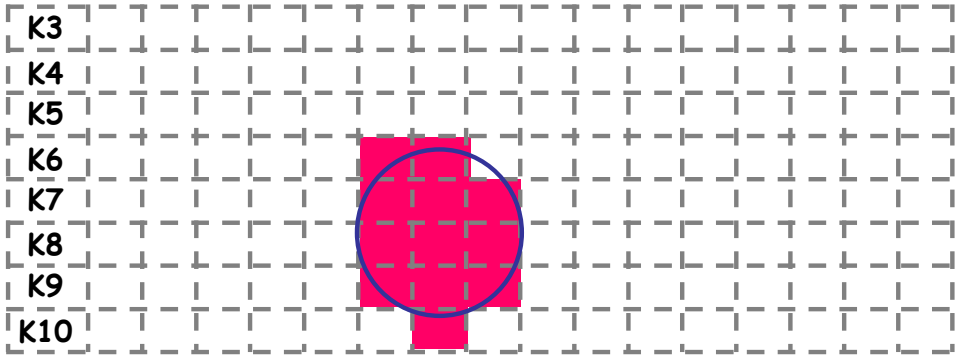
Pas de déplacement : 0,1 µm



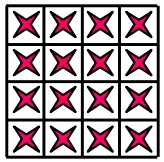
Chiffré



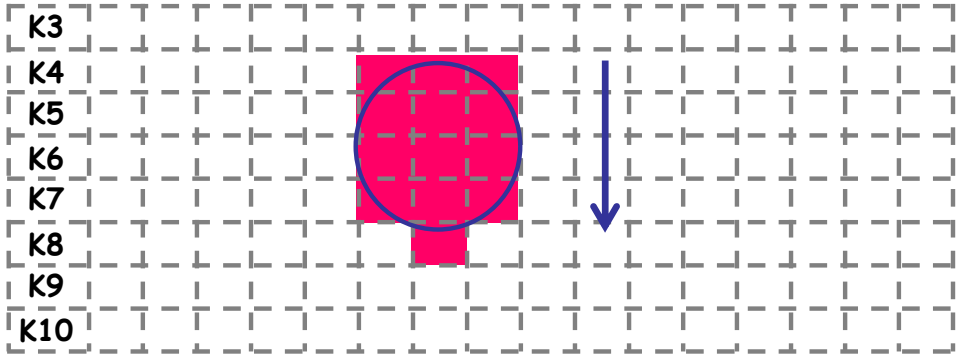




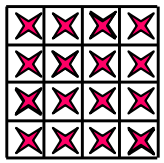
Chiffré



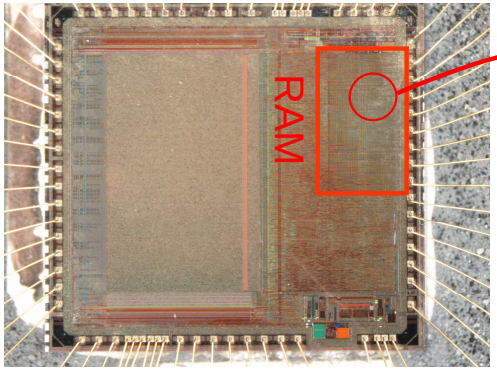
Pas de déplacement : 0,1 µm

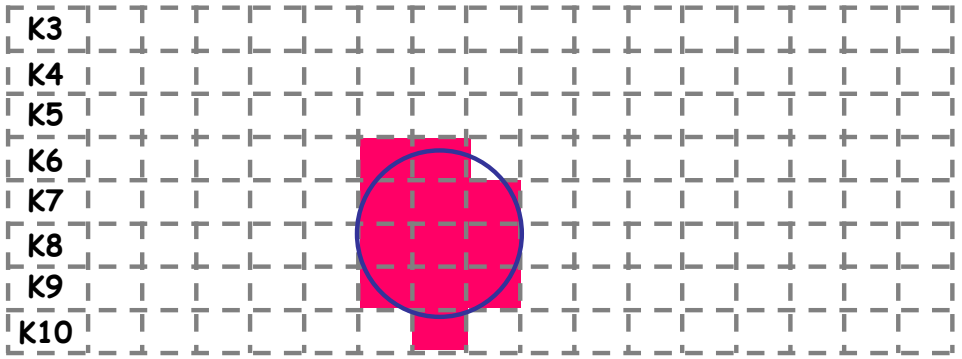


Chiffré

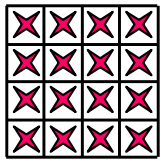


Injection en ronde 8
avant le AddRoundKey

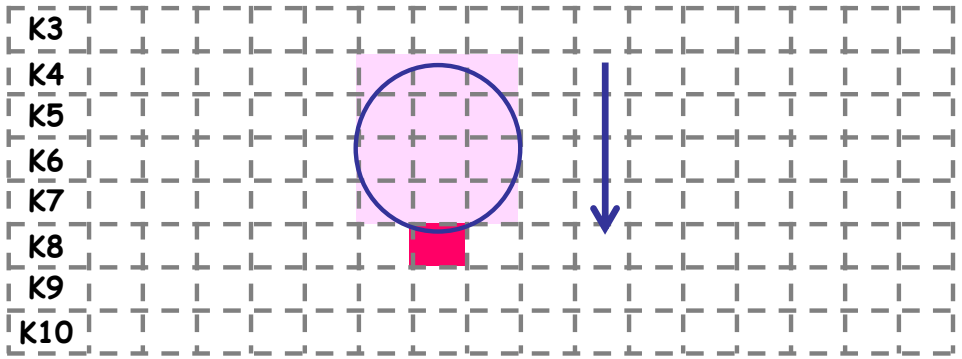




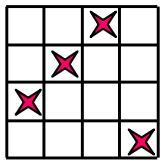
Chiffré



Pas de déplacement : 0,1 µm



Chiffré



Injection en ronde 8
avant le AddRoundKey

⇨ Algorithmique : faute mono-octet

Physique : fautes multi octets

	Contrôle de			reproductibilité	coût	facilité d'emploi
	instant d'injection	localisation	focalisation			
Glitch d'horloge (numérique)	maximum	moyen	très bon	bonne	faible	très bonne
Glitch d'alimentation (analogique)	bon[1]	moyen	très bon	bonne	moyen	bonne
Overclocking Baisse V_{DD} Température	faible	moyen	bon	bonne	faible	bonne
Laser	bon[2]	très bon	très bon	bonne	élevé	bonne

[1] selon électronique de commande

[2] selon électronique de commande et technologie

[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 Cryptograhy, 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
[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.
[Rob07] B. Robisson, P. Manet, Differential Behavioral Analysis, Accepted paper to CHES 2007.
[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.
[Guilley08] S. Guilley, L. Sauvage, J.-L. Danger, N. Selmane, R. Pacalet, *Silicon-level Solutions to Counteract Passive and Active, Attacks,* FDTC2008