



HAL
open science

Éteindre votre composant électronique ne le protège pas !

Paul Grandamme, Lilian Bossuet, Jean-Max Dutertre

► To cite this version:

Paul Grandamme, Lilian Bossuet, Jean-Max Dutertre. Éteindre votre composant électronique ne le protège pas !. JAIF 2024 - Journée thématique sur les attaques par injection de fautes, Oct 2024, Rennes, France. ⟨hal-04935027⟩

HAL Id: hal-04935027

<https://hal.science/hal-04935027v1>

Submitted on 7 Feb 2025

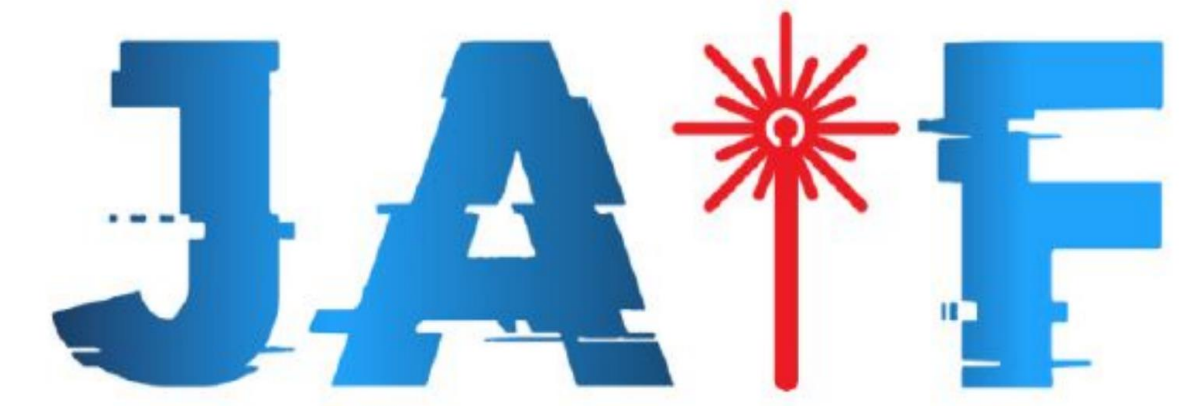
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Éteindre votre composant électronique ne le protège pas !



Paul Grandamme^{1,2}, Lilian Bossuet¹, Jean-Max Dutertre²

¹Laboratoire Hubert Curien, Université Jean Monnet, CNRS, Saint-Étienne - paul.grandamme@univ-st-etienne.fr, lilian.bossuet@univ-st-etienne.fr

²Mines Saint-Étienne, CEA Leti, Centre CMP, Gardanne - dutertre@emse.fr

Contexte

État de l'art

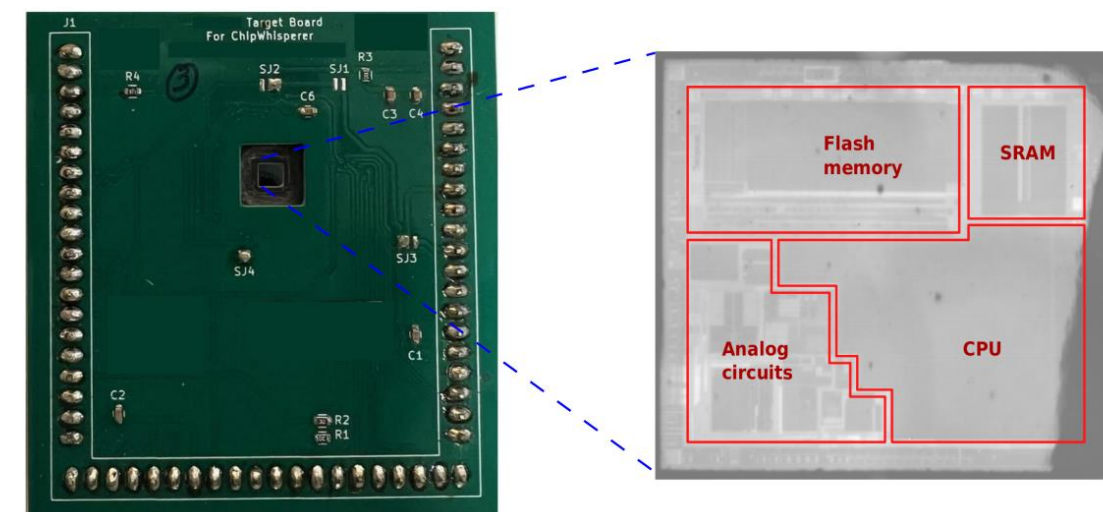
La majeure partie des **attaques par injection de fautes** sont réalisées sur des composants en fonctionnement donc **alimentés en énergie**.

Problème

Des capteurs internes peuvent détecter l'attaque et permettre aux composants électroniques de réagir.

Dispositif expérimental

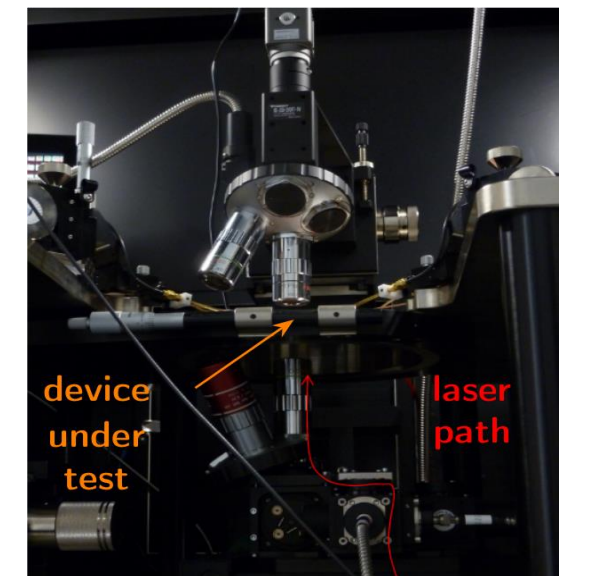
DUT



- STM32F1
- Flash : 128 pages de 1kB
- 2048 bitlines et 512 wordlines

Source laser

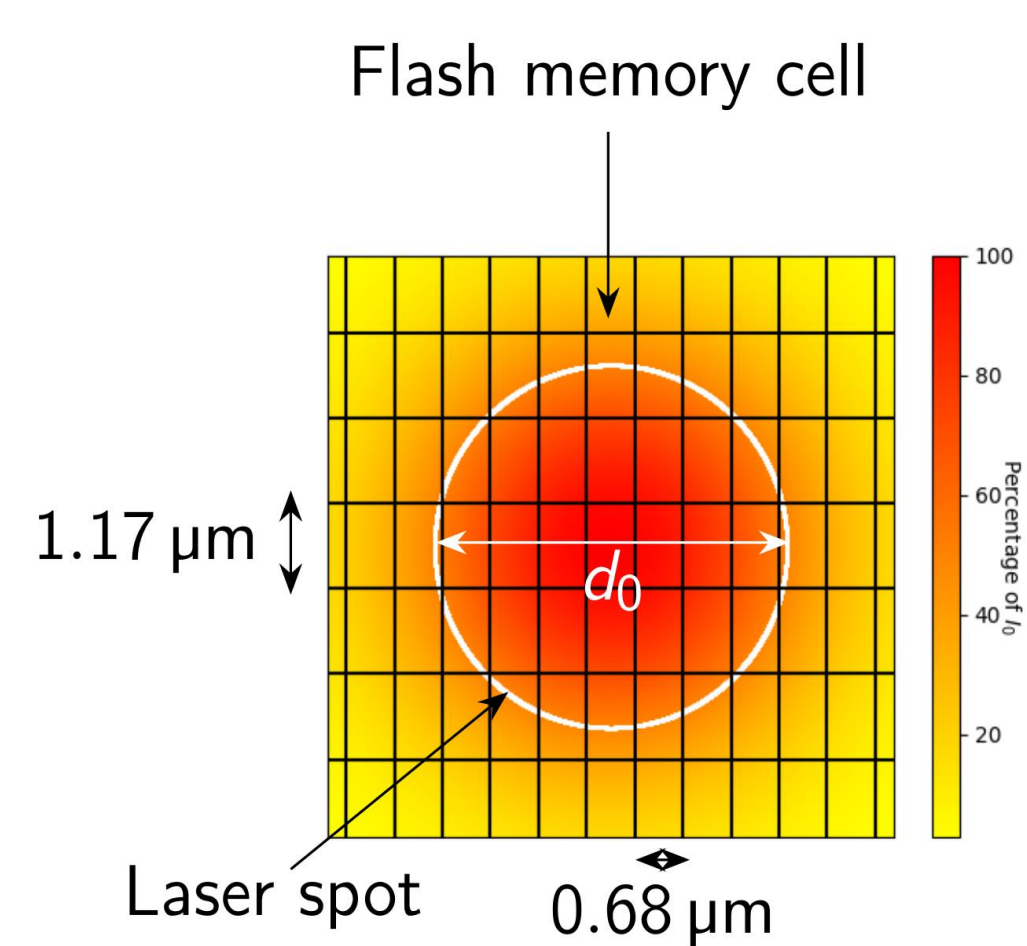
- 1064 nm (IR)
- Tirs de 0,9s
- Puissance de 1W
- Grossissement x20



Modèle de faute

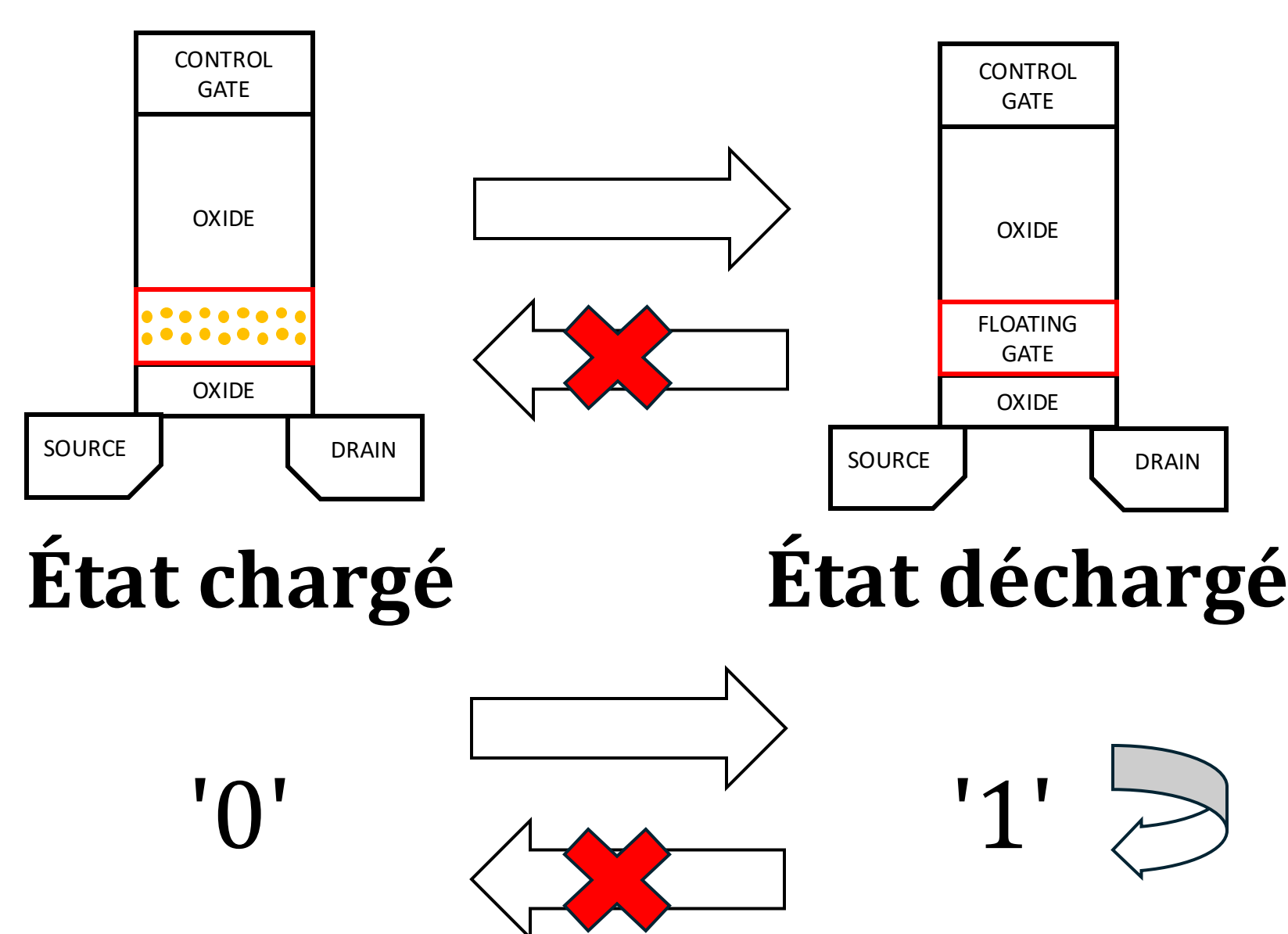
Niveau physique

- L'exposition du circuit à un **rayon laser** génère une **augmentation de température**.



- L'élévation de température conduit à la **décharge des transistors à grille flottante**.

Niveau logique



- Modèle de faute **unidirectionnel** et **data-dépendant**
- **Fautes persistantes**

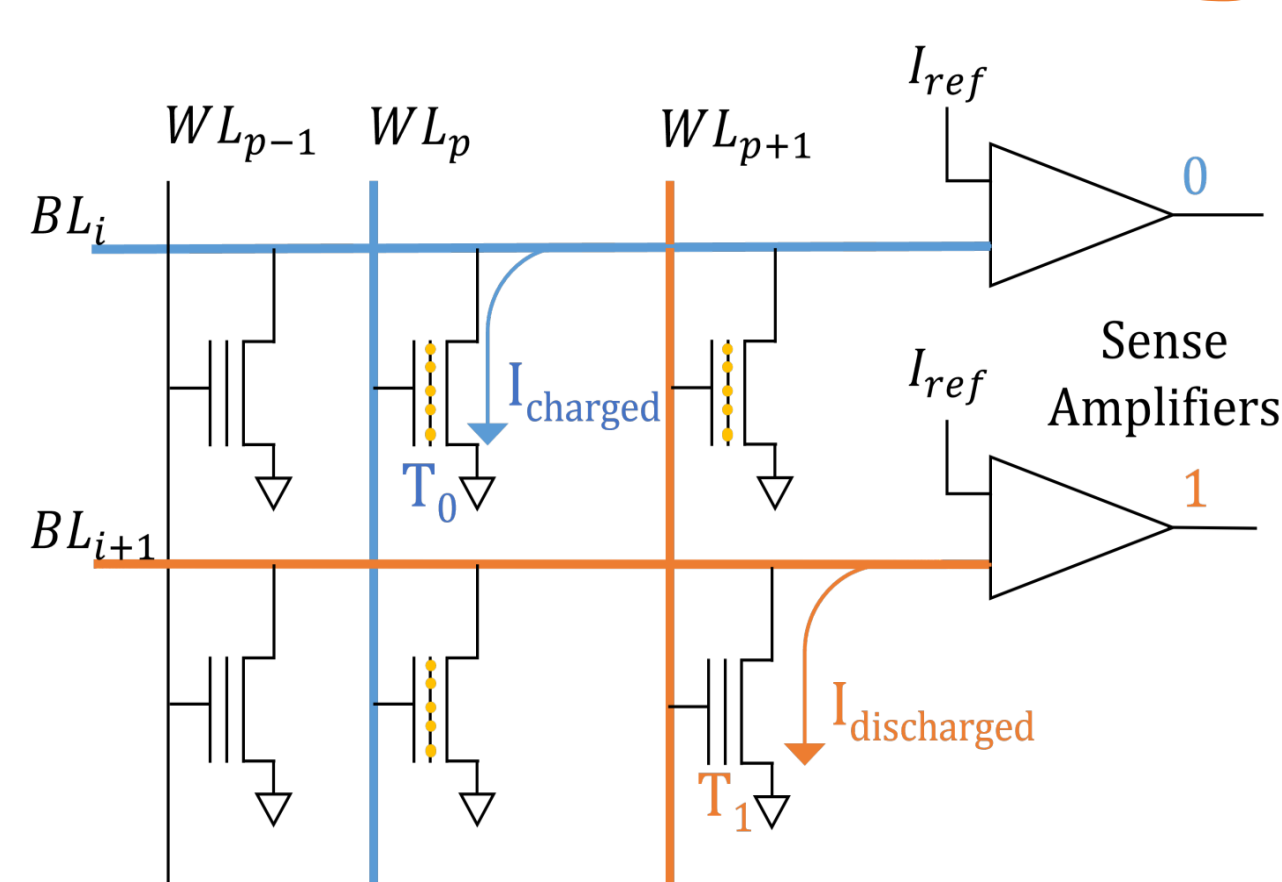
Niveau mémoire

- Corruption de firmware [1]

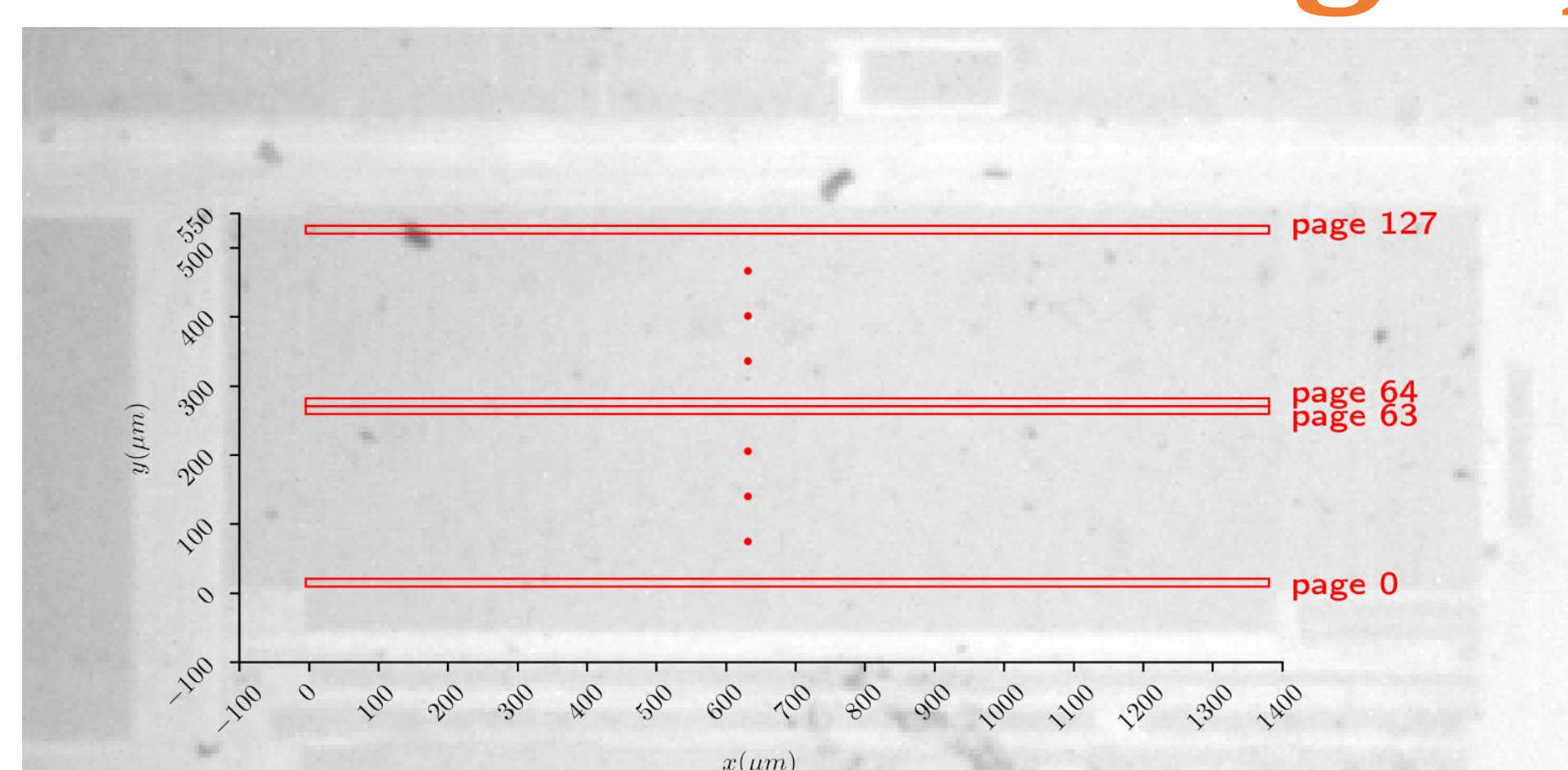
[31]	[30]	[29]	[28]	[27]	[26]	[25]	[24]	[23]	[22]	[21]	[20]	[19]	[18]	[17]	[16]	[15]	[14]	[13]	[12]	[11]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]	[0]		
Generic MOVW																																	
1	1	1	1	0	1	1	0	0	1	0	0	1	mm4	0	1	mm3	Rd																
MOVW, R0, 0																																	
1	1	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
MOVW, R0, 4																																	
1	1	1	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
MOVW, R1, 0																																	
1	1	1	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
MOVW, R0, 0																																	
1	1	1	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

- Mémoires Flash également utilisées pour stocker des constantes, droits d'accès, clés cryptographiques, etc.
- Notamment, la **S-box de l'AES**.

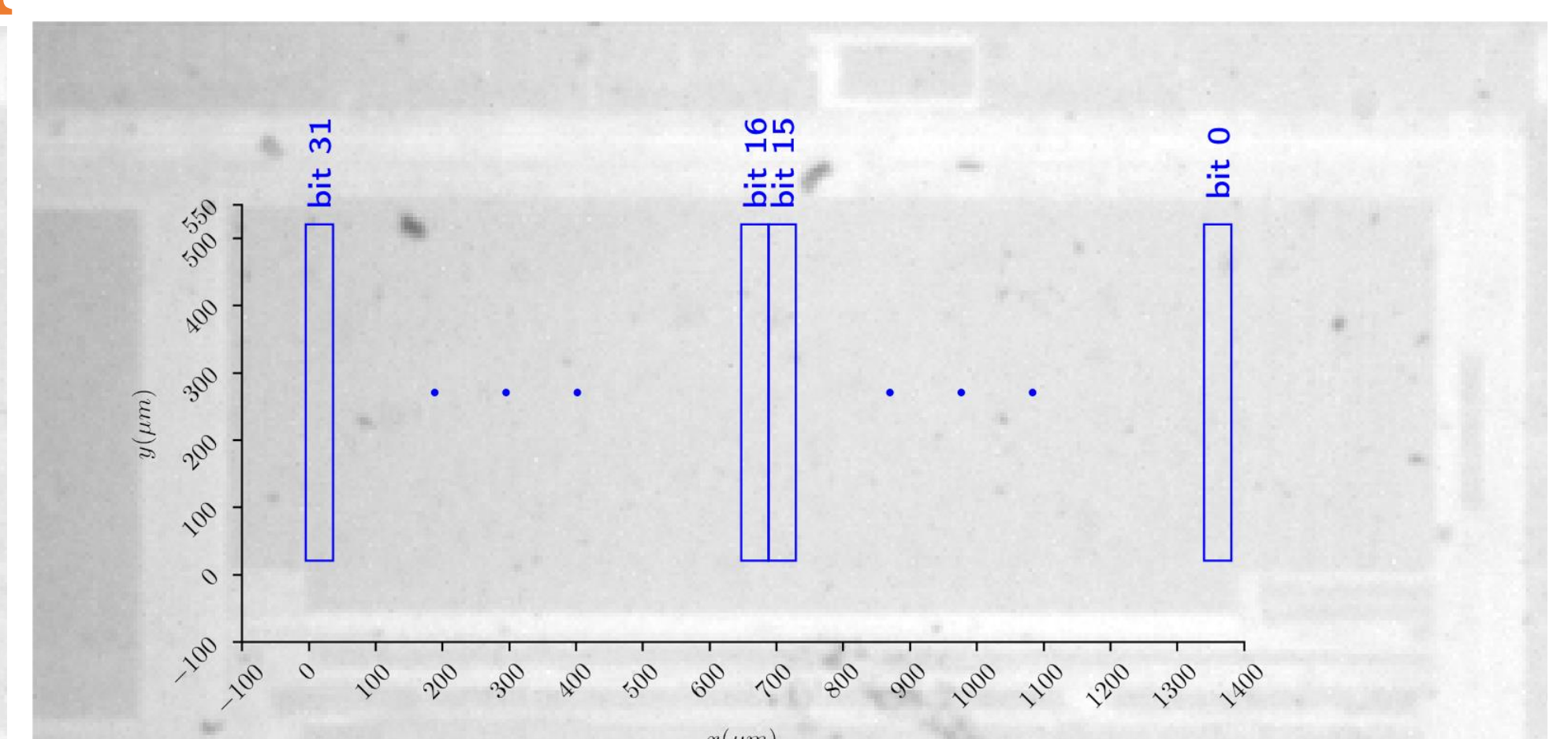
Rétro-ingénierie de la cartographie de la Flash



Opération de lecture en Flash



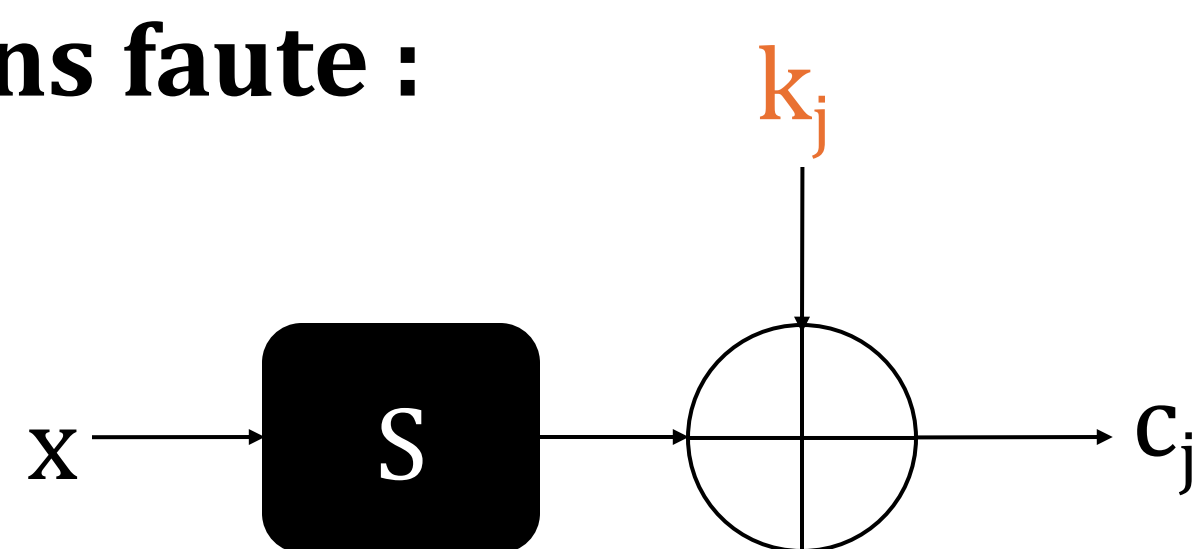
Au niveau des pages



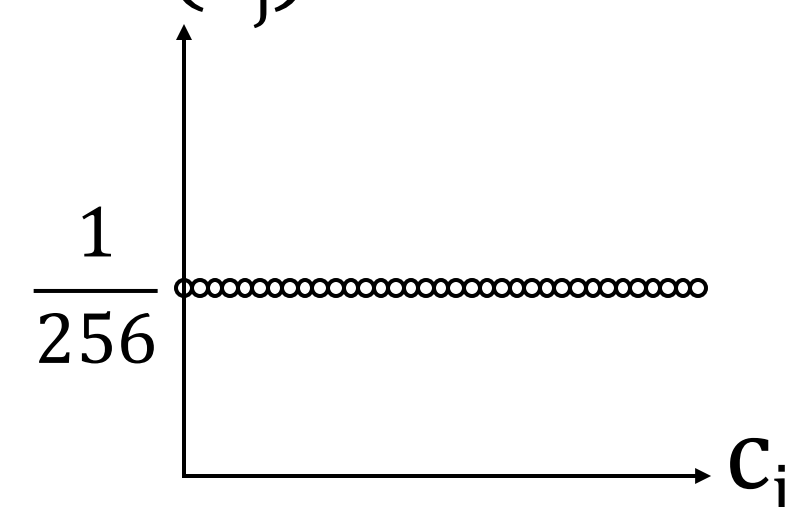
Au niveau des bits

Application : Persistent Fault Analysis [2]

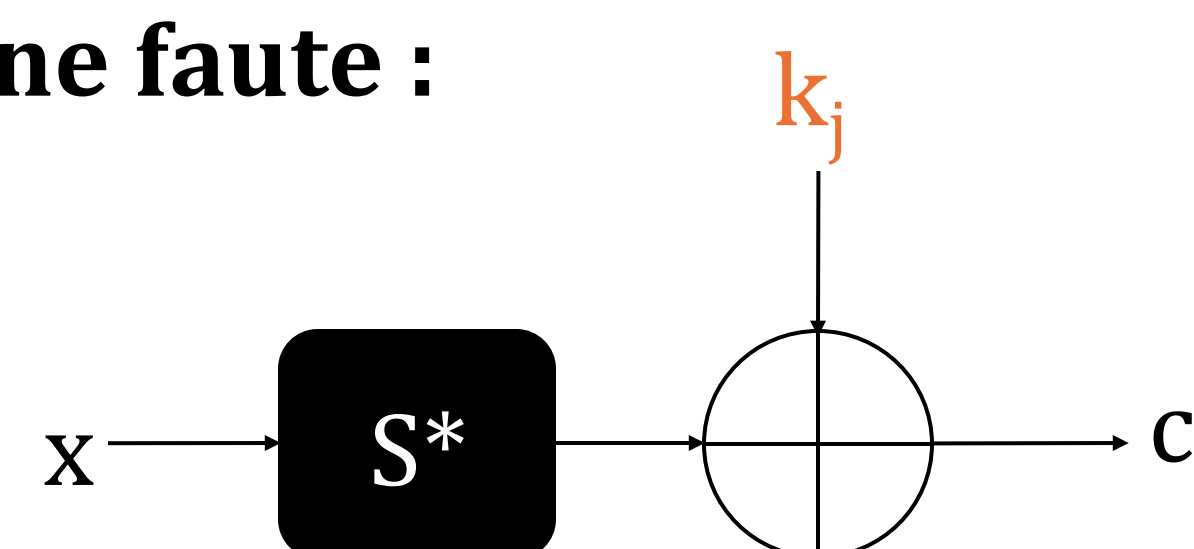
Sans faute :



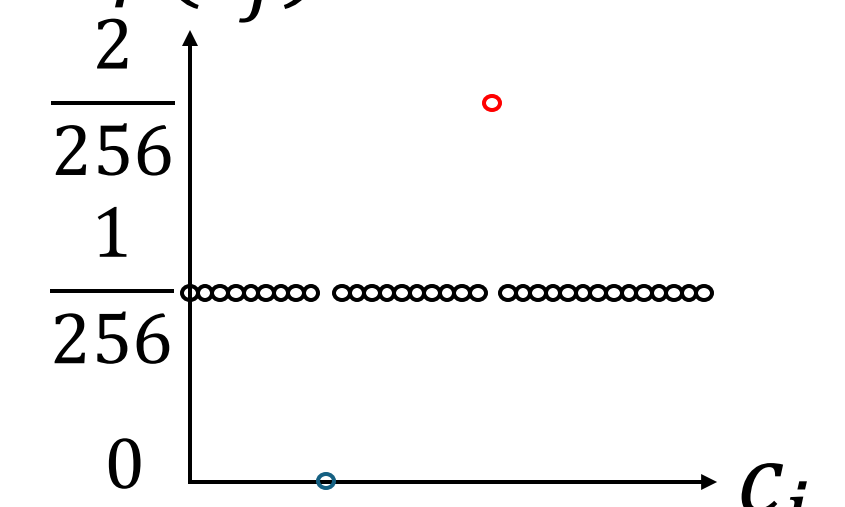
$\Pr(c_j)$



Avec une faute :



$\Pr_r(c_j)$



Conclusion

- Publié à TCHES 2024 [3].
- Scénario réaliste de la PFA.
- Les fabricants de semiconducteurs doivent systématiquement intégrer des dispositifs de protection des mémoires.

Références

- [1] Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller" HOST 2019
- [2] Zhang et al. "Persistent Fault Analysis on Block Ciphers" TCHES 2018
- [3] Grandamme et al. "Switching Off your Device Does Not Protect Against Fault Attacks" TCHES 2024