Éteindre votre composant électronique ne le protège pas !

Paul Grandamme, Lilian Bossuet, Jean-Max Dutertre

Éteindre votre composant électronique ne le protège pas !

Paul Grandamme[1,2], Lilian Bossuet[1], Jean-Max Dutertre[2]

[1]Laboratoire Hubert Curien, Université Jean Monnet, CNRS, Saint-Étienne - paul.grandamme@univ-st-etienne.fr, lilian.bossuet@univ-st-etienne.fr
[2] Mines Saint-Étienne, CEA Leti, Centre CMP, Gardanne - dutertre@emse.fr

Contexte

État de l'art

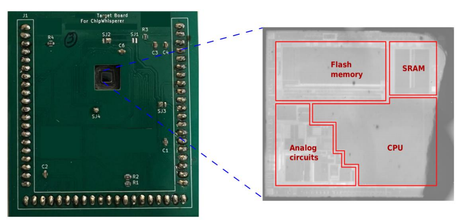
La majeure partie des **attaques par injection de fautes** sont réalisées sur des composants en fonctionnement donc **alimentés en énergie.**

Problème

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

Dispositif expérimental

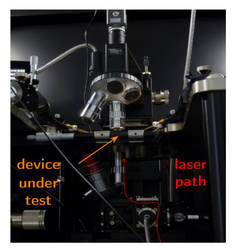
DUT



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

Source laser

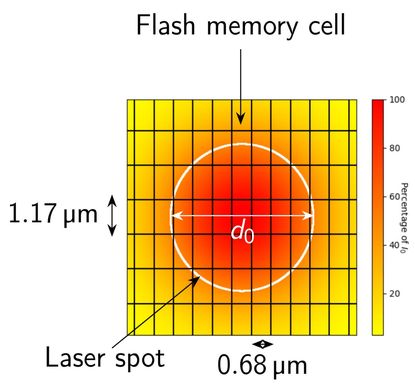
- 1064 nm (IR)
- Tirs de 0.9s
- Puissance de 1W
- Grossissement x20



Modèle de faute

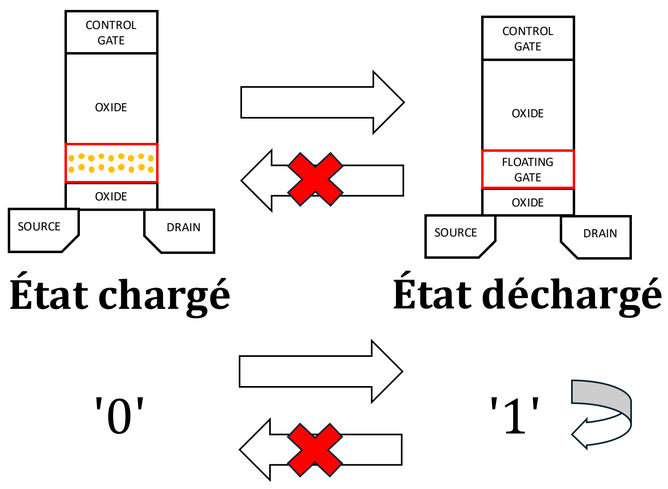
Niveau physique

- 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.**

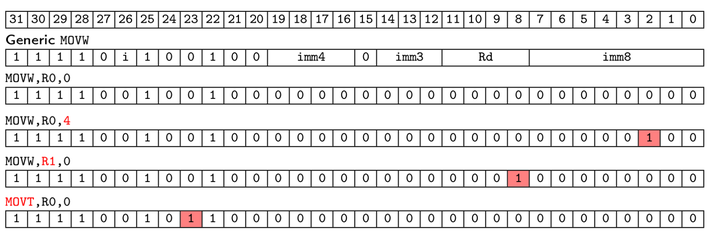
Niveau logique



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

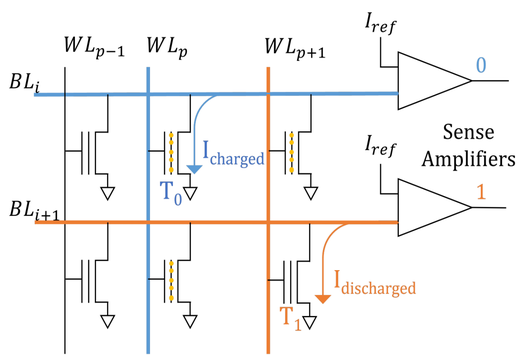
Niveau mémoire

- Corruption de firmware [1]

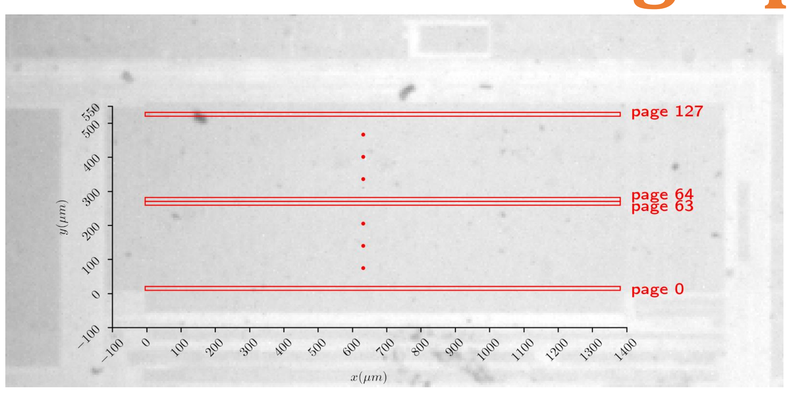


- Mémoires Flash également utilisées pour stocker des constantes, droits d'accès, clés cryptographiques, etc.
- Notamment, la **S-box de l'AES**.

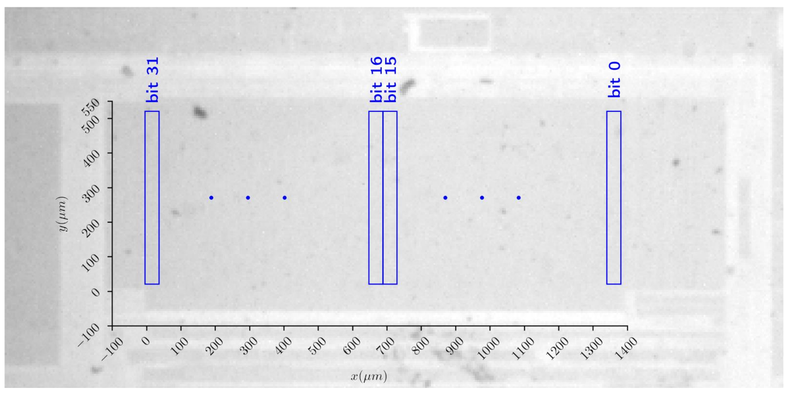
Rétro-ingénierie de la cartographie de la Flash



Opération de lecture en Flash



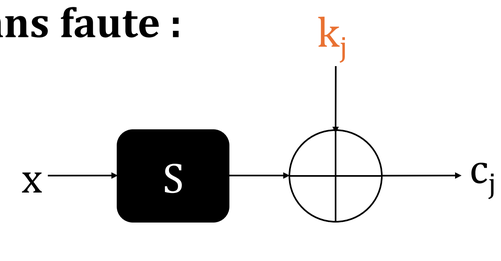
Au niveau des pages

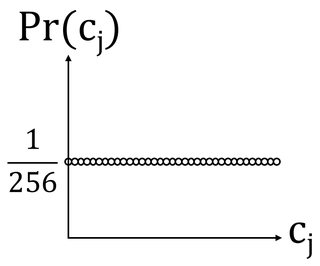


Au niveau des bits

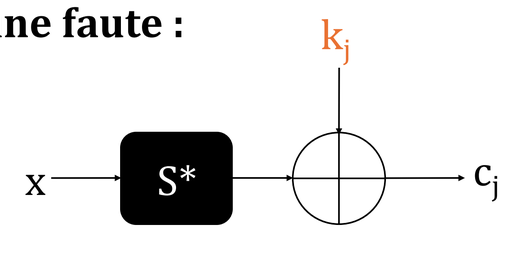
Application : Persistent Fault Analysis [2]

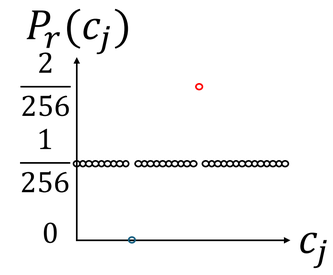
Sans faute :





Avec une faute :





Conclusion

- Publié à TCHES 2024 [3].
- Scénario réaliste de la PFA.
- Les fabricants de semiconducteurs doivent systématiquement intégré 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

Laboratoire Hubert Curien
UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne

MINES Saint-Étienne

anr agence nationale de la recherche