

Techniques avancées d'attaques par injection de fautes sur circuits intégrés

Paul GRANDAMME
3 Février 2025



Devant le jury composé de :

Stéphanie ANCEAU, Examinateuse
Giorgio DI NATALE, Rapporteur
Sylvain GIRARD, Examinateur
Jérémy POSTEL-PELLERIN, Rapporteur
Vincent POUGET, Examinateur
Michel AGOYAN, Invité

Direction de thèse :

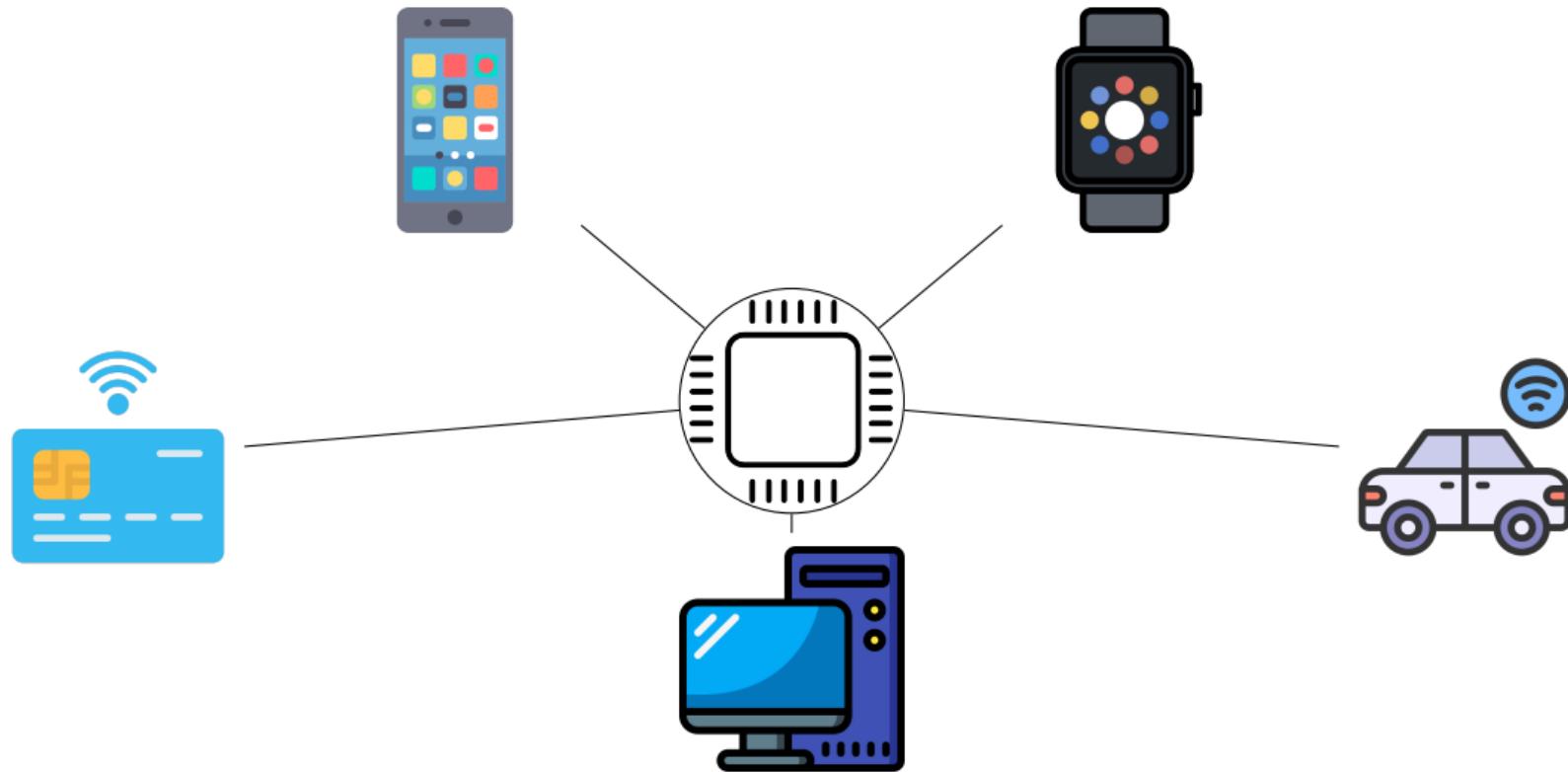
Lilian BOSSUET
Jean-Max DUTERTRE



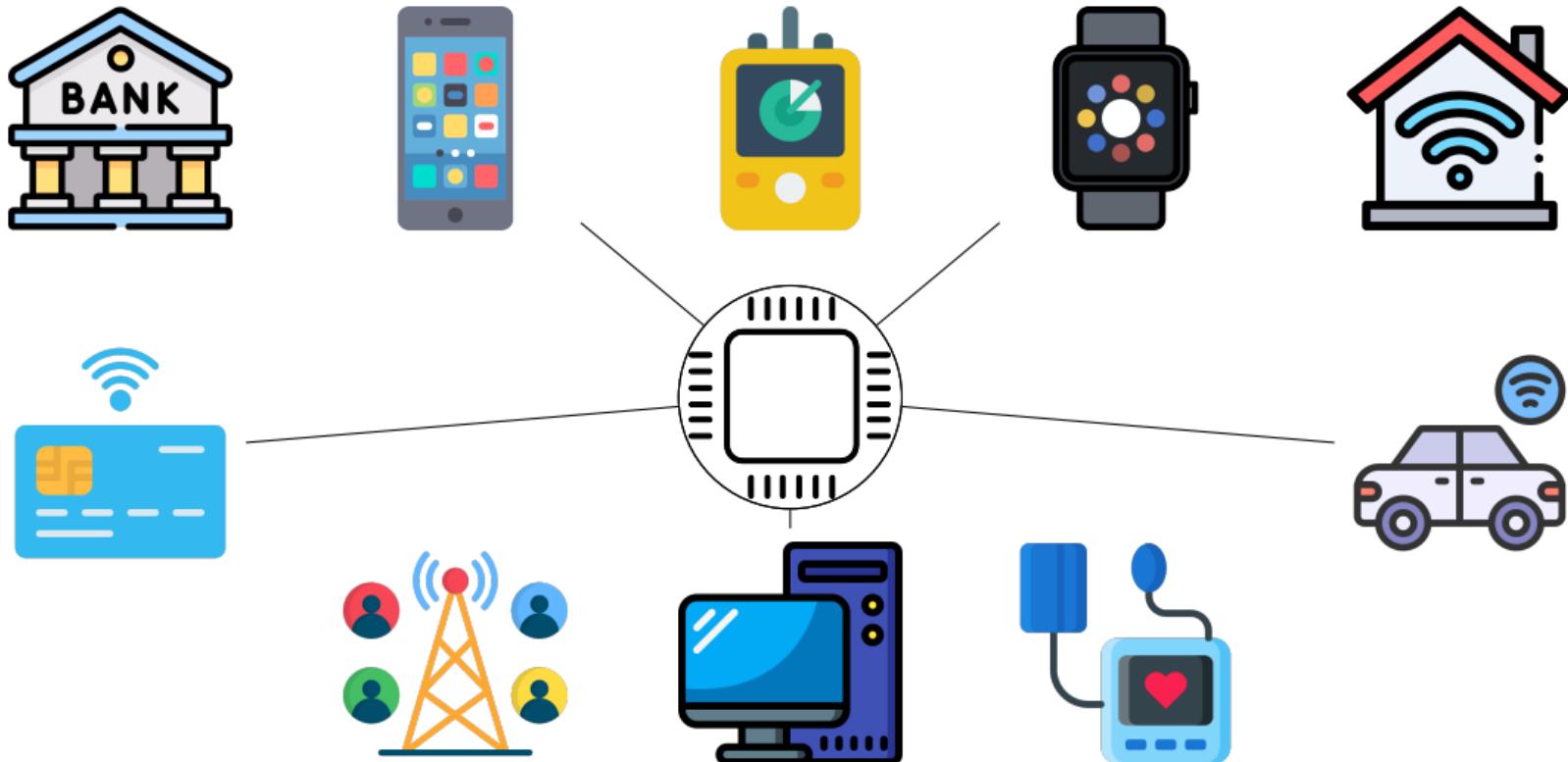
Contexte



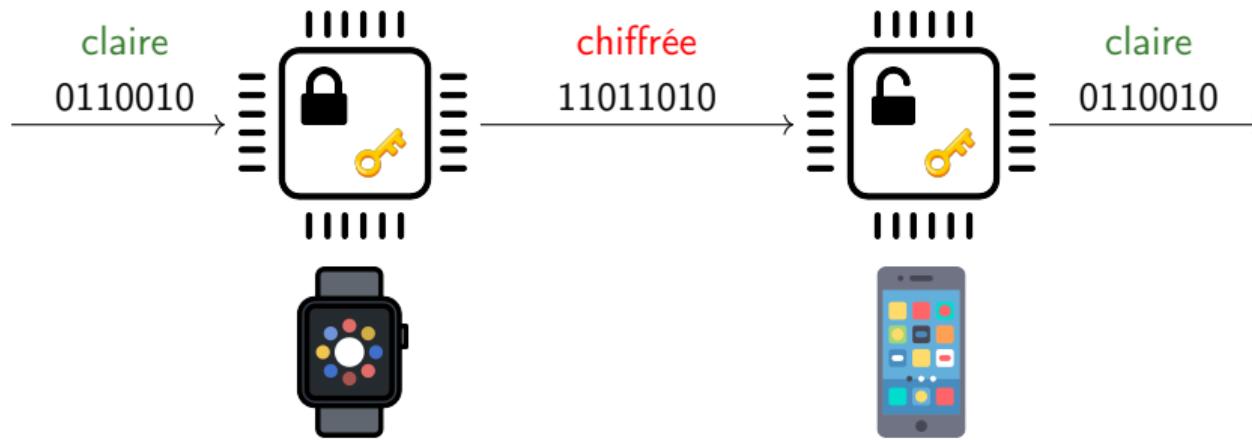
Contexte



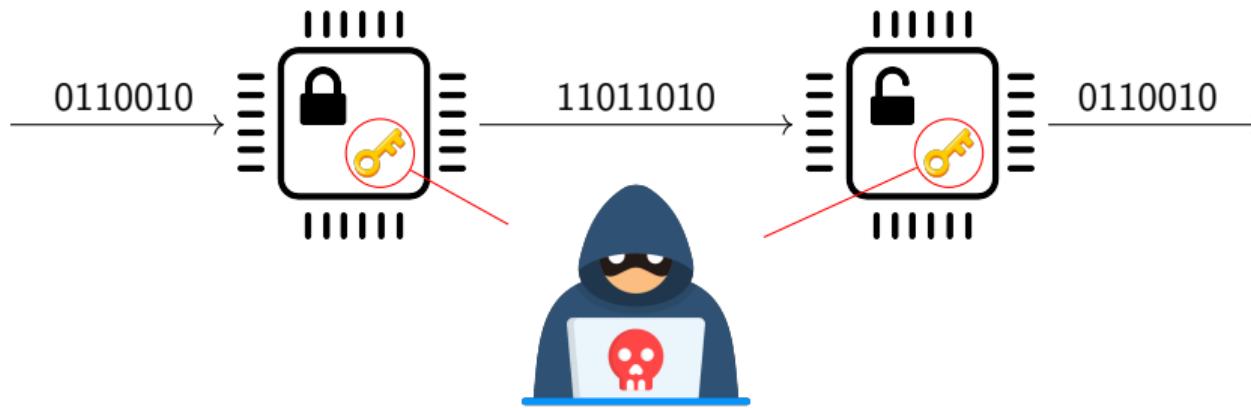
Contexte



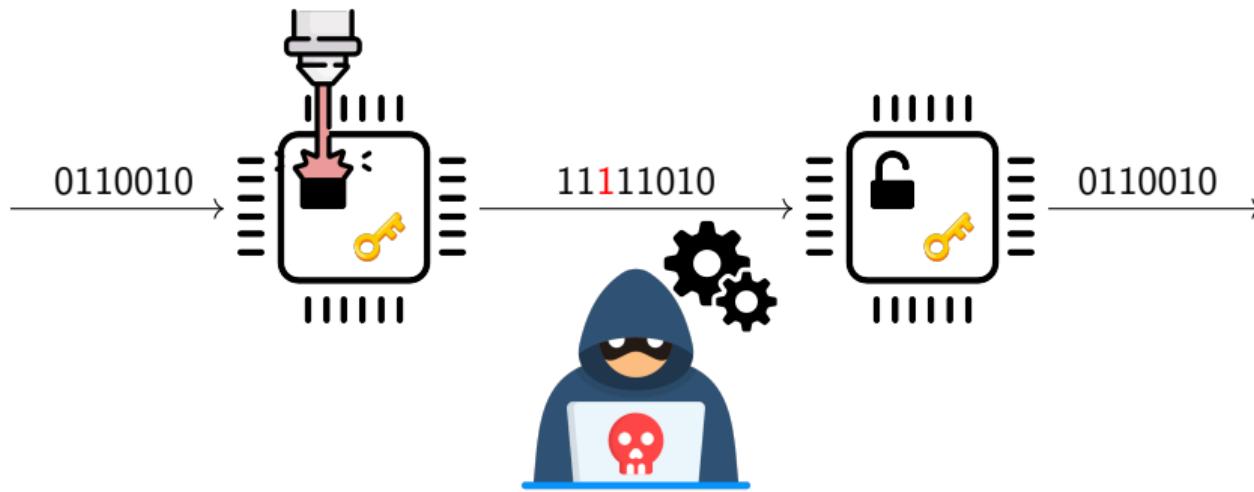
Communications sécurisées



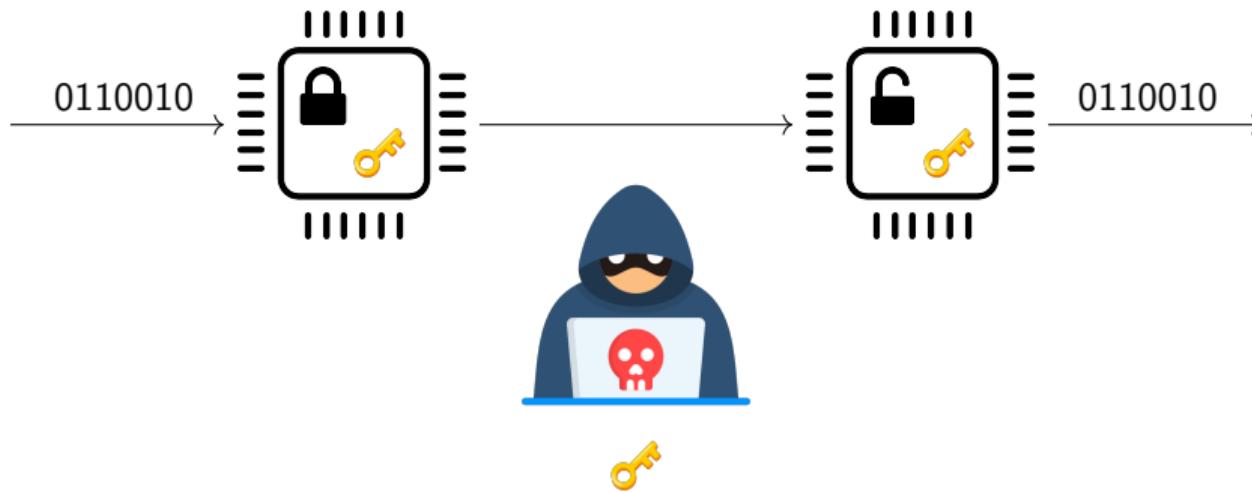
Communications sécurisées



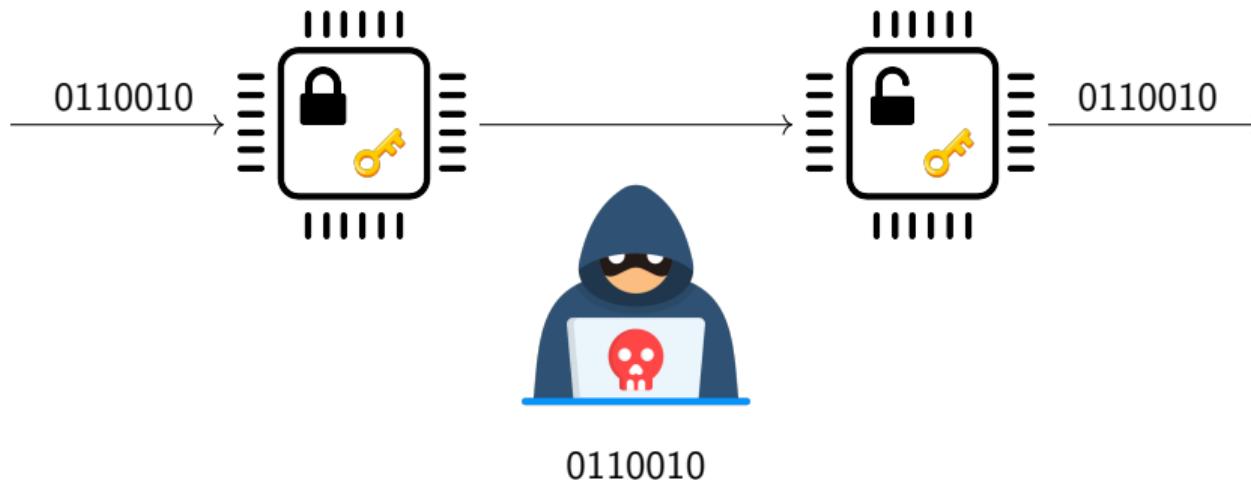
Communications sécurisées



Communications sécurisées



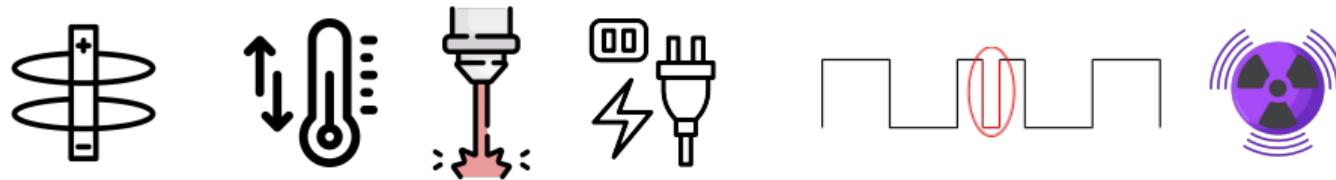
Communications sécurisées



Attaque par injection de faute

Définition

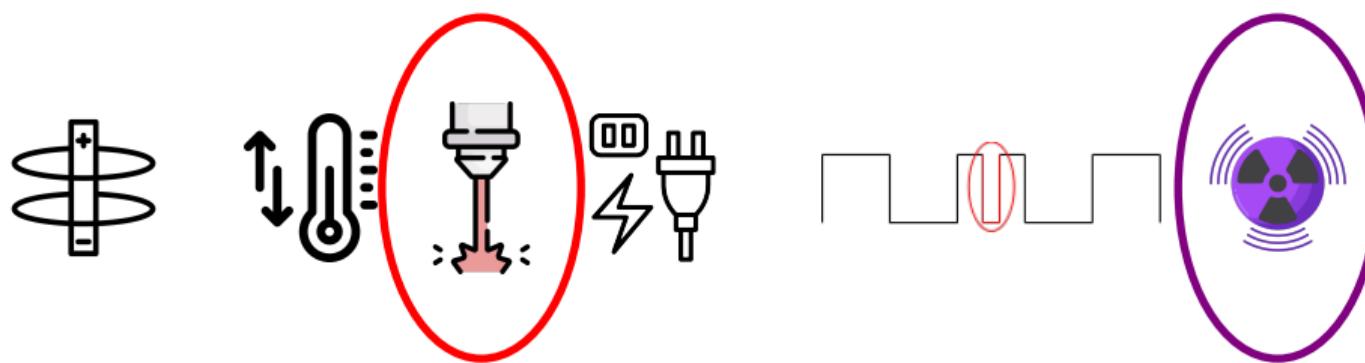
Perturbation du circuit intégré dans l'objectif de modifier son fonctionnement afin d'extraire de l'information ou de désactiver des mécanismes de protection internes.



Attaque par injection de faute

Définition

Perturbation du circuit intégré dans l'objectif de modifier son fonctionnement afin d'extraire de l'information ou de désactiver des mécanismes de protection internes.



Chronologie

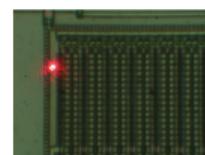
2002

2009

Flash d'appareil
photo¹



Lampe UV²
Laser³



¹Sergei P. Skorobogatov and Ross J. Anderson. "Optical Fault Induction Attacks". In: *CHES 2002*.

²Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos. "Optical Fault Attacks on AES: A Threat in Violet". In: *FDTC 2009*.

³Sergei P. Skorobogatov. "Local Heating Attacks on Flash Memory Devices". In: *IEEE HOST 2009*.

⁴Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: *IEEE HOST 2019*.

⁵Alexandre Menu et al. "Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation". In: *FDTC 2020*.

⁶Brice Colombier et al. "Multi-Spot Laser Fault Injection Setup: New Possibilities for Fault Injection Attacks". In: *CARDIS 2022*.

Chronologie

2002

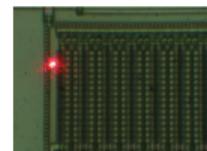
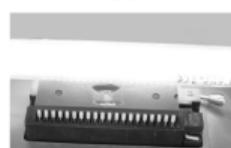
2009

2019 2020

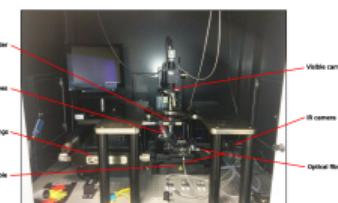
Flash d'appareil photo¹



Lampe UV²
Laser³



Compréhension complète
du modèle de faute^{4,5}



¹Sergei P. Skorobogatov and Ross J. Anderson. "Optical Fault Induction Attacks". In: *CHES 2002*.

²Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos. "Optical Fault Attacks on AES: A Threat in Violet". In: *FDTC 2009*.

³Sergei P. Skorobogatov. "Local Heating Attacks on Flash Memory Devices". In: *IEEE HOST 2009*.

⁴Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: *IEEE HOST 2019*.

⁵Alexandre Menu et al. "Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation". In: *FDTC 2020*.

⁶Brice Colombier et al. "Multi-Spot Laser Fault Injection Setup: New Possibilities for Fault Injection Attacks". In: *CARDIS 2022*.

Chronologie (CARDIS 2022)

2002

2009

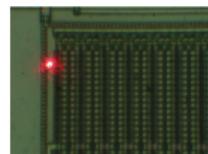
2019 2020

2022

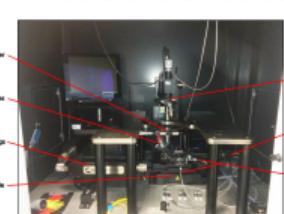
Flash d'appareil photo¹



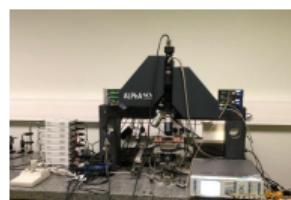
Lampe UV²
Laser³



Compréhension complète
du modèle de faute^{4,5}



Banc multispot⁶



ALPhANOV
Optics & Lasers Technology Center

¹Sergei P. Skorobogatov and Ross J. Anderson. "Optical Fault Induction Attacks". In: *CHES 2002*.

²Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos. "Optical Fault Attacks on AES: A Threat in Violet". In: *FDTc 2009*.

³Sergei P. Skorobogatov. "Local Heating Attacks on Flash Memory Devices". In: *IEEE HOST. 2009*.

⁴Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: *IEEE HOST 2019*.

⁵Alexandre Menu et al. "Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation". In: *FDTc 2020*.

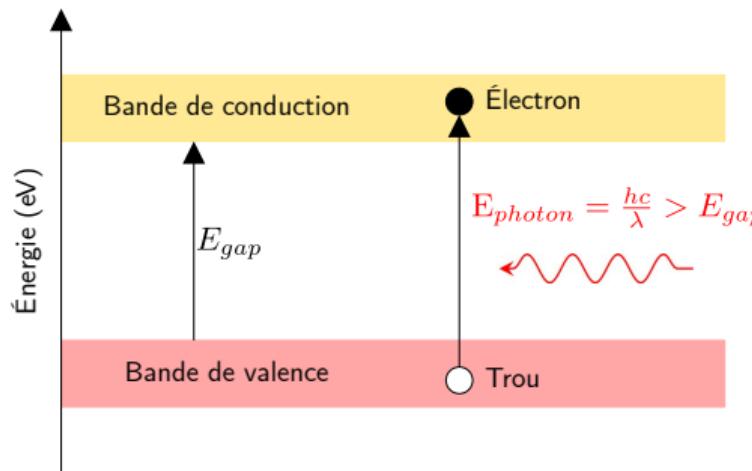
⁶Brice Colombier et al. "Multi-Spot Laser Fault Injection Setup: New Possibilities for Fault Injection Attacks". In: *CARDIS. 2022*.

Effet photoélectrique

$$E_{photon} = \frac{hc}{\lambda}$$

Effet photoélectrique

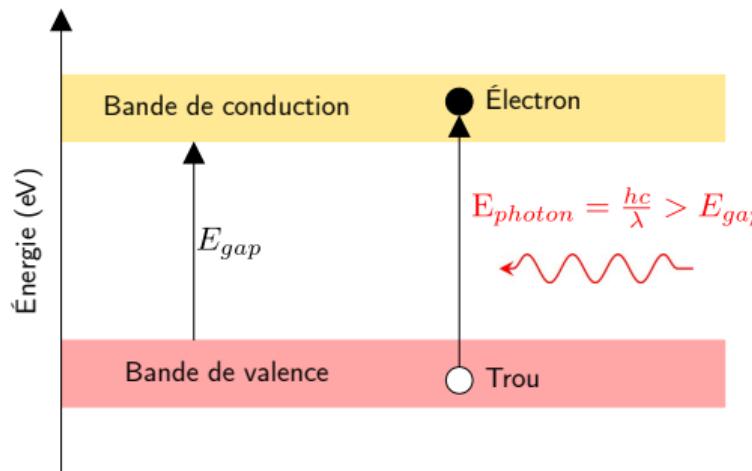
$$E_{photon} = \frac{hc}{\lambda}$$



Effet photoélectrique

$$E_{photon} = \frac{hc}{\lambda}$$

$$E_{photon} > E_{gap} \Rightarrow \lambda < \frac{hc}{E_{gap}} \approx 1100 \text{ nm}$$

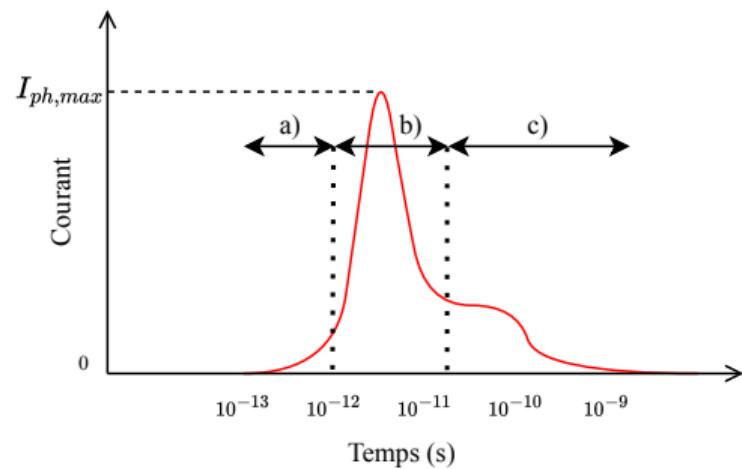
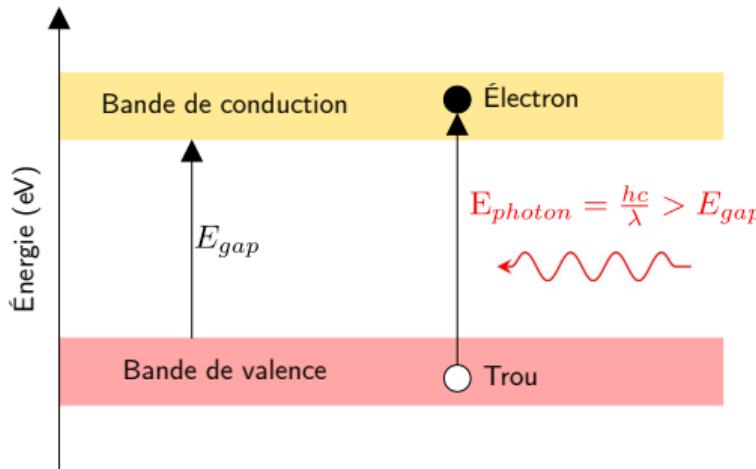


Effet photoélectrique

$$E_{photon} = \frac{hc}{\lambda}$$

$$E_{photon} > E_{gap} \Rightarrow \lambda < \frac{hc}{E_{gap}} \approx 1100 \text{ nm}$$

Si présence d'un champ électrique :

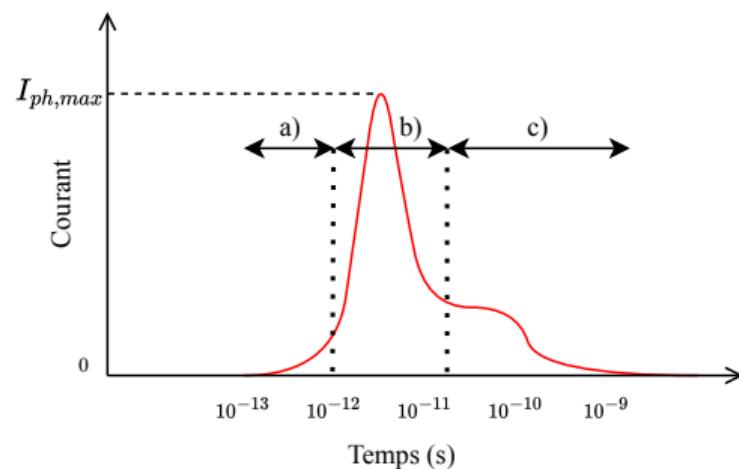
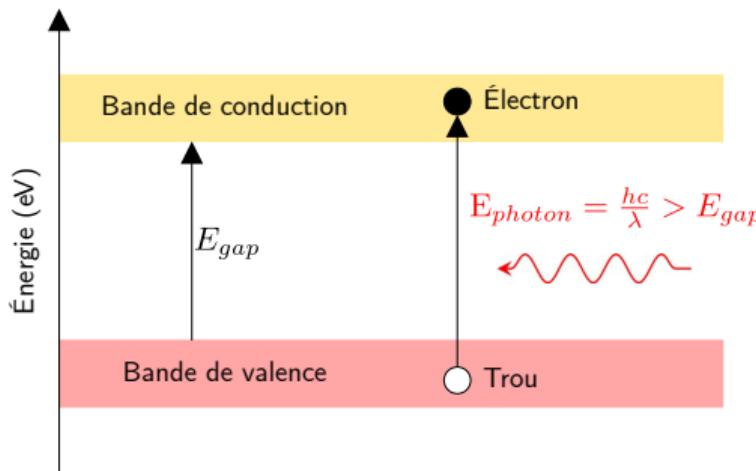


Effet photoélectrique

$$E_{photon} = \frac{hc}{\lambda}$$

$$E_{photon} > E_{gap} \Rightarrow \lambda < \frac{hc}{E_{gap}} \approx 1100 \text{ nm}$$

Si présence d'un champ électrique :

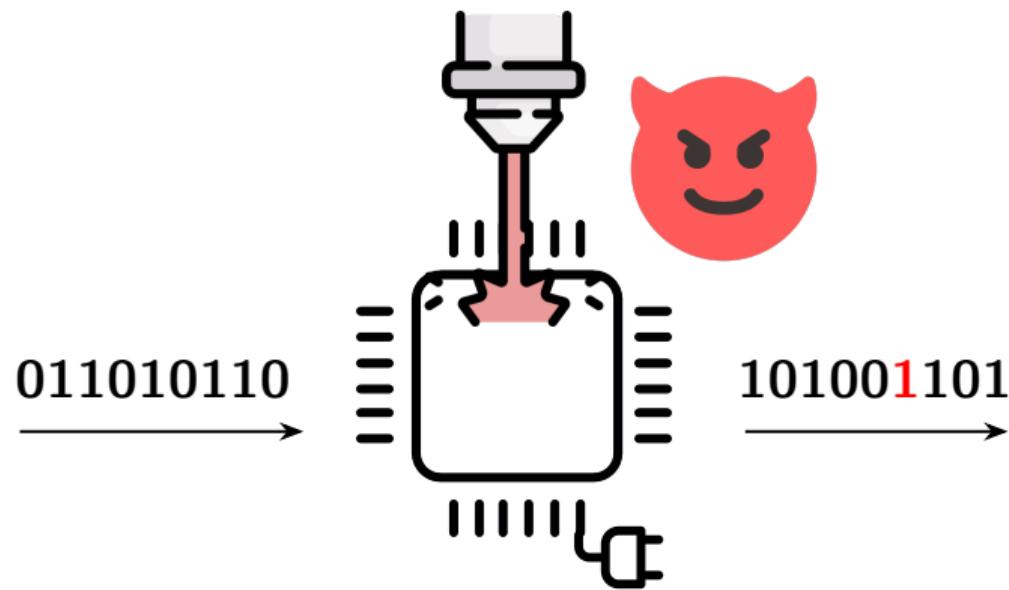


Effet thermique également présent à 1064 nm

Contexte

État de l'art

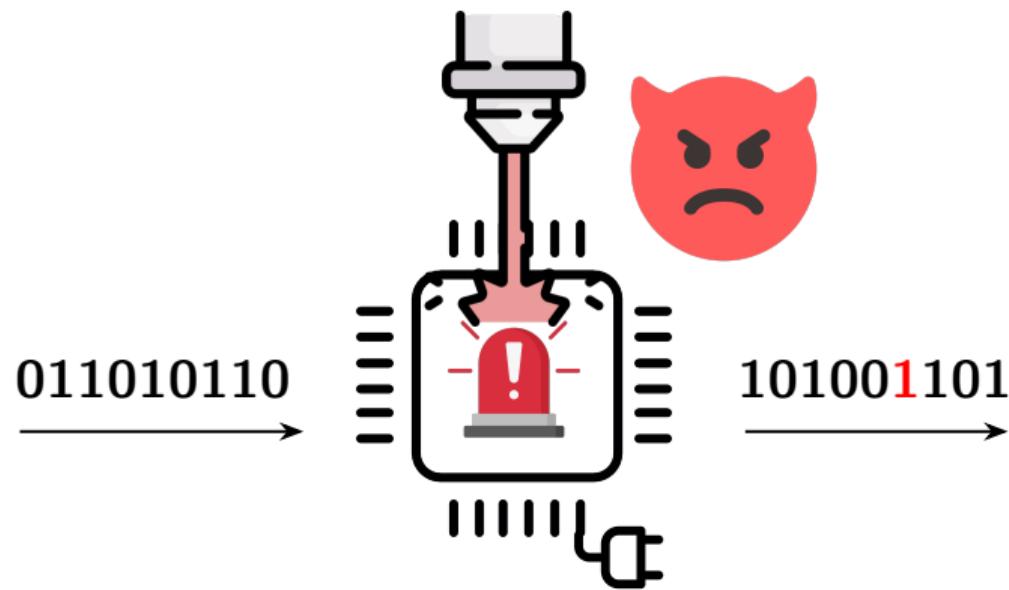
Quasiment toutes les attaques sont menées sur des circuits alimentés



Contexte

État de l'art

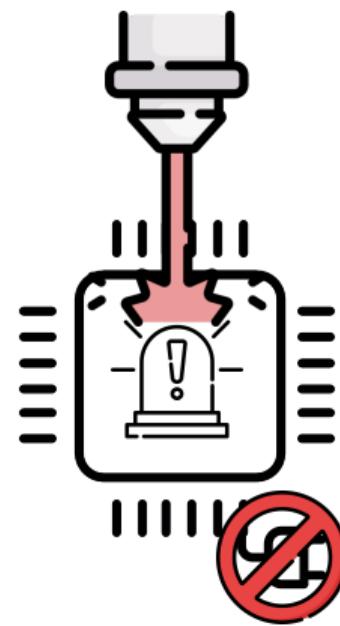
Quasiment toutes les attaques sont menées sur des circuits alimentés



Contexte

Etat de l'art

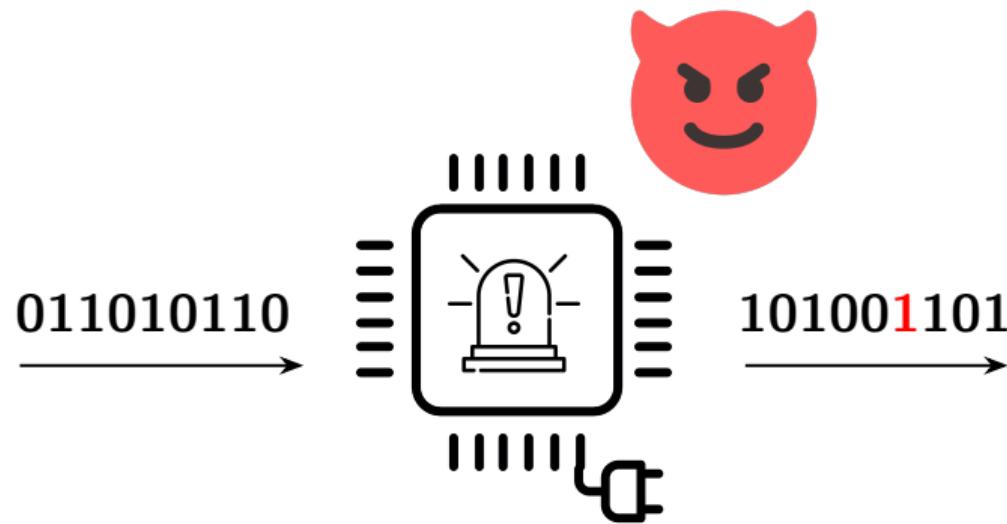
Quasiment toutes les attaques sont menées sur des circuits alimentés



Contexte

Etat de l'art

Quasiment toutes les attaques sont menées sur des circuits alimentés



Contexte

Problème

Peut-on injecter des fautes au laser sur des circuits non alimentés?

Projet POP

Attaquer des composants non alimentés

- Pas de détection possible ⇒ Pas de réaction possible
- Pas de synchronisation nécessaire

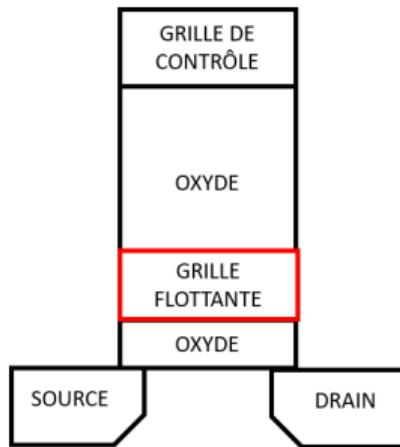


Idée

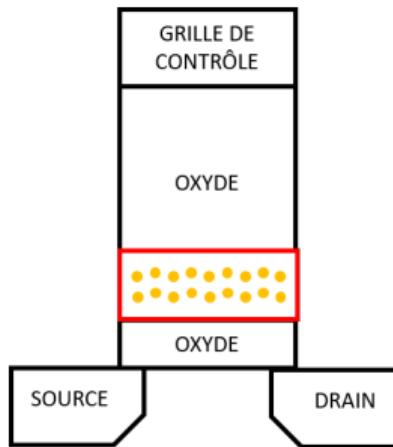
- Corrompre les données stockées : mémoires non-volatiles (Flash)

- ① Fonctionnement des mémoires Flash
- ② Injection laser de fautes sur circuit non alimenté
- ③ Injection de fautes par exposition aux rayons X
- ④ Conclusion

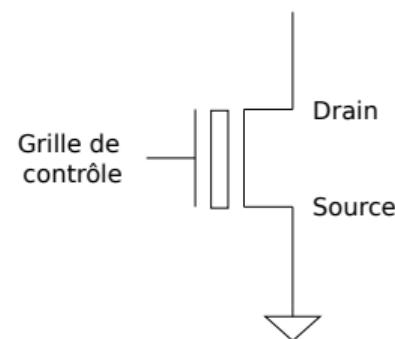
Transistor à grille flottante



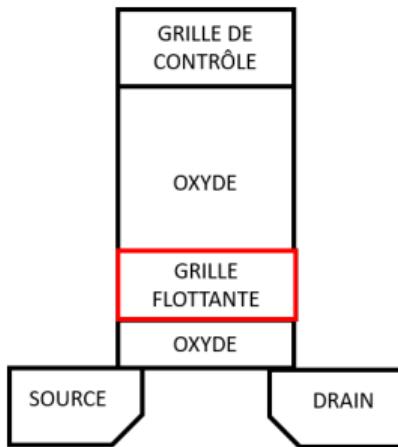
Cellule déchargée



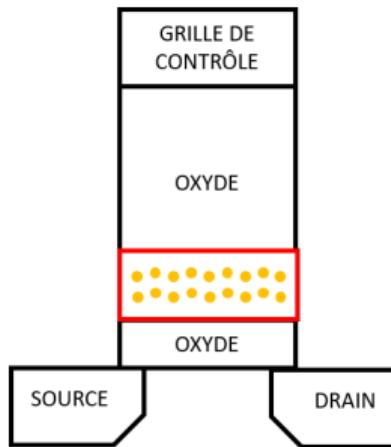
Cellule chargée



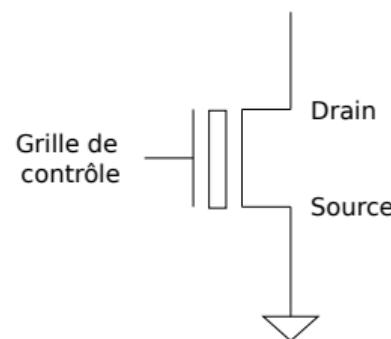
Transistor à grille flottante



Cellule déchargée



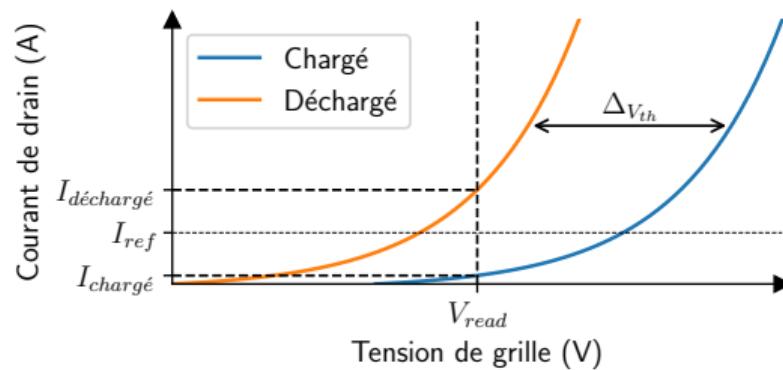
Cellule chargée



Convention :

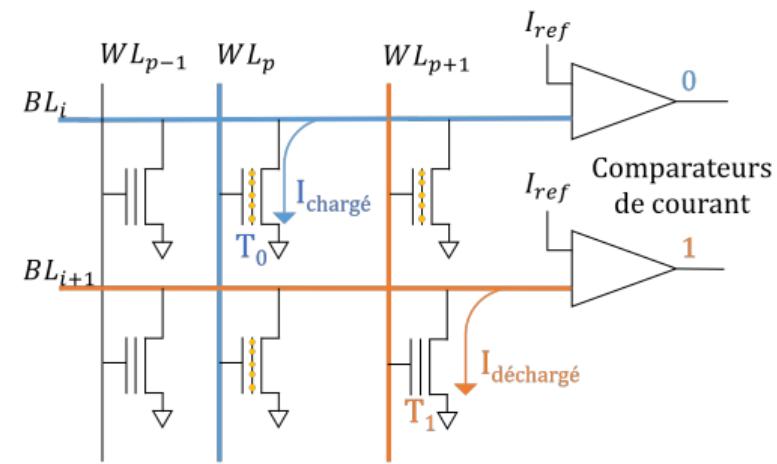
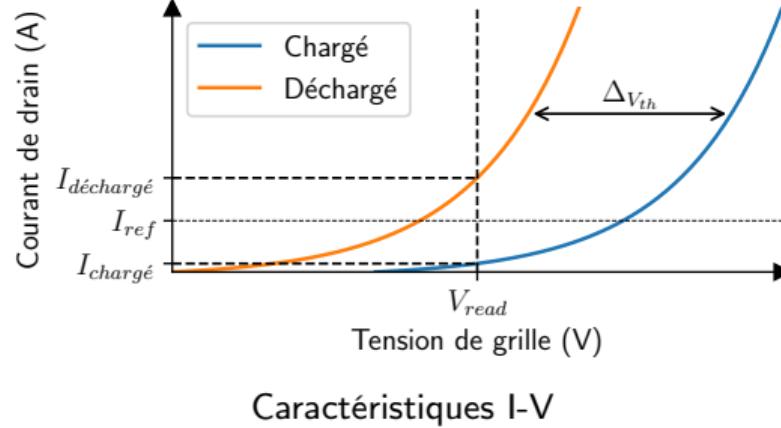
- Chargé = '0'
- Déchargé = '1'

Mécanisme de lecture



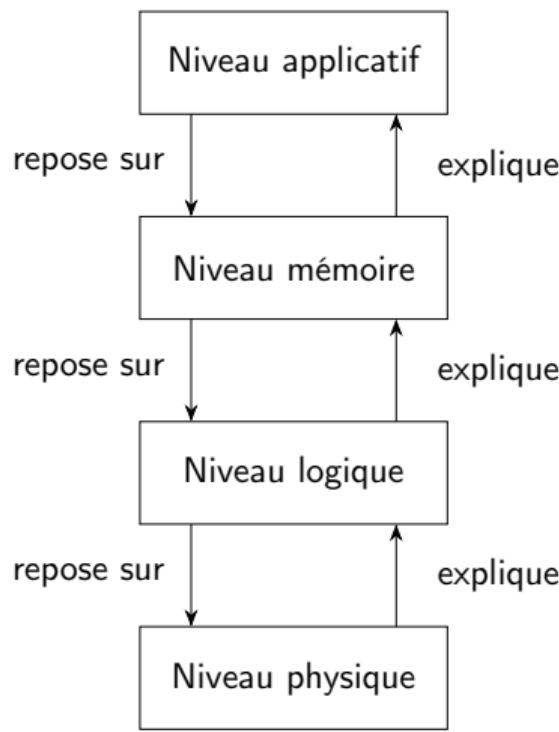
Caractéristiques I-V

Mécanisme de lecture

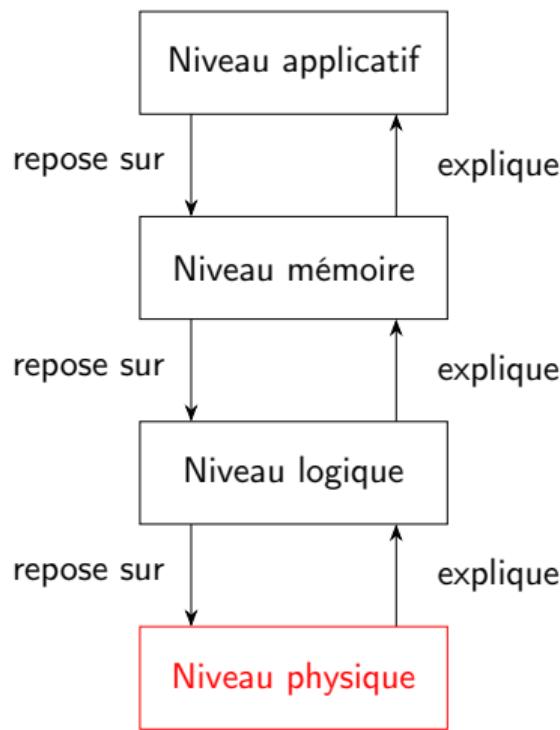


- ① Fonctionnement des mémoires Flash
- ② Injection laser de fautes sur circuit non alimenté
- ③ Injection de fautes par exposition aux rayons X
- ④ Conclusion

Niveaux d'abstraction



Niveaux d'abstraction



Niveau physique

- Énergie du rayon lumineux
- ⇒ Élevation de température
- ⇒ Décharge des transistors à grille flottante^a

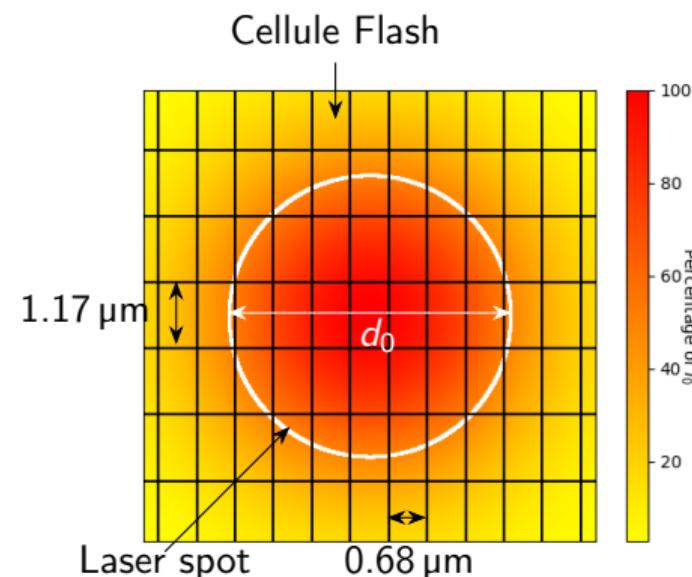
Intensité du faisceau laser :

$$I(r) = I_0 \cdot e^{-\frac{2r^2}{\omega_0^2}} \text{ avec } \omega_0 = \frac{2\lambda}{\pi \times NA}$$

Critère *FWHM* (Largeur à mi-hauteur) ⇒

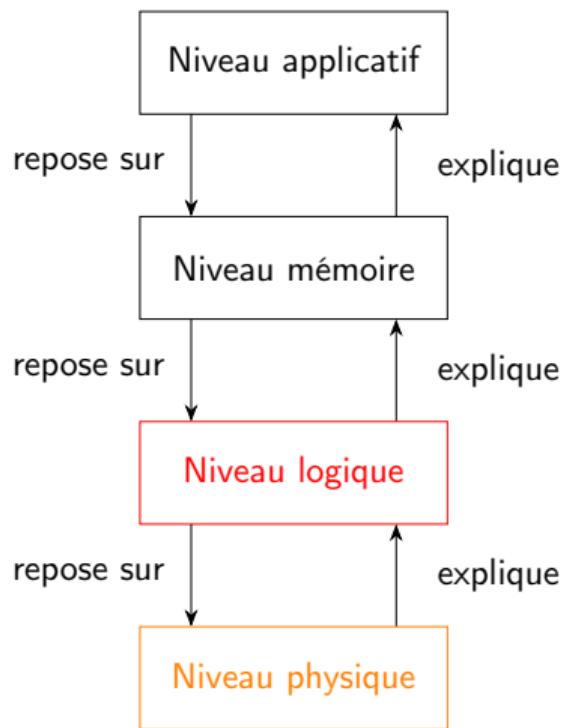
$$d_0 = \omega_0 \sqrt{\frac{\ln 2}{2}} \approx 5 \mu\text{m}$$

^aSergei P. Skorobogatov. "Local Heating Attacks on Flash Memory Devices". In: IEEE HOST. 2009.



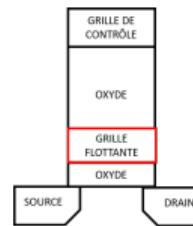
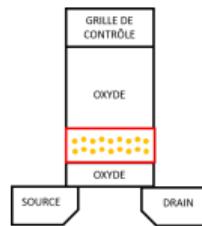
Carte thermique induite par l'exposition laser
(simulation numérique avec $\lambda = 1064 \text{ nm}$ et
 $NA = 0.16$)

Niveaux d'abstraction



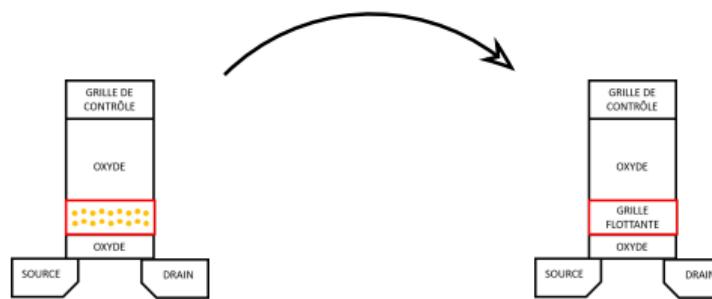
Niveau logique

Du niveau physique :



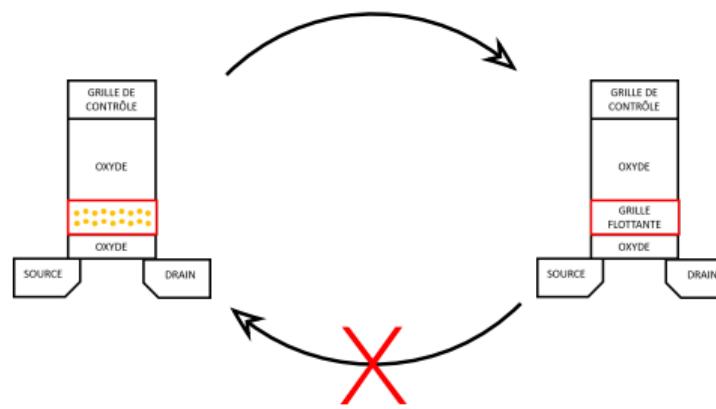
Niveau logique

Du niveau physique :



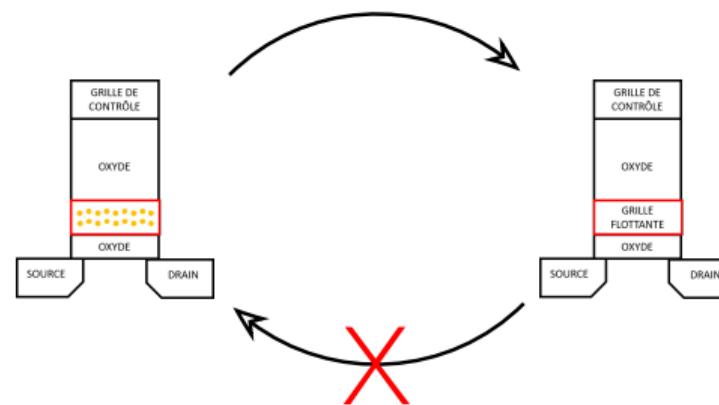
Niveau logique

Du niveau physique :



Niveau logique

Du niveau physique :



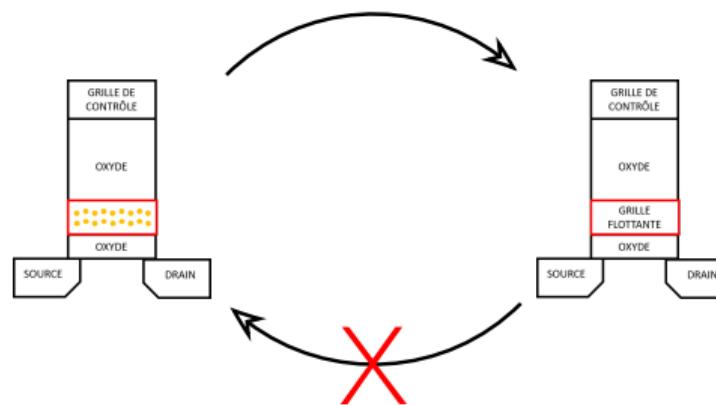
Au niveau logique :

'0'

'1'

Niveau logique

Du niveau physique :

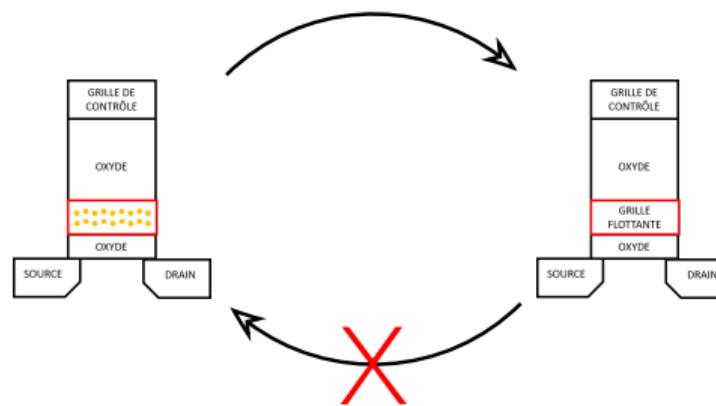


Au niveau logique :



Niveau logique

Du niveau physique :

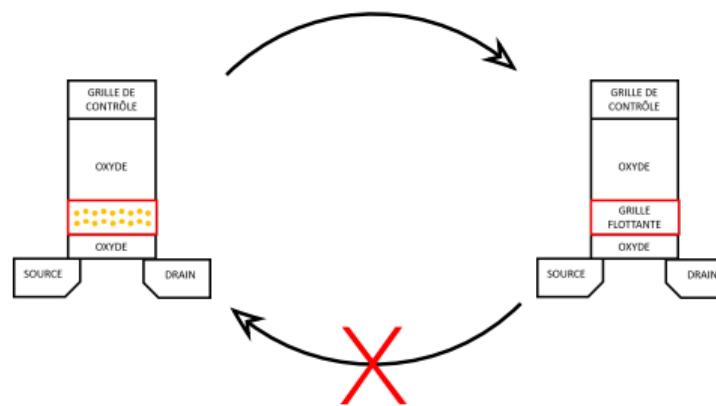


Au niveau logique :

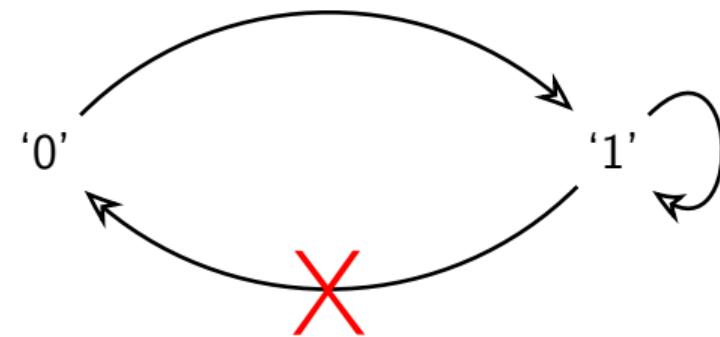


Niveau logique

Du niveau physique :

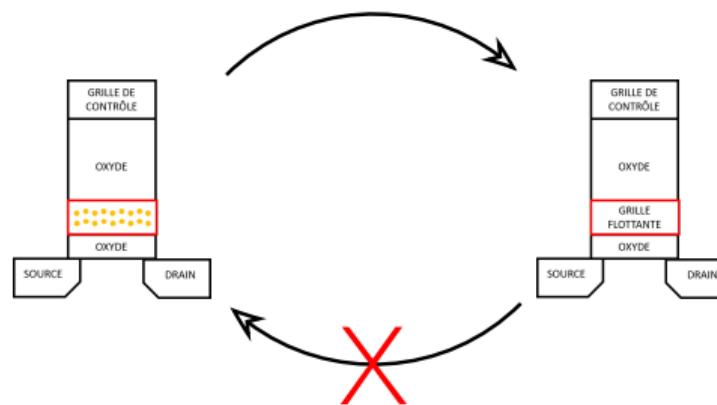


Au niveau logique :

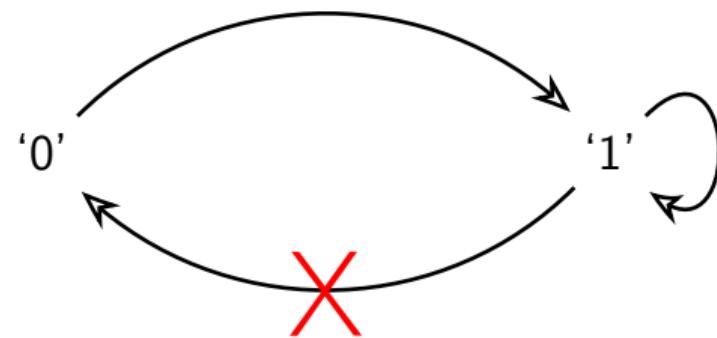


Niveau logique

Du niveau physique :



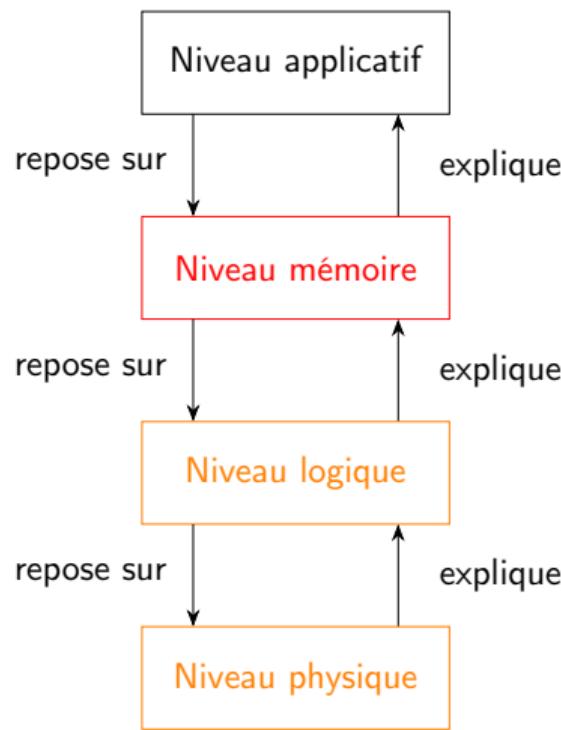
Au niveau logique :



⇒ Modèle de faute unidirectionnel et data-dépendant

- ⇒ Bitsets pour notre cible
- ⇒ Fautes permanentes (possibilité de reprogrammer la mémoire Flash)

Niveaux d'abstraction



Niveau mémoire

Mémoires Flash

- Notamment utilisées pour stocker le code, les constantes, etc.

Niveau mémoire

Mémoires Flash

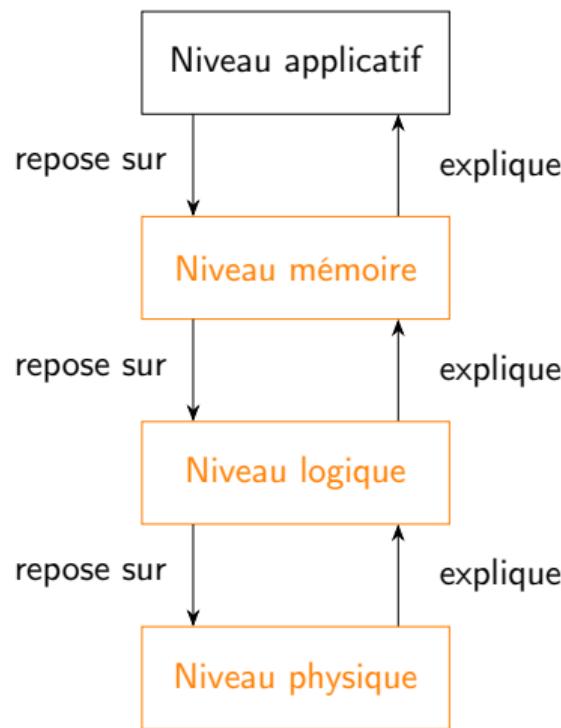
- Notamment utilisées pour stocker le code, les constantes, etc.

Code source

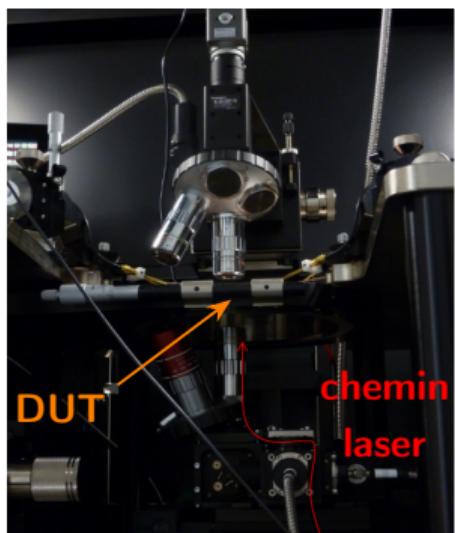
Code stocké en Flash

- Injection de fautes ⇒ Corruption du code

Niveaux d'abstraction



Banc d'injection laser



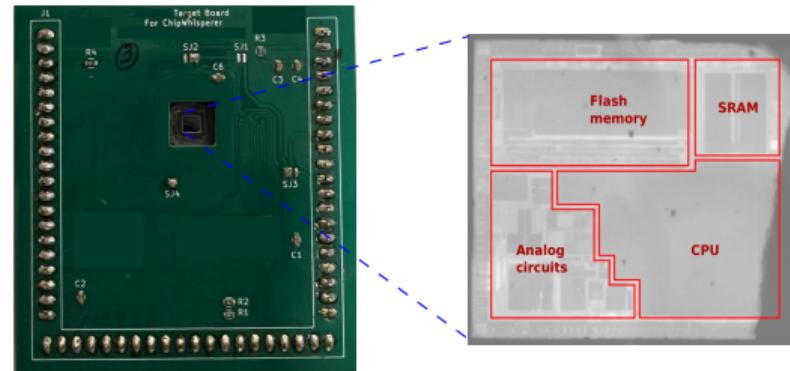
Caractéristiques

- Source laser 1064 nm (proche-IR)
- Impulsion laser de 0.9 s
- Spot de 5 µm avec un grossissement x20
- Vue arrière possible grâce à une caméra infrarouge
- Banc laser couramment utilisé pour l'injection laser sur circuits alimentés

Matériel expérimental

Cible matérielle

- Microcontrôleur 32 bits (Technologie CMOS 80 nm) dédié aux applications IoT
- Coeur ARM Cortex-M3
- 128 kB de mémoire Flash (128 pages de 1 kB)
- Ouvert en face arrière pour avoir un accès au substrat



Cartographie des fautes injectées

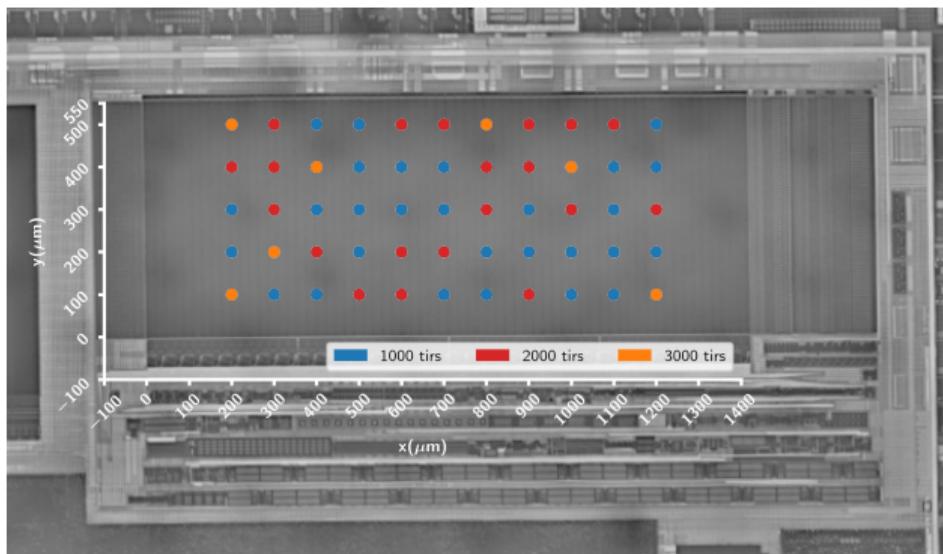
Require: $X_{min}, X_{max}, X_{step}, Y_{min}, Y_{max}, Y_{step}$

```
1: for  $x \in \text{range}(X_{min}, X_{max}, X_{step})$  do
2:   for  $y \in \text{range}(Y_{min}, Y_{max}, Y_{step})$  do
3:     Initialisation de la mémoire
4:     do
5:       Déplacement du laser vers  $(x,y)$ 
6:       Extinction de la cible
7:       for  $i \in [0, \dots, 999]$  do
8:         Tir laser
9:         Alimentation de la cible
10:        Lecture de la mémoire
11:        while #faults == 0
12:          mapping[x][y] = #faults
13: return mapping[x][y]
```



Carte de sensibilité au laser

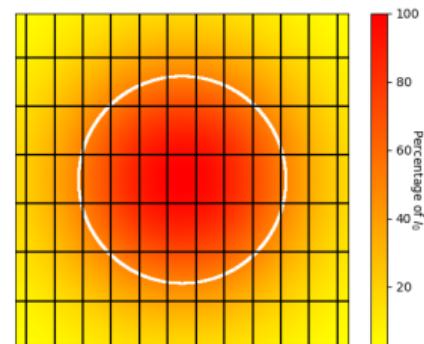
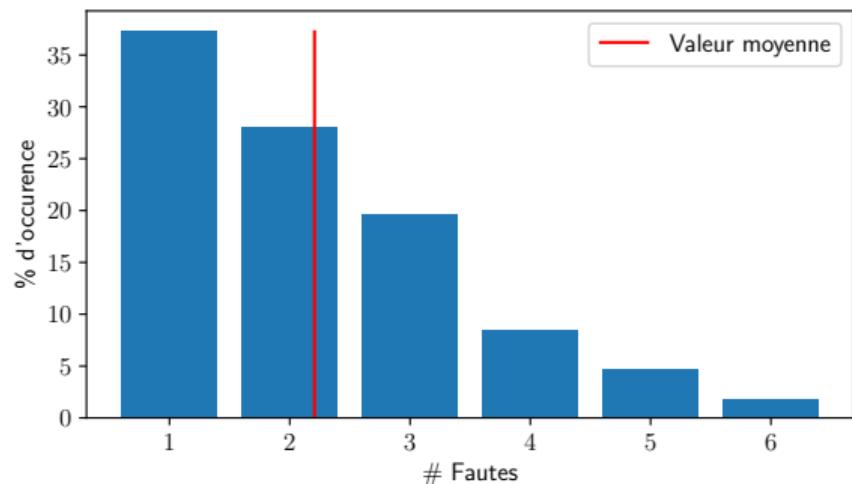
- Mémoire initialisée à 0x00000000 (programmée) avant l'exposition au laser



Cartographie des fautes injectées. $P_{laser} = 1 \text{ W}$, $f_{laser} = 1 \text{ Hz}$, $T_{pulse} = 0.9 \text{ s}$

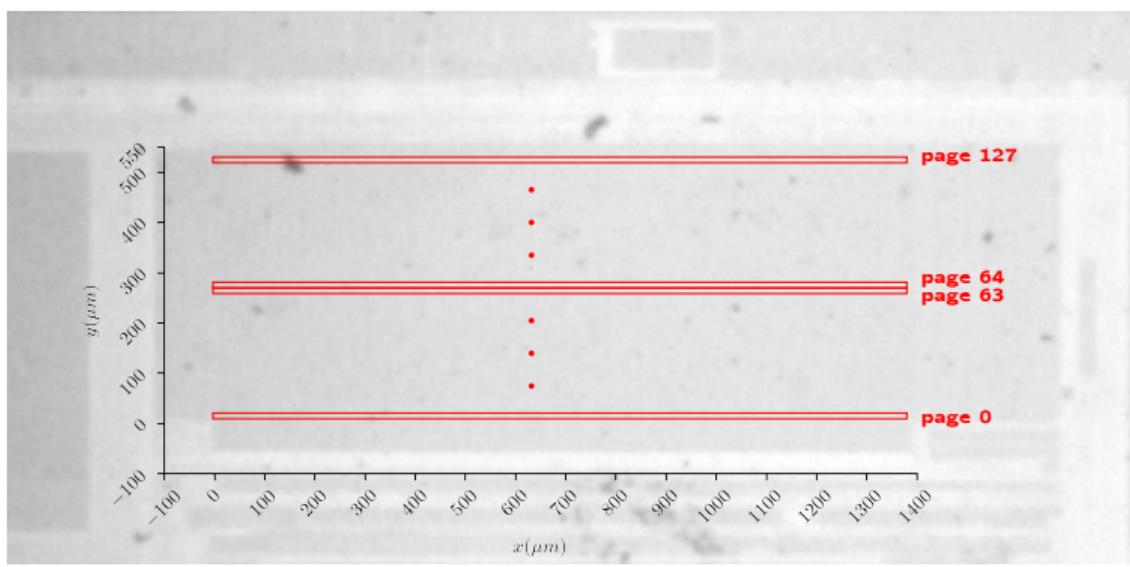
⇒ Valeurs et adresses des fautes (uniquement des bitsets) connues

Distribution expérimentale



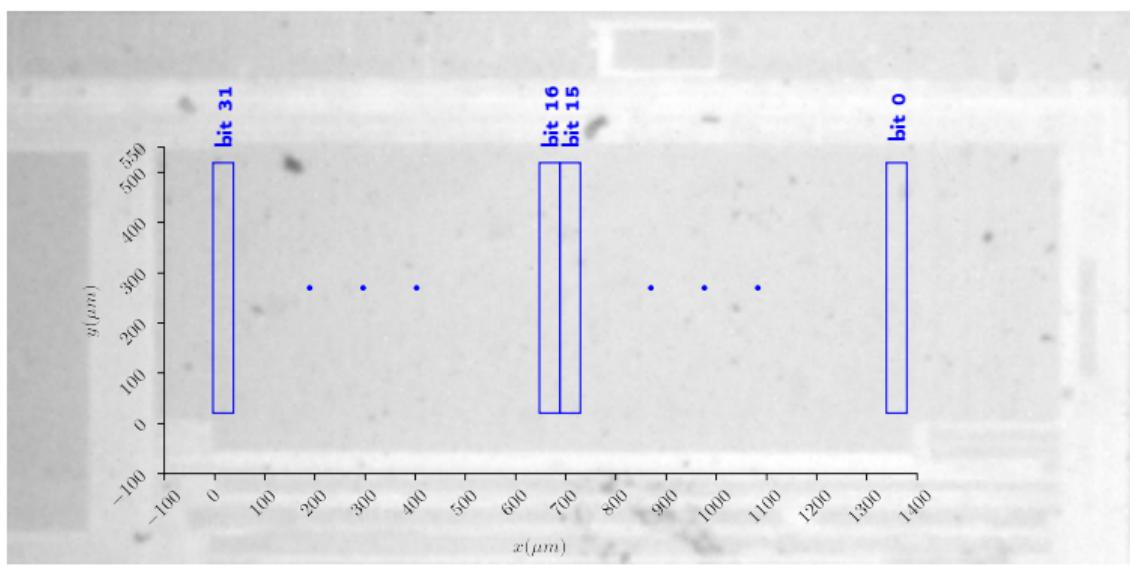
- 2,2 bits fautés en moyenne sur une mémoire initialisée à 0x00000000
- **Fautes monobits** dans 33% des cas
- Pas de corrélation entre #tirs et #fautes

Ingénierie inverse 1/2



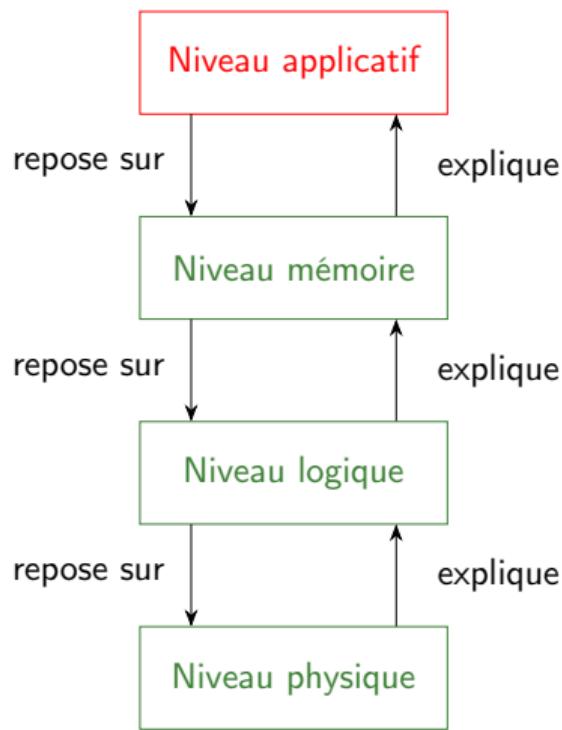
Ingénierie inverse au niveau des pages

Ingénierie inverse 2/2



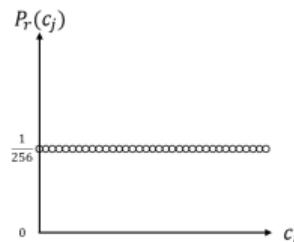
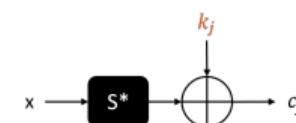
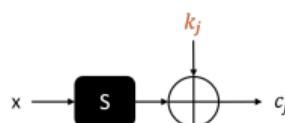
Ingénierie inverse au niveau des bits

Niveaux d'abstraction

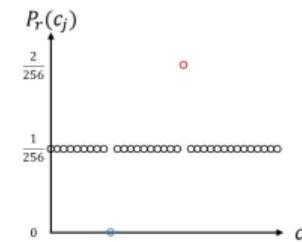


Analyse de Faute Persistante (PFA) : Théorie⁷ (CHES 2018)

- Injection d'une faute permanente dans la boîte de substitution (S-Box)
 - AES : 256 valeurs connues stockées en mémoire Flash
- Étude statistique sur les octets des textes chiffrés
- Exploitation du biais permet de retrouver la clé de chiffrement



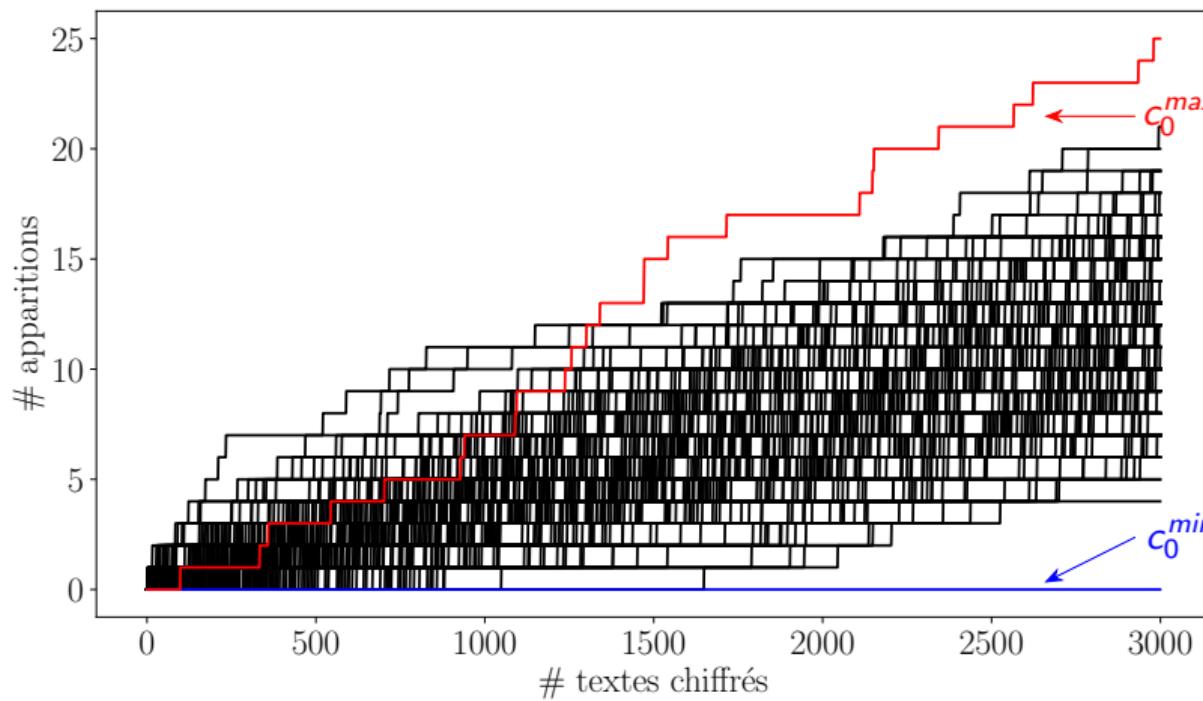
Sans faute



Avec un octet fauté

⁷Fan Zhang et al. "Persistent Fault Analysis on Block Ciphers". In: IACR TCHES. (2018).

Apparition des valeurs d'octets



Résultats expérimentaux (IACR TCHES 2024)

① Ingénierie inverse du *firmware*

⇒ S-box stockée entre les adresses 0x080012F4 et 0x080013F3

② Depuis la cartographie

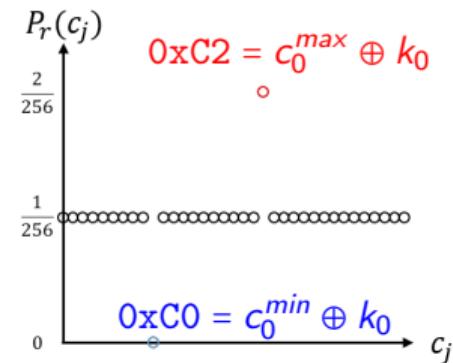
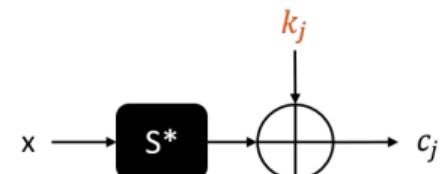
⇒ la position (x,y) = (44.3,300) est dans la S-Box

③ Injection laser de fautes sur circuit non alimenté

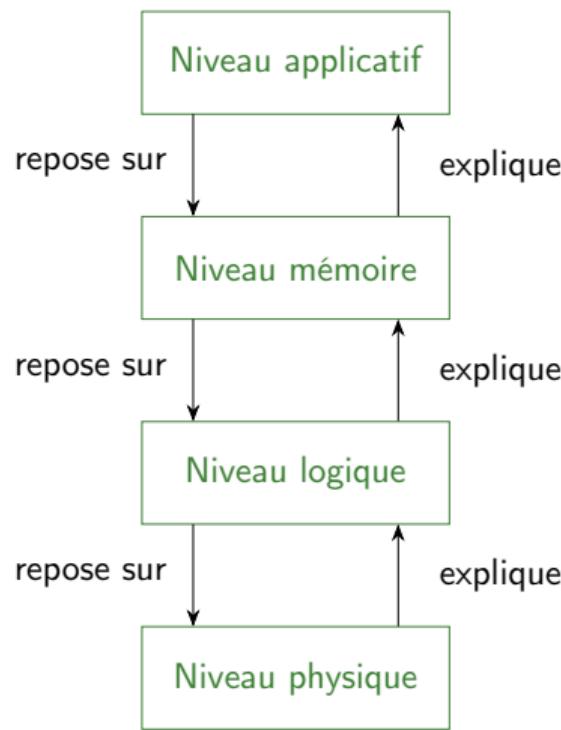
⇒ faute 0x00000002 à l'adresse 0x08001310
32^{ème} valeur de la S-box fautée (0xC2 au lieu de 0xC0)

PFA réussie

Première réalisation expérimentale de la PFA sur circuit éteint



Niveaux d'abstraction



Conclusion

Synthèse

- Injection de fautes au sein de composants non alimentés
- Possibilité d'injecter des fautes localisées au sein de mémoires Flash au laser
- Fautes monobits, permanentes, de type bitsets
- Description d'un modèle de faute complet
- Mise en oeuvre : Analyse de Fautes Persistantes (PFA)

Conséquences

- Sécurisation des circuits dédiés aux applications IoT (codes EDAC)
- Intérêt de la PFA renforcé
 - Contremesures spécifiques à la PFA⁸

⁸Pierre-Antoine Tissot, Lilian Bossuet, and Vincent Grosso. "BALoo: First and Efficient Countermeasure Dedicated to Persistent Fault Attacks". In: *IEEE IOLTS*. 2023.

- ① Fonctionnement des mémoires Flash
- ② Injection laser de fautes sur circuit non alimenté
- ③ Injection de fautes par exposition aux rayons X
- ④ Conclusion

État de l'art

- Effacement de transistor à grille flottante au sein de composants alimentés à l'aide de rayons X^{9,10,11}

Objectif

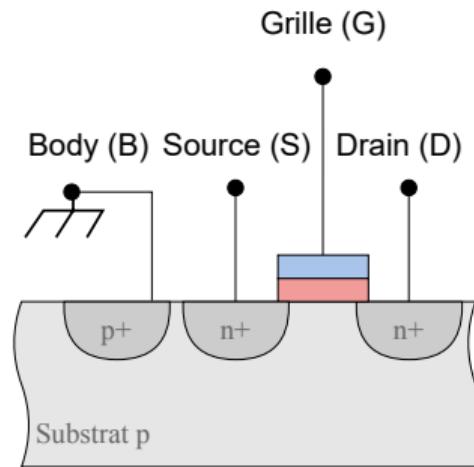
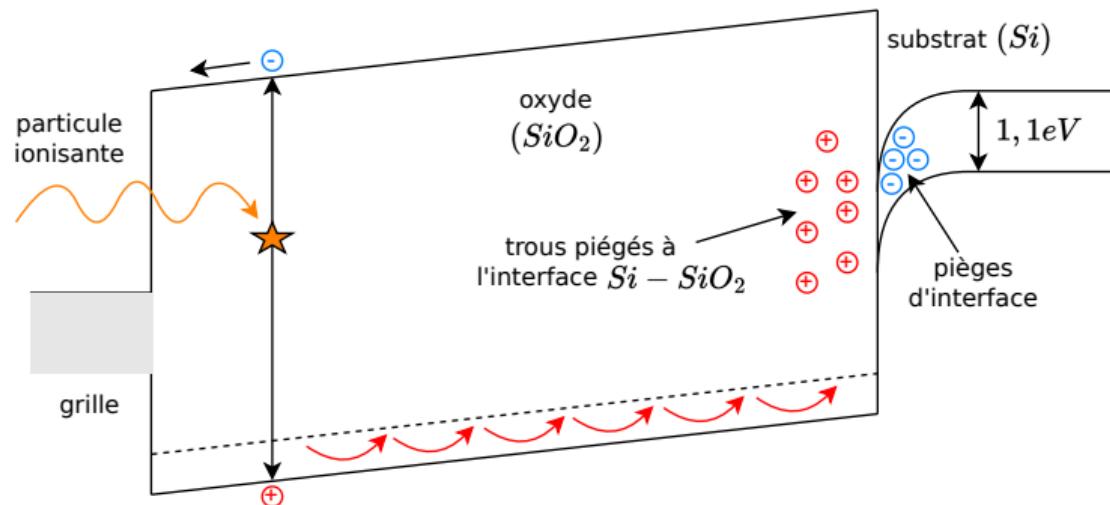
- Évaluer la possibilité d'injecter des fautes au sein de composants non alimentés

⁹Stéphanie Anceau et al. "Nanofocused X-Ray Beam to Reprogram Secure Circuits". In: *IACR TCHES 2017*.

¹⁰Laurent Maingault et al. "Laboratory X-rays Operando Single Bit Attacks on Flash Memory Cells". In: *CARDIS 2021*.

¹¹S. Bouat et al. "X ray nanoprobe for fault attacks and circuit edits on 28-nm integrated circuits". In: *IEEE DFT 2023*.

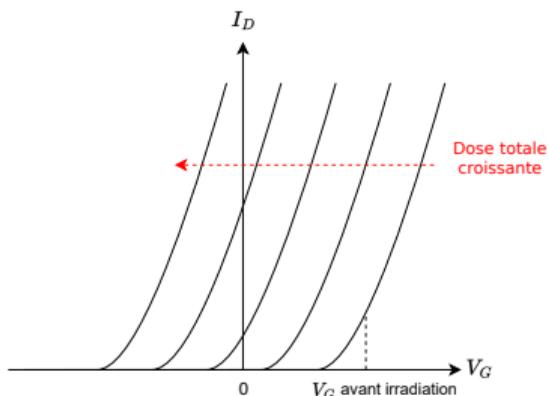
Effet de dose totale sur les transistors MOS¹²



Représentation en bande d'énergie d'une vue en coupe d'un transistor MOS

¹²H. J. Barnaby. "Total-Ionizing-Dose Effects in Modern CMOS Technologies". In: *IEEE Transactions on Nuclear Science* (2006).

Effet de la dose totale sur la caractéristique d'un transistor MOS¹³



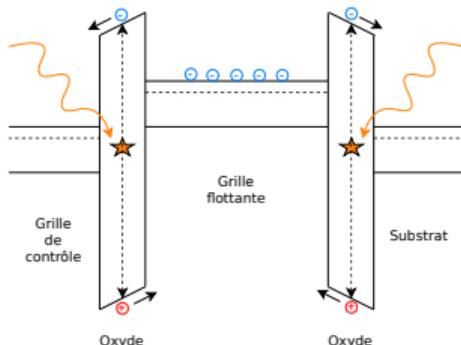
Cas d'un transistor NMOS

Conséquences

- Les NMOS deviennent passants plus facilement, voire de façon permanente
- Les PMOS deviennent bloquants plus facilement, voire de façon permanente

¹³Ashok K. Sharma. *Semiconductor Memories: Technology, Testing and Reliability*. 2002.

Effets de dose totale sur les transistors à grille flottante¹⁴

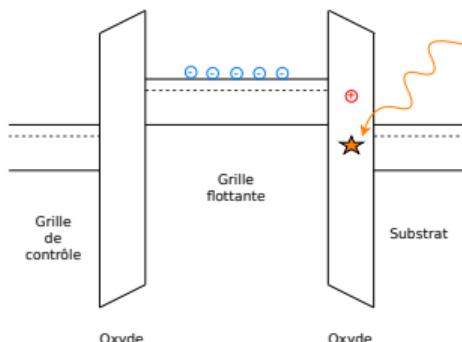


Premier effet

- Création de paires e^+ / h^- par les radiations
- Séparation de ces paires par le champ électrique présent
- Évacuation des électrons par la grille de contrôle
- Injection des trous dans la grille flottante
- Recombinaison avec les charges stockées
- Diminution de la charge stockée

¹⁴S. Gerardin et al. "Radiation Effects in Flash Memories". In: *IEEE Transactions on Nuclear Science* (2013).

Effets de dose totale sur les transistors à grille flottante¹⁴

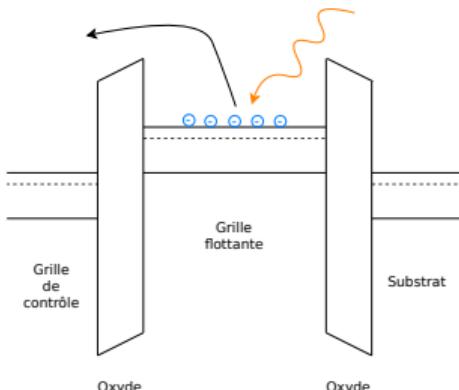


Deuxième effet

- Piégeage des charges dans les oxydes
- Phénomène peu significatif au vu de l'épaisseur des oxydes

¹⁴S. Gerardin et al. "Radiation Effects in Flash Memories". In: *IEEE Transactions on Nuclear Science* (2013).

Effets de dose totale sur les transistors à grille flottante¹⁴

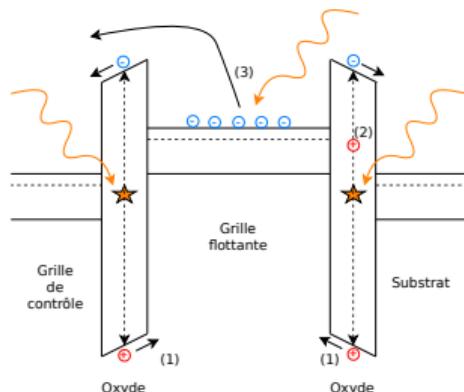


Troisième effet

- Les charges stockées obtiennent assez d'énergie pour franchir la barrière de potentiel
- Diminution de la charge stockée
⇒ Photoémission

¹⁴S. Gerardin et al. "Radiation Effects in Flash Memories". In: *IEEE Transactions on Nuclear Science* (2013).

Effets de dose totale sur les transistors à grille flottante¹⁴

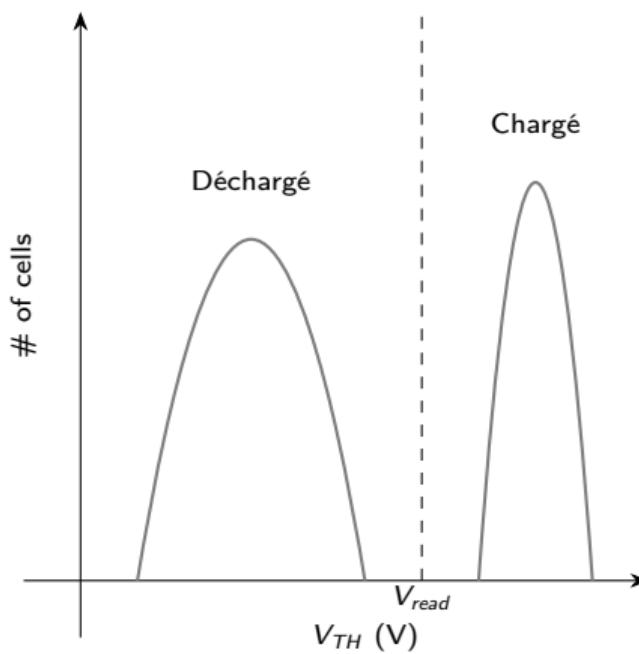


Trois mécanismes distincts :

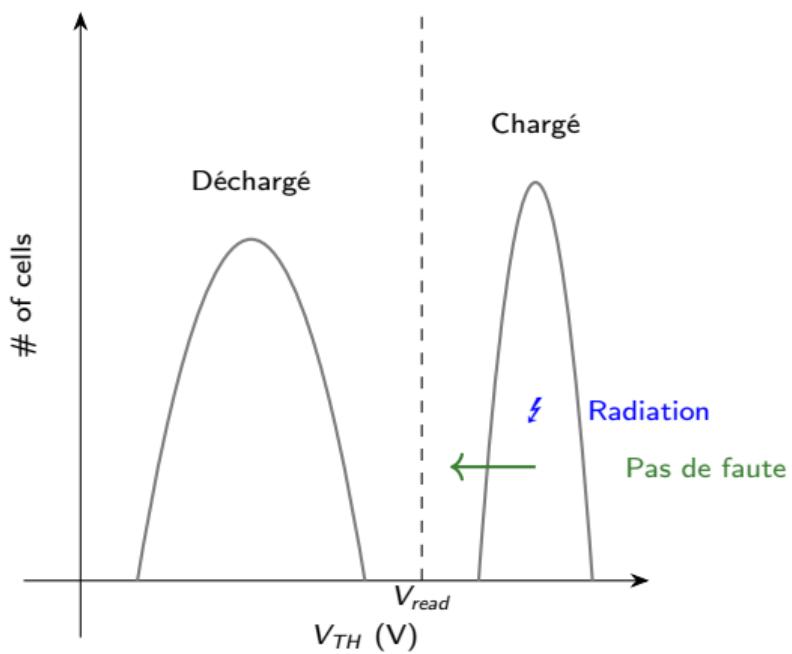
- Génération de paires électron/trou dans les oxydes
- Piégeage de charges dans les oxydes
- Photoémission

¹⁴S. Gerardin et al. "Radiation Effects in Flash Memories". In: *IEEE Transactions on Nuclear Science* (2013).

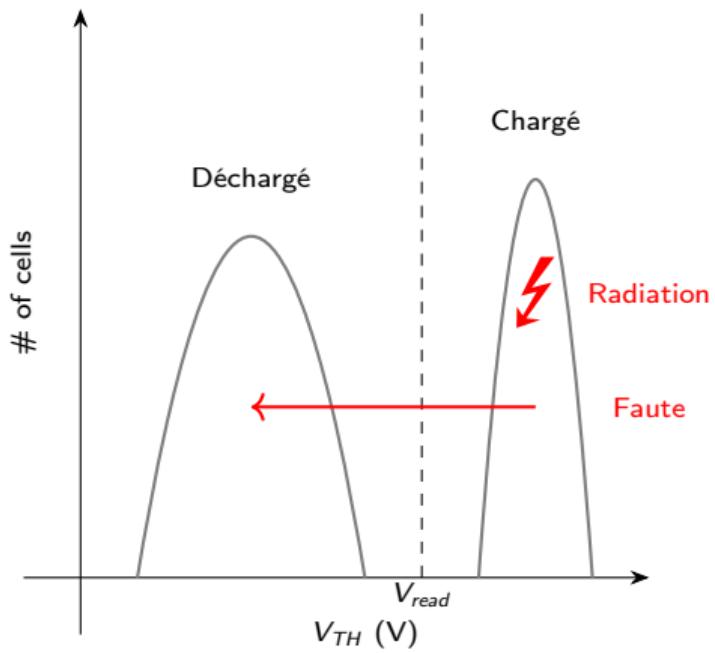
Impact sur la distribution des tensions de seuil



Impact sur la distribution des tensions de seuil

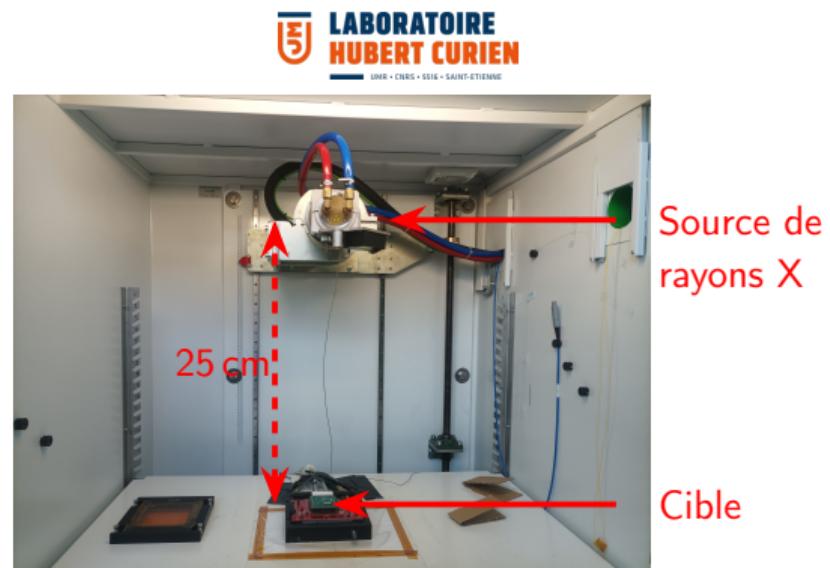


Impact sur la distribution des tensions de seuil



Description du montage expérimental

| | |
|------------------------|---------------------|
| Tube à rayons X | COMET MXR-165 |
| Tension maximale | 160 kV |
| Courant maximal | 45 mA |
| Matériau de l'anode | Tungstène (W) |
| Angle de l'anode | 30° |
| Couverture du faisceau | 50° |
| Filtrage du faisceau | 4 mm Béryllium (Be) |



Toute la cible est irradiée !

Merci à l'équipe MOPERE du laboratoire Hubert Curien !

P. Grandamme

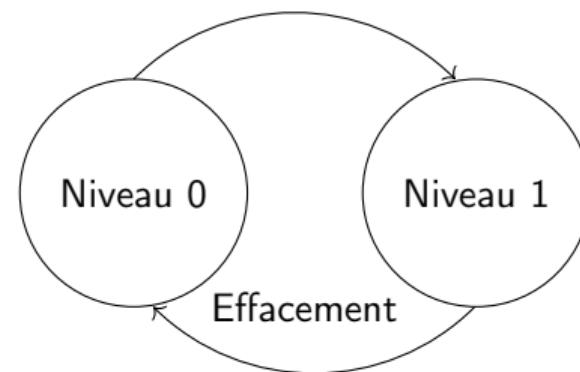
Techniques avancées d'attaques par injection de fautes sur circuits intégrés

Soutenance de thèse

Cible

2 niveaux de protection en lecture

- Niveau 0 : Aucune restriction
- Niveau 1 : Lecture de la Flash impossible lorsque le *debugger* est connecté



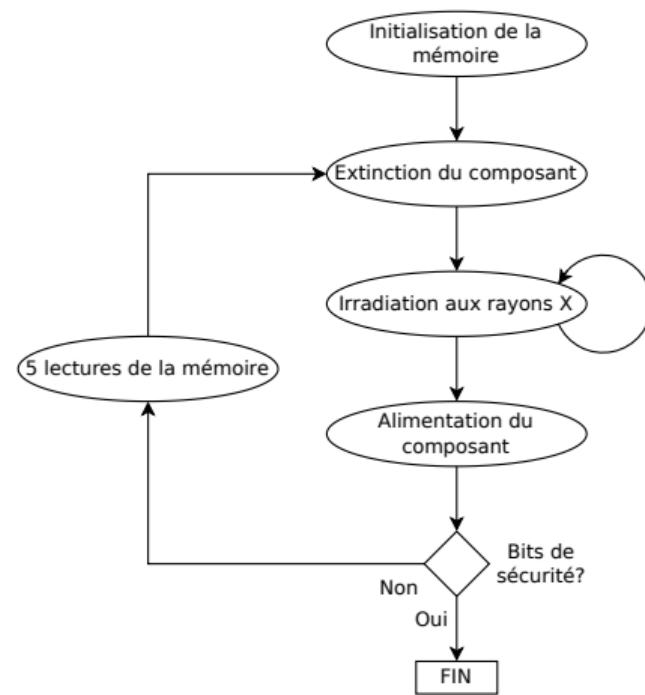
| RDP | nRDP | Statut | Niveau |
|------|-------------|-----------------------------------|--------|
| 0xFF | 0xFF | Protégé | 1 |
| 0xA5 | 0x5A | Non protégé | 0 |
| 0xXY | \neq 0xXY | Protégé | 1 |
| 0xXY | 0xXY | Non précisé dans la documentation | ? |

Table 1: Statut de la protection de la mémoire Flash selon les valeurs de RDP et nRDP

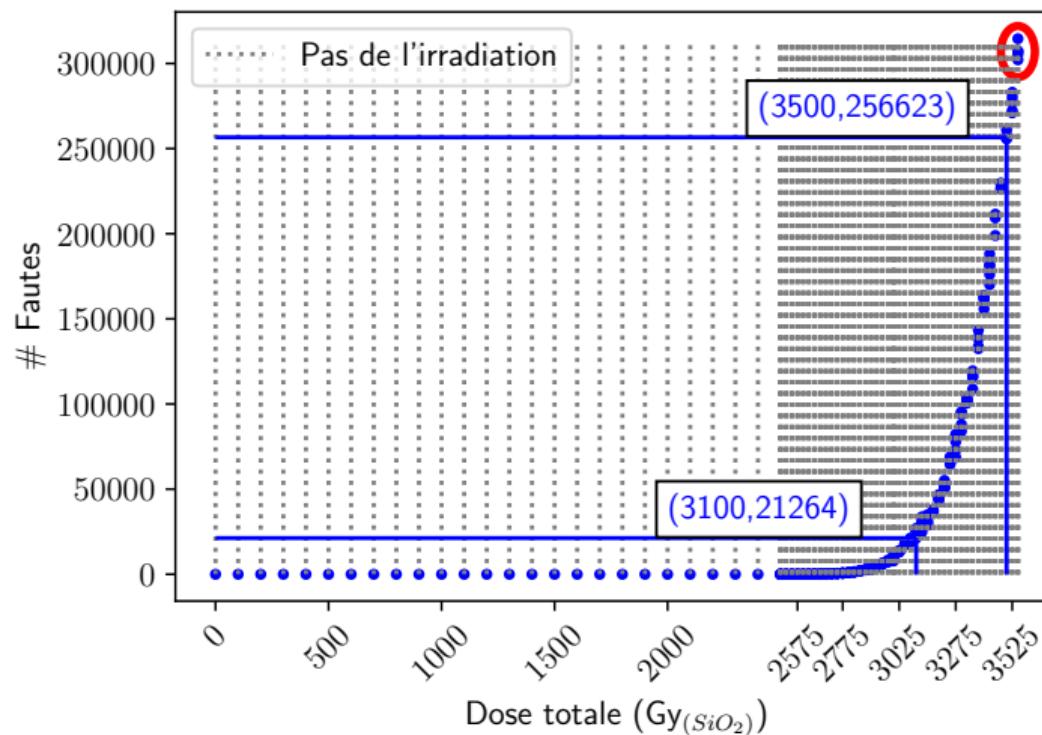
Protocole expérimental

Paramètres de la source

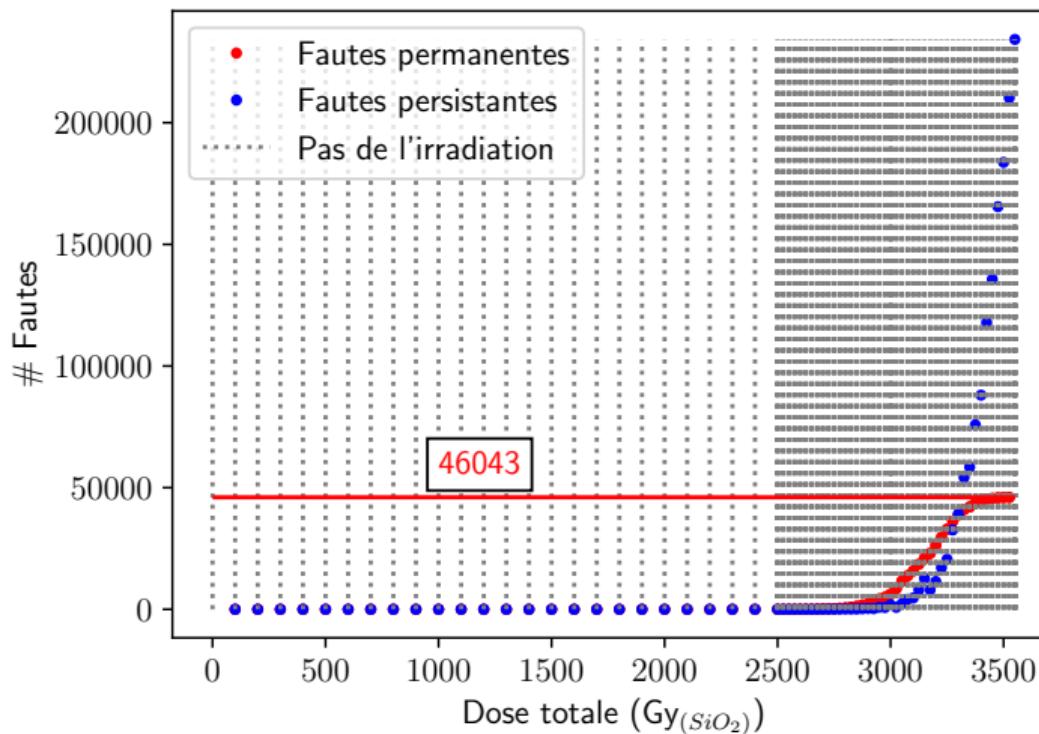
- 100 kV et 45 mA
- ⇒ Photons avec une énergie de 40 keV
- Débit de dose : $1 \text{ Gy}_{(SiO_2)}/\text{s}$



Résultats (Flash)

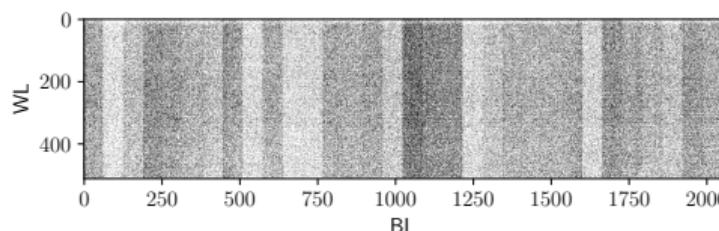


Résultats (Flash)



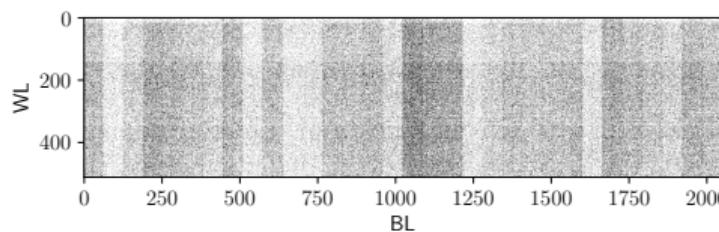
Phénomènes de récupération

Après l'irradiation



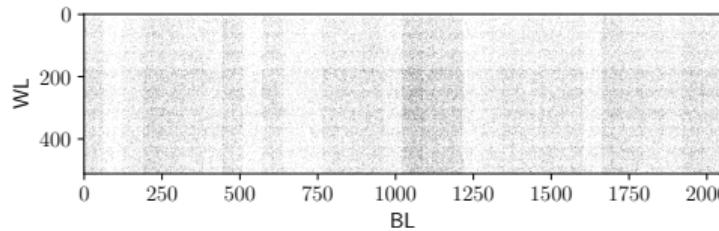
$\approx 300\,000$ fautes

Après récupération
temporelle
7 jours à température ambiante



$\approx 225\,000$ fautes
(-25%)

Après récupération
thermique
2h à 150 °C



$\approx 70\,000$ fautes
(-69%)

Synthèse (IEEE PAINÉ 2023)

Deux types de fautes

- Décharge des transistors à grille flottante par photoémission
- Dérive des tensions de seuils des transistors MOS par piégeage de charges
 - Récupérations temporelle et thermique possible

Limites

- Injection de fautes non localisées donc non exploitables

Synthèse

Deux types de fautes

- Décharge des transistors à grille flottante par photoémission
- Dérive des tensions de seuils des transistors MOS par piégeage de charges
 - Récupérations temporelle et thermique possible

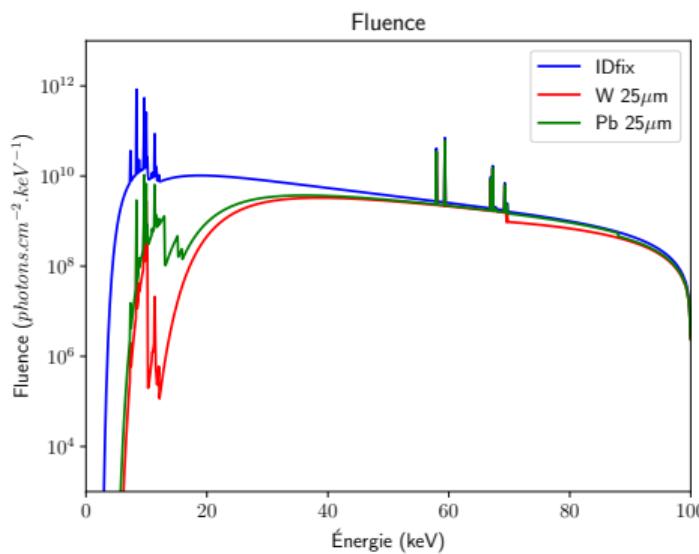
Limites

- Injection de fautes non localisées donc non exploitables

Réalisation d'un masque de focalisation

- Deux matériaux possibles:
 - Tungstène (W)
 - Plomb (Pb)

Simulation des masques



| Masque | Atténuation globale |
|-------------------------------|---------------------|
| Tungstène (25 μm) | $\simeq 75\%$ |
| Plomb (25 μm) | $\simeq 70\%$ |

Conclusion

Masque en tungstène plus efficace



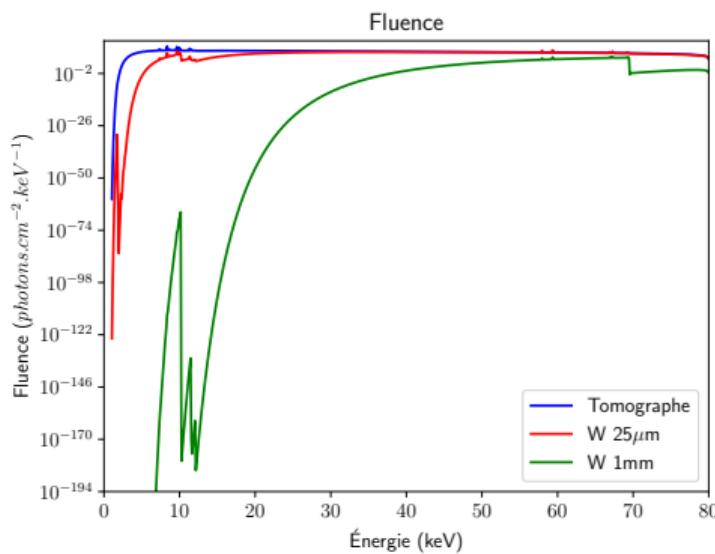
Merci à l'équipe GPM2 du SIMaP et au CEA-Leti pour les masques!

P. Grandamme

Techniques avancées d'attaques par injection de fautes sur circuits intégrés

Soutenance de thèse

Simulation des masques



| Épaisseur | Atténuation globale |
|-----------|---------------------|
| 25 µm | ≤ 80 % |
| 1 mm | ≤ 99.99 % |



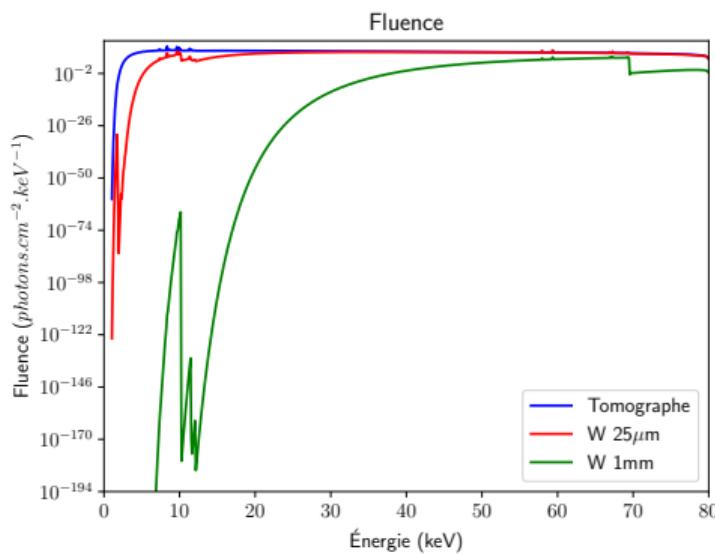
Merci à l'équipe GPM2 du SIMaP et au CEA-Leti pour les masques!

P. Grandamme

Techniques avancées d'attaques par injection de fautes sur circuits intégrés

Soutenance de thèse

Simulation des masques



| Épaisseur | Atténuation globale |
|-----------|---------------------|
| 25 µm | ≤ 80 % |
| 1 mm | ≤ 99.99 % |

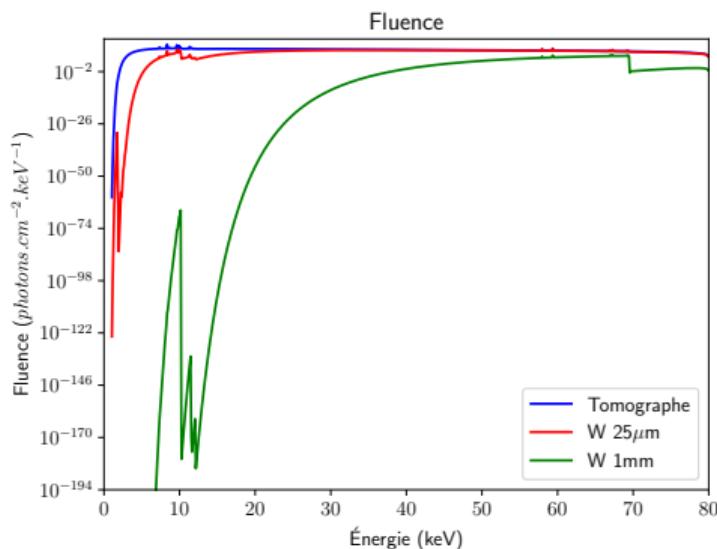
Efficacité des masques

- Conditions expérimentales non propices à l'utilisation du masque 25 µm



Merci à l'équipe GPM2 du SIMaP et au CEA-Leti pour les masques!

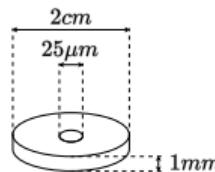
Simulation des masques



| Épaisseur | Atténuation globale |
|-----------|---------------------|
| 25 µm | $\approx 80\%$ |
| 1 mm | $\approx 99.99\%$ |

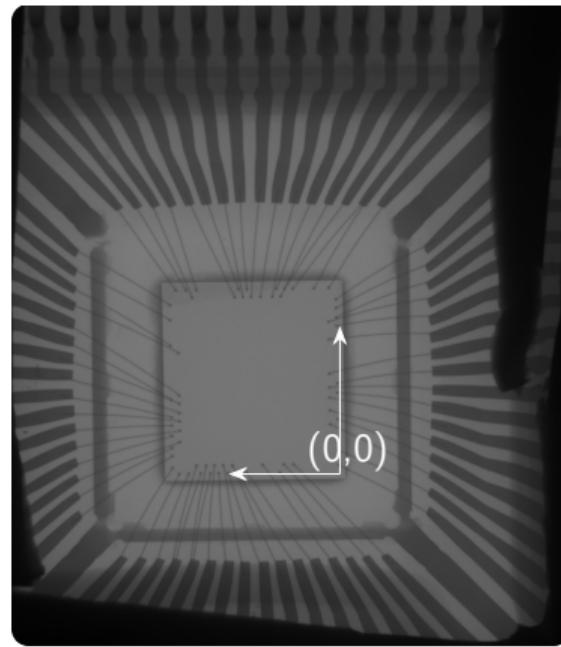
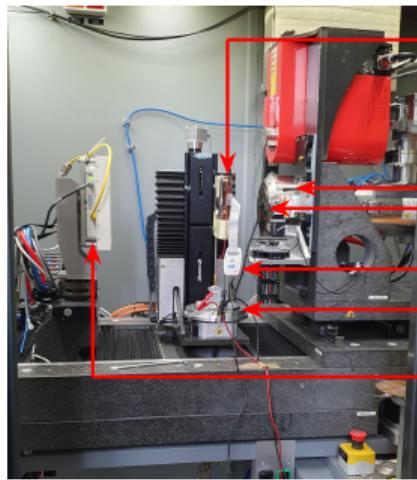
Efficacité des masques

- Conditions expérimentales non propices à l'utilisation du masque 25 µm



Dimensions du masque

Description du tomographe



Merci à l'équipe GPM2 du SIMaP !

P. Grandamme

Techniques avancées d'attaques par injection de fautes sur circuits intégrés

Soutenance de thèse

48 / 61

Images obtenues

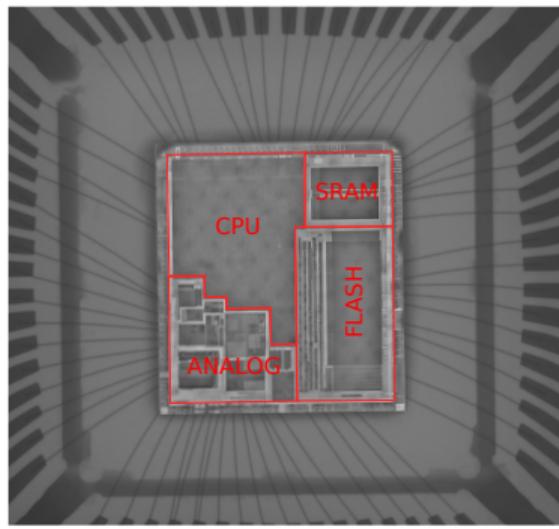
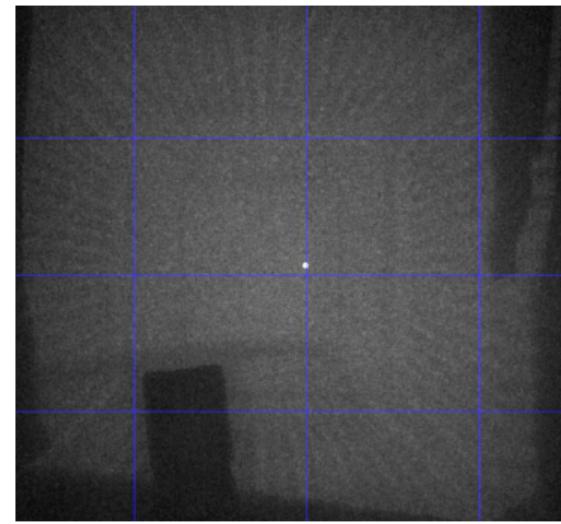


Image infrarouge superposée à l'image obtenue au tomographe

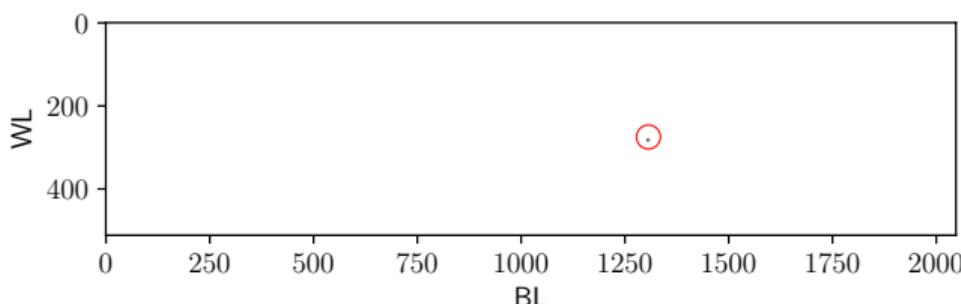


Masque d'épaisseur 1 mm

Campagne d'irradiations : Circuit alimenté

3 positions différentes

- Position ①: (0.6 mm, 1.1 mm)
- Position ②: (0.6 mm, 1.2 mm)
- Position ③: (0.7 mm, 1.2 mm)



Résultats

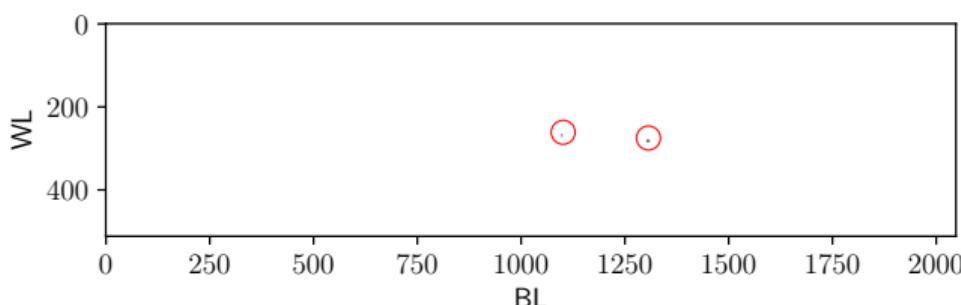
Environ 40 fautes localisées

État de la mémoire Flash après 80 min d'exposition à la première position

Campagne d'irradiations : Circuit alimenté

3 positions différentes

- Position ①: (0.6 mm, 1.1 mm)
- Position ②: (0.6 mm, 1.2 mm)
- Position ③: (0.7 mm, 1.2 mm)



État de la mémoire Flash après 60 min d'exposition à la deuxième position

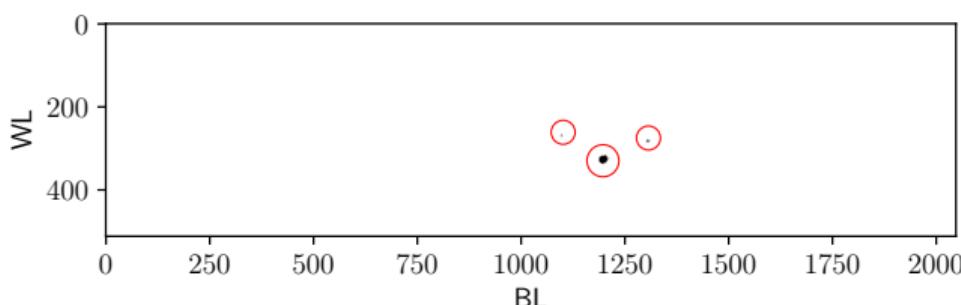
Résultats

Environ 10 fautes localisées

Campagne d'irradiations : Circuit alimenté

3 positions différentes

- Position ①: (0.6 mm, 1.1 mm)
- Position ②: (0.6 mm, 1.2 mm)
- Position ③: (0.7 mm, 1.2 mm)



État de la mémoire Flash après 180 min d'exposition à la troisième position

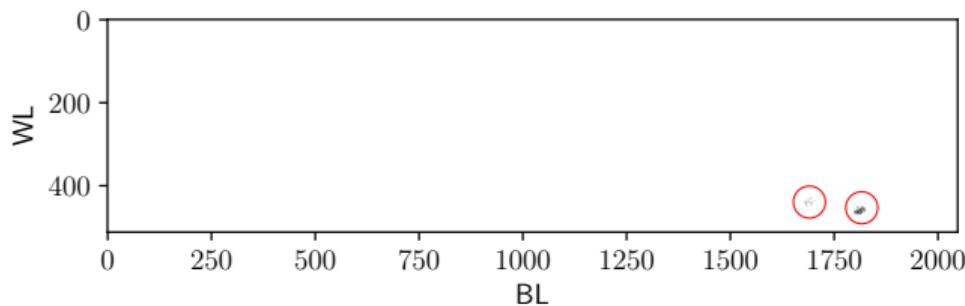
Résultats

Environ 300 fautes localisées

Campagne d'irradiations : Circuit éteint

3 positions différentes

- Position ①: (0.6 mm, 1.2 mm) \Rightarrow 1 h d'irradiation
- Position ②: (0.6 mm, 1.1 mm) \Rightarrow 2 h15 min d'irradiation

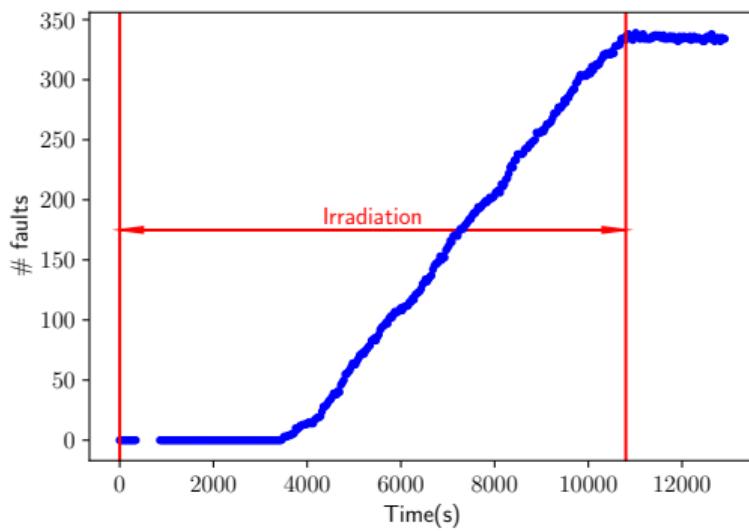


État de la mémoire Flash après les irradiations des deux positions

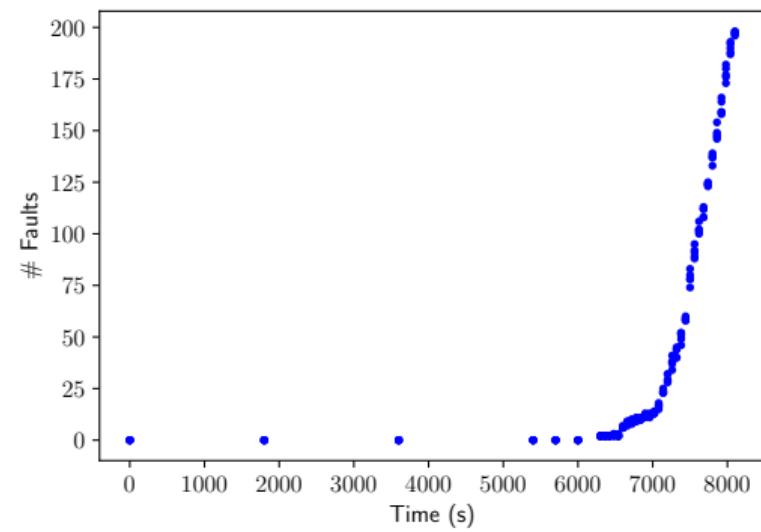
Résultats

- Environ 70 fautes localisées à la position ①
- Environ 300 fautes localisées à la position ②

Évolution temporelle



Circuit alimenté



Circuit éteint

Conclusion

Deux types de fautes

- Décharge des transistors à grille flottante par photoémission
- Dérive des tensions de seuils des transistors MOS par piégeage de charges
 - Récupérations temporelle et thermique possibles (plus efficace)

Focalisation des fautes (soumission en cours)

- Possibilité de focaliser l'injection de fautes en utilisant un masque en tungstène d'épaisseur 1 mm

Limites

- Fabrication des masques contraignent la focalisation
- Peu de scénarios d'attaques sécuritaires envisageables

- ① Fonctionnement des mémoires Flash
- ② Injection laser de fautes sur circuit non alimenté
- ③ Injection de fautes par exposition aux rayons X
- ④ Conclusion

Conclusion

Circuits non alimentés

- Réalité de la menace de ces attaques
- Capteurs matériels ne fonctionnent pas
- Pas de synchronisation nécessaire

Laser

- Nouveau modèle de faute allant du niveau physique au niveau applicatif
- Validation d'un scénario d'attaque de type PFA



Rayons X

- Injection de fautes permanentes et non permanentes
- Possibilité de focaliser l'injection de fautes à l'aide d'un masque



Perspectives

Court terme

- Circuits sécurisés (comportant des contremesures)
 - Capteurs matériels
 - Codes détecteurs et correcteurs d'erreurs
- Circuits reconfigurables (FPGA, SoC-FPGA)
 - Notamment dans le cadre des PUF et TRNG (Oscillateurs en anneau)

Long terme

- Conception de contremesures
 - Capteurs physiques à lecture systématique au démarrage (FGmos sensibles)
 - Spécifiques aux analyses propres aux attaques sur circuits non alimentés

Publication dans un journal international

- Paul Grandamme, Pierre-Antoine Tissot, Lilian Bossuet, Jean-Max Dutertre, Brice Colombier, Vincent Grosso. "**Switching Off your Device Does Not Protect Against Fault Attacks**". IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2024), Septembre 2024.

Conférences internationales avec comité de lecture

- Brice Colombier, Paul Grandamme, Julien Vernay, Émilie Chanavat, Lilian Bossuet, Lucie de Laulanié, Bruno Chassagne. "**Multi-spot laser fault injection setup : New possibilities for fault injection attacks**". 20th Smart Card Research and Advanced Application Conference (CARDIS 2021), Novembre 2021.
- Paul Grandamme, Lilian Bossuet, Jean-Max Dutertre. "**X-Ray Fault Injection in Non-Volatile Memories on Power OFF Devices**". 2023 IEEE Physical Assurance and Inspection of Electronics (PAINE 2023), Octobre 2023.

Présentations à un congrès international sans acte

- Paul Grandamme. "**X-Ray Fault Injection on Power OFF devices**". Cryptographic architectures embedded in logic devices (CryptArchi 2023), Cantabria, Espagne, Juin 2023
- Paul Grandamme. "**Laser Fault Injection on power off devices**". RADLAS 2024 : 6 th Workshop on Laser Testing of Radiation Effects on Components and Systems, Noordwijk, Pays-Bas, Septembre 2024.

Présentations à un congrès national sans acte

- Paul Grandamme. "**X-Ray Fault Injection on Power OFF Devices**". Journée des doctorants de l'équipe SAS, Gardanne, France, Juin 2023.
- Paul Grandamme. "**X-Ray Fault Injection on Power OFF devices**". Journée thématique sur les Attaques par Injection de Fautes (JAIF 2023), Gardanne, France, Septembre 2023.
- Paul Grandamme. "**Éteindre votre composant électronique ne le protège pas !**". Journée thématique sur les Attaques par Injection de Fautes (JAIF 2024), Rennes, France, Octobre 2024.

Posters

- Paul Grandamme. "**Attaque laser de primitives de sécurité non alimentées**". Journée thématique sur les Attaques par Injection de Fautes (JAIF 2022), Valence, France, Novembre 2022.
- Paul Grandamme. "**Injection de fautes dans les circuits électroniques non alimentés**". Journée de la recherche de l'école doctorale EDSIS, Saint-Étienne, France, Juin 2023.
- Paul Grandamme. "**Éteindre votre composant électronique ne le protège pas !**". Journée thématique sur les Attaques par Injection de Fautes (JAIF 2024), Rennes, France, Octobre 2024.

Merci pour votre attention !

Cette thèse est réalisée dans le cadre du projet *Power-Off laser attacks on security Primitives* (POP) ou *Attaques laser de primitives de sécurités non alimentées* financé par l'Agence Nationale de la Recherche (ANR).



Techniques avancées d'attaques par injection de fautes sur circuits intégrés

Paul GRANDAMME
3 Février 2025



Devant le jury composé de :

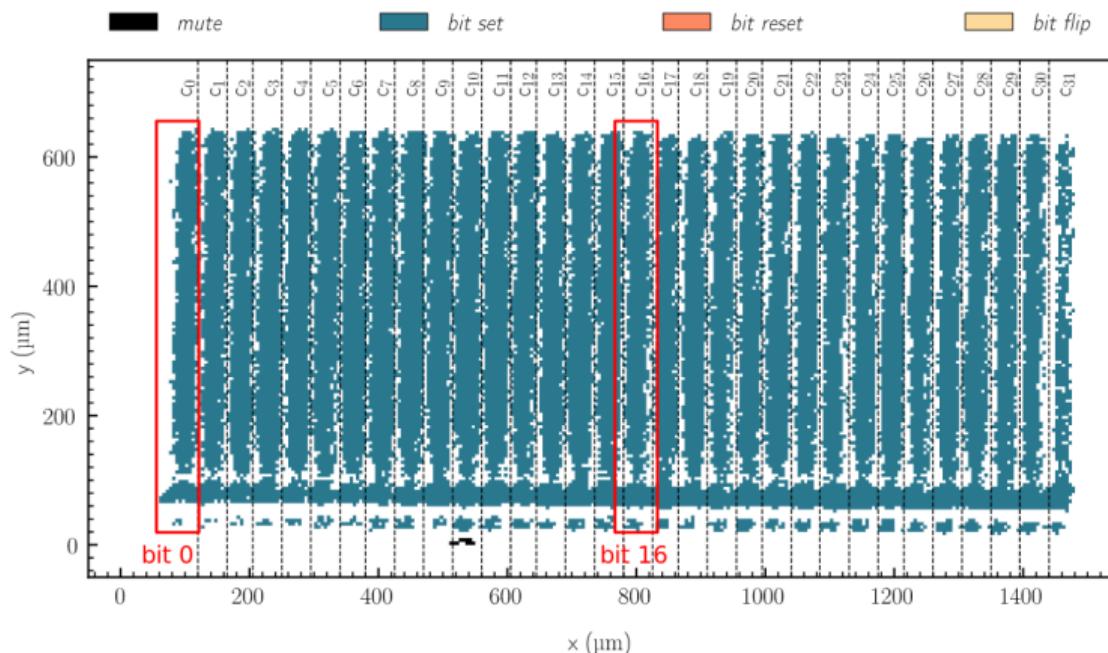
Stéphanie ANCEAU, Examinateuse
Giorgio DI NATALE, Rapporteur
Sylvain GIRARD, Examinateur
Jérémy POSTEL-PELLERIN, Rapporteur
Vincent POUGET, Examinateur
Michel AGOYAN, Invité

Direction de thèse :

Lilian BOSSUET
Jean-Max DUTERTRE



Slides de back-up



Dépendance spatiale des fautes sur la mémoire Flash d'un microcontrôleur STM32F100¹⁵

¹⁵Alexandre Menu. "Sécurité matérielle des objets connectés". Thèse de doctorat. École des Mines de Saint-Étienne, Nov. 2021.

Caractéristiques du modèle de faute

- Direction: bitset, bitreset, bitflip
- Cardinalité: monobit, multibits, octet
- Répétabilité: probabilité que la faute intervienne selon un ensemble de paramètres

⇒ Deux caractéristiques sont manquantes:

- **Contiguïté**
- **Aspect temporel**

Contiguïté

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Faute multibits contiguë: réalisable avec un seul spot laser

Contiguïté

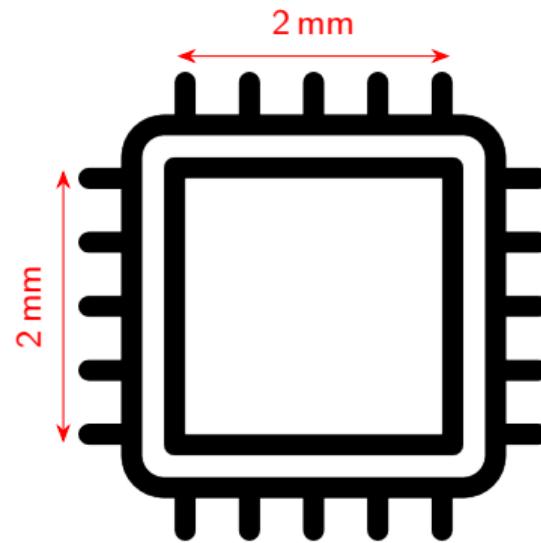
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
| 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Faute multibits contiguë: réalisable avec un seul spot laser

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Faute multibits non contigüe: irréalisable avec un seul spot mais réalisable avec plusieurs spots laser

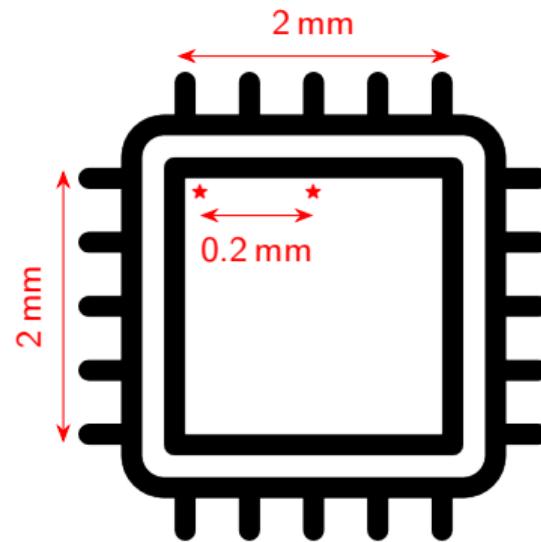
Aspect temporel



Hypothèses:

- Vitesse de déplacement du système mécanique: 20 mm s^{-1}
- Fréquence de l'horloge: 10 MHz

Aspect temporel

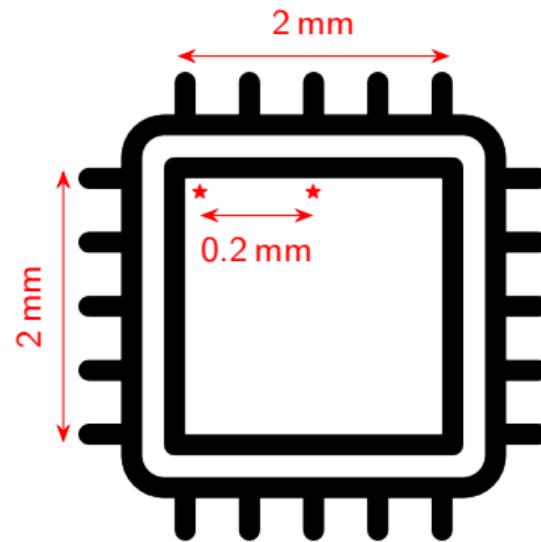


Hypothèses:

- Vitesse de déplacement du système mécanique: 20 mm s^{-1}
- Fréquence de l'horloge: 10 MHz
- Deux positions distantes de 10 % de la puce

$$\begin{aligned}\Delta t_{t,min} &= \frac{d_{target}}{v_{max}} = \frac{2 \times 0.1}{20} \\ &= 0.01 \text{ s} \\ &= 10^5 \text{ périodes d'horloge}\end{aligned}$$

Aspect temporel



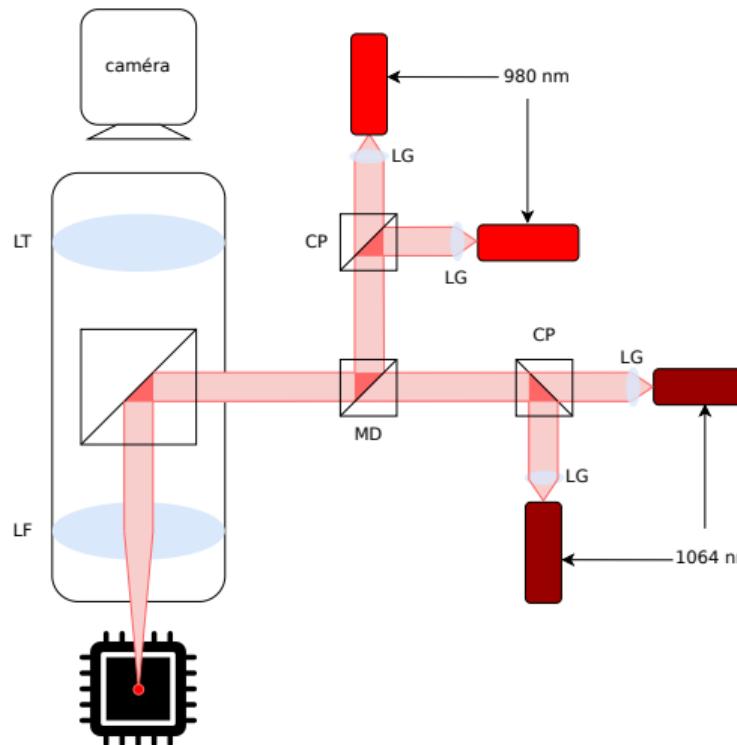
Hypothèses:

- Vitesse de déplacement du système mécanique: 20 mm s^{-1}
- Fréquence de l'horloge: 10 MHz
- Deux positions distantes de 10 % de la puce

$$\begin{aligned}\Delta t_{min} &= \frac{d_{target}}{v_{max}} = \frac{2 \times 0.1}{20} \\ &= 0.01 \text{ s} \\ &= 10^5 \text{ périodes d'horloge}\end{aligned}$$

Conclusion: Deux fautes différentes proches dans le temps sont impossibles !

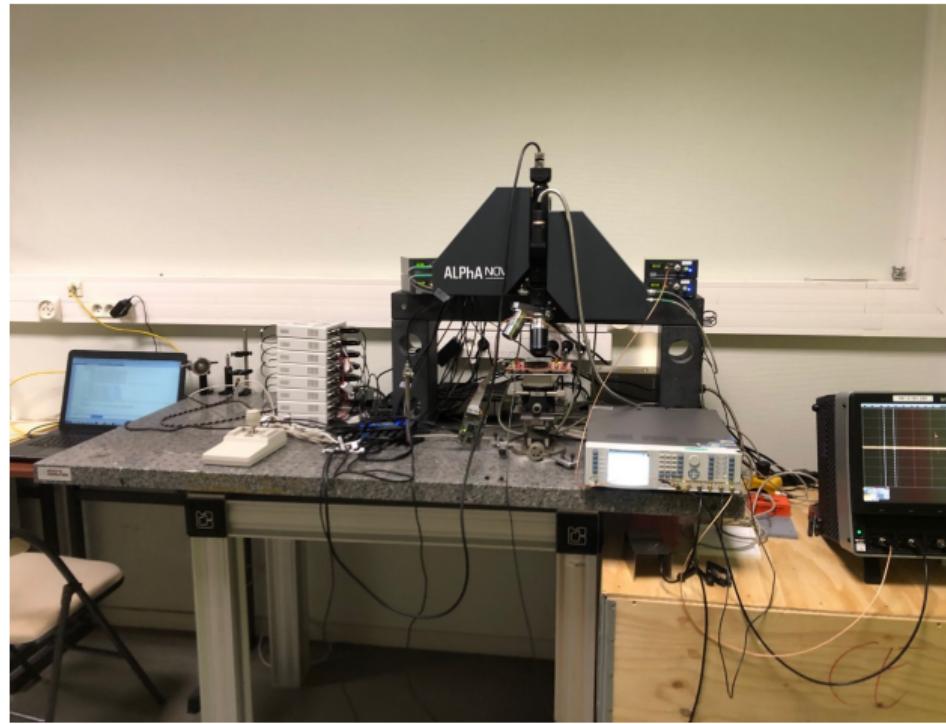
Présentation du banc laser multispot



- LG: Lentille grossissante
- CP: Cube séparateur de faisceaux de polarisation
- MD: Miroir dichroïque
- LT: Lentille tubulaire
- LF: Lentille de focalisation

ALPhANOV
Optics & Lasers Technology Center

Photographie du banc laser



Caractéristiques

Capacités

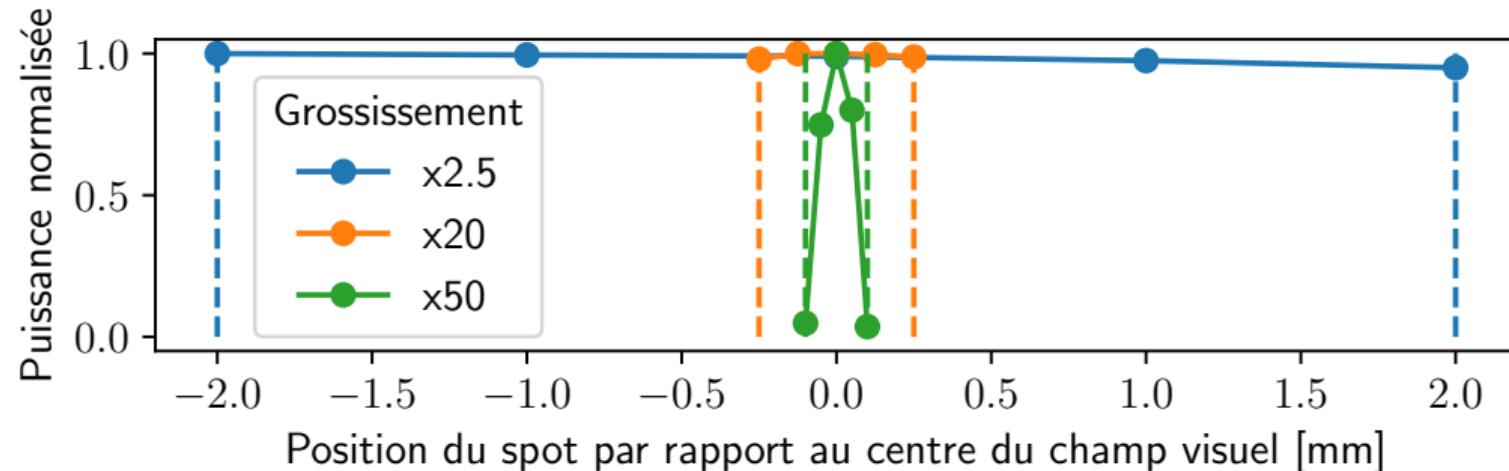
- 4 sources laser
- Indépendante en temps et en positions
- Possibilité de partager les signaux de *trigger*

Limitations

- Distance entre les spots limitées selon l'objectif

| Grossissement | Champ visuel | Diamètre minimal du spot |
|---------------|--------------|--------------------------|
| x2.5 | 4 mm | 25 µm |
| x20 | 500 µm | 2.2 µm |
| x50 | 200 µm | 1.3 µm |

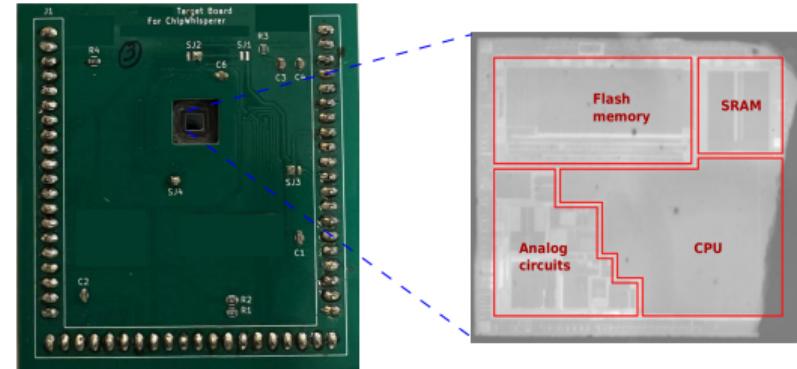
Puissance relative des sources laser du banc multispot



Matériel expérimental

Cible matérielle

- Microcontrôleur 32 bits
- Coeur ARM Cortex-M3
- 128 kB de mémoire Flash
- Ouvert en face arrière pour avoir un accès au substrat



Premier code de caractérisation: Description

```

1 // Raise trigger signal
2 MOV R0, 0x00
3 // Lower trigger signal
4 // Read back R0

```

Code source assembleur

| | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|

Instruction correcte (MOV): Rd = imm8

| | | | | | | |
|---|---|---|---|---|----|------|
| 0 | 0 | 1 | 0 | 0 | Rd | imm8 |
|---|---|---|---|---|----|------|

Instruction correcte (MOV): R0 = 0x00

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Instruction fautée (MOV): R0 = 0x55

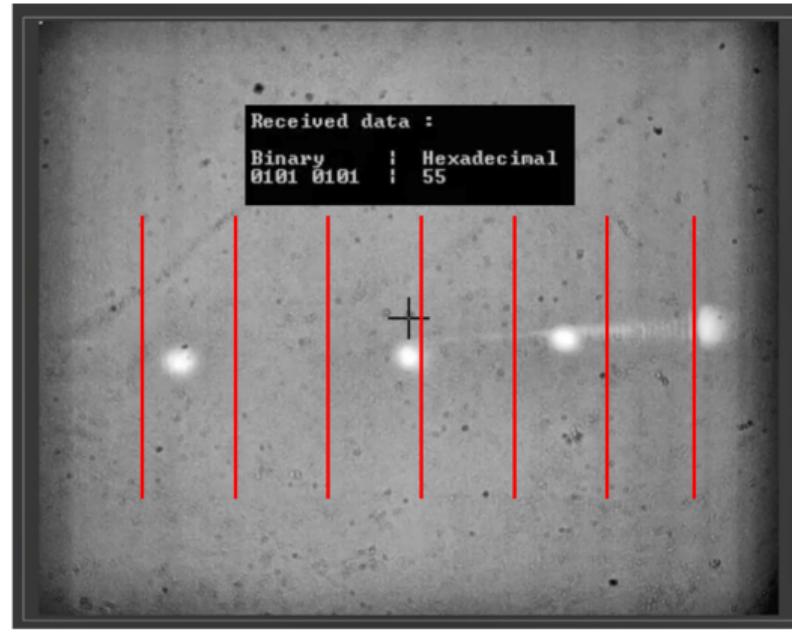
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Chargement de donnée fautée

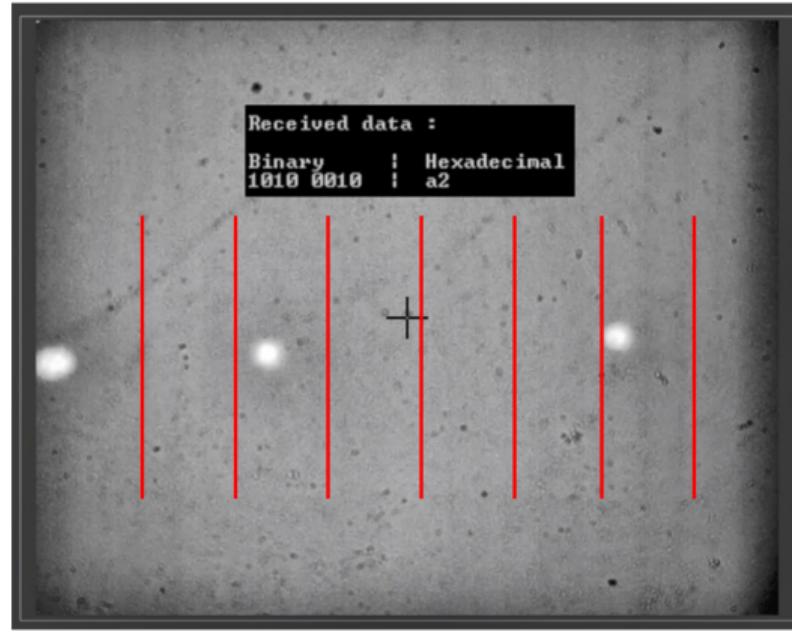
Paramètres d'injection laser

- Puissance laser à 1.5 W
- Durée de l'impulsion laser à 135 ns
- 4 spots distants de 90 µm

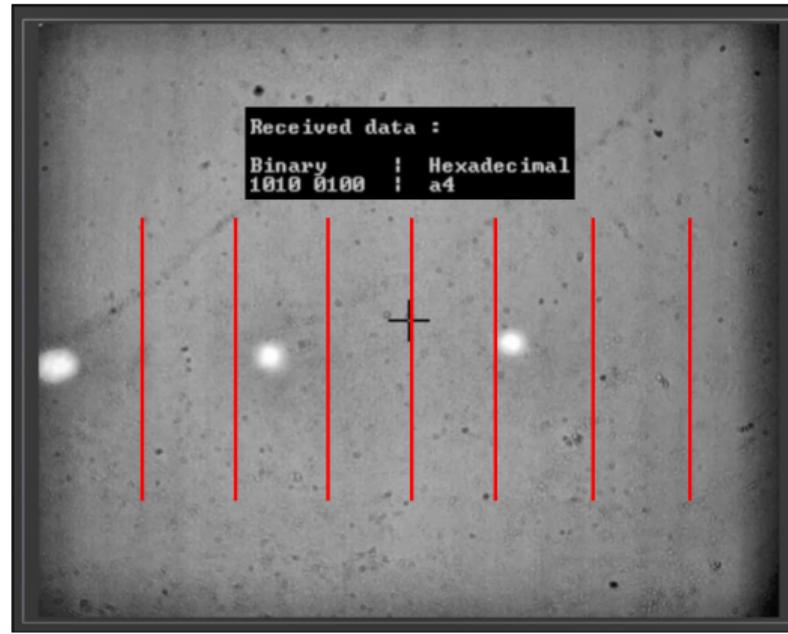
Premier code de caractérisation: Résultat



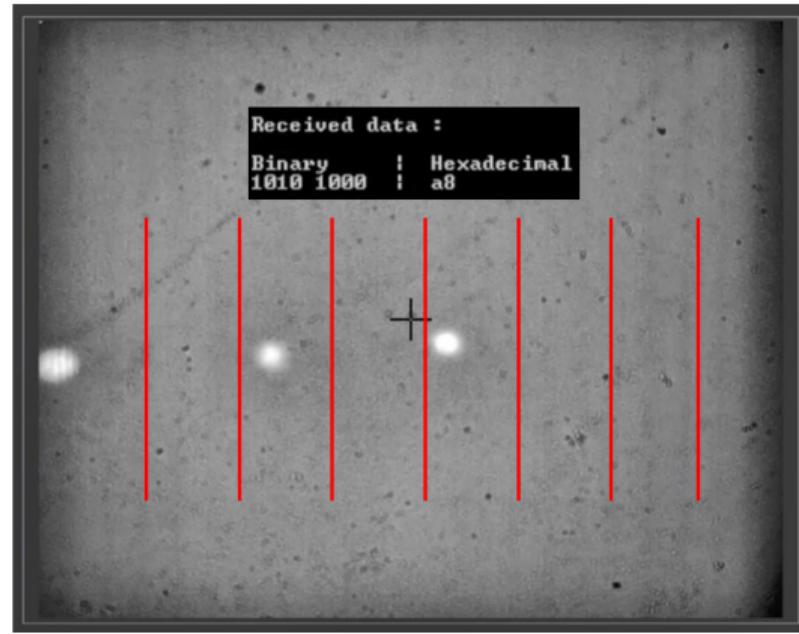
Premier code de caractérisation: Résultat



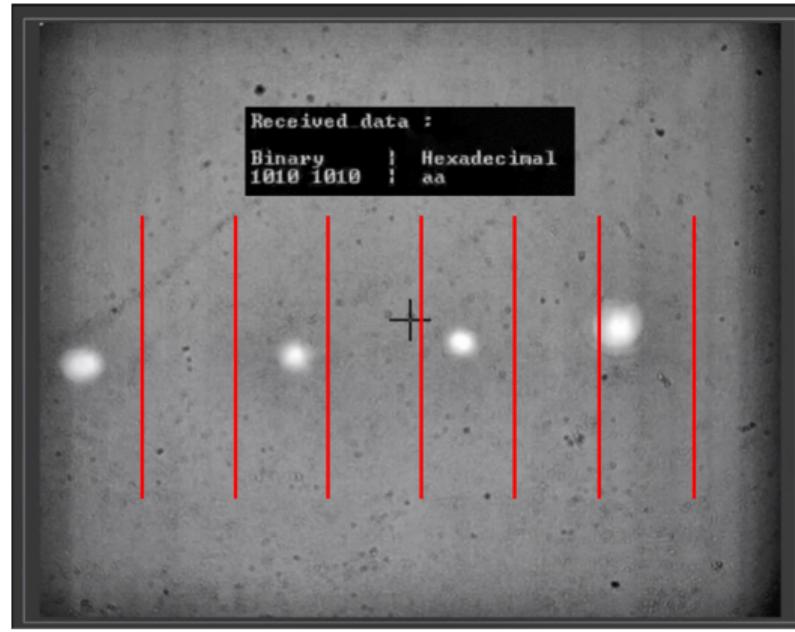
Premier code de caractérisation: Résultat



Premier code de caractérisation: Résultat



Premier code de caractérisation: Résultat



Second code de caractérisation: Description

```

1 #define N_ITER 1000
2 void charac_func(void) {
3     volatile uint32_t ref_count = 0;
4     uint32_t results[2] = {0, 0};
5     uint32_t XOR, ADD = 0;
6     trigger_high();
7     for (volatile uint32_t iter = 1;
8          iter <= N_ITER;
9          iter++) {
10        ref_count++;
11        XOR = iter ^ iter;
12        ADD = iter + iter;
13        results[1] += (XOR == ADD);
14    }
15    results[0] = N_ITER - ref_count;
16    trigger_low();
17    // Read back results
18 }
```

| | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|

Instruction correcte (ADD): $Rdn = Rdn + imm8$

| | | | | | | |
|---|---|---|---|---|-----|------|
| 0 | 0 | 1 | 1 | 0 | Rdn | imm8 |
|---|---|---|---|---|-----|------|

Instruction correcte (ADD): $Rdn = Rdn + 1$

| | | | | | | | | | | | | | |
|---|---|---|---|---|-----|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | Rdn | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|-----|---|---|---|---|---|---|---|---|

Instruction fautée (ADD): $Rdn = Rdn + 5$

| | | | | | | | | | | | | | |
|---|---|---|---|---|-----|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | Rdn | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|-----|---|---|---|---|---|---|---|---|

Faute sur l'incrément de la boucle

| | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|

Instruction correcte (EORS): $Rdn = Rdn \oplus Rm$

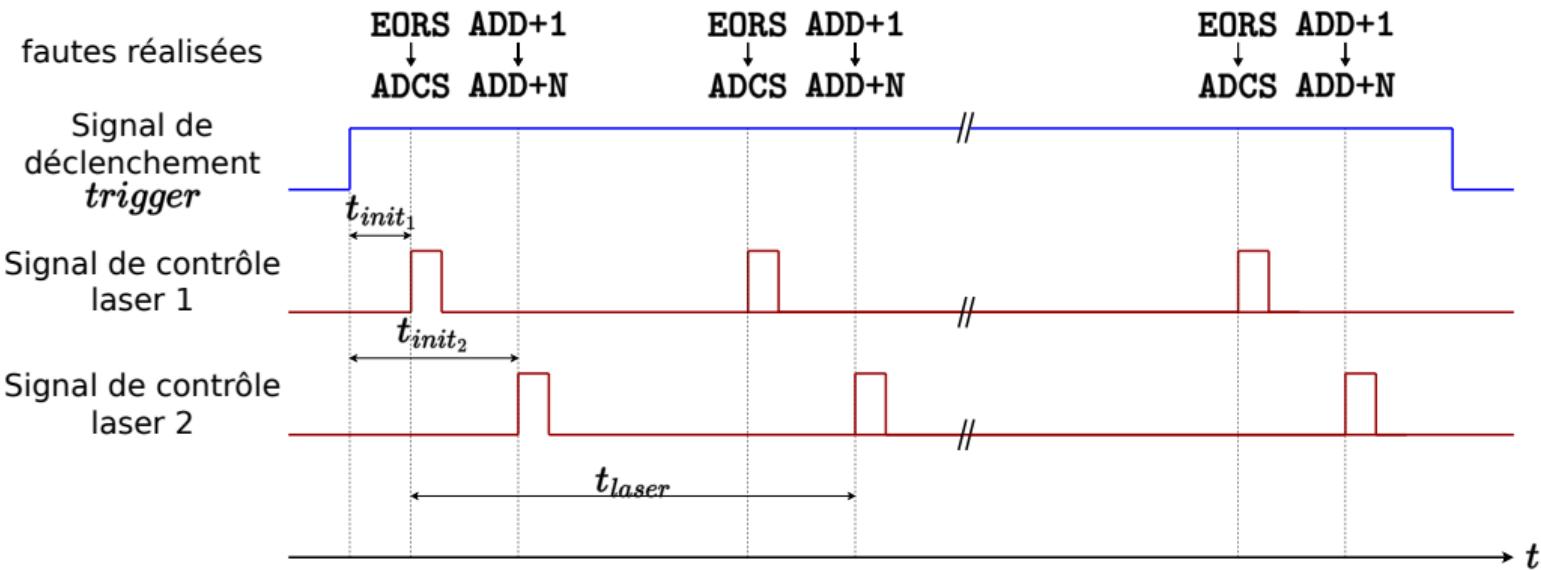
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|----|-----|--|--|--|--|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | Rm | Rdn | | | | |
|---|---|---|---|---|---|---|---|---|---|----|-----|--|--|--|--|

Instruction fautée (ADCS): $Rdn = Rdn + Rm$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|----|-----|--|--|--|--|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | Rm | Rdn | | | | |
|---|---|---|---|---|---|---|---|---|---|----|-----|--|--|--|--|

Faute sur l'opération OU-exclusif

Second code de caractérisation: Résultat



Conclusion

Synthèse

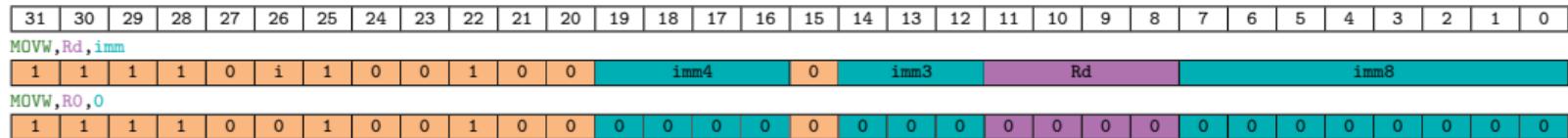
- Possibilité d'injecter des fautes non contigües simultanément
- Possibilité d'injecter des fautes à des positions différents très proches dans le temps

Limitations

- Existence de contremesures matérielles:
 - capteurs d'injection laser

Niveau mémoire

Corruption de code (ARMv7 ISA)

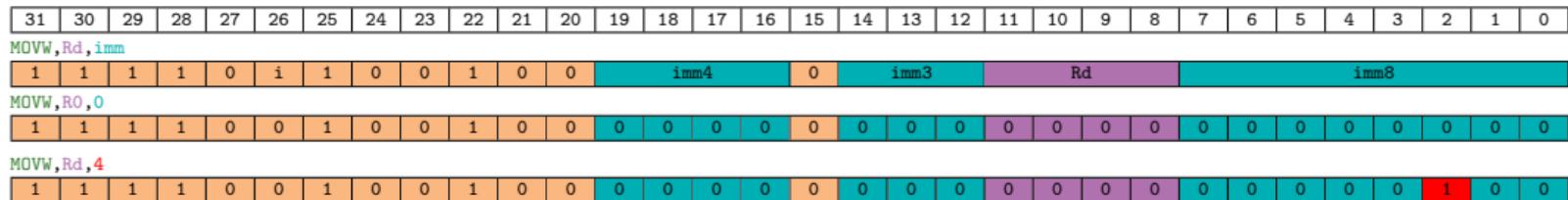


Exemples de corruptions possibles d'une instruction MOVW¹⁶

¹⁶ Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: *IEEE HOST 2019*.

Niveau mémoire

Corruption de code (ARMv7 ISA)



Exemples de corruptions possibles d'une instruction MOVW¹⁶

¹⁶ Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: IEEE HOST 2019.

Niveau mémoire

Corruption de code (ARMv7 ISA)

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------------|----|----|----|----|----|----|----|----|----|----|----|------|----|------|----|------|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|---|--|--|
| 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 | | | |
| MOVW, Rd, imm | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | i | 1 | 0 | 0 | 1 | 0 | 0 | imm4 | 0 | imm3 | Rd | imm8 | | | | | | | | | | | | | | | | | | |
| MOVW, R0, 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 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 | | | |
| MOVW, Rd, 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | | | |
| MOVW, R1, 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | | |

Exemples de corruptions possibles d'une instruction MOVW¹⁶

¹⁶ Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: IEEE HOST 2019.

Niveau mémoire

Corruption de code (ARMv7 ISA)

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------|----|----|----|----|----|----|----|----|----|----|----|------|----|------|----|------|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|---|
| 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 | |
| MOVW,Rd,imm | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | i | 1 | 0 | 0 | 1 | 0 | 0 | imm4 | 0 | imm3 | Rd | imm8 | | | | | | | | | | | | | | | | |
| MOVW,RO,0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 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 | |
| MOVW,Rd,4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | |
| MOVW,R1,0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| MOVW,Rd,0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Exemples de corruptions possibles d'une instruction MOVW¹⁶

¹⁶ Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: IEEE HOST 2019.

Niveau mémoire

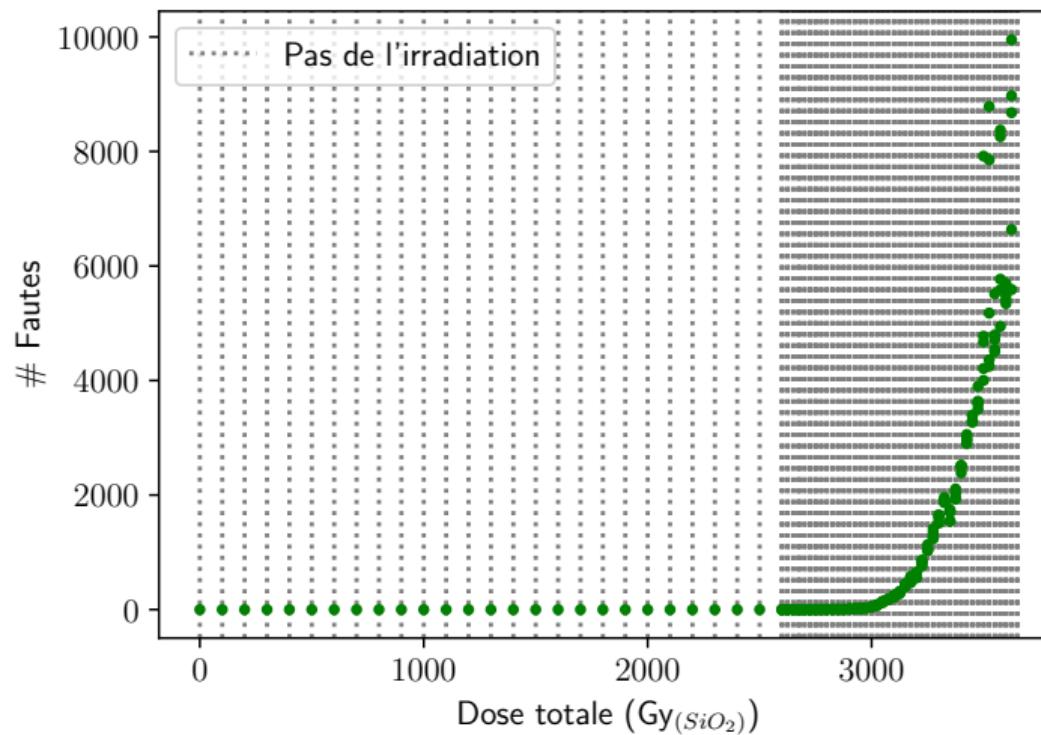
Corruption de code (ARMv7 ISA)

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------|----|----|----|----|----|----|----|----|----|----|----|------|----|------|----|------|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|---|
| 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 | |
| MOVW,Rd,imm | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | i | 1 | 0 | 0 | 1 | 0 | 0 | imm4 | 0 | imm3 | Rd | imm8 | | | | | | | | | | | | | | | | |
| MOVW,RO,0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 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 | |
| MOVW,Rd,4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | |
| MOVW,R1,0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| MOVW,Rd,0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Exemples de corruptions possibles d'une instruction MOVW¹⁶

¹⁶ Brice Colombier et al. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In: IEEE HOST 2019.

Résultats (EEPROM)



Utilisation d'un tomographe : Principe

