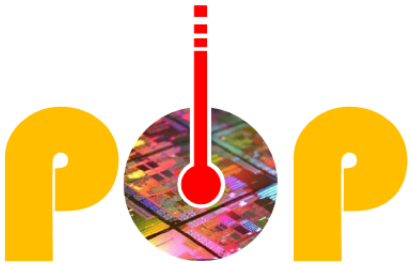
X-Ray Fault Injection in non-volatile memories of Power Off Devices

Paul Grandamme[1,2]
PhD thesis supervised by Lilian Bossuet[1] and Jean-Max Dutertre[2]

[1]Université Jean Monnet Saint-Etienne, CNRS, Institut d'Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France
[2]Mines Saint-Etienne, CEA Leti, Centre CMP, 13541 Gardanne, France

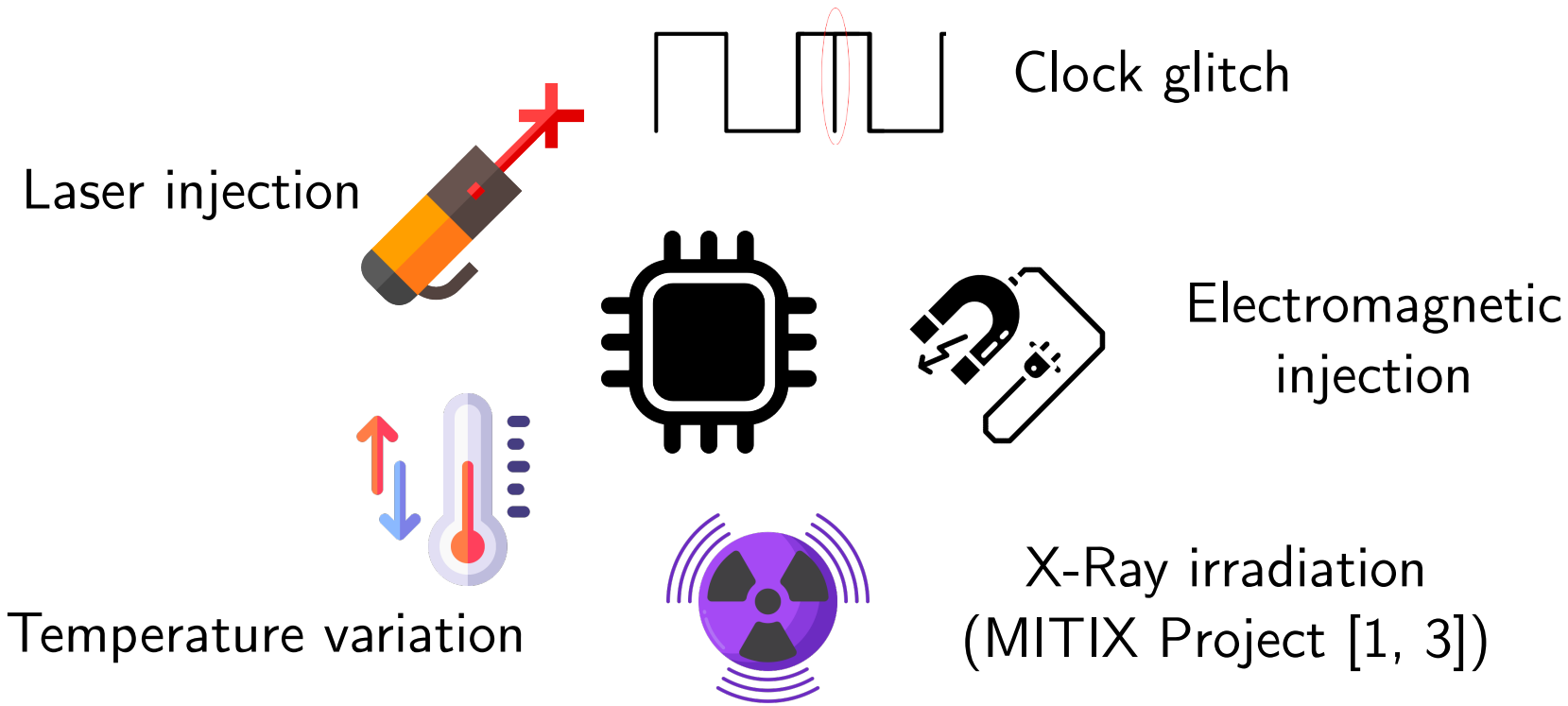


September 28th 2023

Introduction

Fault Attack

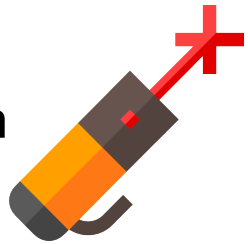
Disturbing the device to modify its behavior to obtain information or disable internal protection mechanisms

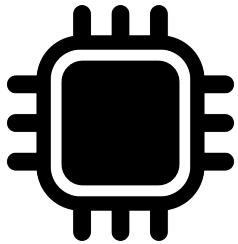


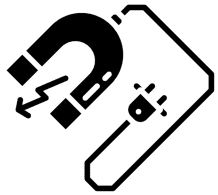
[1] Anceau S. et al. Nanofocused X-Ray Beam to Reprogram Secure Circuits. CHES 2017.
[3] Maingault L. et al. Laboratory X-rays Operando Single Bit Attacks on Flash Memory Cells. CARDIS 2021.

Introduction

Laser injection







Electromagnetic injection

Benefits

High time and spatial accuracy

Limitations

The device must be powered $\Rightarrow$ some countermeasures exist

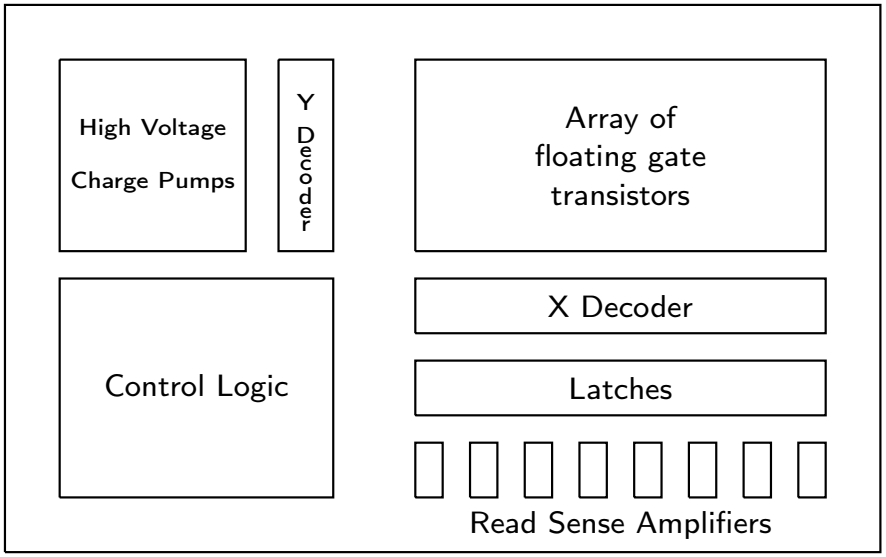
Advantages

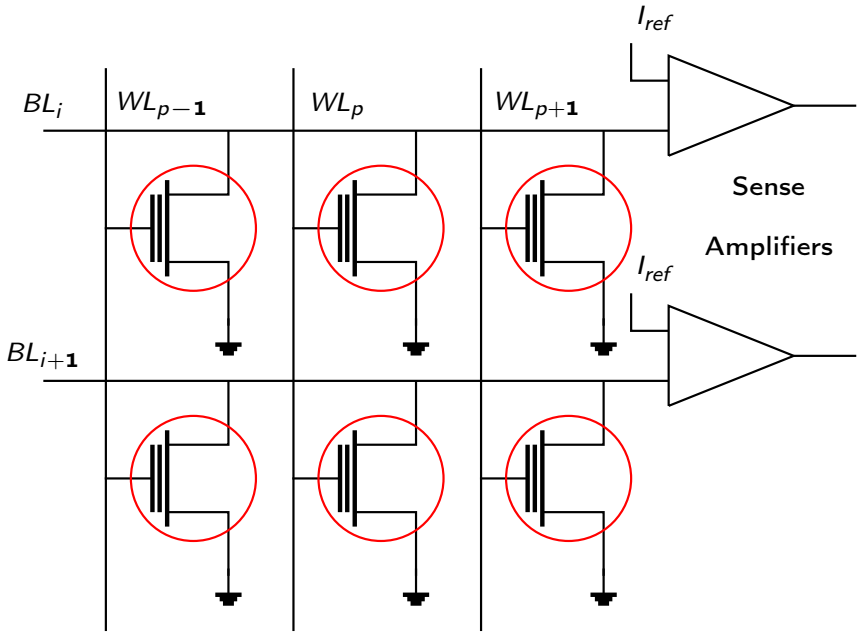
X-Ray can have an effect in non-volatile memories of power off devices

Table of contents

Overview

Usual organization of Flash memories

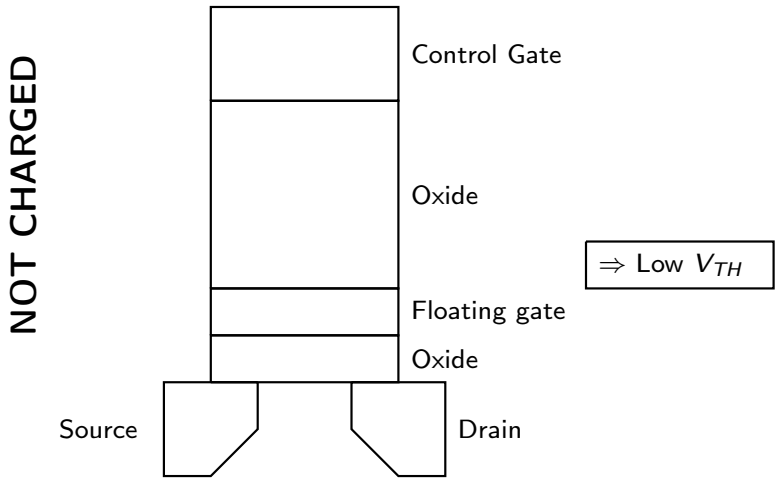


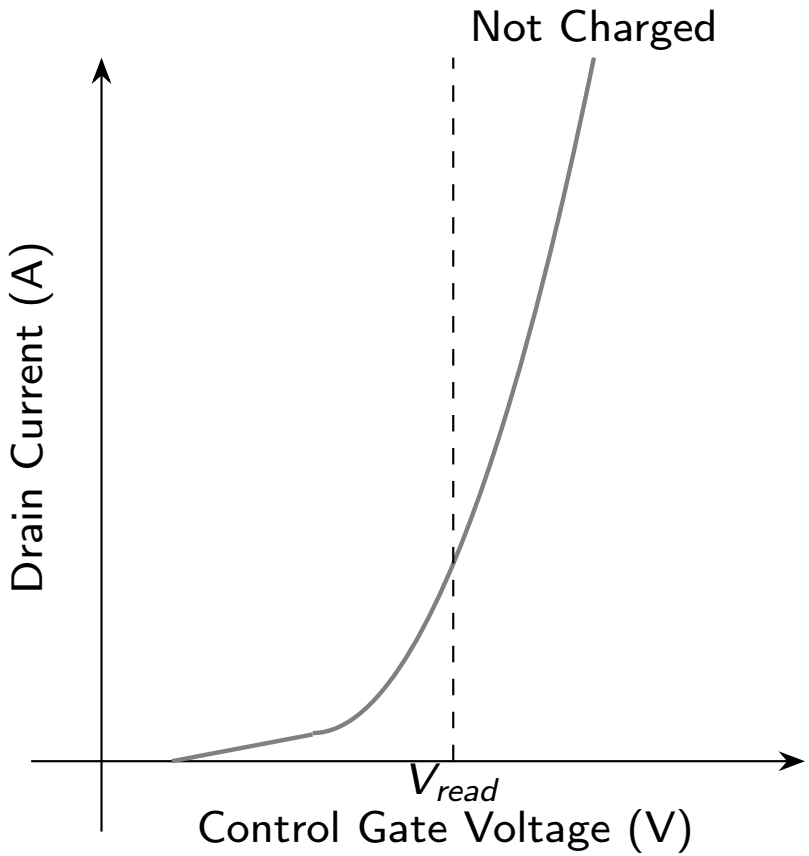


Floating gate transistors

[4] S. Skorobogatov, 'Optical Fault Masking Attacks', in 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, Santa Barbara, CA, TBD: IEEE, Aug. 2010, pp. 23–29

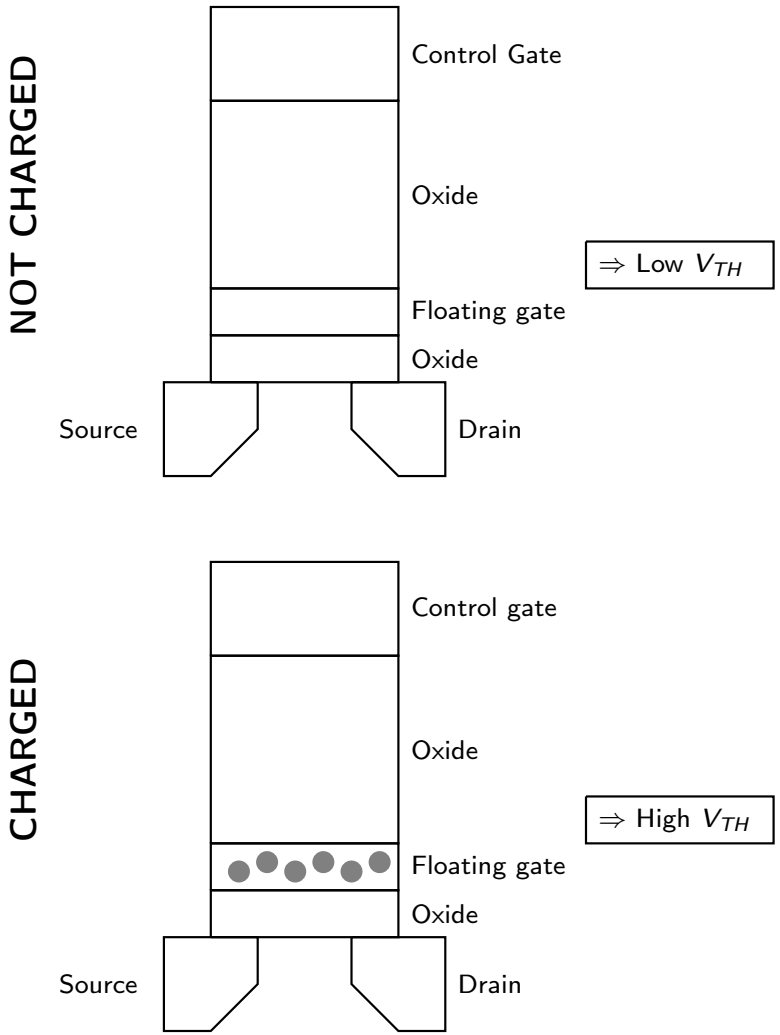
Floating gate transistor

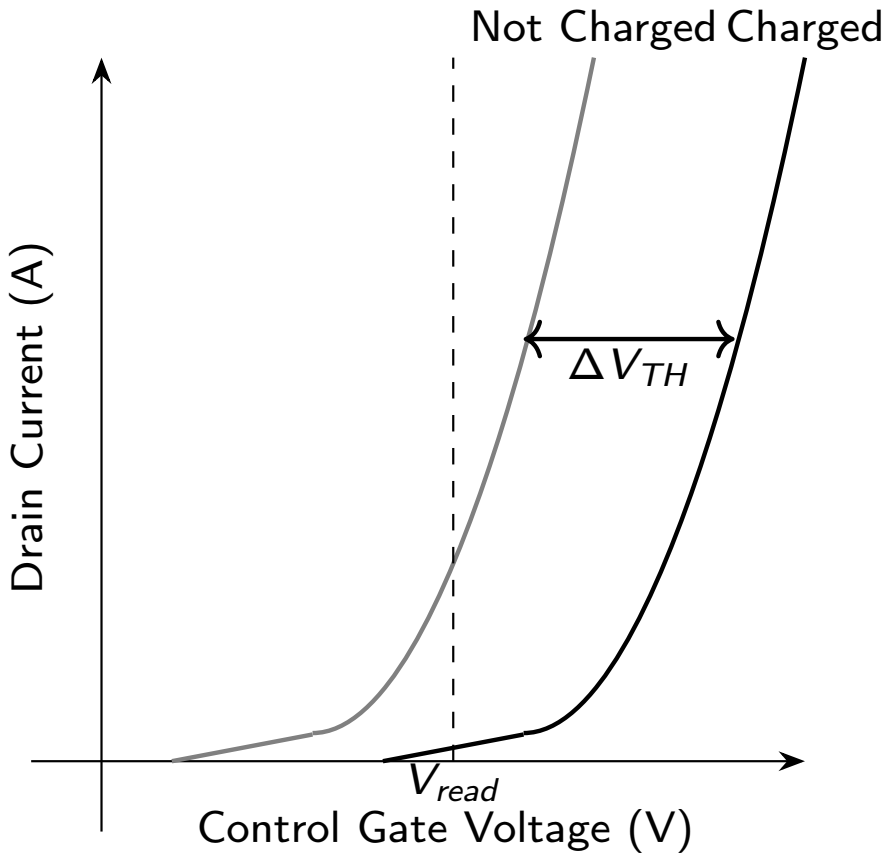




[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Floating gate transistor

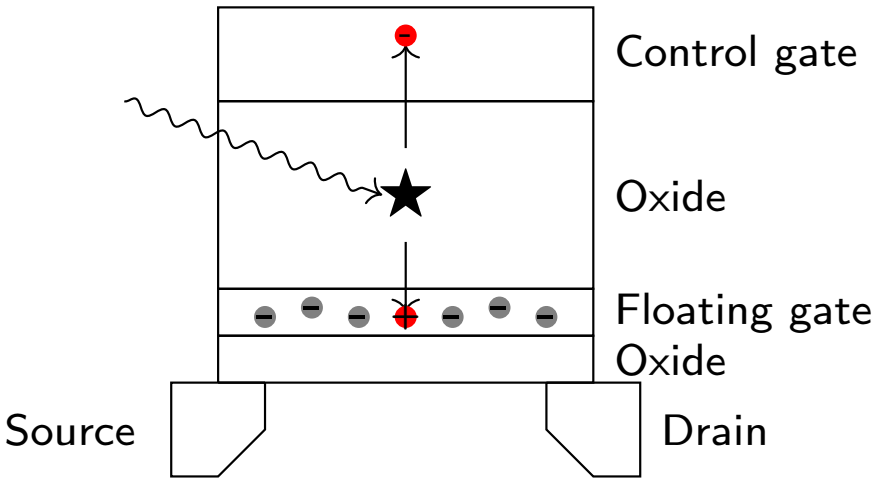




[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Overview

TID mecanisms in floating gate transistor



Effect 1

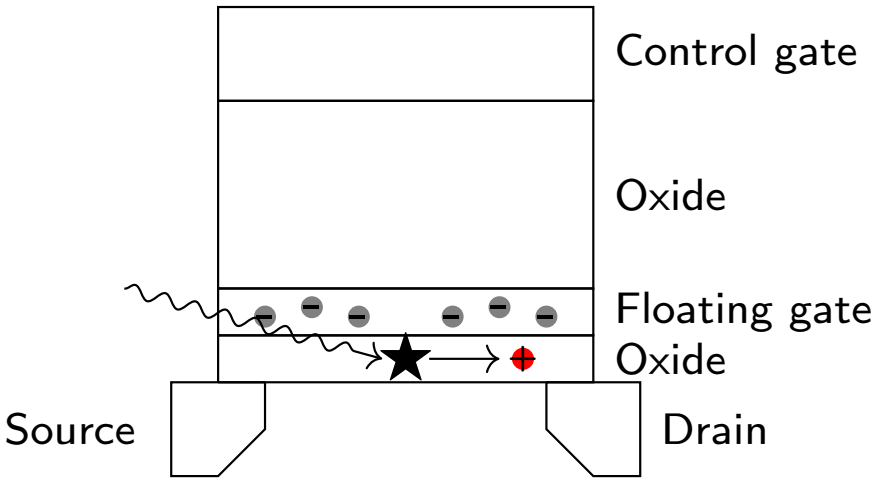
- e^-/h^+ pair created by radiation is separated by the electric field
- one of them escapes through the control gate
- the other one is injected into the floating gate

$\Rightarrow$ recombination with stored charges

$\Rightarrow$ decrease of the charge

[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

TID mecanisms in floating gate transistor

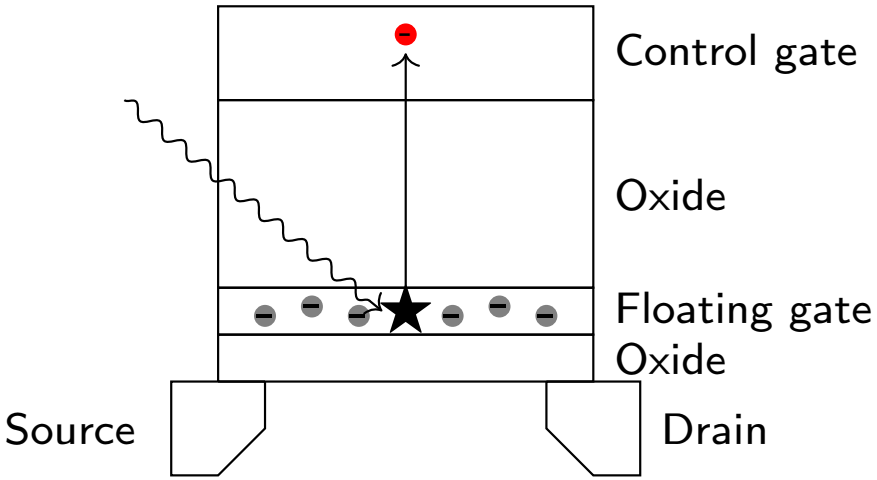


Effect 2

- the charge can be trapped in the oxide
- Phenomenon is not significant because of the thinness of the oxides

[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

TID mecanisms in floating gate transistor



Effect 3: *photoemission*

- charges stored in the floating gate get enough energy from the radiation to escape from the potential well

$\Rightarrow$ decrease of the stored charge

[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

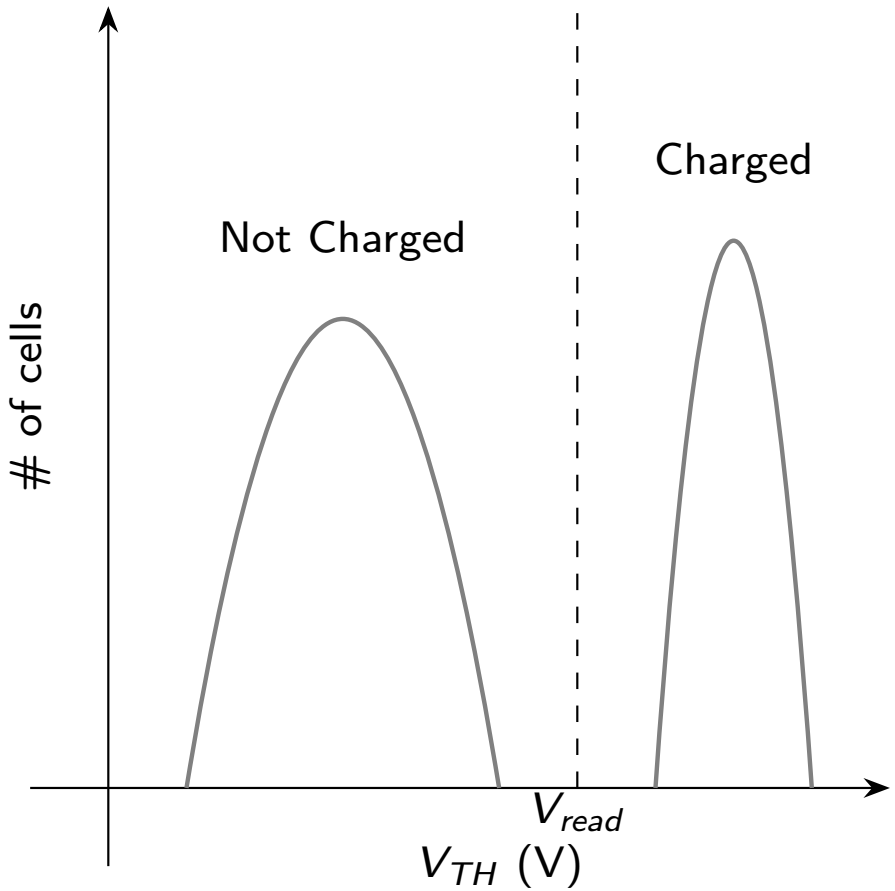
TID mecanisms in floating gate transistor

3 different effects:

- electron-hole pair generation in the oxide
- charge trapping in the oxide
- **photoemission**

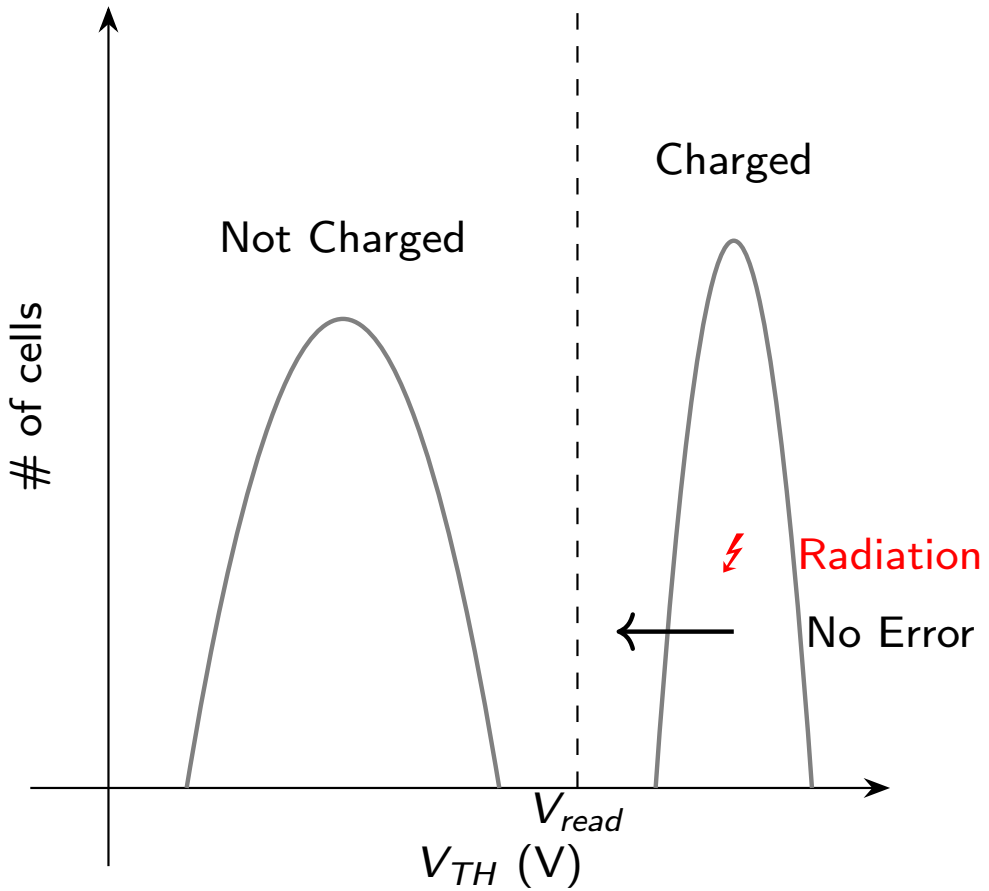
[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Influence of ionizing radiation on the threshold voltage distribution



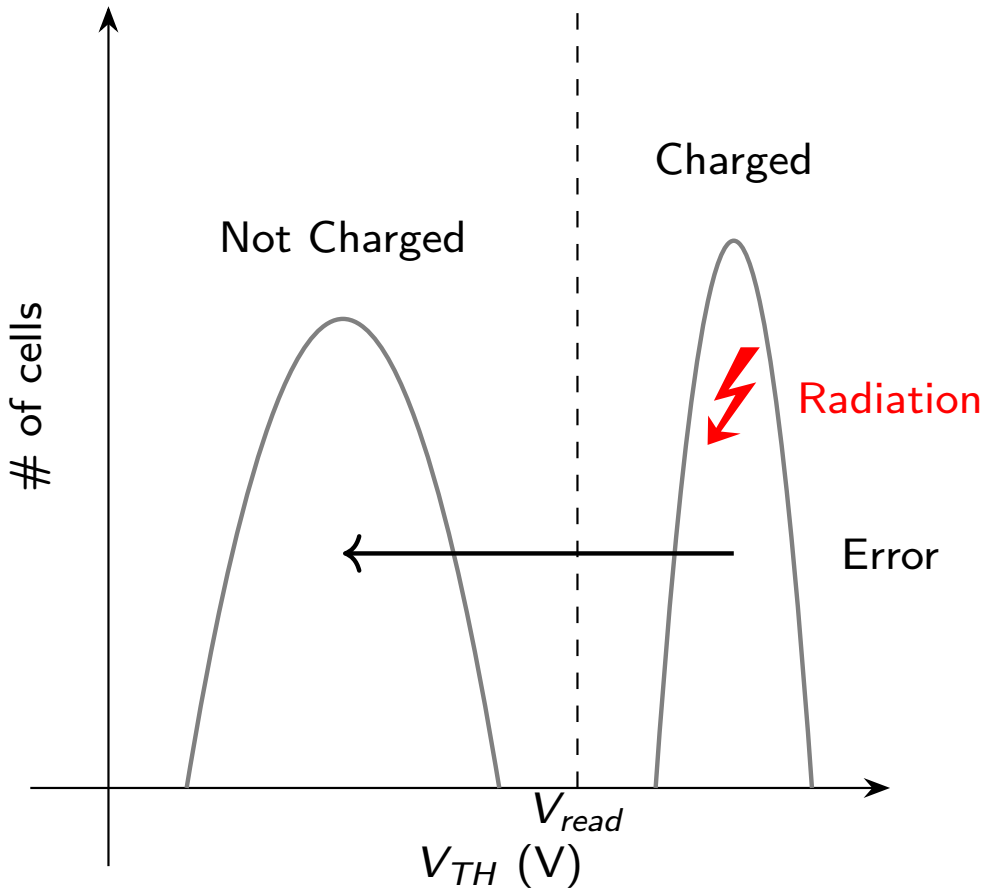
[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Influence of ionizing radiation on the threshold voltage distribution



[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Influence of ionizing radiation on the threshold voltage distribution

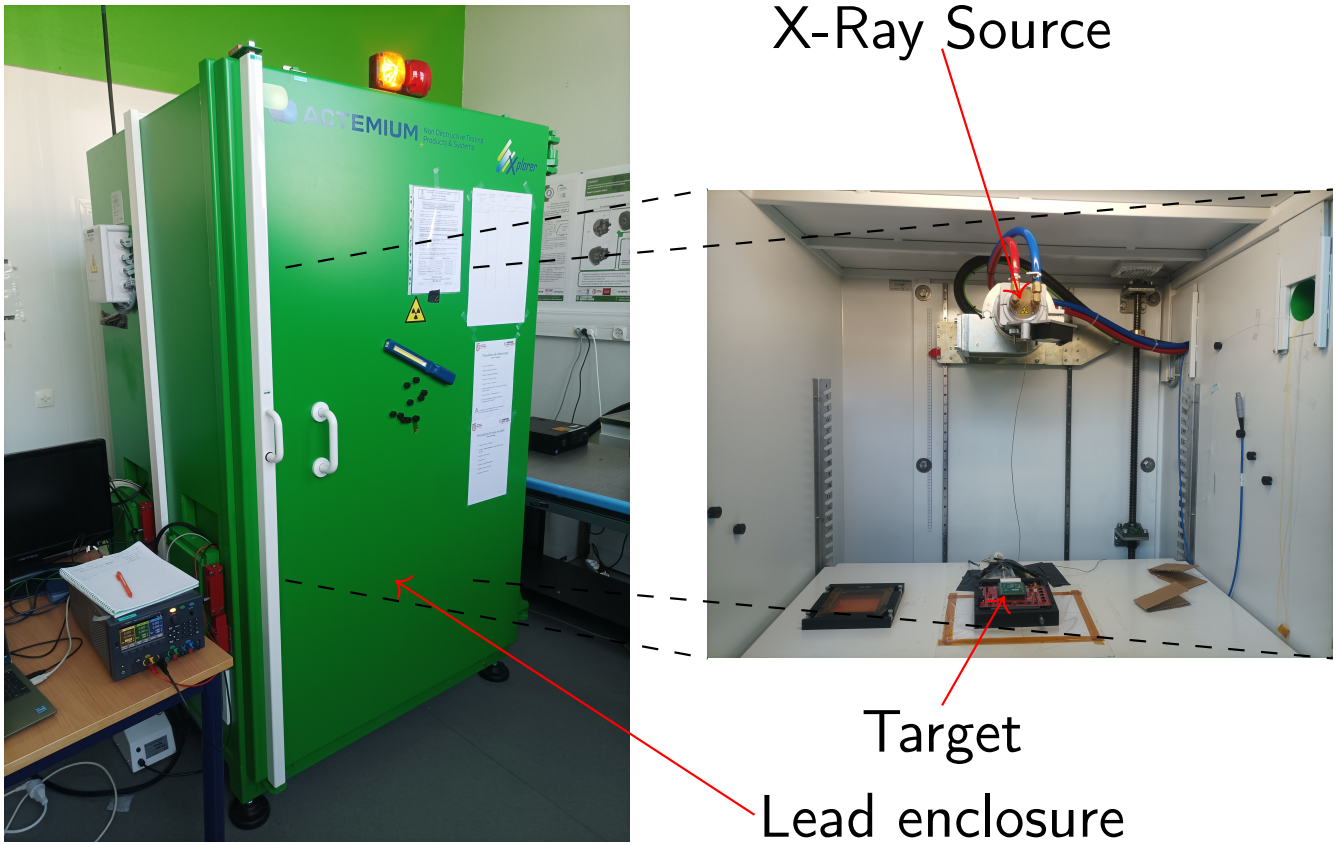


[2] S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Table of contents

Overview

X-Ray irradiator

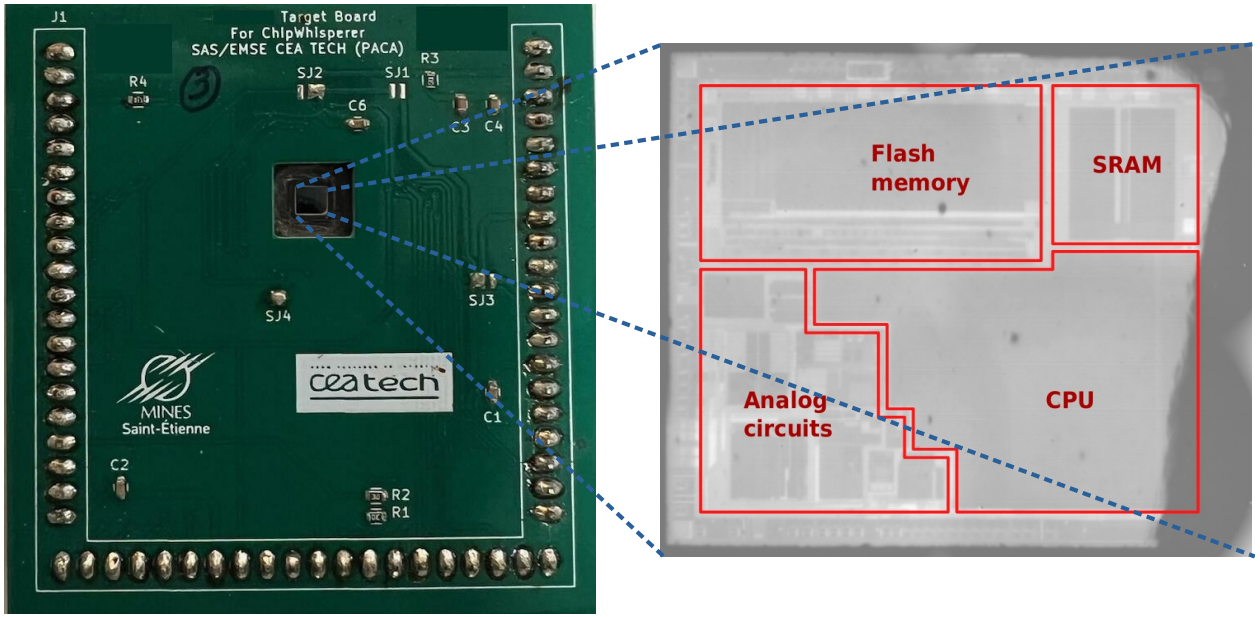


Settings

- Tungsten (W) anode
- Source : 100kV and 45mA $\Rightarrow$ photons with 40keV energy

Overview

Targets



Targets settings

- 32-bit microcontroller with ARM Cortex-M3 core
- 128 kB of Flash memory (erase state : `0xFFFFFFFF`)
- 2048 bitlines and 512 wordlines
- security bits preventing from reading memory if activated

Overview

Protocol

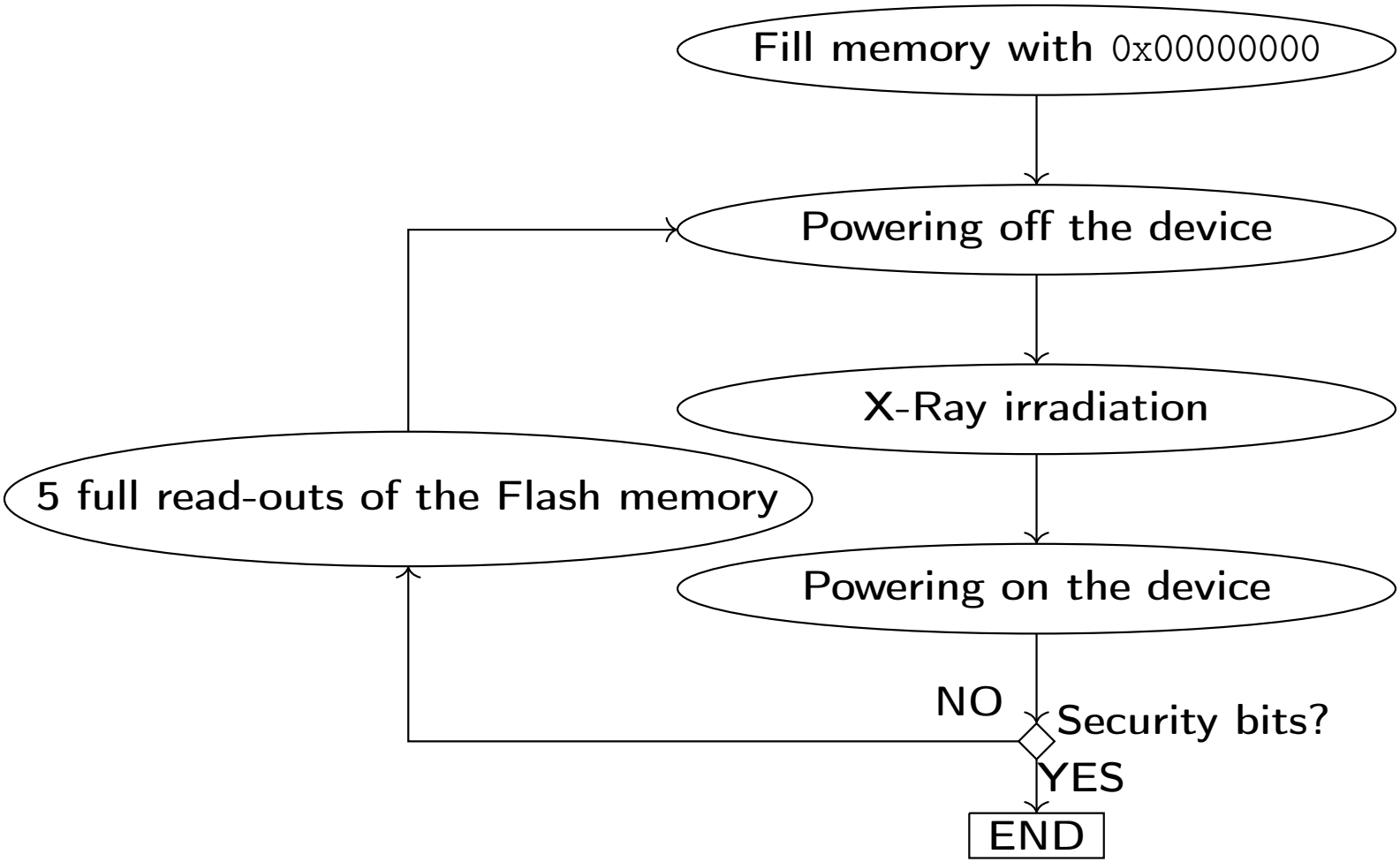

Fill memory with 0x00000000
Powering off the device
X-Ray irradiation
Powering on the device
Security bits?
NO
YES
END
5 full read-outs of the Flash memory

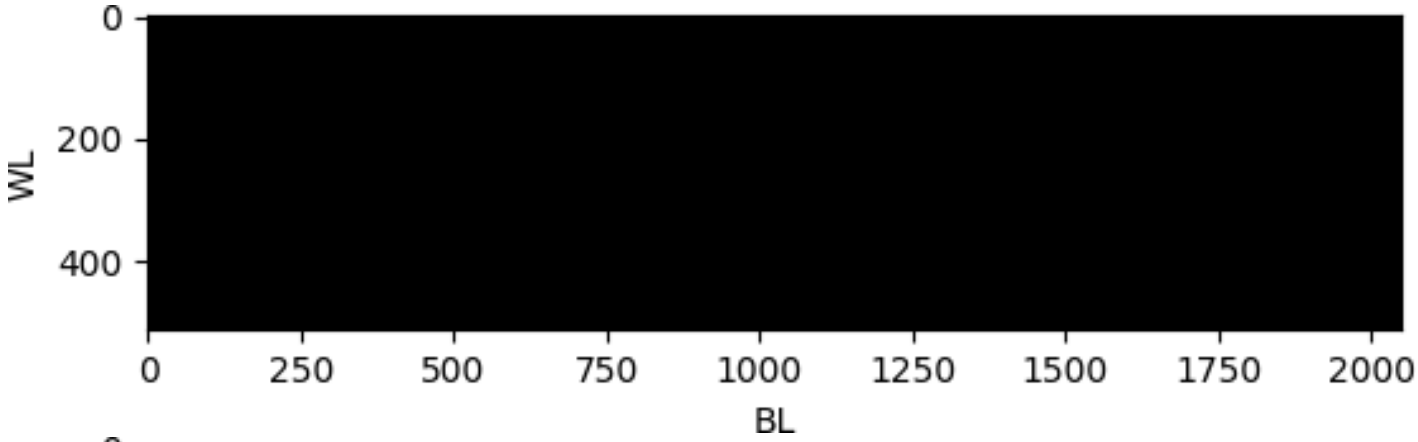
Table of contents

Overview

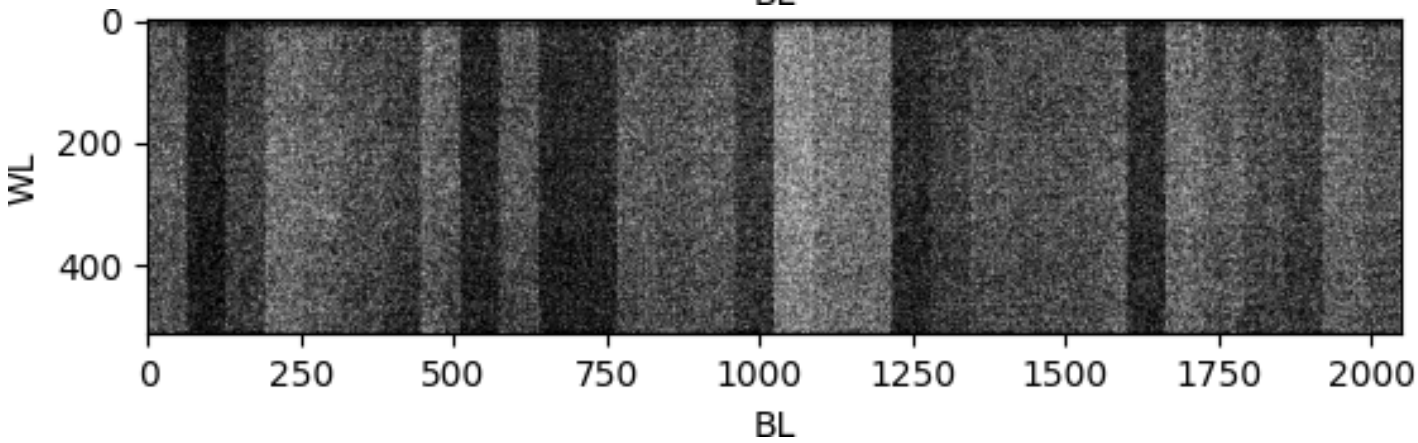
Bitsets in Flash memory

Color	Bit Value	Faulty	FGMOS state
White	1	Yes	Discharged
Black	0	No	Charged

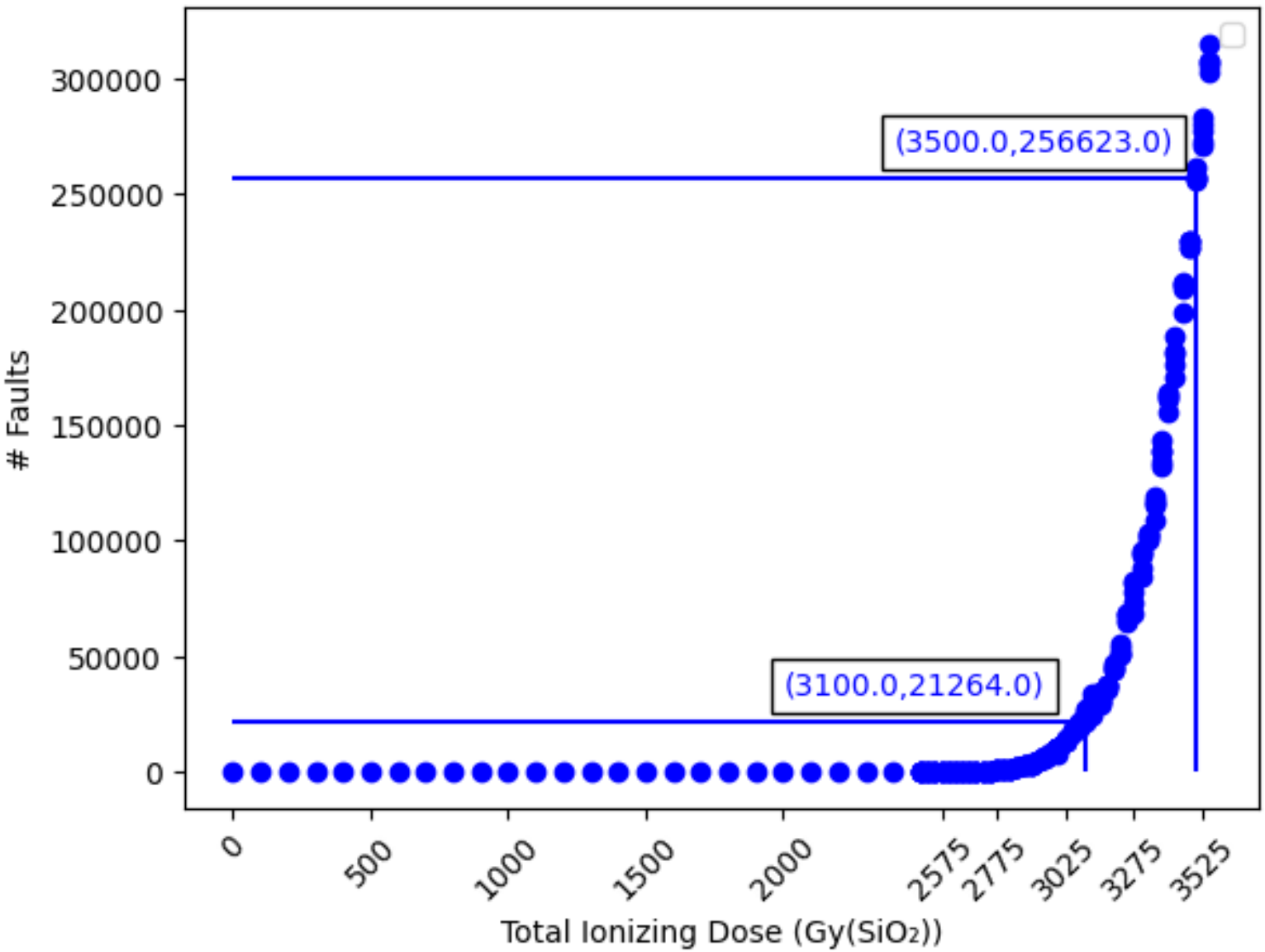
Before irradiation:



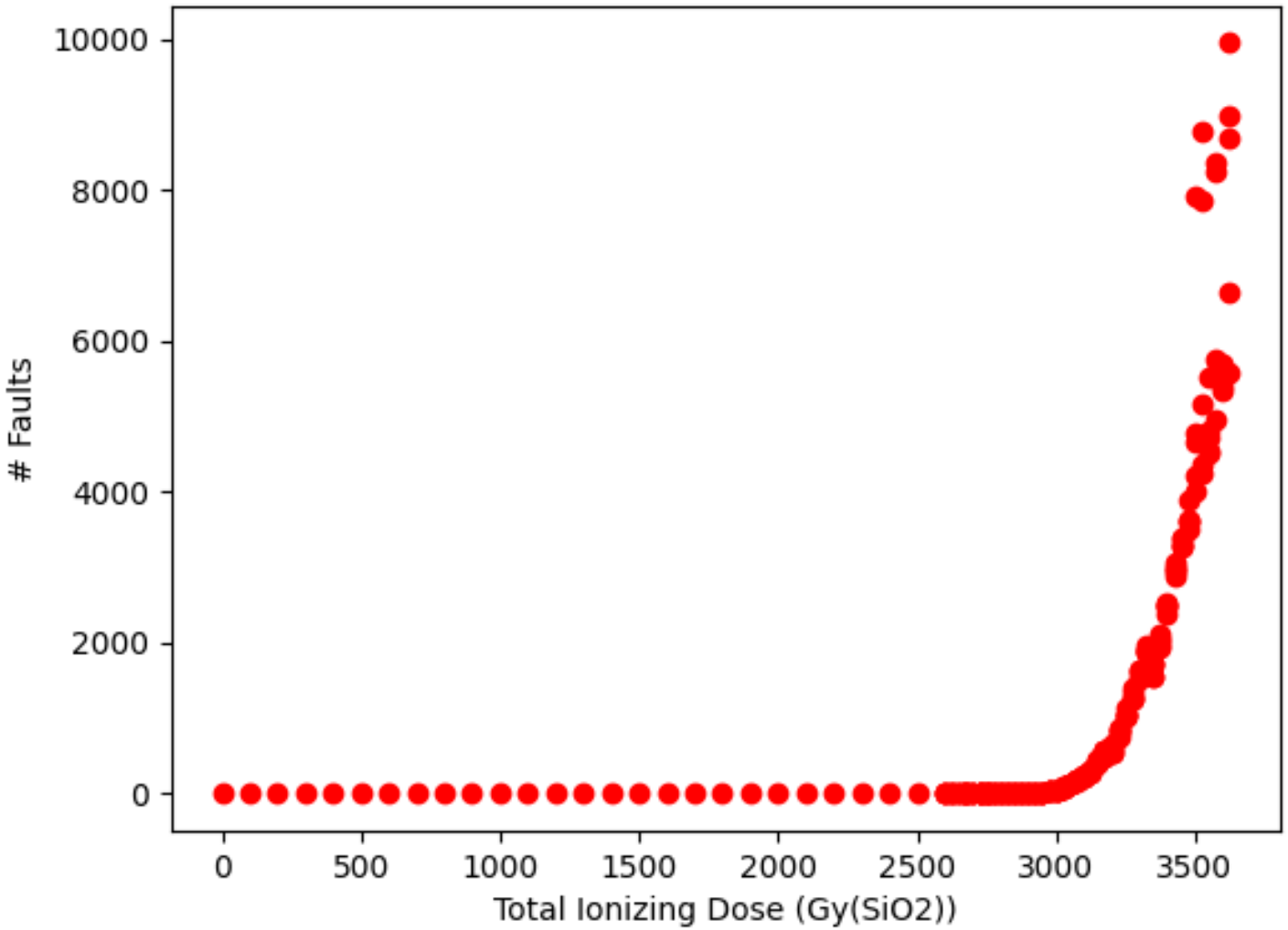
After irradiation:



Faults in Flash memory



Faults in EEPROM memory



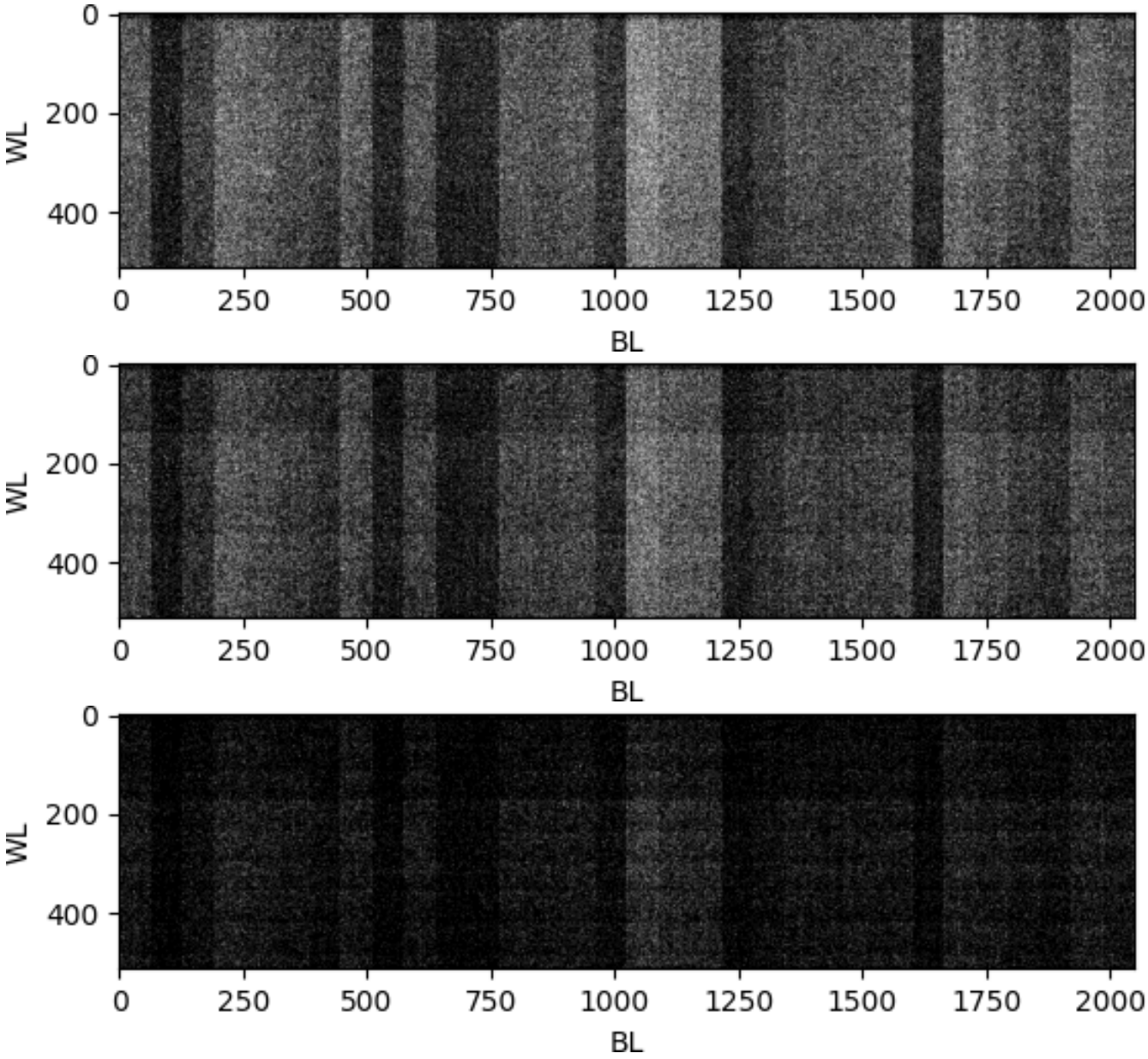
Overview

Time and thermal recovery

After irradiation:

After time recovery:
7 days @ room temperature

After thermal recovery:
2h @ 150°C



Permanent VS non-permanent faults

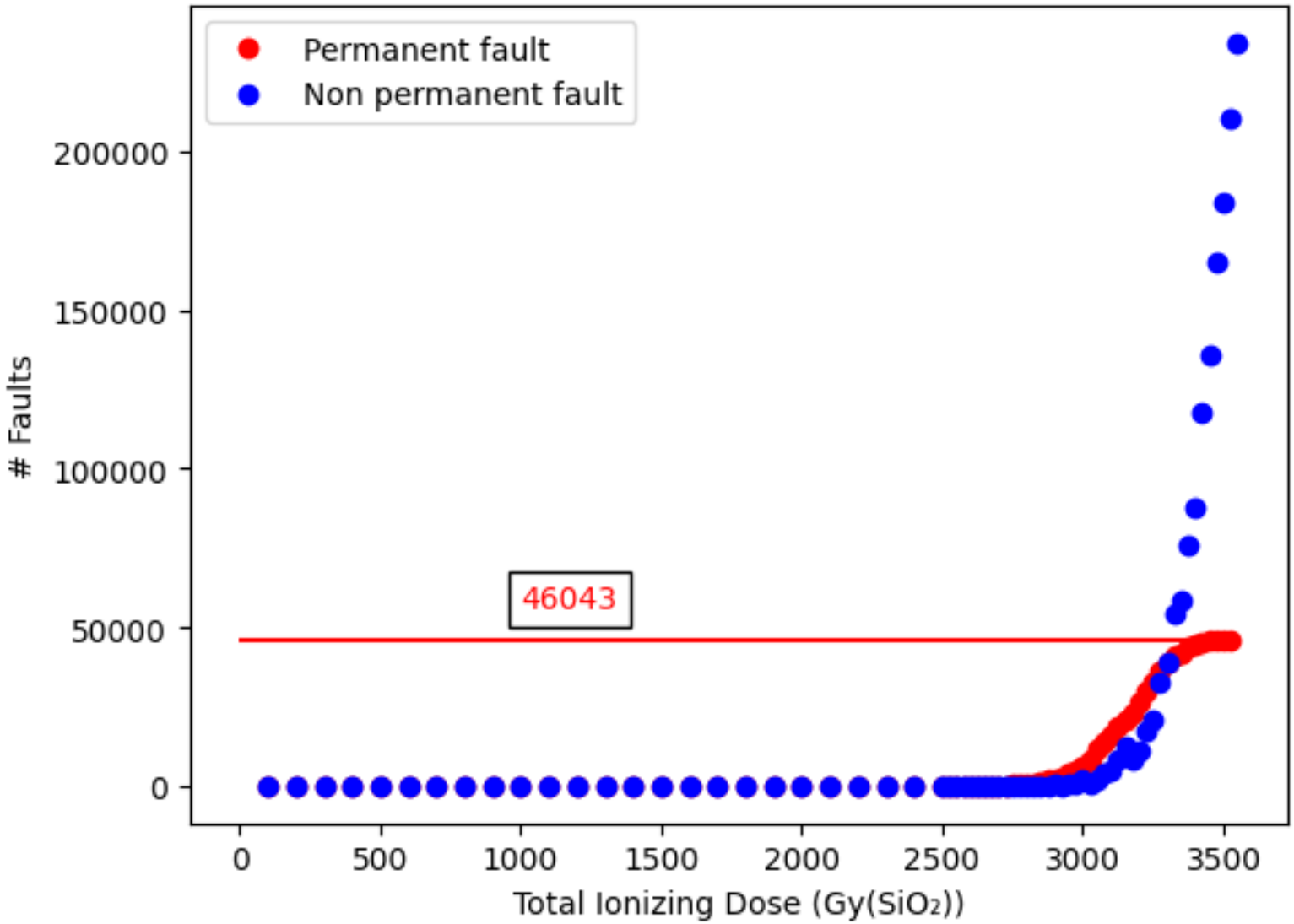


Table of contents

Conclusion and future works

Conclusion

- X-Ray can have an effect on non-volatile memories of power off devices
- Exponential dependance between the total ionizing dose and the number of faults
- Thermal recuperation is possible for the non-permanent faults
- Permanent faults are due to the discharge of the floating gate transistors

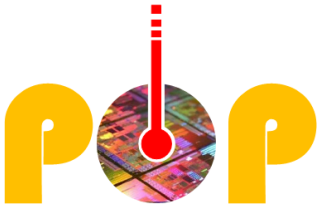
Ongoing work

- Lead shield design and fabrication to target specific part of the device
- Application on cryptographic algorithm attack

Thank you for listening. Do you have any questions?

This work is funded by a french ANR program, along with the project POP.

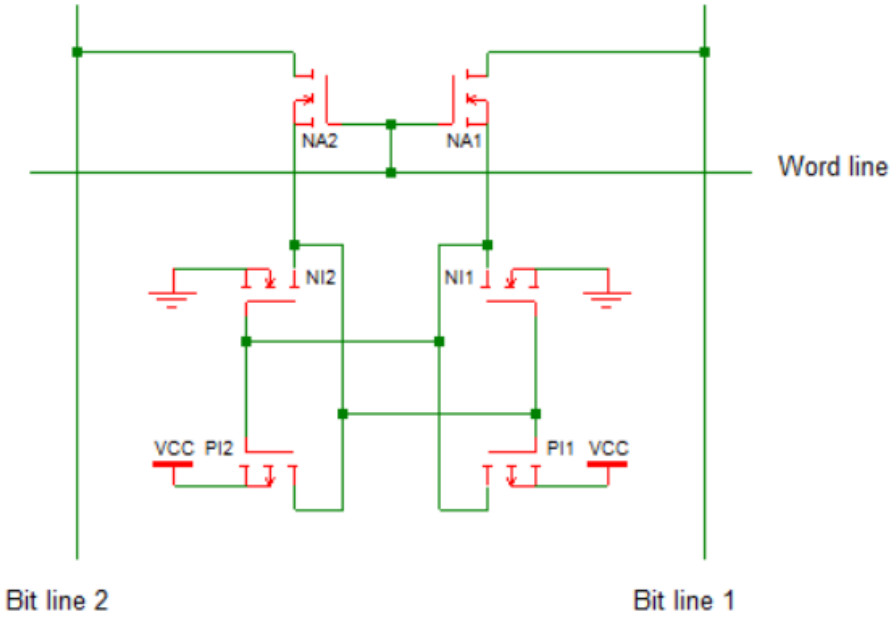
Thanks to the MOPERE team (LabHC) for the access to the X-Ray source.



Existing works

Anceau S. et al. Nanofocused X-Ray Beam to Reprogram Secure Circuits. CHES 2017.

- 6T SRAM cell:



- NI2 $\rightarrow$ Stuck at 0
- NI1 $\rightarrow$ Stuck at 1
- Thermal annealing possible

- Non-volatile memories:
  - whole column is reset (Thermal annealing possible)
  - single bit is reset

  $\Rightarrow$ Same phenomemon

Existing works

Maingault L. et al. Laboratory X-rays Operando Single Bit Attacks on Flash Memory Cells. CARDIS 2021.

- Use of a conventional W target X-rays source
- Perform frontside attack
- Some proposal of mask conception

Bibiography

Stéphanie Anceau, Pierre Bleuet, Jessy Clédière, Laurent Maingault, Jean-Luc Rainard, and Rémi Tucoulou.

Nanofocused x-ray beam to reprogram secure circuits.

In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 175–188. Springer, 2017.

S. Gerardin, M. Bagatin, A. Paccagnella, K. Grürmann, F. Gliem, T. R. Oldham, F. Irom, and D. N. Nguyen.

Radiation effects in flash memories.

IEEE Transactions on Nuclear Science, 60(3):1953–1969, 2013.

Laurent Maingault, Stéphanie Anceau, Manuel Sulmont, Luc Salvo, Jessy Clédière, Pierre Lhuissier, Emrick Beliard, and Jean-Luc Rainard.

Laboratory x-rays operando single bit attacks on flash memory cells.

In Vincent Grosso and Thomas Pöppelmann, editors, *Smart Card Research and Advanced Applications - 20th International Conference, CARDIS 2021, Lübeck, Germany, November 11-12, 2021, Revised Selected Papers*, volume 13173 of *Lecture Notes in Computer Science*, pages 139–150. Springer, 2021.

Sergei Skorobogatov.

Optical fault masking attacks.

In Luca Breveglieri, Marc Joye, Israel Koren, David Naccache, and Ingrid Verbauwhede, editors, *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010, Santa Barbara, California, USA, 21 August 2010*, pages 23–29. IEEE Computer Society, 2010.