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]

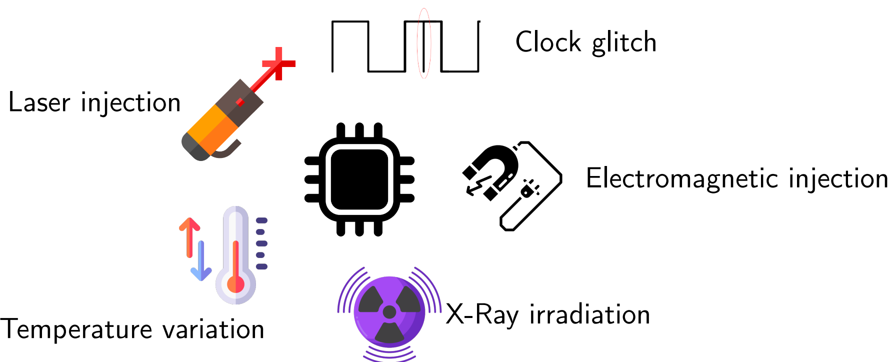
[1]Université Jean Monnet Saint-Etienne, CNRS, Institut d Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France
[2]Mines Saint-Etienne, CEA Leti, Centre CMP, 13541 Gardanne, France

June 13th 2023

Introduction

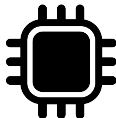
Fault Attack

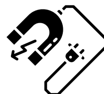
Disturbing the device to modify its behavior to obtain information or disable internal protection mechanisms



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

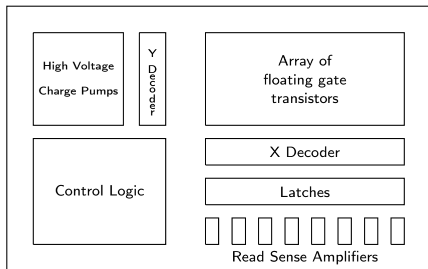
Table of contents

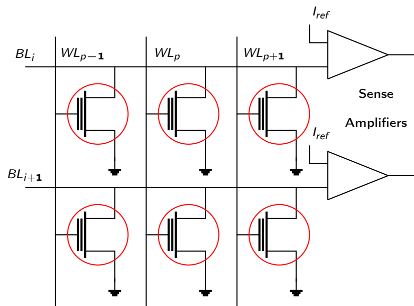
1. Flash memory, floating gate transistor and X-ray effects
   - Flash Memory and floating gate transistor
   - X-Ray effects on floating gate transistor
2. Experiments
3. Results
4. Conclusion

Overview

1. Flash memory, floating gate transistor and X-ray effects
   - Flash Memory and floating gate transistor
   - X-Ray effects on floating gate transistor
2. Experiments
3. Results
4. Conclusion

Usual organization of Flash memories

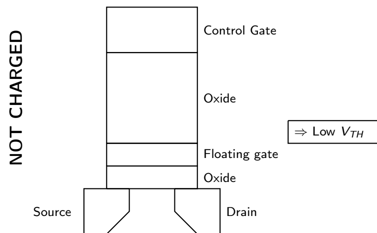


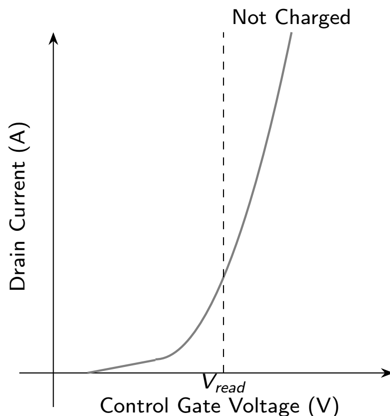


Floating gate transistors

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

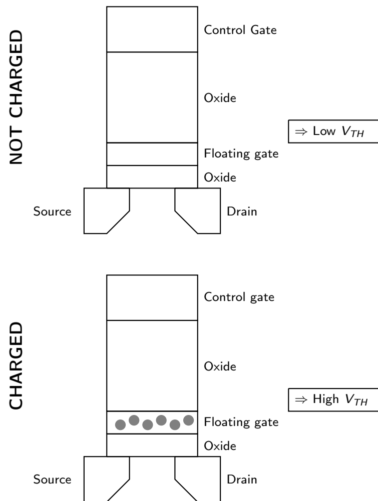
Floating gate transistor

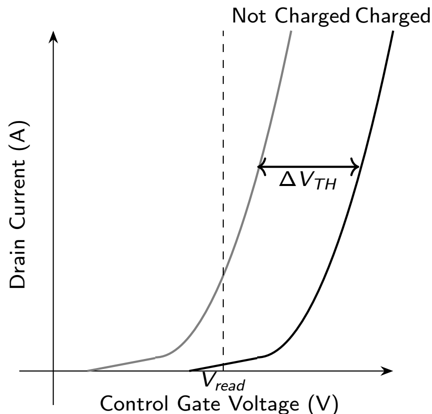




S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Floating gate transistor



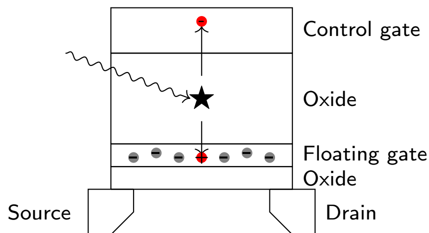


S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Overview

1. Flash memory, floating gate transistor and X-ray effects
   - Flash Memory and floating gate transistor
   - X-Ray effects on floating gate transistor
2. Experiments
3. Results
4. Conclusion

TID mecanisms in floating gate transistor



Effect 1

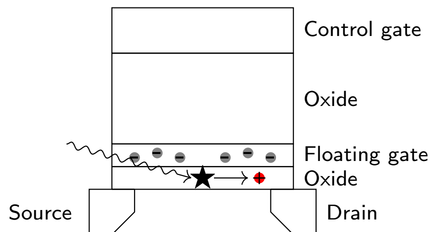
- e^+/h^- pair created by radiation is separated by the electric field
- one of them escapes through the control gate
- the other one is injected into the floating gate

⇒ recombination with stored charges

⇒ decrease of the charge

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

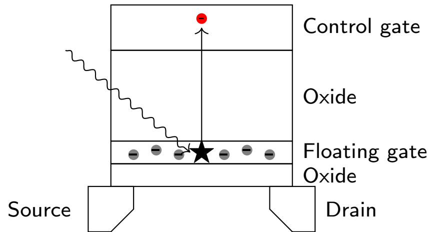


Effect 2

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

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

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

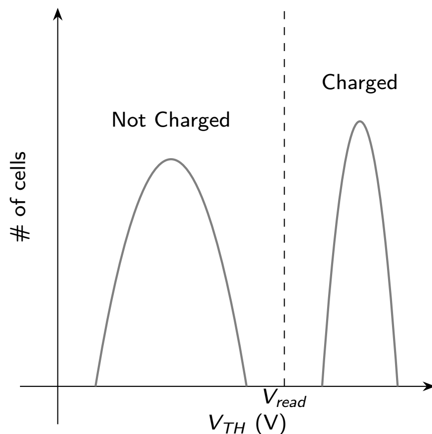
TID mecanisms in floating gate transistor

3 different effects:

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

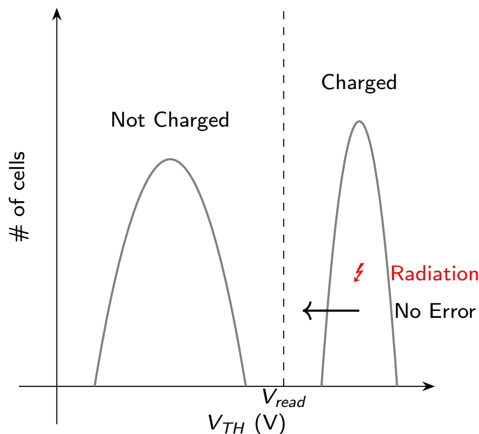
S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Influence of ionizing radiation on the threshold voltage distribution



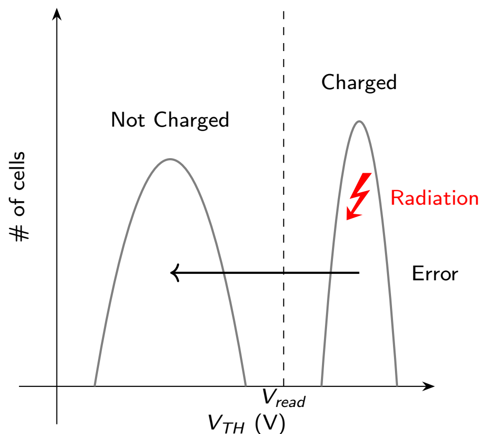
S. Gerardin et al., 'Radiation Effects in Flash Memories', IEEE Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, Jun. 2013

Influence of ionizing radiation on the threshold voltage distribution



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



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

1 Flash memory, floating gate transistor and X-ray effects

2 Experiments
- X-Ray setup
- Targets
- Protocol

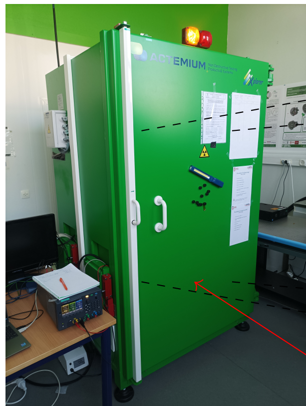
3 Results

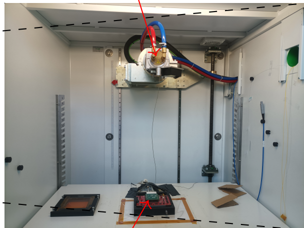
4 Conclusion

Overview

1. Flash memory, floating gate transistor and X-ray effects
2. Experiments
   - X-Ray setup
   - Targets
   - Protocol
3. Results
4. Conclusion

X-Ray irradiator





X-Ray Source

Target

Lead enclosure

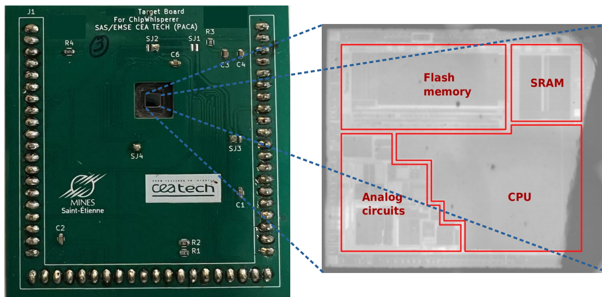
Settings

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

Overview

1. Flash memory, floating gate transistor and X-ray effects
2. Experiments
   - X-Ray setup
   - Targets
   - Protocol
3. Results
4. Conclusion

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

1. Flash memory, floating gate transistor and X-ray effects
2. Experiments
   - X-Ray setup
   - Targets
   - Protocol
3. Results
4. Conclusion

Protocol

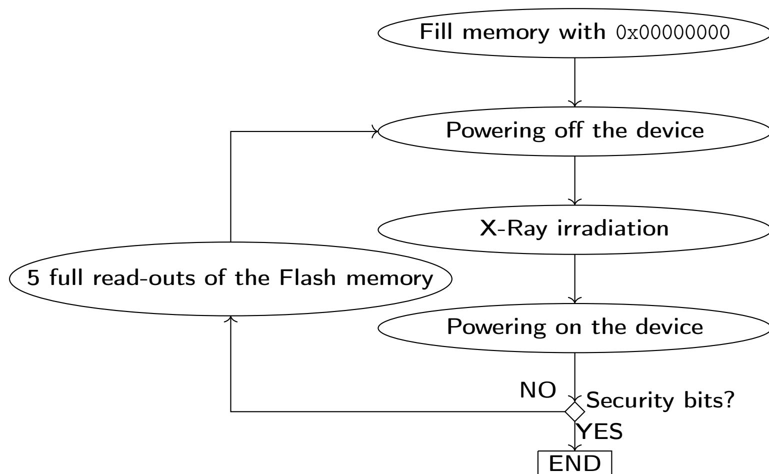


Table of contents

1 Flash memory, floating gate transistor and X-ray effects

2 Experiments

3 Results
- X-Ray effects
- Time and thermal recuperation

4 Conclusion

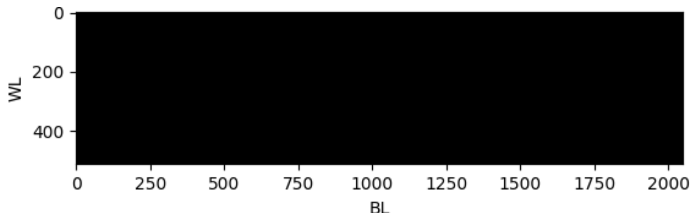
Overview

1. Flash memory, floating gate transistor and X-ray effects
2. Experiments
3. Results
   - X-Ray effects
   - Time and thermal recuperation
4. Conclusion

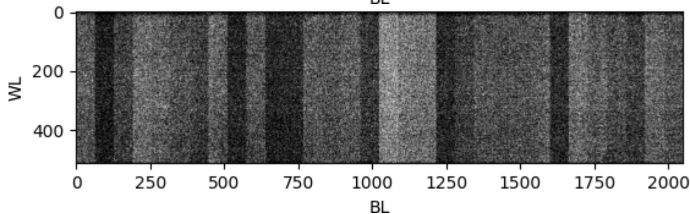
Bitsets in Flash memory

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

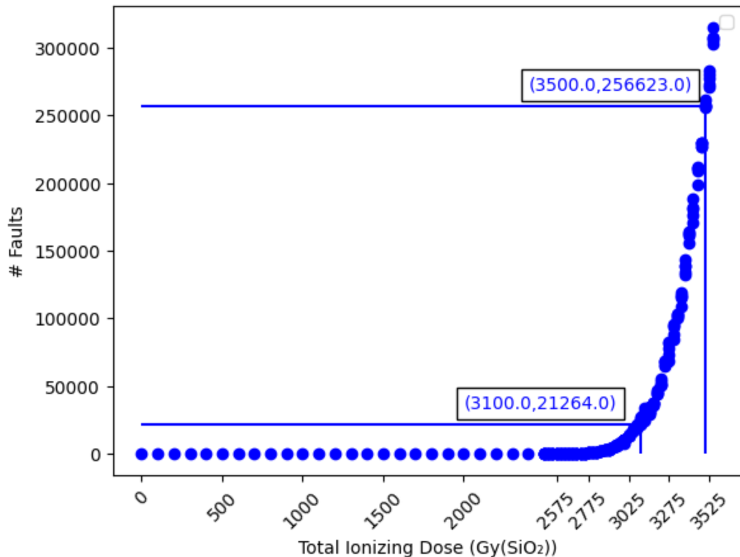
Before irradiation:



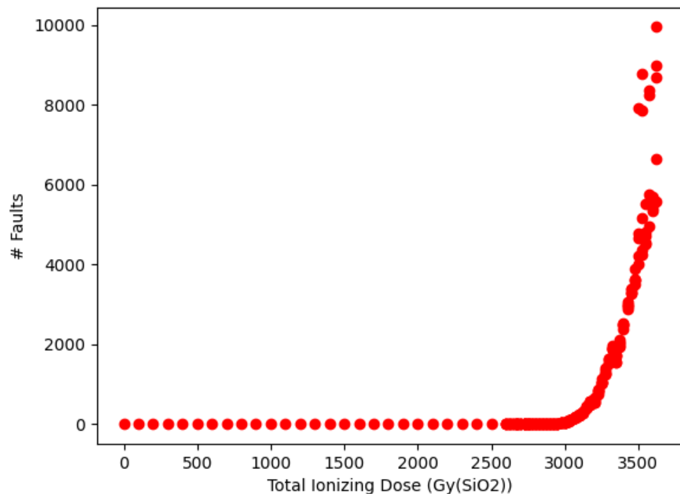
After irradiation:



Faults in Flash memory



Faults in EEPROM memory

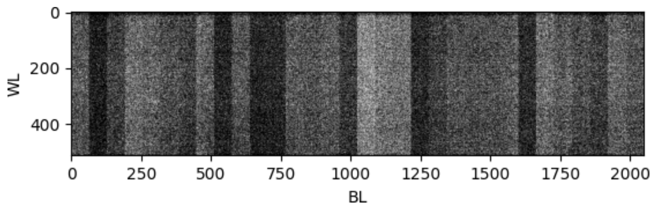


Overview

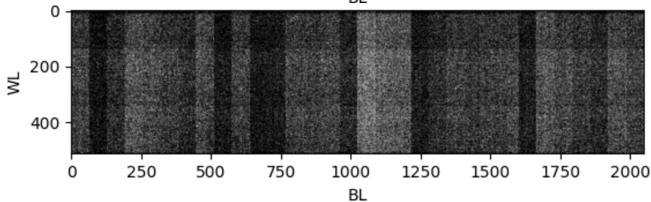
1. Flash memory, floating gate transistor and X-ray effects
2. Experiments
3. Results
   - X-Ray effects
   - Time and thermal recuperation
4. Conclusion

Time and thermal recovery

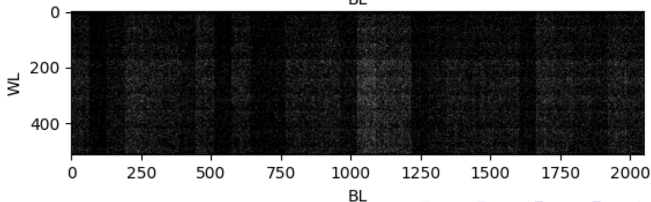
After irradiation:



After time recovery:
7 days @ room temperature



After thermal recovery:
2h @ 150°C



Permanent VS non-permanent faults

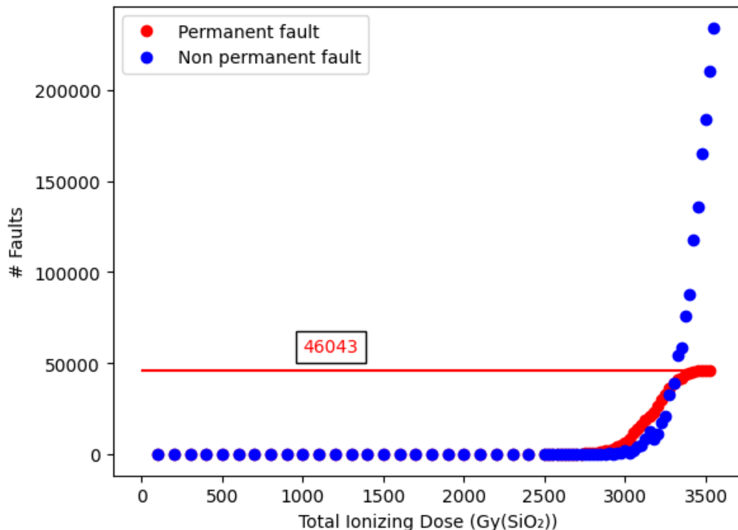


Table of contents

1 Flash memory, floating gate transistor and X-ray effects

2 Experiments

3 Results

4 Conclusion

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

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 acces to the X-Ray source.