X-Ray Fault Injection in Non-Volatile Memories on Power OFF Devices

Paul Grandamme, Lilian Bossuet, Jean-Max Dutertre

Authors' version
PAINE 2023
https://doi.org/10.1109/PAINE58317.2023.10318018

X-Ray Fault Injection in non-volatile memories on Power OFF devices

Paul Grandamme
Laboratoire Hubert Curien UMR 5516,
Université Jean Monnet Saint-Etienne, CNRS,
F-42023, SAINT-ETIENNE, France
paul.grandamme@univ-st-etienne.fr

Lilian Bossuet
Laboratoire Hubert Curien UMR 5516,
Université Jean Monnet Saint-Etienne, CNRS,
F-42023, SAINT-ETIENNE, France
lilian.bossuet@univ-st-etienne.fr

Jean-Max Dutertre
Mines Saint-Etienne
CEA, Leti, Centre CMP
F-13541 GARDANNE, France
dutertre@emse.fr

***Abstract*—For several years, electronic components have taken an increasingly important place in our societies. Their security has become an dominant matter as they can contain sensitive data. To assess their security, new means of fault injection are set up. X-Ray effects on electronic devices have been studied for space applications but only a few recent papers deal with the security point of view. The state of the art shows that X-Ray can more easily have an effect on power off devices than other means of fault injection like laser injection or electromagnetic injection.**

This article gives experimental results on an X-Ray fault injection campaign on power off microcontrollers dedicated for IoT devices. Some of these X-Ray effects on the Flash embedded non-volatile memory of these microcontrollers highlighted in this study can be reversed performing thermal recuperation. This paper substantiates that the number of faults injected in a memory has an exponential dependency with the total ionizing dose according to a bitset fault model.

***Index Terms*—Permanent fault injection, Flash memory, X-Ray, power off attacks, total ionizing dose**

I. Introduction

Electronic devices have been suffering from hardware attacks such as laser fault injection for the past few years.

Indeed, the first effect of light on microcontrollers was shown by Skorobogatov in 2003 by exposing circuits to flash-ligths and laser beams [1]. In 2009, he also demonstrated the erasure of bits value using 650nm wavelength laser by heating the cells. Nowadays, laser fault injection is often considered as one of the most efficient fault injection technique as it provides high temporal and spatial accuracy. On power on devices, the fault model is well understood from the algorithmic level down to the physical level [2], [3].

More recently, electromagnetic injection attacks have also been used to disrupt the device behaviour. The first proposal of fault injection based on EM injection phenomenon is [4]. An experimental demonstration is made in [5] and improved in [6] with a strong temporal and spatial precision.

These two types of attacks require the circuit to be powered on. However on-board sensors can detect fault injection as proposed in [7]. However, they cannot protect a power-off device which open a novel attack path : injecting fault when the power source is switched off. Thus it is interesting to evaluate X-Ray impacts on power off devices.

This work in funded by a French ANR program, along with the project POP (ANR-21-CE390004)

X-Ray effects on electronic devices have been studied for space applications [8], [9] but only a few papers deal with security applications [10], [11].

In this paper, we incrementally irradiate a powered off device and evaluate the X-Ray effect on non-volatile Flash memories. Embedded Flash memories are used to store microcontrollers' program and security features (e.g. cryptographic keys, access rights, etc.). Hence, the assessement of their vulnerability to faults injected through X-Ray exposure is a security concern. We highlight an exponential dependency between the total ionizing dose and the number of faulty bits in the memories.

The rudiments the operating principles of Flash memories and radiations effects are explained in Section II. Section III describes the experimental setup and method used. Section IV analyses experimental results with respect to the fault mechanism. Lastly, Section V reports the encountered limitations and improvements to be made.

II. Backgrounds

This section recalls the operation of non-volatile Flash memory and of the floating gate transistors that are used to store data bit of information. It also describes the effects of radiation on them.

A. Flash Memory and floating gate transistors

In microcontrollers, all permanent data are stored in non-volatile memories like EEPROM or Flash. Both have the same main parts. The high-level architecture of these memories is depicted in Figure 1.

They use floating gate transistors to store information. There are two main types of Flash memory: NOR and NAND. NOR Flash architecture provides enough address lines to map the entire memory range. This gives the advantage of random access and short read times, which makes it ideal for code execution. NAND Flash architecture does not permit random access and has shorter write and erase times, which makes it ideal for data storage. The elements targeted in this study, the floating gate transistors, do not change from one type of Flash memory to another. Hence, the results of this study can be applied to both types of Flash memory. This study only deals with NOR Flash memory as they are the ones used in

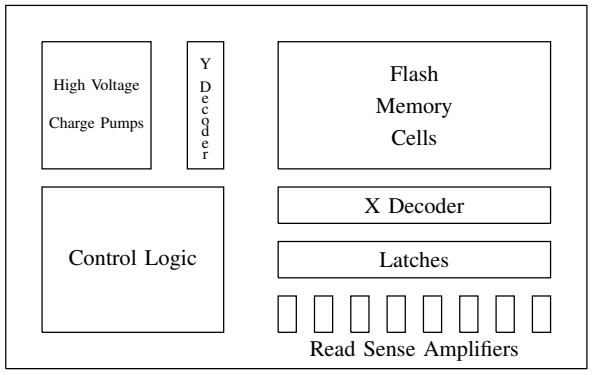

Fig. 1. Usual organization of Flash memories [12].

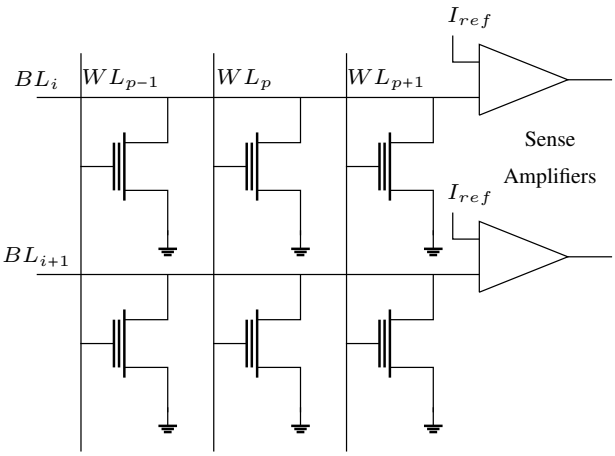

Fig. 2. Simplified layout of NOR Flash memory.

microcontrollers. The simplified layout of the latter can be seen in Figure 2. The control logic manages the mapping between the logical and physical addresses and then selects the cells by controlling the X and Y decoders. The sense amplifiers are used to compare the current drawn with a current reference to determine whether the selected cell is programmed or erased. The memory usually contains as many sense amplifiers as the width of the data bus. For instance, in order to fetch one 32-bit word, one wordline (WL) and 32 bitlines (BL) have to be selected. High voltages are required to modify the content of Flash memories (through erase and program steps), especially for the control logic and the charge pumps. Therefore, it is necessary to place the Flash memory outside the rest of the chip logic. It makes it easier for an attacker to locate the Flash memory.

Figure 3 shows the simplified structure of a floating gate transistor. A charge storing element is added in the oxide layer between the control gate and the silicon bulk. This floating gate is electrically isolated from the rest of the structure. When charges are stored in the floating gate, the field created by the carriers bends the oxide energy bands. The presence of charges in the floating gate defines the state of the cell by affecting its threshold voltage. To read the content of a cell the control

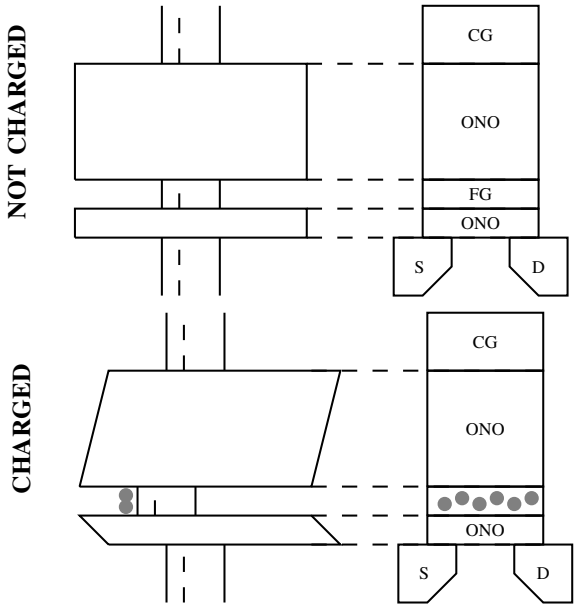

Fig. 3. Simplified view of a floating gate transistor with corresponding energy band diagram (adapted from [13]).

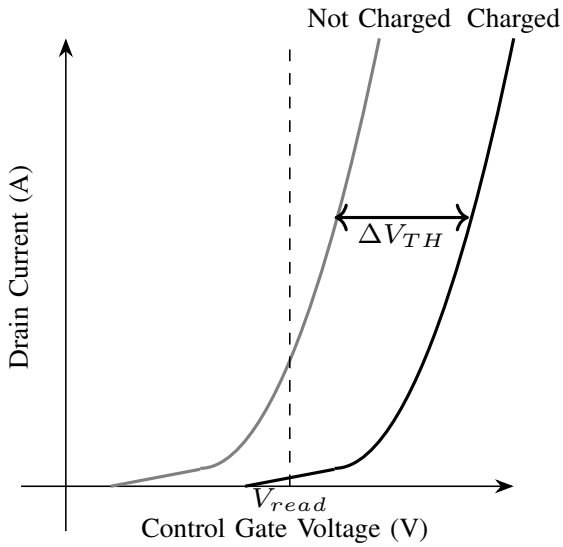

Fig. 4. I-V characteristics for floating gate transistor (adapted from [13]).

gate is biased at a fixed voltage V_{read} (between the threshold of a charged cell and an uncharged cell) and the current drawn by the cell is compared to a reference by the sense amplifier. The carriers stored in the floating gates generate a shift in the I-V characteristics of the cell as represented in Figure 4.

Thus if we manage to alter the stored charge in the floating gate, we can change the state (programmed or erased) of the cell.

B. X-Ray effects on floating gate transistors

X-Ray are a form of electromagnetic radiation made up of photons. Effects of X-Ray on electronic devices can be divided

in two parts: the cumulative effect and the transient effect. In this work, we study the effect of radiation on power off devices. Thus we can ignore transient effects.

This study focuses on the *Total Ionizing Dose* (TID) effect. When a photon collides with an atom of the material, a high energy electron in generated by photoelectric effect. This electron generates electron-hole pairs along his path into the material. These charges lead to an error in a floating gate cell when the ionizing dose induces a threshold voltage shift large enough to bring the cell threshold voltage below the read voltage as represented in Figure 5. If the shift is not sufficient the cell remains unfaulted. Near the threshold voltage V_{read}, the cell may be unstable *i.e.* read once like charged once like discharged.

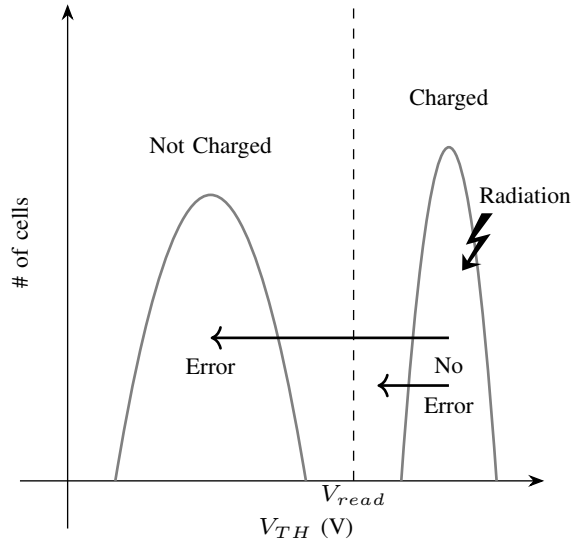

Fig. 5. Influence of ionozing radiation on the threshold voltage distribution (adapted from [13]).

In the literature, three phenomena are identified as responsible for the TID response of a floating gate transistor [13]. They are represented in Figure 6 and detailed below:

1) the electron-hole pair created by radiation is separated by the electric field present in the oxides. One of the charges can escape through the control gate and the other one is injected into the floating gate. The latter can recombine with the stored charges into the floating gate and thus decrease the amount of charge in the floating gate.
2) the charge can be trapped in the tunnel oxide.
3) the charges in the floating gate get enough energy from the radiation to escape from the potential well. It is called *photoemission*.

The second phenomenon is not significant because of the small thickness of the oxides. The first one needs an electric field in the oxides so it can not happen in power off devices, while the last one is considered as the main effect on power off devices.

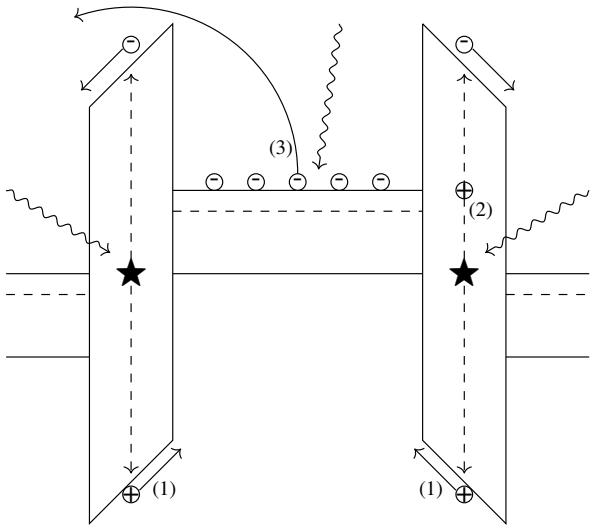

Fig. 6. TID mecanisms in floating gate transistor [13].

C. X-Ray effects on MOS transistors

In MOS transistors, electron-hole pairs can also be created by X-Ray exposure. Created charges can be trapped in the oxide of the transistor. This accumulation of charges near the transistor channel generates a shift in the transistor's characteristic curve $I_D = f(V_{GS})$ and especially in the threshold voltage V_{TH} of the transistor. This is also a TID effect: the more the device is irradiated, the more charges are trapped and the $I_D = f(V_{GS})$ curve shifted. This effect can be recovered with thermal annealing and affects all the MOS transistors on the device including those in the Flash memory control logic (X,Y decoders, read sense amplifiers, ...). When affected, NMOS transistors are more likely to conduct. They can even become permanently conducting, while PMOS transistors are more likely to block and even to become permanently blocking[10], [11]. This effect impacts the value read from the Flash memory instead of the value stored in the Flash memory.

All these elements suggest that X-Ray injections can be useful in the framework of power-off attacks. The next section describes this study's conducted experiments.

III. Experimental method

This section is focused on the description of our experimental setup including the X-Ray irradiator, our targets and the protocol we followed.

A. X-Ray setup

Figure 7 shows the irradiator which contains an X-Ray tube of the Comet MXR-165 type with a tungsten (W) anode. The irradiations are carried out at room temperature. The source has a voltage of 100kV and a current of 45mA which generate 40keV-energy photons. A dosimetry with a ionization chamber PTW23344 had been done before each experiment to ensure repeatability and to make sure that the radiation level

corresponds to the setpoint. More details on the operation of X-Ray sources can be found in [14].

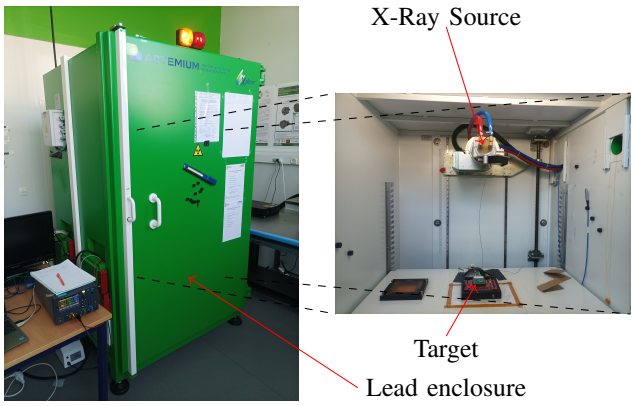

Fig. 7. Picture of the irradiator

B. Targets

The hardware target is a 32-bit microcontroller placed on a custom board for a ChipWhisperer platform [15]. The target was initially planned for laser fault injection,thus it was prepared for backside access [16]. The microcontroller embeds an ARM Cortex-M3 core and 128kB Flash Memory. For this device, the *erase* state of the Flash memory is represented by the value `0xFFFFFFFF` at 32-bit word level. A picture and an infrared picture of the target can be seen in Figure 8. The mapping between the physical location and the logical address of the data is described in [3]. The Flash memory contains 2048 bitlines and 512 wordlines. This device contains security features such as security bits preventing anyone from reading the memory when activated. Disabling these security bits results in a complete erasure of the memory if it is done with software.

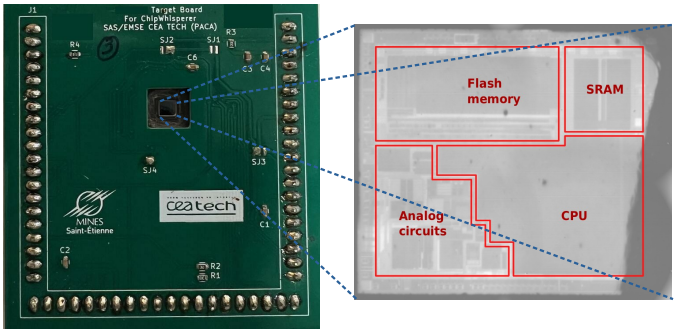

Fig. 8. Picture of the hardware target (left) and infrared image of the DUT (right).

C. Experimental protocol

Previous experiments had been done on a powered off device with a Flash memory filled with a `0x55555555` pattern at a 32-bit word level. It showed that all obtained faults are unidirectional : only bitsets (change from a 0 value to a 1 value) can be done. That is why we chose to follow the protocol described below. The same protocol has been used during these study's experiments and is described in Figure 9. First, we filled the memory with a `0x00000000` pattern before powering off the device. Then we irradiated the device. After the irradiation, the device was powered on and if the security bits were not enabled, the memory was read 5 times to evaluate the instability for the cells for which $V_{TH} \approx V_{read}$.

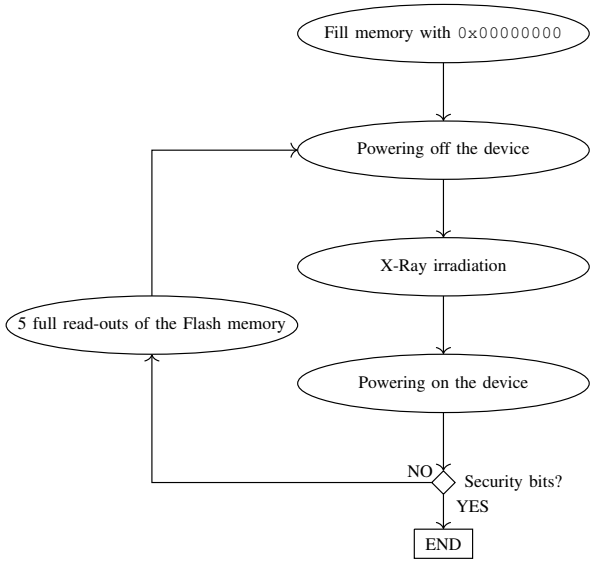

Fig. 9. Experimental protocol.

IV. Experimental Results

A. X-Ray effects on non-volatile memories

All results described in this part are obtained on three similar devices. Experiments are done with a dose rate of 1 Gy(SiO_2)/s. First, the component is irradiated with a step of 100 Gy(SiO_2) and then, when the first faults appeared, with a step of 25 Gy(SiO_2). Figure 10 presents the evolution of the number of faults injected in the Flash memory. Each blue dot corresponds to a Flash memory read out. The first faults appear around 2525 Gy(SiO_2). An exponential dependency of the number of faults w.r.t. the total ionizing dose can be observed. At the end of the experiments, around 300,000 bits are faulty which corresponds to approximately a third of the Flash memory. Experiments were stopped when security bits began to be faulty. If the latter are permanently faulty, the Flash memory can not be read without a prior erase.

One can see that for a given dose the number of faults is not constant but is of the same order of magnitude. For instance, on Figure 10, the five dots circled in red correspond to the same radiation dose. It means that some bits are unstable. Figure 11 shows the evolution of the permanent faults and the unstable bits with the total ionizing dose. It can be seen that the number of permanently fautly bits reaches a threshold.

Similar results are obtained on an EEPROM memory of another component and can be seen on Figure 12. Such

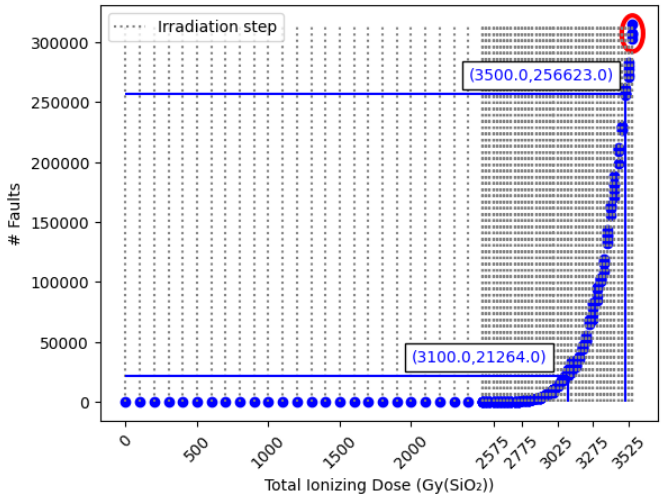

Fig. 10. Evolution of the number of faults in the Flash memory during x-Ray irradiations. Each blue dot corresponds to a Flash memory acquisition.

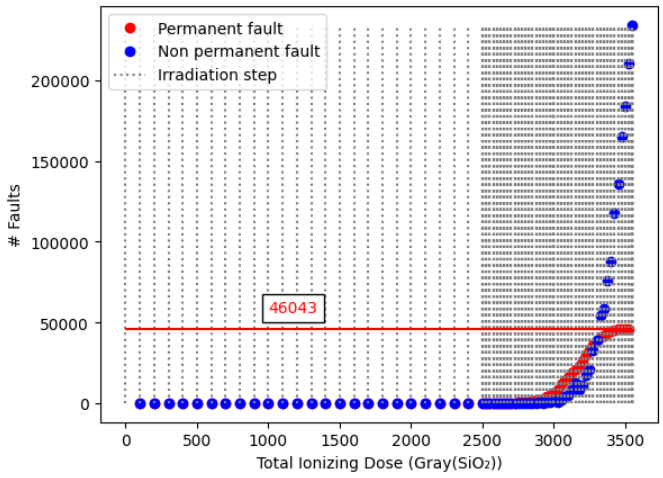

Fig. 11. Evolution of the number of permanent in red and non permanent faults in blue in the Flash memory.

memory also uses floating gate transistors to store information (though it slightly differs and is older).

Figure 13 shows the physical location of the faulty bits highlighted by white dots in the Flash memory. Each vertical band contains all the bits for a given index of the 32-bit data words. For instance, the first one contains all the bits at index 0, the second one all the bits at index 1 and the last one all bits at index 31. If the faults were only due to the discharge of the floating gate transistors, a uniform distribution of faults would have been obtained. One can easily observed that some vertical bands are lighter than other which means that some elements outside the Flash memory cells (X,Y decoders or read sense amplifiers) are also faulty. We assume that a threshold voltage drift of MOS transistors of analogue parts is responsible for this phenomenon.

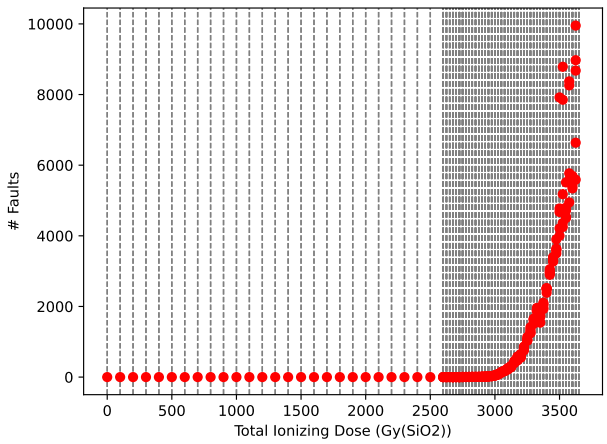

Fig. 12. Evolution of the number of faults in the EEPROM memory during X-Ray irradiations. Each red dot corresponds to an EEPROM memory acquisition.

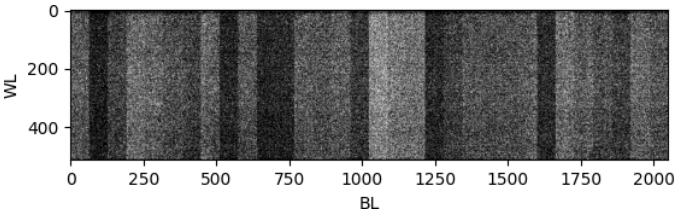

Fig. 13. Bitsets in Flash memory. White dots represent value 1, black dots represent value 0.

To sum up, we managed to create faults due to the discharge of floating gate transistors with the photoemission effect and faults due to threshold voltage shift of MOS transistors.

B. Temporal and thermal recovery

X-Ray effects are known to be reversible with time and temperature. In order to evaluate the recuperation of the radiation, one of the irradiated circuit was left to rest at room temperature for several days. Figure 13 depicts the memory after irradiation and before recovery. Figure 14 shows the state of the Flash memory after time recovery. It can be seen that the latter picture is darker than the previous one meaning that there are less faulty bits. Moreover, we can see new horizontal pattern showing that the control logic of the wordlines does not recover evenly.

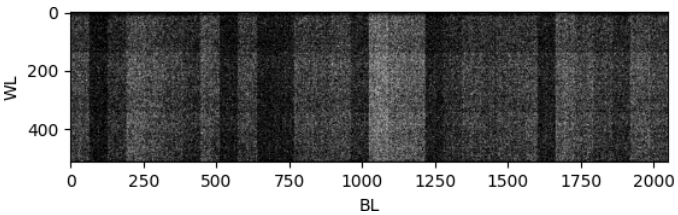

Fig. 14. Bitsets in Flash memory after time recovery. White dots represent value 1, black dots represent value 0.

Lastly, a thermal recovery was done by heating the same device at 150°C for 2 hours in a heat chamber after X-Ray exposure and time recovery. Figure 15 shows the state of the same memory after thermal recovery. Once again we can see that there are even fewer errors. The horizontal phenomenon is even more pronounced.

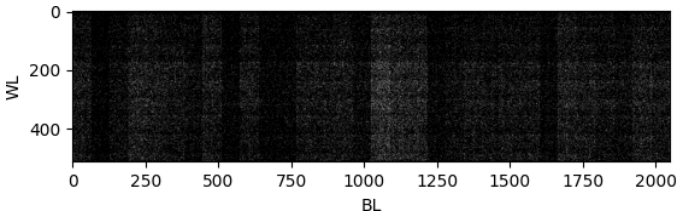

Fig. 15. Bitsets in Flash memory after time recovery. White dots represent value 1, black dots represent value 0.

To conlude, Table I shows that a significant drop of the number of faulty bits can be observed. Thus, we can conclude that a short but high temperature recovery is more effective than a long recovery at room temperature.

TABLE I
TEMPORAL AND THERMAL RECOVERY

	# faults in bits	decrease
End of X-Ray irradiation	≃ 300,000	-
After Time Recovery (around a week)	≃ 225,000	-25%
After Thermal Recovery (2h at 150°C)	≃ 70,000	-69%

The remaining faults are those due to Flash memory's floating gate transistor's discharge and slightly change over time. All faults that have disappeared with the recoveries are due to threshold voltage shift of MOS transistor which make up the read sense amplifiers because recoveries can not restore charges into the floating gate transistors.

V. DISCUSSION

A. X-Ray-focused injection

Designing a mask following described method in [10] and [11] could add protection for specific parts of the memory. The main constraints are the dimensioning, the making and the placement of the mask. Lead (Pb) is the best candidate. A lead mask could protect security bits from radiations and allow an attacker to fault the whole memory and, in the bast case, to fault specific bits. This could be very interesting for encryption algorithm attack. For instance, we could imagine setting a cryptographic key to a known value. This practice has also been used in UV light attacks on EEPROM memory, using an ink mask to reveal the mapping between logical and physical addresses [17].

B. Security Bytes

For the component we chose, two bytes are used to store the value allowing or not to read the Flash memory content. One is the two's complement of the other. The default value (allowing reading the memory) of these bytes are composed of bits sets to 1 and bits sets to 0. Therefore with our unidirectional fault model we can not downgrade the security level because we should set bits to 1 and other bits to 0. Other components with not well implemented security bits will also be investigated. Indeed, it is possible that X-Ray effects lower the level of security of the memory protection *i.e.* enable the reading, writing or erasing of the memory.

VI. CONCLUSION

This paper demonstrates the efficiency of X-Ray faults injection on Flash and EEPROM memories of power off devices. An exponential dependency between the total ionizing dose and the number of faults injected is highlighted. A fault model according to the experimental results is also described. In addition, it is shown that a thermal annealing is possible and corrects the major part of the faults.

ACKNOWLEDGMENT

The experiments were carried out thanks to the MOPERE team of the Hubert Curien Laboratory at the University of Saint-Etienne. This work was supported by a research grant from the french Agence Nationale de la Recherche (POP project, ANR-21-CE390004).

REFERENCES

[1] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers* (B. S. K. Jr., Ç. K. Koç, and C. Paar, eds.), vol. 2523 of *Lecture Notes in Computer Science*, pp. 2–12, Springer, 2002.

[2] B. Colombier, A. Menu, J. Dutertre, P. Moëllic, J. Rigaud, and J. Danger, "Laser-induced single-bit faults in flash memory: Instructions corruption on a 32-bit microcontroller," in *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2019, McLean, VA, USA, May 5-10, 2019*, pp. 1–10, IEEE, 2019.

[3] A. Menu, J. Dutertre, B. Colombier, J. Rigaud, P. Moëllic, and J. Danger, "Single-bit laser fault model in NOR flash memories: Analysis and exploitation," in *17th Workshop on Fault Detection and Tolerance in Cryptography, FDTC 2020, Milan, Italy, September 13, 2020*, pp. 41–48, IEEE, 2020.

[4] D. Samyde, S. P. Skorobogatov, R. J. Anderson, and J. Quisquater, "On a new way to read data from memory," in *Proceedings of the First International IEEE Security in Storage Workshop, SISW 2002, Greenbelt, Maryland, USA, December 11, 2002*, pp. 65–69, IEEE Computer Society, 2002.

[5] J.-M. Schmidt and M. Hutter, "Optical and em fault-attacks on crt-based rsa: Concrete results," in *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pp. 61–67, Verlag der Technischen Universität Graz, 2007. Austrochip 2007 ; Conference date: 11-10-2007 Through 11-10-2007.

[6] F. Poucheret, L. Chusseau, B. Robisson, and P. Maurine, "Local electromagnetic coupling with cmos integrated circuits," in *2011 8th Workshop on Electromagnetic Compatibility of Integrated Circuits*, pp. 137–141, 2011.

[7] E. H. Neto, I. Ribeiro, M. G. Vieira, G. I. Wirth, and F. L. Kastensmidt, "Using bulk built-in current sensors to detect soft errors," *IEEE Micro*, vol. 26, no. 5, pp. 10–18, 2006.

[8] R. Micheloni, L. Crippa, and A. Marelli, *Inside NAND Flash Memories*. Springer Science, 2010.

[9] G. Cellere, A. Paccagnella, A. Visconti, M. Bonanomi, S. Beltrami, J. R. Schwank, M. R. Shaneyfelt, and P. Paillet, "Total ionizing dose effects in nor and nand flash memories," *IEEE Transactions on Nuclear Science*, vol. 54, no. 4, pp. 1066–1070, 2007.

[10] S. Anceau, P. Bleuet, J. Clédière, L. Maingault, J. Rainard, and R. Tucoulou, "Nanofocused x-ray beam to reprogram secure circuits," in *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings* (W. Fischer and N. Homma, eds.), vol. 10529 of *Lecture Notes in Computer Science*, pp. 175–188, Springer, 2017.

[11] L. Maingault, S. Anceau, M. Sulmont, L. Salvo, J. Clédière, P. Lhuissier, E. Beliard, and J. Rainard, "Laboratory x-rays operando single bit attacks on flash memory cells," in *Smart Card Research and Advanced Applications - 20th International Conference, CARDIS 2021, Lübeck, Germany, November 11-12, 2021, Revised Selected Papers* (V. Grosso and T. Pöppelmann, eds.), vol. 13173 of *Lecture Notes in Computer Science*, pp. 139–150, Springer, 2021.

[12] S. Skorobogatov, "Optical fault masking attacks," in *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010, Santa Barbara, California, USA, 21 August 2010* (L. Breveglieri, M. Joye, I. Koren, D. Naccache, and I. Verbauwhede, eds.), pp. 23–29, IEEE Computer Society, 2010.

[13] 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*, vol. 60, no. 3, pp. 1953–1969, 2013.

[14] J. A. Seibert, "X-ray imaging physics for nuclear medicine technologists. part 1: Basic principles of x-ray production," *Journal of Nuclear Medicine Technology*, vol. 32, no. 3, p. 139–147, 2004.

[15] C. O'Flynn and Z. D. Chen, "Chipwhisperer: An open-source platform for hardware embedded security research," in *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers* (E. Prouff, ed.), vol. 8622 of *Lecture Notes in Computer Science*, pp. 243–260, Springer, 2014.

[16] R. S. Lima, R. Viera, J.-M. Dutertre, A.-L. Ribotta, M. Pommies, and A. Bertrand, "Target preparation methodology for semi-invasive attacks on microcontrollers," in *2022 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pp. 1–7, 2022.

[17] J. J. Fournier and P. Loubet-Moundi, "Memory address scrambling revealed using fault attacks," in *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp. 30–36, 2010.