Laboratory X-rays operando single bit attacks on flash memory cells

L.Maingault[1], S. Anceau[1], M. Sulmont[1], L.Salvo[2], J. Clediere[1], P. Lhuissier[2], E.Beliard[1], J.L. Rainard[1]

[1] CEA-Leti, 17 av. Des Martyrs 38054 Grenoble, France
[2] Université Grenoble Alpes, CNRS UMR5266, Grenoble INP, Laboratoire SIMaP, 38000 Grenoble, France

Abstract. The need to increase the level of digital security standards requires a sustained research effort on new means of perturbations likely to disturb the processing of integrated circuits. X-rays modification is a powerful semi-permanent fault injection technique with a high spatial accuracy, which allows an adversary to modify efficiently secret data from an electronic device. Experimental results demonstrate that several semi-permanent bit erase faults can be injected in code and data with corrupting flash memory, even with an X-rays spot from an X-rays laboratory source of less than 10 µm in diameter. This is the order of magnitude of 15 memory cells with a process node of 350 nm in the presented experiments. The article also presents the specificity of performing an X-rays attack without the need of a synchrotron-focused beam, as presented in CHES 2017[1].

Keywords: X-rays, physical attacks, cybersecurity,

1 Introduction

The possibility of using visible and IR light to perform attack on integrated circuit was revealed by Skorobogatov and Anderson [2]. The physical phenomena have been studied and explained by the failure-analysis community [3-6]. Laser light can be synchronized and focused in order to induce transient and persistent faults. During the security-evaluation practice, these attacks may give powerful results. In order to further investigate the wavelength spectrum of perturbations, it is proposed here to study the effects of ionizing radiation like X-rays. Compare to fault perturbations induced in a circuit by a laser light, where the spot size is few microns, X-rays beam allows to obtain a spot size down to 50 nm using synchrotron source and down to 400 nm in laboratory nano sources. This is therefore more suitable to modify one single transistor for the most advanced technology mode. It is physically possible to modify one single bit transistor with the X-rays and the limitation is only coming from the way used to focus the beam. Security countermeasures can be deactivated in the flash block memory or the registers in the glue logic for example. The second advantage of X-rays is their potential to penetrate deeply through materials and induced semi-permanent faults on flash memory cells and NMOS transistors. The X-rays beam can penetrate through the plastic or ceramic package, through the front

side active shield of the circuit or the backside die paddle. This semi-permanent perturbation of the X-rays is completely reversible with a simple heat treatment in a classical oven and no physical modification is visible after the X-rays perturbations. X-rays interaction with electronic circuits has been analyzed [7-22], but its use for security evaluation has been mainly restricted to die and package imaging or occasional perturbation with no practical success [23-24] before the single bit semi-permanent fault injections performed at the European synchrotron facility in Grenoble [1].

Since the late 90s, the flash memory cells are known to be vulnerable to the cyber attacks of secure integrated circuits. However, significant improvements have been done to secure electronic devices: The stored data, that often contains critical secret keys, is indeed now ciphered and scrambled in the flash memory blocks. Nowadays it is difficult to reread the flash memory content for the actual technology node. It is therefore interesting to develop another method for the modification of the memory content. This document demonstrates the feasibility of semi-permanent X-rays modifications of localized several flash memory cells using backside and frontside attack with laboratory X-rays source. For the purpose of this article, we chose to attack ATmega128P devices. Despite its large technology node compared to standard devices in the cybersecurity field, it is a perfect demonstrator of an attack feasibility. Furthermore, the availability in DIP packages allows to easily decapsulate the target device and, even if the device is damaged by the X-rays fault injection, it can easily be replaced. We will first present the methods to prepare the circuit for X-rays attacks, the methodology of an attack with a laboratory X-rays source and the results obtained using both backside and frontside attack.

2 Materials and methods

2.1 Preparation of integrated circuit ATmega128P for X-rays attack

In this work, we target an 8-bit AVR microcontroller, the Atmel ATmega128P. It has 128 kB of flash memory, 4 kB of EEPROM and 4 kB of RAM. The technology node is 350 nm and the 128 kB flash memory block is visible on the right part of **Fig. 1**.

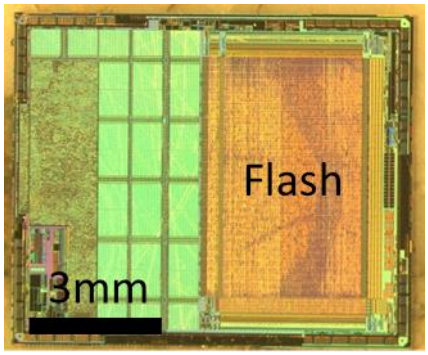

Fig. 1. : ATmega128P integrated circuit after package removal.

The backside of the chip's package together with the copper paddle was removed using a cheap ASAP milling machine. The metal connections of the package are returned to the opposite side: each connection is brazed to strengthen the connection in order to avoid any breakdown during multiple manipulations (**Fig. 2**).

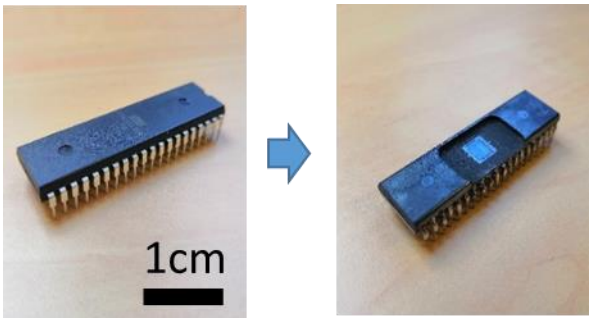

Fig. 2. ATmega128P device sample without preparation (left picture). The ASAP milling machine for the device backside thinning is used and the ATmega128P device backside pads are returned and milled (right picture).

The device protection shown in **Fig. 2** relies on four steps::

i. Deposition of 20 µm thickness W over 300 µm diameter on the flash memory.
ii. Drilling of a 10 µm diameter hole into the W layer.
iii. A square Pb foil (1 cm × 1 cm) with thickness of 300 µm is drilled to make a hole of 250 µm.
iv. The Pb foil is placed over the W deposit in order to protect the circuit and keep the 10 µm hole visible.

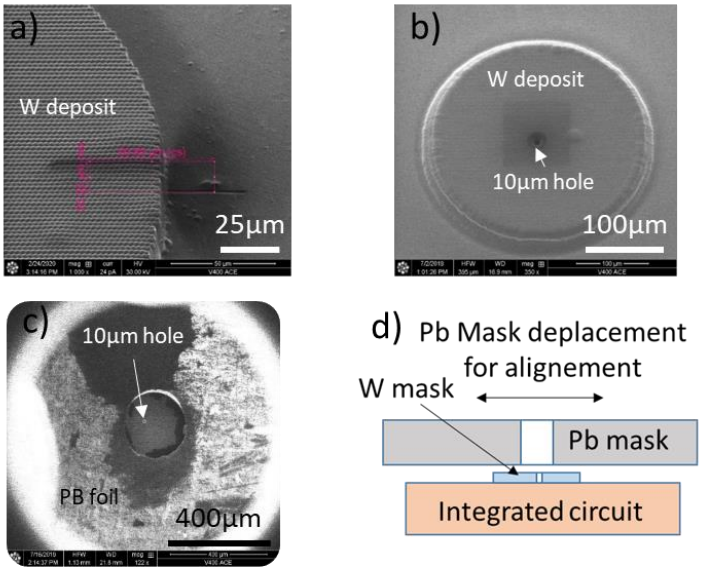

Fig. 3. (a) Thickness measurement of the W mask deposited on the ATmega128P device backside surface. (b) 10 µm diameter hole visible on the same W mask used for the X-rays focalization. (c) Lead mask shown on the circuit. (d) Principle of Pb mask alignment

Step (i) is performed with a V400 Focused Ion Beam (FIB). We put the sample on the right part of on a sample holder inside the FIB vacuum chamber. The sample holder is custom made and its dimensions are optimized for the following experimentation. First, the backside memory block is localized thanks to an in-situ infrared camera. Then gas is injected for the circle deposition of tungsten thickness of 20 µm localized in the center of the memory block on the backside surface of the device. The precise positioning in the center of the memory block is possible thanks to the piezoelectric XY table with a movement precision of 0.2 µm. The thickness of the deposited tungsten layer is measured with a quick etching of a single line on the border of the tungsten deposition layer. The sample is then tilted to an angle of 45° inside the FIB vacuum chamber. The diameter of the W deposit is 300 µm. We check the diameter and the thickness value of the tungsten (W) mask and the result is visible on the left picture of the **Fig. 3**.

Step (ii) is also performed in the V400 FIB using a 65 nA current without any gas. 2 hours are required to make a hole of 10 µm diameter and 20 µm thickness in the W deposit. The hole can be seen in **Fig. 3** (b).

Step (iii) the Pb foil is drilled with a 200 µm drill bit using a conventional tabletop drilling machine.

Step (iv) The Pb foil is superposed on the Tungsten (W) mask under the inversed optical microscope on the backside sample surface. For that, the sample is fixed under the microscope with several stickers. Then the Pb foil is positioned slowly and we check that

there is a good superposition of the two masks. Then we use a transparent UV light polymerization glue in order to fix the Pb foil in the right position. The viscosity of the UV sticker is correct for the border fixation of the Pb foil on the backside device surface at the right position. We still check with the microscope that the Pb foil does not move under the microscope during the glue polymerization. The result of the Pb and W foil superposition is visible in **Fig. 3** (c).

2.2 X-rays source laboratory :

We used an Hamamatsu nano-tube with Lab6 and Mo target. Operating condition was 40kV with 1.9W in large spot configuration (meaning a focus of the spot of around 2 µm). Imaging is done with a Varian flat panel allowing to easily see the W hole made with the FIB. The experimental setup, the principle of attack on the sample and a radiograph of the system are shown in **Fig. 4**. Bright pixels in a very small area are visible and correspond to the position of the 10 µm diameter of W mask hole on the surface of the ATmega128P backside device (see arrow). The shape around the W mask corresponds to the PCB soldering X-rays picture in transmission on the dedicated electronic card.

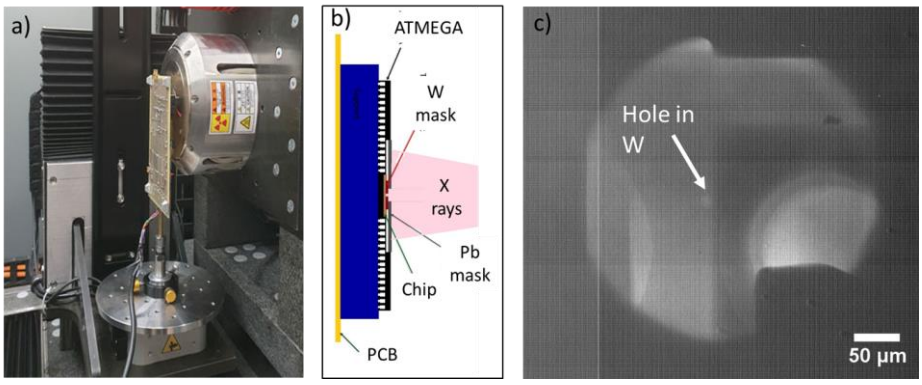

Fig. 4. (a) Experimental setup of the X-rays source laboratory experiment. The ATmega128P sample electronic PCB mounted near the nano X-rays source. (b) Transmission image of the component with the 10 µm hole can be seen in (c).

2.3 Operando analysis of ATmega128P device during X-rays exposure

Two interfaces have been made for the frontside and the backside of the device in order to use a PC with a USB port for the functionality exploitation of the ATmega128P device. Python programs have been developed for the CESTI laboratory in order to write and read the flash memory block of the ATmega128P device. We used PyQt5 for the GUI, numpy and matplotlib for data treatment and image visualization and library Ftd2xx to communicate with the Atmega circuit. This program detects the faulted errors during the

reading sequence and allows the visualization of the faults during the experiment. It is possible to follow in operando the fault that are created. **Fig. 5** presents the program interface. The first window on the left allows connecting to the circuit, program the flash and read it. The log windows indicates at each pass the number of faulted bits and the last window is an image of the faulted memory cells.

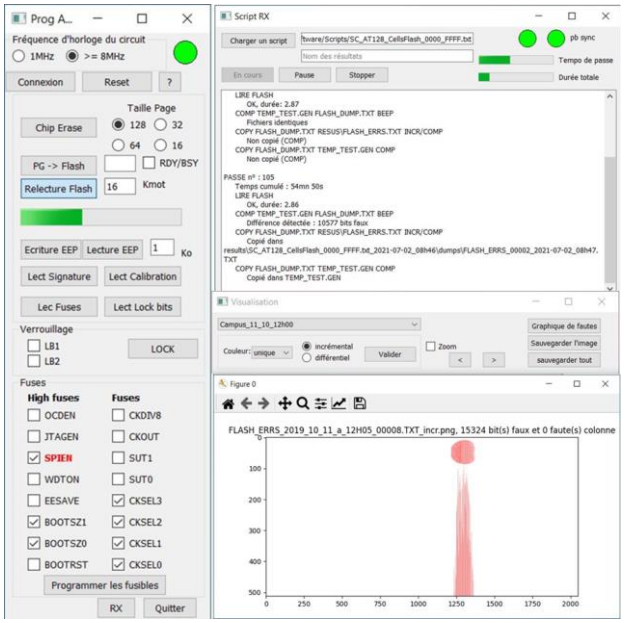

Fig. 5. : Interface of the program controlling the operando experiment

3 Results and discussion

Fig. 6 presents the number of faults created at each time as well as some images showing the fault location during backside X-rays attack. The first faults are observed after 520 s and two bits were faulted as it can be seen on the image shown in **Fig. 6**.

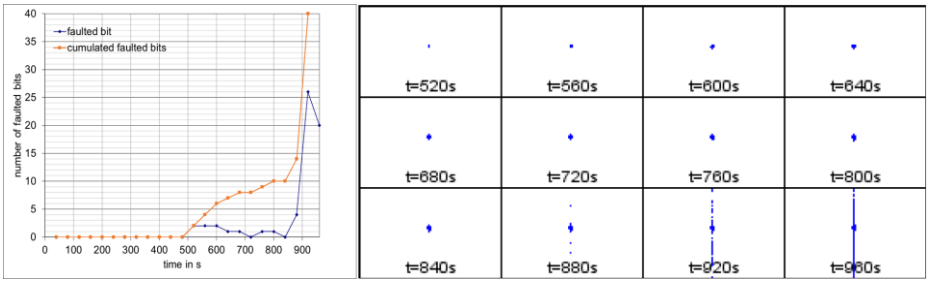

Fig. 6. : Number of faulted transistors with various X-rays exposure duration and visualization of the faulted transistors.

The first part of the faulted results (before 880 s) correspond to the floating gate transistor erasing: electrons are evacuated from the floating gate to the substrate as shown on the left of **Fig. 7**. The second part of the faulted results appears at 880 s where columns start to be faulted. This type of fault transistors correspond to the semi-permanent conduction of the NMOS transistors. These transistors correspond to the NMOS access transistors of each memory cell and the permanent conduction of the NMOS transistor. The ionization of the oxide layer between the NMOS transistor generates positive charge at the interface with the substrate. This induces electron leakage in the substrate channel at the interface as shown on the two figures on the right of **Fig. 7**. These erase and conduct phenomena are well explained in the aerospace applications studies in which radiation naturally occurs and prevents chips from functioning properly. All these extensive effect studies are used for the protection of the devices in the space environment [7-22]. The so-called semi-permanent effect is based on the fact that a simple one-hour heat annealing treatment at 150°C allows recovering the previous device functional behavior [1]. However, if the X-rays irradiation lasts too long it will be impossible to retrieve the initial behavior.

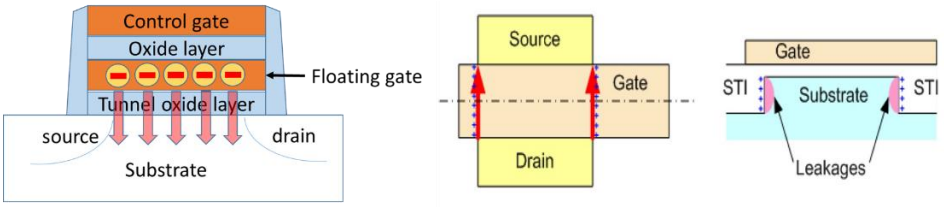

Fig. 7. Erased memory cell mechanism illustration (left image) and permanent conductivity mechanism of the NMOS access transistor illustration (right images) [ref pour le images?]

The functionality of the flash memory block is presented on **Fig. 8**. On the left, it is possible to see the erased cells faulted results and on the right, the NMOS access transistor faulted result. The evolution of the corruption with time exposure is shown on **Fig. 8**. After 520 seconds, the memory cells in the W mask hole are corrupted and the floating gates of the memory cell transistors are emptied thanks to the photoemission of carriers stored in the floating gates. This result is visible during the reading of the corresponding line of the corrupted memory cells. After 880 seconds, the access to any line of the exposed array is corrupted due to these NMOS transistors that are conductive, even if the corresponding line is not selected. This is due to charge trappings in insulating layers, inducing Vt shifts in NMOS transistors. If we stop the X-rays irradiation between 520 seconds and 880 seconds, the programed memory cells will remain in the erased state during the next writing operation.

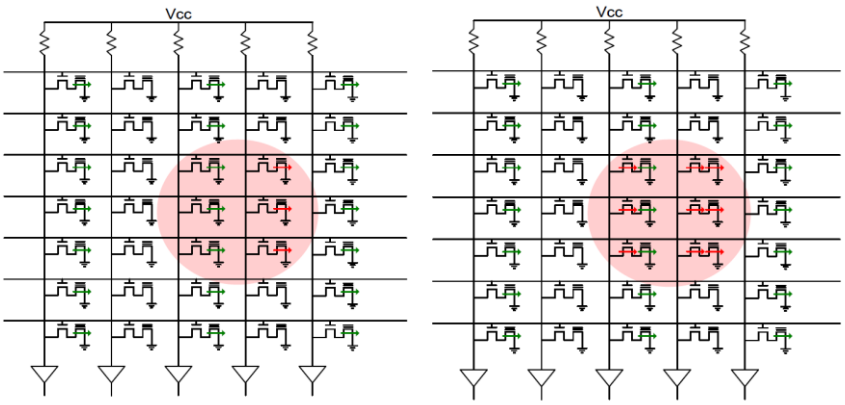

Fig. 8. The figure presents the logical representation of part of the flash memory block in the X-rays exposed area (red circle). The logical functionality of part of the flash block memory cells is visible during the X-rays irradiation. The two parts of the attack process are clearly visible: on the left picture, the floating gates of the memory cells are in an erased state and on the right picture, the NMOS access transistors are conductive. The state of the fault floating gate transistors and the fault NMOS access transistor is conductive; the red arrows represent each fault memory cell and each fault transistor.

The flash block memory cells are programed with alternating 1s and 0s for each memory cell side by side we have programmed the flash memory block with 5555 logic values. It is clearly possible to stop the experiment after the first part of the faulted results (i.e. before 880s) in order to keep only the erased memory cell faults and performed an exploitable security attack. **Fig. 9** presents longitudinal and transverse cross sections allowing to measure the size of the block cell which is approximately (1.3 µm × 3.5 µm). **Fig. 9** also presents a schematic of the memory cell blocks indicating that sixteen floating gate transistors could be irradiated in the 10 µm diameter hole. Only half of the sixteen floating gates are full of electrons and thus will be faulted, which means eight floating gate transistors. During the experiment, seven floating gate transistors were faulted (see **Fig. 6**). This difference may be due to the fact that the tungsten hole might be slightly smaller or not exactly in the position shown in **Fig. 9**.

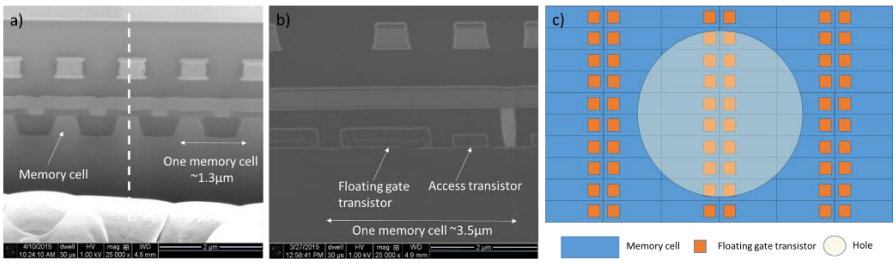

Fig. 9. (a) Frontside perpendicular FIB cross section and SEM pictures of the flash block memory cells of the ATMEGA128P device. (b) Transverse cross section (dashed white line of (a)). (c) Schematic of the memory cell blocks with the W hole.

4 Towards simple single bit attacks with laboratory X-rays source

The principle of using W mask to perform X-rays attack on backside integrated circuits has been clearly validated in the previous section. We therefore tried to simplify the sample preparation and explored the availability of performing frontside attack. Knowing the flash zone position, a lead film (10 mm height × 20 mm width × 50 µm thickness) was glued on the frontside of the component to protect the surrounding electronic components. We choose to start with a lead film, easier to manipulate and cut than W plate and to limit the FIB use to the drilling of holes. Different square holes with edge length ranging from 5 µm to 10 µm were drilled directly in the Pb film with the FIB with a 65 nA current during 3 hours. The main advantage of this procedure is that we avoid several tricky steps of the sample preparation procedure presented in the previous section: there is no need to return the metal legs connecting the component to the board-connection as necessary in backside attack, to use ASAP machining neither to align Pb film with W deposit and hole as explained earlier. Furthermore, we also simplified the X-rays attack: in this case, we do not use a Mo target, which is not a classical target, but a W target that is available in common X-rays sources. The X-rays attack conditions were similar: 40 kV, 1.9 W with large spot size of around 2 µm focalization. **Fig. 10 (a)** presents the sample with the Pb lead directly glued on the front side with carbon tape. **Fig. 10 (b, c)** presents FIB images of the holes performed in the flash and a X transmission image of the device mounted in the X-rays source, showing holes in white.

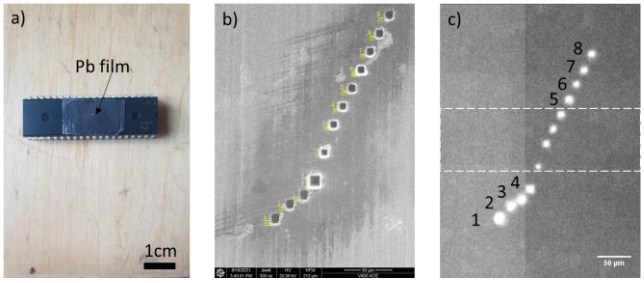

Fig. 10. : (a) Frontside component with Pb film of 50 µm thickness protecting the circuit in the middle. (b) FIB images of the series of hole made in the Pb film. (c) X-rays transmission image of the component showing holes.

Fig. 11 presents the images of the faulted bits with various X-rays exposure durations. The first fault appears in less than one hour (at 2960 s) and it is a single bit fault (see red arrows on **Fig. 11**). Other faults appear with time in the different holes. It is interesting to note that in each hole we start by a single bit fault as indicated by red arrows. The second bit fault in each hole is generally coming after 60 s to 120 s after the first fault. This could let time to switch off the X-rays in order to perform only single bit attack, keeping only the single erased memory cell fault and perform an exploitable attack. However, it would be better to reduce the size of the holes and thus only attack one transistor. It can be seen from the last image of **Fig. 11** that some holes are not

presenting faults when compared to **Fig. 10** : only eight holes present faults. This is due to the 5555 programming of the flash where 128 columns are set to 1 and 128 columns are set to 0 alternatively. Only columns set to 1 can be changed to 0 and produce a fault. This explains why four holes in between the white dashed lines of **Fig. 10** are not producing faults.

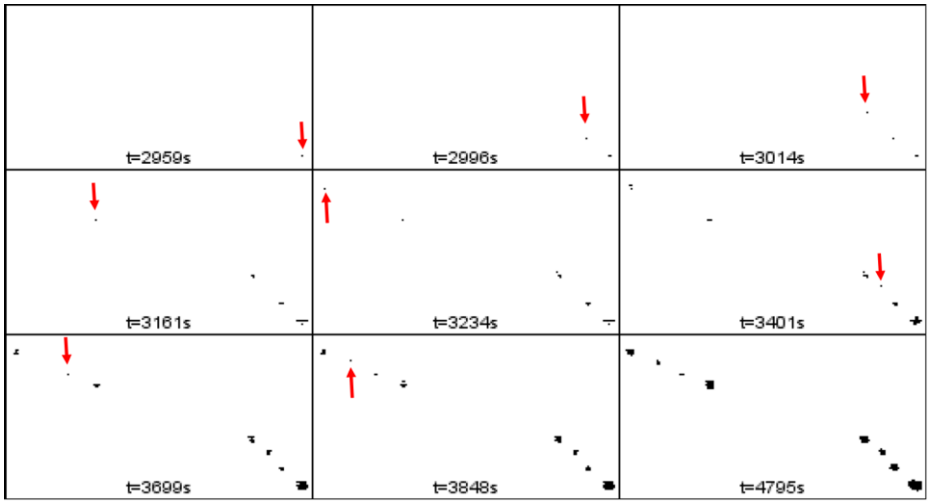

Fig. 11. Images of the faulted bits with time during front side X-rays attacks of Atmega: red arrow indicates the single bit fault.

5 Conclusion

It is possible to attack only several flash memory block cells and NMOS access transistors with a simple X-rays laboratory source. The seven erased cells may allow a program change stored in the memory block or to deactivate a countermeasure when this one needs a flash memory cell reading. This work is the continuation of what has been done in Grenoble ESRF with a 50 nm focalized synchrotron source [1]. The fact that we do not need a synchrotron and that a conventional W target X-rays source can be used for managing such an attack is a very interesting feature. Furthermore, we show that it is possible to perform frontside attacks with a quite simple sample preparation to protect the circuit. We show that single-bit attacks can be done but we need to reduce the size of the holes in order not to fault other transistors around. It is interesting to note that the Pb film with hole down to µm size can be prepared with FIB and then put in front of the components (not glued on it) to perform random single-bit attacks in the flash memory. This limits drastically the use of the FIB to perform attacks: indeed, this removable protective film can be reused to attack other components with different technology node. The 350 nm technology of the Atmega128 is a proof of concept and the aim is to perform such attacks on more advanced technology nodes.

References

1. Anceau S. , Bleuet P., Clédière J., Maingault M., Rainard J.L., Tucoulou R., Nanofocused X-ray Beam To Reprogram Secure Circuits, CHES 2017, Taiwan.,1 : CEA-Leti, 2 : European Synchrotron Research Facility (ESRF)
2. Skorobogatov S.P., Anderson R. J.: Optical Fault Induction Attacks. In Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, CHES, 2002.
3. Habing D.H.: The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits. IEEE Transactions on Nuclear Science, vol. 12, pp. 91-100, 1965.
4. Henley F.J.: Logic failure analysis of CMOS VLSI using a laser probe. In Reliability Physics Symposium, 22nd Annual, pp. 69-75, 1984. -75, 1984.
5. Burns D., Pronobis M., Eldering C., Hillman R.: Reliability/design assessment by internal-node timing-margin analysis using laser photocurrent injection. In 22nd Annual Proceedings on Reliability Physics 1984, pp. 76-82, IEEE, 1984.
6. Hériveaux L., Clédière J., Anceau S.: Electrical Modeling of the Effect of Photoelectric Laser Fault Injection on Bulk CMOS Design. ISTFA, 39th International Symposium for Testing and Failure Analysis, 2013.
7. Micheloni R., Crippa L., Marelli A.: Inside NAND Flash Memories. Springer, pp. 537-571, 2010.
8. Oldham T.R., McLean F.B.: Total Ionizing Dose Effects in MOS Oxides and Devices. IEEE Transactions on Nuclear Science, vol. 50, pp. 483-499, June 2003.
9. Oldham T.R.: Ionizing Radiation Effect in MOS Oxides. Advances in Solid State Electronics and Technology (ASSET) Series, 1999.
10. Soucarros M., Clediere J., Dumas C., Elbaz-Vincent P.: Fault Analysis and Evaluation of a True Random Number Generator Embedded in a Processor. Journal of Electronic Testing, 2013.
11. Ma T.P., Dressendorfer P.V.: Ionizing radiation effects in MOS devices and circuits. Wiley, New York, 1989.
12. Shaneyfelt M.R., Schwank J.R., Fleetwood D.M., Winokur P.S., Hughes K.L., Sexton F.W.: Field dependence of interface trap buildup in polysilicon and metal gate MOS devices. IEEE Transactions on Nuclear Science, vol.37, no.6, p.1632, 1990.
13. Caywood J., Prickett B.: Radiation-induced soft errors and oating gate memories. In Proceedings of 21st Annual Reliability Physics Symposium, pp. 167-172, 1983.
14. Snyder E., McWhorter P., Dellin T., Sweetman J.: Radiation response of floating gate EEPROM memory cells. IEEE Transactions on Nuclear Science, vol. 36, pp. 2131-2139, Dec. 1989.
15. McNulty P., Yow S., Scheick L., Abdel-Kader W.: Charge removal from FGMOS floating gates. IEEE Transactions on Nuclear Science, vol. 49, pp. 3016-3021, Dec. 2002.
16. Cellere G., Paccagnella A., Visconti A., Bonanomi M.: Ionizing radiation effects on oating gates. Applied Physics Letters, vol. 85, pp. 485-487, July 2004.
17. Cellere G., Paccagnella A., Visconti A., Bonanomi M., Caprara P., Lora S.: A model for TID effects on oating gate memory cells. IEEE Transactions on Nuclear Science, vol. 51, pp. 3753-3758, Dec. 2004.
18. Cellere G., Paccagnella A., Lora S., Pozza A., Tao G., Scarpa A.: Charge loss after 60Co irradiation of ash arrays. IEEE Transactions on Nuclear Science, vol. 51, pp. 2912-2916, Oct. 2004.
19. Wang J., Samiee S., Chen H-S., Huang C.-K., Cheung M., Borillo J., Sun S-N.,

Cronquist B., McCollum J.: Total ionizing dose effects on flash-based field programmable gate array. IEEE Transactions on Nuclear Science, vol. 51, pp. 3759-3766, Dec. 2004.
20. Wang J., Kuganesan G., Charest N., Cronquist B.: Biased-irradiation characteristics of the floating gate switch in FPGA. In Proc. IEEE Radiation Effects Data Workshop, pp. 101-104, Jul. 2006.
21. Cellere G., Paccagnella A., Visconti A., Bonanomi M., Beltrami S., Schwank J., Shaneyfelt M., Paillet P.Total ionizing dose effects in NOR and NAND ash memories. IEEE Transactions on Nuclear Science, vol. 54, pp. 1066-1070, Aug. 2007.
22. Nguyen D.N., Lee C.I., Johnston A.H.: Total ionizing dose effects on flash memories. IEEE Radiation Effect Data Workshop, p.100, 1998.
23. Gerardin S., Bagatin M., Paccagnella A., Grurmann K., Gliem F., Oldham T.R., Irom F., Nguyen D. N.: Radiation Effects in Flash Memories. IEEE Transactions on Nuclear Science, vol. 60, no. 3, pp. 1953-1969, June 2013.
24. Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C.: The Sorcerer's Apprentice Guide to Fault Attacks. IACR Cryptology ePrint Archive, 2004.