Nanofocused X-Ray Beam To Reprogram Secure Circuits

Stéphanie Anceau[1,2], Pierre Bleuet[1,2], Jessy Clédière[1,2], Laurent Maingault[1,2], Jean-luc Rainard[1,2], and Rémi Tucoulou[3]

[1] Univ. Grenoble Alpes, 38000 Grenoble, France
[2] CEA, LETI, MINATEC Campus, 38054 Grenoble, France
{stephanie.anceau, pierre.bleuet, jessy.clediere, laurent.maingault, jean-luc.rainard}@cea.fr
[3] ESRF, The European Synchrotron, 71 Avenue des Martyrs, 38043 Grenoble, France
tucoulou@esrf.fr

Abstract. Synchrotron-based X-ray nanobeams are investigated as a tool to perturb microcontroller circuits. An intense hard X-ray focused beam of a few tens of nanometers is used to target the flash, EEPROM and RAM memory of a circuit. The obtained results show that it is possible to corrupt a single transistor in a semi-permanent state. A simple heat treatment can remove the induced effect, thus making the corruption reversible. An attack on a code stored in flash demonstrates unambiguously that this new technique can be a threat to the security of integrated circuits.

Keywords: X-ray, flash, EEPROM, RAM, ATmega, circuit edit, MOS Stuck-At

1 Introduction

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. The possibility of using visible and IR light was revealed by Skorobogatov and Anderson [1]. The physical phenomena have been studied and explained by the failure-analysis community [2–5]. Laser light can be synchronized and focused in order to induce transient faults. In the security-evaluation practice, these faults may give powerful results. Electromagnetic radiation perturbation allows a new breach that corrupts circuits [6–8]. Access to the circuit is less restrictive since depackaging is not necessarily required.

In order to further investigate the wavelength spectrum of perturbations, it is proposed here to study the effects of ionizing radiation like X-rays. For one thing, hard X-rays offer the great advantage of deeply penetrating through materials. Every embedded component within the chip can be reached compared to only the silicon substrate and doped regions with visible or IR light. X-ray interaction with electronic circuits has been analyzed [9–12], but its use for security evaluation has been mainly restricted to die and package imaging, and an occasional

mention as a perturbation means without practical or successful results [13, 14]. Focusing exclusively on a selected area of the device under test may be seen as the ultimate goal of a perturbation technique and the lack of practical tests in the literature may be due to the difficulty to focus these high energy photons down to the nanoscale. The recent advent of third-generation synchrotron nano-probe beamlines makes possible to focus hard X-ray beams down to a few tens of nanometers. This paves the way to single transistor corruption during operando experiments. It must be mentioned that the work detailed hereafter is unprecedented, mostly because such beamlines have existed for only a few years; before that, only micro-focusing was possible, i.e. single-transistor irradiation was simply impossible.

The experimental setup, the physics of the X-ray interaction with MOS transistors and the possibility of using fluorescence techniques are detailed in section 2. Experimental results are given on an ATmega1284P circuit in section 3 for RAM, flash and EEPROM memory blocks. A real attack on this circuit for flash is reported in section 4, demonstrating the possibility of permanently modifying the code of an application. The conclusion outlines all the potential of using X-ray in the security-testing domain.

2 Nanofocused X-ray beam

2.1 Experiment setup

A very intense multi-keV X-ray nanobeam is required to perform single-transistor X-ray corruption, to profit from high penetration depth and locally create a sufficient number of photo-electrons to induce faults. Unfortunately, hard X-ray beams featuring decananometer resolution are unachievable today using laboratory systems. Moreover, the extreme brilliance of new third-generation synchrotron long beamlines, combined with high-efficiency X-ray focusing optics, offers completely new possibilities in terms of X-ray characterization and X-ray-based attacks. The work detailed in this paper is based entirely on the use of the ID16B beamline at the European Synchrotron Radiation Facility (ESRF) fully described by Martinez-Criado et al [15]. For readers' convenience, the general principle of the X-ray microscope and essential numbers follow: the low-divergence X-ray source located in the main storage ring of the ESRF (844 m circumference) is demagnified using Kirkpatrick-Baez optics located 165 m from the source. This optical scheme produces a beam of $60 \times 60\,\mathrm{nm}^2$ (full width at half minimum [FWHM]) in the case of the results detailed in this paper, with a high monochromaticity (18 keV, $\Delta E/E \approx 10^{-4}$) and a photon flux of 2×10^9 ph/s. The brilliance is high enough to generate very locally a significant number of electrons (called X-ray beam induced current or XBIC) able to induce faults, and the probe is sufficiently local even for the latest nanoelectronic nodes. On top of that, a comfortable working space around the sample enables performing operando experiments and accommodating X-ray detectors. It operates in ambient air, i.e. with no vacuum constraint. It is therefore well suited for the experiment described here. A rough overview of the optical scheme is shown in

Fig. 1, with horizontal and vertical planes of the beam, the characteristic distances in meters, and a picture of the space between the optics and the sample.

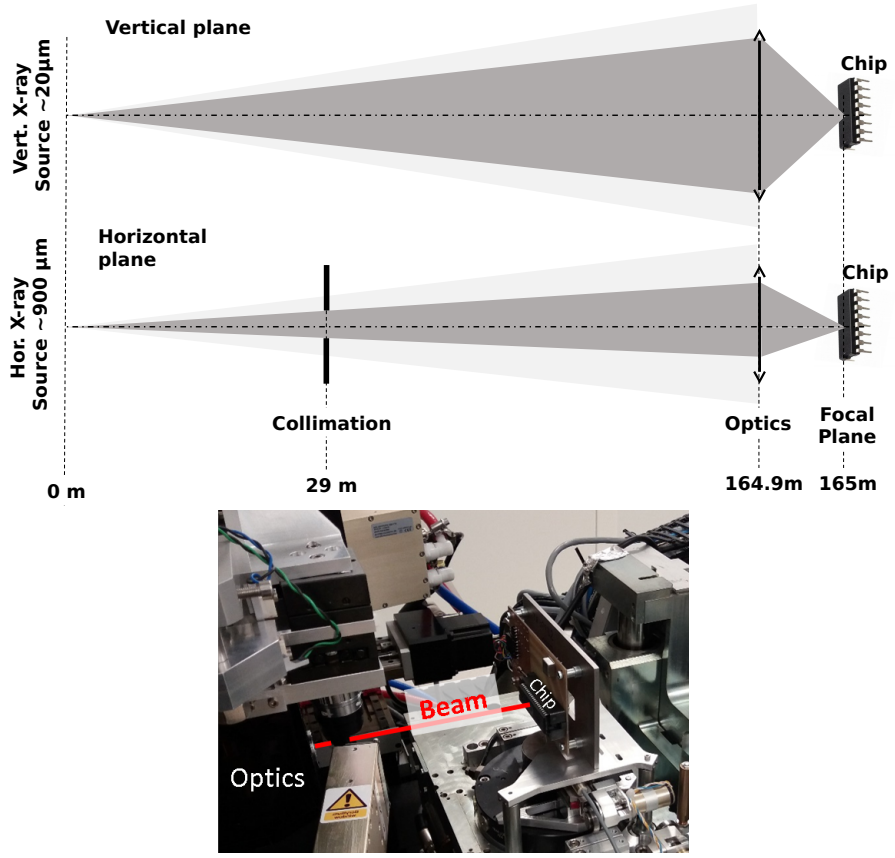

Fig. 1. ID16B setup. Schematic of the line with the X-ray source (sizes are given FWHM), optics (Kirkpatrick-Baez) and device under test (chip) in the focal plane. Space between optics and the chip.

There are nearly 50 synchrotrons worlwide, including three very large facilities (ESRF in Europe, APS in USA and Spring-8 in Japan) operating multi-GeV storage rings; very few beamlines in the world can operate sub-100 nm beams with hard X-rays.

2.2 Local positioning on the device under test by X-ray fluorescence

The ID16B test-bench is equipped with a long working distance optical microscope aligned with the X-ray beam and having its focal plane coplanar with the

one from the X-ray microscope, allowing a pre-positioning on the sample surface (10× magnification, field of view of 1×1 mm^2). Obviously, this visible-light microscope can be used only if the circuit packaging has been removed.

Although the visible-light microscope is ideal for pre-localization, its resolution is not high enough to precisely locate the transistors and therefore to place the one to be irradiated exactly in the focused X-ray beam. Fine-tuning is required using another asset of the ID16B beamline, which is scanning X-ray fluorescence (XRF). It is indeed possible to run a 2D scan of a region of interest (ROI) and, at every position, to record a local X-ray fluorescence spectrum using a multi-element energy-dispersive detector. A 2D map is obtained for each chemical element in the sample. These maps can be obtained either by selecting a peak in the spectra or, better, by fitting background and peaks using the PyMca software [16], as shown in Fig. 2. Since the sample is located in the common focal plane, it can be mapped precisely with a step size equal to the focused beam size.

XRF visualization mode can be particularly interesting when addressing an unknown circuit or when the attacker does not want to open the circuit's packaging. Results on ATmega1284P presented in this paper are obtained with a front-side opened circuit. However, it can also be performed without opening the package, as it was checked on a Thin Quad Flat Package (TQFP).

2.3 X-ray interaction

At 18 keV, the photoelectric effect is the main contributor driving the X-ray absorption in semiconductor materials. The absorption coefficient greatly varies with the atomic number (Z). A regular silicon chip is composed of very thin layers of possibly high-Z metals (W, Au) and thicker layers of small atomic number elements (Si, O, N), in which hard X-rays are weakly absorbed. They can therefore deeply penetrate into the device and reach logic gates with irradiation from the top surface or even through the package. After absorption, a high number of carriers are generated within the material. These localized carriers can deeply perturb an operating chip, especially when absorption occurs in the oxide layers. It should be noted that it is impossible to generate carriers in the oxide with an IR laser. Oxide band gaps are much larger than IR photon energy. Depending on the types of gates that are targeted, two effects are of interest with X-rays:

- charge trappings in insulating layers, inducing V_t shifts in MOS transistors
- photoemission of carriers stored in floating gates.

These effects have been extensively studied[9–12, 17–28], especially for aerospace applications, in which radiation naturally occurs and prevents chips from functioning properly. This paper gives a short summary of the most important effects, focusing on the application for circuit perturbations and the two types of memory in the experiment.

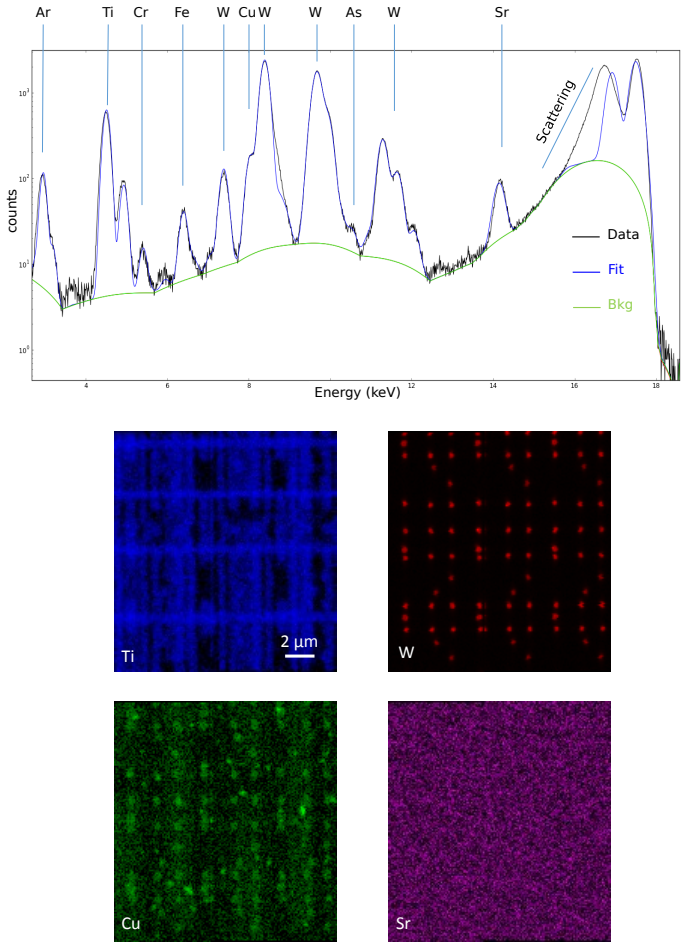

Fig. 2. Typical fluorescence spectrum (log scale) of the ATmega circuit (top). The energy unit is keV. It shows the sum of all measured spectra (black) and the corresponding fitted sum spectrum and background (blue and green, respectively). The scattering peak mismatch at 18 keV is due to multiple Compton scattering (only first-order Compton scattering is modeled). The Ar peak at low energy comes from the Ar naturally present in air. A selection of elemental 2D mappings for Ti, W, Cu and Sr is shown below.

Charge trapping Electron-hole pairs created by X-rays are separated by the electric field applied to the grid: electrons are drained away through the grid thanks to their higher mobility, while lower mobility holes move inside the oxide towards the transistor channel. Reaching the Si/SiO_2 interface, holes can be trapped into defect sites, which are numerous at this interface. This positive charge accumulated near the transistor channel results in a shift of $I_D(V_{GS})$ curves to lower gate voltages (Fig.3). From an electrical point of view:

- a NMOS transistor becomes more easily conducting, even permanently conducting
- a PMOS transistor becomes less easily conducting, even permanently blocking.

This is a total ionizing dose (TID) effect: the more the device is irradiated, the more holes are trapped and curves shifted (Fig.3). Also, trapped charges can escape when temperature is increased thanks to thermal excitation. Thermal annealing can restore normal behavior of irradiated devices. As a result, these faults can be viewed as "semi-permanent faults": "permanent" as its effect remains after irradiation has ceased, and "semi" because annealing can restore the chip to a normal-state.

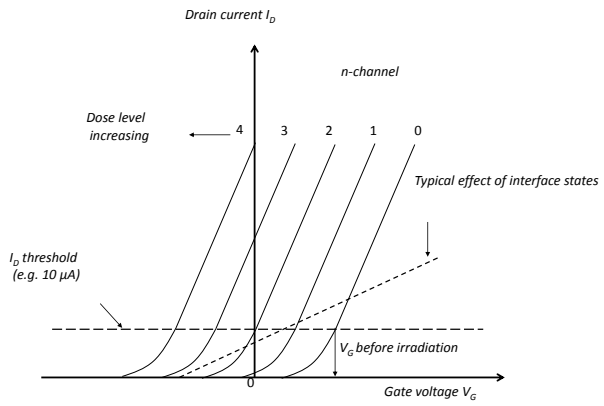

Fig. 3. Effect of dose level increasing (1 to 4, arbitrary unit) on $I_D(V_{GS})$ of a NMOS device (extracted from [29]). The more the dose is increased, the greater the shift of $I_D(V_{GS})$ curve toward lower gate voltages. The NMOS transistor becomes more easily conducting, even permanently-conducting.

Effects on floating gates floating gates are used in non-volatile memories, such as EEPROM and flash. A charge-storage element (floating gate) is placed between the silicon channel and the control gate (normal transistor gate). By

changing the amount of electrons and holes in the floating gate, the threshold voltage of the transistor can be altered. For ATmega1284P, the state with positive or no charge in the floating gate is the erased state, whereas negative charges present in the floating gate are the programmed state of the cell.

This is the interpretation detailed in reference [12]:

- a first effect is very similar to the one that affects classical MOS transistors, resulting in a semi-permanent shift of $I_D(V_{GS})$ curves: the cell is then semi-permanently stuck in the erased state, but
- additionally, it is likely that the photoemission of the carriers in the floating gate gets enough energy from the radiation to escape from this storage-element potential. It is also possible that the positive charges created in the surrounding oxides are injected into the floating gate. The injected holes recombine with the stored electrons. This results in a decrease of the number of electrons in the floating gate, which induces the memory cell erasure.

If the first effect dominates, stuck-at faults of the cell will be observed and the cell cannot be programmed any more. If the second effect dominates, the cell will not be semi-permanently faulted, and can be reprogrammed as a normally erased cell.

3 Experimental results

3.1 RAM

RAM in the ATmega128 uses a classic six-transistor cell, as shown in Fig. 4. It comprises two cross-coupled inverters (transistors NI1, PI1 and transistors NI2, PI2), and two access transistors (NA1, NA2) connecting inverters to the two-bit lines. Access-transistor grids are driven by the word line, allowing read-and-write operations. The inverters' PMOS (PI1, PI2) are weak transistors to facilitate writing operations.

The attack was directed at the ESRF bench targets' inverter's NMOS transistors. Accurate location of transistors to be targeted was obtained using fluorescence mapping, allowing localization of tungsten vias in the device. Superposition of fluorescence and SEM pictures (Fig. 5) show location of RAM transistors and allow precise focused irradiation of any individual transistors in a cell. If NMOS NI2 is irradiated, this becomes a conducting device, whatever the value applied to its grid. Inverter output is then stuck at logical value 0 and the cell value remains semi-permanently at 0. A heat annealing of 150 °C for one hour at ambient atmosphere restores normal behavior of NI2. Attacking NI1 transistor symmetrically causes the cell to become stuck at logical value 1. Experimental results are shown in Fig. 5. Several bit cells are targeted to semi-permanently have them stuck at logical value 0 or 1.

Every RAM cell of the circuit can be stuck at a desired value 0 or 1.

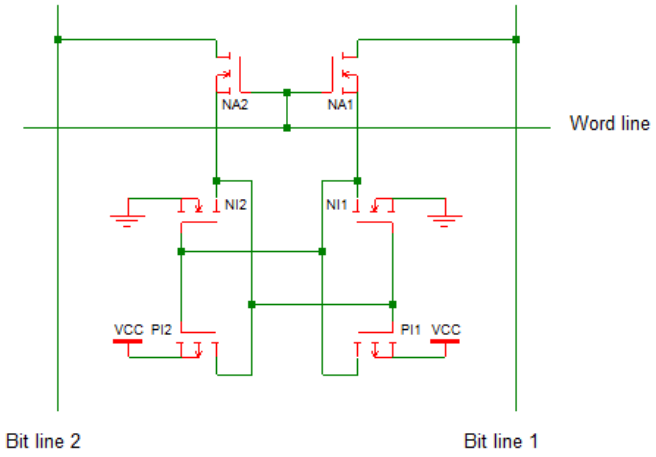

Fig. 4. Six-transistor RAM cell of the ATmega128.

3.2 Non volatile memories

The ATmega1284P device has 128 KB of flash and four kilobytes of EEPROM for non volatile memories (NVM). Both memories have the same cell structure: a floating gate transistor dedicated to store the carriers and a second MOS transistor to select the cell.

The two memory blocks are tested with the same protocol. The chip was first erased (all bytes set to 0xFF). With the help of a fluorescence image for localization inside the memory cell, the chip was irradiated by the nano beam for a few seconds. Reading the memory afterwards showed whether modification in the memory was successful or not.

Two types of memory modifications are observed:

- a whole column is reset
- a single bit is reset.

These two behaviors are explained by the physical effects described in Section 2.3. A whole column is reset if the beam affects the selection transistor of the cell. The NMOS transistor becomes conductive and the entire column is always read as logical value `0`. This fault was semi-permanent: a thermal annealing (150 °C for one hour at ambient atmosphere) removes holes from defect sites to restore the transistor to its normal behavior. A single bit was reset when the beam was focused on the floating gate transistor. In this case, electrons stored in the floating gate were removed either by recombining with holes created in the neighboring oxides or by direct photoemission. The cell was emptied and reset. The transistor kept its normal operating conditions: the cell could be erased/programmed again. The semi-permanent effect on the floating gate transistor was

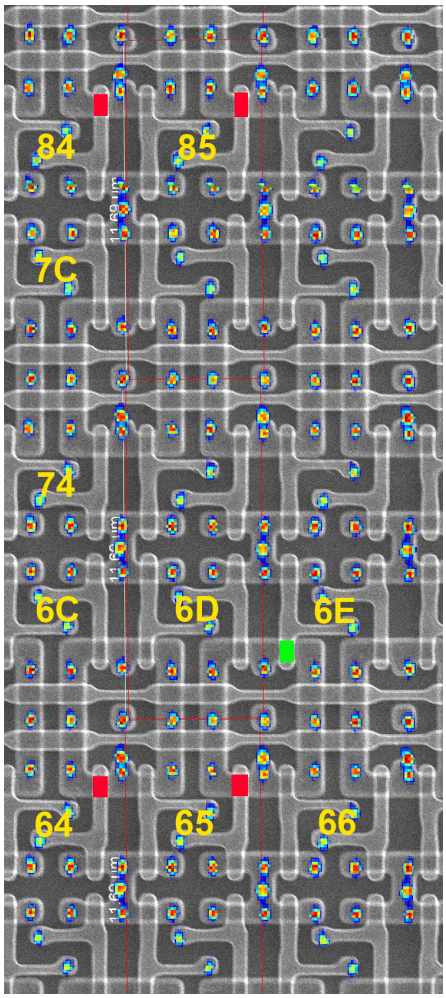

Fig. 5. RAM faults. Background: SEM picture of etched RAM, showing transistor grids (metals are removed); colored dots: superimposed result of fluorescence mapping; red and green rectangles: irradiated transistors, causing the cell to be faulted at logical value 1 (red) or 0 (green); in yellow: addresses of corresponding RAM cells.

not observed during this experiment. EEPROM and flash memory exhibited the same behavior.

This is an unprecedented demonstration of the ability to modify a single bit at any given address in an NVM memory. Targeting a specific address is possible with reverse-engineering of the memory mapping. Memory mapping (the relation between physical position and logical address) was retrieved after several irradiations over the memory surface. This mapping is presented in Fig. 6. It is possible to individually modify any data or program stored in the NVM from an attacker's point of view. An attack example using this feature is presented in Section 4.

3.3 Comparison with laser attacks

Compared to laser-induced faults, classically used in secured smart-card attacks, focused X-ray results in different kinds of faults:

- X-ray faults are semi-permanent: fault effect remains after irradiation has ceased. Normal operation can be restored with a thermal annealing or erasing NVM memory. Laser faults are fugitive, i.e. they are present only during laser irradiation.
- X-ray attacks can be used for "circuit editing": by individual irradiation, NMOS can be made always conductive, while PMOS can be blocked. Functions or parts of a device can be modified; for example, to deactivate security countermeasures or detectors. Moreover, X-rays penetrate regular protective shields that prevent focused ion beam (FIB) attacks.
- X-ray attacks can be used to directly modify non-volatile memories programming, while laser attacks can corrupt only NVM reading or writing.
- X-ray can be focused down to nanometric size, to target a single transistor, while laser is limited to micrometric scale (Rayleigh criterion).

4 Real attack on flash program

In this investigation, a full attack path was performed to illustrate the feasibility of circuit reprogramming. An authentication program was stored in the flash boot sector in one ATmega1284P circuit. After start-up of the circuit, this program waited for a four-digit PIN sequence to be sent on UART0. Code analysis of the dumped assembly code [30] pointed out that the authentication relies on a single statement at flash address 0x0000015c:

```
0000015c:        b1 f6    BRNE.-84   ;0x10a <main+0x2e>
```

The branch if not equal (BRNE) statement catches the 9999 erroneous, presented PIN. Modifying the BRNE op-code to a branch if equal (BREQ) op-code would allow reversing the situation and accepting the 9999 erroneous PIN and rejecting the genuine PIN. Thus, without the correct PIN, an assailant would have a probability of 9999 of 10 000 to pass the authentication (instead of one of 10 000 previously).

Comparing the BRNE and BREQ op-codes (1) shows that a single-bit reset is needed in flash memory to modify the assembly. This bit reset can be performed by X-ray lighting of the floating gate transistor storing the bit value.

Instruction	hexadecimal code	binary code
BRNE .-84	0xf6b1	1111011010110001
BREQ .-84	0xf2b1	1111001010110001

Table 1. Comparison of BRNE and BREQ op-code of ATmega circuit.

Without the correct PIN, it is impossible to use the circuit: a well-implemented PIN-try counter limits the exhaustive search to a single PIN trial. With the results obtained in 3.2, it is possible to transform the code stored in flash in order to change the BRNE to BREQ at address 0x0000015c. The CPU address 16 bits of flash (words). Address 0x0000015c corresponds to 0xae = $174 = 128+5\times8+6$. Thus, the targeted bit is stored on the second line, sixth strip and seventh column of the flash memory block. Fig. 6 presents the routing of ATmega's flash memory and the position of the floating gate transistor holding the stored value to attack.

The X-ray beam is focused once on the desired bit of the target circuit for 500 ms. The first attempt was successful. The circuit was then permanently reprogrammed, and PIN security bypassed by choosing any incorrect PIN among the 9999 possibilities.

In order to perform such an attack, the code analysis must take into account the error model. For a flash memory block, this error model is a permanent reset of chosen bit(s).

5 Conclusion

Nano-focused X-ray beams turned out to be an efficient means of corrupting the integrity of integrated circuits. It has been shown that targeting a single MOS transistor is possible. A RAM cell can be stuck at a logical value 0 or 1 semi-permanently, and a heat treatment can then remove the corruption. Discharging the floating gate can reset the flash and EEPROM cells. A real attack has been demonstrated on a flash cell to modify the secure start-up sequence of a programmed circuit. Fluorescence mapping at the nanoscale provided a very powerful opportunity to obtain a precise location in the layout of the circuit to successfully target the desired transistor.

The results presented in this paper were obtained on an ATmega circuit with an ancient technology (350 nm). Ongoing experiments are producing similar results with an up-to-date technology node: a microcontroller circuit in 45 nm has been tested. The size of the X-ray beam (60 nm) is not restrictive as soon

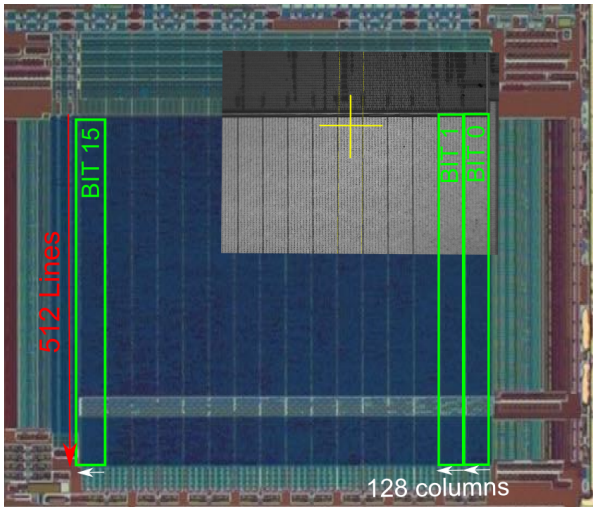

Fig. 6. Optical microscope images of the flash of an ATmega chip. The strip to attack should be chosen in one of the green rectangles. Then the nine most significant bits of the address correspond to the lines, whereas the seven least significant bits represent the column inside the green box. The position of the actual attack is shown by the yellow cross. The superimposed image corresponds to the ID16B's optical microscope view.

as the distance between two transistors is increased. A single transistor will still be targeted in future technology nodes.

Results are presented for RAM, flash and EEPROM memory block. However, transistors in the logic part of a circuit can also be targeted. NMOS transistors can be made conductive and PMOS transistors blocked. The corresponding CMOS cell can be stuck at logical value `0` or `1` depending on the implemented functionality. For a complex cell, the Karnaugh map could be modified to a selected state. Although not tackled in this paper, this feature provides a new way to approach the circuit-editing technique and an alternative to the FIB system. Considering the fact that it is not necessary to open the package of the circuit and that the size of the technology node is not a constraint, X-ray circuit edit could play an important role.

In the context of security application, X-ray nanofocusing provides many opportunities for attacking electronic circuits. Among them, let's note the possibility to cause permanent faults in cryptographic algorithms, deactivation of counter measures, reprogramming of memories, etc. Nanofocused X-ray are a serious threat to circuit security. At present, access to third-generation synchrotron sources equipped with a nanofocus beamline is, obviously, a major concern. The work discussed here is completely exploratory and was performed through the so-called academic beamtime regulated by scientific committees, with time constraints incompatible with routine analyses. However, access to

beamtime through the industrial channel is much easier and faster, making X-ray nanoprobe a new tool to corrupt circuits at the single transistor level.

6 Acknowledgements

The experiments were performed on beamline ID16B at the European Synchrotron Radiation Facility (ESRF), Grenoble, France.

Thanks to Olivier Hériveaux and Olivier Meynard for their pertinent contributions during days and nights at ID16B in May 2016.

References

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Quisquatter J-J., Samyde D.: Eddy current for magnetic analysis with active sensor. In proceedings of Esmart, 2002.
7. Schmidt J-M., Hutter M.: Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results. In 15th Austrian Workshop on Microelectronics, Austrochip 2007.
8. Poucheret F., Tobich K., Lisart M., Chusseau L., Robisson B., Maurine P.: Local and Direct EM Injection of Power Into CMOS Integrated Circuits. Fault Diagnosis and Tolerance in Cryptography, FDTC 2011.
9. Micheloni R., Crippa L., Marelli A.: Inside NAND Flash Memories. Springer, pp. 537-571, 2010.
10. 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.
11. Oldham T.R.: Ionizing Radiation Effect in MOS Oxides. Advances in Solid State Electronics and Technology (ASSET) Series, 1999.
12. Gerardin S., Bagatin M., Paccagnella A., Grürmann 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.
13. Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C.: The Sorcerer's Apprentice Guide to Fault Attacks. IACR Cryptology ePrint Archive, 2004.
14. Soucarros M., Clédière 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.

15. Martinez-Criado G., Villanova J., Tucoulou R., Salomon D., Suuronen J.-P., Labouré S., Guilloud C., Valls V., Barrett R., Gagliardini E., Dabin Y., Baker R., Bohic S., Cohen C., Morse J.: ID16B: a hard X-ray nanoprobe beamline at the ESRF for nano-analysis. Journal of Synchrotron Radiation, 2016.
16. http://pymca.sourceforge.net/, ESRF.
17. Ma T.P., Dressendorfer P.V.: Ionizing radiation effects in MOS devices and circuits. Wiley, New York, 1989.
18. 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.
19. Caywood J., Prickett B.: Radiation-induced soft errors and floating gate memories. In Proceedings of 21st Annual Reliability Physics Symposium, pp. 167–172, 1983.
20. 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.
21. 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.
22. Cellere G., Paccagnella A., Visconti A., Bonanomi M.: Ionizing radiation effects on floating gates. Applied Physics Letters, vol. 85, pp. 485–487, July 2004.
23. Cellere G., Paccagnella A., Visconti A., Bonanomi M., Caprara P., Lora S.: A model for TID effects on floating gate memory cells. IEEE Transactions on Nuclear Science, vol. 51, pp. 3753–3758, Dec. 2004.
24. Cellere G., Paccagnella A., Lora S., Pozza A., Tao G., Scarpa A.:Charge loss after 60Co irradiation of flash arrays. IEEE Transactions on Nuclear Science, vol. 51, pp. 2912-2916, Oct. 2004.
25. 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.
26. 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.
27. Cellere G., Paccagnella A., Visconti A., Bonanomi M., Beltrami S., Schwank J., Shaneyfelt M., Paillet P.:Total ionizing dose effects in NOR and NAND flash memories. IEEE Transactions on Nuclear Science, vol. 54, pp. 1066–1070, Aug. 2007.
28. Nguyen D.N., Lee C.I., Johnston A.H.: Total ionizing dose effects on flash memories. IEEE Radiation Effect Data Workshop, p.100, 1998.
29. Sharma A.K.: Semiconductor Memories, Technology, Testing and Reliability. Chapter 7: Semiconductor Memory Radiation Effects, p. 328, IEEE, 1997.
30. ATMEL AVR Assembler
http://www.atmel.com/webdoc/avrassembler/