Nanofocused X-ray beam to reprogram secure circuits

Stephanie Anceau, Pierre Bleuet, Jessy Clediere, Laurent Maingault, Jean Luc Rainard, Remi Tucoulou

Nanofocalized 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, F-38000 Grenoble France,
[2] CEA, LETI, MINATEC Campus, F-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, 38000 Grenoble, France
remi.tucoulou@esrf.fr

Abstract. Synchrotron X-ray nano-beamlines is investigated as a tool to perturb microcontroller circuits. This technique is used to target the Flash, EEPROM and RAM memory of a circuit. The obtained results are very promising and show that it is possible to corrupt a single transistor in a semi-permanent state. A simple heat treatment can remove the induce effect, thus making the corruption reversible. A concrete attack on a code stored in Flash is demonstrated.

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

1 Introduction

Hardware security labs and the need to corrupt the processing of recent circuits lead to a constant research of new perturbations means. The possibility to use visible and IR light was revealed by Skorobogatov and Anderson [1]. The physical phenomenon have been studied and explained in the failure analysis community [2–5]. Laser light can be synchronized and focalized in order to induce transient faults. In the security evaluation practice, these faults may give powerful results. Electromagnetic radiation perturbation give a new breach for circuit corruption [8, 6, 7]. This mean may not be as versatile as light but can give also very interesting results. The access to the circuit is less restrictive, a depackaging is not necessarily required.

In order to continue to investigate the wavelength spectrum of perturbation, it is propose here to give a glance to X-ray possibilities. X-ray interaction with electronic circuits have been analyzed in the past [9–12], but the usage for security evaluation has been mainly restricted to die and package imaging, and mentionned as a perturbation mean but without practical results.

Focalization on a specific area of the device under test may be seen as the key point of a perturbation technique. The ultimate challenge may be the focalization down to a single transistor on an aggressive technology node. Synchrotron equipment enable to achieve this goal with X-ray radiation.

The setup of the equipment, the physics of the X-ray interaction with MOS transistors, the possibility to use fluorescence techniques is detailed in the next section 2. Experimental results are given on an ATMEGA1284P circuit in section 3 for RAM, Flash and EEPROM memory block. A concrete attack on this circuit is given in section 4 for Flash, thus demonstrating the possibility to permanently modify an application code. The conclusion section will outline all the potential to use X-ray in the security testing domain.

2 Synchrotron X-ray radiation

2.1 Experimental setup

détailler le setup et la focalisation, photo de la manip, du synchrotron?
donnez le nombre de synchrotrons dans le monde

Fig. 1. The European Synchrotron (ESRF Grenoble).

2.2 X-ray interaction

Two kinds of X-Ray interaction mechanisms in CMOS circuitry are of interest in our experiments:

- charge trappings in insulating layers, inducing V_t shifts in MOS transistors, which will be used later in this paper for RAM attacks,
- effects on electron storage in floating gates, which will be used for EEPROM and Flash attacks.

These effects have been extensively studied, especially for aerospace applications [9–24]. So in this paper we will just give a short summary of the most important results.

Charge trapping Due to the high energy of X-rays, ionization induces electron-hole pairs creation in the oxide layer [4]. These electron-hole pairs are separated by the electric field applied to the grid: high mobility electrons are eliminated through the grid, while lower mobility holes move inside the oxide towards the transistor channel. Arriving at the Si/SiO2 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 (see Fig.2). From an electrical point of view :

- NMOS will become more easily conductive, even permanently conductive,
- PMOS will become less easily conductive, even permanently blocked.

This is a TID (Total Ionizing dose) effect : the more the device is irradiated, the more holes are trapped and curves shifted (Fig.2). Notice also that trapped charges can be eliminated by heat annealing : heating treatment can restore normal behaviour of irradiated devices. So these faults can be viewed as "semi-permanent faults" : "permanent" as its effect remains after irradiation have ceased, and "semi" because annealing can restore a normal behaviour.

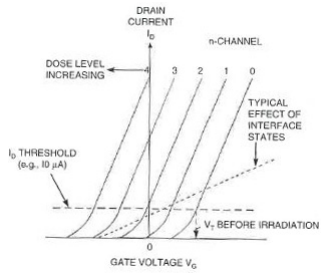

Fig. 2. Effect of dose level increasing (1 to 4) on NMOS device (extracted from [25]).

Effects on floating gates Floating gates are used in non volatile memories, such as EEPROM and Flash memories. A charge storage element (floating gate) is placed between the silicon bulk 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. The state with positive or no charges in the floating gate is the erased state whereas a negative charges present in the floating gate is the programmed state of the cell.

It seems from [12] that two different effects could occur :

- a first effect very similar to the one which 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,

[4] Let's note that low energy Infra-Red laser beam is unable to ionize oxide.

– but, additionally, it is likely that the photoemission of the carries in the floating gate get enough energy from the radiation to escape from this storage element potential. It is also possible that the positives charges created in the surrounding oxides are injected into the floating gate. The injected holes recombine with the stored electrons. The result is a decrease of the amount of electrons in the floating gate which induce the erasing of the memory cell.

If the first effect dominates, we will observe "stuck-at" faults of the cell, which cannot be programmed any more. But if the second effect dominates, the cell is not semi-permanently faulted, and can be reprogrammed as a normally erased cell.

We observed these two behaviors with different kinds of non volatile memories tested during our experiments.

2.3 Fluorescence for localization

expliquer la fluorescence

It is not always possible to have GDS2 files in order to have an accurate localization of the perturbation to perform on a given circuit. Local reverse engeenering and the use of fluorescence technique on some materials give a good opportunity to get a perfect localization.

3 Experimental results

3.1 RAM

RAM of the ATMega128 uses a classical 6 transistors cell, as shown in Fig. 3. It comprises two cross coupled inverters (inverters *NI2*, *PI2* and *NI1*, *PI1*), and of two access transistors (*NA2*, *NA1*) connecting inverters to the two bit lines. Access transistors grids are driven by the word line, allowing read and write operations.

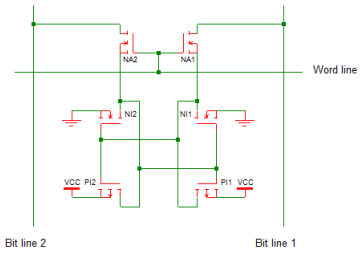

Fig. 3. 6 transistors RAM cell.

Notice that inverter's PMOS (*PI1*, *PI2*) are "weak" transistors, in order to facilitate writing operations. The attack performed on the ESRF bench targets

inverter's NMOS : for example, if NMOS *NI2* is irradiated, this device will become conducting whatever the value applied to its grid. So inverter's output will be stuck at logical value 0, then cell value will always remain at 0, until a heat annealing restores normal behaviour of *NI2*. Notice that attacking *NI1* transistor will symmetrically cause a stuck at logical value 1 fault of the cell.

Accurate location of transistors to be targeted was obtained using fluorescence cartography, allowing accurate localization of tungsten vias in the device. Superposition of fluorescence and SEM pictures (as in Fig. 4) shows location of RAM transistors and allows accurate focused irradiation of any individual transistors in a cell.

Experimental results are shown in Fig. 4:

- background : SEM picture of etched RAM, showing transistors grids (metals are removed),
- coloured dots : superimposed result of fluorescence scanning,
- red and green rectangles : irradiated transistors, causing stuck at "1" (red) or stuck at "0" (green) faults,
- in yellow, addresses of corresponding RAM cells.

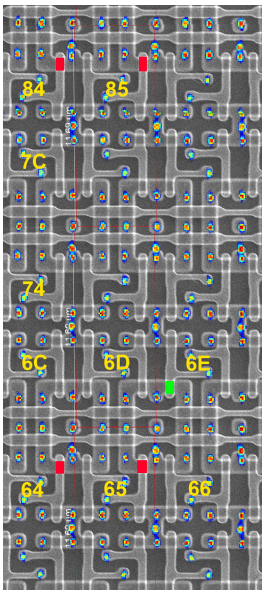

Fig. 4. RAM faults.

3.2 Flash

expliquer succintement le mapping mémoire de l'ATMEGA

3.3 EEPROM

résultats sur l'EEPROM

3.4 Comparison with laser attacks

Compared to laser induced faults, classically used in secured smart cards attacks, we have to notice that focused X-Ray gives totally different kinds of faults:

- X-ray faults are semi-permanent: fault effect remains after irradiation have ceased. Normal function can be restored by mean of heat annealing.
- Laser faults are fugitive, present only during laser illumination.
- X-ray attacks can be used for "circuit editing" : by individual irradiation, NMOS can be made always conductive, whilst PMOS can be blocked. Functions or parts of a device can be modified, for example to deactivate security countermeasure or detectors.
- X-ray attacks can also be used to modify non volatile memories programming, when laser attacks can only fault read or program operation results.

4 Concrete attack on Flash program

To illustrate the feasibility of circuit reprogramming, a full attack path is performed. In one ATMEGA1284P circuit, an authentification program is stored in Flash boot sector and wait, after start-up, for a four digits PIN sequence to be sent on UART0. Code analysis of the dumped assembly code [26] have shown that the authentification rely on a single statement at Flash address 0x0000015c:

```
15c:    b1 f6    brne.-84  ;0x10a <main+0x2e>
```

The Branch if Not Equal statement catch the 9999 erroneous presented PIN. Modifying the brne op-code with a Branch if Equal (breq) op-code would allow to reverse the situation and make accept 9999 presented PIN and reject the solo genuine PIN. Thus an assailant not knowing the correct PIN will have a much better probablility to pass the authentification (9999 on 10000 instead of 1 on 10000).

The comparison of brne and breq op-code (see table 1) show that to modify the assembly, a single bit reset is needed in Flash memory. 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.

Not knowing the correct PIN, it is not possible to use safely the circuit: a well implemented PIN try counter limit the exhaustive search to a single PIN trial. Using 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 adressing 16 bits Flash words, address `0x0000015c` correspond to `0xae` $= 174 = 128 + 5 \times 8 + 6$. Thus, the targeted bit is stored on the second line, sixth strip and seventh column of the Flash memory block.

The circuit to attack is put in the bench and the X-ray beam is focalized once on the desired bit for 500 ms. First attempt led to success. After all, the circuit is permanently reprogrammed, and the PIN security can be bypass by choosing any incorrect PIN among the 9999 possibilities.

In order to perform such attack, let's note that the code analysis must take into account the error model. For Flash memory block, this error model is reset of chosen bit(s).

5 Conclusion

Focalized X-ray radiation turn out to be an efficient mean to corrupt the integrity of integrated circuit. It is possible to target a single MOS transistor in a circuit. A RAM cell can be stuck to a logical value 0 or 1 semi-permanently, a heat treatment can then remove the corruption. Flash and EEPROM cells can be reset by discharging the floating double gate. A real attack have been demonstrated on a Flash cell to modify the secure start-up sequence of a programmed circuit. Fluorescence technique give a very powerful opportunity to have a precise localization in the layout of the circuit in order to successfully target the desired transistor.

The results of this paper are obtained on an ATMEGA circuit with an ancient technology (350 nm). Ongoing experiments are giving similar results with up to date technology node: a microcontroller circuit in 45 nm and a NOR Flash in 110 nm has been tested. The focalization of the X-ray beam (50 nm) is not a restrictive parameter if the distance between two transistors is considered. A single transistor will still be targeted on future aggressive technology node.

Results have been given for RAM, Flash and EEPROM memory block. However, transistors in the logical part of a circuit can also be targeted. NMOS transistors can be stuck at logical value 1 and PMOS transistors to logical value 0. Although not tackle in this paper, this property give a new way to approach circuit edit technique and an alternative to Focused Ion Beam 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 technique give a lot of opportunities for attacking electronic circuit. Among them, let's note the possibility to cause permanent faults in cryptographic algorithm, deactivation of countermeasure, reprogramming of memories ...

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, CHES2002.
2. Habing D. H.: The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits. IEEE Transactions on Nuclear Science, volume 12, pp. 91-100, 1965.
3. Henley F. J.:Logic failure analysis of CMOS VLSI using a laser probe. In Reliability Physics Symposium, 1984. 22nd Annual, pp. 69 –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 2013, 39th International Symposium for Testing and Failure Analysis.
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 Trans. Nucl. Sci., 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 Trans. Nucl. Sci., vol. 60, no. 3, pp. 1953–1969, June 2013.
13. Ma T.P., Dressendorfer P.V.: Ionizing radiation effects in MOS devices and circuits. Wiley, New York, 1989
14. 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
15. Caywood J., Prickett B.:Radiation-induced soft errors and floating gate memories. In Proc. 21st Annu. Reliab. Phys. Symp., Apr. 1983, pp. 167–172.
16. Snyder E., McWhorter P., Dellin T., Sweetman J.: Radiation response of floating gate EEPROM memory cells. IEEE Trans. Nucl. Sci., vol. 36, pp. 2131–2139, Dec. 1989.
17. McNulty P., Yow S., Scheick L., Abdel-Kader W. : Charge removal from FGMOS floating gates. IEEE Trans. Nucl. Sci., vol. 49, pp. 3016–3021, Dec. 2002.
18. Cellere G., Paccagnella A., Visconti A., Bonanomi M.: Ionizing radiation effects on floating gates. Appl. Phys. Lett., vol. 85, pp. 485–487, Jul. 2004.
19. Cellere G., Paccagnella A., Visconti A., Bonanomi M., Caprara P., Lora S.: A model for TID effects on floating gatememory cells. IEEE Trans. Nucl. Sci., vol. 51, pp. 3753–3758, Dec. 2004.

20. Cellere G., Paccagnella A., Lora S., Pozza A., Tao G., Scarpa A.:Charge loss after 60Co irradiation of flash arrays. IEEE Trans. Nucl. Sci., vol. 51, pp. 2912-2916, Oct. 2004.
21. 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 Trans. Nucl. Sci., vol. 51, pp. 3759–3766, Dec. 2004.
22. 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.
23. 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 Trans. Nucl. Sci., vol. 54, pp. 1066–1070, Aug. 2007.
24. Nguyen D.N., Lee C.I., Johnston A.H.: Total ionizing dose effects on Flash memories. IEEE Radiation Effect Data Workshop, p.100, 1998.
25. ESA Radiation design Handbook Draft, 1987.
26. ATMEL AVR Assembler
http://www.atmel.com/webdoc/avrassembler/