Adjusting laser injections for fully controlled faults

Franck Courbon[1,2], Philippe Loubet-Moundi[1], Jacques J.A. Fournier[3], and Assia Tria[3]

[1] GEMALTO, Security Labs, La Ciotat, France
firstname.lastname@gemalto.com
[2] Ecole des Mines de Saint-Etienne, CMP-GC/LSAS, Gardanne, France
firstname.lastname@mines-stetienne.fr
[3] CEA, CEA Tech Region, DPACA/LSAS, Gardanne, France
firstname.lastname@cea.fr

Abstract. Hardware characterizations of integrated circuits have been evolving rapidly with the advent of more precise, sophisticated and cost-efficient tools. In this paper we describe how the fine tuning of a laser source has been used to characterize, set and reset the state of registers in a $90nm$ chip. By adjusting the incident laser beam's location, it is possible to choose to switch any register value from '0' to '1' or vice-versa by targeting the PMOS side or the NMOS side. Plus, we show how to clear a register by selecting a laser beam's power. With the help of imaging techniques, we are able to explain the underlying phenomenon and provide a direct link between the laser mapping and the physical gate structure. Thus, we correlate the localization of laser fault injections with implementations of the PMOS and NMOS areas in the silicon substrate. This illustrates to what extent laser beams can be used to monitor the bits stored within registers, with adverse consequences in terms of security evaluation of integrated circuits.

Keywords: Laser fault injection, registers attacks, bit set and reset, fault model

1 Introduction

Several attacks can be performed on integrated circuits to bypass security mechanisms or access sensitive data. Those attacks are usually classified into four categories: logical attacks where the attacker exploits a weak software implementation [3]; side-channel attacks where power or electromagnetic or timing based information are used to learn about the data manipulated by a given device (SPA [15], DPA [11] and CPA [4]); invasive attacks where the device is physically and irreversibly modified[1]; and fault attacks where external perturbations are used to induce faults during the execution of a given sensitive program or on the sensitive data being manipulated [19,2]. This last kind of attack can be performed using several means like a flash light, laser beam, electromagnetic pulse [5], voltage or clock glitches.

In this paper we focus on the use of a laser beam as a security characterization tool for Integrated Circuits (IC): with such means, precise and localized effects can be induced into the device without damaging the latter (usually a simple decapsulation of the chip is enough) at relatively low costs ($\approx 20 Keuros$), thanks to the decreasing costs of laser sources. We describe how the precise use of a laser beam can be used to characterize, set and reset the state of registers in a $90nm$ IC. We correlate laser faults injection results with physical implementations of the PMOS and NMOS. The explanation for the observed phenomenon is obtained by the use of imaging techniques.

The paper is organized as follows. We first introduce some of the hardware design concepts used in the paper as well as some background information on laser-based fault injection techniques. Then we describe the experimental set-up used, the device under test (DUT) and the methodology applied. The monitoring of registers using laser-based fault injections is then depicted: we describe the tests performed and show the overlay between the laser fault-based mapping and the register's physical implementation. We then discuss about our findings relative to recent publications, we describe limitations and future work before concluding on how such techniques can have adverse consequences in terms of security.

2 Hardware design aspects

2.1 IC physical layers

Integrated circuits are made out of silicon wafers. The different manufacturing steps are performed on only one side of the wafer usually called the active side, top side or front side. For our laser fault injections, we will use the other side, called the backside, which can be thinned and polished. Either way, the final wafer thickness is relatively high - 100 times - compared to the active layer. This parameter must be considered for setting up the laser.

The active layer is made, from bottom to top, of P or N doped silicon regions to constitute a transistor's drain and source. A polysilicon layer is used to make transistor gates with minimal dimensioning. Then, the first metal layer is used to connect the different transistors to build a logic gate. Those gates are linked together by interconnection or supplied by power routing lines. All metal layers are separated by insulation layers. Finally, a passive layer protects the chip from corrosion or packaging or handling stresses.

2.2 Logic gate consideration

Integrated circuits are made up of elementary functional gate structures also called standard cells. During the place and route phase of the circuit's design the arrangement of standard cells is optimized to reach the best compromise between area, timing and power constraints. In a typical secure product, basic blocks - i.e. CPU, coprocessors, logic functions - are scrambled and are part of

the synthesized logic. Depending on the chip complexity, several thousands to millions of logic gates are implemented. The smallest gate is the inverter which is composed of two transistors (as we are in Complementary MOS circuit design). The number of transistors used in other, more complex, logic gates can be ten times larger. Basic gates function are NOT, AND, NOR, XOR, NAND and few others like flip-flops or latches. Even if the number of logic functions provided is relatively small, the number of basic gates available in the standard cell library could be more than 10 times larger, depending on the number of inputs (i.e. NAND2, NAND3), the amount of current driven or on the presence of optional reset or clock signals. It is possible to temporarily store a single bit of data in a register which can be either a latch or a flip-flop. A latch output is constantly affected by its input as long as the enable signal is set. On the other hand, a flip-flop updates its value only at a rising or falling edge of the enable signal which usually is the clock signal. This article only deals with flip-flops even if it could be extended to any CMOS based logic gate or to volatile storage structures.

2.3 Register hardware structure

Storing bits within the synthesized logic requires several transistors: about 20 to 30 transistors are needed to build a single flip-flop. We focus in this paper on bistable flip-flops that are standard cells implemented within the synthesized logic in order to store temporary values or to speed up the data access. They are widely used in core processor unit or in cryptographic coprocessors.

The structure of flip-flops depends on their types; i.e D type or E type (enable) and if there is a synchronous reset input or an asynchronous one. Typically, for a $90nm$ technology a flip-flop size is of the order of $15\mu m^2$ and becomes bigger when an enable and a reset signal are implemented. Flip-flops such as other memory elements require specific timing requirements including set up and hold times on data and minimum pulse widths on clock inputs [10].

The flip-flop considered here is of D-type with an asynchronous reset from which any edge-triggered type storage element can be designed with a few extra gates. For performance, layout density and energy efficiency, gates are always designed and optimized at the transistor level. Their implementation requires several stages: inverting input buffer, two types of latches, possibly an output multiplexer, output buffers, clock preparation and asynchronous reset signal.

A basic D flip-flop layout is given in Figure 1; we acknowledge that this type of gate is more complex that those studied in previous works [16]. This flip-flop contains 24 transistors and a theoretical study of a laser beam's effect over such a gate would require dedicated and custom tools to be able to run significant simulations.

3 Laser beam injection

3.1 Laser/Matter interaction in CMOS circuits

Within a single flip-flop logic gate, several pairs of NMOS and PMOS transistors are implemented. Implanting P-type dopants into some N-type base material,

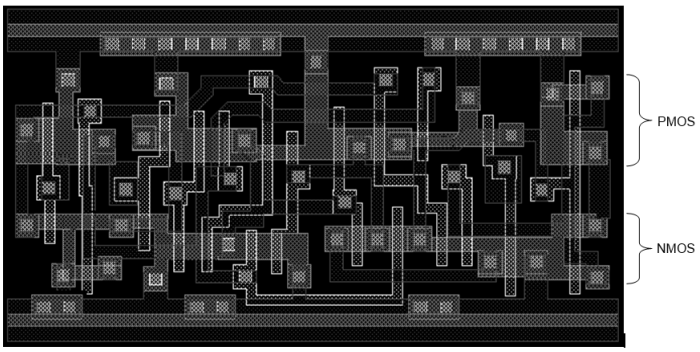

Fig. 1. A flip-flop layout

or vice versa, create PN junctions. Those junctions are sensitive to a photoelectric effect when exposed to a laser beam [8]. This induced photocurrent may switch a transistor's state thus affecting the output of a logic gate. Previous works based on an inverter [16] showed that when the input is '1', the drain of the NMOS 'becomes the sensitive' part and when the input is '0' the drain of the PMOS 'becomes the sensitive' one. Moreover, depending on the type of targeted MOS transistors the required power to switch a transistor is more or less important [17]. Measurements made by Sarafianos *et al.* [17] give a difference of photocurrent 6 times higher for a specific NMOS junction (N+/P-sub, large ellipse) than for a PMOS one (P+/N-well, small ellipse) in $90nm$ technology and for a given process.

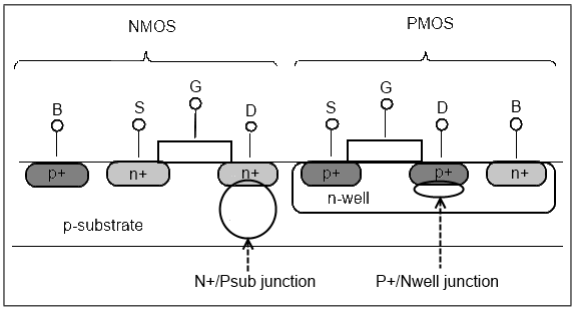

Fig. 2. NMOS, PMOS and generated photocurrent

In [18], the author also notes that the N-well/P-sub junction (present only for PMOS transistors as seen in Figure 2) despite having the largest surface, creates a small photocurrent. Furthermore, as our shoot duration is superior to tens of ns, we use the model given for a shoot duration over $8ns$ and in this model, even if pnp associations are present, currents created with parasite bipolar junction

transistors are neglected. Without any knowledge of our flip-flop layout, based on these previous works, we can guess that a bit initialized at '1' would be more sensitive to a laser beam. Indeed, as PMOS transistors are connected to the upper rail voltage and NMOS ones to the lower rail voltage, reaching a '0' value might be performed through the switching of the state of one or several NMOS transistors.

3.2 Laser based fault attacks

The laser bench used to perform faults in integrated circuits evaluation is characterized by:

- High spatial precision
- Local effect area
- Accurate timing
- High fault repeatability
- Multiple faults capability

Thus, using laser fault injections, several types of attacks are feasible against cryptographic operations: such as safe error attacks where the attacker can guess for example key value by observing the output after a single bit modification [14,13]; algorithm modification attacks [6] where the attacker can change a single bit of a register and reduce, for instance, the number of rounds performed in a cryptographic algorithm; and differential fault attacks [7] where an attacker can exploit fault injections to guess a key. This paper deals with the laser effect over a complex logic gate.

4 Experimental set-up

4.1 Device under test and methodology

In our experiments, we use a recent IC microcontroller with a technology node of $90nm$. We focus our investigations onto the synthesized logic of the sample covering about a fourth of the global integrated circuit's size. Due to dense metal routing on the top side of the chip, we decided to use backside analysis in order to ensure that a uniform laser power reaches the active layer. Thus, the DUT's backside is opened and then placed under the microscope which focuses the laser beam through the substrate. The DUT is monitored and we perform the following experimental operations:

- A. Load data register.
- B. Perform laser shoot.
- C. Read back register value.
- D. Move XY stage and perform A/B/C repeatedly.

Using an open sample, we only read a unique register value. The resulting output file is a matrix of the faulted XY positions which displays only the faults injected into this single register.

4.2 Laser platform

The laser test platform is composed of a microscope with different focusing capabilities, a laser cavity, an electrically controlled XYZ stage, an oscilloscope, a device under test (DUT) and electronic boards to drive the different equipments and to precisely synchronize them together. The set up must be well defined in terms of:

- Pulse shape and characteristics such as wavelength, energy, duration.
- Pulse repeatability.
- Spatial localization on the chip.
- Temporal localization in the process (not really applicable for static registers approach though).

Our platform enables us to measure the power reaching the integrated circuit's backside. We measured this for each input command value applied to our laser source. This output power can vary from few mW to $800mW$ peak and we can set the pulse duration as short as tens of ns. According to power measurements and oscilloscope signal observations, we can measure the energy reaching the backside surface of the die.

$$E = P_{peak} * \Delta T$$
$$E(Joules) = P_{peak}(W) * \Delta T(s)$$

We use a $1064nm$ laser wavelength that enables us to obtain a trade-off in terms of photoelectric effect and substrate absorption [9]. The optical absorption of a laser beam in the silicon depends on the substrate doping concentration and the wavelength used. Our set up has a spatial precision of the order of the μm.

5 Monitoring register bits using a laser beam

In the rest of this paper, we assume that timing constraints are not an issue as we perturb a static register which stores the programmed data during the entire execution of our process. The hardware design of those registers does not include a dynamic return to the previous value so we can fault a register at any time, and then read the value back. Within the following subsections we describe how to find a register location over the entire DUT (5.1), how a localized laser beam can control the bit value (5.2), how the bit value can be obtained with a laser mapping (5.3) and how a power controlled laser beam can clear a register value (5.4).

5.1 Finding the area of interest

The entire synthesized logic block is scanned with a large step (around $25\mu m$) and a large beam spot (around $10\mu m$). This allows finding the bits of interest over the entire chip. Some bits are missing as we attack with a large scanning step. We also obtain multiple-bit faults with such energy and spot sizes. However, once a

register bit is found, chances are high of finding all the others nearby, even if the synthesized logic scrambles the structure. The precision of our experimental set-up is the key point for the success of our experiments. After empirical tests, we found a set up for a hundred percent faults injection success rate by applying an energy of tens of nJ on the backside of the circuit. With these laser parameters, no particular alarm is triggered by the chip.

For the rest of our experiments, we limit the area of interest to the area where some bits of the register have been revealed. This area becomes the new region to scan. Thus, the next figures only display a small part of the integrated circuit. This is less time consuming, more attacks can be performed with different sets of parameters. After finding this area of interest, we then use a smaller step (around $1\mu m$) and a smaller laser spot size (around $2\mu m$). We increase the magnification with a $50\times$ objective and we target an area of $30 \times 38\mu m^2$. The laser scans are performed with an X and Y step of $1\mu m$. We hence have $30 \times 38 = 1140$ positions to analyze.

5.2 Controlling the modification of a register by localization

A flip-flop is usually implemented using a large number of transistors and there are only two values that can be stored in a flip-flop logic gate, a '1' or a '0'.

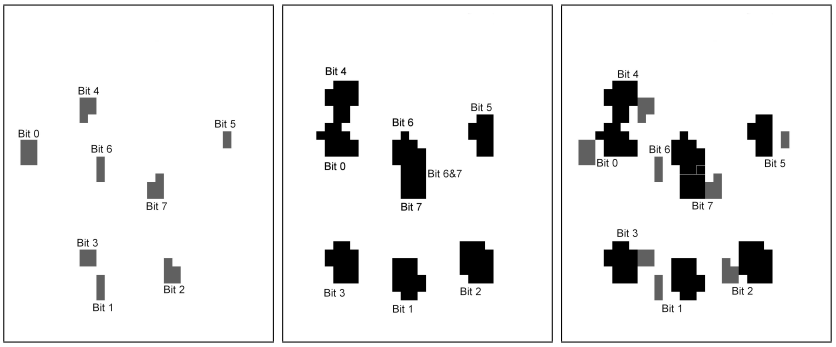

Fig. 3. '0' to '1' bits faults, '1' to '0' bits faults, '1' to '0' and '0' to '1'

Over the reduced scan area defined in (5.1), only 8 bits are implemented, and for the first scan on the left of Figure 3, we set the register value with '00000000' before scanning the $30 \times 38\mu m^2$. As the registers are all programmed with a '0' value, we are only able to detect when the laser shoot switches the output value to '1'. As naming convention we talk about 'reset' or 'bit reset' when the value switches from '1' to '0' and 'set' or 'bit set' when the value switches from '0' to '1'. In the figures to come, the grey or black squares represent a bit switch whereas white pixels are used when no error is recorded. For the middle part of Figure 3, inversely we set the initial register bits with '1's. It gives us another mapping on which we see the positions where the laser beam switches a bit to

'0'. Both mappings put together give the "superposed representation" on the rightmost picture of the figure.

We thus localize characteristic patterns: for each bit set in Figure 3 for instance, we get a specific location where the laser could be applied to change the bit value. 8 distinguishable locations are found, one for each of the 8 register bits. With the second mapping we get the same status to have bit reset. However with the third part of the image we can say that bit set or bit reset sensitive areas are distinct areas. As another result, if we assume that the same logic gate is used for all the bits, we also get some information about pattern rotation. For instance if bit number 1 has a reference rotation, then bit number 3 is mirrored. We thus suppose the flip-flop gate physical implantation to be mirrored. For each of those eight logic gates, using one laser shoot targeting the right sensitive positions, we can exactly control the stored value at the logic gate output.

In Figure 4, we show that half of the bits present over this area have their bit set sensitive part on the left side of the reset sensitive part. This gives some information about the orientation of each logic gate.

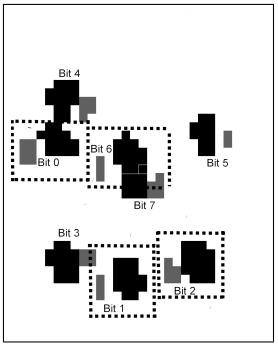

Fig. 4. Logic gates orientation

5.3 Differentiating register bit values with laser mapping

Figure 5 shows the mapping of faulted values that were observed for 4 different initial settings of the 8-bit register. In the upper left picture, the register is programmed with all zeros. In the upper right picture, all ones are written before performing the laser scanning. The pattern '11110000' is written in the case of the lower left picture and in the lower right one, '00001111' is programmed in the register.

We observe that the bit set and bit reset have different sensitivities. The observation of the location where the faults occurred gives direct information about the initial value of the bit. In our tests the "larger" sensitive areas correspond to an initial state at '0' and the "smaller ones" are representative of an initial state of '1'.

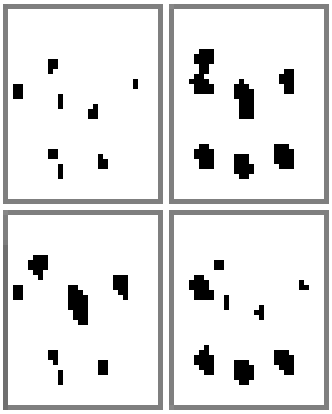

Fig. 5. Laser fault injection mappings at $39nJ$ with different initial values; top-left: '00000000', top-right: '11111111', bottom-left: '11110000', bottom-right: '00001111'

5.4 Controlled register clearing by power selection

We observed that the laser location can be tuned to change in a controlled way the stored value in a register flip-flop. So, another test campaign was conducted to find if other laser parameters can be used to increase our capabilities to change registers' contents in a controlled way. Therefore, we set the initial register value to '00001111' and consecutively change the laser exposure time and the laser beam power, resulting in a successively decreasing the energy. If we look at the pictures from the left to the right in Figure 6, the energy hitting the chip's backside is successively $32nJ$, $13nJ$ and $10nJ$.

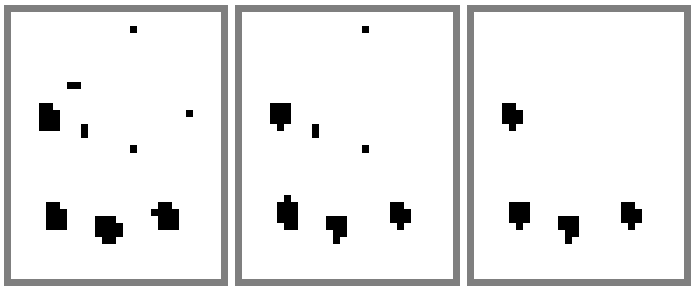

Fig. 6. Pertubation of the register initialized at '00001111' with different energies; left: $32nJ$, middle: $13nJ$, right: $10nJ$

Figure 6 shows that a careful control (an energy high enough to perturb a type of transistors without perturbing the other type of transistors) of the injected energy only allows to reset bits and to let bit initialized at '0' unchanged. The

contents can be controlled very precisely with this set up. Using a large spot size and adequate energy, an attacker could clear all the bits of the flip-flops present under the laser beam.

A sensitivity map is drawn from the experiments done, it well illustrates obtained effects depending on the level of energy applied. Obviously, table 1 is valid over this given circuit and for the spot size and wavelength used.

Case number	1	2	3	4	5
Energy level	Few nJ	10nJ	13nJ	32nJ	Over several tens of nJ
Bit reset	Not all bits switched	All bits switched at a given location	All bits switched at a given location	All bits switched at a given location, different of bit set zone	All bits switched but no more sub-gate spatial resolution
Bit set	No bit set	No bit set	Not all bits switched	All bits switched at a given location, different of bit reset zone	All bits switched but no more sub-gate spatial resolution

Table 1. Observed effect depending on level of energy hitting the circuit backside

6 Correlating fault attacks and transistors implementation

The effects depicted in the previous sections are linked to the underlying hardware implementation. Based on the results of the different laser injection effects obtained on the chip, we decided to implement an invasive approach on a second identical sample. For that purpose, the chip is first depackaged with nitric acid. Then, the device is dipped into a hydrofluoric acid bath, and then rinsed with water to remove all metal and oxide layers. The chip is dried before performing scanning electron microscopy (SEM) image acquisition. Figure 7 is the "bulk" level picture of the area scanned during our laser tests. '8' columns of logic gates are visible and the P-well or N-well active areas - representative of CMOS process - of each column can be easily distinguished. In the same picture, a logic gate is highlighted by a black rectangle whereas the white circle gives an idea of the size of the laser spot used ($\approx 2\mu m$).

In CMOS circuits the output current of PMOS or NMOS transistors can be approximated by $I \approx \mu_{p,n} * W/L$ where μ is the mobility of the carriers, W and L respectively the width and length of the transistor gate. L is fixed by

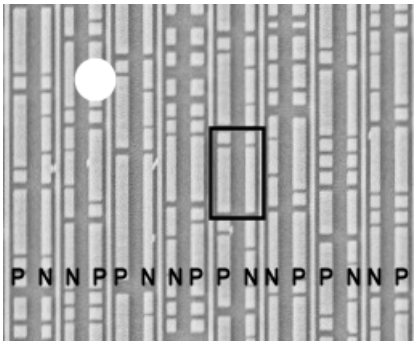

Fig. 7. N and P-well implementation, single gate and spot size representation

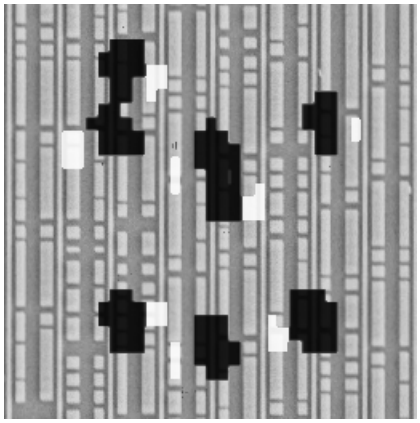

Fig. 8. Laser faults mapping overlaid on Scanning Electron Microscope image

the technology node. This output current must be balanced. So, this is partially realized by adjusting the W parameter. The mobility μ_p of the hole carriers is smaller than that of the electrons μ_n. So, the width of the gate of PMOS transistors must be larger. On the SEM image, this property is used to clearly identify PMOS or NMOS location.

If the laser fail map is overlaid with the SEM image (Figure 8), we can directly see that the relative locations of the bit set (white squares) or bit reset areas (black squares) within a gate are respectively over the PMOS area and the NMOS area. In addition, for the energy of laser shoot, the sensitive area is larger when the bit is initially programmed at '1' (bit reset, black squares). For the flip-flop gate used in the analyzed register, shooting with the laser on the NMOS will reset the bit whereas shooting on the PMOS will set the bit from '0' to '1'.

7 Discussion and future work

Comparison to SRAM fault model and generated junction photocurrent: The work of Roscian *et al.* [16] targeted a SRAM memory element with a valid bit set and bit reset model. In their work the experimental results are in line with the electrical simulations performed. In our work we target a more complex gate where the layout of the flip-flop and the logic gate transistors schematic were not available. Moreover, we showed a strong dependency between laser fault injection behavior and PMOS or NMOS areas. In addition, we also validated this model on a more recent technology - $90nm$ vs $0.25\mu m$ - used in current standard smart card devices.
In [17], Sarafianos *et al.* observed a difference between the generated photocurrents over an NMOS pn junction and those over a PMOS pn junction. This result is also confirmed by our results as NMOS transistors reveal a higher sensitivity.

Limitations and future works: As the internal design of the gate studied was unknown and as our laser spot size was not capable of targeting a single transistor it is impossible to validate this experimental result with electrical simulations. For example, the number of transistors disturbed by the laser effect is unknown. The contribution of each disturbed transistor to the final flip-flop switching is missing. This knowledge is very significant for a designer who wants to make a standard cell more resistant against laser attacks. The future work will be to reproduce the same experiments on a device where all the data of the standard cell used for bit storage registers are available. Simulations and deeper fault modeling at transistor and gate level would also be possible.

Threats and countermeasures: Our experiments reveal a threat introduced by the capability of controlling the values of registers bits with a proper laser set up. As an evolution of the work of Leveugle *et al.* [12], and from an attackers point of view, bit set, bit reset or register reset could now be considered as really practicable fault models, even on very recent semiconductor technologies. We can reasonably think that state of the art cryptographic implementations are protected against safe errors or DFA but vulnerabilities introduced on other sensitive registers must be carefully analyzed. If no existing hardware countermeasures - such as hardware redundancy - are provided by the device to protect against registers modifications, the software must monitor those registers' integrity frequently. For example, randomly check of register coherence could be performed before and after sensitive operations. This may imply significant performances loss though.

8 Conclusion

We present in this paper the realization of practical laser tests performed on a $90nm$ device. Our initial target was to analyze the effect of the laser beam on flip-flops of a register and to reach the limits provided by our equipment. We

highlight that a reliable fault injection requires to perfectly monitor the laser beam positioning, the laser beam size and the laser pulse parameters. With the correct set up, it is possible to control with a 100% success rate the fault injection effect on a single bit: '0' to '1' or '1' to '0'. We also succeed in tuning our laser parameters to only reset the register bits initialized at '1' whereas register bits with initial value at '0' are left unchanged. Finally, we correlate the laser fault mapping with the physical image of the area under test. With this observation, we are able to explain that the difference of sensitivity is due to the nature of the active area (PMOS or NMOS) exposed within the standard cell. This latest result shows the interest for security characterization to use laser beam sizes smaller than the logical gate's width. The fault models usually used in cryptographic attacks - e.g. safe errors, register reset - are validated by the present study. High injection rates with fine tuned laser beam increase the requirements of strong software or hardware counter measures against fully controlled faults.

Acknowledgment

We gratefully acknowledge technical support and knowledge sharing of Pascal Moitrel. We also would like to thank Francis Olivier for proofreading this paper.

References

1. Anderson, R., Kuhn, M.: Low cost attacks on tamper resistant devices (1997)
2. Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C.: The sorcerer's apprentice guide to fault attacks. IACR Cryptology ePrint Archive p. 100 (2004)
3. Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S.P., Anderson, R.J.: Chip and skim: cloning emv cards with the pre-play attack. CoRR (2012)
4. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: CHES. pp. 16–29 (2004)
5. Dehbaoui, A., Dutertre, J.M., Robisson, B., Tria, A.: Electromagnetic transient faults injection on a hardware and a software implementations of aes. In: FDTC. pp. 7–15 (2012)
6. Dutertre, J.M., Mirbaha, A.P., Naccache, D., Ribotta, A.L., Tria, A., Vaschalde, T.: Fault round modification analysis of the advanced encryption standard. In: Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on. pp. 140–145 (2012)
7. Giraud, C.: Dfa on aes. In: Advanced Encryption Standard - AES, 4th International Conference, AES 2004. pp. 27–41. Springer (2003)
8. Habing, D.: The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. Nuclear Science, IEEE Transactions on 12(5), 91–100 (1965)
9. Johnston, A.: Charge generation and collection in p-n junctions excited with pulsed infrared lasers. Nuclear Science, IEEE Transactions on 40(6), 1694–1702 (1993)
10. Kaeslin, H.: Digital Integrated Circuit Design: From VLSI Architectures to CMOS Fabrication. Cambridge University Press, New York, NY, USA, 1st edn. (2008)
11. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: CRYPTO. pp. 388–397 (1999)

12. Leveugle, R., Ammari, A., Maingot, V., Teyssou, E., Moitrel, P., Mourtel, C., Feyt, N., Rigaud, J.B., Tria, A.: Experimental evaluation of protections against laser-induced faults and consequences on fault modeling. In: Proceedings of the Conference on Design, Automation and Test in Europe. pp. 1587–1592. DATE '07, EDA Consortium, San Jose, CA, USA (2007), http://dl.acm.org/citation.cfm?id=1266366.1266715
13. Loubet-Moundi, P., Vigilant, D., Olivier, F.: Static fault attacks on hardware des registers. IACR Cryptology ePrint Archive 2011, 531 (2011)
14. Marc Joye, P.P., Yen, S.M.: Secure evaluation of modular functions (2001)
15. Mayer-Sommer, R.: Smartly analyzing the simplicity and the power of simple power analysis on smartcards. In: Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems. pp. 78–92. CHES '00, Springer-Verlag, London, UK (2000), http://dl.acm.org/citation.cfm?id=648253.752540
16. Roscian, C., Sarafianos, A., Dutertre, J.M., Tria, A.: Fault model analysis of laser-induced faults in sram memory cells. In: Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on. pp. 89–98 (2013)
17. Sarafianos, A., Roscian, C., Dutertre, J.M., Lisart, M., Tria, A.: Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an {SRAM} cell. Microelectronics Reliability 53(September 2011), 1300 – 1305 (2013), http://www.sciencedirect.com/science/article/pii/S0026271413003016, european Symposium on Reliability of Electron Devices, Failure Physics and Analysis
18. Sarafianos, A.: Injection de fautes par impulsion laser dans des circuits sécurisés. These, Ecole Nationale Supérieure des Mines de Saint-Etienne (Sep 2013), http://tel.archives-ouvertes.fr/tel-00944943
19. Skorobogatov, S.P., Anderson, R.J.: Optical fault induction attacks. In: CHES proceedings. pp. 2–12. Springer-Verlag (2002)