LLFI: Lateral Laser Fault Injection Attack

Joaquin Rodriguez, Alex Baldomero, Victor Montilla, and Jordi Mujal
IT Labs
Applus+ Laboratories
Bellaterra (Barcelona), Spain
{*joaquin.rodriguez.c, alex.baldomero, victor.montilla, jordi.mujal*}*@applus.com*

***Abstract*—In this work, a novel technique of fault injection attack on secure integrated circuits (ICs) devices is presented: Lateral Laser Fault Injection (LLFI). Laser Fault Injection with backside illumination is typically the most efficient and widely used technique to perturb secure ICs. However, the appearance of new packaging techniques and new physical countermeasures that may block or difficult the IC backside access may limit the efficiency of such technique in the future. In this context, a new Laser Fault Injection alternative is proposed. The IC is attacked through the side of the chip, by focusing the incident laser beam on that area. This novel concept is presented and experimentally proven in this paper.**

***Keywords*-Laser; LLFI; Fault Injection Attack; Secure chip; HW Security**

I. Introduction

Secure ICs are designed to protect the confidentiality and the integrity of sensitive information against logical and physical attacks. Fault injection attacks imply actively manipulating chip internals in order to cause a fault during the execution of some process. This technique with different variants has been proven to be very powerful [4]. The most widely known techniques for inducing such faults are Laser Fault Injection (LFI)[14], [15], Electromagnetic Fault Injection (EM-FI)[13], [7], Body Biased Injection (BBI)[12] and voltage or clock glitches [3].

The most common hardware physical countermeasures against this type of attacks are passive and active shields to protect the chip against physical access and manipulation, and a variety of sensors to detect anomalies in terms of temperature, voltage, light, or clock frequency. Today, efficient countermeasures for glitch attacks are implemented in security chip design, which has caused that, EM-FI, BBI and especially LFI have become the main used techniques to induce faults in modern secure ICs.

LFI is believed to be the technique that obtains the most precise results. On the other hand, it is the most expensive, and requires having access to the silicon surface in order to inject light successfully. Both frontside and backside were successfully proven to be used with this technique. However, the frontside of the chip is harder to attack due to specific physical countermeasures implemented or the metal circuitry itself, which may block the light. Therefore, the vast majority of laser FI attacks are carried out through the backside of the chip.

A partial IC package decapsulation may be enough to expose the bare silicon and to focus the laser light on its surface. It has been demonstrated that this can be feasible on standard packages [10], [16]. However, IC encapsulations are evolving into more complex structures, which means that new challenges are arising.

Three-dimensional silicon integration like the ones exposed in figure 1, is a promising technique that offers an improvement in terms of performance, integration density and cost. From a security point of view, the impact of this new technology has not been studied in depth, and only few works exist [1], [8], [9]. In any case, it is agreed that this type of package intrinsically adds some difficulty to access the chips surface, and consequently hindering some typical semi-invasive attacks, such as EMA analysis for side channel, or LFI for fault injection.

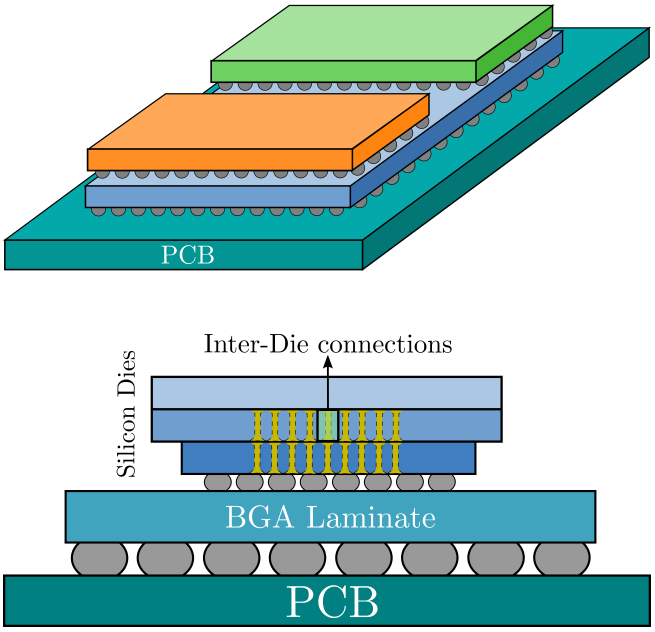


Figure 1: Two examples of 3D stacked ICs integration from different views

Furthermore, new physical countermeasures are being developed to protect the IC's backside against laser fault injection [5], [2], [11]. These prevent access to the active

area of the silicon die, even when the backside surface of the chip is available. Hence, it is clear that the LFI technique may become more difficult to apply, as new packaging techniques are consolidating, and several physical countermeasures are appearing to protect the IC backside from laser attacks.

Within this context, the contribution of this work is to propose a new FI technique (LLFI) that uses the side of the chip as a new surface of attack and which could bypass some of the current LFI limitations presented above.

In order to provide evidence of the effectiveness of this new attack technique, different experiments have been carried out on two different secure chips. The results obtained from the LLFI attacks were compared with standard backside LFI attacks.

The paper is organized as follows; Section 1 gives some background for this paper proposal. Section 2 explains the proposal of a new FI attack. Section 3 describes the experimental setup used for the tests. Section 4 presents the testing results of the LLFI attack compared to standard backside LFI. Finally, conclusions are presented in section 5.

II. Background

Laser Fault Injection attacks are based on the photoelectric effect resulting from the interaction of the light with semiconductor's PN junction. Laser radiation can generate an electron-hole pair in these regions if its photon energy exceeds the semiconductor band gap. The induced photocurrent derived from this interaction can change the state of a transistor and, therefore, alter the output of a logic gate. The bandgap for Silicon at room temperature (300 K) is 1.12 eV [17]. The equation for photon energy E in eV:

$$E = \frac{hc}{\lambda} \tag{1}$$

where h is the Planck's constant expressed in eVs, c is the speed of light in vacuum, and λ is the wavelength of the electromagnetic radiation.

According to equation (1), laser beams with wavelength longer than 1100 nm, cannot generate an electron-hole pair and they are not suitable for use in fault injection attacks. On the other hand, the penetration depth of the laser beam is also dependent on both the wavelength and the substrate where is focused the beam. The intensity of laser I decays exponentially with depth x according to the Beer-Lambert law:

$$I(x) = I_0 e^{-\alpha x} \tag{2}$$

Where I_0 is the intensity of the beam just inside the surface and α is the absorption coefficient of the substrate material.

Consistent with equation (2), laser beams with wavelength shorter than 800 nm are absorbed in the first few μm of the silicon substrate while longer wavelengths penetrate within the IC [6]. Therefore, they could be used for fault injection attacks from the frontside, but not from the backside, where the photon must go through the silicon substrate to reach the circuitry of the chip. That is why typically a laser with a wavelength of 1064 nm is used to carry out an LFI from the backside.

III. A new FI proposal: LLFI

As it is known, the standard light perturbation attack consists of focusing the laser source on the backside or the frontside of the chip, with the purpose to change the IC behavior while it is executing a security function. Considering the evolution of new 3D stacking packages and new countermeasures that hinder the access to the silicon through the back and front sides, an alternative surface is proposed to perform an LFI attack.

In this paper, a new variant of LFI attack is presented through the side of the chip. Therefore, the hypothesis is that the side of the chip is also a valid surface to inject light with the aim to carry out an LFI attack. Then, this new attack surface could be a potential threat when devices are protected with backside and frontside physical countermeasures, or use packages that make their access difficult. This idea is presented in figure 2, where a standard scenario, in which backside LFI can be applied, is compared to an alternative scenario, in which this technique cannot be applied, and only LLFI may be directly applicable.

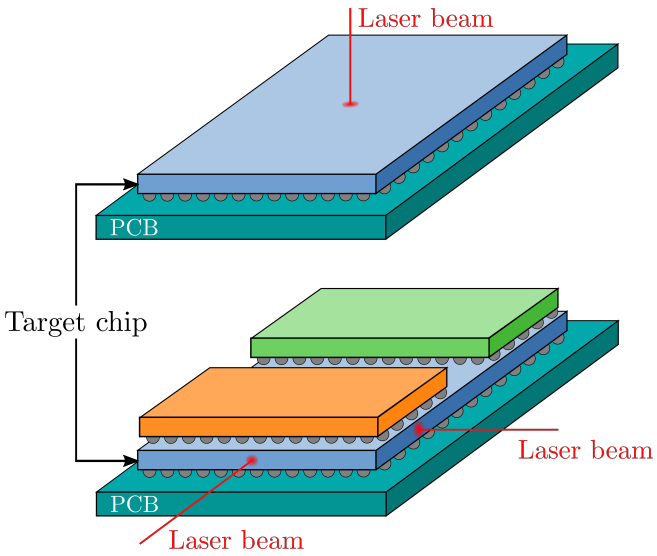


Figure 2: Standard backside LFI attack (left) vs new proposal LLFI attack (right)

The light would require as much penetration as possible into the die, through the silicon substrate, in order to reach sensitive faulty regions. These regions may be located from a few microns to few millimeters from the side surface.

Hence, according to the previous analysis, the 1064 nm laser wavelength should be the most suitable for this type of attacks. The work is presented as a proof of concept and as an experiment to compare LLFI with LFI, that is why two security chips with a standard encapsulation were used for the tests.

IV. Experimental Setup

In order to demonstrate the feasibility of LLFI attacks, two different secure ICs were tested and compared with standard backside LFI.The two chips implement typical security measures which are in the current state of the art, such as: voltage detector, glitch detector, laser detector, active shield, or error detection mechanisms in memories. Different sides of the chips and different laser parameters were used to evaluate the effectiveness of the attack and its behavior. The laser setup used to carry out the different tests was a standard arrangement for LFI attacks based on an infrared laser with the following characteristics: 1064 nm wavelength, maximum pulse width of 2500 ns and maximum pulse power of 2 W. The optical path outputs a laser spot diameter of 12 μm at the focal point with the use of a lens with a $X5$ magnification. The device under test (DUT) was positioned under the optics with the target side at a right angle to the laser beam. Figure 3 shows the DUT A under the optics of the setup.

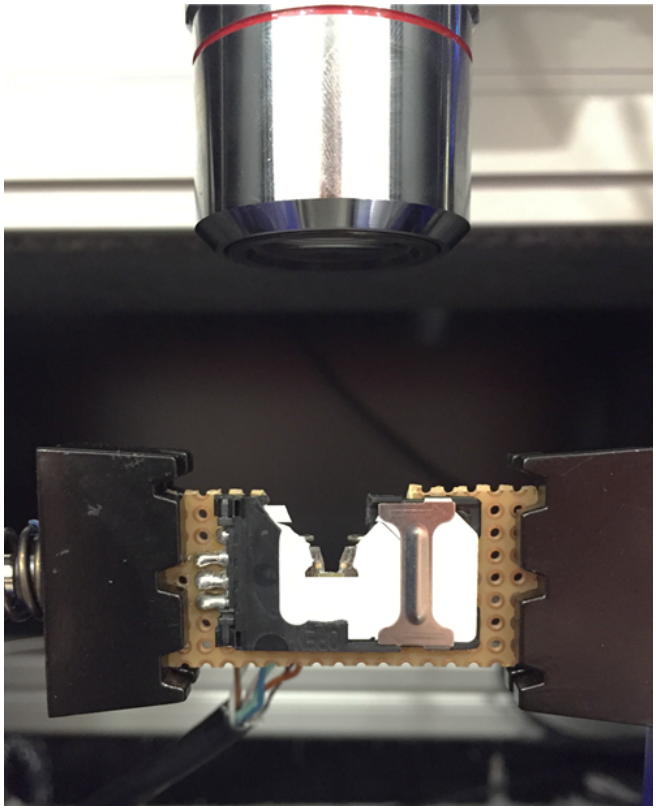


Figure 3: LLFI setup, DUT A under the laser optics.

Table I summarizes the physical properties of each DUT.

DUT	Chip area	Thickness	Exposed sides
A	3.1×2.8 mm^2	150 μm	Backside (a) Side b Side c
B	3.4×3.4 mm^2	150 μm	Backside (a) Side b Side c Side d

Table I: Physical properties of the devices under test.

DUT A: The chip was prepared by de-packaging the integrated circuit die by mechanical means, and exposing part of the silicon surface. No polishing has been done on any of the attacked surfaces. Sides d and e were not involved in the testing, as the wires connecting the chip with the metal contacts were located there and difficult whole access to these surfaces (Figure 4).

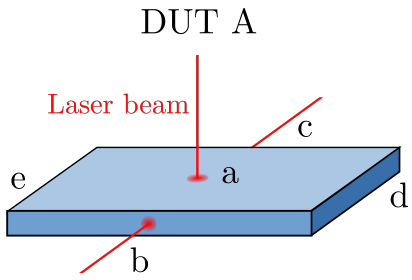


Figure 4: Attacked sides on DUT A

DUT B: The chip was prepared by de-packaging the integrated circuit die by chemical means, and exposing part of the silicon surface. No polishing has been done on any of the attacked surfaces. Side e was not involved in the testing, as the wires connecting the chip with the metal contacts were located there and difficult whole access to this surface (Figure 5).

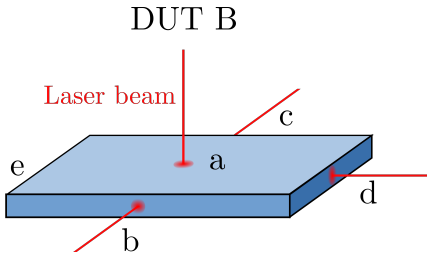


Figure 5: Attacked sides on DUT B

The IC de-packaging techniques used are the standard ones and the same as for backside LFI [10]. In order to evaluate the effectiveness of the attack, a custom code was loaded in the device. It executes a simple security check that

verifies if a password value sent by the user is the same as the reference one stored in the device and returns the result. During the experiment, a wrong password value is sent to the device, and a FI attack is carried out during the comparison in order to force a correct matching result. Hence, the result of the check determines whether the CPU program flow was modified and the attack was therefore successful.

V. Results

The experiments performed were aimed at obtaining results in three important aspects in the context of FI attacks; the spatial location of the faults, the laser energy required to achieve a fault, and the success rate of the attack.

A. Spatial analysis

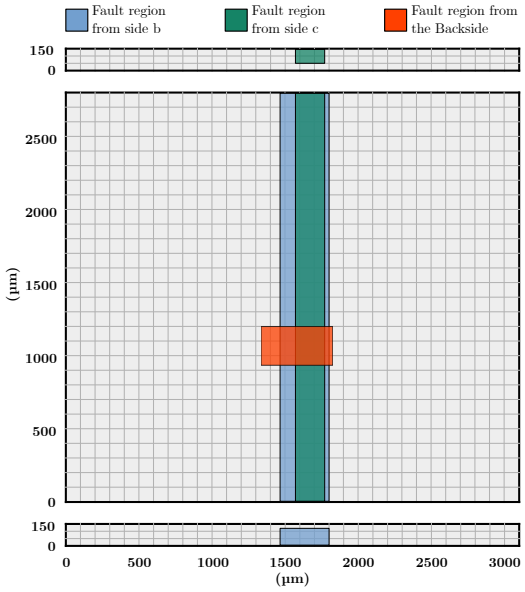
The exposed areas (backside and laterals) of each DUT were fully scanned in order to locate points with faulty behavior. For each location, the laser parameters such as power and pulse width were modified to map the sensitivity of the chip in each region. After scanning the surface multiple times with different parameters, it was possible to perturb the program flow using both LFI and LLFI, and locating vulnerable points in the different surfaces. The faults obtained were analyzed spatially to investigate whether the vulnerable zones for each surface had some kind of relationship. Figure 6 shows the areas where the attack was successful in each surface.

As can be observed, there is some kind of overlap region when projecting surface coordinates in which faulty executions were achieved.

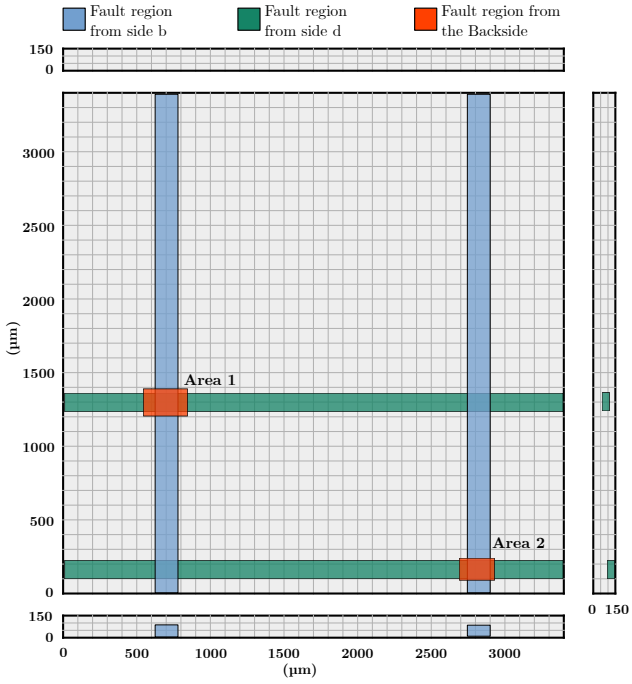
DUT A: There is an overlap regarding the faulty areas projection for each side that suggests that the same physical region is stimulated when faults are obtained.

DUT B: Two areas were identified where a faulty execution could be achieved from the backside, and sides b and d of of the chip. Once again, there is an overlap with respect to the faulty areas of each side. In this device is even more clear that the vulnerable areas detected in the three sides corresponds to the same physical region. However, it was not possible to obtain a faulty execution from the c side of the chip. The explanation for this behavior may be the sensitivity of the circuitry through which the laser beam has to pass until the vulnerable area is reached. If the laser causes a malfunction by affecting this circuitry, it will prevent from achieving a faulty execution.

Furthermore, it can also be concluded that the size of the vulnerable area is dependent on the attacked side. The backside was the surface where the vulnerable area was bigger for all cases. Another important aspect to consider in LLFI attack is the sensitivity of the IC when the laser is focused near the circuitry of the chip (frontside). In this area, the laser causes a malfunction on the IC and hinders the success of the attack.



(a) Vulnerable areas on DUT A



(b) Vulnerable areas on DUT B

Figure 6: Spatial analysis of the vulnerable areas for each DUT and attacked side.

B. Laser energy analysis

The energy required to obtain a faulty execution is also an important parameter to be considered to compare the behavior of the LLFI. This energy is derived from the power and pulse width of the laser beam used for each attack attempt. After identifying the physical vulnerable point, several executions were carried out with different values of energy (combinations of power and pulse width). Then, an analysis of the energy required to obtain a faulty behavior was carried out where the 100% of the energy corresponds to the maximum power with the maximum pulse width of the laser. Figure 7 and 8 show the probability of obtaining a fault depending on the energy used during the attack.

The main conclusion that can be extracted from these tests is that the minimum energy required to achieve a faulty execution is less from the backside than from the lateral. In general, the more distance from the surface to the vulnerable area, the more energy is also required to achieve a faulty execution. The energy required to obtain a fault is as dependent on the attacked device as on the side used to attack. Several reasons could explain these differences, but the most significant ones are: the existing distance between the incident surface and the vulnerable region and the specific layout and the circuitry that compose the chip.

C. Success rate analysis

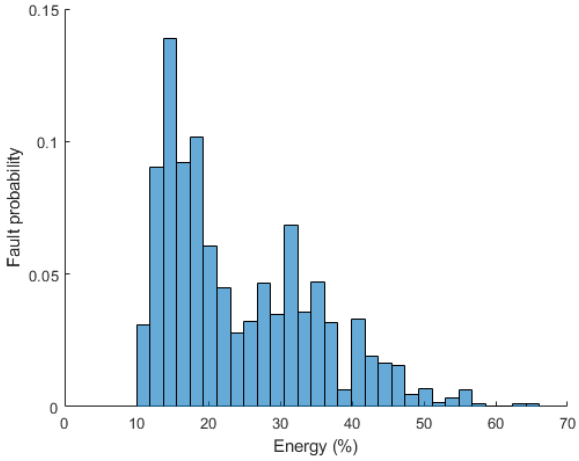
Another very important aspect studied was the success rate of the attack (i.e. faulty executions percentage of total executions). For each vulnerable area and side, laser parameters were adjusted in order to achieve the maximum possible success rate. Different chips were attacked in the same faulty region in order to evaluate the consistency of the obtained results.

Table II summarizes the results of the fault injection rate obtained during the tests on the DUT A.

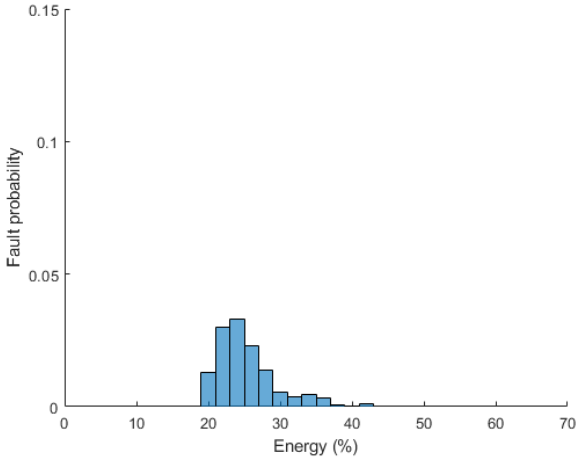
Exposed side	**Success rate**
Backside (LFI)	17.5%
Side b (LLFI)	5.1%
Side c (LLFI)	4.5%

Table II: Success rate of DUT A depending on the attacked surface.

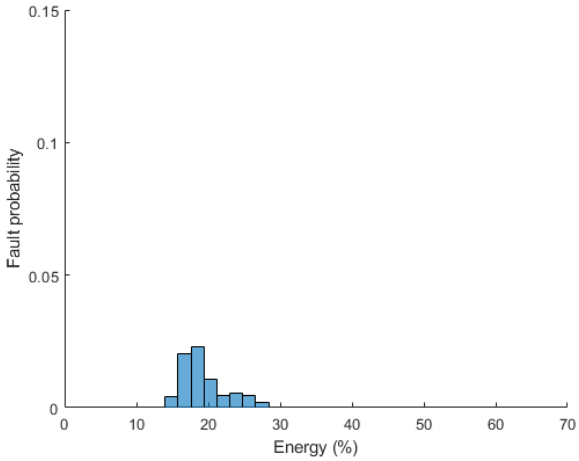
Table III summarizes the results of the fault injection rate obtained during the tests on DUT B. Note that this device has two vulnerable areas, so the maximum success rate was differentiated for each zone.



(a) Exposed side, Backside

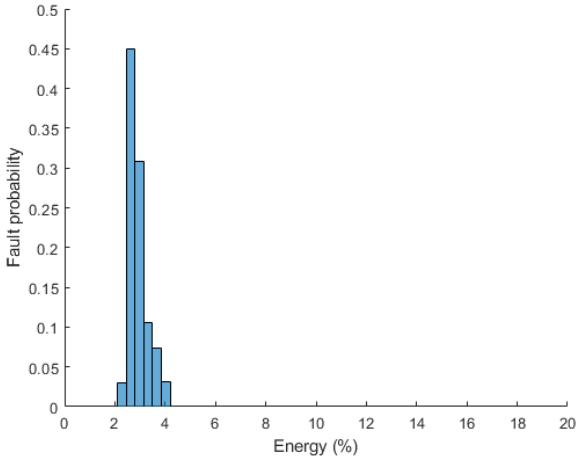


(b) Exposed side, b

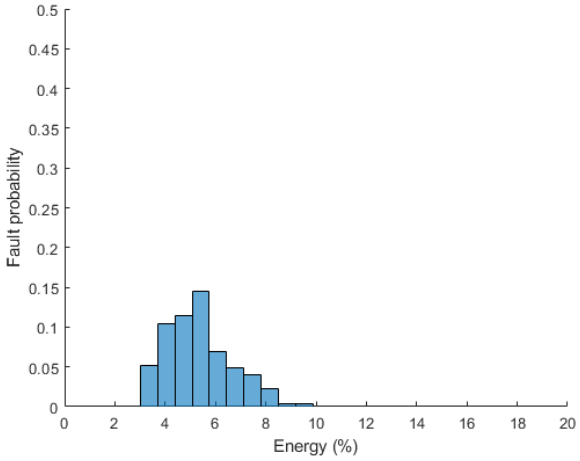


(c) Exposed side, c

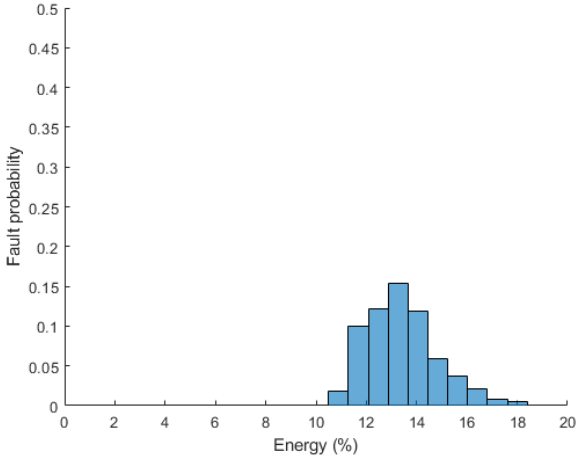
Figure 7: Energy required to achieve a fault execution; DUT A



(a) Exposed side, Backside



(b) Exposed side, b



(c) Exposed side, d

Figure 8: Energy required to achieve a fault execution; DUT B, area 1

Exposed side	Success rate, area 1	Success rate, area 2
Backside (LFI)	74.3%	6.6%
Side b (LLFI)	34.1%	2.9%
Side c (LLFI)	0%	0%
Side d (LLFI)	22.1%	2.8%

Table III: Success rate of DUT B depending on the attacked surface.

As can be observed in the tables II and III, depending on the attacked side, the success rate can vary significantly or even make it impossible to obtain a faulty execution. The differences observed in the success rate can be explained by the same reasons that affect the variations in the previous tests: distance to vulnerable zone and circuitry type over the light path. If this circuitry is more sensitive from one side than the other, the ratio of interrupted executions by critical malfunctions is higher, and therefore, the success rate is lower or even not exist.

VI. Conclusion

In this paper a new method for LFI into secure ICs is presented. This technique is known as Lateral Laser Fault Injection. The results of the experiments showed the effectiveness of the LLFI technique for laser-induced faults in secure ICs. The main advantage of the technique is that opens the door to a new surface of attack where a laser fault injection can be carried out. This can be relevant when the adversary is trying to attack a device using 3D packaging techniques or using backside physical countermeasures to block the laser light.

The experimental results also brought interesting results on the behaviour of this technique. It was showed that there is a kind of overlap between the regions of the laterals and the backside where faults are retrieved. These results corroborate the hypothesis that the same vulnerable region is stimulated independently from the light injection surface used. In the case of the energy required to obtain a faulty execution, the laterals required always more energy than the backside. Also, the faulty rate was lower in the laterals than in backside. Additionally, for the LLFI, it was observed that it could be a relationship between the distance from the surface of attack to the vulnerable region and the success rate. However, this could also depend on the light sensitivity of the circuitry over the light path to the vulnerable region. This could explain why it was not possible to get faults from an specific lateral. In fact, this also suggests that some kind of (sensitive) protection ring could be a valid countermeasure against this type of attacks.

The evaluation of the LLFI is not considered complete and various work directions were identified. For instance, a better understanding how the laser light spreads through the substrate until reach the vulnerable region and what dependency exists on the circuitry sensitivity path. Nevertheless,

it can be already concluded that LLFI is a new efficient way to carry out a fault injection attack through the side of the chip. Therefore, it is a potential threat for ICs and this need to be taken into account.

REFERENCES

[1] Soha Alhelaly, Jennifer Dworak, Theodore Manikas, Ping Gui, Kundan Nepal, and Alfred L Crouch. Detecting a trojan die in 3d stacked integrated circuits. In *2017 IEEE North Atlantic Test Workshop (NATW)*, pages 1–6. IEEE, 2017.

[2] E Amini, A Beyreuther, N Herfurth, A Steigert, R Muydinov, B Szyszka, and C Boit. Ic security and quality improvement by protection of chip backside against hardware attacks. *Microelectronics Reliability*, 88:22–25, 2018.

[3] Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, and Claire Whelan. The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE*, 94(2):370–382, 2006.

[4] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, 2012.

[5] Stephan Borel, L Duperrex, E Deschaseaux, J Charbonnier, J Cledière, R Wacquez, J Fournier, J-C Souriau, G Simon, and A Merle. A novel structure for backside protection against physical attacks on secure chips or sip. In *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)*, pages 515–520. IEEE, 2018.

[6] Matthew S Brown and Craig B Arnold. Fundamentals of laser-material interaction and application to multiscale surface modification. In *Laser precision microfabrication*, pages 91–120. Springer, 2010.

[7] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, Philippe Orsatelli, Philippe Maurine, and Assia Tria. Injection of transient faults using electromagnetic pulses-practical results on a cryptographic system-. *IACR Cryptology EPrint Archive*, 2012:123, 2012.

[8] Jaya Dofe, Qiaoyan Yu, Hailang Wang, and Emre Salman. Hardware security threats and potential countermeasures in emerging 3d ics. In *Proceedings of the 26th edition on Great Lakes Symposium on VLSI*, pages 69–74. ACM, 2016.

[9] Peng Gu, Shuangchen Li, Dylan Stow, Russell Barnes, Liu Liu, Yuan Xie, and Eren Kursun. Leveraging 3d technologies for hardware security: Opportunities and challenges. In *2016 International Great Lakes Symposium on VLSI (GLSVLSI)*, pages 347–352. IEEE, 2016.

[10] Philippe Loubet Moundi. Cost effective techniques for chip delayering and in-situ depackaging, 2013.

[11] Salvador Manich Bou, Daniel Arumi Delgado, Rosa Rodríguez Montañés, Jordi Mujal Colell, and David Hernández García. Backside polishing detector: a new protection against backside attacks. In *DCIS'15-XXX Conference on Design of Circuits and Integrated Systems*, 2015.

[12] Philippe Maurine, Karim Tobich, Thomas Ordas, and Pierre Yvan Liardet. Yet another fault injection technique: by forward body biasing injection. In *YACC'2012: Yet Another Conference on Cryptography*, 2012.

[13] J-J Quisquater. Eddy current for magnetic analysis with active sensor. *Proceedings of Esmart, 2002*, pages 185–194, 2002.

[14] Sergei P Skorobogatov and Ross J Anderson. Optical fault induction attacks. In *International workshop on cryptographic hardware and embedded systems*, pages 2–12. Springer, 2002.

[15] Jasper GJ Van Woudenberg, Marc F Witteman, and Federico Menarini. Practical optical fault injection on secure microcontrollers. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 91–99. IEEE, 2011.

[16] Christian Wittke, Zoya Dyka, Oliver Skibitzki, and Peter Langendoerfer. Preparation of sca attacks: Successfully decapsulating bga packages. In *International Conference for Information Technology and Communications*, pages 240–247. Springer, 2016.

[17] Horst Zimmermann. Basics of optical emission and absorption. In *Integrated silicon optoelectronics*, pages 1–10. Springer, 2000.