The case of using CMOS FD-SOI rather than CMOS bulk to harden ICs against laser attacks

Jean-Max Dutertre, Vincent Beroulle, Philippe Candelier, Louis-Barthelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hely, Régis Leveugle, Paolo Maistri, Giorgio Di Natale, et al.

▶ To cite this version:

Jean-Max Dutertre, Vincent Beroulle, Philippe Candelier, Louis-Barthelemy Faber, Marie-Lise Flottes, et al.. The case of using CMOS FD-SOI rather than CMOS bulk to harden ICs against laser attacks. IOLTS: International On-Line Testing Symposium, Jul 2018, Platja d'Aro, Spain. pp.214-219, 10.1109/IOLTS.2018.8474230 . emse-01856000

HAL Id: emse-01856000
https://hal-emse.ccsd.cnrs.fr/emse-01856000v1

Submitted on 18 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

https://dx.doi.org/10.1109/IOLTS.2018.8474230
IOLTS: International On-Line Testing Symposium

The case of using CMOS FD-SOI rather than CMOS bulk to harden ICs against laser attacks

Jean-Max Dutertre*, Vincent Beroulle¶, Philippe Candelier‡, Louis-Barthelemy Faber‡,
Marie-Lise Flottes§, Philippe Gendrier‡, David Hély¶, Regis Leveugle†,
Paolo Maistri†, Giorgio Di Natale§, Athanasios Papadimitriou¶, and Bruno Rouzeyre§,
* Mines Saint-Etienne, CEA-Tech, Centre CMP, F - 13541 Gardanne France, name@emse.fr
†Univ. Grenoble Alpes, CNRS, Grenoble INP, TIMA, 38000 Grenoble, France, surname.name@univ-grenoble-alpes.fr
‡STMicroelectronics, 850 rue Jean Monnet, 38926 Crolles, firstname.name@st.com
§LIRMM, University of Montpellier, CNRS, 161, rue Ada, 34095, Montpellier, France, name@lirmm.fr
¶Univ. Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France, surname.name@esisar.grenoble-inp.fr

***Abstract*—At first used to emulate the effects of radioactive ionizing particules passing through integrated circuits (ICs), laser illumination is also used to inject faults into the computations of secure ICs for the purpose of retrieving secret data. The CMOS FD-SOI technology is expected to be less sensitive to laser faults injection than the more usual CMOS bulk technology. We report in this work an experimental assessment of the interest of using FD-SOI rather than CMOS bulk to decrease laser sensitivity. Our experiments were conducted on test chips at the 28 nm node for both technologies with laser pulse durations in the picosecond and nanosecond ranges.**

***Index Terms*—Laser fault injection, FD-SOI, CMOS bulk.**

I. Introduction

Laser injection was first introduced and studied by the radiation effects community as a tool to emulate Single Event Effects (SEE) induced by ionizing particules into CMOS ICs [1], [2]. More recently, the use of a laser beam to inject faults into the computations of an IC was first reported by S. Skorobogatov and R. Anderson in 2002 [3]. Since then, laser is considered as a very efficient tool to carry out fault attacks (FAs) for the purpose of retrieving secret data concealed into secure ICs. It permitted an accurate injection of faults both in space and time [4]. Besides, despite the scaling down of IC's technologies, it makes it possible to inject faults with high accuracy (at byte or even at bit level [5]), which is mandatory to apply most of the known FA schemes [4].

The radiation effect community was also the first to study and develop countermeasures against SEEs. Several principles were introduced to mitigate radiation-induced errors: Error Detection And Correction techniques (or EDAC, eg based on spatial or temporal redundancy), sensors monitoring the currents at the root cause of SEEs [6], cells hardening through architecture redesign [7], or even the use of Silicon On Insulator (SOI) technology as an alternative to the usual CMOS bulk. Because the mechanism of laser fault injection is similar to that of radiation-induced SEEs, these countermeasures may be used to thwart laser attacks against secure ICs. However, EDAC, sensors, and cells redesign are often associated to performance degradation both in execution time and power consumption and also with an increase in silicon area. For its part, SOI has evolved into a mature technology, Ultra-Thin Body and Box Fully-Depleted SOI (UTBB FD-SOI), available at several chip makers (STMicroelectronics, Samsung, GlobalFoundries). FD-SOI technology makes it possible to reduce the power consumption of systems on chips devices (especially their static current leakage) and offers a body biasing capability for low voltage operations. Hence, this technology is available for radiation or cost sensitive security applications without the once extra costs of using the first SOI technologies.

There are many papers highlighting, often on experimental basis, the advantages of SOI or FD-SOI over CMOS bulk regarding sensitivity to SEEs [8]–[14]. These experimental results were mostly obtained on elementary test elements (either transistors or logic gates), and partly conducted with laser emulation. SEE laser emulation is done with settings chosen to mimic the passing of a ionizing particle through silicon [2]: a wavelength in the near Infrared (IR), a laser pulse duration in the picosecond range (from several ps to a few tens of ps), and a laser beam diameter set to 1 μm (the minimal size achievable with an air gap lens). Regarding the interest of using FD-SOI rather than CMOS bulk to mitigate laser fault injection, there are very few published papers [15], [16]. Moreover, their experimental results were as well obtained on elementary test elements. There was still no reported experimental evidence of the interest of choosing FD-SOI to design ICs hardened against laser attacks.

In this paper we report the research work we did to ascertain, on experimental basis, the interest in using FD-SOI to decrease IC's sensitivity to laser attacks. We compared two almost identical chips designed at the 28 nm technology node both in FD-SOI and CMOS bulk. They both implement the same design of a custom IP block implementing the Advanced Encryption Standard (AES) algorithm. The laser illumination tests we performed used settings suitable for radiation testing (near IR, picosecond range, 1 μm beam diameter) and extended settings suitable for laser attacks (nanosecond range and wider beam diameter). Our intent was to verify whether the hardening properties of FD-SOI was still valid for a complex IP block and for the settings of laser used for fault injection.

This article is organized as follows. Section II describes

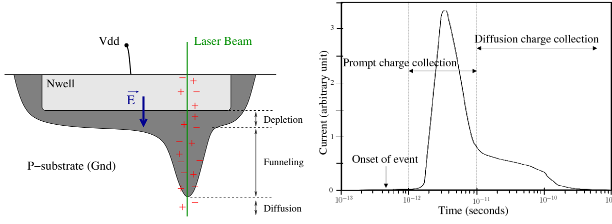

Fig. 1. Photoelectric effect of a laser beam through a PN-junction (left) - Transient current resulting from charge collection after a laser shot [17] (right).

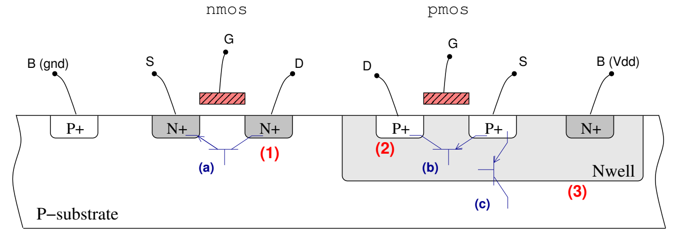

Fig. 2. Cross sectional view of CMOS bulk technology.

the theory of laser injection and the structural differences between CMOS bulk and FD-SOI that explain the lower laser sensitivity of the latter. An experimental state-of-the-art of both technologies' sensitivity to laser-induced faults is made in section III. Then, section IV describes the test chips and the laser injection bench we used. It also reports the laser fault injection thresholds we obtained for various experimental settings. Finally, our findings are discussed and summarized in section V with some perspectives.

II. Theory of Laser Fault Injection

A. Photoelectric effect

Laser may be used to emulate SEEs or to inject faults into ICs because of the photoelectric effect resulting from its interaction with silicon. A laser beam passing through silicon creates electron-hole pairs along his path, the so-called photoelectric effect, provided that its wavelength corresponds to an energy level higher than the silicon bandgap. These charge carriers may recombine without any noticeable effect on the target's activity. An exception exists when the laser beam passes through a transistor's reverse biased PN junction (drain/bulk, source/bulk or Nwell/Psubstrate): a place where there exists a strong electric field (as depicted in the left part of Fig. 1). As a consequence, the charge carriers drift in opposite directions and a current pulse is induced. This photocurrent pulse vanishes as the charges are exhausted. It may last a few hundreds of picoseconds after the laser pulse ceased [2] and may have an amplitude as large as a few mA. In turn, this current pulse creates a transient voltage pulse, which may induce a fault if induced (1) directly in a memory cell (a Single Event Upset, SEU) or (2) in a logic gate and then travelling to and stored into a downstream Flip-Flop (a Single Event Transient, SET).

This charge carriers collection phenomenon can be decomposed in two successive parts described in [17]. At first, the depletion region (hence the electric field) is stretched along the laser beam, the charges nearby are collected in a few picoseconds generating a peak current: a phenomenon called funneling. In a second time, the remaining charges are collected in a longer phenomenon, called diffusion. The current decreases slowly until all charges are collected. The outline of the corresponding photocurrent is displayed on the right part of Fig. 1. The magnitude of this laser-induced photocurrent depends of several parameters: it is proportional to the PN junction area and it increases linearly with the junction reverse voltage [18]. It also rely on the size of the funnel region.

B. CMOS bulk sensitivity to laser fault injection

We recalled in the previous subsection II-A that laser fault sensitivity arises from the laser illumination of reverse biased PN junctions. Fig. 2 highlights where such sensitive places are found for the usual CMOS bulk technology. It displays the cross sectional view of a NMOS and a PMOS transistors.

There are three types of PN junctions that may undergo the outbreak of a photocurrent (respectively labeled 1, 2, and 3 in Fig. 2):

1) the Psub-N^+ junction between a NMOS diffusion and the circuit's bulk (i.e. the P-type substrate),
2) the P^+-Nwell junction between a PMOS diffusion and its Nwell,
3) the Psub-Nwell junction between a PMOS Nwell and the circuit's bulk.

It is testimony to the high sensitivity of CMOS devices to laser injection. CMOS technology also encompasses three bipolar parasitic structures (depicted in blue in Fig. 2 and labeled a,b, and c respectively). They may be triggered by a laser shot as the local potential of their base may increase sufficiently (as a result of a photocurrent) to bias their emitter-base junction in direct mode. By doing so, they may be part of the fault injection process.

C. FD-SOI sensitivity to laser fault injection

The structure of the $28\,nm$ UTTB FD-SOI technology considered in this paper is expected to bring reduced sensitivity to laser attacks. However, it does not provides a full immunity as reported hereafter.

1) FD-SOI structure: FD-SOI technology was pushed forward by ST Microelectronics. It is supposed to replace CMOS bulk for advanced technology nodes with reduced static consumption leakage. It is mainly dedicated to low power applications. It provides, thanks to well biasing techniques, the ability to dynamically optimize the circuit's speed versus its power consumption [19]–[21]. FD-SOI is also expected to bring reduced sensitivity to laser attacks due to the thin oxide box that isolates the transistors from their wells [11], [22]. Indeed, the laser induced charge generation volume of FD-SOI transistors is smaller than that of CMOS bulk transistors: in Fig. 2 the funnel charge collection region has a lot of room to

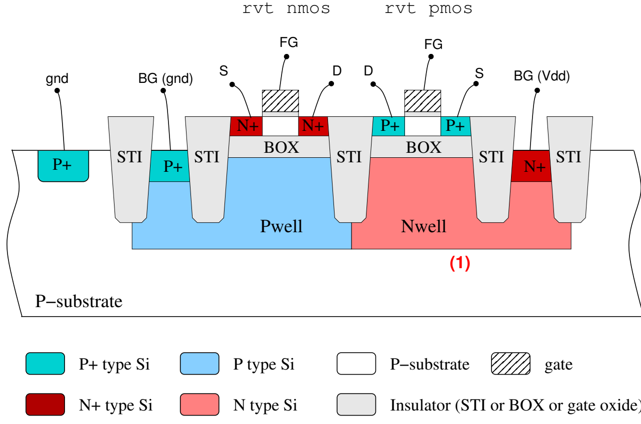

Fig. 3. Cross sectional view of FD-SOI technology: regular V_t transistors.

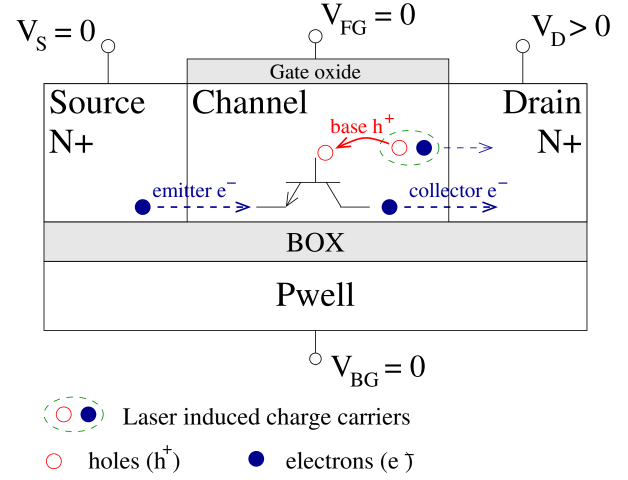

Fig. 4. Parasitic bipolar transistor activation in a FD-SOI NMOS transistor due to laser illumination [23].

expand under PN junctions, while it no longer exists in FD-SOI (its charge collection region is reduced to the transistor channel itself). As a result, any laser-induced photocurrent should be reduced both in time and magnitude. Fig. 3 depicts the cross sectional view of the 28 nm FD-SOI technology of our test chip (we used regular V_t transistors denoted rvt).

Consider the rvt NMOS: it is built on an isolation thin box (less than 30 nm thick) that isolates it from its Pwell. The transistor's channel is an intrinsic silicon, its thickness is less than 10 nm. The rvt PMOS is built with complementary doped silicons. The main distinctive feature of FD-SOI w.r.t. CMOS bulk regarding laser sensitivity is that it has no reverse biased PN junctions between the transistors' diffusions and their wells. The most laser sensitive part of rvt transistors should be the Psub-Nwell junction that exists between the Nwell of a PMOS and the P-substrate (marked (1) in Fig. 3).

At first sight, the parasitic bipolar transistors found in CMOS technologies are no longer present. Hence, there is no parasitic thyristor structure that may create a destructive SEL (Single Event Latchup) in FD-SOI circuits when triggered.

2) FD-SOI laser-induced fault injection mechanism: Setting aside the Psubstrate/Nwell junction marked (1) in Fig. 3 that is not directly connected to the logic gates' electrical nodes, the laser sensitive parts of FD-SOI circuits are the channels of their transistors. [11] estimates that FD-SOI structure, when compared to CMOS bulk structure, brings two main contributions for a lower laser sensitivity: (1) by of a factor of at least 10 due to the isolation box under each transistor (in fact a buried oxide) that has the effect to truncate the charge collection volume and (2) by a factor of at least 2 due to a smaller sensitive area (that of a channel w.r.t. that of a diffusion-well PN junstion). This decrease of the charge collection region has two additional effects that may further decrease the laser sensitivity of FD-SOI : (1) the laser-induced current pulses shall have no tail (the diffusion part in the pulse of Fig. 1) and hence their effect shall last less time; and (2) the effect area of a laser beam shall be reduced because only a direct hit on a transistor's channel shall be able to induce a photocurrent. In turn, this latter effect shall reduce the effect of charge sharing between several PN junctions at advanced technology nodes, making fault injection less likely.

Despite all these mitigation effects, experimental results reveal that faults are still induced into FD-SOI ICs by laser illumination (as reported in section III) with a sensitivity level higher than expected. It is due to the activation of the intrinsic parasitic bipolar transistor associated with every transistor. Its activation under laser illumination has an amplification effect on the charge carriers induced by photoelectric effect in the channel [23]. Fig. 4 illustrates its structure and its activation mechanism in the case of a NMOS transistor. The laser-induced holes are collected by the parasitic bipolar base, while the electrons are collected by the NMOS drain. The corresponding current increases the channel potential (note that the channel is floating) to the point of bipolar activation, hence inducing a drain to source electrons current. It results an amplification effect of the laser-induced current into a greater bipolar current. This mechanism is significantly different from the mechanism related to CMOS transistors. However, this laser-induced current may be large enough to discharge an electrical node inside a logic gate and to lead to a fault injection.

III. Experimental State-of-the-Art

A. Radiation focused experimental State-of-the-Art

Several works from the radiation effect community assess the lower laser-sensitivity of FD-SOI on experimental basis. They were mainly carried out on elementary blocks (transistors or single logic gates) by means of pulsed-laser or particules irradiation. They are reported in the following.

In 2004, [8] performed a neutron-induced SEU evaluation of on-the-shelf SRAM chips designed in CMOS bulk (0.18 μm and 0.25 μm processes) and in SOI (0.2 μm) technologies. The SOI SRAM was found ten times less sensitive than its CMOS bulk counterparts.

In 2007, the authors of [10] carried out heavy ion and laser testing of a single FD-SOI test transistor (embedded in a 50 nm process test chip). They recorded the laser-induced pulse currents they obtained (laser settings: 1 ps duration, 590 nm wavelength, 1.1 μm laser spot diameter). They obtained short current pulses with a duration of ∼50 ps and a current peak as large as 1 mA. The shape of the measured pulse currents confirmed the hypothesis of the absence of a tail component (as stated in subsection II-C). These results also attest that laser-induced pulse currents in FD-SOI may still induce SEEs.

[12] reports the pulsed laser (590 nm, 1 ps, 1.1 μm) testing of single test Fin-FET transistors designed in SOI and CMOS bulk (for gate lengths of 125 nm and 130 nm respectively). At 22.4 pJ laser energy they recorded, respectively for CMOS and SOI, current pulses with: (1) a 310 ps duration and a peak amplitude of ∼1 mA and (2) a 80 ps duration and a peak amplitude of ∼100 μA. These differences in current pulses characteristics reveals a lesser laser-sensitivity of SOI technologies.

Very recently, [24] designed test elements embedded in a 28 nm UTBB FD-SOI test chip for the purpose of measuring the widths of SETs induced either by heavy ions or laser illumination (1290 nm[1], 1.5 μm). The authors measured pulses widths in the 300-400 ps range for different laser energies. They also report a difference of two orders of magnitude in sensitivity to heavy ions when comparing their FD-SOI test chip to a CMOS bulk counterpart. [14] reports similar results from experiments carried out on D flip-flops from a 28 nm UTBB FD-SOI test chip.

These various experiments assess the lower sensitivity of FD-SOI to laser illumination. However, they were carried out on elementary test blocks and with laser parameters related to the radiation domain (ps range duration and beam diameter close to 1 μm).

B. Security focused experimental State-of-the-Art

Very few works report comparisons of the laser sensitivity of FD-SOI w.r.t. that of CMOS bulk from a security perspective. The authors of [15], [16], [25] performed such experiments at the 28 nm technological node on elementary test transistors. Their main purpose was to build electrical models of the laser illumination of FD-SOI transistors. Their experiments were carried out with laser settings commonly used for laser attacks (complementary to that reported in III-A): pulse durations in the ns and μs ranges, laser spot diameter as large as 5 μm. The obtained results were a confirmation of the lower sensitivity of FD-SOI:

- a laser-induced peak current an order of magnitude lower for FD-SOI than for CMOS bulk,
- a lesser extension of the laser sensitive areas of FD-SOI transistors w.r.t. to CMOS transistors. For FD-SOI, the sizes of laser sensitive areas were approximately equal to the laser spot diameters. For CMOS bulk, the laser sensitive areas sometimes extended several tens of μm beyond transistors.

[1] at this wavelength, charge carriers are induced by a two-photons absorption (TPA) phenomenon [2].

C. Conclusion on the experimental State-of-the-Art

The research papers cited in this section provide strong evidences of the lower laser sensitivity of the FD-SOI technology w.r.t. CMOS bulk. However, they were obtained for elementary test elements and few results are based on laser settings other than those used to emulate SEEs. The question was still open for more complicated circuits (i.e. featuring several kgates).

IV. Laser sensitivity assessment of FD-SOI and CMOS bulk test chips

A. Experimental setup

1) Target description: We designed two functionally identical test chips resp. in UTBB FD-SOI and CMOS bulk at the same 28 nm technology node. Our intend was to ascertain and measure experimentally the advantage of FD-SOI over CMOS bulk in terms of laser sensitivity. Each chip embeds two identical AES implementations (at RTL level), which feature fault detection techniques based respectively on parity codes and on redundancy (the AES DDR of [26]). Fig. 5 displays views of the test chips AES functional blocks shown in their cavity, FD-SOI appears paler. Both chips were thinned to the same thickness of ∼100 μm on order to lessen the absorption of the laser beam energy when accessing the targets sensitive areas through their backside. The core power supply voltage was set to 1.2 V and the clock frequency to 100 MHz.

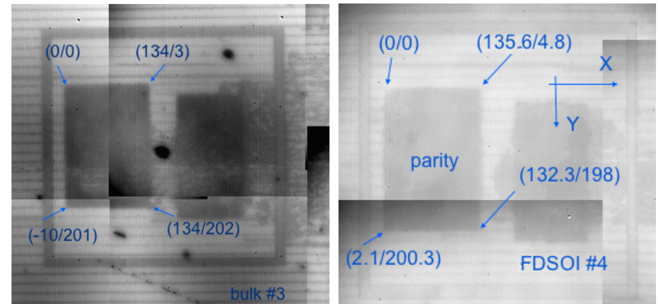

Fig. 5. Microphotographies of the AES test elements of the CMOS bulk (left) and the FD-SOI (right) 28 nm test chips. Views taken from ICs rear sides.

2) Laser bench description: We used two different pulsed-laser sources during our experiments to cover large laser settings:

- a picosecond range laser source at 1,030 nm wavelength with a constant pulse duration of 30 ps and a maximal energy of 100 nJ suitable for radiation emulation,
- a nanosecond range laser source at 1064 nm with a pulse duration tunable from 5 ns to 1 s and a maximal power of 3 W for pulses above 50 ns, but limited to 1 W below.

Note that laser intensity is expressed in terms of energy for our picosecond range laser source and of power for our nanosecond range laser source due to their design (which is usual practice). Our experiments were carried out through the chips backside at two different laser spot diameters, 1 μm

TABLE I
FD-SOI V. CMOS BULK: COMPARISON OF LASER FAULT INJECTION THRESHOLDS.

Technologies ⟶	CMOS bulk		FD-SOI	
Laser pulse duration and beam diameter	laser threshold	density	laser threshold	density
30 ps / 1 μm	0.2 nJ	16.9 pJ/μm^2	0.6 nJ	50.6 pJ/μm^2
30 ps / 5 μm	0.3 nJ	2.2 pJ/μm^2	2.1 nJ	15.4 pJ/μm^2
10 ns / 1 μm	0.45 W	38 mW/μm^2	0.8 W	67.5 mW/μm^2
10 ns / 5 μm	0.6 W	4.4 mW/μm^2	-	-
50 ns / 5 μm	0.3 W	2.2 mW/μm^2	2.2 W	16 mW/μm^2

and 5 μm, thanks to a 100x and a 20x optics with 26 % and 57 % power transmission coefficients respectively. During laser testing, the test chips were mounted on a XY mechanical stage that makes it possible to roam their surface with a displacement step as small as 0.1 μm.

3) Experiments description: The carried out experiments aimed at measuring the laser fault injection threshold of our test chips (refereed as laser sensitivity hereafter). We expressed it as the laser energy (or power) threshold corresponding to the injection of faults: below that threshold no fault is induced, beyond it faults start to appear (at a growing rate as the laser energy is further increased). Threshold measurements were done from numerous faults injection attempts during the course of the AES calculations of our targets at different and growing laser energies and for various locations of the laser shots over the AES blocks. An accurate evaluation of such thresholds require a significant number of injection attempts, each value reported in this paper was obtained from more than 2,000 tries. These tests were performed at room temperature (climate control set to 21°C).

B. Radiation-centric experimental results

The first comparison was drawn with radiation-centric laser settings: 30 ps duration and 1 μm spot diameter. It aimed at assessing the results from the state-of-art for elementary test elements (see III-A). We measured a 0.2 nJ laser sensitivity for the FD-SOI test chip and a 0.6 nJ laser sensitivity for the CMOS bulk device. Hence, the use of FD-SOI brought a factor three decrease of laser sensitivity, which appears disappointing compared to the one or two order of magnitudes reported in the state-of-the-art.

The next experiments were performed with the same 30 ps laser duration but a spot size of 5 μm. The FD-SOI laser sensitivity slightly increased to 0.3 nJ while that of CMOS bulk was upped to 2.1 nJ. With this settings the laser sensitivity of CMOS bulk was seven times that of the FD-SOI: a result in line with the one order of magnitude reported in the state-of-the-art.

C. Attack-centric experimental results

The laser settings used for fault injection often use longer pulse durations. At 10 ns duration and 5 μm spot diameter the laser sensitivity of the CMOS bulk test chip was measured at 0.6 W. Interestingly, because a 10 ns laser pulse duration restricts the power setting to 1 W, the FD-SOI device was found immune to laser fault injection.

With a 1 μm laser spot diameter and a 10 ns pulse duration, the laser sensitivity of CMOS bulk was decreased to 0.45 W. Faults were also injected into the FD-SOI target, the measured laser sensitivity was 0.8 W: a sensitivity ratio close to 2 w.r.t. CMOS bulk.

The last experiment series were carried out with a 50 ns pulse duration and a 5 μm spot diameter. Laser sensitivities of 0.3 W and 2.2 W were measured respectively for the CMOS bulk and FD-SOI test chips.

D. Analysis

Table I gathers all the obtained experimental results for the sake of readability. It also includes an expression of the laser sensitivity as the density of the power or energy thresholds. It is calculated from the laser sensitivity and the area of the laser spot at focus, it takes into account the lenses transmission coefficients. It emerges an advantage of using FD-SOI rather than CMOS bulk to decrease a device laser sensitivity: for 1 μm laser spot diameter the comparative factor is 2-3, it is increased to a factor of 7 at 5 μm spot diameter.

We observed mostly single-byte and single-bit faults when their injection timing corresponded to the last two rounds of the AES at a laser energy and power near the sensitivity threshold. We did not observed a noticeable difference in their occurrence rates between the two test chips.

V. Discussion and Conclusion

Although assessing the interest of choosing FD-SOI rather than CMOS bulk for the purpose of lowering laser sensitivity, the extent of the gain, between 2 and 7 depending on the laser settings, is lower than expected. The previous state-of-the-art reported in section III-A for elementary test patterns was indeed promising an improvement between 1 and 2 orders of magnitude. An explanation of this result may be linked to the laser-sensitive Nwell-Psubstrate junction found in FD-SOI (marked (1) in Fig. 3). It is always reserve biased (at $V_{dd,core}$) and has a large area (two factors in favor of a large laser-induced transient current). When exposed to laser illumination it will undergo a pulse photocurrent between Vdd and Gnd, inducing an IR drop phenomenon that may encourage the injection of faults as reported in [27].

However, considering that hardening an IC against laser attacks is generally done by using several different types of countermeasures (often referred as multilayered security), we shall recommend choosing FD-SOI over CMOS bulk at

advanced technology nodes. Indeed, any increase in the laser-induced fault injection threshold will force an attacker to use a higher laser energy. This may force the attacker to operate closer to the target's destructive threshold, thereby making his experiments harder to conduct. This would also increase the ability of laser sensors to detect the attack. The efficiency of Bulk Built-In Current Sensors [28] designed to detect laser attacks by monitoring the induced currents shall be significantly increased by the use of FD-SOI. As, the Nwell-Psub junction of FD-SOI (marked (1) in Fig. 3) has a sensitivity area and level similar to that found in CMOS bulk, while the intrinsic gain of using FD-SOI forces the use of higher laser power. It is a perpective worth to explore.

Acknowledgment

This work was supported by a research grant from the French Agence Nationale de la Recherche (LIESSE project, ANR-12-INS-0008-01).

References

[1] D. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *Nuclear Science, IEEE Transactions on*, vol. 12, pp. 91–100, Oct 1965.

[2] S. Buchner, F. Miller, V. Pouget, and D. McMorrow, "Pulsed-laser testing for single-event effects investigations," *Nuclear Science, IEEE Transactions on*, vol. 60, pp. 1852–1875, June 2013.

[3] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, pp. 2–12, Springer-Verlag, 2002.

[4] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, pp. 3056 – 3076, 2012.

[5] M. Agoyan, J.-M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta, and A. Tria, "How to flip a bit?," in *16th IEEE International On-Line Testing Symposium (IOLTS 2010), 5-7 July, 2010, Corfu, Greece*, pp. 235–239, 2010.

[6] B. Gill, M. Nicolaidis, F. Wolff, C. Papachristou, and S. Garverick, "An efficient bics design for seus detection and correction in semiconductor memories," in *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2005*, pp. 1530–1591, 2005.

[7] T. Calin, M. Nicolaidis, and R. Velazco, "Upset hardened memory design for submicron CMOS technology," *IEEE Transactions on Nuclear Science*, vol. Dec. 1996; 43(6) pt. 1, pp. 2874–8, 1996.

[8] J. Baggio, D. Lambert, V. Ferlet-Cavrois, C. D'Hose, K. Hirose, H. Saito, J. Palau, F. Saigne, B. Sagnes, N. Buard, and T. Carriere, "Neutron-induced seu in bulk and soi srams in terrestrial environment," in *IEEE International Reliability Physics Symposium Proceedings*, pp. 677–678, 2004.

[9] V. Ferlet-Cavrois, P. Paillet, D. McMorrow, A. Torres, M. Gaillardin, J. S. Melinger, A. R. Knudson, A. Campbell, J. Schwank, G. Vizkelethy, M. Shaneyfelt, K. Hirose, O. Faynot, C. Jahan, and L. Tosti, "Direct measurement of transient pulses induced by laser and heavy ion irradiation in deca-nanometer devices," *Nuclear Science, IEEE Transactions on*, vol. 52, pp. 2104–2113, Dec 2005.

[10] M. Gaillardin, P. Paillet, V. Ferlet-Cavrois, J. Baggio, D. Mcmorrow, O. Faynot, C. Jahan, L. Tosti, and S. Cristoloveanu, "Transient radiation response of single- and multiple-gate FDSOI transistors to pulsed laser and heavy ion irradiation," *IEEE Transactions on Nuclear Science*, vol. 54, pp. 2355–2362, Dec. 2007.

[11] M. Alles, R. Schrimpf, R. Reed, L. Massengill, R. Weller, M. Mendenhall, D. Ball, K. Warren, T. Loveless, J. Kauppila, and B. Sierawski, "Radiation hardness of fdsoi and finfet technologies," in *SOI Conference, 2011 IEEE International*, pp. 1–2, Oct 2011.

[12] F. El-Mamouni, E. X. Zhang, R. D. Schrimpf, R. A. Reed, K. F. Galloway, D. McMorrow, E. Simoen, C. Claeys, S. Cristoloveanu, and W. Xiong, "Pulsed laser-induced transient currents in bulk and silicon-on-insulator finfets," in *Reliability Physics Symposium (IRPS), 2011 IEEE International*, 2011.

[13] P. Roche, J.-L. Autran, G. Gasiot, and D. Munteanu, "Technology downscaling worsening radiation effects in bulk: Soi to the rescue," in *Technical Digest - International Electron Devices Meeting, IEDM*, pp. 31.1.1–31.1.4, 2013.

[14] H.-B. Wang, J. S. Kauppila, K. Lilja, M. Bounasser, L. Chen, M. Newton, Y.-Q. Li, R. Liu, B. L. Bhuva, S.-J. Wen, R. Wong, R. Fung, S. Baeg, and L. W. Massengill, "Evaluation of SEU Performance of 28-nm FDSOI Flip-Flop Designs," *IEEE Transactions on Nuclear Science*, vol. 64, pp. 367–373, Jan. 2017.

[15] V. Beroulle, P. Candelier, S. De Castro, G. Di Natale, J.-M. Dutertre, M.-L. Flottes, D. Hély, G. Hubert, R. Leveugle, F. Lu, P. Maistri, A. Papadimitriou, B. Rouzeyre, C. Tavernier, and P. Vanhauwaert, "Laser-induced fault effects in security-dedicated circuits," in *VLSI-SoC: Internet of Things Foundations*, vol. 464 of *IFIP Advances in Information and Communication Technology*, pp. 220–240, Springer International Publishing, 2015.

[16] J.-M. Dutertre, S. De Castro, A. Sarafianos, N. Boher, B. Rouzeyre, M. Lisart, J. Damiens, P. Candelier, M.-L. Flottes, and G. Di Natale, "Laser attacks on integrated circuits: From cmos to fd-soi," in *Design Technology of Integrated Systems In Nanoscale Era (DTIS), 2014 9th IEEE International Conference On*, pp. 1–6, May 2014.

[17] F. Wang and V. Agrawal, "Single event upset: An embedded tutorial," in *VLSI Design, 2008. VLSID 2008. 21st International Conference on*, pp. 429–434, Jan 2008.

[18] M. Lacruche, N. Borrel, C. Champeix, C. Roscian, A. Sarafianos, J.-B. Rigaud, J.-M. Dutertre, and E. Kussener, "Laser fault injection into sram cells: Picosecond versus nanosecond pulses," in *On-Line Testing Symposium (IOLTS), 2015 IEEE 21st International*, pp. 13–18, July 2015.

[19] C. Fenouillet-Beranger *et al.*, "Hybrid fdsoi/bulk high-k/metal gate platform for low power (lp) multimedia technology," in *Electron Devices Meeting (IEDM), 2009 IEEE International*, pp. 1–4, Dec 2009.

[20] C. Fenouillet-Beranger *et al.*, "Impact of local back biasing on performance in hybrid fdsoi/bulk high-k/metal gate low power (lp) technology," in *Ultimate Integration on Silicon (ULIS), 2012 13th International Conference on*, pp. 165–168, March 2012.

[21] D. Golanski *et al.*, "First demonstration of a full 28nm high-k/metal gate circuit transfer from bulk to utbb fdsoi technology through hybrid integration," in *VLSI Technology (VLSIT), 2013 Symposium on*, pp. T124–T125, June 2013.

[22] V. Ferlet-Cavrois *et al.*, "Direct measurement of transient pulses induced by laser and heavy ion irradiation in deca-nanometer devices," *Nuclear Science, IEEE Transactions on*, vol. 52, pp. 2104–2113, Dec 2005.

[23] F. Liu, I. Ionica, M. Bawedin, and S. Cristoloveanu, "Extraction of the parasitic bipolar gain using the back-gate in ultrathin fd soi mosfets," *IEEE Electron Device Letters*, vol. 36, no. 2, pp. 96–98, 2015.

[24] R. Liu, A. Evans, L. Chen, Y. Li, M. Glorieux, R. Wong, S.-J. Wen, J. Cunha, L. Summerer, and V. Ferlet-Cavrois, "Single Event Transient and TID Study in 28 nm UTBB FDSOI Technology," *IEEE Transactions on Nuclear Science*, vol. 64, pp. 113–118, Jan. 2017.

[25] S. De Castro, G. Di Natale, M.-L. Flottes, B. Rouzeyre, and J.-M. Dutertre, "Figure of merits of 28nm si technologies for implementing laser attack resistant security dedicated circuits," in *VLSI (ISVLSI), 2015 IEEE Computer Society Annual Symposium on*, pp. 362–367, July 2015.

[26] P. Maistri and R. Leveugle, "Double-data-rate computation as a countermeasure against fault analysis," *IEEE Transactions on Computers*, vol. 57, no. 11, pp. 1528–1539, 2008.

[27] R. Viera, P. Maurine, J.-M. Dutertre, and R. Possamai Bastos, "Role of laser-induced ir drops in the occurrence of faults: Assessment and simulation," in *Digital System Design (DSD), 2017 Euromicro Conference on*, IEEE, 2017.

[28] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Experimental validation of a bulk built-in current sensor for detecting laser-induced currents," in *On-Line Testing Symposium (IOLTS), 2015 IEEE 21st International*, pp. 150–155, July 2015.