Sensitivity to Laser Fault Injection: CMOS FD-SOI vs. CMOS bulk

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

Authors' version
IEEE Transactions on Device and Materials Reliability, 2018
https://dx.doi.org/10.1109/TDMR.2018.2886463

Sensitivity to Laser Fault Injection: CMOS FD-SOI vs. CMOS bulk

Jean-Max Dutertre, Vincent Beroulle, Philippe Candelier, Stephan De Castro, Louis-Barthelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hély, Régis Leveugle, *Senior member, IEEE,* Paolo Maistri, Giorgio Di Natale, *Senior member, IEEE,* Athanasios Papadimitriou, and Bruno Rouzeyre.

***Abstract*—Integrated circuits (ICs) laser illumination was originally used for emulation of radioactive ionizing particules effects on that devices. Today, it is also a mean for injecting 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 fault 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. We also discuss the interest of using bulk current sensors along with FD-SOI technology to achieve optimal detection of laser fault injection attempts.**

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

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 particles 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 now 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 is still no reported experimental evidence of the interest of choosing FD-SOI for the purpose of designing 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 [17]. We compared two almost identical chips designed at the 28 nm node in CMOS FD-SOI and bulk technologies. They both implement the same design of a custom IP block implementing the Advanced Encryption Standard (AES) algorithm. The laser illumination tests we performed first use settings suitable for radiation testing (near IR, picosecond range, 1 µm beam diameter)

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

J.-M. Dutertre is with IMT, Mines Saint-Etienne, Centre CMP, Equipe Commune CEA Tech, F-13541 Gardanne France, name@emse.fr.

R. Leveugle and P. Maistri are with Univ. Grenoble Alpes, CNRS, Grenoble INP (Institute of Engineering Univ. Grenoble Alpes), TIMA, 38000 Grenoble, France, surname.name@univ-grenoble-alpes.fr.

P. Candelier, L.-B. Faber and P. Gendrier are with STMicroelectronics, 850 rue Jean Monnet, 38926 Crolles, firstname.name@st.com.

M.-L. Flottes, G. Di Natale and B. Rouzeyre are with LIRMM, University of Montpellier, CNRS, 161, rue Ada, 34095, Montpellier, France, name@lirmm.fr.

V. Beroulle, D. Hély and A. Papadimitriou are with Univ. Grenoble Alpes, Grenoble INP (Institute of Engineering Univ. Grenoble Alpes), LCIS, 26000 Valence, France, surname.name@esisar.grenoble-inp.fr.

S. De Castro was both with LIRMM University of Montpellier, CNRS, and Mines Saint-Etienne.

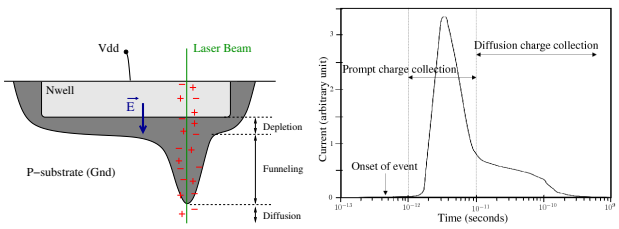

Fig. 1. Photoelectric effect of a laser beam through a PN-junction (left) - Transient current resulting from charge collection after a laser shot [21] (right).

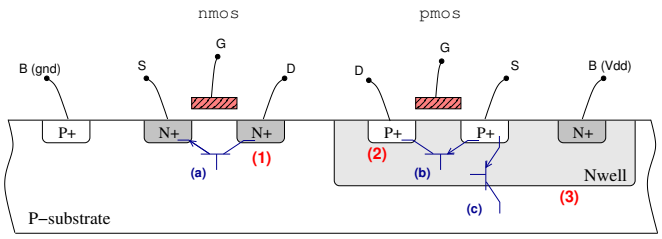

Fig. 2. Cross sectional view of CMOS bulk technology.

but are also extended to 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. We also studied on experimental basis how the properties of the FD-SOI technology may further increase the efficiency of bulk current sensors (the so-called bulk built-in current sensors, or BBICS [18]–[20]) at detecting laser-induced fault injection attacks.

This article is organized as follows. Section II describes 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 and discusses the laser fault injection thresholds we obtained for various experimental settings. Section V describes how the use of BBICS sensors in FD-SOI ICs may bring an increased detection ability of laser injection. The concluding section VI recalls the obtained results and provides 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 a photon energy 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 [21]. 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 [22]. It also relies 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 work is expected to bring reduced sensitivity to laser attacks. However, it does not provide a full immunity as reported hereafter.

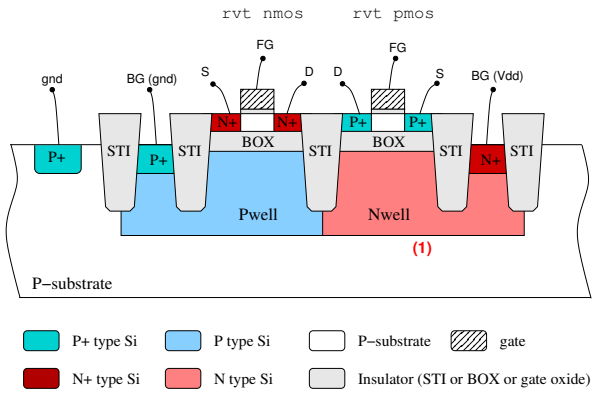

Fig. 3. Cross sectional view of FD-SOI technology: regular V_t transistors.

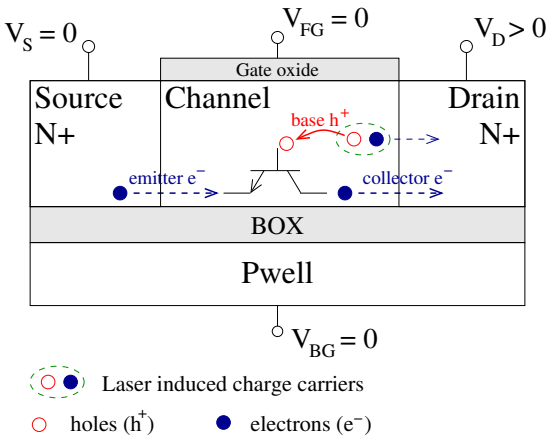

Fig. 4. Parasitic bipolar transistor activation in a FD-SOI NMOS transistor due to laser illumination [27].

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 [23]–[25]. 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], [26]. 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 expand under the transistors 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 there is no reverse biased PN junctions between the transistors' diffusions and their wells (due to the isolation box that lies under transistors). 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 Psub-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 junction in CMOS bulk). 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 (this phenomenon is further analysed in section V based on actual experiments reported in Fig. 8). 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 [27]. Fig. 4 illustrates its structure and its activation mechanism in the case of a NMOS transistor in OFF mode (its front gate FG and back gate BG are grounded). As its source is at 0 V and its drain is biased positively, 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 bulk 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 particles 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 process) 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 pulse 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 wavelength, 1 ps pulse duration, 1.1 µm laser spot diameter) testing of single test FinFET transistors designed in SOI and CMOS bulk (with 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, [28] 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] wavelength, 1.5 µm laser spot diameter). 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 w.r.t. CMOS bulk. 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], [29] 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 to laser illumination of FD-SOI:

- a laser-induced peak current an order of magnitude lower for FD-SOI transistors 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 micrometers beyond transistors.

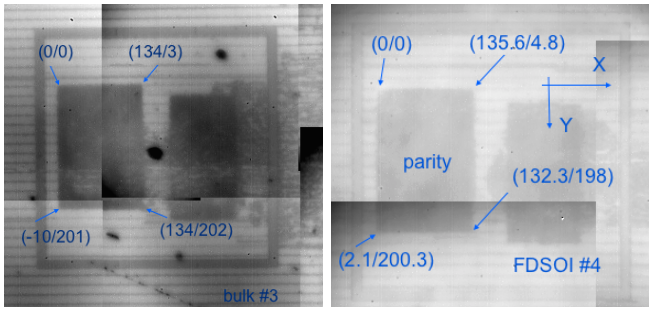

Fig. 5. Microphotographies of the AES test elements of the CMOS bulk (left) and the FD-SOI (right) 28 nm test chips. Views taken from ICs rear sides.

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 complex circuits (i.e. featuring several kgates) during their operations (i.e. for clocked and running devices).

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. Each chip embeds two AES implementations featuring fault detection techniques[2] based respectively on parity codes and on redundancy (the AES DDR of [30]); the AES of the two test chips being identical at RTL level. Our intend was to ascertain and measure experimentally the advantage of FD-SOI over CMOS bulk in terms of laser sensitivity. 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 in order to lessen the absorption of the laser beam energy when accessing the targets sensitive areas through their rear side.

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

[2] It is worth to mention that the lack of a reference unprotected AES had no influence on the obtained results because the aforementioned detection techniques did not changed the circuits sensitivity to fault injection, they act by raising a detection flag.

TABLE I
FD-SOI VS. 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

The core power supply voltage was set to 1.2 V and the clock frequency to 100 MHz.

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 1,064 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). Fault injection was performed through the rear side of the targeted chip (i.e. through its silicon substrate; note that the use of a laser source emitting in the near IR is mandatory to access the laser-sensitive parts of an IC through its substrate [2]). Our experiments were carried out at two different laser spot diameters[3], 1 µm and 5 µm, thanks to a 100x and a 20x optics with 26 % and 57 % power transmission coefficients respectively. An infrared camera was used to adjust the focus of the spot. 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 requires a significant number of injection attempts: each value reported in this work 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 on elementary test elements (see III-A). We measured a 0.2 nJ laser sensitivity for the CMOS bulk test chip and a 0.6 nJ laser sensitivity for the FD-SOI 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 (see section III-A).

The next experiments were performed with the same 30 ps laser duration but a laser spot size of 5 µm. The CMOS bulk laser sensitivity slightly increased to 0.3 nJ while that of FD-SOI was upped to 2.1 nJ. With these 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, typically in the nanosecond range. We chose to conduct our first attack-centric experiments a laser pulse duration equal to the target's clock period: 10 ns. 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 of our ns range laser source to 1 W, the FD-SOI device was found immune to laser fault injection (i.e. no fault was injected at the 1 W max power, note that faults would have been injected at a higher laser power).

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 in using FD-SOI rather than CMOS bulk to decrease a device laser sensitivity: for 1 µm laser spot diameter the comparative factor is between 2 and 3, it

[3]The diameters of the gaussian laser beams were measured using the knife-edge technique [31] and defined at FWHM (Full Width at Half Maximum) as expressed in [2].

is increased to a factor of 7 at 5 µm spot diameter. These figures are disappointing relatively to the previous state-of-the-art (see sections III-A and III-B) which reported a lesser SEU sensitivity of one or two orders of magnitude for FD-SOI w.r.t. CMOS bulk. This discrepancy may come from the test patterns used to carry out the reported experiments. Our experimental results were indeed obtained on running complex IPs (implementations of the AES encryption algorithm) while those of the previous works were obtained mostly on simpler test patterns (transistors or DFFs) in static mode (with no running clocks).

An explanation of this higher than expected laser-sensitivity of FD-SOI may be linked to an IR drop phenomenon (i.e. a current flowing from Vdd to ground in running ICs that induces a decrease of their power supply voltage swing that may be large enough to cause performance degradation or even malfunction [32]). Such a phenomenon may be induced in FD-SOI ICs because of the laser-sensitive PN junction that exists between every Nwell and the P-substrate (it is marked (1) in Fig. 3). This PN junction is always reverse biased (at Vdd) 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 photocurrent pulse between Vdd and ground, hence inducing an IR drop phenomenon that may encourage the injection of faults as reported in [33], [34]. This assumption is consistent with both the previous state-of-the-art and our results. Experiments carried out on elementary test patterns may indeed have not experienced any IR drop while our experiments on larger functional blocks shall have.

A tendency related to the laser spot diameter also emerges from our results (see table I). For a 1 µm laser spot diameter, the interest of using FD-SOI is expressed by a disappointing factor 2-3 (at 10 ns and 30 ps laser duration). While, for a 5 µm laser spot diameter, this factor is increased to 7 for both 50 ns and 30 ps laser duration (at 10 ns no fault was induced in the FD-SOI test chip). Considering the CMOS bulk technology alone, an increase from 1 µm to 5 µm of the laser spot diameter leads to a 30 % and a 50 % increase of the laser fault injection threshold at 10 ns and 30 ps laser duration respectively. The increase of the laser fault injection threshold of the FD-SOI test chip is 350 % for the same 1 µm to 5 µm increase of spot diameter at 30 ps laser pulse duration. Our explanation of this difference is that most of the laser-induced charge-carriers generated in the area of a large laser spot are lost to the photocurrent generation that happen only in the channel of FD-SOI transistors (i.e. charge carriers induced outside transistor channels can not be collected because of the isolation box found underneath FD-SOI transistors, see Fig. 3 as an illustration). This is not the case for CMOS bulk devices as most charge carriers may be collected at distance from transistors [11]. This difference in the charge collection mechanism explains that the interest in using FD-SOI w.r.t. CMOS bulk technology increases with the laser spot diameter. This has implications in terms of security because the cost of a laser fault injection bench increases significantly with its ability to output smaller laser spots, hence increasing the investment needed to perform effective attacks against FD-SOI targets.

An accurate description of the characteristics of the faults (what is called a fault model) injected during our experiments is out of the scope of this work. However, 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. The interested reader can find a complete analysis of the laser fault model obtained for the 28 nm CMOS bulk technology in [35].

Though higher than expected, our experiments demonstrate on experimental basis that the laser-sensitivity of the FD-SOI technology is lower than that of the CMOS bulk technology (at worst a comparison factor close to 2 was obtained). This interest of using FD-SOI technology can be further increased thanks to the use of sensors designed to detect laser attacks by measuring the induced bulk currents. Using FD-SOI would force an attacker to increase the power (or energy) of its laser pulses hence proportionally increasing the efficiency of such sensors. We address this approach in the next section.

V. Using BBICS to harden FD-SOI circuits against laser fault injection

Section IV reports on experimental basis the interest of using FD-SOI technology rather than CMOS bulk technology to decrease ICs sensitivity to laser fault injection. In a worst case (10 ns laser pulse duration and 1 µm spot diameter) the laser fault injection threshold of FD-SOI is only about twice that of CMOS bulk. Though disappointing, this factor becomes significant if it can be passed on to the efficiency of a laser illumination sensor. In this section, we describe the use of both FD-SOI technology and Bulk Built-In Current Sensors (BBICS), which are sensors used to monitor the bulk currents induced by laser illumination [18]. We provide experimental measures to show that the laser efficiency of BBICS shall be the same for FD-SOI and for traditional bulk technologies. As a result, given the higher laser fault injection threshold of FD-SOI, an attacker shall be forced to increase the laser power (or energy) to cause an error, and therefore be more susceptible to detection by BBICS.

A. BBICS *principles*

A BBICS is a bulk current sensor designed to detect any unexpected bulk current, induced by laser illumination or by a radioactive particle [18], [19]. In normal operation, bulk currents (i.e. the currents flowing through the biasing contacts of the P-substrate and Nwells) are low, typically in the µA range. They may rise to a magnitude of hundreds of µA or of several mA due to the photocurrents induced by laser illumination [36]. The purpose of a BBICS is to raise an alarm flag when a certain threshold of bulk current is exceeded, indicating that a circuit is under laser attack. This threshold shall be higher than the normal operation bulk currents, but lower than the level of laser-induced photocurrent needed to induce a fault.

Fig. 6 illustrates the principle of a pBBICS (first introduced by [18] to detect radiation-induced SEEs in CMOS bulk technology): a type of BBICS designed to detect laser attacks on

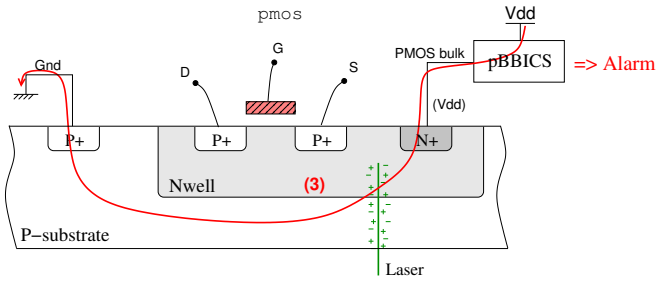

Fig. 6. PMOS-type BBICS principle in CMOS bulk technology (cross sectional view).

PMOS transistors[4]. The figure depicts a cross-sectional view of a PMOS Nwell and the photocurrent induced by a laser beam passing through the associated Psub-Nwell junction. The pBBICS is inserted between the Vdd power supply and the N+ diffusion region used to bias the Nwell, it is also in charge of providing the Vdd biasing to node PMOS_bulk: as a result, the laser-induced current flowing from Vdd to ground has to pass through the pBBICS itself. If this current exceeds the pBBICS detection threshold an alarm is raised ([18] gives the pBBICS architecture at transistor level and explains its mechanism); then, further actions may be taken as countermeasure (CM) against the detected attack. [20] provides an experimental validation of BBICS efficiency and CM triggering.

B. BBICS *in a* FD-SOI *device*

Considering Fig. 3, which gives the cross-sectional view of the FD-SOI technology, a BBICS can be inserted between the PMOS Nwell biasing contact (denoted BG, or back gate, and normally biased at Vdd) and the power supply in an arrangement similar to that used for CMOS bulk technology. As an example, the BBICS shown in Fig. 7 would be able to monitor and detect any bulk current surge induced by laser illumination of the Psub-Nwell junctions (marked (1) in Fig. 7).

The very interest of using BBICS in a FD-SOI device relies on the double assumption that (1) FD-SOI transistors are less

[4]nBBICS also exists, to monitor the bulk currents of NMOS transistors, and BBICS that can detect both types of bulk currents [37].

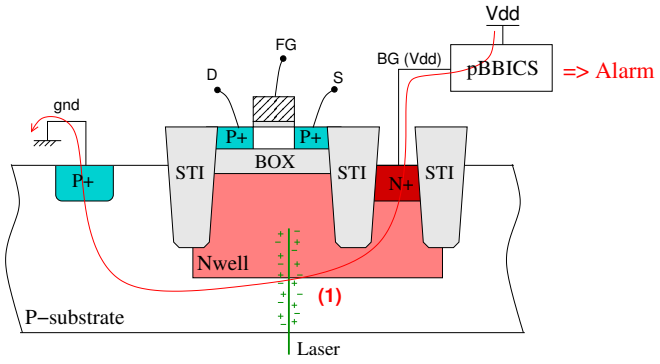

Fig. 7. BBICS principle in FD-SOI technology (cross sectional view).

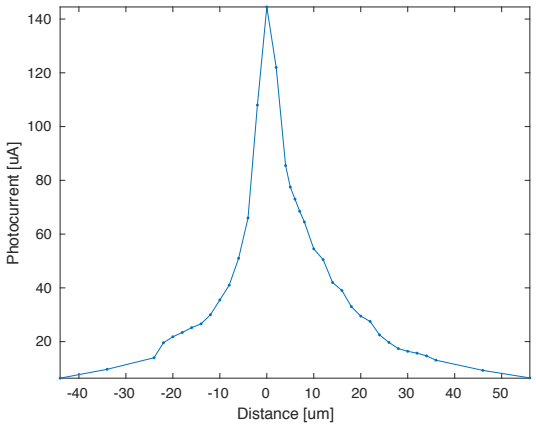

Fig. 8. Laser-induced photocurrent peak amplitude (in µA) of a FD-SOI NMOS transistor as a function of the distance of the laser spot from the transistor (in µm).

sensitive to laser illumination, and that (2) the efficiency of a BBICS is not affected by this phenomenon. To the best of our knowledge, there is yet no mention in the literature of any experimental testing of BBICSs in FD-SOI.

We tested those assumptions with the following laser settings: a wavelength of 1,064 nm, a pulse duration of 50 µs, a spot diameter of 5 µm, and rear side illumination of the test patterns.

1) Experimental testing of assumption (1): Fig. 8 reports the laser-induced photocurrent peak amplitude obtained during laser illumination of a FD-SOI NMOS transistor, as a function of the distance between the transistor's center and the laser spot. The measured current flowed from drain to source of the transistor biased in OFF mode: its source and gate were grounded, and its drain biased at 1.2 V. The target was a regular V_t NMOS transistor with a channel length and width resp. equal to 30 nm and 500 nm. The laser power was set to 1 W.

A maximum photocurrent peak amplitude of 144 µA was measured when the laser spot was centered on the transistor's channel (i.e. distance equal to 0). As the laser spot distance from the transistor increases, the peak amplitude decreases rapidly. It is halved for a distance of 5-6 µm, which is approximately the size of the laser spot: the laser-induced photocurrent starts to vanish as the laser spot ceases to illuminate directly the transistor channel. This is due to the isolation box lying under the transistor channel as explained in paragraph II-C1. It is testimony to the lesser laser-sensitivity of FD-SOI w.r.t. CMOS bulk (for the latter technology it may take several tens of µm to halve the photocurrent peak amplitude [16]); it is also a confirmation of assumption (1).

2) Experimental testing of assumption (2): Fig. 9 reports the results of a similar experiment carried out on a $4\,\mu m \times 4\,\mu m$ Psub-Nwell junction (marked (1) in Fig. 3). The same laser settings were used except for the laser power that was halved to 500 mW. The drawn photocurrent was measured flowing from the Vdd biasing contact BG to the P-substrate biasing contact (biased at ground).

The maximum measured peak current is 230 µA for a laser spot centered on the junction (distance equal to 0). It takes

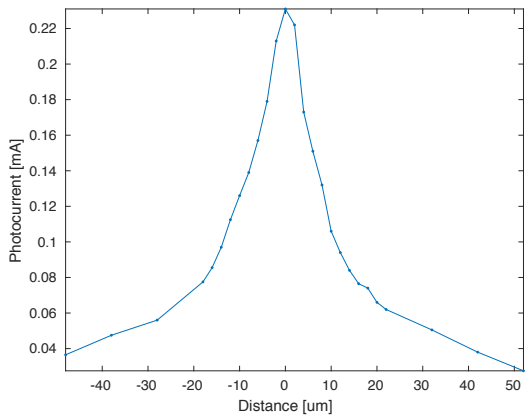

Fig. 9. Laser-induced photocurrent peak amplitude (in mA) of a Psub-Nwell junction as a function of the distance of the laser spot from the junction (in µm).

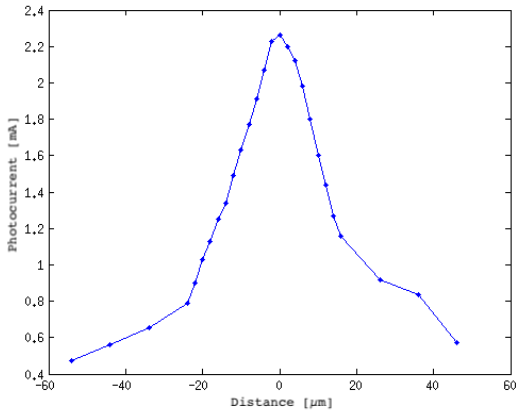

Fig. 11. Laser-induced photocurrent peak amplitude (in mA) of a Psub-DeepNwell junction as a function of the distance of the laser spot from the junction (in µm).

a distance of 12-14 µm to halve the peak amplitude (more than twice the size of the 5 µm laser spot). This illustrates that Psub-Nwell junctions in FD-SOI technologies can collect laser-induced bulk currents at a distance. This is a confirmation of the second assumption.

These experiments provide strong evidence that laser-induced bulk currents in FD-SOI technology are large and induced at a distance: two features in favor of an easy detection by BBICS. On the other hand, photocurrents induced in transistors (those responsible for fault injection) are weaker unless the attacker targets directly the transistors or uses a higher laser power. This combination increases the efficiency of BBICS when embedded in a FD-SOI device.

3) Using DeepNwell in FD-SOI *to further increase* BBICS *detection efficiency:* In addition, FD-SOI technology (similarly to CMOS bulk) also offers the ability to create Pwells isolated from the P-substrate thanks to a DeepNwell optional layer as depicted in Fig. 10. The DeepNwell layer is electrically connected to the Nwell, and it is biased through the Nwell biasing contact BG.

As a result, a PN junction between the Pwell and the DeepNwell is obtained (marked (2) in Fig. 10) in addition to the Psub-DeepNwell junction (marked (1) in Fig. 10). The use of a DeepNwell layer further increases the laser-induced bulk currents. This is illustrated by the experiments reported in Fig. 11, which displays the photocurrent peak amplitude we measured in a Psub-DeepNwell junction (4 µm × 4 µm). Experimental settings were similar, but for a laser power of 1.5 W. A maximum laser-induced photocurrent peak amplitude of ∼2.3 mA was measured for a laser spot centered on the junction (distance equal to 0). It is halved as the laser spot is moved away from the junction center by 17-18 µm. Hence, using a DeepNwell layer further increases the laser-induced bulk currents and the distance at which they are induced by laser illumination. This shall also further reinforce the laser detection capability of BBICS used with FD-SOI technology.

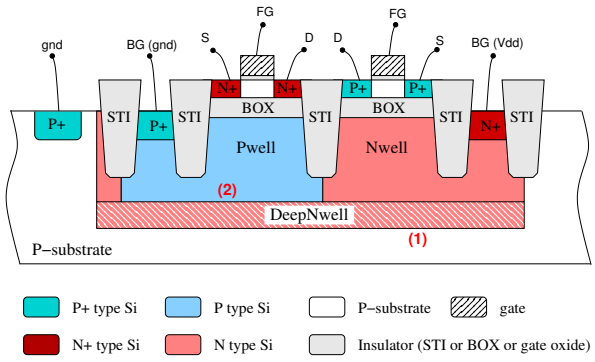

Fig. 10. Cross sectional view of FD-SOI technology: regular V_t transistors with DeepNwell.

C. Conclusion

We provided in this section experimental results showing the interest of using BBICS sensors along with FD-SOI technology to increase their laser attack detection capability. These experiments showed that FD-SOI transistors have reduced laser-sensitive areas, while the PN junctions collecting the bulk currents monitored by BBICS are sensitive to laser illumination even at a distance.

VI. Conclusion

In this work, we reported an experimental evaluation of the laser-sensitivity of the CMOS bulk and the UTTB FD-SOI technologies. Although assessing the interest of choosing FD-SOI rather than CMOS bulk for the purpose of lowering laser sensitivity, the extent of the gain revealed in our tests, 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.

We provided an explanation of this result. It may be linked to the laser-sensitive Psub-Nwell junction found in FD-SOI (marked (1) in Fig. 3). It is always reserve biased 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 photocurrent pulse between Vdd and Gnd, inducing an IR drop phenomenon that may encourage the injection of faults as reported in [33].

We also proposed an explanation of the better comparison factor of 7 obtained in favor of FD-SOI at 5 µm laser spot diameter (it is close to 2 for a 1 µm spot diameter). Our assumption is that only a fraction of the charge carriers induced when using a large laser spot participates to the photocurrent inducing faults. Indeed, charge carriers induced outside the channel of a FD-SOI transistor cannot be collected into the laser-induced drain to source current at the root cause of fault injection because of the isolation box lying underneath FD-SOI transistors.

Moreover, 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 would increase the ability of laser sensors to detect the attack. We discussed on experimental grounds, the interest of choosing a FD-SOI technology to increase the efficiency of Bulk Built-In Current Sensors [18], [20]. Their ability to detect laser attacks by monitoring the induced bulk currents shall be significantly increased because the Psub-Nwell junction of FD-SOI has a laser-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. This may also force an attacker to operate closer to the target's destructive threshold, thereby making his experiments harder to conduct.

The design and experimental test of a FD-SOI test chip embedding BBICS is a perspective worth to explore further. Our assumption on the role of an IR drop component taking part in the higher than expected laser-sensitivity of the FD-SOI technology is also worth to study on experimental basis. Its effect may be partly mitigated thanks to proper biasing arrangements making it possible to approach the one or two order of magnitude decrease in laser sensitivity promised in the former state-of-the-art.

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, no. 5, pp. 91–100, Oct 1965. doi: 10.1109/TNS.1965.4323904

[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, no. 3, pp. 1852–1875, June 2013. doi: 10.1109/TNS.2013.2255312

[3] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in 4th International Workshop on Cryptographic Hardware and Embedded Systems, ser. CHES '02. Springer-Verlag, 2002. doi: 10.1007/3-540-36400-5 pp. 2–12.

[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. doi: 10.1109/JPROC.2012.2188769

[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, 2010. doi: 10.1109/IOLTS.2010.5560194 pp. 235–239.

[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, 2005. doi: 10.1109/DATE.2005.54 pp. 1530–1591.

[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. doi: 10.1109/23.556880

[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, 2004. doi: 10.1109/RELPHY.2004.1315447 pp. 677–678.

[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, no. 6, pp. 2104–2113, Dec 2005. doi: 10.1109/TNS.2005.860682

[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, no. 6, 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, Oct 2011. doi: 10.1109/SOI.2011.6081714 pp. 1–2.

[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. doi: 10.1109/IRPS.2011.5784597

[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, 2013. doi: 10.1109/IEDM.2013.6724728 pp. 31.1.1–31.1.4.

[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. doi: 10.1109/TNS.2016.2630022

[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, ser. IFIP Advances in Information and Communication Technology. Springer International Publishing, 2015, vol. 464, pp. 220–240.

[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, May 2014. doi: 10.1109/DTIS.2014.6850664 pp. 1–6.

[17] J.-M. Dutertre, V. Beroulle, P. Candelier, L.-B. Faber, M.-L. Flottes, P. Gendrier, D. Hély, R. Leveugle, P. Maistri, G. Di Natale, A. Papadimitriou, and B. Rouzeyre, "The case of using cmos fd-soi rather than cmos bulk to harden ics against laser attacks," in On-Line Testing Symposium (IOLTS), 2018 IEEE 24th International, 2018.

[18] E. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. Kastensmidt, "Using bulk built-in current sensors to detect soft errors," Micro, IEEE, vol. 26, no. 5, pp. 10–18, Sept 2006. doi: 10.1109/MM.2006.103

[19] C. Champeix, J.-M. Dutertre, V. Pouget, B. Robisson, M. Lisart, N. Borrel, and A. Sarafianos, "Laser testing of a double-access bbics architecture with improved see detection capabilities," in Radiation Effects on Components and Systems, Radecs 2016, 2016. doi: 10.1109/RADECS.2016.8093172

[20] K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, and N. Miura, "A 286f2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack," in 2018 IEEE International Solid - State Circuits Conference - (ISSCC), 2018. doi: 10.1109/ISSCC.2018.8310329

[21] F. Wang and V. Agrawal, "Single event upset: An embedded tutorial,"

in VLSI Design, 2008. VLSID 2008. 21st International Conference on, Jan 2008. doi: 10.1109/VLSI.2008.28 pp. 429–434.

[22] 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, July 2015. doi: 10.1109/IOLTS.2015.7229820 pp. 13–18.

[23] 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, Dec 2009. doi: 10.1109/IEDM.2009.5424251 pp. 1–4.

[24] ——, "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, March 2012. doi: 10.1109/ULIS.2012.6193383 pp. 165–168.

[25] D. Golanski, P. Fonteneau, C. Fenouillet-Beranger, A. Cros, F. Monsieur, N. Guitard, C. Legrand, A. Dray, C. Richier, H. Beckrich, P. Mora, G. Bidal, O. Weber, O. Saxod, J. Manouvrier, P. Galy, N. Planes, and F. Arnaud, "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, June 2013, pp. T124–T125.

[26] 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, no. 6, pp. 2104–2113, Dec 2005. doi: 10.1109/TNS.2005.860682

[27] 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. doi: 10.1109/LED.2014.2385797

[28] 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. doi: 10.1109/TNS.2016.2627015

[29] 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, July 2015. doi: 10.1109/ISVLSI.2015.76 pp. 362–367.

[30] 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. doi: 10.1109/TC.2008.149

[31] J. A. Arnaud, W. M. Hubbard, G. D. Mandeville, B. de la Clavière, E. A. Franke, and J. M. Franke, "Technique for fast measurement of gaussian laser beam parameters," Appl. Opt., vol. 10, no. 12, pp. 2775–2776, Dec 1971. doi: 10.1364/AO.10.002775

[32] S. Zhao and K. Roy, "Estimation of switching noise on power supply lines in deep sub-micron cmos circuits," in VLSI Design, 2000. Thirteenth International Conference on, 2000. doi: 10.1109/ICVD.2000.812604. ISSN 1063-9667 pp. 168–173.

[33] 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. doi: 10.1109/DSD.2017.43

[34] R. A. Viera, J.-M. Dutertre, P. Maurine, and R. P. Bastos, "Standard cad tool-based method for simulation of laser-induced faults in large-scale circuits," in Proceedings of the 2018 International Symposium on Physical Design, ser. ISPD '18. New York, NY, USA: ACM, 2018. doi: 10.1145/3177540.3178243 pp. 160–167.

[35] J.-M. Dutertre, V. Beroulle, P. Candelier, S. De Castro, L.-B. Faber, M.-L. Flottes, P. Gendrier, D. Hély, R. Leveugle, P. Maistri, G. Di Natale, A. Papadimitriou, and B. Rouzeyre, "Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model," in FDTC 2018, ser. 5th Workshop on Fault Diagnosis and Tolerance in Cryptography, 2018.

[36] J.-M. Dutertre, R. P. Bastos, O. Potin, M. Flottes, B. Rouzeyre, G. D. Natale, and A. Sarafianos, "Improving the ability of bulk built-in current sensors to detect single event effects by using triple-well cmos," Microelectronics Reliability, vol. 54, no. 9-10, pp. 2289 – 2294, 2014. doi: 10.1016/j.microrel.2014.07.151

[37] J.-M. Dutertre, R. Possamai Bastos, O. Potin, M. Flottes, B. Rouzeyre, and G. Di Natale, "Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection," Microelectronics Reliability, vol. 53, no. 9, pp. 1320–1324, 2013. doi: 10.1016/j.microrel.2013.07.069

Jean-Max Dutertre received the M.S. and Ph. D. degrees in electronics from the University of Science of Montpellier, France, in 1998 and 2002, respectively. In 2008, he joined the Ecole Nationale Supérieure des Mines de Saint-Etienne (MSE) as an Assistant-Professor. He is with the secured architectures and systems department (SAS) a joint R&D team between MSE and the CEA. His research interests include the study of fault attacks against cryptosystems and the development of the relative countermeasures.

Vincent Beroulle received the M.S. and Ph. D. degrees in microelectronics from the University of Science of Montpellier, France, in 1999 and 2002, respectively. In 2002, he joined the Grenoble Institute of Technology (Grenoble INP) as an Assistant-Professor. He is with the LCIS laboratory in Valence. His research interests include the security and safety of heterogeneous systems.

Philippe Candelier received the Ph. D. degree in microelectronics from the University of Science of Grenoble, France, in 1997. He joined ST Microelectronics in 1998, where he held the position of Power Management & eNVM Design team manager.

Stephan De Castro received the Ph. D. degree in electronics from the University of Science of Montpellier, France, in 2016. He studied the laser illumination of FD-SOI devices to derive the related electrical models.

Louis-Barthélemy Faber is a design hardware staff engineer at ST Microelectronics. He started his career first by modeling magnetic tunnel junctions (IEF U-PSUD) and then digital components (LETI-CEA). He mainly designs now one-time-programmable memory controllers with specific requirements in terms of hardware security.

Marie-Lise Flottes is researcher at the French National Scientific Research Center. She has been conducting research in the domain of digital system testing at LIRMM laboratory - France, since 1990. Her interests include Design-for-Testability, Design-for hardware security and trust, with a focus since early 2000 on testability and fault tolerance on systems dedicated to secure applications.

Philippe Gendrier joined ST Microelectronics in 2000. He is project engineer in digital design and secure devices.

David Hély received the master degree from the National Institute of Applied Sciences of Lyon, in 2002, and the Ph.D. degree from the University of Monpellier 2, in 2005, with a focus on the design for testability of secure IC in collaboration with STMicroelectronics and the LIRMM Laboratory. From 2005 to 2009, he held several industrial positions, where he was focused on the design of secure system-on-chip. Since 2009, he has been an Associate Professor with the Grenoble Institute of Technology.

Regis Leveugle (M'91-SM'14) received a Ph.D. degree in Microelectronics from INPG (France) in 1990 and is Professor at Grenoble Institute of Technology since 1999. His main interests include computer architecture, VLSI design methods and tools, fault-tolerant and secure circuit architectures, and dependability analysis.

Paolo Maistri is currently a CNRS researcher at the Techniques of Informatics and Microelectronics for Integrated Systems Architecture (TIMA) Laboratory, Grenoble, France. His major interests include efficient and secure implementations of cryptographic systems, implementations attacks, and the development of efficient and effective countermeasures against side channel and fault analysis.

Giorgio Di Natale is director of research for the National Research Center of France at the LIRMM laboratory in Montpellier. His research interests include: hardware security and trust, reliability, fault tolerance, test. He is the vice chair of the TTTC, Golden Core member of the Computer Society and Senior member of the IEEE.

Athanasios Papadimitriou received a diploma degree in Applied Physics from the School of Applied Sciences of the National Technical University of Athens in 2012. In 2016 he received a PhD degree from the Univ. of Grenoble Alpes in the field of hardware security. The PhD studies were carried out at the LCIS laboratory of Grenoble INP with a focus on fault modeling of laser attacks on secure ICs. Currently he is a Hardware Security Research Engineer for Grenoble INP - ESISAR in the framework of ESYNOV/SACCO platform.

Bruno Rouzeyre is Professor at the University of Montpellier, and conducts his research with LIRMM Laboratory. His current research interests include several aspects of CAD for digital circuits and are particularly oriented toward optimization, verification, test and test synthesis of digital and secure circuits.