Assessing BBICS Efficiency in Monitoring Triple-Well Logic and Picosecond LFI

Axel Guichaoua[1,2], Samuel Lesne[1], Jean-Baptiste Rigaud[2], and Jean-Max Dutertre[2]

[1] IDEMIA StarChip firstname.lastname@idemia.com
[2] Mines Saint-Etienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France
lastname@emse.fr

Abstract. Laser Fault Injection (LFI) is a threat to the security of integrated circuits (ICs). Bulk Built-in Current Sensors (BBICSs) were introduced to detect anomalous transient currents induced in the bulk of ICs when hit by ionizing particles. As LFI also exhibits characteristic bulk currents, the detection capabilities of this family of sensors against LFI has been a point of interest in literature.
Although some experimental results are documented, LFI parameters and technological node exploration remain incomplete. Furthermore, proposed results for Triple-Well CMOS technology are rare. A 65 nm CMOS technology node ASIC implementation was tested for targets in Dual-Well and Triple-Well CMOS technology. Detection ranges and thresholds of the studied sensors were compared to fault injection thresholds of standard cells to assess BBICS capability at detecting LFI.
Our experimental results extend the state-of-the-art by assessing the efficiency of BBICS in detecting picosecond laser pulses and in monitoring Triple-Well logic (contrarily to previous research for the latter). We report detection thresholds that are significantly lower than fault sensitivity and detection radiuses up to a hundred micrometers.

Keywords: Laser Fault Injection (LFI) · Bulk Built-in Current Sensor (BBICS) · Picosecond · Triple-Well.

1 Introduction

Fault Injection Attacks (FIAs) have been shown to be a serious threat to the security of Integrated Circuits (ICs). Physical disruption of devices can provoke exploitable malfunction (faults), resulting in security vulnerabilities. Research proved they could be leveraged to retrieve cryptographic keys [2,3,4,17], which would allow an attacker to access confidential data and commit forgery. FIAs can also be used to tamper with program control flow [25], enabling security check bypass.

Among various means for FIAs listed throughout literature [2], Laser Fault Injection (LFI) [40] provides a remarkable level of accuracy even when it comes to recent technology nodes [20]. It can yield micrometer-range area of effect

and temporal resolution down to the picosecond-range. Development of effective countermeasures to address this threat is an ongoing process as technology and attacks evolve.

The use of redundancy checks has been a point of interest to the scientific community to address LFI vulnerabilities [1,26,33]. Such mechanisms provide a response to actual fault occurrences and their structure allows technology-agnostic digital implementations. However, their behavior relies on fault sampling and knowledge of fault model to ensure efficiency. Furthermore, a strong overhead and careful design is needed to provide sufficient fault coverage without introducing additional Side-Channel Analysis (SCA) vulnerabilities [9,12,13,18].

Several LFI sensor designs were proposed to detect LFIs in order to trigger appropriate response of ICs. Their mechanism is data independent, providing detection without introduction of SCA vulnerabilities. Detection is not based on fault occurrence measurement but rather on side-effects of FIAs leading to inherent Statistical Ineffective Fault Analysis (SIFA) [17] robustness at the cost of possible false-negative and false-positive. We denote two main approaches:

- *direct* sensors [26,43], aiming to be the unwanted target of attacks trading ease of integration for high area overhead.
- and *indirect* sensors, detecting long-range effects of LFIs such as laser induced transient bulk voltage disruption [29] or IR drop [21].

In this work, we propose an experimental characterization of an *indirect* LFI sensor, the Single Bulk Built-In Current Sensor (BBICS) [19]. Our work focuses on providing additional results on the sensor's LFI detection capabilities in order to complement existing studies [14]. The main contributions of this work are:

- an experimental validation of the Single BBICS on a 65 nm CMOS technology implementation while monitoring logic gates,
- a validation of the increased LFI detection capacity of the Single BBICS while monitoring a Triple-Well test pattern,
- an extension of the BBICS testing state-of-the-art to CMOS logic monitoring against picosecond-range laser pulses.

2 Bulk Buit-In Current Sensors

BBICSs were originally designed to detect abnormal transient bulk current in ICs, characteristic of Single Event Effects (SEEs) due to ionizing particle collision [30,31]. As lasers were adopted as a mean for SEE emulation [23,34] and later as a potent malicious attack tool [40], BBICS were found to be a point of interest regarding LFI detection. Several architectures were derived and described throughout the literature [32,38,39,42], leveraging different strategies to improve detection capabilities and overhead.

This work focuses on the Single BBICS, a dual-access architecture proposed by [19] and experimentally tested by [6,14]. In this section, we first introduce the LFI physical principle and its relevant implications regarding the BBICS

detection mechanism. An overview of the BBICS principle is then developed. Finally, we address the interest of using a Triple-Well-based CMOS logic to increase the monitoring efficiency of BBICS.

2.1 Laser Fault Injection

The ionizing behavior of light on silicon was found to be responsible for parasitic current generation in ICs' reverse bias PN junctions [10,11,24]. Excess charge carriers generated by light absorption are partially collected by the electric field of neighboring PN junctions' depletion region, resulting in a transient photocurrent. This photoelectric effect can tamper with transistors and thus logic gates behavior as represented in Figure 1 (on the cross-sectional view of and inverter gate).

Upon laser illumination, the reverse biased junction D_p/N_{well} (resp. P_{sub}/N_{well}) generates a transient photocurrent $I_{ph,fault}$ (resp. $I_{ph,SC}$). The load capacitance of the inverter gate is then charged by the current $I_{ph,fault}$. If $I_{ph,fault}$ exceeds the current I_{CMOS} that can flow through the ON NMOS transistor, it leads to a transient switching of the output logic state. This Single Event Transient (SET) can possibly lead to a Single Event Upset (SEU) upon sampling by the fanout logic.

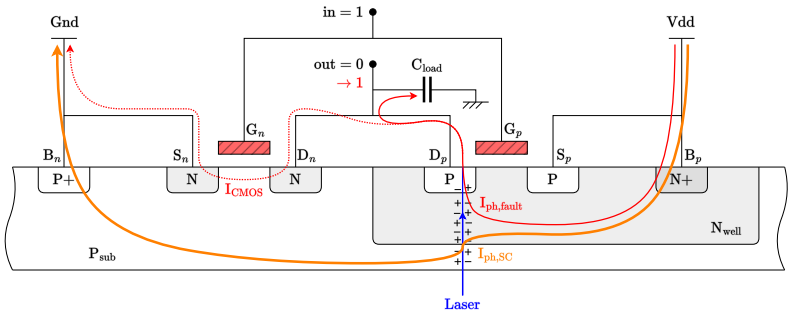


Fig. 1: LFI principle: generation of laser-induced photocurrents in an inverter resulting in a transient fault (case of a high logic level input).

Photocurrents also induce IR-drops along their paths. Local Substrate Potential Bounce (SPB) and Nwell Potential Drop (NPD) occur, both spreading in their respective doped regions [29], possibly leading to parasitic bipolar activation causing additional currents (not represented Fig. 1) participating in the fault process [5,7,36]. In turn, potential disruption can propagate at circuit level through the Power Delivery Network (PDN) [41].

Although Fig. 1 represents the laser as a point beam, the spatial distribution of its intensity is more akin to a bell-curve [11], due to optical properties. Additionally, excess charge carriers can diffuse to the depletion areas further

increasing the effective range of junction charge collection. Photocurrent generation in PN junctions were reported up to hundreds of micrometers away from the laser focus point [35,36]. This makes it impossible to target a single transistor in state-of-the-art technologies.

Both laser beam power distribution and charge collection through diffusion renders the surface of PN junctions a determining factor for the intensity of the generated currents as modeled in [16,27]. As a consequence, $I_{ph,SC}$ is significantly superior to $I_{ph,fault}$ [35] because the area of the P_{sub}/N_{well} junction is greater than that of the D_p/N_{well} junction. Additionally, the range of charge generation and collection ensure $I_{ph,SC}$ is present even upon targeting of NMOS transistors. This strong laser-induced photocurrent flows through both biasing contacts of the gate bulk (B_n and B_p in Fig. 1).

2.2 BBICS Principle

As mentioned above, LFI exhibits characteristic transient bulk currents, typically two orders of magnitude higher than during normal ICs operation [14]. A BBICS aims at detecting those currents by monitoring any abnormal current flowing through the biasing contacts of the logic it monitors. The studied Single BBICS architecture is a double-access BBICS, i.e. it monitors simultaneously both NMOS and PMOS bulks. Figure 2 illustrates the BBICS principle.

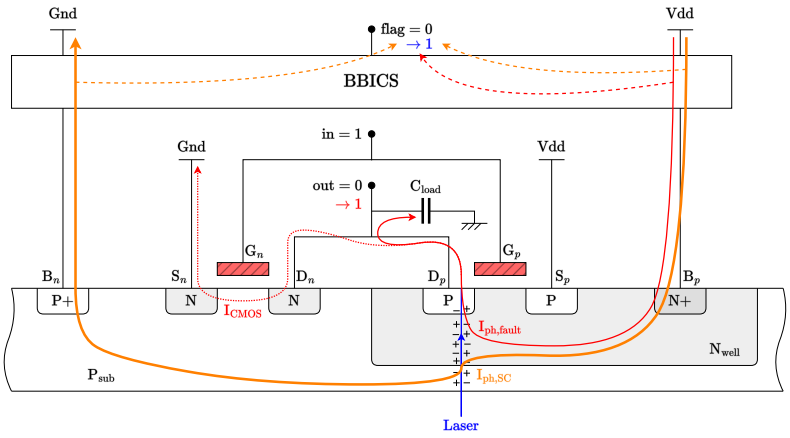


Fig. 2: BBICS principle, illustrated on a cross-sectional view of an inverter gate.

The bulk biasing contacts (B_n and B_p) are disconnected from the ground and power distribution networks and connected to the BBICS. The sensor is built to provide the correct biasing voltages (Gnd and Vdd to B_n and B_p respectively), ensuring capture of bulk currents while monitoring them.

The BBICS is designed to raise an alarm flag upon abnormal current detection. The alarm state is memorized until reset. Although only two taps (or

biasing contacts) are shown in Fig. 2, such a sensor can monitor multiple logic cells. Furthermore, a BBICS can be connected to a remote target by stretching wires from its target taps to its dedicated terminals. The double-access nature of the Single BBICS architecture (further described in Section 4) allows bulk-to-bulk photocurrents, the strongest contributors, to participate twice in the detection process.

It is to be noted that multiple taps in the design can capture a part of the laser-induced bulk currents. This can increase the detection range of the BBICS as currents generated by illumination of a non-monitored region is partially captured by a monitored tap. However, it can also increase the detection threshold as current generated in monitored region can also be captured by non-monitored taps.

The aforementioned Source-Bulk-Drain parasitic bipolar activation occurring upon LFI [5,7] can also hinder the BBICS detection capabilities as it decreases the fault injection threshold without increasing the amount of bulk current.

2.3 Triple-Well Logic Monitoring

Triple-Well CMOS technology, pictured in Figure 3, consists in isolating NMOS bulks from the substrate with a deep Nwell layer. Triple-Well reduces the impact of the substrate's electronic noise and enables the use of forward or reverse body biasing techniques for performance purposes. This technology modifies the junction topology compared to the usual Dual-Well approach (as pictured in Fig. 2), impacting photocurrent generation upon laser illumination [5,7,8] but also parastic bipolar transistor effects [5,7,8,22].

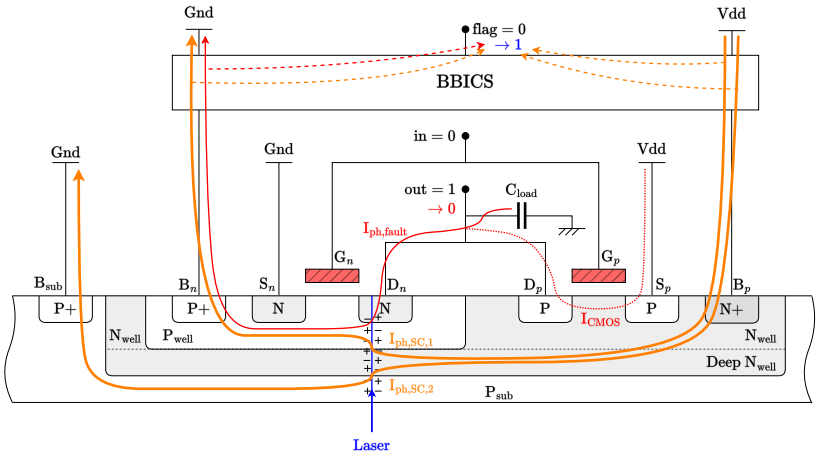


Fig. 3: BBICS Triple-Well monitoring principle.

Dutertre *et al.* [19] proposed to leverage Triple-Well technology to improve BBICS detection capabilities. Indeed, these implementations feature additional

reverse biased PN junctions compared to their Dual-Well counterparts. These large junctions generate additional photocurrents upon illumination, $I_{ph,SC,1}$ and $I_{ph,SC,2}$ depicted in Fig. 3, which then both take part in the BBICS triggering process. As a result, Triple-Well logic comes with greater laser-induced bulk currents that shall increase a BBICS monitoring capacity.

3 BBICS State-of-the-Art

LFI detection using a BBICS is hard to model accurately at electrical simulation level as it requires a precise modeling of both the laser-induced currents and of how the bulk currents propagate in the substrate from their generation point to the biasing contacts that capture them. A rigorous simulation would require running a 3D model with a physical simulator fed with all the relevant parameters of the technology considered. Therefore, experimental validation is necessary to assess BBICS behavior and their efficiency as LFI detection sensor.

This section proposes an overview of the State-of-The-Art experimental results in order to contextualize our contribution.

3.1 BBICS Validation on Dedicated Test IP

The first experimental validations of BBICS were carried out on dedicated test IP designed specifically for this purpose. Their aim was more about proving that the principle of monitoring the bulk currents to detect laser attacks was sound rather than evaluating their use on a target close to a real integrated circuit.

Champeix *et al.* [15] proposed an experimental characterization on a 90 nm Dual-Well technology circuit with laser pulse widths ranging from 50 ns to 200 ns. Their test target was made of a unique Single BBICS monitoring a $45\,\mu m \times 13\,\mu m$ block made of combinational gates. Their results showed that BBICS can detect laser-induced bulk currents. They also underlined that mixing bulk biasing contacts connected to the BBICS and others connected to Gnd and Vdd in close vicinity creates competition in capturing the bulk currents between the BBICS and the power supply that negatively impacts the sensor detection capability.

The impact of the use of Triple-Well logic on BBICS behavior described by Dutertre *et al.* [19] was experimentally investigated by Borrel *et al.* [6] in a comparative study led on a CMOS 90 nm technology test chip (it used the same test target as [15]). Experiments were performed using laser pulses duration ranging from nanoseconds to microseconds. Significantly smaller BBICS sensitive area were reported for Triple-Well target implementation compared to their Dual-Well counterpart. The assumption of a lower current generation on the wells in Triple-Well compared to Dual-Well was adopted. Since then, the use of Triple-Well logic has been considered to be avoided when using a BBICS.

3.2 BBICS on a Representative Target

Matsuda *et al.* [28] proposed an experimental validation of BBICS integrated in a dense CMOS 180 nm AES implementation. This is, to date, the only successful test of BBICS on a target representative of a real application case.

The sensors' architecture of [14] has been divided into a front-end (head), for biasing and sensing, and a back-end (tail), for alarm generation and memorization. Front-end parts are located directly in place of the taps (one head per tap, i.e. a 1:1 ratio) in a $60\mu m \times 5\mu m$ grid (chosen based on previous observation of SPB and NPD ranges [29]). Back-end parts were pooled with a 15:1 head-to-tail ratio for area optimization and detection range redundancy.

Laser testing with 60 ns laser pulses revealed an exhaustive coverage of the target AES with a significant margin between the detection and fault thresholds (2.6 ratio). Full LFI coverage was realized with a 28% layout area overhead compared to the unprotected implementation (note that this overhead includes the logic implementing a security policy triggered upon LFI detection).

3.3 Opportunities for Further Tests

Although several experimental results are present in the bibliography, as reported in Table 1, they remain rare. Furthermore, the reported used laser pulse widths were always in the nanosecond-range when the tested BBICS were monitoring logic gates (though [14] considered picosecond laser pulse with a BBICS connected to a test pattern that contained no actual logic gates).

Table 1: Single BBICS state-of-the-art experimental parameters.

Reference	[15]	[6]	[28]	**This Work**
BBICS head per tail ratio	1:1	1:1	15:1	1:1
BBICS tapping ratio	50%	100%	100%	100%
Technology	90 nm	90 nm	180 nm	65 nm
Target	Dual-Well logic	Dual-Well logic Triple-Well logic	Dual-Well AES core	Dual-Well logic Triple-well logic
Laser pulse duration	200-50 ns	long μs to short ns	60 ns	50 ns and 30 ps

The current BBICS state-of-the-art does not include an experimental validation of their detection capability of picosecond-range laser pulses. Lacruche *et al.* [27] studied the difference between nanosecond-range and picosecond-range laser pulse widths for laser-induced SEUs in SRAM cells. They pointed out a fault capability improvement due to an increased locality, rendering layout-based photocurrent counterbalancing [37] ineffective. Their work highlights a global reduction of the induced photocurrent, though the photocurrent at the root cause of fault injection remains above the injection threshold. Later, Da Cruz *et al.* [16] established pulse width as a governing factor regarding the locality of photocurrent generation. In addition to their increased spatial accuracy, picosecond-range

pulses provide temporal accuracy allowing for monocycle faults on higher clock frequencies than nanosecond-range pulses.

Aside from their concerning fault injection capabilities, picosecond-range laser pulses properties may affect their detection. Indeed, shorter pulse width implies increased capacitive filtering of bulk currents, upon which BBICS detection relies. Furthermore, narrowed charge collection area leads to overall less photocurrent generation, especially on those bulk-to-bulk junctions that play a key role in the BBICS detection (see Section 2.2). Although some results on a well-only test structure are documented [14], BBICS relevance in detecting picosecond-range LFI in CMOS logic is yet to be demonstrated.

Regarding the monitoring of Triple-Well logic by BBICS, despite the disappointing experimental results reported by the only known reference [6], additional testing appeared to be useful for confirmation purposes.

4 Sensor Characterization Methodology and Experimental Set-up

Our experiments were carried out on a CMOS 65 nm technology test chip (with a core voltage of 1.2 V). In this section, we present the methodology used to assess BBICS detection performances and we provide an overview of the sensor implementation used for our experiment. The test structures are presented as well as the laser setup and the parameters used.

4.1 Methodology

BBICS are laser attack detection sensors that use a detection mechanism based on bulk current monitoring. Although their triggering mechanism is related to fault injection, they do not provide a direct acknowledgment of a fault occurrence, they rather provide an indication of an unusual bulk current event. Their ability in detecting fault injection attempts lies in their alarm threshold to be lower than the fault injection threshold of the logic they monitor. These thresholds are expressed by several parameters of the laser pulse: power (or energy), duration, and location.

From a practical point of view, for a given laser power and duration, maps of fault sensitivity and alarm triggering are drawn (i.e. the locations of the laser spot that yield a fault or a detection). When the corresponding fault area is contained inside the detection area (i.e there is no undetected fault), the BBICS fulfills its purpose. The spatial margin between the detection and fault maps provides an assessment on the robustness of BBICS detection. The BBICS evaluation methodology we followed, consisted in:

- assessing the fault injection threshold of D flip-flops and combinational gates in terms of laser power (or energy) and pulse duration,
- and experimentally drawing the BBICS detection maps on different test patterns (presented in Section 4.3) implemented in Dual-Well or Triple-Well technology, for different laser parameters.

The extent of the detection areas then provides an assessment of their efficiency and of the logic area they can monitor.

4.2 Single BBICS Implementation

The schematic of the Single BBICS implementation used throughout our experiments is given in Figure 4. Its main parts are:

- Two heads, a NMOS bulk head and a PMOS bulk head made respectively of transistors Mn0-1 and Mp0-1, used to sense the bulk currents and connect the biasing contacts to Gnd or Vdd.
- A tail, made of two cross-coupled inverters (transistors Mn2-Mp4 and Mn4-Mp2) and two additional transistors in ON state (Mn3 and Mp3), used to memorize the state of the alarm flag.
- A reset logic (Mn5 and Mp5).

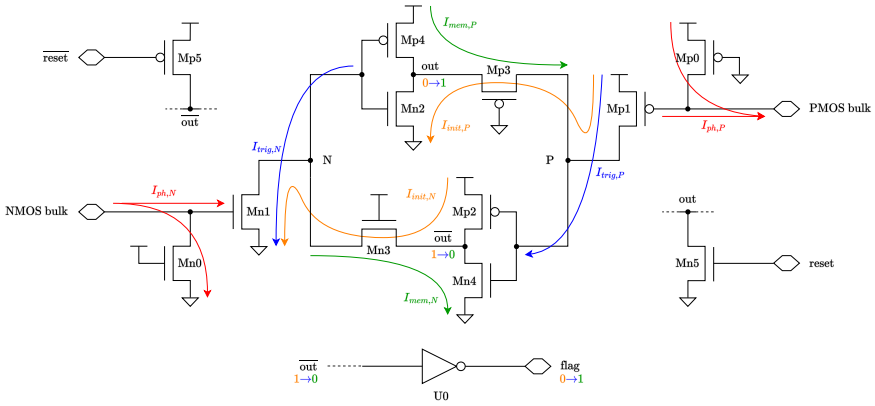


Fig. 4: Single BBICS schematic with illustration of the triggering process upon sensing of transient bulk currents.

In monitoring mode, the BBICS flag output is at logical state 0, the tail internal nodes N and P are respectively at 1 and 0 logical levels. A qualitative depiction of the detection mechanism is achieved by representing the named currents in Fig. 4:

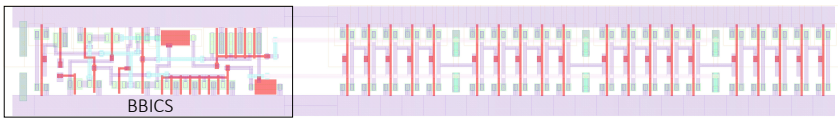
- $I_{ph,N}$ and $I_{ph,P}$ (red) represent the target NMOS and PMOS bulk transient currents occurring during LFI. As they flow through Mn0 and Mp0 they induce a voltage transient at the gates of transistors Mn1 and Mp1.
- $I_{trig,N}$ and $I_{trig,P}$ (blue) represent charge movement on the gates of transistors Mn2, Mp4, Mp2 and Mn4 due to activation of transistors Mn1 and Mp1.
- $I_{init,N}$ and $I_{init,P}$ (orange) are currents flowing through Mp2 and Mn2 respectively when transistors Mn1 and Mp1 are switched ON (the BBICS being initially in detection mode). Drain currents of transistors Mn1 and Mp1 are required to surpass these currents for $I_{trig,N}$ and $I_{trig,P}$ to occur.

– $I_{mem,N}$ and $I_{mem,P}$ (green) finally replace $I_{init,N}$ and $I_{init,P}$ respectively due to P and N voltage transient caused by $I_{trig,N}$ and $I_{trig,P}$. They achieve the switching and stabilize the detection state of the sensor.

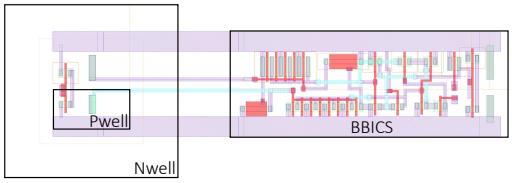
The design differs from the canonical architecture of [6,14,15]. It features several transistors with low and high threshold voltages (LVT and HVT resp.) in addition to standard Vt (SVT) transistors in order to lower the BBICS detection threshold (as detailed in [19]). Furthermore, additional transistors Mn3 and Mp3 are present. They enhance detection capabilities by limiting $I_{init,N}$ and $I_{init,P}$ thus increasing $I_{trig,N}$ and $I_{trig,P}$ and therefore lowering the detection threshold. Their resistive effect is stronger at the initial state due to the nature of the transistor used, asymmetrically affecting the state switching in favor of detection.

4.3 Test Structures

Figure 5 represents the two test structures used to study BBICS detection thresholds and areas. The first test structure, displayed in Fig.5a is composed of a Single BBICS Dual-Well implementation (left) monitoring the 6 taps (or biasing contacts) of a 20 Dual-Well inverter chain (right). The second one, in Fig.5b, features the exact same BBICS (right) monitoring the 2 taps of a single Triple-Well inverter (left).



(a) BBICS monitoring a 20 Dual-Well inverter chain.



(b) BBICS monitoring a Triple-Well inverter.

Fig. 5: Test structures layout.

The Triple-Well test pattern circuit depicted in Fig. 5b is equivalent to the circuit represented in Fig. 3. The P_{well} and N_{well} are monitored by the BBICS whereas the P_{sub} biasing is directly connected to the PDN.

Both test structures feature BBICS relatively close to their target biasing contacts. This reduces the resistive component of the equivalent RC filter connecting the monitored taps to the sensor thus ensuring that the associated filtering does not lower the BBICS detection threshold.

4.4 Laser Setup

The test chip substrate was thinned to 120 μm in order to perform backside LFI. A 1,064 nm wavelength laser source was used for nanosecond-range pulse generation, whereas a 1,030 nm wavelength one was used for 30 ps pulses.

A laser spot diameter of 5 μm (resp. 1 μm) was achieved using of a $\times$20 (resp. $\times$100) magnification lens [11]. It is to be noted that these lenses yield different laser transmission coefficients: 26 % and 57 % at $\times$100 and $\times$20 magnification respectively.

5 Experimental Results

5.1 Laser fault Injection Threshold

The laser fault injection threshold of our CMOS 65 nm test target was measured on a 16 DFF shift register and its reset tree, it provides the threshold for register faults (a so-called SEU) and for logic faults (or SET). The characterization was realized in a static scenario, meaning all signals held constant during fault injection. The results reported in Table 2 indicates the lowest power/energy for which faults were observed (i.e. defining the LFI threshold). The reported fault thresholds for DFF covers all possible configuration of held data and clock values. The lowest LFI thresholds were obtained on the DFF for a 1 μm spot diameter: 1.7 W at 50 ns and 2 nJ at 30 ps. Note that the laser pulse amplitude is reported in power (W) for our nanosecond source and in energy (nJ) for our picosecond source. This unity disparity will not be normalized to account for the actual laser source parameters.

Table 2: Observed laser fault injection thresholds.

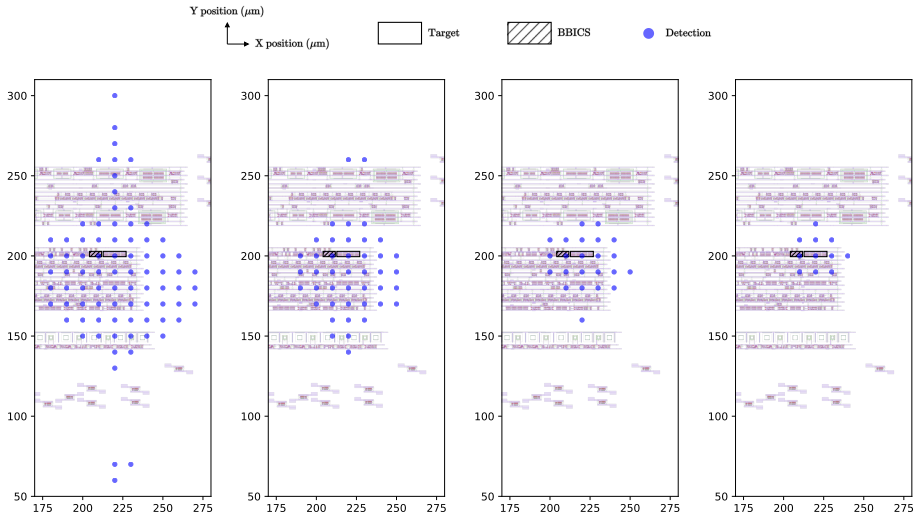
Cell	DFF				buffer			
Pulse duration	50ns		30ps		50ns		30ps	
Spot diameter	5 μm	1 μm	5 μm	1 μm	5 μm	1 μm	5 μm	1 μm
Fault injection threshold	1.9 W	**1.7 W**	5 nJ	**2 nJ**	2.1 W	-	5 nJ	3 nJ

The fault threshold for the buffer cell has been investigated by observation of faults in the reset tree. That is to say the considered logic has high fanout capacitance and might not be representative of dense logic. Faults injection thresholds were only established for non-monitored Dual-Well targets. However, [6] presents a comparison of fault threshold for targets in Dual-Well and Triple-Well indicating a halved fault threshold for Triple-Well DFF i.e. a higher LFI sensitivity compared to their Dual-Well counterpart.

5.2 BBICS Detection of Nanosecond Range LFI

Our first experiments were carried out using nanosecond-range laser pulse duration. Figure 6 reports the detection area of the Dual-Well test structure (shown

in Fig. 5a) for a 50 ns laser pulse and with a spot size of 5 μm at various laser power (from 1.7 W down to 0.1 W).



(a) Power = 1.7 W (b) Power = 0.7 W (c) Power = 0.3 W (d) Power = 0.1 W

Fig. 6: Single BBICS LFI detection map for a Dual-Well target (20 inverters) at various power (50 ns pulse duration, 5 μm spot diameter).

The monitored test pattern was fully contained within the BBICS detection area for all tested parameters, indicating a reliable LFI detection below the fault injection threshold (down to 0.1 W). Table 3 reports the BBICS detection range and extent for various laser power (estimated from arbitrarily defined inlier points). At 1.7 W, which is below the DFF fault threshold (1.9 W for the chosen set of laser parameters), the detection area is 7,000 μm^2, which significantly exceeds the monitored logic area (40 μm^2) for a BBICS area overhead of 22 μm^2. This high LFI detection capability is in line with the results of [28].

Table 3: BBICS detection range and area for 50 ns laser pulses.

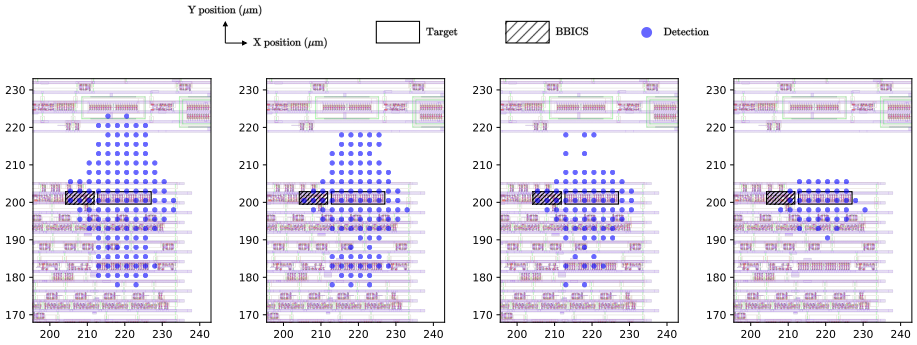
Laser power (W)	**1.7**	0.7	0.3	0.1
Detection area (μm^2)	**7,000**	4,100	2,200	1,100
X extent (μm)	90	70	50	40
Y extent (μm)	100	90	50	40

Detection areas have an uneven shape. This can be attributed to two competing phenomena. Firstly, the difference in photocurrent generation depending on the laser spot location, favoring regions dense in strongly biased PN junctions

(where laser-induced bulk currents appear). Secondly, the presence (or not) of bulk biasing taps competing with those monitored by the BBICS. At high laser power, outlier detection points also appear. Their location overlaps with the large metal paths of the PDN, possibly indicating a laser reflection toward the monitored pattern.

5.3 BBICS Detection of Picosecond Range LFI

Further experiments were performed using a picosecond range laser pulse duration: 30 ps which is a fixed value linked to the used laser source. Figure 7 reports the detection area of the same Dual-Well test structure (shown in Fig. 5a) for a spot size of 1 μm at various laser energy (from 0.5 nJ to 2 nJ).



(a) Energy = 2 nJ (b) Energy = 1.5 nJ (c) Energy= 1nJ (d) Energy = 0.5 nJ

Fig. 7: Single BBICS LFI detection map for a Dual-Well target (20 inverters) at various laser energy (30 ps pulse duration, 1 μm spot diameter).

The monitored test pattern was still fully contained within the BBICS detection area for all tested laser parameters. Table 4 reports the BBICS detection range and extent for various laser energy. At 2 nJ, which is equal to the DFF fault injection threshold for this set of laser parameters, the detection area is 819 μm^2, which still significantly exceeds the monitored logic area (40 μm^2) for a BBICS area overhead of 22 μm^2.

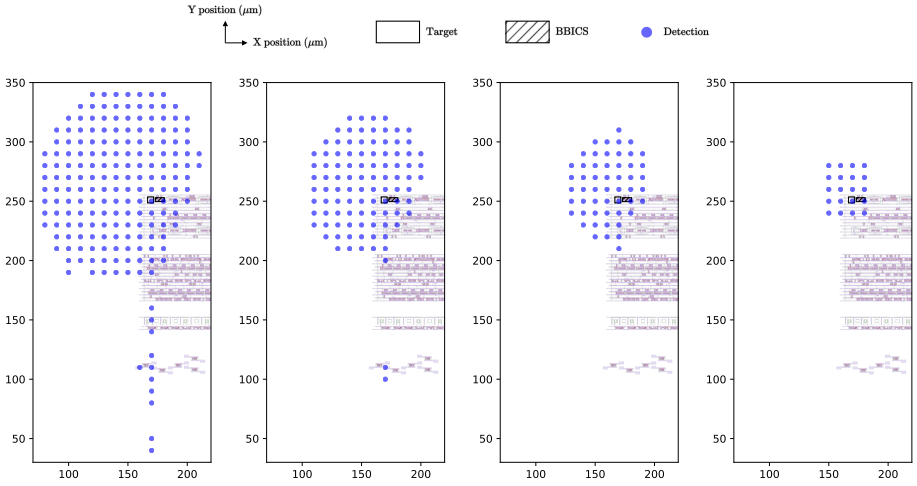
Table 4: BBICS detection range and area for 30 ps laser pulses.

Laser energy (nJ)	**2**	1.5	1	0.5
Detection area (μm^2)	**819**	656	406	219
X extent (μm)	30	28	28	20
Y extent (μm)	45	40	20	15

5.4 Triple-Well BBICS Detection Assessment

The previously described set of experiments was also carried out on the Triple-Well test structure (shown in Fig. 5b). Figure 8 reports the obtained LFI detection results for a pulse width of 50 ns whereas Figure 9 provides the detection maps for 30 ps pulses. Note that the "target" label represented in these figures refers to the N_{well} represented in Fig. 5b.

For the sake of relevance, it is to be noted that Triple-Well implementations yield different fault thresholds than their Dual-Well counterparts. As no Triple-Well fault thresholds were observed (due to the lack of a dedicated test structure on our test vehicle), we followed a conservative approach and considered a fault injection threshold of half that of a Dual-Well technology implementation (based on experiments presented in [6]).



(a) Power = 1.7 W (b) Power = 0.7 W (c) Power = 0.3 W (d) Power = 0.1 W

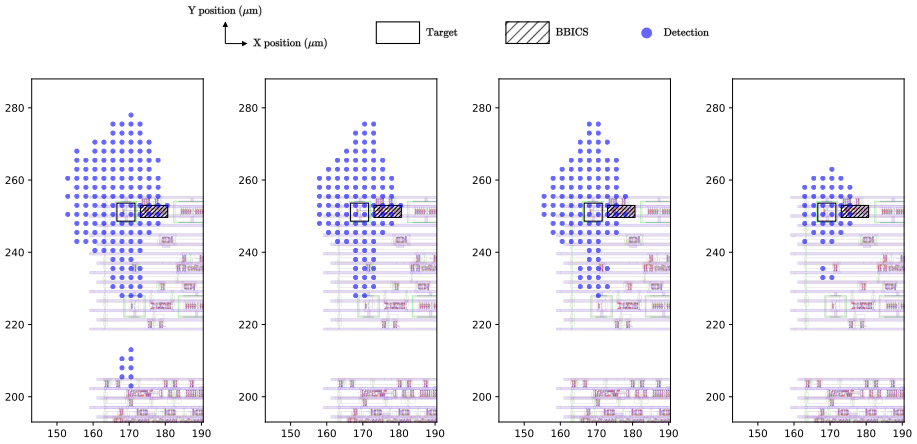
Fig. 8: Single BBICS LFI detection map for a Triple-Well target (a single inverter) at different laser power (50 ns pulse duration, 5 μm spot diameter).

The results plotted in Fig. 8 and summarized in Table 5 show large detection areas clearly stretching towards a logic-free area. At 0.7 W, below the estimated fault injection threshold (0.85 W) for a DFF Triple-Well implementation, the detection area is 9,500 μm^2. This outmatches the Dual-Well test structure detection area (4,100 μm^2 at 0.7 W) even though the monitored target area is smaller (25 μm^2).

Outlier detection points are present for higher powers as mentioned in Section 5.2. They also overlap with the metal layer tracks in Fig. 8a but only with a high drive buffering cell in Fig. 8b.

Table 5: BBICS detection range and area for 50 ns laser pulses.

Laser power (W)	1.7	**0.7**	0.3	0.1
Detection area (μm^2)	17,700	**9,500**	5,300	2,000
X extent (μm)	130	90	70	40
Y extent (μm)	160	120	100	50



(a) Energy = 2 nJ (b) Energy = 1.5 nJ (c) Energy = 1 nJ (d) Energy = 0.5 nJ

Fig. 9: Single BBICS LFI detection map for a Triple-Well target (a single inverter) at different laser energy (30 ps pulse duration, 1 μm spot diameter).

The detection areas reported for picosecond-range pulses in Fig. 9 are noticeably smaller and less asymmetrical. Although, the detection ranges feature a remarkable Y extent for high energy pulses, they remain relatively centered on the X axis compared to ranges associated to nanosecond-range pulses. Table 6 indicates a detection range of 638 μm^2 at the estimated Triple-Well DFF fault threshold (1 nJ), covering the entire target area (25 μm^2).

Table 6: BBICS detection range and area for 30 ps laser pulses.

Laser energy (nJ)	2	1.5	**1**	0.5
detection area (μm^2)	900	681	**638**	256
X extent (μm)	25	23	23	15
Y extent (μm)	53	50	48	23

6 Discussion on the Obtained Results

In this paper, we proposed an experimental characterization of the LFI detection capability of the Single BBICS architecture. A comparison between Dual-Well and Triple-Well monitoring was realized to complement existing results [6]. Furthermore, testing with 30 ps pulses demonstrated the BBICS capability in monitoring logic against such pulses, extending the state-of-the-art.

6.1 Coverage Analysis

Nanosecond-range pulses (with a spot diameter of 5 μm) revealed large detection areas for Dual-Well monitoring, supporting the results of previous studies [6,28]. Our experiments were carried out for laser powers down to 0.1 W ($\times$17 smaller than the reported Dual-Well DFF fault threshold), revealing an unprecedented detection threshold. In addition, contrarily to what was previously reported in the state-of-the art [6], the Single BBICS proved to be able to monitor a Triple-Well test pattern with an efficiency superior than for a Dual-Well target (confirming the intuition of [19]).

Although, the reported detection ranges for 30 ps laser pulses (at 1 μm spot diameter) are significantly smaller than for nanosecond-range laser pulses (at 5 μm spot size), BBICS were found to be able to fully monitor their target area. Experiments revealed a detection coverage even below the fault threshold, down to 0.5 nJ ($\times$4 smaller than the Dual-Well DFF fault threshold). The overall decrease of detection range compared to 50 ns pulses was expected according to the model proposed in [16]. Indeed, it anticipates a more localized photocurrent generation (in PN junctions) range around the laser spot focus point.

Reference fault thresholds reported in Section 5.1 were obtained by studying non-monitored Dual-Well logic. Although the reported fault thresholds constitute an important comparative indicator of BBICS efficiency, previous results [22,31] indicate that further research is needed to assess the impact of BBICS monitoring on SEE sensitivity.

6.2 Test Chip Specific Phenomena

Nanosecond-range pulse testing of our Triple-Well test structure exhibits a notable asymmetry of the detection area. As shown in Fig. 8, its shape extends significantly more in the logic-free area located to the left and above our test element than towards its right and below, where Dual-Well logic elements are located. An explanation of this behavior could be that the surrounding Dual-Well logic junctions collect a significant portion of the laser-induced charge carriers, thus reducing the amount of photocurrent captured at the Triple-Well biasing contacts. In contrast, some of the charge carriers induced in the logic free area can travel to the Triple-Well logic and be detected. This could explain the larger detection range we report compared to [6]. Unfortunately, we do not have access to the layout used in [6] to verify our assumption. This observed asymmetry is not present for picosecond-range pulses.

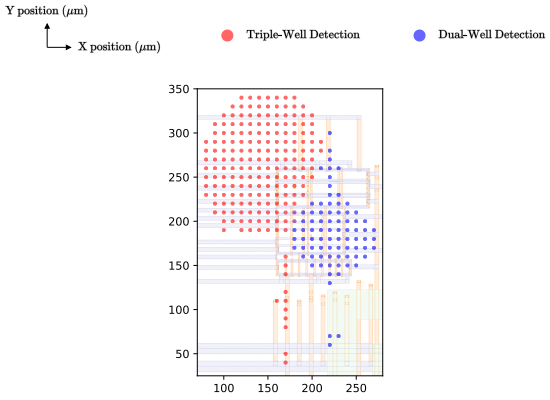


Fig. 10: Detection maps from Fig.6a and Fig.8a reported on metal layers layout.

At high power of nanosecond-range pulses, several outlier detection points aligning with the metal tracks were observed. This phenomenon is illustrated in Figure 10 where BBICS detection areas are overlaid on a layout showing the upper metal paths. Our assumption is that of a laser reflection on these metal paths toward the monitored pattern. We emphasize that the studied test chip is not representative of an actual industrial integrated circuit, the metal density above the test pattern was kept low during design to allow for frontside laser testing (though we only report on backside LFI). This phenomenon would be worth investigating as a circuit with a high density of metal lines and tiles may favor LFI detection due to similar laser beam reflection and scattering.

7 Conclusion

This research work provides an experimental characterization of the LFI detection capabilities of a Single BBICS sensor embedded in a 65 nm CMOS technology test chip. Tests were conducted on both Dual-Well and Triple-Well CMOS logic targets with pulse durations ranging from nanoseconds to picoseconds. We also report on the first laser picosecond-range pulse testing of a BBICS monitoring targets made of actual logic gates. The three main contribution of our work are as follows.

First, the observed BBICS efficiency in detecting nanosecond-range laser pulses in Dual-Well logic is consistent with the state-of-the-art results [28]. A large detection range of approximately 100 μm at a laser power below the LFI threshold was obtained. This further confirms the interest of using BBICS sensors to detect LFI.

Second, our nanosecond-range LFI experiments carried out on a Triple-Well test pattern revealed large detection areas, which extend significantly beyond the monitored target. This constitutes a reversal of the current experimental state-of-the-art [6] that reported a detection area failing to cover the whole monitored

test element. Our experiment-based results validate that using BBICS to monitor Triple-Well logic is fully efficient [19].

Third, the efficiency of BBICS in monitoring picosecond-range laser pulses was not ascertained on actual logic gates. In fact, [27] underlined that picosecond-range pulses come with a reduced effect area with respect to nanosecond-range ones. This could have resulted in an impaired BBICS detection area. Our experimental results prove this doubt wrong as 30 ps laser pulses were fully detected when targeting both Dual-well and Triple-well targets. The test patterns were fully enclosed into the detection area that also extended significantly beyond them.

All our experiments revealed an exhaustive coverage of the monitored area for all used laser parameters and test structures. At laser power or energy corresponding to the LFI threshold, the coverage significantly exceeds the targets area. This constitutes a strong indicator of BBICS robustness in detecting LFI.

References

1. Aghaie, A., Moradi, A., Rasoolzadeh, S., Shahmirzadi, A.R., Schellenberg, F., Schneider, T.: Impeccable circuits. Cryptology ePrint Archive, Paper 2018/203 (2018)
2. Barenghi, A., Breveglieri, L., Koren, I., Naccache, D.: Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. Proceedings of the IEEE **100**(11), 3056–3076 (2012)
3. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Kaliski, B.S. (ed.) Advances in Cryptology — CRYPTO '97. pp. 513–525. Springer Berlin Heidelberg, Berlin, Heidelberg (1997)
4. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults. In: Fumy, W. (ed.) Advances in Cryptology — EUROCRYPT '97. pp. 37–51. Springer Berlin Heidelberg, Berlin, Heidelberg (1997)
5. Borrel, N., Champeix, C., Kussener, E., Rahajandraibe, W., Lisart, M., Sarafianos, A.: Electrical model of a pmos body biased structure in triple-well technology under pulsed photoelectric laser stimulation. In: 2015 IEEE 22nd International Symposium on the Physical and Failure Analysis of Integrated Circuits. pp. 134–137 (2015)
6. Borrel, N., Champeix, C., Kussener, E., Rahajandraibe, W., Lisart, M., Sarafianos, A., Dutertre, J.M.: Influence of triple-well technology on laser fault injection and laser sensor efficiency. In: 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). pp. 85–90 (2015)
7. Borrel, N., Champeix, C., Lisart, M., Sarafianos, A., Kussener, E., Rahajandraibe, W., Dutertre, J.M.: Electrical model of an nmos body biased structure in triple-well technology under photoelectric laser stimulation. In: 2015 IEEE International Reliability Physics Symposium. pp. FA.1.1–FA.1.6 (2015)
8. Borrel, N., Champeix, C., Kussener, E., Rahajandraibe, W., Lisart, M., Dutertre, J.M., Sarafianos, A.: Characterization and simulation of a body biased structure in triple-well technology under pulsed photoelectric laser stimulation. vol. 2014 (11 2014)
9. Bringer, J., Carlet, C., Chabanne, H., Guilley, S., Maghrebi, H.: Orthogonal direct sum masking: A smartcard friendly computation paradigm in a code, with builtin

protection against side-channel and fault attacks. Cryptology ePrint Archive, Paper 2014/665 (2014)
10. Buchner, S.P., Wilson, D., Kang, K., Gill, D., Mazer, J.A., Raburn, W.D., Campbell, A.B., Knudson, A.R.: Laser simulation of single event upsets. IEEE Transactions on Nuclear Science **34**(6), 1227–1233 (1987)
11. Buchner, S.P., Miller, F., Pouget, V., McMorrow, D.P.: Pulsed-laser testing for single-event effects investigations. IEEE Transactions on Nuclear Science **60**(3), 1852–1875 (2013)
12. Carlet, C., Daif, A., Guilley, S., Tavernier, C.: A masking method based on orthonormal spaces, protecting several bytes against both SCA and FIA with a reduced cost. Cryptology ePrint Archive, Paper 2023/1746 (2023)
13. Carlet, C., Daif, A., Guilley, S., Tavernier, C.: Quasi-linear masking against SCA and FIA, with cost amortization. IACR Transactions on Cryptographic Hardware and Embedded Systems **2024**(1), 398–432 (Dec 2023)
14. Champeix, C., Dutertre, J.M., Pouget, V., Robisson, B., Lisart, M., Borrel, N., Sarafianos, A.: Laser testing of a double-access bbics architecture with improved see detection capabilities. In: 2016 16th European Conference on Radiation and Its Effects on Components and Systems (RADECS). pp. 1–4 (2016)
15. Champeix, C., Borrel, N., Dutertre, J.M., Robisson, B., Lisart, M., Sarafianos, A.: Experimental validation of a bulk built-in current sensor for detecting laser-induced currents. In: 2015 IEEE 21st International On-Line Testing Symposium (IOLTS). pp. 150–155 (2015)
16. Da Cruz, W.S., Viera, R., Rigaud, J.B., Hubert, G., Dutertre, J.M.: An experimentally tuned compact electrical model for laser fault injection simulation. In: 2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS). pp. 1–5 (2022)
17. Dobraunig, C., Eichlseder, M., Korak, T., Mangard, S., Mendel, F., Primas, R.: SIFA: Exploiting ineffective fault inductions on symmetric cryptography. Cryptology ePrint Archive, Paper 2018/071 (2018)
18. Doulcier-Verdier, M., Dutertre, J.M., Fournier, J., Rigaud, J.B., Robisson, B., Tria, A.: A side-channel and fault-attack resistant AES circuit working on duplicated complemented values. In: 2011 IEEE International Solid-State Circuits Conference. pp. 274–276 (2011)
19. Dutertre, J.M., Bastos, R.P., Potin, O., Flottes, M., Rouzeyre, B., Natale, G.D., Sarafianos, A.: Improving the ability of bulk built-in current sensors to detect single event effects by using triple-well CMOS. Microelectronics Reliability **54**(9-10), 2289 – 2294 (2014)
20. Dutertre, J.M., Beroulle, V., Candelier, P., De Castro, S., Faber, L.B., Flottes, M.L., Gendrier, P., Hély, D., Leveugle, R., Maistri, P., Di Natale, G., Papadimitriou, A., Rouzeyre, B.: Laser fault injection at the CMOS 28 nm technology node: an analysis of the fault model. In: 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). pp. 1–6 (2018)
21. Ebrahimabadi, M., Mehjabin, S.S., Viera, R., Guilley, S., Danger, J.L., Dutertre, J.M., Karimi, N.: Detecting laser fault injection attacks via time-to-digital converter sensors. In: 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). pp. 97–100 (2022)
22. Gasiot, G., Giot, D., Roche, P.: Multiple cell upsets as the key contribution to the total SER of 65 nm CMOS SRAMs and its dependence on well engineering. IEEE Transactions on Nuclear Science **54**(6), 2468–2473 (2007)

23. Habing, D.H.: The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. IEEE Transactions on Nuclear Science **12**(5), 91–100 (1965)
24. Johnston, A.: Charge generation and collection in p-n junctions excited with pulsed infrared lasers. IEEE Transactions on Nuclear Science **40**(6), 1694–1702 (1993)
25. Khuat, V., Danger, J.L., Dutertre, J.M.: Laser fault injection in a 32-bit microcontroller: from the flash interface to the execution pipeline. In: 2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC). pp. 74–85 (2021)
26. Kumar, R., Varna, A.L., Tokunaga, C., Taneja, S., De, V., Mathew, S.K.: A 100-gbps fault-injection attack-resistant AES-256 engine with 99.1%–99.99% error coverage in intel 4 CMOS. IEEE Journal of Solid-State Circuits **59**(1), 79–89 (2024)
27. Lacruche, M., Borrel, N., Champeix, C., Roscian, C., Sarafianos, A., Rigaud, J.B., Dutertre, J.M., Kussener, E.: Laser fault injection into sram cells: Picosecond versus nanosecond pulses. In: 2015 IEEE 21st International On-Line Testing Symposium (IOLTS). pp. 13–18 (2015)
28. Matsuda, K., Fujii, T., Shoji, N., Sugawara, T., Sakiyama, K., Hayashi, Y.I., Nagata, M., Miura, N.: A 286 f2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor. IEEE Journal of Solid-State Circuits **53**(11), 3174–3182 (2018)
29. Matsuda, K., Miura, N., Nagata, M., Hayashi, Y.i., Fujii, T., Sakiyama, K.: On-chip substrate-bounce monitoring for laser-fault countermeasure. In: 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST). pp. 1–6 (2016)
30. Neto, E.H., Kastensmidt, F.L., Wirth, G.I.: Tbulk-bics: A built-in current sensor robust to process and temperature variations for set detection. In: 2007 9th European Conference on Radiation and Its Effects on Components and Systems. pp. 1–8 (2007)
31. Neto, E., Ribeiro, I., Vieira, M., Wirth, G., Kastensmidt, F.: Using bulk built-in current sensors to detect soft errors. IEEE Micro **26**(5), 10–18 (2006)
32. Possamai Bastos, R., Guimarães, L.A., Sill Torres, F., Fesquet, L.: Architectures of bulk built-in current sensors for detection of transient faults in integrated circuits. Microelectronics Journal **71**, 70–79 (2018)
33. Rabii, H., Neumeier, Y., Keren, O.: High rate robust codes with low implementation complexity. IEEE Transactions on Dependable and Secure Computing **16**(3), 511–520 (2019)
34. Richter, A.K., Arimura, I.: Simulation of heavy charged particle tracks using focused laser beams. IEEE Transactions on Nuclear Science **34**(6), 1234–1239 (1987)
35. Sarafianos, A., Gagliano, O., Lisart, M., Serradeil, V., Dutertre, J.M., Tria, A.: Building the electrical model of the pulsed photoelectric laser stimulation of a pmos transistor in 90nm technology. In: Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA). pp. 22–27 (2013)
36. Sarafianos, A., Gagliano, O., Serradeil, V., Lisart, M., Dutertre, J.M., Tria, A.: Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology. In: 2013 IEEE International Reliability Physics Symposium (IRPS). pp. 5B.5.1–5B.5.9 (2013)
37. Sarafianos, A., Lisart, M., Gagliano, O., Serradeil, V., Roscian, C., Dutertre, J.M., Tria, A.: Robustness improvement of an sram cell against laser-induced fault injection. In: 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). pp. 149–154 (2013)

38. Sill Torres, F., Possamai Bastos, R.: Robust Modular Bulk Built-In Current Sensors for Detection of Transient Faults. In: SBCCI'2012: 25th Symposium onIntegrated Circuits and Systems Design. pp. 1–6. Brasilia, Brazil (Aug 2012)
39. Simionovski, A., Wirth, G.I.: A bulk built-in current sensor for set detection with dynamic memory cell. In: 2012 IEEE 3rd Latin American Symposium on Circuits and Systems (LASCAS). pp. 1–4 (2012)
40. Skorobogatov, S.P., Anderson, R.J.: Optical fault induction attacks. In: Kaliski, B.S., Koç, ç.K., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2002. pp. 2–12. Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
41. Viera, R.A.C., Maurine, P., Dutertre, J.M., Possamai Bastos, R.: Simulation and experimental demonstration of the importance of ir-drops during laser fault injection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **39**(6), 1231–1244 (2020)
42. Zhang, Z., Wang, T., Chen, L., Yang, J.: A new bulk built-in current sensing circuit for single-event transient detection. In: CCECE 2010. pp. 1–4 (2010)
43. Zooker, D., Weizman, Y., Fish, A., Keren, O.: Silicon proven 1.29 μm $\times$ 1.8 μm 65nm sub-vt optical sensor for hardware security applications. IEEE Access **11**, 136269–136278 (2023)