IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 November 2023, accepted 25 November 2023, date of publication 30 November 2023,
date of current version 8 December 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3338001*

RESEARCH ARTICLE

# Silicon Proven 1.29 μm × 1.8 μm 65nm Sub-Vt Optical Sensor for Hardware Security Applications

**DAVID ZOOKER, YOAV WEIZMAN, (Member, IEEE), ALEXANDER FISH, (Member, IEEE), AND OSNAT KEREN**

Faculty of Engineering, Bar-Ilan University, Ramat Gan 5290002, Israel

Corresponding author: David Zooker (david.zooker@biu.ac.il)

The work of Alexander Fish was supported by the Israel Science Foundation under Grant 2511/20. The work of Osnat Keren was supported by the Israel Science Foundation under Grant 1266/20.

**ABSTRACT** Optical fault injection is a type of attack vector targeting cryptographic circuits where the adversary injects faults during system operation to bypass defenses or reveal secret information. Since preventing this kind of attack is generally impractical, most known countermeasures focus on indirect (logic based) or direct detection. Indirect detection mechanisms monitor the effects of optical fault injections in a circuit, whereas direct sensors track the illumination itself. In this paper, we present a compact $1.29\mu\text{m}\times1.8\mu\text{m}$ direct optical sensor implemented in 65nm CMOS technology located inside the digital logic fabric. Because it is based on standard CMOS technology, it can be implemented using standard design flow. Measurements on four dedicated chips showed high sensitivity to fault injection attacks: the sensor was 2 to 6 times more sensitive than the combinational logic it protects. As a result of the sub-Vt operation of the transistors, these sensors exhibited post-attack self-recovery ability and high reliability, with a false positive rate under PVT of less than $\mathbf{10}^{-7}$.

**INDEX TERMS** Direct sensor, hardware security, laser fault injection, optical sensor.

## I. INTRODUCTION

Cryptographic modules implemented in hardware can be targeted by fault injection attacks where the adversary injects faults into the system to obtain secret information from the malfunctioning device [1], [2], [3]. Some fault injection methods involve the use of optical techniques such as a high-end laser [4], [5], [6], [7]. The advantage of a focused laser beam when combined with a precision stage is that it can locally illuminate the integrated circuit (IC), which unlike other attack methods translates into the ability to inject faults at high resolution (Laser Fault Injection (LFI)).

LFI attacks are proven to be effective in several attack scenarios. For example, a straightforward attack uses LFI to bypass the Personal Identification Number (PIN) check on a smartcard. In this scenario the laser targets the microprocessor's core at a precise time frame [7], [8]. A more complex attack involves injecting faults into a block cipher (such as AES) at a specific round during encryption and using differential fault analysis (DFA) to recover the secret key [9], [10]. These two attack scenarios require both spatial and temporal precision.

As photons with sufficient energy hit the depletion region (or doped regions near the depletion region) of a p-n junction, charge carriers are generated and are immediately torn apart by the electric field such that the electrons are shunted to the n-type side, and the holes to the p-type side. The excess electron-hole pairs forward biases the p-n junction, thus creating a *photocurrent* [11], [12], [13]. Fig. 1 illustrates this mechanism in the case of a simple CMOS inverter. A laser beam with sufficient energy that strikes the drain p-n junction of a MOSFET can induce a photocurrent that alters the node's voltage [14].

The associate editor coordinating the review of this manuscript and approving it for publication was Leandros Maglaras.

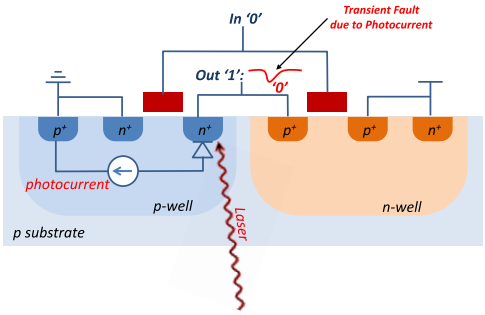


**FIGURE 1.** Laser Fault Injection (LFI) mechanism in the case of a simple CMOS inverter.

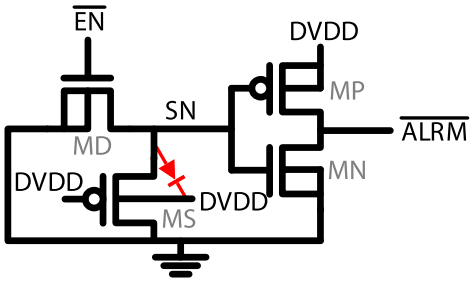


**FIGURE 2.** Proposed 4-Transistor Optical Sensor (4tOS).

A LFI can be carried out through the front, back or the sides of the silicon [15]. There are numerous countermeasures aimed at the *prevention* of this type of attack. Although protecting the front side is straightforward and can be done at the packaging stage (using metal mesh) or during the standard physical design (dense metal fill [16]), protecting the back is more complex. Recent studies have suggested using non-standard fabrication processes such as Through-Silicon Via (TSV) [17] (which creates cavities inside the silicon to weaken the structure, thus hindering the ability of the adversary to decapsulate and thin out the die) and Backside Buried Metal (BBM) [18], [19], [20] (which is a kind of Cu mesh buried inside the silicon during the last fabrication step). To date, the most typical LFI approach is via the back, since it is the hardest to protect. Although mechanical protection methods can help, they are less attractive because they require non-standard fabrication.

A different (and orthogonal) approach is the *detection* of a LFI. The failure can be detected in real time or after the fault has manifested itself as an error in the computation. In general, detection-based countermeasures can be divided into two types with respect to the logic they protect: *Indirect* and *Direct* detectors.

*Indirect detectors* detect the faults or errors in the circuit under protection. These detectors can be implemented at the algorithm level and all the way down to the circuit level. Online algorithm-level detectors utilize redundant hardware either to infect the circuit's output in the presence of a fault, or to detect an erroneous input and/or output to the circuit [21], [22]. In the latter case, checkers for linear and non-linear error detection codes need to be implemented in hardware. In general, non-linear codes are more suitable against a sophisticated attacker. For example the robust codes in [22], [23] are non-linear codes with deterministic encoding that can detect *every error*, whereas the codes in [24], [25], [26], and [27] are codes with random encoding whose security properties depend on the entropy of the random portion.

Bulk built-in detectors [28], [29] are also indirect detectors; these are circuit-level detectors that detect abnormal currents in the bulk during fault injection and thus have the ability to detect the fault even before it manifests as an error in the computation.

The main drawback of these indirect detectors is that they are designed to sense a fault on the data path and thus leak information. Since the manifestation of a fault depends on the state of the logic gate under attack (Fig. 1), the adversary can monitor the response of the system to the attack (whether the alarm was raised or not), and depending on the response, probe the output of the logic gate indirectly (using Side Channel Analysis (SCA)) to acquire information [30], [31], [32].

*Direct detectors* can detect a LFI immediately when the laser hits them or in their vicinity. Thus, they can be implemented alongside the logic. This type of detector consists mainly of optical and digital sensors [33], [34], [35], [36], [37]. By nature, they generally provide lower coverage than indirect detectors. However, because they are implemented independently of the system, they do not leak information on the data path. In addition, they can be easily ported between systems, without much design overhead or reliability issues.

In [33] the authors described both direct and indirect detectors, where the indirect detectors were intended mainly for other types of fault injection (such as undervoltage attacks), and the direct detectors (noted as *Laser Detection Circuit (LDC)*) were designed for the detection of LFI. The LDC units were built from six standard-cell inverters, a NOR and a NAND, to collect the charge created by the laser and amplify the resulting pulse.

Another approach consists of creating new standard library cells that incorporate the detectors. In [34] the authors suggested incorporating reverse-biased transistors (which act as photodiodes) inside the logic cells to protect against Laser Voltage Probing (*LVP*), a kind of laser attack that requires less laser energy and thus more sensitive sensors.

In this paper we present a novel sensor dubbed "4tOS" (short for 4-Transistor Optical Sensor). This direct, *compact* photodiode sensor is based on a standard CMOS MOSFET that can be implemented in a *standard flow* without alteration of the standard cells or the backend. The sensor is *standalone*; i.e., it produces a digital alarm signal without any additional logic, and offers *high sensitivity* and *self recovery* after an attack due to its operation in the sub-Vt region.

The sensor was implemented in standard 65nm CMOS technology and tested under Laser Fault Injection (LFI).

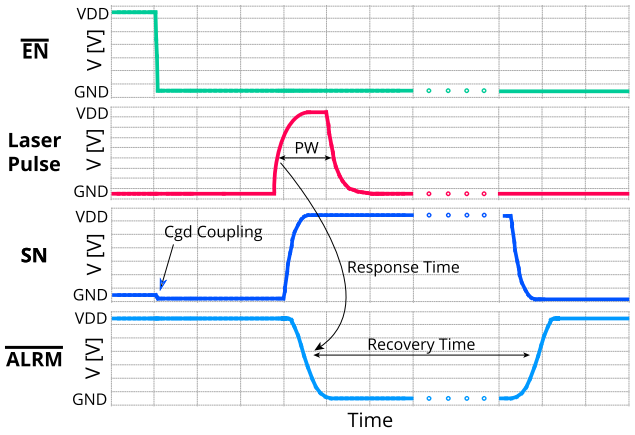


**FIGURE 3.** Operation of 4tOS.

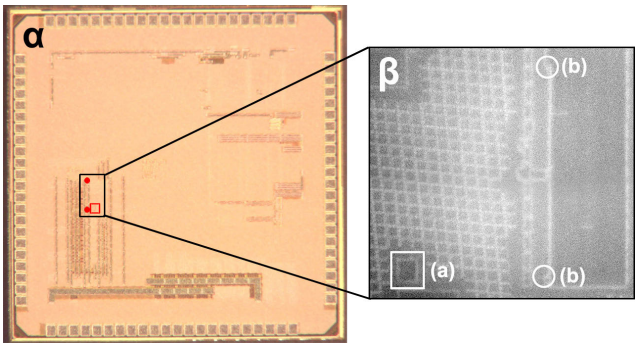


**FIGURE 4.** At the left (α) shows a microscope photo of the chip. At the right (β) shows a photo of the sensors taken from the backside using the laser system. The sensors were implemented in two ways: (a) a sensor array of 4 × 3 sensors, or (b) two asynchronous sensors.

The sensor's efficiency was on a par with the results of the pre-silicon simulation of this sensor reported in [38].

The remainder of the paper is organized as follows. Section II provides a brief description of the sensor, and Section III describes the experimental setup for the measurements. Section IV presents the results of the experiments. Section V compares the proposed sensor to state-of-the-art publications, and Section VI concludes the paper.

## II. THE 4-TRANSISTOR OPTICAL SENSOR

The 4tOS concept was first introduced in our previous paper [38]. It is depicted in Fig. 2. It consists of two NMOS transistors and two PMOS transistors. The voltage at the *Sensing Node* (SN) indicates whether the circuit is under attack or not. Fig. 3 depicts the sensor operation. First, in order to reset the sensor, the SN needs to be discharged. This is achieved by assigning '1' (VDD) to the active-low $\overline{EN}$ signal. Since the *MD* transistor is an NMOS, SN is discharged to the ground, and the alarm signal $\overline{ALRM}$ is pulled HIGH. Then, $\overline{EN}$ is lowered to '0' (GND), SN is slightly discharged a bit below the ground (due to coupling between the gate and the drain), which in turn keeps the inverter (which consists of MP and MN transistors) gates stable. The steady-state voltage at the SN node is mainly determined by subthreshold leakages of the MD and MS transistors, which tend to discharge the node to the ground. At this stage the diode between the bulk of the MS and its Source is in reverse bias, and acts as a photodiode.

When an adversary illuminates the sensor with a laser beam at a defined pulse width (*PW*), the photons hit the p-n junction (photodiode) between the Bulk and the Source of MS, generating a photocurrent, which in turn charges the SN. If the photocurrent is high enough, the voltage at the SN will exceed the switching threshold of the inverter, and will flip its output $\overline{ALRM}$ to low voltage ('0'). The time elapsed between laser illumination and the flipping of the $\overline{ALRM}$ is termed the *Response Time*, which is calculated as 50% of the laser pulse and 50% of the falling $\overline{ALRM}$ signal.

When the sensor is enabled ($\overline{EN}$ is pulled LOW), MD and MS conduct in the sub-threshold region. Because of this low conduction, the SN is close to floating, so that the sensor presents high sensitivity with a fast response time compared to a standard CMOS logic gate. In a regular CMOS gate such as an inverter (Fig. 1), the induced photocurrent makes an attempt to discharge the drain node through the NMOS' bulk, while the open PMOS is still "fighting" to charge it. This explains the need for a substantial photocurrent to enable a successful attack.

After the laser pulse, the SN slowly discharges through MD and MS. This period is termed the *Recovery Time* $t_{RT}$. During this period, the system needs to capture the alarm state. At the end of the recovery time the sensor returns to an enabled state (ready to sense a future attack). The recovery time is expressed as 50% of the falling $\overline{ALRM}$ signal and 50% of its rising.

As described above, the 4tOS is a direct sensor that monitors optical illumination by using the MOSFET as a photodiode. The novelty of this sensor lies in its sensitivity (resulting from its sub-Vt operation), size, reliability and ability to be easily implemented inside the logic fabric without impacting the reliability of the logic or requiring a non-standard design flow. Section V compares the 4tOS to other state-of-the-art sensors (both direct and indirect).

## III. EXPERIMENTAL SETUP

The 4tOS was designed and fabricated in standard 65nm CMOS technology. The MS, MD and MN transistors were set to have a minimum size, whereas the MP was double the minimum.

Fig. 4 shows a microscope photo of the fabricated chip (α) on the left and an enlargement of the area of the sensors taken from the back of the die using the imaging function of the laser system (β) on the right. The sensors were implemented in two forms:

- An array of 12 sensors (Fig. 4(a)). All the sensor outputs were sampled in a register that was later read to observe their status. The array size was 5.46 $\mu$m × 7.2 $\mu$m.
- Two (asynchronous) sensors, as shown in Fig. 4(b), were placed near a cryptographic function. The outputs of these sensors were directly connected (without being

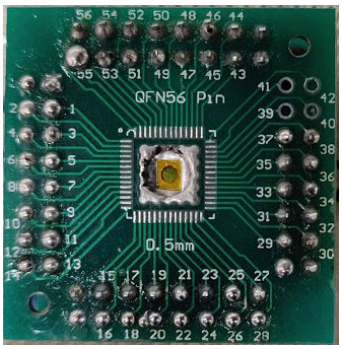


**FIGURE 5.** DUT with the round cutout to reveal the back side of the silicon.

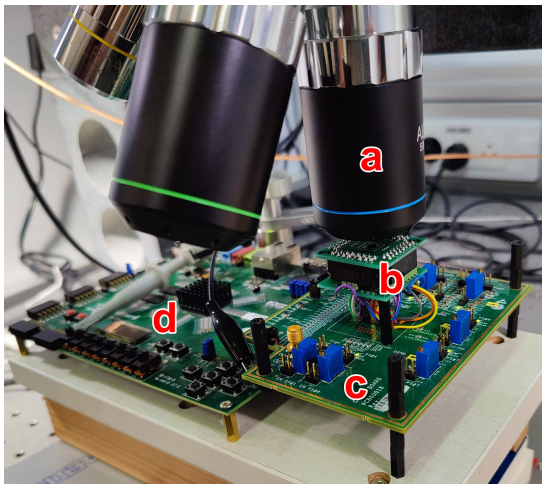


**FIGURE 6.** Measurement Setup. The laser beam illuminates the DUT through a 50X lens (a). The DUT (b) is connected to a custom adapter (c) for voltage control. A Zedboard FPGA (d) is used as a host to control and communicate with the DUT.

sampled) to the chip's IO to allow observation of their temporal behavior. The size of each sensor was $1.29\,\mu\text{m} \times 1.8\,\mu\text{m}$.

Most of the measurements presented in this paper were conducted on the asynchronous sensors, whereas the sensor array was measured mainly for testing the coverage.

The fabricated chip was set in a standard QFN64 package, with a round cutout in the metal plate to reveal the back of the silicon. The package was then mounted on a brakeout board, again with a hole to reveal the die (Fig. 5). In total we had 4 chips for measurements, labeled A to D.

This setup was then mounted on an adapter and connected to a host FPGA for control signals and readout (Fig. 6).

Laser illumination was performed using an ALPhANOV fault injection system. The laser wavelength was $1064nm$. At $1064nm$ the silicon is partly transparent to the laser beam, which means that it lets the laser beam penetrate the back of the die while generating the electron-hole pairs.

The laser's spot size was set to a minimum of $0.76\,\mu\text{m}$ using the largest (x50) objective to obtain the maximum power concentration. This is also an adversary's most likely configuration since it provides the most accuracy.

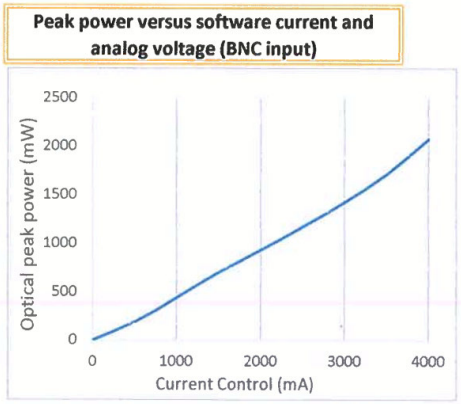


**FIGURE 7.** ALPhANOV Power/Current measurement at a pulse width of 100ns and pulse frequency of 100KHz, based on the manufacturer's specifications [39].

**TABLE 1.** Setup parameters.

| Parameter | Value |
|---|---|
| Technology | 65 nm |
| Sensor size | $1.29 \times 1.8\,\mu\text{m}$ |
| Spot diameter | $0.76\,\mu\text{m}$ |
| Wave length | $1064nm$ |
| Pulse frequency | $10KHz$ |
| Pulse width | Up to $100ns$ |
| Laser current ($I$) | Up to $1400mA$ |
| # Tested chips | 4 |
| # Tested sensors | 8 |
| # Tests per sensor | $65K$ |

The laser was set to pulsed operation, and the sensors were measured using various pulse widths $PW$ and powers. The laser power was controlled by varying the amount of current provided to the diode. The manufacturer's specifications state that the relationship between the optical power and the laser current during a typical operation of a 100 ns pulse width is about half, as can be seen in Fig. 7. The setup parameters are summarized in Table 1.

The pulse frequency was set at $10KHz$ so that the time period (delta) between the pulses would be longer than the recovery time (shown in Section IV-B). Each sensor was measured about $65K$ times for the sensing probability analysis, each time at various pulse widths (from $5ns$ to $100ns$) and various laser currents (up to $400mA$ for the sensors, and up to $1400mA$ for the combinational logic).

## IV. RESULTS AND DISCUSSION

The typical response of the sensor to LFI is shown in Fig. 8. Specifically, an asynchronous sensor was measured (sensor 1 on chip B) using a laser beam with typical parameters (a pulse width of $PW = 100ns$ and a laser current of $I = 200mA$). The full dynamics of the laser and the sensor can be seen in the bottom plot, whereas the two top plots zoom into sections of the bottom. The figure shows the response of the sensor output $\overline{ALRM}$ to the laser pulse (with a typical

**TABLE 2.** Sensor evaluation metrics.

| Metric | Definition | Results |
|---|---|---|
| Absolute Sensitivity | $P_{sensor}(detect\|I, PW)$ | Fig. 9 |
| Relative Sensitivity | $I_{laser}(P_{bit-flip} \approx 0)/I_{laser}(P_{detection} = 1)$ | Section IV-A, Fig. 9,10 |
| Response time | $t_{RSP}$ | Section IV-B, Fig. 8 |
| Recovery time | $t_{RCV}$ | Table III, Fig. 11 |
| Coverage | Min. Distance [ µm] | Fig. 12 |
| False alarm | $P_{sensor}(falsealarm)$ | Section IV-D |
| Robustness | $P_{sensor}(detect)$, $t_{RCV}$ | Fig. 13 |

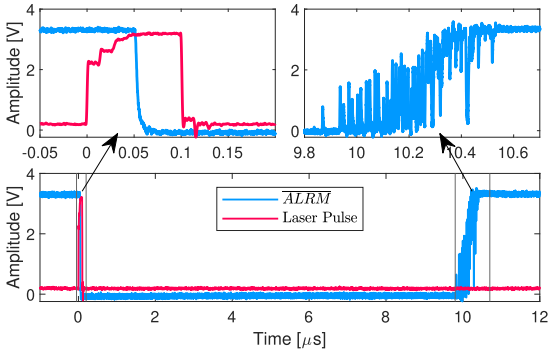


**FIGURE 8.** Typical operation of sensor 1 on chip B. The laser pulse width is $PW = 100ns$ and the laser current is $I = 200mA$.

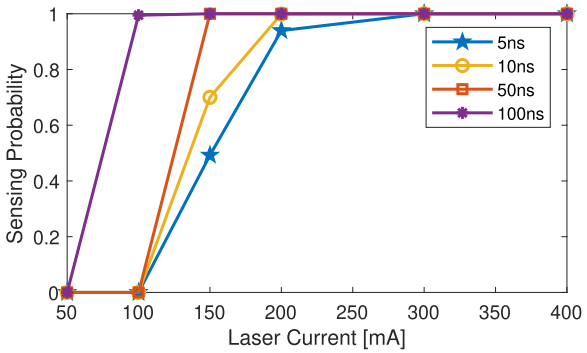


**FIGURE 9.** Probability $P_{sensor}(detect)$ of sensor 2 on chip D to sense various laser pulse widths at increasing laser current.

response time of $\sim 50ns$), along with the expected recovery after $\sim 10\mu s$. The return to the idle state of the sensor was not monotonic because the voltage on the *SN* drove the output inverter to a meta-stable state.

The effectiveness of the sensor was evaluated based on several metrics as detailed in Table 2.

### A. ABSOLUTE AND RELATIVE SENSITIVITY

The most important metric is the *absolute sensor sensitivity* for a given laser current $I$ and pulse width $PW$; i.e., the probability of detecting LFI at different laser currents. Formally, $P_{sensor}(detect|I, PW)$ is the ratio of the number of tests in which the $\overline{ALRM}(t) = 0$ at $t < t_{RCV}$ to the total number of tests. The probability of sensing LFI for a given laser current was evaluated on the asynchronous sensors.

Fig. 9 shows the probability that a single sensor (sensor 2 of chip D) could sense (for a minimum spot size of $0.76\mu m$) pulses of widths ranging from $5ns$ to $100ns$ as a function of the laser current. It is clear from the figure that wider pulses were detected with higher probability. Moreover, the sensor reliably sensed LFI at a low laser current of about $300mA$ for all pulse widths, which was expected due to the nature of the sensor.

However, the absolute sensitivity in and of itself is not sufficient for evaluating the sensor's effectiveness; instead, it needs to be compared to the sensitivity of the logic it aims to protect. This sensitivity is referred to as the *Relative Sensitivity RS*.

To achieve high sensing reliability, the sensor must be triggered at a lower laser current than the logic it is trying to protect. Here, to measure the sensitivity of the logic, a combinational block was targeted with the same laser parameters and was routed to the same asynchronous IO as used by the sensor. The reference block we chose consisted mainly of MUX and buffers since they provide a good example of CMOS logic.

Fig. 10 shows the response of the combinational logic to the laser pulse. The top plot shows the response at the output for a typical laser pulse with a width of $PW = 100ns$ and a laser current of $I = 1400mA$. The bottom plot shows the probability of flipping the output of the combinational block for different laser pulses at increasing laser currents. The measurements were made on Chip A. The results were similar on different chips and showed that the minimum laser current needed to cause a temporal bit-flip was around $600mA$ to $800mA$ at a laser pulse of $100ns$, whereas short pulses of $5ns$ and $10ns$ did not impact the combinational logic in this power range. Moreover, the flip duration was dramatically shorter than $t_{RT}$, ranging from $20ns$ to $30ns$.

In general, the number of bit flips that will (always) be detected by an error detection code (EDC) depends on the Hamming distance between legal output combinations. Since even a single bit flip is sufficient for detection, the number of bit flips is not a factor. Hence, we defined the *sensitivity ratio* for detection as the ratio of the probability that the sensor would respond (detect) to the probability that at least one bit flip would occur for a given laser current (at a typical pulse width of $PW = 100ns$):

$$\frac{P_{sensor}(\text{detect}|I, PW = 100ns)}{P_{logic}(\text{bit flips occurred}|I, PW = 100ns)}$$

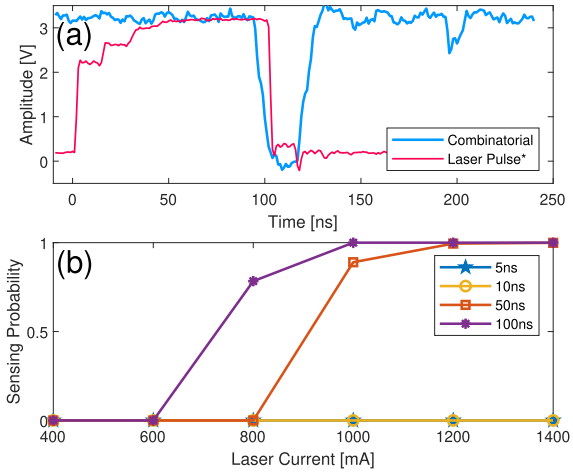


**FIGURE 10.** (a) The response of the combinational circuit on chip A to a laser pulse with $PW = 100ns$ and a laser current of $1400mA$. *Laser plot is estimated. (b) Typical flip probability $P_{logic}(bit\ flip|I, PW)$ of the same block for different laser pulses at different currents.

This is a good candidate metric for the relative sensitivity; however, the results showed that the sensors and the logic responded to two distinct regions of the laser current, which made the probability ratio infinite (e.g. for a laser current of $I = 150mA$ the sensing probability is 1 while the bit flip probability is 0).

Another approach is to measure the *threshold current ratio* $R_{TC}$; i.e., the ratio of the minimal laser current at which a detection occurs (with a conservative probability of 1 for all laser pulses) to the minimal laser current at which a bit flip occurs (with a conservative probability of near 0 for a typical laser pulse of $PW = 100ns$):

$$R_{TC} = \frac{I_{laser}(P_{detection} = 1|PW = 100ns)}{I_{laser}(P_{bit-flip} \approx 0|PW = 100ns)}$$

Finally, to quantify the greater sensitivity of the 4tOS over the logic it protects, we defined the *Relative Sensitivity* as

$$RS = \frac{1}{R_{TC}}$$

thus the *conservative* relative sensitivity is

$$RS = \frac{1}{R_{TC}} = \frac{600mA}{300mA} = 2$$

In terms of less conservative values (the results showed that the sensor detected the $100ns$ pulse width with a laser current of $100mA$ almost 100% of the time), this figure was found to reach $RS \approx 6$. This means that the sensors' sensitivity was 2 to 6 times higher than the CMOS logic they were protecting.

### B. RESPONSE AND RECOVERY TIME

Another important metric is the *response time* $t_{RSP}$. A short response time is critical to ensure that the sensor triggers immediately. The $\overline{ALRM}$ signal of the sensor is asynchronous. Its response is immediate when the SN node is charged by the photocurrent, such that the response time is comparable

**TABLE 3.** Minimum recovery time for different sensors.

| Chip | Sensor # | $\min(t_{RCV})$ |
|---|---|---|
| A | 1 | 1.9 µs |
| A | 2 | 44 µs |
| B | 1 | 10 µs |
| B | 2 | 6.8 µs |
| C | 1 | 11 µs |
| C | 2 | 3.4 µs |
| D | 1 | 6.7 µs |
| D | 2 | 21 µs |

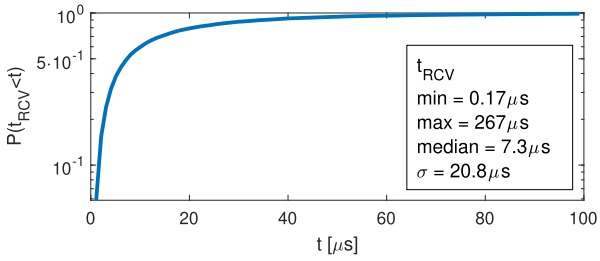


**FIGURE 11.** 8000-point monte carlo simulation on the post-layout implementation of the 4tOS. The plot shows the probability that the recovery time $t_{RCV}$ will be smaller than $t$, as shown on the horizontal axis, with additional values of $t_{RCV}$.

to the response time of the logic under attack. The exact response time cannot be easily measured since the signal passes through several logic gates and IO cells, but is typically in the nano-second range. Fig. 8 shows a typical $t_{RSP} \approx 50ns$ including external delays.

The *recovery time* $t_{RCV}$ of the sensor was defined as the pulse width of $\overline{ALRM}$. This interval needs to be long enough for the signal to be registered. When an adversary injects current into the parasitic diode of MS and charges SN, both MD and MS will try to discharge the node. Based on the structure of the sensor, when the $\overline{EN}$ is pulled low, the SN node is "pulled" slightly towards 0 because of the sub-vt operation of MD and MS (Fig. 2). This produces a "recovery" mechanism, where after the attack, the sensor returns to the enabled state.

The fact that the recovery time was determined by the sub-vt operation of the transistors resulted in large variations in $t_{RCV}$ due to inter- and intra-chip process variations. A total of 8 sensors were measured on 4 different chips using typical laser parameters ($PW = 100ns$, $I = 200mA$), and the worst case $t_{RCV}$ was calculated over $65K$ cycles. The results are shown in Table 3. These results suggest that the recovery time was sufficient to safely sample the $\overline{ALRM}$ signal during an attack, since the system clock is usually fast ($> 10$ MHz). The sub-vt operation ensured the reliability of the sensor, because it eventually discharged SN to the ground and prevented it from staying in a meta-stable state.

To further study the variances in $t_{RCV}$ we ran a 8000-point Monte Carlo simulation on the post-layout implementation of the 4tOS. Fig. 11 shows the probability that the recovery time $t_{RCV}$ will be smaller than $t$, as depicted on the horizontal axis

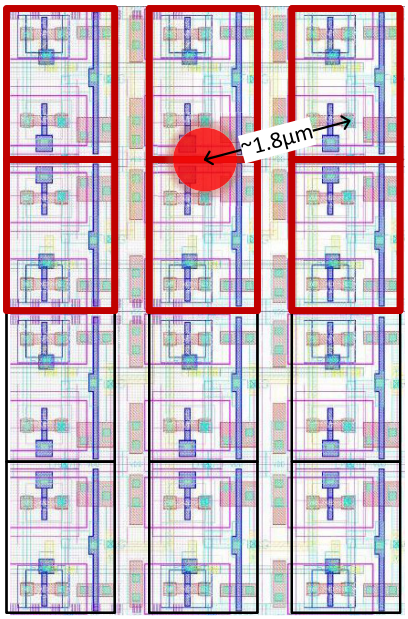


**FIGURE 12.** The plot shows the laser spot compared to the sensor array (a layout view for convenience) to scale. The laser location was estimated. The sensors that detected the illumination are highlighted. The arrows show the maximum distance between the center of the laser beam to the farthest sensor that detected the beam. The measurements were made on chip B.

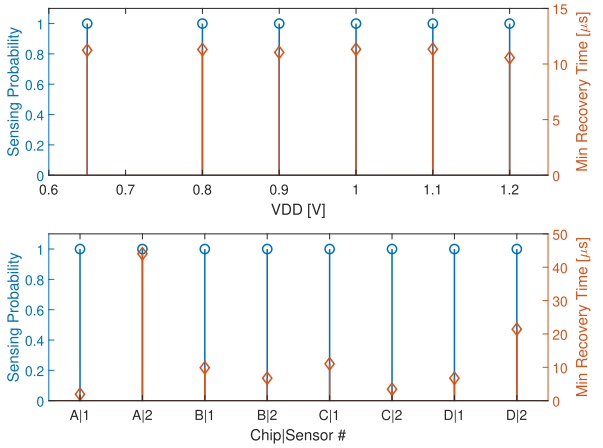


**FIGURE 13.** The top plot shows the sensing probability and minimum recovery time of sensor 1 of chip B for different supply voltages. The bottom plot shows the sensing probability and minimum recovery time for different inter- and intra-chip sensors @VDD = 1.2V (as described in Table 3).

with additional values of $t_{RCV}$. The graph indicates that the variance was fairly large mainly due to process variations that affected the sub-Vt leakage. However, while the minimum $t_{RCV}$ was $\sim 0.16\mu s$, 99% of the samples were over $\sim 0.5\mu s$ and 95% were over $\sim 1\mu s$. On the other hand, a long recovery time did not affect the operation of the sensor since it has an $\overline{EN}$ signal for reset.

### C. SENSOR COVERAGE

Since the sensors were relatively small and could easily be embedded within the design, we measured their *coverage zone*. The coverage zone was defined as the number of sensors that could detect a single laser pulse. This provided an estimate of the distribution needed to protect a circuit.

To measure the coverage of the sensors, the laser was set to the minimum spot size (0.76 $\mu$m) and a typical laser current of 200$mA$ (for high sensing probability). The laser was fired periodically at a fixed spot (chosen randomly) inside the sensor array of chip B. By marking the sensors that detected the illumination, a coverage map was produced, as depicted in Fig. 12. It shows that six sensors responded to the laser illumination. A conservative estimate of the laser spot indicated that the maximum distance between the center of the laser beam and a sensor diode was about $1.8\mu m$.

### D. ROBUSTNESS AND RELIABILITY

To test the robustness of the sensors, several sensors were measured across different chips and a single sensor (sensor 1 of chip B) was measured across varying supply voltages. The laser pulse was set to a typical 100$ns$ width with a 200$mA$ current. Fig. 13 shows that the probability of detection was not affected by the supply voltage or process variations for a typical injection setup. The minimum recovery time $t_{RCV}$ was also not affected by the different supply voltages, but varied under process variations, as was shown in Table 3.

Finally, we examined the *reliability* of the sensor in terms of false alarms $P_{sensor}(falsealarm)$. Multiple sensors on multiple dies were measured under various voltages and temperatures (PVTs) during normal system operation (cryptographic functions) for long periods of time. No false positives were detected. Specifically, various asynchronous sensors (Fig. 4) were measured from various chips and several asynchronous sensors were measured with a supply voltage ranging from 0.65V to 1.3V and at temperatures ranging from $-10°C$ to $80°C$. The typical frequency of the system clock was 30MHz, and the sensors were measured for $10^9$ clock cycles. The results showed no false positives during this time frame, thus indicating that $P_{sensor}(falsealarm) \ll 10^{-7}$.

## V. COMPARISON TO PREVIOUS WORKS

Table 4 presents the results of a comparison of the 4tOS to three state-of-the-art works. Much like the sensor presented in this paper, the sensors in both [33] and [34] relied on the voltage change at the transistor diffusion node caused by the photocurrent, whereas [28] was focused on sensing the current at the bulk node. However, 4tOS exploited the sub-vt operation to make the sensor compact, sensitive and endowed it with a self-recovery feature.

While both the 4tOS and [33] were implemented alongside the logic and did not affect it during the design process, [28] required a special backend design for the bulk sensors, and [34] suggested a new library of std-cells that integrated the detection mechanism as part of the cell.

**TABLE 4. Comparison to previous work.**

| Parameter | **This Work** | [28] | [33]* | [34] |
|---|---|---|---|---|
| Technology | 65nm | 180nm | Intel 4 | 28nm |
| Sensor Type | sub-Vt photodiode | BBICS | std-cell INV | photodiode |
| Detection | Direct | Indirect | Direct | Direct |
| Custom Design of Logic | **NO** | YES | NO | YES |
| Target Attack | LFI | LFI | LFI | LFI & LVP |
| Relative Sensitivity | $\sim 2$ | $\sim 2.33$ | $\sim 1$ | $\sim 18$ |
| Response Time | 50ns*** | 2ns | NA | 6ms**** |
| Sensor Area** | $\sim$ **2** | $\sim 5$ | 1 | 2 |
| Performance Overhead | **0%** | 6.8% | 0% | 0% |

*Only compared to the direct optical sensor. **Compared to a typical inverter gate in the technology. ***Including external delay. ****Including external delay, for Laser Voltage Probing attack.

To compare the sensitivity of the sensors, we calculated the relative sensitivity as described in Section IV-A. Based on the results reported in [28], the minimum laser energy for fault injection was $4.2nJ$ whereas the minimum energy for detection was $1.8nJ$ (in the worst position), so that the relative sensitivity was about 2.33. In [33] the authors did not provide explicit results for sensor sensitivity, but based on their architecture, the sensitivity was likely to be comparable to the logic it protects. In [34] the authors measured sensitivity for a practical Laser Voltage Probing (LVP) attack, and showed that the minimum laser power for detection was $7mW$ whereas the *typical* laser power for an attack was $125mW$, which yielded a relative sensitivity of about 18.

The response time of the 4tOS to the LFI was measured externally, that is, between the trigger of the laser pulse and the response to the alarm signal on the chip pad. This means that external delays are added to the measurement, resulting in a total response time of 50ns. In [28] the authors integrated logic inside the die to measure the response time and measured an internal response time of $2ns$ from the illumination to the response of the system. In [33] the authors did not report the response time, and in [34] the authors reported that the internal response time was $\sim 400\mu s$, while the response time including external delays (additional logic) was 6ms (in this work the measurement was carried out only for the LVP attack). While it was challenging to measure the response time under uniform conditions, it can be seen that the response time of the 4tOS is in the range of tens of nanoseconds and should be comparable to the sensor of [33] (based on its structure).

The area of 4tOS is about 2 inverters, and is a standalone sensor, which means it produces a digital alarm signal that can then be used to trigger a response mechanism. In [28] the authors stated that the area of the backend part of the sensor is about 2.6 NAND2s (or about 5 inverters), but that there is an additional frontend part shared with several backend circuits, so that its area is not significant. In [33] a single sensing unit is a single inverter, but it is part of a larger *Laser Detection Unit (LDC)* which comprises six inverters, a NOR and a NAND, which eventually produces the alarm signal.

Finally, in [34] the authors stated that the protected inverter in their library was the size of two regular inverters, and that an additional detection cell was used to obtain the response of several individual sensing cells.

## VI. CONCLUSION

This paper presented a compact and standalone optical sensor against Laser Fault Injection (LFI) that can be implemented alongside the cryptographic function without altering the standard design flow. Depending on specific chip measurements, the sensor is 2 to 6 times more sensitive than the neighboring combinational logic (which is the target of LFI), and has a self-recovery feature where it returns to its ready state several microseconds after the laser hits (which is plenty of time for the system to respond). Using a sensor array, the coverage measurements achieved a minimum pitch of $1.8\mu m$. Exhaustive testing showed a negligible probability of false positives.

As was described, the main advantage of the 4tOS is the fact that it is compact, standalone, and can be implemented in a conventional CMOS process using standard design flow. However, these come at the expense of non-uniformity of the recovery time due to process variations, sensitivity and response time. Further research suggests separating the back-end of the sensor (MS, see Fig. 2) and the front-end (MD, MP, MN), and connecting several back-end units to one front-end. This can potentially improve the area, coverage, and uniformity of the recovery time.

As was shown, the simplicity and small size of the 4tOS make it a promising solution for LFI hardware security applications. However, future research will also evaluate the efficiency of the sensor under electromagnetic (EM) injection attacks [40], as the sensor response under both LFI and EM attacks (injected currents) should be similar.

## REFERENCES

[1] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1997, pp. 37–51.
[2] J. Breier and X. Hou, "How practical are fault injection attacks, really?" *IEEE Access*, vol. 10, pp. 113122–113130, 2022.

[3] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012.

[4] L. Lavdas, M. T. Rahman, and N. Asadizanjani, "Application of optical techniques to hardware assurance," in *Emerging Topics in Hardware Security*, M. Tehranipoor, Ed. Cham, Switzerland: Springer, 2021, pp. 471–491.

[5] D. Karaklajic, J.-M. Schmidt, and I. Verbauwhede, "Hardware Designer's guide to fault attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 12, pp. 2295–2306, Dec. 2013.

[6] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2002, pp. 2–12.

[7] J. G. J. van Woudenberg, M. F. Witteman, and F. Menarini, "Practical optical fault injection on secure microcontrollers," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr.*, Sep. 2011, pp. 91–99.

[8] A. Gangolli, Q. H. Mahmoud, and A. Azim, "A systematic review of fault injection attacks on IoT systems," *Electronics*, vol. 11, no. 13, p. 2023, Jun. 2022.

[9] C. Roscian, J.-M. Dutertre, and A. Tria, "Frontside laser fault injection on cryptosystems—Application to the AES' last round," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2013, pp. 119–124.

[10] C. Giraud, "DFA on AES," in *Proc. Int. Conf. Adv. Encryption Standard*, Bonn, Germany, May 2004, pp. 27–41.

[11] A. K. W. Chee, "Quantitative dopant profiling by energy filtering in the scanning electron microscope," *IEEE Trans. Device Mater. Rel.*, vol. 16, no. 2, pp. 138–148, Jun. 2016.

[12] A. K. Chee, "The mechanistic determination of doping contrast from Fermi level pinned surfaces in the scanning electron microscope using energy-filtered imaging and calculated potential distributions," *Microsc. Microanal.*, vol. 28, no. 5, pp. 1538–1549, Oct. 2022.

[13] C. Dervos, P. Skafidas, J. Mergos, and P. Vassiliou, "P-n junction photocurrent modelling evaluation under optical and electrical excitation," *Sensors*, vol. 4, no. 5, pp. 58–70, Jul. 2004.

[14] 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 *Proc. 9th IEEE Int. Conf. Design Technol. Integr. Syst. Nanosc. Era (DTIS)*, May 2014, pp. 1–6.

[15] J. Rodriguez, A. Baldomero, V. Montilla, and J. Mujal, "LLFI: Lateral laser fault injection attack," in *Proc. Workshop Fault Diagnosis Tolerance Cryptography (FDTC)*, Aug. 2019, pp. 41–47.

[16] D. Petryk, Z. Dyka, J. Katzer, and P. Langendörfer, "Metal fillers as potential low cost countermeasure against optical fault injection attacks," in *Proc. IEEE East-West Design Test Symp. (EWDTS)*, Sep. 2020, pp. 1–6.

[17] S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Cledière, R. Wacquez, J. Fournier, J.-C. Souriau, G. Simon, and A. Merle, "A novel structure for backside protection against physical attacks on secure chips or SiP," in *Proc. IEEE 68th Electron. Compon. Technol. Conf. (ECTC)*, May 2018, pp. 515–520.

[18] T. Miki, M. Nagata, H. Sonoda, N. Miura, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, and K. Kikuchi, "A Si-backside protection circuits against physical security attacks on flip-chip devices," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2019, pp. 25–28.

[19] K. Monta, H. Sonoda, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, K. Kikuchi, N. Miura, T. Miki, and M. Nagata, "3-D CMOS chip stacking for security ICs featuring backside buried metal power delivery networks with distributed capacitance," *IEEE Trans. Electron Devices*, vol. 68, no. 4, pp. 2077–2082, Apr. 2021.

[20] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for IC chip level hardware security," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 1, pp. 5–14, Jan. 2022.

[21] A. Baksi, D. Saha, and S. Sarkar, "To infect or not to infect: A critical analysis of infective countermeasures in fault attacks," *J. Cryptograph. Eng.*, vol. 10, no. 4, pp. 355–374, Nov. 2020.

[22] M. G. Karpovsky, K. J. Kulikowski, and Z. Wang, "Robust error detection in communication and computational channels," in *Proc. Spectral Methods Multirate Signal Process. SMMSP Int. Workshop*. Princeton, NJ, USA: Citeseer, 2007, pp. 1–15.

[23] H. Rabii, Y. Neumeier, and O. Keren, "High rate robust codes with low implementation complexity," *IEEE Trans. Depend. Secure Comput.*, vol. 16, no. 3, pp. 511–520, May 2019, doi: 10.1109/TDSC.2018.2816638.

[24] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," in *Advances in Cryptology—EUROCRYPT 2008*. Cham, Switzerland: Springer, 2008, pp. 471–488.

[25] M. Karpovsky and Z. Wang, "Design of strongly secure communication and computation channels by nonlinear error detecting codes," *IEEE Trans. Comput.*, vol. 63, no. 11, pp. 2716–2728, Nov. 2014.

[26] X. T. Ngo, S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "Linear complementary dual code improvement to strengthen encoded circuit against hardware trojan horses," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Washington, DC, USA, May 2015, pp. 82–87.

[27] S. Dziembowski, K. Pietrzak, and D. Wichs, "Non-malleable codes," *J. ACM*, vol. 65, no. 4, pp. 1–32, 2018.

[28] K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y.-I. Hayashi, M. Nagata, and N. Miura, "A 286 F2/Cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor," *IEEE J. Solid-State Circuits*, vol. 53, no. 11, pp. 3174–3182, Nov. 2018.

[29] K. Matsuda, S. Tada, M. Nagata, Y. Komano, Y. Li, T. Sugawara, M. Iwamoto, K. Ohta, K. Sakiyama, and N. Miura, "An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density," *Jpn. J. Appl. Phys.*, vol. 59, no. SG, Apr. 2020, Art. no. SGGL02.

[30] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, and R. Primas, "SIFA: Exploiting ineffective fault inductions on symmetric cryptography," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2018, pp. 547–572, Aug. 2018.

[31] T. Sugawara, N. Shoji, K. Sakiyama, K. Matsuda, N. Miura, and M. Nagata, "Side-channel leakage from sensor-based countermeasures against fault injection attack," *Microelectron. J.*, vol. 90, pp. 63–71, Aug. 2019.

[32] Y. Li, R. Hatano, S. Tada, K. Matsuda, N. Miura, T. Sugawara, and K. Sakiyama, "Side-channel leakage of alarm signal for a bulk-current-based laser sensor," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, Nanjing, China, Dec. 2019, pp. 346–361.

[33] R. Kumar, A. Varna, C. Tokunaga, S. Taneja, V. De, and S. Mathew, "15.5 A 100 Gbps fault-injection attack resistant AES-256 engine with 99.1-to-99.99% error coverage in Intel 4 CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2023, pp. 1–3.

[34] H. Zhang, L. Lin, Q. Fang, and M. Alioto, "Laser voltage probing attack detection with 100% area/time coverage at above/below the bandgap wavelength and fully-automated design," *IEEE J. Solid-State Circuits*, vol. 58, no. 10, pp. 2919–2930, 2023, doi: 10.1109/JSSC.2023.3274596.

[35] F. Lu, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Customized cell detector for laser-induced-fault detection," in *Proc. IEEE 20th Int. On-Line Test. Symp. (IOLTS)*, Jul. 2014, pp. 37–42.

[36] D. El-Baze, J.-B. Rigaud, and P. Maurine, "An embedded digital sensor against EM and BB fault injection," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr. (FDTC)*, Aug. 2016, pp. 78–86.

[37] W. He, J. Breier, and S. Bhasin, "Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks," in *Proc. Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.* Cham, Switzerland: Springer, 2016, pp. 27–46.

[38] D. Zooker, A. Fish, O. Keren, and Y. Weizman, "Compact sub-Vt optical sensor for the detection of fault injection in hardware security applications," in *Proc. 10th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Jun. 2019, pp. 1–5.

[39] *Test Report PDM HPP*, Alphanov, Talence, France, Jun. 2020.

[40] F. Poucheret, K. Tobich, M. Lisarty, L. Chusseauz, B. Robissonx, and P. Maurine, "Local and direct EM injection of power into CMOS integrated circuits," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr.*, Sep. 2011, pp. 100–104.

**DAVID ZOOKER** received the B.Sc. and M.Sc. degrees in electrical engineering from Bar-Ilan University, Israel, in 2016 and 2018, respectively, where he is currently pursuing the Ph.D. degree.

His current research interests include hardware security (power analysis countermeasures, RNGs, and optical sensors) in various abstraction levels: from the transistors level to the software level, from full custom to EDA tools, from design, layout, and simulations to chip measurements.

**YOAV WEIZMAN** (Member, IEEE) received the Ph.D. degree in physics from Ben-Gurion University.

He has over 20 years of experience in basic and applied research, development, and design. In 2000, he joined Freescale Semiconductor, Herzelia, where he was involved in the development of tools and techniques for IC diagnostics and later he became the Product Analysis and Characterization Manager leading research activities in failure analysis, signal integrity, and special IC diagnostics structures for yield enhancement and process tuning. In 2013, he joined Bar Ilan University as a Research Fellow and he is involved since in numerous studies of IC reliability, circuit methods to mitigate HW tempering, and eavesdropping. He also developed several unique approaches for PUF and RNG implementations, which were implemented successfully in test chips. He has published over 50 articles and 16 patents.

**ALEXANDER FISH** (Member, IEEE) received the B.Sc. degree in electrical engineering from the Technion—Israel Institute of Technology, Haifa, Israel, in 1999, and the M.Sc. and Ph.D. (summa cum laude) degrees from Ben-Gurion University (BGU), Israel, in 2002 and 2006, respectively.

He was a Postdoctoral Fellow with the ATIPS Laboratory, University of Calgary, Canada, from 2006 to 2008. In 2008, he joined Ben-Gurion University as a Faculty Member with the Electrical and Computer Engineering Department. There he founded the Low Power Circuits and Systems (LPC&S) Laboratory, specializing in low power circuits and systems. In July 2011, he was appointed as the Head of the VLSI Systems Center, BGU. In October 2012, he joined Bar-Ilan University, Faculty of Engineering, as an Associate Professor and the Head of the Nanoelectronics Track. In March 2015, he founded Emerging Nanoscaled Integrated Circuits and Systems (ENICS) Laboratories. Currently, he is a Full Professor and the Co-Director of the EnICS Impact Center at Bar-Ilan University, Faculty of Engineering. He has authored over 190 scientific papers in journals and conferences. He also submitted more than 30 patent applications of which 22 were granted. He has published three book chapters and two books as an editor. His research interests include power reduction methodologies for high speed digital and mixed signal VLSI chips, energy efficient SRAM and eDRAM memory arrays, CMOS image sensors and biomedical circuits, systems, and applications, and cryogenic CMOS circuits.

Prof. Fish is a member of the Technical Committee of the European Solid-State Circuits Conference. He is also a member of the VLSI Systems and Applications and Bio-Medical Systems Technical Committees of IEEE Circuits and Systems Society. He also served as the program chair and the chair of different tracks for various IEEE conferences. He was a Co-Organizer of many special sessions at IEEE conferences, including IEEE ISCAS, IEEE Sensors, and IEEEI conferences. He founded and served as an Editor-in-Chief for the *Journal of Low Power Electronics and Applications* (JLPEA) (MDPI), from 2012 to 2018, and he was an associate editor of IEEE various journals. He is also an Associate Editor of IEEE Access journal, *Microelectronics Journal* (Elsevier), and *Integration, the VLSI Journal* (Elsevier).

**OSNAT KEREN** received the M.Sc. degree in electrical engineering from the Technion—Israel Institute of Technology, in 1988, and the Ph.D. degree from Tel-Aviv University, Israel, in 1999. Between 1988 and 1994, she held a chip design and senior DSP engineer position with National Semiconductor, and between 1999 and 2003, she was the Chief Scientist with Millimetrix Broadband Networks. Since 2004, she has been with the Faculty of Engineering, Bar-Ilan University, Israel. Her current research interests include coding theory, hardware security, spectral methods in logic design, and countermeasures against invasive and non-invasive side channel attacks.