Detecting Failures and Attacks via Digital Sensors

Md Toufiq Hasan Anik, *Graduate Student Member, IEEE*, Jean-Luc Danger, *Member, IEEE*, Sylvain Guilley, *Member, IEEE*, and Naghmeh Karimi, *Member, IEEE*

***Abstract*—Detection of abnormal behaviors is essential in complex and/or strategic systems requiring a high level of safety and security. Sensing environmental conditions to ensure that the device is not operating out-of-specifications is highly useful in detecting anomalies caused by failures or malevolent actions. In this regard, digital sensors (DSs) are particularly attractive as they are portable and can be easily calibrated. In contrast to analog sensors, DSs have an interesting property that considers the operating environmental conditions as a whole, i.e., they are sensitive to temperature, voltage, and process altogether, without precise knowledge about each. This property endows DSs with fewer false positives compared to analog sensors. This article studies a low-cost DS, discusses its presilicon architecture and post-silicon calibration such that it detects system failures accurately in the designer's preferable range of operating conditions. The impact of aging in this sensor is studied extensively. Tradeoffs between false positive and undetection rates are discussed. As an example, we target the substitution box (S-Box) of the PRESENT cipher assuming that it can be the target of fault injection attacks launched via abruptly changing the operating temperature and voltage. We show that such malfunction can be accurately detected by our DS, i.e., with a very negligible percentage of false and missed alarms (<1% totally). The results show that the number of false alarms raises with aging (while the rate is highly negligible), whereas the number of missed alarms remains at a reasonable low rate.**

***Index Terms*—Aging, detection accuracy, digital sensor (DS), false positives (type I errors), missed alarms (type II errors), PRESENT, process–voltage–temperature (PVT), substitution box (S-Box).**

I. Introduction

SENSING environmental conditions, such as *temperature* and *voltage*, is highly useful for embedded systems as such sensing not only can help in optimizing system performance depending on operational conditions but also can be essential for safety and security in order to prevent failures or detect attacks. It is necessary to equip mission-critical chips with sensors raising alarms when the chips are operated out-of-specifications caused either by the harsh environments or by physical attacks. Reaction to a raised alarm is a logical action that reflects the safety/security policy in place. *Analog* sensors have been deployed for a long time in this respect but they encounter several issues including.

1) Their calibration is not obvious, and may require costly *laser trimming* on a chip-by-chip basis.
2) Their adaption to either a new technological node or even to a version of the physical design kit (PDK) library requires an extensive recalibration.

Digital sensors (DS) provide portability among digital technologies and can be distributed in the circuit die such that they are placed physically close to sensitive areas, like cryptographic cores which can be the target of attacks. This increases the sensing accuracy. In practice, the sensitivity of sensing-related failure detection could be wrecked havoc by aging which becomes significant in recent CMOS technologies. Thereby, it is highly crucial to design DSs that can accurately detect system's malfunctions during its expected lifetime span, i.e., the sensor outcome should be robust against aging.

This article presents a methodology to design an aging-resilient DS. In this article, by designing we mean how to dimension a DS structure presilicon, and configure it post-silicon (by software), thereby tolerating process variability. We target a sensor placed near[1] a substitution box (S-Box) part of a PRESENT cipher algorithm in the same chip. This research allows the designer to check the consistency of detection with real failures or attacks on the S-Box, and how aging affects it.

A. Motivation

To overcome some of the shortcomings of the analog sensors mentioned earlier, DSs are considered in specific vertical markets. Below, we detail two applications of these sensors.

Assuring both safety and security in the automotive industry (e.g., ISO 26262 and ISO/SAE 21434, respectively) requires high level of confidence in the embedded sensors, which is typically attained by correlating sensors of different nature (refer to part 5 of ISO 26262 [1]). For instance, analog sensors can be gracefully complemented by sensors implemented in digital logic. ISO/PAS 21448 defines functionality where proper situational awareness is critical to safety, and where

Manuscript received April 22, 2020; revised July 8, 2020; accepted August 24, 2020. Date of publication September 1, 2020; date of current version June 18, 2021. This work was supported by the French FUI (AAP-22) Program CSAFE+. This article was recommended by Associate Editor Y. Jin. *(Corresponding author: Naghmeh Karimi.)*

Md Toufiq Hasan Anik and Naghmeh Karimi are with the Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD 21250 USA (e-mail: toufiqhanik@umbc.edu; nkarimi@umbc.edu).

Jean-Luc Danger and Sylvain Guilley are with the Think Ahead Business Line, Secure-IC S.A.S., Institut Polytechnique de Paris, 91120 Paris, France (e-mail: jean-luc.danger@telecom-paris.fr; sylvain.guilley@secure-ic.com).

Digital Object Identifier 10.1109/TCAD.2020.3020921

[1]The sensor is interwoven with the target circuit such that both sensor and the circuit have similar operating conditions and are very likely to be hit simultaneously by an attack. Moreover, as the DS is implemented using the very same standard cells as the logic it protects, it is "camouflaged," hence sheltered from invasive attacks which would aim at surgically disabling it by means of FIB for instance.

that situational awareness is derived from complex sensors and processing algorithms.

In highly secure applications, sensors are required to detect invasive (e.g., destructive attacks, or those altering the chip structure, such as circuit edition with Focused Ion Beam, etc.) and semi-invasive attacks (e.g., fault injection attacks, such as glitching the clock, reset signals, or power supply). Therefore, these sensors become the target of motivated attackers, aiming at overcoming them as part of their attack path. This threat is considered in Common Criteria, for instance in *smartcards* evaluation, such as CCDB [2, p. 24, Sec. 5.2]. To thwart such attacks, ad hoc sensing has been proposed in the literature (e.g., [3] against attacks tampering specifically the reset tree lines). However, *holistic* approaches are still the subject of intense research.

An important requirement for accurate sensing is being able to accurately sense not only separate operating conditions, such as $T \leq T_{\text{worst}}$ and $V \geq V_{\text{worst}}$ where T_{worst} and V_{worst} denote the worst-case conditions the underlying system can tolerate, but conditions in pair (V, T) in which the circuit operates properly for a given process P, even if one of T (temperature) or V (voltage) has been violated. For example, the circuit may work properly despite $T > T_{\text{worst}}$, provided that V is large enough to make up for the unpropitious temperature condition. This can be achieved by our DS.

B. Contributions and Outline

The main contributions of this article are as follows.

1) An extensive study of a DS architecture and a demonstration of how it can react in terms of propagation delay to any process–voltage–temperature (PVT) variation to detect failures or attacks.
2) A method to characterize the status of the embedded DS sensor, and in turn the underlying device, based on which failures and attacks can be detected.
3) A methodology and corresponding detailed algorithm to dimension the sensor based on the underlying circuit's expected operating conditions to balance the anomaly detection and the imposed overhead.
4) A calibration scheme to take into account the technology and the process quality, e.g., process drifts and process variations.
5) A thorough investigation of how our sensor reacts when the device (and its embedded sensor) has been aged.
6) A comparison of our tailored sensor regarding anomaly detection (thanks to considering voltage and temperature conditions as pair) with the analog sensors that consider voltage and temperature quantities separately.
7) Extensive experimental results in terms of false and missed alarm rates for dependable chips;
8) A discussion on the security of the DSs against security attacks.

We notably demonstrate that DSs generate less false alarms, compared to analog sensors, thanks to their broader range of voltage-temperature (VT) consideration.

The remainder of the article is structured as follows. Section II presents the preliminary backgrounds on DSs and device aging. Section III compares DSs with their analog counterparts. Section IV discusses the deployed sensor and its characterization. The sensor *presilicon* design and *post-silicon* calibration is discussed in Section V. Section VI discusses the experimental results. Conclusions and future directions are drawn in Section VII.

II. Preliminary Backgrounds

A. Background on Digital Sensors

Deviating from nominal operating conditions (intentional or unintended) may cause circuit failures or leakage of sensitive data. For example, adversarially fooling sensors can cause car accidents [4]. Besides, timing attacks (such as Clockscrew [5]), temperature attacks [6], voltage attacks (PlunderVolt [7], VoltJockey [8], [9], `v0ltpwn` [10]), mixed timing+temperature [11], and timing+voltage [12] attacks all aim at extracting keys from cryptographic devices. Those attacks usually place the device beyond the *worst case* condition it can tolerate. Note that some attacks place the device in *best case* condition to wear it out too fast, thereby reducing its lifetime (e.g., [13]). Unintentional changes of environmental conditions such as temperature may also result in device malfunction via increasing the critical-path delay of the victim circuit. Thereby, sensing environmental conditions is crucial to detect such malfunctions.

In practice, multiple deviations from nominal conditions may occur, such as change of operating temperature or voltage, exposure to intense fields, aggressive irradiation by particles, and so on. Dedicated sensors can be deployed to monitor each operating condition (e.g., temperature and voltage) separately, but then aggregating their measurements raises an obvious problem as each sensor operates on a different, incommensurable scale. Therefore, a traditional approach is starting not from the cause of the stress, but from its consequence. Accordingly, sensors are designed to detect functional failures instead of measuring multiple specific physical quantities. A common reversible failure mode is the violation of the *timing* constraints, typically the setup time [14]. If a timing path is not met at the clock active (rising or falling) edge, then an incorrect value is sampled, resulting in a single event upset (SEU).

DSs consist of artificial critical paths inserted into the chip logic such that if the chip is operated in abnormal conditions, setup time violations occur in the first place on the DS intentionally long path which is usually as simple as a delay chain. The idea is to assess whether an edge (positive or negative) manages to propagate safely to the end of the chain at the considered clock period [15, Fig. 14]. Failing to do so is the evidence of environmental disruptions or manipulations. To better characterize the amplitude of the timing violation, the delay chain is sampled in many places. Such a snapshot allows to determine whether the violation is small or large, i.e., somehow digitizes the amount of stress applied to the circuit [16].

Bandgap reference circuits with NPN and PNP diodes were proposed to measure temperature [17], [18] in DRAMs. These methods suffer from high area overhead. On the other hand,

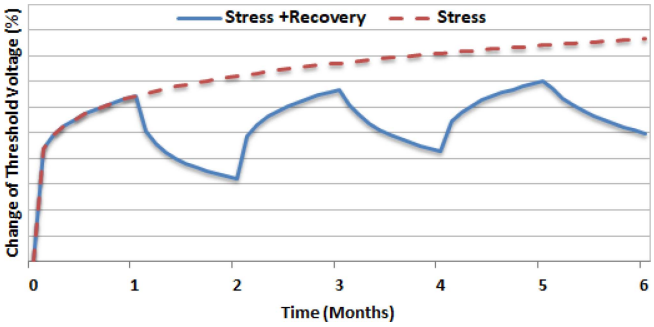

Fig. 1. Threshold-voltage shift of a pMOS transistor under NBTI effect [24].[3]

they only extract temperature value and fail to detect anomalies based on the combination of voltage and temperature conditions.

Vinshtok-Melnik and Shor [19] replaced the BJT transistors in bandgap sensors with ring oscillators in their proposed temperature sensor. Zhang *et al.* [20] proposed a ring-oscillator-based temperature sensor that reflects temperate changes. However, both methods only deal with temperature variations and assume that the circuitry is driven with a constant voltage source. Moreover, ring-oscillator-based DSs incur more latency than the delay-chain-based sensor we used in this article.

It is noteworthy to mention that although several types of sensors are available in the literature, they mainly aim at measuring physical quantities whereas the concentration of this article is to detect whether the operating conditions have been departed from the nominal operating conditions or not. To the best of our knowledge, this is a new sensing approach.

B. Background on Integrated Circuits Aging

A variety of DSs have been devised for measuring abnormal environmental conditions (e.g., [15, p. 189, Fig. 14], [21, p. 441, Fig. 3], and [22]). They share the property of using only simple digital gates, including D-Flipflops (DFFs), buffers, etc., and of having maximal activity, thereby (as a drawback) being especially prone to aging.

Aging mechanisms result in performance degradation and eventual failure of digital circuits over time. The two leading factors in CMOS technology are negative bias temperature-instability (NBTI) and hot-carrier injection (HCI) [23]. Both aging sources result in increasing switching and path delays.

NBTI Aging: NBTI affects a pMOS transistor when a negative voltage is applied to its gate. A pMOS transistor experiences two phases of NBTI depending on its operating condition. The first phase, the so-called stress phase, occurs when the transistor is on ($V_{gs} < V_t$). Here, positive interface traps are generated at the Si–SiO_2 interface which lead to an increase of the threshold voltage of the transistor. The second phase, the so-called recovery phase, occurs when the transistor is off ($V_{gs} > V_t$). The threshold voltage drift that occurred during the stress phase will partially recover in the recovery phase. Threshold voltage drifts of a pMOS transistor under stress depend on the physical parameters of the transistor, supply voltage, temperature, and stress time [25], [26]. The last three parameters (so-called external parameters) are used as acceleration factors of the aging process. Fig. 1 shows the threshold voltage drift of a pMOS transistor that is continuously under stress for 6 months and a transistor that alternates stress/recovery phases every other month. As shown, the NBTI effect is high in the first couple of months but the threshold voltage tends to saturate for long stress times. Tiwari *et al.* presented the equations to evaluate the NBTI-induced increase in the threshold voltage of a pMOS transistor [27, eqs. (2) and (3)].

HCI Aging: HCI occurs when hot carriers are injected into the gate dielectric during transistor switching and remain there. HCI is a function of switching activity and degrades the circuit by shifting the threshold voltage and the drain current of transistors under stress. HCI mainly affects nMOS transistors. HCI-induced threshold voltage drift is sensitive to the number of transitions occurring in the gate input of the transistor. In fact, the threshold voltage changes sublinearly with the number of transitions occurring in the input of an nMOS transistor. HCI has a dependency on temperature, clock frequency, usage time, and activity factor of the transistor under stress, i.e., the percentage of cycles in which the transistor is switching [23]. The details on evaluating the HCI-induced threshold voltage shift in a transistor has been presented in [27, eq. (4)].

III. Digital Versus Analog Sensors

Historically, sensors are analog devices. Indeed, they are considered transducers from an environmental quantity (such as temperature, voltage, etc.) to some quantized value, such as a digital value [where they are designated as analog to digital (A2D) converters] or a comparison with a predefined threshold (where they are designated as alarm generators) [28]. In practice, analog sensors are calibrated to track a certain environmental variable. Even some security-specific sensors, such as light (to detect attackers opening the chip) or pressure (MEMS to detect circuit grinding by invasive attackers) are researched but are hard to calibrate [29]. In contrast, DSs are fully made up of digital standard cells, and are not specific to any given environmental condition. Instead, they react in synchronization with the user digital logic [15, p. 189, Fig. 14].

Note that both digital and analog sensors are deployed to measure physical variables (e.g., temperature and voltage) represented by analog values. However, in DSs such measurement is performed via digital gates. In practice, the main differences of digital and analog sensors can be categorized as below.

1) The target technology and design methods for DSs is fully digital; thereby the sensor architecture is portable across different PDKs while analog sensor design is full-custom.
2) The calibration of DSs is low-cost and can be done fully in software, while analog sensors rely on costly calibration schemes, e.g., chip-by-chip laser trimming.
3) In contrast to analog sensors, digital counterparts do not need high level of accuracy in extracting the measured values (e.g., temperature) as they are only used to detect failures and attacks to raise an alarm accordingly (rather than extracting voltage and temperature values). In fact, digital and analog sensors follow different goals.

What follows discusses the other differences of analog and DSs in more details.

A. Efficiency

As DSs are only made up of standard cells, their design is highly optimized: power- and area-wise, as they combine optimizations at register transfer and netlist levels. On the contrary, analog sensors require manual dimensioning. Besides, many analog sensors are based on "always-on" logic gates, whereas DSs (in CMOS logic) never consume power, unless upon clock edges (which trigger a value toggling) [30]. Therefore, from the performance perspective, DSs are thus more efficient than analog sensors. Moreover, DSs are more controllable, as techniques such as clock gating are easy to implement automatically using standard EDA tools.

B. Sensitivity

Analog logic does not rely on electrical level discretization. Instead, it considers signals carrying a continuous value. However, analog logic is subject to process variability (and to dynamic noise, but this is also the case of DSs). Thereby there is an ambiguity in defining a threshold for nominal versus abnormal situations in analog sensors [31]. Trimming (e.g., by laser adjustment) is an option, but such a technique is costly [32] and also opens the door to other attacks (discussed in Section III-C below). This results in a great disparity in analog sensors' sensibility status [29].

It is noteworthy to mention that DSs detect environmental changes fast, hence are suitable for both slow-stress (e.g., global perturbation [33]) and transient attacks (e.g., glitches, or local electromagnetic field/laser light injections).

C. Resistance Against Attacks

Sensors aim at detecting attacks, hence attackers can envision to carry out a two-step attack: first neutralize the sensors, then perform the attack on the chip deprived from its defenses. As already mentioned, an analog sensor is typically implemented using full custom layout. Such physical structure does differ from the rest of the sea of gates, all being sibling instances from a standard cell library. For this reason, analog sensor patterns do stand out, and are therefore clear to identify visually (see [34, Fig. 21], where the temperature sensor is large and identifiable, whereas the contents of the digital logic looks random). Accordingly, their bypass is easy, i.e., once the analog sensor is spotted, a local reverse-engineering work can straightforwardly allows to infer the digital alarm signal that the sensor generates. Therefore, the expected level of difficulty to circumvent an analog sensor is considerably less than the one required to bypass a DS. In terms of Common Criteria [35, p. 24, Sec. 5.2], such invasive attack is considered realistic, therefore DSs provide a decisive advantage over analog sensors, in terms of certification.

Besides, the stealthy nature of DSs (as they are undistinguishable from user functional logic) makes it possible for the sneak insertion of several instances, thereby reducing exponentially the probability that an attack succeeds. Indeed, the more DSs, the more difficult for an attacker to perpetrate an undetected attack.

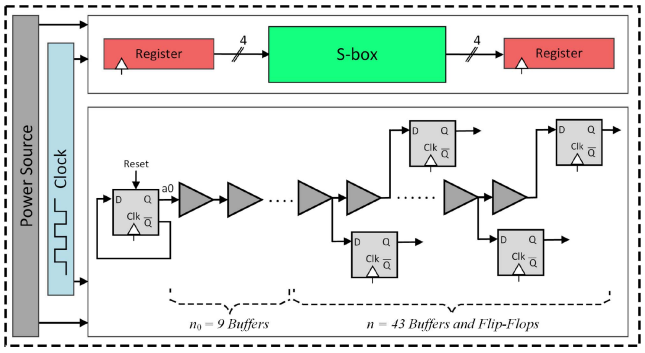

Fig. 2. Architecture of the sensor-integrated target system.

D. Accuracy and False Alarms

Most importantly, analog sensors do measure individual physical quantities (e.g., voltage alone, temperature alone, etc.). Even if all the drawbacks of analog sensors underlined earlier are mitigated, there remains the question of sensors measurement fusion into an alarm status. When independent analog sensors are deployed for the measurement of quantities, such as voltage and temperature, the nominal conditions shall be defined using *hard* decisions: nominal operations consist in cases whereby the temperature is less than a threshold and voltage is beyond another threshold. Such decision making is illustrated in Fig. 4. In contrast, DSs need only one threshold in the full temperature-voltage plane (namely, the AFN—detailed subsequently in Section IV). Accordingly, the fault detection in DSs is *soft*, and some environmental conditions that would result in false alarms in analog sensors (typically: low voltage but low temperature at the same time, or high temperature but high voltage) allows functional circuit usage without raising a false alarm when DSs are deployed despite the environmental condition change as such change does not result in circuit malfunction. Accordingly, analog sensors are more prone to false alarms than their digital counterparts [36].

In the remainder of this article, we refer to analog sensors as sensors where multimodal physical quantities cannot be measured at the same time, hence *hard* decisions shall be taken.

IV. Target Sensor

Fig. 2 depicts the high-level view of our sensor-integrated target system. As shown, a DS including a chain of 52 buffers is embedded in the circuitry. The sensor is placed close to the circuit to protect it. In this research, we target the S-Box of the PRESENT cipher (Section V discusses the reasons in more details). However, the S-Box can be replaced by any other target system. As shown, in the designed sensor, the last 43 buffers of the chain each feeds an individual flip-flop. The sensor outcome would be the output of these flip-flops. All flip-flops are operating under the same clock signal at frequency F, and the first buffer is fed with a toggle flip-flop generating a periodic signal $a0$ with the frequency of $F/2$.

The number of flip-flops and buffers included in the DS needs to be decided carefully as although less number of these gates is preferred for the sake of overhead, the sensor may result in significant false positive/negative failure detections if it is too small. The buffer-chain's length and the number of deployed flip-flops vary based on the PVT corners considered for the chip. If the PVT corners are larger in range, the size of the sensor chain increases to be able to sense the stress at a larger scale. Similarly, if the PVT corners are bounded, the sensor requires shorter buffer-chain and less flip-flops.

In practice, during the design flow, operational corners are decided (e.g., industrial grade $\Rightarrow$T$\in$ [$-$40°C, . . . , 85°C]). Any violation from such corners may result in wrong outputs. Our sensor can detect such violations as discussed below. To find the number of required buffers and flip-flops, we propose Algorithm 1 (in Section V). In practice, in each clock cycle of CC_i, when this sensor is fed with $a0$, the first $FN_i - 1$ flip-flops are in phase A (say $0 \rightarrow 1 \rightarrow 0$) and the next ones are in the complementary phase $\overline{\text{A}}$ (say $1 \rightarrow 0 \rightarrow 1$). Here, FN_i refers to the index of the flip-flop in which phase $\overline{\text{A}}$ starts in clock cycle CC_i. We benefit from this property for characterizing the sensor. We extract the average of all FN_is over all clock cycles. This average, so-called AFN is used for characterization. We refer to this characterization as average-based method (ABM).

Our experimental results confirm the high accuracy of this sensor in sensing environmental conditions, and in turn in system failure detection. Note that the phase change happens at lower indexes when the chip is operating slower, and at higher indexes when faster than expected. In practice, due to the noise as well as the metastability that may occur in some of the flip-flops in the designed/deployed sensor, the FN can fluctuate a bit in different clock cycles, thereby, we consider the average value of FNs (AFN) over a number of clock cycles as the sensor index. Note that the metastability cannot be avoided as the delay of the underlying buffers in the DS is changed when it operates in different VT conditions. This can cause metastability in some VT conditions, and thereby a fractional value for AFN.

Fig. 3 shows the flip-flop outputs in different operating conditions. In particular, Fig. 3(a) depicts the sensor outcome for Vdd = 1.0 V and temperature = 85 °C when the device is new (no-aged), *we refer to this operating condition as the worst-case condition, and to its related AFN as* AFN_{wc} hereafter. As shown, the first phase change occurs in the 17th flip-flop (*dff_17*), i.e., the first 16 flip-flops have the same phase A and the following ones are in complementary phase $\overline{\text{A}}$; resulting in AFN = 17. This trend is changed in other voltage/temperature or aging conditions. For example, Fig. 3(b) depicts the sensor outcome for Vdd = 1.2 V and temperature = 27 °C. As shown, in this case, phase change occurs in the 31 st flip-flop resulting in AFN = 31. Similarly, Fig. 3(c) depicts the sensor outcome for Vdd = 1.2 V and temperature = 120 °C. As shown, here the AFN fluctuates between 15 and 16 in different clock cycles due to metastability, thereby AFN = 15.5.

In practice, in the conditions under which the circuit operates slower (higher temperature and lower voltage), the delay of the buffer chain increases, resulting in the phase change

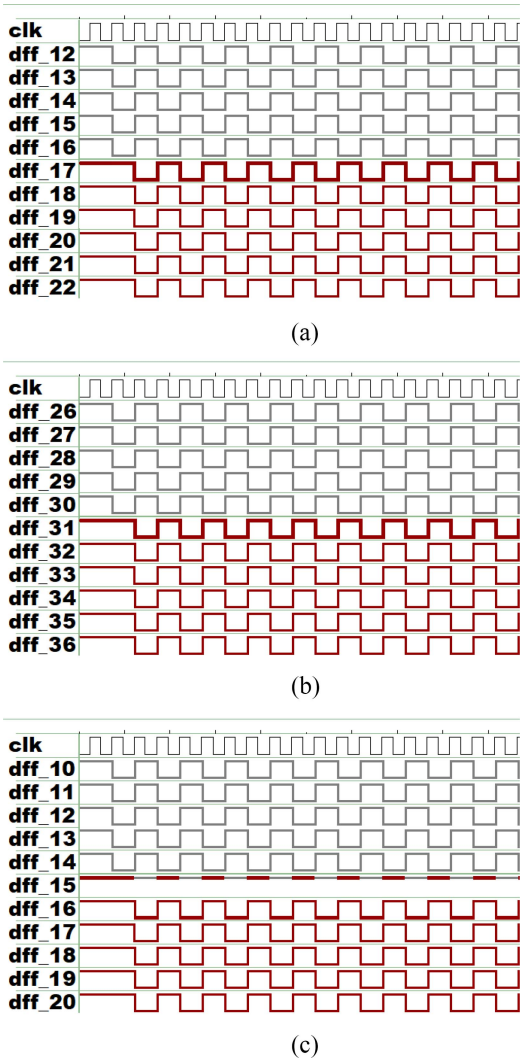

Fig. 3. Waveforms of Fig. 2 in different operating conditions. (a) Vdd = 1.0 V, Temp = 85 °C, Age = 0. (b) Vdd = 1.2 V, Temp = 27 °C, Age = 0. (c) Vdd = 1.2 V, Temp = 120 °C, Age = 0.

(from *A* to $\overline{\text{A}}$) being observed in the flip-flops with lower indexes (closer to the leading Toggle flip-flop). However, with the increase of voltage and decrease of temperature, the delay chain operates faster. This results in higher values of FN_i.

For characterization and in turn failure detection, the AFN is calculated at runtime and is compared with AFN_{wc}. In fact, the slower the sensor's buffer chain, the lower the AFN. Therefore, AFNs lower than the AFN_{wc} denote circuit failure (as both circuit and sensor are underlying in the same chip), and result in raising an alarm. Also, for any abnormal behavior like multiple changes of the phase an alarm is raised.

A. Deployed Sensor Versus the State-of-the-Art Digital Sensors

1) Delay-Based Digital Sensors: Delay-based DSs consist in the insertion of an artificial critical path in the system. This path is monitored on a regular basis (ideally at every clock cycle) to check for the absence of setup time violation. Such a principle has been first introduced in [15, p. 189, Fig. 14].

TABLE I
DS CONFUSION MATRIX

	S-Box latched value is incorrect (successful injection!)	**S-Box latched value is correct** (no or ineffective injection)
AFN $<$ 17 (red area in Fig. 4)	True positive	Alarm for no reason! False positive (type I error; aka false alarms)
AFN $\geq$ 17 (grey area in Fig. 4)	Undetected attack! False negative (type II error; aka missed alarms)	True negative

The DS we study in this article is a delay-based sensor with a basic structure for sensing delays, which can be enriched for smarter stress characterization (in addition to its mere detection). For example, the embodiments given in Figs. 5, 6, 8, 9, and 10 of patent application [37], allow to test if the perturbation is local or not (by interleaving two identical sensors), long or short (by appending shift registers to sample the status over time), etc. Another variation of the delay-based sensors consider having the delay chain be closed, so as to form a loop. In these sensors, the fluctuations of the loop frequency attest to an attack [38]. This approach is interesting, though more power demanding compared to our basic DS. To summarize, our study is generic insofar as it focuses on the main architectural principle upon which all derived designs are based.

2) Impulse-Based Digital Sensors: This type of sensors can protect the underlying circuit against other threats, such as typically the impulsive attack in which a strong perturbation is applied very timely and shortly. One such sensor that aims at detecting very brief perturbations is proposed in [21] and [22]. However, such structures are not able to detect gentle local stress, as would delay-stress DSs. Indeed, they only manage to check inconsistencies between DFFs' states.

V. SETUP AND CALIBRATION

A. Sensor-Integrated Target System

The sensor-integrated system that we target in this article is the S-Box of the PRESENT cipher. PRESENT is a lightweight block cipher with 64-b blocks and a bit-oriented permutation layer, standardized as ISO/IEC 29192-2:2012 [39]. It includes 31 rounds and supports two key lengths of 80 and 128 b. Each encryption round consists of a bitwise XOR operation, a nonlinear substitution layer, and a linear permutation layer. The nonlinear layer uses a single 4-b S-Box applied 16 times in parallel in each round. The reason for targeting S-Box is that first it is the focal point for attacks, as it is the most complex part of block ciphers, hence the more amenable to perturbation attacks. Second, S-Boxes are hard to model in terms of timing, as each output bit (here, amongst 4) has a different timing depending on the 4-b input word. Hence, strategies based on timing prediction are hard, let alone *suboptimal* worst-case situations (i.e., critical path violation detection in any PVT corner). This S-Box makes it possible to confront the DS to real faults, the NULL hypothesis being "*is the S-Box evaluated correctly?*." Accordingly, the definition of DS various figures of merit is provided in Table I.

Algorithm 1: DS Dimensioning

input : Design kit for the target technology, desired clock period, safety margin of K buffers
output: Sensor dimensions n_0 and n; values to be used for architecturing the sensor aiming at failure detection during run time

1 Build a netlist consisting of a DFF which samples its inverted output, and feeding an infinite chain of buffers; each buffer feeds also a separate flip-flop
2 Set the conditions to `worst case` (e.g., slow process, high temperature, low voltage) — point **B** in Fig. 4
3 Determine the position (N) of first sampling inversion error
4 Remove the Flip-flops connected to the first N buffers
5 Set the conditions to `best case` (e.g., fast process, low temperature, high voltage) — point **A** in Fig. 4
6 Determine the position (AFN_high) of first sampling inversion error
7 **return** $(n_0 = \mathrm{N} - K, n = \mathrm{AFN\_high} - n_0 + K)$

To be able to *exhaustively* simulate the S-Box module for all possible input combinations and in turn verify the capability of our sensor in failure detection in all possible cases, our simulated circuitry includes our DS, as well as a 4-b counter feeding the S-Box implementation in each clock cycle and a register to store the result. The sensor is integrated to detect the stress and to notify any abnormal behavior.

B. Experimental Setup

The sensor and the target S-Box were implemented in the transistor level using 45-nm NANGATE technology [40]. We used Synopsys HSpice for the transistor-level simulations, and the HSpice built-in MOSRA Level 3 model to assess the effect of NBTI and HCI aging [41]. Both sensor and S-Box outputs were extracted under different voltage and temperatures and for different aging durations; up to 7 years of operation in steps of two months. The sensor was simulated for temperatures between -10 °C and 150 °C with 1 °C steps, and for the voltage source (*Vdd*) between 0.4 and 1.4 V with 0.05-V steps.

Architecturing the DS consists in the determination of the number n_0 of leading buffers as well as the number n of sampling flip-flops and their related buffers in the delay chain. For the sensor shown in Fig. 2, $n_0 = 9$ and $n = 43$. Algorithm 1 explains how these dimensions are extracted based on operating conditions. This algorithm ensures that whatever environmental conditions (from *worst* to *best*) are, the DS is able to sense it (using the position of the first inverted edge) with a safety margin of K buffer elements.

As shown in Algorithm 1, to design our DS, we first consider a chain of infinite number of buffers each feeding a flip-flop (line 1). Then, we simulate the circuit under the worst-case condition based on which, we decide about the number of leading buffers (lines 2 and 3). In practice, we extract the index of the flip-flop in which the first change occurs (refer to AFN in Section IV) and remove all the flip-flops before that as this flip-flop violates the setup time, thereby, its index can be used to represent the worst-case condition (under which it was running). After such pruning, we simulate the remaining structure under the best-case condition to decide about the number

Algorithm 2: AFN Calibration

input : Voltage V or (V_1, V_2) for DVFS
output: AFN threshold (AFN_{wc})

1 Set the conditions to worst case T °C, voltage V, V_1 or V_2 — point **B** in Fig. 4; AFN $\leftarrow 0$
2 **for** $i \in \{1, \ldots, M\}$ **do**
3 Determine position (FN) of 1st sampling inversion error
4 AFN $\leftarrow$ AFN + FN
5 **return** AFN/M // Average of FN on M measures

of required flip-flops (lines 5 and 6) as our sensor should be able to extract the AFN up to the best case condition. Finally, we update the extracted numbers of buffers and flip-flops with the safety margin of K (line 7). This safety margin (K) is considered to ensure that the sensor can report the malfunctions of the underlying circuit under a larger range of VT conditions, i.e., even beyond worst-case condition (between points **B** and **C** in Fig. 4). Note that less number of leading buffers increases the failure detection range for the conditions that make the circuit slower, and more flip-flops extends the failure detection range for the conditions in which the circuit operates faster.

C. Calibration for Process and DVFS Management

Once the circuit is fabricated, the AFN which represents the detection threshold is determined in order to take the real state of the process P, and possibly the dynamic voltage-frequency scaling (DVFS) management into account. DVFS is a system-level feature which allows parts of the chip to save power by reducing the power supply, while at the same time lowering the frequency to meet the timing constraints. In practice, a few DVFS configurations are defined (typically two). AFN shall adapt to each of these configurations. The threshold values (AFN) are thus not hardcoded within the DS block, but made reprogrammable by software, hence stored locally in one-time programmable (OTP) memory. Algorithm 2 explains how the AFN is calibrated after fabrication. The worst-case voltage V is considered without DVFS, and V_1 and V_2 are two worst-case voltages corresponding to two DVFS configurations. Note that the AFN is averaged after M measurements (typically, $M \approx 100$) in order to mitigate noise and metastability impacts.

VI. Experimental Results and Discussion

A. Impact of Environmental Conditions on DS Characterization

Fig. 4 shows the AFN in different voltage and temperature combinations. As expected, AFN is lower for the conditions in which the underlying circuit operates slower, i.e., in low voltages and high temperatures, while its value increases by moving toward lower temperatures and higher voltages. For example, in the room temperature (27 °C) when $Vdd = 1.2$ V, AFN is 31. This value increases to 40, when $Vdd = 1.4$ V and temperature = 0 °C, and decreases to 15 in case of $Vdd =$ 1.0 V and temperature = 100 °C. The first takeaway point from this observation is that using AFN signatures can be useful to report sensing conditions as it is highly sensitive to the operating voltage and temperature.

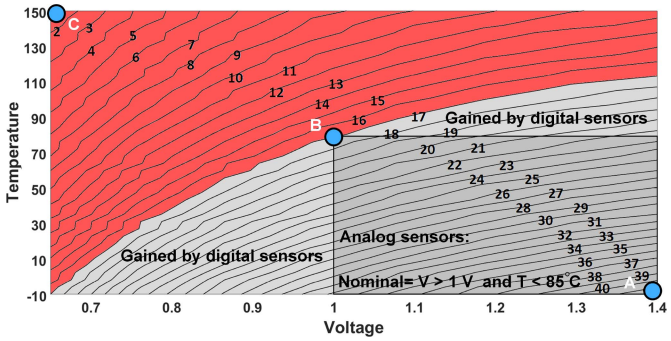

Fig. 4. AFN variation in different voltage and temperature pairs.

As discussed in Section IV, we deploy the sensor's AFN for the system's failure detection, i.e., to predict if the system works properly or not based on the operating conditions. In this article, our S-Box works properly in temperatures below 85 °C and with a Vdd beyond 1.0 V. As shown in Fig. 4, the AFN is equal to 17 in this condition ($AFNwc = 17$). The worst-case condition is shown with point **B** in Fig. 4). Accordingly, during the system normal operation, any AFN below 17 predicts an intentional/unintentional system failure, and results in raising an alarm to notify such malfunction.

Another interesting observation from Fig. 4 is the comparison between analog and DSs. DSs react in terms of propagation delay to any PVT variation (in our case VT as the sensor is calibrated post-fabrication). Thereby, being sensitive to the mutual effect of such variations, DSs result in less false alarms when used for failure detection. However, analog sensors consider sharp limits for voltage and temperature separately when detecting failures (rectangle shape shown in dark gray in Fig. 4. This flexibility of DSs results in covering a broader (but still harmless) range of VT (areas shown in light or dark grey), and accordingly highly limits false positive failures, also known as false alarms. For example, in Fig. 4, a high temperature (>85 °C) can be made up by a higher voltage (>1.0 V) when a DS is used.

The corners shown as **A** and **B** in Fig. 4, respectively, represent the best case, $(V, T) = (1.4V, -10\ °C)$, and the worst case, $(V, T) = (1.0V, 85°C)$ conditions based on which our sensor was designed in this article, i.e., the VT range in which we expect our underlying circuit (S-Box here) works properly. The upper left corner in this figure, shown as **C**, extends the range by considering a safety margin (refer to Algorithm 1), i.e., **C** represents the condition in which sensor still is reliable (it can predict correctly that S-Box works properly or not).

B. Accuracy of the AFN-Based Failure/Attack Detection

To show the correspondence between the extracted AFN and the circuit's working status (failure or proper functionality), Fig. 6(a) depicts the AFN-based sensor prediction and Fig. 7(a) depicts the real S-Box operation status (pass or fail) in different VT combinations. In Fig. 6(a), the failures relate to the cases in which AFN is lower than the $AFNwc$, i.e., 17. The sensor predicts a pass, otherwise. Fig. 7(a) shows the correctness of the real S-Box output in each VT pair. Any mismatch

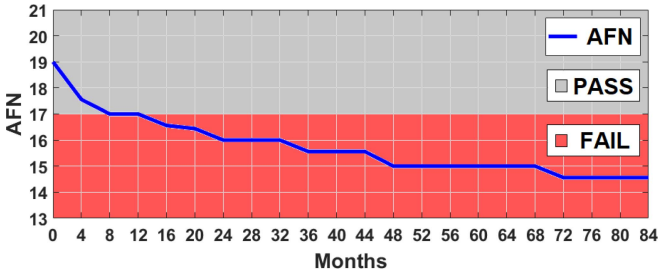

Fig. 5. Effect of aging on AFN in ABM scheme (Vdd = 1.2 V, temperature = 95 °C). The sensor predicts system failure when AFN < 17, and predicts proper functionality (i.e., pass) otherwise.

TABLE II
ACCURACY OF OUR DS IN DIFFERENT AGING DURATIONS

Age	New	4 months	2 years	4 years	6 years	7 years
Acc.(%)	99.17	98.70	98.43	98.14	98.28	98.43

between the S-Box output and the expected output is considered as fail and shown in red. For example, at Vdd = 1.0 V and temperature = 100 °C, the S-Box output is not correct, i.e., it fails [a red point is shown for this VT pair in Fig. 7(a)]. Meanwhile, for the same VT combination, AFN is 15. This results in firing an alarm by sensor predicting a malfunction [the related point is shown in red in Fig. 6(a)]. Comparing Fig. 7(a) and Fig. 6(a) depicts that the pass/fail conditions in both figures match in over 99.17% of cases (3353 out of the 3381 cases). A closer look into these results reveals that for the VT pairs that sensor prediction and S-Box status (pass or fail) do not match, the AFN is very close to 17 (i.e., in range of [16.44,17.56]). The takeaway point from these observations is that AFN can accurately detect the system's failures and attacks.

C. Impact of Aging on Chip Failure Detection

Fig. 5 depicts how aging affects the sensor characterization and in turn the failure detection rate. Aging results in a lower AFN as it makes the sensor slower. As shown, the AFN decreases from 19 (age: 0) to 14.5 after 7 years of aging when the temperature is 95 °C and Vdd = 1.2 V. The change rate of AFN is higher in the first 2 years, and becomes slower afterward ($\approx$ 7.8% decrease per year for the first 2 years and $\approx$ 1.8% per year for the following 5 years). This observation is correlated with the impact of aging over time as in CMOS circuits the aging rate is higher in the beginning yet saturates after some time. The takeaway point from this observation is that aging may result in false alarms (predicting the system as erroneous whereas it works properly). Thereby, the aging effects need to be taken into account. Below we will discuss the impact of aging on the proposed failure detection scheme in details.

Fig. 6 depicts the system failure's prediction via our DS and Fig. 7 illustrates the real status of the system in different VT conditions over time. The two curves are similar *by design*: both functional logic (PRESENT) and the sensing logic (DS) are made of standard cells, share the same power and clock signals, hence *naturally track* in terms of behavior (e.g., propagation delay). As mentioned earlier, an AFN lower than 17

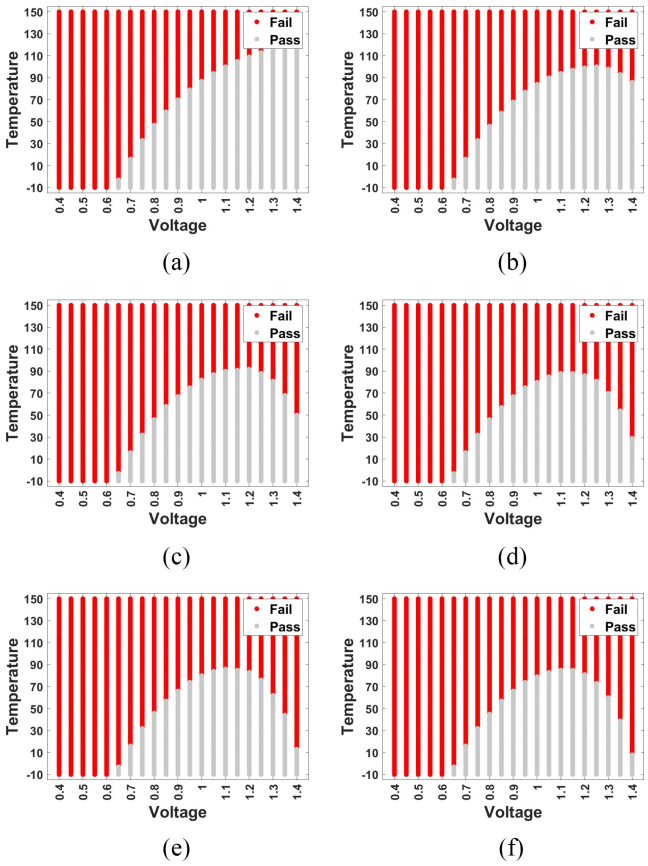

Fig. 6. Effect of aging on the failure prediction (via Sensor's AFN value) in different VT conditions. (a) New Device (Age: 0). (b) Age: 4 months. (c) Age: 2 years. (d) Age: 4 years. (e) Age: 6 years. (f) Age: 7 years.

is reported as failure by sensor (red points in Fig. 6). As expected and shown in Fig. 7, system failure rate increases with aging. For example, the S-Box circuit works properly under Vdd = 1.2 V and temperature 105 °C when new (age: 0) but after 4 months it experiences malfunction. Note that our DS predicts both situations correctly, i.e., predicts that S-Box works properly under this VT condition [shown in Fig. 6(b)] when the device is new while fails after 4 months of usage.

We compared the results shown in Fig. 6(b)–(f) vis-a-vis their related results in Fig. 7 to evaluate the accuracy of the deployed DS in different aging durations. Table II shows the results. As shown, the accuracy of this DS is 99.17% when new, and remains very similar after aging. The first takeaway point from this observation is that the aging-induced accuracy loss of our DS is negligible. As shown, the VT corners of the S-Box circuit is changed with aging. For example, when Vdd = 1.2 V, a new S-Box operates properly in temperature below 105 °C, while this T corner decreases to 101 °C, 94 °C, and 86 °C after 4 months, 2 years, and 7 years of aging, respectively. Moreover, this effect is more significant under high voltages, e.g., when Vdd = 1.4 V, the S-Box can operate properly for temperatures below 125 °C, while this range decreases to 95 °C, 57 °C, and 6 °C after 4 months, 2 years, and 7 years of aging, respectively. These results confirm the necessity of embedding a robust DS in the chip circuitry to detect those failures even for aged circuits. As the results show,

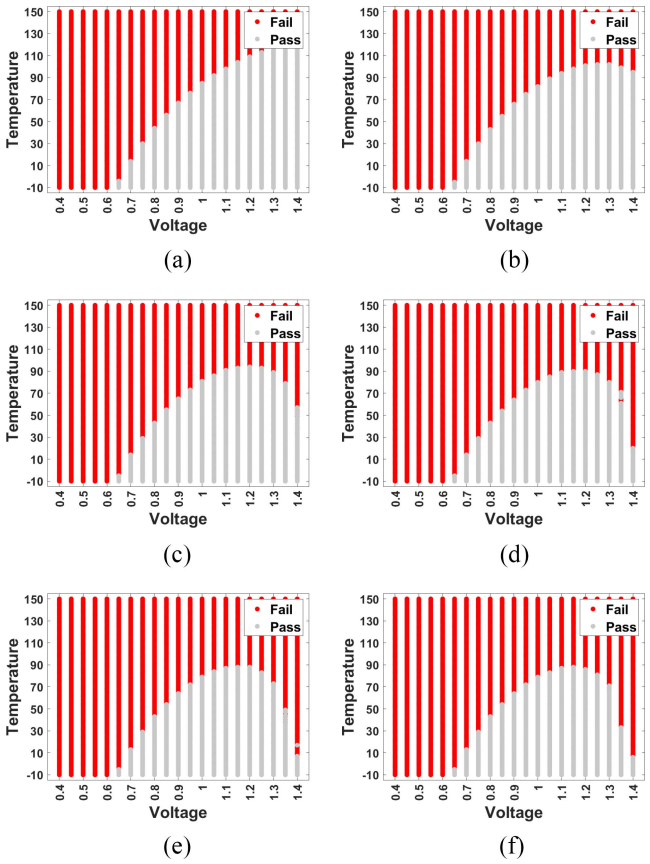

Fig. 7. Effect of aging on real system (S-Box) operation status (pass/fail) in different VT conditions. (a) New Device (Age: 0). (b) Age: 4 months. (c) Age: 2 years. (d) Age: 4 years. (e) Age: 6 years. (f) Age: 7 years.

our DS can detect failures of the underlying circuits with a high accuracy even after 7 years of aging.

D. Missed and False Chip Failure Detection

Although the accuracy of failure detection via our DS decreases after aging, the reduction rate is not significant. Ideally, the sensor should raise an alarm whenever the S-Box output is not correct. Moreover, ideally, no false positives (raising alarms when the circuit works properly) should be observed. Fig. 8(a) shows the rate of false and missed alarms in different aging durations. The former denotes to the cases where the sensor raises an alarm in a particular VT condition while it should not as the circuit works properly in that condition. However, missed alarms refer to the cases in which the circuit does not work properly but the DS cannot detect it via its AFN; hence it does not fire an alarm. Even though false alarms are not destructive but it is costly to not care such conditions. However, missed alarms are unhealthy for any system. Therefore, both missed and false alarms need to be taken care of. The former affects security and the latter results in availability problems. Fig. 8(a) shows the missed and false alarms in different aging duration overall 3381 VT pairs. Note that this result was extracted for AFN = 17 (using the proposed Algorithms and the values shown in Fig. 4). As shown in Fig. 8(a), for a new device, in $\approx$ 99.17% of cases, the DS predicts the functionality status (proper versus erroneous) of the circuit correctly and only in 0.83% cases, the

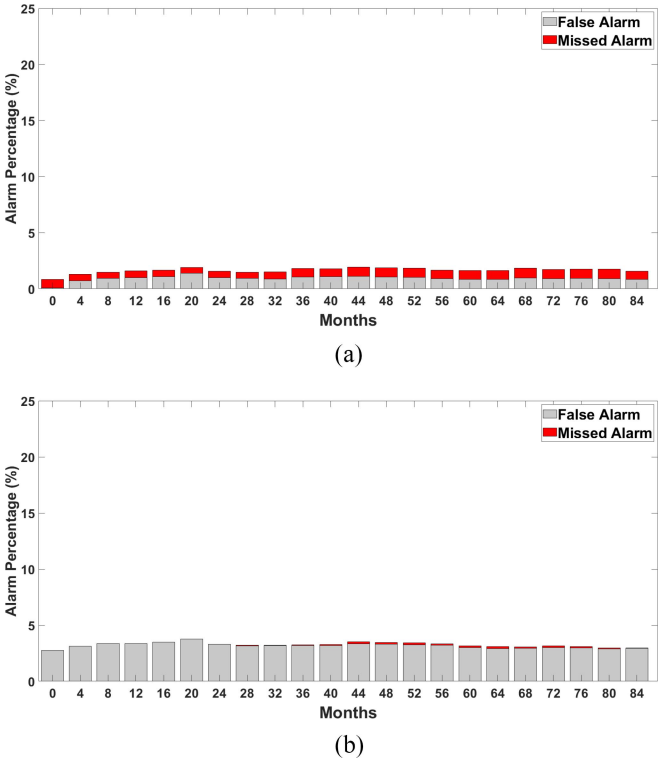

Fig. 8. Effect of aging on ABM missed/false alarms from DS. (a) Effect of aging on ABM missed/false alarms from DS (AFN 17). (b) Effect of aging on ABM missed/false alarms from DS (AFN 18).

circuit experiences either a false or a missed alarm (25 missed and 3 false alarms among all 3381 cases). The rate of missed alarms is approximately constant and does not change after aging. However, false alarms increase after aging albeit with a very slow rate; the increasing rate is higher for the first couple of months then saturates. As shown over 7 years of aging (84 months), the failure detection accuracy (no missed/false alarms) is at least 98.43% (compared to 99.17% for a new device). This confirms the robustness of our DS against aging.

In fact, the very few missed alarms reported for a new device in Fig. 8(a) is related to the VT pairs that are in the border of pass/fail sectors (red/gray areas) in Fig. 4. If for an application, even such low missed alarm rate is not tolerated, the chip security owner can slightly increase the AFN value used for firing alarms. This results in no missed alarm, albeit increases the false alarm rate. Please note that there is a trade-off between missed and false alarms, in that both cannot be avoided simultaneously. Fig. 8(b) shows the missed and false alarm rates when the AFN is considered as 18 (instead of nominal value 17). As shown, there is no missed alarms in this case (for an age = 0 device).

To compare the efficiency of the deployed DS vis-a-vis with its analog sensor counterpart, we extracted the rate of the missed and false alarms of the analog sensor. As discussed earlier and depicted in Fig. 4, the analog sensor considers sharp limits for voltage and temperature separately when detecting failures, i.e., as shown in this figure, temperatures higher than 85 °C and voltage higher than 1.0 V, each denote to the circuit failure. Thereby, the analog sensor fails to consider that a high temperature (>85 °C) can be made up by a higher

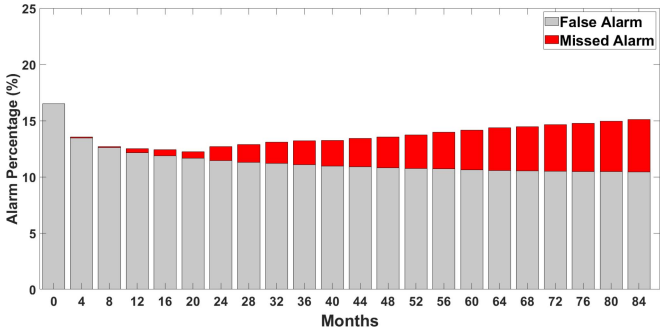

Fig. 9. Effect of aging on missed/false alarms from the analog sensor.

voltage (>1.0 V). Fig. 9 demonstrates the missed and false alarms of the analog sensor in different aging duration overall 3381 VT pairs. As shown, for each aging duration the rate of the false alarms are more significant compared to the DS counterpart in the same age. In addition, although for newer sensors (younger than 1-year-old), the analog sensor results in less false negatives (missed alarms) compared to the DS shown in Fig. 8(a), the trend changes when the sensor is used more than one year.

E. Process Quality and Process Mismatch

As mentioned earlier, after fabrication each sensor is calibrated. This results in taking the effect of process quality (P) into account. In addition, as each sensor chip is calibrated separately, process mismatch does not affect the sensor outcome in terms of failure detection rate.

F. Sensor's Performance and Security

Scalability of the Sensor in Terms of the Time Required to Dimension the Sensor Architecture: In practice, to properly dimension the DS, Algorithm 1 should be executed. As discussed, this algorithm requires multiple SPICE simulations of at least two netlists in order to build the DS structure incrementally. However, it is noteworthy to mention that Algorithm 1 finishes in deterministic time. In addition, it is executed only one time (offline) before the characterization of the DS (specifically, network of curves displayed in Fig. 4). Thereby, the required configuration time is reasonable.

Security of the Sensor Against Side-Channel Attacks on Protected Chips: History tells us that sensitive systems can be subject to attacks whereby some analog logic is leaking information about the digital logic. Such leakage can be passive, for instance the analog logic is a communication channel which transports information from running cryptography. An example of such threat, so-called TEMPEST, is discussed in [42]. Protection against TEMPEST requires to attenuate the compromising emanation of digital data through analog channels (communication wire, power line, radiated electromagnetic field, etc.). The documents NATO SDIP-27 and USA NSTISSAM report the level of residual leakage admissible for different attack scenarios. Typically, three situations are considered (corresponding to NATO SDIP-27 levels C, B, and A): the attacker is further than 100 m away, then further than 20 m, and eventually in a neighboring room, at 1 m distance.

Recent researches such as [43], highlight that with the advent of mixed-signal System-on-Chips, the TEMPEST measurement could actually arise from within the chip. Indeed, embedded A2D converters (A2DC) could be subverted to capture "ground noise" traces during the execution of software or hardware cryptography.

Extrapolating even further, the attacker could leverage not only some A2DC, but actually the DSs themselves. An example is a smart attack in which defensive elements are paradoxically repurposed for attacking. The idea is that due to the sensitivity of cryptographic modules to perturbation attacks [44], it is expected that DSs are instantiated close to them. Thus, DSs constitute excellent (side-channel) oscilloscopes to monitor the activity of the cryptographic module which is protected via the same DS against fault attacks. Although theoretically feasible (and indeed put in place in the context of multitenant FPGAs [45]), such trace collection is challenging in practice because the DSs' status is not publicly available. As a matter of fact, from a system-level point of view, DSs are slaves on the system-bus, which is typically addressable only through privileged instructions. Therefore, unless the attacker manages to escalate her privileges, the information related to DSs' status is segregated from the external world. But in any case, it is worth mentioning that the confidentiality of the DSs values has to be protected, as preciously as its configuration (one shall not be able to disable the DS, for instance).

VII. Conclusion

DSs allow to detect out-of-specification environmental conditions by accurately tracking temperature (T) and voltage (V) variations. A design methodology is presented, which takes as input the operational corners, under the form of best and worst cases. The architecture of the DS is dimensioned presilicon and it is configured (by a threshold named AFN) post-silicon, thereby tolerating process variability. The coverage of the DS in the VT plane is detailed and it is shown that it covers a larger area than the intersection of best/worst case intervals considered independently for temperature and voltage. A thorough aging analysis reveals that the accuracy, in terms of false and missed alarm rate, only shifts by 1 percent over a lifespan of 7 years.

The structure of the DS can be pruned such that it only includes two flip-flops, placed after the n_0 leading buffers, at positions n_0 and $n_0 + 1$. This is indeed enough to monitor the VT conditions from passing the AFN threshold. Alternatively, the current DS structure (described as in Algorithm 1), can be further leveraged to detect "better" than best cases, which can be the signature of an adversarial accelerated aging attack or hardware Trojan activation. As a continuation of this study, we will develop an integrated framework to quantify the on-chip voltage and temperature via a combination of the embedded sensor circuitry discussed in this research and neural network models. Realizing this DS on real-silicon to confirm our findings is another avenue we will pave in this research in the near future.

ACKNOWLEDGMENT

The authors are grateful to Xuan Thuy Ngo and Thomas Perianin for helping with FPGA validation.

REFERENCES

[1] *Road Vehicles—Functional Safety—Part 5: Product Development at the Hardware Level*, Standard ISO/SAE 26262-5:2018, 2018.

[2] *Application of Attack Potential to Smartcards, Mandatory Technical Document, Version 2.9, Revision 2*, document CCDB-2013-05-002, Common Criteria Develop. Board, Gaithersburg, MD, USA, May 2013. [Online]. Available: http://www.commoncriteriaportal.org/files/supdocs/CCDB-2013-05-002.pdf

[3] D. Lee, D. Choi, J. Seo, and H. Kim, "Reset tree-based optical fault detection," *Sensors*, vol. 13, no. 5, pp. 6713–6729, 2013.

[4] Y. Shoukry, P. D. Martin, P. Tabuada, and M. B. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems (CHES)*. Heidelberg, Germany: Springer, 2013, pp. 55–72.

[5] A. Tang, S. Sethumadhavan, and S. J. Stolfo, "CLKSCREW: Exposing the perils of security-oblivious energy management," in *Proc. 26th USENIX Security Symp. USENIX Security*, Vancouver, BC, Canada, 2017, pp. 1057–1074. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/tang

[6] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature attacks," *IEEE Security Privacy*, vol. 7, no. 2, pp. 79–82, Mar./Apr. 2009.

[7] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens, "Plundervolt: Software-based fault injection attacks against Intel SGX," in *Proc. IEEE Symp. Security Privacy*, San Francisco, CA, USA, 2020, pp. 1466–1482.

[8] P. Qiu, D. Wang, Y. Lyu, and G. Qu, "VoltJockey: Breaching TrustZone by software-controlled voltage manipulation over multi-core frequencies," in *Proc. Conf. Comput. Commun. Security (CCS)*, 2019, pp. 195–209.

[9] P. Qiu, D. Wang, Y. Lyu, and G. Qu, "VoltJockey: Breaking SGX by software-controlled voltage-induced hardware faults," in *Proc. Asian Hardw. Orient. Security Trust Symp. (AsianHOST)*, Xi'an, China, 2019, pp. 1–6.

[10] Z. Kenjar, T. Frassetto, D. Gens, M. Franz, and A.-R. Sadeghi, "V0LTpwn: Attacking x86 processor integrity from software," in *Proc. 29th USENIX Security Symp.*, Boston, MA, USA, Aug. 2020, pp. 1445–1461. [Online]. Available: https://github.com/zkenjar/v0ltpwn

[11] T. Korak, M. Hutter, B. Ege, and L. Batina, "Clock glitch attacks in the presence of heating," in *Proc. Workshop Fault Diagn. Tolerance Cryptogr. (FDTC)*, Busan, South Korea, 2014, pp. 104–114.

[12] T. Korak and M. Hoefler, "On the effects of clock and power supply tampering on two microcontroller platforms," in *Proc. Workshop Fault Diagn. Tolerance Cryptogr. (FDTC)*, Busan, South Korea, 2014, pp. 8–17.

[13] N. Karimi, A. K. Kanuparthi, X. Wang, O. Sinanoglu, and R. Karri, "MAGIC: Malicious aging in circuits/cores," *ACM Trans. Archit. Code Optim. (TACO)*, vol. 12, no. 1, pp. 1–25, 2015.

[14] N. Selmane, S. Guilley, and J.-L. Danger, "Practical setup time violation attacks on AES," in *Proc. 7th Eur. Depend. Comput. Conf. (EDCC)*, Kaunas, Lithuania, 2008, pp. 91–96.

[15] N. Selmane, S. Bhasin, S. Guilley, and J.-L. Danger, "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET Inf. Security*, vol. 5, no. 4, pp. 181–190, Dec. 2011, doi: 10.1049/iet-ifs.2010.0238.

[16] M. Anik, S. Guilley, J.-L. Danger, and N. Karimi, "On the effect of aging on digital sensors," in *Proc. 33rd Int. Conf. VLSI Design 19th Int. Conf. Embedded Syst. (VLSID)*, Bangalore, India, 2020, pp. 189–194.

[17] J.-Y. Sim *et al.*, "A 1.8-v 128-mb mobile dram with double boosting pump, hybrid current sense amplifier, and dual-referenced adjustment scheme for temperature sensor," *IEEE J. Solid-State Circuits*, vol. 38, no. 4, pp. 631–640, Apr. 2003.

[18] J.-H. Ahn *et al.*, "Adaptive self refresh scheme for battery operated high-density mobile dram applications," in *Proc. Asian Solid-State Circuits Conf.*, Hangzhou, China, 2006, pp. 319–322.

[19] N. Vinshtok-Melnik and J. Shor, "Ultra miniature 1850 μm^2 ring oscillator based temperature sensor," *IEEE Access*, vol. 8, pp. 91415–91423, 2020.

[20] R. Zhang, Z. Liu, K. Yang, T. Liu, W. Cai, and L. Milor, "Impact of front-end wearout mechanisms on FinFet sram soft error rate," *Microelectron. Rel.*, vols. 100–101, Sep. 2019, Art. no. 113487.

[21] D. El-Baze, J. Rigaud, and P. Maurine, "A fully-digital EM pulse detector," in *Proc. Design, Autom. Test Eur. (DATE)*, Dresden, Germany, 2016, pp. 439–444.

[22] D. El-Baze, J. Rigaud, and P. Maurine, "An embedded digital sensor against EM and BB fault injection," in *Proc. Workshop Fault Diagn. Tolerance Cryptogr. (FDTC)*, Santa Barbara, CA, USA, 2016, pp. 78–86.

[23] F. Oboril and M. B. Tahoori, "ExtraTime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *Proc. Int. Conf. Depend. Syst. Netw. (DSN)*, Boston, MA, USA, 2012, pp. 1–12.

[24] N. Karimi, J. Danger, and S. Guilley, "Impact of aging on the reliability of delay PUFs," *J. Electron. Test. Theory Appl.*, vol. 34, no. 5, pp. 571–586, 2018.

[25] S. Khan, N. Z. Haron, S. Hamdioui, and F. Catthoor, "NBTI monitoring and design for reliability in nanoscale circuits," in *Proc. Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS)*, Vancouver, BC, Canada, 2011, pp. 68–76.

[26] M. A. Alam, H. Kufluoglu, D. Varghese, and S. Mahapatra, "A comprehensive model for PMOS NBTI degradation: Recent progress," *Microelectron. Rel.*, vol. 47, no. 6, pp. 853–862, 2007.

[27] A. Tiwari and J. Torrellas, "Facelift: Hiding and slowing down aging in multicores," in *Proc. 41st Annu. IEEE/ACM Int. Symp. Microarchit.*, 2008, pp. 129–140.

[28] R. P. Bastos, F. S. Torres, J.-M. Dutertre, M.-L. Flottes, G. D. Natale, and B. Rouzeyre, "A bulk built-in sensor for detection of fault attacks," in *Proc. Int. Symp. Hardw. Orient. Security Trust (HOST)*, Austin, TX, USA, 2013, pp. 51–54.

[29] D. Shahrjerdi, J. Rajendran, S. Garg, F. Koushanfar, and R. Karri, "Shielding and securing integrated circuits with sensors," in *Proc. Int. Conf. Comput.-Aided Design (ICCAD)*, San Jose, CA, USA, 2014, pp. 170–174.

[30] A. De Marcellis and G. Ferri, *Analog Circuits and Systems for Voltage-Mode and Current-Mode Sensor Interfacing Applications* (Analog Circuits and Signal Processing). Dordrecht, The Netherlands: Springer, 2011.

[31] G. van der Horn and J. L. Huijsing, *Integrated Smart Sensors: Design and Calibration* (International Series in Engineering and Computer Science), vol. 419. New York, NY, USA: Springer, Dec. 1997.

[32] J. Williams, *Analog Circuit Design: Art, Science and Personalities*. Boston, MA, USA: Newnes, 1991.

[33] S. Guilley and J.-L. Danger, *Global Faults on Cryptographic Circuits*. Heidelberg, Germany: Springer, 2012, Ch. 17, pp. 297–314.

[34] D. A. Kamakshi, A. Shrivastava, and B. H. Calhoun, "A 0.2 V, 23 nW CMOS temperature sensor for ultra-low-power IoT applications," *J. Low Power Electron. Appl.*, vol. 6, no. 2, p. 10, Jun. 2016.

[35] *Application of Attack Potential to Smartcards, Mandatory Technical Document, Version 2.9, Revision 2*, document CCDB-2013-05-002, Common Criteria Develop. Board, Gaithersburg, MD, USA, May 2013, [Online]. Available: http://www.commoncriteriaportal.org/files/supdocs/CCDB-2013-05-002.pdf

[36] M. Anik, R. Saini, S. Guilley, J.-L. Danger, and N. Karimi, "Failure and attack detection by digital sensors," in *Proc. Eur. Test Symp. (ETS)*, Tallinn, Estonia, 2020, pp. 1–2.

[37] S. Guilley, A. Facon, and N. Bruneau, "Quantitative digital sensor," Patent EP3 506 548 A1, Nov. 2018.

[38] W. He, J. Breier, and S. Bhasin, "Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks," in *Proc. Security Privacy Appl. Cryptogr. Eng. Conf. (SPACE)*, 2016, pp. 27–46.

[39] *Information Technology–Security Techniques–Lightweight Cryptography–Part 2: Block Ciphers*, Standard ISO/IEC 29192-2:2012, 2012.

[40] *Nangate 45nm Open Cell Library*. Accessed: May 2019. [Online]. Available: http://www.nangate.com

[41] *HSPICE User Guide: Basic Simulation and Analysis*, Synopsys, Mountain View, CA, USA, 2016.

[42] H. Tanaka, "Information leakage via electromagnetic emanations and evaluation of tempest countermeasures," in *Proc. Int. Conf. Inf. Syst. Security (ICISS)*, vol. 4812, 2007, pp. 167–179.

[43] D. R. E. Gnad, J. Krautter, and M. B. Tahoori, "Leaky noise: New side-channel attack vectors in mixed-signal IoT devices," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2019, no. 3, pp. 305–339, 2019.

[44] M. Joye and M. Tunstall, Eds., *Fault Analysis in Cryptography*. Heidelberg, Germany: Springer, 2012, doi: 10.1007/978-3-642-29656-7.

[45] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, "An inside job: Remote power analysis attacks on FPGAs," in *Proc. Design, Autom. Test Eur. Conf. (DATE)*, Dresden, Germany, 2018, pp. 1111–1116.

Md Toufiq Hasan Anik (Graduate Student Member, IEEE) received the B.S. degree in electrical and electronics engineering from BRAC University, Dhaka, Bangladesh, in 2016. He is currently pursuing the Ph.D. degree in computer engineering with the University of Maryland Baltimore County (UMBC), Baltimore, MD, USA.

He was a Hardware Security Researcher Intern with Intel IPAS, Hillsboro, OR, USA, in summer 2020. He conducts research with the Secure, Reliable and Trusted Systems Research Lab, UMBC. His research interest includes hardware security and in particular, power analysis attacks and countermeasures, as well as sensor-assisted secure and reliable design.

Jean-Luc Danger (Member, IEEE) received the engineering degree in electrical engineering from École Supérieure d'Électricité, Gif-sur-Yvette, France, in 1981.

He is a Full Professor with TELECOM Paris, Paris, France. He is the Head of the digital electronic system research team involved in research in security/safety of embedded systems, configurable architectures, and implementation of complex algorithms in ASICs or FPGAs. He authored more than 250 scientific publications and patents in architectures of embedded systems and security, and is the Co-Founder and a Scientific Advisor of the Secure-IC company. After 12 years in industrial laboratories (PHILIPS and NOKIA), he joined TELECOM ParisTech in 1993, where he became a Full Professor in 2002. His personal research interests are trusted computing, cyber-security, random number generation, and protected implementations in novel technologies.

Sylvain Guilley (Member, IEEE) is an Alumni of École Polytechnique, Palaiseau, France, and TELECOM-ParisTech. He is a General Manager and a CTO with Secure-IC, Cesson-Sévigné, France, a company offering security for embedded systems. Secure-IC's flagship technology is the multicertified SECURYZR integrated Secure Element. Within Secure-IC, he is also the Director of "Threat Analysis" and "Think Ahead" business lines, which develop, respectively, security evaluation tools and advanced research. He is also a Professor with TELECOM-Paris, Paris, France, an Associate Research with École Normale Supérieure, Paris, and an Adjunct Professor with the Chinese Academy of Sciences, Beijing, China. Since 2012, he has been organizing the PROOFS workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems. He is also the Lead Editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of noninvasive testing tools), and ISO/IEC 24485 (White Box Cryptography). He is the "High Level Principles for Design/Architecture" Team Leader for the drafting of Singapore TR68 standard on Cyber-Security of Autonomous Vehicles. He has coauthored more than 250 research papers and filed more than 40 patents. His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods.

Mr. Guilley is an Associate Editor of the *Journal of Cryptography Engineering* (Springer). He is a member of the IACR and a Senior Member of the CryptArchi club.

Naghmeh Karimi (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer engineering from the University of Tehran, Tehran, Iran, in 1997, 2002, and 2010, respectively.

She was a Visiting Researcher with Yale University, New Haven, CT, USA, From 2007 to 2009, and a Postdoctoral Researcher with Duke University, Durham, NC, USA, from 2011 to 2012. She was a Visiting Assistant Professor with New York University, New York, NY, USA, and Rutgers University, Newark, NJ, USA, from 2012 to 2016. She joined the University of Maryland Baltimore County, Baltimore, MD, USA, as an Assistant Professor in 2017, where she leads the Secure, Reliable and Trusted Systems Research Lab. She has published three book chapters and authored/coauthored more than 50 papers in referred conference proceedings and journal manuscripts. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability.

Dr. Karimi is a recipient of the National Science Foundation CAREER Award in 2020. She serves as an Associate Editor for the *Journal of Electronic Testing: Theory and Applications* (Springer).