Using Digital Sensors to Leverage Chips' Security

Mohammad Ebrahimabadi*, Md Toufiq Hasan Anik*,
Jean-Luc Danger†‡, Sylvain Guilley‡† and Naghmeh Karimi*

*CSEE Department
University of Maryland Baltimore County
Baltimore, US

†LTCI, Télécom Paris
Institut Polytechnique de Paris
Paris, France

‡Secure-IC S.A.S.
Think Ahead Business Line
Paris, France

***Abstract*—One way for an attacker to break a system is to perturb it. Expected effects are countermeasure deactivation or data corruption to disclose sensitive information. The prevention of such actions relies on detection of abnormal operating conditions. Digital sensors can play this role. A digital sensor is built out of the very same standard cells as the user logic to be protected. This ensures the advantage that the sensor and the user logic are exposed to the same stress. Balancing True positives and False negatives is a tough question in field of sensors. This is a general issue, and the best way to mitigate this paradox is to thoroughly investigate their properties, through simulations and real experiments. This results in characterizations, which in turn allows for intuitions on how to handle sensing values. In this paper, we exhibit the complex relationships between propagation times in logic and environmental conditions. Those results reinforce the relevance of the digital sensor versus the adversarial manipulation of environmental conditions: fewer false alarms are raised even if temperature (resp. voltage) is extreme, provided the effect is balanced by voltage (resp. temperature). Owing to the complex relationship between propagation delays, temperature and voltage, this cannot happen with a set of independent temperature and voltage sensors.**

I. Introduction

The physical challenges incurred by the rapidly shrinking feature size and reduced power supply voltage of deep submicron semiconductor fabrication technologies continue to give rise to various design robustness and security concerns. In practice, chips are designed to work in well-defined environmental conditions (e.g., within a specific range of temperature and voltage), deviation of which can result in circuits' wearout and jeopardizing their reliability and/or security. In addition, process variations that occur due to the imperfections of semiconductors' fabrication process can impact the chip performance. Accordingly, foundries define so-called PVT (short for Process-Voltage-Temperature) corners in which chips are supposed to function nominally.

Although the integrated circuits are supposed to be placed under the PVT conditions for which they have been designed, they can be subject to various stresses such as very high temperature and/or under-supply violating the intended PVT that characterized the chip at design time. Such abnormal conditions can be related to a harsh environment the circuity is embedded in (e.g., placing the chip near the explosion engine in automotive industry) or a malicious attack aiming at denial of service, malfunction or even leak of sensitive data. The problem is exacerbated for cryptographic devices which are supposed to enhance security and conceal the data being processed. The violation of PVT corners in these chips can result in catastrophic consequences such as secret keys leakage by fault analysis [1]. Accordingly, sensing temperature and voltage is highly crucial for embedded systems to be able to optimize the performance, and detect (and in some cases prevent) unintentional chip failures as well as intentional attacks. To notify the user when a chip is working out of the expected PVT conditions, and in turn to leverage the chip's reliability and security, sensors are being embedded in the target chips. These embedded sensors raise an alarm to call for proper action when the underlying chips operate out-of-specification.

The costly post-fabrication calibration of the analog sensors (to account for the process variations) and the difficulty of their adaptation to new technological nodes make analog sensors [2] less suitable compared to their digital counterparts. Digital sensors have been introduced in low-power literature (e.g., for finetuning the Dynamic-Voltage-Frequency-Scaling [3]), and in 2011 in the security-related literature [4, Fig. 14, page 189] and were used thereafter in industry [5] and government sectors. As will be discussed in more details in Section II, digital sensors consider the operating environmental conditions as a whole, i.e. they are sensitive to temperature, voltage and process altogether, without precise knowledge about each. This results in a lower false alarm rate compared to the analog sensors that consider each of these conditions separately.

In this paper, we first motivate using digital sensors by comparing the digital and analog sensors from different perspectives, confirming the superiority of digital sensors over their analog counterparts. We then discuss our method for the deployed digital sensor's characterization and present both simulation and FPGA results confirming such characterization is highly applicable and can be used for sensing environmental conditions (i.e., voltage and temperature) and in turn detecting attacks as well as unintentional malfunctions.

II. Analog Versus Digital Sensors

Historically, analog sensors have been developed and integrated in electronic systems as transducers converting a given environmental condition (such as temperature T and voltage V) into quantized values, which can be read from within an electronic chip. Obviously, analog sensors can be leveraged as alarm generators. The rationale is straightforward: a predefined threshold [6] is defined, and the sensor's output is compared to it. The alarm is raised as soon as the sensor's output value is beyond the threshold. However, these sensors suffer from different weaknesses. Amongst them, we can stress:

- the difficulty of their calibration after manufacturing has received a lot of attention in recent years [7];

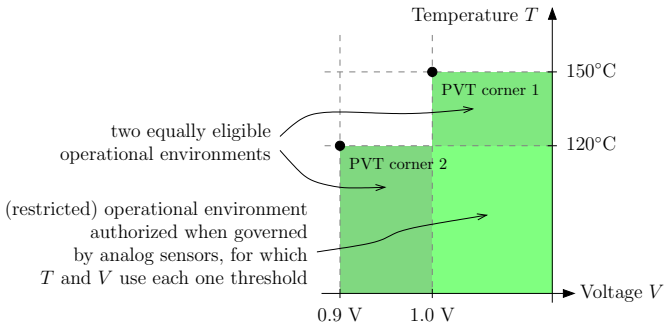


Figure 1. Example of a chip allowed to work in two operational conditions, and intersection of those, as the only authorized working condition in the presence of two analog sensors.

- the fact that their technology (e.g., using large transistors) differs from that of the user digital logic, thus their behavior after aging differs and the threshold becomes less relevant;
- an analog sensor generates false alarms, because it needs to make "hard decisions"; if the nominal operating conditions are defined by several PVT corners, say $T < 150$°C and $V > 1.0$ V, and say $T < 120$°C and $V > 0.9$ V, then the design would have no other choice than setting the temperature threshold at 120°C and the voltage threshold at 1.0 V. This situation is illustrated graphically in Fig. 1.

Below we explore the weaknesses of analog sensors and motivate the reasons behind deploying digital sensors in this study.

A. Architecture

In general, analog sensors are designed in full custom layout. Given the peculiarity of those structures, they happen to be hard to calibrate [7]. In contrast, digital sensors are entirely composed of digital standard cells. Their behavior can be modeled at logical level: contrary to analog sensors, which require electrical (e.g., SPICE) simulation, digital sensors can be simulated using an event-driven simulation engine (e.g., Mentor Graphics ModelSim). Hence, the dimensioning of digital sensors is cheap [8]. Moreover, they are not specific to any given environmental condition, and instead react in synchronization with the user digital logic [4, Fig. 14, page 189].

In terms of portability, analog sensors require revalidation by new simulations when the technology Physical Design Kit (PDK) is updated, and a complete redesign when changing technology from a foundry or when moving to another foundry. On the contrary, digital sensors simply require a basic recalibration (length of the delay chain) in any of those situations.

B. Efficiency

Digital sensors are highly more optimized regarding area and power compared to their analog counterparts. Such optimization is achieved during the synthesis process in the automated design flow. In contrast, optimization is barely possible for the analog sensors in which calibration is manual. Moreover, analog sensors depend on the "always-on" logic gates consuming power continuously, whereas digital sensors are more controllable and never consume power unless they face toggling [9] on clock edge. Digital sensors can also easily be clock-gated for further power saving, and can be calibrated to work in different Dynamic Voltage/Frequency Scaling (DVFS) configurations.

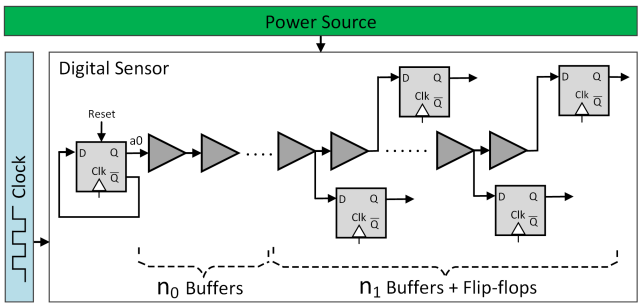


Figure 2. The architecture of the target digital sensor.

C. Sensitivity

Both digital and analog sensors suffer from process variation and dynamic noise. However, analog sensors counter ambiguities in defining a threshold for nominal vs abnormal situations, while their digital counterparts resolve this issue via electrical level discretization [10]. This implies that digital sensors can be made *smart*, i.e., their digital output can be processed by intelligent algorithms to make the most of the raw digital status they produce [11], [12].

D. Resistance against attacks

Analog sensors are more prone to attacks compared to their digital counterparts. This is due to their implementation using full custom layout, which differs the sensors from the rest of the *intractable* sea of gates. Accordingly, an adversary can easily identify the analog sensor embedded in the chip (e.g., Fig. 21 in [13]), and bypass it. In terms of Common Criteria [14, §5.2, page 24], such invasive attack is considered realistic, therefore digital sensors provide a decisive advantage over analog sensors, in terms of security certification.

E. Accuracy

In terms of failure or attack detection, analog sensors generate more false alarms than digital sensors [12]. This is because analog sensors deal with physical quantities separately (e.g., voltage alone, temperature alone, etc.), i.e., detecting if the temperature is beyond a threshold or voltage is below another threshold. Accordingly, they fail to consider that the circuit may work properly even under a low voltage if the temperature is low at the same time, or high temperature and high voltage simultaneously. Such hard decisions result in more false alarms raised by analog sensors than the digital ones. In contrast, digital sensors need only one threshold in the full temperature-voltage plane (namely, the AFN—detailed subsequently in Section IV). Such soft decisions made by digital sensors would result in false alarms in analog sensors.

III. Motivation

Digital sensors are meant to sense environmental conditions. This can allow to detect safety issues (e.g., hazards) as well as security concerns (e.g., attacks). Digital sensors are thus leveraged in industrial products certified according to one or more of the following standards:

- IEC 61508 in general and ISO 26262 for automotives,
- Common Criteria (ISO/IEC 15408), ISO/IEC 19790 (or USA NIST FIPS 140-3) for cyber-physical standards.

IV. Target Sensor

A digital sensor can be realized via inserting artificial critical paths (as simple as delay chains) into the chip logic such that if the chip is operated in abnormal conditions, setup time violations occur in the first place on the sensor intentionally long path [15]. A rising or a falling edge feeds this delay chain, and it is checked if such an edge manages to propagate to the end of the chain at the considered clock period [4, Fig. 14]. Failing to do so is the evidence of environmental disruptions or manipulations. A number of flip-flops are inserted in different parts of this delay chain to be able to sample the delay chain and characterize the amplitude of the timing violation, and thus digitize the amount of stress applied to the circuit [16].

Figure 2 shows the digital sensor deployed in this paper. It includes n_0 leading buffers as well as n_1 buffers each feeding a D flip-flop. The sensor outcome is represented by the output of these flip-flops working under the same clock signal at frequency F. The first buffer is fed with a toggle flip-flop generating a periodic signal $a0$ with the frequency of $F/2$. Note that the number of buffers and flip-flops are decided based on the operational range of the underlying circuitry embedded in the same chip. In fact, based on their applications, chips are usually designed in different temperature grades (e.g., commercial, industrial, military, etc) each consider a different range of temperatures under which the chip is expected to be functional. In practice, this sensor is a transducer from "time" (collected as "delays") into alarms raised when the operating condition is not in the predefined range of operation.

This digital sensor considers the voltage and temperature together, not as separate quantities. The idea behind this is that a circuit may still operate properly even if one of its temperature or voltage quantities is out of the range given that the other quantity can compensate for it, e.g., the device is functional in case of $T > T_{worst}$ provided that V is large enough to make up for the unpropitious temperature condition.

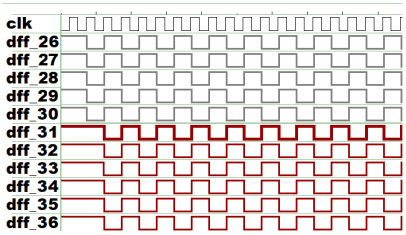
Sensor Characterization: To characterize the sensor status and raise an alarm when the circuitry is working out of the expected range of operating condition, we deploy a metric, so-called Average Flip-flop Number (AFN), that is extracted based on the flip-flop outputs in each voltage and temperature combination, noted as (V, T) hereafter. The idea behind using this metric is that the propagation delay of the buffers resided in the delay chain of the deployed digital sensor (shown in Fig. 2) is affected by the temperature and voltage quantities, and so a different set of values are captured by the embedded flip-flops in different (V, T) combinations. In other words, in each clock cycle of CC_i, when this sensor is fed with $a0$, the first FN_i 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 $1 \rightarrow 0 \rightarrow 1$), where FN_i refers to the index of flip-flop in which phase $\overline{\text{A}}$ starts in clock cycle CC_i. The value of FN_i changes in different (V, T) combinations. The average of all FN_is over all clock cycles, so-called AFN, is used for characterization.

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 (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, and FN_i would be higher. Note that process variations (P) can also affect the AFN value.

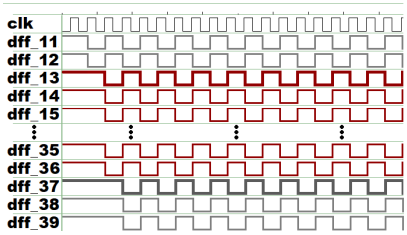
Fig. 3 shows sample waveforms for the sensor of Fig. 2 in different (P, V, T) combinations as well as the related AFN values. The waveforms extracted from the sensor with n_0 =9 leading buffers followed by n_1 =43 buffers and flip-flops. As shown the slower the circuit (due to voltage and temperature conditions) the lower the AFN. This figure also shows that due to process variations the AFN may slightly change from chip to chip. However, such change is not significant.

V. Experimental Setup and Results

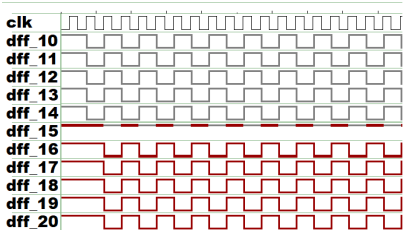
We present two sets of results: one based on HSpice simulations and the other based on the FPGA implementation. The number of buffers and flip-flops realizing these sensors are different. This is due to the different technologies they realize.



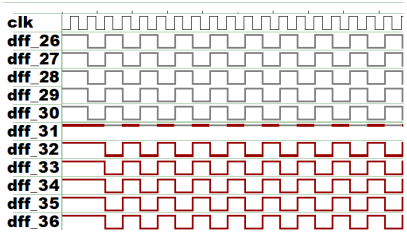
(a) V= 1.2V, T= 27°C, P= 1



(b) V= 1.0V, T= 120°C, P= 1



(c) V= 1.2V, T= 120°C, P= 1



(d) V= 1.2V, T= 27°C, P= 2

Operating Conditions	AFN
V= 1.2, T= 27°C, P= 1	31
V= 1.0, T= 120°C, P= 1	13
V= 1.2, T= 120°C, P= 1	15.5
V= 1.2, T= 27°C, P= 2	31.5

(e) AFN of Fig. 3(a), 3(b), 3(c), 3(d)

Figure 3. Waveforms of Fig. 2 in different operating conditions. Voltage, temperature and process are displayed with their initial letter V, T, and P, respectively.

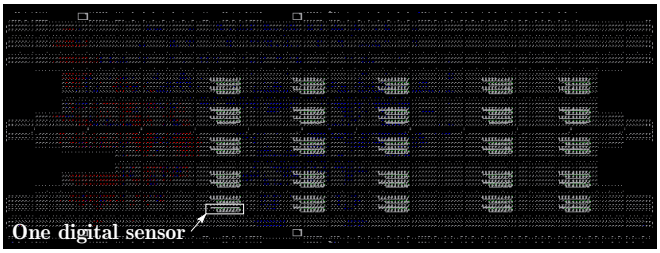


Figure 4. The layout of the 50 sensors (10×5) implemented on a single Spartan 6 FPGA resided on a SAKURA-G board (rotated 90° in this figure).

For the simulation model, our sensor circuitry includes n_0=9 leading buffers followed by n_1=43 buffers and flip-flops (refer to Fig. 2). This sizing has been determined in order to have at least one phase change for all the PVT corners, for the range of (V, T) we considered in this study, as explained in Section IV. For the simulation, the sensor circuitry has been implemented in the transistor level using 45-nm NANGATE technology [17], and the simulation has been conducted by Synopsys HSpice. We realized 16 different sensors (to show the effect of process variations and our post-fabrication calibration) using Monte-Carlo simulations with a Gaussian distribution: transistor gate length L: $3\sigma = 10\%$, threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. Each sensor was simulated for the temperatures between -10°C degree and 150°C and the voltage source (Vdd) between $0.8V$ to $1.4V$. In this set of experiments, the AFN value has been computed based on the outcome of the sensor's embedded flip-flops in 9 consecutive clock cycles.

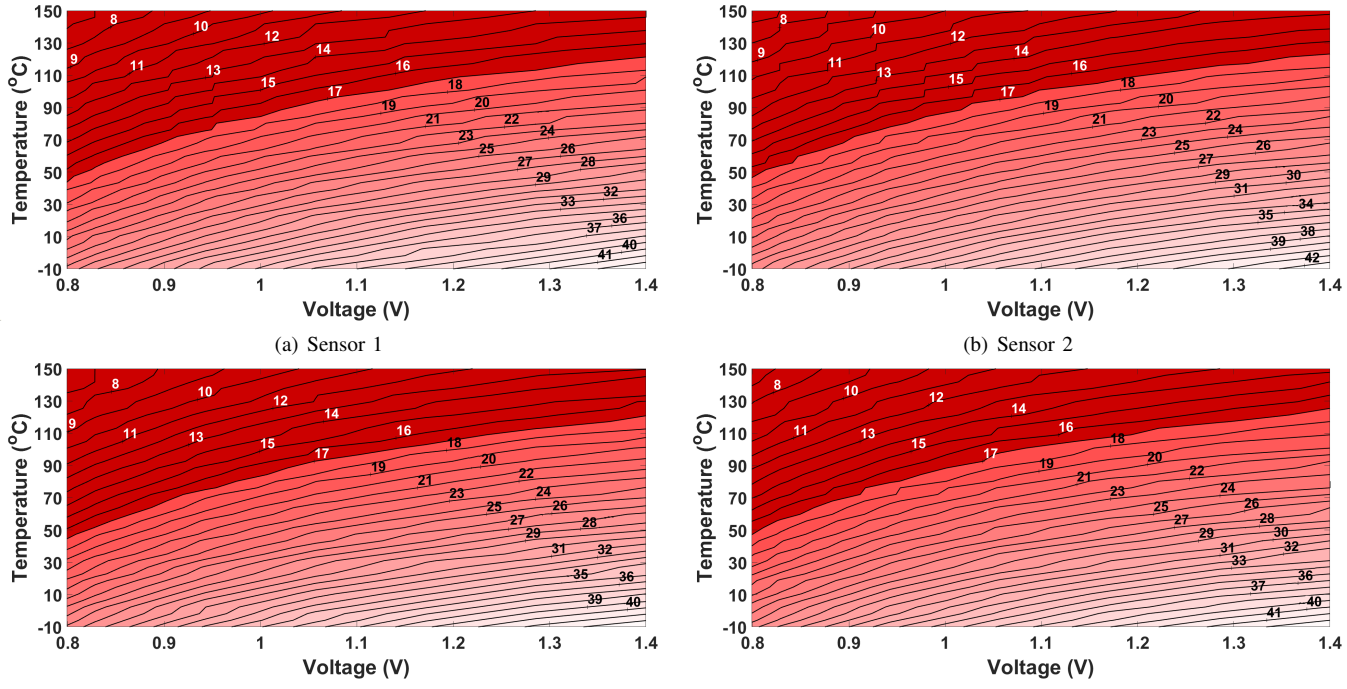
The second set of experiments realized by implementing our sensor on a Xilinx Spartan 6 FPGA resided on a SAKURA-G board. The layout is shown in Fig. 4. We implemented 50 sensors in 5 rows (on a single FPGA) each with 70 leading buffers, and 32 sampling flip-flops and their related buffers. In these experiments, the temperature changes between 0°C and 80°C and the voltage alters in the range of $0.985V$ and $1.15V$. Here, the AFN value is computed based on the flip-flop outcomes in 20 consecutive clock cycles.

In both set of experiments the threshold AFN was considered as 17. This relates to T=60°C and V=1.05V for the FPGA implementation, and T=85°C and V=1.0V for simulations.

AFN Evolution (Simulation Results): The first set of results depicts the AFN value in different voltage and temperature combinations. In particular, Fig. 5 illustrates the results for 4 Monte-Carlo HSpice simulations of the sensor. As expected in high temperatures and low voltages, lower AFN is achieved. This is because the circuit operates slower in these conditions, thus preventing the edge fed from the leading flip-flop (signal $a0$ in Fig 2) from propagating to the whole delay chain, i.e., the edge fails to propagate to the rest of the chain after passing a couple of flip-flops. Similarly, in cases where the circuit operates faster (i.e., higher voltages and lower temperatures) higher AFN values are attained.

Note that the contour plots depicted in Fig. 5 illustrate the isohypse lines in term of AFN, and it is clear that the relationship is not linear with respect to temperature and voltage. Thereby, the definition of simple eligible operational environment "templates" (cf. Fig. 1) would not respect the delay behavior of the studied technology.

Another interesting observation from Fig. 5 is the effect of process variations on the AFN value achieved in each (V, T). The four contour plots (related to 4 Monte-Carlo simulations of the sensor) depicted in Figures 5(a)-5(d), although seem very similar they have some differences regarding AFN values in some (V, T) combinations. For example, Sensor 3 results in AFN=16.89 in (V, T)=(0.95V, 75°C), while Sensor 4 relates this operating condition to AFN=18. Such difference may be



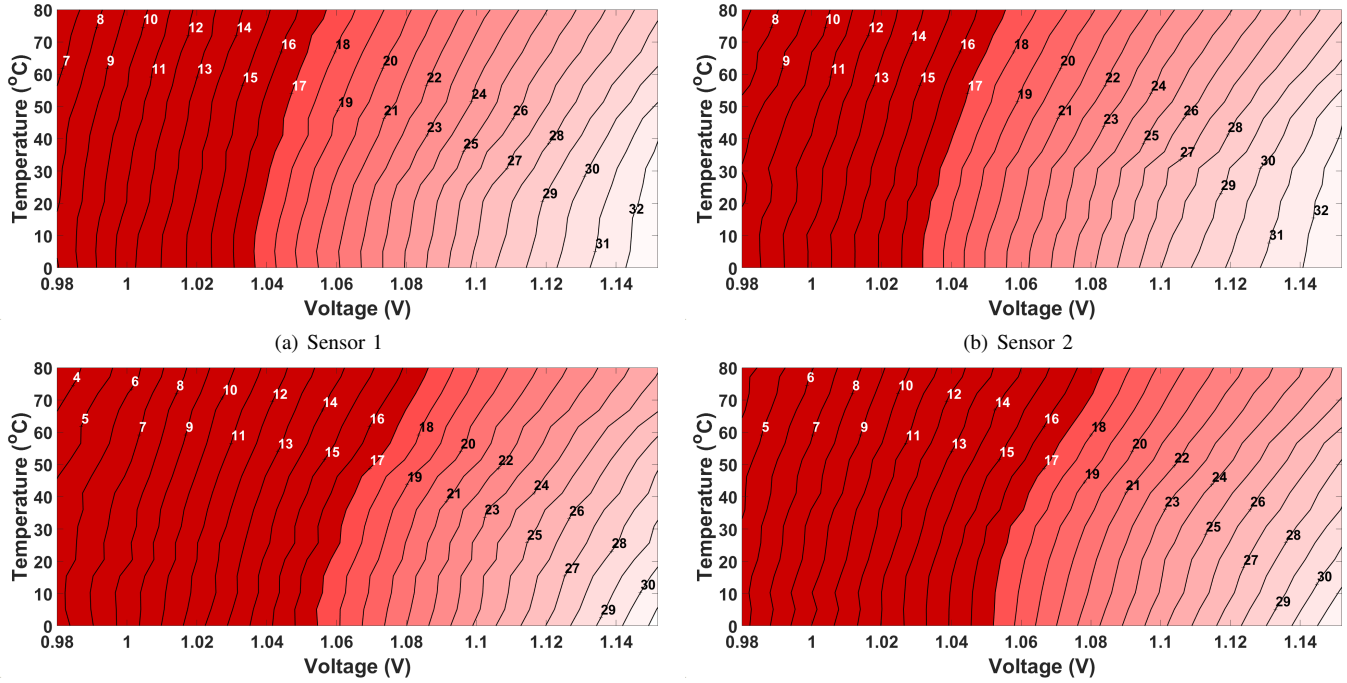
(a) Sensor 1

(b) Sensor 2

(c) Sensor 3

(d) Sensor 4

Figure 5. AFN variation in different voltage and temperature pairs for 4 sample sensors realized by simulation.



(a) Sensor 1

(b) Sensor 2

(c) Sensor 3

(d) Sensor 4

Figure 6. AFN variation in different voltage and temperature pairs for 4 sample sensors realized on FPGA.

insignificant in simulation results as the HSpice simulations do not include placement and routing information. However, as we will show below, the real-silicon results (FPGA implementation in our case) demonstrate a higher effect of process variation on the AFN values.

AFN Evolution (FPGA Implementation): Fig. 6 illustrates the AFN values for four sensors (out of the 50) implemented on FPGA. As depicted, the FPGA results follow the simulation observations; confirming the applicability of AFN for sensing temperature and voltage. As mentioned earlier, the number of flip-flops and buffers are different in simulation and FPGA models, and so is the technology. Thereby, obviously our simulation and FPGA implementations result in different AFN values in the same (V, T) condition. However, the crucial observation is how these contour plots relate to the operating conditions; making our AFN-based characterization method suitable for operating condition sensing.

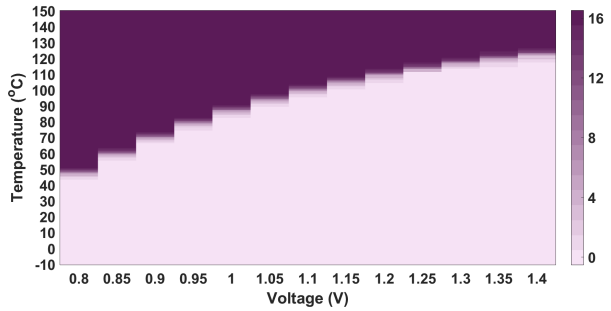
Note that the temperature for the HSpice simulations represents the junction temperature, while for the FPGA implementation the reported temperature relates to the external (environment) temperature. That's why the simulations show more sensitivity to temperature. Note that these results are given as a proof of concept and if the junction temperatures are extracted, the AFNs shown to be more sensitive to temperature in FPGA implementation as well.

Another interesting observation from the four plots shown in Figures 6(a)-6(d) is the effect of process variation which is more prominent in our FPGA results compared to the simulation, e.g., in $1.04V$ & 50°C, Sensor 1, represents the AFN value of 16.6 while the AFN value in Sensor 2, Sensor 3, and Sensor 4 is 16.8, 13.1, and 13.7, respectively.

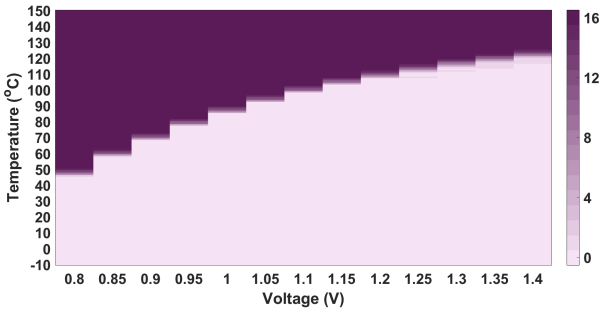
In these experiments, without loss of generality, we assumed the worst case conditions as $(1.0V, 85°\text{C})$ for simulation and (V, T)=$(1.05V, 60°\text{C})$ for the FPGA implementation, i.e., we expect the sensor to raise an alarm in any (V, T) combination if it operates slower than when works in the worst case condition. Accordingly, we considered the threshold AFN as 17 (which is related to these operating conditions according to Fig. 5(a) and Fig. 6(a)). Note that the threshold value can be extracted for each sensor based on the worst case condition under which the device is expected to work.

Assuming threshold AFN equal to 17, in Fig. 5 and Fig. 6, we illustrate the conditions in which an alarm is raised in dark red notifying that the circuit is operating slower than the worst case condition it was designed for. Another observation made from these figures is that in some operating conditions, one sensor may raise an alarm while the other may not. For example when operating under $1.06V$ and 60°C, Sensor 1 and Sensor 2 do not raise alarm as their related AFN value in this condition (17.9 and 18.2, respectively) is higher than the considered threshold for AFN (i.e., 17). However, under the same condition, Sensor 3 and Sensor 4 raise an alarm due to their lower AFN, i.e., 14.4 and 15, respectively. To decrease the effect of process variations, we propose to conduct post AFN-measurement calibration, the details and results of applying which are given through the next set of results.

Need for Post-Characterization Calibration: As shown through the previous set of results, the AFN value is sensitive to process variations. This calls for a calibration process after sensor characterization done based on the AFN factor. This process can be conducted after the fabrication process. To illustrate the process variation effects more clearly, we present the distribution of the alarms raised by each of the 16 sensors implemented through simulation as well as the 50 sensors real-

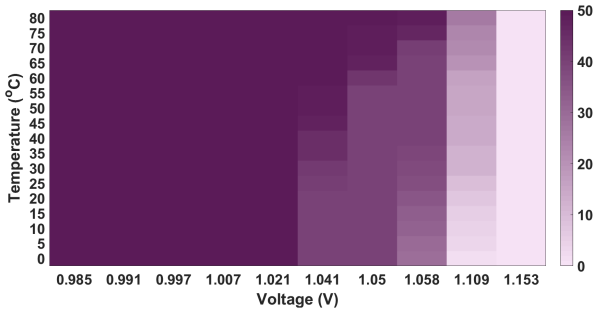


(a) Pre Calibration

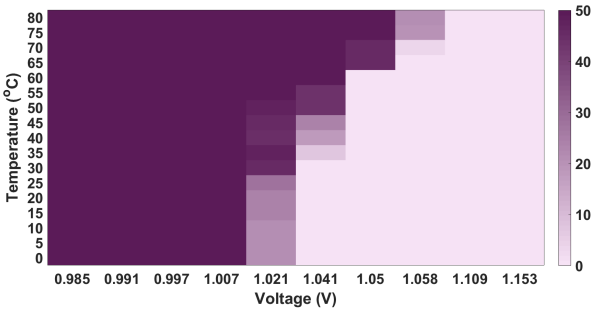


(b) Post Calibration

Figure 7. Effect of process variation on the raised alarms in 16 simulated sensors.



(a) Pre Calibration



(b) Post Calibration

Figure 8. Effect of process variation on the raised alarms in 50 sensors implemented on FPGA.

ized in FPGA in different operating conditions. The heatmaps shown in Fig. 7(a) and Fig. 8(a) depict how many of the target sensor circuits will raise alarms in each (V, T) combination for the simulation and FPGA implementations, respectively. As shown, for the simulated sensors, in 95.1% of conditions either no sensor raised an alarm or all of them raised the alarm. This shows the low impact of process variations in our simulations. However, this rate decreases to 63.5% for FPGA implementation. This confirms the need for calibration of the AFN threshold value after realization of each sensor.

To calibrate the threshold AFN, we place each sensor under the worst case condition and find the AFN. We then repeat this process multiple times (say 100) in order to mitigate noise and metastability impacts. The average of the AFNs will be used as the AFN threshold value. We conduct this process on our simulation-based as well as FPGA-implemented sensors. The post-calibration results (for the FPGA experiments) shown in Fig. 8(b), depict that after calibration, in 87.6% of the operating conditions at least 48 out of 50 sensors behave similarly (all raise alarms or all do not raise alarms) while without calibration only 68.2% of the sensors operated in a similar way. This confirms the strength of our calibration in reducing false and missed alarms.

VI. Conclusion

Sensing operating conditions is crucial for detecting anomalies and malicious attacks. Analog sensors suffer from a number of weaknesses among which the high rate of false alarms makes these sensors unsuitable when high anomaly detection accuracy is needed. Digital sensors, with considering voltage and temperature altogether, alleviate this shortcoming. This paper presents both simulation and FPGA implementation of a delay-chain based digital sensor and discusses its characterization using its embedded flip-flops' outcome. The results confirm the applicability of the deployed characterization in real-silicon.

References

[1] M. Joye and M. Tunstall, *Fault Analysis in Cryptography*. Springer-Verlag Heidelberg, March 2011, DOI: 10.1007/978-3-642-29656-7.

[2] W. Granig et al., "Calculation of failure detection probability on safety mechanisms of correlated sensor signals according to iso 26262," *SAE Int'l Journal of Passenger Cars-Electronic and Electrical Systems*, vol. 10, no. 2017-01-0015, pp. 144–155, 2017.

[3] B. Amrutur, N. Mehta, S. Dwivedi, and A. Gupte, "Adaptative Techniques to Reduce Power in Digital Circuits," *Journal of Low Power Electronics and Applications*, vol. 1, no. 2, pp. 261–276, July 2011.

[4] N. Selmane et al., "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET Information Security*, vol. 5, no. 4, pp. 181–190, 2011.

[5] S. Guilley, R. Newell, and T. Porteboeuf, "Reliability analysis of digital sensors against perturbations of FPGAs," in *Cryptarchi*, July 2014.

[6] R. Possamai et al., "A bulk built-in sensor for detection of fault attacks," in *HOST*, 2013, pp. 51–54.

[7] D. Shahrjerdi et al., "Shielding and securing integrated circuits with sensors," in *ICCAD*, 2014, pp. 170–174.

[8] S. Guilley and T. Porteboeuf, "Device and method for calibrating a digital sensor," Patent, May 24, 2017, Patent EP2960665B1.

[9] A. De Marcellis et al., *Analog Circuits and Systems for Voltage-Mode and Current-Mode Sensor Interfacing Applications*. Springer, 2011.

[10] G. van der Horn and J. L. Huijsing, *Integrated Smart Sensors: Design and Calibration*. Springer, 2012, vol. 419.

[11] S. Guilley et al., "Quantitative digital sensor," Patent, EP3506548A1.

[12] M. T. H. Anik et al., "On-chip voltage and temperature digital sensor for security, reliability, and portability," in *ICCD*, October 18-21 2020.

[13] D. Akella et al., "A 0.2 V, 23 nW CMOS Temperature Sensor for Ultra-Low-Power IoT Applications," *Journal of Low Power Electronics and Applications*, vol. 6, no. 2, June 2016.

[14] Common Criteria Development Board, "Application of Attack Potential to Smartcards, Mandatory Technical Document, Version 2.9, Revision 2, CCDB-2013-05-002," May 2013.

[15] M. T. H. Anik et al., "Detecting failures and attacks via digital sensors," *IEEE TCAD*, 2020, DOI: 10.1109/TCAD.2020.3020921.

[16] M. T. H. Anik, S. Guilley, J.-L. Danger, and N. Karimi, "On the effect of aging on digital sensors," in *VLSI Design Conf. (VLSID)*, 2020.

[17] "Nangate 45nm open cell library," "http://www.nangate.com".