On the Effect of Aging on Digital Sensors

Md Toufiq Hasan Anik, Sylvain Guilley, Jean-Luc Danger, Naghmeh Karimi

▶ **To cite this version:**

Md Toufiq Hasan Anik, Sylvain Guilley, Jean-Luc Danger, Naghmeh Karimi. On the Effect of Aging on Digital Sensors. 2020 33rd International Conference on VLSI Design and 2020 19th International Conference on Embedded Systems (VLSID), Jan 2020, Bangalore, India. pp.189-194, 10.1109/VLSID49098.2020.00050 . hal-03034857

HAL Id: hal-03034857

https://telecom-paris.hal.science/hal-03034857v1

Submitted on 7 Jul 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the Effect of Aging on Digital Sensors

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

*CSEE Department
University of Maryland Baltimore County
Baltimore, MD 21250
{toufiqhanik, nkarimi}@umbc.edu

†LTCI, CNRS, Télécom ParisTech
Université Paris-Saclay
75013 Paris, France
firstname.lastname@telecom-paristech.fr

***Abstract*—Sensing environmental variables is an important step for autonomous devices which operate in different conditions. For this purpose, the digital chips embed sensors, preferably digital for portability reasons, to ensure that they are not operating out-of-specifications. However, a digital sensor is exposed to various stress as well as aging during its lifetime. Aging makes the sensors' output deviate from the original intended one, resulting in an incorrect report of the operating condition and in turn improper actions based on such reports. This paper presents a thorough study on the effect of aging on digital sensors. We first propose two low-overhead characterization schemes for these sensors. Then, we investigate the accuracy of such characterizations on different processes, voltages, temperatures and aging conditions. Our results show that sensors' ability to detect attacks (as well as false detections) varies with aging, notably in the first 5 years of usage. Indeed, comparing new versus aged sensor shows that 3% to 12% of the alarms that would raise if the sensor were new, will not be fired for a 5 year old device, while 15%-25% false alarms are raised for the device after 5 years of usage. This brings a great concern to the reliability as well as the security of the digital sensors which can not be used as is after aging. It is also shown that these results stay the same whatever the variation of the process. Consequently, it is recommended to associate an aging correction to digital sensors, such as in-field calibration techniques, and/or sensor replication.**

I. Introduction

Chips are designed to work in well-defined environmental conditions (e.g., within some temperature and voltage ranges). Process variation at the time of fabricating the chips also impacts the performances of the chips. For these reasons, foundries define so-called PVT (short for Process-Voltage-Temperature) corners in which chips are supposed to function nominally. However, in practice, chips are subject to various stresses, although expected to operate as intended. Examples of stress are: very hot atmosphere and/or under-supply, which clearly violates the intended PVT characterized the chip at design time. Reason for such stress can be due to chips being used in harsh environments (in the automotive industry, chips must operate close to explosion engines or electric engines, both generating strong fields and high temperatures; in space or nuclear plants, similar situations occur, etc). Abnormal behaviors can also be caused by physical attacks intended to disrupt the chip normal operation. Example of attacks are intentional instruction skip(s) in processors (e.g., to bypass some verifications or to hijack the execution flow), and corruption of data or code in cryptographic applications to recover some information of the secret keys (refer to [1]). It is therefore necessary to equip chips with sensors raising alarms when the chips are operated out-of-specifications caused either by the harsh environment or attacks.

Reaction to a raised alarm is a logical action that reflects the safety/security policy in place. However, it depends on the quality of detection. It is therefore paramount that sensors achieve their function reliably. Whilst those are calibrated at design time but need to operate properly along the whole life-cycle of the chip. Thereby, to be able to perform a proper reaction, the unavoidable aging effects in the deployed sensors should be taken into account. In practice, with the advance of VLSI technology and moving towards smaller feature sizes, the effect of aging mechanisms has increased [2]. Aging-related degradation may result in transistors' parameters shift during the operation time and eventually performance degradation and/or functional failures of the sensors [3]. Thereby, characterizing the impact of aging degradation on sensors is crucial. *In this paper, we investigate how digital sensor (DS) outputs deviate over time and how frequent calibration is required to compensate such effect.* Among aging mechanisms, the effect of Negative-Bias Temperature-Instability (NBTI) and Hot-Carrier Injection (HCI) are more dominant than other aging mechanisms [4]. In this paper, we focus on these two aging mechanisms, use a digital sensor as a target, and investigate how the sensor output is affected via PVT and aging. We then discuss how such effects can be treated via calibration. The contributions of this paper are as follows:

- Two aging characterization methods to assess the impact of aging on a digital sensor;
- Detailed HSpice MOSRA simulations to evaluate the effect of NBTI and HCI degradation on different Voltage, Temperature and Process;
- In-field sensor calibration suggestions to compensate for the effect of aging.

The rest of this paper is organized as follows. Section II presents the preliminary backgrounds on aging mechanisms and describes the digital sensor used in this study. Section III presents the proposed characterization schemes to evaluate the impact of PVT and aging on digital sensors. Section IV presents the results. Conclusions and future extensions of this research are drawn in Section V.

II. Preliminary Backgrounds

A. Detection for Safety vs Security

At this stage, it is worth recalling the basic difference between chip *safety* and *security* objectives. A chip failing

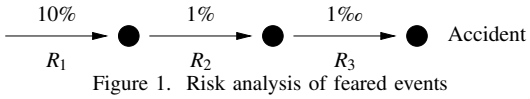


Figure 1. Risk analysis of feared events

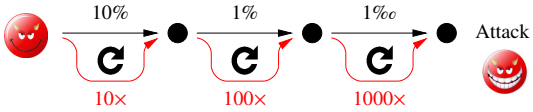


Figure 2. Security analysis of feared events

can of course constitute a security issue, but the natural question regards the probability of such event occurring. Safe systems employ risk analysis methodological tools to rate possible failures. We generally represent failures according to their probability of occurrence. In failure paths, several malfunctions may occur (independently), hence a risk probability is being estimated as the product of each individual feared event (see Fig. 1). However, when envisioning security failure, considering realistically, each failure step is prepared conscientiously. This results in an (updated) probability of attack considering the worst case between events involved in the attack paths. Figure 2 illustrates (numerically) this fact.

B. Background on Digital Sensors

Sensing environment conditions is delicate in practice: indeed, deviations from nominal conditions are multiple (temperature, voltage, exposure to intense fields and/or irradiation by particles, etc). As a result, 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 [5].

Digital sensors (DS) consist of artificial critical paths inserted into the chip logic: in case the chip is operated in abnormal conditions, setup time violations occur in the first place on the digital sensor intentionally long path. This path is usually as simple as a delay chain. The idea is to assess whether an edge (positive or negative) manages to propagate until the end of the chain within each and every clock period. (refer for instance to [6, Fig. 14, page 189]). Failing to do so is the evidence of some environmental disruption or manipulation. In practice, in order 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—somehow, it enables to digitize the amount of stress applied to the circuit.

Figure 3 represents the digital sensor we target in this research. The sensor includes a chain of 64 buffers. The last 33 buffers in this 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. In addition, the first buffer is fed with a toggle flip-flop generating a periodic signal $a0$ working at $F/2$. The clock frequency should be determined precisely such that when the circuit is fed with $a0$, the first half of flip-flops are in phase A (say $0 \rightarrow 1 \rightarrow 0$) and the second half in the complementary phase $\overline{\text{A}}$ (say $1 \rightarrow 0 \rightarrow 1$) . This property will be used afterwards for characterization as will be discussed in Section III. Note that the clock frequency is determined for the nominal condition (i.e., Power Voltage Vdd = 1.2V and Temperature = 25°C) for a new device. Figure 4 shows the

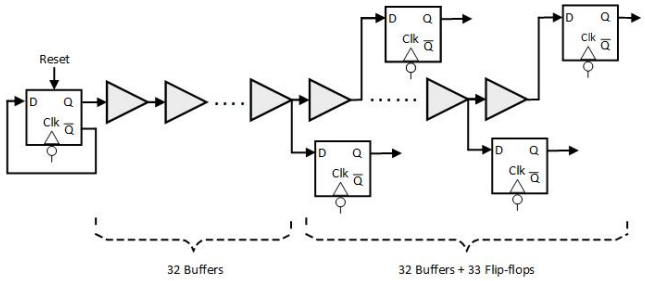
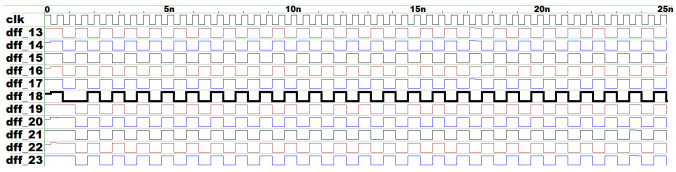
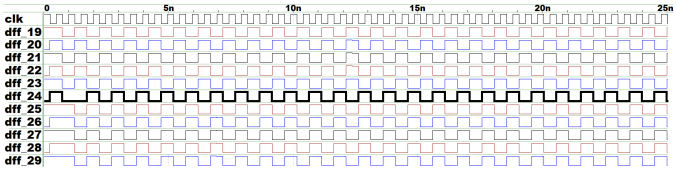


Figure 3. Architecture of the deployed digital sensor.

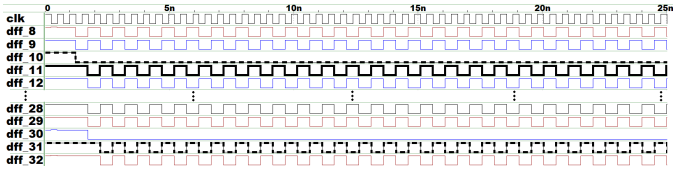
waveforms representing the flip-flop outputs in different conditions. In particular, Fig. 4(a) depicts the flip-flop outputs in the nominal condition of the new (no-aged) sensor. As shown, the first phase change occurs in the 18th flip-flop (*dff_18*), the first 17 flip-flops have the same phase A and the last 16 flip-flops are in complementary phase $\overline{\text{A}}$. This trend is changed when the circuit operates under different voltage/temperature or aging conditions. For instance, Fig. 4(b) represents the sensor outcome when the temperature is 0°C. In this case, the first change occurs in the 24th flip-flop (*dff_24*). Fig. 4(c) shows the status of the sensor operating under Vdd = 1.4V and temperature = 40°C after 7 years of usage. In this condition, multiple phase changes can be observed, as well as metastable states, i.e., both *dff_11* and *dff_31* experience a value different from their previous flip-flops which have a constant value due to metastability at sampling time.



(a) Voltage = 1.2V, Temperature = 25°C, Age = 0



(b) Voltage = 1.2V, Temperature = 0°C, Age = 0



(c) Voltage = 1.4V, Temperature = 40°C, Age = 7 years

Figure 4. Flip-flop outputs in different conditions.

C. Background on Aging

Aging mechanisms including Negative-Bias Temperature-Instability (NBTI), Hot-Carrier Injection (HCI), Time-Dependent Dielectric Breakdown (TDDB), and Electro-Migration (EM) result in performance degradation and eventual failure of digital circuits over time [7]. Among all, NBTI

and HCI are the two leading factors in the performance degradation of digital circuits [4]. Both mechanisms 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, 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, 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 [8]. The last three parameters (so-called external parameters) are used as acceleration factors of the aging process. Figure 5 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.

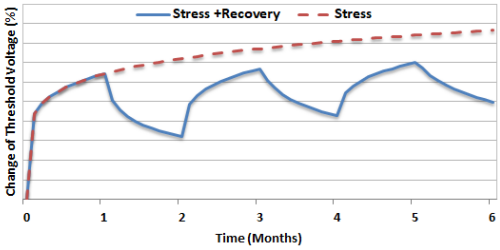


Figure 5. Threshold-voltage shift of a PMOS transistor under NBTI effect[3].[2]

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 highly sensitive to the number of transitions occurring in the gate input of the transistor under stress. HCI rate is dependent on temperature, clock frequency, usage time, and activity factor of the transistor under stress, where activity factor represents the ratio of the cycles the transistor is switching and the total number of cycles the device is utilized [4].

III. Digital Sensor Characterization

In this paper, we deploy two different methods to characterize the status of the utilized sensors and investigate how the sensors' outcome can be affected via change of temperature/voltage/process condition and/or device aging.

A. Difference-Based Method (DBM):

The first scheme, so-called Difference-Based Method (DBM), compares the output of first and middle (17th) flip-flop with each other and report an anomalous if they don't match. The comparison is performed over multiple clock cycles and any mismatch in any clock cycle fires an alarm. For example, for the condition shown in Fig. 4(c), DBM characterization scheme raises an alarm. This method is more suitable for the cases in which the circuit operates under higher temperature or lower voltage, i.e., operates slower than expected. As in such cases, the propagation delay of flip-flops are increased, thereby although the clock frequency had been set such that the 18th flip-flop experiences the first phase change, the change occurs in a flip-flop with a lower index. Aging also makes the circuit slower and result in raising alarms when DBM scheme is used. Regarding the hardware overhead, DBM overhead is slightly negligible as it can be implemented using a single XOR gate.

B. Average-based Method (ABM):

Our second characterization scheme is referred to as Average-Based Method (ABM). In this scheme, the first flip-flop (among all 33 flip-flops) that experiences a change in its output (compared to its prior flip-flop) is determined in each clock cycle of CC_i. The index of that flip-flop is referred to as Flip-flop Number (FN_i). Then the average of all FN_is over all clock cycles is calculated. This average, so-called Average value of Flip-flop Number (AFN) is used for characterization. In practice, the AFN for the nominal condition in our sensor is 18, since as mentioned in Section II-B, the clock frequency is chosen such that the first change occurs at the 18th flip-flop. For characterization and detection purpose, the AFN is calculated at runtime and compared with the nominal AFN. In case of a mismatch, an alarm is fired.

Due to the change of operation conditions, the AFN is impacted. Contrary to DBM, the ABM allow to rise an alarm in both cases: either when the sensor operates slower or faster than the nominal case.

To ignore negligible changes in operating conditions and the measurement noise, we consider a confidence range around the AFN. In this paper, we consider the range between [-5,+5], i.e., any measured AFN between 18$\pm$5 is considered as acceptable, while an alarm is fired otherwise. Moreover, ABM characterization has been implemented such that in cases of multiple changes (as in Fig. 4(c)) an alarm is raised as well.

IV. Experimental Setup and Results

In this section, we first provide details of the simulation setup used to characterize the targeted sensors. Then, we present results and discuss our observations.

A. Experimental Setup

We implemented the sensor circuitry in the transistor level using 45-nm NANGATE technology [9]. We used Synopsys HSpice for the transistor-level simulations and deployed the HSpice built-in MOSRA Level 3 model to assess the effect of NBTI and HCI aging [10]. The sensor outputs were extracted for different usage (aging) times. The effect of aging was evaluated for 7 years of device operation in time steps of two months under different voltage and temperature conditions.

[2]Values on Y axis are not shown to make the graph generic for different technologies.

The sensor was simulated for temperatures between $0°C$ degree and $40°C$ with $4°C$ steps, and for the voltage source (Vdd) between 1V to 1.4V with 0.04V steps. The clock period was extracted based on the nominal condition, i.e., for a fresh (no-aged) sensor operating in $25°C$ and fed with Vdd = 1.2V.

B. Experimental Results and Discussion

1) Effect of aging on a single buffer: The first set of results deals with the impact of aging on the propagation delay of a single buffer. The data was gathered for a fresh (no-aged) device as well as the devices aged up to seven years. Figure 6 depicts how the propagation delay of a buffer changes with different values of Vdd, temperature and aging duration. From these observations, we can check that with the increase of device age, the buffer works slower. Moreover the higher the Vdd or higher the temperature, the higher the slowing rate due to aging. It clearly shows that aging effects need to considered to interpret sensor outputs.

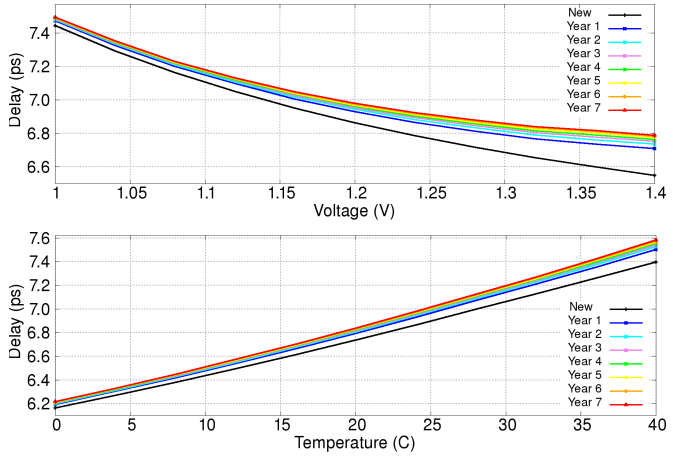


Figure 6. Effect of aging on the delay of a single buffer (a) in different voltages (Temperature = 24°C) (b) in different temperatures (Voltage = 1.2V).

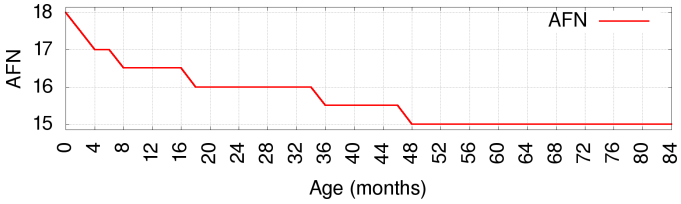
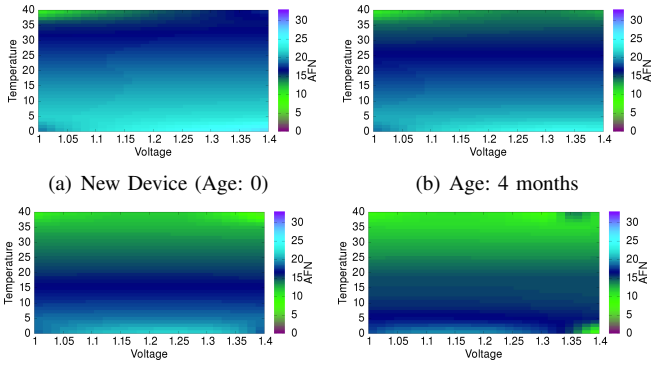


Figure 7. Effect of aging on AFN in ABM scheme (Voltage = 1.2V, Temperature = 25°C)

2) Effect of aging on ABM characterization: We first depict the impact of aging on the AFN of the ABM characterization scheme. As aging makes the sensor slower, it results in lower AFN. Figure 7 illustrates the change of AFN when the circuit is aged under the nominal condition. The AFN decreases from 18 (age: 0) to 15 after 4 years of aging.

To demonstrate the effect of temperature, Vdd and aging on the reliability of the digital sensor characterized via the ABM scheme, we generated the heatmap for different conditions as illustrated in Figure 8.



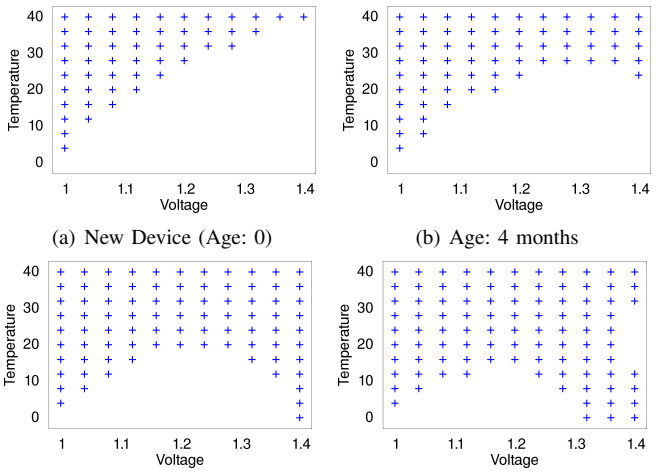
(a) New Device (Age: 0) (b) Age: 4 months

(c) Age: 2 years (d) Age: 7 years

Figure 8. Effect of aging on heatmap.

As shown in Fig. 8(a), for a new sensor operating in $25°C$, the AFN is ≈ 13.5 for Vdd = 1.0V while it increases to ≈ 21.5 for Vdd = 1.4V. Similarly, for a new sensor, operating in Vdd = 1.2V and $0°C$, the AFN represents ≈ 24 as the circuit operates faster in low temperatures while AFN for the same voltage but $40°C$ decreases to ≈ 14.5. The first takeaway points 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.

As shown in Fig. 8(b)- 8(d), the effects of aging also changes the AFN. In practice, aging increases the propagation delay of the deployed buffers, hence makes the circuit operate slower. Thereby, as expected AFN decreases with the increase of aging. For instance, for a sensor operating in $24°C$ and fed with Vdd = 1.2V, the AFN decreased to 17.5 after 4 months of usage, 16 after 2 years and 15 after 7 years of usage compared to 18.5 for a new device operating under similar voltage and temperature. The change rate of AFN is higher in the first 3 years, while it becomes slower after that. The results show that the decreasing rate of AFN is $\approx 4.5\%$ per year for the first 3 years, while for the next 4 years decreasing rate of AFN is $\approx 0.8\%$ per year. This observation is correlated with the impact of aging over time. As in CMOS circuits, the rate of aging impact is higher in the beginning while it saturates after some time of usage (Fig. 5).



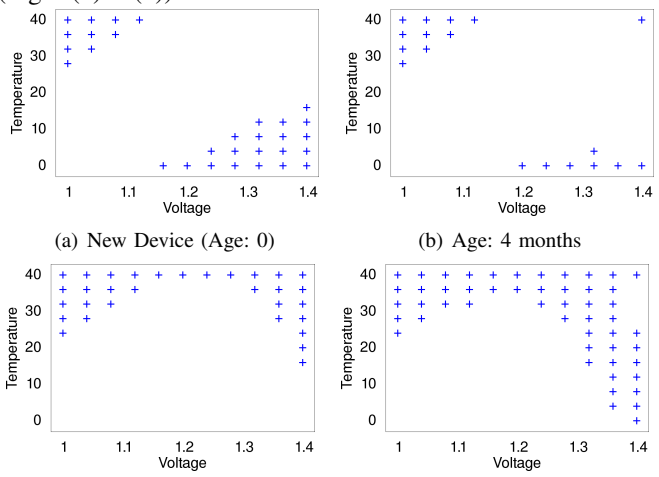
(a) New Device (Age: 0) (b) Age: 4 months

(c) Age: 2 years (d) Age: 7 years

Figure 9. Effects of aging on DBM alarms. ("+" shows an alarm)

3) Impact of aging on the raised DBM alarms: The third set of results deals with the sensor outcome when the DBM characterization is considered. As mentioned in Section III-A, the output of the first and the middle flip-flop (17th flip-flop in our sensor including 33 flip-flops) are compared with each other and any mismatch fires an alarm. When an alarm is fired, required actions are taken accordingly to preserve safety and security. However, in practice, due to the aging of sensor itself, the output of the targeted flip-flops may not match with the nominal condition even in a reasonable range for voltage and temperature, i.e., these outputs may match with the nominal outputs on a specific voltage and temperature for a new device but may differ after aging. Figure 9 shows the outcome of the DBM characterization in different aging duration. In particular, Fig. 9(a) shows the alarms fired for a new device due to such mismatch in the output of the targeted flip-flops. The first observation is that for a new device (age: 0), the alarms mainly appear in high temperatures and low voltages as such conditions make the underlying buffers operate slowly, thereby the values launched to the first and 17th flip-flop do not match.

The alarms raised in different aging durations are depicted in Figures 9(b)- 9(d). As shown, with aging, we get more alarms. The older the device, the more alarms we get. The second observation is that for aged devices, the alarms appear more in high temperatures even for high voltages. The reason is that although aging rates are affected by both voltage and temperature, the impact of temperature is more significant than voltage. Thereby, for the aged sensors, alarms will appear when increasing the temperature even for a couple of months of aging. More usage time results in a slower sensor and therefore in raising more alarms even in low temperatures (Fig. 9(b)- 9(d)).



(a) New Device (Age: 0)

(b) Age: 4 months

(c) Age: 2 years

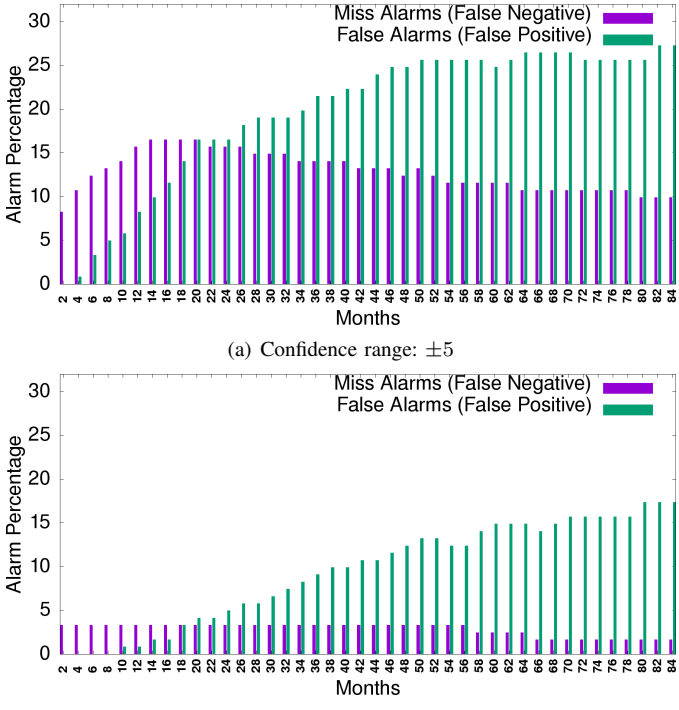
(d) Age: 7 years

Figure 10. Effects of aging on ABM alarms. ("+" shows an alarm)

4) Impact of aging on the raised ABM alarms: The next set of results deal with the outcome of the sensor when the ABM characterization method is deployed. Figure 10 shows the alarms of ABM methods in different voltage/temperature conditions and timestamps. As discussed in Section III-B, in this characterization we consider a confidence range for the extracted index. In this experiment, we consider the range between [-5,+5], i.e., as the nominal index is 18 (we have 33 flip-flops), an index between 18±5 is considered as acceptable and an index below 13 or beyond 23 fires an alarm.

Figure 10(a) depicts the alarms raised for a new device. As shown, this characterization is more sensitive to high temperatures (while voltage is low) and high voltages (when the temperature is low). The former makes the circuit slower than nominal and therefore results in lower indexes (below 13) while the latter makes the circuit faster than nominal and results in higher indexes (beyond 23). The outcome for the aged sensors is shown in Figures 10(b)- 10(d). With aging, the circuit gets slower and thereby the extracted index gets smaller gradually and finally out of range. Another observation is that with aging the alarms that were related to high voltage and low temperatures, simultaneously, disappear gradually. For example in a new device for temperature = 0°C and Vdd = 1.32V, we had an alarm while the alarm is not raised for the same condition when the circuit is aged for two years.

Comparing the outcome of ABM and DBM characterizations depicts DBM considerably results in more false alarms, thereby jeopardizing the safety. Accordingly, we recommend deploying the ABM characterization, and therefore discuss other aspects of this characterization in the following sections.



(a) Confidence range: ±5

(b) Confidence range: ±8

Figure 11. Effect of aging on miss & false alarms in ABM Characterization.

5) Miss and false alarms for ABM characterization: Raising alarms may change due to aging. In practice, when using ABM scheme, some voltage and temperature conditions may result in an alarm for a new device while considered normal when the device is aged, i.e., in our experiments, the related index is below 13 or beyond 23 for the new sensor yet in range of [13,23] for the aged one. We refer to these cases as *miss alarms*. On the other hand, there are some cases in which the

new device does not fire an alarm while the aged one does. These cases are referred to as *false alarms*. Both miss alarms and false alarms need to be taken care of. The former affects security and the latter results in privacy problems.

Figure 11(a) depicts the miss and the false alarms for the ABM scheme with a nominal AFN at 18 and a confidence interval of [-5,+5]. As shown, false alarms increase when the device is aged, yet miss alarms increase in the first 14 months and then decreases. The increase rate for false alarms is faster in the beginning, i.e., $\approx 21.5\%$ in the first 3 years, while $\approx 27.3\%$ in 7 years. On the other hand, miss alarm rate increases in the first 14 months (reaches to 16.5%) and then decreases to $\approx 10\%$ after 5 years of usage.

These results largely depend on the confidence interval and the knowledge of AFN (discussed in Section IV-B7). Figure 11(b) depicts the miss and false alarm rates for ABM with a higher confidence interval of [-8,+8]. The evolution shape of miss/false alarms with aging is rather similar but the level is reduced by a factor around 4 for the miss alarms and around 2 for the false alarms ($\approx 15\%$ after 5 years). In fact, high confidence interval is appropriate when the security is a concern while the low interval is suitable for safety concerns.

6) Process variation results: Due to process variations that occur during the manufacturing process, the specifications of the fabricated sensors can be slightly different. To quantify the impact of process variations in the outcome of the ABM characterization, we conducted Monte Carlo simulations using a Gaussian distribution: transistor gate length L: $3\sigma = 10\%$, threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. Parameters reflect a 45-nm process in commercial use today [11].

In this research, we conducted 5 Monte Carlo simulations. To be able to investigate the effect of process variations more precisely, we generated a heatmap that depicts how many of the considered circuits will raise alarms in different voltage and temperature conditions. Figure 12 shows the results. In 91.7% of conditions either no sensor raised an alarm or all of them raised the alarm. This observation confirms that process variation does not have a significant effect on the ABM sensor characterization scheme. Similar results were extracted for the aged circuit which was not shown due to the limited space.

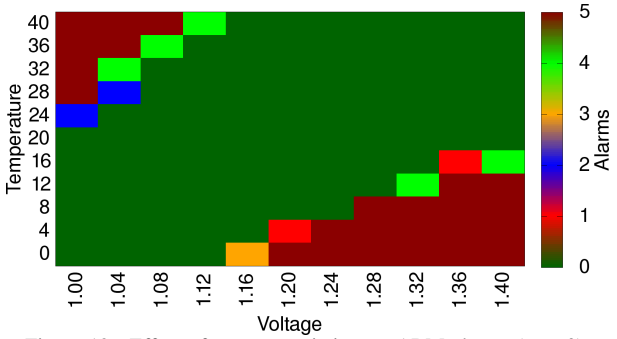


Figure 12. Effect of process variation on ABM alarms (age: 0).

7) Solutions to decrease the aging impact: This study clearly shows that the digital sensors can raise unexpected alarms, or miss required alarms with aging. Therefore, it is necessary to compensate for the time drift in order to permanently adjust the AFN to the current environment.

A first solution is to operate frequent calibration by knowing precisely the Process, Voltage and Temperature in order to take into account only the aging factor. This can be done by using embedded analog PVT sensors or operating this calibration in a laboratory with external instruments.

Another solution would be to clone the sensor such that the cloned sensor is never active, hence rarely aged. It wakes up only for the calibration phase during which a comparison with the aged sensor is carried out. The timing difference between the two sensors allows the device to know the correction that should be applied.

V. Conclusion and Future Directions

We characterized the digital sensors with respect to PVT and aging, and noticed that sensors' ability to detect attacks (as well as false detections) varies with aging. Although those figures get stable after about 4 years of usage. Thereby, digital sensors cannot be used in operational conditions as is, since after 5 years of usage, about 3 to 12% of faults are not detected and there is 15-25% of false alarms. In realistic setups, the detection condition (index between nominal plus/minus 5) shall be relaxed, which would limit the false positives. However, in that case, a larger amount of attacks will be undetected. To mitigate this issue, several independent sensors (albeit placed "close" from one another) can be leveraged. With two sensors, it is possible to correct the drifting effect caused by aging, by considering the differential output (subtraction cancels the aging effect). In addition, the accuracy of detection can be improved via machine learning techniques.

References

[1] M. Joye and M. Tunstall, *Fault analysis in cryptography*. Springer, 2012.

[2] K. Huang, X. Zhang, and N. Karimi, "Real-time prediction for IC aging based on machine learning," *IEEE Trans. on Instrumentation and Measurement*, pp. 1–9, 2019.

[3] N. Karimi et al., "Impact of aging on the reliability of delay PUFs," *J. Electronic Testing, Theory and App.*, vol. 34, no. 5, pp. 571–586, 2018.

[4] F. Oboril and M. B. Tahoori, "Extratime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *DSN*, 2012, pp. 1–12.

[5] N. Selmane, S. Guilley, and J.-L. Danger, "Practicalsetup time violation attacks on AES," in *European Dependable Computing Conf.*, 2008.

[6] 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, 2011.

[7] K. K. Kim, "On-chip delay degradation measurement for aging compensation," *Indian J. of Science and Technology*, vol. 8, no. 8, 2015.

[8] S. Khan et al., "NBTI monitoring and design for reliability in nanoscale circuits," in *DFTS*, 2011, pp. 68–76.

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

[10] Synopsys, "HSPICE User Guide: Basic Simulation and Analysis," 2016.

[11] N. Karimi and K. Chakrabarty, "Detection, diagnosis, and recovery from clock-domain crossing failures in multiclock socs," *IEEE Trans. on CAD*, vol. 32, no. 9, pp. 1395–1408, 2013.