Failure and Attack Detection by Digital Sensors

Md Toufiq Hasan Anik*, Rachit Saini*, Jean-Luc Danger†‡, Sylvain Guilley‡† and Naghmeh Karimi*
*CSEE Department
University of Maryland Baltimore County
Baltimore, MD 21250
{toufiqhanik, rachit1, nkarimi}@umbc.edu
†LTCI, Télécom Paris
Institut Polytechnique de Paris
75 013 Paris, France
firstname.lastname@telecom-paris.fr
‡Think Ahead Business Line
Secure-IC S.A.S.
75 015 Paris, France
firstname.lastname@secure-ic.com

***Abstract*—Timely notification of abnormal behaviors is essential in 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. 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 paper proposes a low-cost digital sensor that can detect system failures accurately in the designer's preferable range of operating conditions. Our experimental results show the high accuracy of this sensor in detecting circuits failure which occurred due to change of the operating temperature and supply voltage.**

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 chips with sensors raising alarms when they happen to be operated out-of-specifications caused either by the harsh environments or malevolent fault attacks. Analog sensors have been deployed for a long time in this respect. However, their adaption to new technological nodes requires an extensive re-calibration. In contrast, Digital Sensors (DS) have raised the lion's share of attention in recent years.

In highly secure applications, sensors are required to detect invasive and semi-invasive attacks, e.g., temperature and voltage attacks [1], [2] launched to extract keys from cryptographic devices. Such attacks usually place the device beyond the *worst case* condition it can tolerate. 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.

One important requirement for smart sensing is to accurately sense not only separate operating conditions, such as $T \leq T_{worst}$ and $V \geq V_{worst}$ where T_{worst} and V_{worst} denote to the worst case conditions the underlying system can tolerate, but conditions in pair (V, T) in which the circuit operates properly even if one of T or V has been violated. For example, the circuit may work properly despite $T > T_{worst}$, provided that V is large enough to make up for the unpropitious temperature condition. 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 [3]. If a timing path is not met at the clock active edge, an incorrect value is sampled and results in a single event upset (SEU).

Digital sensors 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 a delay chain. The idea is to assess whether an edge (positive or negative) manages to propagate to the end of the chain at the considered clock period [4]. Failing to do so is the evidence of environmental disruptions or manipulations. Such a snapshot can be used to digitize the amount of stress applied to the circuit [5].

In this research, we propose a lightweight DS architecture and demonstrate how it can react in terms of propagation delay to any VT (Voltage-Temperature) variation to detect failures or attacks. We target a sensor placed near a S-Box part of a PRESENT cipher in the same chip. This setup allows the designer to check the consistency of detection with real failures or attacks on the S-Box. We notably demonstrate that DSs generate less false alarms, compared to analog sensors.

II. Target Sensor

Figure 1 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. In this research, we target the S-Box of the PRESENT cipher. However, the S-Box can be replaced by any other target system. In the deployed 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.

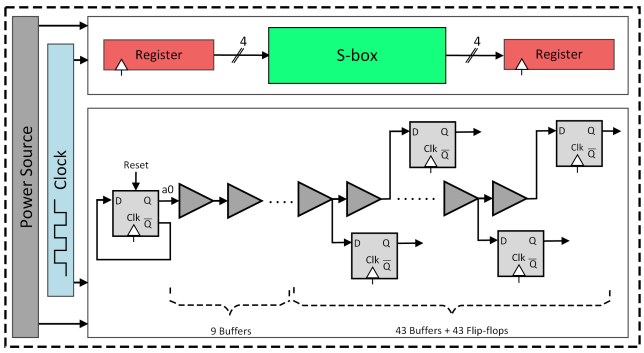
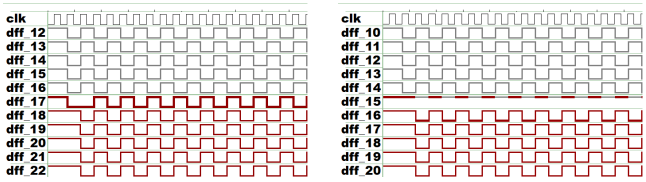


Figure 1. The architecture of the sensor-integrated target system.

The number of flip-flops and buffers included in the DS needs to be decided carefully to take both overhead and false positive/negative failure detections into account. In practice, during the design flow, operational corners are decided. Any violation from such corners may result in wrong outputs. Our proposed sensor can detect such violations as discussed below.

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 phase $\overline{\text{A}}$ ($1 \rightarrow 0 \rightarrow 1$). Here, FN_i refers to the index of the flip-flop in which phase $\overline{\text{A}}$ starts in clock cycle CC_i. We extract the average of all FN_is over all clock cycles, and use this average (AFN) for characterization [5]. Our experimental results confirm the high accuracy of this sensor in sensing operating conditions, and in turn system failure detection. The phase change happens at lower (higher) indexes when the chip is operating slower (faster) than expected.

978-1-7281-4312-5/20/$31.00 ©2020 IEEE



(a) $Vdd = 1.0V$, Temp.= 85°C (b) $Vdd = 1.2V$, Temp.=120°C

Figure 2. Waveforms of Fig. 1 in different operating conditions.

Figure 2 shows the flip-flop outputs in different operating conditions. When $Vdd = 1.0V$ and temperature = 85°C, referred to as *worst case* condition, the first phase change occurs in the 17^{th} flip-flop, i.e., the first 16 flip-flops have the same phase A and the following ones are in complementary phase $\overline{A}$. Thereby, here AFN is 17 and is referred to as AFN_{wc}. This trend is changed in other operating conditions, e.g., for $Vdd = 1.2V$ and temp.= 120°C, the FN fluctuates between 15 and 16 in different clock cycles due to metastability, hence AFN=15.5.

For characterization and failure detection, the AFN is calculated at runtime and compared with AFN_{wc}. The slower the sensor's buffer chain, the lower the AFN. Hence, AFNs lower than the AFN_{wc} denote to failure and result in an alarm.

III. Experimental Setup and Results

The sensor-integrated system targeted in this paper is the S-Box module of the PRESENT cipher [6]. The sensor and the target S-Box were implemented in the transistor level using 45-nm NANGATE technology [7]. We used Synopsys HSpice for the simulations. Both sensor and S-Box outputs were extracted under different voltage and temperatures, i.e., temperatures between -10°C and 150°C with 1°C steps, and for the voltage (Vdd) between $0.65V$ to $1.4V$ with $0.05V$ steps.

For each DS the number of leading buffers and the sampling flip-flops and their related buffers in the delay chain are extracted based on operating conditions such that whatever environmental conditions (from *worst* to *best*) are, the DS is able to sense it. The sensor design algorithm will be treated in our future research. To take the effect of process into account, the threshold value of AFN is calibrated after fabrication, and is stored locally in a One-Time Programmable (OTP) memory to be used as a reference during the chip lifetime.

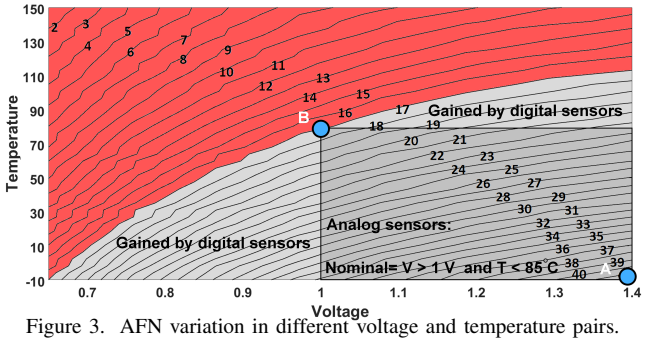


Figure 3. AFN variation in different voltage and temperature pairs.

Figure 3 shows the AFN in different voltage/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 towards lower temperatures and higher voltages. For example, in the room temperature (27°C) when $Vdd = 1.2V$, AFN is 31. This value increases to 40, when $Vdd = 1.4V$ and temp.=0°C, and decreases to 15 in case of $Vdd = 1.0V$ and temp.=100°C. This observation confirms that using AFN signatures can be useful to report sensing conditions as it is highly sensitive to the operating voltage and temperature.

We deploy the sensor's AFN for system's failure detection, i.e., to predict if the system works properly or not based on the operating conditions. In this paper, our S-Box works properly in temperatures below 85°C and with a Vdd beyond 1.0V. As shown in Fig. 3, the AFN is equal to 17 in this condition (shown with point *B*). 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 observation from Fig. 3 is the comparison between analog and digital sensors. 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. 3. 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 alarms. For example, in Fig. 3, a high temperature (> 85°C) can be made up by a higher voltage (>1.0V) when a digital sensor is used. Note that the corners shown as *A* and *B* in Fig. 3, 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 paper, i.e., the VT range in which we expect our underlying circuit (S-Box here) works nominally.

To show the efficacy of using the sensor's AFN in predicting the underlying circuit's working status (failure or proper functionality), we compared vis-a-vis the status of the real S-Box operation status (pass or fail) in different VT combinations with the sensor AFN-based prediction (which predicts circuit failure when the AFN is lower than the $AFNwc = 17$). The results show that the sensor predicts the system operating status correctly in over 99.17% of the cases.

IV. Conclusion and Future Directions

Digital sensors (DSs) allow to detect out-of-specification environmental conditions by accurately tracking temperature and voltage variations. We designed a DS to detect attacks/failures based on the change of voltage/temperature. Our DS covers a larger area than the intersection of best/worst case intervals considered independently for temperature and voltage.

References

[1] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature Attacks," *IEEE Security & Privacy*, vol. 7, no. 2, pp. 79–82, 2009.
[2] K. Murdock et al., "Plundervolt: Software-based Fault Injection Attacks against Intel SGX," Tracked as CVE-2019-11157.
[3] N. Selmane, S. Guilley, and J.-L. Danger, "Practical setup time violation attacks on AES," in *European Dependable Computing Conf.*, 2008.
[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, 2011.
[5] M. Anik, S. Guilley, J.-L. Danger, and N. Karimi, "On the effect of aging on digital sensors," in *VLSID*, 2020.
[6] ISO/IEC 29192-2:2012, "Information technology – security techniques – lightweight cryptography – part 2: Block ciphers."
[7] "Nangate 45nm open cell library," "http://www.nangate.com".