On-Chip Voltage and Temperature Digital Sensor for Security, Reliability, and Portability

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

*CSEE Department
University of Maryland Baltimore County, Baltimore, USA
{toufiqhanik,ebrahimabadi,hpirsiav,nkarimi}@umbc.edu

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

‡Secure-IC S.A.S.
Think Ahead Business Line
firstname.lastname@secure-ic.com

***Abstract*— The integrated circuits can be exposed to various stresses during run-time due to unexpected environmental conditions or attacks. Ensuring that a circuit is not working out-of-specification via sensing its operating conditions, e.g., temperature and voltage, is highly useful in detecting anomalies. Analog sensors have been used to monitor the operating conditions for a long time, however, weaknesses including lack of portability to thin technology nodes, costly & complex calibration process, and low attack resistance make such sensors inefficient. Digital sensors, via considering the temperature and voltage effects altogether instead of treating each separately, have been demonstrated as a qualified replacement. In this paper, we develop an integrated framework for continuous monitoring of the operating voltage and temperature of each chip. The framework includes an embedded on-chip sensor circuitry along with a Neural Network model that quantifies the temperature and voltage values via processing the data collected by this sensor. The experimental results confirm the high accuracy of the proposed framework in tracking on-chip voltage and temperature variations, i.e., with the average error of 0.014V in a range of 0.65V to 1.4V, and the average error of 3.9°C in a range of -10°C to 150°C, respectively.**

I. Introduction

With the aggressive scaling of the electronic device's feature size ensuring the reliability and security of these circuitries has received a lot of attention. In practice, chips are designed to work in well-defined Process-Voltage-Temperature (PVT) conditions. However, they can be subject to various stresses, e.g., very high temperature and/or under-supply violating the intended PVT that characterized the chip at design time due to a harsh environment or a malicious attack aiming at denial of service, malfunction or even leak of sensitive data. Actually, faults in cryptographic programs can seriously endanger the security of applications, such as authentication skips in remote login or firmware updates, or even as secret/private keys exposition by fault analysis [1].

Equipping the chips with sensors raising alarms when a chip is operated out-of-specification has received the lion's share of attention in recent years [2]. Such alarms may call for proper actions to prevent catastrophic consequences such as safety breakdown (e.g., in automotive industry, and in particular autonomous cars), security breakage (e.g., leaking secret information from smartcards via launching fault attacks through voltage glitches), or reliability wearout (e.g., malfunctions in highly critical applications like medical and space).

Analog sensors have been broadly used in industrial applications to monitor the chip behaviors [3], especially in the field of safety. However, they suffer from various weakness, e.g., the need for post manufacturing calibration due to process variation, and difficulty of their adaptation to new technological nodes. To overcome these obstacles, digital sensors have been introduced in low-power (e.g., for finetuning the Dynamic-Voltage-Frequency-Scaling [4]) and security literatures [5], and were used thereafter in industry [6] and government sectors.

In this paper, we develop an integrated framework for continuous monitoring of chips' operating voltage and temperature via designing an embedded Digital Sensor (DS) that uses machine learning schemes. Our DS architecture relies on two delay sensors operating under different conditions, and reacts in terms of propagation delay to PVT variations. We propose a Neural Network (NN) assisted method to determine the voltage and temperature by exploiting the deployed DS output.

II. Analog Versus Digital Sensors

In contrast to digital sensors that are fully made up of digital standard cells, analog sensors are realized using full custom layout and are hard to calibrate [7]. Analog sensors are less portable, requiring revalidation by new simulations when the technology Physical Design Kit (PDK) is updated and a complete redesign when changing the technology or the foundry. On the contrary, digital sensors simply require a basic recalibration in any of those situations. Digital sensors are more optimized regarding area and power compared to the analog ones. Both sensors suffer from process variation and dynamic noise. However, analog sensors counter ambiguities in defining a threshold for nominal vs abnormal situations, while digital sensors resolve this issue via electrical level discretization [8]. Moreover, analog sensors are more prone to attacks due to their noticeable implementation [9] using full custom layout. In terms of failure or attack detection, analog sensors generate more false alarms than digital sensors [2].

III. Motivation

The operating voltage V can be transduced from measuring a timing within the chip through tabulation. However, as the delay depends on the temperature T, a temperature sensor is needed to find the V from the T. If temperature sensor is *NOT* available, there is no unique solution due to the existence of iso-delay curves (see our characterizations in Fig. 3). To overcome this problem, we propose a differential approach with two Digital Sensors: one with High-speed and Low-leakage, V around 1.0V and another around 1.2V. In this case, unique (V, T) can be found from the intersection of those two curves. As storing the combination of values for both sensors would be large, we leverage Machine Learning (ML) algorithms for interpolating the data.

In practice, temperature factor is less important than voltage to be accurate, because the attacks require drastic changes in temperature to be effective. Fault injection can be perpetrated either via *hot* temperatures [10]–[12] or *extremely low* temperatures as the "cold boot attack" [13].

2576-6996/20/$31.00 ©2020 IEEE
DOI 10.1109/ICCD50377.2020.00091

IV. Target Sensor

A. Digital Sensor Rationale

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. The sensor is usually as simple as a delay chain [2]. An edge (positive or negative) feeds such delay chain, and it is checked if the edge manages to propagate to the end of the chain at the considered clock period [5, 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, via the D-Flip-Flops (FFs) embedded in the chain. Such a snapshot digitizes the amount of stress applied to the circuit [14].

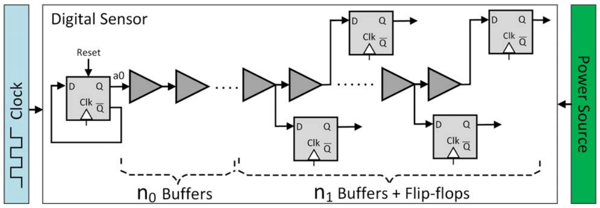
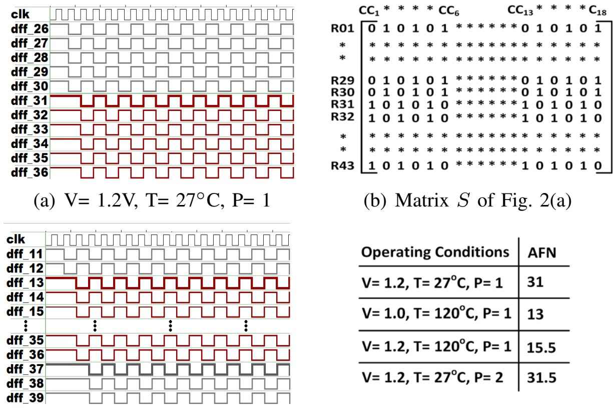


Figure 1. The architecture of the target digital sensor.

Figure 1 depicts the schematic of the DS we deploy in this research. This sensor includes $n_0 + n_1$ buffers among which the last n_1 buffers each feeds a FF. The output of these FFs represent the sensor's outcome. All FFs operate at similar clock frequency F. The first buffer is fed with a toggle FF generating a periodic signal $a0$ with the frequency of $F/2$. The number of buffers and FFs are decided based on the operational range of the underlying circuitry embedded in the same chip. In this paper, we will use two sensors, the **sensor pair**, operating at different conditions to derive two independent physical values: "voltage" and "temperature".

B. Characterization

We deploy two different methods to characterize the sensor pair and in turn extract the voltage and temperature.



(a) V= 1.2V, T= 27°C, P= 1

(b) Matrix S of Fig. 2(a)

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

(c) V= 1.0V, T= 120°C, P= 1

(d) AFN

Figure 2. Waveforms of Fig. 1 in different operating conditions. Here, voltage, temperature and process are shown with V, T, and P, respectively.

1) Matrix-Bases Method (MBM): The MBM scheme extracts the output of the individual FFs in i consecutive clock cycles. Depending on voltage and temperature (V, T) combinations, the propagation delay of the delay chain changes resulting in a different set of values captured by the FFs. As shown in Fig. 1, in each clock cycle of CC_i, when this sensor is fed with a0, the first FN_i FFs are in phase A (say $0 \rightarrow \underline{1} \rightarrow 0$) and the next ones are in the complementary phase $\overline{\text{A}}$ (say $1 \rightarrow 0 \underline{\rightarrow} 1$), where FN_i (referring to the index of FF in which phase $\overline{\text{A}}$ starts in clock cycle CC_i) changes in different (V, T). When the circuit operates slower, the delay of the buffer chain increases resulting in a phase change (from A to $\overline{\text{A}}$) in the FFs with lower indexes. However, with the increase of V and decrease of T, the delay decreases, and the FN_i increases.

The binary matrix S, representing the sensor status in each (V, T) combination includes N (# of FFs in the sensor) rows, and CC (# of clock cycles the sensor is observed for characterization) columns. As an example, consider the waveforms shown in Fig. 2 with a sensor having n_0 =9 leading buffers and n_1 = 43 buffers and FFs. This figure shows the FF outputs in different operating conditions. In particular, Fig. 2(a) shows the sensor outcome for V = 1.2V and T = 27°C. As shown, the first 30 FFs are in the same phase while the rest are in the opposite phase. In both waveforms in Fig. 2, we showed the FF values for 18 clock cycles. Fig. 2(b) depicts the matrix S for the waveform in Fig. 2(a).

Figure 2(c) shows the outcome of the sensor for Vdd= 1.0V and T= 120°C. As shown, the sensor outcome is different from Fig. 2(a), and in this case multiple phase changes occur (one in FF 13 and one in FF 37). The takeaway point from these observations is that firstly, operating conditions can change the matrix S, thereby, we can use this matrix to infer the operating conditions. Secondly, as the process variations affect the sensor outcome, we should take it into account.

2) Average-Bases Method (ABM): As MBM uses the whole matrix S, to reduce the NN training set size, we propose ABM where in each clock cycle CC_i $(1 \leq i \leq CC)$, the index of the first FF whose phase is different from its prior FFs in the delay chain is extracted, what we called FN_i earlier. Here, the average of all FN_is over all clock cycles, so-called AFN, is used for characterization. As AFN changes in different operating conditions, it can represent the operating condition. Figure 2(d) shows the AFN values for different PVT combinations. For example, when $Vdd = 1.2V$ and T = 27°C, the sensor is characterized by AFN = 31, while AFN is 13 when operating under $Vdd = 1.0$ and T = 120°C. Figure 2(d) shows that even in the same operating conditions ($Vdd = 1.2V$ and T = 27°C), AFN may slightly change due to the process variations. Moreover, for $Vdd = 1V$ and temperature = 120°C, AFN is 13 referring to the first phase change occurring in each clock cycle although multiple phase changes are experienced in each clock cycle.

V. Proposed Voltage and Temperature Prognosis Methodology

Figure 3 depicts how AFN is affected by the operating conditions. As expected, AFN is lower in high temperatures and low voltages as the circuit operates slower In contrast, in the conditions under which the circuit operates faster (high voltage and low temperature) the AFN is high. The same AFN value may represent different operating conditions as AFN relates to both voltage and temperature as a pair and not their individual values. For example, in both cases when (V, T)= (1.0V, 85°C) and (V, T)= (1.2V, 105°C), AFN is 17.

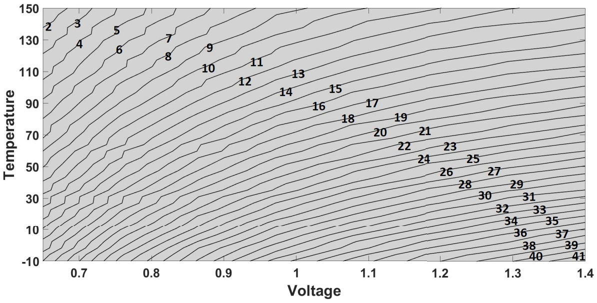


Figure 3. Variation of AFN in different voltage and temperature pairs.

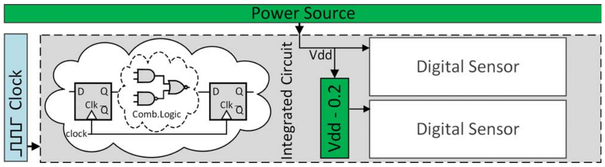


Figure 4. An integrated circuit with two embedded digital sensors.

As the relation between S (as well as AFN) and (V, T) is not one-to-one, to predict the voltage and temperature values accurately, we should be able to distinguish the cases that have similar S or AFN from each other. We address this issue by using a second sensor, as shown in Fig. 4, which operates under different voltage: Vdd -ΔVdd. In this paper, we considered ΔVdd = 0.2V. [1].

To determine the operating conditions based on the outcome of the sensor pair, we leverage Neural Networks. To train the model, we only need the simulation data of K sensor pairs. This approach has two advantages. Firstly, training the model using multiple sensor pairs' data results in mitigating the effect of process variations in the sensor's outcome as the model learns the process variation effects gradually during the training with multiple sensor pair data, and benefits from such learning in inferring the (V, T) conditions. Secondly, conducting Monte Carlo (MC) simulations relieves us from the need for multiple fabricated-chips data. The steps taken in our approach are as follows:

- **Step 1:** Conduct K MC Simulations of the sensor pairs;
- **Step 2:** Train an NN model using the Step 1 data;
- **Step 3:** Feed the model during the manufacturing to each chip that consists of the designed sensor pair;
- **Step 4:** Extract the operating condition values during the circuit operation to detect attacks and malfunctions.

We consider two different scenarios and tailor an NN for each (Step 2 discussed above). $Scenario$ 1 occurs when the system is equipped with an accurate temperature sensor. In this case, we can use the temperature along with either AFN or Matrix S to infer the voltage value. Leveraging AFN reduces the amount of data needed for training compared to the S matrix. As the results presented in Section VI shows, inferring the voltage based on AFN is as accurate as using the S matrix. On the other hand, in $Scenario$ 2 both voltage and temperature are quantified based on the outcome of the embedded sensor pair. We use S matrix to train the model in this scenario to enhance the accuracy of the outcome. The scenario based on existing voltage sensor to infer temperature has not been considered, as the voltage variations are faster than temperature changes and are directly impacted by fault injection attacks the sensor has to detect.

VI. Experimental Setup and Results

We implemented a sensor including n_0=9 leading buffers followed by n_1=43 buffers and flip-flops (Fig. 1) using 45-nm NANGATE technology [16] in the transistor level and deployed Synopsys HSpice for the simulations. This sizing leads to at least one phase change for all PVT corners for the considered range of (V, T), i.e., $-10°\text{C} \leq T \leq 150°\text{C}$ (step =1°C) and $0.65V \leq V \leq 1.4V$ (step = $0.05V$). We realized 16 different sensor pairs using MC simulations (to mitigate the impact of PV on the model's accuracy) and deployed their S matrix or AFN in each (V, T) combination to train our NN models. The MC simulations follow a Gaussian distribution: transistor gate length L: $3\sigma = 10\%$, threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. We implemented three fully connect 4-layers NN architecture, namely NN_1 infers the voltage when the temperature and matrix S are given (MBM model), NN_2 predicts the voltage based on the temperature and AFN value (ABM model), and NN_3 predicts both voltage and temperature based on matrix S (MBM model) as using AFN solely imposes higher error rates. NN_1 includes 774 input neurons (related to one sensor pair where each sensor characterized by a 43 flip-flop outputs in 9 clock cycles) and an extra input neuron for temperature. For NN_2, the input layer consists of 2 neurons for AFNs and 1 for temperature. NN_1 and NN_2 each includes one output neuron to infer the voltage. NN_3 includes 774 input neurons, and two output neurons (to infer voltage and temperature).

Rectified Linear Unit and Stochastic Gradient Descent are the activation function and optimizer used in our modeling, respectively. The loss function is the Mean Square Error. We conducted MC simulations for 16 sensor pairs and trained each of our three models with the dataset related to M sensor pairs (M ∈{3,6,12,15}), while the other 16-M pairs are used in the inference phase.

A. Experimental Results and Discussion

1) Stand alone Voltage Sensor: This experiment investigates the accuracy of assessing voltage given that an on-chip temperature sensor is available ($Scenario1$ in Section V). We used two models to predict voltage; NN_1 (via matrix S) and NN_2 (via AFN). In both cases, multiple sensor pairs are used for training the Neural Network. Figure 5 depicts (in blue) the average absolute error of assessing voltage via $NN1$ when M ∈{3,6,12,15} sensor pairs in different voltage and temperature combinations were used for training, and the other 16-M sensors were used for test in each case. As shown, the average error in assessing the voltage is 0.07V when the training dataset was gathered from 3 sensor pairs. Involving more sensor pairs in the training process reduces this error significantly, e.g. 0.005V for 15 sensor pairs. Fig. 5 also depicts (in red) the amount of voltage prediction error when AFN is used in modeling. When modeling based on 3 sensor

[1] It is mandatory in safety applications (e.g., [15, Chapter 2]) to leverage correlated sensors to improve the reliability of their measurement. Our use-case is different in that the two sensors are of similar kind yet operating in different conditions to allow for uniquely rending their (V, T) measurement.

pairs' data, NN_2 outperforms NN_1, however, with involving more sensor pairs in training, firstly the accuracy of both models enhances considerably, and secondly both methods converge, i.e., perform very similarly.

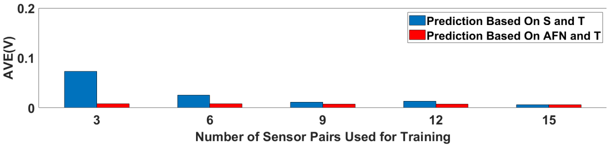


Figure 5. Average Voltage Error (AVE) using NN_1 (prediction based on status matrix and temperature) and NN_2 (prediction based on AFN and temperature) models. Each model was trained with the dataset of M sensor pairs, M ∈{3,6,12,15}, and tested against the rest of 16-M sensor pairs.

In practice, to assess voltage accurately via NN_2 very few (as low as 3) sensor pair data is required. NN_1 is highly accurate when using an appropriate dataset (as low as 9 sensor pairs in our experiments). Recall that the required training dataset is always provided via simulation; hence can be easily extended to get higher accuracy if needed. Then the NN weights are embedded in each chip during fabrication.

To ensure that we get approximately the same level of errors regardless of the target circuitry, we performed K-Fold Cross-Validation, and considered one of the K=16 sensor pairs for inference, and the other 15 circuits for training in each experiment. As shown in Fig 6, the voltage prediction error fluctuates between 0.005V and 0.018V for NN_1 (blue) while the error range is [0.006V,0.010V] for NN_2 (red), with the average error of 0.010V for NN_1 and 0.007V for NN_2.

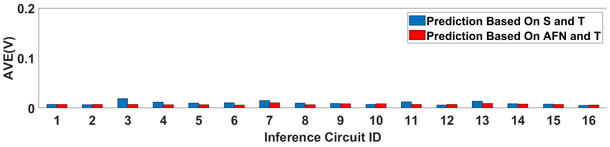


Figure 6. Average Voltage Error (AVE) using NN_1 (prediction based on status matrix and temperature) and NN_2 (prediction based on AFN and temperature) models. Each model was assessed against I^{th} sensor pair, where I ∈{1,...,16}, and is trained with the other 15 sensor pairs.

These observations show that both NN_1 and NN_2 models can assess the voltage accurately while NN_2 is preferred over NN_1 because of its simplicity. Moreover, the results show how training with multiple datasets related to different sensor pairs mitigates/removes the effect of process variation.

2) Combined Voltage-Temperature Sensor: This experiment shows the accuracy of NN_3 to assess both voltage and temperature quantities based on S matrix ($Scenario$ 2 where a separate temperature sensor is not available). Fig. 7 depicts the average error of assessing temperature and voltage via NN_3 model (in blue) when trained with 3, 6, 12, and 15 sensor pair datasets, and tested against the rest of 16 sensor pairs. The average error in assessing the voltage diminishes significantly from 0.12V to 0.014V by increasing the number of sensor pairs used in training from 3 to 15. Temperature assessment follows a similar trend, i.e., as shown (in red), the average temperature prediction error in NN_3 is ≈16.1°C if 3 sensor pairs are used for training. Such error is diminished significantly to 2.5°C by increasing the training size set to 16 sensor pairs.

Based on cross validation results in Fig 8, the voltage prediction error is reported between 0.01V (for the 16^{th} circuitry) and 0.04V (the circuitry with ID=3), while the average error over all 16 circuitries is 0.02V. Similarly, the temperature assessment error is in range of 2.3°C and 7.1°C, with the average as low as 3.9°C.

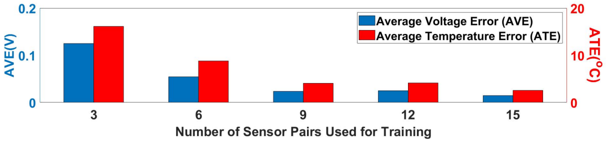


Figure 7. Average voltage & temperature errors using NN_3 model. The model was trained with the dataset related to M sensor pairs, where M ∈{3,6,12,15}, and tested against the rest of 16-M sensor pairs.

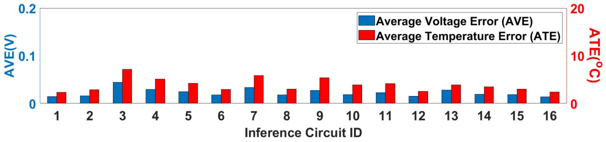


Figure 8. Average voltage & temperature errors using NN_3 model. The model was assessed against I^{th} sensor pair, where I ∈{1,...,16}, and is trained with the other 15 sensor pairs.

VII. Conclusion

Anomalies can be detected via sensing circuits' operating conditions such as voltage and temperature. Digital sensors have received a lot of attention to replace their costly analog counterparts. We presented a Neural Network assisted digital sensor framework that can assess the operating temperature and voltage with high accuracy. The assess methodology is not affected by process variations as the training dataset is gathered from multiple sensors simulated under different voltage and temperature conditions. The results confirm the high accuracy of our framework in predicting voltage and temperature with mean error of 0.014 V and 3.9 °C, respectively.

References

[1] M. Joye and M. Tunstall, *Fault Analysis in Cryptography*. Springer LNCS, March 2011, ISBN: 978-3-642-29655-0.

[2] M. T. H. Anik, R. Saini, J.-L. Danger, S. Guilley, and N. Karimi, "Failure and Attack Detection by Digital Sensors," in *ETS*, 2020.

[3] 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.

[4] 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.

[5] 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.

[6] S. Guilley et al., "Reliability analysis of digital sensors against perturbations of FPGAs," June 29–July 2 2014.

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

[8] G. van der Horn and J. L. Huijsing, *Integrated Smart Sensors: Design and Calibration*, ser. Int'l Series in Engineering and Computer Science book series (SECS). Springer, 2012, vol. 419.

[9] 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.

[10] J. Brouchier et al., "Temperature Attacks," *IEEE Security & Privacy (S&P)*, vol. 7, no. 2, pp. 79–82, 2009.

[11] T. Korake et al., "Clock glitch attacks in the presence of heating," in *Fault Diagnosis and Tolerance in Cryptography*, 2014, pp. 104–114.

[12] C. Labrado et al., "Use of Thermistor Temperature Sensors for Cyber-Physical System Security," *Sensors*, vol. 19, no. 18, p. 3905, 2019.

[13] J. A. Halderman et al., "Lest we remember: cold-boot attacks on encryption keys," *Commun. ACM*, vol. 52, no. 5, pp. 91–98, 2009.

[14] 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.

[15] J. R. Pimentel, *The Safety of Controllers, Sensors, and Actuators: Book 5 - Automated Vehicle Safety*. SAE International, March 7 2019.

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