IC age estimation methodology using IO pad protection diodes for prevention of Recycled ICs

Srisubha Kalanadhabhatta, Rashi Dutt, Saqib Khursheed, and Amit Acharyya

***Abstract*—Recycled ICs have become a major threat to the ICs used in safety critical systems. In the current state-of-the-art techniques, recycled ICs are detected by measuring the frequency, current, path delay or power-up values to estimate the HCI, BTI and EM effects on the transistors with age. Some of the state-of-the-art techniques require additional on-chip sensors to detect and estimate the age of an IC while others use existing logic like SRAM and Flip-flops to detect the recycled ICs. In this paper, we provide a methodology to detect a recycled IC and also to estimate its age by using the existing IO pad structures. For the first time, age is estimated by measuring voltage drop across the protection diodes present in IO pad structure. With this methodology, no additional sensors have to be added and hence there is no area overhead. With this proposed methodology, ICs that are used for a minimum period of a day can be effectively detected by using the concept of extended Kalman filtering technique for the first time in this domain. By stressing the part for five days, our proposed methodology can estimate the age of the IC aged between 1 month to 5 years with 95% percent of accuracy.**

***Index Terms*—Counterfeit, Aging, Recycled ICs, Diode, Input-Output(IO) pad, protection diodes, Kalman Filter, Non Volatile Memory(NVM), Original Chip Manufacturer(OCM)**

I. Introduction

RECYCLED ICs are the ICs that are recovered from an used system and misinterpreted as a new IC from the OCM [1]. Recycled ICs are not reliable as aging effects the reliability of an IC. Recycled ICs exhibit lower performance and have a shorter life time. Usage of such ICs in safety critical systems like Health Care, Aerospace, Automation etc., may be catastrophic [2]. Recent news articles [3] - [5] show that the recycled ICs are purchased by defense contractors for military use. Thus, recycled IC detection is a critical issue and demands specific detection strategies. State-of-the-art methodologies detect the recycled ICs by measuring HCI, BTI and EM effects on the transistors with age. Some of these techniques use on-chip sensors. Ring Oscillator(RO) sensor proposed in [6] includes a frequency comparison between two identical ROs, a stressed RO and a reference RO. When the circuit is in operation, only stressed RO is enabled and the reference RO is not enabled. The oscillation frequency of both the ROs is compared and the magnitude of frequency difference between both the ROs is used as a parameter to predict whether the IC under test is new or recycled. This circuit has been improved in [7] - [9] to reduce the area and improve the detection efficiency. Resistance difference between Electro Migration(EM) stressed wire set and EM reference wire is used in [10] to detect if the IC is a new one or recycled. Path delay difference between the reference circuit and stressed circuit is used in [11] to detect recycled ICs. In [12], the RO frequency of IC under test is compared with the initial RO frequency(stored into an NVM) and based on the deviation, the IC is classified as new or recycled. A time sensor is used in [13] to measure the increase in the power-rail discharge time of power-gated circuits. The IC under test is classified as a recycled IC if the time is above a threshold. The age of the IC is also determined using a counter. Chained Binary Aging Elements (BAE) are employed to measure use and age of the chip in [14] where the chip age can be read out as a thermometer coded binary value by polling each BAE state. In [15], every SRAM is subjected to enrollment(room and high temperature) phase and threshold estimation phases. The Electronic Chip ID(ECID) obtained in threshold estimation phase is stored in the database. During verification phase, the power up values are compared with ECID and according to the skew the IC is classified as recycled or new. Authors of [16] assumes the power up states of SRAM to be 50% 1's and 0's. This is tested for N power ups on a sampled set of ICs and the error threshold is calculated. The SRAM values of DUT are read and it is detected as a recycled IC if the error is above threshold. The concept of [16] is extended to flip-flops in [17] by the same authors. It uses a differential self-referencing methodology based on two selected groups of FFs in the part, one group that mostly ages in the 0 state, and the other which ages in the 1 state. The percentage of 1s observed at power-up in these two groups is virtually the same when a chip is new, due to the commonality in design and process. The set of flip-flops identified for an IC is saved and the same set of flip-flop's value at the power-up is noted during test. If the difference in skew in the two groups is more, it is detected as a recycled IC. In self-similarity-based microchip integrity analysis (SeMIA) approach, as explained in [18] intrinsic structural self-similarity in a design is exploited to isolate recycled chips. Few test vectors are identified and if I_{DDT} difference between these two structures exceeds a threshold, the IC is detected as recycled. Difference in quiescent supply current(IDDQ) is measured for two pre-defined patterns in [19] and the IC is classified as recycled if it exceeds threshold.

The fore mentioned methods [6] - [11] compare a reference structure with a stressed structure and based on the difference detects a recycled IC. The methods [12] - [14] use on chip

Srisubha Kalanadhabhatta, Rashi Dutt and Amit Acharyya are with Department of Electrical Engineering, Indian Institute of Technology(IIT), Hyderabad, Telangana, India. Saqib Khursheed is with Department of Electrical Engineering and Electronics, University of Liverpool, UK. This work is partially supported by Ceremorphic India Pvt. ltd. and Centre of Advanced Computing (CDAC), Ministry of Electronics and Information Technology (MEITY), Govt of India funded "I-PREVENT" project with Grant Number IITH/EE/F091/G304 dated November 2020.

sensors to detect the recycled IC and also estimate its age. These on-chip structures have to be inserted before fabrication i.e. at the pre-silicon stage itself and hence cannot be applied for chips already in production. Furthermore, if any additional circuitry like on-chip sensors is required to be embedded, that may incur area overhead and more power consumption. The methods [15] - [19] does not require a sensor and can be applicable for ICs in production. However, they can only detect if an IC is recycled but cannot estimate the age of the IC.

Motivated by the above mentioned limitations of the existing techniques, here we introduce for the first time an Extended Kalman Filter based methodology to detect and estimate the age of recycled ICs. Voltage drop across the IO pad protection diodes which increases with age is used as a measure to estimate the age of an IC.

The key contributions of the paper are as follows:

- No extra sensors needs to be embedded in the design and hence the proposed methodology can be applied for the chips in production.
- The proposed methodology not only detects the recycled ICs but also estimates its age by stressing it for five days.
- This is the first methodology which is focused on diode aging. So far, state-of-the-art techniques are focused on transistor aging.

The paper is organized as follows. Section II presents the proposed methodology. Results and discussion are presented in section III and section IV concludes the paper.

II. Proposed Methodology

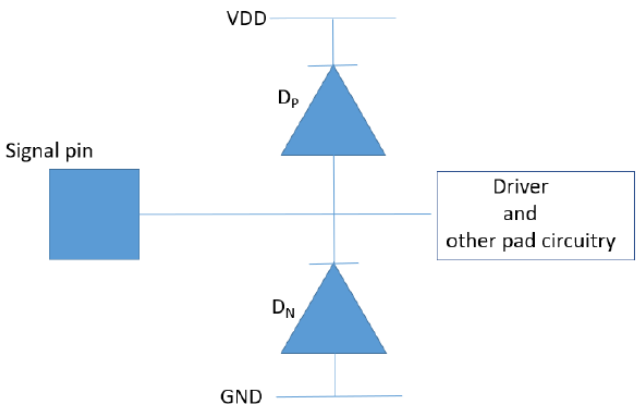


Fig. 1: IO Pad structure

In the state-of-the-art methodologies, recycled ICs are detected or the age is estimated by measuring HCI, BTI and EM effects on the transistors with age. In our proposed methodology, we focus on the aging effects of the protection diodes in the pads. IO pads are inserted in an IC to communicate between chip and external world [20] . There can be different types of pads, Input pads, Output pads, Input-Output(IO) pads and Power pads. Adding the protection devices at input/output (I/O) pad as shown in Fig.1 can increase the circuit reliability [21] - [22]. VDD protection diode(D_P) and VSS protection diode(D_N) protect the pad circuit from low and high signal swings at the pin. While the pad is in normal operating mode, signal pin is connected to either logic zero or one. In this case, the two protection diodes D_P and D_N are in reverse biased mode. During the complete operation of the chip, these diodes are reverse biased and hence stressed with negative voltage across them. Considering 40nm technology, for a 3.3v pad, logic 0 value can range from -0.3v to 0.99v and logic 1 can range from 2.31v to 3.63v. Any signal pad that has a constant value(stress voltage) through out the circuit operation has to be chosen. Active high reset pad is one such pad which has to be at logic 1 through out the chip operation. During this period, the VSS protection diode(D_N), is reverse biased with a voltage which can range from 2.31v to 3.63v. So, it can be assumed that the VSS protection diode(D_N) of this pad is stressed for a time duration which is equivalent to the time the IC is in operation. Current through the diode, i, can be represented as a function of voltage v across it as shown in equation 1.

$$i(v) = IS(exp(v/\eta V_T) - 1) \quad (1)$$

where IS is the reverse saturation current,
V_T is the volt equivalent of temperature, and
η is the emission coefficient.

In [23], authors have suggested a model for the change in saturation current through the diode in reverse biased mode as a function of voltage, temperature and stress duration as shown in equation 2.

$$\Delta IS = BIS \times exp(-EIS/V_T) \times v^{ALPHA}/agingtime^{BETA} \quad (2)$$

where BIS is overall proportionality,
EIS is aging dependency on stress temperature,
ALPHA is aging dependency on stress bias and
BETA is aging dependency with time

Keeping the temperature constant at 25°C, the change in saturation current is a function of stress duration and the reverse biased voltage across the diode. At 25°C, the voltage drop across the diode increases with stress duration as shown in Fig. 2. The voltage drop across the diode for different reverse bias voltages is also plotted in Fig. 2. This implies that the voltage drop across the diode varies with the signal level for logic 1 (2.31v to 3.63v) that is provided when IC in operation.

The aim is to detect an IC if it is recycled or new and also estimate its age. Voltage drop across the diode can be measured using the open-shorts testing [24] during manufacturing. To detect an open or short across the VDD protection diode(D_P) of a signal pin, VSS, VDD, and all other signal pins are connected to ground and a minimal current of 100 uA or 200uA is forced into the signal pin. If the VDD protection diode operates correctly, then it will become forward-biased and the current will flow between the signal pin and VDD. By measuring the voltage drop across the forward-biased VDD diode, we can determine whether it is functioning correctly. Similarly by forcing a negative current into the signal pin, an open or short across the VSS protection diode(D_N) can be verified. This is done for each and every pad as part of manufacturing test. The voltage drop is influenced by two variables, stress voltage and stress duration. The stress voltage(logic 1 level at the signal pad) that is applied when the IC was in operation is unknown. While our interest is to find out stress duration, we need to find out a way to remove the dependency on the stress voltage to arrive at an estimated age(stress duration) of the IC. There are two methods that can be applied, one just to detect if the IC is new or recycled in few minutes using a reference value stored in NVM and other to estimate its age also by stressing the part at 2.9V for 5 days. The methods are described below.

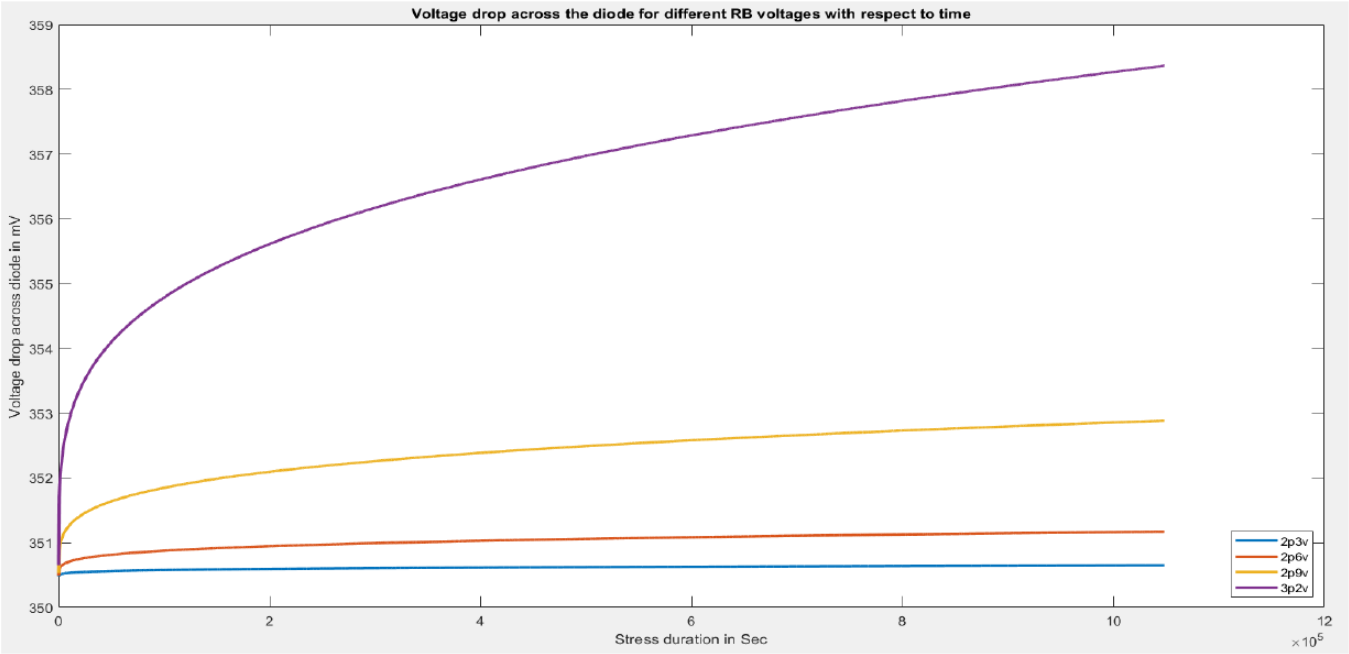
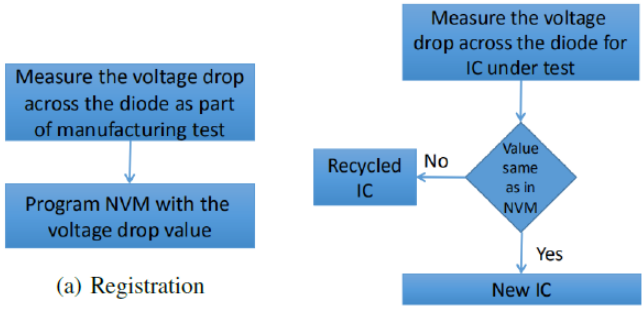


Fig. 2: Voltage drop across diode for different stress duration

A. *Recycled IC detection*

A two step methodology has to be followed for recycled IC detection as shown in Fig. 3. Registration phase is during the manufacturing test phase where the voltage drop across the diode is measured and programmed into on-chip Non-volatile Memory(NVM). As described in [12] the process has to be made secure so that the data is not leaked. In the authentication process, the voltage drop across the diode is measured and compared with the value in NVM. if both are same, the IC under test is detected as new IC, else it is detected as recycled IC. ICs that are used for a minimum period of a day can be effectively detected using this method.



(a) Registration

(b) Authentication

Fig. 3: Recycled IC detection

B. *Recycled IC Age estimation*

The age of the IC is estimated as per the procedure shown in Fig. 4. The voltage drop across the diode for IC under test is measured and marked as v1. The device is stressed by connecting the reset pad to logic 1(reverse bias of 2.9v) for 5 days. The voltage drop is again measured and marked as v2. Kalman filtering is an algorithm that provides estimates of some unknown variables given the measurements observed over time. Kalman filters are used to estimate states based on linear dynamical systems in state space format. The extended Kalman filter(EKF) is utilized for nonlinear problems like bearing-angle target tracking and terrain-referenced navigation. Our model is non-linear and hence Extended Kalman filter [25] - [26] is used for creating models for a stress voltage of 2.9v for different stress duration with a difference of 5 days. The difference of v2-v1 is compared with the Kalman model in the model identification as described in [25] and the nearest value to the difference is identified as age of the IC under test. This value remains the same irrespective of stress applied to the recycled part during its operation. This is because we are comparing the difference of two values to get the incremental change for five days instead of the absolute value. For the first time, Kalman filter is used for such an application.

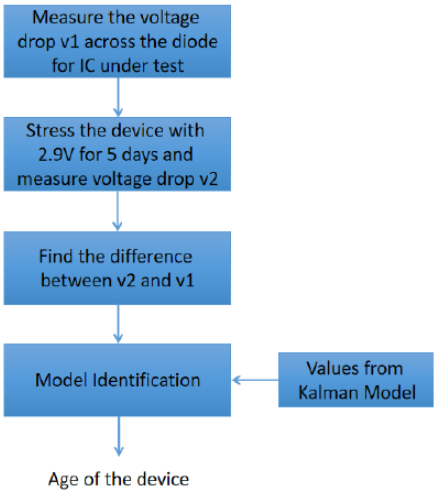


Fig. 4: Recycled IC Age estimation

III. Results and Discussion

Our proposed methodology is compared with the state-of the art techniques and is tabulated in Table I. As can be observed from Table I, our proposed methodology has no extra structure to be added to the IC, is applicable for the ICs in production and can detect the recycled IC as well as estimates its age.

Extended Kalman Filter model is created for a stress duration of 1 to 59 months with one month interval. That is the model is developed

TABLE I: Comparison with state-of-the-art techniques

Feature	[6] - [11]	[12] - [14]	[15] - [19]	Proposed Methodology
Characteristic measured	Transistor HCI, BTI and EM	HCI, BTI and EM	HCI, BTI and EM	Diode vdrop for RB stress
For chips already in production	Not applicable	Not applicable	Applicable	Applicable
Extra structure required	Yes	Yes	No	No
Estimates the age	No	Yes	No	Yes

TABLE II: Age Estimation with Extended Kalman filter model

S.No	Actual Age	Estimated Age	Error
1	30 days	1 month	0 days
2	60 days	2 months	0 days
3	90 days	3 months	0 days
4	120 days	3 months	30 days
5	150, 180 days	3 to 7 months	0 days
6	210, 240, 270, 330 days	6 to 13 months	0 days
7	300 days	12 to 25 months	65 days
8	360, 390, 420, 450, 480, 510, 540, 570 days	12 to 25 months	0 days
9	600	More than 24 months	130 days
10	630, 660, 690, 720, 750, 780, 810, 840, 870, 900, 930, 960, 990, 1020, 1050, 1080, 1110, 1140, 1170, 1200, 1230, 1260, 1290, 1320, 1350, 1380, 1410, 1430, 1470, 1500, 1530, 1560, 1590, 1620, 1650, 1680, 1710, 1740, 1770 days	More than 24 months	0 days

for 1 month, 2 months, 3 months, ... , 59 months. At every stress duration the difference for 5 days is calculated. That is the voltage difference for (35-30) days, (65-60) days etc., is calculated. As shown in Fig. 4, v1 is measured for IC under test and the IC is stressed under 2.9v for 5 days to get v2. Diode model as per [23] is used to arrive at values of v1 and v2. v2-v1 is compared with the voltage difference from Kalman model and the model identification chooses the model whose difference is near to this. For example if the v2-v1 is near to the (35-30) days from the Kalman model, the age is estimated as 30 days. As per the diode equation, the voltage drop difference gets reduced with age. Hence, the age can be more accurately found when the device is stressed for lesser time. Hence we have classified the age of an IC as 1 month, 2 months, 3 months, 3 to 7 months, 6 months to 13 months, 12 months to 25 months or more than 24 months. The code is run in matlab and the results are as tabulated in Table II. There are 59 data points which span from 30 days to 1770 days. Age is estimated correctly for 56 data points which gives us 95% accuracy in prediction. The error in estimated age is 30 days for an actual age of 120 days, 65 days for an actual age of 300 days and 130 days for an actual age of 600 days where the error % is 33.3%, 21.6% and 21.6% respectively.

IV. Conclusion

This paper presents a novel methodology to detect and estimate the age of recycled ICs using the diode characteristics, by measuring voltage drop across the protection diodes present in IO pad structure. There is no extra circuitry that needs to be added to the design and hence is applicable for the chips in production. By writing the initial voltage drop into NVM, this methodology can detect the recycled ICs in few minutes. This methodology can detect ICs which are used for a minimum period of a day and can also estimate the age by stressing the part for 5 days at 2.9v and by comparing it with Kalman filter model. As per our knowledge, this is the first methodology using Diode characteristics for estimating age and also using Kalman filter for this purpose.

V. Acknowledgements

The authors would like to thank Franz Sishka for helping with the queries related to diode modeling. Authors would like to thank Ceremorphic India Pvt Ltd and Centre of Advanced Computing (CDAC), Ministry of Electronics and Information Technology (MEITY), Govt of India funded "I-PREVENT" project with Grant Number IITH/EE/F091/G304 dated November 2020 for partially funding the work.

References

[1] Mohammad Tehranipoor et al., "Anti-Counterfeit Techniques: From Design to Resign", 2013 14th International Workshop on Microprocessor Test and Verification.

[2] F. Koushanfar, et al., "Can EDA Combat the Rise of Electronic Counterfeiting?" DAC, 2012, pp. 133-138

[3] https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits

[4] https://www.latimes.com/socal/daily-pilot/news/tn-dpt-me-cm-counterfeit-electronics-20190604-story.html

[5] http://www.saelig.com/news/articles/ic-counterfeiting.pdf

[6] X. Zhang and M. Tehranipoor, "Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 22, no. 5, pp. 1016-1029, May 2014, doi: 10.1109/TVLSI.2013.2264063.

[7] U. Guin, D. Forte and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 4, pp. 1233-1246, April 2016, doi: 10.1109/TVLSI.2015.2466551.

[8] S. R. Sahoo, K. Sudeendra, A. Mahapatra, A. K. Swain and K. K. Mahapatra, "On-chip RO-Sensor for Recycled IC Detection," 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Bhopal, 2017, pp. 252-256, doi: 10.1109/iNIS.2017.60.

[9] S. R. Sahoo and K. Mahapatra, "A novel area efficient on-chip ro-sensor for recycled ic detection,"Integration, vol. 70, pp. 138–150,2020.

[10] K. He, X. Huang and S. X. -. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, 2015, pp. 146-151, doi: 10.1109/ICCAD.2015.7372562.

[11] Zhichao Xu, Aijiao Cui, and Gang Qu, "A New Aging Sensor for the Detection of Recycled ICs", In Proceedings of the 2020 on Great Lakes Symposium on VLSI (GLSVLSI '20). Association for Computing Machinery, New York, NY, USA, 223–228. DOI:https://doi.org/10.1145/3386263.3407656

[12] M. Alam, S. Chowdhury, M. M. Tehranipoor and U. Guin, "Robust, low-cost, and accurate detection of recycled ICs using digital signatures," 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, 2018, pp. 209-214, doi: 10.1109/HST.2018.8383917.

[13] D. Rossi, V. Tenentes, S. Khursheed and S. M. Reddy, "Recycled IC detection through aging sensor," 2018 IEEE 23rd European Test Symposium (ETS), Bremen, 2018, pp. 1-2, doi: 10.1109/ETS.2018.8400713.

[14] N. E. C. Akkaya, B. Erbagci and K. Mai, "Secure chip odometers using intentional controlled aging," 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, 2018, pp. 111-117, doi: 10.1109/HST.2018.8383898.

[15] Z. Guo, X. Xu, M. T. Rahman, M. M. Tehranipoor and D. Forte, "SCARe: An SRAM-Based Countermeasure Against IC Recycling," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 4, pp. 744-755, April 2018, doi: 10.1109/TVLSI.2017.2777262.

[16] U. Guin, W. Wang, C. Harper and A. D. Singh, "Detecting Recycled SoCs by Exploiting Aging Induced Biases in Memory Cells," 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 2019, pp. 72-80, doi: 10.1109/HST.2019.8741032.

[17] W. Wang, U. Guin and A. Singh, "A Zero-Cost Detection Approach for Recycled ICs using Scan Architecture," 2020 IEEE 38th VLSI Test Symposium (VTS), San Diego, CA, USA, 2020, pp. 1-6, doi: 10.1109/VTS48691.2020.9107583.

[18] Y. Zheng, S. Yang and S. Bhunia, "SeMIA: Self-Similarity-Based IC Integrity Analysis," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 35, no. 1, pp. 37-48, Jan. 2016, doi: 10.1109/TCAD.2015.2449231.

[19] P. Chowdhury, U. Guin, A. D. Singh and V. D. Agrawal, "Two-Pattern IDDQ Test for Recycled IC Detection," 2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID), Delhi, NCR, India, 2019, pp. 82-87, doi: 10.1109/VLSID.2019.00033.

[20] Neil H.E. Weste and Kamran Eshraghian, "Principles of CMOS VLSI design," 2nd ed., Addison-Wesley Publishing Company, California, pp. 41-96,156-167,262-370,1993.

[21] S. Cao, J.-H. Chun, S. G. Beebe, and R. W. Dutton, "ESD design-strategies for high-speed digital and RF circuits in deeply scaled sil-icon technologies,"IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57,no. 9, pp. 2301–2311, Sep. 2010

[22] B. Peng and C. Lin, "Low-Loss I/O Pad With ESD Protection for K/Ka-Bands Applications in the Nanoscale CMOS Process," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 10, pp. 1475-1479, Oct. 2018, doi: 10.1109/TCSII.2018.2857403.

[23] Franz Sischka, Bertrand Ardouin, "Modeling of Device Aging Example: Diode a step-by-step tutorial", MOS-AK Workshop, Munich, 2018. http://www.mos-ak.org/munich_2018/presentations/T_8_Sischka_MOS-AK_Munich_2018.pdf.

[24] http://www.ni.com/tutorial/6980/en/

[25] C.K. Vala, M. French, A. Acharyya, B.M. Al-Hashimi, "Low-complexity architecture for cyber-physical systems model identification", IEEE Trans. Circt. Syst. II, 66 (8) (2019), pp. 1416-1420.

[26] Christian Campestrini, Thomas Heil, Stephan Kosch, Andreas Jossen, "A comparative study and review of different Kalman filters by applying an enhanced validation method", Elsevier,2016.