Self-contained LDO Odometer to Detect Recycled Counterfeit AMS Chips

Sourav Roy
University of Florida
Email: sourav.roy@ufl.edu

JinHong Chen
Ohio State University
Email: chen.8230@osu.edu

Domenic Forte
University of Florida
Email: dforte@ece.ufl.edu

***Abstract*—Counterfeit electronics is a growing threat with widespread impacts on many aspects of modern civilization including defense, communication, health-care, manufacturing industry, agriculture and all other areas dependent on integrated circuits (ICs) or chips. Among all of the counterfeit chips types, recycled and remarked are the most prevalent. These are the chips that are taken from discarded, obsolete electronics board and then sold as new. Therefore, these chips are aged and deteriorated with short remaining lifespan, proneness to failure, etc. Research has been conducted to identify recycled chips but those methods are not equally applicable to all kinds of chips. Specifically, hardware security primitives such as cryptographic primitives, physical unclonable functions (PUFs), true random number generators (TRNG), silicon odometers etc. are primarily developed for digital circuits and not easily ported to analog and mixed signal (AMS) chips. Recently, an LDO-based odometer was proposed to detect recycled AMS chips which requires external measurements through exposed pins which is both expensive and poses a security vulnerability. In this work, we propose a self-contained design that overcomes these issues while still being able to detecting aging in AMS chips.**

I. Introduction

A counterfeit integrated circuit (IC) can be recycled, re-marked, overproduced, cloned, tampered, defective or one with forged documentation. A complete description of each type of counterfeit can be found in [1]. Among these types of counterfeits, more than 80% are recycled and remarked [2]. As a result, methods of detecting recycled and remarked counterfeit chips have been widely researched. Cryptographic and hardware security primitives such as physically unclonable functions (PUFs) [3] and silicon odometers [4]–[6] have been developed mainly for digital circuits and thus are not easily portable to AMS chips.

Low dropout regulators or LDOs are crucial part of power distribution network of not only analog but also digital ICs. In order to detect recycled analog and mixed signal (AMS) chips, an LDO-based odometer was recently introduced and the degradation of its power supply rejection ratio (PSRR) was measured to identify counterfeit chips [7]. Since LDOs are used in power supply networks of almost all types of ICs, an LDO-based odometer can be a low-cost readily available method to detect recycled chips of any kind. The LDO-based odometer in [7] uses a reference LDO path which is used only during measurement and a normal LDO path which is used during normal operation as well as during measurements also termed as stressed path. The design is shown in Figure 1. During measurement the reference path and normal path are selected by using external pins which poses a security vulnerability for this design. Specifically, an attacker may exploit this vulnerability by intentionally aging the reference path (which is supposed to be idle during normal operation and thus unaged) rendering the PSRR degradation due to aging between reference and normal path negligible .

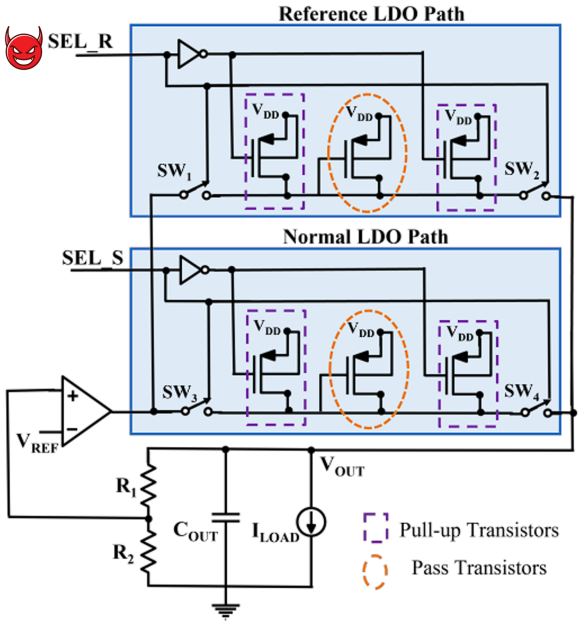


Fig. 1. LDO-based odometer proposed in [7] with external pins SEL_R and SEL_S for measurement where attacker can access reference path through SEL_R.

In this paper, we propose an upgraded LDO-based odometer that is capable of on-chip measurements to detect counterfeit chips – making it completely self-contained and unreliant on external equipment. This odometer requires only one external enable pin to switch between normal operation and aging measurement operation. As a result, the attacker cannot age the reference path separately which was possible in [7]. The contributions of this work are summarized as follows:

- To the best of our knowledge, this is the first self-contained LDO based odometer. Unlike the previous design that required an external equipment to measure LDO PSRR, the proposed odometer uses an on-chip

circuit to compare the threshold voltage of an aged LDO pass transistor to that of an un-aged reference.
- We introduce an LDO odometer design that does not require separate enable pins for reference and normal path and no switching between reference and normal path is needed. Only one enable pin is required to enable or disable aging measurement mode and both reference and normal path are activated during measurement mode so that attacker cannot age the reference path separately.
- We design different components such as inverter delay chain, ring oscillator (RO), XOR gate, transmission gate switches to switch between normal mode and measurement mode, etc. and integrate them to an on-chip aging detector for the LDO pass transistor.
- We analyze the effect of bias temperature instability (BTI) and hot carrier injection (HCI) induced aging on the LDO pass transistor and calibrate the LDO design to enhance sensor reliability. We utilize Monte Carlo analysis to simulate process variation to analyze sensor sensitivity and accuracy.

The rest of this paper is organized as follows. In Section II, we introduce the application of LDO in analog IC counterfeit detection by monitoring aging related threshold voltage degradation. In Section III-A, we propose the upgraded self-contained LDO odometer design. In Section IV, we discuss the simulation results and finally we draw conclusion in Section V.

II. Background

A. Low Dropout Regulator (LDO)

An LDO has three main components: error amplifier, pass transistor and reference voltage, V_{REF} generator as shown in Figure 2a. In this configuration, the pass transistor used is of PMOS type. A resistor divider with resistors R_1 and R_2 is used to produce a positive feedback to the error amplifier. The source of pass transistor is connected to the supply voltage, V_{DD} which is regulated by the LDO. The LDO maintains a constant voltage, V_{OUT} at the drain of the pass transistor which depends on values of V_{REF}, R_1 and R_2. For example, for equal values of R_1 and R_2 and a V_{REF} value of 450mV, LDO maintains a constant output, V_{OUT} of 900mV with supply voltage, V_{DD} of 1.1V. In this case, the dropout is 200mV. Even if the supply voltage, V_{DD} varies between 900mV and 1.1V the output voltage stays constant at 900mV through the positive feedback system. For a stable LDO system the error amplifier should have high open loop gain and a phase margin of above 60 degrees.

B. LDO-based Recycled IC Detection

The idea of exploiting this to defend against analog IC counterfeiting was introduced in 2019 [8], [9]. This method was limited to standalone LDOs from different vendors. Later this work was extended to LDOs in system-on-chips (SoCs) with less promising results [10]. In all these works degradation of PSRR was used as a metric to measure aging of AMS chips or SoCs. A new LDO design re-purposing the already existing LDO in a chip was described in [7]. In the progression of this work, to achieve higher level of automation and to minimize security vulnerability, in this work we propose an improved LDO odometer design with on-chip measurement capability.

In vehicles, an odometer measures the distance traveled which represents the wear-and-tear experienced by the engine. Similarly, the LDO odometer measures how much the LDO has been used or aged. The odometer has a reference path which is designed to be dormant during normal operation and does not age due to usage and a normal path which is active during normal operation and thus ages. As the normal path ages the difference in output of normal and reference path increases. The aging happens primarily due to the BTI and HCI effects described below.

C. Hot Carrier Injection (HCI)

HCI occurs in a transistor when electrons or carriers in the channel gain enough energy to be injected into the gate and gets trapped. As a consequence, threshold voltage of the transistor increases and the damage increases exponentially with the increase of gate to source voltage. The threshold voltage degradation is given as

$$\Delta V_{th} \approx \frac{1}{\sqrt{L}} t^{n_{HC}} e^{\alpha_3 V_{GS} + \alpha_4 V_{DS}} \tag{1}$$

where L is the transistor channel length, n_{HC} is the time exponent, and α_3 and α_4 are technology dependent parameters.

D. Bias Temperature Instability (BTI)

BTI is mainly caused by constant electric fields that degrade the dielectric by trapping holes in the dielectric bulk. As a result, the device threshold voltage increases. The trapped holes are released when the device is turned off and thus it enters recovery phase. Usually with conventional dielectrics used in semiconductor industry, BTI mainly affects PMOS transistors. The threshold voltage degradation due to BTI is given as

$$\Delta V_{th} \approx e^{\alpha_1 V_{GS}} t^{n_P} + V_{GS}^{\alpha_2} \left(C_R + n_R \log_{10} t\right) \tag{2}$$

where n_P and n_R are the time exponents, α_1 and α_2 are technology dependent voltage scaling factors, and C_R is the process dependent capacitance value.

III. Self-contained LDO Odometer Design

A. Overview

Figure 2b shows the setup for the self-contained LDO with on-chip measurement capability. At normal operating condition, 'EN' signal is low. The gate voltage of the pass transistor in the reference path is logic '1'; thus the transistor is turned off and is not aged. The gate of the pass transistor in normal (stressed) path is connected to the output of error amplifier and drain is connected to the resistor divider thus works as a regular LDO and the pass transistor ages due to usage.

During aging measurement, 'EN' signal is set to logic high. In this condition, both the pass transistor in reference path and stressed path have similar configuration where the pass transistor gate is connected to the drain and source voltage

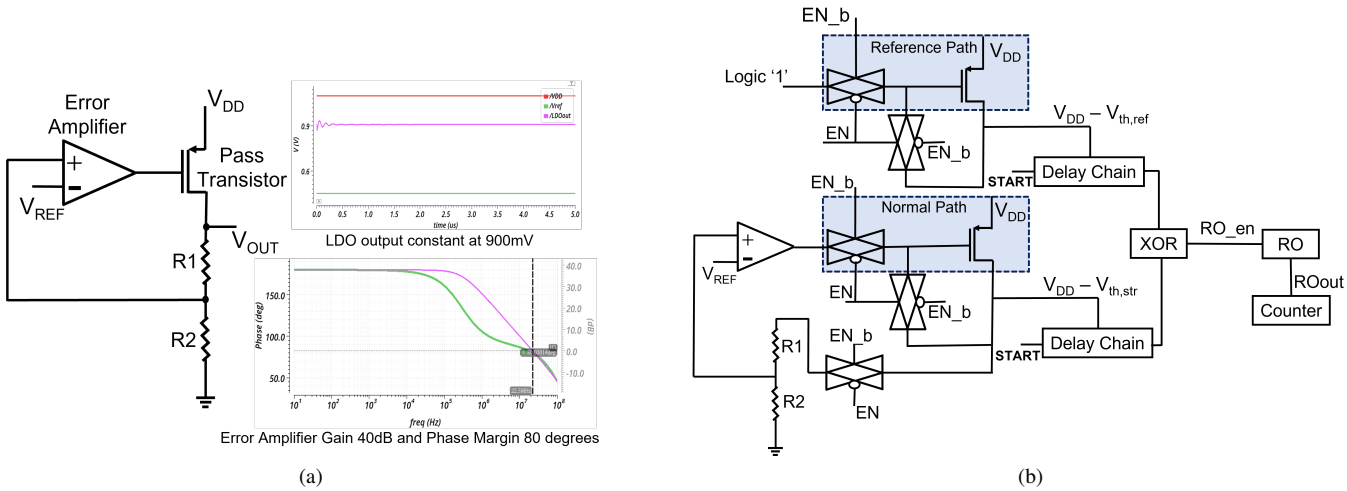


Fig. 2. (a) LDO schematic (b) LDO odometer with on-chip measurement of LDO output of normal and reference path at no load for recycled AMS chip detection.

is V_{DD}. In such configuration, the drain voltage is threshold voltage less than V_{DD} for both reference and stressed paths. The threshold voltage of pass transistor in the reference path and stressed path are $V_{th,ref}$ and $V_{th,str}$ respectively and drain voltages are $V_{DD} - V_{th,ref}$ and $V_{DD} - V_{th,str}$ respectively. During normal operating condition, the threshold voltage of the pass transistor in the stressed path increases over time due to usage.

After a few months of usage the threshold voltage of the stressed pass transistor increases enough so that $V_{th,str} > V_{th,ref}$ as the reference pass transistor is inactive at normal operating condition. Consequently, at that time, when 'EN' signal is set to high for aging measurement, the drain voltage of stressed pass transistor is smaller than the drain voltage of reference pass transistor. A measurement circuit is used to measure this difference.

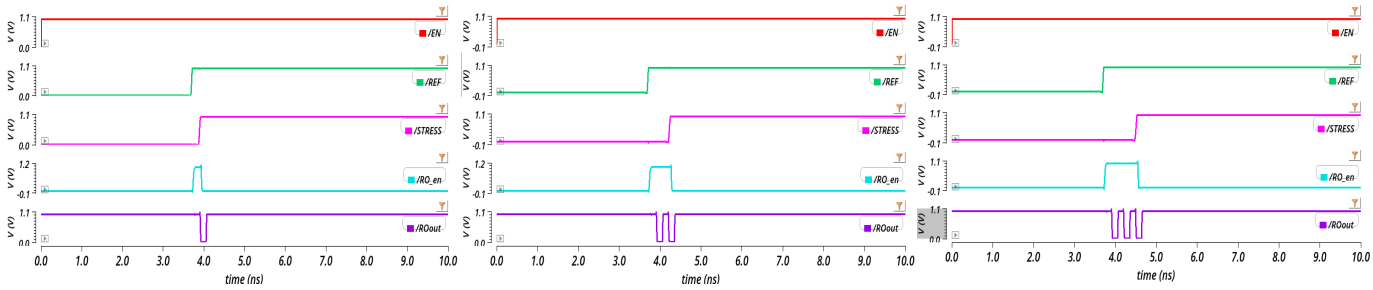
- Two identical inverter delay chains are driven by these two drain voltages with a 'START' signal as the input of both delay chains. 'START' signal of both delay chains are asserted at the same time; the 'EN' signal can be re-purposed for this so that only one external pin is needed. Although both delay chains are identical and both inputs are asserted at the same time, the output depends on the supply voltage which comes from the drain voltage of the pass transistors of reference and stressed path. As the drain voltage of stressed path is lower, the delay chain powered by the stressed path experiences more delay and the output arrives later compared to the delay chain powered by the reference path.
- Output of the delay chains are used as inputs of an XOR gate. The output of the XOR gate is a signal which is asserted for a period of time which is equal to the delay between the delay chain outputs of reference path and stressed path. This span of time indicates the extent of aging of the stressed path which increases the threshold voltage of stressed pass transistor, lowers its drain voltage and introduces longer delay in the delay chain in the stressed path compared to the delay chain in the reference path.
- The output of XOR gate is used as an enable signal of a ring oscillator (RO) which oscillates at a frequency which can be controlled by number of inverters in the RO chain. To accommodate the enable pin, the first inverter of the RO chain is replaced by a NAND gate.
- The RO output is used as a clock pin of a counter which counts number of positive edges of the RO output. As the stressed pass transistor undergoes more and more aging, the delay chain output mismatch increases, increasing the time XOR gate output is asserted. In turn, the RO is enabled for longer and there are more positive edges at RO output which are then counted by the counter.

Aging can be estimated by observing the count value.

B. Implementation Details

1) LDO: In our LDO-based odometer design, we use the configuration shown in Figure 2b with two pass transistors, one in reference path (inactive in normal operating condition) and the other in stressed path or normal path (active in normal operating condition).

2) Inverter Delay Chain: Inverter delay chain consists of even number of inverters connected one after another. The delay generated by the delay chain is proportional to the number of inverters in the chain. The delay also depends on the supply voltage of the delay chain where delay increases with decreasing supply voltage. In our LDO-based odometer design, this phenomena is used. The supply voltage of the delay chain in the reference path is higher compared to the supply voltage of the delay chain in the stressed path. Thus, the delay of stressed path is higher. The input, $START$ of both delay chains is the same signal which is EN. The output of the delay chains have different logic high levels due to different supply voltage. To make delay chain output rail to rail, buffers



(a) About 1 month of aging (b) About 2 months of aging (c) About 3 months of aging

Fig. 3. Simulation of Ring Oscillator (RO) output at different duration of aging. In the figures 'ROout' represents the RO output and 'Count' value is the number of positive edges in 'ROout'

with V_{DD} as supply voltage are used at both reference path and stressed path delay chain output. The rail to rail outputs of the delay chains are used as inputs to the XOR gate as shown in Figure 2b.

3) XOR Gate: XOR gate outputs logic high when the inputs are different (one logic high and the other logic low) and logic low when the inputs are same (both logic high or both logic low). In our LDO-based odometer design, the inputs to the XOR gate are the outputs of the delay chains of reference and stressed path. These two inputs are identical except for the delay duration. During this delay duration the inputs to XOR gate are different and XOR gate outputs logic high. All other times, XOR gate outputs logic low. The output of XOR gate is used as an enable signal, RO_{en} to the ring oscillator as shown in Figure 2b.

4) Ring Oscillator: The ring oscillator or RO has odd number of inverters connected one after another where the output of the last inverter is connected to the input of the first inverter. As a result, The output of the RO is an oscillation where the RO frequency is determined by the number of inverters in the RO chain. Here in our LDO-based odometer design, we convert the first inverter of the RO chain to a NAND gate to accommodate the enable signal, RO_{en} which comes from the XOR gate output. The output of the RO chain, RO_{out} oscillates at RO frequency as long as RO_{en} is logic high.

IV. Results and Discussion

For the simulation, we use Cadence Virtuoso version IC6.1.7. We use 45nm process library with model library set up to `tt` (i.e., typical typical). The width and length of the pass transistor in our LDO design is $90\mu m$ and $450nm$ respectively. Considering Equations (1) and (2), we can estimate the increase in threshold voltage due to aging of the pass transistor in our LDO design which is shown in Table I.

From the table, we see that a threshold voltage increase of about 40mV, 60mV and 80mV corresponds to about one month, two months and three months of aging. We simulate these three conditions by adjusting the threshold voltage of the stressed path pass transistor accordingly in our LDO odometer design.

TABLE I
Threshold Voltage Increase of LDO Pass Transistor Due to Aging

Time (days)	Threshold Voltage Increase (mV)
1	10.8
5	22.2
15	36.5
30	49.9
60	68.1
90	81.7
120	93.0
180	111.6
240	127.1

In our simulation, we design the error amplifier to have open loop gain of about 40dB and phase margin of about 80 degrees to ensure stability of closed loop LDO operation. In the inverter delay chains we use 80 inverters back to back. We design the XOR gate in traditional CMOS technology where the inputs come from the outputs of the delay chains. In the ring oscillator chain we use 13 inverters among which the first inverter is a NAND gate to accommodate the enable signal coming from the output of XOR gate.

We simulate threshold voltage increase of 40mV, 60mV and 80mV of stressed path pass transistor corresponding to about one month, two months and three months of aging and observed the ring oscillator output RO_{out}. We consider the number of positive edges in RO_{out} as 'Count' value. The count value is 1, 2 and 3 for one month, two months and three months of aging as shown in Figure 3a, Figure 3b and Figure 3c respectively.

A. Classification Accuracy under Process Variation

The correct classification by the LDO odometer (i.e., new vs. recycled/used) depends on the delay in the delay chain outputs between reference and stressed paths due to reduced supply voltage of stressed path delay chain as a consequence of aging of stressed path pass transistor. If no process variation is considered, for a new chip reference path and normal path pass transistors should be identical. Thus, they should provide identical supply voltages to delay chains and there should not be any delay between reference and stressed delay

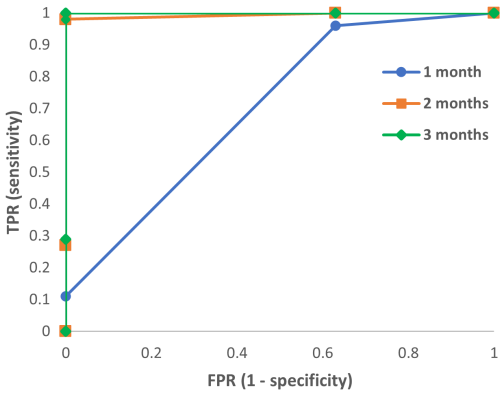


Fig. 4. ROC curve for one month, two months and three months aged LDO pass transistor.

chain outputs. As a result, XOR gate output should not be asserted and RO is not enabled leading to a 'Count' value of 0. However, due to process variation, even for new chips there is mismatch in delay between reference and stressed path.

We performed a Monte Carlo simulation of 500 random points to simulate process variation for new, one month, two months and three months aged chips. In case of new chips, about 38% of the times the 'Count' value is 0 as expected and rest of the times 'Count' value is 1. In the case of one month aged pass transistor, 'Count' value is 0, 1 and 2 for 4%, 85% and 11% of the times respectively. For two months old pass transistor, 'Count' value is 1, 2 and 3 for 2%, 72% and 26% of the times respectively. Fot the three months aged pass transistor case, 'Count' value is 2 for 2%, 3 for 70% and 4 for 28% of the times. We generate a receiver operating characteristic (ROC) curve with true positive rate (TPR) versus false positive rate (FPR) for one month, two months and three months aged chips which is shown in Figure 4. TPR is the measure of sensitivity and FPR is a measure of specificity. If a threshold value for 'Count' is chosen to be 2 for counterfeit detection, it is possible to detect one month old chips 11% of the times, two months old counterfeit 98% of the times, three months old counterfeit 100% of the times with 0 false positive. Thus, a threshold 'Count' of 2 is suitable for detecting counterfeited chips that are at least two months old with high accuracy.

B. Comparison to Previous LDO Recycled Chip Detection

In previous work [8], degradation of PSRR due to aging of standalone LDO is used to detect counterfeit. This design has no extra area overhead and is capable of detecting aged LDO of about 10 days with an accuracy up to 97%. But, PSRR measurement is an external time consuming step. In the LDO design of [7] also, PSRR degradation is used. Here, the area overhead is only the pass transistor area for the reference path and this design is capable of detecting counterfeit with up to 99% which are aged 10 days or more. PSRR is measured by switching between reference and normal path externally using two pins which can be accessed by any adversary posing a security vulnerability. In contrast, our LDO odometer has extra area overhead due to the presence of two identical delay chains, an XOR gate, an RO and a counter. Also, our detection accuracy is up to 98% for chips which are two months old or more which is six times more aging requirement to achieve comparable accuracy of previous work. But, our design is self-contained and does not require external time-consuming PSRR measurement. Also, our design does not require external pin to activate the reference path which removes the security vulnerability described earlier. In short, our LDO odometer provides enhance security with comparable accuracy of counterfeit detection at a cost of some area overhead.

V. Conclusion and Future Work

Counterfeit electronics is a threat to system security and integrity. With complex horizontal supply chain of electronics chips manufacturing spanning the whole world, preventing counterfeit is becoming more and more challenging. Robust methods to detect and remove counterfeits from supply chain is of imperative importance. Our improved self-contained LDO-based odometer capable of detecting counterfeit with on-chip measurement is a step towards answering the global counterfeit chip problem. In future further improvement can be done on our LDO-based odometer design to optimize area, performance and power consumption. Also silicon results along with simulation could further justify the use of LDO-odometer for counterfeit detection with high reliability and accuracy.

Acknowledgment

The authors would like to acknowledge Air Force's Center of Excellence for Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN) under the contract number FA8650-19-1-1741 for this research.

References

[1] U. Guin, D. Forte, and M. M. Tehranipoor, "Anti-counterfeit techniques: From design to resign," *2013 14th International Workshop on Microprocessor Test and Verification*, pp. 89–94, 2013.

[2] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: detection, avoidance, and the challenges ahead," *Journal of Electronic Testing*, vol. 30, pp. 9–23, 2014.

[3] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.

[4] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ics," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 22, no. 5, pp. 1016–1029, 2013.

[5] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost on-chip structures for combating die and ic recycling," in *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2014, pp. 1–6.

[6] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233–1246, 2015.

[7] R. Y. Acharya, M. V. Levin, and D. Forte, "Ldo-based odometer to combat ic recycling," *IEEE 34th International System-on-Chip Conference(SOCC)*, pp. 206–211, 2021.

[8] S. Chowdhury, F. Ganji, T. Bryant, N. Maghari, and D. Forte, "Recycled analog and mixed signal chip detection at zero cost using ldo degradation," in *2019 IEEE International Test Conference (ITC)*, 2019, pp. 1–10.

[9] S. Chowdhury, H. Shen, B. Park, N. Maghari, and D. Forte, "Aging analysis of low dropout regulator for universal recycled ic detection," in *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2019, pp. 604–609.

[10] S. Chowdhury, F. Ganji, and D. Forte, "Recycled soc detection using ldo degradation," *SN Computer Science*, vol. 1, pp. 89–94, 2020.