Recycled Analog and Mixed Signal Chip Detection at Zero Cost Using LDO Degradation

Sreeja Chowdhury, Fatemeh Ganji, Troy Bryant, Nima Maghari and Domenic Forte

Abstract— **Counterfeit electronics impact the global economy and pose life-threatening risks to critical systems and infrastructure. Analog/mixed-signal (AMS) chips are the most widely reported counterfeit chip type, but existing countermeasures are impractical for detecting them. In this paper, we propose a method to detect recycled AMS counterfeits that exploits degradation of power supply rejection ratio (PSRR) in low drop out (LDO) regulators. Our zero cost approach does not require information about the component's design. Moreover, due to the ubiquity of LDOs, it may apply to active and legacy AMS system on chips (SoCs). To evaluate the feasibility and effectiveness of our method, we use an automated test setup to collect PSRR data from commercial off-the-shelf LDOs before and after aging. Machine learning algorithms ranging from unsupervised to supervised are applied to differentiate between aged (i.e., synthetically recycled) and new LDOs. Silicon results confirm that semi-supervised and supervised algorithms are effective even with LDOs used less than 10 days.**

I. Introduction

The number of counterfeit parts appearing in the electronics supply chain is increasing every day, and poses serious threats to economy, security, and safety. While there are many categories of counterfeit integrated circuits (ICs) [1], the recycled type is reportedly the most common. Recycled counterfeits are used components that are harvested from discarded printed circuit boards (PCBs) and then sold as new on the market. Such ICs are prone to failure and should not be used in critical applications. Counterfeit IC detection has received considerable attention from researchers, but has mostly focused on digital ICs. This is unfortunate because the analog ICs make up the largest percentage of counterfeits (25% in 2011 [2]).

Existing research for counterfeit IC prevention and detection can be broadly divided into two categories: (1) Counterfeit detection for new digital ICs require additional circuitry. Physical unclonable functions (PUFs) are a promising approach falling into this category. PUFs leverage the inherent process variations in the chip to create unique identifiers for every chip, thus preventing cloning and overproduction [3]. In [4], the combating die and IC recycling (CDIR) sensor was developed to detect aging in recycled ICs by acting as an odometer; (2) Counterfeit detection for active and obsolete ICs do not require modifications to the IC design and mostly consist of general electrical tests. These tests examine the parameters of a device/IC and compare them to a specification. They are suitable for detection of out-of-spec/defective, recycled and remarked counterfeit types, but are impractical to implement on the wide variety of ICs in the market. Several other approaches (e.g., [5]) that detect the degradation of parameters in recycled ASICs and FPGAs require measurements from known new ICs (golden data) to be available for comparison.

The above techniques are either restricted to digital ICs or have limitations with respect to AMS ICs. First, design approaches like PUFs and CDIRs require additional logic and input/output (I/O) pins which are limited in AMS ICs. Second, electrical tests require golden data/models. For example, targeted electrical test exclusively for AMS ICs were proposed in [6], but they require an accurate simulation model of the design (unavailable for commercial-off-the-shelf ICs) to determine the amount of aging/recycling. Third, the existing techniques do not cover all types of AMS ICs. Given the variety of AMS ICs available in market, a single inexpensive technique for all of them has been elusive. Further, a technique applicable to detect a recycled IC for an AMS IC from one vendor may not be applicable to another vendor since the designs are likely different and often proprietary.

In this paper, we propose a novel technique for detection of AMS recycled counterfeits which focuses on a ubiquitous element in AMS ICs – low dropout regulators (LDOs). LDO is a crucial component present in the power supply in most types of ICs (including AMS and digital). Thus, detection of aging effects on a LDO may help in detecting any type of recycled IC at zero cost[1]. Our major contributions are summarized as follows:

- We exploit chip aging effects of an LDO's power supply rejection ratio (PSRR) to determine if the IC is recycled. PSRR is a critical metric available in any LDO specification sheet which measures the ripple rejection capability of an LDO. Our analysis reveals how the LDO performance (PSRR) changes at lower and mid frequency range.
- Using an automated test setup, we continuously collect data from 128 LDOs of four different vendors at 1 hour time intervals. For vendor 1 (V1) and vendor 2 (V2),new and used LDOs are separable in as little as 4 hours of accelerated aging (approximately 4 days in real-time). For vendor 3 (V3) and vendor (V4) only 1-2 hour of accelerated aging is enough for separation of new and aged LDOs.
- We employ supervised to unsupervised machine learning (ML) methods to automatically determine a boundary between aged and non-aged PSRR and classify recycled ICs. With supervised ML, our accuracy to detect a recycled LDO is $\approx$ 94.25% for V1 and $\approx$ 97.43% for V2 with 4 hours of accelerated aging. Whereas, the

[1]No additional chip design area, power and delay

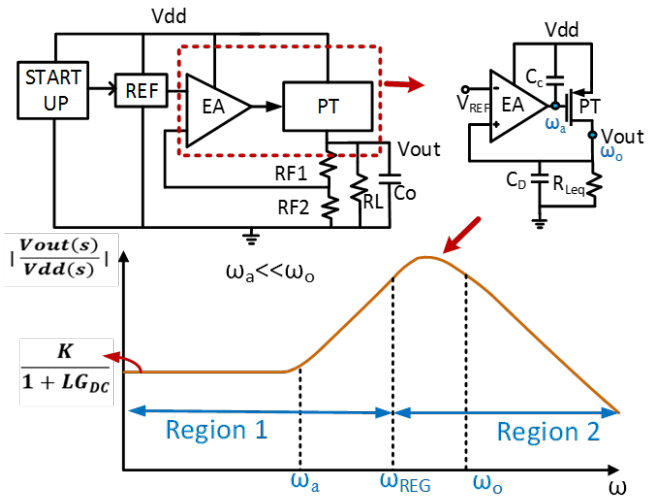


Fig. 1: LDO block diagram with PSR (linear scale) curve

mean accuracy for V3 and V4 are ≈ 87% and 91% after 1 hour of accelerated aging. While training with the classifier extracted from V1 and applying on V2, V3 and V4, we get an average accuracy of ≈ 78% with 4 hours of accelerated aging. Whereas, extracting the classifier from V3 and testing on all the other vendors V1, V2 and V4 gives an approximate accuracy of 90.5% thus, relaxing labeled LDO requirements. We also find cases where unsupervised ML is promising which has been able to detect recycled LDOs with an average accuracy of ≈70%.

The rest of the paper is organized as follows. The background on LDOs and IC aging sources are introduced in Section 2. The proposed methodology, aging analysis and ML concepts are described in Section 3. The results and discussion are explained in Section 4. Finally, we conclude and discuss future research in Section 5.

II. Background

A. LDO Preliminaries

An LDO is a type of linear regulator which is capable of maintaining an output voltage even when the input is very close to the output (low drop-out). Drop-out voltage is defined as the input to output differential voltage at which the regulator fails to regulate the output voltage until further reduction of the input voltage. As shown in Figure 1, the block diagram of an LDO consists of a feedback loop with an error amplifier (EA), a pass transistor (single NMOS or PMOS) and a resistor divider. A bandgap circuit provides a fixed reference voltage to the EA. The pass transistor (PT) acts as a variable resistor which is controlled by the EA and the feedback resistor divider circuit level-shifts the output voltage to the EA input. The EA monitors the error between the input and the output voltage and accordingly controls the gate to source voltage (v_{gs}) of the PT to regulate the output at a fixed voltage. If the feedback voltage is smaller than the reference voltage then the gate voltage of the PT is lowered increasing the v_{gs} as well as the current flowing through the PT; thus increasing output voltage. While, if the feedback voltage is higher than the reference, the v_{gs} of PT is decreased, reducing the current as well as the output voltage. The drop-out voltage for a generic LDO as shown in Figure 1, is actually the drain to source voltage drop which appears across PT.

The role of an LDO is indispensable in the power supply of any AMS IC. It provides isolation between the input and output, thus rejecting the noise and ripples (glitches) in the input supply at the output to provide a stable, low noise, fixed output voltage. One of the major performance metrics of an LDO is it's capability of rejecting the ripples of the input supply at it's output. This is represented by the power supply rejection ratio (PSRR) of the LDO. The ripple can originate from the power supply or from a DC/DC converter or even due to sharing an input supply between different circuit blocks in the system. PSRR is expressed as $PSRR = 20\log(\frac{v_{out}}{v_{in}})$ where, v_{out} and v_{in} are magnitudes of voltage glitch at output and input, respectively.

B. General Concepts of Transistor Aging

Transistor aging is one of the major causes of reliability issue faced by modern ICs including AMS ICs. It is the resultant of trapped charges and broken bonds at gate dielectric interfaces which results in increase of threshold voltage (V_{th}) and switching activity thereby, deteriorating transistor performance in scaled modern devices. *Bias temperature instability (BTI)* results in a positive shift in the absolute value of V_{th} in both PMOS and NMOS. BTI is the condition often referred to as DC stress when the PMOS/NMOS has already pulled up/down but the gate is still biased in strong inversion. The drain to source voltage becomes zero signifying negligibly small lateral electric field. For PMOS, the condition is called negative BTI (NBTI) whereas for NMOS it is positive BTI (PBTI). *Hot carrier injection (HCI)* occurs when the transistor is switching under strong inversion ($|v_{gs}| \approx V_{dd}$) and the lateral electric field is high ($|v_{ds}| \approx V_{dd}$). During transistor switching, the accelerated carriers drift towards the drain under the influence of the lateral electric field. Channel hot carriers (CHC) are generated when the source to drain current flowing though the channel reaches an energy above the lattice temperature. These hot carries gain energy and gets injected into the gate oxide forming charge traps. As a result, this causes shift in the device performance like V_{th}, transconductance and saturation current of transistor as discussed in [7]. HCI degradation increases as $t^{1/2}$ (where t is time) and BTI increases as a factor of t^n where $n = 0.1$ to 0.2. But the multiplicative constant of HCI is much smaller than that of BTI, thus for short amount of time, BTI overshadows HCI as suggested in [8]. But for longer time, HCI may effect in equal or more degradation in device parameters as BTI.

The impact of the above aging phenomena on the reliability of analog/AMS circuits has not been explored extensively. We have found very few papers [9] that discuss how the presence of some specific structures like feedback and diode connected transistors in analog circuits can aggravate the aging degradation. Further, there are very few models present in the literature which can simulate accurately analog circuit aging. The models presented in [9] only simulate a few

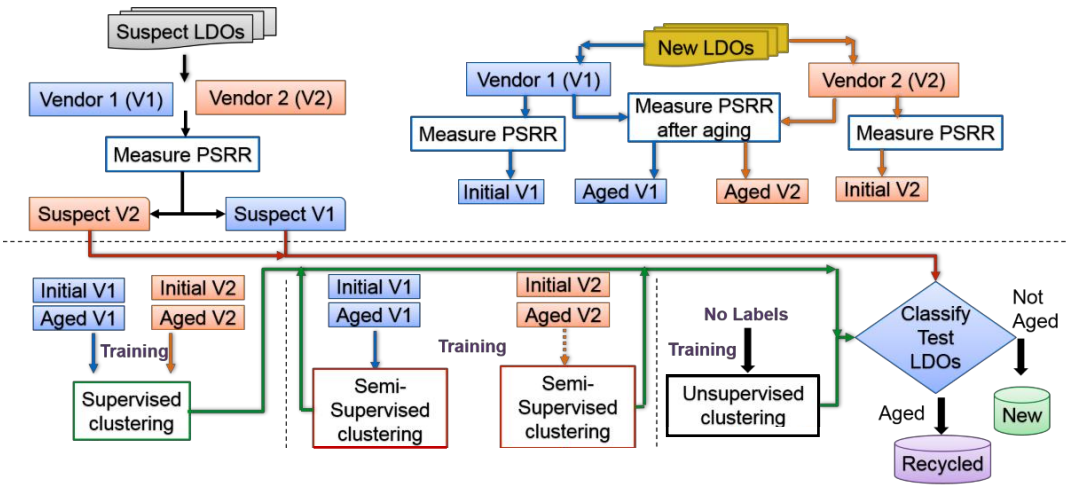


Fig. 2: Flowchart of proposed method for recycled LDO detection in supervised, semi-supervised, and unsupervised ML

specific and simple structures, and may not be able to tackle more complex analog designs.

III. Proposed Methodology

We propose to detect recycled AMS ICs by exploiting the aging degradation of LDO PSRR and machine learning (ML) algorithms. The flowchart of the proposed method is given in Figure 2. We only have shown two vendors for simplicity. First, ML models are trained using input data (PSRR) from LDOs. Note that the input features (PSRR from new and/or aged LDOs from multiple vendors) vary based on the type of ML used (supervised, unsupervised, or semi-supervised); (1) For supervised learning, training and testing data set both belong to different samples from the same vendor. In total, we have data from four vendors (V1 through V4) and use K-nearest neighbour (KNN) algorithm for supervised learning; (2) In case of semi-supervised ML, we train the classifier with one vendor but test it on another vendor. For instance, we train with samples from V1 and test them on V2, V3 and V4. This same pattern is repeated for all the other vendors; (3) For unsupervised, no labels are provided during training. In this paper, we employ variational bayesian state space model, the k-means clustering for unsupervised ML and KNN algorithm for supervised ML (more details forthcoming). When an LDO (or SoC with an LDO) is purchased from the market, it is considered as "suspect". The suspect LDO PSRR is measured and the above classifiers are used to detect whether it is recycled (aged) or new.

Note the following about assumptions for our method and experiments found in this paper: (1) We assume that the LDO output pin is accessible for proper implementation of our method. In most LDOs, the output node is connected to a capacitor to ensure stability. Industrial LDOs even mention the minimum capacitor load that must be attached to the LDO output to stabilize its operation, in their spec sheets. Thus, it is easy to reverse engineer the LDO output pin in an SoC or printed circuit board (PCB); (2) We use commercial off-the-shelf (COTS) LDO chips from the leading vendors to verify the proposed method. This makes the entire method usable to everyone without any requirement of additional design or logic added to the system; (3) Due to the unavailability of recycled LDOs, we artificially age LDOs (by thermal heating at elevated temperature) to create synthetic recycled counterfeit LDOs; (4) We only validate our approach on standalone LDOs in this paper for simplicity. We emphasize that our approach is generic and should be applicable to LDOs embedded in AMS SoCs. In fact, this method can be applied to any PCB/SoC which consists of an LDO be it AMS or digital. This will be verified in future work; (5) Also, we have analyzed the aging degradation of an LDO with respect to a generic LDO design. The internal designs of the LDOs which we inspected is proprietary to individual design houses. However, the general principles should apply to most LDO designs.

A. Analysis of Aging on LDO PSRR

In order to understand the effect of transistor aging in LDOs, one needs to examine the transfer function of the PSRR. Referring to Figure 1 and the explanation given in [10], the power supply rejection of a generic LDO, i.e., *PSR* (in linear model), can be represented as

$$PSR = \frac{v_{\text{out}}(s)}{v_{\text{dd}}(s)} = \frac{K(1+\frac{s}{\omega_{\text{a}}})}{(1+\frac{s}{\omega_{\text{a}}})(1+\frac{s}{\omega_{\text{o}}})+A_{\text{a}}A_{\text{o}}} \quad (1)$$

$$= \frac{K}{(1+\frac{s}{\omega_o})(1+LG(s))} \quad (2)$$

where

$$K = \frac{R_{\text{Leq}}}{R_{\text{Leq}}+r_{\text{dsP}}}, \quad \omega_{\text{a}} = \frac{1}{ro_{\text{ea}} * C_{\text{c}}}, \quad \omega_{\text{o}} = \frac{1}{(r_{\text{dsP}}||R_{\text{Leq}}) * C_{\text{D}}}$$

$$A_{\text{a}} = g_{\text{ma}} * r_{\text{oa}}, \quad A_{\text{o}} = g_{\text{mP}}(r_{\text{dsP}}||r_{\text{out}}) \quad (||\,denotes\,parallel) \quad (3)$$

$$g_{\text{m}} \propto v_{\text{eff}}, \qquad v_{\text{eff}} = v_{\text{gs}} - V_{\text{th}} \quad (4)$$

LG is the loop gain of the LDO feedback. r_{dsP} refers to the drain to source small signal resistance of PT while r_{oa} is the small signal output resistance of the amplifier. The equivalent output resistance at the node v_{out} is taken as r_{out}. The error amplifier and the pass transistor have respective

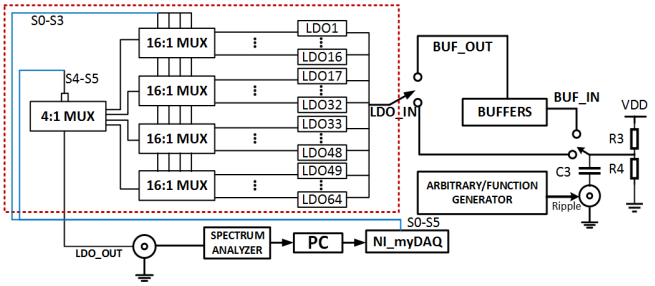


Fig. 3: Block diagram of experimental setup

transconductances of g_{ma} and g_{mP} and loop gains A_a and A_o. The pole due to the node capacitance (C_c) at the output of the error amplifier originates at frequency ω_a while the one due to the equivalent output capacitance (C_D) at the output node originates at ω_o. R_{Leq} is the equivalent capacitance at output and we assume ω_a as our dominant pole. The PSRR curve of most LDOs can be divided into two distinct regions (see Figure 1). The first one (region 1) occurs in the low and mid frequency range till the unity bandwidth frequency (ω_{reg} : where the DC loop gain becomes 1) of the LDO regulator. The second region (region 2) is in the higher frequency range located after the regulator bandwidth frequency. In region 1, the PSRR is actively controlled by loop gain *LG*. In region 2, the loop gain has little effect and the PSRR is dominated mainly by parasitics from input to output, the output capacitor, PT impedance and the PCB.

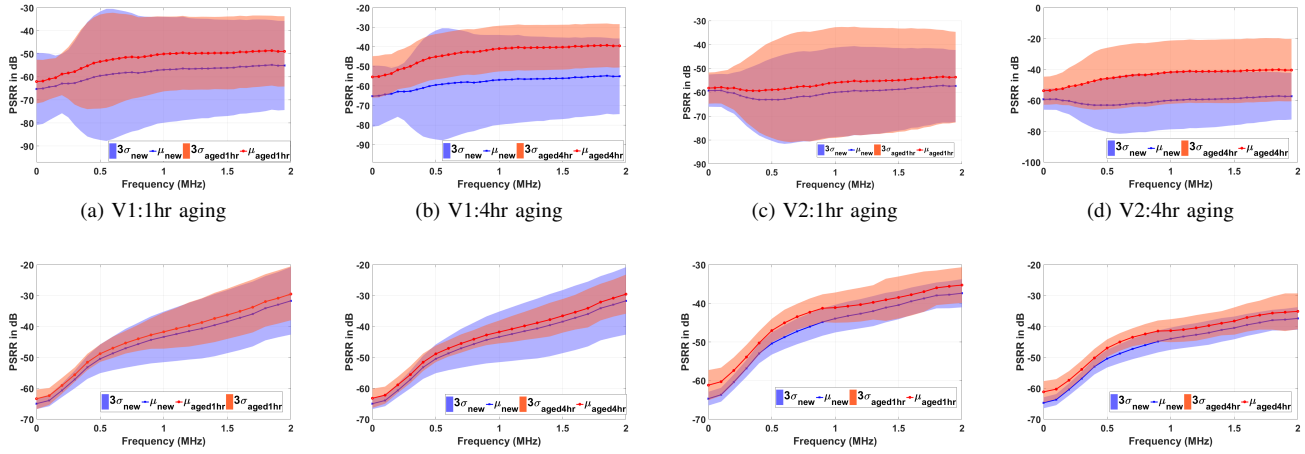
PSRR Aging in Region 1: As shown in Equation (1), the absolute value of *PSR* increases as *LG* decreases with increasing frequency. This signifies that the capability of the LDO to reject ripples decreases. The smaller the *PSR*, the better the rejection as less ripples from V_{dd} appear at V_{out}. High loop gain *LG* of the LDO ensures better rejection in region 1. The loop gain of the LDO is directly proportional to the individual open loop gains of the EA and PT respectively as shown in Equation (1). The open loop gain, on the other hand, is directly proportional to the transconductance of the PT and the input transistors of the EA as shown in Equation (3). Since V_{th} increases with both BTI and HCI [9], transconductance g_m and the overall loop gain of the LDO (see Equations (4) and (3)) are degraded, thus impacting PSRR. In AMS circuits, the transistors are biased to operate in saturation region for maximum small signal gain and linearity. This configuration causes more HCI degradation as shown by the authors in [9]. They also show that the degradation (increase) in V_{th} is enhanced due to the presence of feedback loops in circuits. The feedback loops dynamically vary the operating condition in AMS circuits to stabilize the circuit operation thus aging the transistors more. Lastly, configuration of transistors also impact respective aging degradation. Certain configurations like diode connected transistors where $V_{gs} = V_{ds}$ receive the worst stress as shown for technology node of 65nm and 28nm in [9]. A generic LDO also consists of a feedback loop which continuously monitors the error voltage (difference between expected and actual output voltage) at the output. This may enhance the stress on the input transistor of the EA and the pass transistor increasing the respective V_{th} and further accelerating transistor aging. Also, presence of diode connected transistors in the EA as well as in current biasing circuit can further aggravate aging.

PSRR Aging in Region 2: At the LDO unity gain bandwidth (ω_{REG} in Figure 1), $LG = 1$ and the PSRR curve mainly behaves as a resistor divider (K in equation 3). Thus *LG* has less/no impact while the capacitances including the parasitics affect the PSRR curve. The major capacitances include C_C and C_D as shown in Figure 1; which are effective in formation of the poles at ω_a and ω_o. With accelerated aging, the gate to source and gate to drain capacitance of PT may change leading to shift in the pole frequencies (See equation 3). This phenomena of the variation of gate capacitance (C_{gd} and C_{gs}) with respect to hot carrier degradation has been exemplified for a 64-Mb DRAM chip in [11]. They performed an electron beam probing to detect the difference in gate capacitance before and after hot-carrier stress for the DRAM chip. The experimental results show that the precharge time of the DRAM chip increased from 20ns to 22ns after a 47 hour hot carrier stress demonstrating significant change in gate capacitances. As the PT is usually a huge transistor in generic LDO design, the increase in the capacitance may substantially change the structure of PSRR curve. We can see such changes in Figure 5d below for V4 where the structure of PSRR curve is changing with aging. We see certain peaks appearing at approximately 1.2 MHz, 2.3 MHz and 4MHz for V4 which were not present in the initial PSRR curve. We suspect these are due to the shifting of non-dominant poles and zeros with the changes in gate capacitance of the PT due to HCI as well as BTI. We plan to investigate the effect of transistor aging on the gate capacitance of the PT of an LDO in our future works.

B. Experimental Setup and LDO Aging Results

In this section, we discuss the experimental setup and the data collection procedure used throughout the paper. To verify the above analysis, we collected data from 128 LDOs from four different vendors (32 each) using an automated test setup. The LDOs are aged at an accelerated rate using 80°C in a Summit 12000B automated probe station and the PSRR data is collected at 1 hour intervals for 9 hours. Collecting aging data every hour enables us to determine the optimum amount of aging required to detect recycled LDOs. We have only used temperature acceleration factor here. This is because, LDOs are designed to operate at a range of input voltages, thus there is no specific operating voltage for a LDO. According to [12], the elevated temperature converts to an accelerating factor of 21. Thus, 9 hours of accelerated aging converts to approximately 9 days of constant real time aging. *Note that we have verified in separate experiments that the aging effects on the multiplexer and PCB are negligible. Thus the aging shown in Figure 4 and 5 is solely due to the LDOs.*

The automated setup consists of the 64 LDOs (2 vendors) on a PCB which are multiplexed through four 16 channel and one 4 channel multiplexer as shown in Figure 3. We have used 2 such PCBs to cover four vendors. (V1 and V2 in PCB 1 while V3 and V4 in PCB 2) The output current of the LDOs are maintained at approximately 30mA.



(a) V1:1hr aging (b) V1:4hr aging (c) V2:1hr aging (d) V2:4hr aging

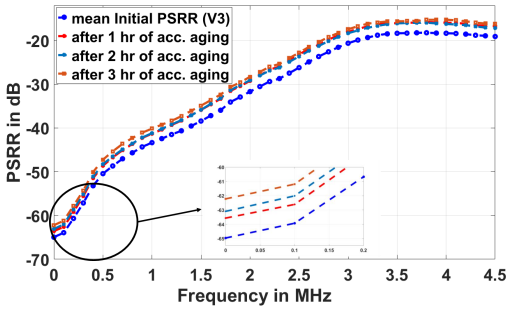
(e) V3:1hr aging (f) V3:4hr aging (g) V4:1hr aging (h) V4:4hr aging

Fig. 4: Silicon data showing mean PSRR degradation of LDO for V1, V2, V3, and V4 for 1 hr (a,c,e,g) and 4 hr (b,d,f,h), respectively. Note that for V3 and V4, the aging degradation of mean PSRR saturates after 3-4 hours of aging shown in Figure 5 below

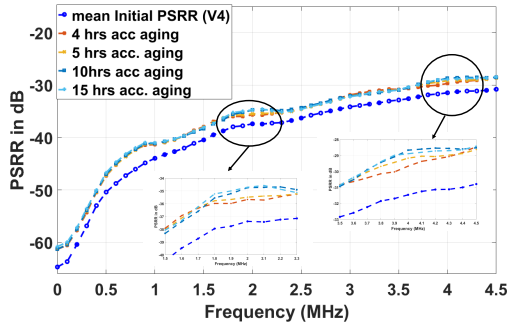
The input pins of LDOs include the supply voltage, an enable pin, a ground pin, and a feedback pin. There is a single output pin which provides the regulated output. We applied an input supply voltage of 3V which is approximately the mean voltage of the common operating voltage range (0-5V) of the LDOs from the vendors. This ensured that we are not applying a voltage too high or too low at the input. We tried to mimic the standard operating condition in which chips/SoCs operate and 3V is one of the standard supply voltages. The LDOs were running during the entire accelerated aging procedure, thus the enable pin was high. The feedback pin was connected to a resistor divider, while the resistors were chosen using the product data sheet. The output pin was connected to a capacitor (4.7uF for V1,V3 and V4 and 1uF for V2) as mentioned in the product data sheet to stabilize the LDO operation. The output pin was also attached to a load resistor whose value was chosen to maintain a 30mA output current. We initially tried to use a high output current to accelerate the aging process, but it was limited by the maximum output current drive of the buffers on board and the function generator. As we had 32 LDOs (each vendor) running simultaneously during aging we could not exceed 30mA. We aged the LDOs at 80°C which is one of the standards for reliability testing as shown in [13].

We generate a noise signal of 500 mV(p-p) using an arbitrary function generator and couple it to the power supply V_{dd} with a capacitor. This procedure of PSRR measurement is shown as one of the standards in [14]. The noise signal is chosen such that: $Vac_{\max} + Vdc < V_{\text{ABS}}$ (max) of the LDO and $Vdc - Vac > V_{\text{UVLO}}$ of the LDO. UVLO or the undervoltage-lockout of an LDO is the electronic circuit used to turn off the power when the input voltage drops below the operating value of the LDO. This only means that when the AC signal noise is applied one must be careful that the voltage input still remains in the operating range of the LDO. This signal is passed through a buffer and is applied at the input of the LDOs. The select lines of the multiplexers are applied using National Instruments (NI) myDAQ and the output of the LDO is connected to a spectrum analyzer to measure the power spectrum. A Matlab program from a PC is used to apply select signal to the NI myDAQ and collect the output from the spectrum analyzer serially. The PSRR curves are generated for each LDO across a range of frequency from 1Hz to 2MHz at intervals of 5KHz.

The silicon data depicting transistor aging effect on PSRR of 128 different LDOs from 4 different vendors (32 LDO each vendor) is shown in Figures 4 and 5. The PSRR (in dB) is shown in negative as it implies suppression of output ripples. The more the absolute value of PSRR ($|PSRR|$), the better the suppression. As we see in Figure 4, for V1 and V2, $|PSRR|$ degrades with aging for all the vendors. The frequency range 1Hz-500KHz refers to the lower frequency range where the PSRR is actively controlled by the loop gain of the LDO as explained in Section III-A. With 1 hour of accelerated aging at 80°C, the mean PSRR degrades for both the vendors V1 and V2 but it is difficult to discern because of the process variation (shown by shaded regions) in between the LDOs. But as we increase the time of accelerated aging to 4 hours, we see the mean PSRR degrade with aging and the separation between them can be easily distinguished. Due to the wide process variation in between chips (considering 3σ variation shown by shaded region in Figure 4), the aged PSRR distribution still overlap with the new one. But the new and aged PSRR distribution is completely separable considering 1σ process variation (applicable to V1 and V2 after 4hr of aging and V3 and V4 after 2 hrs of accelerated aging). For the other vendors V3 and V4, the PSRR also degrades after 1 hour of accelerated aging as we see in Figure 5 but unlike V1 and V2, the PSRR degradation for V3 and V4 saturates after 1-1.5 hours of aging. After that for V3, we see very small shifts in mean PSRR till 3 hr of aging as in Figure 5a. For V4, with increased accelerated aging, we



(a)



(b)

Fig. 5: Silicon data showing (a) mean PSRR degrading across 1hr, 2hr and 3hr of accelerated aging for V3 after which it saturates (b)shift in poles at higher frequencies and saturation of degradation across 4hr, 5hr, 10hr and 15hr of accelerated aging for V4.

see certain undulations on PSRR curve which increases till 15 hours of aging as depicted in Figure 5b. It can be seen that the curves increase from 4 hrs through 15 hrs of aging whereas the mean PSRR degradation has already saturated after 4 hrs. As discussed in Section III-A, this can be due to shifting of intrinsic capacitances of the pass transistor which may shift the dominant (ω_o) as well as the non dominant poles (ω_a). Also at higher frequency, the gate to drain and gate to source capacitance of the PT may behave as a short circuit and can directly couple the V_{dd} noise to the gate of the PT and the output of the LDO, resulting in degraded PSRR at the output. It is also interesting to note that the process variation (3*sigma*) in between PSRRs decreases with the aging of the chips which is evident for all the vendors V1 through V4 in Figure 4.

The difference in the aging behaviour among V1, V2, V3 and V4 may be attributed to the inherent differences in the design of the LDO including the technology nodes applicable to each of them. The input voltage range for V1 and V2 were approximately 0-5.5V whereas that for V3 and V4 were 0-20V. The output current range for all the vendors were from 10mA to 100mA. For similarity of test conditions and to limit power consumption for each PCB we have taken the common input voltage (0-5.5V) range among all the vendors and applied a mean 3V input. But, considering V3 and V4 can operate at higher voltage ranges, the degradation can be different for V3 and V4 compared to V1 and V2. Irrespective of the aging behaviour, the degradation is prevalent in all the vendors and in all the cases the degradation is maximum at initial hours of aging and saturates after a given aging time. Instinctively, it can be concluded that, since the mean PSRR values before and after aging can be separated, if we feed this data to supervised machine learning (ML) algorithms then a boundary between new and aged (synthetic recycled) can be obtained. For unsupervised ML, it can be challenging given the variability between vendors and process variation within a specific vendor.

C. Applicability of Gaussian Mixture Models

As one of the key steps for ML is data representation, we begin by explaining how the aforementioned experimental data can be prepared to feed into an ML algorithm. One can observe that our dataset is multidimensional and collected over pre-defined time and frequency ranges. For an LDO and at given frequency, the PSRR measurements are done every hour in a 9 hour window. It is clear that over this dimension, the sequence of the measured values can be represented as a time series. If we examine our dataset over the other dimension, i.e., frequency, we observe that the sequence of the measured PSRRs is ordered and exhibits irregularities, e.g., environmental noise. In other words, this sequence exhibits the characteristics of a time series, although being non-temporal naturally. Therefore, our problem of classifying/clustering the data collected from LDOs over a range of frequency can be thought of as a sequence labeling problem, where the sequences are non-temporal, but time series-like. In the ML-related literature, such a problem can be tackled by applying time-series analysis adapted to reflect the non-temporal nature of the data, see, e.g., [15], [16]. A common approach to analyze a sequential, structured, time series-like data is to employ a state-space model (SSM).

State-space model (SSM). In an SSM, it is assumed that a sequence of measured data y (in a vector form) $\mathbf{y}_1, \mathbf{y}_2, \cdots$ is generated by some *hidden* state variables $\mathbf{x}_1, \mathbf{x}_2, \cdots$ with joint probability,

$$p(\mathbf{x}_{1:F}, \mathbf{y}_{1:F} \mid \theta) = \prod_{f=1}^{F} p(\mathbf{x}_f \mid \mathbf{x}_{f-1}, \theta)\, p(\mathbf{y}_f \mid \mathbf{x}_f, \theta)$$

where θ is the model parameter, $\mathbf{x}_{1:F}$ and $\mathbf{y}_{1:F}$ are the sequence of F sequences of the hidden state variables and the measurements, respectively. Note that the indices f and F stress that our data is collected over a frequency range in an ordered manner. In this paper, we stick to the most straightforward type of SSMs, i.e., linear-Gaussian state-space models composed of multivariate Gaussian-distributed variables with a linear relationship, as formulated in Equation (5) [16].

$$\begin{aligned} \mathbf{y}_f &= C\mathbf{x}_f + \mathbf{v}_f \\ \mathbf{x}_f &= A\mathbf{x}_{f-1} + \mathbf{w}_f \end{aligned} \tag{5}$$

The linear relationship is shown through C and A matrices, and the vectors $\mathbf{v}$ and $\mathbf{w}$ represent *uncertainty*. These two vectors also follow Gaussian distributions, with covariance matrices R and Q, respectively. In the context of our problem, $\theta = (A, C, Q, R)$ are the parameters of an LDO. The vectors $\mathbf{v}$ and $\mathbf{w}$ account for the total impact of aging, environmental

noise, uncertainty imposed by the measurement process, etc. While the former requires more elaboration, it is common to assume a Gaussian distribution for the latter ones. To this end, we emphasize that for our ML approach, instead of a gate-level characterization of aging, it suffices to model the impact of aging as an uncertainty – represented by a Gaussian variable (see, [17] for an extensive discussion on this model).

Markov Assumption. With regard to the above definition of linear-Gaussian SSMs, another important aspect of data representation is the dependency of the hidden state variables $\mathbf{x}_f$ on one another, or, more precisely, having first-order Markov dynamics. In practice, this variable can be related to the physical characteristics of an LDO. However, for the purpose of our analysis, we adopt the frequency, from which we begin to measure the PSRR values. This choice is very natural since it is known that if we measure the PSRR value at a given frequency, i.e., f_i, and then switch to the frequency f_{i+1}, the value of the PSRR measured at this frequency depends heavily on the frequency f_i. This holds according to the transfer function of PSRR in Equation (1), where, PSRR (see Figure 1) degrades as a function of the initial *LG*.

Parameter Optimization. To learn the parameters of the linear Gaussian SSM defined above, a well-studied approach is the Expectation-Maximisation (EM) algorithm [16]. Informally, this algorithm first fits some arbitrary density function over the hidden variables for a fixed model parameter (i.e., the step "E"), and then in the next step, "M", the model parameter is re-estimated by maximizing the likelihood (see [18], [16] for more details). Despite the fact that this algorithm is applicable in our case, one should consider applying it carefully since, similar to other maximum likelihood approaches, the EM algorithm may fail to determine the best model size and structure due to the complexity of the model. To address this issue, it is suggested to perform variational Bayesian inference over the parameters of probabilistic models in conjunction with the EM algorithm [16], [19]. This type of approximation is helpful to face two major obstacles. First, Bayesian approaches enable us to *guess* some prior distribution over the space of parameters $p(\theta)$ and improve it step-by-step, when analyzing the data. However, this is computationally heavy while all of the so-called *model uncertainties*, i.e., all possible model parameters θ and their respective $p(\theta)$, should be taken into account. The second contribution of variational Bayesian inference is to resolve this issue, and consequently, reduces the amount of data required for the learning process [19].

To sum up the above discussion, we emphasize that according to the complexity of our linear Gaussian SSM caused by the uncertainties imposed by the nature of our data, we apply a combination of variational Bayesian inference and EM algorithm, hereafter called the *VB method* in this paper. It is also important to observe the close relationship between the EM algorithm and the k-means algorithm, widely accepted as a standard approach to cluster the data. Therefore, in the next section, we present the results obtained by applying the k-means algorithm as well as the VB method.

Besides, we demonstrate the applicability of supervised algorithms in our scenarios as well. To this end, as one of the closest approaches to the VB and the k-means methods, we apply the KNN algorithm [18]. The rationale behind this approach is that examples exhibiting similar properties should be in close proximity to one another in a dataset. Hence, when an unseen, new example is given to the algorithm, its label should be similar to the label of its nearest neighbors. These k nearest neighbors are determined according to a distance metric (e.g., Euclidean distance), and then the label of the new example is the most common label of those k nearest neighbors. Therefore, for KNN, the number of neighbors plays an important role. Regarding this, to classify a new example correctly, a large k should be selected if the algorithm has to deal with highly noisy examples. On the other hand, if the classes of the examples are located within a close distance, a smaller k should be chosen [20].

IV. Results and Discussion

Using the experimental setup and data from Section III-B, we present and discuss the results of applying ML algorithms to distinguish aged and new LDOs.

Experiment Design: To conduct ML analyses, we consider three main scenarios. 1) *Supervised classification:* We begin with the most straightforward setting, where the labels for LDOs from one vendor are given to the algorithm. The core idea here is to learn from a subset of LDOs (new and/or aged) and verify to what extent the obtained model can be generalized to other LDOs from the same vendor. 2) *Semi-supervised classification:* This scenario is of great importance to our framework since the model is trained on a subset of LDOs produced by a vendor and then tested on LDOs from another vendor. This relaxes the above assumption so that golden data (i.e., PSRR from known new LDOs) need only be available from a single vendor. 3) *Unsupervised clustering:* In this setting, no label is required, although at least one golden LDO (new or aged), as chosen by a subject matter expert, should be provided. To figure out whether unseen LDOs are new or aged, an unseen LDO and the golden LDO are taken into consideration. It is evident that if these LDOs are of the identical age, solely one cluster would be delivered after the learning process. But if there is solely a slight difference between their ages, the algorithm should be able to cluster them by taking one of the LDOs as the new one. Under this scenario, two possible approaches can be taken. In *Case 1*, we solely measure the PSRR of the component, when it is given to us. Afterward, we give the algorithm the measured values in a pair-wise manner (i.e, golden and suspect), and based on the clusters made by the algorithm, the LDO that is identified as new or aged. On the other hand, in *Case 2* we measure the PSRR of the component and repeat this after a while, e.g., after following a synthetic aging (partially destructive) procedure on suspect LDOs. This case is relevant when an additional aging can be performed.

In all the above scenarios, as mentioned in Section III-B, our data set is collected from LDOs manufactured by four different vendors. From each LDO, PSRR values are measured over a wide frequency range, i.e., from 1 Hz to 2 MHz, every 5 kHz. This range is chosen with respect to an observation made during analysis and experimentation–

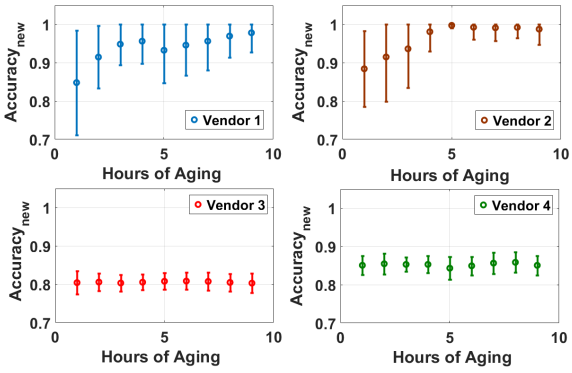


Fig. 6: Supervised classification: detecting accuracy of new chips over hours of aging by applying kNN classifiers to our dataset [dot:mean (μ) ; bar:standard deviation (3σ)].

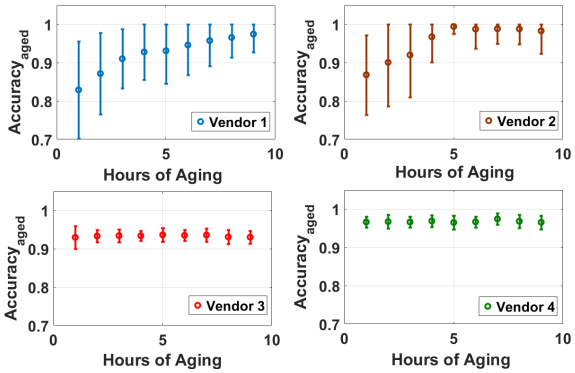


Fig. 7: Supervised classification: detecting accuracy of aged chips over hours of aging by applying kNN classifiers to our dataset [dot:mean (μ) ; bar:standard deviation (3σ)].

the greatest possible separation between the new and aged LDOs (on average) can be observed in this frequency range. Moreover, we use ML algorithms that are publicly available, for instance, embedded in Matlab software package [21]. The point here is that no special know-how in ML algorithm development is required to employ our detection.

Results for Supervised & Semi-supervised Classification: In these experiments, the labels of the LDOs are given to the classification algorithm. In our experiment, k is chosen by fitting the best classifier to our data automatically. For all of the vendors, after running the KNN algorithm provided in the Matlab software package, k is set to 5 by the algorithm as the best possible parameter.

The results for detecting new and aged LDOs, obtained by employing the KNN algorithm, are shown in Figure 6 and Figure 7, respectively. For both groups of new and aged LDOs, to assess the accuracy of the classification, we adopt the 10-fold cross-validation method, and the average and the standard deviation (over the set of LDOs from each vendor) of the accuracy are reported. In other words, the results illustrated in Figure 6 and Figure 7 are obtained after running the algorithm 10 times. In each round of this experiment, the algorithm is trained on 9 folds (i.e., portions) of the dataset and tested on the remaining fold. By doing so, we assure that the unseen folds are chosen uniformly, and the accuracy of the label prediction is computed in a fair manner, i.e., exhibiting less bias [22]. The most important message that these results convey is that a classification model extracted for a given LDO from each vendor can be used to classify the other LDOs from the same vendor, with a sufficient level of accuracy, i.e., up to 97%.

A natural question to ask would be whether, for one vendor to another, such generalization is possible. To answer this, we conduct another set of experiments, whose results are presented in Figure 8 and 10. More specifically, classifiers are extracted from the datasets containing the data collected from a new and an aged (i.e., aged for 1 hour, 4 hours and 9 hours) LDOs from a vendor. These classifiers are further used to categorize unseen LDOs from the other vendors. For a given set of LDOs, new (i.e., the hours of aging equal zero) or aged, the average and standard deviation over the set is computed and plotted in Figures 8 and 10.

As can be seen in these figures, if we take the average over the age of the suspect LDOs, the classifiers extracted from V1 can distinguish whether an LDO manufactured by V2, V3, or V4 is new or aged, with the probability up to 71.31%, 79.72%, 82.29%, respectively. Following the same procedure, if the classifier is extracted from V3 is examined on the LDOs from V1, V2, or V4, the accuracy is up to 92.18%, 93.56%, and 85.88%, respectively. We repeat this experiment on all possible combination of vendors, i.e., extracting a classifier from LDOs made by vendor Vi ($1 \leq i \leq 4$) and testing that on LDOs from Vj ($i \neq j$). The minimum average accuracy computed over the age of the suspect LDOs is 69.27%. The conclusion can be made that implementing this strategy is feasible, if an aged LDO and a new one from the same vendor are available, which holds in practice.

Results for Unsupervised Clustering: Contrary to the above mentioned scenario, no label is given to the clustering algorithm in this experiment. We use the k-means function embedded in the Matlab [21] as well as the VB method included in a publicly available software package [23]. When applying the k-means function, in order to improve the accuracy of clustering, we apply the Silhouette method to validate the consistency within clusters. Furthermore, we take advantage of the replication (i.e., re-sampling) technique to find lower, local minima of the Euclidean distances between examples. Moreover, once the k-means algorithm is run, the centroids it determines are further used to rerun the algorithm to deal with possibly noisy examples. Figure 9- Figure 13 illustrate the results of applying either the k-means or the VB method in two cases.

In Case 1, the PSRR values measured from the golden LDO and the suspected one are fed into the algorithm, whereas in Case 2, both of these LDOs undergo a synthetic aging procedure for 1 hour to 4 hours. The PSRR values corresponding to these hours of artificial aging, along with the initial values measured in Case 1, are fed into the algorithm. The accuracy of the clustering after each stage of artificial aging is reported. Note that on the X-axis, we report the minimum age of the LDOs under test. Moreover, by initial aging equals zero we mean that a new LDO is

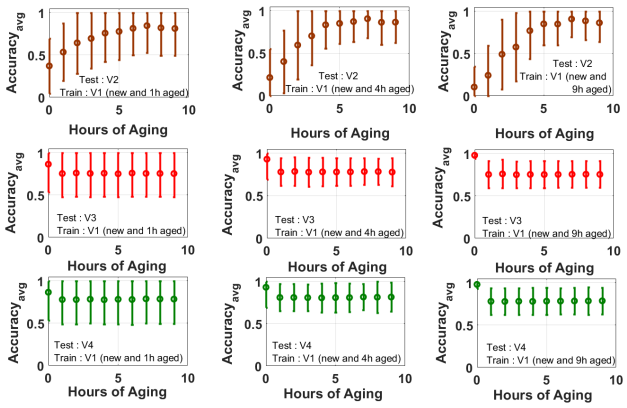


Fig. 8: Semi-supervised Machine Learning: Training with Vendor 1 (V1) and testing on all other vendors [dot:mean (μ) ; bar:standard deviation (3σ)].

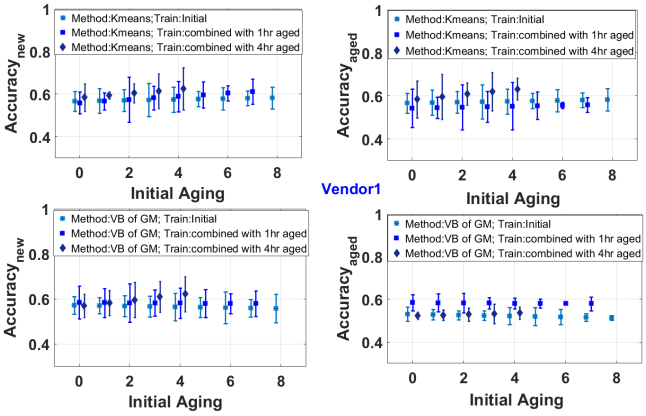


Fig. 9: Unsupervised Classification for V1: Detecting new and aged chips by training with initial data; initial data combined with 1 hr aging; initial data combined with 4 hr aging [dot:mean (μ) ; bar:standard deviation (3σ)].

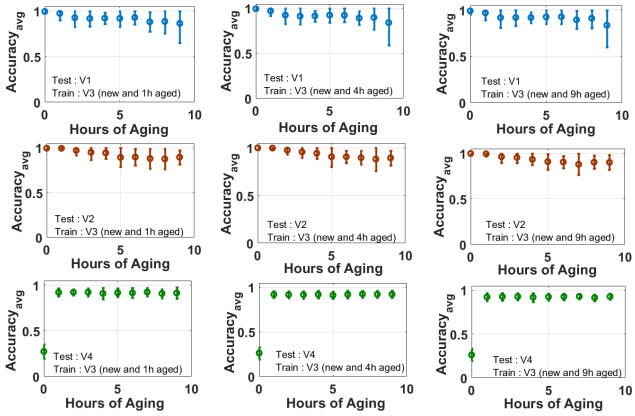


Fig. 10: Semi-supervised Machine Learning: Training with Vendor 3 (V3) and testing on all other vendors [dot:mean (μ) ; bar:standard deviation (3σ)].

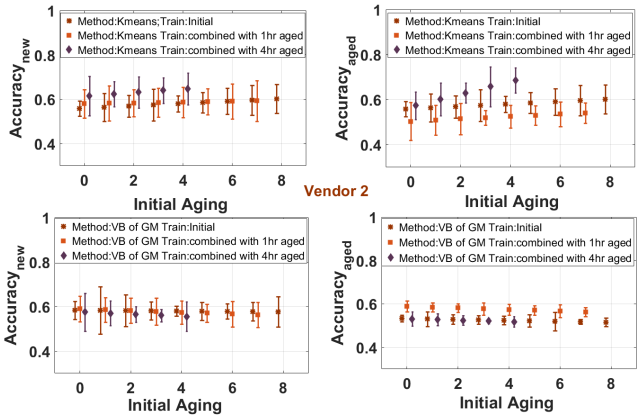


Fig. 11: Unsupervised Classification for V2: Detecting new and aged chips by training with initial data; initial data combined with 1 hr aging; initial data combined with 4 hr aging [dot:mean (μ) ; bar:standard deviation (3σ)].

involved in the experiment. Additionally, we present the accuracy of clustering –over the set of LDOs from each vendor– as either a new or aged. In other words, the curves show how accurately a new component is clustered as new, and similarly for aged ones.

As can be seen, although VB method and the k-means algorithm are from the same family of clustering methods, there is a difference between their results. This can be explained by the fact that the k-means clusters the data in precisely two clusters, which does not hold for VB method that can deliver even one cluster after the learning phase. Moreover, there is a slight difference in the results associated with four vendors in general. More interestingly, we observe that the results for including data acquired after 1 hour or 4 hours of artificial aging do not vary significantly for V3 and V4. Therefore, Figure 12 and Figure 13 present the results obtained for the initial values (Case 1) and Case 2 with 1 hour of artificial aging [dot:mean (μ) ; bar:standard deviation (3σ)]. Besides, the fluctuations in the results achieved for each case shown in Figure 9- Figure 13 reflect the fact that due to the variation of the impact of aging, the accuracy cannot be steadily improved/degraded. In addition, regarding the difference in the technology used by the vendors, in some cases, the unsupervised algorithms can perform more effectively, see Figure 13 as an example. Nevertheless, the average maximum accuracy in Case 1 is 74.21% (averaged over all vendors), whereas it is 86.19% in Case 2. As can be seen in Figure 9- Figure 13, compared with Case 1, the accuracy is improved in Case 2. Last but not least, note that this improvement is achieved at the cost of employing a destructive procedure, i.e., artificial aging.

Summary of Results and Discussion: To recap this section, we highlight the possibilities and constraints of the ML methods applied to distinguish between new and aged LDOs. From the point of view of ML, the most straightforward problem is to classify an unseen LDO by employing a model extracted from the labeled, seen LDOs, so-called supervised classification. By doing so, with a high probability (up to 97%, on average), the unseen LDO can be classified. Nevertheless, this is possible only if a set of new and aged LDOs from each vendor is available to train the model.

This can be tackled (partially), by deriving the information from LDOs made by a vendor, and using it to classify the LDOs from another vendor (semi-supervised approach in our

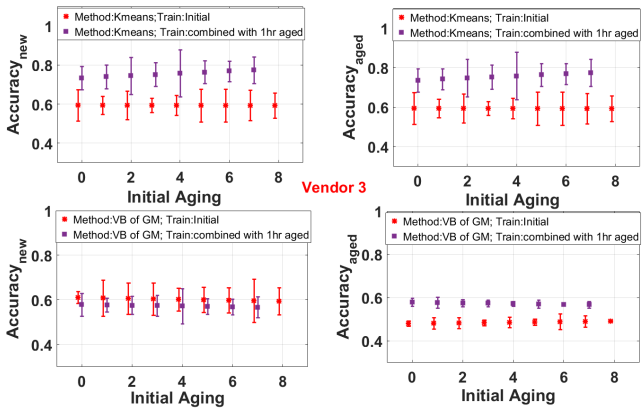


Fig. 12: Unsupervised Classification for V3: Detecting new and aged chips by training with initial data; initial data combined with 1 hr aging [dot:mean (μ) ; bar:standard deviation (3σ)].

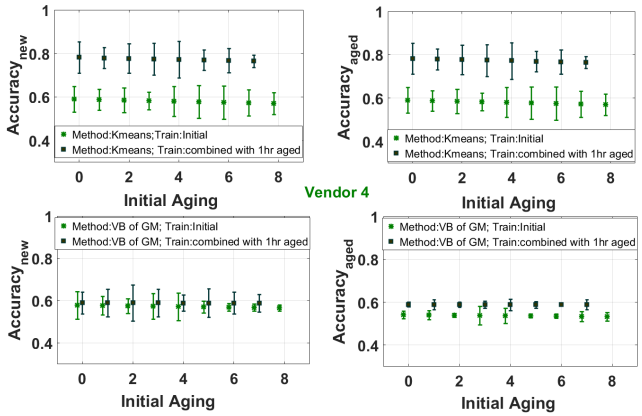


Fig. 13: Unsupervised Classification for V4: Detecting new and aged chips by training with initial data; initial data combined with 1 hr aging [dot:mean (μ) ; bar:standard deviation (3σ)].

paper). Although a slight degradation in the classification accuracy of unseen LDOs can be observed here, this approach is of great significance in practice as it is not required to have new and aged LDOs from each and every vendor.

Finally, if only a golden LDO manufactured by a vendor is available, it is still possible to distinguish between new and aged LDOs in an unsupervised manner, i.e., without any label. In the latter case, the age prediction accuracy is of course less than the supervised and semi-supervised approaches. However, by performing additional artificial aging process, the accuracy can be improved by approximately 12% to achieve the maximum accuracy 86.19%. It is interesting to observe that this acceptably high level of accuracy can be achieved even if solely one golden LDO is accessible.

V. Conclusion and Future Work

In this paper, we presented an inexpensive method to detect recycled AMS ICs that exploits the degradation of the PSRR of COTS LDOs. Silicon data from LDOs of two vendors shows that recycled LDOs can be accurately detected by supervised and semi-supervised ML algorithms. We also provided an analysis explaining the degradation of the LDO PSRR with transistor aging. In future, as industrial designs are proprietary, we plan to extend our analysis by experimenting with simple known LDO designs. In doing so, we will more accurately understand LDO aging mechanisms and perhaps even predict the amount of use in a recycled chip. We also aim to broaden this work to detect recycled SoCs with embedded LDOs.

References

[1] U. Guin, D. Forte, and M. Tehranipoor, "Anti-counterfeit techniques: From design to resign," in *2013 14th Intl. Wkshp. on Microprocessor Test and Verification*, 2013.

[2] S. S. T. channel, "Top 5 counterfeited semiconductors: Analog ics top the list — solid state technology," http://electroiq.com/blog/2012/04/top-5-counterfeited-semiconductors-analog-ics-top-the-list/., 2015.

[3] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. of the IEEE*, 2014.

[4] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ics," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, 2014.

[5] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ics," in *2012 IEEE Intl. Symp. on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2010.

[6] D. Chang, S. Ozev, O. Sinanoglu, and R. Karri, "Approximating the age of rf/analog circuits through re-characterization and statistical estimation," in *2014 Design, Automation Test in Europe Conf. Exhibition (DATE)*.

[7] J. B. Bernstein, "Chapter 3 - failure mechanisms," in *Reliability Prediction from Burn-In Data Fit to Reliability Models*. Academic Press, 2014, pp. 31 – 48.

[8] S. S. Sapatnekar, "What happens when circuits grow old: Aging issues in cmos design," 2013.

[9] K. B. Sutaria, A. Mohanty, R. Wang, R. Huang, and Y. Cao, "Accelerated aging in analog and digital circuits with feedback," *IEEE Trans. on Device and Materials Reliability*, 2015.

[10] P. K. Hanumolu, "Low dropout regulators," in *Custom Integrated Circuits Conf. (CICC), 2015 IEEE*. IEEE, 2015, pp. 1–37.

[11] Y. Huh, Y. Sung, and S. M. Kang, "A study of hot-carrier-induced mismatch drift: a reliability issue for vlsi circuits," *IEEE Journal of Solid-State Circuits*, 1998.

[12] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm cmos," in *2012 Proc. of the ESSCIRC*, 2012.

[13] A. Vassighi and M. Sachdev, *Burn-in as a Reliability Screening Test In:Thermal and Power Management of Integrated Circuits*. Springer, Boston, 2006.

[14] S. Pithadia, S. Lester, and A. Verma. (2017) Ldo psrr measurement simplified. [Online]. Available: http://www.ti.com/lit/an/slaa414a/slaa414a.pdf

[15] A. Graves, "Supervised sequence labelling," in *Supervised sequence labelling with recurrent neural networks*. Heidelberg: Springer, 2012, pp. 5–13.

[16] Z. Ghahramani, "Unsupervised learning," in *Advanced lectures on machine learning*. Heidelberg: Springer, 2004, pp. 72–112.

[17] F. Dabiri and M. Potkonjak, "Hardware aging-based software metering," in *Proc. of the Conf. on Design, Automation and Test in Europe*. European Design and Automation Association, 2009, pp. 460–465.

[18] C. M. Bishop and T. M. Mitchell, *Pattern Recognition and Machine Learning*. Heidelberg: Springer, 2014.

[19] Y. Gal, *Uncertainty in deep learning*. University of Cambridge, 2016.

[20] D. Wettschereck, D. W. Aha, and T. Mohri, "A review and empirical evaluation of feature weighting methods for a class of lazy learning algorithms," *Artificial Intelligence Review*, vol. 11, no. 1-5, pp. 273–314, 1997.

[21] MATLAB, *Version 9.0.0.341360 (R2016a)*. The MathWorks Inc., 2016.

[22] M. Kuhn and K. Johnson, *Applied predictive modeling*. Springer, 2013, vol. 26.

[23] M. Chen, "Matlab code for machine learning algorithms," https://github.com/PRML/PRMLT/ [accessed 20 Nov. 2018], 2018.