Recycled IC Detection Based on Statistical Methods

Ke Huang, *Member, IEEE*, Yu Liu, *Student Member, IEEE*, Nenad Korolija,
John M. Carulli, Jr., *Senior Member, IEEE*, and Yiorgos Makris, *Senior Member, IEEE*

***Abstract*—We introduce two statistical methods for identifying recycled integrated circuits (ICs) through the use of one-class classifiers and degradation curve sensitivity analysis. Both methods rely on statistically learning the parametric behavior of known new devices and using it as a reference point to determine whether a device under authentication has previously been used. The proposed methods are evaluated using actual measurements and simulation data from digital and analog devices, with experimental results confirming their effectiveness in distinguishing between new and aged ICs and their superiority over previously proposed methods.**

***Index Terms*—Degradation curve sensitivity analysis (DCSA), one-class classifier (OCC), parametric burn-in test, recycled integrated circuit (IC) detection.**

I. Introduction

As THE integrated circuit (IC) supply chain grows more complex, with parts being sourced from various suppliers across the globe, ensuring authenticity and trustworthiness of each part becomes very challenging. Indeed, IC counterfeiting has become a profitable activity and a major headache which poses a significant threat to end applications, especially when deployed in sensitive domains such as military, financial, health, etc. Counterfeit ICs have turned up in almost all industrial sectors, including computers, telecommunications, automotive electronics, and even military systems [1], [2]. Evidently, the tools and technologies utilized by untrusted suppliers have become extremely sophisticated and well-financed. In turn, this also calls for more sophisticated methods to detect counterfeit electronic parts entering the market [3], [4].

Counterfeiting is a multifaceted problem, with counterfeit ICs coming in various flavors, such as recycled, remarked, overproduced, cloned, defective, tampered-with, fake, etc. [5]. As shown in a recent report on counterfeit ICs [1], the number of reported incidents of recycled ICs, i.e., those which have been previously used and are sold as new or higher-grade by untrustworthy suppliers, makes for a significant percentage among all other counterfeit types. While these ICs may work initially, the fact that they are used/aged implies that they will have a reduced lifetime and, therefore, may pose reliability risks. Given the prevalence of this type of IC counterfeiting, the focus of this paper is on developing methods for detecting recycled ICs. We note, however, that the proposed methods will also detect other types of counterfeit ICs whose parametric profile does not match the expected profile of new devices.

In this paper, we propose two statistical methods for detecting recycled ICs through the use of one-class classifiers (OCCs) and degradation curve sensitivity analysis (DCSA). Both techniques rely on the fact that, due to silicon aging, the parametric profile of an IC drifts with usage time. Accordingly, the proposed methods seek to statistically learn the expected parametric behavior of new devices and use it as a reference point which can be used to detect recycled ICs. The parametric measurements used in the proposed methods are taken from typical production early failure rate analysis required to release most products and do not require dedicated on-chip sensors; hence, they are applicable to both new and existing products and do not incur additional cost in terms of design, test, and area/power overhead.

The OCC method learns a boundary which encloses the region wherein the parametric signatures of new devices are expected to be in the space of parametric measurements. The trained classifier can then decide whether a device in question is new or aged by examining whether its parametric signature lies within the boundary, which is learned using only new devices [6]. While OCC is quite effective, it can be sensitive to process variation. Indeed, the larger the process variation, the broader the acceptable region in the space of parametric measurements and, by extension, the longer it might take for a used IC to drift outside this boundary. On the other hand, the DCSA technique aims at analyzing the sensitivity of the parametric degradation curve of an IC. Specifically, the underlying conjecture is that, under the same stress conditions, the rate at which an IC ages is a function of its usage time, while the impact of process variations on this degradation curve is negligible for the purpose of recycled IC identification. This, in turn, enables development of a recycled IC identification method which is robust to process variations.

The remainder of this paper is structured as follows. In Section II, we discuss existing methods for combating the problem of recycled ICs and we contrast them to the proposed statistical approaches. In Section III, we provide a brief

Manuscript received July 1, 2014; revised December 30, 2014; accepted February 16, 2015. Date of publication March 6, 2015; date of current version May 20, 2015. This work was supported in part by the National Science Foundation under Grant NSF 1318860, and in part by the Army Research Office under Grant Army Research Office (ARO) W911NF-12-1-0091. This paper was recommended by Associate Editor R. Karri.

K. Huang is with the Department of Electrical and Computer Engineering, San Diego State University, San Diego, CA 92115 USA (e-mail: khuang@mail.sdsu.edu).

Y. Liu and Y. Makris are with the Department of Electrical Engineering, University of Texas at Dallas, Richardson, TX 75080 USA.

N. Korolija is with the School of Electrical Engineering, University of Belgrade, Belgrade 11000, Serbia.

J. M. Carulli, Jr., is with Texas Instruments Inc., Dallas, TX 75243 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCAD.2015.2409267

0278-0070 © 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

description of the basic IC aging mechanisms. In Section IV, we introduce the OCC method, which distinguishes between new and aged ICs based on a trained OCC. In Section V, we discuss the limitations imposed on OCC by process variations. In Section VI, we address these limitations through the introduction of the DCSA method, which employs the performance degradation rate as an indicator of prior IC usage to identify recycled ICs. In Section VII, we evaluate the proposed methods on measurements and simulation data from industrial devices. In Section VIII, we discuss limitations and future work, and in Section IX, we draw conclusions.

II. Combating the Problem of Recycled ICs

Recycled ICs pose a significant threat both for semiconductor design/manufacturing companies and IC consumers. For the former, recycled ICs may increase the cost of mitigating the risk and replacing failed parts, may decrease revenue from legitimate sales, and may cause damage to their business reputation. For the latter, recycled ICs may significantly increase reliability issues and may pose safety concerns. Therefore, several approaches among multiple directions have been proposed to combat this problem [7].

Perhaps the most straightforward method for detecting recycled and other counterfeit types of ICs is visual inspection. In this approach, a device is inspected by examining its external or internal physical appearance through X-ray, scanning acoustic microscopy, or other imaging methods [5] to identify signs of prior utilization. Besides the high cost of the needed equipment and the time for such analysis, counterfeiters are continuously improving their refurbishing techniques, making it harder to detect recycled devices using only visual inspection.

In another direction, security mechanisms can be incorporated in the design of ICs in order to enable tracing of chips as they travel through the supply chain. For example, hardware metering [8] attempts to uniquely tag each chip produced from a certain design through active or passive methods. Similarly, radio-frequency identification (RFID) tracking provides an encrypted number for each produced device through an RFID tag [9], [10]. Physical unclonable functions [11], which are a form of hardware intrinsic security [12] methods, aim to measure the responses of hardware to certain given inputs, which depend on the unique physical properties of the device, since process variations affect each device in a unique and unclonable fashion. Such methods, may not only link each device to a legitimate user but may also prevent the usage of unauthorized copies of an IC by locking its functionality prior to first usage. However, besides the small additional design cost, they require a central track-and-trace system which can be cumbersome to maintain, especially for devices that are permanently enabled after authentication. Finally, these methods cannot be applied to legacy ICs that are already circulating in the supply chain without such provisions, or for very low-cost commodity ICs for which the added effort would result in insufficient profit.

Along a different direction, the inclusion of various on-chip aging sensors has been proposed to facilitate detection of recycled devices [13]–[17]. Such sensors are essentially silicon odometers which reflect the amount of utilization/degradation that an IC has been subjected to, and can expose recycled ICs whose aging sensor readings do not comply with the values expected for unused chips. Once again, such methods incur additional hardware overhead and can only be applied to new ICs that incorporate such sensors.

In contrast, statistical methods such as the ones proposed herein, as well as path-delay fingerprinting, which was first introduced in [18] in the context of hardware Trojan detection and was later adapted for detecting recycled ICs in [19], do not incur additional area or power overhead and can be readily applied to both new and existing ICs. They also do not require any complex track-and-trace system and do not impose strenuous requirements on the infrastructure required at the IC buyer's side, as the equipment used for incoming inspection would typically suffice for taking the parametric measurements needed for applying these methods.

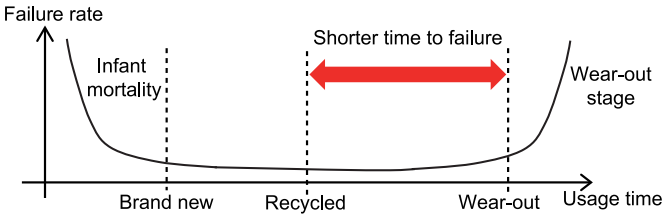


Fig. 1. Bathtub curve illustrating typical device failure characteristics.

III. Aging in ICs

During the lifetime of an IC, its performances continuously degrade due to various aging mechanisms. Fig. 1 illustrates the typical characteristics of device failure, commonly known as the bathtub curve [20], where failure rate is defined as the probability that a device will fail in the time interval between t and $t+\delta t$, given that it has survived until time t [21]. As can be observed in Fig. 1, recycled devices are expected to have shorter time to failure, as compared to brand new devices. As a result, the use of recycled ICs instead of brand new ones reduces the ability of an IC to perform its intended functionality for a prolonged period of time and jeopardizes reliability and robustness of the application wherein it is deployed. In this section, we provide a brief description of two of the most common aging phenomena, namely negative bias temperature instability (NBTI) and hot carrier injection (HCI).

A. NBTI

NBTI occurs in pMOS devices stressed with negative gate voltages at elevated temperatures. In the reaction-diffusion model, the interface traps located near the gate oxide/silicon channel boundary are pacified with a hydrogen species. The bonds of the hydrogen species can be easily broken and allow for diffusion. This movement of charge impacts the V_{th} of the transistor. For nMOS transistors, the equivalent phenomenon is positive bias temperature instability. For pure oxide and nitrided oxides, this has not been a dominant degradation mode, but this may change with Hi-k metal gate.

The degradation of V_{th} exhibits logarithmic dependence on time [22].

Bhardwaj *et al.* [23] proposed a long-term aging model for characterizing NBTI. The model provides an analytical upper bound estimation of NBTI impact over time. As shown in [24], the NBTI-induced threshold shift model can be simplified to

$$\Delta V_{\text{th}}(T, \alpha, t) = be^{-\frac{nE\alpha}{kT}} \left(\frac{\alpha}{1-\alpha}\right)^n t^n \tag{1}$$

where T is the average temperature, α is the average signal duty cycle, t denotes usage time, n is the time exponent, k is the Boltzmann constant, $E_\alpha = 0.49\ eV$, and b is a fitting constant. A primary advantage of using (1) to characterize the aging effect is that, given a reference model precharacterized at T_{ref} and α_{ref}, the aging effect under any arbitrary T and α can be efficiently calculated using parameter scaling.

B. HCI

HCI occurs in MOS devices when a carrier gains sufficient kinetic energy and is, consequently, injected from the conducting channel of the silicon substrate into the gate dielectric. Injected carriers that do not get trapped in the gate oxide become gate current. Over prolonged periods, the presence of such mobile carriers in the oxide can lead to deviations of device parameters, such as threshold voltage V_{th}. In [25], the degradation in V_{th} caused by HCI is expressed as

$$\Delta V_{\text{th}} = C(\exp(L_0/L_{\text{eff}}))(\exp(-V_0/V_d))(t/t_0)^n \tag{2}$$

where C is a constant in mV, L_0/V_0 is a characteristic length/voltage depending on the device, L_{eff} is the effective length, V_d is the drain voltage, t denotes the usage time, and t_0 is a constant.

IV. Recycled IC Identification Based on OCC

In this section, we introduce a method for distinguishing between new and recycled ICs through the use of an OCC.

A. Method Overview

The fundamental concept of this method is to train an OCC to learn the boundary that separates new and aged ICs in a multidimensional space of parametric measurements. The conjecture is that as these parametric measurements drift over time due to aging, the distributions of new and aged ICs will become statistically distinguishable. Fig. 2 illustrates this idea in a 2-D measurement space. The first step of this method involves collection of a set of parametric measurements from a training set of known new devices, which reflect the typical variation of the fabrication process and which can be obtained from a trustworthy provider. Formally, let

$$\vec{m}_i = [m_1, m_2, \ldots, m_d] \tag{3}$$

denote the parametric test measurement vector of the ith device, where d denotes the number of considered parametric measurements. Each measurement is characterized by its specification interval $m_j = (m_{jl}, m_{jh})$, $j = 1, \ldots, d$, that is, the acceptable region for all considered measurements is $A = [m_{1l}, m_{1h}] \times \cdots \times [m_{dl}, m_{dh}]$. Only devices which contain

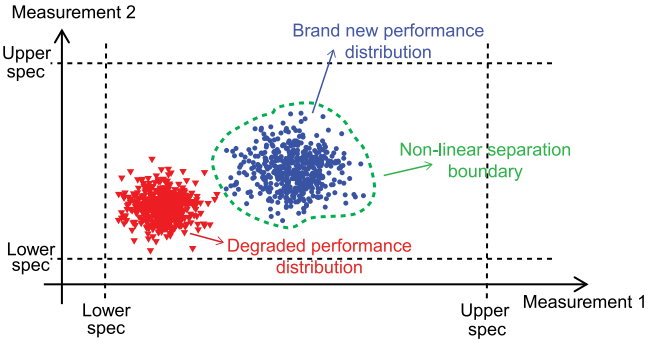


Fig. 2. Recycled identification based on OCC.

no defect, i.e., devices with $\vec{m} \in A$, are used to train the OCC. Let the set

$$M = \{\vec{m}_1, \vec{m}_2, \ldots, \vec{m}_n\} \tag{4}$$

denote the devices used to train the OCC, where n is the number of considered devices under process variations. It should be noted that the value of n is not prohibitive, typically a few tens of devices are sufficient to train the OCC, and such training is a one-time effort.

In this approach, only new devices are used to train the OCC, i.e., no prior information of recycled IC behavior is needed. For this purpose, we use a one-class support vector machine (SVM) [26], in order to allocate a decision function f, where $f(\vec{m}) = 1$ when the device is considered to belong to the group used to train the OCC, i.e., it is considered to be brand new and $f(\vec{m}) = -1$ when the device is considered to be aged. Details of the one-class SVM are given in Section IV-B. Once the OCC is trained, we can readily use it to examine devices from untrusted providers by providing the OCC with the pattern $\vec{m}'$ of each DUA

$$f\left(\vec{m}'\right) = \begin{cases} 1 & \text{DUA is new} \\ -1 & \text{DUA is recycled.} \end{cases} \tag{5}$$

B. One-Class SVM

SVMs were originally designed to solve binary classification problems, in which an SVM is trained with samples from both classes and maps a new sample to one of the two classes in the feature space. In [26], a one-class SVM is presented using kernels to compute inner products in the feature space to support the domain of unsupervised learning. Formally, we consider the training data

$$\vec{m}_1, \vec{m}_2, \ldots, \vec{m}_n \in O \tag{6}$$

where n is the number of new devices under process variations which are used to train the SVM and O is the original input space. Let Φ be a feature map $O \mapsto F$, that is, a map into an inner product feature space F such that a simple separation boundary can be drawn in F to distinguish between training samples and other samples from a foreign distribution. The separation boundary can be considered as a d'-dimensional sphere with radius R and center point c, as shown on the right side of Fig. 3, where d' is the dimension of the transformed

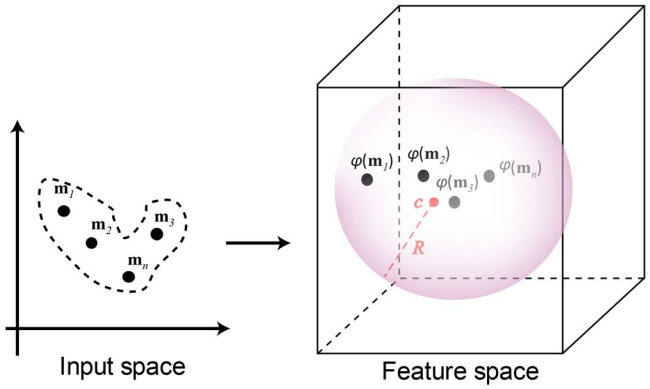


Fig. 3. One-class SVM.

feature space F. Then, one-class SVM training is equivalent to solving the following optimization problem:

$$\begin{aligned} \underset{R\in\Re,\xi\in\Re^n,c\in F}{\text{minimize}} \quad & R^2+\frac{1}{\nu n}\sum_i \xi_i \\ \text{subject to} \quad & |\Phi(\vec{m}_i)-c|^2 \le R^2+\xi_i, \\ & \xi_i \ge 0 \text{ for } i\in\{1,\ldots,n\} \end{aligned} \tag{7}$$

where the slack variables ξ_i are penalization parameters in the objective function, ν is a characterization parameter which can be tuned during the training of the SVM, and c can be considered as the center point of the sphere [26]. The goal of the training is to develop an algorithm that returns a function f which takes the value $+1$ in a small region capturing most of the training data points and -1 elsewhere.

For a new point $\vec{m}'$, the value $f(\vec{m}')$ is determined by evaluating whether this point is inside or outside the separation sphere in the feature space

$$f(\vec{m}') = \text{sgn}\Big(R^2 - \big|\Phi(\vec{m}')-c\big|^2\Big). \tag{8}$$

Here, we use the convention that sgn(z) = 1 for $z \ge 0$ and -1, otherwise. Via the freedom to use different types of kernel functions, this space transformation corresponds to a variety of nonlinear estimators in the input space [26]. In other words, by using a kernel transformation, we are able to separate highly nonlinear data in the input space regardless of their distribution form. Intuitively, the optimization algorithm in (7) consists of finding the smallest sphere that all the training data live in.

Since it is difficult to solve the optimization problem in (7), one can also solve this problem by introducing Lagrange multipliers α, which leads to the following dual optimization problem:

$$\begin{aligned} \text{minimize} \quad & \sum_{ij}\alpha_i\alpha_j\Phi^T(\vec{m}_i)\Phi(\vec{m}_j) - \sum_i \alpha_i\Phi^T(\vec{m}_i)\Phi(\vec{m}_i) \\ \text{subject to} \quad & 0\le\alpha_i\le\frac{1}{\nu n}, \sum_i\alpha_i = 1 \end{aligned} \tag{9}$$

and the solution

$$c = \sum_i \alpha_i\Phi(\vec{m}_i) \tag{10}$$

can be used to compute the decision function defined in (8). By substituting (8) and (10), we obtain

$$f(\vec{m}') = \text{sgn}\left(R^2 - \left(\Phi^T(\vec{m}')\Phi(\vec{m}') - 2\sum_i \alpha_i\Phi^T(\vec{m}_i)\Phi(\vec{m}') + \sum_{ij}\alpha_i\alpha_j\Phi^T(\vec{m}_i)\Phi(\vec{m}_j)\right)\right). \tag{11}$$

Crucially, (9) and (11) are formed as a function of inner product $\Phi^T(\vec{m}_i)\cdot\Phi(\vec{m}_j)$, permitting us to leverage the kernel trick and express (9) and (11) as a function of kernel function $k(\vec{m}_i,\vec{m}_j)$

$$k(\vec{m}_i,\vec{m}_j) = \big(\Phi^T(\vec{m}_i)\cdot\Phi(\vec{m}_j)\big). \tag{12}$$

In other words, the optimization algorithm for training and the decision function for a new point $\vec{m}'$ in the feature space can be expressed as a function of points in the input space using the kernel function. Among a variety of kernels, the most prevalent one is the squared exponential, also known as the radial basis function kernel. In this paper, we employ the radial basis function kernel

$$k(\vec{m}_i,\vec{m}_j) = \exp\Big(-\gamma|\vec{m}_i-\vec{m}_j|^2\Big) \tag{13}$$

where γ is some characteristic length-scale of the radial basis function kernel. Employing this kernel is equivalent to training a classifier with an infinite-dimensional feature space.

C. Group Classification

When evaluating a set of ICs obtained from an untrusted supplier, the accuracy of this evaluation may potentially improve by generalizing the individual IC decision function in (5) to a group decision function $f(M')$, where M' denotes a set of devices under authentication

$$M' = \{\vec{m}'_1,\vec{m}'_2,\ldots,\vec{m}'_{n'}\} \tag{14}$$

where n' is the number of devices under authentication. In this paper, we derive the group decision function $f(M')$ by employing the multivariate Hotelling's [27] two-sample t^2 test. In particular, let $\vec{\mu}_1$ denote the d-dimensional mean vector of the trusted set M and $\vec{\mu}_2$ denote the d-dimensional mean vector of the set M'. The Hotelling's two-sample t^2 statistic is defined

$$t^2 = \frac{nn'}{n+n'}(\vec{\mu}_1-\vec{\mu}_2)'\mathbf{W}^{-1}(\vec{\mu}_1-\vec{\mu}_2) \tag{15}$$

where n and n' denotes the number of samples in M and M', respectively, and $\mathbf{W}$ is the pooled covariance matrix between the two sets M and M' [27]. The corresponding two-side p value can be computed as

$$p = 2\times\left(1-\int_{-\infty}^{t}\frac{\Gamma\left(\frac{\nu+1}{2}\right)}{\Gamma\left(\frac{\nu}{2}\right)}\frac{1}{\sqrt{\nu\pi}}\left(1+\frac{t^2}{\nu}\right)^{-\frac{\nu+1}{2}}dx\right) \tag{16}$$

where ν is the degree of freedom defined as $\nu = n+n'-2$. If we set a 10% significance level, then the decision function can be specified as

$$f(M') = \begin{cases} 1 & \text{if } p\ge 0.1 \\ -1 & \text{otherwise.} \end{cases} \tag{17}$$

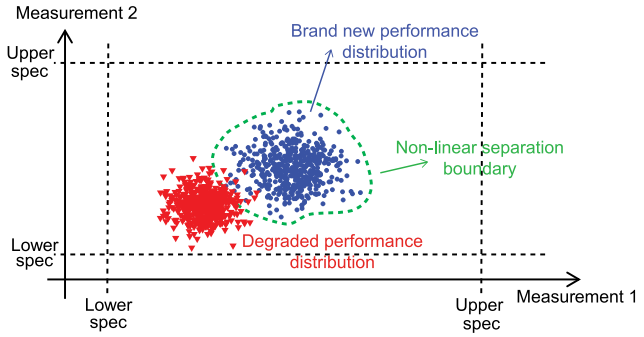


Fig. 4. Overlap of new and aged populations due to large process variations.

The group identification approach allows us to determine whether a set of ICs under evaluation is new or recycled by examining the significance of the difference between the mean vector of the group under evaluation and the original training set of new devices.

V. OCC Limitations Due to Process Variations

While the OCC approach allows us to distinguish between new and aged populations, its effectiveness may be adversely affected by process variations. As shown in Fig. 4, new and aged device populations may overlap due to large process variations. The aged devices shown in Fig. 4 may be identified as a whole group, however, aged devices in the overlapping area between the new and the aged populations may not be correctly identified individually. The larger the expected process variations, the higher the chance of misclassification. To address this limitation, in this section, we take a closer look at the impact of process variation on performance degradation, seeking an aging characteristic that is less sensitive to process variations than the parametric signature used by OCC.

A. Impact of Process Variation on Performance Degradation

As discussed in [24], the aging-induced performance degradation depends not only on circuit run-time conditions but also on manufacturing-determined process parameters, such as the initial threshold voltage V_{th} and the oxide thickness t_{ox}. Due to these process variations, the aging process and its impact on a circuit parametric signature become a random process. Lu *et al.* [24] proposed a stochastic collocation method to model circuit performances under uncertainty. If we consider a set of process parameters as a random variable vector with normal distribution

$$\vec{\xi} = [V_{\text{th}}, t_{\text{ox}}, \dots] \tag{18}$$

then the IC parametric measurement value m at time t can be expressed as follows:

$$m\left(\vec{\xi}, T, \alpha, t\right) = m_0\left(\vec{\xi}\right) + \Delta m\left(\vec{\xi}, \vec{s}, t\right) \tag{19}$$

where $m_0(\vec{\xi})$ is the initial parametric measurement value after chip fabrication, $\vec{s}$ is a vector denoting the stress condition, $\vec{s} = [T, \alpha, V_{dd}, \dots]$, and $\Delta m(\vec{\xi}, \vec{s}, t)$ represents the time-dependent performance aging effect.

Process variation and aging have both drawn significant attention. Most of the past work treats them as two independent issues and addresses the impact of each of them on IC reliability and performance separately. Nevertheless, it was recently reported that IC reliability may be jointly affected by both effects [23]. As reported in [28], the difference in V_{th} degradation between two devices can reach around 5% due to process variations. However, as will be shown later, for the purpose of recycled IC identification, the impact of process variations on parametric aging degradation is negligible. Indeed, Wang *et al.* [28] concluded that statistical analysis of both aging effects and process variations on 65-nm silicon data reveals that the performance degradation rate and its standard deviation are independent of the type and amount of process variations. In order to predict the mean and the variance of circuit aging, only the characteristics of transistor degradation and circuit performance sensitivity to aged parameters are required. The degradation of circuit speed and parametric measurements, such as *Iddq*, shows a power law dependence on the stress time.

Based on the above observation, we can further simplify (19) as follows:

$$m\left(\vec{\xi}, \vec{s}, t\right) = m_0\left(\vec{\xi}\right) + \Delta m(\vec{s}, t). \tag{20}$$

As can be observed in (20), under the same stress conditions for a given design, performance degradation depends only on the usage time t. If we assume the power law dependence of IC parametric measurements on stress time and identical stress conditions, we can further write (20) as

$$m\left(\vec{\xi}, \vec{s_{\text{ref}}}, t\right) = m_0\left(\vec{\xi}\right) + c_r t^n \tag{21}$$

where c_r is a constant depending on the stress conditions (i.e., T_{ref}, α_{ref}, V_{dd}, and n). By taking the derivative of (21), we obtain

$$\frac{\delta m\left(\vec{\xi}, \vec{s_{\text{ref}}}, t\right)}{\delta t} = c_r \cdot n \cdot t^{n-1}. \tag{22}$$

As can be observed in (22), under the same stress conditions, the derivative of IC performance degradation at time t is independent of its initial value at $m_0(\vec{\xi})$ and is a monotonic function of t. This observation is the cornerstone of a recycled IC identification method which is less sensitive to process variations, as discussed in the following section.

VI. Recycled IC Identification Based on DCSA

In this section, we introduce a method for distinguishing between new and recycled ICs through DCSA.

A. Method Overview

The fundamental concept of this method is that the parametric performance degradation of a new chip is distinguishably different than that of an aged chip and largely independent of process variations. Fig. 5 shows a high-level description of the DCSA approach for identifying recycled ICs.

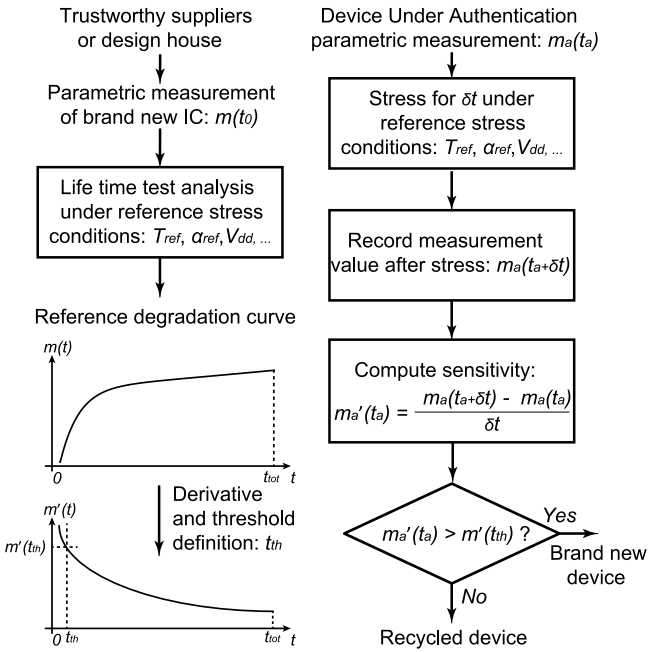


Fig. 5. Recycled IC identification based on DCSA.

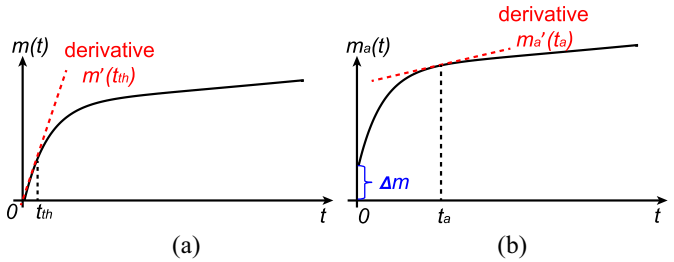


Fig. 6. Robustness of proposed DCSA approach to process variation. (a) and (b) Performance degradation curve of two devices under the same stress conditions.

We first select the best available parametric measurement[1] for recycled IC detection through DCSA. Measurement selection is discussed in detail in Section VI-B. Then, lifetime test analysis is performed for a known new device, under reference stress conditions such as T_{ref}, α_{ref}, V_{dd}, etc., in order to obtain the reference degradation curve $m(t)$, as shown on the left side of Fig. 5. This lifetime test analysis can be done through high-temperature operating life analysis, or device parametric shift evaluation. This step is performed by a trustworthy supplier or design house. Note that this analysis is carried out under consistent stress conditions, which will also be employed when we seek to identify recycled devices. The reference stress conditions can be made publicly accessible by the trusted foundry or the chip designer. Here, we discuss the case where a parametric measurement value increases as a result of aging. We can easily convert the case where a parametric measurement value decreases as t increases by setting $m(t) = -m(t)$.

Based on the reference degradation curve $m(t)$, we can obtain the derivative $m'(t)$ as shown in Fig. 5. We propose to approximate $m'(t)$ by computing the sensitivity of $m(t)$ with respect to t

$$m'(t) \approx \frac{m(t+\delta t) - m(t)}{\delta t} \tag{23}$$

where δt denotes a small time interval under which the device is stressed after t.

Once $m'(t)$ is derived, we can easily set a threshold value t_{th} for identifying recycled devices. The value of t_{th} is user-defined: if a strict detection is required, we should choose t_{th} close to 0; if a more lenient detection is acceptable, we can choose a larger t_{th}. It should be noted that obtaining $m'(t)$ is a one-time effort and the total required stress time t_{tot} is small and not prohibitive. Typically, $t_{\text{tot}} > t_{\text{th}}$ is sufficient for recycled IC identification purposes, which makes our method very time efficient and cost-effective.

The recycled IC identification phase is shown on the right side of Fig. 5. We evaluate unknown DUAs by taking the same parametric measurement $m_a(t_a)$, where t_a denotes the actual usage time of the DUA and m_a denotes its measurement value. The sensitivity of the DUA $m'_a(t_a)$ is computed as in (23). In particular, we stress the DUA for δt under the reference stress conditions T_{ref}, α_{ref}, V_{dd}, etc., provided by a trustworthy supplier or design house. Note that δt is chosen to be small enough to ensure negligible performance degradation by the identification process. Theoretically, an infinitely small δt value is sufficient to identify recycled devices. As will be shown in Section VII, δt as small as less than one day of normal usage is sufficient to detect most recycled devices.

We then employ a decision function $f(m_a)$ such that $f(m_a) = 1$ denotes that the DUA is considered new, and $f(m_a) = -1$ denotes that it is recycled

$$f(m_a) = \begin{cases} 1 & \text{if } m'_a(t_a) \geq m'(t_{\text{th}}) \\ -1 & \text{otherwise.} \end{cases} \tag{24}$$

As will be shown later, the proposed approach is able to decide whether each individual DUA is new or aged without requiring any information about the distribution of process variations that may impact the device population. Thus, we avoid complications related to the classification-based approach of [6] and [19], such as the overlap between the new and aged IC populations in the space of parametric measurements. The robustness of the DCSA method to process variations is illustrated in Fig. 6, where Δm denotes the difference of measurement values of two devices affected differently by process variations at t_0. It can be observed that under the same stress conditions, the form of the degradation curve remains very similar for both devices, implying the same derivative function.

B. Selection of Best Available Measurement for DCSA

In order to choose a measurement which provides the most efficient recycled IC identification capability, we propose a simple selection algorithm, which is summarized in Algorithm 1. In particular, for the ith considered measurement, we compute the sensitivity ratio r_i between $m'_i(0)$ and $m'_i(t_{\text{th}})$

[1]Extension to multiple such measurements is possible yet was not deemed necessary given the effectiveness of the single-measurement method in our case studies.

Algorithm 1 Selection of Optimal Measurement for DCSA Identification

```
procedure SELECTION
/*d is the number of considered measurements*/
/*m_opt is the selected optimal measurement for DCSA identification*/
r_max ← 0
    for i = 1 to d do
        md_0 ← m'_i(0)
        md_th ← m'_i(t_th)
        r_i ← md_0/md_th
        if r_i > r_max then
            r_max ← r_i
            m_opt ← m_i
end procedure
```

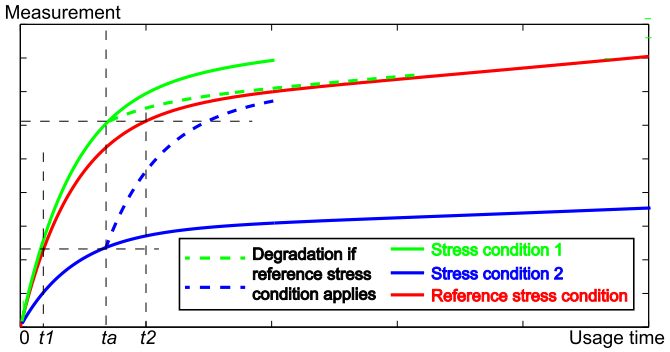


Fig. 7. Performance degradation under different stress conditions.

for $i = 1, \ldots, d$. Then, we select the measurement that has the highest r_i value. By selecting the measurement that has the highest discrepancy in degradation rate between brand new and aged devices, we maximize the expected detection capability in the DCSA approach.

C. Performance Degradation in Different Stress Conditions

As can be observed from (22) and empirical results in the following section, under the same reference stress condition T_{ref}, α_{ref}, V_{dd}, etc., the derivative curve of the DUA $m'_a(t)$ remains the same as $m'(t)$, regardless of the impact of process variations introduced in manufacturing. However, circuit workload may vary over time in the field of operation, e.g., V_{dd}, power gating, or temperature can vary as a function of time, resulting in different stress conditions than the reference ones. Fig. 7 illustrates an example of DUAs under different operation conditions. The red curve shows the reference degradation curve obtained by applying the reference stress conditions. The blue and green curves show the degradation profile of a less and more stressed device, respectively. As can be observed, the performance degradation differs under different stress conditions.

In order to facilitate characterization of the aging effect under varying stress conditions, Lu *et al.* [24] introduced the notion of equivalent aging time t_{eqv}, which denotes the stress time applied under the reference stress conditions to obtain the same performance degradation as the DUA at t_a

$$\Delta m\left(\vec{s_{\text{ref}}}, t_{\text{eqv}}\right) = \Delta m(\vec{s_a}, t_a) \tag{25}$$

where $\vec{s_a}$ is a vector denoting the stress condition under which the DUA operates until t_a. As we can observe in Fig. 7, for a less stressed device at time t_a (shown by the blue curve), the equivalent aging time is t_1, which signifies less aging degradation as compared to the equivalent aging time t_2 for a more stressed device (shown by the green curve). If the reference stress conditions are applied at time t_a for both devices, they will exhibit different degradation behavior, i.e., the less stressed device will exhibit faster degradation than the more stressed device, as shown by the dotted blue and dotted green curves, respectively. Consequently, the DUA represented by the blue curve will be identified as having less degradation due to previous usage than that represented by the green curve.

The equivalent aging time allows us to identify the performance degradation of the DUA without making any assumptions regarding the conditions under which it is operated. Indeed, only the reference stress conditions and the threshold value t_{th} are needed for identifying recycled ICs.

VII. Case Studies

In this section, we demonstrate the proposed methods using actual measurements from a digital signal processor (DSP) and a microprocessor, as well as simulation data from a fully differential folded cascode operational amplifier. In each of the following three case studies, we first describe the dataset that was used and then we evaluate the effectiveness of OCC and DCSA and compare to prior art.

A. Case Study 1

The first case study is an industrial DSP device. The population consists of 35 devices randomly chosen from different lots. Each device has two parametric measurements Fmax and Vmin, thus $\vec{m} = [m_1, m_2]$. These 35 devices are subjected to burn-in test for failure analysis,[2] during which high voltage and temperature are applied to accelerate the aging mechanisms. During this burn-in test process, the same measurements $\vec{m}$ are obtained at seven different time points, $t = t_0, t_1, \ldots, t_6$.[3] These time points are approximately log time-based since aging degradations exhibit logarithmic dependence on time. The measurements taken at time point $t = t_0$ correspond to brand new devices, while those at $t \neq t_0$ correspond to aged devices which, for the purpose of this study, will be considered as recycled ICs.

1) Results for OCC: Fig. 8 shows the projection of the devices at $t = t_0, t_1, t_6$ onto the 2-D normalized measurement space, shown by squares, solid dots, and plus signs, respectively. Note that for demonstration purpose, we plot $-F$max in the figure as Fmax decreases as a function of usage time. As may be observed, an obvious drift of these measurements occurs as t increases. Despite the overlap between

[2]This is different than the production burn-in test used to weed out infant mortality, as it seeks to stress the device all the way to its failure.

[3]Exact hours are not shown here due to industrial confidentiality.

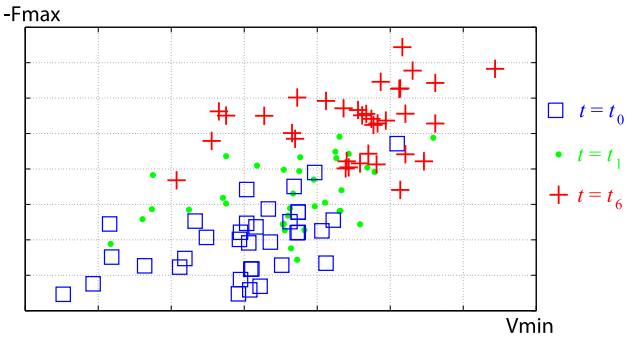


Fig. 8. Projection of devices at $t = t_0, t_1, t_6$.

TABLE I
CLASSIFICATION RATE FOR CASE STUDY 1 AT DIFFERENT TIME POINTS

Group\ Validation size	t_0	t_1	t_2	t_3	t_4	t_5	t_6
17	100%	100%	100%	100%	100%	100%	100%
8	100%	100%	100%	100%	100%	100%	100%
1	100%	30%	60%	70%	80%	80%	100%

TABLE II
CLASSIFICATION RATE FOR CASE STUDY 1 FOR MIXED GROUPS

Group\ Validation size	$\{t_1, \ldots, t_6\}$
100	100%
50	100%
20	100%
10	100%

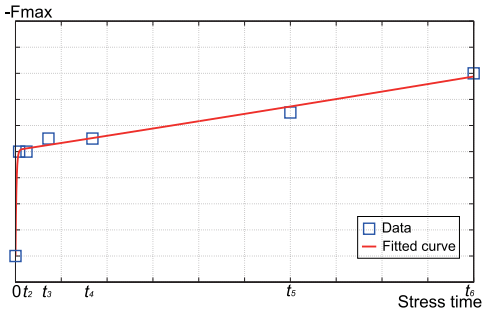


Fig. 9. Fitted exponential curve using available time point samples for the first case study.

groups of measurements from different t_i, the mode/median are statistically different and follow the aging degradation physics.

The following datasets are used to train and validate the OCC.

1) The set S_t contains 18 devices randomly chosen among the 35 devices at $t = t_0$. S_t is used to train the classifier.
2) The set S_v contains seven subsets $\{S_{v0}, S_{v1}, \ldots, S_{v6}\}$, corresponding to the $35 - 18 = 17$ other devices at $t = t_0, \ldots, t_6$, respectively. Thus, S_v contains $17 \times 7 = 119$ devices and is used to validate the classifier.

In this experiment, we used the *LIBSVM* [29] as the classification tool to implement the OCC. The following procedure is used to train the OCC and evaluate its effectiveness.

Step 1: We randomly choose s samples from each of the validation sets S_{vi}, $i = 0, \ldots, 6$ and use the procedure described in Section IV to classify the selected samples. Let I_2 denote the classification accuracy indicator, where $I_2 = 1$ when the classification is correct and $I_2 = 0$ when the classification is erroneous.

Step 2: We repeat step 1 r times in order to consider random effects (i.e., cross-validation). The classification accuracy indicator function for the jth time is denoted by I_2^j.

Step 3: The final classification rate for each validation subset S_{vi}, $i = 0, \ldots, 6$ is computed as

$$C_{vi} = \frac{1}{r} \sum_{k=1}^{r} I_2^k. \tag{26}$$

We first consider the case of evaluating one device of the validation set at a time, i.e., $s = 1$. The last line of Table I shows the correct classification rate computed by (26) using $r = 10$ for all subsets of $S_v : \{S_{v0}, \ldots, S_{v6}\}$. As may be observed, the OCC exhibits the lowest correct classification rate for ICs at time t_1, since these ICs have only been slightly aged and their parametric footprints highly overlap with those of ICs at time t_0. We then repeat the same steps by setting $s = 8$ and $s = 17$ and using the group classification decision function in (17) to collectively decide on all s ICs. The second and third lines in Table I show the classification results for groups of size $s = 17$ and $s = 8$, respectively, with $r = 10$. As may be observed from Table I, the correct classification rate improves as burn-in time increases and as the size of the group increases. This can be explained by observing Fig. 8, where the performance drift is more pronounced as the burn-in test time increases, thereby making the validation set more distinguishable from brand new devices at $t = t_0$.

When evaluating a group of devices under authentication, it is not always guaranteed that all devices in the group have experienced the same aging. Thus, we also repeated the experiment outlined above using mixed recycled devices in the validation set, i.e., we randomly choose devices from the entire set $\{S_{v1}, \ldots, S_{v6}\}$ to create groups of devices under authentication. Nevertheless, as shown in Table II, all groups of mixed aged devices were identified correctly by the proposed OCC approach.

2) Results for DCSA: We first choose the optimal measurement for DCSA using the algorithm outlined in Algorithm 1 by selecting $\delta t = t_1/1000$. Since we have a limited number of time points in our dataset to perform sensitivity analysis (seven in total), we fitted an exponential curve for $m(t)$ using the MATLAB exponential fit function. The selected measurement in this case is Fmax. Note that we use $-F$max in the DCSA analysis as Fmax decreases as a function of usage time. The fitted curve of $-F$max for one device is depicted in Fig. 9, where the data is shown by blue squares and the fitted curve is shown in red.

Fig. 10 shows the degradation curves from time point t_0 to t_6 for $-F$max for all 35 devices. The measurement value points between t_i and t_{i+1} are simply connected by a straight line.

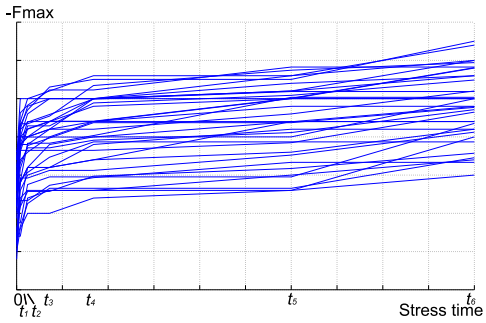


Fig. 10. Degradation curve of $-F\text{max}$ for all 35 devices.

TABLE III
CORRECT IDENTIFICATION RATE USING DEVICES AT $t = t_0$ AS BRAND NEW FOR CASE STUDY 1

Type of device	DCSA	OCC	[19]
Brand new	100%	94.1%	100%
Recycled	100%	82.4%	60.8%

From Fig. 10, we observe that: 1) despite the process variations introduced by manufacturing at t_0, all the devices exhibit similar degradation behavior; 2) devices exhibit much higher degradation rate at time points near t_0; and 3) the degradation rate decreases significantly after time t_4.

We randomly chose one of the 35 devices in the dataset to construct the reference derivative curve $m'(t)$. We also selected the threshold value at $t_{\text{th}} = t_1/2$, i.e., all devices at time points $t > t_1/2$ are considered as used ICs. We computed the sensitivity at t_{th}, as in (23), by selecting $\delta t = t_1/1000$. Note that the value of δt is extremely small, which is equivalent to less than one-minute stressing time under reference stress conditions, or less than one day's usage time under nominal operating conditions. Thus, the aging degradation induced during authentication analysis is negligible.

The following dataset is used to validate the recycled IC detection approach. The set S_v contains $35 - 1 = 34$ devices (excluding the device used to generate the reference curve) and each device has measurements obtained at seven time points $t = t_0, \ldots, t_6$ during the burn-in test. Thus, we have in total $7 \times 34 = 238$ instances of devices to be evaluated, of which 34 are brand new and 204 are recycled. We predict recycled devices as depicted in (24).

The correct identification rates for all brand new and recycled devices are summarized in the second column of Table III. As may be observed, all the devices, whether brand new or aged, are correctly evaluated, resulting in a 100% correct classification rate. To illustrate the significant improvement in terms of correct classification rate using DCSA, the second and third columns of Table III show the equivalent rate using the OCC approach and the convex hull analysis introduced in [19]. Evidently, DCSA is significantly more accurate as compared to other classification methods.

Since devices are often aged through a burn-in analysis before being sent to customers, we have also repeated the same experiment by discarding devices from $t = t_0$ in our dataset. Instead, we use label devices from $t = t_1$ as brand new and devices from $t = t_2, \ldots, t_6$ as recycled. Thus, we have 34 brand new and 170 recycled devices to be evaluated. We set the new threshold value at $t_{\text{th}} = t_1 + (t_2 - t_1)/2$. Table IV summarizes the correct classification rate as before. As may be observed, the correct identification rate has significantly deteriorated using the OCC and convex hull [19] approaches, since the overlap between the brand new and recycled devices has further increased when using devices from $t = t_1$ as brand new. However, the DCSA method is still able to maintain a 100% correct classification rate.

TABLE IV
CORRECT IDENTIFICATION RATE USING DEVICES AT $t = t_1$ AS BRAND NEW FOR CASE STUDY 1

Type of device	DCSA	OCC	[19]
Brand new	100%	76.4%	100%
Recycled	100%	16.5%	10.6%

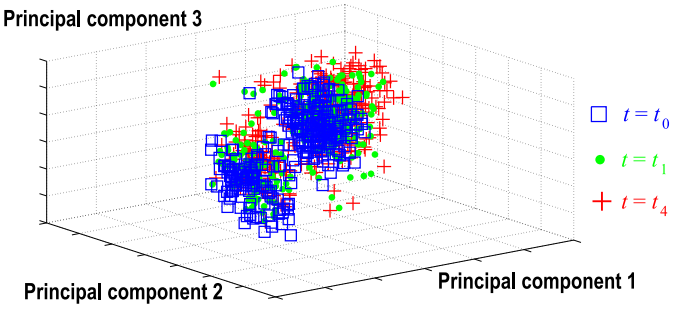


Fig. 11. Projection of devices at $t = t_0, t_1, t_4$.

B. Case Study 2

The second case study is an industrial microprocessor design with 313 devices randomly chosen from different lots. For each device, the dataset includes 49 parametric measurements such as $V\text{min}$, $F\text{max}$, $Iddq$, etc., obtained for various modules of the microprocessor. Thus, $\vec{m} = [m_1, \ldots, m_{49}]$. As before, the same measurements are taken at five different time points $t = t_0, \ldots, t_4$ during the burn-in failure analysis.

1) Results for OCC: Fig. 11 shows the projection of devices at $t = t_0, t_1, t_4$, onto the space of the first three principal components obtained through principal component analysis (PCA), shown by the squares, solid circles, and plus signs, respectively. As before, performance degradation caused by aging mechanisms is accelerated during the burn-in test and it can be readily observed in Fig. 11.

Similarly to case study 1, we use half of the available devices (157 devices) to train the OCC and the other half (156 devices) for validation purpose. Table V shows the classification results for different group sizes. Once again, increasing the validation group size improves the correct classification rate. As can be seen in Table V, we achieve 100% correct classification rate for a group size of as small as ten ICs.

We also repeated the experiment using group of devices with different aging times in the validation set, as in the first case study. As shown in Table VI, all groups of devices with different aging times can be identified correctly by the proposed approach.

TABLE V
CLASSIFICATION RATE FOR CASE STUDY 2 AT DIFFERENT TIME POINTS

Group\ Validation size	t_0	t_1	t_2	t_3	t_4
156	100%	100%	100%	100%	100%
80	100%	100%	100%	100%	100%
20	100%	100%	100%	100%	100%
10	100%	100%	100%	100%	100%
1	100%	60%	80%	100%	100%

TABLE VI
CLASSIFICATION RATE FOR CASE STUDY 2 FOR MIXED GROUPS

Group\ Validation size	$\{t_1, \ldots, t_4\}$
500	100%
100	100%
50	100%
20	100%
10	100%

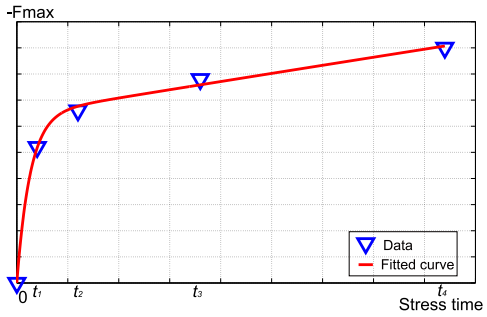


Fig. 12. Fitted exponential curve using available time point samples for the second case study.

2) Results for DCSA: As before, we first choose the optimal measurement for DCSA using the procedure outlined in Algorithm 1 by selecting $\delta t = t_1/1000$. The selected measurement is Fmax. The fitted curve of $-F$max for one device is shown in Fig. 12, where the data is shown by blue triangles and the fitted curve is shown in red.

Fig. 13 plots the degradation curves of $-F$max from time point t_0 to t_4 for all 313 devices in our dataset. Again, the degradation curves remain very consistent across different devices. The same $t_{\text{th}} = t_1/2$ and $\delta t = t_1/1000$ are chosen to minimize degradation introduced by the identification process.

We chose one device to construct the reference stress curve and the remaining 312 devices to validate the method. The correct classification rates for brand new and recycled devices are summarized in the second column of Table VII. As may be observed, DCSA achieves 100% correct classification for both brand new and recycled devices. The second and third columns of Table VII also show the correct classification rate using OCC and the approach proposed in [19]. Once again, DCSA achieves significantly better classification rate as compared to the other two methods.

Table VIII shows the result obtained by discarding the devices at $t = t_0$ and using devices at $t = t_1$ as brand new.

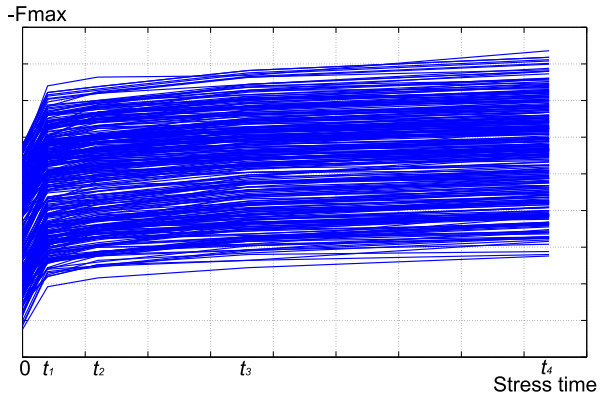


Fig. 13. Degradation curve of $-F$max for all 313 devices.

TABLE VII
CORRECT IDENTIFICATION RATE USING DEVICES AT $t = t_0$ AS BRAND NEW FOR CASE STUDY 2

Type of device	DCSA	OCC	[19]
Brand new	100%	89.7%	92.3%
Recycled	100%	19.2%	16.5%

TABLE VIII
CORRECT IDENTIFICATION RATE USING DEVICES AT $t = t_1$ AS BRAND NEW FOR CASE STUDY 2

Type of device	DCSA	OCC	[19]
Brand new	100%	58.3%	89.7%
Recycled	100%	13%	5.8%

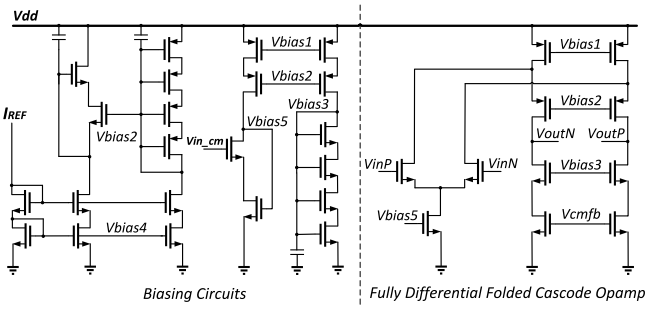


Fig. 14. Schematic of the fully differential folded cascode amplifier.

The classification accuracy has significantly deteriorated for the OCC and convex hull [19] methods as before, however, the correct classification rate of DCSA remains at 100%.

C. Case Study 3

The third case study is a fully differential folded cascode amplifier designed in 45-nm technology from Texas Instruments Inc. The schematic of the amplifier is shown in Fig. 14. Four parametric measurements are considered for recycled IC detection purposes: 1) gain; 2) phase margin; 3) bandwidth; and 4) *Iddq*, thus $\vec{m} = [m_1, \ldots, m_4]$. We performed 100 Monte Carlo (MC) simulations by varying the process parameters specified in the design kit. Then, for each of the 100 instances obtained in MC simulation, we simulated its aging degradation profile by taking into account

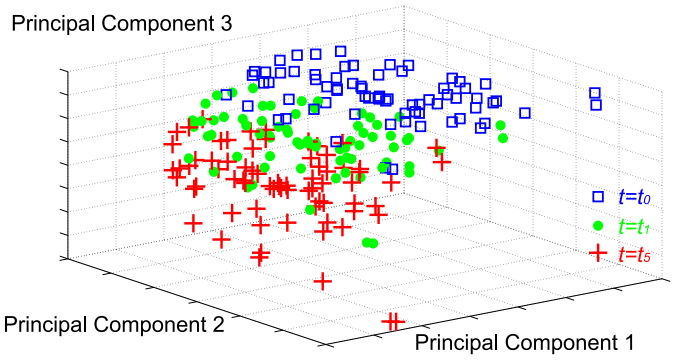


Fig. 15. Projection of devices at $t = t_0, t_1, t_5$.

TABLE IX
CLASSIFICATION RATE FOR CASE STUDY 3 AT DIFFERENT TIME POINTS

Group\ Validation size	t_0	t_1	t_2	t_3	t_4	t_5
50	100%	100%	100%	100%	100%	100%
20	100%	100%	100%	100%	100%	100%
10	100%	100%	100%	100%	100%	100%
1	100%	90%	100%	100%	100%	100%

both NBTI and HCI effects using the *RelXpert* simulator. The same measurements $\vec{m}$ are taken at six different time points $t = t_0, t_1, \ldots, t_5$ during aging simulation: {0, 1 month, 6 months, 1 year, 5 years, 10 years}. The measurements taken at time point $t = t_0$ correspond to brand new devices, while those at $t \neq t_0$ correspond to aged devices which, for the purpose of this study, will be considered as recycled ICs.

1) Results for OCC: Fig. 15 shows the projection of the devices at $t = t_0, t_1, t_5$ shown by squares, solid dots, and plus signs, respectively, onto the space of the first three principal components after having performed PCA on the dataset. As may be observed from Fig. 15, an obvious measurement drift occurs as t increases. While some overlap exists for populations from different times t_i, the mode/median are statistically different and follow the aging degradation physics.

Similarly to the previous case studies, we use half of the available devices (50 devices) to train the OCC and the other half (50 devices) for validation purposes. Table IX shows the correct classification results for different group sizes, based on which similar observations can be made as in the previous case studies: increasing the validation group size improves the classification rate, and a 100% correct classification rate can be achieved for a group size of as small as ten devices. The improved result can be also explained by observing Fig. 15, where the performance drift is more pronounced as we increase the usage time in aging simulation, thereby increasing the likelihood that a group of recycled devices will be distinguishable from devices at $t = t_0$.

We also repeated the experiment using groups of devices with different aging times in the validation set as before. As shown in Table X, all groups of devices with different aging times can be identified correctly by the proposed approach.

TABLE X
CLASSIFICATION RATE FOR CASE STUDY 3 FOR MIXED GROUPS

Group\ Validation size	$\{t_1, \ldots, t_5\}$
200	100%
100	100%
50	100%
20	100%
10	100%

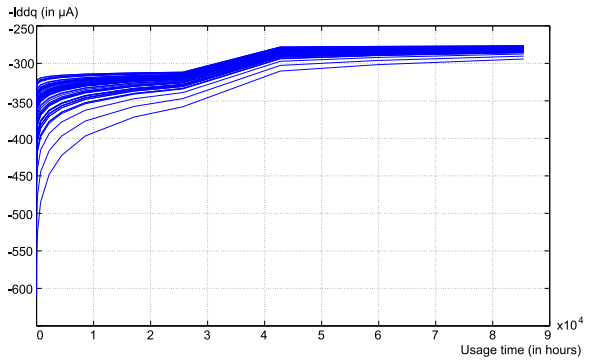


Fig. 16. Degradation curve of *Iddq* for all 100 devices.

TABLE XI
CORRECT IDENTIFICATION RATE USING DEVICES AT $t = t_0$ AS BRAND NEW FOR CASE STUDY 3

Type of device	DCSA	OCC	[19]
Brand new	100%	100%	100%
Recycled	100%	92%	88%

2) Results for DCSA: The selected optimal measurement for DCSA method in this case study is the *Iddq* measurement m_4. Since *Iddq* decreases as a function of usage time, we use $-$*Iddq* in the DCSA analysis. Fig. 16 plots the degradation curves from t_0 to t_5 for $-$*Iddq* for the 100 devices obtained through MC and aging simulations. The measurement value points between t_i and t_{i+1} are simply connected by a straight line. From Fig. 16, we observe that: 1) despite the process variations introduced by MC at t_0, all the devices exhibit similar degradation behavior; 2) devices exhibit much higher degradation rate at time points near t_0; and 3) the range of process variations decreases as t increases. However, the impact of process variations on the degradation curve is negligible for recycled IC identification purposes.

We select $t_{\text{th}} = 1$ month and $\delta t = 1$ day for this case study, and we use one device to construct the reference stress curve and the remaining 99 devices to validate the method as before. The correct classification rates for brand new and recycled devices are summarized in the second column of Table XI. Again, DCSA achieves 100% correct classification for both brand new and recycled devices. The second and third columns of Table XI also show the correct classification rate using OCC and the approach proposed in [19]. As before, DCSA achieves significantly better classification rate as compared to the other two methods.

TABLE XII
CORRECT IDENTIFICATION RATE USING DEVICES AT $t = t_1$ AS BRAND NEW FOR CASE STUDY 3

Type of device	DCSA	OCC	[19]
Brand new	100%	98%	98%
Recycled	100%	12%	8%

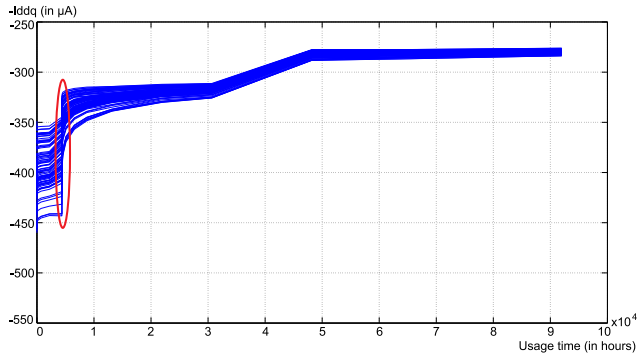


Fig. 17. Degradation curve of *Iddq* for all 100 devices under different stress conditions.

Table XII summarizes the result obtained by discarding the devices at $t = t_0$ and using devices at $t = t_1$ as brand new. The classification accuracy has significantly deteriorated for the OCC and convex hull [19] methods as before, however, the correct classification rate of DCSA remains at 100%, confirming its superiority over the other two methods.

3) Results for DCSA Under Different Stress Conditions: The use of an aging simulation model enables an additional dimension in this third case study, namely application of DCSA to devices which have been used under different stress conditions. In this case, the notion of equivalent aging time, which was introduced in Section VI-C, comes in handy.

To this end, we performed aging simulations for the same 100 devices under two different stress conditions, namely $\vec{s_1}$ and $\vec{s_2}$. In $\vec{s_1}$, a lenient stress condition is applied by setting the temperature at -20 °C while in $\vec{s_2}$, the nominal stress condition is applied. For each of the considered devices, $\vec{s_1}$ is applied between 0 and 7 months and $\vec{s_2}$ is applied from 7 months to 10 years and 6 months. Fig. 17 shows the degradation curve for the parameter *Iddq* under the stress conditions specified above. It can be observed that the *Iddq* values remain almost constant for a short time in the beginning of the stress period. This flat region corresponds to the period 0–7 months, in which lenient stress condition $\vec{s_1}$ is applied. When the nominal stress condition $\vec{s_2}$ is applied at the seventh month, a sharp degradation can be observed as highlighted by the red circle in Fig. 17. These large derivative values at the seventh month illustrate that the equivalent degradation caused by stress condition $\vec{s_1}$ is very low. Indeed, using the proposed DCSA method, all the devices aged under $\vec{s_1}$ from t_0 to t_2, which correspond to 0, 1, and 6 months of usage time, respectively, are classified as new this time. Other devices aged under $\vec{s_2}$ from t_3 to t_5, which correspond to 1, 5, and 10 years of usage time, respectively, are classified as recycled. This example illustrates the notion of equivalent aging time and the effectiveness of the DCSA method in identifying used devices under different stress conditions.

VIII. LIMITATIONS AND FUTURE WORK

A possible limitation of the OCC method is that in order to allocate a trusted boundary in the space of parametric measurements, we first need to obtain a small set of known-new devices from a trusted supplier and subject them to controlled accelerated aging. Employing an aging simulation model and advanced statistical tail modeling techniques, as was done in [30] in the context of hardware Trojan detection may relax this requirement, but access to such information may also be challenging. Additionally, effectiveness of the OCC approach may also be adversely affected by process variations over the lifetime of production of a particular design, which could make new and aged populations start to overlap in the space of parametric measurements. This problem can be alleviated by employing the proposed DCSA approach, which is independent of the starting point of a device, as affected by process variations. On the other hand, the DCSA method requires a more complicated analysis of the aging profile of the device under reference stress conditions. While this is a one-time effort, it is still costly and would best be performed by the design house or a trusted supplier.

In addition to investigating methods for alleviating these limitations and simplifying the process of obtaining the reference thresholds for the OCC and DCSA methods, our future plans include fabrication and stress testing of a complex circuit for which we will have access to both simulation models and actual silicon. Applying the proposed methods on both and correlating the results could provide definitive confirmation of their effectiveness in identifying recycled ICs and facilitate simpler combined approaches that could lower the cost.

IX. CONCLUSIONS

In an effort to address the increasingly troubling problem of recycled ICs, we presented two statistical methods for distinguishing between new and aged devices based on parametric measurements. The first method relies on a trained OCC which decides whether a parametric device fingerprint belongs to the class of new or to the class of aged ICs. The second method employs DCSA and relies on the rate of parametric degradation to decide whether a device is new or not. The conjecture supported by this paper is that parametric profiles obtained from known new devices can serve as a robust indicator of a device's prior utilization and can be used to detect recycled ICs. Effectiveness of the proposed methods has been demonstrated using both simulation and actual silicon data on both digital and analog designs, corroborating their excellent ability in distinguishing between new and aged ICs.

ACKNOWLEDGMENT

The authors would like to thank Texas Instruments Inc., for providing the data on which this research was performed.

REFERENCES

[1] *Defense Industrial Base Assessment: Counterfeit Electronics*, U.S. Dept. Commerce, Washington, DC, USA, Jan. 2010.

[2] *Inquiry Into Counterfeit Electronic Parts in the Department of Defence Supply Chain*, U.S. Senate Committee Armed Services, Washington, DC, USA, May 2012.

[3] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectr.*, vol. 43, no. 5, pp. 37–46, May 2006.

[4] N. Kae-Nune and S. Pesseguier, "Qualification and testing process to implement anti-counterfeiting technologies into IC packages," in *Proc. Design Autom. Test Europe Conf. (DATE)*, Grenoble, France, 2013, pp. 1131–1136.

[5] U. Guin, M. Tehranipoor, D. DiMase, and M. Megrdichian, "Counterfeit IC detection and challenges ahead," *ACM SIGDA Newslett.*, vol. 43, no. 3, 2013, pp. 1–5.

[6] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Proc. IEEE Int. Symp. Defect Fault Tolerance Very Large-Scale Integr. Nanotechnol. Syst. (DFT)*, Austin, TX, USA, 2012, pp. 7–12.

[7] U. Guin *et al.*, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[8] F. Koushanfar and Q. Gang, "Hardware metering," in *Proc. Design Autom. Conf. (DAC)*, Las Vegas, NV, USA, 2001, pp. 490–493.

[9] K. Chatterjee and D. Das, "Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Trans. Compon. Packag. Technol.*, vol. 30, no. 3, pp. 547–549, Sep. 2007.

[10] A. Arbit, Y. Livne, Y. Oren, and A. Wool, "Implementing public-key cryptography on passive RFID tags is practical," *Int. J. Inf. Secur.*, vol. 14, no. 1, pp. 1–15, 2014.

[11] R. Pappu, "Physical one-way functions," Ph.D. dissertation, Dept. Media Arts Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.

[12] V. van der Leest and P. Tuyls, "Anti-counterfeiting with hardware intrinsic security," in *Proc. Design Autom. Test Europe Conf. (DATE)*, Grenoble, France, 2013, pp. 1137–1142.

[13] T. H. Kim, R. Persaud, and C. H. Kim, "Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits," *IEEE J. Solid-State Circuits*, vol. 43, no. 4, pp. 874–880, Apr. 2008.

[14] K. K. Kim, W. Wang, and K. Choi, "On-chip aging sensor circuits for reliable nanometer MOSFET digital circuits," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 10, pp. 798–802, Oct. 2010.

[15] J. Keane, X. Wang, D. Persaud, and C. H. Kim, "An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB," *IEEE J. Solid-State Circuits*, vol. 45, no. 4, pp. 817–829, Apr. 2010.

[16] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2012, pp. 703–708.

[17] D. Chang *et al.*, "Reliability enhancement using in-field monitoring and recovery for RF circuits," in *Proc. IEEE Very Large-Scale Integr. Test Symp. (VTS)*, Napa, CA, USA, 2014, pp. 1–6.

[18] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardw.-Orient. Secur. Trust*, Anaheim, CA, USA, 2008, pp. 51–57.

[19] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance Very Large-Scale Integr. Nanotechnol. Syst. (DFT)*, Austin, TX, USA, 2012, pp. 13–18.

[20] D. Pantic, "Benefits of integrated-circuit burn-in to obtain high reliability parts," *IEEE Trans. Rel.*, vol. 35, no. 1, pp. 3–6, Apr. 1986.

[21] J. M. Carulli and T. J. Anderson, "Test connections—Tying application to process," in *Proc. IEEE Int. Test Conf.*, Austin, TX, USA, 2005, pp. 1–8.

[22] A. T. Krishnan *et al.*, "Material dependence of hydrogen diffusion: Implications for NBTI degradation," in *Proc. IEEE IEDM Tech. Dig.*, Washington, DC, USA, 2005, pp. 691–694.

[23] S. Bhardwaj, W. Wang, R. Vattikonda, Y. Cao, and S. Vrudhula, "Predictive modeling of the NBTI effect for reliable design," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, San Jose, CA, USA, 2006, pp. 189–192.

[24] Y. Lu *et al.*, "Statistical reliability analysis under process variation and aging effects," in *Proc. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2009, pp. 514–519.

[25] K. L. Chen, S. A. Saller, I. A. Groves, and D. B. Scott, "Reliability effects on MOS transistors due to hot-carrier injection," *IEEE J. Solid-State Circuits*, vol. 20, no. 1, pp. 306–313, Feb. 1985.

[26] B. Schölkopf, J. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *J. Neural Comput.*, vol. 13, no. 7, pp. 1443–1471, 2001.

[27] H. Hotelling, "The generalization of student's ratio," *Ann. Math. Statist.*, vol. 2, no. 3, pp. 360–378, 1931.

[28] W. Wang, V. Reddy, V. Balakrishnan, S. Krishnan, and Y. Cao, "Statistical prediction of circuit aging under process variations," in *Solid State Circuits Technologies*. Rijeka, Croatia: InTech, 2010, pp. 101–122.

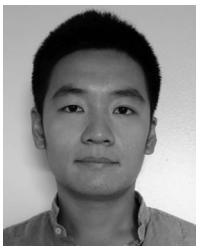
[29] C. C. Chang and C. J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, 2011.

[30] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan detection through golden chip-free statistical side-channel fingerprinting," in *Proc. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2014, pp. 1–6.

Ke Huang (S'10–M'12) received the M.S. degree from Joseph Fourier University (Grenoble I University), Grenoble, France, and the Ph.D. degree from the University of Grenoble, Grenoble, in 2008 and 2011, respectively, both in electrical engineering.

He was a Post-Doctoral Research Associate with the University of Texas at Dallas, Richardson, TX, USA, for two years. He joined San Diego State University, San Diego, CA, USA, as an Assistant Professor in 2014. His current research interests include applications of data mining and machine learning in hardware security, reliability, and analog/RF IC testing.

Dr. Huang was a recipient of the Ph.D. Fellowship by the French Ministry of National Education from 2008 to 2011, the Second Place Winner Award at the IEEE Computer Society Test Technology Technical Council E. J. McCluskey Doctoral Thesis Competition in 2013, and the Best Paper Award from the 2013 Design Automation and Test in Europe Conference.



Yu Liu (S'12) received the B.S. degree in electronic science and technology and the M.S. degree in microelectronics and solid-state electronics from Xidian University, Xi'an, China, in 2008 and 2011, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Erik Jonsson School of Engineering and Computer Science, University of Texas at Dallas, Richardson, TX, USA.

His current research interests include trustworthy wireless cryptographic ICs, analog/mixed signal IC design, very large-scale integration design, and machine learning.

Nenad Korolija received the M.Sc. degree in electrical engineering and computer science from the School of Electrical Engineering, University of Belgrade, Belgrade, Serbia, in 2009.

He was with the School of Electrical Engineering, University of Belgrade. In 2007, he was a Teaching Assistant for the courses such as software project management and business communication—practical course. In 2008, he researched on HiPEAC Project with the University of Siena, Siena, Italy. In 2013, he was an intern with Google Inc., Mountain View, CA, USA, for three months. He researched on various FP7 Projects such as HiPEAC, ARTreat, and ProSense with topics including computer architectures, data mining, and wireless sensor networks. His current research interests include developing software for high performance computer architectures, developing special purpose architectures, programming, and developing algorithms.

Korolija was a recipient of the 3-Month Scholarship in Stuttgart, Germany, in 2004, where he researched on message passing interface project.

John M. Carulli, Jr. (SM'12) received the M.S.E.E. degree from the University of Vermont, Burlington, VT, USA, in 1990.

He is a Distinguished Technical Staff Member with the Analog Engineering Operations Organization, Texas Instruments Inc., Dallas, TX, USA, where he was the Manager of the product reliability and design reliability activities for new technology development in the External Development and Manufacturing Division. His current research interests include outlier analysis, product reliability modeling, performance modeling, and security.

Yiorgos Makris (SM'08) received the Diploma degree in computer engineering from the University of Patras, Patras, Greece, in 1995, and the M.S. and Ph.D. degrees in computer engineering from the University of California, San Diego, La Jolla, CA, USA, in 1998 and 2001, respectively.

From 2001 until 2011 he was on the faculty of Yale University, New Haven, CT, USA, and then he joined the University of Texas at Dallas, Richardson, TX, USA, where he is currently a Professor of Electrical Engineering, leading the Trusted and Reliable Architectures Research Laboratory. His current research interests include applications of machine learning and statistical analysis in the development of trusted and reliable integrated circuits and systems, with particular emphasis in the analog/RF domain. His research activities are supported by the National Science Foundation, ARO, Semiconductor Research Corporation, Defense Advanced Research Projects Agency, Boeing, IBM, LSI, Intel, and Texas Instruments Inc.

Prof. Makris was a recipient of the 2006 Sheffield Distinguished Teaching Award and the Best Paper Award from the 2013 Design Automation and Test in Europe Conference. He served as the Program Chair of the IEEE Very Large-Scale Integration Test Symposium in 2013 and 2014 and Test Technology Educational Program from 2010 to 2012. He also served as a Guest Editor for the IEEE TRANSACTIONS ON COMPUTERS and the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS and a Topic Coordinator and/or a Program Committee Member for several IEEE and ACM conferences.