Estimating Operational Age of an Integrated Circuit

Prattay Chowdhury, *Student Member, IEEE*, Ujjwal Guin, *Member, IEEE*, Adit D. Singh, *Fellow, IEEE*, and Vishwani D. Agrawal, *Life Fellow, IEEE*

***Abstract*—Used ICs being recycled as new replacement parts in maintaining older electronic systems is a serious reliability concern. This paper presents a novel approach to estimate the operational age of chips by measuring I_{DDQ}, the quiescent current from power supply. I_{DDQ} is the total leakage current in steady state, with all supply to ground conducting paths turned off. It decreases as the circuit ages mainly due to the increase in the magnitude of the PMOS transistor threshold voltage, caused by negative bias temperature instability (NBTI). We exploit the fact that the impact of NBTI on individual transistor varies depending on the amount of operational stress caused by the duration of its on state. We use a normalized difference, ΔI, computed from current measurements at two input test patterns as a self referencing circuit age indicator. The first pattern is chosen such that its I_{DDQ} is controlled by a large number of minimally stressed PMOS transistors; for the other it is controlled by approximately equal number of highly stressed PMOS transistors. Clearly, the difference between these two I_{DDQ} values would increase with the circuit age. This approach requires no hardware addition or modification to the design and hence, can be applied to legacy ICs. Simulation results show that we can reliably detect recycled ICs that have been used for as little as six months.**

***Index Terms*—Operational Age, Recycled IC, I_{DDQ}, NBTI, Aging, Process Variation.**

I. Introduction

The performance of a semiconductor device degrades with use, giving the device a finite lifetime. Consequently, its failure probability increases as the remaining useful life (RUL) diminishes. Characteristics such as RUL and reliability can be expressed in terms of the *operational age*, defined as the cumulative operating time since manufacture.

The aging aspect of electronic parts manifests in several ways. Parts from discontinued production lines are sometimes needed to maintain critical infrastructure and defense systems whose operational life may exceed the initially planned deployment period. When the chips are no longer being produced, they are often sourced from less reliable third party suppliers. Recycled ICs can thus enter the supply chain. A report from Information Handling Services Incorporated places the potential annual risk from the global supply chain at $169 billion and increasing each year [2]. Reportedly, recycled ICs constitute almost 80% of all the reported counterfeiting incidents [3]. The reliability of a system becomes questionable because these chips may exhibit poor performance and reduced remaining useful lifetime (RUL) [4]. These chips may also contain defects and other anomalies caused by the relatively crude recycling processes employed, typically consisting of removal of the ICs from scrapped printed circuit boards (PCBs) under extremely high temperatures, followed by sanding, repackaging and remarking [3], [5]. These processes can also create latent defects, such as gate oxide damage, that pass the initial acceptance testing by original equipment manufacturers (OEM) and then cause early life failures in the field [3].

Researchers have proposed several detection and avoidance techniques to identify recycled ICs and prevent them from entering the supply chain [3], [6]–[23]. However, we still need simpler but efficient techniques to isolate especially the ICs already circulating in the market. In this paper, we propose a novel method of detecting aged ICs by measuring the quiescent leakage current of the circuit, referred as I_{DDQ}. Our method requires no hardware modification to the existing design and can be applied to a wide variety of chips, including older legacy designs circulating in the market. The proposed method is simple as it requires the current measurement for just two vectors. Simulation results show that we can accurately detect ICs that have been used for a period as little as six months. Assuming that typical chips are used for several years, the proposed approach is well suited for detecting recycled ICs. Although the current measurement can be performed by laboratory instruments, in a high volume setting commercial IC testers can be readily used. This paper reports results from recent research, whose excerpts have just been announced at a conference [1].

Our proposal exploits the change in transistor threshold voltages caused by Negative Bias Temperature Instability (NBTI) [24], [25] from accumulated operational stress during the chip lifetime in the powered up state. Unused chips are expected to display only minimal threshold voltage changes since manufacture, while the PMOS transistors in used parts will display varying increases in threshold voltage depending on the level of operational stress experienced. We use the externally measured I_{DDQ} for the entire chip to track aggregate shifts in threshold voltages for large number of transistors since it is impractical to directly measure device parameters inside an IC. I_{DDQ} decreases with age because the transistor threshold voltages increase resulting in reduced leakage from off transistors. The key challenge is to find a stable reference current against which this age-driven change in I_{DDQ} can be reliably evaluated. Our innovative solution to this problem is based on the observation that not all transistors within an IC experience the same amount of aging stress during operation. This is because of differing signal probabilities at circuit nodes. PMOS transistors that are mostly off during operation (because their gate nodes are at logic 1 most of the time) are lightly stressed, when compared to those that are mostly on. Therefore, if we select two input vectors, one that mostly

This paper was presented at the 32^{nd} International Conference on VLSI Design, 2019 [1].

The authors are with the Department of Electrical and Computer Engineering, Auburn University, AL, USA (e-mail: {prattay, ujjwal.guin, singhad, agrawvd}@auburn.edu.)

draws I_{DDQ} from minimally stressed PMOS transistors, and the other that draws I_{DDQ} from an equal number of heavily stressed PMOS transistors, then the difference between the two I_{DDQ} values should reflect the age of the chip. Note that the random threshold variations in individual transistors from manufacturing will largely average out in the two large equal sized cohorts. A significantly larger difference, compared to that possible from statistical variations and other sources of noise, would indicate a used chip.

Similar to I_{DDQ}, gate delay is also influenced by the age-related effects of NBTI. However, finding a reference to evaluate increases in path delay from aging is more challenging. On the other hand, our choice of I_{DDQ} allows us to eliminate the effect of systematic process variation by subtracting the aggregate current of the lightly aged transistor group from that of the heavily aged group, because both groups are identically affected by the systematic process variation.

This paper is organized as follows. Prior work on aging and detecting recycled ICs is reviewed in Section II. Section III introduces the modeling of I_{DDQ} for device aging. Section IV discusses the proposed I_{DDQ} solution to the problems of assessing the device age and detecting recycled ICs. Simulation results are given in Section V and Section VI concludes the paper.

II. Prior Work

The present work on IC age determination is motivated by the need to identify recycled counterfeit ICs. Extensive prior research has been performed in this area and methods proposed for identifying such devices are categorized below.

A. Conventional Test Methods

There are existing standards (AS6171, AS5553, CCAP-101 and IDEA-STD-1010), which recommend physical and electrical tests for counterfeit detection [6]–[9]. The physical test methods include – External Visual Inspection (EVI), Radiological Inspection (2D/3D), Acoustic Microscopy (AM), Bond Pull and Die Attach, and Material Composition Analysis [6]. Electrical tests include Curve Trace, DC Test, AC/Switching Tests, Full Functional Tests, Burn-in Tests and Temperature Cycling [6]. These tests primarily focus on detecting defects and anomalies of recycled parts. However, excessive test time and cost, lack of automation, and low confidence in detection ability, has limited their use. Guin et al. [26] proposed a method to select an optimum set of tests considering test cost and time budget. They also developed an online tool for determining counterfeit defect coverage (CDC) [27], which has been acquired by SAE International. The revision II of standard AS6171 is currently in progress to incorporate more test methods to increase the confidence of detection for recycled parts.

B. Statistical Data Analysis Approaches

Zhang et al. [10] proposed a fingerprint based on path-delays in a chip to detect recycled ICs. Paths that contain fast aging gates (e.g., NOR or XOR gates) are selected for this purpose. It is required to use a large number of paths to create a delay-based fingerprint of new (unused) chips. The fingerprint of Chip Under Test (CUT) is compared with the new chip fingerprint. Huang et al. [11] proposed a one-class Support Vector Machines (SVM) classifier to identify recycled chips. The classifier is trained using parametric measurements of new chips and later used for decisions regarding the authenticity of the chip. Zheng et al. [12] used dynamic current (I_{DDT}) signature in their proposal. Dogan et al. [13] proposed a method that uses one-class SVM classifier to detect recycled FPGAs. Zheng et al. [14] proposed a characterization method based on extraction of scan path delay signatures of a chip. Guo et al. [15] exploited an embedded SRAM in their approach. They isolated the unstable and most age sensitive cells and used them to devise a recycled IC detection method.

These solutions require a large inventory of unused circuits from different production runs to gather statistically meaningful electrical data as reference. Most often such data are not available due to the typically limited access to parts when sourcing chips to service obsolete systems. Variations in electrical parameters over large production volumes, manufactured at different times or in multiple fabrication lines also limit the effectiveness of the approach.

C. Design-for-Anti-Counterfeit (DfAC) Measures

Several Design-for-Anti-Counterfeit (DfAC) measures have been proposed as alternatives for the conventional test methods [16]–[22]. On-chip ring oscillators (RO) were proposed by several researchers to detect recycled ICs. Kim et al. [16] proposed a RO-based silicon odometer. They gave two different designs to monitor the effect of negative bias temperature instability (NBTI) and time-dependent dielectric breakdown (TDDB). Improved versions of the odometer [28] can observe NBTI and hot career injection (HCI) effects. Hofmann et al. [29] proposed a product level age monitoring system that separates the dominating NBTI stress and the switching-activity dependent hot carrier stress (HCS). Saneyoshi et al. [30] proposed a hybrid on-chip age monitor containing RO and delay line. The aim of that design was to improve reliability of the system and test rather than focus on maximizing the age degradation.

Zhang et al. [17], [18] proposed a light-Weight on-chip sensor using ring oscillators (ROs) to detect recycled ICs. The design contained a reference RO and a stressed RO. A similar concept is used by others [16], [28]. The reference RO ages at a slow rate while the stressed RO ages at an accelerated rate. To achieve maximum aging in the stressed RO, Guin et al. [19], [20] gave an improved design. He et al. [21] proposed a lightweight on-chip design to exploit electromigration-induced aging effect of the interconnect wire. The design is compact compared to other existing designs but depends on the length and quality of the interconnect wire. Recently, Guin et al. [22] have proposed an approach that uses RO and a digital signature to protect the RO frequency from tampering such that a recycled IC is accurately identified. Unfortunately, all these solutions require on-chip hardware and hence cannot be applied to existing ICs already circulating in the market.

D. Image Processing Approaches

Recycled IC detection through visual inspection is widely used in various standards [6], [9]. The accuracy of detection is heavily dependants on the subject matter experts (SMEs) and the quality of the counterfeiting. For improving detection accuracy, Shahbazmohamadi et al. [31] use advanced image processing techniques to determine any improper texture in a counterfeit part. Other researchers proposed machine learning approaches applied to images of parts [32]–[35]. The training in machine learning approaches requires new chips, which may not be easily available for obsolete or legacy parts. Besides, re-training of the machine learning model becomes necessary as counterfeiters improve their techniques.

III. Modeling of I_{DDQ} for Device Aging

I_{DDQ} is the current drawn from the power supply in the quiescent state by a CMOS circuit. when all gate inputs are in steady state. The basic approach in I_{DDQ} testing is to apply an input test vector and measure the steady state current. Based on this measured value decisions are made. I_{DDQ} testing provides simplicity, low-cost and reduced defect level [36]–[38].

A. Effect of Gate Sizing and Supply Voltage on I_{DDQ}

In a defect free CMOS device, there is no low-resistance power supply-to-ground path once steady state is reached. The I_{DDQ} drawn from the power supply is made up of the sub-threshold leakage currents controlled by OFF transistors and the gate oxide leakage currents in the transistors that are ON. There is also the leakage across the reversed biased isolating junctions, but since our interest here is in the change in I_{DDQ} for two input vectors, we ignore this current, because it remains relatively stable. In the steady state, therefore, the relevant value of I_{DDQ} is mainly determined by the sub-threshold leakage (I_{sub}) through OFF transistors, and gate oxide leakage I_{ox} in ON transistors. The number, individual sizes (gate widths) and topological layouts of transistors also play a role in the total quiescent current (I_{DDQ}) drawn from the power supply. Thus the total leakage current of interest, (I_{leak}) in a MOSFET is a combination of sub-threshold (I_{sub}) leakage and gate-oxide leakage (I_{ox}). I_{sub} can be expressed using the following equations [39], [40]:

$$I_{sub} = A_1 W e^{-V_{th}/nV_T}(1 - e^{-V/V_T}) \tag{1}$$

where A_1 and n are experimentally derived. W and L are width and length of the transistor gate, V_{th} is the threshold voltage, V_T is the thermal voltage and V is the supply voltage. The thermal voltage V_T is approximately $25mV$ at room temperature.

Equation 1 shows that the current is exponentially dependent on the voltage across the drain and source terminals when the transistor is OFF. A small change in voltage may cause a large change in the current. As a result, the current will be significantly lower for stacked two or more series-connected MOS transistors that are OFF and can be neglected in some cases (see details in Section III-B).

Gate-oxide leakage (I_{ox}) currents can be derived from the gate leakage current density, $J_{G,i}$, given by [41]:

$$J_{G,i} = \frac{q^2}{8\pi h \epsilon \phi_{b,i}} \cdot C(V_G, V, t_{phys}, \phi_{b,i}) \cdot exp\Big\{ - \frac{8\pi\sqrt{2m_{eff,i}}(q\phi_{b,i})^{3/2}}{3hq|E|} \cdot \Big[1 - \Big(1 - \frac{|V|}{\phi_{b,i}}\Big)^{3/2}\Big]\Big\} \tag{2}$$

where q is electronic charge, h is Planck's constant, ϵ is dielectric permittivity, t_{phys} is the physical thickness of gate dielectric, $\phi_{b,i}$ is the tunneling barrier height in eV, $m_{eff,i}$ is the carrier effective mass in the dielectric, V is the voltage across the dielectric, and E is the electric field in the dielectric. $C(V_G, V, t_{phys}, \phi_{b,i})$ is an empirical correction factor which can be obtained from the following equation:

$$C(V_G, V, t_{phys}, \phi_{b,i}) = \frac{V_G}{t_{phys}} \cdot N \cdot exp\Big[\frac{20}{\phi_{b,i}}\Big(\frac{|V| - \phi_{b,i}}{\phi_{0i}} + 1\Big)^{\alpha_i} \cdot \Big(1 - \frac{|V|}{\phi_{b,i}}\Big)\Big] \tag{3}$$

where, α_i is a fitting parameter and ϕ_{0i} is the conduction band offset or valence band offset between Si and the gate dielectric. V_G is the potential at gate and N is the density of carriers in the inversion or accumulation layer in the injecting electrode, which can be written as:

$$N = \frac{\epsilon}{t_{phys}}\Big\{n_{inv}V_T \cdot ln\Big[1 + exp\Big(\frac{V_{G,eff} - V_{th}}{n_{inv}V_T}\Big)\Big] + V_T \cdot ln\Big[1 + exp\Big(-\frac{V_G - V_{FB}}{V_T}\Big)\Big] \tag{4}$$

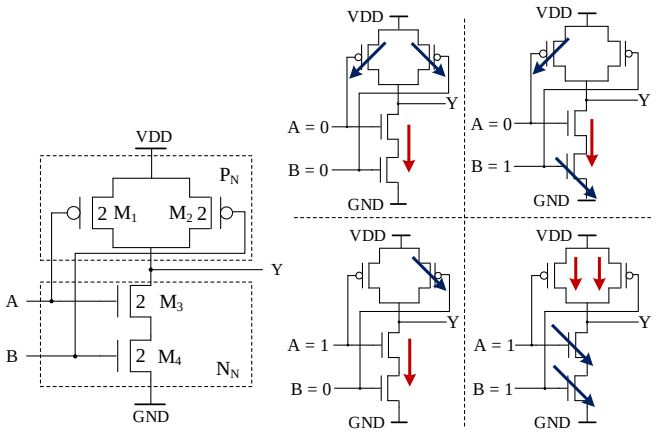
where, V_{FB} is the flatband voltage, and $V_{G,eff} = V_G - V_{poly}$ is the effective gate voltage after accounting for the voltage drop V_{poly} across the poly-Si gate depletion region. The rate of increase of sub-threshold career density is controlled by n_{inv} ($= S/V_T$, where S is the subthreshold swing), which is positive for NMOS transistors and negative for PMOS transistors. The gate oxide leakage current (I_{ox}) can be obtained by multiplying gate tunneling current density ($J_{G,i}$) with the gate area (WL).

From Equations 1 through 4, we can conclude that sub-threshold leakage current (I_{sub}) and gate-oxide leakage current (I_{ox}) are exponentially dependent on the supply voltage (V) and threshold voltage (V_{th}) of a MOSFET. A detailed model for I_{DDQ} is required to incorporate these exponential dependencies when two (or more) OFF transistors are connected in series. Such a model is presented in the following section.

B. I_{DDQ} Modeling for Logic Gates

Figure 1(a) shows the transistor-level circuit diagram of a two input NAND gate with inputs A and B, and output Y. The sizing of MOSFETs is done following the basic gate sizing rules [42]. Here, we select W/L as 2 for all transistors of the NAND gate in Figure 1(a). Figure 1(b) shows I_{DDQ} of the NAND gate for four different input combinations.

When a transistor is OFF, and there is a potential difference between gate and drain/source terminals, substrate leakage



(a) NAND Gate (b) I_{DDQ} Model

Figure 1: Two-input NAND gate and its I_{DDQ} model.

Table I: Leakage currents in two-input NAND gate of Fig. 1.

Input		M_1		M_2		M_3		M_4	
A	B	I_{ox}	I_{sub}	I_{ox}	I_{sub}	I_{ox}	I_{sub}	I_{ox}	I_{sub}
0	0	✓	-	✓	-	-	✓	-	✓
0	1	✓	-	-	-	-	✓	✓	-
1	0	-	-	✓	-	-	-	-	✓
1	1	-	✓	-	✓	✓	-	✓	-

occurs. On the other hand, when the transistor is ON or the gate and drain/source terminals are at different potentials, gate oxide leakage takes place. For 00 input vector, the two NMOS transistors (M_3 and M_4) are OFF, and substrate leakage takes place through the stack. In addition, there is gate leakage from M_1 and M_2. The red and blue arrows represent the substrate leakage and gate leakage, respectively. Table I summarizes the gate leakage and substrate leakage for each transistor. The checkmark (✓) indicates the presence of a leakage component.

Table II summarizes the resultant I_{DDQ} for simple gates. The notations for describing the current are presented below:

- $I_P^{G^*}$, $I_P^{G^\dagger}$ and I_P^G represent gate leakage currents of the PMOS transistors of NAND gate, NOR gate and inverter, respectively. Similarly, $I_N^{G^*}$, $I_N^{G^\dagger}$ and I_N^G represent gate leakage currents of NMOS transistors of NAND gate, NOR gate and inverter, respectively. Note that these leakages may vary from gate to gate due to different sizing.
- $I_P^{S^*}$, $I_P^{S^\dagger}$ and I_S^G represent subthreshold leakage currents of the PMOS transistors of NAND gate, NOR gate and inverter, respectively. Similarly, $I_N^{S^*}$, $I_N^{S^\dagger}$ and I_N^G represent subthreshold leakage current of the NMOS transistors of NAND gate, NOR gate and inverter, respectively.
- $I_P^{SS^*}$ represents the subthreshold leakage current when two OFF PMOS transistors are in series and $I_N^{SS^*}$ represents the subthreshold leakage current when two OFF NMOS transistors are in series. These currents can be very small due to the stacking effect of the OFF MOS transistors.

Table III summarizes the simulated I_{DDQ} of simple gates (e.g., NAND, NOR and inverter) for different input combinations. The *absolute* value of I_{DDQ} (denoted as I_{DDQ}^A) is obtained from HSPICE simulation using the $32nm$ PTM model. I_{DDQ}^A is presented as a summation of different gate leakage currents and subthreshold current for respective inputs (following the order of Table II). The normalized I_{DDQ} values of gates (denoted as I_{DDQ}^U) are shown in Columns 4, 6 and 8. We have normalized different components of I_{DDQ} with the I_{DDQ} component's of an inverter. For 00 input vector applied to NAND, gate leakage current from two PMOS transistors ($2I_P^{G^*}$) is 13.35 pA and NMOS subthreshold current ($I_N^{SS^*}$) is 0.67 pA. The I_{DDQ}^U becomes $2I_P^G + I_N^S/2$ as I_P^G and I_N^S for an inverter are 6.67 pA and 1.71 pA, respectively. For 01 input vector, gate leakage current from M_1 ($I_P^{G^*}$) is $6.67pA$, gate leakage current from M_4 ($I_N^{G^*}$) is $18.56pA$ and subthrehsold leakage from M_3 ($I_N^{S^*}$) is $2.73pA$. I_{DDQ}^A for rest of the gates for all possible inputs are shown in the similar way. The I_{DDQ}^U becomes $I_P^G + 2.5I_N^G + 1.6I_N^S$ as I_N^G of an inverter is 7.56 pA. For 10 input vector, there will be no gate leakage for M_3 as no voltage difference is developed across the gate and source terminals (both at VDD). The resultant I_{DDQ}^A will be 6.67 pA ($I_P^{G^*}$) + 2.25 pA ($I_N^{S^*}$) and I_{DDQ}^U will be $I_P^G + 1.3I_N^S$. Finally, for input vector 11, I_{DDQ}^A will be 37.12 pA ($2I_N^{G^*}$) + 5.18 pA ($2I_P^{S^*}$) and I_{DDQ}^U will be $4.9I_N^G + 2I_P^S$. A NOR gate is analyzed similarly. The analysis can be extended for three-input and four-input gates. A non-inverting gate (AND, OR, etc.) can be modeled as an inverting gate followed by an inverter.

Table II: I_{DDQ} for simple gates.

A	B	NAND	NOR	Inverter
0	0	$2I_P^{G^*} + I_N^{SS^*}$	$2I_P^{G^\dagger} + 2I_N^{S^\dagger}$	$I_P^G + I_N^S$
0	1	$I_P^{G^*} + I_N^{G^*} + I_N^{S^*}$	$I_P^{G^\dagger} + I_N^{G^\dagger} + I_P^{S^\dagger}$	NA
1	0	$I_P^{G^*} + I_N^{S^*}$	$I_N^{G^\dagger} + I_P^{S^\dagger}$	NA
1	1	$2I_N^{G^*} + 2I_P^{S^*}$	$2I_N^{G^\dagger} + I_P^{SS^\dagger}$	$I_N^G + I_P^S$

C. Impact of Aging and Process Variation on I_{DDQ}

Integrated circuits experience aging in their regular operations, which causes an increase in its threshold voltage. One of the major aging phenomena for ICs is negative bias temperature instability (NBTI), which occurs in PMOS transistors when they face negative bias stressing [24], [25]. Due to negative bias, interface traps are created at the Si-SiO_2 interface of PMOS transistor. Releasing the stress can recover some of the traps but cannot recover fully, which results in a net increase in the threshold voltage (V_{th}) of PMOS transistors [43]. In summary, a PMOS transistor ages when it is turned on (the input is at logic 0) and relaxes when it is turned off (the input is logic 1).

Other aging phenomena in CMOS circuits, especially in NMOS devices, are positive bias temperature instability (PBTI) and hot carrier injection (HCI). In older technology nodes, PBTI effect which is the NMOS counterpart of NBTI, was negligible compared to NBTI [44]. After the introduction of high-κ / metal gate transistors, in sub 45nm technologies, the PBTI effect can be significant [45], [46]. Multiple switching electrons receive enough energy to tunnel through the potential barrier and get trapped in Si-SiO_2 interface near the drain terminal which is known as hot carrier injection

Table III: Simulated I_{DDQ} for simple gates.

Inputs		NAND		NOR		Inverter	
A	B	I^A_{DDQ}	I^U_{DDQ}	I^A_{DDQ}	I^U_{DDQ}	I^A_{DDQ}	I^U_{DDQ}
0	0	(13.35 + 0.67) *pA*	$2I^G_P + I^S_N/2$	(29.17 + 3.42) *pA*	$4.4I^G_P + 2I^S_N$	(6.67 + 1.71) *pA*	$I^G_P + I^S_N$
0	1	(6.67 + 18.56 + 2.73) *pA*	$I^G_P + 2.5I^G_N + 1.6I^S_N$	(14.58 + 7.56 + 4.47) *pA*	$2.2I^G_P + I^G_N + 1.7I^S_P$	NA	NA
1	0	(6.67 + 2.25) *pA*	$I^G_P + 1.3I^S_N$	(7.56 + 3.33) *pA*	$I^G_N + 1.3I^S_P$	NA	NA
1	1	(37.12 + 5.18) *pA*	$4.9I^G_N + 2I^S_P$	(15.12 + 0.70) *pA*	$2I^G_N + I^S_P/3.7$	(7.56 + 2.59) *pA*	$I^G_N + I^S_P$

(HCI) effect. An NMOS transistor is primarily affected by HCI, which has practically no effect on PMOS transistors [47]. Like PBTI, HCI effect is small compared to NBTI effect in older technology nodes [44].

We focus on developing a solution that effectively measures the amount of aging for older chips, some of which though obsolete are still circulating in the market. Even though in sub-45nm technologies both PMOS and NMOS devices age, the proposed solution utilizes the aging from the PMOS transistors to detect recycled ICs irrespective of the technology. Note that as the threshold voltage of a PMOS/NMOS transistor increases due to aging, the leakage current I_{DDQ}, which has a negative exponential relation with the threshold voltage (V_{th}), decreases [48]. As a result, the overall I_{DDQ} continually decreases as a chip is used longer in the field.

Process variation (PV) causes the threshold voltage of a transistor to vary from its nominal value [49], [50]. PV can be of two types - inter-die or systematic variation and intra-die variation or random variation [51]. Inter-die variation is the variation among different dies caused by small changes in the environment of fabrication. It moves the threshold voltage of all transistors of chip in one direction. Intra-die or random variation is the variation among the MOS transistors of a die, arising from random dopant fluctuations, line edge roughness and surface orientation [52]–[54].

The process variation causes inaccuracies in determining the age of a chip, as the I_{DDQ} values for different chips vary significantly. It is a challenge to determine whether a change in I_{DDQ} has resulted from aging or process variation. However, the aging causes the I_{DDQ} to decrease, whereas the process variation may cause an increase or decrease in the I_{DDQ}. Our proposed solution based on normalized ΔI_{DDQ} (see Section IV) removes the effect of systematic process variation from the measurement and helps to determine accurately whether or not a chip has been used.

D. Non-Uniform Aging in Circuit

In a complex circuit, not all transistors age at the same rate during an interval of operation. The aging rates of transistors depend upon controllabilities of signal nodes indicating how often they assume 0 or 1 values. SCOAP is a popular analysis of controllability and observability but it estimates the effort of setting a node to some value and observing at a primary output [55]. The SCOAP controllability, does not tell us how frequently the node will assume a 0 or 1 state. Hence, we use an alternative analysis of the circuit topology that provides 1-controllability for each node as the probability of the node being 1 when the circuit receives a random input. The 0-controllability is the complement of 1-controllability.

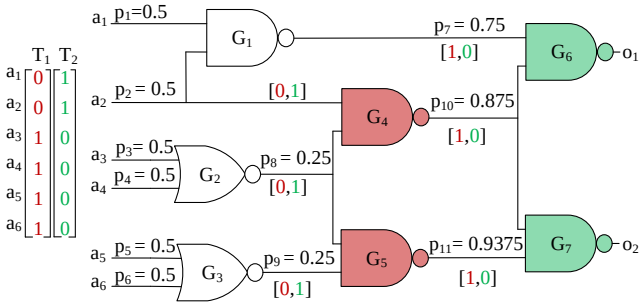


Figure 2: Test pattern selection for ΔI_{DDQ} measurement using controllability analysis.

In a digital circuit, controllabilities vary from node to node. A logic value 1 at a node turns off the PMOS transistor of the next gate, whereas, a logic value 0 turns on the PMOS transistor of that gate. So when a node value is 0 the next gate ages, and when node value is 1 it relaxes. In a regular operation, the node with a higher probability of 0 (low 1-controllability) receives 0 more frequently and ages the next gate faster compared to a gate with an input of high 1-controllability. Consequently, all gates of the circuit do not age at the same rate. A gate ages faster when its inputs have low 1-controllabilities. Evidently, this leads to non-uniform aging across the circuit.

Figure 2 shows the controllability analysis of a circuit. The 1-controllabilities, p_1 through p_{11}, are computed by applying all input pattern combinations and p_i is the ratio of number of 1's on line i to the total numbers of patterns (64 for this circuit). Gates G_4 and G_5 have greater chance of getting aged as one or both inputs receive 0 more frequently. We denote these gates as fast aging gates, highlighted in red. On the other hand, gates G_6 and G_7 have relatively lower chance of getting aged as one or both inputs receive 1 most of the time. We denote these gates as slow aging gates (shown in green).

Our objective is to measure I_{DDQ} for fast aging gates and for slow aging gates, and then take the difference of those two values. We denote this as ΔI_{DDQ}. Previously, *Delta-I_{DDQ}* has been used in testing [56]. It was defined as the difference of I_{DDQ} measurements for any consecutive patterns of an input sequence. In contrast, our ΔI_{DDQ} is obtained for only two carefully selected patterns.

When a chip ages, I_{DDQ} from fast aging gates will decrease rapidly, whereas the I_{DDQ} from slow aging gates will not change as much. This will result in an increasing ΔI_{DDQ} as the chip gets used longer in the field. It is necessary to select the first test pattern (T_1) that selects the PMOS gate leakage

(e.g., using gate inputs $AB = 00$ for NAND gate highlighted in red in Figure 1) of fast aging gates. This pattern T_1 results in I_{DDQ} denoted by I_1. Similarly, we select a second test pattern (T_2) that that selects the PMOS gate leakages of slow aging gates (e.g., using gate inputs $AB = 00$ for NAND gate highlighted in green in Figure 1). For T_2 the I_{DDQ} is denoted by I_2. Note that we choose gate leakage for selecting a gate as its value is much higher than the subthreshold leakage (see Table III).

The test consists of applying T_1 and T_2, and measuring I_1 and I_2. Let us assume that I_{DDQ} is controlled mostly by fast aging gates during T_1 and mostly by slow aging gates during T_2. Then,

$$I_1 = k_1 \times I_P^H + r_1 \times I_N \quad (5)$$

$$I_2 = k_2 \times I_P^L + r_2 \times I_N \quad (6)$$

Where I_P and I_N are currents that depend on the gate leakage of PMOS and NMOS transistors as shown in Table III. "H" and "L" refer to the fast and slow aging conditions created by T_1 and T_2. Coefficients k_1, r_1, k_2 and r_2 depend on the specific signal states and gate structures in the circuit.

Note that $k_1 \times I_P^H$ will reduce significantly as it comes mostly from fast aging gates, whereas $k_2 \times I_P^L$ will remain relatively unchanged with age as it is derived from a majority of slow aging gate. The values of I_P^H and I_P^L are same at time 0 (when the chip is new) and equals I_P if we ignore process variation. On the other hand, both $r_1 \times I_N$ and $r_2 \times I_N$ will remain constant, as I_N results from NMOS transistors.

The difference between these two currents is denoted as ΔI_{DDQ}, and described as follows:

$$\begin{aligned} \Delta I_{DDQ} &= I_2 - I_1 \\ &= \underbrace{k_2 \times I_P^L - k_1 \times I_P^H}_{\Delta I_P} + \underbrace{(r_2 - r_1) \times I_N}_{\Delta I_N} \end{aligned} \quad (7)$$

In Equation 7, ΔI_{DDQ} has two components derived from P-Network (ΔI_P) and N-network (ΔI_N). Our objective for selecting two patterns (T_1 and T_2) will be based on maximizing the aging degradation from the P-network. At the same time, we need to focus on minimizing ΔI_N such that the impact of process variation on ΔI_{DDQ} from the N-network can be eliminated. Roughly, we can say the two patterns should follow $r_2 \approx r_1$.

Of the two types of process variations (systematic and random), systematic variation affects I_{DDQ} from chip to chip. It moves the threshold voltages (V_{th}) for all transistors on a chip in the same way (either increase or decrease). As a result, both I_1 and I_2 are impacted identically, and we should expect ΔI_{DDQ} to be unaffected. However, it is necessary to normalize ΔI_{DDQ} to be in the same range for different process corners. On the other hand, random process variations average out for a circuit with a reasonable number of gates. In our simulation, we have considered four corner cases of process variation. We define normalized ΔI_{DDQ} as follows:

$$\Delta I = \frac{I_2 - I_1}{I_2 + I_1} \times 100 \text{ percent} \quad (8)$$

We will use ΔI to detect recycled ICs.

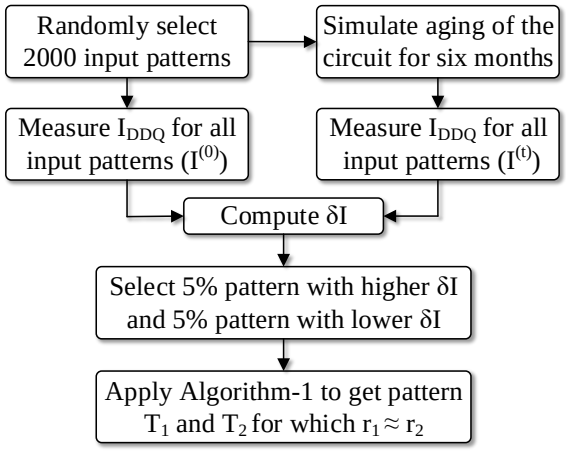


Figure 3: Proposed pattern selection process during characterization.

Note that the discussion given to explain the analysis centers around NBTI for simplicity, although in reality all three effects (NBTI, PBTI and HCI) are accounted for in the numerical data obtained from the Synopsys tool.

IV. Proposed Approach for Detecting Recycled ICs

The proposed flow for detecting recycled ICs is based on the change in the ΔI_{DDQ}, which increases when a chip is used. We can accurately identify a chip as recycled, if normalized ΔI_{DDQ} becomes greater than a threshold value. The procedure comprises of two stages - characterization and test. During characterization, we will derive two test patterns for I_{DDQ} measurement, and a threshold value as the comparison point. During the test, we measure the I_{DDQ} for the two selected test patterns, and a decision is made based on the normalized ΔI_{DDQ} value.

A. Characterization

The first part of the proposed method is to characterize the chip. This is done by the chip manufacturer. The characterization process has two parts: pattern selection and threshold calculation. First, we need to select two input patterns, T_1 for which $I_{DDQ} = I_1$ is controlled mostly by fast aging gates and T_2 for which $I_{DDQ} = I_2$ is controlled mostly by slow aging gates. The second part is to determine a threshold value, ΔI_T, which will be used as a reference to make a decision in the testing phase.

We use a simulation based search for T_1 and T_2 such that the variation of $I_2 - I_1$ is maximized as age of the device increases. To reduce complexity we conduct the search over a random subset of all possible input patterns. As the size of this subset increases, the optimality of our selection would approach closer to that of the global search. We believe that by the time the random subset size increases to 2,000, further benefit of enlarging the subset becomes negligible. One might consider that 2,000 patterns are a random sample set and another independent sample set might produce statistically

Algorithm 1: Test pattern selection

```
   input : Circuit netlist (C), randomly selected 2000 test patterns
           (TP), and δI for all TP (δ)
   output: Two test patterns (T1, T2)
1  begin
2      A ⟵ Max(δ), B ⟵ Min(δ);
3      j, l ⟵ 1;
4      for i ← 1 to 2000 do
5          if δ ≥ 0.95×A then
6              L1[j] ⟵ TP[i] ;
7              r1[j] ⟵ calculate_r(C, TP[i]);
8              j ⟵ j + 1 ;
9          end
10         if δ ≤ 1.05×B then
11             L2[l] ⟵ TP[i] ;
12             r2[l] ⟵ calculate_r(C, TP[i]);
13             l ⟵ l + 1 ;
14         end
15     end
16     for i ← 1 to j do
17         for m ← 1 to l do
18             D(i, m) ← |(r2[i] − r1[m])|;
19         end
20     end
21     [r, c] ⟵ min_element(D);
22     T1 ⟵ L1[r], T2 ⟵ L2[c];
23 end
```

different and possibly better result. However, 2,000 is a large enough sample that statistical variations in the result would be small. This is verifiable from the theory of statistical sampling commonly used in fault coverage analysis tools [36]. Hence, we chose 2,000 random patterns for searching for T_1 and T_2.

The pattern selection process shown in Figure 3 works as follows:

1) Two thousand input patterns are selected randomly to find out two patterns (T_1 and T_2) that may result in maximal degradation (ΔI, see Equation 8) when an IC gets used in the field. We choose 2,000 input patterns for characterization as it is a large sample size, which can fairly represent the whole input pattern set. Note that one can also use a larger number of input patterns.
2) We use HSPICE to simulate the circuit, and determine I_{DDQ} for all 2,000 input patterns. Suppose, the current for ith pattern is $I_i^{(0)}$. See the simulation details in Section V. Note that this characterization can be done in a foundry by measuring the I_{DDQ} for a new chip.
3) Aging simulation is performed by using Synopsys MOSRA (see Section V) to find out two patterns that cause maximum degradation. We perform aging for six months at a temperature 25°C, and the nominal supply voltage of 1V. After aging, I_{DDQ} for the same 2,000 test patterns is determined. Aged I_{DDQ} can be represented as $I_i^{(t)}$. Note that a manufacturer can also perform an accelerated aging at the foundry.
4) The percentage change in I_{DDQ} due to six months of aging is calculated for each pattern using the following equation:
$$\delta I = \frac{I^{(0)} - I^{(t)}}{I^{(0)}} \times 100 \quad (9)$$
5) Finally, Algorithm 1 is applied to select two input patterns T_1 and T_2.

Algorithm 1 selects two test patterns (T_1 and T_2) such that ΔI_P is maximized (largest aging degradation) and ΔI_N is minimized (lowest impact of process variation on ΔI_{DDQ} from NMOS transistors (see Equation 7). The algorithm takes the circuit netlist (C), 2,000 randomly selected test patterns (TP), and previously calculated/measured δI (see Equation 9) for all these patterns (δ) as input, and returns two test patterns (T_1 and T_2) as output. The algorithm starts by selecting the maximum and minimum δI (Line 2). Two groups of patterns (L_1, L_2) are selected from 2,000 input patterns that include patterns with maximum and minimum δI with 5% tolerance limit (Line 4-15). Note that one can also vary this tolerance to obtain these groups. The coefficient r_1 for I_N in Equation 5 is computed using *calculate_r* function (Line 7), which takes the netlist (C) and a test pattern ($TP[i]$) as inputs. It uses Synopsys VCS simulation to obtain the internal node values. Finally, r_1 is calculated using Table III. Similarly, r_2, which is the coefficient of I_N in Equation 6 is computed using *calculate_r* function (Line 12). A matrix D is computed, where each element is the difference of r_1 and r_2 (Line 16-19). The row and column indexes of the minimum element in matrix D are selected, where *min_element()* function returns the row and column indexes of the minimum element of a matrix (Line 21). These indexes are used to select the desired test patterns, T_1 and T_2.

The second part of the characterization process is to calculate the threshold value to determine whether or not a chip is recycled. As I_{DDQ} varies with the process variation (see Section III-C), it is necessary to consider all corner cases of process variation. The four cases have been modeled as four netlists. *Netlist-1* is the circuit with no systematic process variation. *Netlist-2* is the same circuit with 10% increased V_{th} for all MOS transistors. *Netlist-3* is also the same circuit with 10% decreased V_{th} for all MOS transistors. *Netlist-4* is the circuit with 10% increased V_{th} for all PMOS transistors, and 10% decreased V_{th} for all NMOS transistors. A random variation of 5% of V_{th} is added to all four netlists.

Netlist-1 represents the ideal case where there is no systematic process variation. For *Netlist-2* both I_P and I_N of Equation 7 will be decreased due to the increased V_{th}. On the other hand, both I_P and I_N will be increased due to a reduced V_{th} in *Netlist-3*. For *Netlist-4*, I_P will be reduced, whereas I_N will be increased. *Netlist-4* represent the most severe case, as it will increase the noise effect during the measurement (see Equation 7). We measure ΔI for all four cases and consider the maximum of all the fours as our threshold value, which is denoted as ΔI_T. The threshold value selection process of our proposed method is shown in Figure 4 which can be summarized as follows:

1) Create four netlists for different process corners.
2) Apply two input patterns, T_1 and T_2, to all four netlists and measure I_{DDQ}.
3) Normalized I_{DDQ} and ΔI are calculated for all four netlists.
4) The maximum value of ΔI found in Step 3 will be considered as the threshold value (ΔI_T) for detecting recycled chips.

Note that we do not need to perform the simulation when we have access to the new chips. In the foundry, two previously

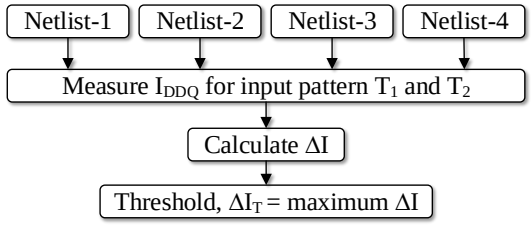


Figure 4: Calculation process of threshold

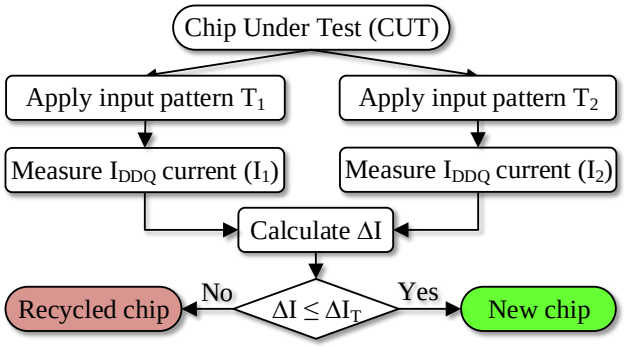


Figure 5: Proposed flow for detecting recycled ICs using ΔI.

selected input patterns, T_1 and T_2, can be applied to a reasonably large number of ICs and ΔI measured. The threshold value will be the maximum of all ΔIs.

B. Tests for Identifying Recycled ICs

The testing process for detecting recycled ICs is fairly straightforward. Two test patterns, T_1 and T_2, are required during the test. These two patterns can be obtained from the characterization phase (see Section IV-A), which can be completed either by simulation using any commercial tool or at the manufacturing floor using fabricated chips. The proposed flow of detection method is shown in Figure 5. The steps for detecting recycled ICs are as follows:

1) Input patterns T_1 and T_2 are applied to the chip under test.
2) I_{DDQ} for these patterns, I_1 and I_2, are measured using a commercial tester.
3) ΔI is calculated using Equation 8.
4) If ΔI is greater than ΔI_T, the chip is classified as a recycled chip. Otherwise, it is a new chip.

V. Results and Discussion

To verify the proposed method of detecting recycled chips, we performed aging simulation on ISCAS'85 benchmark circuits [57]. We used MOS Reliability Analysis (MOSRA) in HSPICE, an integrated circuit reliability analysis tool from Synopsys [58], and Synopsys $32nm$ technology library [59]. MOS transistor parameters were based on $32nm$ low power metal gate Predictive Technology Model (PTM) [60]. The aging simulation was done for $25°C$ temperature and nominal supply voltage of 1V. The benchmark circuits were synthesized in Synopsys Design Compiler and converted into HSPICE netlist by Synopsys IC Validator. We used Synopsys VCS to perform the gate level analysis needed in Algorithm 1.

Simulation results for five benchmark circuits are given in Tables IV and V. Table IV contains I_{DDQ} for both patterns for each netlist, when the circuit is new. The first column represents the usage of the chip. I_{DDQ} from *Netlist-1* for patterns T_1 and T_2 (I_1 and I_2 in nanoamperes) are shown in Columns 3 and 4, respectively. ΔI (see Equation 8) is shown in Column 5. The values for *Netlist-2* are shown in Columns 6-8, and those for *Netlist-3* and *Netlist-4*, in Columns 9-11 and Columns 12-14, respectively. Maximum value of ΔI, which is the threshold (ΔI_T) for each circuit is shown in Column 15. For c432 benchmark circuit, ΔI values in new circuit for four netlists that represent process corners, are 3.30%, 3.31%, 3.15% and 3.45% respectively. The maximum value 3.45% is the threshold ΔI_T. Similar analysis can be performed for all other benchmark circuits.

Table V summarizes I_{DDQ} data after six months and one year of aging. The columns of this table are similar as in Table V, except the last one. Column 15 represents the minimum value of the ΔI obtained from the four netlists. We can detect recycled ICs if the value of Column 15 is greater than ΔI_T (Column 15 of Table IV). For the c432 circuit, after six months of aging, the ΔI values are 6.07%, 6.09%, 5.89% and 6.37%. The minimum value is 5.89% which is greater than its threshold ($\Delta I_T = 3.45\%$). The same analysis can be performed for other benchmark circuits. Note that the ΔI value further increases when the circuit is aged beyond one year.

VI. Conclusion

The two-pattern ΔI_{DDQ} test effectively identifies recycled ICs that may have been previously used for as little as six months as majority of recycled chips those are already circulating in the market, have been used several years. The advantage of our proposed method is that it does not require any design modification, and thus, can be applied to the commercial off the shelf (COTS) products. In addition, it can be applied by any available automatic test equipment (ATE) and the test is quick and economical because it involves application of just two patterns for which I_{DDQ} is measured. An important feature is the suppression of interference from systematic process variation.

Because activity varies from signal to signal, not all transistors experience the same level of NBTI induced aging. In one of the two test patterns I_{DDQ} is controlled by the least aged transistors, while in the other pattern it is controlled by the most aged transistors. The test patterns used in our illustration were selected from 2,000 random patterns and cannot be considered optimal. Finding an optimal pattern pair will be a relevant problem to solve.

In the area of testing, very large circuits present a problem for I_{DDQ} based methods. This is because the aggregate from a large number of gates affects the ability to detect small variations. How well the I_{DDQ} based counterfeit detection will work for large circuits should be investigated. Intuitively, adding the aging effects from a large number of gates may benefit the detection capability. Besides analyzing large circuits, our plans also include actual hardware tests using the available Advantest T2000GS ATE at Auburn University.

Table IV: I_{DDQ} for new circuits.

Usage	Bench-	Netlist-1			Netlist-2			Netlist-3			Netlist-4			$\Delta I_T\ \% = max(\Delta I)$
months	marks	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	
0	c432	22.14	23.65	3.30	23.19	24.78	3.31	54.18	57.71	3.15	29.38	31.49	3.45	3.45
	c499	185.67	190.67	1.33	144.91	148.71	1.29	204.79	209.8	1.21	193.92	199.227	1.35	1.35
	c880	361.05	397.01	4.74	241.04	265.69	4.86	349.86	386.61	4.99	270.09	296.13	4.59	4.99
	c1908	55.36	59.96	3.99	34.39	37.34	4.11	123.79	134.69	4.22	90.61	98.95	4.39	4.39
	c3540	136.19	146.55	3.66	87.86	94.75	3.77	286.29	305.73	3.28	195.21	210.59	3.79	3.79

Table V: I_{DDQ} for used circuits.

Usage	Bench-	Netlist-1			Netlist-2			Netlist-3			Netlist-4			$min(\Delta I)$
months	marks	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	$I_1\ nA$	$I_2\ nA$	$\Delta I\ \%$	%
6	c432	17.32	19.56	6.07	17.96	20.29	6.09	34.98	39.36	5.89	25.86	29.38	6.37	5.89
	c499	149.32	160.08	3.48	112.93	120.99	3.45	166.53	178.14	3.37	164.87	176.91	3.52	3.37
	c880	290.29	328.24	6.14	231.82	242.64	6.31	337.73	385.29	6.58	257.79	291.41	6.12	6.12
	c1908	44.06	50.66	6.97	28.81	33.26	7.17	82.75	95.74	7.28	78.3	90.52	7.24	6.97
	c3540	111.51	123.56	5.13	74.06	82.24	5.23	197.46	218.28	5.01	171.49	190.55	5.26	5.01
12	c432	16.70	19.19	6.94	17.25	19.83	6.96	32.81	37.53	6.71	24.94	28.74	7.08	6.71
	c499	143.02	154.86	3.97	107.22	115.79	3.84	159.70	172.31	3.79	155.28	168.16	3.98	3.79
	c880	278.26	315.85	6.33	202.85	231.24	6.54	323.97	370.8	6.74	242.91	275.55	6.29	6.29
	c1908	42.39	49.02	7.25	27.82	32.29	7.44	77.89	90.52	7.49	75.03	87.09	7.44	7.25
	c3540	107.62	119.91	5.40	71.58	79.92	5.50	186.79	207.16	5.17	164.95	183.74	5.39	5.17

The last column of Table IV shows that not all circuits are affected by process variation in the same way. Future investigation on structure and function dependence of this effect may lead to design principles that minimize process variability.

ACKNOWLEDGMENT

This work was supported in parts by the National Science Foundation under Grant Numbers CNS-1755733 and CCF-1527049.

REFERENCES

[1] P. Chowdhury, U. Guin, A. D. Singh, and V. D. Agrawal, "Two-pattern ΔI_{DDQ} test for recycled IC detection," in *Proc. 32nd International Conference on VLSI Design*, Jan. 2019, pp. 82–87.

[2] IHS iSuppli, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," 2011, http://press.ihs.com/press-release/design-supply-chain/top-5-most-counterfeited-parts-represent-169-billion-potential-cha.

[3] M. M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.

[4] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[5] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[6] G-19A Test Laboratory Standards Development Committee, "Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts," 2016, https://saemobilus.sae.org/content/as6171.

[7] G-19CI Continuous Improvement, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," 2009, https://saemobilus.sae.org/content/as5553.

[8] CTI, "Certification for Counterfeit Components Avoidance Program," 2011, http://www.cti-us.com/pdf/CCAP101Certification.pdf.

[9] IDEA, "Acceptability of Electronic Components Distributed in the Open Market," 2017, http://www.idofea.org/products/118-idea-std-1010b.

[10] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ics," in *2012 IEEE International symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT)*, October 2012, pp. 13–18.

[11] K. Huang, J. Carulli, and Y. Makris, "Parametric counterfeit IC detection via Support Vector Machines," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, December 2012, pp. 7–12.

[12] Y. Zheng, A. Basak, and S. Bhunia, "CACI: Dynamic current analysis towards robust recycled chip identification," in *Proceedings of the 51st Annual Design Automation Conference*, June 2014, pp. 1–6.

[13] H. Dogan, D. Forte, and M. M. Tehranipoor, "Aging analysis for recycled fpga detection," in *2014 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT)*, October 2014, pp. 171–176.

[14] Y. Zheng, X. Wang, and S. Bhunia, "SACCI: Scan-based characterization through clock phase sweep for counterfeit chip detection," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 5, pp. 831–841, 2015.

[15] Z. Guo, M. T. Rahman, M. M. Tehranipoor, and D. Forte, "A zero-cost approach to detect recycled soc chips using embedded sram," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2016, pp. 191–196.

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

[17] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE-ACM Design Automation Conference*, June 2012.

[18] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 5, pp. 1016–1029, 2014.

[19] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost On-Chip Structures for Combating Die and IC Recycling," in *Proc. of ACM/IEEE Design Automation Conference*, 2014.

[20] U. Guin, D. Forte, and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233–1246, 2016.

[21] K. He, X. Huang, and S. X. D. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2015, pp. 146–151.

[22] M. Alam, S. Chowdhury, M. Tehranipoor, and U. Guin, "Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures," in *IEEE Int. Symposium on Hardware Oriented Security and Trust (HOST)*, April 2018.

[23] M. Miller, J. Meraglia, and J. Hayward, "Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts," in *SAE Aerospace Electronics and Avionics Systems Conference*, October 2012.

[24] D. K. Schroder and J. A. Babcock, "Negative bias temperature instability: Road to cross in deep submicron silicon semiconductor manufacturing," *Journal of applied Physics*, vol. 94, no. 1, pp. 1–18, 2003.

[25] V. Reddy, A. T. Krishnan, A. Marshall, J. Rodriguez, S. Natarajan, T. Rost, and S. Krishnan, "Impact of negative bias temperature instability

on digital circuit reliability," *Microelectronics Reliability*, vol. 25, no. 1, pp. 31–38, 2005.
[26] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.
[27] http://cdctool.sae.org/.
[28] J. Keane, X. Wang, D. Persaud, and C. H. Kim, "An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 4, pp. 817–829, 2010.
[29] K. Hofmann, H. Reisinger, K. Ermisch, C. Schlünder, W. Gustin, T. Pompl, G. Georgakos, K. v. Arnim, J. Hatsch, T. Kodytek *et al.*, "Highly accurate product-level aging monitoring in 40nm CMOS," in *Proc. Symposium on VLSI Technology*, June 2010, pp. 27–28.
[30] E. Saneyoshi, K. Nose, and M. Mizuno, "A precise-tracking NBTI-degradation monitor independent of NBTI recovery effect," in *IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, Feb. 2010, pp. 192–193.
[31] S. Shahbazmohamadi, D. Forte, and M. Tehranipoor, "Advanced physical inspection methods for counterfeit ic detection," in *ISTFA 2014: Conference Proceedings from the 40th International Symposium for Testing and Failure Analysis*. ASM International, 2014, p. 55.
[32] P. Ghosh and R. S. Chakraborty, "Counterfeit ic detection by image texture analysis," in *2017 Euromicro Conference on Digital System Design (DSD)*. IEEE, 2017, pp. 283–286.
[33] N. Asadizanjani, M. Tehranipoor, and D. Forte, "Counterfeit electronics detection using image processing and machine learning," vol. 787, no. 1, p. 012023, 2017.
[34] P. Ghosh and R. S. Chakraborty, "Recycled and remarked counterfeit integrated circuit detection by image processing based package texture and indent analysis," *IEEE Transactions on Industrial Informatics*, 2018.
[35] N. Asadizanjani, N. Dunn, S. Gattigowda, M. Tehranipoor, and D. Forte, "A database for counterfeit electronics and automatic defect detection based on image processing and machine learning," in *Proceedings of the 42nd International Symposium for Testing and Failure Analysis. Texas, USA*, 2016, pp. 1–8.
[36] M. L. Bushnell and V. D. Agrawal, *Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits*. Springer, November 2000.
[37] S. Chakravarty and P. J. Thadikaran, *Introduction to IDDQ Testing*. Springer, 1997.
[38] R. Rajsuman, "Iddq testing for CMOS VLSI," *Proceedings of the IEEE*, vol. 88, no. 4, pp. 544–568, 2000.
[39] A. P. Chandrakasan, W. J. Bowhill, and F. Fox, *Design of high-performance microprocessor circuits*. Wiley-IEEE Press, 2000.
[40] N. S. Kim, T. Austin, D. Baauw, T. Mudge, K. Flautner, J. S. Hu, M. J. Irwin, M. Kandemir, and V. Narayanan, "Leakage current: Moore's law meets static power," *Computer*, vol. 36, no. 12, pp. 68–75, 2003.
[41] Y.-C. Yeo, T.-J. King, and C. Hu, "Mosfet gate leakage modeling and selection guide for alternative gate dielectrics based on leakage considerations," *IEEE Transactions on Electron Devices*, vol. 50, no. 4, pp. 1027–1035, 2003.
[42] N. H. Weste and D. Harris, *CMOS VLSI design: a circuits and systems perspective*. Pearson Education India, 2015.
[43] D. K. Schroder, "Negative bias temperature instability: What do we understand?" *Microelectronics Reliability*, vol. 47, no. 6, pp. 841–852, 2007.
[44] S. Kiamehr, A. Amouri, and M. B. Tahoori, "Investigation of NBTI and PBTI induced aging in different LUT implementations," in *Proc. International Conference on Field-Programmable Technology*, 2011, pp. 1–8.
[45] S. Zafar, Y. Kim, V. Narayanan, C. Cabral, V. Paruchuri, B. Doris, J. Stathis, A. Callegari, and M. Chudzik, "A comparative study of NBTI and PBTI (charge trapping) in SiO2/HfO2 stacks with FUSI, TiN, Re gates," in *Symposium on VLSI Technology, Digest of Technical Papers*, 2006, pp. 23–25.
[46] J. H. Stathis, M. Wang, and K. Zhao, "Reliability of advanced high-k/metal-gate n-FET devices," *Microelectronics Reliability*, vol. 50, no. 9-11, pp. 1199–1202, 2010.
[47] E. Takeda, Y. Nakagome, H. Kume, N. Suzuki, and S. Asai, "Comparison of characteristics of n-channel and p-channel MOSFET's for VLSI's," *IEEE Transactions on Electron Devices*, vol. 30, no. 6, pp. 675–680, 1983.
[48] W. Wang, V. Reddy, B. Yang, V. Balakrishnan, S. Krishnan, and Y. Cao, "Statistical prediction of circuit aging under process variations," in *Proc. Custom Integrated Circuits Conference (CICC)*, September 2008, pp. 13–16.
[49] A. Asenov, "Simulation of statistical variability in nano MOSFETs," in *Proc. IEEE Symposium on VLSI Technology*, June 2007, pp. 86–87.
[50] R. Rao, A. Srivastava, D. Blaauw, and D. Sylvester, "Statistical estimation of leakage current considering inter-and intra-die process variation," in *Proc. International Symposium on Low Power Electronics and Design*, August 2003, pp. 84–89.
[51] K. J. Kuhn, M. D. Giles, D. Becher, P. Kolar, A. Kornfeld, R. Kotlyar, S. T. Ma, A. Maheshwari, and S. Mudanai, "Process technology variation," *IEEE Transactions on Electron Devices*, vol. 58, no. 8, pp. 2197–2208, 2011.
[52] C. Shin, X. Sun, and T.-J. K. Liu, "Study of random-dopant-fluctuation (RDF) effects for the trigate bulk MOSFET," *IEEE Transactions on Electron Devices*, vol. 56, no. 7, pp. 1538–1542, 2009.
[53] A. Asenov, S. Kaya, and A. R. Brown, "Intrinsic parameter fluctuations in decananometer MOSFETs introduced by gate line edge roughness," *IEEE Transactions on Electron Devices*, vol. 50, no. 5, pp. 1254–1260, 2003.
[54] K. Kuhn, C. Kenyon, A. Kornfeld, M. Liu, A. Maheshwari, W.-k. Shih, S. Sivakumar, G. Taylor, P. VanDerVoorn, and K. Zawadzki, "Managing Process Variation in Intel's 45nm CMOS Technology," *Intel Technology Journal*, vol. 12, no. 2, 2008.
[55] M. L. Bushnell and V. D. Agrawal, *Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits*. Springer, 2000.
[56] M. S. John, D. Counce, J. Pair, and T. J. Powell, "Delta Iddq for Testing Reliability," in *Proc. 18th IEEE VLSI Test Symposium (VTS)*, Montreal, Canada, May 2000, pp. 439–443.
[57] ISCAS-85 Benchmark Circuits, http://www.pld.ttu.ee/ maksim/benchmarks/iscas85/.
[58] B. Tudor, J. Wang, W. Liu, and H. Elhak, "MOS device aging analysis with hspice and customsim," *Synopsys, White Paper*, 2011.
[59] Synopsys 32/28nm Generic Library for Teaching IC Design, https://www.synopsys.com/COMMUNITY/UNIVERSITYPROGRAM/Pages/32-28nm-generic-library.aspx.
[60] Predictive Technology Model (PTM), http://ptm.asu.edu/modelcard/LP/32nm_LP.pm.

Prattay Chowdhury (S'19) received his B.Sc. degree from the Department of Electrical and Electronics Engineering, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 2016. He received his M.S. degree from the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL, USA, in 2019. His research interest includes hardware security, VLSI design and test, and digital system.

Ujjwal Guin (S'10–M'16) received his PhD degree from the Electrical and Computer Engineering Department, University of Connecticut, in 2016. He is currently an Assistant Professor in the Electrical and Computer Engineering Department of Auburn University, Auburn, AL, USA. He received his B.E. degree from the Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, Howrah, India, in 2004 and his M.S. degree from the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA, USA, in 2010. Dr. Guin has developed several on-chip structures and techniques to improve the security, trustworthiness, and reliability of integrated circuits. His current research interests include Hardware Security & Trust, Supply Chain Security, Cybersecurity, and VLSI Design & Test. He is a co-author of the book *Counterfeit Integrated Circuits: Detection and Avoidance*. He has authored several journal articles and refereed conference papers. He was actively involved in developing a web-based Counterfeit Defect Coverage Tool (CDC Tool), *http://www.sae.org/standardsdev/cdctool/*, to evaluate the effectiveness of different test methods used for counterfeit IC detection. SAE International has acquired this tool from the University of Connecticut. He is an active participant in SAE International's G-19A Test Laboratory Standards Development Committee. He is a member both of IEEE and ACM.

Adit D. Singh (S'81–M'83–SM'00–F'02) received the B.Tech. from IIT Kanpur, and the M.S. and Ph.D. from Virginia Tech, all in Electrical Engineering. He is currently James B. Davis Professor of Electrical and Computer Engineering at Auburn University, USA. Before joining Auburn in 1991, he served on the faculty at the University of Massachusetts in Amherst, and Virginia Tech in Blacksburg. He has also held several visiting positions during sabbaticals, most recently at the University of Tokyo, Japan, and the University of Freiburg, Germany. His technical interests span all aspects of VLSI technology, in particular integrated circuit test and reliability. He has published nearly two hundred fifty research papers and holds international patents that have been licensed to industry. He is especially recognized for pioneering contributions to statistical methods in test and adaptive testing. He has served as a consultant to many major semiconductor, test and EDA companies, and as an expert witness on patent litigation cases. He has also had leadership roles as General Chair/Co-Chair/Program Chair for dozens of international VLSI design and test conferences, served on the editorial boards of several journals, and on the Steering and Program Committees of many of the major IEEE international test and design automation conferences. He served two elected terms (2007-11) as Chair of the IEEE Test Technology Technical Council (TTTC), and (2011-15) on the Board of Governors of the IEEE Council on Design Automation (CEDA). Dr. Singh was elected Fellow of IEEE in 2002. He is Golden Core member of the IEEE Computer Society.

Viswani D. Agrawal (S'68, M'70, SM'80, F'86, LF'09) is Professor Emeritus in the Electrical and Computer Engineering Department at Auburn University, Alabama. He has over forty years of industry and university experience that includes Bell Labs, Murray Hill, NJ; Rutgers University, New Brunswick, NJ; TRW, Redondo Beach, CA; IIT, Delhi, India; EG&G, Albuquerque, NM; and ATI, Champaign, IL. His areas of work include VLSI testing, low-power design, and microwave antennas. He received a BE degree from the University of Roorkee (renamed Indian Institute of Technology), Roorkee, India, in 1964; ME from the Indian Institute of Science, Bangalore, India, in 1966; and PhD in electrical engineering from the University of Illinois, Urbana-Champaign, in 1971. He has published over 400 papers, has coauthored five books and holds thirteen United States patents. His textbook, Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits, co-authored with Michael Bushnell, was published in 2000. He is the founder and Editor-in-Chief (since 1990) of the Journal of Electronic Testing: Theory and Applications, and a past Editor-in-Chief (1985-87) of the IEEE Design Test of Computers magazine. During 2003-08, he served on the Editorial Board of the IEEE Transactions on VLSI Systems. He is the Founder and Consulting Editor of the Frontiers in Electronic Testing Book Series of Springer. He is a co-founder of the International Conference on VLSI Design, and the International Symposium on VLSI Design and Test, held annually in India. He has served on numerous conference committees and is a frequently invited speaker. He was the Keynote Speaker at the 25th International Conference on VLSI Design, Hyderabad, India, January 2012, invited Plenary Speaker at the 1998 International Test Conference, Washington D.C., and Keynote Speaker at the Ninth Asian Test Symposium, Taiwan, December 2000. During 1989 and 1990, he served on the Board of Governors of the IEEE Computer Society, and in 1994, chaired the Fellow Selection Committee of that Society. He has received nine Best Paper Awards and two Honorable Mention Paper Awards. In 2006, he received the Lifetime Achievement Award of the VLSI Society of India, in recognition of his contributions to the area of VLSI Test and for founding and steering the International Conference on VLSI Design in India. In 1998, he received the Harry H. Goode Memorial Award of the IEEE Computer Society, for innovative contributions to the field of electronic testing, and in 1993, received the Distinguished Alumnus Award of the University of Illinois at Urbana-Champaign, in recognition of his outstanding contributions in design and test of VLSI systems. Dr. Agrawal is a Fellow of the IETE-India (since 1983), a Life Fellow of the IEEE and a Fellow of the ACM (since 2002). He has served on the advisory boards of the ECE Departments at University of Illinois, New Jersey Institute of Technology, and the City College of the City University of New York. See his website – http://www.eng.auburn.edu/ vagrawal.