Journal of Electronic Testing (2021) 37:25–40
https://doi.org/10.1007/s10836-021-05927-3

Estimating Operational Age of an Integrated Circuit

Prattay Chowdhury[1] · Ujjwal Guin[2] · Adit D. Singh[2] · Vishwani D. Agrawal[2]

Received: 27 April 2020 / Accepted: 13 January 2021 / Published online: 7 June 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC part of Springer Nature 2021

Abstract

Recycling of used ICs 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 CMOS chips by measuring I_{DDQ}, the quiescent current from power supply or the total leakage current in steady state. This current decreases as the circuit ages, largely 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 an individual transistor depends upon the operational stress based upon the duration of its ON state. Novelty of our technique is a normalized difference, $\boldsymbol{\Delta I}$, computed from current measurements at two input test patterns and is proposed as a self referencing circuit age indicator. The first pattern is chosen such that its $\boldsymbol{I_{DDQ}}$ is controlled by a large number of minimally stressed PMOS transistors; for the other the $\boldsymbol{I_{DDQ}}$ is controlled by approximately equal number of highly stressed PMOS transistors. The difference between these two $\boldsymbol{I_{DDQ}}$ values increases with the circuit age. This approach requires no hardware modification in the circuit and, hence, can be applied to legacy ICs. Simulation results show that we can reliably identify recycled ICs that have been used for as little as six months.

Keywords Aging · Counterfeit IC · Hardware security · $\boldsymbol{I_{DDQ}}$ · NBTI · Process variation · Operational age · Recycled IC · Residual useful life (RUL).

1 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 lifetime (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.

Responsible Editor: N. Karimi

✉ Ujjwal Guin
ujjwal.guin@auburn.edu

Prattay Chowdhury
prattay.chowdhury@utdallas.edu

Adit D. Singh
adsingh@auburn.edu

Vishwani D. Agrawal
agrawvd@auburn.edu

[1] Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX 75080, USA

[2] Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849, USA

The age of electronic parts comes into play in several ways. Parts from discontinued production lines are sometimes needed to maintain critical infrastructure and defense systems whose operational life exceeds the initially planned deployment period. The chips no longer in production, might be sourced from less reliable third party suppliers. Previously used or recycled integrated circuits (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 [36]. Reportedly, recycled ICs constitute almost 80% of all reported counterfeiting incidents [65]. The reliability of a system becomes questionable because these chips may exhibit poor performance and reduced remaining useful lifetime RUL [27]. These chips may also contain defects and other anomalies due to relatively crude recycling procedures, such as removal of ICs from scrapped printed circuit boards (PCBs) under extremely high temperatures, followed by sanding, repackaging and remarking [25, 65]. These procedures may create latent defects like gate oxide damage, that pass the initial acceptance testing by original equipment manufacturers (OEM) and then cause early life failures in the field [65].

Researchers have proposed methods to identify recycled ICs and prevent them from entering the supply chain [1,

3, 12, 18, 23, 26, 28, 30–33, 35, 40, 44, 65, 73–77]. However, we still need simpler and efficient techniques to isolate 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 to as I_{DDQ}. The method of I_{DDQ} measurement has only been used in the past for fault detection [53].

Our method requires no hardware modification to an existing design and can be applied to a wide variety of chips, including older legacy designs. The proposed method is simple as it only requires 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 is easily performed by laboratory instruments, in a high volume setting commercial automatic test equipment (ATE) can be readily used. This paper reports results from recent research, whose excerpts were announced at a conference [15].

We exploit the change in transistor threshold voltages caused by Negative Bias Temperature Instability (NBTI) [52, 58] due to the operational stress during the chip lifetime in powered up state. Unused chips are expected to display only minimal threshold voltage changes since manufacture, while the PMOS transistors in the 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. Suppose we select two input vectors, one that mostly 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.

Enhancements included in this paper over the conference paper mentioned above [15] are as follows:

- In Section 3, we have replaced the approximate lumped resistance model of I_{DDQ} [15] by an improved model. Here an OFF transistor is modeled by a current source. This technique correctly estimates I_{DDQ} when two or more OFF transistors are stacked. Thus, the results in Section 5 are more accurate than those presented in [15].
- The effects of device sizing and supply voltage variation, not discussed in the previous work [15], are considered in Section 3.1. Hence, Subthreshold leakage current through OFF transistors and gate oxide leakage current through ON transistors are now included in I_{DDQ}. Both components depend on the gate size and supply voltage, and are functions of the threshold voltage of the MOS transistor. This provides the necessary background for the current source model that now replaces the resistance model used in our prior work [15].
- We have added Section 2 on prior work that includes references from the latest research. Newly added Figs. 3, 4 and 5 in Section 4 summarize the procedures for pattern selection, threshold estimation, and recycled IC identification, respectively. Table 3 is added to derive pattern dependent I_{DDQ}. We have updated Tables 4 and 5 based on the new model.

This paper is organized as follows. Prior work on aging and detecting recycled ICs is reviewed in Section 2. Section 3 introduces the modeling of I_{DDQ} for device aging. Section 4 discusses the proposed I_{DDQ} solution to the problems of assessing the device age and detecting recycled ICs. Simulation results are given in Sections 5 and 6 concludes the paper.

2 Prior Work

Majority of reported methods for determining the operational age of an IC require either insertion of hardware or availability of a reference device. The need to eliminate these two requirements has motivated our research. First, we review the existing techniques.

2.1 Test-Oriented Methods

There are existing standards (AS6171, AS5553, CCAP-101 and IDEA-STD-1010), which recommend physical and electrical tests for counterfeit detection [1, 12, 31, 32]. 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 [31]. Electrical tests include Curve Trace, DC Test, AC/ Switching Tests, Full Functional Tests, Burn-in Tests and Temperature Cycling [31]. These tests primarily target 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. [24] proposed a method to select an optimum set of tests considering test cost and time budget. They developed an online tool for determining counterfeit defect coverage (CDC) [54], which was acquired by SAE International. Revision II of standard AS6171 now in progress will incorporate more test methods to increase the confidence in detecting recycled parts.

2.2 Statistical Data Analysis Approaches

Zhang et al. [75] 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) are selected. One uses 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. [35] 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. [76] used dynamic current (I_{DDt}) signature in their proposal. Dogan et al. [18] also use one-class SVM classifier to detect recycled FPGAs. Zheng et al. [77] proposed a characterization method based on extraction of scan path delay signatures for a chip. Guo et al. [30] exploited an embedded SRAM in their approach. They isolated the unstable and most age sensitive cells to devise a recycled IC detection method.

The above methods 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 to service obsolete systems. Variations in electrical parameters over large production volumes, manufactured at different times and possibly in multiple fabrication lines, also limit the effectiveness of these methods.

2.3 Design-for-Anti-Counterfeit (DfAC) Measures

Several Design-for-Anti-Counterfeit (DfAC) measures have been proposed as alternatives for the methods listed above [3, 26, 28, 33, 40, 73, 74]. On-chip ring oscillators (RO) are considered by several researchers to detect recycled ICs. Kim et al. [40] proposed a RO-based silicon odometer. They give two separate designs to monitor the effect of negative bias temperature instability (NBTI) and time-dependent dielectric breakdown (TDDB). Improved versions of the odometer [37] can observe NBTI and hot career injection (HCI) effects. Hofmann et al. [34] 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. [55] 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. [73, 74] proposed a lightweight on-chip sensor using ring oscillators (ROs) to detect recycled ICs. The design contains a reference RO and a stressed RO. A similar concept is used by others [37, 40]. 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. [26, 28] gave an improved design. He et al. [33] proposed another lightweight on-chip design to exploit electromigration-induced aging effect of interconnect wires. The design is compact compared to other designs but depends on the length and quality of interconnect wires. Recently, Guin et al. [3] 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 methods require on-chip hardware and hence cannot be applied to existing ICs already circulating in the market.

2.4 Image Processing Approaches

Recycled IC detection through visual inspection is widely used in standards [1, 31]. The accuracy heavily depends on the available subject matter experts (SMEs) and the quality of the counterfeiting. For improving detection accuracy, Shahbazmohamadi et al. [60] 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 [5, 6, 20, 21]. Training in the 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.

3 Modeling of I_{DDQ} for Device Aging

I_{DDQ} is the current drawn from the power supply of a CMOS circuit in the quiescent state, i.e., when all signals 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 [11, 13, 29, 49].

3.1 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 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 as follows [14, 39]:

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

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 as explained in Section 3.2.

Gate-oxide leakage (I_{ox}) currents can be derived from the gate leakage current density, $J_{G,i}$, given by [71]:

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

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 given by 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 silicon 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 and is expressed 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-silicon 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 Eqs. 1–4, we conclude that sub-thre-shold 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.

3.2 I_{DDQ} Modeling for Logic Gates

Figure 1a shows the transistor-level schematic 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 [70]. Thus, $W/L = 2$ for PMOS transistors M_1 and M_2, as well as for NMOS transistors M_3 and M_4. Figure 1b 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, subthreshold leakage occurs. On the other hand, when the transistor is

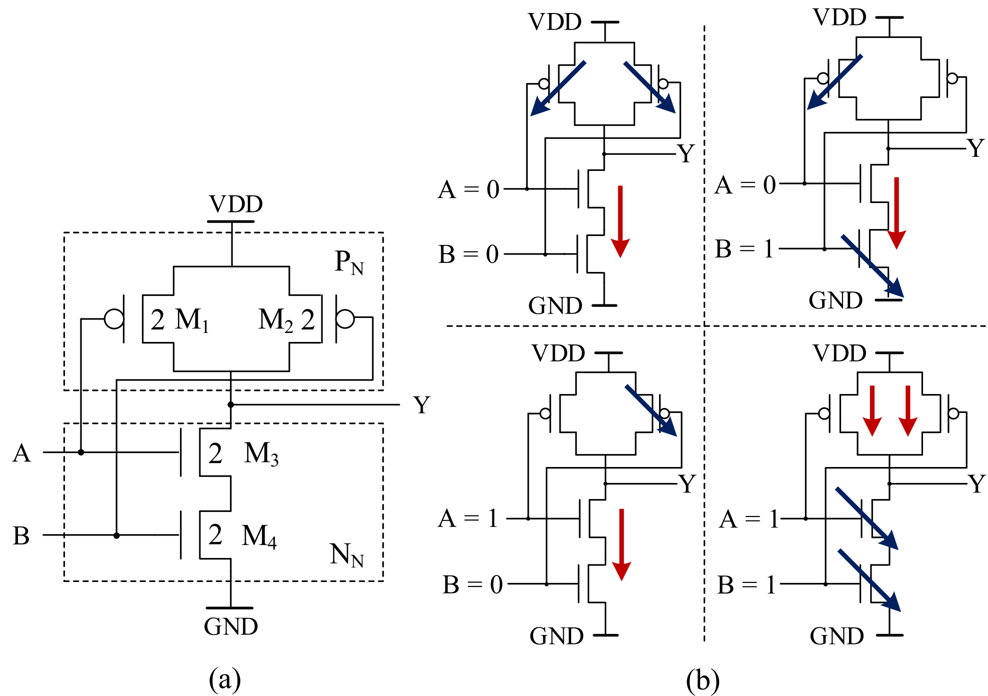

Fig. 1 Two-input NAND gate (**a**), and its I_{DDQ} model (**b**)

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 subthreshold leakage current flows through the stack. In addition, there is gate leakage from M_1 and M_2. The red and blue arrows represent the subthreshold leakage (I_{sub}) and gate leakage (I_{ox}), respectively. Table 1 summarizes the gate leakage and subthreshold leakage for each transistor. Check marks (✓) indicate the presence of leakage components.

Table 2 summarizes the resultant I_{DDQ} for simple gates. The notations used are as follows:

- $I_P^{G^*}$, $I_P^{G^\dagger}$ and I_P^G are 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 are gate leakage currents of NMOS transistors of NAND gate, NOR gate and inverter, respectively. Note that these currents may vary from gate to gate due to different sizing.
- $I_P^{S^*}$, $I_P^{S^\dagger}$ and I_S^G are 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 are subthreshold leakage current of the NMOS transistors of NAND gate, NOR gate and inverter, respectively.
- $I_P^{SS^*}$ is the subthreshold leakage current when two OFF PMOS transistors are in series and $I_N^{SS^*}$ is 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 transistors.

Table 3 summarizes the simulated I_{DDQ} of simple gates (i.e., NAND, NOR and inverter) for various input combinations. The *absolute* value of I_{DDQ} (denoted as I_{DDQ}^A) is obtained from HSPICE simulation using the 32*nm* PTM model [48]. It is the sum of various gate leakage currents and subthreshold current for respective inputs (following the order of Table 2). 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 respective I_{DDQ} components of an inverter. For 00 input vector applied to NAND, the gate leakage current from two PMOS transistors ($2I_P^{G^*}$) is 13.35 pA and NMOS

Table 1 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	-	✓	-	✓	✓	-	✓	-

Table 2 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	$2I_N^{G^*} + 2I_P^{S^*}$	$2I_N^{G^\dagger} + I_P^{SS^\dagger}$	$I_N^G + I_P^S$

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, $I_P^{G^*} = 6.67pA$, gate leakage current from M_4, $I_N^{G^*} = 18.56pA$ and subthrehsold leakage from M_3, $I_N^{S^*} = 2.73pA$. I_{DDQ}^A for other gates and for all other inputs are similar. Current I_{DDQ}^U becomes $I_P^G + 2.5I_N^G + 1.6I_N^S$ as I_N^G for an inverter is 7.56 pA. For input vector 10, there will be no gate leakage for M_3 as no voltage difference exists across the gate and source terminals (both are at VDD). The resultant $I_{DDQ}^A = I_P^{G^*} + I_N^{S^*}$ = (6.67 + 2.25) pA and $I_{DDQ}^U = I_P^G + 1.3I_N^S$. Finally, for input vector 11, $I_{DDQ}^A = 2I_N^{G^*} + 2I_P^{S^*}$ = (37.12 + 5.18) pA and $I_{DDQ}^U = 4.9I_N^G + 2I_P^S$. A NOR gate is analyzed similarly. Non-inverting gates (AND, OR, etc.) can be modeled as respective inverting gates each followed by an inverter.

The analysis can be easily extended for more than three inputs. For example, the total leakage current will be $3I_P^{G*} + I_N^{SSS*}$ for input pattern 000 applied to a 3-input NAND gate, where I_N^{SSS*} is the subthreshold leakage for three series NMOS transistors. Similarly, one can compute the leakage currents for other input combinations. For complex gates, including exclusive-OR or those involving transmission gates, one may use standard cell libraries and simulation tools as discussed in Section 5.

3.3 Impact of Aging and Process Variation on I_{DDQ}

Integrated circuits experience aging in their regular operation, mainly causing increase in transistor threshold voltages. A predominant factor in aging is negative bias temperature instability (NBTI), which occurs in PMOS transistors when they experience stress due to negative bias on the gate terminal [52, 58]. Due to negative bias, interface traps are created at the Si-SiO_2 interface in the PMOS transistor. Releasing the stress can recover some but not all traps, effectively resulting in a net increase of threshold voltage (V_{th}) for the PMOS transistor [57]. 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 that mainly affect NMOS transistors, are positive bias temperature instability (PBTI) and hot carrier injection (HCI). In older

Table 3 Simulated I_{DDQ} for simple gates

Inputs		NAND		NOR		Inverter	
A	B	I_{DDQ}^A	I_{DDQ}^U	I_{DDQ}^A	I_{DDQ}^U	I_{DDQ}^A	I_{DDQ}^U
0	0	(13.35 + 0.67) pA	$2I_P^G + I_N^S/2$	(29.17 + 3.42) pA	$4.4I_P^G + 2I_N^S$	(6.67 + 1.71) pA	$I_P^G + I_N^S$
0	1	(6.67 + 18.56 + 2.73) pA	$I_P^G + 2.5I_N^G + 1.6I_N^S$	(14.58 + 7.56 + 4.47) pA	$2.2I_P^G + I_N^G + 1.7I_P^S$	NA	NA
1	0	(6.67 + 2.25) pA	$I_P^G + 1.3I_N^S$	(7.56 + 3.33) pA	$I_N^G + 1.3I_P^S$	NA	NA
1	1	(37.12 + 5.18) pA	$4.9I_N^G + 2I_P^S$	(15.12 + 0.70) pA	$2I_N^G + I_P^S/3.7$	(7.56 + 2.59) pA	$I_N^G + I_P^S$

technology nodes, PBTI effect, which is the NMOS counterpart of NBTI, was negligible compared to the NBTI effect [38]. However, after the introduction of high-κ and metal gate transistors in sub-45nm technologies, the PBTI effect became more notable [4, 62, 72].

In hot carrier injection (HCI) effect, multiple switching electrons receive enough energy to tunnel through the potential barrier and get trapped in Si-SiO_2 interface near the drain terminal. NMOS transistors are primarily affected by HCI, which has practically no effect on PMOS transistors [64]. Like PBTI, HCI effect is small compared to the NBTI effect in the older technology nodes [38].

We focus on the problem of estimating the amount of aging in 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 still 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 relationship with the threshold voltage (V_{th}), decreases [69]. As a result, the overall I_{DDQ} continues to decrease as a chip is used longer in the field.

Process variation (PV) causes the threshold voltage of transistors to vary from the nominal value [7, 51]. PV can be of two types - inter-die or systematic variation and intra-die or random variation [2, 41]. 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 on a die, arising from random dopant fluctuations, line edge roughness and surface orientation [8, 42, 61].

While the intra-die variation effects on the total I_{DDQ} of the chip tend to cancel out, the inter-die variations cause chip-to-chip difference in I_{DDQ} values. A challenge, therefore, is to determine whether a change in I_{DDQ} has resulted from aging or process variation. Observing the fact that aging always causes the I_{DDQ} to decrease, whereas the process variation may randomly increase or decrease I_{DDQ} for all devices on a chip, we have proposed a solution of normalizing ΔI_{DDQ} (see Section 4). This removes the effect of process variation that uniformly affects all transistors on the chip.

3.4 Non-Uniform Aging in Circuit

In a complex circuit, not all transistors age at the same rate. The aging rates of transistors depend upon controllabilities of signals that determine how often they assume 0 or 1 values. SCOAP is a popular analysis of controllability and observability. It estimates the effort of setting a signal node to a specific value and observing the state of the node at a primary output [11, 22]. However, 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. Algorithms to compute these probabilities from circuit topology [9, 45, 56, 59] basically make trade offs between computational complexity and accuracy. Any of the available tools can be used, though for simplicity, in this work we use logic simulation with random inputs to efficiently estimate signal probabilities with reasonable accuracy.

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 that transistor ON. 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, highlighted in red, as fast aging gates. 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, shown in green, as slow aging gates.

The circuit of Fig. 2 has six primary inputs and we used an exhaustive set of $2^6 = 64$ patterns in this example. For large circuits an exhaustive set would be impractical and instead a random subset of patterns may be used. To keep the error margins in the estimates of signal probabilities within narrow statistical bounds the number of patterns should be 5 to 10 thousand or larger.

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 [47, 66]. It was defined as the difference of I_{DDQ} measured for consecutive patterns of an input sequence. Alternatively, a large number of measurements of I_{DDQ} have been combined into signatures [19, 50] to enhance the fault detection accuracy. In contrast, our ΔI_{DDQ} is obtained for only two carefully

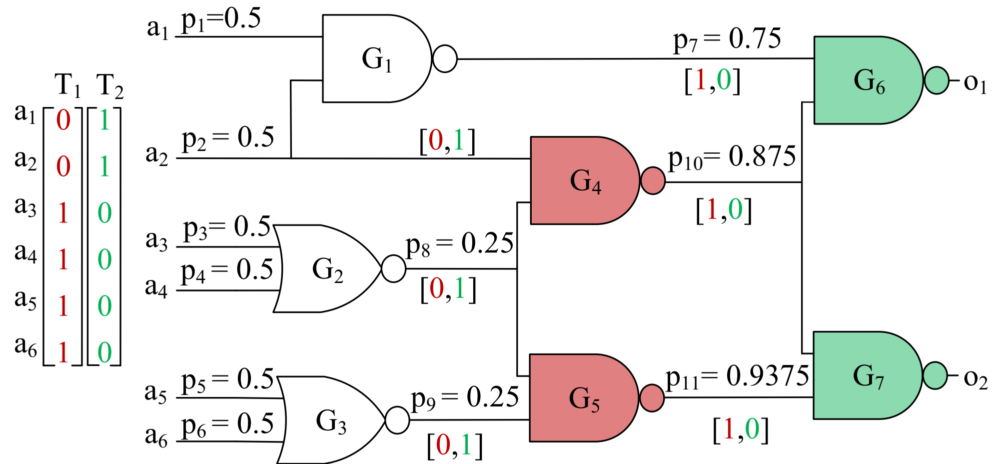

Fig. 2 Test pattern selection for ΔI_{DDQ} measurement using controllability analysis

selected patterns. Our procedure for eliminating the effects of process variation has similarity to the current ratio method [43] used in testing.

Consider two patterns, T_1 and T_2, for which we measure the quiescent currents, I_1 and I_2, respectively. We obtain $\Delta I_{DDQ} = I_2 - I_1$. The following discussion explains the ideas behind these two 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 fast. The patterns T_1 and T_2 are so selected that I_1 is largely controlled by PMOS devices of fast aging gates and I_2 by PMOS devices of slow aging gates. This will result in increasing ΔI_{DDQ} as the chip continues to be used in the field.

For example, consider the circuit of Fig. 2, which also shows patterns T_1 and T_2. As explained earlier, based on signal probabilities gates G_4 and G_5 are fast aging gates and G_6 and G_7 are slow aging. Pattern T_1 applies 11 to fast aging gates so that their PMOS transistors will control the leakage. Note that the dominant component of leakage is the gate leakage as shown in Fig. 1 for input 11 applied to the NAND gate by T_1, which also applies 00 to slow aging gates such that their leakage will be controlled by NMOS transistors. Pattern T_2 creates an opposite situation.

The test consists of application of T_1 and T_2, and measuring I_1 and I_2. These are controlled mostly by PMOS devices in fast aging gates during T_1 and mostly by PMOS devices in slow aging gates during T_2. Then,

$$I_1 = k_1^H \times I_P^H + r_1^H \times I_N \tag{5}$$

$$I_2 = k_2^L \times I_P^L + r_2^L \times I_N \tag{6}$$

Where I_P and I_N are currents that depend on the gate leakage of PMOS and NMOS transistors as shown in Table 3. "H" and "L" refer to the fast and slow aging conditions created by T_1 and T_2. Coefficients k_1^H, r_1^H, k_2^L and r_2^L depend on the specific signal states and gate structures in the circuit.

Note that $k_1^H \times I_P^H$ will reduce significantly with age as it comes mostly from fast aging gates, whereas $k_2^L \times I_P^L$ will remain relatively unchanged 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 $r_1^H \times I_N$ and $r_2^L \times I_N$ will remain constant, because I_N is controlled by NMOS transistors.

The difference between these two currents is denoted by ΔI_{DDQ} expressed as follows:

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

In Eq. 7, ΔI_{DDQ} has two components derived, respectively, from the pull-up P-network (ΔI_P) and pull-down N-network (ΔI_N). Our objective for selecting two patterns (T_1 and T_2) is to maximize 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 satisfy $r_2^L \approx r_1^H$.

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 reasonably large number of gates. In our simulation, we have considered four corner cases of process variation. We define normalized ΔI_{DDQ} as follows:

$$\Delta I = \frac{I_2 - I_1}{I_2 + I_1} \times 100\% \tag{8}$$

Another benefit of normalization is to cancel out the influence of any phenomenon that identically affects all measurements. A typical case is electromigration [16], which increases the interconnect resistance with usage. Its effect on power and ground interconnects will reduce both I_1 and I_2 in similar proportion, leaving ΔI unaffected. We will use ΔI to detect recycled ICs.

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 [67].

4 A Method for Detecting Recycled ICs

The proposed flow for detecting recycled ICs is based on the change in ΔI_{DDQ}, which progressively increases as 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. To characterize, we will derive two test patterns for I_{DDQ} measurement and a threshold value for ΔI_{DDQ}. 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.

4.1 Characterization

The first stage in the proposed method is to characterize the chip. This is done by the chip manufacturer through pattern selection and threshold calculation. We find 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. We then determine a threshold value, ΔI_T, which will be used as a reference to make a decision in the testing stage.

We use a simulation based search for T_1 and T_2 so that the difference $I_2 - I_1$ is maximized as age of the device increases. To illustrate the concept of random sample-based search, adopted here for simplicity, we conduct the search over a randomly generated subset of all possible input patterns. As the size of this subset increases, the optimality of our search would approach closer to that of the global search. According to the theory of random sampling routinely applied to deal with high complexity, e.g., in digital testing [11], once a sample size exceeds 1,000, further benefit of enlarging the sample becomes small. We, therefore, use a sample of 2,000 random patterns. The pattern selection process of Fig. 3 works as follows:

1. Two thousand randomly generated input patterns are used to select patterns T_1 and T_2 that may result in maximal aging degradation (highest ΔI from Eq 8) when an IC gets used in the field. Since 2,000 patterns is an adequate sample size to statistically represent the whole input pattern set, a larger sample may give only marginal improvement in the result at a greater computing cost.
2. We use HSPICE to simulate the circuit, and determine I_{DDQ} for all 2,000 input patterns. Simulation details are given in Section 5. The current for ith pattern is denoted as $I^{(0)}[i]$, where the superscript refers to the time the device has been aged through. Alternatively, this characterization can be done in a foundry by measuring the I_{DDQ} for a new chip.
3. Aging simulation is performed by Synopsys MOSRA (see Section 5) to find two patterns that cause maximum degradation. We perform aging for six months at 25 °C temperature and 1 volt nominal supply voltage. After aging, I_{DDQ} for the same 2,000 test patterns is determined. For ith pattern I_{DDQ} of an aged device is represented as $I^{(t)}[i]$. Alternatively, a manufacturer can perform an accelerated aging at the foundry.
4. We define aging degradation $\delta[i]$ of ith pattern as percentage change in its I_{DDQ} due to six month usage. It is calculated as:

$$\delta[i] = \frac{I^{(0)}[i] - I^{(t)}[i]}{I^{(0)}[i]} \times 100 \quad \text{percent} \tag{9}$$

5. Finally, Algorithm 1 is applied to select two test patterns T_1 and T_2.

Algorithm 1 Test pattern selection.

```
input : Circuit netlist {C}, randomly selected 2,000 input
        test patterns (TPs), aging degradation (δ) for 2,000
        TPs ;
output: Two test patterns {T1, T2} ;
1  begin
2    A ⟵ Max(δ), B ⟵ Min(δ);
3    j, l ⟵ 1;
4    for i ← 1 to 2,000 do
5      if δ[i] ≥ 0.95×A then
6        L^H[j] ⟵ TP[i] ;
7        r^H[j] ⟵ calculate_r(C, TP[i]);
8        j ⟵ j + 1 ;
9      end
10     if δ[i] ≤ 1.05×B then
11       L^L[l] ⟵ TP[i] ;
12       r^L[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) ← |(r^L[i] − r^H[m])|;
19     end
20   end
21   [r, c] ⟵ min_element(D);
22   T1 ⟵ L1[r], T2 ⟵ L2[c];
23 end
```

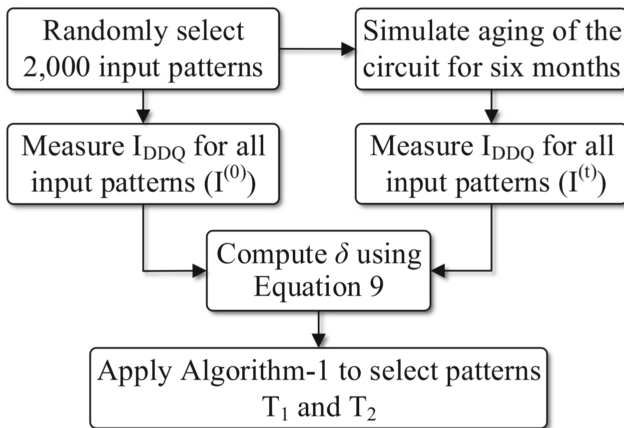

Fig. 3 Proposed pattern selection process during characterization

As defined by Eq. 7, the difference ΔI_{DDQ} for test pattern-pair, T_1 and T_2, has two components, ΔI_P, the part controlled by PMOS transistors, and ΔI_N, the part controlled by NMOS transistors. Algorithm 1 selects T_1 and T_2 such that ΔI_P is maximized (largest degradation in ΔI_{DDQ} from aging of PMOS transistors; see Eq. 7) and ΔI_N is minimized (lowest impact of process variation on ΔI_{DDQ} from NMOS transistors). The algorithm takes the circuit netlist $\{C\}$, 2,000 randomly selected input test patterns $\{TP\}$, and their previously calculated/measured aging sensitivities $\{\delta\}$ (see Eq. 9) as inputs, and returns two test patterns (T_1 and T_2) as outputs.

As explained in the discussion following Eq. 7, the selection criteria for the required pattern-pair are to maximize ΔI_P and minimize ΔI_N. A simple brute-force approach would examine ${}^{2000}C_2 = \frac{2000(2000-1)}{2} = 1,999,000$ unique pairs of patterns. Instead, Algorithm 1, which has much lower complexity, first selects two small groups of patterns, one with largest aging influence and the other with least aging influence. Next, it draws one pattern from each group such that the pair meets the required criteria.

The algorithm starts by finding the maximum and minimum values (A and B) of aging degradation δ among all patterns in $\{TP\}$ (Line 2). Two groups of patterns $\{L_1\}$ and $\{L_2\}$ are then selected from $\{TP\}$ (Lines 4-15). $\{L_1\}$ contains patterns with top 5% aging degradation and $\{L_2\}$ contains those with bottom 5% aging degradation. The 5% degradation range, although somewhat arbitrary, reduces the computational complexity for reasonable program execution. One can select other values depending on the available computational resources. The coefficient r_1^H for I_N in Eq. 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 simulator [68] to obtain the internal node values. Finally, r_1^H is calculated using Table 3. Similarly, r_2^L, which is the coefficient of I_N in Eq. 6 is computed using *calculate_r* function (Line 12). A matrix D is computed, where each element is the difference of r_1^H and r_2^L (Line 16-19). The function, *min_element()*, is used to obtain the row and column indexes r and c, respectively, of the minimum element of matrix D (Line 21). These indexes are used to select the desired test patterns, T_1 and T_2.

The second part of the characterization process calculates a threshold value to determine whether or not a chip is recycled. As I_{DDQ} varies with the process variation (see Section 3.3), it is necessary to consider all corner cases of process variation. Four cases are modeled by 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 the circuit with 10% decrease in V_{th} for all MOS transistors. *Netlist-4* is the circuit with 10% increase in V_{th} for all PMOS transistors, and 10% decrease in V_{th} for all NMOS transistors.

To account for intra-die process variation, random variations of 5% in threshold voltages are added to the four netlists [2, 42]. Thus, the nominal value V_{th} of threshold voltage for a transistor on the chip is modified by an independent Gaussian random variable with mean V_{th} and standard deviation $\sigma = 0.05V_{th}$. Based on the process foundry information, the percentage for σ can be changed. However, as pointed out in Section 3.4, the resulting fluctuations of individual gate I_{DDQ} values tend to average out when summed up for a large number of gates of a circuit. Hence, the intra-die process variation, although it provides realism to our simulation, has no significant effect on the chip I_{DDQ} or aging assessment.

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

1. Create separate netlists for four process corners.
2. Apply input patterns T_1 and T_2 to all four netlists and measure I_{DDQ}.
3. Calculate normalized I_{DDQ} and ΔI for all four netlists.
4. The maximum value of ΔI found in Step 3 is selected 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 new (unused) chips. In the foundry, two previously selected input patterns, T_1 and T_2, can be applied to a reasonably large number of ICs and ΔI measured. The threshold value is then the maximum of all ΔI's.

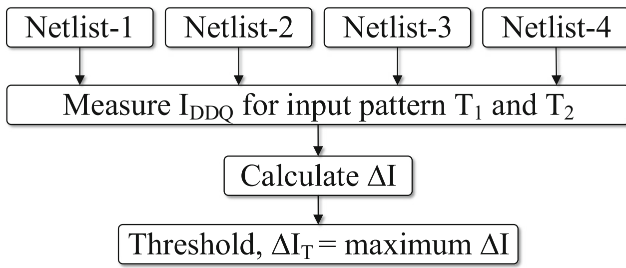

Fig. 4 Calculation of threshold ΔI_T

4.2 Test for Identifying Recycled ICs

The test for detecting recycled ICs consists of application of the two patterns, T_1 and T_2, derived in the characterization phase, which also determines a threshold ΔI_T (see Section 4.1). The proposed flow of the detection method is shown in Fig. 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 laboratory instrument or an automatic test equipment (ATE).
3. ΔI is calculated using Eq. 8.
4. If ΔI is greater than ΔI_T, the chip is classified as a recycled chip. Otherwise, it is a new chip.

5 Results and Discussion

We performed aging simulation for several ISCAS'85 benchmark circuits [10]. This was done through MOS Reliability Analysis (MOSRA) in HSPICE integrated circuit reliability analysis tool available from Synopsys [67]. Synopsys 32*nm* technology library [63] was used. MOS transistor parameters were based on 32*nm* low power metal gate Predictive Technology Model (PTM) [48]. The aging simulation assumed 25 °C temperature and a nominal 1 volt

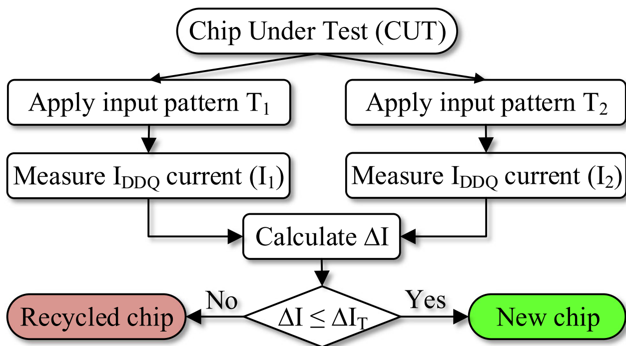

Fig. 5 Proposed flow for detecting recycled ICs using ΔI

Table 4 I_{DDQ} for new (unused) circuits

Usage	Bench-	Netlist-1			Netlist-2			Netlist-3			Netlist-4			ΔI_T % =
Months	Marks	I_1 nA	I_2 nA	ΔI %	I_1 nA	I_2 nA	ΔI %	I_1 nA	I_2 nA	ΔI %	I_1 nA	I_2 nA	ΔI %	$max(\Delta I)$
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	209.80	1.21	193.92	199.23	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
	c1355	213.55	221.28	1.78	166.31	172.51	1.83	235.51	243.37	1.64	223.12	231.09	1.75	1.83
	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
	c2670	268.71	289.97	3.81	179.76	193.88	3.78	585.75	633.82	3.94	398.39	430.87	3.92	3.94
	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
	c5315	405.93	432.12	3.13	259.46	275.19	2.94	856.73	914.25	3.25	577.58	613.88	3.05	3.25

Table 5 I_{DDQ} for used circuits

Usage	Bench-	Netlist-1			Netlist-2			Netlist-3			Netlist-4			$min(\Delta I)$
Months	Marks	$I_1\ nA$	$I_2\ nA$	ΔI %	$I_1\ nA$	$I_2\ nA$	ΔI %	$I_1\ nA$	$I_2\ nA$	ΔI %	$I_1\ nA$	$I_2\ nA$	ΔI %	%
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
	c1355	172.72	186.98	3.96	133.55	145.24	4.19	190.53	204.98	3.65	180.95	194.88	3.71	3.65
	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
	c2670	222.03	246.33	5.18	149.04	165.20	5.14	483.28	539.13	5.46	330.21	366.74	5.24	5.14
	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
	c5315	341.98	380.47	5.33	216.94	241.17	5.29	721.65	806.54	5.55	484.77	540.01	5.39	5.29
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
	c1355	165.47	181.18	4.53	127.94	140.74	4.76	182.53	198.11	4.09	173.71	189.03	4.22	4.09
	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
	c2670	211.88	239.04	6.02	141.74	159.88	6.01	461.86	522.59	6.17	314.13	355.25	6.14	6.01
	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
	c5315	322.43	367.36	6.51	205.59	233.43	6.34	687.37	784.14	6.58	461.63	524.91	6.41	6.34

supply voltage. The benchmark circuits were synthesized in Synopsys Design Compiler [17] and converted into HSPICE netlist by Synopsys IC Validator [46]. Synopsys VCS [68] provided the gate level analysis in Algorithm 1.

Simulation results for eight benchmark circuits are given in Tables 4 and 5. Table 4 contains I_{DDQ} for both patterns for each netlist when the circuit is new. The first column gives the usage period of the chip in months. 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 Eq. 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 representing 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 applies to all other benchmark circuits.

Table 5 summarizes I_{DDQ} data after six months and one year of aging. The columns of this table are similar to those in Table 5, except the last one. Column 15 here gives the minimum values of ΔI obtained from the four netlists. We can detect a recycled IC if the value of Column 15 is greater than ΔI_T (Column 15 of Table 4). For c432, after six months of aging, ΔI values are 6.07%, 6.09%, 5.89% and 6.37%, respectively. The minimum value 5.89% is greater than its threshold ($\Delta I_T = 3.45\%$). Similar analysis applies to other benchmark circuits. Note that ΔI will further increase when the circuit is aged beyond one year.

The temperature has roles in aging and its measurement. In our proposed technique, the actual temperature during current measurements may differ from 25 °C assumed in the analysis. However, patterns T_1 and T_2 are applied in quick succession, and current measurements are likely to be conducted at the same temperature. As a result, the increase or decrease in I_1 and I_2 will be in the same proportion. Thus, the effect of temperature variation will cancel out in the normalized ΔI, according to Equation 8. The other effect of temperature is related to the rate of aging degradation in the device itself when it is used at temperatures different from the nominal 25 °C. It is well known that aging becomes faster at elevated temperatures, a phenomenon used in accelerated testing or burn-in [11]. Since our scale of age is calibrated through simulation at 25 °C, the age estimated by the two-pattern test will be the real (accelerated) age and not the calendar age.

6 Conclusion

The two-pattern ΔI_{DDQ} test can effectively identify IC usage as short as six months. This is significant because, in general, a majority of recycled chips circulating in the market have been used for several years. An advantage of the 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 implemented on 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 in an IC varies from gate to gate, 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 exercise.

Aging and counterfeit detection of sequential circuits are definitely of interest. Many clocked synchronous circuits use the scan methodology for testing [11]. For such circuits, any pattern can be applied to the combinational part. Thus, two patterns can be generated for the combinational logic using the method described here. However, leakage through the flip-flops with the clock in the inactive state should be included. For non-scan synchronous circuits and asynchronous circuits, the generation and application of a suitable pair of patterns are not as straightforward and require research.

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 recycled IC detection will work for large circuits should be investigated. Intuitively, adding aging effects from a large number of gates may benefit the detection capability. Besides analyzing large circuits, our plans include actual hardware tests using the available Advantest T2000GS ATE at Auburn University.

The last column of Table 4 shows that not all circuits are affected by process variation in the same way. Future investigation on structure and function dependence of aging may lead to design principles that minimize process variability.

It is reasonable for the future to assume that the two-pattern aging test could become a part of the device specification. In that case, the test may be generated when the design is completed by the design or test engineer who would have access to the design and technology details, libraries, and simulation tools. For the old legacy devices, some perhaps no longer in production, one must face the challenge to dig out from a design house or foundry the information needed to generate the aging tests.

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

References

1. Acceptability of Electronic Components Distributed in the Open Market (2017). http://www.idofea.org/products/118-idea-std-1010b
2. Al Tarawneh Z (2011) The Effects of Process Variations on Performance and Robustness of Bulk CMOS and SOI Implementations of C-Elements. Ph.D. Thesis, Newcastle University
3. Alam M, Chowdhury S, Tehranipoor M, Guin U (2018) Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures. In: Proc. IEEE Int. Symposium on Hardware Oriented Security and Trust (HOST)
4. Amrouch H, Mishra S, van Santen V, Mahapatra S, Henkel J (2017) Impact of BTI on dynamic and static power: From the physical to circuit level. In: Proc. IEEE International Reliability Physics Symposium (IRPS)
5. Asadizanjani N, Dunn N, Gattigowda S, Tehranipoor M, Forte D (2016) 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, pp 1–8
6. Asadizanjani N, Tehranipoor M, Forte D (2017) Counterfeit electronics detection using image processing and machine learning. J Phys Conf Ser 787(1):012–023
7. Asenov A (2007) Simulation of statistical variability in nano MOSFETs. In: Proc. IEEE Symposium on VLSI Technology, pp 86–87
8. Asenov A, Kaya S, Brown AR (2003) Intrinsic parameter fluctuations in decananometer MOSFETs introduced by gate line edge roughness. IEEE Trans Electron Dev 50(5):1254–1260
9. Brglez F (1984) On Testability Analysis of Combinational Networks. In: Proc. International Symp. Circuits and Systems, pp 221–225
10. Brglez F, Fujiwara H (June 1985) A Neutral Netlist of 10 Combinational Benchmark Circuits and a Targeted Translator in FORTRAN, Special Session on ATPG and Fault Simulation. In: Proc. 1985 IEEE Int. Symp. on Circuits and Systems (ISCAS'85), pp 663–698. Benchmark circuit netlists are available at http://www.pld.ttu.ee/~maksim/benchmarks/iscas85/verilog/
11. Bushnell ML, Agrawal VD (2000) Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits. Springer
12. Certification for Counterfeit Components Avoidance Program (2011). http://www.cti-us.com/pdf/CCAP101Certification.pdf
13. Chakravarty S, Thadikaran PJ (1997) Introduction to IDDQ testing. Springer
14. Chandrakasan AP, Bowhill WJ, Fox F (2000) Design of high-performance microprocessor circuits. Wiley-IEEE Press
15. Chowdhury P, Guin U, Singh AD, Agrawal VD (2019) Two-pattern ΔI_{DDQ} test for recycled IC detection. In: Proc. 32nd International Conference on VLSI Design, pp 82–87
16. Christou A (1993) Electromigration and Electronic Device Degradation. Wiley, New York
17. DC Ultra: Concurrent Timing, Area, Power, and Test Optimization, https://www.synopsys.com/implementation-and-signoff/rtl-synthesis-test/dc-ultra.html
18. Dogan H, Forte D, Tehranipoor MM (2014) Aging analysis for recycled FPGA detection. In: Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp 171–176
19. Gattiker AE, Maly W (1997) Current Signatures: Application. In: Proc. International Test Conference, pp 156–165
20. Ghosh P, Chakraborty RS (2017) Counterfeit ic detection by image texture analysis. In: Proc. Euromicro Conference on Digital System Design (DSD). IEEE, pp 283–286
21. Ghosh P, Chakraborty RS (2018) Recycled and remarked counterfeit integrated circuit detection by image processing based package texture and indent analysis. IEEE Trans Ind Inf 15(4):1966–1974
22. Goldsein LH (September 1979) Controllability/Observability Analysis of Digital Circuits. IEEE Trans Circ Syst CAS-26(9):685–693
23. Guin U, Asadizanjani N, Tehranipoor M (2019) Standards for hardware security. GetMobile: Mob Comput Commun 23(1):5–9
24. Guin U, DiMase D, Tehranipoor M (2014) A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment. J Electron Test 30(1):25–40
25. Guin U, DiMase D, Tehranipoor M (2014) Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead. J Electron Test 30(1):9–23
26. Guin U, Forte D, Tehranipoor M (2016) Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling. IEEE Trans Very Large Scale Integr (VLSI) Syst 24(4):1233–1246
27. Guin U, Huang K, DiMase D, Carulli JM, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. Proc IEEE 102(8):1207–1228
28. Guin U, Zhang X, Forte D, Tehranipoor M (2014) Low-cost On-Chip Structures for Combating Die and IC Recycling. In: Proc. of ACM/IEEE Design Automation Conference
29. Gulati RK, Hawkins CF (eds.) (1993) I_{DDQ} Testing of VLSI Circuits. Springer
30. Guo Z, Rahman MT, Tehranipoor MM, Forte D (2016) A zero-cost approach to detect recycled SoC chips using embedded SRAM. In: Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp 191–196
31. G-19A Test Laboratory Standards Development Committee (2016) Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. https://saemobilus.sae.org/content/as6171
32. G-19CI Continuous Improvement (2009) Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition. https://saemobilus.sae.org/content/as5553
33. He K, Huang X, Tan SXD (2015) EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs. In: Proc. IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp 146–151
34. Hofmann K, Reisinger H, Ermisch K, Schlünder C, Gustin W, Pompl T, Georgakos G, von Arnim K, Hatsch J, Kodytek T et al (2010) Highly accurate product-level aging monitoring in 40nm CMOS. In: Proc. Symposium on VLSI Technology, pp 27–28
35. Huang K, Carulli JM, Makris Y (2012) Parametric counterfeit IC detection via Support Vector Machines. In: Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems, pp 7–12
36. IHS iSuppli (2011) Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market. http://press.ihs.com/press-release/design-supply-chain/top-5-most-counterfeited-parts-represent-169-billion-potential-cha
37. Keane J, Wang X, Persaud D, Kim CH (2010) An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB. IEEE J Solid-State Circ 45(4):817–829
38. Kiamehr S, Amouri A, Tahoori MB (2011) Investigation of NBTI and PBTI induced aging in different LUT implementations. In: Proc. International Conference on Field-Programmable Technology, pp 1–8

39. Kim NS, Austin T, Baauw D, Mudge T, Flautner K, Hu JS, Irwin MJ, Kandemir M, Narayanan V (2003) Leakage current: Moore's law meets static power. Computer 36(12):68–75
40. Kim T-H, Persaud R, Kim CH (2008) Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits. IEEE J Solid-State Circ 43(4):874–880
41. Kuhn KJ, Giles MD, Becher D, Kolar P, Kornfeld A, Kotlyar R, Ma ST, Maheshwari A, Mudanai S (2011) Process Technology Variation. IEEE Trans Electron Dev 58(8):2197–2208
42. Kuhn K, Kenyon C, Kornfeld A, Liu M, Maheshwari A, Shih W, Sivakumar S, Taylor G, VanDerVoorn P, Zawadzki K (2008) Managing Process Variation in Intel's 45nm CMOS Technology. Intel Technol J 12(2)
43. Maxwell P, O'Neill P, Aitken R, Dudley R, Jaarsma N, Quach M, Wiseman D (1999) Current Ratios: A Self-scaling Technique for Production IDDQ Testing. In: Proc. International Test Conference, pp 738–746
44. Miller M, Meraglia J, Hayward J (2012) Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts. In: Proc. SAE Aerospace Electronics and Avionics Systems Conference
45. Parker KP, McCluskey EJ (June 1975) Probabilistic Treatment of General Combinational Networks. IEEE Trans Comput C-24(6):668–670
46. Physical Verification: Using IC Validator, https://www.synopsys.com/implementation-and-signoff/physical-verification.html
47. Powell TJ, Pair J, John MS, Counce D (2000) Delta Iddq for Testing Reliability. In: Proc. 18th IEEE VLSI Test Symposium (VTS), Montreal, pp 439–443
48. Predictive Technology Model (PTM), http://ptm.asu.edu/
49. Rajsuman R (2000) Iddq testing for CMOS VLSI. Proc IEEE 88(4):544–568
50. Rao L, Bushnell ML, Agrawal VD (November 2007) Graphical I_{DDQ} Signatures Reduce Defect Level and Yield Loss. IEEE Trans Very Large Scale Integr (VLSI) Syst 15(11):1245–1255
51. Rao R, Srivastava A, Blaauw D, Sylvester D (2003) Statistical estimation of leakage current considering inter-and intra-die process variation. In: Proc. International Symposium on Low Power Electronics and Design, pp 84–89
52. Reddy V, Krishnan AT, Marshall A, Rodriguez J, Natarajan S, Rost T, Krishnan S (2005) Impact of negative bias temperature instability on digital circuit reliability. Microelectron Reliab 25(1):31–38
53. Sabade SS, Walker DMH (April 2004) I_{DDX}-based Test Methods: A Survey. ACM Trans Des Autom Electron Syst 9(2):159–198
54. SAE Counterfeit Defect Coverage Tool, http://cdctool.sae.org/
55. Saneyoshi E, Nose K, Mizuno M (2010) A precise-tracking NBTI-degradation monitor independent of NBTI recovery effect. In: IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), pp 192–193
56. Savir J, Ditlow GS, Bardell PH (January 1984) Random Pattern Testability. IEEE Trans Comput C-33(1):79–90
57. Schroder DK (2007) Negative bias temperature instability: What do we understand? Microelectron Reliab 47(6):841–852
58. Schroder DK, Babcock JA (2003) Negative bias temperature instability: Road to cross in deep submicron silicon semiconductor manufacturing. J Appl Phys 94(1):1–18
59. Seth SC, Agrawal VD (1989) A New Model for Computation of Probabilistic Testability in Combinational Circuits. Integr Vlsi J 7:49–75
60. Shahbazmohamadi S, Forte D, Tehranipoor M (2014) 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 , pp 55
61. Shin C, Sun X, Liu T-JK (2009) Study of random-dopant-fluctuation (RDF) effects for the trigate bulk MOSFET. IEEE Trans Electron Dev 56(7):1538–1542
62. Stathis JH, Wang M, Zhao K (2010) Reliability of advanced high-k/metal-gate n-FET devices. Microelectron Reliab 50(9-11):1199–1202
63. Synopsys 32/28nm Generic Library for Teaching IC Design, https://www.synopsys.com/community/universityprogram/teaching-resources.html
64. Takeda E, Nakagome Y, Kume H, Suzuki N, Asai SHOJIRO (1983) Comparison of characteristics of n-channel and p-channel MOSFET's for VLSI's. IEEE Trans Electron Dev 30(6):675–680
65. Tehranipoor MM, Guin U, Forte D (2015) Counterfeit Integrated Circuits: Detection and Avoidance. Springer
66. Thibeault C (1997) A Novel Probabilistic Approach for IC Diagnosis Based on Differential Quiescent Current Signatures. In: Proc. 15th IEEE VLSI Test Symposium, pp 80–85
67. Tudor B, Wang J, Liu W, Elhak H (2011) MOS device aging analysis with HSPICE and Customsim. Synopsys, White Paper
68. VCS: Industry's Highest Performance Simulation Solution, https://www.synopsys.com/verification/simulation/vcs.html
69. Wang W, Reddy V, Yang B, Balakrishnan V, Krishnan S, Cao Y (2008) Statistical prediction of circuit aging under process variations. In: Proc. Custom Integrated Circuits Conference (CICC), pp 13–16
70. Weste NHE, Harris D (2015) CMOS VLSI design: a circuits and systems perspective. Pearson Education India
71. Yeo Y-C, King T-J, Hu C (2003) MOSFET gate leakage modeling and selection guide for alternative gate dielectrics based on leakage considerations. IEEE Trans Electron Dev 50(4):1027–1035
72. Zafar S, Kim Y, Narayanan V, Cabral C, Paruchuri V, Doris B, Stathis J, Callegari A, Chudzik M (2006) 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, pp 23–25
73. Zhang X, Tehranipoor M (2014) Design of on-chip lightweight sensors for effective detection of recycled ICs. IEEE Trans Very Large Scale Integr (VLSI) Syst 22(5):1016–1029
74. Zhang X, Tuzzio N, Tehranipoor M (2012) Identification of recovered ICs using fingerprints from a light-weight on-chip sensor. In: Proc. IEEE-ACM Design Automation Conference
75. Zhang X, Xiao K, Tehranipoor M (2012) Path-delay fingerprinting for identification of recovered ics. In: Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp 13–18
76. Zheng Y, Basak A, Bhunia S (2014) CACI: Dynamic current analysis towards robust recycled chip identification. In: Proceedings of the 51st Annual Design Automation Conference, pp 1–6
77. Zheng Y, Wang X, Bhunia S (2015) SACCI: Scan-based characterization through clock phase sweep for counterfeit chip detection. IEEE Trans Very Large Scale Integr (VLSI) Syst 23(5):831–841

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Prattay Chowdhury received his BSc degree from the Department of Electrical and Electronics Engineering, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 2016. He received his MS degree from the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL, USA, in 2019. He is currently pursuing his PhD degree at the Electrical and Computer Engineering department, University of Texas at Dallas. He is a Student Member of the IEEE.

Ujjwal Guin 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 BE degree from the Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, Howrah, India, in 2004 and his MS 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, Blockchain, 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 tool, 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 G-19A Test Laboratory Standards Development Committee, and G-32 Cyber Physical Systems Security Committee. He is a member of the IEEE and ACM.

Adit D. Singh received the BTech from IIT Kanpur, and the MS and PhD 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 a Golden Core member of the IEEE Computer Society. Currently, he is an Editor of the Journal of Electronic Testing: Theory and Applications.

Viswani D. Agrawal is Professor Emeritus at Auburn University, Alabama, USA, where prior to retiring in September 2016 he was the James J. Danaher Professor of Electrical and Computer Engineering. He has over 45 years of industry and university experience, working at 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 obtained his BE degree from the Indian Institute of Technology (IIT), 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 coauthored over 450 papers and five books. He holds 13 US patents. His textbook, Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits (Springer), co-authored with M. L. 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. 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 VLSI Design and Test Symposium, held annually in India. 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 ten Best Paper Awards and two Honorable Mention Paper Awards. He is the recipient of the 2014 James Monzel Award from the IEEE North Atlantic Test Workshop, the 2012 Lifetime Contribution Medal from the Test Technology Technical Council of the IEEE Computer Society, and the 2006 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. He has received two Distinguished Alumnus Awards, from Indian Institute of Technology, Roorkee in 2019 and University of Illinois at Urbana-Champaign in 1993. Dr. Agrawal is a Fellow of the IEEE, ACM and IETE. He has served on Advisory Boards of ECE Departments of the University of Illinois at Urbana- Champaign, New Jersey Institute of Technology, and the City College of the City University of New York. See his website at http://www.eng.auburn.edu/~vagrawal.