2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)

Two-Pattern ΔI_{DDQ} Test for Recycled IC Detection

Prattay Chowdhury, Ujjwal Guin, Adit D. Singh and Vishwani D. Agrawal
Dept. of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849, USA
Email: {prattay, ujjwal.guin, singhad, agrawvd}@auburn.edu

***Abstract*—Increasing numbers of used and recycled integrated circuits (ICs) being fraudulently marketed as new, is a serious concern for government and industry because these chips can pose serious reliability problems. This paper presents a novel approach to detect recycled chips already in circulation in the market by measuring I_{DDQ}, the quiescent (steady state) current from power supply. The measured I_{DDQ} is the leakage from off transistors, and decreases as the circuit ages due to the increase in the magnitude of the transistor threshold voltages caused by negative/positive bias temperature instability (NBTI/PBTI). To eliminate the influence of chip-to-chip process variation, we use a normalized difference, ΔI, from measurements at two input test patterns. Focusing on NBTI, in one pattern I_{DDQ} is controlled by a large number of minimally stressed PMOS transistors and in the other it is controlled by an equal number of heavily stressed PMOS transistors. The new approach requires no hardware addition or modification to the design. A standard IC tester can be used to measure I_{DDQ} and identify these recycled parts. Our simulation results show that we can detect recycled ICs that have been used for as little as six months.**

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

I. Introduction

The recycled integrated circuits (ICs) pose a severe threat to the electronic component supply chain and call for urgent solutions to detect them. Parts from old production lots are commonly needed to maintain critical infrastructure and defense systems whose operational life often extends beyond 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 easily enter the supply chain due to the lack of effective detection and avoidance methods. A report from Information Handling Services Inc. shows that these fake ICs represent a potential annual risk of $169 billion in the global supply chain, with the number continuing to increase each year [1]. Note that recycled ICs constitute almost 80% of all the reported counterfeiting incidents [2]. The reliability of a system becomes questionable if recycled chips are used in it because these chips often exhibit poor performance and significantly reduced remaining useful lifetime (RUL) [3]. In addition, these chips may also display defects and other anomalies caused by the crude recycling processes commonly employed, typically consisting of removal of the ICs from scrapped printed circuit boards (PCBs) under extremely high temperatures, followed by sanding, repackaging and remarking [2], [4]. The recycling process can also create latent defects that pass the initial acceptance testing by original equipment manufacturers (OEM) but are susceptible to early life failures in the field [2].

Researchers have proposed several detection and avoidance techniques to detect recycled ICs and prevent them from entering the supply chain. These approaches are broadly classified into four categories: (i) There are several standards (AS6171, AS5553, CCAP-101 and IDEA-STD-1010) in use, which recommend physical and electrical tests for counterfeit detection [5]–[8]. These tests primarily focus on detecting defects and anomalies of recycled parts. However, excessive test time and cost, lack of automation, and particularly low detection confidence, limit their effectiveness in detecting recycled ICs. (ii) Statistical data analysis approaches have been proposed [9]–[14]. These solutions require a large number of new circuits from different production runs to gather statistically sufficient electrical data on unused parts to reliably identify recycled ICs. This data may not always be available due to the typically limited access to new parts when sourcing chips to service obsolete systems. Variations in electrical parameters over large production volumes, often manufactured in multiple fabrication lines, also limits the effectiveness of this approach. (iii) Different design-for-anti-counterfeit (DFAC) measures have been proposed as an alternative to the conventional test methods [15]–[21]. Unfortunately, these solutions cannot be applied to unprotected ICs already in use and circulating in the market. (iv) Finally, DNA markings are now commercially available and provide traceability for electronic parts [22]. However, a complex authentication process, excessive implementation and test cost limit its application in practice [23].

In this paper, we propose a novel method of detecting aged recycled ICs by measuring I_{DDQ}. This method requires no hardware modification to the existing design and can be applied to a wide variety of chips, including existing designs already circulating in the market. The proposed method is simple, straightforward, and accurate. Simulation results show that we can accurately detect ICs that have been used for a period as little as six months. As most chips are typically used for several years, the proposed approach is well suited for detecting recycled ICs. Note that commercial IC testers can be readily used to measure I_{DDQ}, as is commonly done by many test facilities.

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. Note that while we focus on NBTI, which is often dominant and impacts the PMOS transistors, the methodology can be readily extended to include PBTI for technologies where NMOS degradation is also significant. We use the externally measured I_{DDQ} for the entire chip to track aggregate shifts in threshold voltage for large numbers of transistors since it is impractical to directly measure device parameters inside an IC. I_{DDQ} decreases with aging stress because the transistor threshold voltage magnitude increases 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} of a chip can be reliably evaluated. Our innovative solution to this problem is based on the observation that not all the transistors within an IC experience the same amount of aging stress during operation. This is because of differing signal probabilities at

2380-6923/19/$31.00 ©2019 IEEE
DOI 10.1109/VLSID.2019.00033

circuit nodes. Those PMOS transistors that are mostly off during operation (because their gate nodes are statistically at logic 1 most of the time) are lightly stressed, when compared to those that are mostly on. Therefore, if we can identify 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 transistors, then the difference between the two respective 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 significant difference, which is larger than that possible from statistical variations and other sources of test noise, would indicate a used chip.

Similar to I_{DDQ}, gate delay is also influenced by the age-related effects of NBTI. 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, both of which are likely to be identically affected by the systematic process variation.

The rest of the paper is organized as follows. Section II introduces the modeling of I_{DDQ} for device aging. Section III discusses the proposed I_{DDQ} solution to the problem of detecting recycled ICs. Simulation results are given in Section IV and Section V concludes the paper.

II. Modeling of I_{DDQ} for Device Aging

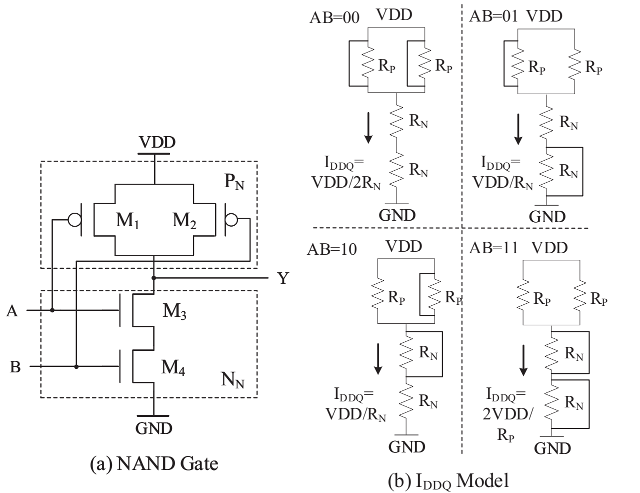
I_{DDQ} is the current drawn from the power supply in the quiescent state by a CMOS circuit. In this state, all gate inputs are static. The basic principle is to apply an input test vector and measure the steady state current. Based on this current testing decisions are made. I_{DDQ} testing provides simplicity, low-cost and high-quality [26].

A. I_{DDQ} Modeling for Logic Gates

Any CMOS gates is a series combination of a P-Network (P_N) and a N-Network (N_N). For an input pattern, one among the P_N or N_N becomes ON, and the other remains OFF, which prevents a direct path from the supply (VDD) to ground (GND). I_{DDQ} of the gate is the leakage from either P_N or N_N whichever is OFF.

Figure 1(a) shows the transistor-level circuit of a two input NAND gate with inputs A, B and output Y. The I_{DDQ} will result from the P_N or N_N, which is turned OFF and will be modeled as the leakage current. Figure 1(b) shows the resistor-level diagram of this gate with four different input combinations. We assume that R_P and R_N are the OFF-resistances of PMOS and NMOS transistors, respectively. In this paper, we model I_{DDQ} as the leakage current, which flows between drain and source terminals of an OFF transistor. For the NAND gate, we can have four different I_{DDQ} values based on input combinations, shown in Figure 1(b). When a MOSFET is turned on, the equivalent resistance between the drain and source terminals is negligible and can be treated as short.

Table I shows the I_{DDQ} for different inputs for different gates. For NAND gate when the input is 00 the equivalent OFF resistance is the series combination of two NMOS OFF resistances. So the *absolute* value of I_{DDQ} (denoted as I^A_{DDQ}) is $V/2R_N$. For 01 and 10 input the equivalent OFF resistance is R_N which results from only one NMOS transistor, and I^A_{DDQ} is V/R_N. For input 11 the equivalent resistance is the parallel combination of two PMOS OFF resistances, and the I^A_{DDQ} is $2V/R_N$. Let us assume that $I_P = VDD/R_P$ and $I_N = VDD/R_N$, we will get *unit* I_{DDQ} (denoted as I^U_{DDQ}) in terms of I_N and I_P. Similar argument can be made for other inverting gates, such as an inverter or a NOR gate. A non-inverting gate (AND, OR, etc.) can be modeled as an inverting gate followed by an inverter. The equivalent resistances between VDD and GND and I_{DDQ} for various inputs of NAND, NOR and inverter are summarized in Table I. Similar analysis can be performed for gates with three or more inputs.



(a) NAND Gate

(b) I_{DDQ} Model

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

Table I: I_{DDQ} for two-input 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	$V/2R_N$	$I_N/2$	$2V/R_N$	$2I_N$	V/R_N	I_N
0	1	V/R_N	I_N	V/R_P	I_P	NA	NA
1	0	V/R_N	I_N	V/R_P	I_P	NA	NA
1	1	$2V/R_P$	$2I_P$	$V/2R_P$	$I_P/2$	V/R_P	I_P

B. 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 [27]. 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).

Another aging phenomenon in CMOS circuits, specially in NMOS devices, is hot carrier injection (HCI). Due to multiple switching electrons receive enough energy to tunnel through the potential barrier, and get trapped in Si-SiO_2 interface near the drain terminal [28]. An NMOS transistor is primarily affected by HCI, which has practically no effect on PMOS transistors [29]. Note that the HCI effect is small compared to NBTI effect in older technology nodes. As a result, we focus on developing a solution that effectively measures the amount of aging for the obsolete chips, which are already circulating in the market. The proposed solution utilizes the aging from the PMOS transistors to detect recycled ICs. Note that as the threshold voltage of PMOS increases due to aging, the leakage current I_{DDQ}, which has a negative exponential relation with the threshold voltage (v_{th}), decreases [30]. As a result, the overall I_{DDQ} decreases when a chip is used in the field.

Process variation (PV) causes the threshold voltage of a transistor to vary from its nominal value [31], [32]. PV can be of two types - inter-die or systematic variation and intra-die variation or random variation [33]. 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 [34]–[36].

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 III) removes the effect of systematic process variation from the measurement and helps to determine accurately whether or not a chip has been used.

C. 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 [37]. 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.

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 purple).

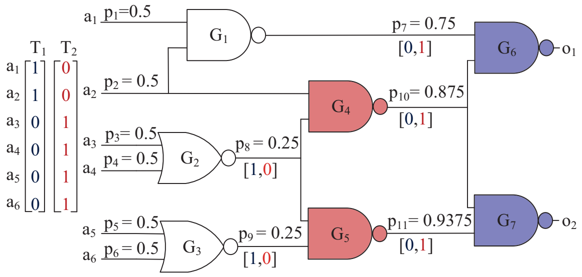


Figure 2: Test pattern selection for ΔI_{DDQ} measurement using controllability analysis.

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 [38]. 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 bypasses N-networks (e.g., $AB = 11$ for NAND gate in Figure 1) of slow aging gates. This pattern T_1 results in I_{DDQ} denoted by I_1. Similarly, we select a second test pattern (T_2) that bypasses N-networks of fast aging gates. For T_2 the I_{DDQ} is denoted by I_2.

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 slow aging gates during T_1 and mostly by fast aging gates during T_2. Then,

$$I_1 = k_1 \times I_P^L + r_1 \times I_N \tag{1}$$

$$I_2 = k_2 \times I_P^H + r_2 \times I_N \tag{2}$$

Where I_P and I_N are currents that depend on leakage resistances of PMOS and NMOS transistors as shown in Table I. "L" and "H" refer to the slow and fast 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 $k_1 \times I_P^L$ will remain relatively unchanged with age as it is derived from a majority of slow aging gates, whereas $k_2 \times I_P^H$ will reduce significantly as it comes mostly from fast aging gates. The values of I_P^L and I_P^H 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:

$$\begin{aligned} \Delta I_{DDQ} &= I_1 - I_2 \\ &= \underbrace{k_1 \times I_P^L - k_2 \times I_P^H}_{\Delta I_P} + \underbrace{(r_1 - r_2) \times I_N}_{\Delta I_N} \end{aligned} \tag{3}$$

In Equation 3, 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 $r_1 \approx r_2$.

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:

$$\Delta I = \frac{I_1 - I_2}{I_1 + I_2} \times 100 \text{ percent} \tag{4}$$

We will use ΔI to detect recycled ICs.

III. 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 will be done by the chip manufacturer. The characterization process has two parts: pattern selection and threshold calculation. First, we need to select two input patterns for testing. 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. The input pattern selection process is as follows:

1) Two thousand input patterns are selected randomly to find out two patterns (T_1 and T_2) that can result in maximum degradation (ΔI, see Equation 4) 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 measure I_{DDQ} for all 2,000 input patterns. Suppose, the current for ith pattern is $I_i^{(0)}$. See the simulation details in Section IV. 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 in Section IV) 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 measured. 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} is calculated for each pattern for six months of aging. The calculation can be done using equation 5.

Algorithm 1: Test pattern selection

```
   input  : Circuit netlist ($C$), randomly
            selected 2000 test patterns ($TP$), and $\delta I$ for all $TP$ ($\delta$)
   output : Two test patterns ($T_1$, $T_2$)
1  begin
2      $A \longleftarrow Max(\delta)$, $B \longleftarrow Min(\delta)$;
3      $j, l \longleftarrow 1$;
4      for $i \leftarrow 1$ to 2000 do
5          if $\delta \geq 0.95 \times A$ then
6              $L_1[j] \longleftarrow TP[i]$ ;
7              $r_1[j] \longleftarrow calculate\_r(C, TP[i])$;
8              $j \longleftarrow j + 1$ ;
9          end
10         if $\delta \leq 1.05 \times B$ then
11             $L_2[l] \longleftarrow TP[i]$ ;
12             $r_2[l] \longleftarrow calculate\_r(C, TP[i])$;
13             $l \longleftarrow l + 1$ ;
14         end
15     end
16     for $i \leftarrow 1$ to $j$ do
17         for $m \leftarrow 1$ to $l$ do
18             $D(i, m) \leftarrow |(r_1[i] - r_2[m])|$;
19         end
20     end
21     $[r, c] \longleftarrow min\_element(D)$;
22     $T_1 \longleftarrow L_1[r]$, $T_2 \longleftarrow L_2[c]$;
23 end
```

$$\delta I = \frac{I^{(0)} - I^{(t)}}{I^{(0)}} \times 100 \tag{5}$$

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 3). The algorithm takes the circuit netlist (C), 2,000 randomly selected test patterns (TP), and previously calculated/measured δI (see Equation 5) 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 1 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 I. Similarly, r_2, which is the coefficient of I_N in Equation 2 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 II-B), 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

Table II: I_{DDQ} for new 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	20.57	22.13	3.65	12.95	13.93	3.65	48.04	51.52	3.50	32.81	35.40	3.80	3.80
	c499	62.52	64.25	1.36	36.14	37.27	1.54	130.35	134.64	1.62	96.43	99.15	1.39	1.62
	c880	42.07	45.81	4.26	25.26	27.62	4.46	90.99	99.86	4.65	68.19	74.73	4.58	4.65
	c1908	57.05	59.55	2.14	34.30	35.97	2.38	124.37	131.42	2.76	91.85	97.41	2.94	2.94
	c3540	145.01	156.29	3.74	86.55	93.48	3.85	281.32	305.95	4.19	196.17	211.99	3.88	4.19

Table III: 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	16.99	18.84	5.16	11.10	12.29	5.09	32.48	35.88	4.97	28.36	31.49	5.23	4.97
	c499	49.25	52.57	3.26	30.39	32.60	3.51	83.01	89.14	3.56	83.02	88.71	3.31	3.26
	c880	33.74	37.49	5.26	21.61	24.10	5.45	61.09	68.41	5.65	49.96	55.82	5.54	5.26
	c1908	44.96	49.05	4.35	28.85	31.62	4.58	83.44	91.68	4.71	79.45	87.60	4.88	4.35
	c3540	113.77	125.39	4.86	72.87	80.39	4.91	194.86	216.12	5.17	171.49	189.55	5.00	4.86
12	c432	16.40	18.26	5.37	10.74	11.95	5.33	30.61	33.96	5.19	27.25	30.41	5.48	5.19
	c499	47.21	50.73	3.59	29.34	31.66	3.80	77.73	84.01	3.88	79.32	85.22	3.59	3.59
	c880	32.49	36.23	5.44	20.92	23.41	5.62	57.65	64.76	5.81	47.68	53.51	5.76	5.44
	c1908	43.19	47.34	4.58	27.88	30.71	4.83	78.58	86.88	5.02	76.09	84.25	5.09	4.58
	c3540	109.28	120.85	5.03	70.41	77.93	5.07	184.27	204.98	5.32	164.95	182.84	5.14	5.03

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 3 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 3). 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 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 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 III-A), which can be completed either by simulation using any commercial tool or at the manufacturing floor using fabricated chips. 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 4.
4) If ΔI is greater than ΔI_T, the chip is classified as a recycled chip. Otherwise, it is a new chip.

IV. Results and Discussion

To verify the proposed method of detecting recycled chips, we performed aging simulation on ISCAS'85 benchmark circuits [39]. We used MOS Reliability Analysis (MOSRA) in HSPICE, an integrated circuit reliability analysis tool from Synopsys [40], and Synopsys $32nm$ technology library [41]. MOS transistor parameters were based on $32nm$ low power metal gate Predictive Technology Model (PTM) [42]. 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 II and III. Table II 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 4) 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 3.65%, 3.65%, 3.50% and 3.80% respectively. The maximum value 3.80% is the threshold ΔI_T. Similar analysis can be performed for all other benchmark circuits.

Table III summarizes I_{DDQ} data after six months and one year of aging. The columns of this table are similar as in Table III, 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 II). For the c432 circuit, after six months of aging, the ΔI values are 5.16%, 5.09%, 4.97% and 5.23%. The minimum value is 4.97% which is greater than its threshold ($\Delta I_T = 3.80\%$). 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.

V. Conclusion

The two-pattern ΔI_{DDQ} test effectively identifies recycled ICs that may have been previously used for as little as six months. The test requires no added hardware or design change in the device. 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.

The last column of Table II shows that not all circuits are affected by process variation in the same way. Circuit c499 is least affected and c880 is most affected. 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 1755733 and 1527049.

References

[1] IHS iSuppli, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," 2011.

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

[3] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, pp. 1207–1228, 2014.

[4] 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.

[5] 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.

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

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

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

[9] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, October 2012.

[10] 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*, 2012, pp. 7–12.

[11] Y. Zheng, A. Basak, and S. Bhunia, "CACI: Dynamic current analysis towards robust recycled chip identification," in *Design Automation Conference (DAC)*, June 2014, pp. 1–6.

[12] H. Dogan, D. Forte, and M. Tehranipoor, "Aging analysis for recycled FPGA detection," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Oct 2014.

[13] Y. Zheng, X. Wang, and S. Bhunia, "SACCI: Scan-based characterization through clock phase sweep for counterfeit chip detection," *IEEE Trans. Very Large Scale Integration (VLSI) Systems*, 2014.

[14] Z. Guo, M. T. Rahman, M. M. Tehranipoor, and D. Forte, "A zero-cost approach to detect recycled soc chips using embedded sram," in *IEEE Int. Symp. on Hardware Oriented Security and Trust*, 2016.

[15] 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.

[16] 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.

[17] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Transactions on Very Large Scale Integration Systems*, pp. 1016–1029, 2014.

[18] 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.

[19] 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.

[20] 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*, Nov. 2015, pp. 146–151.

[21] 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)*, 2018.

[22] 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.

[23] Semiconductor Industry Association (SIA), "Public Comments - DNA Authentication Marking on Items in FSC5962," November 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*, 2005.

[26] R. Rajsuman, "Iddq testing for CMOS VLSI," *Proceedings of the IEEE*, vol. 88, no. 4, pp. 544–568, 2000.

[27] D. K. Schroder, "Negative bias temperature instability: What do we understand?" *Microelectronics Reliability*, pp. 841–852, 2007.

[28] B. Shakya, U. Guin, M. Tehranipoor, and D. Forte, "Performance optimization for on-chip sensors to detect recycled ICs," in *Proc. 33rd IEEE International Conference on Computer Design (ICCD)*. IEEE, 2015, pp. 289–295.

[29] 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.

[30] 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)*, 2008, pp. 13–16.

[31] A. Asenov, "Simulation of statistical variability in nano MOSFETs," in *Proc. IEEE Symposium on VLSI Technology*, 2007, pp. 86–87.

[32] 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*, 2003, pp. 84–89.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] M. L. Bushnell and V. D. Agrawal, *Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits*. Springer, 2000.

[38] 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, 2000, pp. 439–443.

[39] ISCAS-85 Benchmark Circuits, http://www.pld.ttu.ee/ maksim/benchmarks/iscas85/.

[40] B. Tudor, J. Wang, W. Liu, and H. Elhak, "MOS device aging analysis with hspice and customsim," *Synopsys, White Paper*, 2011.

[41] Synopsys 32/28nm Generic Library for Teaching IC Design, https://www.synopsys.com/COMMUNITY/UNIVERSITYPROGRAM/Pages/32-28nm-generic-library.aspx.

[42] Predictive Technology Model (PTM), http://ptm.asu.edu/modelcard/LP/32nm_LP.pm.