# A Zero-Cost Detection Approach for Recycled ICs using Scan Architecture

Wendong Wang, Ujjwal Guin and Adit Singh
Dept. of Electrical and Computer Engineering, Auburn University
Auburn, AL, 36849
{wzw0027, ujjwal.guin, adsingh}@auburn.edu

***Abstract*—The recycling of used integrated circuits (ICs) has raised serious problems in ensuring the integrity of today's globalized semiconductor supply chain. This poses a serious threat to critical infrastructure due to potentially shorter lifetime, lower reliability, and poorer performance from these counterfeit new chips. Recently, we have proposed a highly effective approach for detecting such chips by exploiting the power-up state of on-chip SRAMs. Due to the symmetry of the memory array layout, an equal number of cells power-up to the 0 and 1 logic states in a new unused SRAM; this ratio gets skewed in time due to uneven NBTI aging from normal usage in the field. Although this solution is very effective in detecting recycled ICs, its applicability is somewhat limited as a large number older designs do not have large on-chip memories. In this paper, we propose an alternate approach based on the initial power-up state of scan flip-flops, which are present in virtually every digital circuit. Since the flip-flops, unlike SRAM cells, are generally not perfectly symmetrical in layout, an equal number of scan cells will not power-up to 0 or 1 logic states in most designs. Consequently, a stable time zero reference of 50% logic 0s and 1s cannot be used for determining the subsequent usage of a chip. To overcome this key limitation, we propose a novel solution in this paper that reliably identifies used ICs from testing the part alone, without the need for any additional reference data or even the netlist of the circuit. Through scan testing of the IC, we first identify a significant number of asymmetrically stressed flip-flops in the design, divided into two groups. One group of flip-flops is selected such that it mostly experiences the 1 logic state during functional operation, while the other group mostly experiences the 0 state. The resulting differential stress during operation causes growing disparity over time in the number of 0s (and 1s) observed in these two groups at power-up. When new and unaged these two groups behave similarly, with similar percentage of 1s (or 0s). However, over time the differential stress makes these counts diverge. We show that this changing count can be a measure of operational aging. Our simulation results show that it is possible to reliably detect used ICs after as little as three months of operation.**

***Index Terms*—Recycled ICs, scan flip-flops, bias temperature instability, power-up state.**

## I. Introduction

The illicit recycling of used ICs as new poses a severe threat to the reliability and security of electronic systems due to the lack of effective detection methods to identify such parts. Recycled ICs, which are taken out from used printed circuit broads (PCBs), can be easily introduced into the globalized semiconductor supply chain. Obsolete parts, which are no longer being manufactured but are needed to repair and maintain legacy systems, must often be purchased from any available source, including untrusted distributors. This puts large parts of critical infrastructure and defense systems at risk because government budgetary constraints often force such systems to be deployed well beyond their planned lifetime, and are therefore in need of a steady supply of spare parts [1]. Recycled parts can pose severe reliability issues due to the many defects and anomalies that can result from damage due to the often harsh recycling processes which can inflict significant mechanical and high temperature stress on the part. Moreover, these part are commonly recovered from discarded electronic waste, which is poorly handled with respect to conditions such as humidity, ESD protection, etc. As a result, recycled parts often exhibit lower reliability, shorter lifetime, and sometimes also degraded performance [2] [3].

The existing approaches for detecting recycled ICs, and thereby preventing them from getting into the electronics supply chains can be classified into several categories. First, on-chip sensors have been proposed as part of design-for-anti-counterfeit (DfAC) measures to enhance traditional tests for detecting these old chips [4]–[10]. Unfortunately, the vast majority of chips that can be potentially recycled are already manufactured and deployed, and cannot be detected using DfAC measures as these solutions require the design to be modified. Second, a number of conventional test methods have been recommended in different "counterfeit" detection standards (*e.g.*, AS6171 [11], AS5553 [12], CCAP-101 [13] and IDEA-STD-1010 [14]). However, all these suffer from excessive test time and cost, lack of automation, and, most critically, low detection confidence [15]. Third, a number of researchers have also proposed methods that use statistical analysis of test data that identifies outliers as recycled parts [16]–[21]. Unfortunately, a large number of chips are often required to create the statistical models, which may be difficult to find for obsolete parts. Furthermore, process changes and variations over a long multi-year production run can make it difficult to extract stable reference parameter values from a handful of "new" parts for reliable outlier identification of recycled counterfeit parts in the mix.

Recently, we have proposed a novel and very effective approach for detecting recycled ICs and systems-on-chip (SoCs) using the power-up state of an on-chip SRAMs [22]. Importantly, in our new approach, the process of determining whether a chip is recycled or not uses a reference that is an invariant property of all new SRAMs; it does not need any reference data to be measured and obtained from new parts. Note that since each SRAM cell in a large memory array is designed with perfect symmetry, its power up logic state will depend on the random manufacturing process variations within each cell, as well as the electrical and thermal noise experienced during power-up. As these processes are Gaussian in nature, observing the power-up state in a large number of cells should yield 50% 1s and 50% 0s in a new unused SRAM. This inherent initial property of all new SRAMs gets skewed over time due to aging stress from normal usage in the field because the memory content of each cell, averaged over all the time in operation, is rarely unbiased. Cells that spend the majority of the time in the 1 state increase their bias towards powering up in the 0 state, while those that mostly experience the 0 state increase their bias towards powering up in the 1 state. As was verified by the silicon experiments reported in [22], a shift in

either direction from a balanced number of 1s and 0s can be used to identify a used part. Since SRAMs cores are commonly found today in processors and SoCs, this method for detecting recycling has wide applicability. However, a variety of older digital ICs circulating in today's complex supply chain, and also some modern ICs, may not have on-board SRAMs. Recycling of these parts cannot be detected using the solution as proposed in [22].

*In this paper, we propose a new recycled part detection approach that can be applied to virtually every large digital circuit, even older parts already in the supply chain. Our new approach is based on the power-up state of the flip-flops (FFs) in the circuit, accessed directly through the scan chains [23]. Importantly, it only requires the scan testing the part alone, and no additional information or even the netlist of the circuit.*

The new approach uses the power-up state of the scan FFs to determine whether a chip has been used and recycled. However, unlike our previous approach for SRAMs [22], a stable time zero reference of 50% logic 0s and 1s at power-up cannot be relied upon because the FFs memory cells may not be perfectly symmetrical in layout. As a result, they may display some systematic bias at power-up. (Note however, that any bias is typically small, since it must be minimized by the cell designers so as to maximize cell stability and noise margins.) Nevertheless, while the FFs in a new IC cannot be expected to always display an equal number cells powering-up to the 0 and 1 logic states, in a new unstressed part, any statistically large subset of identical FFs should power-up to the same percentage of 0s and 1s. We propose to use this alternate time zero reference property for the FFs in this paper. Our new approach exploits the differential NBTI aging stress in two groups of FFs that mostly experience the logic 0 and logic 1 states, respectively, during functional operation. These two groups, one strongly biased towards 0s and the other towards 1s, can be easily identified through scan testing. While their numbers may be only 1-3% of the total, they would still be at least a thousand or more in each group for a large design. The power up states of these two groups of FFs in a new part (at time zero) can be expected to be statistically very similar as discussed above (although not 50% 1s and 0s as is the case for SRAMs), before operational stress is applied. However, over time the differential stress in operation causes the statistics for 0 and 1 states in the two flip-flop groups to move in opposite directions from their time zero percentages. We show in later Sections that this growing difference in the percentage of 0s (or 1s) observed at power-up in the two groups of flip flops is quite stable (for large groups of at least a few hundred FFs) and can be used to reliably detect used parts after only a few months of aging. Observe that this new approach does not need any statistical data from other parts, nor any recorded reference data from the part when new, to identify used parts.

The main contributions of the paper are summarized below:

- To the best of our knowledge, this is the first approach that can detect any used and recycled digital IC, by testing the part alone, without the need for any additional information or even the netlist of the circuit. There is no need for any stored time-zero reference data for each new part, or even statistical aggregate data that characterizes new unused parts. It is primarily the unavailability of such reference data for discontinued parts that limits the detection of recycled ICs through tests for signal degradation in use.
- We show that the diverging percentage of 0s (or 1s) at power-up in the two groups of selected FFs can provide an indication of the operational age of the digital circuit. In general, age detection accuracy depends on the size of the chip, and the resulting number of flip-flips that can be identified as strongly 0 biased and strongly 1 biased during operation. For large circuits with hundreds of thousands of FFs, our simulation results show that it is possible to reliably detect recycled chips in use for as little as three months in the field.

The rest of the paper is organized as follows. Section II introduces modeling of the power-up state for a flip-flop, and how it is impacted by the aging. Section III discusses the our proposed approach for detecting recycled ICs in detail. Simulation results are presented in Section IV. Finally, we conclude the paper in Section V.

## II. Modelling of the Flip-flop Power-up State of a Digital Circuit

Unlike SRAM cells, the initial power-up value of a D flip-flop (DFF) is not equally likely to be logic 0 or 1 due to possible asymmetry in the cell layout. In this section, we present the power-up behavior of a DFF, and the impact of manufacturing process variations and aging on it during operational deployment.

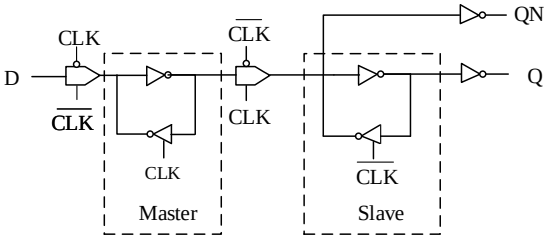



Figure 1: The schematic of a DFF.

### A. Power-up State of a Flip-Flop

Figure 1 shows the typical structure of a D-type Flip-flip (DFF). Observe that the output of the clocked inverters shown in each latch are enabled by the appropriate clock signal; they assume a high impedance state when not enabled. We focus on the logic state acquired at power up by the latches in the flip-flop. Note from Figure 1, that depending on whether the clock signal $CLK$ is held high or low during power-up, only one of the two latches (either master or slave) will have the its feedback path enabled to act as a storage element. For example, if the value of $CLK$ is held at logic 0, the slave latch will be active and decide the power-up state of the FF. Also, the input lines to the latch will not influence this power up state since the slave latch is completely isolated by the middle transmission gate during power up time. While a power-up state can also be captured in the master latch by holding the clock high during power-up, in this paper we work with the slave latch. We assume throughout (including in our simulation experiments) that $CLK$ is at logic 0 during the power-up time. In addition, we assume that the state of the slave latch is the same as that of the DFF for purposes of the following discussion. A similar analysis can be performed for the master latch with $CLK$ held at logic 1.

Figure 2 shows a simplified schematic of the slave latch of a DFF. The latch usually contains two back to back inverters, where one of them, as discussed earlier, is a tri-state inverter controlled by the $CLK$ signal. The latter is implemented using two additional transistors as shown in the figure. In the design, $M_1$, $M_3$ and $M_2$, $M_4$ consist of two back to back inverters, while $M_5$,$M_6$ are controlled by $CLK$. Note that $CLK$ must to be set to

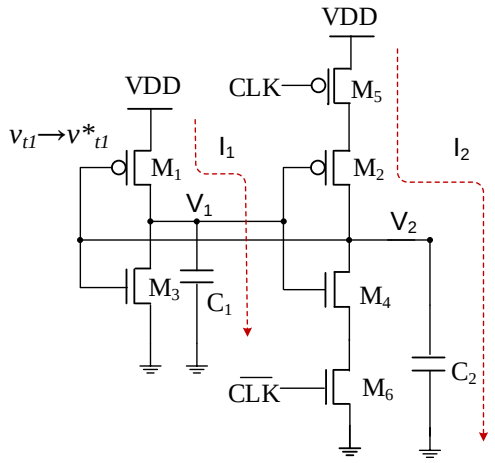



Figure 2: Simplified schematic of slave D latch.

logical 0, in order to isolate the slave latch from the master latch. Consequently $M_5$ and $M_6$ are always on as long as $CLK$ is 0, and can be approximately modelled by their channel resistances, $R_{on}$. Note that $R_{on}$ for the NMOS and PMOS transistors may be different due to transistor sizing and device parameters. Moreover, the capacitances $C_1$ and $C_2$ may also end up with different values due to asymmetry in the layout. Thus, when compared with the perfectly regular layout of 6 transistor SRAM cells [22], the latches in a FF have several potential sources of asymmetry. In practice, the cell designers do attempt to minimize such asymmetry and resulting biases in the latches because such biases reduce noise immunity and makes the FFs more vulnerable to bit flip errors. However, in general, the latches will not attain a perfect 50% chance to power-up to 0 or 1, even if the $M_1 - M_2$ and $M_3 - M_4$ transistor pairs are designed to be identical in the layout.

### *B. Impact of process variation and aging on the power-up states*

In this subsection, the impact of aging and process variation will be investigated in detail using Figure 2. Recall that the slave latch in a DFF can have inherent biases due to differences in node capacitances, $C_1$, $C_2$, and the presence resistance $R_{on}$ in one path. Furthermore, any bias in the layout is further impacted by process variation in the transistors and passive components. For simplicity, we ignore differences in the NMOS transistors as the power-up state primarily depends on the PMOS transistors when a fast ramp is applied to the power supply [24]. As depicted in Figure 2, assume $V_{t1}$ increases to $v^*_{t1}$ due to process variation. Consequently, $I_1$ will decrease, which leads to a larger time needed to change the voltage across $C_1$. If the voltage $V_1$ increases less than the voltage $V_2$, the latch will power-up to logical 1 (output node $V_2 = 1$ and $V_1 = 0$). In our simulations, the threshold voltage of each MOS transistor is taken from a Gaussian distribution with a standard deviation of 5% of the mean value. The possibility that threshold voltage of $M_1$ exceed $M_2$ is exactly 50%. However, based on previous analysis, in order to power-up to logical 1, this threshold voltage difference between $M_1$ and $M_2$ should be large enough to overcome any other biases in the latch. .

The next step is to investigate the impact of aging. For simplicity, we assume that all the transistor pairs, $M_1$, $M_2$ and $M_3$, $M_4$, have the same threshold voltages. We now age this latch with logical 0 ($V_2 = 0$ and $V_1 = 1$). The (magnitude of the) threshold voltage of the stressed (ON) transistor $M_1$ starts to increase due to NBTI and reaches to $v^*_{t1} (> v_{t1})$ while the threshold voltage of the unstressed (OFF) transistor $M_2$ will remain the same. Consequently, the latch will begin to power-up to the logic 1 state when the impact of aging exceeds that of the other imbalances in the cell in the opposite direction. We can therefore conclude that more DFFs will power up with logical 1 values over time when aged in the logic 0 state, and vice versa.

Table I: Start-up value of 1000 DFFs with 3 months of usage.

| **% of 0s in aging patterns** | 100 | 80 | 60 | 40 | 20 | 0 |
|---|---|---|---|---|---|---|
| **% of 1s in power-up state** | 21.5 | 19.5 | 12.5 | 9.6 | 7.2 | 4.3 |

Table I shows HSPICE simulation results that include the impact of aging for 1000 latches (in DFFs). The 3 month aging experiment was repeated for the latches randomly preset to different percentages of 0s ranging from 100% to 0%. The simulations were run using 32*nm* bulk Predictive Technology Model (PTM) [25], with 20 mV (standard deviation) random process variation introduced into the threshold voltages of each MOS transistor ($M_1$, $M_2$, $M_3$, and $M_4$). This aging simulation wsas performed using Synopsys HSPICE MOS Reliability Analysis (MOSRA) [26]. Table I shows the percentage of 1s observed in the power-up states of the latches (DFFs) in each experiment. First observe that latch has an inherent bias towards the 0 state because the percentage of 1s is always less than 50%. Nevertheless, the percentage of 1s observed at power-up increases when the latches are mostly aged in the 0 state, as compared to being aged in the 1 state. It is this observation that is the basis of the proposed recycling detection approach.

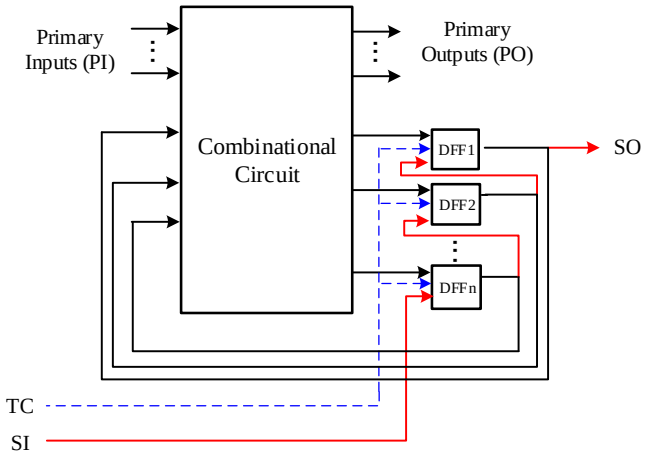



Figure 3: Schematic of a sequential circuit.

### *C. Non-uniformed Aging*

In a typical sequential circuit, not all flip-flops will experience same rate and bias from aging after deployment. The aging of each individual flip-flop will be determined by its aggregate logic state over time (described in Section II-B), which is governed by the relative frequencies of 0s and 1s at its input. It is therefore possible to identify flip-flops which age mostly in the 0 or 1 state from their input controllability measures. The controllability of a node is defined by the probability that it is observed in the 0 or 1 state. For example, the SCOAP testability measure are widely used by test tools [23]. However, testability measures such as SCOAP are only approximate, and when possible, circuit simulations or actual test measurements through the use of scan chains for a large set of test patterns, can more accurately

estimate circuit signal probabilities. Importantly, the scan testing proposed here avoids the need for a netlist. Observing a high percentage of logic 0s (1s) in a flip-flip during test indicates that the flip-flop will mostly be found in the 0 (1) state in operation.

Figure 3 shows the classical schematic of a sequential circuit where the flip-flop states can be directly accessed through the scan chains. The state probability of each flip-flop can be estimated through scan testing as follows:

- *Step 1*: A random pattern is shifted into the scan chains ($TC = 1$).
- *Step 2*: The response of the combinational part is captured in the FFs ($TC = 0$).
- *Step 3*: The states of the individual FFs are shifted out and recorded ($TC = 1$).

A different random pattern is selected and Steps 1-3 are performed. We apply a large number (*e.g.*, 10,000) of these random patterns to determine the each FFs probability of being in the 1 (0) state using the following equation:

$$Pr(1) = \frac{\#1s \text{ observed in the target FF}}{\#\text{Total patterns}} \quad (1)$$

Similarly, the $Pr(0)$ can be calculated by replacing 1s with 0s in Equation 1. Note that single cycle operation from random initial states may not precisely mimic continuous functional operation, which can introduce some error in the estimated input controllability values. However, such inaccuracies are allowed for by the inherent statistical nature of the proposed approach.

Figure 4 shows the distribution for the input probability of 1 ($Pr(1)$) for all the FFs in b19 benchmark circuit (ITC'99) to demonstrate asymmetric aging. We observe a near normal distribution, where the two tails are of our interest. The first group, denoted as *Group-1*, contains FFs that age with mostly 1, and second group, denoted as *Group-2*, which experiences mostly 0 in operation. As the FFs in *Group-1* are mostly stressed in the 1 state during operation, this group will exhibit an increase in the number of 0s at power-up over time. As a result, the percentage of 1s in this group will reduce. On the other hand, the FFs in *Group-2* will age with 0 and the percentage of 1s in this group at power-up will increase over time. The difference in the percentage of 1s (or 0s) among these two groups will reflect the length of the usage of a chip in the field. Ideally, the percentage of 1 in power-up state for two groups should be exactly the same (given a relatively large number of FFs in each group) for a new part that has not experienced any aging. However, based on the previous discussion, random process variation will have some impact on power-up state of FFs. Consequently, the initial percentage of 1 in power-up state for two groups can have some statistical difference, which scales down as the number of FFs in group increases. We define this difference as $\Delta$. Generally, the value of $\Delta$ is be very small (less 2% ) if we select a large number of FFs (see details in Section IV). In practice, this can be ignored when when evaluating recycled chips those have been used for many months of years.

## III. Proposed Approach for Recycled IC Detection Based on Power-up State of Flip-Flops

The proposed approach utilizes the power-up state of the scan FFs to determine the prior usage of a chip, and can be effectively used for detecting recycled ICs. However, the power-up state of a FF will be skewed due to its inherent asymmetry. It is necessary to construct two groups of FFs,

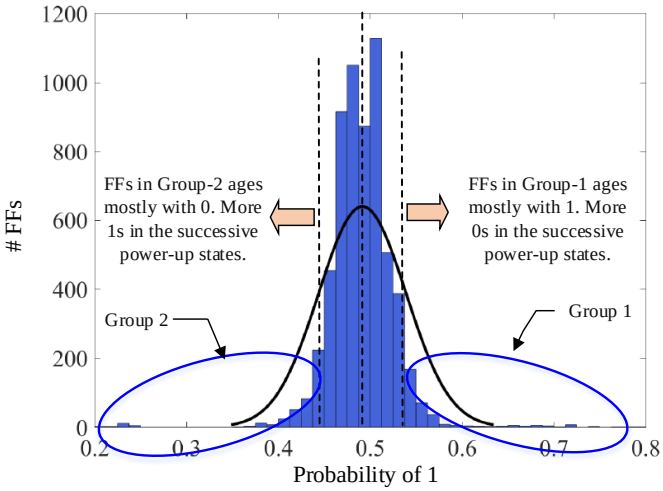
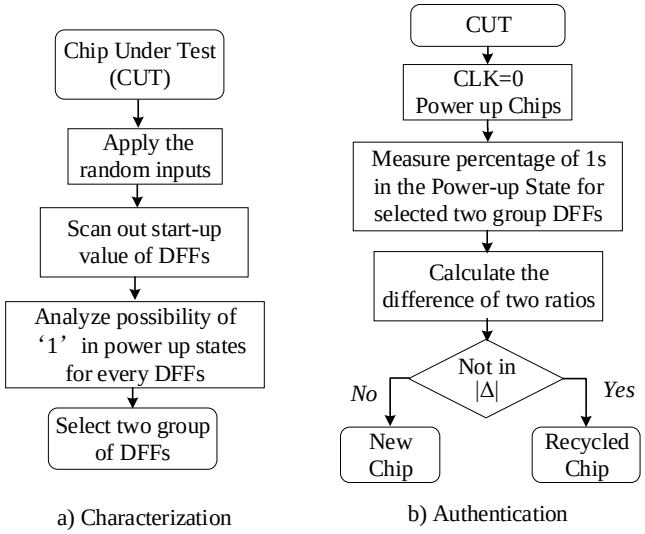



Figure 4: Impact of aging on different groups of FFs.

which mostly ages with 0 and 1, respectively. In this section, we develop a detailed step-by-step process for the detection.




a) Characterization b) Authentication

Figure 5: proposed method to detect recycled ICs by power-up state of FFs.

Figure 5 shows our proposed approach for detecting recycled digital chips, which consists of two phases. In Phase I, the characterization is performed and is shown in Figure 5.a. Two groups of FFs are selected for future authentication. The authentication for a chip whether it is new or recycled is performed in Phase II. The details for these two phases are summarised as follows:

- *Phase I – Characterization*: To identify two groups of FFs – one mostly aged with 0 and the other aged with 1 – is primary objective of this phase. We extract the FF input controllability information from the chip under test (CUT). We apply 1000 random input patters, capture the response in FFs and shifted out the state using the scan chains (see the details in Section II-C). Based on the input probabilities, two different groups of FFs are constructed for authentication. *Group-1* is the group of FFs which will most likely age with logical 1 , and *Group-2* is the group of FFs which will experience logical 0 with higher possibilities. Note that both these groups will have similar statistics (*e.g.*, percentage of 1s

or 0s) at time zero with a small error, which can be less than 1% when a large number of FFs are selected (see Table II).

- *Phase II – Authentication*: The process of determining a chip being recycled is relatively straight-forward. For any CUT, it is necessary to measure the start-up value of all the FFs. Note that we need to keep the clock at logic 0 ($CLK = 0$) during the power-up so that the slave latch of the DFFs are selected. One can also make $CLK = 1$ to select the master latch. Two groups of FFs are now constructed based on the data from the characterization phase described above. For each group, percentage of 1 are calculated. The difference of percentage of 1s for two group are calculated. If this difference lies within $\Delta$ (which is negligible for a large group of FFs and approximately 1%), the chip will be identified as new, otherwise, it is an used/recycled one.

## IV. Simulation Results and Analysis

In order to verify our proposed method of detecting recycled ICs, we perform the HSPICE aging simulation on different benchmark circuits [27]. We use the MOS Reliability Analysis (MOSRA) tool by Synopsys [26] to perform aging analysis. Synopsys 32nm technology library is used for implementing DFF for simulation [28]. MOSFET models are based on 32nm low power metal gate Predictive Technology Model [25]. Aging simulation is performed at 25°C room temperature and nominal supply voltage of 1V. The benchmark circuits are synthesised in Synopsys Design compiler (DC) and IC Validator is used to covert synthesized netlist to SPICE netlist. We use Synopsis VCS to perform logic simulation to compute the probabilities at the input of each FF.

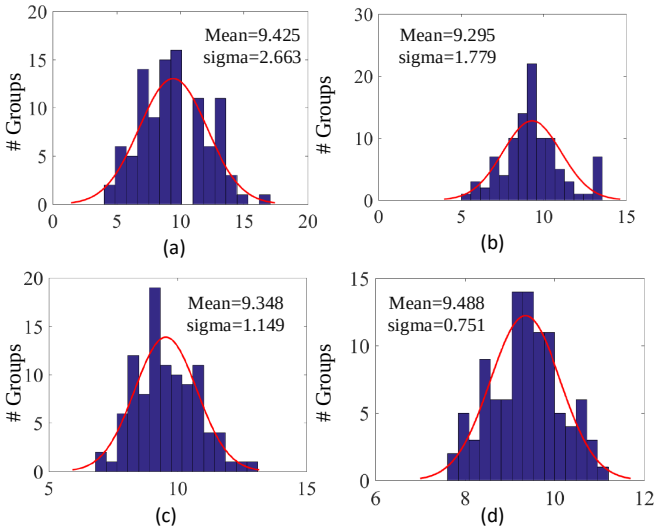



Figure 6: Threshold ($\Delta$) estimation for different group sizes with varying number of DFFs. (a) Group size of 100, (b) Group size of 200, (c) Group size of 500, and (d) Group size is 1000.

The first experiment is performed to show that the different groups of FFs have similar percentage of 1 before a chip has been deployed in the field. To implement process variation, we add random variation with standard deviation $\sigma$ of 20 mV to the threshold voltage of each MOS transistors. We measure percentage of 1s for 100 groups of unaged FFs and plot the corresponding distribution. In addition, different FF group sizes are also explored to find out how the percentage of 1s varies among these groups. Figure 6 shows the distribution of percentage of 1 for different group sizes. X-axis represents the percentage of 1 in power-up state for every groups, whereas, the Y-axis represents the number of such groups. From the figure, it is obvious that the standard deviation ($\sigma$) decreases with the increase of the group size. Note that $\sigma$ drops to 0.751 from 2.663, when the group sizes are increases to 1000 DFFs from 100. Note that we expect an error of 68%, 95%, and 99.7% when we consider $\sigma$, $2\sigma$, and $3\sigma$ values [29]. In other words, if we take any two groups of DFFs, the similarity of the percentage of 1s among different groups will 68%, 95%, and 99.7% if we consider the threshold ($\Delta$, see Figure 5 for details) of $\sigma$, $2\sigma$, and $3\sigma$. We choose $\Delta$ of $2\sigma$ value in detecting recycled ICs. However, one can choose $3\sigma$ to increase the confidence.

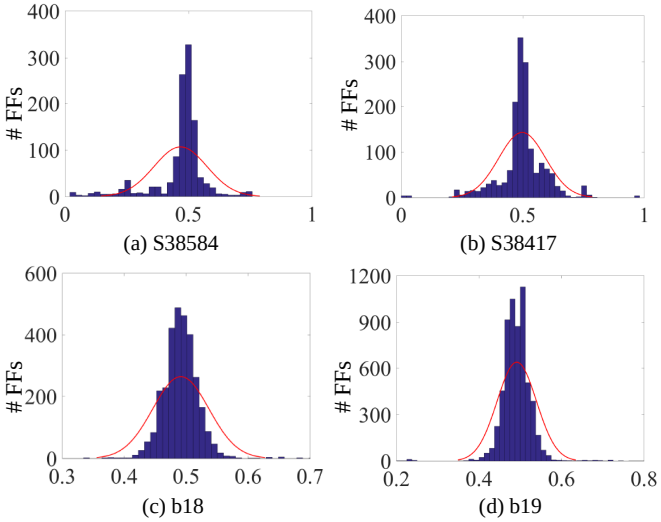



Figure 7: Probability of getting 1 ($Pr(1)$) at input of DFFs for (a) S38584 (b) S38417 (c) b18 (d) b19 benchmark circuits.

The second experiment is performed to verify the effectiveness of our proposed method using ITC'99 [30] and ISCAS'85 [27] benchmark circuits. We perform the necessary steps to to select two groups of FFs, where one group is aged mostly with 0, the other is aged with 1 (see Figure 5.a). Figure 7 shows the distribution of the inputs of each FF for different benchmarks circuits. The X-axis represents the probability of getting 1 at the input of a DFF, whereas, the Y-axis represents the number of FFs. We observe Gaussian distributions for all four benchmark circuits. Generally, 2/3 of the FFs in these circuits experience uniform aging with 1 or 0s. On the other hand, 1/3 of the total FFs experience non-uniform aging and those are of our interest for selecting two groups. Figure 7.a, shows the distribution for a medium size S38548 benchmark circuit. We have selected 500 FFs from both the tails of the distribution to form the two groups. Figure 7.s, shows the distribution for a large b19 benchmark circuit, where we can easily find 1000 FFs for each group. Similar analysis can be performed for Figure 7.b and 7.c.

Table II represents the simulation result with aging intervals of 3 months, 6 months and 12 months. As 1/3 of total FFs experience non-uniform aging (see Figure 7 for details), we will distribute these FFs in two different groups. As b18 and b19 contains thousands of FFs, it is easy to form these two groups with 1000 FFs. On the other hand, we do not have enough FFs to form groups with 1000 FFs for b22, s38417 and s38548 benchmark circuits. As a result, 500 FFs are assigned to each group. The first column of Table II denotes the aging duration. The second, third, and forth columns represent the benchmark circuits, the

Table II: Power-up value of FFs for used benchmark circuit

| Usage (months) | Bench -marks | Group Size | $2\sigma$ Value | $\%1s$ for G1 | $\%1s$ for G2 | Differ -ence |
|---|---|---|---|---|---|---|
| 3 | b22 | 500 | 2.3 | 9.95 | 13.12 | 3.17 |
| | b17 | 500 | 2.3 | 6 | 12.49 | 6.49 |
| | b18 | 1000 | 1.5 | 9,14 | 16.3 | 7.16 |
| | b19 | 1000 | 1.5 | 8.06 | 15.7 | 7.64 |
| | s38417 | 500 | 2.3 | 8.14 | 14.65 | 6.51 |
| | s38584 | 500 | 2.3 | 10.44 | 17.89 | 7.45 |
| 6 | b22 | 500 | 2.3 | 9.41 | 15.61 | 6.2 |
| | b17 | 500 | 2.3 | 5.62 | 15.01 | 9.39 |
| | b18 | 1000 | 1.5 | 8.14 | 17.98 | 9.84 |
| | b19 | 1000 | 1.5 | 7.86 | 17.11 | 9.25 |
| | S38417 | 500 | 2.3 | 8.05 | 15.08 | 7.03 |
| | S38584 | 500 | 2.3 | 10.48 | 20.62 | 10.14 |
| 12 | b22 | 500 | 2.3 | 9.27 | 16.47 | 7.2 |
| | b17 | 500 | 2.3 | 5.57 | 15.88 | 10.31 |
| | b18 | 1000 | 1.5 | 8.12 | 18.14 | 10.02 |
| | b19 | 1000 | 1.5 | 7.62 | 17.2 | 9.58 |
| | S38417 | 500 | 2.3 | 7.88 | 16.3 | 8.42 |
| | S38584 | 500 | 2.3 | 10.38 | 20.87 | 10.49 |

group size, and the 2 threshold value, respectively. The fifth and sixth columns represent the percentage of 1s for group 1 (G1) and group 2 (G2), respectively. The last column represents the difference of percentage of 1 for two group after aging.

We can detect the recycled ICs, if the value of last column exceeds $2\sigma$ threshold value (shown in the forth column of Table II). For example, the difference of percentages of 1s for G1 and G2 are 7.16%, 9.25%, 9.58% after 3, 6, 12 months of aging, respectively for b19 benchmark circuit. Note that the difference of percentages of 1s for the two groups increases as the chips are used for a longer duration. As the $2\sigma$ value (threshold, $\Delta$) is only 1.5% and difference of percentages of 1s for two groups are much greater than $\Delta$, it is safe to conclude that we can detect recycled b19 designs when they have been used al least for three months. The same analysis can be performed for other benchmark circuits. Note that the accuracy of our proposed solution increases with the size of the circuit.

## V. Conclusion

In this paper, we have proposed a zero-cost approach to detect recycled ICs by observing the power-up states of the scan flip-flops in the chip. The proposed solution performs scan tests on only the target IC, and does not require any other information such as reference data for new parts, or even the netlist. Instead, it uses a differential self-referencing methodology based on two selected groups of FFs in the part, one group that mostly ages in the 0 state, and the other which ages in the 1 state. The percentage of 1s observed at power-up in these two groups is virtually the same when a chip is new, because of the commonality in design and process. However, after aging in use, due to the differential NBTI stress, the percentage of 1s increases for one group and decreases for the other. This creates a differential signal indicating functional use which increases in magnitude over time. Our current future work is focused on implementing this and related solutions in silicon.

## Acknowledgment

This work was supported in parts by the National Science Foundation under Grant Numbers CNS-1755733, CCF-1527049 and CCF-1910964.

## References

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

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

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

[15] U. Guin, N. Asadizanjani, and M. Tehranipoor, "Standards for hardware security," *GetMobile: Mobile Computing and Communications*, vol. 23, no. 1, pp. 5–9, 2019.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] U. Guin, W. Wang, C. Harper, and A. D. Singh, "Detecting recycled socs by exploiting aging induced biases in memory cells," in *IEEE Int. Symposium on Hardware Oriented Security and Trust (HOST)*, 2019, pp. 72–80.

[23] M. Bushnell and V. Agrawal, *Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits*. Springer Science & Business Media, 2004, vol. 17.

[24] W. Wang, A. Singh, U. Guin, and A. Chatterjee, "Exploiting power supply ramp rate for calibrating cell strength in sram pufs," in *Test Symposium (LATS), 2018 IEEE 19th Latin-American*, 2018.

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

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

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

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

[29] D. J. Wheeler, D. S. Chambers *et al.*, *Understanding statistical process control*. SPC press, 1992.

[30] ITC-99 Benchmark Circuits, https://www.cerc.utexas.edu/itc99-benchmarks/bench.html.