Detecting Recycled SoCs by Exploiting Aging Induced Biases in Memory Cells

Ujjwal Guin, Wendong Wang, Charles Harper, and Adit D. Singh
Dept. of Electrical and Computer Engineering, Auburn University
Email: {ujjwal.guin, wendong, charles.harper, singhad}@auburn.edu

Abstract—**The rise of recycled ICs being sold as new through the global semiconductor supply chain is a serious threat due to their inferior quality, shorter remaining life, and potentially poorer performance, compared to their authentic counterparts. While solutions, such as on-chip age monitors, have been proposed for new designs, detecting the recycling of older legacy ICs already in use is much harder; no reliable solution currently exists. In this paper, we propose a new and highly effective approach for detecting recycled ICs by exploiting the power-up state of on-chip SRAMs to evaluate the age of the chip. Our methodology does not require the introduction of any special aging detection circuitry, nor the recording and saving of historical circuit performance data as a reference to detect degradation from use. Instead, we exploit the novel observation that in a new unused SRAM, an equal number of cells power up to the 0 and 1 logic states, and also that this distribution becomes skewed in time due to aging in operation. Since SRAMs exist in virtually all systems-on-chip (SoCs), this simple aging detection method is widely applicable to both old and new designs. It is also low cost since does not require any special test equipment. We present experimental results using commercial off-the-shelf SRAM chips to validate the effectiveness of the proposed approach.**

Index Terms—**Recycled ICs, aging, bias temperature instability, SRAM power-up state.**

I. Introduction

The problem of old recycled integrated circuits (ICs) being supplied and sold as new continues to grow due to the lack of efficient detection and avoidance techniques. The entry of these ICs into the critical global infrastructure (defense, aerospace, transportation, medical, etc.) can result in system and security failures with potentially serious consequences for societal well being. Electronic parts from old, discontinued production runs are often required to maintain outdated infrastructure and defense systems as the operational life of such systems is frequently extended far beyond initial plans because of budget limitations. (B-52 bomber aircraft that first flew in the 1950s are today being flown by the grandchildren of some of the original pilots.) The original component manufactures (OCMs) have, meanwhile, long moved on to newer designs and technologies, and discontinued production of the obsolete ICs. To meet this critical need, maintenance and repair facilities have no option but to reach out to all possible suppliers of the legacy ICs, including untrusted third party suppliers overseas. Information Handling Services Inc. has reported that counterfeit ICs represent a potential annual risk of $169 billion in the global supply chain [1]. Recycled ICs contribute around 80% of all the reported counterfeiting incidents [2]. As these recycled ICs often exhibit lower performance and reduced remaining useful lifetime [3], the reliability and safety of any system is significantly compromised if recycled chips are used in it. Additionally, the dis-assembly, cleaning and restoration processes often employed to make a recycled part look new can also create other defects and anomalies [2]–[4] that can cause system malfunction.

Detection methods for recycled ICs can be broadly classified into two categories: test methods for detecting recycled ICs that are already in the market, and design for anti-counterfeit (DfAC) measures that can be implemented in new designs being readied for manufacturing. For the older designs, there are different standards (AS6171, AS5553, CCAP-101 and IDEA-STD-1010) currently in practice, which recommend conventional tests for detecting recycled ICs [5]–[8]. Among these standards, AS6171 has been adopted by the U.S. Department of Defense (DoD). The primary challenges in implementing the test methods recommended in these standards are excessive test time and cost, lack of automation, and low detection confidence. While DNA markings are now commercially available for providing traceability of electronic parts [9] in the supply chain, the complexity of the authentication process, and excessive test costs, limit their wide adoption by the semiconductor industry [10]. Over the years, a number of researchers have also proposed test methods based on statistical data analysis to identify recycled parts [11]–[16]. However, a large number of chips are often required for creating the statistical models, which may be difficult to acquire for obsolete ICs. In recent research, several design-for-anti-counterfeit (DfAC) measures have been proposed as an alternative to the conventional recycling detection methods [17]–[23]. Unfortunately, DfAC measures cannot be applied for detecting recycled ICs already manufactured and circulating in the market.

In this paper, we propose a novel approach for detecting recycled ICs with the help of the power-up state of one or more SRAMs available in the chip. Our proposed solution does not require any hardware modification to the existing design, and can be applied to a wide variety of SoCs that have SRAM based memory, including FPGAs. This solution can be applied to both, ICs already circulating in the market, as well as those to be manufactured in the future. The proposed approach is simple, effective and low-cost, and requires minimal test support: a capability to read out the initial power-up state of the on-chip SRAM. Our experimental results show that we

978-1-5386-8064-3/19/$31.00 ©2019 IEEE

can accurately detect if the IC has been used in operation for a period as little as few days.

Our new approach exploits the degradation in device threshold voltages caused by stress due to aging in operation. Unfortunately, identification of a chip as recycled based on parameter shifts over time critically requires the initial parameter values for a new and unused part against which any degradation in use can be evaluated. Prior approaches suffered from the lack of an accurate reference parameter due to the significant process variations that are experienced in IC manufacturing. Such starting differences in circuit parameters among new parts can often exceed any changes from aging in operation. This makes recycling detection virtually impossible, except for the highly unlikely case where the target parameters for individual ICs were measured at manufacture and are still available when the part is to be evaluated many years, even decades, later.

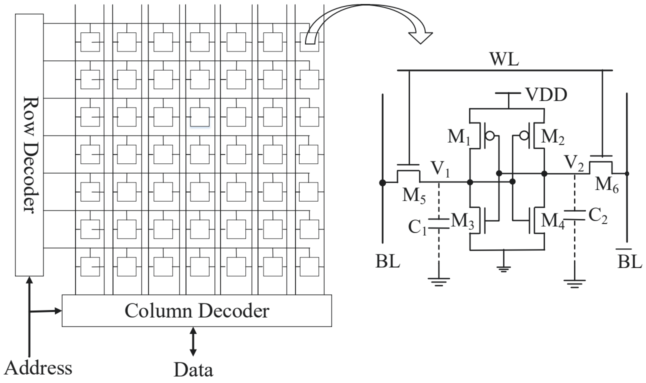
The critical innovation in our proposed approach is that it does not need such a saved reference. Instead, it exploits two key properties of SRAMs: (i) that individual SRAM cells are designed to be completely symmetric in layout (so as to maximize noise margins), and therefore completely unbiased with respect to the logic state they acquire at initial power-up, and (ii) any bias that is introduced by the random manufacturing variations can be in either direction with equal probability, *i.e.*, any imbalances in the memory cells caused by process variations result in an equal likelihood of the cell being biased to power up in either the 0 or 1 logic state. Consequently, in a newly manufactured SRAM, at initial power-up, the percentage of 1s in the memory cells should be the same as the 0s, both very close to 50% (typically well within one percent) because of the statistically large number of cells. This initial 50% statistic, which holds for all new SRAMs, forms a reliable base reference for a new memory.

The 50% number degrades over time due to asymmetric shifts in the SRAM cell transistor threshold voltages from Bias Temperature Instability (BTI), which is mostly observed to impact PMOS transistors as Negative BTI (NBTI) in traditional bulk technologies [24], [25]. (The discussion here equally applies to PBTI, which is also experienced by the NMOS transistors in some technologies.) Observe that it is virtually impossible for every individual cell in the memory to store a 1 and a 0 logic value for exactly the same total time during an operating life of arbitrary duration, and thereby always retain its initial bias in use. Any imbalance in this storage time results in asymmetric shifts in transistor threshold voltages in the cell from NBTI aging which causes changes in the cell power-up bias. Skewed data patterns in functional memory usage further ensure that these changes from operational stress with the cells result in a move away from the initial balanced 50% 1 and 0 cell bias. For example, Wei et al. [26] have reported that the ratio of 1s to 0s in most files is less than 50%. This number is even lower, at only 20 to 35%, for system files. In addition, many SRAMs, such as the block RAMs (BRAMs) in Xilinx FPGAs, are initialized to 0 [27], which again increases the fraction of time the memory cells are stressed in the 0 state. The detection of recycled ICs in the proposed approach is based on this inevitable shift in the percentages of 1s and 0s in the power-up state as an SRAM is used. We validate our methodology with results from ongoing silicon experiments in our effort to collect long term data.

The rest of the paper is organized as follows. Section II introduces the modeling of power-up state for an SRAM, and how it is impacted by the aging. Section III discusses the our proposed for detecting recycled SoCs. Experimental results are results are given in Section IV. Finally, we conclude our paper in Section V.

II. Effect of Threshold Voltage Variation on the Power-up State

The power-up state of an SRAM cell depends on the threshold voltages (v_{th}) of the MOS transistors. This section presents the effect of threshold voltages on the power-up state of an SRAM cell. Note that an SRAM array consists of multiple SRAM cells, and each cell consists of six transistors shown in Figure 1. The four transistors (M_1, M_2, M_3 and M_4) form a bistable latch to store 1-bit of data. BL, and $\overline{BL}$ provides the access to the latch through M_5 and M_6 transistors.



(a) A typical SRAM array. (b) A six-transistor SRAM cell.

Figure 1: Simplified architecture of an SRAM array and a six-transistor SRAM cell.

When an SRAM array is powered-up, initially each individual memory cell randomly acquires either a logic 0 or logic 1 value. During design, the MOS transistors in each matched pair ($M_1 - M_2$, $M_3 - M_4$ and $M_5 - M_6$ in Figure 1(b) are carefully made completely identical, including all their layout related parasitic components. The perfect symmetry of the memory latch in the SRAM cell maximizes noise margins during operation. Consequently, each SRAM cell should ideally have a 50% chance of acquiring either logic 0 or logic 1 when powered up, the actual value decided by random unbiased noise. However, in practice most MOS transistor pairs will not be perfectly matched due to random manufacturing process variations, the most significant of which, in the context of this discussion, are the small variations in the threshold voltages in each MOSFET. The v_{th} differences in the PMOS and NMOS transistor pairs can either cause a cell bias in the same direction or in opposite directions. The net imbalance decides the overall bias towards either 1 or 0 at power-up. A larger net imbalance in the transistor pairs result in a more skewed SRAM cell. If the net v_{th} difference is small, the power-up values may be still be somewhat random, with a bias towards either 0 or 1. On the other hand, for relatively large net v_{th} imbalances, the power-up state will be stable and always the same over multiple power-up cycles.

The effect of the transistor threshold voltages on the power-up behavior of an SRAM cell can be seen in more detail with the help of Figure 1(b). The SRAM cell is basically two inverters connected in a ring. The output of one inverter is connected to the BL. Similarly, the output of the second inverter is connected to $\overline{BL}$. We model the output node capacitances by adding two lumped capacitors, C_1 and C_2, at node 1 (output of inverter 1) and node 2 (output of inverter 2), respectively. The effect of the transistors (M_5, and M_6) on the power-up state can be mostly ignored as they remain off during the power-up time. At the design stage, all transistors are balanced so that $M_1 - M_2$, and $M_3 - M_4$ have the same parameters, and all parasitics are same for both inverters. Assume (for simplicity) that after manufacture, the threshold voltage changes only for M_1 due to process variation, and it's threshold voltage increases (in magnitude) to v_{t1}^*. Initially, the threshold voltages for both M_1 and M_2 were identical, i.e. $v_{t1} = v_{t2}$. Clearly after manufacturing, $v_{t1}^* > v_{t2}$. If we consider a relatively fast ramp rate at the power supply during the power-up time, this PMOS transistor mismatch will decide the state of the SRAM cell [28]. As the v_{th} of M_1 is larger (in magnitude) than M_2, M_2 with the smaller threshold magnitude will turn on first, forcing it's output high and the complimentary M_1 output low. The cell will power-up to 0.

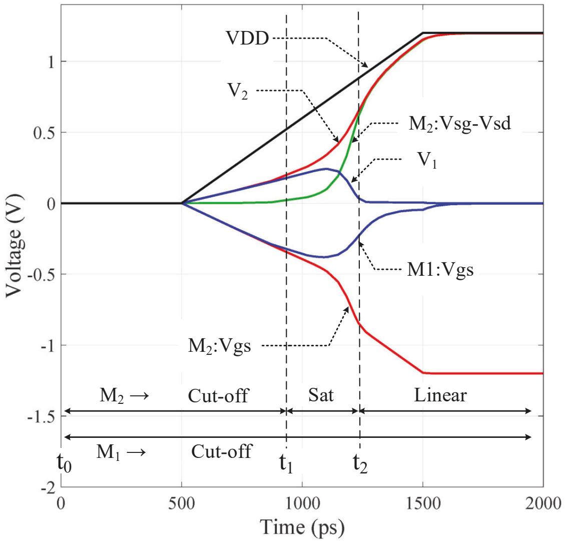


Figure 2: Timing diagram of internal nodes of an SRAM Cell during the power-up.

Figure 2 shows the timing diagram of the potentials at different nodes of a single SRAM cell using the Synopsys HSPICE simulation tool. $32nm$ bulk Predictive Technology Model (PTM) is selected for the simulation. The nominal threshold voltages (v_{th}) of NMOS, and PMOS transistors are 0.42252V and -0.41174V, respectively. To simplify the situation, the process variation in NMOS transistor parameters have been ignored. The new threshold voltage of M_1 (v_{th1}^*) has been increased 20% (in magnitude) from its nominal value. Initially, the potentials at node 1 (V_1) and node 2 (V_2) rise at the same rate. The currents, I_1 and I_2, result from the subthreshold leakages of M_1, and M_2. The potentials V_1 and V_2 are of the same order. At time t_1, transistor M_2 goes to saturation as $V_{sg} - V_{sd} < |v_{th}|$ and $V_{sg} > |v_{th}|$. On the other hand, transistor M_1 still remains in the cutoff region as $V_{sg} < |v_{th}|$. This happens due to $v_{t1}^* > v_{t2}$. We observe a sharp rise in V_2, as M_2 is in saturation and can provide much larger current ($I_2 \gg I_1$). Finally at time t_2, transistor M_2 goes to the linear region as $V_{sg} - V_{sd} > |v_{th}|$ and $V_{sg} > |v_{th}|$, and we observe a different slope in V_2. Note that transistor M_1 never gets out of the cut off region.

III. Proposed Approach for Detecting Recycled System on Chips

Detection of used and recycled SoCs can be performed effectively by observing either the percentage of 1s ($\%1s$) or percentage of 0s ($\%0s$) in the power-up state of an on-chip SRAM. As discussed earlier, the requirement for a reference parameter from the chip in the unused state, which is generally needed to make a decision whether the chip recycled or not, is not necessary. This is because the $\%1s$ and $\%0s$ are known to virtually identical in a new chip, typically to well within a percent. Detection can easily be carried out by observing even a small change in $\%1s$ from this reference value of 50%. In this section, we will provide a more in-depth analysis of our proposed counterfeit detection approach, particularly with regard to how the SRAM start-up state is impacted by process variations and device aging in operation.

A. Effect of Process Variation on Transistor Threshold Voltages

Process variations (PV) cause the threshold voltage of a transistor to vary from its nominal value [29], [30]. This variation has two components – (i) systematic variation and (ii) random variation [31]. Systematic variation is the variation among different dies (chips or regions in chips), and may resulted from the imperfections in the lithographic process (mask alignment errors, lens aberrations, etc.), and small changes in the environmental conditions during the fabrication. It moves the threshold voltage of all transistors of chip in one direction. On the other hand, random process variation is the variation among the MOS transistors within a die. In advanced technology nodes, this arises from factors such as the random fluctuations in the numbers of dopant atoms in the channel, gate line edge roughness and surface orientation [32]–[34].

Random variations are commonly modelled using the zero mean Gaussian process [31].

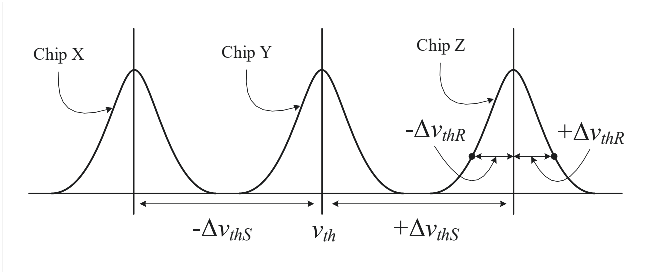


Figure 3: Systematic and random process variations.

Figure 3 shows plots of the resulting variations, where the mean of the random variation within each chip is determined by the systematic variation. The threshold voltage of a transistor can be represented as: $v_{th} = v_{th0} \pm \Delta v_{thS} \pm \Delta v_{thR}$, where Δv_{thS} and Δv_{thR} represent the change in threshold voltage due to systematic and random variations, respectively. The threshold voltage difference between the two PMOS and NMOS transistors in a SRAM cell (see Figure 1(b) will result from the random process variation, as the systematic variation moves the v_{th} for all the transistors in a chip in the same direction. This can be described as:

$$\begin{aligned} \Delta v_{th} &= v_{th1} - v_{th2} = (v_{th0} + \Delta v_{thS} + \Delta v_{thR1}) \\ &\quad -(v_{th0} + \Delta v_{thS} + \Delta v_{thR2}) \\ &= \Delta v_{thR1} - \Delta v_{thR2} \end{aligned} \tag{1}$$

where v_{th0}, Δv_{thS}, and Δv_{thR} represent nominal threshold voltage, systematic and random v_{th} variations, respectively. From Equation 1, we can conclude that the distribution for Δv_{th} will be zero mean Gaussian, since the distribution for random process variation is zero mean Gaussian. This reveals the interesting fact that there is a 50% probability of v_{th1} is greater than v_{th2}, and vice versa.

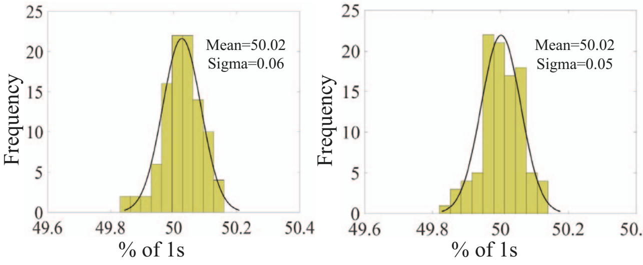
B. Effect of Aging on the Power-up State

The threshold voltage of a transistor increases under operational stress when the chip is used in the field. This is also true for an SRAM circuit, when it is used for storing data. One of the main aging phenomena in ICs is negative bias temperature instability (NBTI), which occurs in PMOS transistors when they are negatively stressed [24], [25]. Interface traps are created at the Si-SiO_2 interface of PMOS transistor when its gate is pulled down to logic 0. Releasing the stress can achieve some but not complete recovery. As a result, the threshold voltage (v_{th}) of PMOS transistors increases over time [35]. This increase tends to saturate over a period of months, and becomes minimal after 5-10 years in use. 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). NMOS transistors experience much smaller threshold shifts from PBTI aging, although that may change at advanced technology nodes. A different aging phenomenon in CMOS circuits is hot carrier injection (HCI). [36], [37]. Some high energy electrons can attain sufficient energy when the transistor is conducting (on) to get trapped in the Si-SiO_2 interface near the drain terminal due to the lateral gate electric field. NMOS transistors are primarily affected by HCI because of higher carrier mobility, whereas it has very little effect in PMOS transistors [38]. Observe, however, that HCI occurs when there is current flow in the transistor channel. In practice, the impact of HCI in SRAM cells is minimal, and can be ignored, because the transistors in memory cells are mostly non-conducting and experience much less switching activity than logic.

The effect of aging on the power-up behavior of an SRAM cell can be explained using Figure 1(b). To begin with, we ignore process variation and assume all the transistor pairs possess the same device parameters. As a result, the threshold voltages of (M_1 and M_2) have same value ($v_{t1} = v_{t2}$). Similarly (M_3 and M_4) are identical. (We ignore any PBTI aging in the NMOS transistors.) Assume that for some initial period, the cell contains 1 ($BL = 1$, and $\overline{BL} = 0$), which sets the internal nodes $V_1 = 1.2V$, and $V_2 = 0V$. Consequently, the transistor M_1 will experience aging due to NBTI (as its V_{gs} is negatively stressed) and its threshold voltage will increase in magnitude over this time to $v^*_{t1} (> v_{th})$. Based on discussion in the previous subsection, this SRAM cell is now biased and will power-up with logical 0 ($V_1 = 0$ and $V_2 = 1$) as threshold voltage of M_1 becomes larger (in magnitude) than M_2 after aging. *If we age the cell with 0, it will power up with 1 (and vice versa), for a perfectly balanced SRAM cell.*

C. Effect of Noise on the Power-up State

The power-up state of an SRAM can be affected by the noise, and percent of 1s in the power-up state of an SRAM array can vary from the mean (*i.e.*, 50%). We perform an experiment to analyze the effect of noise on the power-up state. A commercial off-the-shelf (COTS) SRAM (Microchip 23A640-I/SN: SPI Bus Low-Power Serial SRAM) chip is powered up 100 times and its power-up states are measured. Figure 4 shows the histogram plot of the percentage of 1s in the power-up states. We also perform the same experiment for different environmental conditions to determine the effect of noise in the power-up states.



(a) 25˚C (b) 50˚C

Figure 4: Effect of noise on the power-up state of an SRAM array.

We observe a Gaussian distribution for percentage of 1s with mean (μ) of approximately 50% for two different (25°C and 50°C) environmental conditions. The standard deviation (σ) also varies slightly at different environment corners (see Figures 4.a and 4.b). The value of σ is 0.06, and 0.05 when we perform the experiment at 25°C and 50°C, respectively. We can conclude from this experiment, that the noise has little effect on the power-up behavior of an SRAM array.

D. Proposed Approach based on Memory Power-up State

As the percentages of 1s and 0s in the power-up state of an SRAM array are virtually identical in a new chip, we can detect recycled ICs using this information. When a chip ages, the mean value of percentage of 1s (or percentage of 0s) shifts over time, and a decision can be made based on this shift. Note that this proposed solution does not require any hardware modification in any way to an existing design, and thus can be applied to a wide variety of SoCs, which contain SRAM memory. This approach is designed for detecting old chips, those are already circulating in the market. It is not necessary to have any knowledge of the inner details of the circuit to determine whether a chip is recycled or not.

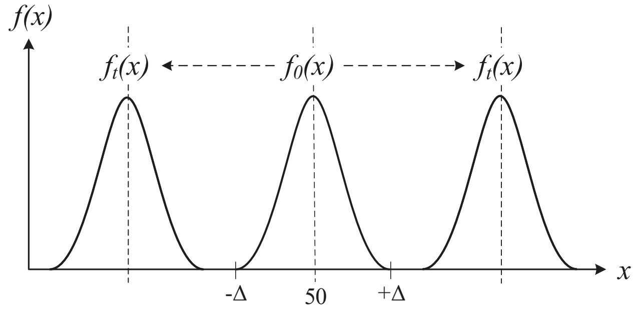
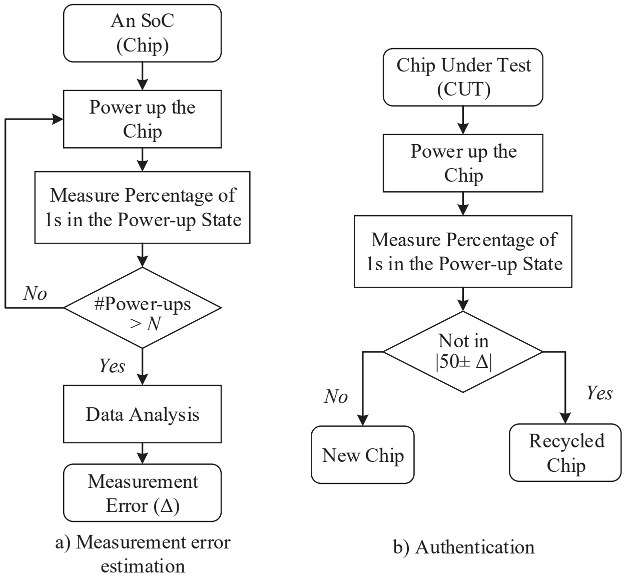


Figure 5: The probability density functions of %1s over time.

Figure 5 shows the distribution of %1s (represented as $f()$ with variable x) for a new chip and old chip, respectively. The distribution for a new SRAM chip ($f_0(x)$) is centered near 50% as the random process variation is a zero mean Gaussian process. There is an equal probability that an SRAM cell will power up either 1 or 0. Due to the noise, the %1s can vary slightly and we observe a Gaussian distribution (see Figure 4). During normal operation, the data stored in an SRAM chip causes biasness and can age an SRAM cell opposite towards its stability. Moreover, majority of the on-chip SRAMs are initialized to 0 (or 1) until the memory is overwritten with a random data. As a result, the distribution of %1s for an old SRAM chip ($f_t(x)$) can either shift to right or left. We can clearly identify a recycled chip if the %1s distributions, $f_0(x)$ and $f_t(x)$, do not overlap each other. Misprediction (*i.e.*, recycled ICs identified as new and vice versa) may arise if these two distributions overlap. Note that the impact of noise can be minimized while considering a large SRAM array. The spread of %1s distribution from a COTS SRAM with 64K bits is very small (*i.e.*, $\sigma = 0.06$).



a) Measurement error estimation

b) Authentication

Figure 6: Proposed approach for detecting recycled ICs using memory power-up state.

The proposed approach for detecting recycled ICs using the memory power-up state is illustrated in Figure 6. Note that it is not necessary to know the value of measurement error (Δ), when a chip is used more than a week (see silicon results in Section IV). However, it is necessary to determine Δ due to the noise, which impacts the power-up state of an SRAM, and this process is depicted in Figure 6.a, when the chips are manufactured. The process of measuring Δ is described as follows:

- *Step-1*: The power-up state of the SRAM array is recorded after powering up an SoC.
- *Step-2*: The percentage of 1s ($\%1s$) is measured from the recorded power-up state.
- *Step-3*: *Step-1* and *Step-2* are repeated N (large enough for statistical inference) times. We perform 100 power-ups to plot the distribution, which is shown in Figure 4.
- *Step-4*: Data analysis is performed to measure Δ from the distribution. We can choose 3σ as the measurement error Δ, and record this value for future.

It is recommended that this process is repeated with more than one SoC to accurately measure the effect of noise. In addition, measurement at different environmental conditions (*e.g.*, 50°C) helps up to measure Δ, such that accuracy of identifying a chip is recycled is increased. The effect on the noise can also be minimized using considering larger size memory.

The authentication process of determining a chip being recycled is a straight forward process, and shown in Figure 6.b. The Chip Under Test (CUT) is powered up and its power-up state is recorded. The percentage of 1s in the power-up state is calculated. If the $\%1s$ does not fall within $50 \pm \Delta$, the chip can be identified as recycled chip; otherwise, it is new. Note

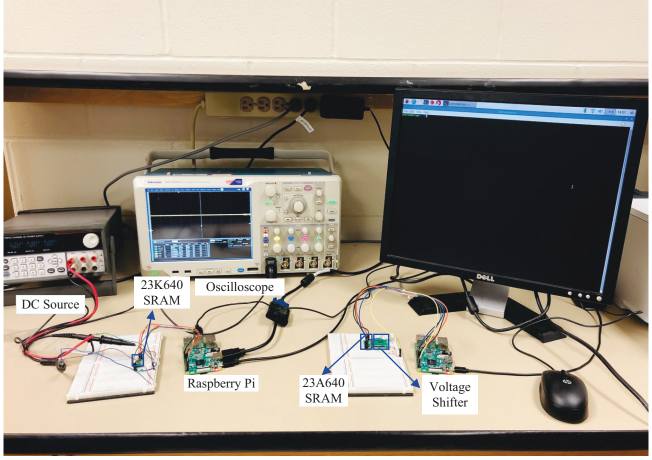


Figure 7: Experimental set-up to measure SRAM power-up states.

that it is not necessary to have the information of Δ during authentication. As the shift of the distribution (*e.g.*, shift in mean μ) is much larger than Δ (see the silicon data in Section IV), a decision can be made just observing this shift.

IV. Silicon Experimental Results

This section presents a detailed analysis of the effect of aging in the power-up state of SRAM arrays. We have conducted experiments using two different types of commercial off-the-shelf (COTS) SRAM memories to demonstrate the effectiveness of our proposed approach for detecting recycled ICs. These are Microchip 23A640-I/SN [39], and 23K640-I/SN [40] SPI Bus Low-Power Serial SRAM memories. The total memory capacities of both SRAM chips are 64K bits .

Figure 7 shows the experimental set-up for measuring the power-up state of these Microchip SRAMs. The supply voltage for chip 23A640 is 1.8V. It is thus necessary to use a voltage shifter to interface with the Raspberry Pi, which is programmed to collect the power-up states of these SRAMs. We use Texas Instruments PCA9306 Dual Bidirectional I^{2}C Bus and SMBus Voltage-Level Translator [41] for this purpose. On the other hand, we can directly interface the Raspberry Pi with Microchip 23A640 due to its supply voltage requirement is 3.3V. The first set of experiments are conducted at the room temperature. *Note that new SRAM chips must be used at the start of each new experiment to ensure a starting 50% distribution of 1s and 0s.*

Figure 8 shows the distribution of 1s ($\%1s$) at the power-up state for a Microchip 23A640 memory chip (denoted as Chip 1). The power-up states of this SRAM chip are measured 100 times, and the $\%1s$ distributions are plotted. The chip is aged after loading and then holding all 0s in all the memory locations. After 3 days of aging interval, the power-up states of the SRAM chip are collected 100 times, and the $\%1s$ distributions are plotted. From the figure, we observe that the initial distribution for the new chip is quite tight and centered almost exactly at 50% (*e.g.*, $\mu = 50\%$). The distribution significantly shifts rapidly towards the right once the chip is aged. The non-overlapping property of the new and aged SRAM distributions indicates that we can reliably detect recycled ICs by observing $\%1s$ in the SRAM power-up states.

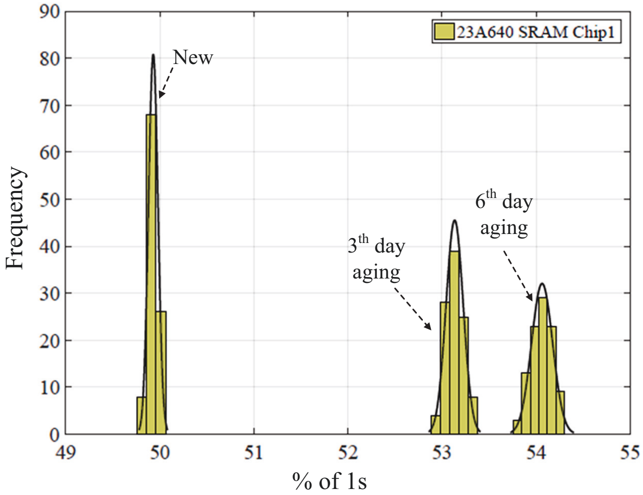


Figure 8: The distribution of $\%1s$ on the power-up states for Microchip SRAM chips.

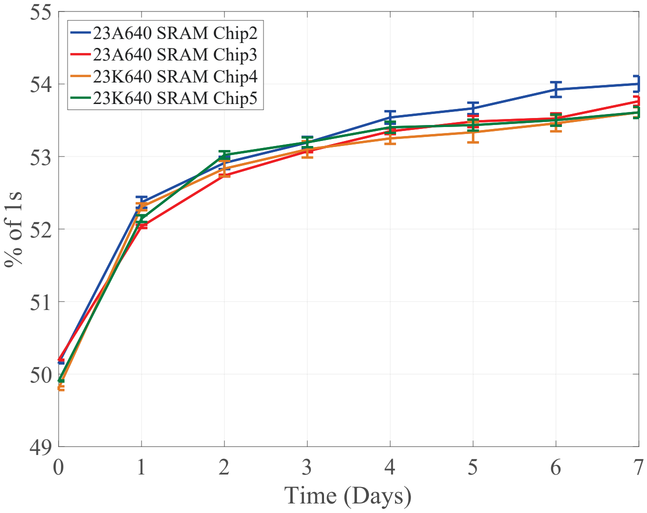


Figure 9: The shift of mean of $\%1s$ distribution over time.

The initial reference value (approximately 50% of 1s in the power-up state) shifts over time due to asymmetric shifts in the V_{th} of transistors in SRAM cells from Bias Temperature Instability (BTI). It is thus necessary to study how the mean of $\%1s$ distributions shift over time to ensure the accurate detection of recycled ICs. We have analyzed four Microchip SRAMs (two 23A640 and two 23K640) to reliably evaluate this shift. Figure 9 shows the change in mean of the of $\%1s$ distribution. Each point on this plot is bounded by $\pm 3\sigma$ over the mean (μ) of the $\%1s$ distribution. The μ and σ values are computed over 100 measurements of the power-up states

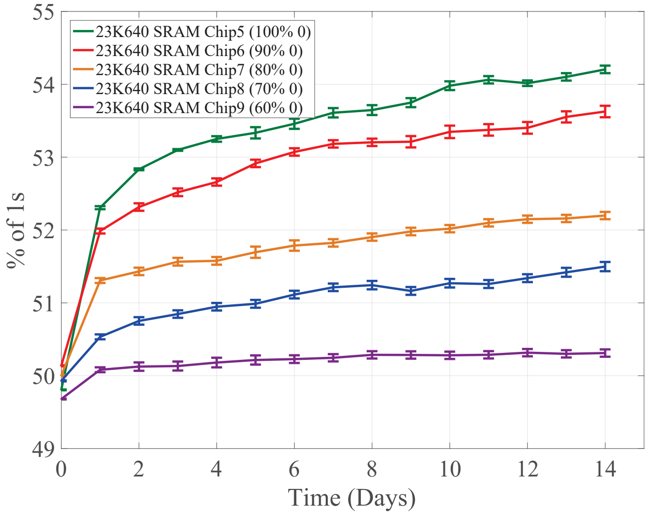


Figure 10: The shift of mean of $\%1s$ distribution over time with different work load.

after every one day of aging. The mean of $\%1s$ distribution changes around 2% after one day of aging. The mean changes at an accelerated rate over the early period of aging. After a week of aging, we have observed a shift of around 4% for all the SRAM chips. We also observe a minor increase in the standard deviation once the chip is getting aged. However, these 3σ values are much smaller than the change in μ values.

While the first set of experiments stress the SRAM chips with 0s in all locations, it is also important to study the shift of the μ of $\%1s$ distribution from stress caused by normal operation, as this would occur in typical use in the field. Even in this scenario, the data bits in an SRAM memory are not random over time. It has been reported that there are usually more 0s (65-80%) [26]. Therefore, to mimic the normal operation, we perform aging with data that with different percentage of 0s. We choose five new SRAM chips (Microchip 23K640) and perform aging with 100%, 90%, 80%, 70% and 60% of 0s stored in them. We update the contents of the SRAM chips in every 5 minutes during the aging to mimic the realistic operation in the field. The experiment for aging is conducted at room temperature. Figure 10 shows the shift of μ of $\%1s$ distribution over time. The x-axis represents the normal aging time and y-axis represents the μ of $\%1s$ distribution. This figure provides an insight that rate of aging degradation depends on the percentage of 0s. If we perform aging with more zeros, the percentage shift becomes larger. For example, the μ of $\%1s$ becomes 52.30%, 51.98%, 51.30%, 50.5%, 50.08% after one day of aging, while the aging pattern contains 100%, 90%, 80%, 70% and 60% of 0s, respectively. After 14 days of aging, we observe a shift of 4.20%, 3.62%, 2.20%, 1.49%, 0.63% from their initial approximate 50% value for SMAM Chip 5, 6, 7, 8 and 9, respectively.

As the rate of shift for $\%1s$ distribution when aged with 60% of 0s is comparatively low, accelerated aging is performed using a ThermoSpot direct contact probe system (see experimental setup for accelerated aging in Figure 11). This system is an industry standard benchtop temperature cycling system, used for accelerated aging [42]. The device supports temperatures ranging from -65°C to 175°C, with a transition rate of less than 35 seconds over 25°C to -40°C. Accelerated aging has been performed at $85°C$ with "functional" random patterns, which contain 60% 0s and 40% 1s.

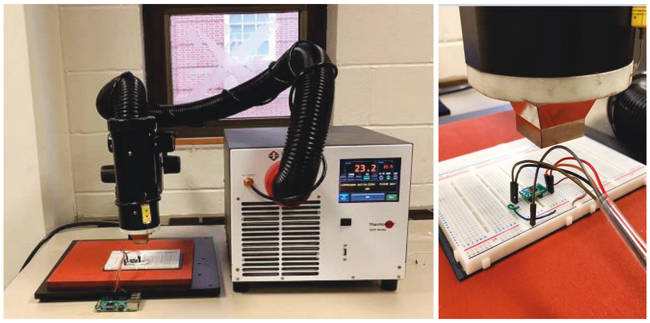


Figure 11: Accelerated aging set-up using ThermoSpot direct contact probe system [42].

Figure 12 shows the distribution of $\%1s$ with 60% 0s during the aging. The update of SRAM contents are performed in every 5 minutes while aging like before. The power-up states are also measured 100 times when the chip is cooled down to the room temperature. We have noticed the change of the mean at an accelerated rate compared to Figure 10. Approximately, 1% change in mean is observed after 2 Hrs of accelerated stress. Similar trend for the rate of change of the mean is also observed. Finally, we see a change of 2.23% after 70 hours of accelerated stress.

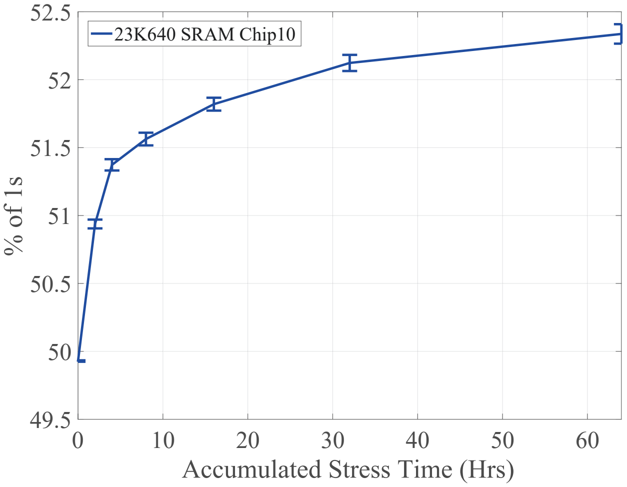


Figure 12: The distribution of $\%1s$ on the power-up states for Microchip 23K640 by aging with random patterns that contains 60% 0s and 40% 1s at $85°C$.

The final set of experiments are conducted to analyze the recovery from the aging degradation. The recovery of transistor threshold voltages is common when a device experiences no

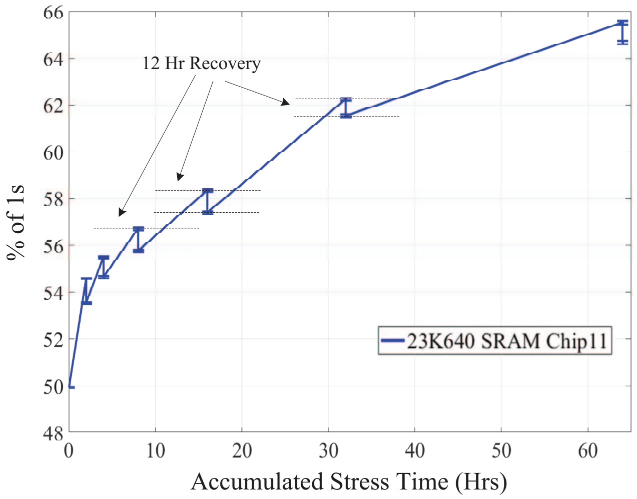


Figure 13: Accelerated aging and normal recovery.

stress. We have carefully looked and analyze the shift of $\%1s$ distribution when a chip sits on the shelf. First, we performed an accelerated stress to age the chips at a much faster rate and then relax the chip for 12 hours. Figure 13 shows the aging and recovery behavior for an SRAM memory (Chip 11). The chip has been aged with all 0s to accelerate the aging degradation. The power-up states are measured after the chip is cooled down to the room temperature as before. After 2 hours of accelerated stress, 4.68% change in the mean of $\%1s$ distribution is observed. We find a 1.04% of recovery occurred after 12 hours of relaxation. The amount of recovery gets reduced when the chip is relaxed multiple times. For example, we observed 0.7% of recovery after 32 hours of accumulated stress.

We also analyzed the recovery of these chips when they are sitting on the shelf. As aging was performed at different times, all our aged SRAM chips get time to recovered as if they are in the shelf. Table I summarizes the result. The first column of this table represent the recovery time period for each selected chips. Next two columns indicate the specific chip number and previous aging condition (whether aging is performed at an elevated temperature or not). The fourth and fifth columns represent the initial % of 1s (before the start of aging) and final % of 1s (after completion of aging). Finally, the last column represents the % of Δ recovery, which can be defined as the following equation:

$$\%\ of\ \Delta\ \text{Recovery} = \frac{\mu_F - \mu}{\mu_F - \mu_I} \times 100\%$$

where,
μ_F : Mean of $\%1s$ distribution when aging is complete.
μ_I : Mean of $\%1s$ distribution before aging is started.
μ : Mean of $\%1s$ distribution when measurement for recovery is performed.

From Table I, we can observe that chip can experience about 15% recovery for first day. The recovery slows down significantly afterwards. For example, the chip only gets a cumulative recovery of 20% in 8 days and then 22% in 10 days. However, we observe a different behavior for Chip 11. It only recovers 5% in 4 days. This anomaly can be explained as this chip have already experienced multiple recovery cycles during the accelerated aging experiment (see Figure 13).

Table I: Recovery of aged chips sitting on the shelf.

Recovery Time	**SRAMs**	**Aging Condition**	**Initial $\%1s$**	**Final $\%1s$**	**% of Δ Recovery**
1 day	Chip 8	Normal	49.929	51.232	15.70
4 days	Chip 11	Accelerated	49.919	64.080	5.09
8 days	Chip 7	Normal	50.002	52.027	19.68
10 days	Chip 5	Normal	49.805	54.626	22.10

It is practically infeasible to recover all degradation, and we have shown that some amount of aging can be recovered if the chips remain idle. In conclusion, the recovery is never complete, and majority of the aging degradation typically remains. From this analysis, we can safely conclude that recycled chips can be detected even though they are on the shelf for a long time.

V. Conclusions

The excessive growth of recycled ICs in the DoD and other critical infrastructures poses a serious threat because of their inferior quality, shorter remaining life and lower performance. Lack of efficient detection and avoidance technologies make our critical infrastructure vulnerable to these counterfeit chips. In this paper, we have presented a low-cost approach to detect the recycled SoCs using the power-up state of on-chip memories. This method does not require any prior information regarding a chip, which makes this solution well suited for the chips already circulating in the market. Our solution can be attractive to different test laboratories as it requires a simple test setup which consists of a extremely low-cost Raspberry Pi to read out the SRAM state. We have validated our proposed method using two different types of commercial off-the-shelf SRAM chips and have shown the efficiency of detecting recycled chips.

Acknowledgment

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

[10] Semiconductor Industry Association (SIA), “Public Comments - DNA Authentication Marking on Items in FSC5962,” November 2012.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[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] D. Wei, L. Deng, P. Zhang, L. Qiao, and X. Peng, “Nrc: A nibble remapping coding strategy for nand flash reliability extension,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1942–1946, 2016.

[27] 7 Series FPGAs Memory Resources User Guide, https://www.xilinx.com/support/documentation/user_guides/ug473_-7Series_Memory_Resources.pdf.

[28] 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.

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

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] K.-L. Chen, S. Saller, I. Groves, and D. Scott, “Reliability effects on mos transistors due to hot-carrier injection,” *Electron Devices, IEEE Transactions on*, vol. 32, no. 2, pp. 386 – 393, February 1985.

[37] S. Mahapatra, D. Saha, D. Varghese, and P. Kumar, “On the generation and recovery of interface traps in mosfets subjected to nbti, fn, and hci stress,” *Electron Devices, IEEE Transactions on*, vol. 53, no. 7, pp. 1583 –1592, July 2006.

[38] 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.

[39] Microchip 23A640/23K640: 64K SPI Bus Low-Power Serial SRAM, https://www.mouser.com/datasheet/2/268/22126B-54007.pdf.

[40] Microchip 23A640/23K640: 64K SPI Bus Low-Power Serial SRAM, http://ww1.microchip.com/downloads/en/DeviceDoc/22126E.pdf.

[41] PCA9306 Dual Bidirectional I2C Bus and SMBus Voltage-Level Translator,http://www.ti.com/lit/ds/symlink/pca9306.pdf.

[42] ThermoSpot DCP-201-1010-2 ThermoStream Thermal Inducing System.