A Novel Self-referencing Approach Using Memory Power-up States for Detecting COTS SRAMs

Gaines Odom
Electrical and Computer Engineering
Auburn University
Auburn, AL, USA
gaines.odom@auburn.edu

Zakia Tamanna Tisha
Electrical and Computer Engineering
Auburn University
Auburn, AL, USA
zakia.tisha@auburn.edu

Ujjwal Guin
Electrical and Computer Engineering
Auburn University
Auburn, AL, USA
ujjwal.guin@auburn.edu

***Abstract*—The surge in counterfeit Integrated Circuits (ICs) in the electronics supply chain, particularly those reclaimed from recycled components of old and discarded electronics, poses a significant threat to our critical infrastructures. Unfortunately, this threat persists due to the absence of effective detection techniques. In pursuing a reliable detection method, a previous study introduced the idea of identifying recycled ICs using SRAM power-up states, leveraging the inherent symmetry in the logic states of 0s and 1s in newly manufactured SRAM cells. However, in SRAMs produced with older technology nodes, the reference parameter of 50% 1s is often less prominent due to systematic design variation biasing all cells in a specific direction. To address this challenge, this paper proposes a robust self-referencing approach for detecting recycled ICs. The power-up states of an IC under test are segmented into subregions for similarity analysis of the percent of 1s within them. Our study establishes that the percent of 1s in all subregions of a newly manufactured IC is statistically more similar to each other than that in a recycled IC. Our experimental results demonstrate a substantial rise in the standard deviation of the percent of 1s for subregions in the aged SRAM, occurring after just a few days of aging. This approach aims to enhance the reliability of counterfeit IC detection, particularly in the context of older technology nodes where conventional methods may fall short.**

***Index Terms*—Recycled IC, SRAM power-up state, process variation, aging.**

I. Introduction

The rising threat of counterfeit integrated circuits (ICs) and system-on-chips (SoCs) obtained from discarded electronics being recycled and sold as new continues to grow due to the lack of effective detection techniques. The entry of such knock-off ICs into key systems comprising the critical global infrastructure can result in system and security failures with potentially disastrous consequences for societal well-being. IHS Inc. has reported that counterfeit ICs represent a potential annual risk of $169 billion in the global supply chain [1]. These recycled ICs often exhibit poorer reliability, reduced useful remaining lifetime, and degraded performance [2], [3]. The crude process of disassembly, cleaning, and restoration often employed to a recycled part as new can also create additional defects, resulting in electrostatic damage and other anomalies that can cause system malfunction [2]–[5]. As most Department of Defense (DoD) infrastructures are designed well beyond their lifetime of electronics, they are critically dependent on a continuing supply of legacy commercial off-the-shelf (COTS) components for maintenance and repair and often encounter recycled parts. It is thus essential to detect counterfeits efficiently to prevent the widespread infiltration of these parts in the semiconductor supply chain.

979-8-3503-6378-4/24$31.00 ©2024 IEEE

This paper aims to develop reliable electrical aging-based counterfeit detection tests using self-referencing methods. As the degradation of electrical parameters from aging is comparable with manufacturing process variation, prior approaches require storing device-specific parameters for all new ICs for later use as the reference parameter, which is practically infeasible considering all different part types. This paper's proposed robust self-referencing test methodologies address the shortcomings of the prior approaches and have the following properties for broad adoption. First, these tests will not require the generation of databases of characterization tags for every new IC. Second, no hardware modification to an existing design is necessary to implement these tests to target various chips, including older legacy COTS parts. Finally, the test laboratories do not need to know the circuit details of a chip. Only accessing memory is required to obtain the power-up states.

The test method developed by Guin et al. [6] detects recycled ICs that use the 50 percent (%) 1s in the SRAM power-up states as the time zero reference parameter. As all the SRAM cells are designed to be completely symmetric in layout to maximize noise margins, an unbiased SRAM cell powers up a state equally likely to logic 0 and logic 1, resulting in a close 50% of 1s ($p1s$) or 0s ($p0s$) in a newly manufactured SRAM chip. This is because the statistically significant number of cells in an SRAM array cancels the effect of noise and random process variation, which is Gaussian. The above approach for identifying recycled SRAMs has shown potential in identifying recently manufactured chips where random process variations dominated over design variations. The systematic variation from the fabrication mask designs can play an important role in the power-up state. Often, in such legacy SRAMs, the combined effect of random process variations and aging stress is too small to influence the power-up state due to this stronger systematic design bias. This changes the balance of the power-up statistics of 50 $p1s$.

This paper presents a novel approach, using self-referencing, to detect COTS SRAMs where the initial power-up statistics of 1s and 0s are not symmetric to 50%. The self-referencing approach relies on differential aging resulting from the asymmetry of the 1s and 0s in the data stored on the SRAM chip during normal operation. Previous studies, such as the work by Guin et al. [6], have established that an SRAM cell

is more likely to power up with a 1 if it has been aged with a 0. Consequently, the portion of the SRAM chip that initially contains more 1s during the aging process is likely to power up with more 0s and vice versa. This inherent differential aging phenomenon manifests in the variance of the $p1s$ (or $p0s$) when the SRAM power-up state is divided into smaller regions and $p1s$ ($p0s$) is computed for each. Our experimental findings reveal a significant increase in the standard deviation (σ) in an aged SRAM when contrasted with the new SRAM after merely a few days of aging. This increase in variance demonstrates the efficacy of the self-referencing approach in detecting deviations from symmetric power-up statistics, providing a promising avenue for detecting recycled ICs.

The rest of the paper is organized as follows. Section II covers prior works on the detection of recycled ICs. Section III elaborates on the underlying principle of the self-referencing test method introduced in this paper. We present and analyze the experimental findings in Section IV. Finally, we conclude the paper based on our findings in Section V.

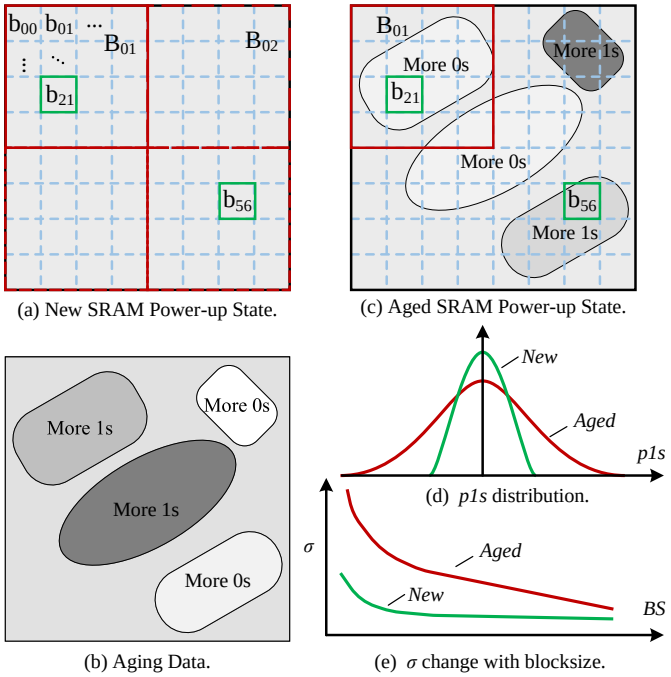
II. Prior Work

Extensive prior work has been performed on identifying recycled ICs through different tests, including physical inspection, electrical tests, aging data analysis, design-for-anti-counterfeit, and image processing methods. Several standards have been developed (*e.g.*, AS6171 [7], CCAP-101 [8], and IDEA-STD-1010 [9]), which recommend physical inspection and electrical tests for counterfeit detection. These tests primarily focus on detecting significant defects and anomalies in the recycled parts. However, used parts extracted from discarded electronics with minimal physical damage can often escape detection.

While traditional physical and electrical tests aim to detect physical damage to identify used and recycled parts, statistical data analysis approaches attempt to target the circuit's electrical degradation (wear-out) from mechanisms such as NBTI using statistical references from a large and diverse collection of new parts [10]–[13]. In addition, Several Design-for-Anti-Counterfeit measures have been proposed as an alternative to the conventional test methods [14]–[23]. Unfortunately, all of these solutions require on-chip hardware and cannot be applied to older ICs already in use and circulating in the market.

Recycled IC detection using machine learning through images from optical and X-ray inspections can also be used [7], [9], [24]–[27]. Training in the machine learning approaches requires new chips, which may not be readily available for obsolete or legacy parts. As counterfeiting is an evolving threat, re-training the machine learning model becomes necessary as counterfeiters improve their process technologies over time.

Thus, identifying a chip as recycled based on either electrical parameter shift or physical inspection over time critically requires the initial parameter values for a new and unused part against which any degradation can be evaluated. These prior approaches suffered from the lack of an accurate reference parameter due to the significant process variations 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 improbable cases where the target



(a) New SRAM Power-up State. (b) Aging Data. (c) Aged SRAM Power-up State. (d) *p1s* distribution. (e) σ change with blocksize.

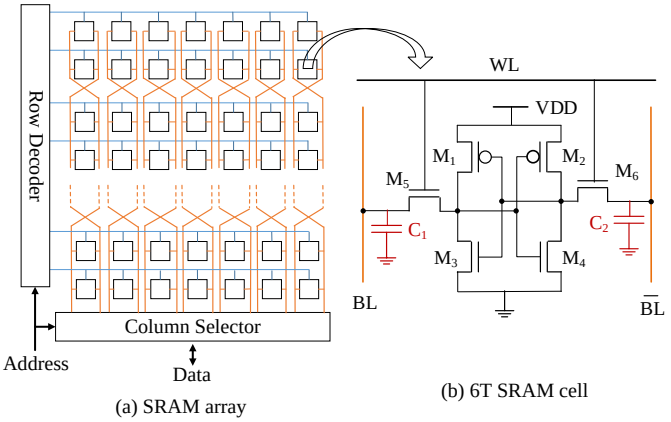
Figure 1: Conceptual view of differential aging-based recycled IC detection.

parameters for individual ICs were measured at manufacturing and are still available when the part is to be evaluated many years, even decades later. To address these shortcomings, Guin et al. developed an effective approach that uses the 50% 1s in the SRAM power-up states as the golden reference parameter [6]. Unfortunately, the legacy COTS SRAM chips, manufactured with older technology nodes, do not have a uniform distribution of 1s and 0s in the power-up state, and 50% of 1s can not be used as the reference parameter.

III. Proposed Self-Referencing Approach

The core principle of the self-referencing approach is centered on the hypothesis of differential aging within SRAM cells. It posits that, over time, these cells may undergo distinctive aging degradation, thereby impacting their power-up characteristics. This premise delves into the dynamic nature of aging degradation, emphasizing the influence of non-uniform data stored in the array, which contributes to non-uniformity in the aging process. The initial power-up state of a new device exhibits uniformity, determined almost entirely by random manufacturing process variation. Previous research has indicated that subjecting an SRAM cell containing a particular logic value during the aging results in a gradual reduction of the probability of the memory cell initializing to the same logic value upon successive power-ups [6].

When this characteristic is extrapolated to the entire device, it becomes evident that the power-up state exhibits a growing inverse correlation with the loaded data over time. In other words, if a device is aged with a deterministic dataset, its power-up state begins to mirror determinism. Consequently, it is no longer solely determined by incidental factors; instead, the power-up state of an SRAM device invariably succumbs to



(a) SRAM array (b) 6T SRAM cell

Figure 2: An SRAM array with bitline twisting.

aging effects over time. As the uniformity of power-up values deteriorates, certain sections or "blocks" of this power-up state retain logic-1 or logic-0 values inconsistent with the average incidence rate of these values across all memory cells in the device.

Figure 1 shows the overall concept of recycled IC detection using the self-referencing approach. In the power-up state of a new SRAM device, logic 1s, and logic 0s are uniformly distributed due to Gaussian manufacturing process variation, as depicted in Figure 1(a). Consequently, blocks of varying sizes, such as B_{01}, B_{02}, and smaller ones like b_{21}, b_{56}, will exhibit similar statistics of logic 1s, denoted as $p1s$. Conventionally, the data stored in SRAM during normal operation, such as firmware for an IoT device, does not exhibit a uniform distribution of 1s or 0s. Instead, there are distinct regions with varying concentrations of 1s and 0s, as illustrated in Figure 1(b). The aging process of an SRAM, influenced by non-uniform data, exerts a notable impact on the subsequent power-up states. This imprinting effect is evident in Figure 1(c). Consequently, regions like b_{21}, which were initially uniform, undergo a shift towards a higher presence of 0s when aged with predominantly 1s. Conversely, regions like b_{56} exhibit an increased presence of 1s after being aged with predominantly 0s.

We exploit this phenomenon by examining the occurrence of the percentage of 1 values ($p1s$) in memory cells on a block-by-block basis and monitoring the standard deviation (σ) of $p1s$. Aging effects lead to a deterioration in the uniformity of the SRAM power-up state. Consequently, the discrepancy between blocks intensifies, resulting in an elevated recorded σ value, as illustrated in Figure 1(d). Finally, the shift in σ with varying block sizes illustrates the distinction between a new chip and an aged one, shown in Figure 1(e). This discrepancy arises due to the nature of the clustering of 1s and 0s across a power-up state. When considering the $p1s$ of a larger block like B_{01}, it tends to be akin to that of B_{02} even after aging. In such expansive regions, identifying non-uniformity becomes challenging, as concentrations of 1s and 0s tend to balance out overall. However, when focusing on smaller regions like b_{21} or b_{56}, these differences become more apparent, allowing for a clearer observation of concentrated pockets of 1s and 0s. Given the minimal non-uniformity in the power-up state of a new device, $p1s$ values remain consistently similar, leading

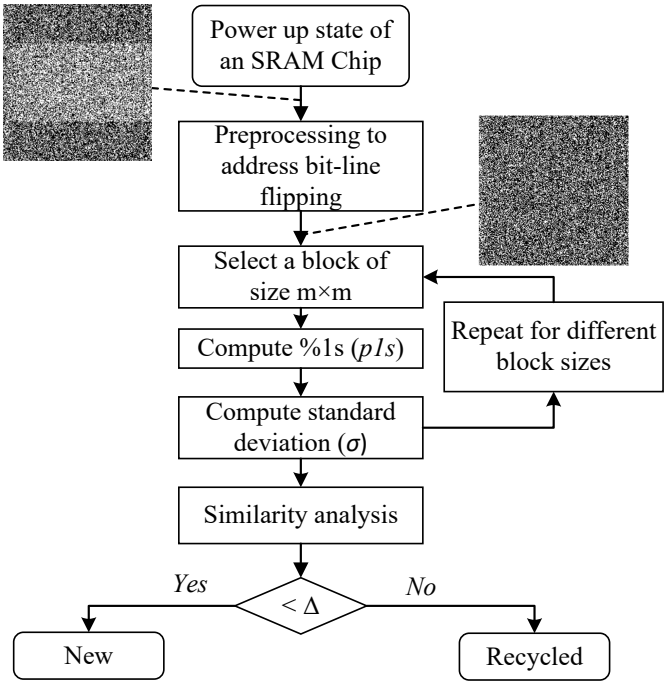


Figure 3: Proposed approach for detecting COTS SRAM chips.

to a more stable σ with less variance across block sizes. By contrasting σ with block size, a definitive distinction between aged and new SRAM COTS becomes evident.

While the assumption that the power-up state of an SRAM is uniform holds true for newer technologies, legacy SRAM devices often feature bitline twisting, also known as bitline interleaving. As shown in Figure 2, this process swaps the positioning of BL and $\overline{BL}$ after a certain number of memory cells. This process typically occurs two or more times within one device, causing the bitmaps of these legacy chips to consist of "bands" in accordance with the number of twists. These bands are inherently biased to logic 1 or logic 0, causing a bitmap to inherit dark or light regions upon power-up. Though all SRAM cells are designed with perfect symmetry, the cumulative effect of node capacitors can skew the overall BL and $\overline{BL}$ capacitances [28], biasing portions of the power-up state to 0 or 1. It is because of this factor that the power-up state of a legacy SRAM device must be pre-processed.

Figure 3 shows the proposed flow of the self-referencing approach to detect recycled COTS SRAM chips manufactured with older technology nodes. The chip is first powered up to obtain the initial power-up states. To address the bitline flipping in legacy SRAMs, it becomes necessary to pre-process the bitmap. This pre-processing operation involves inverting the power-up states of the complementary bands. Through this step, a relatively consistent power-up state is achieved, devoid of any discernable bands. After pre-processing, the uniform bitmap is split into blocks of size $m \times m$. The percent of 1s, $p1s$, in the memory cells of each block is then computed. Following the computation of $p1s$, the standard deviation (σ) of the $p1s$ in each sub-block is calculated. This entire sequence, spanning from the division of the bitmap into blocks to the calculation of σ, is carried out for a range of n values.

Algorithm 1: Preprocessing of SRAM power-up states.

Input : SRAM power-up state (OPS), number of chip sections (B), sections to flip (F)
Output: Bitline compensated power-up state ($BCPS$)

```
1  function setSectionLimits (OPS,B) is
2      BL ← length(OPS)/B;
3      PSS[][] ← ∅;
4      for i ← 0 to B do
5          PSS[i][0 : (BL − 1)] ←
            OPS[i ∗ BL : ((i + 1) ∗ BL − 1)];
6      end
7      return PSS;
8  end
9  function invertSection (PSS) is
10     NPS[][] ← ∅;
11     foreach (i, j ∈ |PSS|) do
12         NPS[i][j] ← PSS[i][j];
13     end
14     return NPS ;
15 end
16 function preProcessing (OPS, B, F) is
17     BCPS[] ← ∅;
18     PSS ← setSectionLimits(OPS, B);
19     for k ← 0 to B do
20         if (k == F) then
21             BCPS[k] ← invertSection(PSS[k]);
22         else
23             BCPS[k] ← PSS[k];
24     end
25     return BCPS;
26 end
```

Subsequently, a comparative analysis is conducted between the blocks of varying sizes. This can be achieved by assessing the spread, σ, of $p1s$ for each block size. A decision on whether a chip is recycled can be made if the σs are well separated across the blocks. This is due to differential aging that creates an increased difference of $p1s$ in the power-up state. On the contrary, σs of the $p1s$ of the new chips are expected to display greater resemblance across various block sizes.

Algorithm 1 outlines the overall pre-processing approach to compensate for the effect of bitline flipping for a legacy COTS SRAM power-up state. It is required to invert the flipped regions. We denote the original power-up state as OPS, the total number of regions in the chip as B, and the particular sections that need flipping as F. The `setSectionLimits` function takes OPS and B as inputs. The band length BL can be described as the total size of one region of OPS or the total size of OPS divided by B, Line 2. To divide the original power-up state into regions, the contents of each section are stored in a 2D sectioned power-up state array PSS, where each row has the contents of one region, Lines 4-6. The inversion of a region can be accomplished by the `invertSection` function, Lines 9-14. It takes PSS as its input, Line 9. A new power-up state array NPS is populated with the inverse of all elements in the input array PSS, Lines 10-12. The `preProcessing` function describes the general functionality of the pre-processing method, Lines 15-25. It takes inputs OPS, B, and F. The power-up state is broken into a sectioned power-up state array, Line 18. The bitline compensated power-up state is produced by inverting all sections indicated by input parameter F, Lines 19-25.

Algorithm 2: Computation of standard deviation (σ).

Input : n $BCPSs$
Output: σ of $p1s$ for different block sizes.

```
1  function computePercentOnes (BCPS[]) is
2      block[][] ← ∅, X[][] ← ∅;
3      b[] ← Block sizes;
4      foreach ( m = 1 : |b| ) do
5          foreach ( i = 1 : n) do
6              foreach (j = 1 : b[m]) do
7                  block ←
                    extractSubBlock(BCPS[i], j) ;
8                  X[m, i + j] ← calPercentOnes
                    (block) ;
9              end
10         end
11     end
12     return X ;
13 end
14 function computeSigma (BCPS[]) is
15     X ← computePercentOnes(BCPS[]) ;
16     foreach ( m = 1 : |b| ) do
17         σ[m] ← standardDeviation (X[m, :]) ;
18     end
19     return σ ;
20 end
```

Algorithm 2 shows the computation of standard deviation, σ, for different block sizes. As we measure the power-up state multiple times, it takes n bitline compensated power-up states ($BCPS$) as the inputs and results σs for different block sizes. First, the `computePercentOnes` function computes $p1s$ and is described in Lines 1-14. These $p1s$ values are used to calculate the standard deviation (σ) for their corresponding number of sub-blocks, Lines 15-21. The algorithm initiates with the input of an array of bitline compensated values, denoted as $BCPS[]$, in the `computePercentOnes` function, Line 1. The initialization of the 2D arrays, $block$ and X, that represent a part of the power-up states and the percentage of logic 1s within these states, respectively, are described in Line 2. Another array, b, is initialized and denotes the number of blocks for which $p1s$ is to be computed and shown in Line 4. The function iterates through all power-up states, sub-divides them into blocks using the values in b, calculates the percentage of logic 1s, and stores these values in the array X, Lines 5-14. Algorithm 2 invokes `computeSSigma` function that takes n $BCPS$ as inputs, calls `computePercentOnes` iteratively to compute σ of $p1s$ for each block size across all power-up states, Lines 15-20.

IV. Experimental Results

To validate the effectiveness of our proposed approach, we performed experiments with six different commercial off-the-shelf (COTS) 23A640-I/SN SPI Bus Low-Power Serial SRAM memories [29]. Each SRAM chip had a total memory

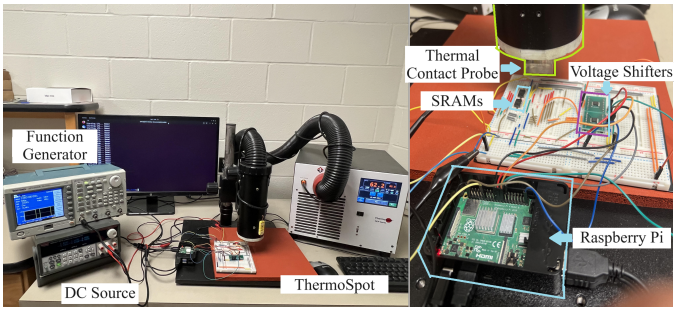


Figure 4: Experimental setup of accelerated aging using Thermospot system.

capacity of 64K bits. Figure 4 provides a detailed view of the experimental setup. The accelerated aging of the chips was performed using a Temptronic ThermoSpot DCP-201 system at the constant temperature of 100°C. All SRAMs were aged with the same black-and-white binary image to reflect the operational aging. One hundred power-up states of an SRAM were recorded every 6 hours of aging. This power-up state data was collected by the Raspberry Pi through the SPI interface. During power-up state collection, the SRAM was powered by a PWM signal from a function generator, generating a power-up state every two seconds. Simultaneously, a custom C program allowed the Raspberry Pi to read the complete power-up state at the positive edge of this signal. The collected SRAM data were then pre-processed using Algorithm 1 to compensate for bitline flipping via in-house Python scripts. Following that, the data was analyzed using Algorithm 2 in MATLAB.

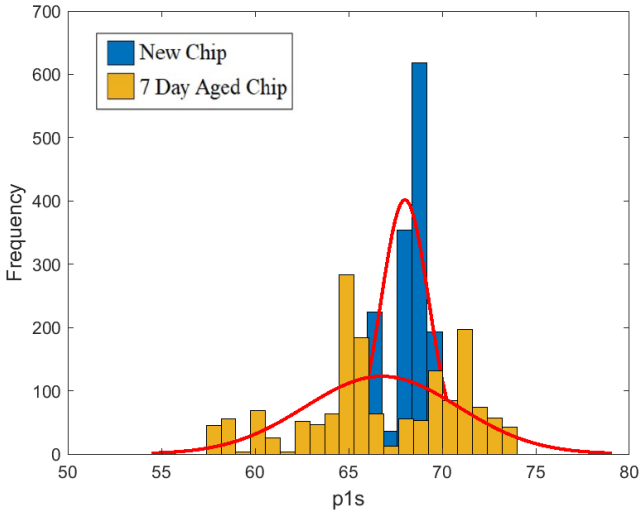


Figure 5: Distribution of $p1s$ of 64x64 blocksize of the power-up states of an SRAM Chip.

To validate our hypothesis on differential aging, we conducted experimental analyses of the distribution of 1s for various block sizes in both a new and an aged chip. As outlined in Section III, we anticipate that an aged chip will demonstrate a broader distribution of $p1s$ compared to a new chip, especially for a specified block size. Illustrated in Figure 5 is the $p1s$ distribution in the power-up states of a new and an aged SRAM chip, focusing on a block size of 64×64. Notably, as the chip ages, the $p1s$ distribution displays a wider spread, coupled

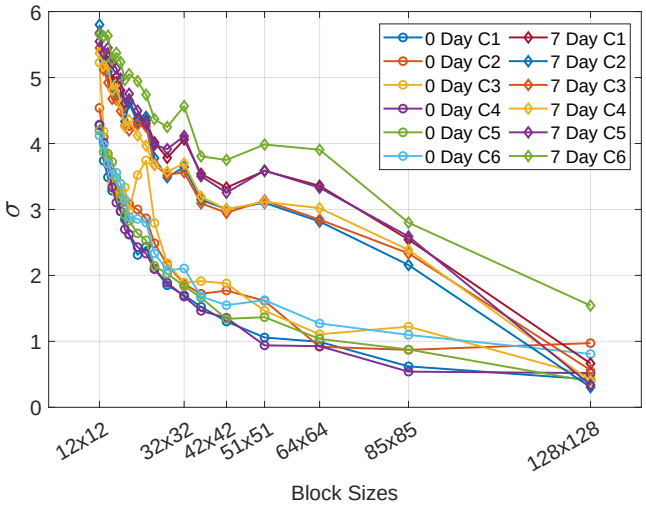


Figure 6: Standard deviation (σ) as a function of block size for new and aged SRAM chips.

with a leftward shift of the mean. The mean of $p1s$ values has a left-bound tendency over time because more 1s are stored at the SRAM array. This observation strongly aligns with our hypothesis, indicating that aging introduces more dissimilarities in the percent of 1s during the power-up state of the SRAM. Further justification for selecting a 64×64 block size for this investigation will be explained in the subsequent discussion.

A crucial consideration in the data analysis for our proposed approach involves the judicious selection of an optimal block size. To ensure a comprehensive examination of the percentage of 1s across diverse regions within the power-up state, we vary the block size, encompassing a range from smaller dimensions, such as 12×12, to larger configurations, extending up to 128×128. This systematic exploration allows us to scrutinize the impact of varying block sizes on the distribution of 1s in the power-up state, providing us insights to choose the most suitable block dimension for our study.

Figure 6 shows the variation in σ of $p1s$ across different block sizes for both new and aged chips. The chips are denoted as C1, C2, and so forth. We observe the inverse relationship between σ values and block size, with this effect more pronounced in aged chips. For block sizes smaller than 32×32, a sharp reduction trend was noted across all chips, regardless of their age, attributed to the limited impact of the averaging effect on $p1s$ values within smaller blocks. The graph for a block size of 32×32 exhibited a slight increase, explained by the clustering nature of 1s and 0s in the aging data's power-up state for this specific block size. Notably, a significant difference in σ values was observed between aged chips (top curves) and new chips (bottom curves) for larger block sizes. For instance, at a block size of 42×42, the σ of new chips ranged from approximately 1.3 to 1.9, while for old chips, it ranged from about 3.0 to 3.8. In subsequent block sizes, the spread for new chips remained relatively stable, around or below 1.0, whereas σ values for old chips remained significantly larger and varied widely across different block sizes. However, for very large block sizes, such as 128×128, the averaging effect of $p1s$ within the blocks balances out concentrations of 1s and 0s on the power-up states, lowering the standard

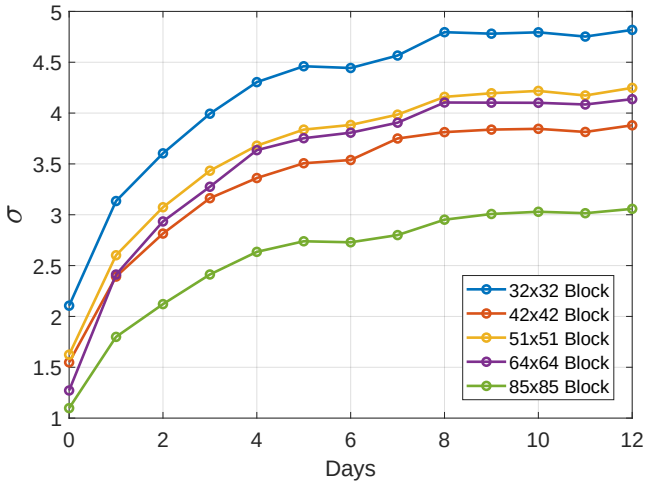


Figure 7: The change of σ of an SRAM Chip over a period of 12 days.

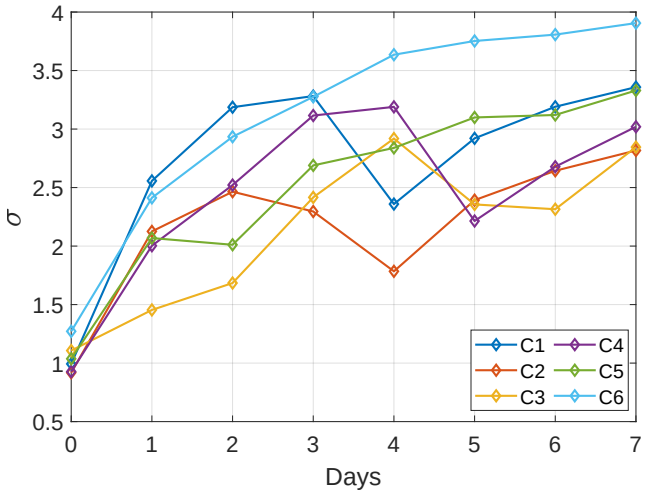


Figure 8: The change of σ for six SRAM chips over a period of 7 days.

distribution and rendering it unsuitable for our study. Based on the above analysis, it is evident that in new chips, there is a consistent and uniform behavior across all blocks. However, in the case of old chips, a distinctive pattern emerges, indicating a gradual decrease in σ as the block size increases. This insightful observation forms the crux of our proposed self-referencing-based recycled IC detection approach. The systematic reduction in σ with larger block sizes in old chips serves as a unique signature, offering a robust foundation for developing a reliable method to detect recycled integrated circuits.

TABLE I: Δ FOR DIFFERENT CHIPS.

Chips	C1	C2	C3	C4	C5	C6
New Δ	0.63	0.64	1.00	0.42	0.97	0.81
7 days aged Δ	2.92	2.79	2.57	2.72	3.25	2.44

Table I presents the similarity results for new and aged chips. Due to the pronounced change in slope observed up to the block sizes of 42×42, we recommend utilizing the Δ calculated from block sizes ranging between 51×51 to 128×128 for the purpose of recycled IC detection. We define the similarity index as the slope of these curves, expressed by the following equation.

$$\Delta = \sigma_{51\times51} - \sigma_{128\times128} \tag{1}$$

The columns specify the chips (C1 to C6), and rows indicate the Δ values for the new and 7-day aged chips. The values within the table cells represent the calculated the differential σ for each respective chip under the specified conditions. We note a consistent Δ pattern with values consistently below 1.00 for new chips. In contrast, aged chips exhibit Δ values exceeding 2.40, resulting in a distinct separation. This observed distinction forms the foundational basis for recycled IC detection.

We performed two additional experiments to demonstrate that more aging increases the spread of $p1s$. To demonstrate the effect of aging on the standard deviation of $p1s$, we carried out the same accelerated aging on an SRAM chip for 12 days. The obtained values of σ were plotted for five different block sizes, as depicted in Figure 7. Before starting the aging process, a hundred power-up states were recorded in the initial state, yielding σ values in the range of 0.8 to 2.2 for different block sizes. As the chip undergoes 6 hours of daily aging, the σ for all the blocks exhibited an upward trend. This experiment provides insight into the nature of the relationship between σ and aging duration: as the chip undergoes aging, the rise of σ shows the well-known logarithmic rise.

In conclusion, our findings reveal consistent behavior across all chips studied. The selection of a 64×64 block size was based on the distinct differentiation observed in the corresponding σ data between new and aged chips, as detailed earlier. To validate the effectiveness, we subjected six chips to a seven-day aging process. Figure 8 illustrates the variation in the standard deviation of the $p1s$ of the chips throughout the aging process. Notably, a decrease in σ was observed on Day 4 for C1 and C2 as they underwent a reverse aging process. Similarly, C3 and C4 experienced reverse aging on Day 5 and Day 6, leading to a corresponding decrease in σ. In contrast, C5 and C6 underwent continuous aging throughout the week. The observed σ values followed the anticipated pattern of increase and decrease, aligning with our aging and reverse-aging procedures. While reverse aging effectively diminishes the variation, it never fully restores the value back to its original new state.

V. CONCLUSION

Developing robust testing methods to detect counterfeit or recycled integrated circuits is paramount for safeguarding the integrity of our critical infrastructures. The self-referencing approach outlined in this paper presents an efficient means of identifying counterfeit ICs without imposing significant expenses or necessitating the storage of intricate device parameters. This method only requires a straightforward and affordable test setup for reading the SRAM power-up state, utilizing a low-cost Raspberry Pi. The statistical comparison study conducted between the power-up states of old and new chips demonstrates clarity and simplicity. A recycled chip can be reliably distinguished from a new one by observing the comparative standard deviation of the percent of 1s across various block sizes. The efficacy of the proposed self-referencing test has been successfully validated across six ICs.

ACKNOWLEDGMENT

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-23-1-0312. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force.

REFERENCES

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

[2] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

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

[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] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[6] U. Guin, W. Wang, C. Harper, and A. D. Singh, "Detecting Recycled SOCs by Exploiting Aging Induced Biases in Memory Cells," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 72–80, 2019.

[7] SAE G-19A Test Laboratory Standards Development Committee, "Test methods standard; general requirements, suspect/counterfeit, electrical, electronic, and electromechanical parts," 2016, https://www.sae.org/standards/content/as6171.

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

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

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

[11] 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.

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

[13] 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.

[14] 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, pp. 874–880, April 2008.

[15] 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.

[16] 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.

[17] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-Cost On-Chip Structures for Combating Die and IC Recycling," in *ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, 2014.

[18] 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, 2015.

[19] 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*, pp. 146–151, Nov. 2015.

[20] M. Alam, S. Chowdhury, M. M. Tehranipoor, and U. Guin, "Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 209–214, 2018.

[21] Z. Xu, A. Cui, and G. Qu, "A new aging sensor for the detection of recycled ics," in *Proceedings of the 2020 on Great Lakes Symposium on VLSI*, pp. 223–228, 2020.

[22] T. Alnuayri, S. Khursheed, A. L. H. Martinez, and D. Rossi, "Differential aging sensor to detect recycled ics using sub-threshold leakage current," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1500–1503, IEEE, 2021.

[23] M. Liu and C. H. Kim, "A powerless and non-volatile counterfeit ic detection sensor in a standard logic process based on an exposed floating-gate array," in *2017 Symposium on VLSI Technology*, pp. T102–T103, IEEE, 2017.

[24] P. Ghosh and R. S. Chakraborty, "Counterfeit ic detection by image texture analysis," in *2017 Euromicro Conference on Digital System Design (DSD)*, pp. 283–286, IEEE, 2017.

[25] N. Asadizanjani, M. Tehranipoor, and D. Forte, "Counterfeit electronics detection using image processing and machine learning," vol. 787, no. 1, p. 012023, 2017.

[26] P. Ghosh and R. S. Chakraborty, "Recycled and remarked counterfeit integrated circuit detection by image processing based package texture and indent analysis," *IEEE Transactions on Industrial Informatics*, 2018.

[27] N. Asadizanjani, N. Dunn, S. Gattigowda, M. Tehranipoor, and D. Forte, "A database for counterfeit electronics and automatic defect detection based on image processing and machine learning," in *Proceedings of the 42nd International Symposium for Testing and Failure Analysis. Texas, USA*, pp. 1–8, 2016.

[28] B. S. Amrutur and M. A. Horowitz, "A replica technique for wordline and sense control in low-power sram's," *IEEE Journal of solid-state circuits*, vol. 33, no. 8, pp. 1208–1219, 1998.

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