A Novel Statistical and Circuit-Based Technique for Counterfeit Detection in Existing ICs

Rashmi Moudgil[1], Dinesh Ganta[1], Leyla Nazhandali[1], Michael Hsiao[1], Chao Wang[1], Simin Hall[2]
[1]Department of Electrical and Computer Engineering, Virginia Tech
[2]Department of Mechanical Engineering, Virginia Tech
(rmoudgil, diganta, leyla, hsiao, chaowang, thall57)@vt.edu

ABSTRACT

Previously used ICs, which are resold as new, result in undue lost revenue, cause lower performance, reduced life span, and even catastrophic failure of platforms and systems. Non-invasive and inexpensive techniques are needed to establish the authenticity of such ICs that do not have special in-built structures for counterfeit detection. Although delay of circuit increases with its age, it cannot directly reveal the age of the chip, as it is also greatly influenced by process variation. In this work, we show that the relationship between two or more paths within the chip is a great indicator of its age. Using the proposed statistical and circuit-level technique, we observe over 97% correct detection of an aged IC from a new IC.

Categories and Subject Descriptors

B.8.1 [**Performance and Reliability**]: Reliability, Testing, and Fault-Tolerance

Keywords

Counterfeit, Aging, Process Variation

1. INTRODUCTION

Globalization has provided us with a vast choice of hardware suppliers at various levels of the design and manufacturing flow. Designs and fabricated chips can now come from practically anywhere in the world. However, this has not come without costs. The trustworthiness of the received device is no longer a guarantee. The reliability of a system is directly dependent on the reliability of the components that it is built of. One unreliable IC in a system possibly can result in a catastrophic system failure. An area where this is particularly critical is in defense and medical related systems where the reliability of a system is of utmost importance. Recently, many cases have come to light, which show ICs being scavenged from electronic waste, repackaged and sold as genuine new ICs [1]. The focus of this paper is this specific form of IC counterfeiting.

A report on the counterfeit ICs by IHS iSuppli estimates a $169 billion in potential annual risk to the global electronics business [2-5]. These studies suggest that IC counterfeiting is a serious and growing problem. Some of the direct impacts due to IC counterfeiting are enumerated here: Firstly, consumers do not get what they pay for. The devices get slower and are more prone to failure. Secondly, semiconductor manufacturers incur a significant loss due to lost sale, which eventually hurts everyone related to this industry including consumers. Thirdly, system manufacturers suffer bad reputation when the components fail. In addition, they endure loss for providing warranty. And lastly, in case of critical applications such as avionics, defense systems, and medical devices, untimely IC failures can result in catastrophic events. As a result, it is extremely important to be able to distinguish new authentic ICs from counterfeits and/or used parts.

For the future designs we might have the luxury of inserting specialized circuitry to the chip in order to help establish the age or usage of the chip (e.g., ROM-based fuses can be implemented to act as IC seals or special protected registers can be employed to produce the manufacturing date of the chip). However, determining whether an existing chip is a counterfeit is much harder. For such cases, statistical and testing techniques are needed. Figure 1 illustrates these two categories of counterfeit detection methods.

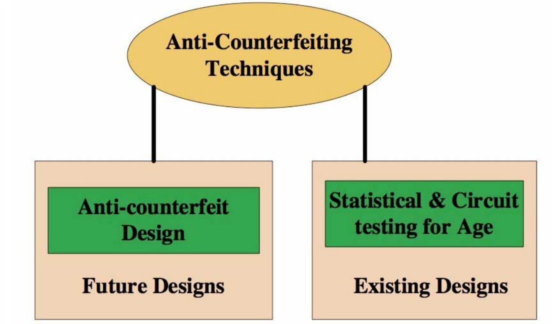
Anti-Counterfeiting Techniques
Anti-counterfeit Design
Future Designs
Statistical & Circuit testing for Age
Existing Designs

Figure 1: Anti-Counterfeit Techniques

Although finding anti-counterfeit methods for future designs is not a trivial problem, it poses a less challenge compared to detecting counterfeits amongst existing chips, where one has to depend on just the original circuit itself to establish the age of the device. This paper focuses on solutions for existing ICs.

The major contributions of this paper are as follows:

1. Based on detailed simulation results, we show that although the delay of a circuit is greatly affected by aging, it cannot be used as an age indicator by itself since delay is also significantly affected by process variation.
2. We show that the relationship between two or more paths in the circuit can be used as an age marker and we propose a statistical method based on this fact, which can correctly predict the age of an IC.
3. We provide an extensive analysis of our proposed method and show its accuracy by implementing on variety of sample circuits, including few cores and ISCAS benchmarks.

The rest of this paper is organized as follows: In Section 2, the related work is discussed. Section 3 presents the background and motivation of this work. Section 4 introduces the anti-counterfeiting techniques proposed in this work and Section 5 highlights the

GLSVLSI'13, May 2–3, 2013, Paris, France.

simulation framework. Results and conclusion are presented in Section 6 and Section 7, respectively.

2. RELATED WORK

In regard to counterfeit prevention and detection, traditional techniques such as printing serial numbers or barcodes to prevent counterfeiting in integrated circuits are not effective as they can be easily cloned or faked. IC Metering [6-8] provides techniques that allow post fabrication control on the ICs. Although metering techniques can be leveraged to prevent counterfeiting, most such techniques require modifying the design significantly, for example, its state machine [6]. In [9], the authors present a technique to prevent piracy of ICs, which renders the ICs inoperative upon fabrication, and it requires a device unique key to take the IC to the functional mode. Recently, some anti-counterfeiting methodologies were presented which use Physical Unclonable Functions (PUFs) [10]. Another odometer based technique to estimate age of ICs has been proposed in [11]. Although, most of these methods are designed to monitor reliability of ICs, they can be deployed for anti-counterfeiting purposes as they provide information on the age of the ICs. Again, an important limitation with all techniques mentioned above is that they are only applicable to designs for the future. Many applications including a wide range of critical applications heavily depend on designs that were created years ago due to the fact that the test cost and time can be prohibitive of they keep deploying newer designs. As a result, it is necessary to distinguish between unused and used (counterfeit) for ICs already manufactured with no anti-counterfeiting capabilities. There are few companies, which deploy inspection techniques using X-ray and Infrared microscopy for this category of ICs, but special high magnification machinery is needed for it [21]. Instead, our paper aims to investigate cost-effective anti-counterfeiting techniques for this purpose.

3. Background and Motivation

This section provides a brief overview of transistor aging, and process variation. Their collective effect on circuit behavior establishes the motivation for our proposed technique.

3.1 *Aging*

In simple terms, aging can be defined as slow but eventually permanent variations that generally deteriorate circuit performance over time. It results from continuous degradation of transistor characteristics, which causes slower operation of circuits, irregular-timing characteristics, increase in power consumption and sometimes even functional failures [13-15]. As shown in Figure 2, the major physical mechanisms behind aging in ICs are the Bias Temperature Instability (BTI), Hot Carrier Injection (HCI) and Time Dependent Dielectric Breakdown (TDDB). They arise both within the gate di-electric and at the boundary of silicon and gate oxide. These effects are particularly prominent at lower technologies due to increasing electric fields in the devices, and decreasing thickness of oxide. Negative Bias Temperature Instability (NBTI) is prominent in PMOS transistors, and can shift (degrade) the PMOS threshold voltage by more than 50mV over ten years. This translates to more than 20% degradation in circuit speed [18-19]. Similarly, Positive Bias Temperature Instability (PBTI) effect occurs in NMOS. In both BTI cases, the amount of charges in the gate dielectric changes with the gate bias, because of charge trapping and de-trapping. HCI effect is more dependent on the switching activity of the transistors, as it is related to carrier injection in presence of high electric fields. TDDB is a consequence of aging, which results in shorting of gate dielectric leading to gate failure. Detailed studies on the factors that contribute to aging of transistors are presented in [12-16]. One of the important facts in regard to aging of transistors is that the amount of activity of the transistors has a direct effect on the aging process.

3.2 *Process Variation*

Process variation (PV) is the random and permanent deviation from the designed, nominal value of a circuit structure, caused by random effects during manufacturing [12]. PV can be separated into two categories: The first category covers variations in process parameters, such as impurity concentration densities, oxide thicknesses, and diffusion depths. These result from non-uniform conditions during the deposition and/or the diffusion of the dopants. The second category covers variations in the dimensions of the devices. These result from limited resolution of the photolithographic process, which in turn causes width and length variations in transistors.

It is important to note, that variation in manufacturing, can introduce mismatch between two transistors sitting within a single die, and on a higher level of abstraction, from one wafer to other, and between manufacturing lots. This spatial classification of process variation is widely grouped as intra-die (within the die), and inter-die (across dies). In general, inter-die variation can have more severe effect on the design compared to intra-die variation.

3.3 Intertwined Effect of PV and Aging

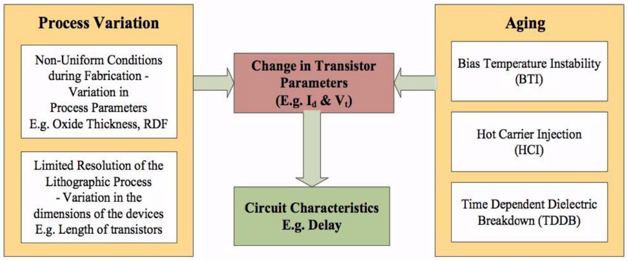
Process Variation
Non-Uniform Conditions during Fabrication - Variation in Process Parameters E.g. Oxide Thickness, RDF
Limited Resolution of the Lithographic Process - Variation in the dimensions of the devices E.g. Length of transistors
Change in Transistor Parameters (E.g. I_d & V_t)
Circuit Characteristics E.g. Delay
Aging
Bias Temperature Instability (BTI)
Hot Carrier Injection (HCI)
Time Dependent Dielectric Breakdown (TDDB)

Figure2. Impact of PV and Aging on an IC

Figure 2 summarizes how both Process Variation (PV) and Aging impact common electrical parameters such as threshold voltage, saturation current and eventually circuit characteristics like delay or power, of an IC. This means the effects of PV and aging are intertwined and very hard to isolate from each other. This makes the counterfeit detection a very challenging problem.

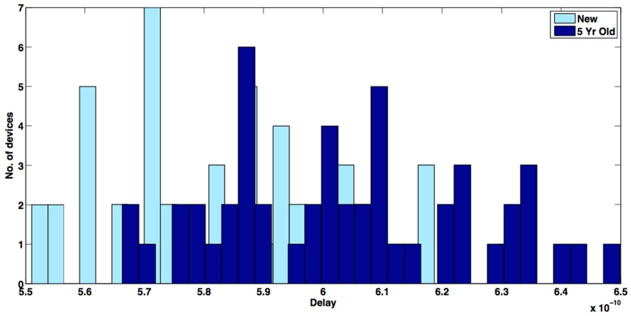

Figure3. Delay Distribution of a path in a new v/s old IC

Figure 3 shows this intertwined effect from simulation point of view. A simple 50-stage inverter chain is simulated both as a new circuit (light-blue histogram) and as a 5-year old circuit (dark-blue histogram). In both cases, the circuit is also subjected to process variation using Monte Carlo simulation. More details of our experimental setup are provided in Section 5. Although the aged circuits are typically slower than new circuits, there is a significant overlap in the range of delay values for the two groups. In fact, more than 70% of both the new and old circuits have delay between 0.565ns to 0.615ns. Suppose we pick a delay value of 0.6ns, it would be impossible to tell if it corresponds to an aged IC – which was originally faster and now has increased delay due to aging or to a new one, which is just slower due to process.

The above observation demonstrates that delay of a single path from the chip is not effective as a direct indicator of the age of an IC. To make matters more complicated, there is recent submicron data showing that aging itself can be affected by process variation [20]. Specifically, there is significant dependence of NBTI and PBTI on device geometry, e.g., channel length, which is variable as virtue of process also. These effects have begun to be modeled by commercial tools [20], but reverse engineering the cumulative effect to isolate age becomes a tedious problem. In this paper, we propose a method that overcomes this challenge by combining the characteristics of more than one path and isolating the effect of aging.

4. ANTI-COUNTERFEIT TECHNIQUES

This section discusses the method we propose for detecting old counterfeit ICs, which lack special anti-counterfeiting. We begin with the goal of just being able to distinguish an old device from a new one and later extend the methodology to accurate predict the age of a chip.

As we saw in Section 3, although delay of a single path is significantly affected by aging, it is a poor indicator of the age of the chip as it is also greatly affected by process variation. Therefore, instead of using a single path, we propose the use of a set of paths from within a chip, such that each path individually has a characteristic aging behavior. The relationship between the delays of the chosen paths is used as an indicator of the age of the chip. The premise of our method is that the pattern that governs the relationship between two delay paths for new ICs are distinguishably different from the pattern governing that of old ICs. This means, if we have a trusted set of new chips and we are able to study them before and after (accelerated) aging, we can characterize these relationship patterns at different ages. Now, when an untrusted chip is under test, the relationship of the same paths is evaluated and it is determined whether it follows the pattern belonging to the new chips or older chips. This is illustrated in Figure 4.

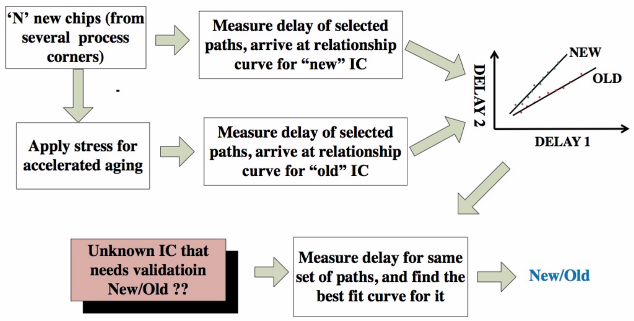
'N' new chips (from several process corners)
Measure delay of selected paths, arrive at relationship curve for "new" IC
Apply stress for accelerated aging
Measure delay of selected paths, arrive at relationship curve for "old" IC
DELAY 2
NEW
OLD
DELAY 1
Unknown IC that needs validatioin New/Old ??
Measure delay for same set of paths, and find the best fit curve for it
New/Old

Figure4. Detection method for New/Old in existing designs

The details of our technique for a 2-path method are described as follows, where the relationship between the two paths is used for determining the age.

1. Two different paths are selected from the chip.
2. The delays of the two paths are measured for a variety of trusted new chips. Ideally the trusted chip pool is big enough to present a realistic mix of chips affected by process variation. Curve fitting is used to identify a pattern relating the two paths to each other, similar to the "AGE0" line shown in Figure 5.
3. The trusted chips undergo accelerated aging by being subjected to more than nominal operating voltages and high temperatures.
4. The delays of the two paths are again measured for all the trusted chips. Once more curve fitting is used for relating the paths to each other, similar to the "AGE5" line in Figure 5.
5. When an untrusted chip is under test, the delays of the same two paths are measured. Based on mathematical methods (e.g. shortest perpendicular distance), it is determined whether the "new ICs" curve is a better fit for the untrusted IC or the "older ICs".

This method can be extended to a 3-path or 4-path method, which uses more than two paths, and the relationship between their delays is fitted to a surface plot instead.

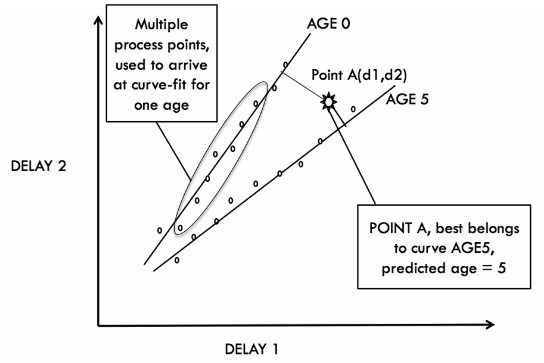
Multiple process points, used to arrive at curve-fit for one age
AGE 0
Point A(d1,d2)
AGE 5
DELAY 2
POINT A, best belongs to curve AGE5, predicted age = 5
DELAY 1

Figure5. Two-Delay method for detection of Age

The important aspect is to decide on the kind of paths to choose. Our method is successful if the paths chosen resemble each other in nature of their delay, e.g., paths with fairly similar capacitive loading, and similar length, but have a distinct aging profile. The latter is achieved by using paths of dissimilar activity – i.e. paths undergoing different number of transitions. The path with higher activity is more affected by age, which means the relationship of the two paths changes significantly over time. In a real chip, some portion of the chip logic is not as active during its lifetime, as other portions. For example, the test paths around the memory test logic will be quite less active or totally inactive, during the lifetime, relative to a functional clock tree path. Such paths, which significantly differ in their activity, are good candidates for this scheme. We provide a detailed sensitivity analysis in Section 6, which details more on the best candidate paths for this method.

4.1 *Just-in-Time Voltage Reduction*

We will show in the Section 6 that the above-proposed technique can achieve only up to 87% accuracy for detecting counterfeit ICs, and almost 1 out of every 3 new chips get falsely detected as old. In order to improve our method, we propose an augmentation technique that we call Just-in-Time Voltage Reduction. In this approach, we reduce the operating voltage of the chip at the time of testing. The rationale is that the effect of aging can be more easily detected at lower voltages. This is explained in more detail in the rest of this section.

The first order equations for gate delay (inverter with symmetrical nmos and pmos), shown in equations (1) and (2), provide the basis for modeling delay in both strong-inversion and sub-threshold regions [22]. The dependence of the delay on the difference of VDD and V_T changes from a linear relation to exponential one as we move into sub-threshold region.

$$t_d = \frac{K C_G V_{DD}}{(V_{DD}-V_T)^{\alpha}} \qquad (1)$$

$$t_{d,sub} = \frac{K C_G V_{DD}}{I_o \exp(\frac{V_{DD}-V_T}{n V_{th}})} \qquad (2)$$

On the other hand, the equations of aging models [17] show how HCI and BTI result in increase to the threshold voltage of the transistor over time. So, it is expected that operating the circuit at lower voltages, especially near or lower than threshold voltage will result in more drop in circuit speed after aging compared to a circuit that is run at nominal voltage.

Simulation results support this hypothesis. Figure 6 shows the plot of the delay of a path, as it is aged from zero to five years. While all circuits are operated at nominal voltage during their lifetime, each is subjected to a different voltage, i.e., 0.5, 0.8 and 1.2V at the time of delay measurement. As expected, the delays are higher at lower voltages. In addition, we observe that at 0.5V, the effect of aging is more distinguishable, as seen by the clear increase in delay after aging. We intend to use this observation to augment our proposed method for improved detection of counterfeit ICs. Section 6 shows the improvement in results using this.

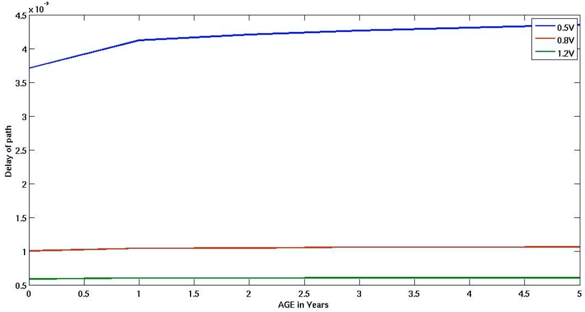

Figure6. Delay v/s Age for diff supply voltage used during post-stress phase (testing phase only)

5. EXPERIMENTAL SETUP

All the circuits are simulated by HSPICE tool using publicly available 90nm Predictive Technology Model (PTM). The effect of aging is simulated through MOS Reliability Analysis (MOSRA) model provided by HSPICE. MOSRA accurately models the HCI and BTI aging mechanisms and analyzes their impact on circuit performance using actual circuit operation and stimulus. It operates in two phases of simulation: pre-stress and post-stress. Different operating voltages can be used for each phase. In our analysis, we use the nominal voltage for the pre-stress phase, which represents the typical usage of the circuit. We use different voltages for the post-stress phase (testing stage).

The effect of process variation is modeled using Monte Carlo (MC) simulation. Specifically, we vary the threshold voltage of transistors (V_{th0}) following Gaussian distributions with means obtained from nominal values in the technology file and 3σ variation (30mV). Using MC, 100 random process points each are evaluated for all age groups. The characterization step, to arrive at reference curves, uses 70 points each for every age group. For the testing phase, the remaining 30 points each (in all 150 unknown chips) are used for validation of prediction scheme.

Test Circuits: A variety of test circuits are used in this paper. The results of Section 6 are based on two sets of circuits. The first set is a variety of inverter chains that differ from each other in their typical delay and activity. Typical delay is the characteristic delay of the path, which has not been affected by either process variation or aging. We modify the depth of the chain and the load capacitance at gate outputs in order to arrive at different typical delays. The input stimulus is controlled to bring desired variation in the activity for different paths. The second set of test circuits for Section 6 consists of typical circuits such as dividers, discrete-cosine-transform circuits and few ISCAS benchmarks.

6. Results, Analysis and Improvements

This section is organized in three parts. In the first part, we use the set of inverter-based circuits for establishing the results of our base method, and the augmented reduced voltage method. In the second part, using the same set of circuits, we show a detailed sensitivity analysis of the method of detection to the type of paths selected. As a remedy to this sensitivity, we introduce 3-path approach, and show the improved results. In the third part, we share our results on some standard circuits. Test results are categorized into two sets: Plain New/Old detection and Exact Prediction of age of the design under test. For exact age analysis, we consider 4 possible ages: 0 (new), 2, 5 and 10 years.

6.1 Basic 2-path method

Table 1 shows the results achieved for the 2-path method as described in Section 4. It also provides some basic information about the two paths involved in this experiment.

Candidate Paths	Transition Activity Ratio	**100:1**
	Typical Delay Difference	**None**
	Post-Stress Voltage	**1.2V**
Prediction of New/Old	Overall Correct Prediction	**87%**
	False Negatives	**6 out of 90**
	False Positives	**10 out of 30**
Exact Prediction of Age	Overall Correct Prediction	**58%**

Table1. Prediction results for Basic 2-Delay method

The result shows that if the two paths have an equal typical delay (in the absence of PV effect) and one of them is 100 times more active than the other, we are able to predict with 87% accuracy, whether a chip is old or new. This method is seen to have a high false positive rate, which means we will be discarding more than 30% authentic chips as potential counterfeits. It is also shown that the exact age prediction is correct only 58% of times.

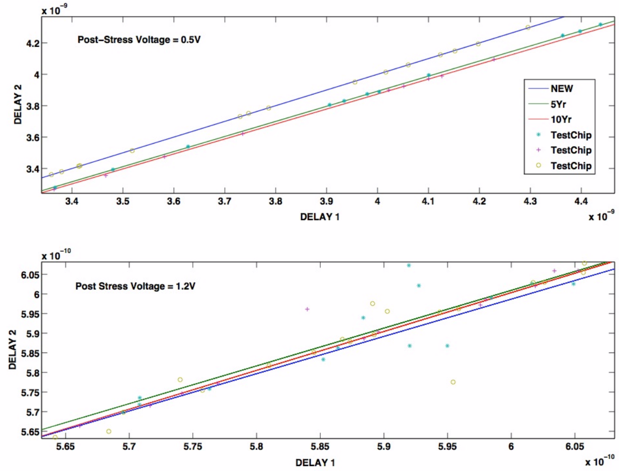

Figure7. Curve-fits across different ages, for different post-stress voltages

Now for the same experimental setup, instead of making the post-stress measurements at 1.2V, we use an operating voltage of 0.5V. As illustrated in Figure 7, the relationship curves obtained at 0.5V are more distinct from one age group to other, and therefore, result in higher correct prediction rate.

With “Just-in-time voltage reduction” method, both false positives and false negatives are reduced to zero, and hence, we are able to achieve 100% accurate detection of old counterfeits from new ICs. Also, the exact age prediction improves to as high as 99%. Nevertheless, this method is very sensitive to the characteristics of the two paths under test. Details of this sensitivity along with a proposed remedy are provided in the next part of this section.

6.2 Sensitivity analysis and Improvements

Broadly, we have analyzed the sensitivity of our detection method, to variation in two characteristics of the paths under test: 1) activity ratio between the selected paths and 2) difference in the typical delays of selected path. Just-in-time voltage reduction is employed for the results of this part.

6.2.1 Sensitivity Analysis

Difference in the activity of the paths is the key reason behind the working of our method. We use the fact that the activity directly influences the aging profile of a path or the degree of aging in a path. One goal is to find out the amount by which they should be different, in order to yield high predictability. In addition, we would like to relax the constraint that the chosen paths should be of same typical delay. For a comprehensive view of the sensitivity to the two factors together, the entire variation matrix is plotted, to show the impact on both test aspects.

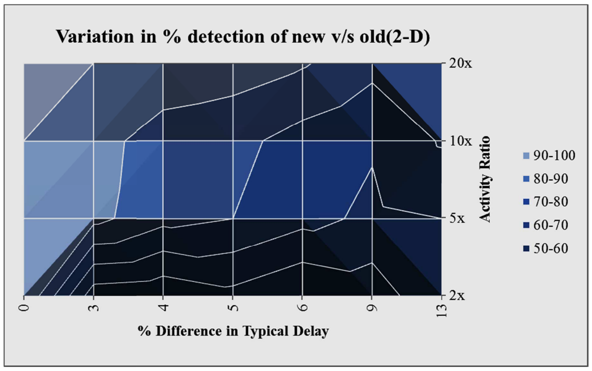

Figure8. Sensitivity of 2-D prediction method (new/old)

For the variation matrix in Figure 8, the typical delay is varied between 0 to 13% and the activity ratio is varied from 2x to 20x. On the activity axis, it is clear that for a fixed set of paths, the prediction result improves as we move from a lower activity difference to a higher one. As for variation to difference in typical delay, it is seen that any deviation from similar typical delay causes deterioration of the detection rate from 100%(as stated in Section 6.1), to even about 50-60%. Similar sensitivity trend is seen for the second test category of exact age prediction, as shown in Figure 9.

In conclusion, for the 2-path method, if we choose paths, which have similar typical delay, an activity difference of 10 times or more is able to produce good prediction results. However, in order to relax the constraint for path selection in terms of typical delay, it is seen that extending the method to include more delay paths can help mitigate the variation, as discussed in following section.

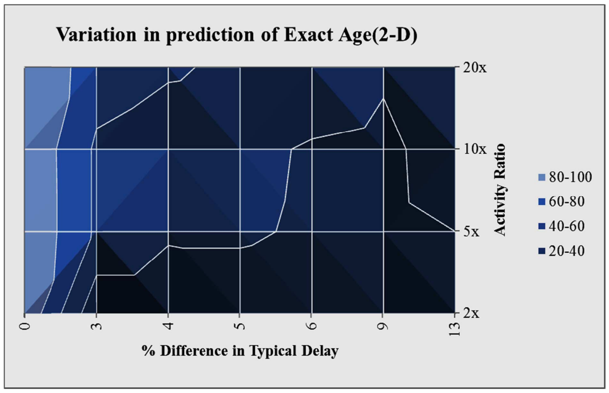

Figure9. Sensitivity of 2-D prediction method (Exact Age)

6.2.2 Further Improvement: 3-path Approach

In the 3-path method, an additional path is chosen. Since the search space for how these three paths should be related to each other in terms of their typical delay and activity is very large, we impose some restrictions by emulating a scenario to a typical design. In this scenario, we assume that we are able to evaluate two critical paths with similar (but not the same) typical delay from a circuit with some moderate to high activity and then, a third path from a test circuit with much lower activity is chosen. Similar to our 2-path method, the relationship curve is defined between the three delay variables using surface fit techniques. And for the unknown test point, minimum residual is used to identify the best-fit surface it belongs to.

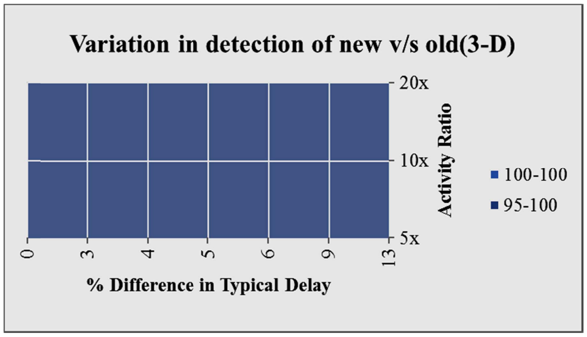

Figure10. Sensitivity with 3-D prediction method (new/old)

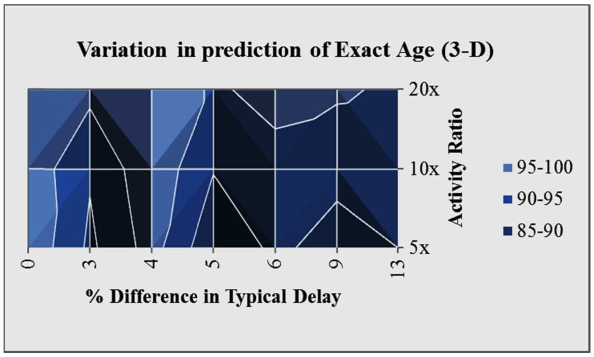

Figure11. Sensitivity with 3-D prediction method (Exact Age)

The improvement in the results for both test types is shown in Figures 10-11. These can be compared to Figures 8-9, as a third path is added to the same couplets that were used to evaluate those results, such that, the following is satisfied in the chosen triplet:

1) Minimum activity ratio between the high activity paths to low activity path is 5x. The activity ratio between the higher activity paths should be minimal.
2) In terms of typical delay, all paths are within 15% difference in typical delay to each other.

In Figures 10-11, for any data cell of the variation matrix, 10 possible triplets are evaluated. On an average, large improvements are observed in the prediction results for all triplets, except for a few outliers. Hence, each data cell value records an average of the %prediction over the chosen triplets. The sensitivity of the plain detection is almost reduced to nil, and percent detection is regained to 100%, and the exact age prediction is also correct over 90% of times, if the activity ratio between high activity and low activity path is at least 10x (minimum activity ratio).

6.3 Real circuits

The 3-D method is deployed on a few standard circuits like multiplier, divider, discrete-cosine-transform (DCT) module, and combinational circuits from ISCAS benchmark. Top critical paths were extracted from the circuits. As expected, the degree of variation in typical delays among the critical paths is not more than 10%. Some sample results for each flavor of circuit, is shown in Table2. The typical delay difference between the 3 chosen paths is also captured, and minimum activity ratio is 10x.

Circuit	**% Diff in typical delay**	**Detection of Old/New**	**Exact Age Prediction**
DCT	6-7%	100%	97.5%
Divider	<1%	100%	98.3%
C6882 (ISCAS)	15%	97.5%	91%

Table 2: Results for standard circuits

This idea can be easily extended to real designs. Finding the candidate paths, as per the requirement of the detection scheme should not be very difficult. Critical paths from a functionally active block can be chosen. And the third path can be chosen from a test path of the chip. If the critical test paths are not as long, we can re-choose the high activity paths such that the typical delay is in the range of the critical test path. Eventually, the aim is to not have more than 10% typical delay difference between the paths. If the typical delays of the chosen paths are almost equal, then even 2 paths of different activity are sufficient for successful detection.

7. Conclusion and Future Work

In this paper, we presented a technique for successful detection of counterfeits among existing ICs which do not have in-built age-detection circuits. For indicating the age of the design, we used a simple parameter of circuit delay, and filtered out the impact of process variation by using the relationship between the delays of paths, instead of using the delay of a single path. Our results that were based on industry-enabled simulation framework show a detection rate of over 97% for identifying an old IC from a new IC. As no circuit study is complete without real chip validation, as future work, we plan a chip tapeout. A variety of paths with varied typical delay will be fabricated. All the chips will be extensively characterized in terms of delay while running at different operating voltages. Later, the chips will undergo accelerated aging using heat and high operating voltage. The chips will be consequently characterized several times and the results will be aggregated. The proposed methodology will then be employed to detect aged versus new devices and prediction rates will be compared to those from simulation results.

8. REFERENCES

[1] http://armed-services.senate.gov/statemnt/2011/11%20November/Sharpe%20Slides%2011-08-11.pdf

[2] http://spectrum.ieee.org/riskfactor/computing/hardware/the-financial-risks-of-counterfeit-semiconductors

[3] http://www.isuppli.com/Semiconductor-Value-Chain/News/pages/Top-5-Most-Counterfeited-Parts-Represent-a-$169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx

[4] http://www.ihs.com/info/sc/a/combating-counterfeits/index.aspx?tid=t4.

[5] http://www.reuters.com/article/2010/10/26/us-china-counterfeit-defence-idUSTRE69P3GH20101026.

[6] F. Koushanfar and G. Qu, "Hardware metering," in *Design Automation Conference (DAC),* pp. 490 –493, 2001 2001.

[7] F. Koushanfar, "Integrated circuits metering for piracy protection and digital rights management: An overview," Invited Paper, 2011.

[8] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium,* SS'07, (Berkeley, CA, USA), pp. 20:1–20:16, USENIX Association, 2007.

[9] W. Griffin, A. Raghunathan, and K. Roy, "Clip: Circuit level ic protection through direct injection of process variations," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on,* vol. 20, pp. 791 –803, may 2012.

[10] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of puf-based "unclonable" rfid ics for anti-counterfeiting and security applications," in *RFID, 2008 IEEE International Conference on,* pp. 58 –64, april 2008.

[11] 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.

[12] P. Gupta and A. B. Kahng, "Manufacturing-aware physical design," in *ICCAD '03: Proceedings of the 2003 IEEE/ACM international conference on Computer-aided design.* Washington, DC, USA: IEEE Computer Society, 2003, p. 681.

[13] A. H. Baba and S. Mitra, "Testing for transistor aging," VLSI Test Symposium, IEEE, vol. 0, pp. 215–220, 2009.

[14] X. Chen, Y. Wang, Y. Cao, Y. Ma, and H. Yang, "Variation-aware supply voltage assignment for minimizing circuit degradation and leakage," in ISLPED '09: Proceedings of the 14th ACM/IEEE international symposium on Low power electronics and design. New York, NY, USA: ACM, 2009, pp. 39–44.

[15] T.Douseki, M.Harada, and T.Tsuchiya,"Ultra-low-voltagemtcmos/simoxtechnologyhardenedtotemperaturevariation," Solid-State Electronics, vol. 41, pp. 519–525, 1997.

[16] D. Lorenz, G. Georgakos, and U. Schlichtmann, "Aging analysis of circuit timing considering nbti and hci," in On-Line Testing Symposium, 2009. IOLTS 2009. 15th IEEE International, June 2009

[17] M. Alam and S. Mahapatra, "A comprehensive model of pmos nbti degradation," Microelectronics Reliability, vol. 45, no. 1, pp. 71 – 81, 2005.

[18] S. Borkar, "Electronics beyond nano-scale CMOS," DAC, 2006.

[19] D. K. Schroder, and J. A. Babcock, "Negative bias temperature instability: Road to cross in deep submicron silicon semiconductor manufacturing," Journal of Applied Physics, pp.1-18, July 2003.

[20] Bogdan Tudor, Joddy Wang, Zhaoping Chen, Robin Tan, Weidong Liu and Frank Lee , Synopsys Inc., "An Accurate and Scalable MOSFET Aging Model for Circuit Simulation", 12th Int'l Symposium on Quality Electronic Design, 2011

[21] http://www.chipscalereview.com/white_papers/DetectingCounterfeitComponents.pdf

[22] "Sub-Threshold Design for Ultra Low-Power Systems", By Alice Wang, Benton H. Calhoun, Anantha P. Chandrakasan, Pg 75