RF Supply Chain Tracking via Multi-Variate ID Assignment

Sule Ozev and Jennifer Kitchen
Arizona State University
Tempe, AZ

Rick Welker
Alphacore Inc.
Tempe, AZ

Abstract— **The integrated circuit (IC) design industry has adopted a globalized design and manufacturing flow where multiple teams contribute to the design of one IC, which gets fabricated in an off-site facility, and possibly tested in another. This paper describes methods for assigning and tracking unique IDs for RF ICs without resorting to additional circuitry. The proposed methodology utilizes performance and other parametric measurements under supply modulation and assigns IDs in a multi-variate manner while taking repeatability and reproducibility errors in measurements into account.**

Keywords— RF IC; unique IDs; circuit testing

I. Introduction

Integration of a multitude of functionalities within the same chip has resulted in enormous design complexity that requires the involvement of many players, including multiple sites, third party intellectual property (IP) suppliers, third party manufacturing, probing, and test facilities [1]. Furthermore, owning and operating a foundry with advanced capabilities can no longer be afforded by most design companies [2-4]. The integrated circuit (IC) design industry has adopted a globalized design and manufacturing flow where multiple teams contribute to the design of one IC, which gets fabricated in an off-site facility, and possibly tested in another. Globalization of IC design and manufacturing flow has successfully ameliorated the design complexity and fabrication cost challenges, and helped deliver cost-effective products. Splitting design and manufacturing into separate businesses has enabled small and innovative design companies to flourish. While such a distributed flow helps meet the stringent time-to-market deadlines and offer a financially viable model, it is also vulnerable to various forms of security threats in the supply chain that involves designers, foundries, test facilities, and distributors until the end-product reaches the customers. These threats include malicious changes in the process and circuit parameters, intellectual property (IP) piracy, and counterfeit ICs due to overproduction by the foundry or ICs recycled from used devices [3-9].

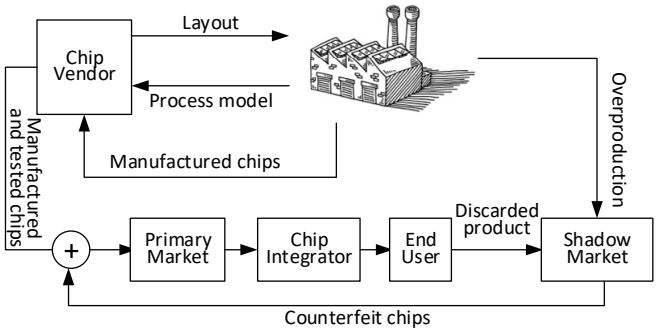

Figure 1: Threat Model

II. Threat Model

As illustrated in Figure 1, among the security threats, the most prominent one has been counterfeit ICs. Aged, rejected, or cloned parts, also known as counterfeit chips, find their way into the supply chain and pose a big threat to profitability, security and reliability of electronic products. It is being reported that counterfeit ICs are among the biggest threats to the semiconductor industry today and result in an annual revenue loss of $100 billion [6]. Among the various sources of counterfeit ICs, the most common is the class of "resold ICs"; these are used ICs that are stripped from the boards, sorted by size and/or lead count, and reprocessed to look like brand-new products. A natural end-result is reduced reliability and loss of reputation to the brand name, as the expected "remaining" lifetime of the resold IC is shorter than that of a brand-new part. Other forms of counterfeit ICs include those that are overproduced by an untrusted fab, in addition to reverse engineered, remarked, or cloned ones.

III. Prior Work

Researchers have been addressing the counterfeit IC problem recently; various techniques are summarized in [7]. In [8], the authors suggest using physical tests through part authentication tools, visual inspection, and X-ray imaging. The use of specialized IC packages to incorporate authentication technologies is another technique to combat counterfeiting [9]. Statistical approaches that aim at detecting "resold" counterfeit parts and differentiating them from authentic ones are presented in [10]; these techniques require either a golden model or samples from a trustworthy supplier for effective differentiation of resold, and thus aged, parts. Insertion of on-chip hardware for counterfeit IC detection is another technique; on-chip odometers [11] or sensors [12] to estimate the age of a device can be useful in the identification of recycled (or resold) components. Other hardware-based solutions include logic obfuscation methods [13] that break the functionality of a device in the absence of the "secret key" applied from a secure on-chip memory location; a counterfeit part would be nonfunctional without a proper key.

Exploiting the process variations and the uniqueness of individual manufactured parts in creating an ID has also been proposed. The use of a physically unclonable function (PUF),

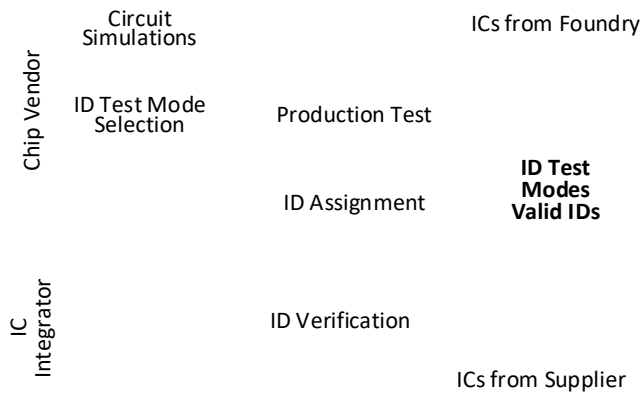

Figure 2: Supply Chain Tracking via Unique Identifiers

which aims at capturing process variations via slight changes in timing or current in generating unique responses to challenges, has been proposed [14]. A special form of a PUF is an SRAM/DRAM with its power-up content acting as a fingerprint of the device; the techniques in [15] utilize on-chip SRAM/DRAMs for intrinsic ID generation.

IV. Proposed Methodology

The goal of circuit identification methodology is to assign a unique identifier to each circuit at production time and track this ID until it is integrated into the system to enable supply chain monitoring. In this way, any unauthorized insertions into the supply chain can be detected with invalid IDs. Another advantage of unique IDs is that chips that have been aged and inserted back into the supply chain can be identified as such since the assigned IDs also change with wearout and a used device can present with an invalid ID.

Figure 2 shows the flow of the proposed supply chain tracking approach. During the design phase, the chip vendor determines the test parameters that will be used for ID generation. These test modes can include functional tests (such as gain, third order input intercept), and non-functional tests, such as supply current or DC offsets. The tests are selected to achieve the best differentiation between devices which can be determined via Monte-Carlo simulations. For all the ICs returned from the foundry, ID assignment is conducted based on pre-determined measurements. The measurement settings and valid IDs are stored in a database maintained by the chip vendor and this database will be open to the public for ID verification purposes. The IC integrator duplicates these measurements before integrating the IC into the system and checks the validity of the IDs against the database. Invalid IDs can be due to test set-up mismatch, aged and recycled ICs whose IDs are no longer valid, and unauthorized ICs that result from overproduction or IP piracy. In order to mimize the misclassification rate, tests should be selected such that they are repeatable across multiple instruments and the ID assignment process should take repeatability and reproducibility errors into account.

A. ID Assignment Process

In order to generate the unique IDs without much hardware overhead and track the aging of the devices with use, we propose to utilize the parametric measurements that are already

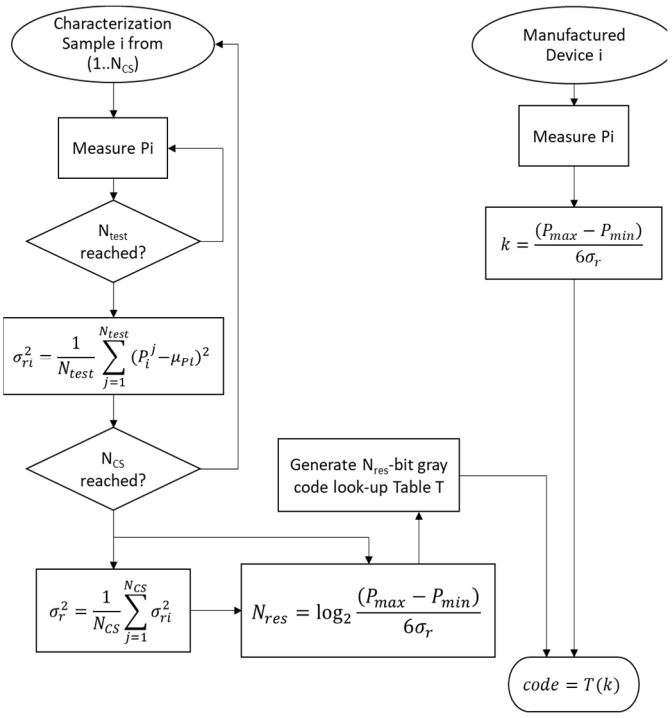

Figure 3: Taking repeatability and reproducibility errors into account during ID assignment

conducted during production testing. Specifically for RF circuits, there are a multitude of performance measurements already conducted for characterization and calibration purposes. The results of these measurements are often underutilized in the sense that a pass/fail decision is made on the device. However, these measurements provide a very accurate snapshot of the location of the device in the process parameter space. Since it is highly unlikely that two devices are identical in terms of process parameters, a unique ID can be generated by using these conducted measurements.

Figure 3 shows the proposed algorithm for multi-variate ID assignment that utilizes the performance measurements from the RF devices. For each characterization sample, we measure the performance parameters. For each device and each performance parameter (P_i), we conduct N_{test} measurements and determine the repeatability (σ_{ri}). This repeatability analysis is conducted and averaged over N_{CS} samples (σ_r). This is the error standard deviation with worst case error being $3\sigma_r$. We set this to half of the least significant bit (LSB) value for digitization. Thus, one LSB is equal to $6\sigma_r$. We also determine the range of the measurements over the characterization samples, which will determine the bit resolution of the code (N_{res}). We generate a gray code lookup table with N_{res} resolution, where the resolution is dynamically determined once the initial characterization set of devices arrive from the foundry. The resolution as well as the maximum and minimum boundaries for the performance parameters will be set during the production ramp-up. However, if the parameter profiles change during the product life cycle of the device, these variables can be adjusted. Since these variables are stored in the database along with the identifiers, dynamically adjusting ID assignment

variables does not lead to duplication or misclassification. Once the devices from manufacture arrive, their parameters will be measured and digitized according to this gray code table, minimum, maximum, and resolution. This process yields a partial identifier based on one performance parameter. The measurement and ID assignment process is repeated for all performance variables and the codes are concatenated to obtain the overall digital ID. Note that since the resolution of the partial IDs depend on the distribution of devices as well as the measurement repeatability and reproducibility, each measurement may provide a partial ID with a different resolution.

For some of the parameters, the measurements may not yield enough resolution when repeatability and reproducibility errors are taken into account. These measurements can be taken out of the ID assignment process. Alternatively, if the repeatability errors are due to environment noise and equipment resolution, their effect can be suppressed by repeating measurements. If a measurement is repeated N_{rep} times, the standard deviation for repeatability will reduce by a factor of $\sqrt{N_{rep}}$ [16].

B. Determining Enhanced Test Modes for ID Uniqueness

In order to generate a unique ID for RF ICs, we rely on inherent process variations and the multitude of measurements that we can obtain from these devices. Unfortunately, when the performance parameters of RF ICs are measured under functional conditions, the goals of ID generation and tracking are in conflict with the goals of the designers who spend enormous effort to suppress the effect of process variations.

While designers strive for process robustness at nominal operating conditions, such as supply voltage, noise, temperature, same robustness is generally difficult to maintain over a large variation in operating conditions. By modifying these operating conditions during testing, we can increase sensitivity to process parameters. Furthermore, we can define additional measurements on the RF ICs that do not correspond to performance parameters. For instance, whereas the overall current consumption is tightly controlled, the current of various building blocks may be smaller and therefore have higher sensitivity to process variations. This sensitivity increase is only temporary and does not result in further degradation of circuit performance. Thus, for ID generation, we rely on this temporary process sensitization to ensure that manufactured ICs can be assigned unique IDs. In this paper, we explore the use of two techniques for unique ID generation:

Using lower supply voltages: Instead of measuring performance parameters only at the supply voltage in the normal operation mode, we enhance the ID generation by measuring the same parameters at lower supply voltages. The motivation behind this approach is that lower supply voltage levels cause greater dispersion in circuit performances, and hence increase the diversity of device behavior. Increased diversity will result in better identification of circuits.

Using direct current (DC) voltages in addition to performance parameters: Circuits are generally designed to suppress process variations via self-stabilization techniques. For instance, bias current stabilization may be used to maintain

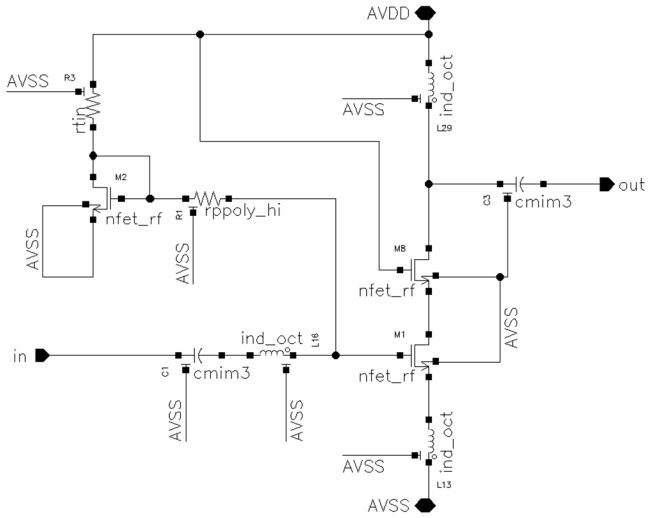

Figure 4: LNA circuit used in the experiments

performance over process variations. Hence, performance may not show much diversity. However, to maintain the bias current, bias voltage needs to be adjusted. Hence, by measuring DC parameters at various nodes, identification can be enhanced.

V. Experimental Set-up and Results

The ID generation technique has been applied to an LNA circuit that is shown in Figure 4 where 1000 Monte-Carlo samples have been evaluated for the uniqueness of the IDs and their Hamming Distance (HD). In addition to simulations, a small sample of commercial LNAs have been evaluated for ID assignments, robustness of ID assignment including repeatability and reproducibility, and progression of IDs as the devices age. Measurements for the LNA include S-parameters, 1dB compression point, DC voltage, Noise Figure, and DC current.

A. ID Uniqueness and Assignment

We have evaluated the repeatability and the reproducibility of the various equipment in the lab to assign the IDs. Measurements include S-parameters, P1dB, noise figure, DC

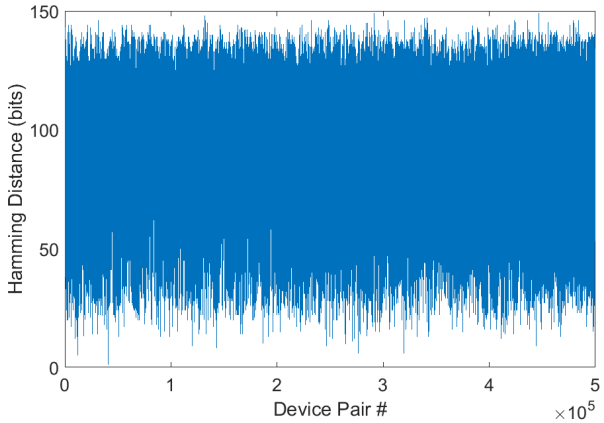

Figure 5: Hamming Distances of IDs for the Device Pairs of 1000 Monte-Carlo Samples (0.1dB measurement repeatability)

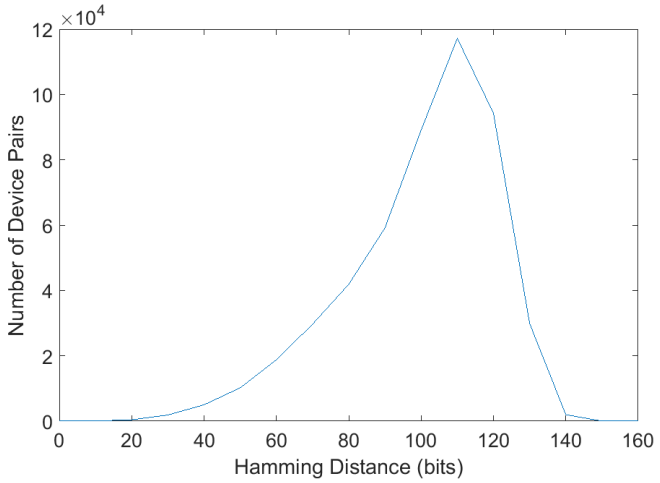

Figure 6: Histogram of Hamming Distances for 0.1dB measurement repeatability

current, and output DC voltage. The repeatability of the S-parameter measurements, as well as P1dB and noise figure measurements is found to be within 0.1dB; the repeatability of the DC current measurements is found to be within 100uA, and the repeatability of the DC voltage measurements is found to be 1mV. We have also confirmed that by repeating the same measurement and taking the average of the results, the repeatability can be reduced according to the square-root law. For instance, if we want to determine the S-parameters with 0.05dB repeatability, then the same measurement needs to be conducted 4 times and the average needs to be taken.

Based on the simulations results of 1000 LNAs under process variations, we have evaluated the ID uniqueness at the baseline repeatability of the measurement equipment (single measurement per parameter is conducted), as well as with improved repeatability by averaging the samples of the same measurement. Thus, each parameter may provide a different length ID. For some parameters, such as the noise figure measurement at 1.0V, the resulting measurements all fall within the equipment repeatability errors and thus this measurement does not provide any distinction between the device pairs. Figure 5 shows the Hamming Distance for device pairs when the S-parameter and P1dB measurements are conducted with 0.1dB repeatability (single measurement result is taken). All generated IDs are unique and the total bit length of the ID is 227 bits. As one can observe from the figure, the majority of Hamming Distances fall around the 40-50% range with the mean of 100 bits.

Figure 6 shows the histogram of the Hamming Distance of device pairs from Figure 5. When a Gaussian distribution is fitted to this histogram, the 3sigma minimum of Hamming Distance evaluates to 38 bits. If this is used as criterion for accepting/rejecting devices, there will be 0.3% yield loss due ID assignment, which is a negligible number compared to yield loss due to process variations as well as defects.

Figure 7 shows the Hamming Distance for device pairs when the S-parameter and P1dB measurements are conducted with 0.05dB repeatability (each measurement is repeated 4 times and the average result is recorded before ID processing). All

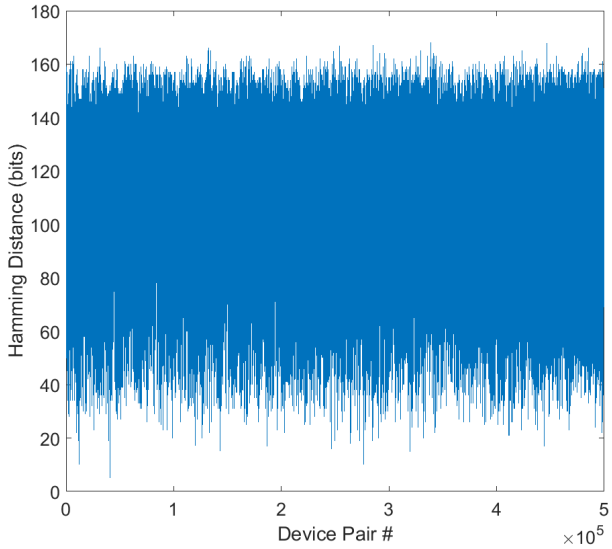

Figure 8: Histogram of Hamming Distances for 0.05dB measurement repeatability

generated IDs are unique and the total bit length of the ID is 260 bits (the resolutions of DC current and voltage measurements have not been increased). As one can observe from the figure, the majority of Hamming Distances fall again around the 40-50% range with the mean of 117 bits. Figure 8 shows the histogram of the Hamming Distance of device pairs from Figure 7. When a Gaussian distribution is fitted to this histogram, the 3sigma minimum of Hamming Distance evaluates to 53 bits. Due to the increased number of ID bits, one can reduce the yield loss by increasing the tolerance, for instance using 4sigma of 6sigma criterion for accepting/rejecting devices. However, this scheme will increase the test time nearly 4-fold since majority of measurements are based on S-parameters.

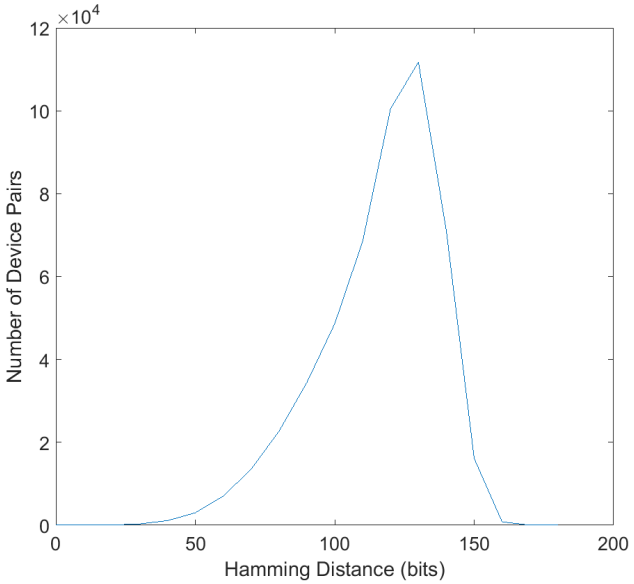

Figure 7: Histogram of Hamming Distances for 0.05dB measurement repeatability

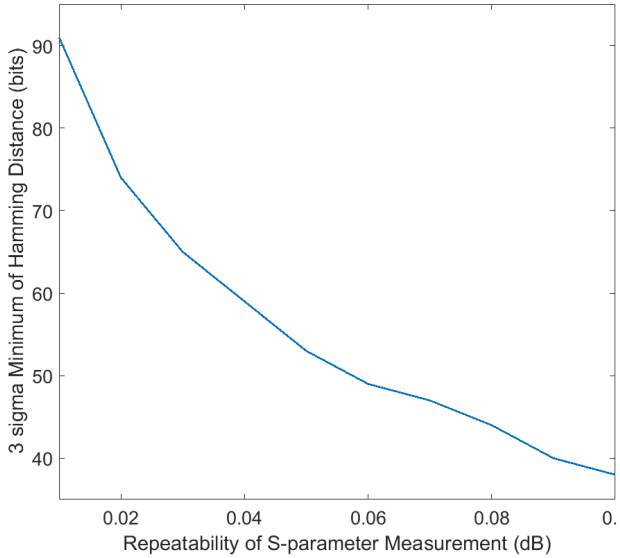

Figure 9: Impact of S-parameter measurement repeatability on minimum Hamming Distance

Finally, Figure 9 shows the impact of measurement repeatability on the 3sigma minimum of the Hamming Distance between device pairs. We observe that reducing repeatability errors by averaging repeated measurements results in better Hamming Distance between device pairs at the expense of increased test time. Comparatively, the S-parameter measurements are fairly quick and can be repeated with a 10ms test time when the test set-up does not need to be changed. Hence, the overall test time impact from repeating 4 times is not deemed prohibitive.

B. ID Aging

An important advantage of using the functional device parameters for ID assignment is that the parameters of the underlying physical structures, such as the threshold voltage of the transistors, will shift with use, resulting in changes in performance parameters. Therefore, as the device ages, the IDs

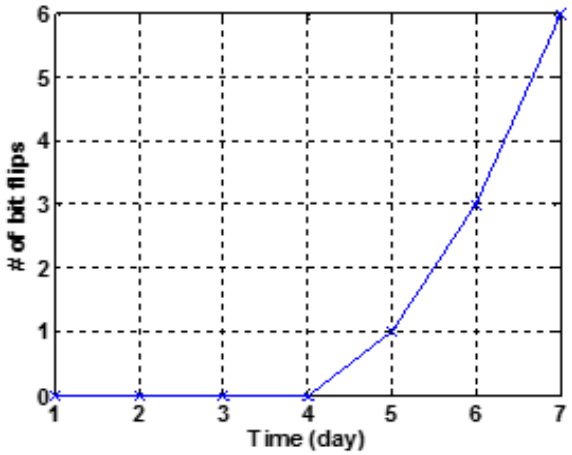

Figure 11: ID bit flips for 7 days of accelerated aging for a commercial LNA device

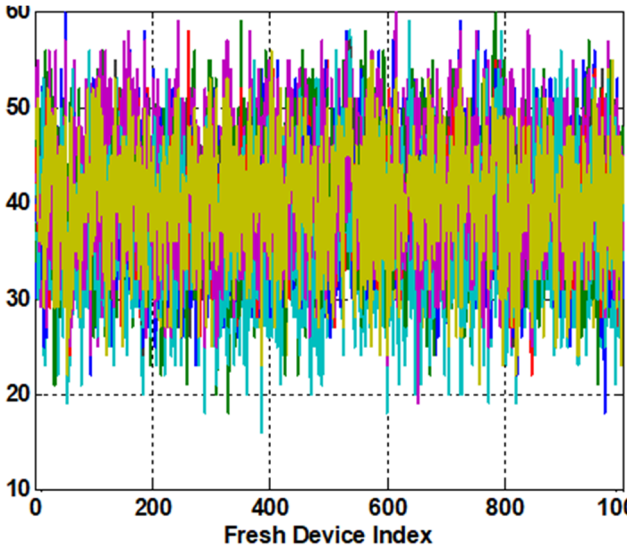

Figure 10: Hamming Distance of 50 aged ID from the 1000 fresh IDs

will start displaying bit flips, and eventually result in invalid entries as compared to the database. This is desirable for supply chain tracking since we would like to be able to detect recycled ICs as well as overproduction and pirated designs. In order to evaluate the ability to detect recylced or re-used ICs, we have used our reliability simulator [17] to age the devices and monitored the changes in performance parameters as well as pairwise Hamming Distance of IDs. Here, we also compared the aged device IDs to their fresh IDs. Since aging simulations are time consuming, 50 devices are selected at random from the 1000 Monte-Carlo samples for aging. Figure 10 shows the Hamming Distance of aged IDs with respect to the 1000 fresh IDs at 4 months of nominal use time. After this point, the 50 aged IDs differ from the fresh IDs by more than the tolerable BER and therefore are deemed as invalid. Thus, we conclude that after about 4 months of use, the IDs will no longer be valid.

We have also verified the effect of aging on ID assignment via limited hardware measurements. We have used a commercial off-the-shelf LNA for this experimental evaluation. 5 copies of the LNA are subjected to accelerated aging [18] at 20% supply voltage overstress and at 200° C temperature for 7 days. The devices are removed from the stress environment periodically to monitor their performance parameters. For this experiment, S11, S22, gain, and supply current are used for ID assignment. Before aging, ID resolution and tolerable BER (5 bits) are determined as outlined in Figures 3 and 6. All 5 devices displayed no bit flips during the first 3 days and started displaying bit flips on the 4th day of the aging experiment. 2 of the devices catastophically failed during the subsequent days. For the 3 remaining devices, performance parameters are monitored and recorded. We determine that after the 7th day of accelerated aging, the devices no longer display valid IDs. As an example, Figure 11 shows the bit flips in the ID of one of the aged devices. For this device, the BER threshold is crossed after Day 6. The other two devices also show simular results (Days 5-6). This accelerated aging duration corresponds to about 4-5 months of nominal use for the LNA device.

VI. ACKNOWLEDGEMENTS

This work was supported by Air Force Research Lab and Alphacore Inc. through the SBIR Phase II Program AF 161-140.

VII. REFERENCES

[1] "International Technology Roadmap for Semiconductors." http://www.itrs.net/Links/2011ITRS/Home2011.htm.

[2] DIGITIMES Research, "Trends in the global IC design service market." http://www.digitimes.com/Reports/Report.asp?datepublish=2012/3/13n&pages=RSn&seq=400n&read=toc.

[3] Intelligence Advanced Research Projects Activity, "Trusted Integrated Circuits Program." https://www.fbo.gov/utils/view?id=b8be3d2c5d5babbdffc6975c370247a6.

[4] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending Piracy of Integrated Circuits," *IEEE/ACM DATE*, pp. 1069–1074, 2008.

[5] R. Chakraborty and S. Bhunia, "HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection," *IEEE TCAD*, vol. 28, no. 10, pp. 1493–1502, 2009.

[6] M. Pecht and S. Tiku, "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectrum*, vol. 43, no. 5, pp. 37–46, 2006.

[7] F. Koushanfar *et. al*., "Can EDA Combat the Rise of Electronic Counterfeiting?" *IEEE/ACM DAC*, pp. 133–138, 2012.

[8] K. Chatterjee and D. Das, "Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Transactions on Component Packaging Technol*ogy, vol. 30, no. 3, pp. 547–549, 2007.

[9] N. Kae-Nune and S. Pesseguier, "Qualification and testing process to implement anti-counterfeiting technologies into IC package," *IEEE/ACM DATE*, pp. 1131–1136, 2013.

[10] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-Delay Fingerprinting for Identification of Recovered ICs" *IEEE DFTS*, pp. 13–18, 2012.

[11] "Detection of counterfeit electronic components," http://www.aeri.com/detection-of-counterfeit.asp.

[12] R. S. Chakraborty and S. Bhunia, "Security against hardware Trojan through a novel application of design obfuscation," *IEEE/ACM ICCAD*, pp. 113–116, 2009.

[13] Y. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," *USENIX Security Symposium*, pp. 291–306, 2007.

[14] B. Gassend et al, "Silicon physical random functions," *ACM Conference on Computer and Communications Security*, pp. 148–160, 2002.

[15] S. Rosenblatt et al, "Field Tolerant Dynamic Intrinsic Chip ID Using 32 nm High-K/Metal Gate SOI Embedded DRAM," *IEEE JSSC*, vol. 48, no. 4, pp. 940–947, 2013.

[16] Burns, Mark, Gordon W. Roberts, and Friedrich Taenzler. An introduction to mixed-signal IC test and measurement. Vol. 2001. New York: Oxford university press, 2001.

[17] Venkatasubramanian, Ramachandran, Doohwang Chang, and Sule Ozev. "Analysis and mitigation of electromigration in RF circuits: An LNA case study." In 2011 Sixteenth IEEE European Test Symposium, pp. 215-215. IEEE, 2011.

[18] Celaya, José R., Philip Wysocki, Vladislav Vashchenko, Sankalita Saha, and Kai Goebel. "Accelerated aging system for prognostics of power semiconductor devices." In 2010 IEEE Autotestcon, pp. 1-6. IEEE, 2010.