Performance Optimization for On-Chip Sensors to Detect Recycled ICs

Bicky Shakya*, Ujjwal Guin†, Mark Tehranipoor*, Domenic Forte*
* Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL
bshakya@ufl.edu, {tehranipoor, dforte}@ece.ufl.edu
†Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT
ujjwal@engr.uconn.edu

***Abstract*—IC recycling has become a grave problem in today's globalized semiconductor industry, with potential impact to critical infrastructures. In order to mitigate this problem, various Design-for-Anti-Counterfeit (DfAC) measures have been recently proposed. In this paper, we look at DfAC strategies based on recycling sensors, most notably the ones based on a pair of ring oscillators, which rely on integrated circuit aging phenomena to detect usage of ICs in the field. We introduce a novel optimization technique that generalizes to most recycling sensors suggested so far in literature and gives manufacturers exact control over parameters that determine sensor performance, such as yield, misprediction and area overhead. A detailed analysis of various factors affecting recycling sensor performance is presented and an optimization problem is formulated and verified using simulations, in order to demonstrate the accuracy of the approach.**

I. Introduction

Counterfeit electronic components pose a great risk to the security and reliability of electronic systems. Due to the global nature of the electronic component supply chain, cases of counterfeit electronics are on the rise. Counterfeit components, whether they are integrated circuits (ICs), dies or electronic systems, can be broadly classified into recycled, remarked, out-of-spec, defective, overproduced and cloned components [1] [2]. Currently, the most prevalent form of counterfeiting is recycling, whereby used or discarded ICs are recovered from printed circuit boards (PCBs) and then reintroduced into the supply chain as if they were new components from the original equipment manufacturer (OEMs). If such ICs are used by critical infrastructures (e.g. military, health-care etc.), their propensity towards failure could lead to catastrophic consequences including the loss of human lives. Aside from the degradation of used parts from silicon aging, the recycling process itself typically involves exposure to high temperatures, water, corrosive acids and sanding. Such a process introduces physical and electrical defects into ICs [2] [3], which lower their performance and durability. Further, latent defects may be introduced during the recycling phase, due to which ICs pass during initial testing but may fail in later stages, such as during operation in the field. Recent news on recycled ICs found in military systems [4] [5] highlight the severity of this problem.

Currently, there is very little research into measures for preventing/detecting counterfeit ICs. Physical and electrical tests [3] [6] can be used to study IC parameters for signs of counterfeit defects . However, such strategies require extensive time and cost, and are not feasible to analyze entire lots of ICs, especially in the case of physical tests. Support vector machines (SVM) [7], aging analysis for FPGAs using ring-oscillators [8] and path-delay fingerprinting [9] have also been suggested to detect counterfeit ICs from genuine ones. Unfortunately, such techniques require comparison of the ICs under test to genuine or 'golden samples', which might not always be available, especially for legacy components. Techniques such as hardware metering [10] lock ICs once they are produced in the foundry and require authentication from the design house, so that only authenticated chips can be accepted. However, metering techniques can only be used for the detection of overproduced/cloned ICs and are not applicable to recycled ICs. In [11], the authors utilized dynamic current analysis to determine the aging difference between high-activity and low-activity portions of functional blocks such as adders at almost zero-overhead. Unfortunately, such an approach requires at least a year of aging for reliable results. Thus, there is a need for design-for-anti-counterfeiting (DfAC) strategies that incorporate self-sufficient anti-counterfeiting mechanisms into chips during the design phase, with minimal overhead. Towards this end, the authors in [12] suggested the use of on-chip sensors based on ring oscillators (ROs) for detecting recycled die and ICs. The difference between the frequencies of a stressed RO, designed to age rapidly, and a reference RO, disabled during normal operation so that it does not experience aging, is used to estimate whether a chip has been previously used. However, they reported a minimum aging duration of at least a month to detect recycling. In [13], CDIR (Combating Die and IC Recycling) sensors, which are designed to account for negative bias temperature instability (NBTI) and therefore, age more rapidly, were introduced to detect ICs used for as little as 3 days. Such short durations are necessary to detect, especially for chips that have been salvaged from overstocked PCBs by crude recycling processes but show signs of aging only from system testing and not from extended use. Unfortunately, the proposed approach in [13] requires accelerated aging of ICs in order to draw aging distributions from the sensors and choose an optimal threshold to decide if a chip is recycled or not, with minimum probability of error. There has also been considerable work on aging-detection sensors such as the silicon odometer proposed in [14]. Although they are functionally equivalent to the ring-oscillator based recycling sensors in [12] and [13], such sensors are specifically designed to monitor IC aging phenomena and are not geared towards the detection of recycled ICs, where aging degradation needs to be maximized for minimum misprediction.

In this paper, we explore an extension of on-chip sensor-based detection schemes, such as those suggested in [12], [13] and [15]. In particular, we use the CDIR sensor, proposed in [13] to derive simulation data and present a novel

This project was supported in part by an AFOSR MURI grant under award number FA9550-14-1-0351.

optimization scheme, which, we believe, can apply to any of the previous recycling-sensor strategies. We analyze various parameters affecting the recycling-sensor performance and introduce measures to effectively detect recycled die/ICs with optimal misprediction rates (detecting new ICs as recycled, and vice-versa) and controllable yield, which relates to how many die/ICs with the sensors are suitable for detecting recycling. Our contributions in this paper can be summarized as follows:

- We present a detailed analysis of the various parameters affecting the sensor performance, such as decision thresholds, yield, misprediction, false alarm and structure of the sensor.
- We also investigate the use of multiple ring oscillators in a single sensor and propose an approach to select the best one out of N ring oscillator pairs for detecting recycling.
- We formulate an optimization problem and determine a solution that gives manufacturers the ability to control the trade-offs between the number of ring oscillators (area overhead) and performance (yield, detection rate), based on the aforementioned parameters. Also, the proposed approach does not require accelerated aging in order to determine an optimal threshold for detection.
- We perform experiments on simulated CDIR data and present results to show the effectiveness of our optimization technique. We compare our technique to making sensor decisions using ad-hoc approaches, and highlight the benefits of our proposed technique. Preliminary results show that the optimization technique presented offers improvements in detecting recycled ICs with lesser number of ring oscillators on a sensor, as compared to ad hoc decision techniques, with better control over the yield that the manufacturer desires, and with minimal error and misprediction rates.

The rest of the paper is organized as follows: Section II presents a brief overview of RO-based recycling sensors, from [9] and [13]. Section III describes the various parameters affecting sensor performance and provides a detailed analysis of their effects on detecting recycled ICs/die. Section IV provides a thorough explanation of our optimization strategy that allows a manufacturer to evaluate the trade-offs between the CDIR sensor structures, decision-thresholds and yield. Section V contains the results obtained from our optimization technique. Finally, section VI concludes the paper.

II. Background and Related Work

A. IC Aging

Integrated circuits experience aging due to operation, which causes a shift in their parameters. Aging phenomena in CMOS circuits can be attributed to two major effects: negative bias temperature instability (NBTI) and hot carrier injection (HCI).

- Negative Bias Temperature Instability (NBTI) occurs predominantly in PMOS devices due to the interface traps that are formed when negative gate voltages are applied at elevated device temperatures [16]. NBTI stress applied over a short term is recoverable but over the lifecycle of an IC, the effects of NBTI stress become permanent. These effects include an increase in the absolute threshold voltage of transistors (V_{th}), along with degradation of carrier mobility, drain current and transconductance in PMOS devices.

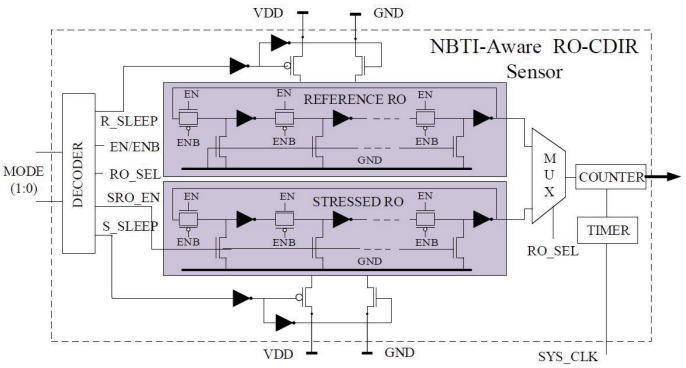

Figure 1. NBTI-Aware RO-CDIR [13]

- Hot carrier injection (HCI) is an aging phenomena contributing to change in parameters of NMOS devices. It occurs as carriers (electrons) tunnel out at elevated temperatures and get trapped near the $Si/Si0_2$ interface at the drain end of NMOS devices during dynamic switching. HCI also causes irreversible elevation of V_{th}.

The cumulative effect of IC aging is decreased chip performance. Although aging phenomena such as NBTI and HCI are a concern for reliability in ICs, they can be exploited to design effective sensors for detecting recycling of ICs.

B. Recycling Sensors

The NBTI-aware ring oscillator-based CDIR (Combating Die and IC Recycling/RO-CDIR) sensor exploiting CMOS aging phenomena was introduced in [13]. The RO-CDIR, shown in Figure 1, relies on the aging degradation and consequent decrease in frequency that the ROs experience as the chips in which they are placed are used. The RO-CDIR is based on a differential design, i.e. the difference in frequency between the reference RO (f_R) and the stressed RO (f_S) is used to estimate the 'age' of the chip. As the chips are used in the field, the reference RO, designed to age minimally, experiences minimal decrease in its frequency whereas the stressed RO's oscillation frequency goes down significantly. Thus, a large difference in frequency ($\Delta_f = f_R - f_S$) between the reference and the stressed RO would imply that the chip has been used and is possibly recycled. It is also to be noted that an initial difference in frequency might exist between the two ROs due to local process variations, leading to false positives at an early stage (global process variations cancel out as the reference and stressed RO pairs are placed close together and experience the same amount of global process variations). This makes the design of the ROs and choice of decision threshold (chosen frequency above which chip is declared recycled) very important.

The RO-CDIR has several operational modes that are controlled using various control signals. During the manufacturing and testing phases, both the reference and the stressed RO are in sleep mode ($R\_SLEEP = 0$ and $S\_SLEEP = 0$), which cuts off the power supply from both the ROs and prevents them from experiencing aging degradation. During the life-cycle of the chip (normal operation mode), the reference RO is still in sleep mode (does not experience NBTI-induced aging) while the stressed RO is in stressed mode (undergoes constant NBTI-induced stress). In order to maximize aging degradation in the stressed RO, the RO-CDIR architecture allows the inverters

in the stressed RO to be pulled to ground during every clock cycle in normal operation mode. This results in constant NBTI-stress of the PMOS transistors in the inverters. A description of other control signals, including those used for reading out the frequencies of the ROs during authentication phase, are given in [13].

The authors in [15] use a modified version of the RO-CDIR (termed as STRO) with voltage boosting, Schmitt-trigger based ROs and calibration to make recycled-IC detection in the range of a few seconds, despite process variation-dictated frequency differences. Unfortunately, the area overhead of the STRO is significant, and its performance is highly dependent on initial calibration and cannot be exactly predicted. Due to this, we use the RO-CDIR in the rest of our discussions. However, it is to be noted that the analysis we perform to optimize sensor performance still applies to the approach in [15] as well as [12] and [13].

III. Analysis of Sensor Parameters

In this section, we consider the following scenario, where a recycling sensor in a chip consists of a reference and a stressed RO (a single RO pair), in order to explain the different parameters involved. If we consider a sample space of all chips fabricated, where each chip contains $N = 1$ RO pairs in a CDIR sensor, we have two distributions of Δ_f (the frequency difference), with one at $t = 0$s (initial or after fabrication) and $t = t$s (after aging or use). Let us assume that the frequency distribution for Δ_f at $t = 0$s follows a normal distribution (we also find during experimentation that the distribution is indeed normal). It should be also be noted that since we are taking the difference of the reference and stressed ROs, both of which are placed close together and experience similar amounts of global variation, the frequency differences at $t = 0$s will be mostly due to local process variations (intra-die variations); the global process variations cancel out. Thus, the distribution at $t = 0$s is due to local variations. We also have a normal distribution of Δ_f at $t = t$s (shifted to the right due to aging degradation), where ts is an arbitrary aging duration. Both distributions are shown in Figure 2. The manufacturer then sets a threshold λ. The decision to declare if any chip C_i is recycled or not, depending on the frequency difference for chip i, $\Delta_{f,i}$, is therefore as follows:

$$\text{If } \Delta_{f,i} \leq \lambda, C_i \Rightarrow \text{new} \quad (1)$$

$$\text{If } \Delta_{f,i} > \lambda, C_i \Rightarrow \text{recycled} \quad (2)$$

While making such a decision, there are two ways of making a misprediction. The striped region in Figure 2 denotes the probability of false alarm (P_{FA}), which refers to deciding that a chip is recycled when it is actually new. This leads to an unnecessary loss of unused/fresh chips or yield loss. The grey region denotes the probability of miss (P_{miss}). P_{miss} has a more severe implication, as it means that a chip is declared as new when it is actually recycled. It is to be noted that in order to determine a λ that minimizes the probability of error ($P_{FA} + P_{miss}$), the distribution at $t = t$s must be known, for which accelerated aging of the chips would be required. On the other hand, the distribution at $t = 0$s is easily obtainable by taking measurements after the chips are fabricated. If we assume that only the distribution at $t = 0$s is available and we have λ, we can define another parameter $P_{FA} = \gamma$. In this case, γ indicates all the chips that have $\Delta_f > \lambda$ (see Figure 2).

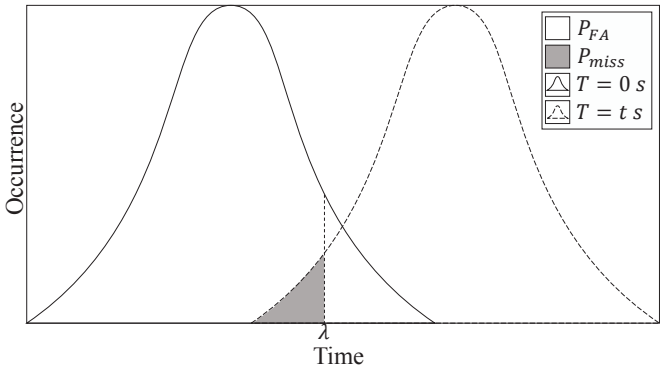

Figure 2. Frequency Distribution Curves for $T = 0$ s and $T = t$ s

Since these are the chips that could possibly cause an overlap between the distributions at $t = 0$s and $t = t$s, these are the chips that cannot be used and have to be discarded. In other words, γ lets the manufacturer pre-specify a yield loss (note here how our definition of yield loss has changed slightly from how yield was previously defined, where it was the chips that were falsely identified as recycled). Also, based on the fact that we only have the $t = 0$s distribution, the manufacturer can now only decide on a specific yield $(1-\gamma)$ and not P_{miss}.

In terms of deciding a threshold, if λ were set at the point of intersection between the two curves, P_{miss} would be equal to the probability of P_{FA}. The sum of P_{miss} and P_{FA} would then correspond to the minimum probability of error. In order to reduce P_{miss}, P_{FA} or both, three strategies can be employed:

- Reduce the spread of the distributions
- Shift distributions away from each other
- Move the threshold (λ).

Reducing the spread of the two distributions and shifting them away from each other results in the reduction of overlap between the distributions, which reduces the probability of error. Moving the threshold to the right (left) ensures that yield loss is minimized (increased) but at the same time, it leads to an increase (decrease) in the probability of miss (detecting a recycled IC as new). Thus, there is a trade-off in how well the sensor can perform with respect to the mispredictions, and the threshold decided. In order to further understand how threshold determination affects sensor performance, we present two different approaches of determining the threshold:

- *Naïve Approach*: Determine a threshold (for example, $\lambda = 0$) without any pre-specified constraints on yield and use it determine both yield loss and P_{miss}. It becomes clear that such an approach, similar to the threshold determination approach in [13], does not give the manufacturer any control over yield, and relies heavily on the aged distribution at $t = t$s being known.
- *Optimized Threshold*: For a desired value of γ, a corresponding value of λ is computed. This is the approach we shall build upon in Section IV.

In [13] and [15], RO-based sensors were proposed to both reduce the spread of the distributions and shift the distributions away from each other. However, the decision threshold (λ) was set based on knowing the exact aged distribution at $t = t$s and minimizing misprediction. This requires accelerated aging of the sensors to obtain the aged distribution and is undesirable from a manufacturer's perspective. Moreover, if we assume that the aged distribution is not available, this would imply that the threshold would have to be decided as per the naïve

approach. In this paper, we also touch on reducing the spread of the distributions and increasing their shift. However, we investigate approaches for determining an optimal threshold (λ) based on parameters such as yield, P_{miss} and number of ROs that the manufacturer desires.

Multiple RO Pairs

CDIR sensors with one RO pair are effective in detecting recycled ICs that have been used for several days [13]. However, the probability of error with such a CDIR sensor goes up when the workload of a chip with the CDIR sensor decreases (i.e. the chip is not 'on' all the time and aging in the ROs is not maximized) and shorter duration of use needs to be detected, especially for critical applications. In order to improve sensor performance, N RO pairs could also be employed on a single CDIR sensor, out of which the 'best' one that minimizes the probability of error could be chosen. In order to pick the 'best' RO pair and utilize the same for detection later on, we need to first decide on a threshold λ. Again, we can have two ways to decide the decision threshold λ. When we have N RO pairs to choose from, the naïve approach simply uses an arbitrary λ to reject chips and disregards any pre-specified constraints on yield loss. As a result, this approach will provide uncontrollable yield. With this approach, yield will increase only if higher number of RO pairs are used. For a more optimized approach, the threshold λ can be computed by deciding on how many RO pairs to use (N) and what yield needs to be achieved (Y) (details on this are provided in Section IV). After the threshold is decided, we can then proceed to pick the best RO pair with the following steps:

- Measure the frequency of each of the N RO pairs on a single sensor at $t = 0$s.
- Out of N RO pairs, select all RO pairs with $\Delta_f < \lambda$ and then, pick the single 'best' RO pair whose Δ_f is closest to λ. Doing so helps in reducing the spread of the distribution and minimizes overlap between the two distributions at $t = 0$s and $t = t$s, thereby minimizing the probability of error. We also term this selection approach as the '*multi-sensor selection rule*'. Note that for a given N, a chip is accepted is there is at least one RO pair out of N available that satisfy the constraint of $\Delta_f < \lambda$. If not, the chip is discarded and counts towards yield loss (γ).
- Once the best RO pair is selected, burn fuses in order to select the RO pair so that at $t = t$s, only the best RO pair is available for recycling detection.
- When a chip is encountered in the supply chain, measure Δ_f from the recycling sensor on the chip and apply Equations (1) and (2) to determine whether the chip is new or recycled. Note that the λ needed to make the decision is the same for an entire batch of chips, and can be assumed to be public knowledge.

With an increasing number of RO pairs, it is more likely that we can find the best RO pair. But this implies that we need extra area on the overall circuit in order to implement the N RO pairs which pushes up the area overhead. Thus, the goal would be to achieve the most optimal misprediction rates possible with minimum number of RO pairs employed. This optimization problem is the focus of the next section.

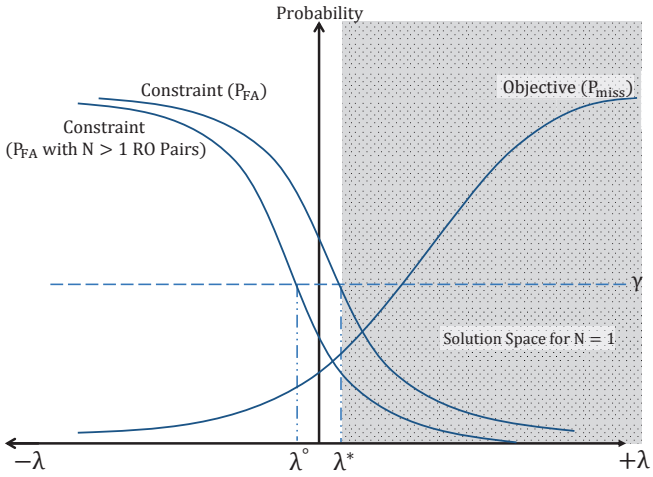

Figure 3. Graphical Representation of the Optimization Problem Scenario

IV. Optimization Problem and Solution

A. Assumptions

In Section III, it was clear that in order to control the probability of error and set a threshold accordingly, both distributions at $t = 0$s and $t = t$s were required. Although it is fair enough to assume that the distribution at $t = 0$s can be obtained by the manufacturer, the same cannot be said for the distribution at $t = t$s. In order to obtain this information, the chips need to be aged by the manufacturer, which is both inconvenient and impractical, especially since misprediction rates and the thresholds will change with aging duration. Let us assume that the only distribution we have is the one at $t = 0$s obtained from a decent sample (e.g. 1000 chips) of the total chips fabricated. We declare this distribution as $f_{t=0s}(x)$, which is a probability density function (pdf) describing the distribution at $t = 0$s (x is the random variable denoting frequency difference). Let us also assume that this distribution is Gaussian (normally distributed) and is described by $N(\mu, \sigma)$ (i.e. mean μ, and standard deviation σ are known). Further, for the case of N RO pairs in a single sensor, we also assume statistical independence for each RO pair i.e. the selection of one RO-pair is not affected by the rest of the RO pairs among N RO pairs considered (they are independent and identically distributed). We make this assumption as variations in oxide thickness and random dopant fluctuation [17] are the main source of variations for nearby ROs and are also independently distributed.

B. Optimization Problem and Parameters

An optimization problem is now formulated, which helps us to find a value for λ which can minimize P_{miss}, given a specified range of yield loss and N RO pairs. For the optimization problem, we consider the following parameters:

- **Predefined yield loss γ**: We set P_{FA} to be less than or equal to γ.
- **N number of RO pairs**: We also consider the scenario where there are N reference and stressed RO pairs, and one optimal RO pair can be chosen out of N RO pairs available.
- **Arbitrary threshold λ**: This is the solution to the optimization problem where we have a fixed γ and N RO pairs, and we seek to minimize P_{miss}.

Given all the parameters defined above, our optimization problem is then formally stated as follows:

$$\lambda^* = \arg\min(P_{miss}) \text{ subject to } P_{FA} \leq \gamma \tag{3}$$

The formulation conveys our goal of wanting to keep the yield at a desired level γ while making sure that recycled chips are detected with high probability (minimizing P_{miss}).

C. Optimization Solution for the Single RO Pair Scenario

A graphical representation of the parameters P_{FA} and P_{miss} is shown in Figure 3. For our Gaussian assumption, we can observe that P_{miss} is an increasing function of λ while P_{FA} is a decreasing function of λ (see also, Figure 2). The constraint that we set ($P_{FA} \leq \gamma$) is satisfied for all $\lambda > \lambda^\star$. In order to minimize our objective (minimize P_{miss}), we have to pick $\lambda = \lambda^\star$, where $\lambda^\star$ is the point where P_{FA} intersects γ (i.e $P_{FA} = \gamma$). Thus, the solution to our optimization problem will help us to pick a threshold ($\lambda^\star$), which is the threshold that can minimize P_{miss} while satisfying the constraints of the optimization problem.

We then solve the problem as follows:

$$\begin{aligned} P_{FA} &= \int_{\lambda}^{\infty} f_{t=0s}(x) = \gamma \\ &= \int_{\lambda}^{\infty} \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left[-\frac{1}{2\sigma_1^2}(\mathrm{x}-\mu_1)^2\right] dx \\ &= 1 - \frac{1}{2}\left[1 + \mathrm{erf}\left(\frac{\lambda-\mu_1}{\sigma_1\sqrt{2}}\right)\right] \end{aligned}$$

In the equation above, erf represents the error function [18] and x is the random variable denoting the Δ_f distribution at $t = 0$s. Solving the equation for λ, we get the following expression which expresses λ in terms of γ.

$$\lambda = \mu_1 + \sigma_1\sqrt{2}\,\mathrm{erf}^{-1}(1-2\gamma) \tag{4}$$

In a similar way, we can derive an expression for γ in terms of λ.

$$\gamma = \frac{1}{2} - \frac{1}{2}\,\mathrm{erf}\left(\frac{\lambda-\mu_1}{\sigma_1\sqrt{2}}\right) \tag{5}$$

D. Optimization Solution for the N RO Pairs Scenario

Similar to the case for $N = 1$, the solution to the optimization problem for N RO pairs will yield λ°, where $\lambda^\circ < \lambda^\star$ as employing N RO pairs increases the probability of picking the best RO pair. This RO pair can minimize the distribution spread for a given yield constraint (see Figure 3). With this in mind, the optimization technique is slightly modified to give us the formulation below, where P_{FA} now depends on the number of RO pairs available i.e, $P_{FA}(n)$:

$$P_{FA}(n) = P(x > \lambda; n) = \gamma \tag{6}$$

$$\binom{n}{N} P(x > \lambda)^N P(x \leq \lambda)^{n-N} = \gamma \tag{7}$$

Equation (6) implies that we have n RO pairs available in a CDIR sensor on a chip and we check if each of the n RO pairs fails the multi-sensor selection rule (Section III) i.e., $P(x > \lambda)$. We then use the independence assumption in Section IV-A to apply Bernoulli trials. This gives us Equation (7), where out of n trials (n RO pairs), we have N failures (N RO pairs failing). In order to simplify the equation, we can observe that we need N RO pairs to fail, out of n RO pairs available, for a chip to count towards yield loss γ. Thus, by setting $n = N$, we can arrive at the following:

$$\binom{N}{N} P(x > \lambda)^N P(x \leq \lambda)^{N-N} = \gamma$$

$$P(x > \lambda) = \gamma^{1/N} \tag{8}$$

With this, Equation (4) may be modified as follows:

$$\lambda = \mu_1 + \sigma_1\sqrt{2}\,\mathrm{erf}^{-1}(1-2\gamma^{1/N}) \tag{9}$$

It should be noted that this formulation can also be used to find N given γ and λ. Thus, given 2 parameters (e.g. γ and λ) that are set by the manufacturer, the formulation allows us to solve for the 3rd parameter (e.g. N). This is particularly useful because a formulation for finding N would help a manufacturer decide on how many RO pairs he would need in a sensor and how much area is available on the circuit, in order to achieve a certain yield $(1-\gamma)$ with λ. Similarly, in order to decide yield, the manufacturer could use the N formulation of Equation (5) in order to assess how much yield loss can be expected for a certain λ and N. If the yield results are poor, λ and N may be modified, depending on which option is more feasible in terms of area overhead and the resulting P_{miss}.

Table I
COMPARISON OF TWO DIFFERENT NAÏVE APPROACHES FOR N ROS AT $T = 10$ HRS WITH THRESHOLDS λ IN MHZ, RESULTING PROBABILITY OF MISS (P_{miss}) AND YIELD ($Y = 1-\gamma$))

	$\lambda = 0$		$\lambda = 3\sigma = 4.30$	
	P_{miss}	Y	P_{miss}	Y
N = 1	1.21	49.4	75.28	99.9
N = 2	1.34	74.4	55.10	100
N = 4	0.85	94.1	33.40	100
N = 6	0.10	98.2	18.30	100
N = 8	0.10	99.7	10.90	100
N = 10	0.00	100	7.00	100

V. EXPERIMENTS

A. Experimental Setup

In order to assess the effectiveness of our approach, the RO-CDIR was simulated using the 90 nm technology node (PTM) in HSPICE. A Monte-Carlo simulation was run to collect data on 1000 chips, each with a CDIR sensor with varying number of RO pairs (N). The frequencies of the reference and the stressed ROs were obtained at $t = 0$ and at $t = 10$ hrs. It is to be noted that for aging durations > 10 hours, sensor performance will only improve as aging degradation gets more pronounced. A worst-case global process variation of 20% for V_t (threshold voltage) and gate length L, and 6% for T_{ox} (oxide thickness), and local variation of 10% for V_t and L, and 3% for T_{ox} was incorporated into the simulations. A 51-stage RO was used in order to achieve the best results in terms of misprediction [13] and the supply voltage was set to $1.2V$.

In order to analyze our optimization approach, the decision threshold λ was computed using the naïve approach and the proposed optimized threshold approach (see Section III). For the scenario with N RO pairs, the multi-sensor selection rule (Section III) was applied. Using the optimization approach in Section IV, λ was computed for various combinations of N and γ. In order to see the accuracy of γ that was

Table II
THRESHOLDS (λ) IN MHZ, RESULTING PROBABILITY OF MISS (P_{miss}), DESIRED YIELD AND ACTUAL YIELD ($Y = 1 - \gamma$) FOR N ROS AT T = 10 HRS

	Desired Yield = 50%			Desired Yield = 75%			Desired Yield = 95%			Desired Yield = 98%			Desired Yield = 99.9%		
	λ	P_{miss}	Y	λ	P_{miss}	Y	λ	P_{miss}	Y	λ	P_{miss}	Y	λ	P_{miss}	Y
N = 1	-0.01	1.21	49.4	0.96	5.81	75.7	2.36	24.79	95.6	2.94	38.41	98.4	4.43	78.38	99.9
N = 2	-0.79	0.63	48.0	-0.01	1.34	74.4	1.09	3.17	94.7	1.54	4.59	98.1	2.66	12.4	100
N = 4	-1.44	0.00	50.0	-0.79	0.40	74.7	0.09	1.05	95.1	0.45	0.30	98.6	1.32	0.40	99.9
N = 6	-1.77	0.20	50.1	-1.18	0.14	73.4	-0.39	0.21	93.4	-0.08	0.10	97.8	0.68	0.10	99.9
N = 8	-1.99	0.00	48.8	-1.44	0.13	75.2	-0.71	0.21	93.5	-0.42	0.21	97.5	0.28	0.10	100
N = 10	-2.16	0.00	51.4	-1.63	0.13	75.7	-0.93	0.11	94.4	-0.66	0.10	97.9	-0.01	0.00	100

previously used in the optimization (i.e. set by manufacturer), we computed the value of γ from the CDIR data for various N and λ (for both the optimized threshold approach and the naïve approach) using the following relationship.

$$\gamma = \frac{\#\ chips\ without\ a\ single\ RO\ pair\ with\ \Delta_f < \lambda}{1000} \times 100\%$$

With the remaining chips or passed samples, P_{miss} was then computed for each λ using the data at $t = t$s by the relationship below:

$$P_{miss} = \frac{\#\ chip\ with\ \Delta_f < \lambda\ at\ \mathrm{t} = \mathrm{t}\ s}{\#\ chips\ with\ \Delta_f < \lambda\ at\ \mathrm{t} = 0\ s} \times 100\%$$

Here, the numerator denotes all the chips at $t = t$s that get detected as new ($\Delta_f < \lambda$) when they are actually recycled ($\Delta_f > \lambda$). The denominator, on the other hand, is the total number of chips that passed at $t = 0$s after discarding chips that did not have a single RO pair with $\Delta_f < \lambda$.

B. Discussion of Results

In Table I, the corresponding P_{miss} and yield ($Y = 1 - \gamma$) are given for the 'naïve' approach where $\lambda = 0$ and $\lambda = 3\sigma$ have been chosen without any constraints on the yield Y and N. For $N = 1$, the naïve approach with $\lambda = 0$ gets us a relatively low value of $P_{miss} = 1.21$. However, the yield turns out to be very poor (49.4%). We have also included data for $\lambda = 3\sigma$. If there were no constraints on Y and N, one could choose such a value of λ in order to account for the variation in the distribution at $t = 0$s and minimize the probability of false alarm. However, the results in Table I show that such an approach provides impressive yield ($\approx 100\%$ for all N) at the cost of high P_{miss} for all N. In either case, we can see that the naïve approach provides us unpredictable yield, and if we try to improve the yield to account for process variation, the probability of error drastically goes up.

Now, we assess the performance of the optimized approach. A sample of the data obtained by choosing various N and yield $Y = 1 - \gamma$ for the optimized approach from Section IV is presented in Table II. Note that in all cases, the probability of false alarm i.e. detecting a new chip as recycled is effectively zero. This is because the selection scheme discards all chips that do not have at least one RO whose $\Delta_f < \lambda$. We can also observe that the desired values of yield that we start with in the optimization problem match very closely with the observed values of yield (Y) that we get from experimental data in Table II. From the results, it is clear that as N is increased, P_{miss} decreases for all cases of expected yield. This is because as N increases, more RO pairs are available in a given sensor, and the probability that the selected RO pair out of N pairs has a Δ_f that is closer to the threshold, goes up. This also implies that with increasing N, the optimized approach lets us decrease λ in order to decrease P_{miss} (see Figure 2) while keeping $P_{FA} = 0$.

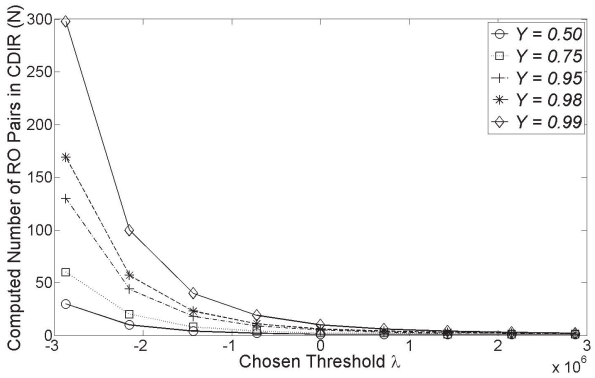

Figure 4. Required Number of RO Pairs for various yields (Y) and λ

We can also compare the performance of the naïve and the optimized approach, from Tables I and II . For $N = 4$, the naïve approach (Table I) with $\lambda = 0$ MHz provides us with $P_{miss} = 0.85$ and yield of 94.1%. Using the optimized approach (Table II), we can see that the best results are achievable for $N = 4$ at a threshold of $\lambda = 0.45$ MHz, which gives us $P_{miss} = 0.30$ and yield of 98.6%. Similar observations can be made for $N = 6$ and $N = 8$, where yield can be improved if the optimized approach is taken. Another drawback of the naïve approach is that in order to achieve similar values of P_{miss} and yield as the optimized approach, a higher number of ROs are required. For example, in order to achieve a yield of around 99%, we can use the optimized approach to give us a P_{miss} of 0.4 with $\lambda = 1.32$ MHz and $N = 4$. However, with the naïve approach with $\lambda = 0$, we would need $N = 10$ to achieve similar results. With $\lambda = 3\sigma$, we would need $N > 10$ in order to achieve a yield of around 99% and $P_{miss} < 1\%$. Similar observations can be made for a desired yield of 98% where $\lambda = 0.45$ MHz with the optimized approach can give us a yield of 98.6% for $N = 4$, whereas with the naïve approach with $\lambda = 0$, we would need additional RO pairs ($N = 6$) to achieve similar results. This has implications in terms of area overhead, as the naïve approach will require us to use more RO pairs than necessary.

Now, we assess the trade-offs between area, number of RO pairs (N) and yield (Y). Figure 4 shows the computed values of N for thresholds (λ) ranging from $-2\sigma_1 \leq 0 \leq 2\sigma_1$ and various values of yield ($Y = 1 - \gamma$), derived from the results of section IV. We can see that if we need to achieve a yield of 99% and we choose a threshold of $-2\sigma_1$, the required number of RO pairs in a CDIR goes above 300. Clearly,

Table III
AREA OVERHEAD ESTIMATES (IN %) FOR N RO PAIRS IN SENSOR

Benchmark	Size (# Gates)	N = 1	N = 2	N = 4	N = 6	N = 10	N = 50	N = 75	N = 100	N = 150
b15	19118	0.91	0.91	3.49	5.21	8.65	43.44	65.16	86.88	130.32
DSP	32436	0.35	0.68	1.35	2.02	3.35	16.83	25.24	33.66	50.48
ethernet	46771	0.24	0.48	0.94	1.40	2.32	11.66	17.49	23.32	34.98
vga_lcd	124031	0.09	0.18	0.35	0.53	0.88	4.41	6.62	8.83	13.24
leon2	780456	0.01	0.03	0.06	0.08	0.14	0.69	1.04	1.38	2.07

in order to make an educated decision about the required number of RO pairs, the optimized results on yield, threshold and available silicon area all need to be considered; ad hoc decisions on the parameters are not feasible. For an estimate of how N can affect area overhead, the RO-CDIR from [13] was inserted into several benchmark circuits for various N. The area overhead estimates (in %), calculated as the total size (number of logic gates) of the sensor to the total size of the benchmark, are shown in Table III. This can give the manufacturers an estimate on how much area overhead they can expect for various number of RO pairs N.

VI. CONCLUSION

In this paper, we have presented an approach to optimize the performance of recycling-detection sensors depending on parameters such as yield, accuracy of detection and number of sensors employed. Compared to ad hoc approaches of determining parameters such as the decision threshold, our approach lets the manufacturer have exact control over the yield and accuracy of the sensors employed on their chips. By performing simulation on the CDIR sensor proposed in [13] as an example, we validated our approach, which is general enough to be applied to all kinds of RO-based recycling-detection sensors that have been proposed in the literature so far. We claim this because the approach presented requires only the frequency distributions and is independent of the actual sensor design. The optimized approach lets the manufacturer assess the trade-offs between the number of RO pairs (N), yield (Y) and accuracy (in terms of P_{FA}) in order to incorporate the best recycling sensor into their chips.

REFERENCES

[1] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug 2014.

[2] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*. Springer Science & Business Media, 2011.

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

[4] J. Reed. (2011, November) Counterfeit parts found on P-8 Poseidons. Online. DefenseTech.org. http://defensetech.org/2011/11/08/counterfeit-parts-found-on-new-p-8-posiedons/.

[5] U. Department of Justice. (2014, June) Massachusetts man pleads guilty to importing and selling counterfeit integrated circuits from China and Hongkong. Office of Public Affairs. [Online]. Available: http://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-importing-and-selling-counterfeit-intergrated-circuits-china

[6] SAE, "G-19A test laboratory standards development committee, Fraudulent Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," *http://standards.sae.org/as5553a/*, 2013.

[7] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 7–12.

[8] H. Dogan, D. Forte, and M. Tehranipoor, "Aging analysis for recycled fpga detection," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2014 IEEE International Symposium on*, Oct 2014, pp. 171–176.

[9] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*, Oct 2012, pp. 13–18.

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

[11] Y. Zheng, A. Basak, and S. Bhunia, "CACI: Dynamic current analysis towards robust recycled chip identification," in *Proceedings of the 51st Annual Design Automation Conference*, ser. DAC '14. New York, NY, USA: ACM, 2014, pp. 88:1–88:6. [Online]. Available: http://doi.acm.org/10.1145/2593069.2593102

[12] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 22, no. 5, pp. 1016–1029, 2014.

[13] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost on-chip structures for combating die and IC recycling," in *Proceedings of the 51st Annual Design Automation Conference*, ser. DAC '14. New York, NY, USA: ACM, 2014, pp. 87:1–87:6. [Online]. Available: http://doi.acm.org/10.1145/2593069.2593157

[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, no. 4, pp. 874–880, April 2008.

[15] W. L. Cheng and S. Ghosh, "Novel self-calibrating recycling sensor using schmitt-trigger and voltage boosting for fine-grained detection," in *IEEE International Symposium on Quality Electronic Design (ISQED)*, 2015.

[16] D. K. Schroder, "Negative bias temperature instability: What do we understand?" *Microelectronics Reliability*, vol. 47, no. 6, pp. 841–852, 2007.

[17] T. Oldham and F. McLean, "Total ionizing dose effects in mos oxides and devices," *Nuclear Science, IEEE Transactions on*, vol. 50, no. 3, pp. 483–499, June 2003.

[18] Wikipedia, "Error function — Wikipedia, the free encyclopedia," April 2015, [accessed 2-May-2015]. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Error_function&oldid=659301707