Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling

U. Guin, *Student Member, IEEE*, D. Forte, *Member, IEEE*, and M. Tehranipoor, *Senior Member, IEEE*

***Abstract*— The recycling of electronic components has become a major industrial and governmental concern, as it could potentially impact the security and reliability of a wide variety of electronic systems. It is extremely challenging to detect a recycled integrated circuit (IC) that is already used for a very short period of time because the process variations outpace the degradation caused by aging, especially in lower technology nodes. In this paper, we propose a suite of solutions, based on lightweight negative bias temperature instability (NBTI)-aware ring oscillators (ROs), for combating die and IC recycling (CDIR) when ICs are used for a very short duration. The proposed solutions are implemented in the 90-nm technology node. The simulation results demonstrate that our newly proposed NBTI-aware multiple pair RO-based CDIRs can detect ICs used only for a few hours.**

***Index Terms*— Combating die and IC recycling (CDIR), counterfeit integrated circuits (ICs), negative bias temperature instability (NBTI)-aware, recycling.**

I. Background

COUNTERFEIT integrated circuits (ICs) can potentially impact the security and reliability of a wide variety of electronic systems. These ICs pose a significant challenge to the global electronic component supply chain due to the lack of efficient, robust, and low-cost detection and avoidance technologies. Although there are different types of counterfeit ICs [2]–[4] (recycled, remarked, cloned, overproduced, and out-of-spec/defective) in the supply chain, it is reported that recycled and remarked ICs contribute to more than 80% of reported counterfeit incidents [5]. A recent report [6] from the IHS (Englewood, CO, USA) shows that the reports of counterfeit parts have quadrupled since 2009. These data have been compiled from two reporting entities: 1) ERAI (Naples, FL, USA) and 2) GIDEP (Norco, CA, USA). This report states that the majority of counterfeit incidents were reported by the U.S.-based military bodies and electronic firms from the aerospace industry. It is also mentioned in [7] that the five most commonly counterfeited components (e.g., analog ICs, microprocessor ICs, memory ICs, programmable logic ICs, and transistors) represent U.S. $169 billion in potential annual risk for the global electronics supply chain based on all reported counterfeit incidents in 2011.

Over the past few years, numerous reports have pointed to counterfeiting issues in the U.S. electronics component supply chain, and multiple investigations have been conducted to keep the entities accountable for participating in the counterfeit IC trade [8].

Recycled ICs are those that are reclaimed or recovered from a used system and are then misrepresented as new components produced by an original component manufacturer. Recycled ICs generally exhibit lower performance and have shorter lifetimes compared with the authentic ones, due to the effects of aging during their prior usage and mishandling during the recycling process. The recycling [9] process consists of aggressively removing components from printed circuits boards under very high temperatures. The components are then subjected to washing, sanding, repackaging, and remarking, all of which could damage the ICs and introduce many defects and anomalies. The recycling process may also introduce latent defects that pass initial testing but are prone to failure in later stages. The electrical defects could be resistive open/short, time-dependent dielectric breakdown (TDDB), out-of-spec leakage current, and out-of-spec dynamic current [8]. These defects could even make the components completely non-functional because of the components' exposure to extreme conditions.

A. Related Work

Guin *et al.* [2], [4], and Koushanfar *et al.* [10] presented a survey of various detection and avoidance measures for counterfeit ICs. The detection and avoidance approaches for the recycled ICs are broadly classified into four different categories: 1) physical and electrical tests; 2) track and trace; 3) data analysis; and 4) aging sensors. First, a wide variety of physical and electrical test methods [2], [4], [8], [11] are currently available for detecting recycled ICs. The goal of these methods is to identify the defects and anomalies present in those recycled ICs, which are not typically found in authentic ones. Since we assume that foundries and assemblies have a fairly consistent manufacturing process and comprehensively test their components, one should not expect to see many defective parts. A counterfeit part often contains one or more different anomalies and deviations from the normal/usual form and/or functionality of a genuine component. These anomalies may be physical (i.e., related to the leads, package, and so on) or electrical (e.g., degradation in its performance or a change

Manuscript received February 26, 2015; revised May 27, 2015 and July 4, 2015; accepted August 3, 2015. Date of publication August 21, 2015; date of current version March 18, 2016. This work was supported in part by the National Science Foundation under Grant CCF-1423282 and in part by the Missile Defense Agency.

U. Guin is with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: ujjwal.guin@uconn.edu).

D. Forte and M. Tehranipoor are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: dforte@ece.ufl.edu; tehranipoor@ece.ufl.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2015.2466551

in its specifications). Tehranipoor *et al.* [8] and Guin *et al.* [12] presented a comprehensive assessment of these test methods. The major limitation and challenges of implementing these test methods are the excessive test time, high cost, and low confidence of identifying recycled ICs.

Zhang *et al.* [13] and Huang *et al.* [14] proposed electrical test approaches for detecting recycled ICs. In [13], the path-delay fingerprinting was used to differentiate recycled digital ICs from genuine ones through changes in their path-delay distribution caused by prior usage. However, this technique requires data from genuine ICs, which can make its implementation impractical. Zheng *et al.* [15] presented a scan-based characterization technique to detect recycled ICs. The access to the scan chains may not be always possible when the chips are already in the market, thus making it difficult to implement because of burnt fuses commonly practiced in industry. Zheng *et al.* [16] utilized a dynamic current analysis to determine the aging difference between high-activity and low-activity portions of symmetric structures. However, this approach requires at least a year of aging for the reliable detection of recycled ICs. In [14], a statistical approach was presented to distinguish recycled ICs by measuring electrical parameters and using a one-class support vector machine (SVM). This technique can be applied to all types of ICs (analog and digital), but requires data from genuine samples for SVM training. Dogan *et al.* [17] proposed a two-phase detection approach that utilizes one-class SVM classifier to detect only recycled FPGAs.

Extensive research has been carried out by the solid-state circuits community to analyze aging degradation in ICs. Karl *et al.* [18] proposed two separate structures to monitor negative bias temperature instability (NBTI) and TDDB. A silicon odometer using on-chip ring oscillators (ROs) has been first proposed in [19] to monitor NBTI-induced degradation by measuring the beat frequency between the reference and stressed ROs. An improved version of the odometer was presented in [20] to separately monitor NBTI- and hot-carrier injection (HCI)-induced degradation. Keane *et al.* [21] presented a measurement system with an array of ROs that utilized the statistical aging measurements to monitor the degradation. Hofmann *et al.* [22] described a product-level aging monitoring system, which consists of a performance critical ARM1176 path. Saneyoshi *et al.* [23] presented a hybrid on-chip aging monitor consisting of an RO and a delay line. The objective of these sensors was to improve the reliability of ICs by accurately measuring the aging degradation, not to accelerate the degradation to its maximum value to identify recycled ICs. To address the shortcomings in these technologies, low-cost structures have been proposed to detect recycled ICs with greater ease [24], [25]. The technique introduced in [24] inserts a lightweight RO-based sensor (similar to one proposed in [19]) in the chip to capture the usage of the chip in the field. We call this sensor the O-CDIR, where "O" stands for original. In [25], two additional antifuse-based structures are proposed to improve the granularity of detection. These structures are composed of counters and an embedded antifuse memory block. The counters are used to record the usage time of ICs while their values are continuously stored in an antifuse memory block. All these sensors will be ineffective for detecting recycled ICs when they have been used for a very short duration with a high process variation (PV).

B. Contributions and Paper Organization

The major difference between detecting recycled ICs by physical and electrical test methods and on-chip sensors is that test methods rely on finding the defects, and anomalies present in the recycled ICs. These test methods are extremely expensive and slow. Moreover, recycling has evolved over the last few years, and the level of sophistication in the recycling process has significantly improved. We believe that this trend will continue and that recyclers will continue to adopt new processes and technologies as time passes, making it more difficult to detect recycled ICs [8]. It may even be possible that we will not find any of today's gross defects and anomalies [8], [12] in the recycled ICs of the future. In addition, recycling processes may introduce latent defects that pass acceptance tests but eventually become visible in the field at some point in their lifetime. Therefore, we cannot completely rely on the traditional test methods to confidently detect recycled ICs.

It is very difficult, if not impossible, to restore the degradation caused by aging in recycled ICs. A shift in circuit parameters due to aging will occur when a chip is used in the field for any period of time. The O-CDIR proposed in [24] works based on utilizing this aging phenomena. However, this design can detect recycled ICs that have only been used for longer duration in the field. This is clearly not sufficient when ICs have to be used in high-risk or critical applications, where recycled ICs could cause catastrophic system failures or pose a significant risk [8], [12]. Thus, this necessitates further improvements of the O-CDIR.

To address these challenges, this paper presents several different CDIR structures based on ROs. We present a significantly improved version of the O-CDIR that can detect recycled ICs used for a very short period of time. This is beneficial, as used ICs are not acceptable, no matter how long they have been used, especially in critical applications. For example, an untrusted entity in the supply chain may use chips for a short period of time for evaluation and then return them. The component could be exposed to abnormal conditions or possibly mishandled. These types of cases may be missed by physical inspections, electrical tests, and the previously proposed sensors. Our contributions include the following.

1) We propose a lightweight CDIR structure suitable for both large and small digital ICs. The structure itself is an RO-based sensor and is similar in spirit to the O-CDIR proposed in [24]. However, our new design is NBTI-aware and exploits aging much more efficiently than the O-CDIR. We call this design as N-CDIR, where "N" stands for NBTI-aware.
2) We propose a new N-CDIR with multiple reference and stressed RO-pairs. We introduce an averaging approach to reduce the impact of PVs during the estimation of a threshold, which will be used in the authentication process (see Fig. 3). We call this design as the multiple

pair NBTI-aware RO CDIR with averaging (AN-CDIR). This design provides a much better detection for ICs used for only a few hours in the field with the cost of small misprediction.

3) We propose another modified design of N-CDIR by adding multiple NBTI-aware reference and stressed RO-pairs like AN-CDIR. However, in this case, we propose a selection algorithm (see Fig. 8) to find the best reference and stressed RO-pair. We call this design the multiple pair NBTI-aware RO CDIR with selection (SN-CDIR). This CDIR with the best selected RO-pair provides even better detection (no misprediction) of recycled ICs, even if they have been used only for a few hours, unlike the AN-CDIR.

This paper is organized as follows. In Section II, we present our N-CDIR sensor design. Section III introduces the AN-CDIR consisting of multiple reference-stressed RO-pairs. Section IV presents our proposed the SN-CDIR consisting of multiple reference-stressed RO-pairs. The experimental results are presented in Section V. We conclude this paper in Section VI.

II. NBTI-Aware RO-Based CDIR Sensor

The detection of recycled ICs by prior approaches [13], [14] has exploited the aging phenomenon. These approaches require that the performance measurements of new chips be collected and analyzed, a challenge for legacy parts when golden ICs may not be available. Furthermore, large PVs in lower technology nodes can make it very difficult to separate recycled ICs from a batch when the PVs outpace aging degradation.

An anticounterfeit structure was proposed in [24] based on ROs that avoided the data collection altogether and applied a self-referencing concept to the measurement of use time with the help of aging degradation. The degradation of an IC's performance can be attributed to two distinct phenomena: 1) NBTI [26]–[28] and 2) HCI [29]–[31], which are prominent in pMOS and nMOS devices, respectively. NBTI occurs in the p-channel MOS devices stressed with negative gate voltages and elevated temperatures due to the generation of interface traps at the Si/SiO_2 interface. A removal of this stress can anneal some of the interface traps, but not completely. As a result, it manifests as an increase in both threshold voltage (V_{th}) and absolute OFF current (I_{OFF}) and a decrease in absolute drain current (I_{DSat}) and transconductance (g_m). HCI occurring in nMOS devices is caused by the trapped interface charge at Si/SiO_2 surface near the drain end during switching. It results in nonrecoverable V_{th} degradation.

The O-CDIR design in [24] embeds two ROs within the chip and compares them to detect the prior IC usage. The first RO is called the reference RO and is designed to age at a slow rate. The second RO is referred to as the stressed RO, and it is designed to age at a much faster rate than the reference RO. As the IC is used in the field, the stressed RO's rapid aging reduces its oscillation frequency while the reference RO's oscillation frequency remains largely static over the chip's lifetime. Thus, a large disparity between the ROs frequencies implies that the chip has been used. To overcome global and local PVs, the two ROs were placed physically very close together, so that the PV and environmental variation between them are negligible.

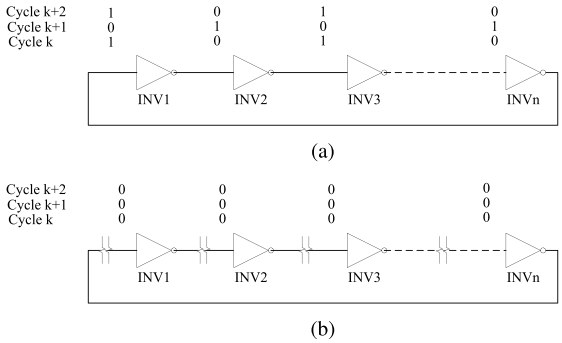


Fig. 1. NBTI stress on stressed ROs. (a) Stressed RO in RO-CDIR sensor [24] in stress mode. (b) Stressed RO in our proposed N-CDIR sensor in stress mode.

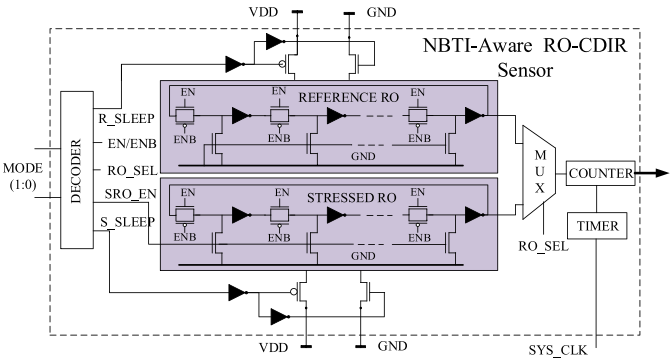


Fig. 2. Architecture of N-CDIR sensor.

Given the objectives for designing CDIRs, the best CDIR sensor (i.e., the one that detects recycled ICs with the highest accuracy) should possess minimal aging in the reference RO and maximum aging for the stressed RO. This cannot be achieved by the O-CDIR proposed in [24] because in the O-CDIR design, only half of the inverters in the stressed RO are under NBTI stress in one oscillation cycle, as shown in Fig. 1(a).

This problem is overcome in our proposed N-CDIR design by giving NBTI stress to all inverters. Fig. 1(b) shows the proposed solution where all the inverters are stressed during normal operation. This is achieved by breaking the connection of each inverter to its prior one and pulling their inputs down to ground. Here, all the inverters of the stressed RO are stressed during the entire time of the operation, so they cannot get a chance to recover from aging. When the chip is completely powered off, a partial recovery may occur; however, the permanent degradation is proved to be much larger than the recovery [32]. We call our proposed sensor N-CDIR.

A. Architecture of N-CDIR

Fig. 2 shows the design of the proposed N-CDIR sensor. The stressed RO is modified in such a way that all the inverters are stressed constantly. To achieve this, we have introduced a pass transistor in between every pair of inverters. The inputs of all the inverters are pulled down to ground

TABLE I
MODES OF OPERATION

MODE	Signals					Description
	R_SLEEP	*EN*	*RO_SEL*	*SRO_EN*	*S_SLEEP*	
00	0	X	X	X	0	Manufacturing and Burn-In Tests: Both ROs are in sleep mode.
01	0	0	X	1	1	Normal Operation: Reference RO in sleep mode and Stressed RO in stressed mode (inverter input GND)
10	1	1	0	0	1	Authentication Mode: Measure frequency of Reference RO
11	0	1	1	0	1	Authentication Mode: Measure frequency of Stressed RO

using an nMOS network. We have mimicked the stressed RO's structure in the reference RO in order to match all the internal parameters (node capacitance, resistance, and so on). This is to ensure that at time 0, when there is no aging, the difference between the two ROs is minimal and is mainly impacted by the small variations present between the two ROs. The *DECODER* generates all the internal signals for a specific mode. When EN = 0, both ROs oscillate while the sleep transistors are ON. The signals *EN* and *SRO_EN* can never be 1 simultaneously as this would create a short circuit in the design. Like O-CDIR, the *COUNTER* measures the cycle count of the two ROs during measurement, which is controlled by the *TIMER*.

Table I highlights the four distinct modes of operation. In manufacturing and burn-in tests (MODE = 00), our objective is to protect both ROs from aging. In this mode, both ROs enter in sleep mode by being cut off from the power and ground line. *R_SLEEP* and *S_SLEEP* will be assigned to 0 during this entire operation. In normal operation (MODE = 01), the reference RO will remain in the sleep mode while the stressed RO will be in the stressed mode. All the inverters in the stressed RO will be given a dc stress by pulling their inputs to ground. In authentication mode (MODE = 10 or 11), the reference RO will be activated to measure its frequency, which should correspond to the RO frequency of the new IC at time 0. Then, the stressed RO will be activated by setting *SRO_EN* to 0, and its degraded frequency will be measured.

To eliminate the confusion among different symbols, which will be introduced shortly, we summarize the notations in Table II.

B. Registration and Authentication Flow

Fig. 3 shows the registration and the authentication flow. The objective of the registration process is to determine a threshold (Δf_{th}), which will be used during the authentication process. The frequency differences of the reference and stressed ROs (Δf) of an IC are measured during authentication. If Δf of an IC is greater than Δf_{th}, then the IC will be treated as recycled; otherwise, it will be marked as new.

During registration phase, a number of new ICs are used to generate the distributions to determine the threshold (Δf_{th}) after the manufacturing test process at the foundry. It is recommended to select the samples from different wafers and lots to capture within-die and within-wafer PVs. The larger this sample space is, the more accurate the Δf_{th} will be. In the following, we describe the Δf_{th} determination process.

Due to the PVs, the difference between the reference and stressed RO frequencies (Δf) will not be zero even though we place these ROs very close to each other in the circuit layout. We observe a Gaussian distribution of Δf when we perform a Monte Carlo (MC) simulation with 1000 samples (see Section V). Fig. 4 shows a simplified representation of the two distributions (probability density functions) of Δf at

TABLE II
NOTATIONS AND THEIR DESCRIPTIONS

Notation[1–3]	Equation	Description
Δf	$\Delta f = f_R - f_S$	Δf is the frequency difference between reference RO (f_R) and stressed RO (f_S).
δf	$\delta f = \Delta f_t - \Delta f_0 = (f_{tR} - f_{tS}) - (f_{0R} - f_{0S}) = -(f_{0R} - f_{tR}) + (f_{0S} - f_{tS}) = -\delta f_R + \delta f_S$	δf is the aging degradation. Δf_0 and Δf_t are the frequency differences at time 0 and t. f_{0R} and f_{0S} are the frequencies of the reference and stressed ROs at time 0. f_{tR} and f_{tS} are the frequencies of the reference and stressed ROs at time t. δf_R and δf_S are the aging degradation of reference and stressed ROs.
∂f_S	$\partial f_S = \frac{f_{0S,V_{DD1}} - f_{0S,V_{DD2}}}{f_{0S,V_{DD2}}}$	∂f_S is the percentage frequency difference of the stressed RO with two different supply voltages ($V_{DD1} > V_{DD2}$) at time 0. $f_{0S,V_{DD1}}$ and $f_{0S,V_{DD2}}$ are the frequencies at supply voltages V_{DD1} and V_{DD2}, respectively.

1 $\hat{}$ denotes minimum mean square error (MMSE) estimator [33].
2 Boldface symbol denotes random variables.
3 $\vec{}$ denotes vectors.

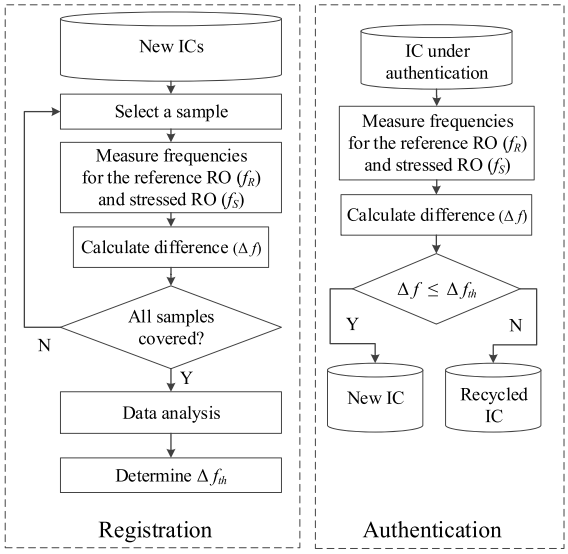


Fig. 3. Registration and authentication flow for N-CDIR.

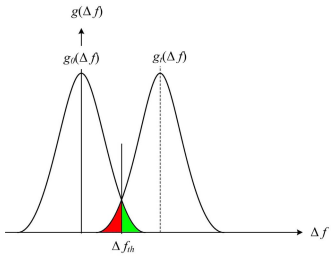


Fig. 4. Probability density function of frequency differences (Δf) between reference and stressed ROs.

times 0 and t ($g_0(\Delta f)$ and $g_t(\Delta f)$). The x-axis represents the frequency differences between the two ROs (Δf), and the y-axis represents the corresponding distribution function. The overlapping area represents the misprediction of identifying new or recycled ICs. The red area represents the probability of identifying recycled ICs as new, whereas the green area denotes the probability of identifying new ICs as recycled. These areas (θ_1 and θ_2) are represented by

$$\theta_1 = \int_{-\infty}^{\Delta f_{\text{th}}} g_t(\Delta f)\, d\Delta f \quad \text{and} \quad \theta_2 = \int_{\Delta f_{\text{th}}}^{\infty} g_0(\Delta f)\, d\Delta f \tag{1}$$

where $g_0(\Delta f)$ and $g_t(\Delta f)$ correspond to the distribution of frequency differences for new and ICs with t amount of usage, respectively. The decision threshold should be the point (Δf_{th}) where both distributions intersect each other. This represents the frequency difference that minimizes the total probability of error ($\theta_1 + \theta_2$).

C. Motivation for a CDIR With Multiple RO-Pairs

The N-CDIR proposed in Section II-A can efficiently detect recycled ICs with little misprediction when the chips are aged for a short period of time. However, when the workload decreases (i.e., the chip is used less frequently in case of mobile and automotive applications), we require the chips to be used much longer for detection, which eventually results in a higher rate of misprediction. In addition, there may be a recycling activity from the overstock of electronic systems where the recyclers extract components from never used systems. The detection of these components can be performed with a CDIR that can detect a small amount of aging (for example, the amount of aging caused during the test of a system). When the application risk is critical [2], [8], [12], we do not have the luxury for any test escapes as the system failure due to using recycled chips could cause a significant financial loss, as well as risks to safety and security. Thus, this necessitates further improvements of the N-CDIR.

Fig. 5 shows the process of reducing the rate of misprediction for identifying a recycled IC as new and vice versa. Misprediction arises from the overlap of the reference and stressed ROs frequency difference distribution at time 0 ($g_0(\Delta f)$) and the distribution at time t ($g_t(\Delta f)$), which is the aged replica of $g_0(\Delta f)$. This overlapping area can be reduced by the following.

1) Increasing the separation of these two distributions. This separation (aging degradation, δf) can be increased by shifting the distribution $g_0(\Delta f)$ to the left ($g'_0(\Delta f)$) or shifting the distribution $g_t(\Delta f)$ to the right $g'_t(\Delta f)$, or by doing both simultaneously [see Fig. 5(a)]. Our proposed N-CDIR provides better detection of recycled ICs by shifting the distribution $g_t(\Delta f)$ to the right as compared with O-CDIR.
2) Reducing the spread of these two distributions. This spread results from their variances (σ_0^2 and σ_t^2). Fig. 5(b) shows no overlap between $g'_0(\Delta f)$ and $g'_t(\Delta f)$ ($\sigma'_0 < \sigma_0$ and $\sigma'_t < \sigma_t$). Our proposed AN-CDIR utilizes this technique to reduce misprediction rate.

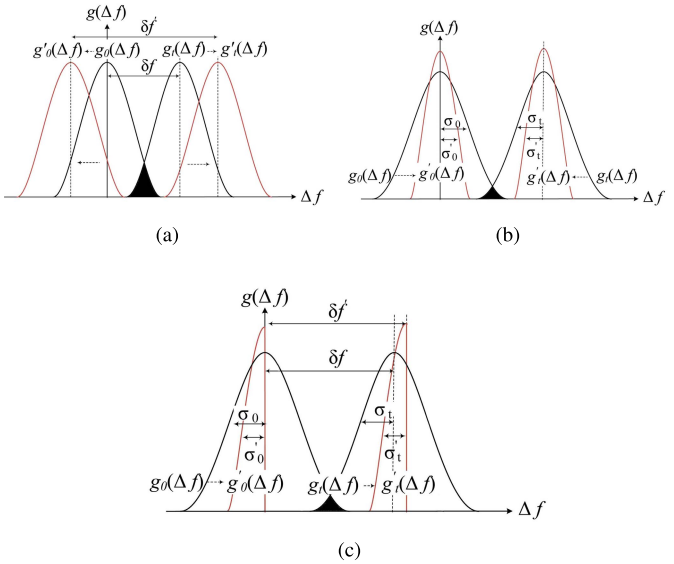


Fig. 5. Reduction of misprediction (overlapped area). (a) Shifting two distributions away from each other. (b) Reduction of spread of two distributions. (c) Reduction of spread and shifting of mean of two distributions.

3) Simultaneously reducing the spread and increasing the separation of two distributions. Fig. 5(c) shows such case. The overall spread can be reduced by discarding the right-hand side, and reducing the left-hand side spread of $g_0(\Delta f)$. The separation can be increased by shifting $g_t(\Delta f)$ to the right. Our proposed SN-CDIR utilizes this technique and provides the best detection of recycled ICs.

By introducing multiple RO-pairs in a CDIR, it becomes possible to achieve 1, 2, and/or 3, thereby reducing misprediction when the ICs are used only for a short period of time. In the following, we describe two different architectures utilizing multiple RO-pairs to minimize the misprediction. It is also analytically proved that both approaches are better than the single N-CDIR. In Section V, the simulations for all sensors support our conclusions.

III. CDIR Sensor With Multiple RO-Pairs and Averaging Approach

The AN-CDIR works based on the averaging of reference and stressed RO frequencies. In the following, we provide a proof that the spread (σ) of $g_0(\Delta f)$ [see Fig. 5(b)] is reduced significantly after averaging. In this method, one must measure all the frequencies of the stressed and reference ROs consecutively and then take the average of the reference RO and stressed RO frequencies.

A. Averaging to Reduce Spread

Let us assume that there are n ROs present in the reference and stressed block of an AN-CDIR. We treat the frequencies of the reference ROs and stressed ROs as random variables, denoted by $\mathbf{X_1}, \mathbf{X_2}, \ldots, \mathbf{X_n}$, and $\mathbf{Y_1}, \mathbf{Y_2}, \ldots, \mathbf{Y_n}$, respectively.

As the distribution of $g_0(\Delta f)$ is formed by the frequency differences of the reference and stressed RO frequencies, we construct the following random variables:

$$\mathbf{Z_i} = \mathbf{X_i} - \mathbf{Y_i}.$$

Here, $\mathbf{Z_i}$s are Gaussian as all $\mathbf{X_i}$s and $\mathbf{Y_i}$s are Gaussian. We also assume that these newly formed variables have the same mean (μ) and variance (σ^2), as all the ROs experience the same PVs.

The objective is to find the mean and variance of a newly formed random variable $\mathbf{W_n}$, where

$$\mathbf{W}_n = \frac{1}{n}\sum_{i=1}^{n}\mathbf{X_i} - \frac{1}{n}\sum_{i=1}^{n}\mathbf{Y_i} \tag{2}$$

$$= \frac{1}{n}\sum_{i=1}^{n}(\mathbf{X_i} - \mathbf{Y_i}) = \frac{1}{n}\sum_{i=1}^{n}\mathbf{Z_i}. \tag{3}$$

As all $\mathbf{Z_i}$s are Gaussian, the resultant random variable $\mathbf{W_n}$ will also be Gaussian, and its statistics will be completely determined by the mean and variance, which can be formulated as

$$E[\mathbf{W}_n] = E\left[\frac{1}{n}\sum_{i=1}^{n}\mathbf{Z_i}\right] = \frac{1}{n}\left(E\left[\sum_{i=1}^{n}\mathbf{Z_i}\right]\right)$$
$$= \frac{n\times\mu}{n} = \mu \tag{4}$$

$$\text{var}(\mathbf{W}_n) = \text{var}\left(\frac{1}{n}\sum_{i=1}^{n}\mathbf{Z_i}\right) = \text{var}\left(\sum_{i=1}^{n}\frac{\mathbf{Z_i}}{n}\right)$$
$$= \frac{1}{n^2}\sum_{i=1}^{n}\text{var}(\mathbf{Z_i}) + \frac{1}{n^2}\sum_{i\neq j}\text{cov}(\mathbf{Z_i},\mathbf{Z_j}). \tag{5}$$

In (4) and (5), $E[A]$ denotes the expected value of random variable A, which is equivalent to the mean for a Gaussian random variable; var(A) denotes the variance of random variable A; and cov(A, B) denotes the covariance between random variables A and B. Let us assume that the frequencies of all the ROs are independent. This results in $\mathbf{Z_1}, \mathbf{Z_2}, \ldots, \mathbf{Z_n}$ being independent. Then, all of the covariances in (5) are zero

$$\text{var}(\mathbf{W}_n) = \frac{1}{n^2}\sum_{i=1}^{n}\text{var}(\mathbf{Z_i}) = \frac{n\times\sigma^2}{n^2} = \frac{\sigma^2}{n}. \tag{6}$$

Thus, the mean (μ) and the standard deviation (σ) of $\mathbf{W_n}$ become

$$\mu_{W_n} = \mu \tag{7}$$

$$\sigma_{W_n} = \frac{\sigma}{\sqrt{n}}. \tag{8}$$

In (4) and (7), the mean of the average difference W_n is unchanged when compared with each Z_i. However, the variance (spread) of W_n is a factor on $\sqrt{n}$ smaller (8). A similar treatment can be performed for the distribution $g_t(.)$ at time t to estimate the resultant mean and variance. This implies that the overlap between the two distributions can be made negligibly small by adding additional RO-pairs, as shown in Fig. 5(b).

B. Architecture of AN-CDIR

Fig. 6 shows our proposed architecture for the AN-CDIR. It consists of a reference RO block and a stressed RO block. Each block again consists of equal numbers of NBTI-aware reference and stressed ROs. The number of ROs in each block depends on the detection of recycled ICs used for a minimum amount of time (we label this time as resolution). For example, our results show that by placing four ROs in each block, we can detect recycled ICs that have been used for only one day with 100% workload (see Table VII). Larger numbers of ROs are necessary to achieve a superfine recycled IC detection resolution. The requisite number of ROs can be determined based on the available area on the chip.

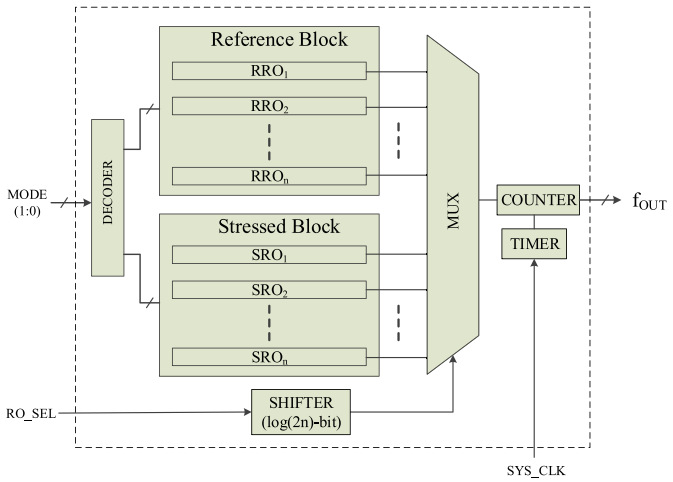


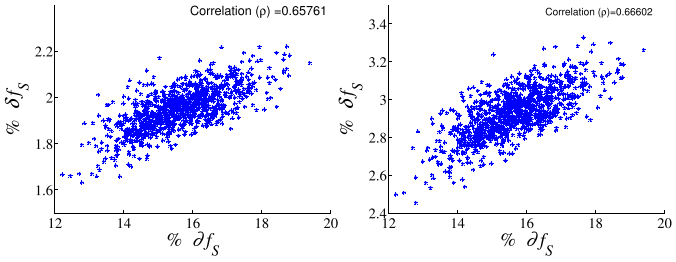
Fig. 6. Architecture of our proposed AN-CDIR.

All the ROs in the reference block and stressed blocks are fed to a multiplexer (*MUX*). The selection input of *MUX* is provided by a shift register of $\log_2(2n)$ bit to minimize the I/O pin count for this CDIR. This register is loaded through a serial in *RO_SEL* pin. The rest of the design is similar to the N-CDIR described in Fig. 2. The *DECODER* generates all the internal signals (see Table I) for the reference and stressed RO blocks. It is not necessary to generate the control signals for each RO in the reference and stressed RO blocks. All the ROs in each block utilize the same internal signals generated by the *DECODER*. The *COUNTER* and *TIMER* operate as described in N-CDIR.

The registration and authentication flow are very similar to the one described in Fig. 3. The only difference is the measurement of Δf, where it is the difference of the average of reference and stressed RO frequencies (2).

IV. CDIR Sensor With Multiple RO-Pairs and Selection Approach

SN-CDIR is based on the selection of the best RO-pair that minimizes misprediction. Increasing the difference between the mean of two distributions (δf) for time t and 0 and reducing their spread (σ_0 and σ_t) are the key parameters for improving the detection of the recycled ICs. The selection of the best RO-pair is the primary objective for minimizing the level of misprediction. As the reference RO remains quiet during normal operations, our objective is to find a stressed RO that degrades the most among all of the available stressed ROs. At the same time, we need to find a reference RO, which is slower than the stressed RO at time 0. In the following, we present a novel RO selection flow to select the best RO-pair for minimizing the misprediction. Let us start with a mathematical proof to find a maximum δf, the aging degradation.



(a) (b)

Fig. 7. Scatter plot of percentage degradation ($\%\delta f_S$) versus percentage frequency differences ($\%\partial f_S$) of stressed ROs. (a) ICs aged for 3 days. (b) ICs aged for 15 days.

A. Correlation Between Aging Degradation (δf_S) and ∂f_S

To find the maximum aging degradation (δf) of a CDIR, we have conducted an experiment to observe how δf varies with the percentage frequency differences (∂f_S) at different supply voltages. As the reference ROs remain quiet during normal operations, we have selected stressed ROs for this experiment. We have performed a MC simulation with 1000 stressed RO samples implemented in the predictive technology model (PTM) 90-nm technology node [34] with two different supply voltages (1.2 and 1.4 V). Fig. 7 shows the scatter plot of δf_S versus ∂f_S at time t, where $\partial f_S = (f_{0S,1.4\text{ V}} - f_{0S,1.2\text{ V}})/f_{0S,1.2\text{ V}}$. Here, $f_{0S,1.4\text{ V}}$ and $f_{0S,1.2\text{ V}}$ are the frequencies of the stressed RO at 1.4 and 1.2 V supply voltage. We have observed a positive correlation (ρ) for aging degradation and normalized frequency differences [see Fig. 7(a) and (b)]. A theoretical proof has been presented in Appendix A.

B. δf Versus ∂f_S

Let us assume that a stressed RO is used for about time t in the field. Due to aging, it slows down and the frequency f_{tS} at time t becomes lower than the frequency f_{0S} at time 0. Thus, its aging degradation, δf_s, becomes

$$\delta f_S = f_{0S} - f_{tS}.$$

The RO is operated at two different supply voltages at time 0 to calculate the percentage frequency differences

$$\delta f_S = \frac{f_{0S,V_{\text{DD1}}} - f_{0S,V_{\text{DD2}}}}{f_{0S,V_{\text{DD2}}}}$$

where $V_{\text{DD1}} > V_{\text{DD2}}$.

There exists a positive correlation ρ [see Fig. 7(a)] between δf_S and ∂f_S. Now, our objective is to select a RO-pair that will maximize the aging degradation (δf) of the SN-CDIR based on the stressed RO percentage frequency differences (∂f_S) at different supply voltages

$$\delta f \xleftarrow{\rho} \partial f_S.$$

Here, the aging degradation for a CDIR is expressed as

$$\delta f = \Delta f_t - \Delta f_0$$

where

$$\Delta f_i = f_{iR} - f_{iS}.$$

Note that δf and ∂f_S are random variables due to PVs.

TABLE III
PROCESS VARIATIONS

Process Variations	Inter-die			Intra-die		
	Vth (%)	L (%)	Tox (%)	Vth (%)	L (%)	Tox (%)
PV0	5	5	2	5	5	1
PV1	8	8	3	7	7	2
PV2	20	20	6	10	10	4

Since we have shown above that a positive correlation exists between δf_S and ∂f_S, it is possible to find an optimal estimate $\hat{\delta f}$ for δf. In particular, the minimum mean-square error (MMSE) estimator [33] for the stressed RO degradation can be expressed as

$$\hat{\delta f_S} = \rho \frac{\sigma_{\delta f_S}}{\sigma_{\partial f_S}}(\partial f_S - \mu_{\partial f_S}) + \mu_{\delta f_S}$$

where ρ represents the correlation between δf_S and ∂f_S; $\sigma_{\delta f_S}$ and $\sigma_{\partial f_S}$ represent the standard deviations for δf_S and ∂f_S, respectively; and $\mu_{\delta f_S}$ and $\mu_{\partial f_S}$ denote the means for δf_S and ∂f_S, respectively.

The MMSE estimator for the CDIR degradation (δf) can be written in terms of ∂f_S as follows:

$$\begin{aligned}\hat{\delta f} &= \hat{\Delta f_t} - \hat{\Delta f_0} = (\hat{f}_{tR} - \hat{f}_{tS}) - (\hat{f}_{0R} - \hat{f}_{0S}) \\ &= -(\hat{f}_{0R} - \hat{f}_{tR}) + (\hat{f}_{0S} - \hat{f}_{tS}) \\ &= \hat{f}_{0S} - \hat{f}_{tS}.\end{aligned}$$

Assuming $\hat{f}_{0R} = \hat{f}_{tR}$ as reference RO ages very little

$$= \hat{\delta f_s} = \rho \frac{\sigma_{\delta f_S}}{\sigma_{\partial f_S}}(\partial f_S - \mu_{\partial f_S}) + \mu_{\delta f_S}.$$

As ρ is positive, maximizing ∂f_S will maximize δf, which is the separation between the two distributions at $t = 0$ and $t = t$. This implies that in the SN-CDIR, where we have several RO-pairs to choose from, it is optimal to choose the one with the largest ∂f_S at $t = 0$. This will maximize the distance between the two distributions of frequency difference, as shown in Fig. 5(a), resulting in a lower probability of misprediction than the single N-CDIR.

C. Proposed Registration and Authentication Flow

Fig. 8 shows the proposed registration flow of the SN-CDIR. The registration flow consists of the selection of the best reference and stressed RO-pair. During registration, a large number of new ICs are used to generate the distributions to determine the threshold after the manufacturing test process at the foundry. It is better to select the samples from different wafers and lots to capture the actual PVs. The larger this sample space is, the more accurate the PVs will be. In our simulation, we selected PV2 (mentioned in Table III) as the extreme case, and we believe that any PVs will be well below PV2. The environmental conditions during measurement should be as uniform as possible to reduce measurement errors. However, we believe that the environmental variations should not impact the measurement as the reference and stressed ROs are placed close to each other, so that environmental conditions will impact all of the ROs uniformly.

The objective of the registration phase is to find the best reference and stressed RO-pair. During this phase, all the ROs in the CDIR are selected, and their frequencies are captured.

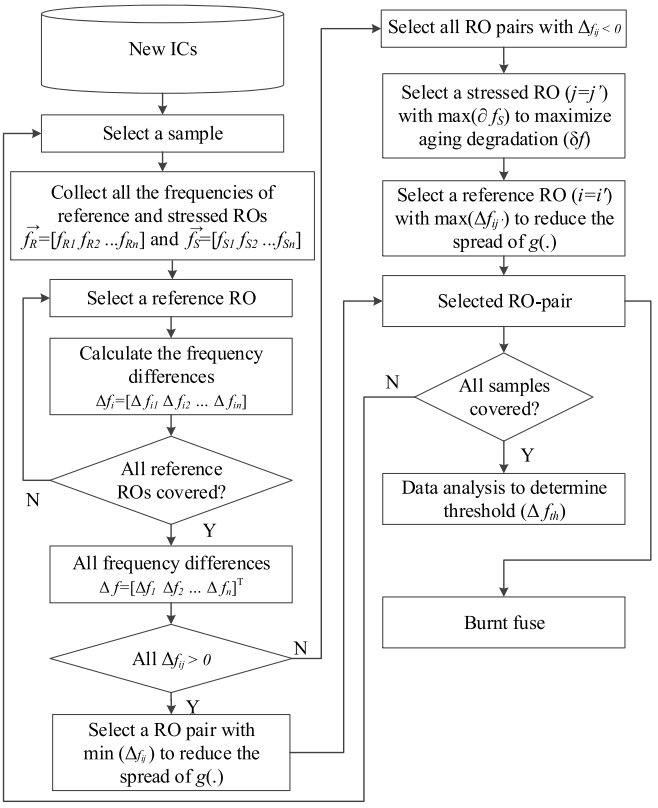


Fig. 8. Proposed registration flow for SN-CDIR.

Let us assume that there are n reference and n stressed ROs in a CDIR. Two vectors $\vec{f_R} = [f_{R1}\ f_{R2} \ldots f_{Rn}]$ and $\vec{f_S} = [f_{S1}\ f_{S2} \ldots f_{Sn}]$ are formed to store all the reference and stressed RO frequencies. Now, all the frequency differences are stored in a matrix $\Delta f = [\Delta f_{ij}]_{n\times n}$, where $\Delta f_{ij} = \vec{f_R}(i) - \vec{f_S}(j)$, $\forall(i, j)$. If all the Δf_{ij} are positive, a reference-stressed RO pair is selected with $\min(\Delta f_{ij})$; otherwise, Δf is updated with only negative Δf_{ij} values. The resultant distribution $g_0'(.)$ by applying these treatments can be visualized in Fig. 5(c) where the spread has been reduced significantly.

It is now necessary to shift the distribution at time t, $g_t(.)$ to the right in order to increase δf even further [see Fig. 5(a)]. A stressed RO is selected, which has maximum $\overrightarrow{\partial f}_S(j) = (\overrightarrow{f_{0S,V_{DD1}}}(j) - \overrightarrow{f_{0S,V_{DD2}}}(j))/\overrightarrow{f_{0S,V_{DD1}}}(j)$. The corresponding reference RO is selected with $\max(\Delta f_{ij})$ to reduce the spread of both $g_0(.)$ and $g_t(.)$ distributions. Once the best RO pair is selected, the frequency difference (Δf_{ij}) is stored to form the distribution ($g_0(.)$). A fuse block is used to select these two ROs permanently. All the ICs go through a similar treatment to find out the best RO pair. Finally, the threshold is calculated, which will be used later for the detection of recycled ICs.

Note that in the worst case, there may not be a correlation present between δf_S and ∂f_S, as some researchers reported a very weak or zero correlation between the aging degradation with threshold voltage [35]. However, this will not impact the result significantly as the removal of the right-hand side and the reduction of the spread of the distribution at $t = 0$ ($g_0(.)$).

The authentication flow is exactly the same as the one described in Fig. 3. The frequency differences (Δf) of the reference and stressed ROs of an IC under authentication are measured and compared with the threshold (Δf_{th}) to determine whether the IC is recycled or not. The CDIR will experience more degradation once it has been used longer in the field, and Δf will be much larger than Δf_{th} making it easier to identify.

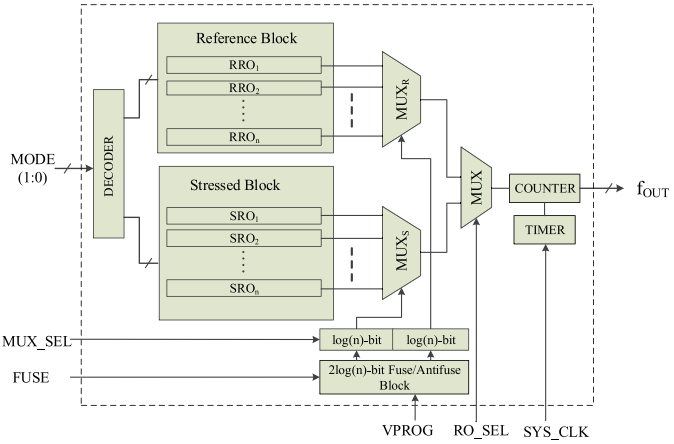


Fig. 9. Architecture of our proposed AN-CDIR.

D. Proposed Architecture of SN-CDIR

Fig. 9 shows our proposed architecture for the SN-CDIR. It also consists of reference RO and stressed RO blocks such as AN-CDIR. Each block consists of an equal number of NBTI-aware ROs. The number of ROs in each block depends on the recycled IC detection resolution. For example, it is required to place four ROs in each block when we want to detect recycled ICs aged for only 12 h with a 100% workload (see Table VII). Larger numbers of ROs are necessary to achieve a superfine recycled IC detection resolution. Like AN-CDIR, the required number of ROs can be determined after observing the available area on a chip.

All the ROs in the reference and stressed blocks are fed to two different multiplexers (MUX_R and MUX_S), respectively. The selection input of MUX_R and MUX_S is provided by the LSBs and MSBs of a shift register. If there are n ROs in each block, the selection input of each multiplexer will be $\log_2(n)$. Thus, the size of the shift register will be $2\log_2(n)$. This shift register can accept data from the *MUX_SEL* pin or a $2\log_2(n)$ bit fuse/antifuse block. During the registration phase, all the ROs are selected to measure their frequencies. In this phase, *MUX_SEL* selects each RO. At the end of the registration phase, the best RO-pair is determined. The selection bits corresponding to these ROs are programmed in a $2\log_2(n)$ fuse/antifuse block. *VPROG* provides the programming voltage to the fuse/antifuse block.

The rest of the design is similar to the N-CDIR described in Fig. 2. The *DECODER* generates all the internal signals (see Table I) for the reference and stressed RO blocks. It is not necessary to generate the control signals for each RO in the reference and stressed RO blocks. All the ROs in each block utilize the same internal signals generated by the *DECODER*. The *MUX*, *COUNTER*, and *TIMER* operate as described before.

TABLE IV
MISPREDICTION RATE

	θ_1 (%)						θ_2 (%)					
	3 Days			15 Days			3 Days			15 Days		
	PV0	PV1	PV2	PV0	PV1	PV2	PV0	PV1	PV2	PV0	PV1	PV2
21-stage RO	0.6	3.53	10.19	0	0.31	2.84	0.45	3.16	10.54	0	0.25	2.87
51-stage RO	0	0.32	2.79	0	0	0.21	0	0.3	2.85	0	0	0.18

V. SIMULATION RESULTS AND ANALYSIS

A. Simulation of N-CDIR

In order to verify the effectiveness of the NBTI-Aware RO-CDIR, we implemented and simulated it using the 90-nm technology node [34]. HSPICE MOSRA from Synopsys is used to simulate and measure the impact of aging on this CDIR sensor. The nominal supply voltage is 1.2 V. In this simulation, we selected 21-stage and 51-stage ROs to compare the results. To model the variation, the MC simulation was performed with 1000 samples of the N-CDIR in HSPICE. Since we were mostly concerned about detecting ICs used in the field for a very short period of time, here, the total aging time was set to 15 days in steps of 3 days. Larger usage time would be easily detected using this sensor.

Three different PVs were considered to investigate the impact of variation on the detection of recycled ICs. Table III shows the different PVs used in our simulation. Moving from PV0 to PV2, interdie and intradie variations both become larger. That is because as feature size decreases and die size increases, PVs are increased significantly due to the complex semiconductor manufacturing process. However, we acknowledge that the impact of PVs on ROs will be minimal as they are placed physically near to each other. PV0 represents the expected PVs between ROs, while the other two are the worst case scenarios.

Fig. 10 shows the simulation results of our proposed N-CDIR sensor. The x-axis represents the frequency difference (Δf) between the reference RO and the stressed RO. The y-axis represents the frequency of occurrence (i.e., # of MC samples). The legend in the figures denotes the aging time (for example, T = 3-D denotes the RO-CDIR is aged for 3 days). The green (0-D aging) distribution for Δf is centered at 0 Hz while the pink and blue (3-D and 15-D aging) distributions shift to the right. This is because the stressed RO has aged and become slower resulting in larger Δf.

We can clearly identify recycled ICs when the two distributions ($T = 0$ and $T =$ 3-D/15-D) do not overlap with each other. The percentage of misprediction (new ICs detected as counterfeit and vice versa) can be estimated as the area of overlap between these two distributions. We apply Gaussian fit to find the mean and variance of the distributions and then calculate the overlapped area. We can certainly identify recycled ICs with aging more than 15 days in almost all cases. Based on the figure, we expect a higher misprediction rate: 1) as the PVs increase and 2) when the 21-stage RO is used rather than the 51-stage RO (see Appendix B). As PVs increase, the variance in Δf grows resulting in larger overlap between 0-D and 3-D/15-D distributions. Similarly, since the 21-stage RO distributions have a larger spread than the 51-stage RO, we should also expect higher misprediction rate. The best case scenario occurs for the 51-stage RO

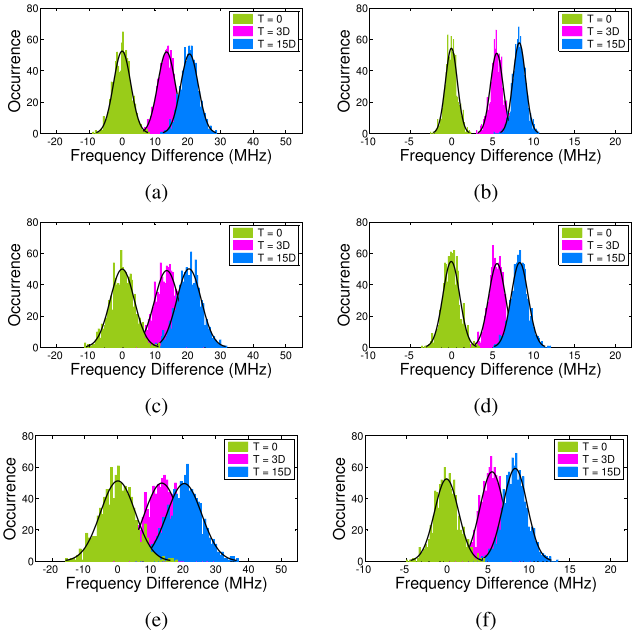


Fig. 10. Distribution of frequency differences between reference RO and stressed RO with different PVs, PV0, PV1, and PV2. (a) PV0: 21 stage RO. (b) PV0: 51 stage RO. (c) PV1: 21 stage RO. (d) PV1: 51 stage RO. (e) PV2: 21 stage RO. (f) PV2: 51 stage RO.

with PV0 where we can detect recycled ICs in 3 days with a negligible penalty of misprediction. This represents a substantial improvement over the prior work [24], which required at least one month of aging to identify recycled ICs. As we described in Section II, the design in [24] only ages 50% of inverters in each oscillation cycle while the other half of inverters recover. This results in a slower aging of the stressed RO. In contrast, our proposed design ages all the inverters in the stressed RO constantly (without recovering) during normal operation. Thus, we expect higher aging for the stressed RO that allows our N-CDIR to detect recycled ICs used much less than one month (as little as 3 days).

Table IV shows the misprediction rate, i.e., recycled ICs identified as new (θ_1) and new ICs identified as recycled (θ_2) for 21-stage and 51-stage N-CDIR sensors, with PVs mentioned in Table III. The rate is higher in PV2 as stressed and reference ROs frequencies differ significantly between two samples due to higher PVs. This results in a higher overlapped area between two distributions. However, we obtain significantly lower θ for 51-stage RO. θ_1 is 2.79% and 0.21% when the N-CDIR has aged 3 days and 15, respectively. For PV1, it is 0.32% and 0% for the same use times. We can predict all the samples as recycled or new when they are aged only 3 days. As we described earlier, with these two ROs placed very close to each other, the variation will be well below PV1. Under different cases, we also observe a similar misprediction rate (θ_2) of identifying new ICs as recycled. In both these cases, the 51-stage RO outperforms the 21-stage RO.

TABLE V
WORKLOAD ANALYSIS

	Workload				
	100%	**75 %**	**50 %**	**10 %**	**1 %**
51-Stage RO-CDIR	3 Days	4 Days	6 Days	30 Days	300 Days

In the simulation, we have only considered PVs. We did not include any results for temperature and power supply variation. As the two ROs are placed very close in the circuit layout, the temperature variation between the two is practically negligible ($\triangle T = 0$) as the temperature variation is a global phenomenon. At higher temperatures, we would also expect more rapid aging in the stressed RO, which should only improve our results. A similar argument can be made for power supply variation.

It is also important to analyze different workloads that impact the detection of recycled ICs. We define workload as the percentage of time per day the IC is in use. The workload/usage depends on the type of application. For example, the ICs used in: 1) medical applications may remain on during the entire day (workload may be 100%) or 2) televisions or laptops may be ON for a fraction of day (workload may be well below 100%). We have considered 100% workload for all the simulations unless specified otherwise. Table V shows the minimum usage time of ICs under various workloads required for proper identification. Note that we have shown the results only for 51-stage N-CDIR as it provides minimum misprediction. The results show that the length of time required to detect the recycled IC increases as the workload decreases. For example, a workload of 10% and 1% requires the IC be used for 30 days and 300 days, respectively. With reduced workload, we can only identify ICs as recycled if the system is used over a longer period of time because when the system is OFF (i.e., not in use), time passes but the stressed RO does not age at all. Note that the impact of low workload environment would be similar for all prior approaches based on aging [13], [14], [24]. Hence, the proposed N-CDIR will outperform all prior works at any workload.

B. Simulation of AN-CDIR and SN-CDIR

In this section, we present the simulation results for the AN-CDIR and SN-CDIR structures. We present the simulation results for the PVs PV2 to evaluate the performance of the CDIRs in the most extreme cases. We believe that these CDIRs will perform better than standard manufacturing processes, as these ROs are placed very close to each other. As in the case of the N-CDIR, we have implemented and simulated these CDIRs using the 90-nm technology node [34]. HSPICE MOSRA from Synopsys is used to simulate and measure the impact of aging on this CDIR sensor. The nominal supply voltage is 1.2 V. In this simulation, we selected the 51-stage ROs as they outperform the 21-stage RO (see Table IV). To model the variation, the MC simulation was performed with 1000 samples of the CDIRs. First, we will present the results when the CDIRs are aged for only 3 days with a 100% workload. Larger usage time than 3 days would be easily detected using these sensors.

Fig. 11 shows the histogram plot of the average frequency difference between the reference and stressed RO-pairs for different numbers of RO-pairs in an AN-CDIR. We have observed that the spread of the distributions at time 0 and 3 days reduced significantly while increasing the RO-pairs in the CDIR. However, the separation between the two distributions remains the same. The threshold (Δf_{th}) for determining whether the ICs under tests are new or recycled is the same for all the different RO-pairs in a CDIR and is $(\mu_{t=0} + \mu_{t=3-D})/2 = 2.77$ MHz. Fig. 11 also reveals the same fact that the detection of recycled ICs aged fewer than 3 days requires more than 2 RO pairs in a CDIR. The higher the number of RO pairs, the better the likelihood that we will be able to detect recycled ICs that have been used less in the field.

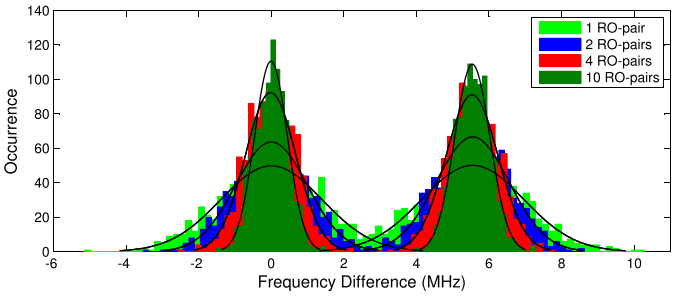


Fig. 11. Frequency difference distribution at PV2 of AN-CDIR with different numbers of RO-pairs.

TABLE VI
MEAN AND VARIANCE f DISTRIBUTION OF AN-CDIR

# RO Pairs	$g_0(.)$				$g_{t=3D}(.)$			
	μ		σ		μ		σ	
	Exp.	Act.	Exp.	Act.	Exp.	Act.	Exp.	Act.
2	0.000	0.004	0.986	0.987	5.553	5.551	0.994	1.007
4	0.000	-0.016	0.697	0.695	5.553	5.533	0.703	0.722
6	0.000	0.003	0.569	0.580	5.553	5.551	0.574	0.608
10	0.000	-0.005	0.441	0.452	5.553	5.542	0.444	0.488

It is relevant to analyze how the mean (μ) and variance (σ^2) of the frequency difference distribution of the AN-CDIR changes with an increased number of RO pairs to estimate the misprediction accuracy and the number of RO-pairs required to achieve nearly a zero misprediction rate. Using the $normfit$ MATLAB function [36], we measure the actual mean and variance (denoted as $Act.$ in Columns 3, 5, 7, and 9 of Table VI) of different distributions with different numbers of RO pairs in a CDIR, and compare them (denoted as $Exp.$ in Columns 2, 4, 6, and 8 of Table VI) with 7 and 8 to measure the accuracy of our averaging algorithm. Table VI shows the values for μ and σ. We have observed an error in the expected value ($Exp.$) compared with the actual value ($Act.$), which is $<0.5\%$ for μ and $<9\%$ for σ.

Now, we will analyze the performance of the SN-CDIR. Fig. 12 shows the histogram plot of the frequency difference between the selected best reference and stressed RO-pairs. We have observed that there is no overlap between the two distributions at time 0 and 3 days for all the figures, Fig. 12(a)–(d). However, the separation between the two distributions increases as the number of RO-pairs increases. The threshold (Δf_{th}) (see Fig. 8) for determining whether the ICs under tests are new or recycled is 2 MHz for all the CDIRs with different RO pairs. Fig. 12 reveals that, to detect a recycled IC aged for only 3 days with zero-misprediction,

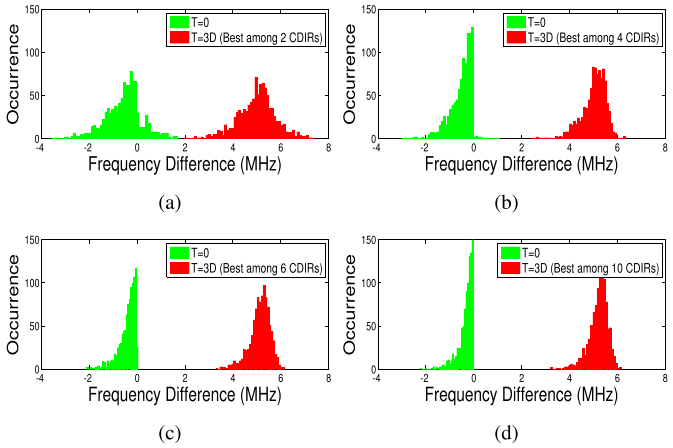


Fig. 12. Frequency difference distribution at PV2 of SN-CDIR with different numbers of RO-pairs. (a) Best of 2 RO-pairs. (b) Best of 4 RO-pairs. (c) Best of 6 RO-pairs. (d) Best of 10 RO-pairs.

TABLE VII
MISPREDICTION ANALYSIS OF AN-CDIR AND SN-CDIR

Aging duration	RO-pairs (n)	AN-CDIR		SN-CDIR		
		$\theta_1(\%)$	$\theta_2(\%)$	Δf_{th}	$\theta_1(\%)$	$\theta_2(\%)$
2 Hrs	2	13.07	12.85	0.4	7.3	7.5
	4	5.46	5.51	0.1	0.8	1.0
	6	2.73	2.77	0	0.0	0.1
	10	0.62	0.81	0	0	0
4 Hrs	2	9.0	8.9	0.7	4.5	4.8
	4	2.8	2.79	0.2	0.5	0.7
	6	1.1	1.15	0	0	0
	10	0.13	0.2	0	0	0
8 Hrs	2	5.58	5.38	1.0	3.1	2.9
	4	1.24	1.12	0.5	0.2	0.2
	6	0.32	0.34	0	0	0
	10	0	0	0	0	0
12 Hrs	2	3.91	3.75	1.0	1.7	2.9
	4	0.64	0.58	0.5	0.1	0.2
	6	0.12	0.14	0	0	0
	≥ 8	0	0	0	0	0
1 Day	2	1.82	1.65	1.4	0.7	0.7
	4	0.14	0.14	1.0	0.0	0.1
	≥ 6	0	0	0	0	0
3 days	2	0.29	0.25	0	0	0
	≥ 4	0	0	0	0	0
15 days	≥ 2	0	0	0	0	0

does not require more than 2 RO-pairs in a CDIR. However, there will be an inevitable overlap between the two distributions when the ICs are aged for fewer than 3 days. In that case, a higher number of RO-pairs in a CDIR would be required.

Table VII shows the prediction accuracy of the AN-CDIR and the SN-CDIR. The rate of misprediction [i.e., recycled ICs identified as new (θ_1) and new ICs identified as recycled (θ_2)] is also estimated using 1 for the AN-CDIR. We cannot apply this equation to estimate the rate of misprediction for the SN-CDIR, as the distributions are no longer Gaussian. These mispredictions are calculated as

$$\theta_1 = \frac{\#\text{samples with } \Delta f < \Delta f_{\text{th}}}{\text{Total samples}} \times 100\%$$

$$\theta_2 = \frac{\#\text{samples with } \Delta f > \Delta f_{\text{th}}}{\text{Total samples}} \times 100\%.$$

Column 1 represents the duration for the two CDIRs that are aged. Column 2 represents the number of RO-pairs in a CDIR. In this simulation, we have implemented a maximum of 10 RO-pairs in a CDIR. We observe from this table that a larger number of RO-pairs are required to detect ICs that have been aged less amount of time. We can identify all ICs (recycled or new) without any error for both CDIRs with 2 RO-pairs when the aging duration is more than 15 days. All ICs with 3 days of prior usage can be detected using the SN-CDIR with 2 RO-pairs without any error, whereas the prediction errors for AN-CDIR with 2 RO-pairs are 0.2938% and 0.2511%. We require 4 RO-pairs for both CDIRs to identify ICs with only 1 day of aging. However, the SN-CDIR provides better prediction accuracy. We require 6 and 4 RO-pairs for the SN-CDIR and the AN-CDIR to identify ICs with only 12 h of aging. For the SN-CDIR, we need to set the threshold (Δf_{th}) carefully such that θ_1 and θ_2 are of similar value.

If there is no overlap between the two distributions ($g_0(.)$ and $g_t(.)$), then one can select a threshold (Δf_{th}) greater than 0. For example, one can select $\Delta f_{\text{th}} = 2$ MHz for Fig. 12(b)–(d). However, in this table, we mention $f_{\text{th}} = 0$ even though there is no overlap. When the ICs are aged with a less amount of time the distribution ($g_t(.)$) shifts very little to the right, and there might be a possible overlap by the tail of $g_t(.)$ with $g_0(.)$. Thus, it is wise to select a threshold (Δf_{th}) near 0.

When the ICs are used for a very small amount of time, the performance of the SN-CDIR outperforms the AN-CDIR. For example, θ_1 and θ_2 are 13.07% and 12.85% for the AN-CDIR with 2 RO-pairs, whereas they are 7.3% and 7.5% for the SN-CDIR. We can detect recycled ICs with 2 h of aging using an SN-CDIR with 6 RO-pairs, whereas it requires an AN-CDIR with 10 RO-pairs. In addition, the misprediction rate is also higher for the AN-CDIR.

TABLE VIII
AREA OVERHEAD ANALYSIS

Benchmark	Size (# Gates)	Area Overhead (%)					
		O-CDIR [24]	N-CDIR	AN-CDIR/SN-CDIR			
				n=2	n=4	n=6	n=10
i2c	1142	5.52	9.98	19.44	38.35	57.3	95.1
spi	3277	1.92	3.48	6.774	13.37	20	33.1
b14	8679	0.73	1.31	2.558	5.047	7.54	12.5
b15	12562	0.50	0.91	1.767	3.487	5.21	8.65
DMA	19118	0.33	0.60	1.161	2.291	3.42	5.68
DSP	32436	0.19	0.35	0.684	1.35	2.02	3.35
ethernet	46771	0.135	0.24	0.475	0.936	1.4	2.32
vga_lcd	124031	0.051	0.09	0.179	0.353	0.53	0.88
leon2	780456	0.008	0.01	0.028	0.056	0.08	0.14

C. Area Overhead Analysis

Table VIII shows the area overhead analysis of all the CDIRs. We simulated several IWLS 2005 benchmarks ranging from low to high sizes to compute the area overhead. The area overhead is defined as the ratio of the size/area of the CDIR with the size/area of the benchmark. We have not considered the size of the timer and counter while calculating the area for the CDIRs as we assume the frequency measurement can be performed off-chip. We also assume that the area for the AN-CDIR and the SN-CDIR with the same number of RO-pairs is almost the same. The additional area for the SN-CDIR comes from the fuse/antifuse block, and we can neglect this for simplicity's sake.

As seen above, the overhead is more than 1% for small benchmarks (*i2c, spi,* and *b14*) for the 51-stage N-CDIR that could make it challenging to use them in small designs.

The area overhead for the 51-stage O-CDIR [24] is lesser than that for our 51-stage N-CDIR. However, for medium and large designs, the area of the O-CDIR or N-CDIR would hardly impact the overall area of the design.

The area overhead for the AN-CDIR and the SN-CDIR is comparably high for higher numbers of RO-pairs. Both CDIRs with 2 RO-pairs can be implemented in designs larger than the benchmark DMA with minimum area overhead. On the other hand, these CDIRs with 10 RO-pairs can only be implemented in large designs. As the size of most current system-on-chips (e.g., microprocessors, digital signal processors, and microcontrollers) are comparable or larger than *vga_lcd* benchmark, we can successfully implement these CDIRs without affecting the area overhead. In summary, the designers can select a CDIR depending on the area budget that can satisfy the requirements on minimum usage time for detection.

D. Attack Analysis

Due to the evolving nature of IC recycling activities, it is of utmost importance to analyze all of the possible attacks on these CDIRs and their vulnerabilities in order to examine their robustness. Recyclers are always in the process of improving their old technologies through experience and adopting new methodologies. In this section, we analyze all the possible attack scenarios and their impact on our CDIRs.

1) Removal or Tampering of the CDIR: The first attack on the CDIRs could be removal or tampering attacks. In this scenario, the attacker tries to replace the stressed RO with a new counterpart or tries to tamper with the connections inside the multiplexer. However, it is fairly impossible to replace the stressed RO with a new one. Currently, recyclers have the capability to tamper with the connections using focused ion beam circuit edit [37]. If we assume that the tampering is possible, then the counterfeiter must remove the old package and again repackage and remark it according to its original specifications. This removal and repackaging may not be cost effective to the counterfeiters. Hence, it is unlikely to be used in practice.

2) Age Reference RO: The attacker will try to intentionally age the reference RO to mask the frequency differences between the reference and stressed ROs. In this scenario, the attacker forces the CDIR to work in authentication mode (MODE 10, in Table I) under accelerated stress conditions. However, in this mode, the stressed RO will also be in oscillation resulting similar amount of aging. To mask the initial aging difference, the recycler must age the chip for a long period of time. Burn-in is very expensive as there are hundreds of different IC types, and the recycler must have an expensive setup for all different ICs. The primary incentive for counterfeiting is cheap recycling, not adding extra cost to the components. There might not be any motivation left for the counterfeiters when they are forced to add burn-in to their recycling process.

VI. Conclusion

In this paper, we have presented three different structures based on NBTI-aware ROs to detect recycled ICs used only for a very short period of time. The reference ROs in these CDIRs remain quiet during the normal operation of the IC while the stressed RO gets aged at an accelerated pace utilizing NBTI of pMOS transistors. This helps to get a reasonable frequency difference between the reference and stressed ROs even though an IC is used only a very short duration. We proposed two different versions of CDIRs with multiple RO-pairs where the designer can select the number of RO-pairs depending on their area budget. These CDIRs provide better prediction accuracy compared with N-CDIR. AN-CDIR with 10 RO-pair can detect recycled ICs aged only for 2 h with a very little misprediction rate. SN-CDIR provides even better accuracy than AN-CDIR. We can detect recycled ICs with certainty even though they have been used only for 2 h in the field.

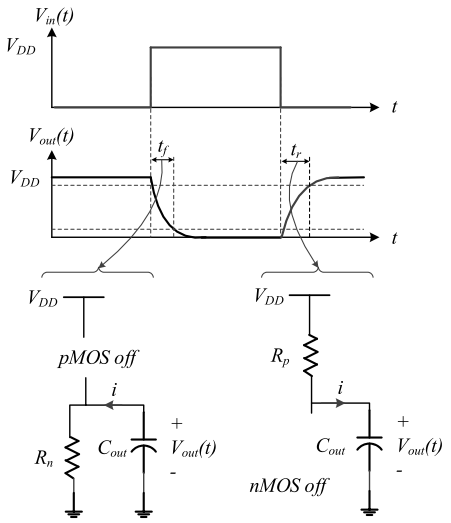


Fig. 13. Transient response of the CMOS inverter.

Appendix

A. Correlation Between δf_S and ∂f_S

The amount of threshold voltage degradation (ΔV_{th}) due to voltage profiles experienced by the pMOS transistor can be represented by [38]

$$\Delta V_{\text{th}} \propto \exp\left(\frac{|V_{\text{gs}}| - |V_{tp}|}{E_0 t_{\text{ox}}}\right)$$

where t_{ox} is the gate oxide thickness, V_{gs} is the gate–source voltage and $E_0 = 2$ MV/cm. Now, differentiating ΔV_{th} with respect to $|V_{tp}|$ results in

$$\frac{d\Delta V_{\text{th}}}{d|V_{tp}|} \propto \frac{-1}{E_0 t_{\text{ox}}} \exp\left(\frac{|V_{\text{gs}}| - |V_{tp}|}{E_0 t_{\text{ox}}}\right) < 0.$$

Thus, ΔV_{th} is a monotonic decreasing function with $|V_{\text{th}}|$, which results in higher degradation in at low V_{th} corner. This will result in a higher δf_S for low V_{th} corner. We can prove a positive correlation between δf_S and ∂f_S if we prove higher ∂f_S leads to the selection of a low $|V_{\text{th}}|$ pMOS transistor.

For simplicity, let us consider a simple RO [see Fig. 1(a)] with n inverters consisting of one pMOS and one nMOS transistors. The frequency of that RO is $f = 1/(2 * n * t_d)$, where t_d is the delay of an inverter. Clearly, the frequency of an RO is inversely proportional to the delay of an inverter while assuming all the inverters are identical.

Fig. 13 shows the transient response of an inverter and the charging and discharging circuits during its switching. The rise time t_r depends on the charging of the output capacitor C_{out} through R_p, while the fall time t_f depends on the discharging of C_{out} through R_n. The RC time constants during charging and discharging are $\tau_p = R_p C_{\text{out}}$ and $\tau_n = R_n C_{\text{out}}$. The rise time and fall time are proportional to τ_p and τ_n, respectively. Now, the propagation delay of an inverter

$$t_d \propto (t_r + t_f) \propto (\tau_p + \tau_n) = (R_p + R_n) C_{\text{out}}$$

where

$$R_p = \frac{1}{\beta_p (V_{\text{DD}} + V_{tp})}$$

and

$$R_n = \frac{1}{\beta_n (V_{\text{DD}} - V_{tn})}.$$

Thus, $f \propto (1/R_p + R_n) = (k/R_p + R_n)$ where k is a constant.

Now, the percentage frequency differences

$$\partial f_S = \frac{f_{0S,V_{\text{DD1}}} - f_{0S,V_{\text{DD2}}}}{f_{0S,V_{\text{DD2}}}} = \frac{\frac{1}{R_{p1}+R_{n1}} - \frac{1}{R_{p2}+R_{n2}}}{\frac{1}{R_{p2}+R_{n2}}} = \left(\frac{R_{p2}+R_{n2}}{R_{p1}+R_{n1}} - 1\right). \tag{9}$$

Differentiating ∂f_S with respect to $|V_{tp}|$

$$\frac{d}{dV_{tp}}(\partial f_S) = \frac{d}{dV_{tp}}\left(\frac{R_{p2}+R_{n2}}{R_{p1}+R_{n1}} - 1\right) = \frac{(R_{p1}+R_{n1})\frac{d}{dV_{tp}}(R_{p2}) - (R_{p2}+R_{n2})\frac{d}{dV_{tp}}(R_{p1})}{(R_{p1}+R_{n1})^2}$$

as R_{n1} and R_{n2} are constants.

Now

$$\frac{(R_{p1}+R_{n1})\frac{d}{dV_{tp}}(R_{p2})}{(R_{p2}+R_{n2})\frac{d}{dV_{tp}}(R_{p1})} = \frac{\left(\frac{1}{V_{\text{DD1}}+V_{tp}} + \frac{1}{V_{\text{DD1}}-V_{tn}}\right) \times \left[-\frac{1}{(V_{\text{DD2}}+V_{tp})^2}\right]}{\left(\frac{1}{V_{\text{DD2}}+V_{tp}} + \frac{1}{V_{\text{DD2}}-V_{tn}}\right) \times \left[-\frac{1}{(V_{\text{DD1}}+V_{tp})^2}\right]} = \frac{V_{\text{DD1}} - V_t}{V_{\text{DD2}} - V_t}$$

assuming $V_{tn} = -V_{tp} = V_t$; $\beta_n = \beta_p > 1$ as $V_{\text{DD1}} > V_{\text{DD2}}$.

Thus, $(d/dV_{tp})(\partial f_S) > 0$ signifies that ∂f_S is a monotonic increasing function with V_{th}. We can infer that the selection of a higher ∂f_S leads to the selection of a lower $|V_{\text{th}}|$ (higher V_{th} as it is negative) pMOS transistor. This results in a positive correlation (>0) between δf_S and ∂f_S.

B. Δf Distribution Versus ROs Stages

Let us consider two n-stage reference and stressed ROs. The frequency of an RO becomes: $f = 1/(2\sum t_{di})$, where t_{di} is the delay for the ith stage. We can express t_{di} as $t_{di} = t_{d0} + \Delta_i$, where t_{d0} is the fixed delay for all the inverters and Δ_i is the variable delay due to PV. Thus, the frequency becomes

$$f = \frac{1}{2nt_{d0} + 2\sum \Delta_i}.$$

Now

$$\Delta f = f_R - f_S = \frac{1}{2nt_{d0} + 2\sum_R \Delta_i} - \frac{1}{2nt_{d0} + 2\sum_S \Delta_i} = \frac{\left(\sum_S \Delta_i - \sum_R \Delta_i\right)}{\left(nt_{d0} + \sum_R \Delta_i\right)\left(nt_{d0} + \sum_S \Delta_i\right)}. \tag{10}$$

From (10), it can be inferred that Δf $(f_R - f_S)$ tends to be near the mean (0) of Δf distribution as n increases due to the numerator increases at the order of n, whereas the denominator increases at the order of n^2. This results in the reduction of the spread of Δf distribution for a 51-stage RO and thus increase in the accuracy.

REFERENCES

[1] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost on-chip structures for combating die and IC recycling," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf.*, Jun. 2014, pp. 1–6.

[2] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *J. Electron. Test.*, vol. 30, no. 1, pp. 9–23, 2014.

[3] U. Guin, D. Forte, and M. Tehranipoor, "Anti-counterfeit techniques: From design to resign," in *Proc. 14th Int. Workshop Microprocessor Test Verification (MTV)*, Dec. 2013, pp. 89–94.

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

[5] L. W. Kessler and T. Sharpe, "Faked parts detection," *Circuits Assembly, J. Surf. Mount Electron. Assembly*, Jun. 2010.

[6] J. Cassell, *Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security*, Apr. 2012.

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

[8] M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. New York, NY, USA: Springer-Verlag, 2015.

[9] B. Hughitt, "Counterfeit electronic parts," in *Proc. NEPP Electron. Technol. Workshop*, Jun. 2010.

[10] F. Koushanfar *et al.*, "Can EDA combat the rise of electronic counterfeiting?" in *Proc. 49th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2012, pp. 133–138.

[11] SAE. *Test Methods Standard; Counterfeit Electronic Parts*. [Online]. Available: http://standards.sae.org/wip/as6171/

[12] U. Guin, D. DiMase, and M. Tehranipoor, "A comprehensive framework for counterfeit defect coverage analysis and detection assessment," *J. Electron. Test.*, vol. 30, no. 1, pp. 25–40, 2014.

[13] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. IEEE Int. Symp. Fault Defect Tolerance VLSI Syst.*, Oct. 2012, pp. 13–18.

[14] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Proc. IEEE Int. Symp. Fault Defect Tolerance VLSI Syst.*, Oct. 2012, pp. 7–12.

[15] Y. Zheng, X. Wang, and S. Bhunia, "SACCI: Scan-based characterization through clock phase sweep for counterfeit chip detection," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 5, pp. 831–841, May 2014.

[16] Y. Zheng, A. Basak, and S. Bhunia, "CACI: Dynamic current analysis towards robust recycled chip identification," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2014, pp. 1–6.

[17] H. Dogan, D. Forte, and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2014, pp. 171–176.

[18] E. Karl, P. Singh, D. Blaauw, and D. Sylvester, "Compact in-situ sensors for monitoring negative-bias-temperature-instability effect and oxide degradation," in *IEEE Int. Solid-State Circuits Conf. (ISSCC), Dig. Tech. Papers*, Feb. 2008, pp. 410–623.

[19] T.-H. Kim, R. Persaud, and C. H. Kim, "Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits," *IEEE J. Solid-State Circuits*, vol. 43, no. 4, pp. 874–880, Apr. 2008.

[20] J. Keane, X. Wang, D. Persaud, and C. H. Kim, "An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB," *IEEE J. Solid-State Circuits*, vol. 45, no. 4, pp. 817–829, Apr. 2010.
[21] J. Keane, W. Zhang, and C. H. Kim, "An array-based odometer system for statistically significant circuit aging characterization," *IEEE J. Solid-State Circuits*, vol. 46, no. 10, pp. 2374–2385, Oct. 2011.
[22] K. Hofmann *et al.*, "Highly accurate product-level aging monitoring in 40 nm CMOS," in *Proc. Symp. VLSI Technol. (VLSIT)*, Jun. 2010, pp. 27–28.
[23] E. Saneyoshi, K. Nose, and M. Mizuno, "A precise-tracking NBTI-degradation monitor independent of NBTI recovery effect," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers (ISSCC)*, Feb. 2010, pp. 192–193.
[24] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. 49th ACM/EDAC/IEEE Design Autom. Conf.*, Jun. 2012, pp. 703–708.
[25] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 5, pp. 1016–1029, May 2014.
[26] M. A. Alam and S. Mahapatra, "A comprehensive model of PMOS NBTI degradation," *Microelectron. Rel.*, vol. 45, no. 1, pp. 71–81, 2005.
[27] S. Bhardwaj, W. Wang, R. Vattikonda, Y. Cao, and S. Vrudhula, "Predictive modeling of the NBTI effect for reliable design," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2006, pp. 189–192.
[28] V. Reddy *et al.*, "Impact of negative bias temperature instability on digital circuit reliability," in *Proc. 40th Annu. Rel. Phys. Symp.*, 2002, pp. 248–254.
[29] K.-L. Chen, S. A. Saller, I. A. Groves, and D. B. Scott, "Reliability effects on MOS transistors due to hot-carrier injection," *IEEE Trans. Electron Devices*, vol. 32, no. 2, pp. 386–393, Feb. 1985.
[30] S. Mahapatra, D. Saha, D. Varghese, and P. B. Kumar, "On the generation and recovery of interface traps in MOSFETs subjected to NBTI, FN, and HCI stress," *IEEE Trans. Electron Devices*, vol. 53, no. 7, pp. 1583–1592, Jul. 2006.
[31] J. W. McPherson, "Reliability challenges for 45 nm and beyond," in *Proc. 43rd ACM/IEEE Design Autom. Conf.*, Jul. 2006, pp. 176–181.
[32] J. Chen, S. Wang, and M. Tehranipoor, "Efficient selection and analysis of critical-reliability paths and gates," in *Proc. GLSVLSI*, 2012, pp. 45–50.
[33] M. K. Steven, *Fundamentals of Statistical Signal Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.
[34] *Predictive Technology Model (PTM)*. [Online]. Available: http://ptm.asu.edu/
[35] T. Sato, T. Kozaki, T. Uezono, H. Tsutsui, and H. Ochi, "A device array for efficient bias-temperature instability measurements," in *Proc. Eur. Solid-State Device Res. Conf. (ESSDERC)*, Sep. 2011, pp. 143–146.
[36] *Normfit*. [Online]. Available: http://www.mathworks.com/help/stats/normfit.html
[37] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, "Breaking and entering through the silicon," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 733–744.
[38] M. Agarwal, B. C. Paul, M. Zhang, and S. Mitra, "Circuit failure prediction and its application to transistor aging," in *Proc. 25th IEEE VLSI Test Symp.*, May 2007, pp. 277–286.

U. Guin (S'10) received the B.E. degree from the Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, Howrah, India, in 2004, and the M.Sc. degree from the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA, USA, in 2010. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA.

He has developed several on-chip structures and techniques to improve the security, trustworthiness, and reliability of integrated circuits. He has co-authored a book entitled *Counterfeit Integrated Circuits-Detection and Avoidance*. He has authored several journal articles and refereed conference papers. His current research interests include counterfeit detection and avoidance, hardware security, VLSI testing, and reliability.

Mr. Guin received the Best Student Paper Award from the IEEE North Atlantic Test Workshop NATW in 2013. He received the SIGDA Ph.D. Forum Scholarship at the Design Automation Conference in 2014. He is an active participant in the SAE International's G-19A Test Laboratory Standards Development Committee.

D. Forte (S'09–M'13) received the B.S. degree from Manhattan College, Riverdale, NY, USA, in 2006, and the M.S. and Ph.D. degrees from the University of Maryland, College Park, MD, USA, in 2010 and 2013, respectively, all in electrical engineering.

He was an Assistant Professor with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA, from 2013 to 2015. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. He has co-authored a book entitled *Counterfeit Integrated Circuits-Detection and Avoidance*. His current research interests include the domain of hardware security, investigation of hardware security primitives, hardware Trojan detection and prevention, security of the electronics supply chain, and anti-reverse engineering.

Dr. Forte was a recipient of the Northrop Grumman Fellowship and the George Corcoran Memorial Outstanding Teaching Award from the Department of Electrical and Computer Engineering, University of Maryland. His work has been recognized through several best paper awards and nominations, including the Conference on Adaptive Hardware Systems in 2011 and the Design Automation Conference in 2012. He has served on the program committees of several workshops and conferences in addition to serving as the Session Chair in many technical events. He will be a Guest Editor of the 2016 IEEE Computer Special Issue on Supply Chain Security for Cyber-Infrastructure.

M. Tehranipoor (S'02–M'04–SM'07) received the Ph.D. degree from the University of Texas at Dallas, Dallas, TX, USA, in 2004.

Prior to joining the University of Florida, Gainesville, FL, USA, he served as the Founding Director of the Center for Hardware Assurance, Security, and Engineering (CHASE) and Comcast Center of Excellence in Security Innovation (CSI), University of Connecticut, Storrs, CT, USA. He is currently the Intel Charles E. Young Professor of Cybersecurity with the University of Florida. He has authored over 300 journal articles and refereed conference papers and has given more than 150 invited talks and keynote addresses. He has also authored six books and 11 book chapters. His current research interests include hardware security and trust, supply chain security, VLSI design, test, and reliability.

Dr. Tehranipoor is a Golden Core Member of the IEEE, and a member of the Association for Computing Machinery (ACM) and the ACM Special Interest Group on Design Automation. He was a recipient of several best paper awards, the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 MURI Award. He serves on the Program Committee of more than a dozen of leading conferences and workshops. He served as the Program Chair of the 2007 IEEE Defect-Based Testing Workshop and the 2008 IEEE Defect and Data Driven Testing (D3T) Workshop, the Co-Program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), the General Chair of 2009 D3T and DFTS, and the Vice General Chair of the 2011 IEEE North Atlantic Test Workshop. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as the General Chair of HOST in 2008 and 2009. He serves as an Associate Editor of the *Journal of Electronic Testing: Theory and Applications*, the *Journal of Low Power Electronics*, the IEEE TRANSACTIONS ON VLSI SYSTEMS, and *ACM Transactions on Design Automation of Electronic Systems*.