Differential Aging Sensor using Sub-threshold Leakage Current to Detect Recycled ICs

Turki Alnuayri, Saqib Khursheed, A. Leonel Hernández Martínez, and Daniele Rossi

***Abstract*—Electronic system components can fall prey to counterfeiting via untrustworthy parties in the semiconductor supply chain, which has established a worldwide span to reduce costs, time to market and increase productivity. Recently, the integrated circuits (ICs) counterfeiting has threatened systems security and reliability that utilize ICs in all domains. This paper focuses on the most counterfeited area—recycled and remarked ICs—and aims to develop a technique to distinguish between new and used digital ICs based on an aging sensor mechanism. Aging sensors have been studied based on path-delay fingerprinting and ring oscillators frequency degradation, but their resolution requires further development to accurately detect short usage. This study proposes a novel differential aging sensor to measure the discharge time (*τdv*) increase that depends on the subthreshold leakage current due to aging with two on-chip designs. Simulations were conducted using the GlobalFoundries 22nm for aging with bias temperature instability and hot carrier injection combined. The results show that the *τdv* increase is 14.72% after 15 days of usage and increases to 60.49% after 3 years. This further increases at higher temperatures; the highest simulated temperature (125°C), *τdv* increases by 55.93% after 15 days, and 310.17% after 3 years. Proposed method also outperformed the traditional frequency degradation based aging estimation method, which at nominal temperature is found to be 5.00% after 15 days and 23.68% after 3 years. Therefore, discharge time is a sensitive indicator for aging, surpasses frequency in detecting previous usage and is robust against process, voltage, and temperature variations.**

***Index Terms*— Counterfeit ICs, Recycled ICs, Subthreshold leakage current, ICs aging effects, HCI and BTI.**

I. Introduction

DUE to the global spread of the semiconductor supply chain, design complexity and involvement of untrustworthy parties, counterfeit integrated circuits (ICs) pose major risks to the security and reliability of electronic systems. Untrustworthy parties, such as fabrication, assembly and packaging facilities, and distributors, could be involved in the untrusted and untrustworthy supply chain businesses affiliated with ICs [1]. In IC components, the term counterfeit refers to an unauthentic copy that does not match the Original Component Manufacturer (OCM) design and/or performance; either the OCM does not produce the unauthentic copy or unauthorized contractors produce it, using the OCM component with false markings/documentation, off-specification, and defective parts, but selling it as new or in working condition [1]. To reduce the cost and time to market, the component manufacturing processes are spread globally from design to distribution. The manufacturing processes and end of component life for all ICs could be exposed to counterfeiting. Electronic systems hardware may be affected by hardware Trojans, physical attacks, and counterfeits. Each of these problems poses challenges for researchers; for example, Trojans may be injected at any stage of the IC fabrication process. The threat of counterfeit ICs is a very serious problem; their use could cause critical systems failures in safety-critical applications, such as automotive, medical, aerospace and defence electronics. Moreover, the threat affects consumers, industries, and governments across a wide variety of domains related to health, public safety, national security, economy, unfair competition for intellectual property (IP) owners and criminal financing sources [1, 2]. There are many types of counterfeit ICs, such as recycled, remarked, overproduced, cloned, out-of-spec/defective, forged documentation and tampered [3]. Mitigation of the number of counterfeit ICs heading to the market requires the government, industry, and academia to collaborate and develop innovative anticounterfeit solutions and to stay updated with new trends [3].

In ICs counterfeiting, the term recycled means a component recovered from an old system and modified in order to be remarked as a new component distributed by the OCM [4]. The recycled component could be aged, and it either has a shorter lifespan due to prior usage or it does not function at all due to the uncontrolled environment of recovery condition [1]. Recovery conditions may damage the component parts or affect their performance due to exposure to high temperatures and the process of removing parts from the boards [1]. Electronic component package markings are used to identify (ID) the component's originality and functionality [4]. A remarked IC could be an old component in which the old markings are

We acknowledge the funding support received from the Department of Computer Engineering, Taibah University, Saudi Arabia, the Department of Electrical Engineering and Electronics, and ODA Research Seed Funding, University of Liverpool, UK, Consejo Nacional de Cienciay Tecnología, Mexico and Italian Ministry of Education and Research in the framework of the CrossLab project (Departments of Excellence) and the Department of Information Engineering, University of Pisa, Italy.

T. Alnuayri is with the Department of Computer Engineering, Taibah University, Saudi Arabia and pursuing his PhD with the Department of Electrical Engineering and Electronics, University of Liverpool, UK (e-mail: Tnuayri@taibahu.edu.sa and T.Alnuayri@liverpool.ac.uk).

S. Khursheed, and L. Hernández are with the Department of Electrical Engineering and Electronics, University of Liverpool, UK (e-mail: S.Khursheed@liverpool.ac.uk; A.L.Hernandez-Martinez@liverpool.ac.uk).

D. Rossi is with the Department of Information Engineering, University of Pisa, Italy (e-mail: daniele.rossi1@unipi.it).

hidden and the component is remarketed as a new component; it could also be a new component that is remarked to improve its grade to earn a high profit [3].

The Information Handling Services (IHS) reported that in the US, the number of incidents of counterfeit IC components in the supply chain increased from 324 to 1363 between 2009 and 2011 [5]. According to a United States (US) Department of Commerce report, 55% of microcircuit producers discovered counterfeit components in their products between 2005 and 2008 [6]. However, this statistic was reported in 2009, when only 25% of electronic waste in the US was thoroughly recycled [7], so the amount of counterfeiting in the remaining unrecycled waste and in the electronic waste of the rest of the world is unknown. Another report stated that the most common IC counterfeiting methods are recycling and remarking, comprising 80% of counterfeiting incidents in the world [1-2]. It is estimated that these components cost the semiconductor supply chain market around USD 169 billion per year, as reported in 2011 [8]. The IHS reported that, for the period between 2007 and 2012, a component was counterfeited every 15 seconds [9].

A. Related Work

The anti-counterfeit ICs methods are divided into two broad categories based on the method of implementation: detection and avoidance methods. Various research surveys were conducted to show recent detection and avoidance measures and future research directions [3, 10, 11, 12]. No single method can identify all types of counterfeit ICs due to the different component types, application risks, design complexities [4] and the counterfeit type that is introduced to a component at a certain stage of the design or at the end of the component's lifecycle. The detection and avoidance measures of counterfeited ICs, including recycled and remarked ICs, is addressed by researchers based on four categories: 1) physical and electrical inspection methods, 2) data analysis 3) track and trace methods and 4) aging degradation sensors [11]. Aging sensors exploit the ICs physical characteristics to detect aging due to changes in transistors' behavior of a period of time [13] that may lead to performance changes such as switching speed (low/fast), and degradation. The aging sensor requires a gold-standard model that refers to the performance of new ICs. This model is used to provide a prior reference measurement to compare the performance results of an aging sensor for the same IC after it has been aged [13] to distinguish between a new and an aged IC. The detection of recycled ICs is typically investigated through aging-based sensors using path delay fingerprinting or ring oscillators (ROs) monitoring [13].

In [14], path-delay fingerprinting was developed to detect recycled ICs through the IC degradation in the field. That study found that the longer the chips have been used the easier it is to observe the recovered IC fingerprinting, but temperature variations may affect the path-delay variations in new ICs making detection impossible [14]. An aging sensor is proposed in [13] to detect recycled ICs by measuring the increase in the discharge time of the sleep transistors due to decrease in their subthreshold leakage current [13]. That aging sensor proved that the sensor is more sensitive to sensors that are used in fine-grained aging degradation sensors [13]. The HSPICE simulation results showed that the discharge time detection is better than the path-delay technique; the increase in the discharge time was three-times better after 1 month and seven-times better after 1 year of usage, and it had a lower area overhead and test time [13].

A considerable amount of research has been undertaken to detect aging mechanisms on the ICs to ensure reliability. Measuring the negative bias temperature instability (NBTI) and the time dependent dielectric breakdown (TDDB) with an independent structure for each aging effect was reported in [15]. The first silicon odometer was proposed by introducing on-chip ring oscillators (ROs) to capture the chip degradation induced by NBTI [16]. This silicon odometer was further improved to detect aging degradation caused by NBTI and hot carrier injection (HCI) [17]. Another technique was proposed based on a statistical measurement system that is designed by utilizing an-array based odometer ROs to detect aging degradation [18]. Saneyoshi *et al.* introduced a hybrid on-chip monitoring to detect aging by combining a RO and a delay line [19].

The main objective of the above-mentioned techniques [15-19] based on ring oscillators (ROs) was to measure the aging degradation and were not meant for detecting recycled ICs. Thus, these techniques [15-19] are unsuitable to detect short usage time with high accuracy with consideration for process and temperature variations [11]. First lightweight ROs-based sensor was presented in [20] to detect chip usage in the field that is motivated by the RO-based sensor in [16] and followed by an improved version in 2014 that consists of counters to continuously record the usage time and an anti-fuse memory block to store usage time [21]. Guin *et al.* [11] proposed three combating die and IC recycling (CDIR) sensors. These versions improved the original CDIR (O-CDIR) proposed in their earlier work [20]. All the CDIR sensors proposed in [11] consisted of a reference ring oscillator (RRO) and a stressed ring oscillator (SRO). The RRO remains quiet until it is required for authentication and the SRO is stressed during the entire operation duration to allow a longer capture window and to increase the resolution of the aging sensor. Only half of the SRO inverters were stressed under NBTI in the O-CDIR [20]. The NBTI-aware (N-CDIR) stressed all inverters in the SRO in order to collect data on aging degradation [11]. Alam *et al.* proposed a solution to detect short recycled ICs usage with a ring oscillator (RO) and a non-volatile memory to structure the on-chip aging sensor [22].

B. Motivation And Contributions

All proposed techniques in [11, 16, 20-22] use ROs frequency to monitor recycled ICs usage with aging degradation. Previous research has shown feasibility of using the subthreshold leakage current (I_{subth}) to detect recycled ICs [13] that aimed to detect recycled ICs based on the I_{subth} decrease to measure the increase in discharge time due to aging degradation over a period of time. However, available methods suffer from process variation effects. This paper addresses this problem by providing two designs. First, it is incorporating two copies of ring oscillators (RRO and SRO) that are identical at time 0 (fresh device), to counter intra-die (within die) process, voltage, and temperature variations (PVTs). Second, only one RO and a non-volatile memory (NVM) has been designed to reduce area overhead. Both designs are used for detecting recycled ROs in [11, 22] but using the frequency fingerprinting.

We combined the N-CDIR aging sensor approach of stressing the SRO and relaxing the RRO during normal operation in [11] and the approach of using the aging sensor based on the subthreshold leakage current to measure the discharge time (τdv) [13] with a view to overcoming the limitations of [11] and of improving the sensitivity obtained in [13] and [23] that would be the new proposed subthreshold leakage current differential aging sensor.

It is essential to review the subthreshold leakage current theory before illustrating the proposed methodology. This study investigates the most frequently encountered aging phenomenon, BTI, and HCI to observe the discharge time changes. The BTI aging effects cause a reduction in the sub-threshold leakage current that makes the aging process beneficial for static power consumption [24, 25]. This occurs due to reduction in the subthreshold leakage current component that is caused by the exponential correlation between the transistor threshold voltage (V_{th}) and the subthreshold leakage current, which results in the discharge time (τdv) increase over time due to aging effects, as derived by (1) [13]:

$$I_{leak} \cong I_{subth} \cong \mu C_{ox} \frac{W}{L} \left(\frac{kT}{q}\right)^2 e \frac{-q\, V_{th}}{nkT} \qquad (1)$$

Where L is the transistor channel length, W is the channel width, μ is the carrier mobility, C_{ox} is the gate oxide capacitance, k is the Boltzmann constant, T is the temperature, q is the electron charge and n is a parameter that depends on the device fabrication (the subthreshold swing coefficient [26]).

The sub-threshold leakage current is the targeted signal for the proposed aging sensor. The I_{subth} current occurs in off-state mode of transistor [26, 27]. The I_{subth} current is active in the weak inversion region, and it occurs between the transistor drain and the source when the gate voltage becomes lower than the V_{th} [26]. As a result, the exponential subthreshold leakage current correlation depends on the V_{th} and the gate-to-source voltage [26, 28]. In recent nanometer CMOS technologies, subthreshold leakage has the highest effect on the static power consumption [28].

Thus, our research overcomes the limitations of [11, 13] and contributes to the IC counterfeiting countermeasures, which can be summarized as follows:

1) Detect recycled and remarked ICs short usage in the field (15 days onwards) with two aging sensors using the subthreshold leakage current.
2) Increase detection percentage using the proposed aging sensor for short usage compared to aging sensors utilizing frequency degradation.
3) Develop an aging sensor that is robust against process, voltage, and temperature variations (PVTs) and considering the most important aging mechanism in modern ICs (BTI and HCI) with BTI recovery.
4) Low cost in term of testing time and area overhead.

The rest of this paper is organized as follows. Section II presents the proposed on-chip aging sensors structure and the proposed methodology. The effectiveness of the proposed solution is discussed through simulation results in Section III. Finally, conclusions are drawn in section IV.

II. Proposed Recycled IC Detection Methods

This section presents on-chip differential aging sensor structure to detect recycled ICs based on measuring discharge time increase of the subthreshold leakage current due to aging. The methodology is divided into two parts. The first part explains the proposed on-chip aging sensor structure and the second part illustrates sensor registration and authentication processes. Table I illustrates the meaning of each abbreviation used in this paper.

A. *Proposed Aging Sensor Structure*

The structure of the aging sensor, which is based on two ROs, consists of the following components (Fig. 1): two identical fresh ROs' copies at time 0, which must have the same RO size (e.g., 13-stage RO, 21-stage RO, etc.), these designs are placed on the silicon beside each other (to keep the process variations (PV) minimal with approximately the same operating temperature), a counter, a comparator and non-volatile memory (NVM). The discharge time reading mechanism is shown in Fig. 2. We are proposing additional signals that could improve the accuracy of the aging sensor to detect recycled ICs that were initially proposed in [11] and modified in [22], and designed with only one RO and an NVM and using the discharge time.

The ROs frequency is measured directly from the RO output, based on the two-ROs (RRO and SRO) design proposed in [11] and the one RO and NVM design in [22]. Reading the discharge

TABLE I
USED SYMBOLS MEANING

Symbol	Meaning
RO	Ring Oscillator
RRO	Reference Ring Oscillator
SRO	Stress Ring Oscillator
I_{subth}	Sub-threshold Leakage Current
τdv	Discharge time
τdv_{RRO}	Reference RO discharge time
τdv_{RRO_0}	Reference RO discharge time at time 0 (Fresh)
$\tau dv_{RRO_{age}}$	Reference RO discharge time at time t (Age)
τdv_{SRO}	Stress RO discharge time
τdv_{SRO_0}	Stress RO discharge time at time 0 (Fresh)
$\tau dv_{SRO_{age}}$	Stress RO discharge time at time t (Age)
$\Delta\tau dv$	Discharge time difference between τdv_{RRO} & τdv_{SRO}
$\Delta\tau dv_{Fresh}$	Discharge time difference between τdv_{RRO_0} & τdv_{SRO_0}
$\Delta\tau dv_{age}$	Discharge time difference between τdv_{RRO_0} & $\tau dv_{SRO_{age}}$
$\Delta\tau dv_{All}$	Discharge time difference between $\Delta\tau dv_{Fresh}$ & $\Delta\tau dv_{Age}$

time in nanoseconds (ns) can be achieved by using a counter clock sensor structure proposed in [23, 29], by counting the clock signals. Fig. 1 and Fig. 2 show the modified versions for measuring the discharge time for the two-RO and one-RO sensor, respectively. The discharge time sensor works as time to digital converter and this type of sensor is used in modern electronic chips infrastructure [29]. The sensor mainly composed of an AND gate, a buffer, and a counter. It operates by counting the number of clock falling edges to capture the RO output drop to logic-0 and the threshold value is 10% of the supply voltage as shown in Fig. 2. Then, multiplying the clock period by the counter value, gives the discharge time measurements.

The proposed sensor is highly accurate and focuses not only on recycled IC detection through subthreshold leakage current but also considers common problems in aging sensors that could bias detection results, that is the effect of process, voltage, and temperature variations (PVTs). PV will be addressed during the registration and authentication steps of the proposed sensor design. Process, voltage, and temperature variations are further described in the simulation results section.

The sensors' main components are two identical ROs: the reference ring oscillator (RRO) and the stress ring oscillator (SRO). Readings of the RO output can be made accessible using a multiplexing technique from the existing primary output, which is on-chip [22]. In addition, there is no need for extra hardware for the counter because it typically exists in modern ICs [21], and ROs can also be chosen from the manufacturing process monitors [22]. A comparator is added to compute the difference between fresh RRO and aged SRO discharge time measurements. The NVM is used to store the RRO fresh discharge time and the difference in discharge time between fresh SRO and RRO readings. The NVM content cannot be modified easily after it has been programmed, but it can be programmed within the supply chain, such as through read-only memory (ROM) and one-time-programmable (OTP) memory [22]. However, this paper mainly focuses on detecting recycled IC with high robustness against the PVTs and data tampering may still happen at any stage of design or IC's lifetime. Security concerns about saving data in the NVM or on-chip memory is beyond the scope of this work.

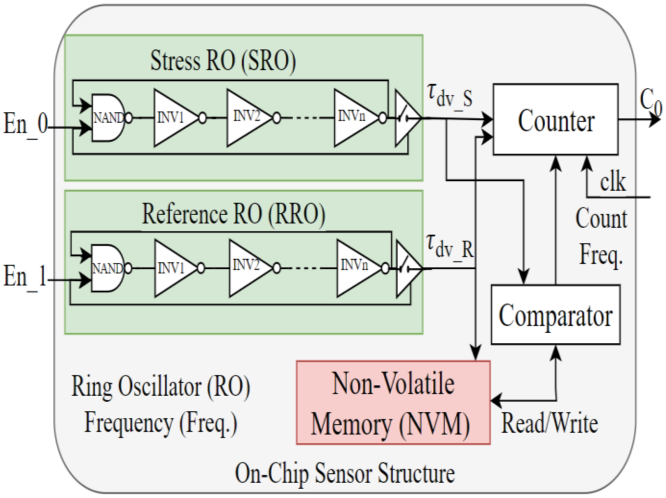

Fig. 1. The proposed aging sensor structure based on two ROs.

TABLE II
SELECTING DISCHARGE TIME READINGS DURING MANUFACTURING

τdv_{RRO_0}	τdv_{SRO_0}	$\Delta\,\tau dv_{Fresh}$	Note
15ns	15ns	0	Ideal
15ns	13.80ns	1.20ns	$\tau dv_{RRO_0} < \tau dv_{SRO_0}$
14.60ns	15ns	0.40ns	Allocate, $\tau dv_{RRO_0} < \tau dv_{SRO_0}$

B. *Registration and Authentication Processes*

1) *A Two-ROs Sensor Design*

During the registration phase, we consider three possible PV scenarios along with normal operation variation when designing the structure of the proposed sensor. The PV scenarios are considered as follows:

a) PV During Manufacturing

This scenario tackles PV during the manufacturing process. Even if the two ROs (RRO and SRO) have been designed with the same parameters, research shows that the PV cannot be avoided; there will always be a difference between the RRO and SRO frequencies [22], and the subthreshold leakage current is no exception. After chips have been manufactured and tested for defects, our proposed sensor starts the registration steps as follows: It firstly measures the fresh discharge time of the RRO and SRO outputs, and sends readings to the comparator component to compute the difference, as in (2):

$$\Delta\tau dv_{Fresh} = \tau dv_{RRO_0} - \tau dv_{SRO_0} \qquad (2)$$

Table II shows assumed examples for possible discharge time readings. During registration, it always determines the greater discharge time value to be assigned for the RRO because readings may vary due to PV. Secondly, it sends the $\Delta\tau dv_{Fresh}$ result to the NVM along with the fresh RRO τdv_{RRO_0} reading at time 0 because a fresh RRO is needed for the third scenario. Thirdly, it programs the NVM with the ROs' data that contain

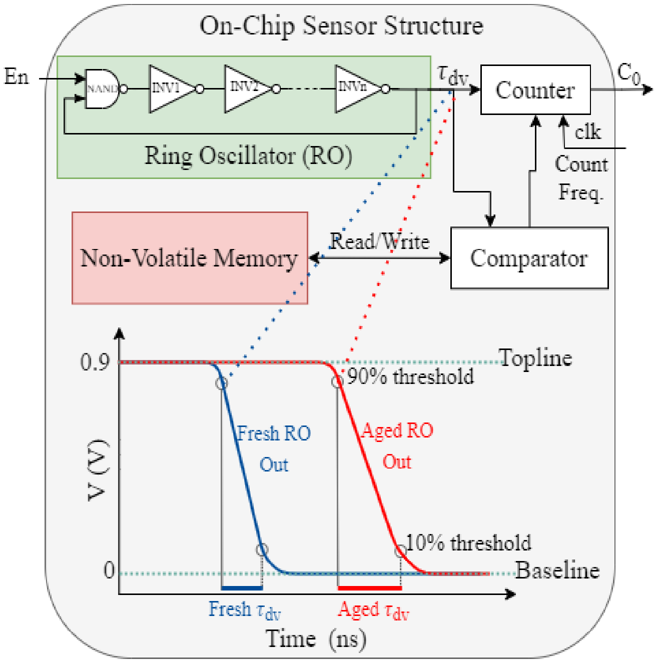

Fig. 2. The proposed aging sensor structure based on a RO and an NVM and simulation setup to measure the RO discharge time output.

discharge time readings along with measurement conditions, such as age time t_0, supply voltage and temperature, and it generates a digital signature to secure the saved data. Programming and securing NVM content with the digital signature process can be found in other publications [22]. The subthreshold leakage current is sensitive to temperature and so is the discharge time. To assure measurement accuracy during authentication, the collected discharge time reading at time t_0 is saved in the NVM. The stored data must also contain the operating temperature to be able to match it at time t of usage. Moreover, having several readings to be stored in the NVM at time t_0 at different temperature values will address the problem and therefore increases the recycled ICs detection accuracy.

b) Variation During Normal Operation

Designing the RRO and SRO with same design parameters should zero the difference $\Delta\tau dv$ between the RRO and the SRO at time 0; however, due to PV, always will be $\tau dv_{RRO_0} \neq \tau dv_{SRO_0}$. As a result, computing the $\Delta\tau dv_{Fresh}$ reading at time 0 will spot the difference of whatever the PV impacts during either manufacturing or other type of normal operation variation. Then, saving $\Delta\tau dv_{Fresh}$ in the NVM will reduce the misprediction rate, and it could be used as a reference measurement when the authentication process is performed with $\Delta\tau dv_{Age}$ at time t of usage (e.g., hours, days, months, and years).

c) RRO Age During Normal Operation

In an ideal case, the mechanism of the proposed sensor is to keep the RRO quiet until it is required for authentication. If RRO experience aging during normal operation, then saving fresh RRO (τdv_{RRO_0}) in NVM during manufacturing can be used as a reference reading and the effect of PV is minimized.

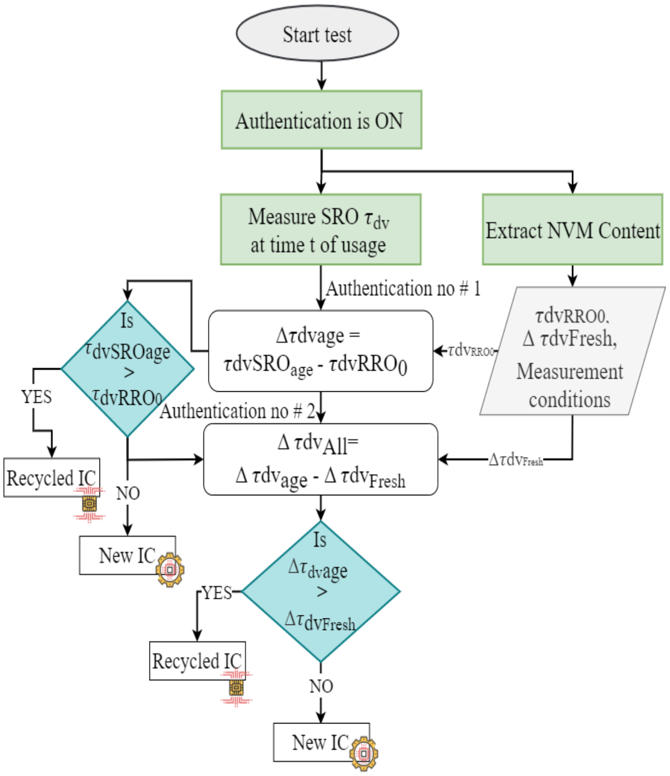
Start test
Authentication is ON
Measure SRO τ_{dv} at time t of usage
Extract NVM Content
Authentication no # 1
τdvRRO0, Δ τdvFresh, Measurement conditions
$\Delta\tau$dvage = τdvSRO$_{age}$ - τdvRRO$_0$
τdvRRO0
Is τdvSROage > τdvRRO0
YES
Recycled IC
NO
New IC
Authentication no # 2
Δ τdv$_{All}$= Δ τdv$_{age}$ - Δ τdv$_{Fresh}$
$\Delta\tau$dv$_{Fresh}$
Is $\Delta\tau_{dvage}$ > $\Delta\tau_{dvFresh}$
YES
Recycled IC
NO
New IC

Fig. 3. The flow of the proposed authentication process.

To keep RRO quiet, the RRO is disconnected from the V_{dd} and it will be connected only if it is required for authentication. This is critical to reduce the misprediction rate. During the authentication phase, the RRO will be read once during manufacturing. It then remains quiet until it is required for authentication. The SRO is stressed during the entire operation to allow for a longer capture window and to increase the resolution of aging detection. The sensor design considers two authentication steps to ensure detection accuracy against PV. The authentication process, which is presented in Fig. 3, and it can be summarized as follows:

1) If the authentication mode is ON, then the sensor begins the validation process as follows:
   A. It measures the SRO discharge time at time t of usage ($\tau dv_{SRO\,age}$).
   B. It extracts the NVM content ($\tau dv_{RRO\,0}$ *and* $\Delta\tau dv_{Fresh}$).
2) For the first authentication, the comparator calculates the difference in discharge time as in (3):

$$\Delta\tau dv_{age} = \tau dv_{SRO\,age} - \tau dv_{RRO\,0} \qquad (3)$$

3) If the $\tau dv_{SRO\,age} > \tau dv_{RRO\,0}$, then the IC under authentication is a recycled IC; otherwise, it is classified as a new IC. To respond to the second and third PV scenarios in the registration process, a second authentication is required.

4) For the second authentication, the comparator calculates the difference in discharge time as in (4):

$$\Delta\,\tau dv_{All} = \Delta\,\tau dv_{age} - \Delta\,\tau dv_{Fresh} \qquad (4)$$

5) If the $\Delta\tau dv_{age} > \Delta\tau dv_{Fresh}$, then the IC under authentication is a recycled IC; otherwise, it is classified as a new IC. Having two stages of authentication will reduce the misprediction rate that could occur due to PV and useful if the contents of NVM are compromised by an adversary.

2) *A One-RO-Based Aging Sensor*

This version of a one-RO-based aging sensor structure consists of the following components (Fig. 2): One RO, a counter, a timer, a comparator, and NVM. Moreover, Fig. 2 shows discharge time reading mechanism for both sensors. The following occurs during registration:

1) The fresh discharge time of the RRO output is measured.
2) The RRO $\tau dv_{RRO\,0}$ reading is saved in the NVM.

During authentication, the following occurs:

1) If the authentication mode is ON, then the sensor begins the validation process by measuring the RRO

discharge time at time t of usage ($\tau dv_{{RRO}_{age}}$), followed by extracting the NVM content ($\tau dv_{{RRO}_{0}}$).

2) For authentication, the comparator calculates the difference in discharge time as in (5):

$$\Delta\tau dv_{age} = \tau dv_{{RRO}_{age}} - \tau dv_{{RRO}_{0}} \tag{5}$$

If the $\tau dv_{{RRO}_{age}} \leq \tau dv_{{RRO}_{0}}$, then the IC under authentication is a new IC; otherwise, it is classified as a recycled IC.

C. Security Evaluation

There is a trade-off between the area overhead and the detection accuracy, which may be biased by PV. In the two-ROs design, the NVM area overhead can be removed in favor of saving space, but this will come at a risk of accuracy degradation. Moreover, where NVM authentication (data tempering or lost) is a concern, then only two ROs (RRO & SRO) can be used for chip authentication. The proposed two-ROs design could be adapted easily using only one RO and a NVM as in [22]. This design is cost efficient in term of area overhead as it does not require a comparison operation between two different ROs. The required storage from the NVM is negligible for recording usage time and generating the digital signature by deploying the hash function (SHA-2/SHA-3) and public key cryptographic primitive (Elliptic Curve Cryptography -ECC) is less than a kbit (around 702 bits) as suggested in [22] to avoid data tempering and secure NVM content. Having a two RO design (SRO and RRO) the hazard associated with tampering data in the NVM is circumvented by direct measurements using the two ROs. This is another reason why a number of configurations (number of ROs and use of NVM) are suggested in this paper, thus allowing designers to select a suitable configuration for their own purposes and design settings.

The proposed aging sensors could face possible attack scenarios through either tampering or removing the ROs, modifying NVM data. We will discuss related attacks that are worth committing and profitable for recyclers. The NVM content integrity is secured by a digital signature to prevent it from modifications. If an attempt takes place to extract the NVM content, then that will cause a failure check because of the signature and mark the chip as a recycled one [22]. To tampered NVM content, it requires the signature using a private key that is only known by the trusted original component manufacturer (OCM). It is possible to modify NVM data if the private key is stolen from the OCM, but such an attempt is impossible or can occur vary rarely [22]. Moreover, keeping the private key large enough will prevent the attempt to recover it by the recyclers. However, a detailed security analysis in response to all relevant economical attack scenarios for recyclers can be found in [22]. Our proposal is robust against them as these attacking scenarios would cost recyclers more than what they could earn from ICs recycling business.

A comparison is shown in Table III to show all trade-off and costs involved within each aging sensor design with several parameters. The comparison parameters are marked with one of the three degrees of evaluation based on results and the senor design structure: *high*, *medium*, and *low*. Marking a sensor with high means that the sensor at its best sensitivity and robust for a particular parameter (i.e., BTI Recovery). Note that the sensor components will be off all the time, and they are not going to age with the IC as they are only used when authentication is required, which is the process that verifies if the IC is a new or an old one. In the two-RO design, only the stressed RO is turned on during the entire operation time, whereas the reference RO, the counter and comparator (Fig. 1) are switched off, which turn on only at the authentication time. Likewise, in case of one RO and NVM design, all parts other than the RO are switched off except at the registration and authentication time. Even if there are inaccuracies in the measurement process, and in presence of process variation, the proposed approach is accurate enough to distinguish if a circuit has been previously used. This is due to the differential nature of the proposed design, which diminishes this impact.

III. Simulation Results And Discussion

A. Simulation Configuration

The current study aims to investigate the most frequently encountered aging phenomenon: bias temperature instability (BTI: positive and negative PBTI, NBTI) and hot carrier injection (HCI), to help detect recycled ICs, develop the proposed aging sensor, and consider process, voltage, and temperature variations (PVT) during sensor design and the simulation tests. The analysis was performed using the Virtuoso RelXpert Simulator from Cadence that simulates ICs degradation due to aging effects. The CMOS technology library used for simulations is the 22nm technology which is provided by GlobalFoundries (GF). It is crucial to consider that different types of stress and degradation could be introduced to ICs due

TABLE III
Trade-off Between Different Aging Sensor Design

Sensor Detector	**τdv**	**τdv**	**τdv**	**Freq.**	**Freq.**	**Freq.**
Aging Sensor **Comparison Parameter**	**2 ROs & NVM** / Encrypting NVM Content 2021	**Only 2 ROs** [23] 2020	**One RO & NVM** / Encrypting NVM Content 2021	**2 ROs** (**NBTI-Aware CDIRs)** [11] 2016	**One RO & NVM** [22] 2018	**Original CDIR** [20] 2012
Detection Accuracy	High	High	High	Medium	Medium	Low
BTI Recovery	High	High	High	Medium	High	Low
PVs Impact	High	High	High	Medium	High	Low
NVM Security	High	NA	High	NA	High	NA
Stress % (Workload) / Consider different applications ON/OFF times	100%	100%	100%	100%	NA	50%
Age Time Detection	15 Days Onwards	15 Days Onwards	15 Days Onwards	3 Days Onwards	One Day Onwards	One Month Onwards

to changes in the switching activity and operating conditions across the chip (temperature and voltage variation) [30]. Simulations were configured with the following parameters: age time from 15 days up to three years, the supply voltage was (V_{dd}) = 0.9V, load capacitance at the RO output was 250fF, temperature was 25°C, 50°C, 75°C, 100°C, and 125°C, and for voltage variation was V_{dd} was set to 0.9V, 0.8V, and 0.7V based on the GF22nm standard use conditions for the nominal operating voltage. The aging effects, including NBTI, PBTI and HCI were simulated. Simulation was configured to measure the RO discharge time readings as shown in Fig. 2 (Doted lines: blue and red). To be able to measure the discharge time mechanism, the supply voltage is turned-on and then switched off to let the nodes discharge through the leakage current. This is the time window for our sensor to collect measurements as illustrated in Fig. 2 for fresh and aged RO output.

B. BTI Recovery

The main objective of our paper is not to estimate how long a chip has been used, but to identify whether it has been used or not. The discharge time (τdv) is measured and BTI recovery is included in the simulations to detect recycled ICs. In [31], after a certain testing time of 27.78 hours (at the initial stages of usage) for continued stress of 2777.78 hours (115.74 days), the effect of NBTI recovery reached a level of saturation and it became negligible as the drain current slope and lifetime had minor degradation. These two trends have also been observed in our accelerated simulation results over 3 years lifetime, confirming that most of NBTI recovery mechanism occurs at the initial stage of the device. Moreover, the sensor is able to detect a $\Delta\tau dv$ for 15 days onwards up to the aged time, in our case 3 years, allowing a reliable detection of recycled ICs using the discharge time parameter and is robust against BTI recovery.

Measuring the ROs lifetime simulations is following the fast system method [32] to address the BTI recovery carefully and represent its effect on the ROs to accurately measure the τdv. Moreover, we are separating simulation tests stages (fresh, stress and aged) to calculate the effect of BTI even with the worst-case simulations by exposing the circuit to stringent stress conditions to observe degradation at their weakest performance based on the CMOS GF recommendation [33]. Test's separation is crucial in detecting the most of BTI recovery for accurate ROs representation for discharge time during the stress and measurement stages [34]. Based on the utilised CMOS technology - GF 22nm, the BTI recovery is included in the aging models to calculate devices lifetime accurately [33].

The stress time may vary from application to application depending on the percentage of circuit usage. For example, a medical device may work for 100% of the time in a pacemaker, whereas personal use devices may work less than 100% such as TVs and laptops [11]. Considering the following hypothetical assumption scenario demonstrates that under various stress times and its corresponding BTI recovery effects, the measure of the τdv can be performed accurately. If a RO is stressed for a period and followed by unstressed period, it may recover due to BTI and it may result in a wrong discharge time readings and therefore biased recycled ICs detection accuracy, which could be used by an adversary to alter ICs age and represent the ICs as a new one. Responding to this scenario, a 100% stress is reported in Fig. 7 and Fig. 8 for discharge time and in Fig. 9 for the frequency over the entire operation time to control the BTI recovery during the stress/un-stress periods. In [11], a 100% stress was applied for frequency measurements. Although, it still has a misprediction rate where frequency distribution overlapped (fresh and age), and two versions of the main NBTI-aware sensor were proposed to solve the misprediction [11], but it comes with the cost of higher area overhead. There is a trade-off between stress time % to account BTI recovery and detection accuracy, and power consumption.

As another way to handle the above scenario, a locking mechanism can be used to lock readings even with the existence of BTI self-healing to show the circuit correct age. We could record usage time reading at a certain peak, time, or percentage of circuit usage in an on-chip memory to minimize the NBTI self-healing and extract BTI effects even with the existence of BTI self-healing. The concept of recording usage time continuously has been used in [21] with the anti-fuse (AF)-based sensor to minimize PV impact. That sensor used for detecting usage time less than a month using different structure that composed of counters to count the clock cycle and switching activities, and an embedded one-time programmable (OTP) memory to store usage time. Instead of recording usage time continuously, this can be done discretely and at various carefully selected time slot may be used for collecting usage time. Applying the same concept could handle BTI self-healing and PVs impact but with the cost of area overhead for the new added parts to the sensor structure and memory space. For example, recording usage time every 3 days and update last stored reading with the new reading can minimize used space in the memory.

The Δτdv measurement is robust against varying stress ratios, we simulated three different stress ratios to represent circuit usage. This was simulated using the 51 RO by reducing stress conditions by varying its load capacitance at a representative temperature of 75°C to observe how the Δτdv behaves under different stress ratios, and therefore to determine the effect of BTI recovery on recycled ICs detection. Obtained results can be seen in Fig. 4. After 3 years of accelerated aging, the Δτdv for 100% stress is equal to 143.38%, 75% stress is 131.74%, 50% stress is 117.22%, and for 25% stress is 100.32%.

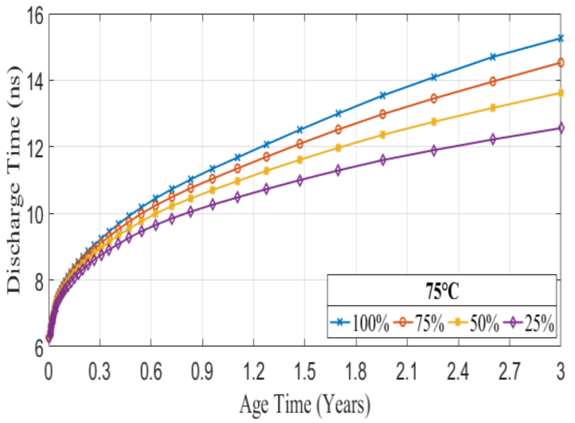

Fig. 4. 51-stage RO discharge time at 75°C with different stress ratios.

C. *Experiments*

1) *Process Variations (PVs)*

The PVs has been demonstrated in Section II with three possible scenarios to avoid misreading aging results and with two sensors design. In the two-ROs design, placing two identical ROs at time 0 (new) will minimize the process variation (intra-die) and environmental effects (operating temperature and supply voltage variation) as much as possible. The one-RO design has less impact by the PV as it has been explained in Section II-B. To demonstrate the proposed sensor robustness against PV, we simulated the proposed solution using Monte Carlo (MC) simulations in Cadence by varying devices parameters (transistor width, length, gate oxide thickness and threshold voltage) using the CMOS 22nm GF model files. The MC was configured to 600 permutations at time 0 (fresh) based on [35] that after 500 permutations it provides reliable data.

During the registration and authentication process, it is important to compute the effect of process variation for intra-die and inter-die along with operating conditions to minimize and control it to an acceptable level, and obtain accurate $\Delta\tau_{dv}$ measurements at the authentication time. Fig. 5 shows a 51-stage RO, and Gaussian distribution with a standard deviation (σ, ±3 process variations) of 423.10ps and a mean (μ) of 10.54ns for intra-die PV, whereas in Fig. 6, the histogram shows a σ of 918.66ps and a μ of 10.42ns for inter-die PV.

It should be observed that the proposed sensor design with two ROs will be placed on the same spatial proximity of a die and therefore the expectation is that the behavior is going to be close enough. As a result, the reference RO will be in a very close proximity with the stressed RO, for example if that is around the mean value, the difference will be less than 0.25-0.5 of one standard deviation. It is unlikely to observe three standard deviations as the two ROs are placed physically close to one another. The difference in discharge time, between the ROs is important for the registration process to assign RRO and SRO during manufacturing to accurately account for PVs impact on the sensor measurement. Thus, recycled IC detection using the τdv offers a reliable and better detection rate compared to the frequency to determine if an IC has been used previously.

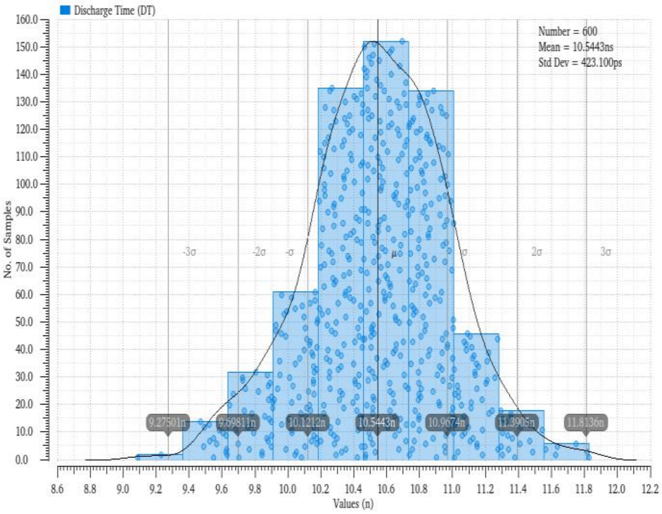

Fig. 5. 51-stage RO distribution for intra-die PVs.

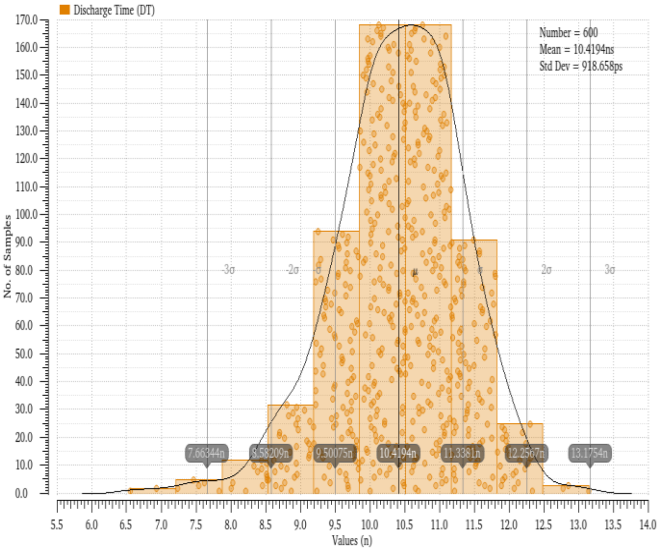

Fig. 6. 51-stage RO distribution for inter-die PVs.

2) *Discharge Time Evaluation*

The analysis was performed to observe the discharge time increase over usage time due to aging. The τdv has been proved in [13, 36] to measure aging and therefore used to detect recycled ICs using a 90-nm technology node. The τdv is defined as the time for the voltage to reach 10% of the supply voltage whereas the charge time is the time it takes to reach 90% of the voltage [36], Table IV shows the discharge time results for 13 and 51-stage ROs output at 25°C, and with usage time from 15 days up to three years in the second column of the Table. Third column represents fresh τdv and followed by the aged τdv in (ns) due to aging effects. The $\Delta\tau_{dv}$ and the %τdv are calculated using (6) and (7), respectively. The $\Delta\tau_{dv}$ calculates the difference between fresh τdv (at t= 0) for RRO and aged τdv for SRO (at t of usage) for the 13 and 51-stage ROs. The %τdv calculates the τdv percentage increase over aging time. Fig. 7 shows the τdv results for 13 and 51 ROs, respectively.

TABLE IV
DISCHARGE TIME INCREASE DUE TO AGING AT 25°C FOR 13 AND 51 ROS

RO Stage	Age Time (Months)	Fresh τ_{dv} (ns)	Aged τ_{dv} (ns)	$\Delta\tau_{dv}$ (ns)	$\Delta\tau_{dv}$ % Increase
13	0.5	13.27	15.12	1.85	13.94
	1		15.28	2.01	15.15
	3		15.93	2.66	20.05
	6		16.52	3.25	24.49
	12		16.97	3.70	27.88
	18		17.26	3.99	30.07
	24		17.67	4.4	33.16
	36		18.15	4.88	36.77
51	0.5	10.53	12.08	1.55	14.72
	1		12.60	2.07	19.66
	3		13.27	2.74	26.02
	6		14.31	3.78	35.90
	12		15.29	4.76	45.20
	18		15.78	5.25	49.86
	24		16.15	5.62	53.37
	36		16.90	6.37	60.49

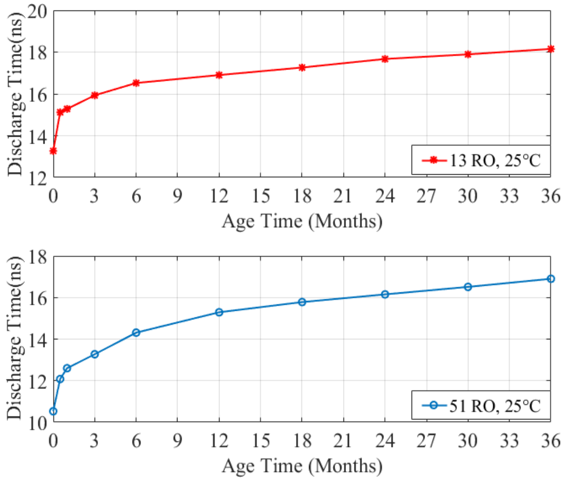

Fig. 7. 13 and 51-stage ROs discharge time samples at 25°C.

$$\Delta\tau_{dv} = Aged\tau_{dv} - Fresh\tau_{dv} \tag{6}$$

$$\%\tau dv = \frac{Aged\tau_{dv} - Fresh\tau_{dv}}{Fresh\tau_{dv}} \times 100 \tag{7}$$

In the 13-stage RO (13 inverters), after one month of usage at 25°C, the $\Delta\tau_{dv}$ is 15.15% and after three years of usage it has increased to 36.77%, an increase of almost 2.43 times. In the 51-stage (51 inverters) the $\Delta\tau_{dv}$ is 19.66% after one month of usage at 25°C; after three years $\Delta\tau_{dv}$ increase reaches 60.49%, an increase of 3.08 times. It can be clearly seen that longer RO chain is providing higher percentage and bigger $\Delta\tau_{dv}$ results, which has a higher number of gates and that takes longer time to discharge. This trend is in line with previously published results [13], with additional value of process variation awareness and temperature. To prove discharge time results with temperature and voltage variations, the following simulation tests were conducted:

TABLE V
13 AND 51-STAGE ROS DISCHARGE TIME IN % WITH TEMPERATURE VARIATION

RO stage	Age Time (Months)	50°C $\Delta\tau_{dv}$(%)	75°C $\Delta\tau_{dv}$(%)	100°C $\Delta\tau_{dv}$(%)	125°C $\Delta\tau_{dv}$(%)
13	0.5	26.09	26.25	44.5	48.75
	1	32.61	32.72	54.25	60.22
	3	40.87	43.85	73	79.57
	6	48.15	55.65	93.75	101.08
	12	54.24	62.46	108.25	114.70
	18	60	69.44	122	127.60
	24	65.54	77.24	131.75	143.37
	36	72.5	85.55	141.25	160.93
51	0.5	20.12	29.82	45.12	55.93
	1	27.09	40.03	60	75.59
	3	39.53	58.53	87.44	109.83
	6	55.47	81.82	121.63	161.02
	12	68.02	104.31	152.33	216.61
	18	74.30	115.95	167.67	239.32
	24	79.53	124.72	181.86	257.97
	36	91.28	143.38	217.67	310.17

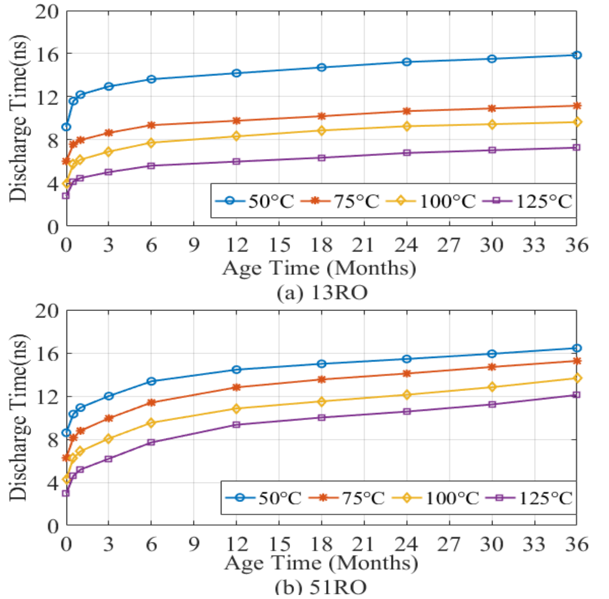

Fig. 8. 13 and 51-stage ROs discharge time samples with temperature variation.

a) Temperature Variation

The temperature variation must be observed in smaller technology node to avoid misreading the age of an IC with a false prediction. Therefore, four temperature values were simulated for both 13- and 51-stage ROs over various operation times, as reported in Table V. First column represents RO stage, second column represents accelerated simulation time in months and third column represents the $\Delta\tau_{dv}$ percentage increase for 50°C, 75°C, 100°C, and 125°C. Fig. 8 presents 13 and 51 ROs discharge time with temperature variation. Towards the end of Table V, for the 13-stage RO and the 51-stage RO, after three years of operation at 125°C, the $\Delta\tau_{dv}$ reaches the highest increase values of 160.93% and 310.17%, respectively.

TABLE VI
13 AND 51-STAGE ROS DISCHARGE TIME IN % WITH VOLTAGE AND TEMPERATURE VARIATION

RO Stage	Age Time (Years)	V_{dd} (V)	Temperature	$\Delta\tau_{dv}$ (%)
13	3	0.7	25°C	9.41
			50°C	7.77
			75°C	18.32
		0.8	25°C	21.31
			50°C	28.01
			75°C	35.54
		0.9	25°C	36.77
			50°C	72.5
			75°C	85.55
51	3	0.7	25°C	6.76
			50°C	11.32
			75°C	17.14
		0.8	25°C	17.96
			50°C	29.44
			75°C	44.99
		0.9	25°C	60.49
			50°C	91.28
			75°C	143.38

b) Voltage Variation

Voltage variation is another crucial parameter that must be considered when working with the small technology nodes. Three voltage variation values V_{dd} = 0.9V, 0.8V, and 0.7V were simulated based on the GF22nm foundry standard use conditions for the nominal operating voltage. It has been tested with three different temperature values of 25°C, 50°C, and 75°C to test the τdv results with temperature and voltage variations combined. The results are presented in Table VI. The τdv shows robust results even when both variations are combined. For instance, after three years of aging for the 13-stage RO at V_{dd} = 0.7V and 75°C, the τdv is detectable and is 18.32%. Taking V_{dd} = 0.8V and 0.9V at the same temperature of 75°C, the τdv is higher than 0.7V and with 1.94 times and 2.41 times increase, respectively.

3) *Comparison with Frequency Evaluation Methods*

Table VII shows the frequency degradation (Δ*f*) results for 13- and 51-stage RO output in % with different temperature variation and with usage time from 15 days up to three years. The Δ*f* results are calculated in % using (8) and (9). Comparing τdv and *f* RO results, the *f* shows an opposite trend compared to the τdv due to aging, and it decreases over usage time as shown in Fig. 9 (a) for the 13-stage RO and Fig. 9 (b) for the 51-stage RO frequency degradation.

$$\Delta f = Aged\ (f) - Fresh\ (f) \qquad (8)$$

$$\%f = \frac{Fresh\ (f) - Aged\ (f)}{Fresh\ (f)} \times 100 \qquad (9)$$

According to the results using the 28nm HPL technology node in [24], the frequency degradation due to aging for ROs output will be higher in the smaller technology node as expected. This trend has been proven by this work and the frequency degradation percentage has increased for the utilized GF22nm technology node (Table VII). For example, an 81-stage RO indicates a deviation of 4.61% after one month of usage [22], whereas the 51-stage RO (smaller RO) in this work shows 7.28% after one month of usage. However, the discharge time is a much more sensitive indicator for aging that shows high-resolution results.

TABLE VII
13 AND 51-STAGE ROS FREQUENCY DEGRADATION IN % WITH TEMPERATURE VARIATION

RO stage	Age Time (Months)	25°C Δ*f* (%)	50°C Δ*f* (%)	75°C Δ*f* (%)	100°C Δ*f* (%)	125°C Δ*f* (%)
13	0.5	8.73	12.28	13.37	16.52	19.71
	1	10.03	13.57	15.47	19.06	22.01
	3	12.48	14.97	18.06	20.11	23.55
	6	14.12	19.01	21.71	25.05	28.94
	12	17.47	20.66	24.90	28.34	32.24
	18	18.91	23.85	27.25	31.59	35.88
	24	20.11	25.50	29.89	33.98	38.22
	36	22.70	28.29	32.58	37.52	42.12
51	0.5	5.00	6.42	8.06	9.77	11.63
	1	7.28	9.34	11.63	13.98	16.48
	3	11.20	14.19	17.33	20.61	23.89
	6	14.48	18.19	22.04	25.89	29.74
	12	16.69	20.83	25.11	29.39	33.52
	18	19.19	23.75	28.39	33.10	37.66
	24	20.90	25.82	30.81	35.81	40.58
	36	23.68	29.10	34.59	40.23	45.44

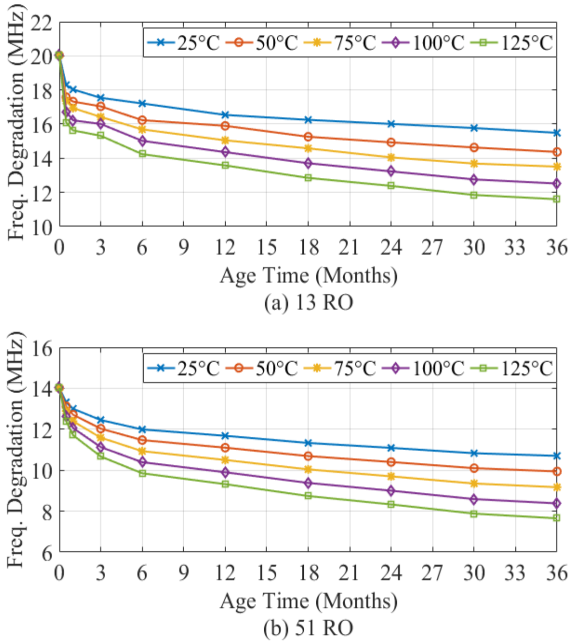

Fig. 9. 13 and 51-stage ROs frequency degradation samples with temperature variation.

A comparison representation between discharge time and frequency in percentage in Fig. 10 and Fig. 11 with temperature variation for 13 RO and 51 RO, respectively. In both figures, red line represents the discharge time and blue line for the frequency data. Five temperature values: 25°C, 50°C, 75°C, 100°C, and 125°C were simulated to create two indication profiles (τdv, *f*) that detect RO age under BTI and HCI. It can be seen clearly that with temperature increase over age time in 13 and 51-stage ROs in Fig. 10 and Fig. 11 the difference between the τdv and *f* is significant. For instance, Fig. 10 shows that at 25°C and after 15 days of usage, the $\Delta\tau dv$ is 13.94%, whereas the Δ*f* is 8.73%. After 3 years of usage, the $\Delta\tau dv$ is increased and it is 36.77% and for Δ*f* is 22.70%. In Fig. 10, as the temperature is moving from 25°C to 125°C and usage time from 15 days to three years, we can notice that the discharge

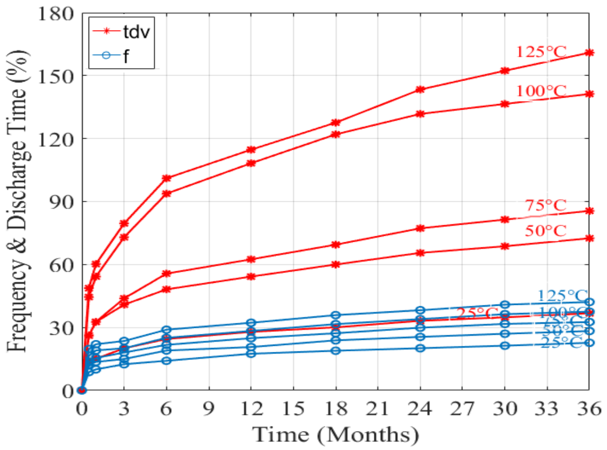

Fig. 10. 13-stage RO discharge time Vs frequency in %.

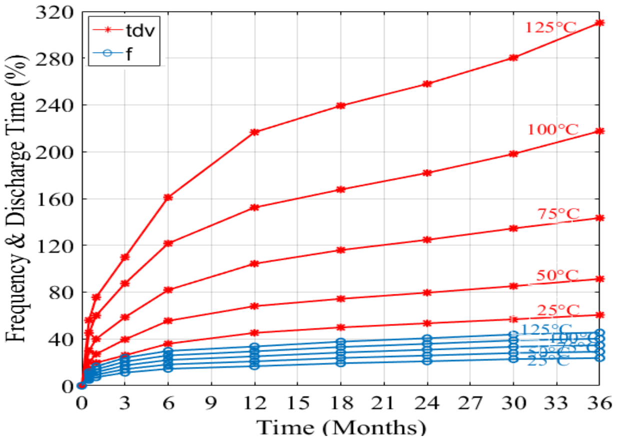

Fig. 11. 51-stage RO discharge time Vs frequency in %.

time is separated, travelled far from the frequency, and reported higher percentage results with aging. For the 51-stage RO in Fig. 11, we can see similar trend to the 13-stage RO in Fig. 10 but with much higher % increase. Thus, with high confidence the discharge time is better aging indicator for ICs than the frequency.

IV. Conclusion

This paper proposed two on-chip aging sensor structures to detect recycled ICs based on the discharge time measurements. The first design is structured with a reference ring oscillator (RRO) and a stressed ring oscillator (SRO) to measure the difference in discharge time measurement due to aging. The second sensor is designed with a single ring oscillator (RO) and a non-volatile memory (NVM) to store the measurements of the RO at manufacturing time. The sensors exploit sub-threshold leakage current characteristic to measure the discharge time changes over usage time, under aging effects of BTI and HCI combined. The proposed sensors are robust against PVT variations and able to detect recycled and remarked ICs even with short usage time (15 days or more). Process variation (PV) is simulated using Monte Carlo analysis to observe intra-die PV and inter-die process variation. All simulations were carried out using Cadence EDA tools and 22-nm CMOS technology provided by GlobalFoundries. Simulation results demonstrate good detectability of recycled ICs when considering the discharge time measurement, with the process, voltage, and temperature variations. To compare the proposed aging sensors that utilise discharge time measurement with sensors using frequency measurements, a comparison was made between them, and the simulation results show that discharge time is a better aging indicator than frequency. The results showed that the discharge time reached 48.75% and 55.93% after 15 days' usage and 160.93% and 310.17% after 3 years for 13- and 51-stage ROs, respectively. By contrast, the frequency degradation for 13-stage RO reached 19.71% after 15 days' usage and 42.12% after 3 years and for 51-stage RO reached 11.63% after 15 days' usage and 45.44% after 3 years.

References

[1] M. M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*, 1st ed., Springer, 2015.

[2] D. Forte and R. S. Chakraborty. Counterfeit integrated circuits: Threats, detection, and avoidance, accessed on Aug. 01, 2020. [Online]. Available: https://ches.iacr.org/2018/slides/ches2018-tutorial1-slides.pdf

[3] U. Guin *et al.*, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, no. 8, pp. 1207–1228, Aug. 2014.

[4] S. Bhunia and M. Tehranipoor. "Electronics Supply Chain," in *Hardware Security: A Hands-on Learning Approach*, 1st ed., Morgan Kaufmann, 2018.

[5] Information Handling Services (IHS), *Reports of counterfeit parts quadruple since 2009, challenging US defense industry and national security*, accessed on Dec. 07, 2020. [Online]. Available: https://www.electronicproducts.com/reports-of-counterfeit-parts-quadruple-since-2009-challenging-us-defense-industry-and-national-security/

[6] U.S. Department of Commerce - Bureau of Industry and Security. *Defence industrial base assessment: Counterfeit electronics*, accessed on Aug. 02, 2020. [Online]. Available: https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

[7] U.S. Environmental Protection Agency - Office of Resource Conservation and Recovery, *Electronics waste management in the United States through 2009*, accessed on Aug. 02, 2020. [Online]. Available: https://www.epa.gov/

[8] Information Handling Services (IHS), *Top 5 most counterfeited parts represent a $169 billion potential challenge for global semiconductor market*, accessed on Dec. 08, 2020. [Online]. Available: https://www.eetimes.com/ihs-counterfeit-parts-represent-169b-annual-risk/#

[9] Information Handling Services (IHS), *One counterfeit part every 15 seconds*, accessed on Mar. 06, 2021. [Online]. Available: https://www.electronicproducts.com/ihs-news-flash-one-counterfeit-part-every-15-seconds/#

[10] E. Oriero and S. R. Hasan, "Survey on recent counterfeit IC detection techniques and future research directions", *Integration*, vol. 66, pp.135–152, May 2019.

[11] U. Guin, D. Forte and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 24, no. 4, pp. 1233–1246, Apr. 2016.

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

[13] D. Rossi *et al.*, "Recycled IC detection through aging sensor," in *Proc. IEEE 23rd ETS*, Bremen, Germany, May. 2018, pp. 1–2.

[14] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. IEEE International Symposium on DFT in VLSI and Nanotechnology Systems*, Austin, TX, USA, Oct. 2012, pp. 13–18.

[15] E. Karl *et al.*, "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*, San Francisco, CA, USA, Feb. 2008, pp. 410–623.

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

[17] J. Keane, *et al.*, "An all-in-one silicon Odometer for separately monitoring HCI, BTI, and TDDB," *IEEE J. of Solid-State Circuits*, vol. 45, no. 4, pp. 817–829, Apr. 2010.

[18] J. Keane, W. Zhang and C. H. Kim, "An array-based Odometer system for statistically significant circuit aging characterization," *IEEE J. of Solid-State Circuits*, vol. 46, no. 10, pp. 2374–2385, Oct. 2011.

[19] 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. - (ISSCC)*, San Francisco, CA, USA, Feb. 2010, pp. 192–193.

[20] X. Zhang, N. Tuzzio and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *DAC*, San Francisco, CA, USA, June 2012, pp. 703–708.

[21] 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.

[22] M. Alam *et al.*, “Robust, low-cost, and accurate detection of recycled ICs using digital signatures,” in *Proc. IEEE Int. Symposium on HOST*, Washington, DC, USA, Apr.-May 2018, pp. 209–214.

[23] T. Alnuayri *et al.*, “Differential aging sensor to detect recycled ICs using sub-threshold leakage current,” in *Proc. DATE*, Feb. 2021, pp. 1500–503.

[24] D. Rossi, *et al.*, “Reliable power gating with NBTI aging benefits,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 24, no. 8, pp. 2735–2744, Aug. 2016.

[25] D. Rossi, *et al.*, “Aging benefits in nanometer CMOS designs,” *IEEE Trans. on Circuits and Systems II: Express Briefs*, vol. 64, no. 3, pp. 324–328, Mar. 2017.

[26] P. F. Butzen and R. P. Ribas, “Leakage current in sub-micrometer CMOS gates,” *Universidade Federal do Rio Grande do Sul*, 2006, pp. 1–28.

[27] S. Mishra, N. K. Singh, and V. Rousseau, “Understanding Power Consumption Fundamentals,” in *System on Chip Interfaces for Low Power Design*, Morgan Kaufmann, 2015.

[28] D. Helms, E. Schmidt, and W. Nebel, “Leakage in CMOS circuits—An introduction,” in *LNCS (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 3254, pp. 17–35.

[29] V. Tenentes, *et al.*, “Coarse-Grained Online Monitoring of BTI Aging by Reusing Power-Gating Infrastructure,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 4, pp. 1397-1407, April 2017.

[30] R. Ezz-Eldin, M. A. El-Moursy and H. F. A. Hamed, “Process Variation,” in *Analysis and Design of Networks-on-Chip Under High Process Variation*, 1^{st} ed., Springer Inter. Publishing, 2015.

[31] Wong *et al.*, “Impact of NBTI Recovery, Measurement System and Testing Time on NBTI Lifetime Estimation,” in *International Conference on Advanced Manufacturing and Industrial Application. Atlantis Press,* Dec. 2015.

[32] *A Procedure for Measuring P-Channel MOSFET Negative Bias Temperature Instabilities,* JESD90, 2004.

[33] CMC GlobalFoundries (GF), “Model Reference Guide - Aging,” unpublished – confidential.

[34] J. Chiu, *et al.*, “Statistical Characterization and Modeling of the Temporal Evolutions of ΔV_t Distribution in NBTI Recovery in Nanometer MOSFETs,” *IEEE Trans. on Electron Devices,* vol. 60, no. 3, pp. 978-984, March 2013.

[35] S. Khursheed, *et al.*, “Delay Test for Diagnosis of Power Switches,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 2, pp. 197-206, Feb. 2014.

[36] S. Khursheed et al., “Improved DFT for testing power switches,” in Proc IEEE ETS, Trondheim, Norway, May 2011, pp. 7–12.

Turki Alnuayri received the bachelor’s degree in Computer Engineering from the Umm Al-Qura University, Makkah, Saudi Arabia, in 2013, and the MSc degree in Embedded Systems Engineering from the University of Leeds, Leeds, UK, in 2017. He holds an academic position at Taibah University, Medina, Saudi Arabia, as a lecturer from January 2014 to the present. He is currently pursuing his PhD with the Department of Electrical Engineering and Electronics, University of Liverpool, UK. He is interested in all issues related to hardware security and reliability of embedded systems, machine learning for security, and Internet of things (IoT) security.

Saqib Khursheed received the Ph.D. degree in electronics and electrical engineering from the University of Southampton, Southampton, U.K. He is currently a Lecturer (Assistant Professor) with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K. He is interested in all issues related to hardware-oriented security, reliability, and test of low-power, high performance designs, and 3-D integrated circuits. He has authored a number of papers in internationally leading journals and conferences in these areas.

Antonio Leonel Hernández Martínez received the MSc degree in microelectronics on November 2018 and is currently a Ph.D. candidate at the University of Liverpool, Liverpool, U.K. His research studies and publications involve testing techniques for electronic embedded systems, aging phenomena in CMOS technology and prediction methods for useful lifetime of electronics, implemented in high reliability and safety domains.

Daniele Rossi received the MSc degree in electronic engineering and the Ph.D. degree in electronics and computer engineering from the University of Bologna, Bologna, Italy, in 2001 and 2005, respectively. He is currently an Associate Professor in Electronics with the Department of Information Engineering, University of Pisa, Italy. His current research interests include hardware security, energy efficient and reliable digital design, and robust design for soft error and ageing resiliency. Dr. Rossi has co-authored over 100 papers published in international journals and conference proceedings and holds one patent.