A Ring-Oscillator-Based Degradation Monitor Concept with Tamper Detection Capability

Javier Diaz-Fortuny[1*], Pablo Saraza-Canflanca[1], Erik Bury[1], Michiel Vandemaele[1,2], Ben Kaczer[1], Robin Degraeve[1]
[1]imec, Kapeldreef 75, 3001 Leuven, Belgium
[2]ESAT, KU Leuven, Kasteelpark Arenberg 10, 3001 Leuven, Belgium
(*mailto: javier.diazfortuny@imec.be)

***Abstract*— Refurbished chips (i.e., chips re-used legally in circular economy) and counterfeited chips (i.e., used chips fraudulently sold as new) are a growing concern for the industry because of their poor reliability. In this context, various solutions for the detection of such chips have been presented in the literature, several of which make use of performance degradation detection circuits. In this work, we propose a new concept for a degradation monitor, which can (1) obtain the age of the chip and (2) detect if the chip has been tampered through high-temperature annealing. To demonstrate the principles of this concept, we designed a novel and versatile array of addressable ring-oscillators (ROs), a type of circuit that has been widely proposed to detect fraudulently recycled chips. The array IC was manufactured in a 28 nm CMOS technology and utilized as a reliability test vehicle. Using this chip, we performed an extensive study of degradation phenomena that affect the ROs, as well as the recovery that they undergo after the stress application has ceased. Finally, we examined the impact that temperature annealing has on the recovery of circuit degradation, thus fraudulently concealing prior usage of the chip.**

***Index Terms*—annealing, array chip, Bias Temperature Instabilities (BTI), Hot Carrier Injection (HCI), integrated circuit reliability, ring-oscillator, tamper detection.**

I. Introduction

Possible refurbishment of used chips in a circular economy, as well as anti-counterfeiting measures, represent new challenges for a trustworthy utilization of reliable ICs by end costumers [1]. On-chip degradation monitoring enables reliable recycling of used chips by assessing their degradation and thereby inferring their remaining lifetime. Moreover, such monitors can also be used for the identification of counterfeited chips by detecting degradation on chips that are (re-)sold as new [2]-[4]. Implementations of such monitor systems have already been presented [5]-[7], and typically rely on ring-oscillator (RO)-based circuits to evaluate degradation undergone by ICs. In the above context, however, these approaches present some shortcomings. First, they are not able to distinguish between the physical degradation of the circuit and its actual age (i.e., the time since fabrication), which could be useful to discard chips that are older than claimed. Second, degraded chips can be deceitfully tampered with, since high temperature annealing [8] enhances recovery of the Bias Temperature Instability (BTI) [9] and Hot-Carrier Injection (HCI) [10] degradation phenomena. Thus, degradation undergone by the on-chip monitors might be concealed to the user, as shown below.

The main objective of this work is to present a new concept of degradation monitor circuit, which can obtain the age of an IC and detect if the chip has undergone tampering through high-temperature annealing. In this scenario, the IC age calculation and the tampering detection capability are deduced from the distinct macroscopic characteristics of the degradation and subsequent relaxation induced by BTI and HCD aging phenomena in ROs. Then, the adequacy of these procedures will be investigated through extensive experimental tests performed on a novel and versatile RO-array chip designed and fabricated in a commercial 28nm high-k metal gate CMOS technology (see Fig. 1).

The paper is organized as follows. Section II discusses the proposed aging monitor concept with the capability to detect IC tampering through high-temperature fraudulent annealing. Section III describes the experimental setup used in this work, that consists of our novel RO-array IC design, as well as the executed RO evaluation methodology. The IC with addressable ROs is used to extensively characterize the time-zero variability and time-dependent degradation in dynamic and static RO operation. In Section IV, the results obtained from the RO characterization are depicted and utilized to describe the principle of triangulation to deconvolute stress time and temperature undergone by the monitors. Moreover, this section also describes the conducted degradation annealing tests on the RO monitors. Finally, conclusions are given in Section V.

II. Tamper-Detection Aging Monitor

Our proposed implementation of an on-chip degradation monitor with tamper detection is shown schematically in Fig. 2. The tamper detection degradation monitor consists of two sets of monitors, each one formed by a pair of ROs.

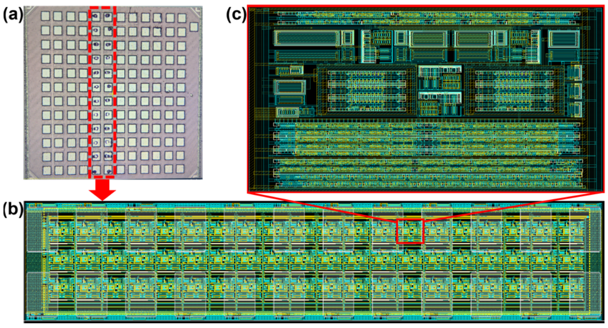

Figure 1. (a) micrograph of the actual fabricated chip of our first-generation RO-array ICs. The fabricated die consists of 6 different RO-array modules each with 24 pads for probe test. (b) GDS illustration of a single RO-array module that harbors 60 individual RO unit cells each containing 2 identically designed ROs. Unit cells are accessed by means of a two-layer shift register. (c) GDS illustration of a unit cell with digital cell control, twin ROs in the middle and 2^{15} frequency dividers + frequency counters.

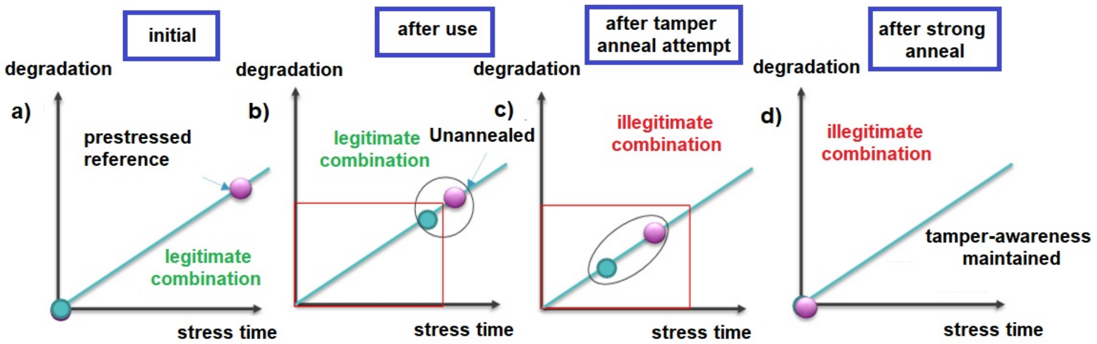

Figure 2. Concept of degradation monitor with tamper detection capability in 4 different scenarios. (a) Initial: fresh (blue) + pre-stressed (pink) monitors. (b) after chip use: expected chip wear- out & extraction of chip 'age', pre-stressed monitor outside the illegitimate combination zone (red rectangle). (c) Illegitimate combination after tampering attempt: pre-stressed monitor enters illegal combination zone due to anneal. (d) Strong tampering detected by pre-stressed monitor.

As depicted in Fig. 2(a), the initial conditions of the two monitors are: one unstressed at time zero, i.e., the blue bubble, that will account for the degradation undergone by the chip during regular operation. The second monitor, i.e., the pink bubble, which will be used to account for the IC relaxation as the tamper-detection capability. This RO-monitor will be intentionally pre-stressed, accumulating a considerable known initial degradation. By evaluating the on-chip degradation and relaxation of the monitors, it can be assessed if the IC has undergone expected degradation and relaxation based upon the understood physics, or whether it has relaxed to an extent that exceeds the expected values, revealing a fraudulent anneal process. In this respect, three different scenarios can occur:

- After legitimate IC use: during regular IC operation, i.e., within the technology defined voltage and temperature margins, the first monitor will progressively degrade with time while the second monitor will relax. As depicted in Fig. 2(b), under regular operation, neither of the two monitors will go beyond a maximum degradation/relaxation window, i.e., red box in Fig. 2(b), In this scenario, both monitors will show that the IC has been operated trustfully and their degradation/relaxation levels are within a legitimate combination thus, it is possible to estimate the age of the chip.
- After use and tamper anneal attempt: in this situation, the chip has been used and it has also been tampered with to pretend that the IC is less used than it really is. In this situation, the pre-stressed monitor enters its forbidden relaxation window because the anneal attempt accelerates its relaxation. When this behaviour is obtained in the field, it unveils an illegitimate combination of both monitors, as depicted in Fig. 1(c), pointing out that a tamper procedure has happened and invalidates the IC age reading obtained from the first monitor.
- After a strong anneal procedure: in this scenario, the chip has undergone a strong anneal process to illegally rejuvenate it. In such anneal scenario, both aging monitors will show almost complete relaxation status, as depicted in Fig. 2(d). Even though the IC seems be to be brand new according to the first degradation monitor, the pre-stressed monitor is located deep into its forbidden region, revealing the strong anneal and maintaining the tamper-awareness of the monitor system.

We also propose a first implementation of such on-chip aging monitor as depicted in Fig. 3. The implementation incorporates a regular RO affected by BTI + HCI (designed as a regular chain of inverter stages always oscillating), an only-BTI RO (incorporating a NAND gate to keep the RO feedback loop always open during IC operation) and an enhanced-HCI RO (designed with increased capacitance load between the inverter stages increasing the drive current during switching and thus the HCI degradation) as the degradation monitors. This RO monitor combination will evaluate the amount of degradation of the BTI-only and the enhanced-HCI ROs. Then, if the degradation behaviour for these two phenomena has been accurately modelled, the monitors can "triangulate" those two degradation values and deconvolute them into a unique pair of operation time and bias conditions undergone by the IC during its operation. Moreover, an analogous pair of significantly pre-stressed ROs are also included in the scheme. This makes use of the different relaxation behaviour of BTI and HCI to perform an analogous triangulation and unveil the recovery conditions (time and temperature) and thereby, detect if the chip has been tampered with.

The distinct relaxation behaviour of BTI and HCI is depicted in Fig. 4 as a function of time and temperature. For BTI, the universal recovery model [9] is used, as it will later be shown that such model fits our data accurately. HCI recovery is modelled according to Stesmans' passivation model for Pb-defects [11], which has been already used to accurately describe HCI recovery under different temperatures [12] (see Fig. 4 (b)).

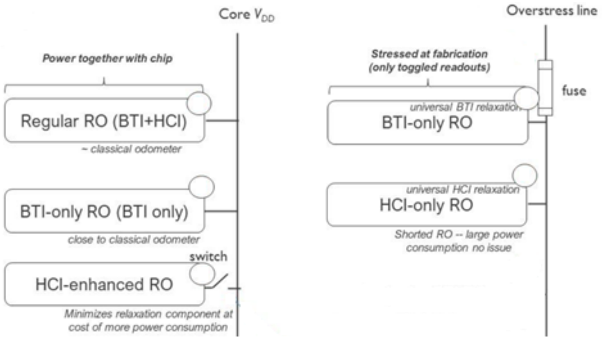

Figure 3. Proposed ring oscillator monitor scheme for chip 'age' extraction and tamper-awareness. The age and degradation monitors connected to VDD core reflecting chip wear-out proportional to operating time. Monitors pre-stressed at fabrication time can be used for fraudulent chip annealing detection.

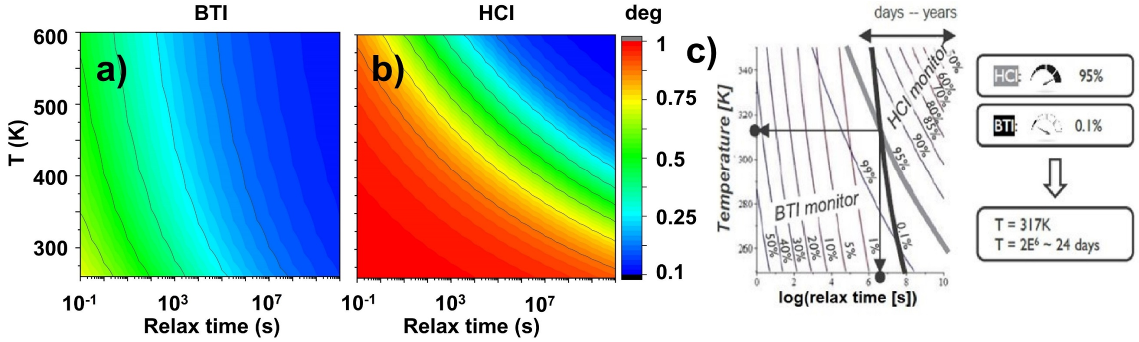

Figure 4. Illustration of the temperature-dependent relaxation of (a) NBTI and (b) HCI as inferred from the models in [11], [12]. (c) Illustration of resolving time and temperature (τ, T) if the degradation status of a relaxing BTI and HCI-stressed monitor is read out.

As depicted in Fig. 4(c), the IC relaxation time and temperature (τ, T) can be resolved by evaluating the intersection point between the evaluated BTI-only and HCI-enhanced ring oscillators of the relaxation monitor. Then the cross point will reveal the anneal temperature and time that the chip has undergone. An analogous triangulation procedure could be performed to obtain the IC stress voltage and temperature conditions during stress.

III. Experimental Setup

All the tests presented in this work have been conducted using our first-generation RO-array chip design fabricated in a commercial and well-characterized [13], [14] 0.9 V 28 nm HKMG technology. The main building blocks of the IC are shown in Fig. 5 and described hereinbelow.

A. *RO-array IC building blocks*

In order to efficiently use the chip area in our experiments, the chip includes a total of 60 ROs pairs designed with 28 nm core devices which are distributed over 3 rows and 20 columns. Each RO pair has been embedded in an individually controlled block named "unit cell" that harbors the necessary digital and analog circuitry to operate the ROs under different test conditions. On-chip unit cell selection is performed by means of a row and column circuitry constructed by two-layer shift registers that permit individual unit cell selection for measurement by a 23-bit selection word, i.e., 3-bit for row selection, and 20-bit for column selection. The array is also equipped with 3 on-chip Force-&-Sense (F&S) biasing paths, i.e., $V_{STRESS\text{-}ST}$, $V_{MEAS\text{-}ST}$ and $V_{MEAS\text{-}REF}$, used to bias the ROs during variability tests and minimize on-chip voltage drop (see Fig. 5(a)). Thanks to this versatile design, different unit cells can be selected for different operations that can occur simultaneously. For instance, when a unit cell is selected for stress operation, its ROs will be connected to the stress biasing paths and, at the same time, another unit cell can be selected for measurement while connected to the measure path. This versatility can be used to conduct parallel stress tests on several ROs simultaneously to significantly reduce the total test time of aging tests. Moreover, the connection of the unit cell ROs to the different biasing paths is done by means of three operation modes, i.e., stress, measurement or standby, that establish a physical connection between the ROs V_{DD} and the biasing paths through a set of dedicated IO transmission gates [15]-[17].

B. *Unit cell circuitry*

Fig. 5(b) shows the detail of the unit cell circuit design. It consists of two 51-stages ROs with a fundamental oscillation frequency of ~2GHz. The RO's feedback loop is controlled by a NAND gate that allows enabling/disabling the RO oscillation, thus allowing to perform dynamic (closed loop) or static (open loop) tests. Moreover, each RO is connected to a 15-stage frequency divider for frequency down-division and to a digital frequency counter for on-chip RO frequency characterization. The on-chip frequency readout can be easily retrieved by means of a digital output interface. As shown in Fig. 5(b), the output of the frequency dividers is also connected to the external pads for off-chip frequency measurements after frequency down division. Finally, the on-chip F&S paths, as well as the unit cell transmission gates have been sized to sustain RO biasing voltages up to 3V and DC currents up to 3mA.

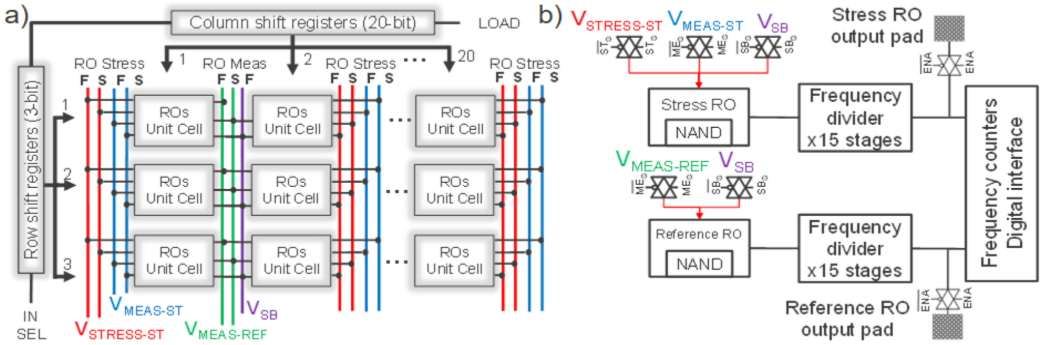

Figure 5. (a) Schematic illustration of the high-level array chip design. (b) a unit cell consisting of the ROs together with a frequency divider circuit for off-chip readout and with appropriately sized force-&-sense pass gates to each RO bias.

The digital control circuitry embedded in each unit cell consists mainly of three single-bit memories. Each memory block stores a 1-bit digital signal corresponding to one operation mode. Therefore, three bits are needed to indicate the operation mode: the stand-by bit “SB”, the measure bit “ME” and the stress bit “ST”.

C. *RO evaluation methodology*

The ROs characterized in this work have been subjected to an enhanced Measurement-Stress-Measurement (eMSM) [16] accelerated Time-Dependent Variability scheme, as depicted in Fig. 6(a). Before the stress, the ROs are subjected to a “fresh” readout to capture their fundamental frequency.

During the stress phase, the RO biasing voltage is raised above the nominal voltage and once the stress time is finished, the RO bias is switched (in less than 100µs) to the nominal supply voltage of 0.9 V for frequency recovery characterization. During accelerated aging tests, when the RO loop is open and therefore, the RO is not oscillating (i.e., static), RO devices undergo DC BTI degradation, whereas when oscillating (i.e., dynamic) they undergo AC BTI and HCI degradation. “Static” and “dynamic” degradation tests with a total accumulated stress time of 3,000 s have been performed in different ROs, with stress voltages ranging from 1.8 V to 2.4 V. Moreover, as depicted in Figs. 6(b) and (c), during stress phases the RO frequency degrades and can only be captured in dynamic operation (see Fig. 6(b)). During measurement phases the RO frequency starts to recover.

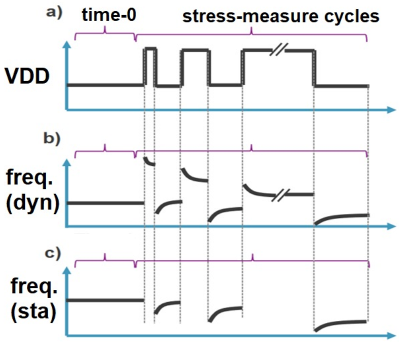

Figure 6. RO test sequence: time-zero followed by eMSM tests: (a) *VDD* waveform, (b) RO frequency in dynamic stress and recovery and (c) in static stress where no frequency can be measured during stress.

After the above discussed stress/measurement dynamic and static tests, all involved ROs have undergone a sequence of controlled anneal tests, as depicted in Fig. 7. Two types of annealing have been conducted on the target ROs after 36 h of room temperature relaxation:

- Thermochuck anneal: all ROs have been subjected to a 12 h and 24 h anneal at 200ºC. Moreover, after each anneal period, all ROs have been characterized to account for the accumulated recovery (T0’).

- Oven anneal: similar to the previous anneal, all target ROs have been ‘baked’ in an oven at 300 ºC for 72 h using a nitrogen gas flow that prevented the array from corroding. Finally, all target ROs have been characterized to obtain their status after this strong annealing (T0’).

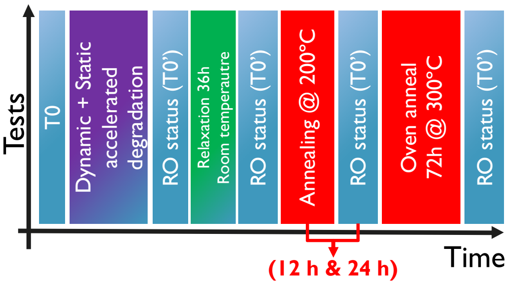

Figure 7 Structure of the degradation + annealing tests. Blue indicates frequency measurement, purple indicates degradation test, green indicates relaxation at room temperature and red indicates high temperature annealing.

IV. Results and Discussion

A. *Principle of triangulation:*

The principle of triangulation proposed in this work requires an accurate understanding of the RO behaviour under several accelerated stress conditions. To this end, multiple ROs have been stressed and their frequency recovery has been precisely captured over 7 decades to understand the impact of the accelerated TDV tests on the RO structures. An example of the RO frequency recovery captured after 10 stress phases is depicted in Fig. 8, showing ubiquitous relaxation [18],[19].

Considering all the different stress conditions, the dependence of the RO frequency degradation with the accumulated stress time and the stress voltage can be obtained, as shown in Figs. 9(a) and (b) respectively. The time exponent (n) and the Voltage Acceleration Factor (VAF) metrics are obtained from the data following a power-law dependence in both cases.

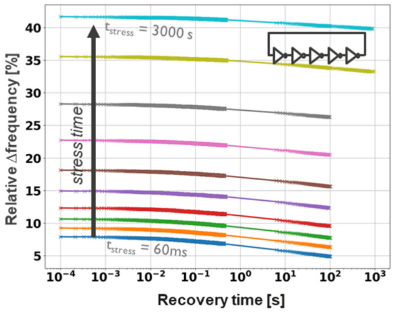

Figure 8 Dynamic frequency relaxation data over 7 decades, illustrating monotonic degradation increase (black arrow) w.r.t. stress time for dynamic stress at 2.4 V and 0.9 V recovery.

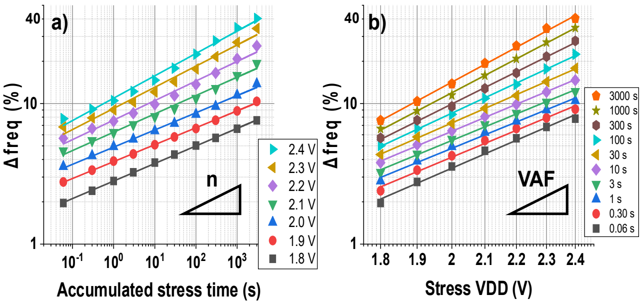

Figure 9. Power law dependence of the RO Δfreq (%) as a function of (a) the accumulated stress time and (b) the stress voltage for dynamic degradation. n and VAF are extracted from these data.

These dependences can be expressed through the time exponent *n* and the voltage acceleration factor *VAF* for a power law degradation model ($\Delta freq = A\cdot t_s^n\cdot VDD^{VAF}$), as shown in Figs. 10(a) and (b). The time exponents at the lower stress voltages are very similar for both static and dynamic degradation.

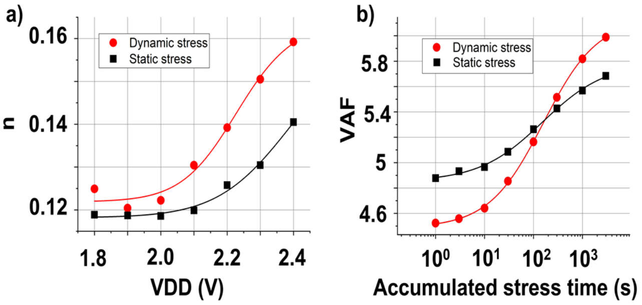

Figure 10. (a) Dependence of *n* on stress *VDD* and (b) of *VAF* on the accumulated stress time. Symbols are data, lines are fittings.

Furthermore, the relaxation behaviour observed for the dynamic stress (Fig. 11), can be well fitted with a universal BTI recovery model [9] at lower stress voltages, e.g., 1.8 V, as shown in Fig. 11(a). On the contrary, for higher stress voltages, for instance 2.4 V, the universal BTI recovery does not fit the data due to the impact of the HCI component, as shown in Fig. 11(b), where fitting lines deviate from experimental data. These two observations indicate that BTI is the predominant degradation mechanism in the dynamic stress at lower voltages, while HCI gains importance at higher ones [7],[20]. For the static stress, the relaxion behaviour follows the universal BTI recovery model for all stress biasing conditions [9].

By fitting the *n* and *VAF* parameters to the experimental data, it is possible to construct a frequency degradation map that accurately replicates the collected data acquired in the characterization window of accelerated stress voltages and logarithmically distributed stress times, as shown in Fig. 12. Moreover, the experimental window can then be extrapolated to longer stress times and lower stress voltages. It can be noted from Fig. 12 that the degradation caused by the two types of aging phenomena is different, so that the triangulation of the degradation suffered by the two ROs and thus, the determination of the historic degradation of the circuit, is feasible.

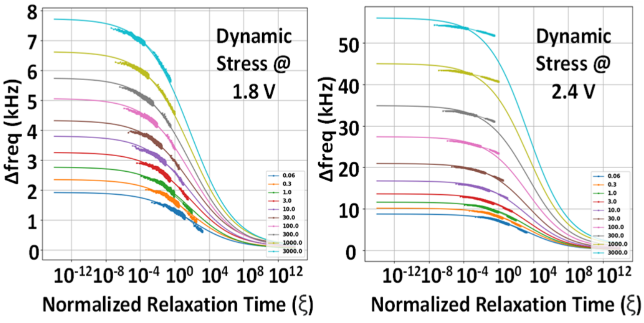

Figure 11. Frequency traces obtained during the relaxation phases of two dynamic tests at 1.8 V and 2.4 V of stress VDD, fitted according to the universal BTI recovery law [4]. Finally, relaxation phases of static degradation tests fit well the universal BTI recovery law for all stress VDD (not shown here).

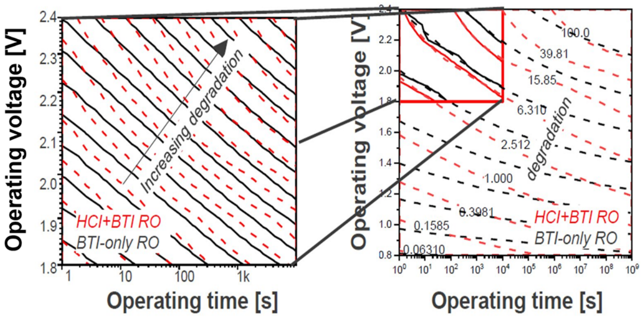

Figure 12. (left) example of degradation of a "HCI+BTI" and a "BTI-only" degraded ROs. The modelled degradation is a result of each mechanisms' particular time, voltage, and temperature activation. (right) extrapolation of the modelled data to operation voltages.

Currently, these two types of degradation may not be orthogonal enough to optimize the accuracy of such procedure. To further differentiate them, HCI should be enhanced under dynamic operation, for example, by increasing the capacitive load of each stage.

B. Tamper-aware annealing tests

As discussed in Section II, IC and circuit anneal can be used to tamper the status of the on-chip degradation monitors altering the obtained IC chip age so, old and/or refurbished chips can look as brand new. In this scenario, our set of pre-stressed monitors are designed to act as a flag when high temperature anneal tampering occurs. To this end, after the accelerated degradation, all overstressed ROs have undergone a series of annealing cycles, as described in Section III C. After each anneal cycle, the ROs are characterized at room temperature and the relative ΔFrequency degradation is obtained. These results are detailed in Fig. 13, showing the relative ΔFrequency of the ROs right after the degradation, and after each anneal phase, for two of the stress voltages (highest 2.4 V and lowest 1.8 V).

As depicted in Fig. 13, for both static and dynamic RO stress modes, the relative frequency reduction due to recovery at room temperature for 36 h is relatively small (~10% for static and ~5% for dynamic). Nevertheless, raising the annealing temperature to 200 °C for 12 h results in a strong anneal of the pre-stressed monitors.

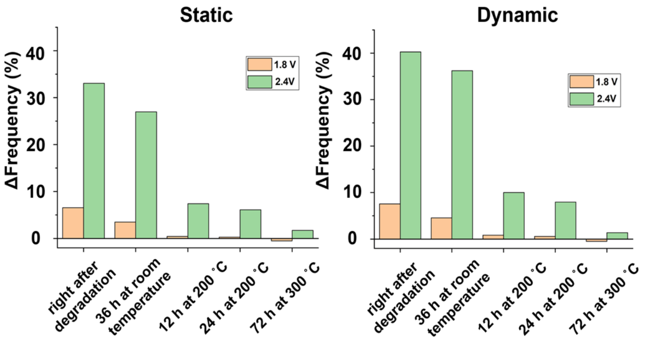

Figure 13. Average frequencies for ROs degraded at 1.8 V and 2.4 V in static and dynamic stress modes, right after stress, after a 36 h of relaxation at room temperature, after 12 h and 24 h of annealing at 200 °C and after 72 h of strong annealing at 300 °C.

It is important to note that conducting a subsequent anneal at the same temperature but, doubling the annealing time does not contribute much to the RO relative ΔFrequency annealed level. Finally, a strong anneal cycle has been executed by increasing the temperature to 300 °C, as well as the experiment time to 72 h.

Results have shown that a significant reduction of the previously pre-stressed ΔFrequency can be achieved by high temperature annealing. For instance, highly pre-stressed RO monitors at 2.4 V, that reached ~40% degradation for dynamic and ~30% for static, can be almost completely annealed out. Moreover, as shown in Fig. 13, pre-stressed RO monitors at lower stress voltages of 1.8 V, result in an almost complete ΔFrequency recovery after 36 h of anneal at 200 ºC and that after high temperature anneal the ΔFrequency is completely annealed out even going below 0%. That clearly indicates the importance of the highly pre-stressed RO monitor to detect high temperature fraudulent anneal procedures to discard tampered chips by the end users.

The relaxation observed in our room temperature and annealing experiments for dynamic and static stress for V_{DD} = 2.4 V and 3,000 s of accumulated stress are summarized in Table I. According to the relaxation behaviour shown in Fig. 4, BTI is expected to recover considerably more than HCI at room temperature, although the amount of expected recovery almost equalizes at high (e.g., 300 °C) temperatures. As depicted in Table I, after room temperature annealing, static degradation has recovered more than dynamic. After the complete annealing cycles, dynamically stressed ROs have been almost completely annealed out while a 10% of relaxation remains on the statically stressed ROs. These results confirm the difference in the recovery behaviour of the two types of degradation.

The orthogonality between the static and the dynamic RO recovery during anneal could be further emphasized through the enhancement of HCI phenomenon in dynamic stress operation, which would allow a better triangulation of the relaxation conditions. Furthermore, even if an accurate determination of these exact conditions could be challenging without such HCI enhancement, the proposed relaxation monitor could be unequivocally utilized as a tamper flag to detect on-chip fraudulent high-temperature annealing.

	36h **25 °C**	**12h** **200 °C**	**24h** **200 °C**	**72h** **300 °C**
Static	0.81	0.22	0.18	0.10
Dynamic	0.89	0.25	0.20	0.03

Table I. Relaxation behaviour after static and dynamic stress at VDD = 2.4 V and 3,000 s of accumulated stress. This stress voltage has been chosen since it is the one at which HCD is more significant in the dynamic degradation. As in Fig. 4, '0' means fully recovered, '1' means no recovery at all. While the recovery at room temperature is larger after static stress, recovery after dynamic stress becomes larger at higher temperatures. This orthogonality in behaviour could be used to retrieve the exact relaxation conditions and, ultimately, detect thermal annealing.

V. Conclusions

In this work, a new concept of on-chip tamper-detection degradation monitor capable of identifying fraudulent high-temperature annealing has been proposed. The proposed monitor utilizes two sets of ring-oscillator-based aging monitors: one to account for the physical age of the chip and another set of intentionally pre-stressed monitors utilized to detect fraudulent high temperature IC annealing.

The individual components of the proposed tamper-detection degradation monitor have been designed and fabricated in a commercial 28 nm 0.9 V technology. The novel and versatile array chip of addressable ring-oscillators incorporates a dedicated circuit design that ensures the ability to perform trustworthy ring-oscillator reliability characterization. The chip harbors sufficient ring-oscillator circuits with feedback loop control to allow the execution of accurate aging tests during static and dynamic ring-oscillator operation. The addition of an on-chip Force-&-Sense voltage biasing system ensures that, during variability characterization, on-chip voltage drops are mitigated, and all defined voltages are correctly applied to the test devices. The IC I/O transmission gates allow applying stress voltages to the ring-oscillator up to 2.4 V and sustaining up to 3 mA of DC current without significant degradation of the access circuitry.

Based on an extensive set of reliability tests, the degradation and recovery behaviours of the ring-oscillator aging monitors have been accurately acquired. By combining the only-BTI and an enhanced-HCI on-chip monitors data, the stress time and voltage conditions that a chip has undergone can be unveiled by the proposed triangulation procedure. Finally, dedicated high-temperature IC anneal controlled experiments have proven that accelerated ring-oscillator degradation can be almost completely recovered, making a used chip look as brand new. Nevertheless, as shown in this work, the latter recovery feature of intentionally pre-stressed ring oscillators will be used to unequivocally detect fraudulent IC high temperature anneal to discard tampered chips.

References

[1] 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," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1207-1228, Aug. 2014, doi: 10.1109/JPROC.2014.2332291.

[2] U. Guin, D. Forte and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233-1246, April 2016, doi: 10.1109/TVLSI.2015.2466551.

[3] X. Zhang and M. Tehranipoor, "Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 22, no. 5, pp. 1016-1029, May 2014, doi: 10.1109/TVLSI.2013.2264063.

[4] A. Dimopoulos, M. Sima and S. W. Neville, "Novel MOSFET Operation for Detection of Recycled Integrated Circuits," 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), 2018, pp. 1038-1041, doi: 10.1109/MWSCAS.2018.8623833.

[5] T. Kim, R. Persaud and C. H. Kim, "Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits," 2007 IEEE Symposium on VLSI Circuits, 2007, pp. 122-123, doi: 10.1109/VLSIC.2007.4342682.

[6] J. Keane, X. Wang, D. Persaud and C. H. Kim, "An All-In-One Silicon Odometer for Separately Monitoring HCI, BTI, and TDDB," in IEEE Journal of Solid-State Circuits, vol. 45, no. 4, pp. 817-829, April 2010, doi: 10.1109/JSSC.2010.2040125.

[7] N. E. C. Akkaya, B. Erbagci and K. Mai, "Combatting IC counterfeiting using secure chip odometers," 2017 IEEE International Electron Devices Meeting (IEDM), 2017, pp. 39.5.1-39.5.4, doi: 10.1109/IEDM.2017.8268523.

[8] D. -I. Moon et al., "Sustainable electronics for nano-spacecraft in deep space missions," 2016 IEEE International Electron Devices Meeting (IEDM), 2016, pp. 31.8.1-31.8.4, doi: 10.1109/IEDM.2016.7838524.

[9] T. Grasser *et al.*, "Simultaneous Extraction of Recoverable and Permanent Components Contributing to Bias-Temperature Instability," *2007 IEEE International Electron Devices Meeting*, 2007, pp. 801-804, doi: 10.1109/IEDM.2007.4419069.

[10] A. Bravaix, C. Guerin, V. Huard, D. Roy, J. M. Roux and E. Vincent, "Hot-Carrier acceleration factors for low power management in DC-AC stressed 40nm NMOS node at high temperature," *2009 IEEE International Reliability Physics Symposium*, 2009, pp. 531-548, doi: 10.1109/IRPS.2009.5173308.

[11] Stesmans, A., 1996. Passivation of P b 0 and P b 1 interface defects in thermal (100) Si/SiO2 with molecular hydrogen. Applied physics letters, 68(15), pp.2076-2078.

[12] M. Vandemaele, J. Franco, S. Tyaginov, G. Groeseneken and B. Kaczer, "Modeling of Repeated FET Hot-Carrier Stress and Anneal Cycles Using Si–H Bond Dissociation/Passivation Energy Distributions," in *IEEE Transactions on Electron Devices*, vol. 68, no. 4, pp. 1454-1460, April 2021, doi: 10.1109/TED.2021.3061025.

[13] E. Bury et al., "Statistical assessment of the full VG/VD degradation space using dedicated device arrays," 2017 IEEE International Reliability Physics Symposium (IRPS), 2017, pp. 2D-5.1-2D-5.6, doi: 10.1109/IRPS.2017.7936265

[14] E. Bury *et al.*, "Array-Based Statistical Characterization of CMOS Degradation Modes and Modeling of the Time-Dependent Variability Induced by Different Stress Patterns in the {V_G,V_D} bias space," *2019 IEEE International Reliability Physics Symposium (IRPS)*, 2019, pp. 1-6, doi: 10.1109/IRPS.2019.8720592.

[15] J. Diaz-Fortuny et al., "A Versatile CMOS Transistor Array IC for the Statistical Characterization of Time-Zero Variability, RTN, BTI, and HCI," in IEEE Journal of Solid-State Circuits, vol. 54, no. 2, pp. 476-488, Feb. 2019, doi: 10.1109/JSSC.2018.2881923.

[16] J. Diaz-Fortuny et al., "Flexible Setup for the Measurement of CMOS Time-Dependent Variability With Array-Based Integrated Circuits," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 3, pp. 853-864, March 2020, doi: 10.1109/TIM.2019.2906415.

[17] P. Saraza-Canflanca et al., "Design Considerations of an SRAM Array for the Statistical Validation of Time-Dependent Variability Models," 2018 15th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), 2018, pp. 73-76, doi: 10.1109/SMACD.2018.8434900.

[18] B. Kaczer *et al.*, "Ubiquitous relaxation in BTI stressing—New evaluation and insights," *2008 IEEE International Reliability Physics Symposium*, 2008, pp. 20-27, doi: 10.1109/RELPHY.2008.4558858.

[19] T. Grasser et al., "The Paradigm Shift in Understanding the Bias Temperature Instability: From Reaction–Diffusion to Switching Oxide Traps," in IEEE Transactions on Electron Devices, vol. 58, no. 11, pp. 3652-3666, Nov. 2011, doi: 10.1109/TED.2011.2164543.

[20] A. Kerber, T. Nigam, P. Paliwoda and F. Guarin, "Reliability Characterization of Ring Oscillator Circuits for Advanced CMOS Technologies," in *IEEE Transactions on Device and Materials Reliability*, vol. 20, no. 2, pp. 230-241, June 2020, doi: 10.1109/TDMR.2020.2981010.