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

Turki Alnuayri[1,2]
[1]*Dept. of Electrical Engineering & Electronics*
University of Liverpool
Liverpool, UK
t.alnuayri@liverpool.ac.uk
[2]*Dept. of Computer Engineering*
Taibah University
Medina, Saudi Arabia

Saqib Khursheed[1]
[1]*Dept. of Electrical Engineering & Electronics*
University of Liverpool
Liverpool, UK
ssk@liverpool.ac.uk

Antonio Leonel Hernandez Martinez[1]
[1]*Dept. of Electrical Engineering & Electronics*
University of Liverpool
Liverpool, UK
sgahern2@liverpool.ac.uk

Daniele Rossi[3]
[3]*Dept. of Information Engineering*
University of Pisa
Pisa, Italy
daniele.rossi1@unipi.it

***Abstract*—Integrated circuits (ICs) may be exposed to counterfeiting due to the involvement of untrusted parties in the semiconductor supply chain; this threatens the security and reliability of electronic systems. This paper focusses on the most common type of counterfeiting namely, recycled and remarked ICs. The goal is to develop a technique to differentiate between new and recycled ICs that have been used for a short period of time. Detecting recycled ICs using aging sensors have been researched using sub-threshold leakage current and frequency degradation utilizing ring oscillators (ROs). The resolution of these sensors requires further development to accurately detect short usage time. This paper proposes a differential aging sensor to detect recycled ICs using ring oscillators with sub-threshold leakage current to detect aging effects using bias temperature instability (BTI) and hot carrier injection (HCI) on a 22-nm CMOS technology, provided by GlobalFoundries. Simulation results confirm that we are able to detect recycled ICs with high confidence using proposed technique. It is shown that the discharge time increases by 14.72% only after 15 days and by 60.49% after 3 years' usage, and outperforms techniques that use frequency degradation only, whilst considering process and temperature variation.**

Keywords— counterfeit ICs, aging sensor, recycled and remarked ICs, subthreshold leakage current, green ICT.

I. Introduction

Due to the global spread of semiconductor supply chain, design complexity and involvement of untrusted parties, counterfeiting of integrated circuits (ICs) poses major risks to security and reliability of electronic systems, concerning consumers, industries, and governments across a wide variety of domains. Untrusted parties, such as vendors, fabricators and assemblers, could be involved in the supply chain businesses affiliated with ICs [1]. In electronics, the term counterfeit refers to an unauthentic copy that does not match the design of original component manufacturer (OCM) and performance; this happens if the OCM produces unauthentic copy or unauthorised contractors produce it in order to market it as new [1]. Due to globalization, electronic components manufacturing processes are spread around the world, from design to fabrication, assembly, packaging and distribution [1]. Each stage could be exposed to counterfeit, including the end of component life of ICs. Electronic counterfeit impacts negatively the global industry, becoming a significant danger for critical systems due to malfunction and high cost for medical, military and aerospace electronics, which are essential for public health, national security and the economy [1]. Furthermore, counterfeiting generates unfair competition for intellectual property (IP) owners and criminal financing sources [2]. There are many types of counterfeit ICs, such as recycled, remarked, overproduced, cloned, out-of-spec/defective, ICs with forged documentation and tampered [1]. This research is focused on the most common types of counterfeiting, namely recycled and remarked ICs. The term recycled ICs means a component recovered from an old system and modified in order to be remarked as a new component distributed by the OCM [3]. Electronic component package markings are used to identify (ID) the originality of component and functionality, however it could be an old component in which the old markings are hidden and the component is remarketed as a new component or could also be a new component that is remarked to improve its grade to earn a higher profit [3].

The Information Handling Services (IHS) reported [4] that the number of incidents of counterfeit IC components in the supply chain increased from 324 to 1363 between 2009 and 2011. The United States (US) Department of Commerce found that 55% of microcircuit producers discovered counterfeit components in their products between 2005 and 2008 [1]. However, this statistic was reported in 2009, when only 25% of electronic waste in the US was thoroughly recycled [1]. The most common IC counterfeiting methods found in the industry are recycling and remarking, comprising 80% of counterfeiting incidents in the world [1-4]. It is estimated that these components cost the semiconductor supply chain market around USD 169 billion per year, as reported in 2011 and IC recycling alone costs around USD 20 billion per year [1-3].

II. Related Work

The detection and avoidance measures for recycled and remarked counterfeit ICs, is addressed by researchers based on four classifications [5]: 1) physical and electrical inspection methods, 2) data analysis 3) track and trace methods and 4) aging degradation sensors, which is the main focus of this paper. A considerable amount of studies propose detection of aging phenomena on ICs to ensure reliability. In [6] the measuring of NBTI and TDDB is proposed with an independent structure for each aging phenomenon. The first silicon odometer was introduced with on-chip ring oscillators (ROs) to capture the degradation induced by NBTI [7]. The silicon odometer in [7] was improved by [8] to be able to detect aging degradation caused by NBTI and HCI. Another technique was proposed based on a statistical measurement system, which utilizes an-array based odometer ROs to detect aging degradation [9]. The above-mentioned techniques [6-9] were proposed between 2008 and 2011 using ring oscillators (ROs) as sensors to measure the aging degradation, but not for the recycled ICs detection [5], which requires high accuracy. In 2012 first lightweight ROs-based sensor was presented in [10] to detect chip usage in the field, motivated by [7] and followed by an improved version in 2014 that consists of counters and an antifuse memory block to continuously record and store usage time [11].

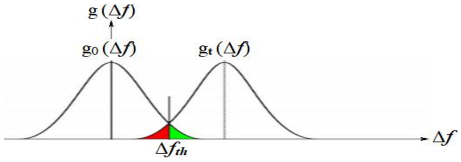

Fig. 1: Probability density function of frequency differences (*Δf*) between reference ring oscillator at time 0 (g_0(*Δ f*) and stressed ring oscillator at time *t* of usage (g_t(*Δ f*)) [5].

In 2016, Guin et al. [5] proposed three combating die and IC recycling sensors (CDIR): NBTI-aware CDIR, selection (SN-CDIR) and averaging (AN-CDIR). The recycled IC detection usage time was one month for the Original-CDIR model in 2012 [10] and in the NBTI-aware CDIR [5] improved to become three days with 100% of workload, but with a misprediction rate caused by frequency distributions overlapping between reference ring oscillator (RRO), detecting new RO as recycled (green) and stressed ring oscillator (SRO), detecting recycled RO as new (red) as shown in Fig.1 [5]. Other two versions of the NBTI-aware sensor were introduced to improve mispredictions, implementing multiple RO-pairs into an AN-CDIR based on averaging and into a SN-CDIR based on a selection algorithm. Nevertheless, such proposals increase area overhead. All the CDIR sensors proposed in [5] consisted of a RRO and a SRO. The RRO remains quiet until it is required for authentication and SRO is stressed during the entire operation time. Only half of the SRO inverters were stressed under NBTI in the Original-CDIR [10]. The NBTI-aware (N-CDIR) stressed all inverters in the SRO in order to collect all data on aging degradation [5].

Aging degradation sensors exploit properties of ICs, for example, when testing the operation speed of an aged IC, it is expected to operate at a slower speed in comparison to a new device, due to aging effects [12]. The aging sensor requires a gold-standard model, which provides the reference for measurements [13]. This could be done by implementing the sensor in a new chip to extract the reference measurement in similar conditions to the chip under test. The detection of recycled ICs has been investigated through aging-based sensors using sub-threshold leakage current and frequency degradation from ring oscillators (ROs) [13]. Path-delay fingerprinting was first introduced in [14] to detect hardware Trojans and later used by [15] to detect recycled ICs. A coarse-grained aging sensor is proposed in [13] to detect recycled ICs, utilising the power-gate infrastructure present in circuits. Such sensor is designed to detect the increase in power discharge time of virtual power (V_{Vdd}) network for sleep transistors, which occurs when a circuit is entering the sleep condition as a result of a decrease in subthreshold leakage current in the power-gated circuit that makes the aging process beneficial for static power consumption [16] . The sensor exploits the exponential correlation between the transistor threshold voltage (V_{th}) increase and the subthreshold leakage current decrease, which results in the discharge time (τ_{dv}) increase over time caused by aging effects of BTI, as can be seen in equation (1) [13]. The discharge time is defined as the time that the voltage takes to drop until 10% of the supply voltage [17].

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

Where L and W is the transistor channel length and width respectively, 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.

III. Proposed method

This section presents the differential aging sensor on-chip to detect recycled ICs by measuring discharge time increase of the subthreshold leakage current due to aging phenomenon. This research study investigates the most frequent aging phenomena of BTI and HCI, utilising a recent CMOS technology library of 22 nm provided by GlobalFoundries (GF). All proposed techniques in [5, 10, 15, 17] use ROs frequency degradation to monitor recycle ICs usage with aging, but recent studies have also shown feasibility of using the subthreshold leakage current (I_{subth}) to detect recycled ICs with lower robustness to process variation (PV) [13]. The I_{subth} decreases due to aging and the discharge time increases, providing a higher detection rate than frequency degradation. In available methods, PV requires further investigation and this paper addresses PV issue by incorporating two copies of ring oscillators (RRO and SRO) that are identical at time 0 (fresh device), considering intra-die (within die) process variation. The proposed sensor is highly accurate and focuses not only on recycled IC detection but also considers common issues in aging sensors that could affect detection results, including process and temperature variation. In addition, our proposal utilizes a new parameter to detect recycled ICs, which is the transistor subthreshold leakage current that provides significant improvement in detection rate, when compared with [5], which has similar configuration but with lower detection rate using the frequency parameter. The proposal has a lower area overhead as only two ROs have been used (RRO and SRO), whereas in [5] detecting the age of an IC with two ROs is achieved using the frequency parameter but with misprediction area (overlapping) as explained in Fig.1. To solve this issue, [5] introduced multiple pairs of ROs, having the cost of higher area overhead and lower percentage rate when compare to our proposal.

The structure of the proposed differential aging sensor consists of the following components (Fig. 2): two identical fresh copies of 51-stage ROs at time 0, with same design parameters of node capacitance and resistance, placed on the silicon beside each other in order to minimize the effect of PV and temperature, a counter and a timer for measuring the RO discharge time when its required for authentication [5]. Readings of the RO output can be made accessible using a multiplexing technique from the existing primary output, which is commonly available on-chip [5]. Furthermore, this proposal does not require extra hardware, since ROs are already present in modern chips for process monitors, as well as on-chip memory, timer and counter for collecting measurements, nevertheless this overhead is small in cases where such infrastructure is not available [18-19]. Selecting ROs from the same die and design parameters should minimize the discharge time difference ($\Delta\ \tau_{\mathrm{dv}}$) between the RRO ($\tau dv_{RRO_0}$) and the SRO ($\tau dv_{SRO_0}$) at time 0. The output of the RO is read when RO turns-off and that let the nodes to discharge through the leakage current, which is the discharge time of the group of inverters.

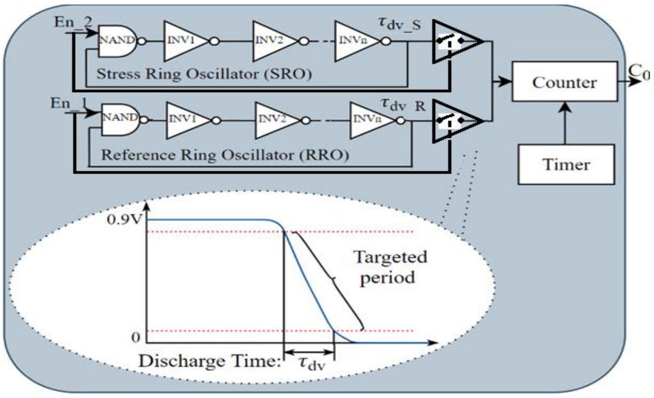

Fig. 2: The proposed aging sensor structure based on two ROs.

As a result, introducing discharge time as a parameter for the differential aging sensor provides higher detection rate compare to frequency and reduce PV impact. During the registration, RRO (τdv_{RRO_0}) will be read (at time 0) during manufacturing and stored by on-chip memory along with measurement conditions such as: supply voltage and operating temperature. The SRO is stressed (ON) during the entire operation time to allow a longer capture window and to increase the resolution of detected aging. The RRO remains turned-OFF and turned ON only if it is required for authentication. Even the RRO is turned OFF, saving fresh RRO (τdv_{RRO_0}) in on-chip memory, the effect of PV is minimized during operation time. Algorithm 1 shows step by step the authentication process.

Algorithm 1. Proposed sensor authentication.

```
START TEST
Initialise authentication
At time t, measure $\tau dv$ from SRO and extract $\tau dv$
stored at time 0 from on-chip memory using RRO.
$\Delta\tau dv = \tau dv_{SRO} - \tau dv_{RRO}$
If $\tau dv_{SRO} \leq \tau dv_{RRO}$
    then is a new IC
    else is recycled IC
END OF TEST
```

IV. Simulation Results And Discussion

The reliability analysis was performed using 22-nm CMOS technology library and aging models provided by GlobalFoundries. RelXpert (Cadence) was used for ICs degradation due to aging effects: NBTI, PBTI and HCI combined. It is crucial to consider that different types of stress and degradation could be introduced to ICs due to changes in the switching activity and operating conditions. Simulations were configured with the following parameters: age time from 15 days up to 3 years, with a supply voltage V_{dd} of 0.9 V, with temperatures of 25°C, 50°C and 75°C. Under these conditions 40 samples were collected for each simulation, in order to produce high-resolution data. The reliability analysis demonstrates the discharge time increase due to aging. Table I shows the discharge time results for 51-stage RO at a temperature of 25°C, and with usage time from 15 days up to three years. In addition, Table I reports τdv from RRO and SRO in nanoseconds (ns) due to aging effects, which demonstrates the increasing trend of discharge time from SRO. The $\Delta\tau dv$ calculates the difference between fresh RRO (t= 0) and aged SRO (t of usage) for 51-stage RO and represented as percentage by % τdv. In a working condition at 25°C, τdv reaches 19.66% after one month of usage and 60.49% after three years, which represent an increase of 3x.

TABLE I
51-Stage RO Discharge Time Increase Due To Aging At 25 °C

Age Time (months)	Fresh τdv (ns)	Aged τdv (ns)	Δ τdv (ns)	τ_{dv} % Increase
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.3 shows discharge time (orange) of 51-stage RO, which increases over three years, and frequency degradation (blue) that demonstrates relatively less degradation over the same period of time at 25°C. The temperature variation is undertaken in this paper in order to avoid misreading the age of an IC with a false negative prediction, which is common is nanometre technology nodes.

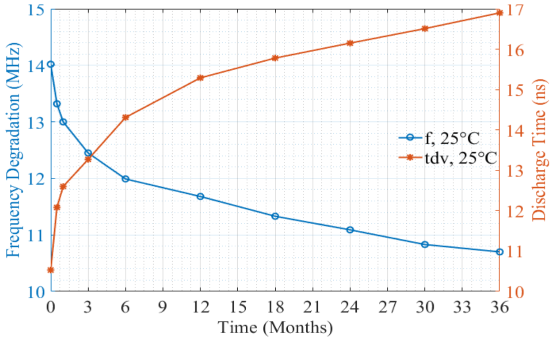

Fig. 3: 51-stage RO frequency and discharge time samples at 25°C.

Table II reports discharge time and frequency degradation at temperatures of 25°C, 50°C and 75°C for 51-stage ROs over various operation times. First column represents accelerated simulation time in months and next columns represents the τdv percentage increase for each temperature, showing a highest increase in τdv of 143.38% after three years of operation, whereas f reaches 34.59%. This trend confirms that I_{subth} leaks slower with aging and causes an increase in the discharge time [20].

TABLE II
51-RO Discharge Time And Frequency In % At 25°C, 50°C And 75°C

Age Time (months)	Discharge time τdv (%)			Frequency Degradation (%)		
	25°C	50°C	75°C	25°C	50°C	75°C
0.5	14.72	20.12	29.82	5.00	6.42	8.06
1	19.66	27.09	40.03	7.28	9.34	11.63
3	26.02	39.53	58.53	11.20	14.19	17.33
6	35.90	55.47	81.82	14.48	18.19	22.04
12	45.20	68.02	104.31	16.69	20.83	25.11
18	49.86	74.30	115.95	19.19	23.75	28.39
24	53.37	79.53	124.72	20.90	25.82	30.81
36	60.49	91.28	143.38	23.68	29.10	34.59

Fig. 4 shows the frequency (*f*) degradation (blue lines) and discharge time (τdv) results (orange lines) for 51-stage RO with three representative 75°C over a period of 3 years. These results demonstrate that τdv provides high confidence as aging indicator and therefore for the proposed differential aging sensor to achieve a better detection rate, when compared with frequency degradation [13].

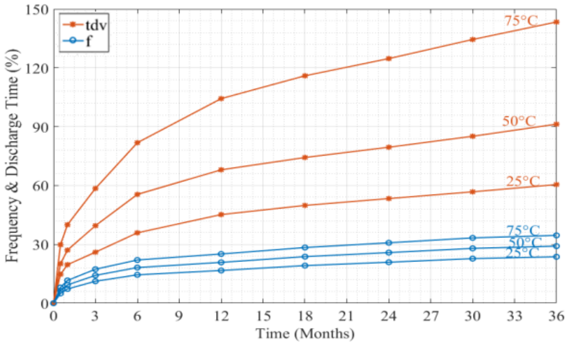

Fig. 4: 51-stage RO percent change of discharge time versus frequency degradation for 3 representative temperatures over 3 years.

Comparing τdv and *f* results from Table II, it can be seen that the latter shows a slower decreasing trend in time, whereas τdv increases more rapidly due to aging. For instance, Fig. 4 shows that at 25°C and after 15 days of usage, the τdv is 14.72%, whereas the *f* is 5 %. Moreover, at 75°C after 3 years of usage, τdv shows a change of 143.38% and *f* changes by 34.59%, demonstrating that the former changes 4.15 times and therefore offers higher confidence than frequency degradation, thus is more suitable to be used as aging sensor, which enables the detection of recycled ICs over short period of time (15 days onwards).

V. Conclusion And Future Work

A differential aging sensor is proposed in this paper to detect recycled ROs using discharge time measurements. The design involves a reference ring oscillator (RRO) and stressed ring oscillator (SRO) to measure the differences in subthreshold leakage current with aging. The proposed sensor exploits sub-threshold leakage current to measure the discharge time changes over usage time under aging effects of BTI and HCI combined. Having two ROs to tackle PV intra-die (within die), robust results are shown, even with temperature variation and over short duration of usage (15 days onwards). Using 22-nm CMOS library and aging models provided by GlobalFoundries, it is shown to provide better detection ability than frequency degradation method, whilst considering process and temperature variation. A future approach for this research would be further investigating PV (inter-die: die-to-die, wafer-to-wafer, lot-to-lot) and further validation of proposed approach.

VI. Acknowledgments

We would like to acknowledge the funding support received from The Department of Computer Engineering, Taibah University, Medina, Saudi Arabia, The Department of Electrical Engineering and Electronics, University of Liverpool, UK, Consejo Nacional de Ciencia y 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.

VII. References

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

[2] F. J. Domenic and C. Subhra Rajat. (2018). Counterfeit Integrated Circuits: Threats, Detection, and Avoidance. Available: https://ches.iacr.org/2018/slides/ches2018-tutorial1-slides.pdf.

[3] S. Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learning Approach. Morgan Kaufmann, 2018.

[4] J. Cassell, "Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security," IHS Markit.Retrieved February, vol. 11, pp. 2019, 2012.

[5] U. Guin, D. Forte and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," IEEE Transactions on very Large Scale Integration (VLSI) Systems, vol. 24, no. 4, pp. 1233-1246, 2016.

[6] E. Karl, P. Singh, D. Blaauw and D. Sylvester, "Compact in-situ sensors for monitoring negative-bias-temperature-instability effect and oxide degradation," in 2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers, 2008, pp. 410-623.

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

[8] J. Keane, X. Wang, D. Persaud, and C. H. Kim, “An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB,” IEEE J. Solid-State Circuits, vol. 45, no. 4, pp. 817–829, Apr. 2010.

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

[10] X. Zhang, N. Tuzzio, and M. Tehranipoor, “Identification of recovered ICs using fingerprints from a light-weight on-chip sensor,” in Proc. 49th ACM/EDAC/IEEE Design Autom. Conf., Jun. 2012, pp. 703–708.

[11] 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.

[12] Tenentes, Rossi, Yang, Khursheed, Al-Hashimi, Gunn, “Coarse-grained online monitoring of bti aging by reusing power-gating infrastructure", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume: 25 , Issue: 4 , April 2017.

[13] D. Rossi, V. Tenentes, S. Khursheed, and S. M. Reddy. “Recycled IC detection through aging sensor”. 2018 IEEE 23rd European Test Symposium (ETS), , Bremen, pp. 1- 2, May 2018.

[14] Y. Jin and Y. Makris, “Hardware trojan detection using path delay fingerprint”, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, pp. 51-57, June 2008.

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

[16] Rossi ; Tenentes ; Yang ; Khursheed ; Bashir M. Al-Hashimi, “Aging Benefits in Nanometer CMOS Designs”, IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 64, no. 3, pp. 324-328, March 2017.

[17] S. Khursheed, S. Yang, B. M. Al-Hashimi, X. Huang, and D. Flynn, “Improved dft for testing power switches”, 2011 Sixteenth IEEE European Test Symposium, Trondheim, pp. 07-12, May 2011.

[18] E. O. Sugasawara, “Process monitor circuitry for integrated circuits,” Sep. 26 2000, US Patent 6124143.

[19] R. Bach, “Process monitor with statistically selected ring oscillator,” Apr. 8 2003, US Patent 6,544,807.

[20] B. Paulo Francisco and R. Perez Ribas, “Leakage current in sub-micrometer cmos gates”, Universidade Federal do Rio Grande do Sul, pp. 1-28, 2006.