On-Chip RO-Sensor for Recycled IC Detection

Sauvagya Ranjan Sahoo, Sudeendra K, A. Mahapatra, A.K. Swain, K.K.Mahapatra
National Institute of Technology, Rourkela
email:{*sauvagya.nitrkl, kumar.sudeendra, kmaha2*}@gmail.com

Abstract— **The presence of recycled IC in the supply chain impacts the reliability of electronics systems used in critical applications. This paper presents a ring oscillator (RO)-based sensor to detect the recycled ICs. Although, ICs are used for a short duration, the proposed sensor is able to detect it. In this paper the modified RO shows more sensitive to negative bias temperature stability (NBTI) aging mechanism. Simulations are carried out using 90 nm CMOS technology to validate efficiency of proposed sensor for detection of recycled IC. Further, the RO with more number of cascaded inverters can detect the ICs used for a few days.**

Keywords— **Ring Oscillator (RO); Recycling; Aging; process variation (PV).**

I. Introduction

In the modern times, the demand for reliability and security in chip design is increasing. Reliability and Security are the new tenets added to the chip design along with the traditional ones like power, performance and area. Further, globalization of semiconductor supply chain [1] from design to end-user induces some security issues. Vulnerable points in supply chain may lead to infiltration of counterfeit components by an adversary. Counterfeit parts damage both reputation and revenue of the chip maker. Further, a counterfeit IC affects the reliability and performance of the system in which they are used. It will be further catastrophic when used in critical applications.

A counterfeit IC [2] may be an unauthorized copy of original manufacturer or a part which is over produced in foundry, cloned design, and defective, out of specification, tampered, recycled or used IC. Recycled IC's are generally extracted from obsolete PCB's and packed as new IC's. Recycled IC's will enter the supply chain more easily than other types of counterfeit parts. The recycled or used ICs make for 80%-90% of all the reported counterfeiting incidents [3]. Further, as reported in [4], the number of recycled IC in supply chain increases with time.

A recycled or used IC generally recovered from a obsolete system or circuit boards and then sold as a genuine component. During recycling process [5], IC is removed from the PCB generally at very high temperature and then undergo processes like cleaning, repackaging and remarking is done to make it look like as a fresh/new IC. So a used/recycled IC possesses various defects like

- Electrical defects like resistive open/short
- Aging [6] related issues like performance degradation, out of specification behavior, etc.

The countermeasure against using recycled IC is required to prevent catastrophes in critical equipment used in defense, aerospace and medical etc., in order to avoid mission failure. It is essential to develop a novel on-chip anti-counterfeiting scheme which is capable of detection of recycled IC even it is used for short period of time. Further, the added on-chip mechanism must be cost effective.

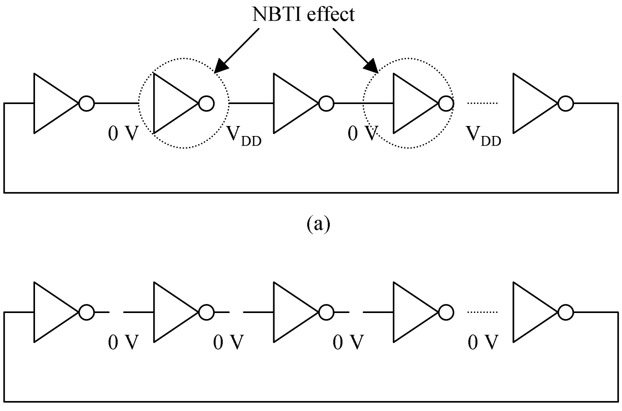
The rest of this paper is organized as follows, a brief discussion related to conventional recycled IC detection approach and impact of aging is given in section II. The architecture and recycled IC detection approach of the proposed modified RO sensor is briefed in section III. Simulation results are presented in section IV and finally we concluded in section V.

II. Preliminaries

When an IC is being used for a prolonged period then its performance degrades due to aging mechanism and this type of degradation is irreversible. So for detecting a recycled IC in the supply chain it is essential to understand the impact of aging upon IC.

Prior work to monitor the overproduction of IC coming out from the foundry includes metering techniques or assignment of unique ID to individual IC using PUF. Although hardware metering technique [7] prevents overproduction of IC but it is not a solution for recycled IC detection. A complete survey on different types of counterfeit IC detection is given in [2]. There are primarily three different counterfeit detection schemes: physical, electrical and aging based fingerprints. As aging is continuous and irreversible phenomenon, hence aging based approach is advantageous to use in detection of recycled IC. Although physical and electrical testing can be used for counterfeit IC detection but these techniques are more complex and time consuming. As aging causes permanent degradation in threshold voltage of MOSFET [6], so several threshold voltage dependent parameters like drain current, propagation delay etc. is used in several proposals [8-10, 13] to detect the recycled IC. In path-delay based fingerprint [8], the delay variation due to aging is used to detect the recycled IC. Although this approach does not consume additional power and area but it requires fingerprints from the golden IC to detect the recycled IC. A support vector machine (SVM) based recycled IC detection is proposed in [9], which requires measurements from golden IC to train SVM. Similarly dynamic current variation [1] in the symmetrical path is used to detect the recycled IC. In all the above techniques the test engineer requires measurement from golden IC comes out of the foundry. Instead of relying on golden IC, sensor based approach [10, 13] is used to detect the recycled IC.

A sensor based approach for recycled IC detection is proposed in [10]. It uses a RO-based on-chip sensor to predict the usage time of the recycled IC. The primary aging mechanisms like NBTI, HCI (Hot Carrier Injection) causes continuous degradation in threshold voltage of MOSFET and the rate of degradation increases depending upon the usage time. An on-chip RO based NBTI monitoring technique is proposed in [11, 12]. Due to the impact of NBTI, distributed ROs in the fresh IC and recycled IC possess difference in oscillation frequency and the difference increases with increase in usage time. This approach is used to design the RO-based sensor [10], which consists two RO i.e. reference RO and a stressed RO. The stressed RO is subjected continuous NBTI by driving it into non-oscillating mode and the reference RO is cutoff from supply voltage to avoid any aging due to NBTI. During authentication mode the oscillation frequency of both the RO is compared to predict the usage time of recycled IC/ chip under test (CUT). A control module generates necessary control signal to increase the aging of stressed RO and enables both the RO for frequency comparison during authentication mode. Larger frequency difference between both the RO shows higher usage time for CUT. Although, recycled IC detection is more efficient by this approach but it can detect only the ICs used for a long period of time (for a period of few months). A new RO-based sensor is proposed in [13], which exploits the aging more efficiently to detect the ICs used only for few hour/day called as NBTI aware RO-sensor. The basic difference between both the architecture (in [10] and [13]) is the way of adding more NBTI stress into the RO as shown in Fig.1.



(a)

(b)

Fig. 1. (a) NBTI effect on RO [10] (b) all inverters are under NBTI stress [13]

In the case of RO-based sensor [10] (Fig.1 (a)) half of the PMOS experience NBTI whereas in [13], all the PMOS experience NBTI. As a result the degradation in oscillation frequency is higher which led to detection of ICs used for a short duration of time. A detail analysis of NBTI impact on oscillation frequency of RO is given in the section III. Further, in order to detect the recycled IC which are used only for a short duration of time ROs are designed with large number of cascaded inverters [13].

(A) Aging Impact on IC

Aging is the primary cause for permanent degradation in the performance of IC over time. Once an IC is being used continuously on the board several aging sources affects its performance. Out of several aging sources [6] like NBTI, HCI, Electromigration etc., NBTI and HCI are the primary aging mechanism which causes significant degradation in the threshold voltage (V_t) of MOSFET. The dependency of V_t on aging is discussed as follows:-

1) NBTI

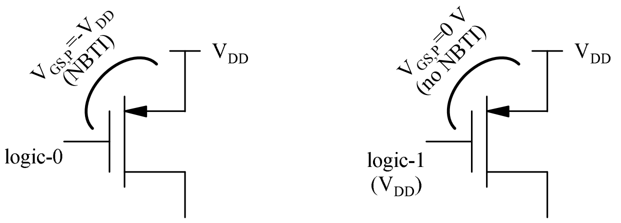


Fig. 2. NBTI effect on PMOS

NBTI causes degradation in the threshold voltage of PMOS when a continuous negative bias is applied across its gate to source terminal. The NBTI effect on PMOS is shown in Fig. 2. The negative bias ($V_{GS,P}$=-V_{DD}) causes few Si-H bonds to break as a result generates traps in the Si/SiO$_2$ interface. These traps led to shift in threshold voltage. After the removal of negative bias PMOS recovered its threshold voltage partially. The change in V_t due to NBTI [6] is:-

$$\Delta V_{t,stress} = A_{NBTI} t_{ox} \sqrt{C_{ox}(V_{DD} - V_t)}\, e^{\left(\frac{V_{DD}-V_t}{t_{ox}E_0} - \frac{E_\alpha}{kT}\right)} t_{stress}^{0.25} \qquad (1)$$

Where A_{NBTI} is a constant proportional to aging rate, t_{ox} is the oxide thickness, C_{ox} is gate capacitance per unit area E_0 and E_α are device dependent parameter, k is Boltzmann constant and t_{stress} is the duration of stress/aging.

From (1) when a PMOS experience continuous negative bias for larger duration (t_{stress}), the shift in its threshold voltage is higher results in overall performance degradation of CUT.

2) HCI

HCI occurs mainly in the NMOS devices by the energetic carriers generated due to logic switching or AC stress at its gate terminal. These energetic carriers creates trap in the gate dielectric led to non-recoverable shift in V_t of NMOS. The mathematical modelling of shift in V_t [6,14], given as follows

$$\Delta V_{t,HCI} = A_{HCI}\alpha f e^{\frac{V_{DD}-V_t}{t_{ox}E}} t_{stress}^{0.5} \qquad (2)$$

Where A_{HCI} is a constant depends upon aging rate, α is the activity factor, f is the frequency and E is a constant equals to 0.8 V/nm. The shift in V_t mainly depends upon switching activity at the gate terminal of NMOS and the duration of applied stress.

So both NBTI and HCI cause degradation in the threshold voltage of MOSFET and the rate of degradation increases with increase in stress duration.

III. Proposed RO Sensor

(A) Architecture

The architecture of the proposed RO sensor is shown in Fig. 3. The basic difference between the proposed architecture and conventional N-CDIR [13] sensor is the way the RO section undergoes aging. The proposed architecture consists of two RO i.e. RO with higher stress $(RO)_{HS}$ and RO with lower stress $(RO)_{LS}$. The function of $(RO)_{HS}$ and $(RO)_{LS}$ is similar to stressed RO and reference RO respectively. The supply voltage section for both the RO is designed in such a way that during stress mode both the RO undergoes different aging and in the authentication mode both the RO oscillates at same supply voltage. The frequency measurement section consist a counter (CNTR) and TIMER block which is similar to the conventional N- CDIR sensor [13].

(B) Operating Mode

A decoder is used to generate four different control signals for each mode of operation. The four different operating modes are represented in Table 1.

Table 1 Modes of Operation

Mode [M1M0]	SLP	$(EN)_{HS}$	$(EN)_{LS}$	RO_SEL	Function	
00	0	0	X	X	Sleep mode for both the RO	
01	1	0	0	X	Stress mode for both $(RO)_{HS}$ and $(RO)_{LS}$	
10	1	0	1	0	Authentication mode	Measure the frequency of $(RO)_{LS}$
11	1	1	0	1		Measure the frequency of $(RO)_{HS}$

1) Test Mode:

In the manufacturing or test mode (M1M0=00), both the ROs are driven into sleep mode i.e. cut-off from supply. Because in the test mode, CUT is subjected to a higher supply voltage/Temperature environment which led to additional aging. To prevent degradation due to aging, decoder enables the control signal SLP by assigning logic-0. For SLP=0, both the ROs are cut-off from supply voltage as a result experience no aging. The SLP remains at logic-1 in remaining operating modes to drive appropriate supply voltage into the RO section.

2) Stress mode:

The stress mode for both the RO is enabled for M1M0=01. The decoder generates necessary control signal (as shown in Table 1) to drive both the RO into non-oscillating mode and to inserts different amount of NBTI stress.

As SLP is at logic-1, it drives different supply voltage to the RO section i.e. V_{DD}-$V_{t,n}$ (where $V_{t,n}$ is the threshold voltage of NMOS) to the $(RO)_{LS}$ through NMOS (TN1) and V_{DD} to $(RO)_{HS}$ through PMOS (T_P). These two different supply voltages led to different amount of NBTI stress [6]. As a result both the RO exhibit different rate of degradation in oscillation frequency.

3) Authentication mode:

In the authentication mode (M1M0=10 or 11) the decoder generates the necessary control signals to measure the oscillation frequency (f_{osc}) of both the RO. In this mode both the RO oscillates at a supply voltage of V_{DD}-$V_{t,n}$. For M1M0=10, the decoder drives logic-0 to RO_SEL and logic-1 to $(EN)_{LS}$ to drive the $(RO)_{LS}$ into oscillating mode. $(RO)_{LS}$ starts oscillating at a scaling voltage of V_{DD}-$V_{t,n}$ through T_{N1} as SLP is at logic-1. Further, the f_{osc} of $(RO)_{HS}$ is measured in the mode M1M0=11. The decoder drives the $(RO)_{LS}$ into non-oscillation mode and $(RO)_{HS}$ into oscillation mode. The $(EN)_{HS}$ is driven to logic-1 to drive a scaling supply voltage of V_{DD}-$V_{t,n}$ through T_{N2}. The decoder drives logic-1 to RO_SEL to measure the f_{osc} of $(RO)_{HS}$.

The above different modes of operation clarifies that both the ROs are remain in non-oscillation mode throughout the life time and driven into oscillation mode only during authentication mode. Out of primary aging mechanism NBTI effect is more pronounced in the non-oscillating mode [14] results in degradation in f_{osc} over time.

(C) NBTI effect on RO

The RO in our proposed architecture is designed by using conventional CMOS inverter. The effect of NBTI on both the RO in non-oscillating mode is shown in Fig. 4. In the stress mode, $(RO)_{LS}$ is driven by a supply voltage scaling of V_{DD}-$V_{t,n}$ and $(RO)_{HS}$ is driven by a supply voltage of V_{DD}. As shown in Fig. 4, alternate logic 0 and 1 (V_{DD}) appears at the gate terminal of PMOS in the cascaded chain of inverter. The logic-0 at the input of the PMOS devices (in the cascaded inverter chain) results in a negative bias voltage across gate to source ($V_{GS,P}$). Due to supply voltage scaling the PMOS in the $(RO)_{LS}$ experience less negative bias ($V_{GS,P}$ = $V_{t,n}$ -V_{DD}) than the PMOS in the $(RO)_{HS}$, which experience a bias of $V_{GS,P}$= -V_{DD}.

Due to different amount of negative bias, degradation in threshold voltage of PMOS in $(RO)_{HS}$ is higher than $(RO)_{LS}$. As a result both the RO experience different rate of degradation in f_{osc}. Further, with increase in stress duration the difference in oscillation frequency of both the RO increases which helps in detecting a recycled IC through f_{osc} comparison.

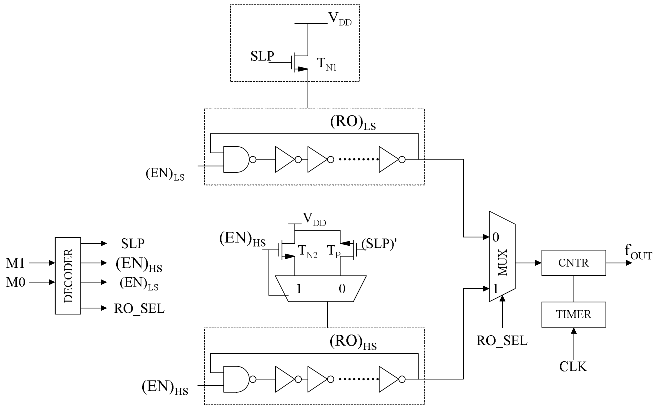
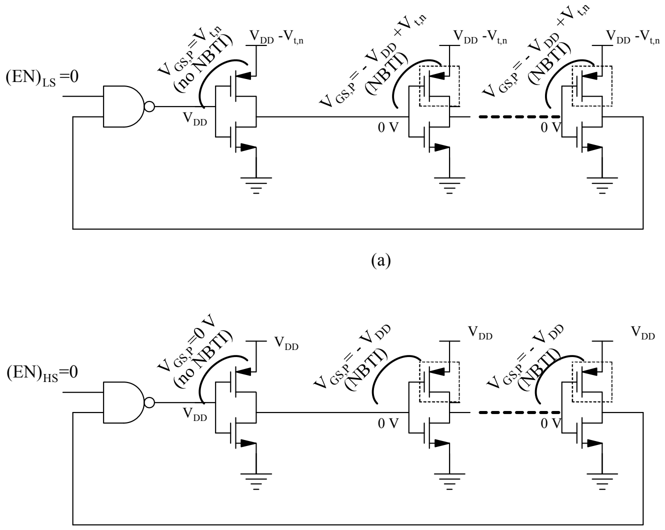


Fig. 3. Proposed Modified RO Sensor



(a)

(b)

Fig. 4. NBTI effect on (a) $(RO)_{LS}$ (b) $(RO)_{HS}$

(D) Registration and Authentication

The recycled IC detection procedure is divided into two parts, registration or fingerprint generation from a new sample of IC and authentication of recycled/used IC. Initially, the fingerprint is collected for the new IC by measuring the frequency difference between both the RO i.e. F_{DIF} = F_{LS} - F_{HS}. Where F_{LS} and F_{HS} is the oscillating frequency of $(RO)_{LS}$ and $(RO)_{HS}$ respectively. A set of frequency across samples of fresh IC is collected to measure the spread in F_{DIF}. Although both the RO oscillates at same supply voltage i.e. V_{DD}-$V_{t,n}$, the magnitude of F_{DIF} is approximately zero, but the manufacturing PV [14] causes slight difference is oscillation frequency. Further, this difference may be positive or negative. This variation in F_{DIF} across all samples is used to create the fingerprint for CUT. During the authentication phase if the F_{DIF} for the CUT is out OF the range of fresh IC sample then CUT is treated as a recycled IC otherwise it is assumed to be a fresh IC.

The spread in F_{DIF} for a group of fresh IC ($F_{dif,0}$) and aged IC ($F_{dif,T}$:after T-days) is shown in Fig. 5. If both the spreads are far apart then a recycled IC can be easily detected. The overlapping area between the spread in Fig. 5 indicates the unpredictable region i.e. in this region a recycled IC may be assumed as a fresh IC. Further, with rise in spread the number of samples of undetected recycled IC increases.

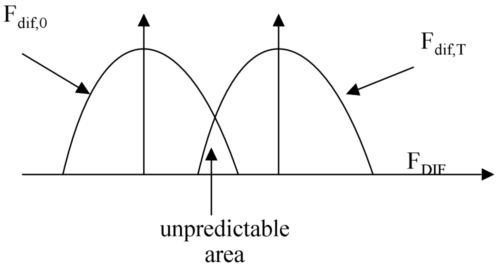


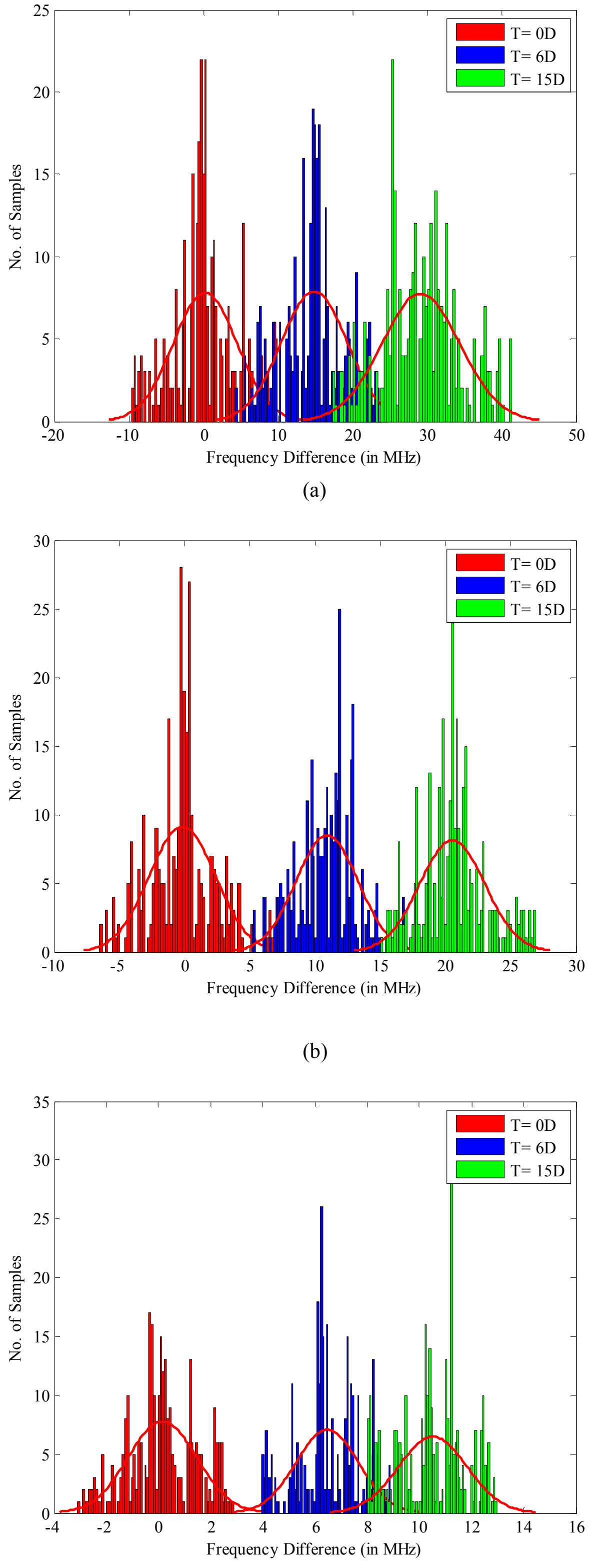
Fig. 5. Distribution of F_{DIF} for fresh IC and used IC

IV. Simulation Results & Discussion

The proposed modified RO sensor is implemented in Virtuoso environment, 90 nm CMOS technology library from UMC is used for simulation purpose. RelXpert simulator in virtuoso environment is used to measure the degradation in oscillation frequency of RO due to aging. Monte Carlo simulation with 300 iterations is carried out using statistical transistor model provided by foundry. The reason for using Monte Carlo run to measure the impact of process variation on the oscillation frequency of RO prior to chip fabrication. The f_{osc} from the fresh IC and aged IC is collected over multiple instances to predict whether the test IC is a recycled one or not. The simulation is carried out at a nominal supply voltage of 1V and 27^0C.

The simulation result for the proposed RO based sensor is shown in Fig. 6(a-c). The result shows variation in frequency difference for both fresh IC and recycled IC (which undergoes continuous aging). The F_{DIF} is measured at T=0D i.e. fresh sample of IC and the variation across 300 instances is shown in Fig. 6. The legend T=0D shows the variation in F_{DIF}. Ideally F_{DIF} should be zero but manufacturing PV causes each RO to oscillate at unique frequency which led to either positive or negative value of F_{DIF} (T= 0D in Fig. 6 (a-c)). As shown in Fig. 6 (a) the fresh IC has a spread from -10 to 10 MHz. Similarly F_{DIF} is measured after a stress interval of 6 and 15-days (D). For our analysis we have considered two aging instances (6D and 15D). In order to measure the F_{DIF} at different aging intervals, first both the ROs are undergoes continuous aging for a period of (6D and 15D) to extract the aged SPICE netlist. Finally, Monte Carlo simulation is carried out to measure the oscillation frequency of both the RO ($(RO)_{HS}$ and $(RO)_{LS}$) across multiple instances in order to calculate the spread of F_{DIF} after T=6D and 15D.

Fig. 6 (a) shows the spread in F_{DIF} after T=0, 6 and 15 days for the RO designed with 15 stages of cascaded inverter. As shown in the figure with increase in aging duration the magnitude of F_{DIF} (frequency difference between the RO) increases. The frequency difference bar chart shows overlap region between the two distribution of F_{DIF} i.e. $(F_{DIF})_{T=0}$ and $(F_{DIF})_{T=6D}$. This overlap region indicates a dilemma i.e. it is difficult to predict whether the CUT is a fresh or recycled one. Further, at T=15D there is no overlapping between the spread of $(F_{DIF})_{T=0}$ and $(F_{DIF})_{T=15D}$. The above simulation result confirms that at higher aging interval, a recycled IC can be easily detected without any error.



(a)

(b)

(c)

Fig. 6. Distribution of F_{DIF} (a) RO with 15 stage (b) RO with 25 stage (c) RO with 51 stage

Further, both the ROs are designed with more number of cascaded inverters i.e. 25 and 51 stages to measure the spread in F_{DIF}. The spread at different aging instances (6D and 15D) is shown in Fig. 6(b and c). The simulation result shows lower spread in F_{DIF} with increase in number of inverter stages. This reduction in spread is due to inverse relationship of spread in F_{DIF} with number of inverter in RO [13].

The spread in F_{DIF} is also lowered in all the considered aging instances i.e. $(F_{DIF})_{T=6D}$ and $(F_{DIF})_{T=15D}$. The simulation result shows that the spread for 51 stages of RO (Fig. 6(c)) is much narrower than both 15th and 25th stages. This narrower spread eliminates the overlapping region even at lower aging instance. As shown in Fig. 6(b), the overlapped area in the case of 25-stages RO between $(F_{DIF})_{T=0}$ and $(F_{DIF})_{T=6D}$ is less than that of 15-stages of RO. So the probability of incorrect prediction reduces significantly, whereas by using 51 stages RO there is no misprediction or unpredicted area for the aging instance of 6D (Fig. 6(c)).

Table 2 represents the number of samples in the overlap region between the proposed RO sensor and conventional RO sensor in [10]. The proposed RO sensor shows lower number of samples in the overlapped region than the conventional RO for equal aging duration. Further, with increase in number of stages less number of samples is found in the overlap region due to reduction in spread of F_{DIF}.

TABLE 2 MISPREDICTION COMPARISON

No. of stages in RO	Aging duration <T>	No. of samples in overlap region <in %>	
		RO sensor [10]	Proposed RO sensor
15	6D	11.27	7.25
25		6.26	1.38
51		1.25	0
15	15D	2.92	1.81
25		0.88	0
51		0	0

V. CONCLUSION

The proposed modified RO-sensor detects the recycled ICs used for a few days. The different amount of NBTI stress on RO results in generating higher frequency difference in a recycled IC than the fresh IC. In the proposed circuit, RO with more number of cascaded inverters increases the efficiency and the proposed sensor is able to detect an IC used only for a few days.

REFERENCES

[1] Yu Zheng, A. Basak and S. Bhunia, “CACI: Dynamic current analysis towards robust recycled chip identification,” *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1-6, 2014.

[2] 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, 2014.

[3] Businessweek. (2008). *Dangerous Fakes*, New York, NY, USA [Online]. Available: http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm.

[4] (2010). Bureau of Industry and Security, U.S. Department of Commence. *Defense Industrial Base Assessment: Counterfeit Electronics*[Online]. Available: http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

[5] B. Hughitt, “Counterfeit electronic parts,” in *Proc. NEPP Electron. Technol. Workshop*, 2010.

[6] A. Tiwari and J. Torrellas, “Facelift: Hiding and slowing down aging in multicores,” *in Microarchitecture, 41st IEEE/ACM International Symposium*, pp. 129-140, 2008.

[7] F. Koushanfar. *Hardware Metering: A Survey* [Online]. Available: http://aceslab.org/sites/default/files/05-fk-metering.pdf, 2011.

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

[9] K. Huang, J. M. Carulli and Y. Makris, “Parametric counterfeit IC detection via Support Vector Machines,” *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pp. 7-12, 2012.

[10] 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, 2014.

[11] 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, 2010.

[12] J. Keane, W. Zhang and C. H. Kim, “An Array-Based Odometer System for Statistically Significant Circuit Aging Characterization,” in *IEEE Journal of Solid-State Circuits*, vol. 46, no. 10, pp. 2374-2385, 2011.

[13] 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, 2016.

[14] S. R. Sahoo, S. Kumar, K. Mahapatra and A. Swain, “A Novel Aging Tolerant RO-PUF for Low Power Application,” *IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, pp. 187-192, 2016.