Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures

Mahabubul Alam*, Sreeja Chowdhury†, Mark M. Tehranipoor†, and Ujjwal Guin*
*Department of Electrical and Computer Engineering, Auburn University, AL
†Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL
{mahabubul.alam, ujjwal.guin}@auburn.edu, {sreejachowdhury, tehranipoor}@ufl.edu

***Abstract*—The continuous growth of recycled integrated circuits (ICs) poses a serious threat to our critical infrastructures due to their inferior quality and has become one of the major concerns to the government and the industry. Detection of these ICs is challenging especially when they have been used for a short period of time, as the process variations (especially in lower technology nodes) could outpace the degradation caused by aging. In this paper, we propose a robust, accurate, and low-cost solution for efficient detection of recycled ICs, even if they have been used for a very short period of time. The proposed solution utilizes a ring oscillator (RO), and a non-volatile memory. It stores the RO frequency, conditions (e.g., supply voltage, temperature, and duration) for the frequency measurement, and a digital signature. The simulation and silicon results demonstrate that we can effectively detect recycled ICs used as low as one day.**

***Index Terms*—Counterfeit ICs, Recycling, Remarking, Semiconductor Supply Chain, Secure Hash Algorithm (SHA), Digital Signature.**

I. Introduction

The counterfeiting of integrated circuits (ICs) continues to expand due to the astonishing rise of electronic waste in recent years. Information Handling Services Inc. reported that counterfeited ICs represent a potential annual risk of $169 billion to the global electronics supply chain [1]. Among all different counterfeit ICs, recycled ICs account for almost 80% of all the reported counterfeiting incidents [2]. The deployment of these recycled chips in a critical infrastructure will be catastrophic as they exhibit lower performance, and lower remaining useful lifetime [3]. In addition, the crude recycling process that consists of removal of the ICs from printed circuit boards (PCBs) under extremely high temperature followed by sanding, repackaging and remarking could potentially create many defects or anomalies [2], [4]. Moreover, the recycling process may also create latent defects that can pass initial acceptance testing by original equipment manufacturers (OEM) but are susceptible to failure in the filed [2].

The detection and avoidance approaches for recycled ICs are broadly classified into four different categories. First, there are several standards [5]–[8] in practice which recommend different physical and electrical tests for the detection purpose. The goal of these tests is to identify defects and anomalies (see details in Chapter 3 of [2]) present in those recycled and remarked ICs. However, there are severe limitations for implementing these tests due to prohibitively excessive test times, test costs, low detection capability, and lack of automation. Second, researchers have proposed several schemes based-on statistical data analysis [9]–[12]. However, these solutions provide limited accuracy when the chips are used for a short period of time, and often required authentic samples to train the model making it infeasible especially for high volume parts. Third, on-chip sensors have been proposed as an alternative to the conventional test methods for efficient detection of these ICs [13]–[17]. Unfortunately, these solutions can provide lower accuracy for designs manufactured with lower technology nodes due to increased process variations. Finally, DNA markings are commercially available to provide traceability for electronic parts [18]. However, a complex authentication process, excessive implementation, and test cost have made its application limited in practice [19].

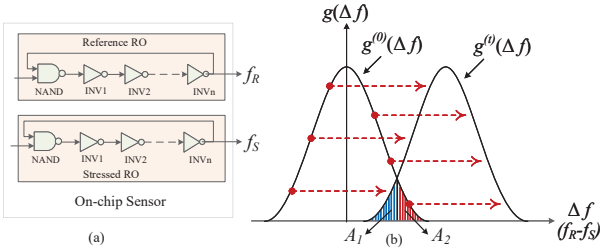

Figure 1: Loss of detection accuracy due to process variation.

A. Motivation

The on-chip sensors using ring oscillators (ROs) proposed in [13]–[16], can be ideal for the detection of recycled ICs if we can eliminate process variation during manufacturing. The frequency of the reference RO must remain constant during normal operation, whereas the frequency of the stressed RO reduces over time due to aging. The difference between these two frequencies determines the age of the circuit. Ideally, the frequencies of these two ROs should be same as they have been designed with same parameters. However, they would always differ due to process variations. In addition, the reference RO experiences some frequency degradation as the sleep transistors cannot prevent it from aging completely. These make the authentication process complicated and may result in false positives/negatives (a recycled IC identified as new (A_1), or a new IC identified as recycled (A_2)).

Figure 1 shows the distribution ($g(\Delta f)$) for new and recycled ICs. Here, g represents the distribution, and $\Delta f = f_R - f_S$ is the frequency difference between reference RO (f_R) and stressed RO (f_S). $g^{(0)}(\Delta f)$ and $g^{(t)}(\Delta f)$ represent the distributions for the new (time 0) and aged (time t) chips, respectively. The objective of these sensors is to reduce the overlapped areas (shaded by blue, A_1 and red, A_2), which represent the detection errors. As a result, the sensor fails to detect recycled ICs with high accuracy when the chip experiences a small amount of aging (larger overlapped region). In addition, we have also observed that the higher process variation increases the spread of the distribution,

which ultimately leads to larger inaccuracy [15]. To address these problems, the authors in [16] proposed an approach that significantly reduces the spread [16]. However, the solution requires large implementation overhead, and cannot eliminate the effect of process variation completely.

As the stressed RO becomes slower while the chip ages, the Δf distribution moves towards the right (see Figure 1). It is worth noting that the Δf for a chip always moves towards the right (highlighted in red dotted arrow) due to aging. If one stores the frequency of the stressed RO ($f_S^{(0)}$) of a new chip at an on-chip non-volatile memory (NVM), one can uniquely determine the age of the chip. Then, there is no need for a reference RO for comparison. However, an adversary could tamper the NVM content with the frequency ($f_S^{(t)}$) of the stressed RO of a recycled chip to pass the authentication. In this paper, we utilize digital signature comparison to detect any such tampering of the NVM content.

B. Contributions

The aforementioned issues motivate us to develop an on-chip structure that can detect recycled ICs effectively. The core of the proposed on-chip structure is utilizing a ring oscillator and a small non-volatile memory. The on-chip structure stores the RO frequency, the measurement conditions, and a digital signature [20] in the NVM. The proposed solution is:

- *robust* as the process variations do not affect the accuracy of the authentication process. Unlike previous approaches [13]–[16], no comparison is performed between different ROs to determine the usage of an IC. Our solution can detect recycled ICs accurately even if a chip was used for a very short period of time (e.g., aging due to manufacturing tests, burn-in, and in-system tests). Moreover, the integrity of NVM content is ensured by verification through digital signatures. Any tampering with the NVM content will be detected during the signature verification process.
- *low-cost* as the on-chip structure consists of a single RO and a small NVM. We do not require any additional overhead as ROs are commonly used in modern ICs to monitor process variation [21]–[23]. Note that no additional pin is required for frequency measurement as the same resource is available for process monitoring [21]. On the other hand, the measurement device only requires a counter and a timer. One can also use this resource from process monitor circuit [23] to measure the RO frequency.
- *accurate* for measuring RO frequency as the measurement error is much less than the degradation (see experimental results in Section III-B).

The rest of the paper is organized as follows: We present our proposed architecture in Section II. The proposed authentication scheme is also discussed in this section. In Section III, simulation and silicon results are presented to evaluate the effectiveness of the proposed scheme. In this section, we also analyze different attacks and their countermeasures. The concluding remarks are given in Section IV.

II. Proposed Approach for Recycled IC Detection

This section focuses on developing an on-chip structure, and a verification process based on a digital signature to detect recycled ICs.

A. Proposed On-Chip Structure

Figure 2 shows our proposed structure for detecting recycled ICs. Main components of the on-chip structure are an RO and an NVM. This RO can be selected from one of the process monitors [21]–[23] currently used in modern chips. The RO output can be made available using an existing primary output (PO) through multiplexing. We require a counter and a timer to measure the frequency of the RO. One can also use the existing on-chip counter and timer for RO frequency measurement [23]. The NVM is programmed with the registration data and a signature of the data (described in Subsection II-C). Test access port and boundary-scan architecture [24] can be used to access the NVM content.

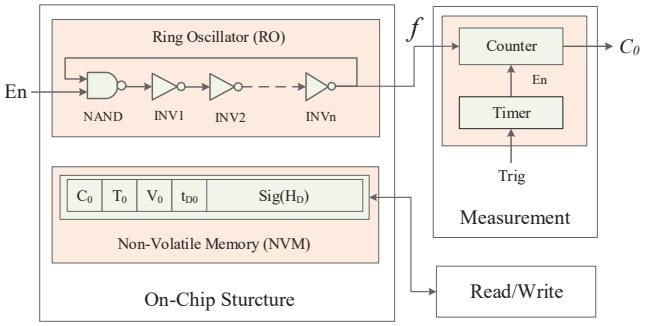

Figure 2: Proposed on-chip aging structure.

The proposed sensor requires one small non-volatile memory that has the capability to hold saved data even if the power is turned off. One can use electrically erasable programmable read-only memory (EEPROM), which is very common in modern chips. In our proposed sensor, the NVM will contain a data and a signature of that data to prevent tampering (discussed in detail in Subsection II-C). The data is formed by concatenating electronic chip ID ($ECID$), measurement conditions (e.g., supply voltage, temperature, and duration), and the counter value. $ECID$ is widely popular to provide an identification of the chip, and now a requirement for all new application specific integrated circuits (ASIC) [25]. This ID can easily be accessible through test access port (TAP) [24]. The conventional approach for creating $ECID$ includes writing the unique ID into a non-programmable memory (One-Time-Programmable (OTP), ROM, etc.) or using post-fabrication external programming techniques, such as laser fuses [26] or electrical fuses (eFuses) [27]. Note that $ECID$ cannot be modified easily once it is programmed into the chip.

The authentication of the devices can be done at any point of the supply chain with a very low-cost measuring device. The measurement of the cycle count of the ring oscillator for a fixed time interval can be implemented with a timer IC and a counter (see Figure 2). A trigger input ($Trig$) is used to start the measurement process.

B. Generation and Verification of Digital Signatures

Digital signature is a widely used to ensure message integrity and end-point authentication. Message integrity verification is necessary in order to find whether the message has been modified, whereas end-point authentication ensures the origin of the message. Public key cryptographic primitives, such as, Rivest-Shamir-Adleman (RSA) [28] or Elliptic-curve cryptography (ECC) [29] are widely used methods for generating digital signatures [20].

As normally the messages (M) are large, instead of encrypting the whole message with the private key (K_{pri}), a fixed length hash (H_M) is produced from the message by using any secure hash algorithm (SHA-2/SHA-3) and then this hash output is used to produce the digital signature (S_M).

$$H_M = Hash_{SHA-2/SHA-3}(M) \tag{1}$$

$$S_M = Sig(H_M) = E_{K_{pri}}(H_M) \tag{2}$$

(M, S_M) pairs are sent to the receiver for signature verification. The receiver reconstructs the hash (H_M^*) from the signature using the public key (K_{pub}) and matches it with the received hash (H_M) from M.

$$H_M^* = E_{K_{pub}}(S_M) \tag{3}$$

A perfect match between (H_M) and (H_M^*) ensures the success of signature verification process.

C. Registration Process

The registration phase starts after the chips are manufactured, and tested for defects. Only the detect-free chips go through the registration process. The proposed registration flow is shown in Figure 3.

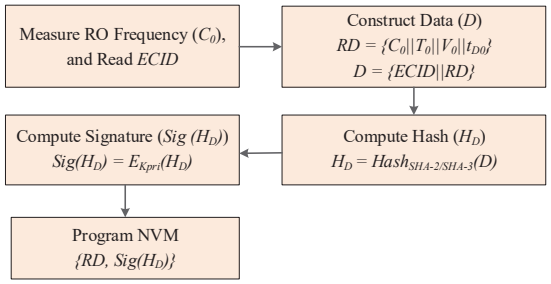

Figure 3: Proposed flow for the registration process.

The registration process of the chips can be performed as follows:

(1) The frequency of the ring oscillator is measured by using the measurement unit described in Section II-A. The counter value (C_0) is recorded for a fixed time interval (t_{D0}). The supply voltage (V_0), and the temperature (T_0) during the measurement process are also recorded. We construct ring oscillator data (RD) by concatenating counter value and measurement conditions.

$$RD = \{C_0||T_0||V_0||t_{D0}\}$$

It is also required to read the $ECID$ value from the chip through TAP [24].

(2) Data (D) is constructed by concatenating $ECID$ and RD.

$$D = \{ECID||RD\}$$

One can also put additional information in D regarding the manufacturer, production site, etc.

(3) A cryptographically secure hash algorithm (SHA-2/SHA-3 [30]) is used to produce a fixed length hash (H_D) from the data using Equation 1.

$$H_D = Hash_{SHA-2/SHA-3}(D)$$

(4) A digital signature ($Sig(H_D)$) (described in Section II-B) is constructed by encrypting the hash output (H_D) with the OCM's private key using Equation 2. This secure private key is only available to the OCM. One can use RSA or ECC to generate the signature [20].

$$S_H = Sig(H_D) = E_{K_{pri}}(H_D)$$

(5) The oscillator data, RD and the digital signature, $Sig(H_D)$ are stored in the NVM of the chip.

Note that one can construct a message authentication code (MAC [31]) on D and store $\{RD, MAC\}$ into the NVM. In such case, $Steps\ 3-4$ can be combined.

D. Authentication Process

The authentication process is fairly straightforward and can be performed at any point of the supply chain with a very low-cost measurement set-up. The set-up has to be equipped with a counter and a timer described in Section II-A. Moreover, it must be able to read the $ECID$ and NVM content of the chip. Figure 4 shows the proposed authentication process.

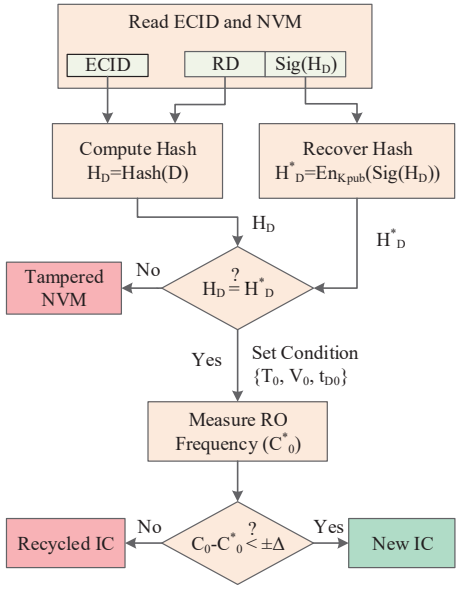

Figure 4: Proposed flow for the authentication process.

Our proposed authentication process can be described as follows:

(1) The NVM content that consists of ring oscillator data (RD) and digital signature ($Sig(H_D)\}$) of the chip under authentication is read through the measurement set-up described in Section II-A. One also needs to read the $ECID$ value. The data (D) is now constructed by concatenating $ECID$ and RD.

$$D = \{ECID||RD\}$$

(2) A hash (H_D) is computed on the data (D) by using Equation 1, and another hash (H_D^*) is recovered from the signature ($Sig(H_D)$) by using Equation 3.

$$H_D^* = E_{K_{pub}}(Sig(H_D))$$

Note that one needs to use the same secure hash function (SHA-2/SHA-3) and cryptographic primitives

(RSA/ECC), which were used during the registration process.

(3) The computed hash (H_D) and the recovered hash (H_D^*) are tested for any mismatches. Any mismatch indicates tampering of the NVM content by an adversary or counterfeiter.

(4) If the hashes match perfectly, the measurement parameters during registration ((T_0), (V_0), and (t_{D0}) are extracted from the ring oscillator data (RD).

(5) The RO clock cycle count (C_0^*) for the fixed time interval (t_{D0}) is measured at the same condition (T_0, V_0) during registration.

(6) The difference between the measured clock cycle count (C_0^*) and the registration clock cycle count (C_0) is calculated. If the difference is greater than the precision of the counter (measurement error), the chip is identified as a recycled chip. Otherwise, the chip is new.

III. Results and Analysis

The deviation of ring oscillator frequency over time due to negative bias temperature instability (NBTI) [32]–[34] and hot carrier injection (HCI) [35]–[37] induced aging degradation has been utilized to develop our proposed on-chip aging sensor. The aging impact on ring oscillator frequency is well documented in the literature [38]. The frequency output of an RO decreases over time due to aging and the impact is more severe in lower technology nodes.

A. Performance Evaluation based on Simulation

The simulation was conducted with HSPICE MOSRA (integrated circuit reliability analysis tool from Synopsys) with combined NBTI and HCI aging effects at 20°C for 81, 101, and 121 stage ROs. The data has been collected for 1, 3, 15, and 30 days of IC usage.

Table I: Frequency deviation of ring oscillators due to aging degradation.

RO Stage	Usage (days)	New CC (M/sec)	Aged CC (M/sec)	Deviation (M)	% Deviation
81	1	1080.50	1060.20	20.29	1.88
	3		1053.72	26.77	2.48
	15		1039.08	41.41	3.83
	30		1030.72	49.78	4.61
101	1	872.21	855.28	16.93	1.94
	3		850.48	21.73	2.49
	15		838.78	33.43	3.83
	30		831.46	40.75	4.67
121	1	730.83	716.89	13.93	1.91
	3		712.85	17.97	2.46
	15		702.83	27.99	3.83
	30		697.25	33.58	4.59

Table I shows the oscillation cycle count (CC) per second, and deviation in the CC for 1, 3, 15, and 30 days of usage for 81, 101, and 121 stage ring oscillators. The first column represents the number of inverters in an RO. The usage of the ring oscillator is put in the second column, whereas, the third column holds the value of the CC for a new RO. The fourth column holds the values of CC for aged RO's, and the last column denotes the percentage deviation in RO frequency due to aging. For instance, the seventh row denotes that a 101 stage RO produces 872.21 Mega cycles per second when it is new. It degrades to 838.78 Mega cycles after 15 days of usage, which indicates a deviation of 33.43 Mega cycles or 3.83%. The simulation result shows that even a single day of usage can reduce the CC by 1.88%. So, a measuring device which has a measurement error of less than 1% (practical devices are expected to have much better accuracy) can detect even a single day of aging. For 30 days of usage, the change in the CC is nearly 5%, which can be measured reliably with very low-cost devices.

B. Performance Evaluation based on Silicon Data

Figure 5 shows the experimental set-up for validating the effectiveness of our proposed recycled IC detection solution, which consists of a Temptronic ATS-605 Thermostream system [39] and Nexys-4 FPGA boards with Artix-7 FPGAs (28nm HPL process) [40]. The Temptronic Thermostream is a thermal inducing system which can control the operating temperature of a device over a wide range of temperature, -20°C to 225°C. The FPGA boards are programmed with one thousand ROs consisting of 21 stages, 31 stages, and 41 stages respectively. The structure of a ring oscillator in an FPGA fabric is significantly different that an ASIC implementation. Consequently, RO frequencies are significantly different than the simulations. The FPGA boards are then aged for two hours at a nominal supply voltage and a temperature of 85°C. The experiments are performed in a room temperature of 27°C. Around 1000 ring oscillators producing oscillations inside the chip increases the chip's internal temperature significantly. Assuming the chips internal temperature is 10°C higher than the environment, we have used a nominal temperature of 37°C for our experiment. An accelerated aging in the above-mentioned conditions corresponds to approximately 1 day of in-field aging as discussed in [41].

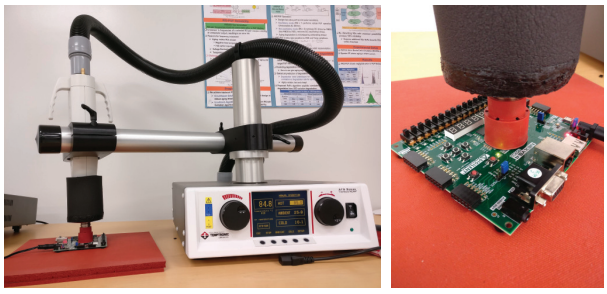

Figure 5: Experimental setup for accelerated aging.

Figure 6 shows the histogram of percentage degradation of RO frequencies. We have implemented 1000 21-stage ROs and performed accelerated aging for 2 hours, 4 hours, and 6 hours. We observe a Gaussian distribution for the percentage degradation for these ROs. The mean (μ) value of the % degradation for 2hr of accelerated aging which is equivalent to 1 day of usage in real-time, is 0.17% with a standard deviation (σ) of 0.032. So, any measuring device with reasonable accuracy (error less than 0.1%) will be able to detect this limited amount of aging with high-level of confidence. For higher usage, the distribution moves towards the right and the recycled ICs can be detected using our solution easily.

Table II summarizes our experimental results. The second column represents the temperature used for accelerated aging, whereas the third column represents the aging duration. We choose 2, 4, and 6 hours, which represent approximately of 1 day, 2 days, and 3 days of usage in the field, respectively. Column 4 and 5 represent the mean (μ) and standard deviation

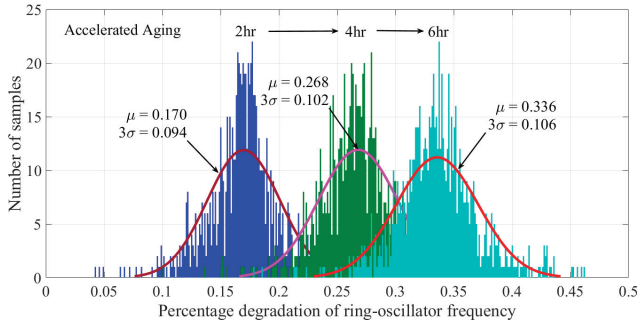

Figure 6: Percentage degradation of ring-oscillator frequency under accelerated aging.

(σ) of percentage frequency degradation distribution, which is constructed from 1000 ROs. We have observed the average (μ) degradation of 0.336% with a standard deviation (σ) of 0.0353 when a 21-stage RO is aged for 6 hours. For 31 stage and 41 stage ROs, the average degradation (μ) of 0.395% and 0.342% have been observed respectively for 6 hours of accelerated aging.

Table II: Percentage frequency degradation under accelerated aging for different ROs.

RO Stage	Temperature (°C)	Aging Duration (Hrs)	Mean (μ)	Standard deviation (σ)
21	85	2	0.170	0.0312
		4	0.268	0.0340
		6	0.336	0.0353
31	85	2	0.257	0.0502
		4	0.339	0.0582
		6	0.395	0.0642
41	85	2	0.239	0.0541
		4	0.281	0.0630
		6	0.342	0.0622

In order to demonstrate the accuracy of our proposed measurement procedure, we have implemented 4 different ring oscillators on an Artix-7 FPGA and measure the RO frequencies using counters realized inside the FPGA (see Figure 2). We have measured the same RO 330 times at 2 second intervals and recorded the frequency. Figure 7 shows the histogram plot for all four ROs. We have observed that the measurement error is less than 0.1% which can be used to detect 1 day of usage in the field as shown in Table II.

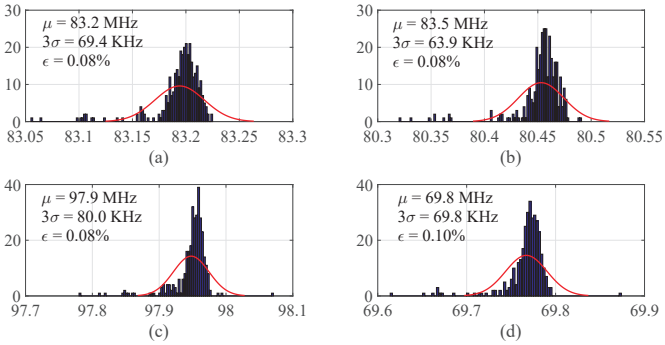

Figure 7: Percentage error during frequency measurement.

C. Security Analysis

In this section, we present different attack scenarios against our proposed solution and assess the performance of the proposed architecture under such attacks. We only consider the attacks that make economic sense to the recyclers. There can be more sophisticated attacks than those we present in this section but such attacks will require a large amount of investment from the recyclers which is against the goal of the whole recycling process.

• *Removal or tampering of the RO*: In this scenario, the attacker tries to replace the RO with a new counterpart or tries to tamper with the connections inside the chip. However, it is fairly impossible to replace the RO with a new one. Currently, recyclers have the capability to tamper with the connections by using FIB circuit edit [42]. If we assume that the tampering is possible, then the counterfeiter must remove the old package and again repackage and remark it according to its original specifications. This removal and repackaging may not be cost-effective to the counterfeiters. Hence, it is unlikely to be used in practice by an adversary.

• *Improper registration*: In this attack scenario, an untrusted entity at the production site can program the chip with a false oscillation count which is significantly less than the measured value. As a result, the counter value can still be found very close to the registration value even though a chip has been used. However, we do not find any financial motive behind such an act from a foundry's perspective as it will only help the counterfeiters. Moreover, we generally consider the foundry as trusted for IC recycling. Thus, manipulating the registration process in this way which clearly helps the counterfeiters does not make any financial sense for the foundries.

• *Modifying the NVM content*: The NVM content integrity is ensured through the digital signature. Any attempt to modify the NVM content will result in an integrity check failure which will expose the chips as compromised ones. A successful tampering of the NVM content will require forming a signature of the modified data using OCM's private key. The private key is only known by the trusted OCM which makes this kind of attack nearly impossible. If only the secret key is stolen from the OCM, this kind of attack can take place. Applying brute force to recover the private key of the OCM is nearly impossible if the key size is kept sufficiently large.

• *Dictionary Attack*: In this attack scenario, an adversary (recycler) constructs a dictionary of RO frequencies from many new chips. Each entry of the dictionary consists of the NVM contents of new chips. After recycling an old chip, the adversary measures the frequency of that RO. If a match (or close enough) is found in the dictionary, he/she can reprogram the NVM with the respective content from the dictionary. Due to the process variation, the RO frequencies vary significantly (generally Gaussian in nature [15]). It can be possible that the RO frequencies of new and recycled chips are of same value. Thus, it seems that a recycler can impersonate an old chip with a new one. However, one can easily detect this attack by verifying the $ECID$ value. Once the recycler copies the contents of one chip to the other, there will be a mismatch of the hash contents and will be detected by signature verification.

D. Design Overhead

Our proposed architecture utilizes ring oscillators (RO) and a small non-volatile memory, which can be added to any CMOS digital circuit without adding much overhead (area, cost, and/or power). Almost every chip is equipped with ROs primarily to monitor the manufacturing process. The same RO

can be used for our proposed structure. We need a small NVM to store the temperature value (T_0) of approximately 10 bits, the registration supply voltage (V_0) of another 10 bits, the oscillation count (C_0) of 32 bits, the fixed time interval (t_0) of 10 bits, and the digital signature (e.g., using EC-DSA [20] of around 80 Byte, which depends on the key size and can be of larger or smaller value). As a result, we require around (less) 1K bits of memory to store $\{RD,Sig(H_D)\}$ into the NVM.

IV. Conclusion

In this paper, we have proposed an on-chip sensor, which consists of a ring oscillator and a small NVM, and can be used to detect recycled ICs very accurately. We have proposed to store the RO frequency into an NVM and use a digital signature to ensure the resistance against tampering with the NVM. The chip registration can be undertaken in the testing facility which ensures that there is no additional cost involved in the registration process. Simulation and silicon results show that our proposed architecture is capable of identifying a very limited amount of aging with the help of very low-cost measuring devices. A heuristic analysis of different probable attacks and their countermeasures are also presented. The design overhead of our proposed solution is significantly small, which makes it a suitable candidate for detecting aging degradation for a broader class of ICs.

Acknowledgments

This work was supported by a new faculty start-up grant from Auburn University.

References

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

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

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

[4] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[5] G-19A Test Laboratory Standards Development Committee, "Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts," 2016, https://saemobilus.sae.org/content/as6171.

[6] G-19CI Continuous Improvement, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," 2009, https://saemobilus.sae.org/content/as5553.

[7] CTI, "Certification for Counterfeit Components Avoidance Program," 2011, http://www.cti-us.com/pdf/CCAP101Certification.pdf.

[8] IDEA, "Acceptability of Electronic Components Distributed in the Open Market," 2017, http://www.idofea.org/products/118-idea-std-1010b.

[9] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ics," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, October 2012.

[10] K. Huang, J. Carulli, and Y. Makris, "Parametric counterfeit IC detection via Support Vector Machines," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, 2012, pp. 7–12.

[11] H. Dogan, D. Forte, and M. Tehranipoor, "Aging analysis for recycled fpga detection," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Oct 2014.

[12] Z. Guo, M. T. Rahman, M. M. Tehranipoor, and D. Forte, "A zero-cost approach to detect recycled soc chips using embedded sram," in *IEEE Int. Symp. on Hardware Oriented Security and Trust*, 2016.

[13] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ics using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE-ACM Design Automation Conference*, June 2012.

[14] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ics," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 22, no. 5, pp. 1016–1029, May 2014.

[15] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost On-Chip Structures for Combating Die and IC Recycling," in *Proc. of ACM/IEEE on Design Automation Conference*, 2014.

[16] 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.

[17] K. He, X. Huang, and S. X. D. Tan, "Em-based on-chip aging sensor for detection and prevention of counterfeit and recycled ics," in *IEEE/ACM International Conference on Computer-Aided Design*, Nov 2015, pp. 146–151.

[18] M. Miller, J. Meraglia, and J. Hayward, "Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts," in *SAE Aerospace Electronics and Avionics Systems Conference*, October 2012.

[19] Semiconductor Industry Association (SIA), "Public Comments - DNA Authentication Marking on Items in FSC5962," November 2012.

[20] Elaine Barker (NIST), "FIPS 186-4: Digital Signature Standard (DSS) ," July 2013.

[21] T.-K. Lee, "Process monitor for cmos integrated circuits," Jan. 23 1996, uS Patent 5,486,786.

[22] E. O. Sugasawara, "Process monitor circuitry for integrated circuits," Sep. 26 2000, uS Patent 6,124,143.

[23] R. Bach, "Process monitor with statistically selected ring oscillator," Apr. 8 2003, uS Patent 6,544,807.

[24] "Ieee standard for test access port and boundary-scan architecture," *IEEE Std 1149.1-2013 (Rev. of IEEE Std 1149.1-2001)*, pp. 1–444, May 2013.

[25] Bill Eklow, "ECID vs Device ID," 2006. [Online]. Available: btw.tttc-events.org/material/BTW10/Presentations/Session%205.2.pptx

[26] K. Arndt, C. Narayan, A. Brintzinger, W. Guthrie, D. Lachtrupp, J. Mauger, D. Glimmer, S. Lawn, B. Dinkel, and A. Mitwalsky, "Reliability of laser activated metal fuses in drams," in *Proc. of IEEE on Electronics Manufacturing Technology Symposium*, 1999, pp. 389–394.

[27] N. Robson, J. Safran, C. Kothandaraman, A. Cestero, X. Chen, R. Rajeevakumar, A. Leslie, D. Moy, T. Kirihata, and S. Iyer, "Electrically programmable fuse (efuse): From memory redundancy to autonomic chips," in *CICC*, 2007, pp. 799–804.

[28] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[29] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[30] National Institute of Standards and Technology, "FIPS 180-4: Secure Hash Standard (SHS)," August 2015.

[31] National Institute of Standards and Technology, "FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC) ," July 2008.

[32] M. Alam and S. Mahapatra, "A comprehensive model of pmos nbti degradation," *Microelectronics Reliability*, vol. 45, no. 1, pp. 71 – 81, 2005.

[33] S. Bhardwaj, W. Wang, R. Vattikonda, Y. Cao, and S. Vrudhula, "Predictive modeling of the nbti effect for reliable design," in *Proc. of IEEE on Custom Integrated Circuits Conference*, September 2006, pp. 189 –192.

[34] V. Reddy, A. Krishnan, A. Marshall, J. Rodriguez, S. Natarajan, T. Rost, and S. Krishnan, "Impact of negative bias temperature instability on digital circuit reliability," in *Proc. on Reliability Physics*, 2002, pp. 248 – 254.

[35] K.-L. Chen, S. Saller, I. Groves, and D. Scott, "Reliability effects on mos transistors due to hot-carrier injection," *Electron Devices, IEEE Transactions on*, vol. 32, no. 2, pp. 386 – 393, February 1985.

[36] S. Mahapatra, D. Saha, D. Varghese, and P. Kumar, "On the generation and recovery of interface traps in mosfets subjected to nbti, fn, and hci stress," *Electron Devices, IEEE Transactions on*, vol. 53, no. 7, pp. 1583 –1592, July 2006.

[37] J. McPherson, "Reliability challenges for 45nm and beyond," in *Proc. of ACM/IEEE on Design Automation Conference*, 2006, pp. 176 –181.

[38] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ics using fingerprints from a light-weight on-chip sensor," in *Proceedings of Design Automation Conference*. ACM, 2012, pp. 703–708.

[39] Temptronic ATS-605 ThermoStream Thermal Inducing System, -20 to +225C.

[40] Nexys 4 Artix-7 FPGA Trainer Board.

[41] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. Van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm cmos," in *Proceedings of the ESSCIRC*, 2012, pp. 486–489.

[42] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, "Breaking and entering through the silicon," in *Proceedings of SIGSAC Conference on Computer and Communications Security*, 2013, pp. 733–744.