Comprehensive Detection of Counterfeit ICs Via On-Chip Sensor and Post-Fabrication Authentication Policy

Yaoyao Ye*, Taeyoung Kim†, Haibao Chen*, Hai Wang‡, Esteban Tlelo-Cuautle§ and Sheldon X.-D. Tan†
*Department of Micro/Nano Electronics, Shanghai Jiao Tong University, Shanghai, China 200240
†Department of Electrical and Computer Engineering, University of California, Riverside, CA, USA 92521
‡School of Microelectronics and Solid-State Electronics
University of Electronic Science and Technology of China, Chengdu, China, 610054
§ Department of Electronics, INAOE, Puebla, Mexico 72840

***Abstract*—Counterfeit integrated circuits (ICs) have posed a major security and safety threat on commercial and mission-critical systems. In this paper, we propose to develop a comprehensive counterfeit ICs detection and prevention strategy, consisting of an innovative multi-functional on-chip sensor and a related post-fabrication authentication methodology. We target at many counterfeit ICs including the recycled/remarked/out-of-spec ICs, as well as cloned and over-produced ICs. First, the new sensor consists of antifuse memory and aging sensors to reduce reference circuit related area overhead of those sensor circuits. Second, the new sensor combines both the ring-oscillator based aging sensor with recently proposed electromigration(EM)-based aging sensor so that it can be effective for estimation of both short and long period time of chip usage. Third, on top of the new sensor, we propose a new post-fabrication authentication methodology to detect and prevent non-defective counterfeit ICs. Simulation results show the advantage of the proposed multi-functional sensor against existing on-chip sensors in terms of functionality, detection coverage and usage time estimation range and accuracy.**

I. Introduction

The counterfeiting of integrated circuits (ICs) has become a major problem in recent years, potentially impacting the security of electronic systems especially for military, aerospace, medical and other critical applications. Based on the report by the International Chamber of Commerce, the costs of the counterfeiting and piracy for G20 nations reach $1.7 trillion by 2015 [1]. The problem is getting worse due to deficiencies in existing detection solutions and lack of effective avoidance mechanisms.

Existing counterfeit detection techniques include physical methods and electrical methods [2]. In general, physical methods can be applied to all part types, but some of them are destructive and take hours to test. On the other hand, conventional electrical test methods are non-destructive and time efficient, yet they can be very expensive. One viable way for fast detection and effectively prevention of recycled chips is to insert a lightweight aging detecting sensor. Some early efforts have been explored [3], [4], [5]. A ring-oscillator (RO)-based aging sensor relying on aging effects of MOSFETs on changing the RO frequency was designed in [4]. However, this method can only give a rough estimation of the usage age of the chip as the shift of the frequency also depends on many other factors. Recently, on-chip aging sensor based on the electromigration (EM) failure mechanism of interconnect wires has been proposed [5]. The main advantage of EM-based aging sensor over RO-based aging sensor is that it can provide a more accurate usage time estimation especially over a long period of time. The design is also simple and lightweight with small area and power overhead. However the EM-based sensor has more area overhead for estimation of short period time of usage as it needs longer interconnect wires.

For detection of non-defective counterfeit ICs, existing physical, electrical methods and aging sensor will not be effective as there is no traceable properties that can be detected. One potential solution is to have a post-fabrication authentication process in which, each IC will be uniquely registered into a global database using challenge-response pairs after fabrication and testing. End users can verify the ICs for proper registration later. This process is similar to the passive hardware metering method, which enables the design house to achieve post-fabrication control of the produced ICs [6], [7]. Unfortunately, existing detection techniques can only detect one type of those counterfeit ICs, not both. Therefore, it is urgently needed to develop new comprehensive, yet cost-effective, counterfeit IC detection techniques.

In this paper, we propose to develop a comprehensive counterfeited ICs detection and prevention strategy, which consists of an innovative multi-functional on-chip sensor and the related post-fabrication authentication methodology. This paper is organized as follows. In Section II, we present the new multi-purpose on-chip sensor circuit architecture. Section III presents the overall authentication flow of the proposed on-chip sensor and detection methodology. Several statistical and variational analysis of the new sensors and comparison analysis are presented in Section IV. Last, Section V concludes.

II. The proposed on-chip sensor circuit

In this section, we present the architecture of the proposed on-chip sensor circuit, which consists of one antifuse memory block, one aging sensor module, one encryption module and one activation module as shown in Fig.1. Each module will be discussed in detail in the following sections.

A. Antifuse memory block

The antifuse memory block is used to store the unique key and other assets for each chip. The antifuse memories are programmed in a programming environment with relative high voltage. Therefore, integrated charge pumps are used to provide sufficiently high voltage in embedded antifuse memories. We use existing antifuse blocks instead of designing a new one.

This work is supported in part by NSF grant under No. CCF-1527324 and under UC MEXUS-CONACYT collaborative research grant under No. CN 16-161. This work is supported by NSFC (Project 61602298).

978-1-5090-5052-9/17/$31.00 ©2017 IEEE

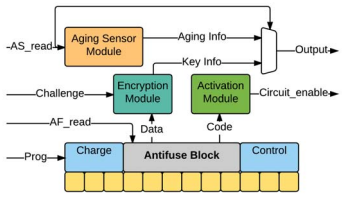


Fig. 1. The proposed on-chip sensor architecture

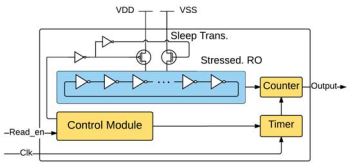


Fig. 2. Structure of RO aging sensor

B. Aging sensor module

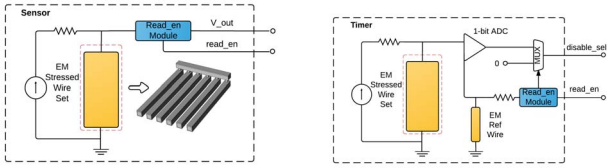
Two different aging sensors to identify recycled ICs are used in this aging sensor module. The RO-based sensor is based on the aging effects on RO. The usage time can be detected by degraded RO frequency. The EM-based sensor relies on the EM aging effects on interconnect wires. The resistance change of the stressed wires can be used to estimate the chip usage time. The RO-based aging sensor is used to detect short-term aging while the EM-based aging sensor is used to detect long-term aging. In addition, the EM-based aging sensor can serve as a timer which can be used to disable the chip after a certain time.

In the new sensor design, the new RO-based sensor shown in Fig. 2 follows the similar design in [4]. However, the new RO-based sensor differs in that it only has one RO, as the reference frequency will be stored in the design house database and can be assessed when the chip ID is read back by challenge-response pairs during the authentication process.

Fig. 3 shows the schematic of the proposed EM-based sensor. The design follows the recent work in [5]. The EM-based sensor has two versions. One version is the aging sensor shown in Fig. 3(a). In this case, we have a group of wires connected in parallel and stressed by DC current. The current densities in the wires are setup so that the wires will be nucleated at a specific time (e.g., one year or 10 years). The initial resistance of the wires will be stored in the design house database as a reference. When the resistance of wires changes by 10%, it can be counted as a failure and time difference between the activation time and current is the usage time. Another version of the EM-based sensor is the timer version as shown Fig 3(b). In this case, the reference wire, which has the same geometry as the stressed wires is used. The sensor can output the signal when the wire resistance changes significantly (by 10%). The signal can be used to lock the chip or lock certain functions of the chip for timed-service of the chip or the system.

C. Encryption and activation module

The encryption module is used to encrypt the data from antifuse blocks with the challenge from the design house database. This module can be any existing encryption module, e.g., Advanced Encryption Standard (AES) method. It is used



(a) The EM sensor-only circuit (b) The EM timer circuit

Fig. 3. The structure of EM aging sensor

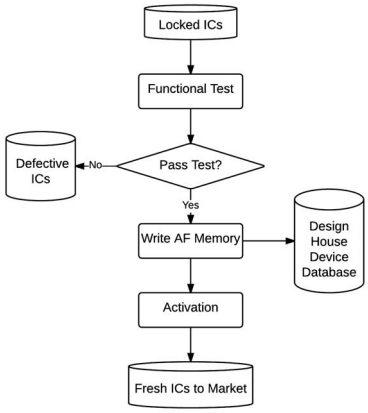


Fig. 4. The proposed post-fabrication authentication

to make sure the key information in the antifuse block cannot be directly accessed by any adversary.

The proposed on-chip sensor also allows one-time activation of a chip or certain chip functions. This is achieved by the activation module. Once the chip passes the post-fabrication testing, the design house can write the key into the antifuse blocks. There are many ways to implement the chip-level activation process [8], [9]. For instance, we check the parity of the bits of the stored key in antifuse memory. The checking circuit inside the activation module can be obfuscated for further protection.

III. The Proposed Counterfeit IC Detection Methodology

In this section, we present the proposed overall counterfeit IC detection methodology and the IC authentication flow based on our new on-chip sensor with antifuse memory.

Fig. 4 shows the proposed post-fabrication authentication. Once chips have been tested and packaged in the assembly stage, they will be sent back to the design house. After a functional test, for the non-defective ICs, a unique chip ID, activation time and other assets will be written into the antifuse memory in the on-chip sensor. And the initial aging reference properties will be stored into the design house global database for future verification. Also the design house can activate the locked chip which will not work after the fabrication process, using the unique content in the antifuse memory.

Fig. 5 shows the proposed comprehensive detection policy for counterfeit ICs. In general, a newly fabricated chip needs to pass two tests to be proved as a fresh and authentic IC. The first test is called fingerprint test. The design house device database generates a random challenge which can be input into the IC. If the IC cannot generate any response or just output an incorrect response, then it hasn't taken the official design

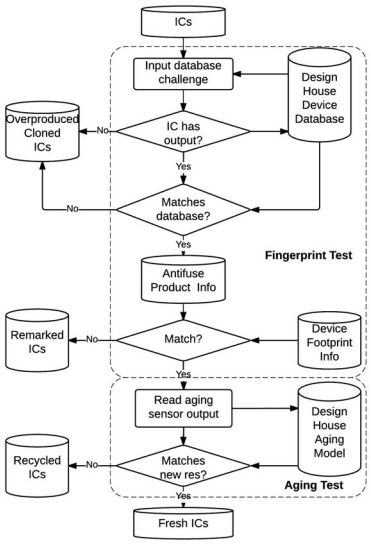


Fig. 5. The proposed comprehensive detection methodology

TABLE I
AGING SENSOR COMPARISON

Feature	RO	EM	Proposed
Short-term usage accuracy	high	low	high
Long-term usage accuracy	low	high	high
Post-fabrication auth	no	no	yes
Detect cloned and over-produced ICs	no	no	yes
Reference circuit	needed	needed	not needed
Activation	no	no	yes
Timed-service	no	no	yes

house antifuse activation. It means this IC never comes back to the design house after fabrication. So it can be detected as an overproduced or cloned IC. If the response of the IC matches the information in the design house database, then we can get its production information. By comparing the antifuse production information and the device footprint information, it's easy to detect it's a remarked IC or not. The second test is called aging test. This test is performed to detect recycled or used ICs or tell the estimated usage time of the chip. By reading the aging sensor output, we can detect if it's recycled IC or not. Based on the aging model employed and the aging output, we can determine the usage time of the chip accurately.

IV. NUMERICAL RESULTS AND DISCUSSIONS

Table I summarizes the major feature comparisons among the RO-based, EM-based and the proposed hybrid aging sensor. The RO-based sensor has high short-term usage accuracy but low long-term usage accuracy. The EM-based sensor has high long-term usage accuracy if we use multiple stressed wires. However, its design is not good for short-term recycled IC detection. Our proposed hybrid aging sensor can maintain high accuracy for both short- and long-term recycled IC detection. The proposed sensor can allow post-fabrication authentication to detect cloned and over-produced ICs. When it is used as a on-chip timer, it also allows activation of the chip and timed services.

A. Results for RO-based aging sensor

The RO-based aging sensor has been implemented and simulated using HSPICE MOSRA from Synopsys. In our implementation, we selected 7-stage and 15-stage ROs to compare the results. In order to model the variation, we performed Monte Carlo(MC) simulation with 1,000 samples of the RO in HSPICE. Similar to the simulation in [4], we considered two process variations to investigate the impact of variation on the detection of the recycled ICs. Table II shows the different process variations used in our simulation. V_{th} is a threshold voltage, L is a gate channel length, and T_{ox} is a gate oxide thickness. RO-based sensors with 7-stage and 15-stage ROs are simulated at 25°C with PV0 and PV1. PV0 represents the expected process variation between ROs while PV1 is the worst-case scenario. Thousand sensors are generated using MC simulation by HSPICE and the total aging time is set at 15 months with a 3-month step.

TABLE II
PROCESS VARIATIONS

	Inter-die			Intra-die		
	$V_{th}(\%)$	L(%)	$T_{ox}(\%)$	$V_{th}(\%)$	L(%)	$T_{ox}(\%)$
PV0	5	5	2	5	5	1
PV1	20	20	6	10	10	3

Fig. 6 shows the simulation results for the RO-based aging sensor. The x-axis represents the frequency difference ($f_{diff} = f_{init} - f_{stressed}$) between the initial value and the stressed RO. Note that we don't need a reference RO because we store the initial frequency in the global database. The y-axis represents the frequency of occurrence. The legend in the figures denotes the aging time (for example, AT = 3M denotes the RO is aged for 3 months). The green distribution represents the new ICs where the RO has not been aged and is centered at 0 MHz. The light blue and dark blue distributions represent 3 months and 15 months of aging respectively. It is clear that aging shifts the distributions to the right as the stressed RO has aged more and become slower resulting in the right shift of f_{diff} distribution.

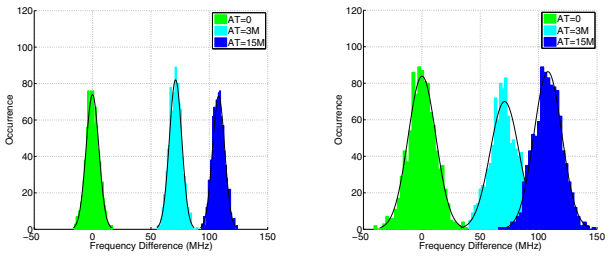
We can clearly identify recycled ICs when the two distributions ($T = 0$ and $T = 3,15M$) do not overlap with one another. In Fig. 6(a), after being used for 3 months, the stressed RO suffers from aging effects and its frequency becomes lower. The lowest frequency difference between the new and the stressed ROs is larger than the largest frequency difference present in the new IC set. Therefore, the recycled IC detection rate for ICs aged for 3 months or longer is 100%. At 15 months, the frequency differences between the new and the stressed ROs can be larger.

Fig. 6(b) shows the frequency difference occurrence rate between the 7-stage new and stressed ROs with process variations PV1. Moving from PV0 to PV1, inter-die and intra-die variations both become larger. As process variation increases, the variance in f_{diff} grows, which results in an overlap between 3M and 15M distributions. In this case, we should expect higher mis-prediction rates.

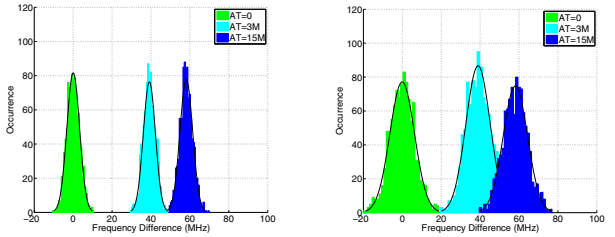
Simulation results for 15-stage ROs using same process variations are shown in Fig. 6(c) and Fig. 6(d). Comparing to the 7-stage ROs, the frequency difference between aged and new ICs is smaller because we use larger stage ROs. Although it impacts the absolute value of the frequency difference, the detection rate will not be impacted significantly.

B. Results for EM-based aging sensor

The proposed EM-based aging sensor circuit has been designed and validated using SPICE simulation. To verify

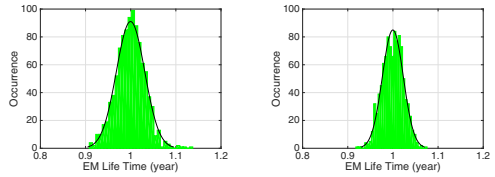


(a) 7-stage RO with PV0 (b) 7-stage RO with PV1



(c) 15-stage RO with PV0 (d) 15-stage RO with PV1

Fig. 6. Process variation impacts on frequency spreading and recycled IC detection probability.



(a) 1 wire (b) 3 wires

(c) 6 wire (d) 10 wires

Fig. 7. The statistical study of stressed wire set with different wire numbers

the effects of aging on it, we performed 1,000 Monte Carlo simulation considering the variation of the failure time for the stressed wires. The failure time can be defined as the time when the wire resistance increases by 10% of its value, which can be predicted by the physical-based EM-model [10], [11]. The simulation is conducted using HSPICE and MATLAB with the physical-based EM-model. The EM stressed wire sets are composed of 1, 3, 6 and 10 wires which will fail around one year. The EM failure time follows lognormal distribution [12]. Simulation results are shown in Fig. 7. The variance of the lognormal distribution is set to 0.001. With one wire, the EM lifetime will fall into $\pm 10\%$ mean lifetime with 99.83% chance and into $\pm 5\%$ mean lifetime with 88.64% chance. If we use 6 wires, we can have 100% chance to achieve $\pm 10\%$ mean lifetime and 98.66% chance for $\pm 5\%$ mean lifetime, which is good enough. We can mitigate the failure time variations by increasing the number of wires.

Fig. 8 shows the power values versus possible wire length (L) and current density j. The 4 red curves show the possible L and j values for 1 year, 3 years, 6 years and 10 years. It clearly shows the trade-off between L (area) and power.

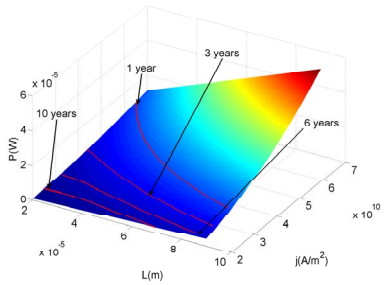


Fig. 8. Power consumption of stress wires versus wire length and current density.

C. Area overhead

The area overhead of the proposed hybrid aging sensor is small. The RO-based sensor only takes n inverters, where n is the number of stages in RO. An EM-based aging sensor with 10 stressed wires costs 100-500um^2 with an SMIC 180nm technology, which depends on the length of the wire. Assuming a total of five EM-based sensors, the overhead is only 0.01% of the area available in a 5mm$\times$5mm chip.

V. Conclusion

In this paper, we proposed a comprehensive counterfeit ICs detection and prevention strategy, which consists of an innovative multi-functional on-chip sensor and the related post-fabrication authentication methodology. The new on-chip sensor can serve as a central on-chip security hardware IP for counterfeit ICs detection, on-chip timer, post-fabrication authentication and even activation module for ICs. Simulated results show the advantage of the proposed multi-functional sensor in terms of functionality, detection coverage and usage time estimation range and accuracy.

References

[1] D. Chardonnal, "Impacts of counterfeiting and piracy to reach US$1.7 trillion by 2015," 2011.
[2] M. Tehranipoor, H. Salmani, and X. Zhang, *Integrated Circuit Authentication*. Springer, 2014.
[3] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. Design Automation Conf. (DAC)*, 2012.
[4] X. Zhang and M. Tehranipoor, "Path delay Fingerprinting for Identification of Recovered ICs," in *IEEE Int. Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems(DFT)*, 2012.
[5] 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 *Proc. Int. Conf. on Computer Aided Design (ICCAD)*, Nov. 2015.
[6] F. Koushanfar and G. Qu, "Hardware Metering," in *Proc. Design Automation Conf. (DAC)*, pp. 490–493, 2001.
[7] M. Rahman, D. Forte, Q. Shi, G. Contreras, and M. Tehranipoor, "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," in *IEEE Int. Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems(DFT)*, 2012.
[8] Y. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Inproceedings of 16th USENIX security symposium*, pp. 1–16, 2007.
[9] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing ic piracy using reconfigurable logic barriers," *IEEE Design & Test of Computers*, vol. 27, pp. 66–75, 2010.
[10] V. Sukharev, "Beyond Black's Equation: Full-Chip EM/SM Assessment in 3D IC Stack," *Microelectronic Engineering*, vol. 120, pp. 99–105, 2014.
[11] X. Huang, T. Yu, V. Sukharev, and S. X.-D. Tan, "Physics-based electromigration assessment for power grid networks," in *Proc. Design Automation Conf. (DAC)*, June 2014.
[12] J. R. Black, "Electromigration-A Brief Survey and Some Recent Results," *IEEE Trans. on Electron Devices*, vol. 16, no. 4, pp. 338–347, 1969.