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

Taeyoung Kim[c], Sheldon X.-D. Tan[d], Chase Cook[d], Zeyu Sun[d]

[a] *Department of Computer Science and Engineering, University of California, Riverside, CA 92521 USA*
[b] *Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA*

Abstract

Counterfeiting of integrated circuits (ICs) has become an increasingly vital concern for the security of commercial and mission-critical systems. Moreover, they pose an immense economic, security, and safety threat. We propose a comprehensive detection and prevention framework consisting of a multi-functional on-chip aging sensor, and post-fabrication authentication methodology. This framework targets several classes of counterfeit ICs, such as recycled, remarked, out-of-spec, cloned, and over-produced ICs. First, the new sensor consists of both antifuse memory and aging sensors. To reduce reference-circuit related area-overhead, the initial electronic properties of sensor circuits are stored in a global database, accessed by unique chip via challenge-response pairs. Second, this work consists of a two aging-sensor approach, based on IC wear-out effects, using a recently proposed electromigration (EM) aging sensor and a ring oscillator aging sensor. This method can be effective for chip usage estimation of both short and long time periods. Hence, it can serve as a more accurate timer for the chip to meter the long term usage, which can allow for timed services of some functionality of a chip, in addition to detection of the recycled/remark ICs. Third, on top of the new sensor, we propose a new post-fabrication authentication methodology to detect and prevent non-defective counterfeit ICs. All fabricated ICs will be registered in a global database and activated with a unique chip ID, which is written into the antifuse memory. Simulation results show that the combined aging sensors have a high degree of accuracy when compared to traditional on-chip sensors.

Keywords: Aging Sensor, Hardware Security, Electromigration, Reliability, Antifuse, Post-fabrication Authentication. Counterfeit IC

☆This work is supported in part by NSF grant under No. CCF-1527324, in part by NSF grant CCF-1816361 and in part by UC-Mexus grant under CN 16-161.

Email addresses: `tkim049@cs.ucr.edu` (Taeyoung Kim), `stan@ece.ucr.edu` (Sheldon X.-D. Tan)

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

Taeyoung Kim[c], Sheldon X.-D. Tan[d], Chase Cook[d], Zeyu Sun[d]

[c] *Department of Computer Science and Engineering, University of California, Riverside, CA 92521 USA*
[d] *Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA*

1. Introduction

Counterfeit integrated circuits (ICs) have become an increasingly urgent problem in recent years posing a threat to both the economy and security. The security threat is especially true for critical systems such as military, aerospace, and medical. A 2008 report by the International Chamber of Commerce found that the counterfeiting and piracy for G20 nations results in losses as high as $775 billion and is estimated to rise as high as $1.7 trillion in 2015 [1]. A secondary effect on the market from counterfeit ICs is the discouragement of innovation and investment into research and development [2]. Unfortunately, these issues continue to mount due to a lack of effective avoidance and detection techniques. What has become apparent from numerous reports [3] is that the issue of counterfeit ICs lies in the U.S. electronic component supply chain, which has a heavy reliance on "untrusted" fabs.

Counterfeit ICs comes from a variety of sources in the electronic supply chain. A counterfeit IC: does not conform to the original component manufacturer's (OCM) design, model, and/or performance; or it is not produced by the original component manufacturer or is produced by unauthorized contractors; it is an off-specification, defective, or used OCM product sold as "new" or working; it has incorrect or false markings and/or documentation [4, 5]. Therefore, counterfeit ICs can be classified into several major categories: (1) recycled and remarked ICs, which is the most widely reported type of counterfeit parts; (2) overproduced, which describes ICs fabricated outside of contract by foundries; (3) out of spec/defective ICs, which should be rejected during testing, but are stolen and sold on open markets; and (4) cloned ICs, which just copy the legal part by reverse engineering or illegal obtaining of IPs.

From the perspective of detection techniques, counterfeit ICs can also be categorized into defective and non-defective. Defective ICs are typically recycled/remarked and out-of-spec/defective. Those counterfeit ICs will show some degree of physical or electrical defects and anomalies due to aging and inherent defects from fabrication. Also, the recycled ICs can cause reliability and security problems for many critical applications. Existing counterfeit detection techniques mainly focus on detecting defective ICs as they account for the majority of the counterfeit components [6, 7, 8].

On the other hand, non-defective ICs such as overproduced or cloned ICs are unauthorized productions without the legal license. This type of IC may be exactly the same as an authorized chip. The non-defective chips, however, undercut the competition with the unlicensed ones, which can cause significant revenue loss and related job loss for the original IC and IP owners and OCMs. Unfortunately, existing detection techniques can only detect one type of counterfeit ICs, not both. Therefore, a new comprehensive, yet cost-effective, counterfeit IC detection technique is urgently needed.

1.1. Review of existing detection method

For defective ICs, especially recycled and remarked ICs, there exists many detection techniques, which can be classified into physical methods and electrical methods [2]. Physical methods consist of incoming inspection methods such as visual inspection, X-ray imaging, package analysis method (laser scanning microscopy), delid method, and material analysis methods(using Fourier transform infrared and X-ray fluorescence). Electrical methods consist of parameter tests, function tests, built-in tests, and structural tests. Typically, physical methods can be applied to any electrical component, but some of the methods are destructive and take hours to test. Because of this, a small portion of a batch of parts must be sampled and observed in order to certify their authenticity. Conventional electrical test methods, on the other hand, are not destructive and are also time efficient. However, these methods have no guarantee of full test coverage and may not detect all defective ICs.

One viable way for fast detection and effective prevention of recycled chips is to insert a lightweight aging detection sensor, which can directly indicate the usage of a chip; some early efforts have been explored in [9, 10, 11, 12].

[☆☆] This work is supported in part by NSF grant under No. CCF-1527324, in part by NSF grant CCF-1816361 and in part by UC-Mexus grant under CN 16-161.

Email addresses: tkim049@cs.ucr.edu (Taeyoung Kim), stan@ece.ucr.edu (Sheldon X.-D. Tan)

The method in [10] designed a ring-oscillator(RO)-based aging sensor that relies on the aging effects of MOSFETs to change an RO frequency in comparison with a reference frequency embedded in the chip. As the chip ages, due to the wear-out mechanisms such as negative-bias temperature instability (NBTI) and hot carrier injection (HCI), the threshold voltage of the MOSFET devices begins to shift, while also changing the frequency of the RO, and provides a simple indicator for the IC age. However, this method can only give a very rough estimation of the usage age of the chip as the shift in frequency depends on many factors.

In order to mitigate the inaccuracy problem, an antifuse (AF)-based sensor was developed in [2]. The AF-based sensor essentially is a counter, which counts the clocks or derivatives of the clock events to log the usage of the chip. The antifuse memory is used to make sure the data in the count will not be erased or altered by attackers. However, AF-based sensors suffer from large area overhead, especially when a more accurate indication of usage is required [2]. Another problem with this method is that it may not reflect the true aging-dependent usage of a chip. For instance, it will log the same usage time for different on-chip temperatures, however, the temperature has been shown to have a dramatic impact on the aging effects from electromigration, NBTI and HCI [13].

Recently, an on-chip aging sensor based on the electromigration (EM) failure mechanism of interconnect wires has been proposed [12]. The main advantage of the EM-based aging sensor over RO-based aging sensor is that it can provide more accurate time usage estimations especially over long periods of time due to the recent advance in the physic-based EM modeling [14, 15, 16]. The design is also simple and light-weight with a small area and power overheads. However, the EM-based sensor has a larger area overhead when designed to detect short-term usage. This is because the EM sensor requires longer wires when the target detection lifetime is short. However, at longer lifetimes, the wires can be much shorter.

For detection of non-defective counterfeit ICs, existing physical, electrical and aging sensor based methods will not be very effective since no traceable properties can be detected in such chips. One potential solution is to have a post-fabrication authentication process in which, after fabrication and testing, each IC will be uniquely registered into a global database using challenge-response pairs. The end users can verify the ICs for proper registration later. This post-fabrication authentication process is similar to the passive hardware metering method, which enables the design house to achieve post-fabrication control of the produced ICs [17, 18, 19]. However, those methods cannot detect the recycled and used ICs.

1.2. New contribution

In this paper, we propose a comprehensive counterfeit IC detection and prevention strategy, which consists of an innovative multi-functional on-chip sensor, and the related post-fabrication authentication methodology. The proposed on-chip sensor can detect recycled/remarked/out-of-spec chips, as well as cloned and over-produced ICs. It can serve as a central on-chip security hardware IP for counterfeit IC detection, on-chip usage timer, post-fabrication authentication, and even activation module for ICs. Our new on-chip sensor has the following features:

- The new on-chip sensor combines an antifuse memory block, which is one-time programmable (OTP), with existing aging sensors. The memory block will not be used as a counter as in the existing methods. Instead, it will store a unique chip ID, time stamp of activation, and other important chip assets, which will be encrypted against tampering and can be verified by challenge-response pairs.
- Second, the new on-chip sensor combines the two types of aging sensors to detect both short-term and long-term aging effects so that it can be effective and area-efficient for both cases. The RO-based sensor is more effective for short-time usage detection and the EM-based aging sensor is more accurate, and area efficient, for long term usage detection. The EM-based aging sensor exploits the natural aging/failure mechanism of interconnect wires to time the aging of the chip. It can serve as a more accurate timer for the chip to meter the usage of long time periods. As a result, it can enable timed service for some functionality of a chip and can also avoid the over-usage of the authorized time period of a chip or a system for certain security requirements.
- Based on the new on-chip sensor, we propose a post-fabrication authentication methodology to detect and prevent non-defective counterfeit ICs. All the fabricated ICs will be uniquely registered and activated with a unique chip ID in a global database. The unique chip ID will be written into the antifuse memory during a registration process and the chip will be activated. This method not only prevents cloned and over-produced ICs, but also mitigates the need for reference circuits in existing aging sensor designs. This significantly reduces area overhead, as the initial electronic properties of the sensor circuits can be stored in the global database.

In this work, antifuse memory block is used to store unique chip ID, both long term and short term aging can be considered and global database for ID can reduce overhead area. With all these advantages, the proposed method is more effective and accuracy comparing with existing methods. Simulated results show the advantage of the proposed multi-purpose sensor against the existing on-chip sensors in terms of functionality, detection coverage, and usage time estimation range and accuracy.

2. 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.

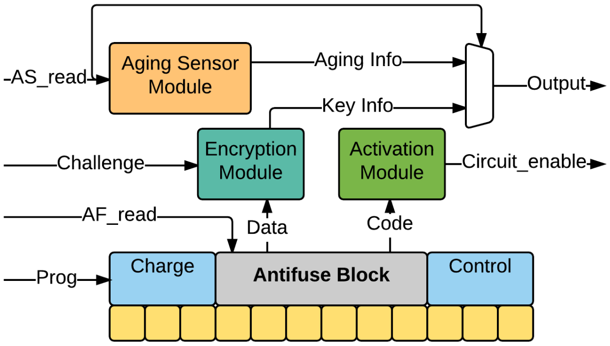


Figure 1: The architecture of proposed on-chip sensor

2.1. Antifuse memory block

An antifuse is an electrical device which performs the opposite function to a fuse. An antifuse starts with a high resistance and is designed to create an electrically conductive path permanently (typically when the voltage across the antifuse exceeds a certain level). It is an OTP memory technology. The antifuse memory is a type of read-only memory (ROM) meaning the data in them is permanent and cannot be changed. Antifuse is non-volatile, area and power efficient, and has high reliability.

Most importantly, antifuse is confidential [20]. Before and after programming, the change on antifuse is extremely small, usually within tens of nanometers. In addition, there are thousands, even millions of antifuse in one component. So reverse engineering is almost impossible. As a result, it is ideal for storing the unique chip ID and activation time in an encrypted form. Additionally, since the antifuse memory is on-chip, additional system design measures may be taken to make the device tamper-proof, such as password protecting the antifuse memory within the system chip. This newer memory technology provides unprecedented physical layer security.

The antifuse memory block is used to store the unique chip ID and other assets for each chip. The antifuse memories are programmed in a programming environment with relatively 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.

2.2. 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. The two aging sensors will be discussed in detail in the following sections.

2.2.1. RO-based aging sensor

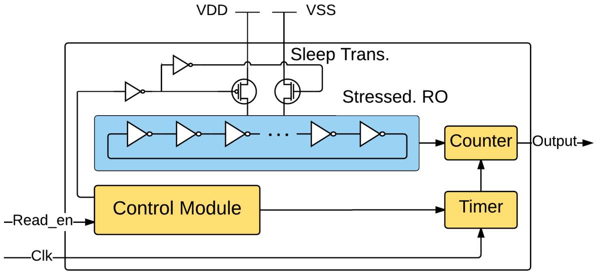


Figure 2: Structure of RO aging sensor

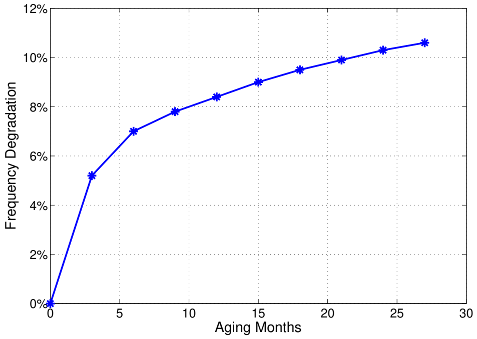
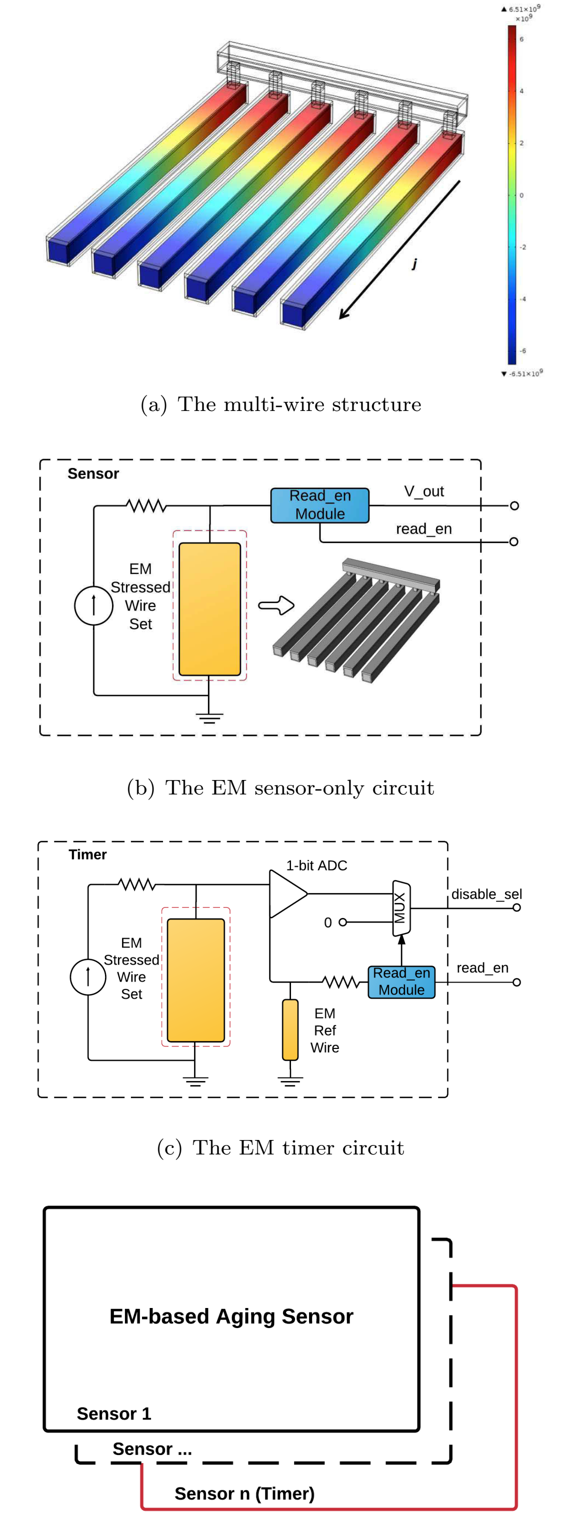


Figure 3: Frequency degradation of a 5-stages RO

In the new sensor design, the new RO-based sensor shown in Fig. 2 follows the similar design in [10]. However, the new RO-based sensor differs in that it only has one RO (compared to the two in the existing works [10]), as the reference frequency will be stored in the design house's database and can be assessed when the chip ID is read back by challenge-response pairs during the authentication process. The details of the whole flow will be discussed in the following section. Fig. 3 shows the typical frequency change over time for the RO-based sensor. As we can see, as time goes by, the frequency change rate goes down, which means that the sensitivity to frequency changes becomes smaller and it will become more difficult and less accurate to estimate time usage based on the frequency changes for long periods of time.



(a) The multi-wire structure

(b) The EM sensor-only circuit

(c) The EM timer circuit

(d) The whole aging sensor with multiple EM sensors and timers

Figure 4: The structure of EM aging sensor

2.2.2. EM-based aging sensor

Fig. 4 shows the schematics of the proposed EM-based sensor. This design follows the recent work in [12]. Fig. 4(a) represents the basic building block of the EM sensor module which is a multi-wire structure to be stressed inside the EM-based sensor and can be utilized in a variety of methods. The proposed EM-based sensor has two versions. One version is the aging sensor shown in Fig. 4(b). 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 measured after manufacturing and stored in the design-house's database as a reference. This output can used by the chip designers in a variety of way. In some cases, it could be read and stored internally, using an ADC for example, or measured externally using a port and a volt-meter. When the resistance of wires change by 10%, it can be considered as failed and the time difference between the activation time and current time is the time usage. Another version of the EM-based sensor is the timer version as shown Fig 4(c). In this case, a reference wire, which has the same geometry as the stressed wires, is used. This sensor, using a simple 1-bit ADC, will output a binary signal when the difference in resistance between the reference and stressed wires change significantly (by 10%). The signal can be utilized by the chip designers for many purposes such as locking the chip, or certain functions of the chip, upon sensor failure.

2.3. Encryption and Activation module

The encryption module is used to encrypt the data from antifuse blocks utilizing a challenge key that would stored in the design house's database. This module can be any existing encryption module, e.g., Advanced Encryption Standard (AES) method. It is used to make sure the unique chip ID and other 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 anti-fuse blocks. There are many ways to implement the chip-level activation process [21, 22]. For instance, we check the parity of the bits of the stored key in anti-fuse memory. We can also check the number of zeros or number of ones as well (bit stream written into antifuse memory needs to enforce some properties in this case). The checking circuit inside the activation module can be obfuscated for further protection. The output of the activation module can drive randomly scattered XOR gates in a chip to enable the unlocking process. This makes it very difficult for counterfeiters to modify the layout.

3. 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 on-chip sensor with antifuse memory.

Fig.5 shows a typical lifetime process that an IC goes through, which includes the design, fabrication, assembly, distribution, and usage in the system until the end of its life. As one can see, there are vulnerabilities associated with each step in this supply chain. In the design stage, an IP can be stolen and cloned. In the fabrication process, an IC can be overproduced. In the assembly phase, out-of-spec/defective ICs can be sold to open market by an untrusted assembly. Illegal activities during distribution and in-the-system (lifetime) may bring different types of counterfeits back into the supply chain (recycled, remarked, etc.).

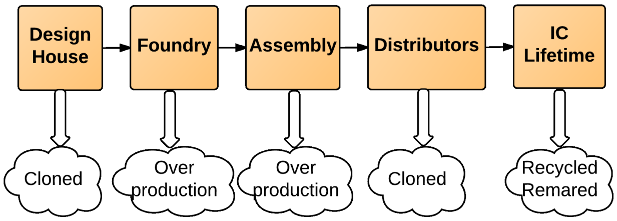


Figure 5: The electronic component supply chain and vulnerabilities

To detect all non-defective counterfeit ICs, we propose a new supply chain flow with post-fabrication authentication process as shown in Fig. 6. Basically, one needs to break the flow from assembly to the distribution. As shown in Fig. 7, once chips have been tested and packaged in the assembly stage, they will be sent back to the design house. After functional verification, 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's global database for future verification. All the information cannot be directly accessed and will be encrypted using a standard cryptography method to prevent attacks and tampering. Also during this process, the design house can activate the locked chip, which will not work after the fabrication process, using the unique content in the antifuse memory. In this way, the design house can have better control of the ICs to prevent cloning and other unauthorized use.

Fig. 8 shows the proposed comprehensive detection policy for counterfeit ICs. In general, a newly fabricated chip needs to pass two tests to be proven fresh and authentic. The first test is called *fingerprint* test. The design house device database generates a random challenge which can be inputted into the IC. If the IC cannot generate any response or outputs an incorrect response, then it has not undergone the official design house antifuse activation.

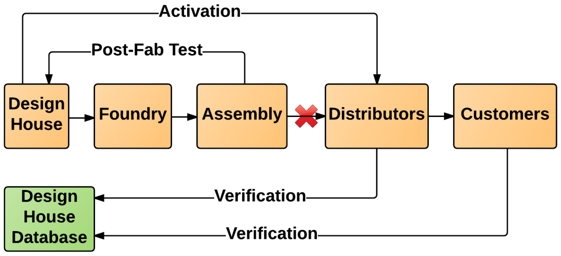


Figure 6: The proposed supply chain with post-fabrication authentication

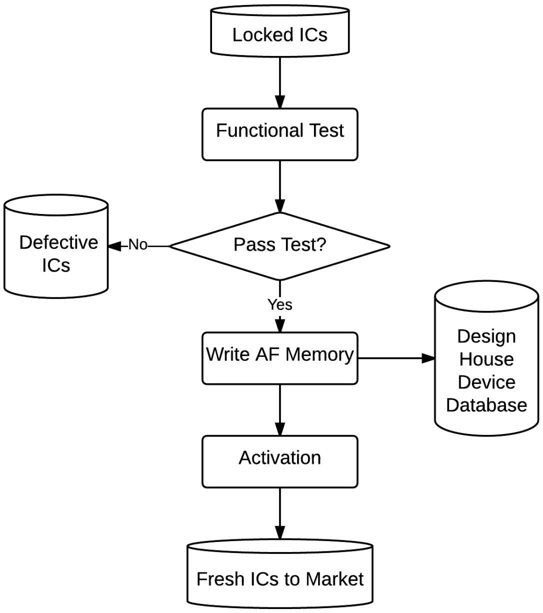


Figure 7: The proposed post-fabrication authentication

This means the IC never came back to the design house after fabrication. So it can be detected and categorized 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 is easy to determine if a chip is a remarked IC or not. The second test is called aging test. This test is performed to detect recycled or used ICs or to tell the user the estimated usage time of the chip. By reading the aging sensor output, we can detect if it is a recycled IC or not. Based on the aging model of the aging sensors employed and its aging output, we can accurately determine time usage of the chip.

4. Numerical results and discussions

In this section, we first summarize the feature comparison among different sensors, then we will present the simulated results of the RO-based and EM-based sensors. The performance and overhead analysis will be discussed.

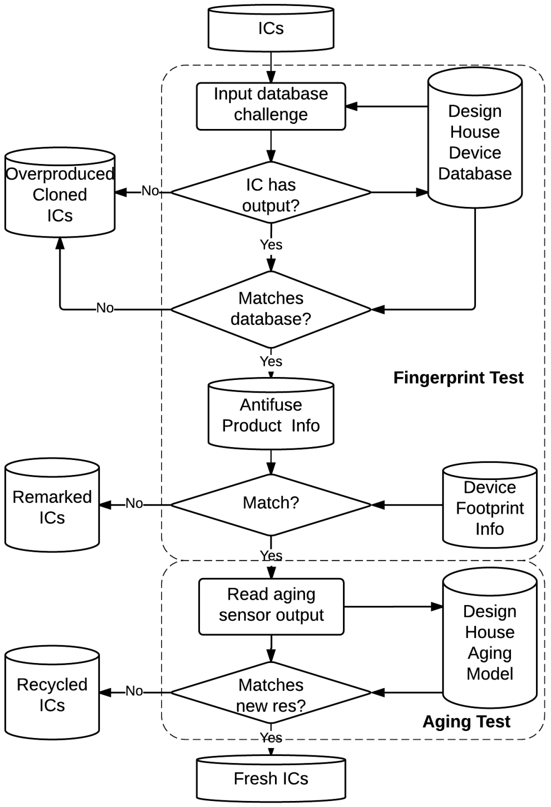


Figure 8: The proposed comprehensive detection methodology for counterfeit ICs

4.0.1. The feature and function comparison among different sensors

Table 1: 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

Table 1 summarizes the major feature comparison 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 also allow post-fabrication authentication to detect cloned and over-produced ICs. It also allows activation of the chip and timed services for ICs when it is used as an on-chip timer.

4.1. 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 [10], we considered two process variations to investigate the impact of variation on the detection of the recycled ICs. Table 2 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. Thousands of sensors are generated using MC simulation by HSPICE and the total aging time is set at 15 months with a 3-month step.

Table 2: 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. 9 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 do not need 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 f_{diff} distribution for 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 becomes 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. 9(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 is even larger.

Fig. 9(b) shows the frequency difference occurrence rate between the 7-stage new and stressed ROs with process variations PV1. Moving from PV0 to PV1, both the inter-die and intra-die variations becomes larger. As process variation increases, the variance in f_{diff} grows, which results in an overlap between 0 and 3,15M distributions. In this case, we should expect higher mis-prediction rates.

The simulation results for 15-stage ROs using same process variations are shown in Fig. 9(c) and Fig. 9(d). In comparison with the 7-stage RO, here the frequency difference between aged and new ICs is smaller. Although this impacts the absolute value of the frequency difference, the detection rate is not impacted significantly.

4.2. Results for EM-based aging sensor

The proposed EM-based aging sensor circuit has been designed and validated using SPICE simulation. We performed 1000 Monte Carlo simulations considering the variation in failure time for the stressed wires. The failure time can be defined as the time when the wire resistance increases by 10% of its original value, which can be predicted by the physics-based EM-model [23, 24].

MC simulations are conducted using HSPICE and MATLAB with the physics-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 a lognormal distribution [25].

The 1000 MC simulation results of the EM-based aging sensor are shown in Fig. 10. The variance of the lognormal distribution is set to 0.001. With 0.001 variance, we can see that with one wire, the EM lifetime will fall into ±10% lifetime mean with 99.83% chance and into ±5% lifetime mean with 88.64% chance. If we use 6 wires, we can have 100% chance to achieve ±10% life mean and 98.66% chance for ±5% life mean, which is sufficient. As we can see, we can mitigate the failure time variations by increasing the number of wires.

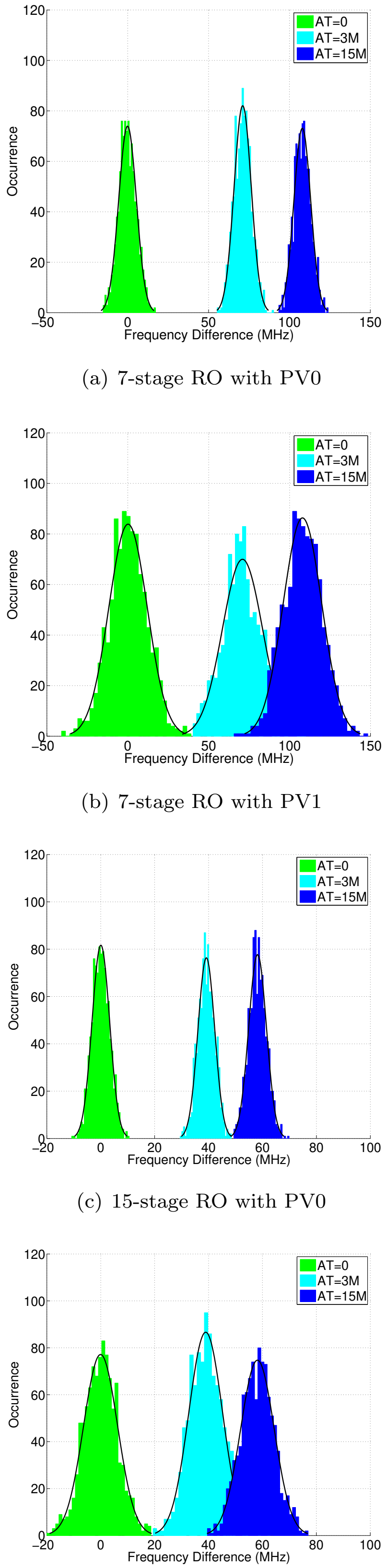
Fig. 11(a) shows the relationship between wire length L and EM lifetime. The current density j is constant and set to $3 * 10^{10} A/m^2$. We show both the nucleation time and the growth phase time predicted by the physics-based EM models. As we can see, the total lifetime increases with decreasing L (so does the area), which shows that shorter failure time will need larger area compared to the longer failure time.

Fig. 11(b) shows the power values versus the 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. We can clearly see the trade-off between L (area) and power.

4.3. Performance analysis and comparison

4.3.1. Accuracy study

Fig. 12 shows the typical frequency change over a long period of time for a 5-stage RO-based sensor. As we can see, the rate-of-change in frequency is very high at the beginning, which is helpful to detect recycled ICs for a short period of time. However, as time goes by, the rate-of-change in frequency goes down, which means that it will be more difficult and less accurate to estimate usage time for long periods of time. Considering the process variances,



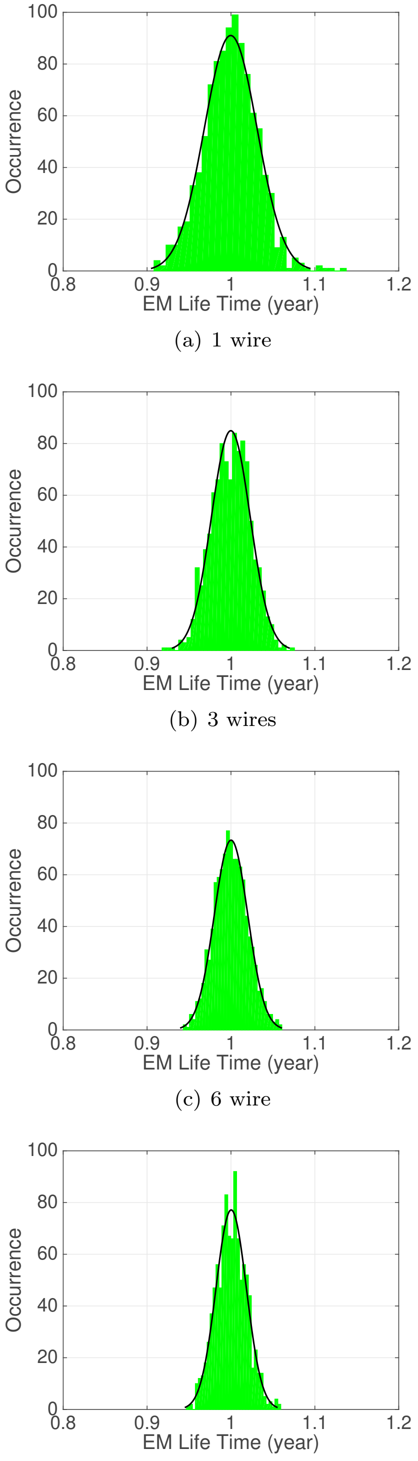
(a) 7-stage RO with PV0

(b) 7-stage RO with PV1

(c) 15-stage RO with PV0

(d) 15-stage RO with PV1

Figure 9: Process variation impacts on frequency spreading and recycled IC detection probability.



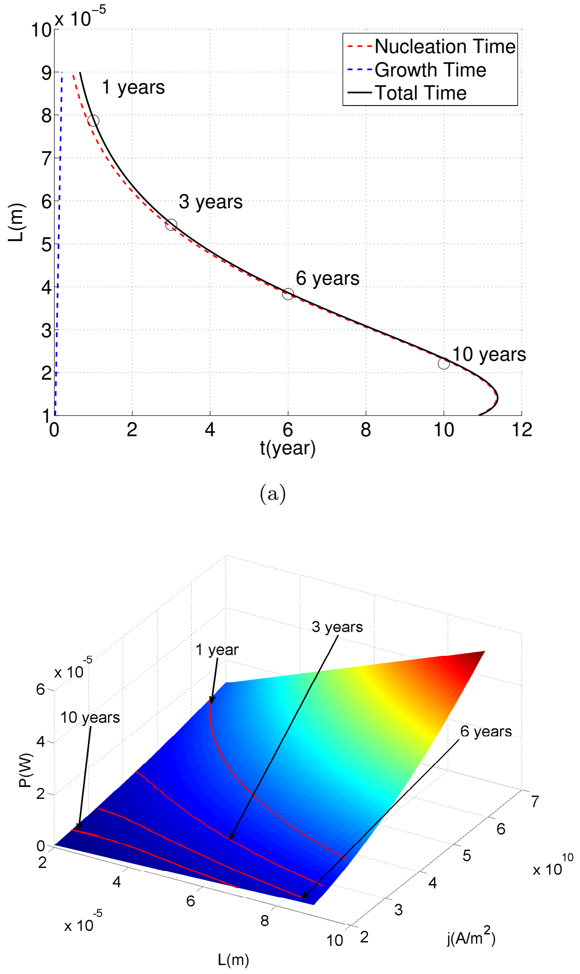
(a) 1 wire

(b) 3 wires

(c) 6 wire

(d) 10 wires

Figure 10: The statistical study of stressed wire set with different wire numbers



(a)

(b)

Figure 11: (a) Length versus EM lifetime of a wire. (b) The power consumption of stress wires versus wire length and current density.

1% frequency difference can lead to a large estimated usage time region (30 months as shown in Fig. 12). So the RO-based sensor is not a good timer for long period use. In contrast, the EM-based sensor can be a good long-period timer because of its accuracy. The estimated usage time region for a long period can be very small if we use multiple stressed wires [12]. In addition, as shown in Fig. 11(b), compared to the 1-year EM-based sensor, the 10-year EM-based sensor has smaller L(area). So the EM-based sensor for long-term use is also area-efficient.

4.3.2. Area overhead study

It's worth noting that the hybrid aging sensor can be inserted into commercial chips, which would easily detect the recycled ICs and show the age of the chip. The accuracy of the proposed sensor, and its feasibility due to it's low area overhead, makes it highly desirable. The RO-based sensor only takes n inverters, where n is the number of stages in RO. Its area is equal to tens of NAND2 gates, which is negligible in comparison to the whole chip. An EM-based aging sensor with 10 stressed wires costs 100-

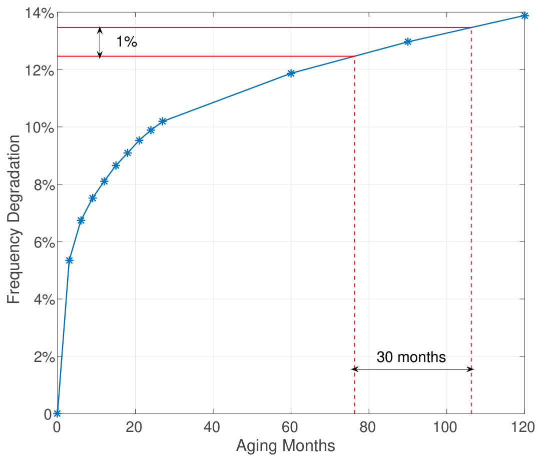


Figure 12: The RO-based aging sensor error rate for long period time

$500\mu m^2$ with an SMIC 180nm technology, which depends on the length of the wire. Assuming a total of 5 EM-based sensors, the overhead is only 0.01% of the $25{,}000{,}000\mu m^2$ area available in a 5 mm × 5 mm chip.

5. Conclusion

In this paper, we proposed a comprehensive counterfeited ICs detection and prevention strategy, consisting of an innovative multi-functional on-chip sensor, and the related post-fabrication authentication methodology. The proposed on-chip sensor can detect many types of counterfeit ICs. The new on-chip sensor, which combines aging sensors with antifuse memory, can also serve as a central on-chip security hardware IP for counterfeit IC detection, on-chip timer, post-fabrication authentication, and even activation module for ICs. In addition to the new sensor hardware, we propose a post-fabrication authentication process to detect and prevent non-defective counterfeit ICs. All the fabricated ICs will be uniquely registered and activated with a unique chip ID in a global database. The unique chip ID will be written into the anti-fuse memory during the registration process and the chip will be activated after this process. Simulated results show the advantage of the proposed multi-purpose sensor against the existing on-chip sensors 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, X. Zhang, Integrated Circuit Authentication, Springer, 2014.

[3] Trust-HUB, `http://trust-hub.org/home`.

[4] U.S. Department of Commerce, "Defense Industrial Base Assessment: Counterfeit Electronics," (Jan. 2010).

[5] U. Guin, D. DiMase, M. Tehranipoor, Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead, Journal of Electronic Testing 30 (2014) 9–23.

[6] L. Kessler, T. Sharpe, Faked Parts Detection, `http://smtcorp.com/ext/manual/united-el-article-2012-08-22.html` (2010).

[7] U. Guin, X. Zhang, D. Forte, M. Tehranipoor, Low-cost on-chip structures for combating die and IC recycling, in: Proc. Design Automation Conf. (DAC), 2014.

[8] U. Guin, D. Forte, M. Tehranipoor, Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling, IEEE Trans. on Very Large Scale Integration (VLSI) Systems 24 (2015) 1233–1246.

[9] X. Zhang, N. Tuzzio, M. Tehranipoor, Identification of recovered ICs using fingerprints from a light-weight on-chip sensor, in: Proc. Design Automation Conf. (DAC), 2012.

[10] X. Zhang, 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.

[11] J. Villasenor, M. Tehranipoor, Are you sure it's new? the hidden dangers of recycled electronics components, in: IEEE Spectrum, 2012.

[12] K. He, X. Huang, 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), 2015.

[13] Failure Mechanisms and Models for Semiconductor Devices, in JEDEC Publication JEP122-A, Jedec Solid State Technolgy Association, 2002.

[14] X. Huang, A. Kteyan, X. Tan, V. Sukharev, Physics-based electromigration models and full-chip assessment for power grid networks, IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems 35 (11) (2016) 1848–1861. `doi:10.1109/TCAD.2016.2524540`.

[15] H. Chen, S. X.-D. Tan, X. Huang, T. Kim, V. Sukharev, Analytical modeling and characterization of electromigration effects for multibranch interconnect trees, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 35 (11) (2016) 1811–1824.

[16] S. X.-D. Tan, H. Amrouch, T. Kim, Z. Sun, C. Cook, J. Henkel, Recent advances in EM and BTI induced reliability modeling, analysis and optimization, Integration, the VLSI JournalIn press. `doi:https://doi.org/10.1016/j.vlsi.2017.08.009`.

[17] F. Koushanfar, G. Qu, M. Potkonjak, Intellectual Property Metering, Springer, 2001.

[18] F. Koushanfar, G. Qu, Hardware Metering, in: Proc. Design Automation Conf. (DAC), 2001, pp. 490–493.

[19] M. Rahman, D. Forte, Q. Shi, G. Contreras, 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.

[20] kilopass White Paper, Three SoC Application Segments Require Embedded OTP Memory, =http://www.kilopass.com/wp-content/uploads/2010/04/Three-SoC-Application-Segments-Require-Embedded-OTP-Memory.pdf.

[21] Y. Alkabani, F. Koushanfar, Active hardware metering for intellectual property protection and security, in: Inproceedings of 16th USENIX security symposium on USENIX security symposium, 2007, pp. 1–16.

[22] A. Baumgarten, A. Tyagi, J. Zambreno, Preventing IC piracy using reconfigurable logic barriers, Vol. 27, 2010, pp. 66–75.

[23] V. Sukharev, Beyond Black's Equation: Full-Chip EM/SM Assessment in 3D IC Stack, Microelectronic Engineering 120 (2014) 99–105.

[24] X. Huang, T. Yu, V. Sukharev, S. X.-D. Tan, Physics-based electromigration assessment for power grid networks, in: Proc. Design Automation Conf. (DAC), 2014.

[25] J. R. Black, Electromigration-A Brief Survey and Some Recent Results, IEEE Trans. on Electron Devices 16 (4) (1969) 338–347.