Contents lists available at ScienceDirect

INTEGRATION, the VLSI journal

journal homepage: www.elsevier.com/locate/vlsi

Detection of counterfeited ICs via on-chip sensor and post-fabrication authentication policy☆

Taeyoung Kim[a], Sheldon X.-D. Tan[b,*], Chase Cook[b], Zeyu Sun[b]

[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*

ARTICLE INFO

Keywords:
Aging sensor
Hardware security
Electromigration
Reliability
Antifuse
Post-fabrication authentication
Counterfeit IC

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.

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

☆ 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.

[*] Corresponding author.
E-mail addresses: tkim049@cs.ucr.edu (T. Kim), stan@ece.ucr.edu (S.X.-D. Tan).

https://doi.org/10.1016/j.vlsi.2018.05.002
Received 10 October 2017; Received in revised form 23 February 2018; Accepted 7 May 2018
Available online 13 July 2018

focus on detecting defective ICs as they account for the majority of the counterfeit components [6–8].

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 Refs. [9–12].

The method in Ref. [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 Ref. [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 [14–16]. The design is also simple and lightweight 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 [17–19]. 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