Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs

Xuehui Zhang and Mohammad Tehranipoor, *Senior Member, IEEE*

***Abstract*— The counterfeiting and recycling of integrated circuits (ICs) have become major issues in recent years, potentially impacting the security and reliability of electronic systems bound for military, financial, or other critical applications. With identical functionality and packaging, it would be extremely difficult to distinguish recycled ICs from unused ICs. In this paper, two types of on-chip lightweight sensors are proposed to identify recycled ICs by measuring circuit usage time when used in the field. Recycled ICs detection based on aging in ring oscillators (ROs-based) and antifuse (AF-based) are the two techniques presented in this paper. For RO-based sensors, statistical data analysis is used to separate process and temperature variations' effects on the sensor from aging experienced by the sensor in the ICs. For AF-based sensor, counters and embedded one-time programmable memory are used to record the usage time of ICs by counting the cycle of system clock or switching activities of a certain number of nets in the design. Simulation results using 90-nm technology and silicon results from 90-nm test chips show the effectiveness of RO-based sensors for identification of recycled ICs. In addition, the analysis of usage time stored in AF-based sensors shows that recycled ICs, even used for a very short period, can be accurately identified.**

***Index Terms*— Circuit aging, counterfeiting, hardware security, recycled integrated circuits (ICs).**

I. Introduction

THE counterfeiting of integrated circuits (ICs) is on the rise, potentially impacting the security of a wide variety of electronic systems. A counterfeit component is defined as an electronic part that is not genuine because it [1]:

1) is an unauthorized copy;
2) does not conform to original component manufacturers design, model, or performance or both;
3) is not produced by the original component manufacturers or is produced by unauthorized contractors;
4) is an off-specification, defective, or used original component manufacturers' product sold as new or working;
5) has incorrect or false markings and/or documentation.

The Office of Technology Evaluation, part of the U.S. Department of Commerce, reported over 10 000 incidents involving the resale of used or defective ICs from 2005 to 2008 alone, which is much more than other types of counterfeits [1] (shown in Fig. 1). From this figure, the number of reported incidents of used ICs being sold as new or remarked as higher grade is much larger than other types of counterfeits. In 2008, Businessweek published an investigation that traced recycled ICs found in U.S. military supplies back to their sources [2]. It was reported in [3] that used or defective products considered 80%–90% of all counterfeits being sold worldwide. With such estimate on the percentage of used ICs being sold, and the numbers relating to semiconductor sales and counterfeiting in general presented in [4], it could be possible that the intentional sale of used or defective chips in the semiconductor market could have considered about $15 billion of all semiconductor sales in 2008 alone. This number could actually be much larger as many of the counterfeit ICs go undetected and are being used in systems today. In addition, from Fig. 1, the trends, shown in [1], suggest that this number is only going to increase over time.

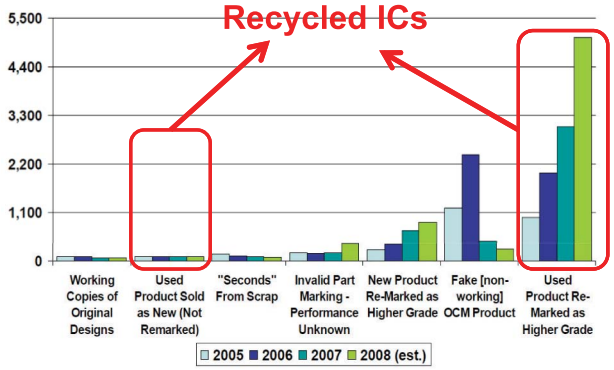


Fig. 1. Counterfeit incidents by type of problem for microcircuits from 2005 to 2008.

These used or defective ICs enter the market when electronic recyclers divert scrapped circuit boards away from their designated place of disposal for the purposes of removing and reselling the ICs on those boards. As the recycling process usually involves a high-temperature environment to remove ICs from boards, there are several security issues associated with these ICs: 1) a used IC can act as a ticking time bomb [5] as it does not meet the specification of the unused (new) ICs and 2) an adversary can include additional die on top of the recycled die carrying a back-door attack, sabotaging circuit functionality under certain conditions, or causing denial of service [6]. Therefore, it is vital that we prevent these recycled ICs from entering critical infrastructures, aerospace, medical, and defense supply chains.

In this paper, the term recycled ICs is used to denote used ICs being sold as new or remarked as higher grades. The terms unused ICs and new ICs represent the ICs that are brand new. On the other hand, most ICs used in the field are not turned on all the time. Consider an IC used in a cell phone, for

Manuscript received October 26, 2012; revised March 22, 2013; accepted May 9, 2013. Date of publication June 21, 2013; date of current version April 22, 2014. This work was supported by the Army Research Office under Grant 57958CS.

The authors are with the Electrical and Computer Engineering (ECE) Department, University of Connecticut, Storrs, CT 06250 USA (e-mail: xuehui.zhang@engr.uconn.edu; tehrani@engr.uconn.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2013.2264063

example; the cell phone may only be powered on during the day for some period. The real (power-on) usage time of the IC would be much shorter than the usage time with power-off intervals. In this paper, the term usage time is used to represent the accumulated power-on time even if the IC is used intermittently.

In general, the recycled ICs have the original appearance, functionality, and markings as the devices they are meant to mimic, but they are used for a period before they are resold. Even the best visual inspection techniques will have difficulty in identifying these ICs with certainty [7]. Additionally, because recycled ICs contain the original correct die internally, decapping technologies will provide little assistance in their detection. It is vital to develop new techniques to help in measuring these ICs' specifications and effectively detect them if they are already used in the field even for a short period.

A. Previous Work

Physical unclonable functions (PUFs) implemented challenge and response authentication for IC identification [12]–[16]. For each physical stimulus, the circuit will react in an unpredictable way because of the complex interaction of the stimulus with the physical structure of the PUF and the inherent process variations. As the physical variations for each IC are unique, a distinct ID can be obtained for each IC through the PUF. Techniques to protect ICs against counterfeiting via active and passive authentication and identification (also known as hardware metering) were proposed in [17]–[19]. Metering techniques attempt to ensure that overproduction of ICs will be prohibited. The above approaches are effective at authenticating ICs but not at identifying recycled ICs as they are expected to have the same IDs as the unused ICs.

The computer-aided design and reliability research community has also seen extensive research on analyzing the aging of ICs. In particular, ring oscillator (RO)-based reliability analysis has become a common practice. For instance, a silicon odometer was proposed to monitor different types of aging effects [20], [21]; however, the objective was to improve the reliability of ICs, not to identify the recycled ICs. Such sensors will be ineffective if they are to be used in detecting recycled ICs because of the presence of process and environmental variations.

The work in [9] and [10] addressed detection of recycled ICs. The first attempt to identify recycled ICs was presented in [9] using an RO-based sensor. The simulation and silicon results demonstrated the effectiveness of this approach. The additional analysis of this sensor will be discussed in this paper to distinguish the impact of process and environmental variations from usage time on ICs. A path delay-based technique is also proposed using clock sweeping techniques to generate fingerprints to identify recycled ICs [10]. Without any area overhead, this technique could be applied to all kinds of digital ICs—even those without sensors.

In addition, physical tests and inspections, described in [8], are often used to identify recycled ICs by visual inspection, blacktop testing, scanning electron microscopy, scanning acoustic microscopy, X-ray imaging, X-ray fluorescence, Fourier transform infrared spectroscopy, and so forth. These methods can efficiently detect recycled ICs with gross defects, such as defects in package, lead, bond wires, and so forth. They, however, cannot detect recycled ICs without these physical defects. Moreover, all the ICs under physical test cannot be verified as most of these tests are based on sampling and decapping. On the other hand, electrical detection methods can be applied to all the ICs under test. SAE AS5553 [8] incorporated some electrical tests such as dc curve trace, full dc test, key (ac, switching, and functional), and full functional tests at ambient temperature and over temperature in their detection procedure. The applicability of these tests to today's complex ICs (microprocessors, memories, programmable logic devices, ASICs, etc.,) are, however, of major concern. Detection of recycled ICs using electrical tests is not yet verified completely and there are currently no available documents to guide recycled ICs detection using electrical tests. In addition, physical and electrical tests are extremely expensive and time consuming. Therefore, new techniques need to be developed to address this global recycling problem.

B. Contributions and Paper Organization

The major difference between recycled ICs and unused ICs is that recycled ICs are already used and experienced aging, as they are removed from their original boards and resold in the market. Aging effects, such as negative-bias temperature instability (NBTI) and hot-carrier injection (HCI), would have had an impact on the performance of the recycled ICs because of the change in threshold voltage. In this paper, we propose two techniques using lightweight sensors (RO-based and AF-based) to help with the detection of recycled ICs.

The RO-based sensor is composed of a reference RO and a stressed RO. The stressed RO is designed to age at a very high rate using high threshold voltage (HVT) gates to expedite aging hence ICs used for a period can be identified. The reference RO is gated off from the power supply during chip operation, hence it experiences less stress. The frequency difference between the two ROs could denote the usage time of the chip under test (CUT); the larger the difference is, the longer the CUT is used, and with a higher probability the CUT could be a recycled IC. With close placement of the two ROs in the RO-based sensor, the impact of intradie process variations could be minimized. Data analysis can effectively distinguish the frequency differences caused by aging from those caused by temperature and interdie process variations, to identify recycled ICs, which is demonstrated by our simulation and silicon results. The RO-based sensor presents a negligible area overhead, imposes no constraint on circuit layout, and is resilient to removal and tampering attacks. The three working modes of the RO-based sensor proposed in this paper ensure that the reference RO cannot be gated on alone, thus the frequency difference between the two ROs cannot be changed to mask detection.

The AF-based sensor, composed of counters and an embedded antifuse (AF) memory block, is also proposed to identify recycled ICs. The counters are used to record the usage

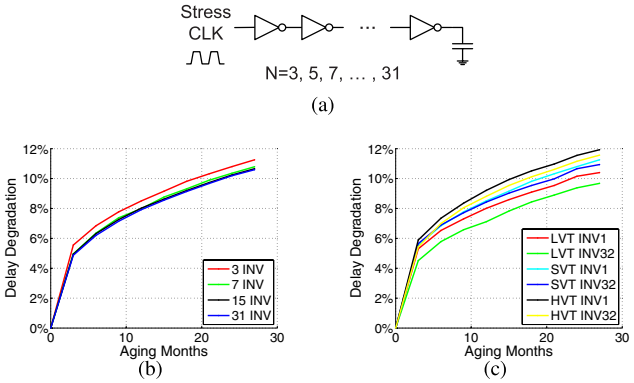


Fig. 2. (a) Inverter chain structure. (b) Degradation of inverter chains with different lengths (stage count). (c) Degradation of a three-inverter chain with different inverter types.

time of ICs and the value is dynamically stored in the AF memory block by controlling the programming signal. As the AF memory block is one-time programmable (OTP), recyclers could not erase the context during recycling process. Therefore, our AF-based sensor is resilient to removal and tampering attacks. Two different structures of AF-based sensor are proposed to measure the usage time of ICs in this paper.

1) AF-based sensor using clock AF (CAF-based) records the cycle count of the system clock during the chip operation. The usage time of recycled ICs can be reported by this sensor and the measurement scale and total measurement time could be adjusted according to the application of ICs.
2) AF-based sensor using signal AF (SAF-based) transition selects a certain number of signals with low switching probability and records their switching activities to calculate usage time to detect recycled ICs with less area overhead compared with CAF-based sensor.

The rest of this paper is organized as follows. Section II outlines the necessary background and analyzes the impact of aging on different circuit elements and ROs. Section III presents the architecture of sensors including RO- and AF-based sensors, Experimental results and analysis are presented in Section IV. Finally, our concluding remarks are given in Section V.

II. Background

In this section, we will briefly describe aging phenomenon in ICs and present their impact on different circuit components, which will be used in our RO-based sensor. The AF OTP memory used in the AF-based sensor will also be briefly introduced in this section.

A. Aging Analysis

When the chip operates in functional mode, the transistors age mainly because of NBTI and HCI. The aging effects of NBTI and HCI could cause parametric shifts and circuit failures, as demonstrated by reliability models [22], [24], [25]. NBTI occurs when a negative gate-to-source voltage is applied at the p-type MOS (pMOS) transistors, which breaks Si–H bonds generating the interface traps. These interface traps can increase the absolute value of the pMOS threshold voltage (V_{th}), resulting in reduced transistor current and increased gate delay. Equation (1) shows the shift of V_{th} caused by NBTI [28]

$$\Delta V_{\text{th}} = \frac{q N_{\text{it,NBTI}}(t)}{C_{\text{ox}}} \tag{1}$$

where C_{ox} is the gate oxide capacitance, q is the electronic charge, and $N_{\text{it,NBTI}}(t)$ is the number of interface traps, which will increase as the transistors continue to operate in the field. HCI occurs when the electron or hole in transistors gains sufficient energy to overcome silicon dioxide barrier to break an interface state. The silicon substrate/gate dielectric interface and dielectric bulk traps caused by HCI can impact device parameters including threshold voltage, shown in

$$\Delta V_{\text{th}} = \frac{q N_{\text{it,HCI}}(t)}{C_{\text{ox}}} \tag{2}$$

where $N_{\text{it,HCI}}(t)$ is the number of interface traps caused by HCI.

As recycled ICs are impacted by these aging effects when used in the field, the circuit parameters of recycled ICs would be different from those of new ICs. If a fast-aging sensor is embedded into the circuit to help detect its usage, then recycled ICs could be identified.

To verify the effects of aging on a circuit's performance, several different inverter chains are simulated using Synopsys 90-nm technology [23]. The delay of these inverter chains will represent the circuit's performance. The simulation is conducted using HSPICE MOSRA (Synopsys' reliability analysis tool) with combined NBTI and HCI aging effects at 25 °C. Fig. 2(a) shows the basic structure of the inverter chains with the same capacitive load and the same stress coming from a 500-MHz clock. These chains are composed of 3, 7, 15, and 31 standard threshold voltage (SVT), HVT, and low threshold voltage (LVT) inverters. Fig. 2(b) shows the delay degradation of inverter chains under clock stress for up to 27 months with no interrupt. From this fig, the number of inverters does not have a significant impact on the degradation of these chains as they receive the same stress, and each inverter's speed degrades at the same rate. Aging effects are also dependent on device's threshold voltage. The three-inverter chains are simulated using SVT, HVT, and LVT and two different size inverters (INVX1 and INVX32). Fig. 2(c) shows that the chain with the HVT inverters experiences more degradation than the chains with SVT or LVT inverters. The INVX1 inverter chain has a larger degradation than the INVX32 inverter chain.

NAND and buffer (BUF) gate chains with HVT are also simulated at 25 °C with a 500-MHz clock stress. The basic structure of these chains is the same as the inverter chains. A NAND gate will function as an inverter when its two inputs are connected together. Fig. 3 shows the simulation results. From this fig, the gate type does not impact the aging speed significantly. The inverter chain, however, ages slightly faster than the others, whereas the NAND gate chain and the BUF chain age at almost the same speed. The difference in the amount of aging depends on the structure of gates. Therefore, inverters (INVX1) with HVT will be used to create the ROs used to detect recycled ICs in our simulation.

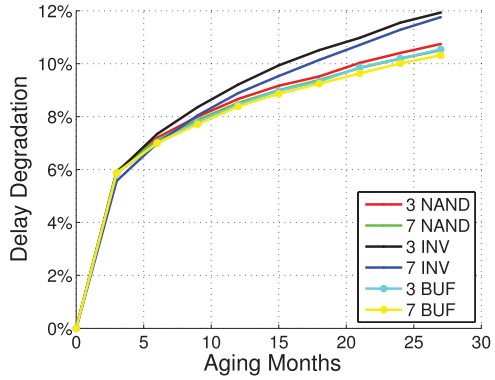


Fig. 3. Delay degradation of NAND, BUF, and INV chains.

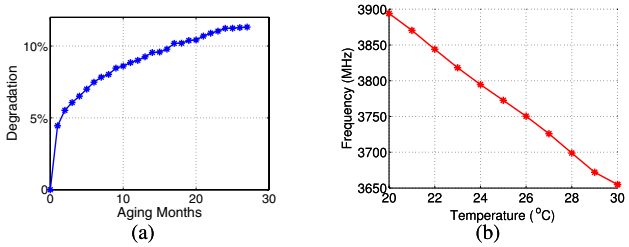


Fig. 4. (a) Frequency degradation of a five-stage RO. (b) Frequency of a five-stage RO decreases with increasing temperature.

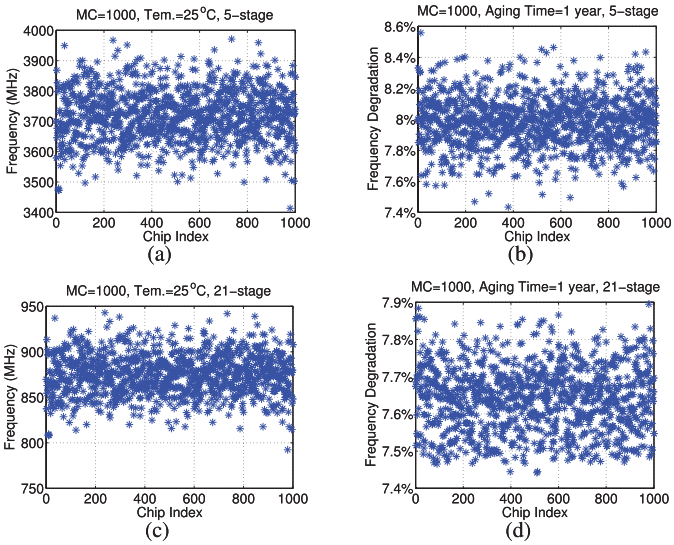


Fig. 5. (a) Frequency of a five-stage RO varying with process variations. (b) Frequency degradation of a five-stage RO aging for one year varying with process variations. (c) Frequency of a 21-stage RO varying with process variations. (d) Frequency degradation of a 21-stage RO varying with process variations.

Fig. 4(a) shows the frequency degradation of a five-stage RO with HVT inverters after aging for 27 months. The frequency of the RO in a recycled IC will be smaller than in a new IC. If there are no environmental or process variations, we could easily identify recycled ICs by measuring the frequency of the RO embedded in the circuit. The variations, however, have a significant impact on the frequency of ROs. Fig. 4(b) shows that the frequency of the five-stage RO will decrease as we increase the temperature, and that the frequency variation could be very large. Increasing temperature can also increase the degradation of the circuit.

The 1000 Monte Carlo (MC) simulation results of the five-stage RO are shown in Fig. 5(a), at a temperature of 25 °C with 3σ: 2% Tox, 5% Vth, and 5% L interdie variations and 1% Tox, 5% Vth, and 5% L intradie variations. The frequency of the RO can vary as much as 20% under process variations. In addition, process variations impact the aging rate of the RO, as shown in Fig. 5(b). The frequency degradation of the 1000 chips varies around 8% (7.4%–8.6%) for one year of aging. This frequency shift caused by the aging effects in recycled ICs can help separate them from those caused by process variations in new ICs if we try to use ROs to detect recycled ICs.

With a fixed stress, the number of inverters does not have a significant impact on an inverter chains' delay degradation. The frequency of an RO is, however, related to the number of inverters, $f = 1/2 * n * t_d$, where n is number of stages in the RO and t_d is the delay of an inverter. Fig. 5(a) shows the frequency shift of a 21-stage RO with HVT inverters. The frequency degradation is shown in Fig. 5(b). Comparing the frequency degradation of the five-stage and 21-stage ROs, the five-stage RO experiences slightly more degradation as its oscillation frequency is higher than the 21-stage RO. A five-stage RO may, however, require a very fast counter which might be difficult to design for timing closure. We will discuss this in detail in Section IV.

B. AF Memory

An AF is an electronic device that changes state from nonconducting/high resistance to low resistance in response to electrical stress. With sufficiently high voltage/current, a large power dissipation in a small area will melt a thin insulating dielectric between polysilicon and diffusion electrodes and form a thin, permanent, and resistive silicon link. The programming performed after manufacturing is irreversible and permanent in AF cells, which will be used in our AF-based sensor to store the usage time of ICs.

The AF-based sensor is composed of counters with usage time of ICs when power-on stored in an embedded AF OTP memory block during the chip operation. Otherwise, the data may be erased or altered in power-off mode by attackers. The reasons for using an AF block in the AF-based sensor are [30] as follows: 1) it consumes less power to program or read compared with other types of OTP structures, such as electrical fuse or CMOS floating gate; 2) the area of an AF is much smaller than an efuse; and 3) it does not require additional mask or manufacturing handing steps during fabrication.

Most AF memories are, however, programmed in a programming environment with relatively high voltage/current. Therefore, integrated charge pumps or voltage multipliers are used to provide sufficiently high voltage/current [31], [32] in embedded AF OTP memories. With those charge pumps or voltage multipliers, no additional power supply is required during programming. The typical interface of the embedded AF memory is shown in Fig. 6 [31], [32], including power supply, address, prog, and data signals. We will use existing

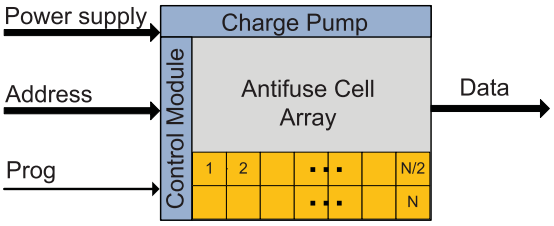


Fig. 6. Typical interface of AF memory.

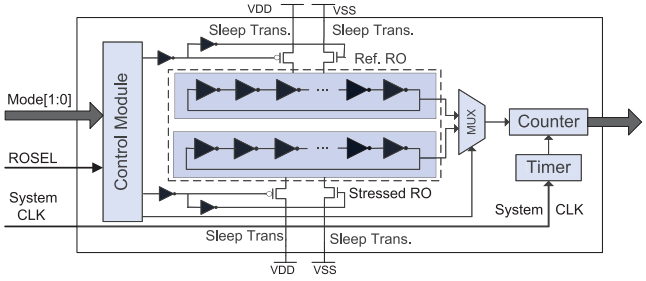


Fig. 7. Structure of the RO-based sensor.

AF blocks with the interface shown in Fig. 6 instead of designing a new embedded AF structure in our AF-based sensor as embedded AF memory is only a small part of the sensor.

III. Recycled-IC Detection Sensors

Two different sensors to identify recycled ICs are proposed in this paper. RO-based sensor is based on the aging differences between two ROs to record the usage time of ICs. RO-based sensor does not require any memory element to store the usage time as it is hidden in the degraded RO frequency because of aging. AF-based sensors count the system clock or the switching activity of signals in the design and store the usage time in an AF OTP block. The two sensors will be discussed in detail in the following sections.

A. RO-Based Sensor

Our main objectives in designing the RO-based sensor are as follows: 1) the sensor must age at a very high rate to help detect ICs used for a short period; 2) the sensor must experience no aging or negligible aging during manufacturing test; 3) the impact of process variations and temperature on RO-based sensor must be minimal; 4) the sensor must be resilient to attacks; and 5) finally, the measurement process must be done using low-cost equipment and be very fast and easy.

As mentioned earlier, aging effects could slow down the frequencies of ROs embedded into ICs. With an embedded RO, these recycled ICs could be identified based on its frequency, which will be lower than that of a new IC. There are, however, many parameters impacting the frequency of an RO, such as temperature and process variations. Our RO-based sensor uses a reference RO and a stressed RO to separate the aging effects from process/environmental variations.

Fig. 7 shows the structure of our RO-based sensor, which is composed of a control module, a reference RO, a stressed RO, a MUX, a timer, and a counter. The counter measures the cycle count of the two ROs during a prespecified time, which is controlled by the timer. System clock is used in the timer to minimize the measurement period variations because of circuit aging. The multiplexer (MUX) selects which RO is going to be measured, and is controlled by the ROSEL signal. The reference and stressed ROs are identical; both are composed of HVT components. The inverters in Fig. 7 could be replaced by any other types of gates (NAND, NOR, etc.,) only if they can construct an RO. It will not change the effectiveness of the RO-based sensor significantly according to the analysis in Section II. We use smaller stage ROs in our RO-based sensor considering the counter's measurement speed limits given a technology. For example, in our 90-nm technology, a 16-bit counter can operate under frequency of up to 1 GHz; an inverter-based RO of at least 21 stages is then required.

Sleep transistors are used to connect the ROs to the power supply in the RO-based sensor; pMOS sleep transistors control the connection between VDD and the inverters and n-type MOS sleep transistors control the connection between VSS and the inverters. Both the reference and the stressed ROs work in three modes that are controlled by the mode signal.

1) When the IC is in manufacturing test mode, the reference and stressed ROs will be disconnected from the power supply and experience no aging. This mode only lasts a short time, depending on the test procedures of the IC;
2) When the IC is in normal functional mode, the reference RO will be disconnected from VDD and VSS but the stressed RO will be gated on and will age. The frequency of the stressed RO will drop, whereas the reference RO will not change a lot. ICs will spend most of their time in this mode;
3) When the IC is in authentication mode (i.e., when an IC is taken from market and its authenticity is to be verified), both the reference and stressed ROs will be gated on by connecting to the power supply.

The timer and counter will be enabled to measure ROs' cycle count and ROSEL signal will select which RO to measure. The rest of the functionality of the IC would be turned off by mode signals and the authentication process takes a very short period. The three modes of operation ensure that 1) the frequency difference between the reference and stressed ROs will be larger over time as the reference RO cannot be gated on alone and 2) it is extremely difficult for adversaries to force the RO-based sensor to operate in authentication mode when it is supposed to be in its normal functional mode, which would eliminate the aging difference. The only method to do that would be to modify the original RO-based sensor module, which is impossible during a simple recycling process.

As shown in Fig. 7, the inverters of the reference and the stressed ROs are placed physically next to each other, designed as a single small module. The process and environmental variations between them should be very small. Therefore, for a new IC, the frequency difference between the reference and the stressed ROs would be within a certain small range. In a recycled IC, the stressed RO will have suffered aging

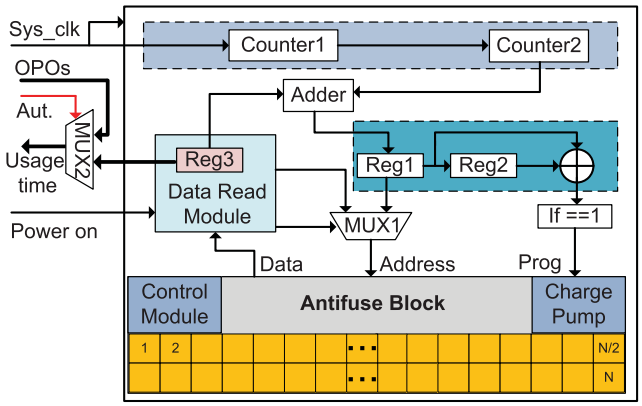


Fig. 8. Structure of the CAF-based sensor.

```
Algorithm for Data Read
01:  initial address = (N/2);
02:  for (i = log(N/2), i > 0, i − −) {
03:      if ([address] == 1)
04:          address = address + 1;
05:          if ([address] == 0)
06:              address = address − 1, $stop;
07:          else
08:              address = address − 1;
09:          address = address + 2^(i−1);
10:      else
11:          address = address − 2^(i+1);
12:  }
```

Fig. 9. Algorithm for data read in CAF- and SAF-based sensors.

from its own oscillation since the chip has been working in normal functional mode for a long time. The reference RO, however, will not have experienced as much aging as it is gated off. The frequency difference between the reference and the stressed ROs will grow larger as the chip operates longer, which is demonstrated by our simulation and silicon results. If the frequency difference is outside of the new ICs' frequency difference range considering process variations, we can conclude with high confidence that the CUT is recycled from used boards. The area overhead of our RO-based sensor is negligible when compared with the millions of gates in modern ICs. Power consumption is also limited to that consumed by the stressed RO in the RO-based sensor. Moreover, the test overhead caused by the RO-based sensor is minimal as it is composed of such a small number of standard gates. In addition, the RO-based sensor can be functional. We can argue that the starting time point of the sensors will be shifted from 0 to some aging time (such as weeks), which makes it difficult to distinguish used and new ICs. As for the impact of the testing process on the sensor, both ROs are kept in off mode using the sleep transistors thus the impact of aging and high temperature during test process will be negligible. Therefore, the starting point will remain the same. In early life failure of the sensor, more than one sensor can be added to the design. This will ensure that one sensor is operating properly in the field.

B. AF-Based Sensor

In the RO-based sensor, the inverters of the reference and the stressed ROs are placed physically next to each other to minimize the impact of intradie process variations. It may still be, however, difficult to completely exclude the impact of interdie process variations on the sensor. In addition, RO-based sensor provides only an approximation of the usage time in a form of aging in the stressed RO. Therefore, the sensitivity (the minimum usage time of recycled ICs detected by sensors) of the RO-based sensor is limited. For example, it may not identify recycled ICs used shorter than 1 month based on our simulation. To eliminate the issue of process variations, provide a more accurate usage time, and identify recycled ICs that are only used for a very short period (such as one day), we propose two AF-based sensors: CAF-based sensor and SAF-based sensor.

1) CAF-Based Sensor: Fig. 8 shows the structure of the CAF-based sensor, which is composed of two counters, a data read module, an adder, and an AF OTP memory block. Sys_clk in the figure is the high-frequency system clock, providing clock for different modules including the data read module, the AF block, and registers. Counter1 is used to divide the high- frequency system clock to a lower frequency signal, as shown in Fig. 8. Counter2 is used to measure the cycle count of the lower frequency signal. The size of the two counters can be adjusted accordingly depending on the measurement scale (T_s: the time unit reported by the sensor) and the total measurement time (T_{total}). For example, if T_s is 1 h and T_{total} is one year based on the specification of an IC, a 38-bit counter1 will meet the requirement to count the usage time from 20 ns (assume system clock = 50 MHz) to 1 h and a 14-bit counter2 will count the usage from 1 h to 8760 h (one year).

As the data stored in registers (counters) could be lost or reset when power supply is off, nonerasable memory is required in this sensor. An embedded AF OTP block is used instead of a field-programmable read-only memory (FPROM) to store the usage time information because FPROM could be tampered or altered by attackers. In the AF block, prog is assigned to be $1'b1$ if the value in counter2 increases by 1. Through connecting the output of counter2 to address in the AF block directly, the related AF cell will be programmed as 1. Therefore, the largest address of the cell whose content is 1 will be the usage time of CUT based on the measurement scale setup by counter1. From the above description, the size of the AF block will be reduced using two counters.

Program and read operations, however, share the same address signals in AF block. Therefore, a MUX (MUX1 in Fig. 8), controlled by data read module, is used to select the address (AF cell) to be read or programmed. Every time power supply is on, the AF block will work in read mode for a short period. During this time, the read address generated by data read module will go through MUX1 and all the AF cells will be traversed based on the traversing binary tree principle. Fig. 9 shows the algorithm for data read in an N-bit AF block. From Fig. 9, there are $\log(N/2)$ loops in the algorithm. The address is increased or decreased by $2^{i-1}[i = 0, \ldots \log(N/2)]$ for the ith loop based on the value in the

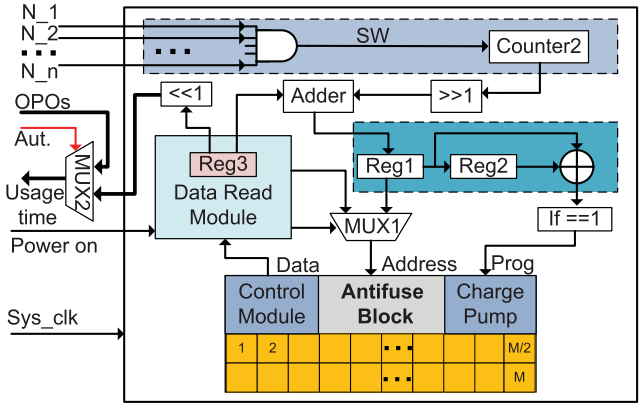


Fig. 10. Structure of the SAF-based sensor.

address. If the value stored in the address is 1 ([address] == 1) and the value stored in the next address is 0, the address will represent the usage time before power-on based on T_s. The read operation will last less than $\log(N/2) + 1$ system clock cycles, depending on the value stored in the AF block; this time will be recorded by counter1, as well.

Once we get the previous usage time, it will be stored in register Reg3 and sent to the adder. The reason for using an adder here is that counters start from 0 every time the power is turned on and the previous usage time must be considered when we calculate the total usage time. In addition, Reg1 is used to sample the data in adder, Reg2 delays the data in Reg1 with one system clock, and XOR gates are used to compare the data in Reg1 and Reg2. If they are different (denoting the usage time increased), the AF OTP block will work in program mode and the data in Reg1 will go through MUX1 to the address in the AF block. Therefore, combined with the value in counter2 (the usage time after power-on), the new total usage time will be stored in the AF OTP block by programming a new AF cell with a larger address. From this discussion, the AF OPT block is programmed internally. Through designing our sensor in this way, we can reduce the probability of altering or tampering attacks on the AF-based sensor.

To eliminate the need for additional pins for authentication purposes on the chip, our CAF-based sensor uses a MUX (MUX2) and an authentication (Aut.) pin to send the usage time to the output pins of ICs. Thus, no extra output pins will be added to the original design. When the IC works in normal functional mode, original primary outputs will go through MUX2. If the IC is in authentication mode by enabling the authentication signal, the data read module will set the AF IP in read mode and the usage time will go through MUX2. In addition, when the IC works in manufacturing test mode, the functionality of our CAF-based sensor will be disabled and structural fault test patterns will be applied to the sensor. The overhead of CAF-based sensor will be compared with the SAF-based sensor in detail in Section IV.

2) SAF-Based Sensor: With two counters, the area overhead of CAF-based sensor could still be considered large for smaller designs. To reduce the area overhead, we propose SAF-based sensor based on signals' switching activity (SW), as shown in Fig. 10. Comparing Fig. 10 with Fig. 8, the structure of SAF-based sensor is similar to that of CAF-based sensor. The difference is that CAF-based sensor counts the cycle of system clock to record the usage time of ICs, whereas SAF-based sensor counts the switching activity (positive edge) of a certain number of nets in the design. With simulations, a certain number of nets are selected to be the input of an AND gate. The rule of nets selection is that the switching activity of the output of the AND gate must meet the requirement of the measurement scale. For example, if T_s is 1 h, one of the choices could be four nets with SW(N_1) = 30/60 min, SW(N_2) = 24/60 min, SW(N_3) = 25/60 min, and SW(N_4) = 24/60 min, respectively. With different functional inputs, the SW, however, could be significantly different. Therefore, only the signals with consistent SW under different inputs are selected when we design a SAF-based sensor. From the analysis, the net selection could be adjusted based on different designs and measurement scales. Then, the positive pulse of the output of the AND gate (SS signal in Fig. 10) will be counted by counter2 in the sensor.

To further reduce the area overhead, an one-bit right shifter is used to divide the value in counter2 by 2 and then the largest address of AF cells with 1 will represent [SW/2]. An one-bit left shifter is used to calculate the switching activity by [SW/2] $*$ 2. The recorded SW will represent usage time of ICs. Therefore, the number of AF cells in SAF-based sensor will be reduced compared with CAF-based sensor. The accuracy of SAF-based sensor is, however, lower than CAF-based sensor because: 1) it is based on the switching activity of a certain number of nets in the netlist, whereas CAF-based sensor counts the cycle count of the system clock; and 2) the SAF-based sensor loses part of the usage time information because of the shifters.

Scan-based test approach would be considered for testing the AF-based sensors. Compared with RO-based sensor, the area overhead of the two AF-based sensors is larger because of the counters and the AF OTP block. Therefore, the manufacturing test cost will be larger, depending on the area overhead and measurement scale. The area overhead and test overhead are, however, still negligible when compared with the millions of gates in modern ICs. The major advantage of AF-based sensor over RO-based sensor is that the usage time stored in the AF-based sensors to identify recycled ICs will not be impacted by technologies (i.e., older technology designs do not age as much as the new ones do), packages, assemblies, or process variations. Even if the design is fabricated at different times in different foundries, the AF-based sensor could still show how long CUT has been used. In addition, AF-based sensors could identify recycled ICs used for a very short period, such as one day, because of the small measurement scale.

IV. Results and Analysis

In this section, we will present the experimental results of the RO- and AF-based sensors including simulation results and silicon results from test chips. Attack analysis on the two sensors will also be discussed.

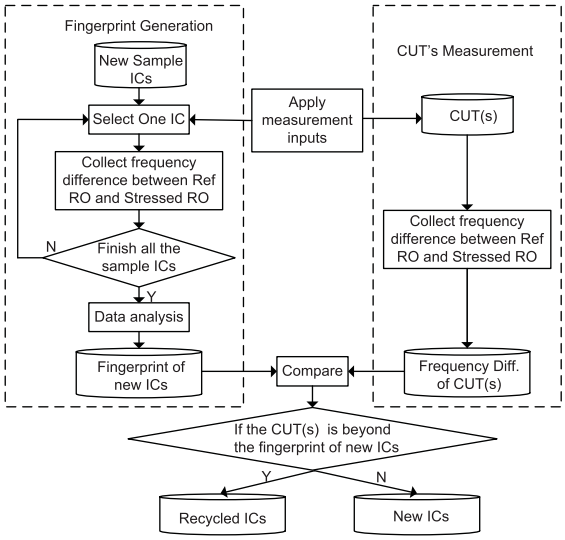


Fig. 11. Measurement flow using RO-based sensor for identifying recycled ICs.

A. RO-Based Sensor

Fig. 11 shows the proposed measurement flow using RO-based sensor for identifying recycled ICs in our experiments. This is done only for the purpose of validation of our proposed sensor. The way RO-based sensor is designed, it eliminates the need for a golden IC, especially when chip is used for a long period in the field. Initially, a certain number of random, new ICs are used as sample chips to generate a fingerprint. The samples can come from the same or from different wafers and lots. The larger this sample is, the more process variation space will be covered, reducing the probability that new ICs with large process variations will be identified as recycled ICs; 1000 sample chips are tested in our simulation. In authentication mode, the reference and stressed ROs frequencies are measured. We acknowledge that temperature variation should not impact the identification results significantly, as the reference and stressed ROs will experience the same environmental temperature.

Once the sample chips are measured, the frequency difference between the reference and stressed ROs would be calculated, with $F_{\text{diff}} = F_{\text{ref}} - F_{\text{str}}$, where F_{ref} is frequency of the reference RO and F_{str} is frequency of the stressed RO. With 1000 sample chips, the range of F_{diff} will be determined using distribution analysis, creating a fingerprint for new ICs. If F_{diff} of the CUT is out of the range of the new ICs' fingerprint, there is a high probability that the CUT is a recycled IC. Otherwise, the CUT is assumed to be a new IC. The longer the CUT is used, the more aging effects it will have experienced, making it easier to identify. The entire measurement procedure for each CUT should take only a very short amount of time (less than few seconds).

1) Simulation Results: To verify the effectiveness of the RO-based sensor, we implement and simulate it using 90-nm technology [23]. HSPICE MOSRA from Synopsys is used to simulate and measure the impact of aging on the RO-based sensor. The nominal supply voltage is 1.2 V. During simulation, in the stress phase, the reference RO is gated off and the stressed RO is gated on, experiencing NBTI and HCI aging. The stress for the stressed RO comes from its own oscillation. In the authentication phase, the reference and stressed ROs are both gated on and measured one by one, selected by the ROSEL signal. The measurement time is set up in the timer as 100 μs in our simulation. As the clock of the counter in the RO-based sensor is from the RO, the cycle count of each RO is given by the counter. The frequency of RO is equal to the cycle count divided by measurement time. The following simulation analysis is based on inverter ROs.

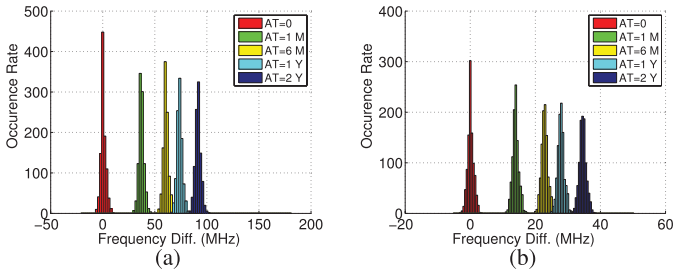


Fig. 12. Frequency difference distribution of RO-based sensor with PV0 using (a) 21-stage ROs and (b) 51-stage ROs.

Stage analysis: RO-based sensors with 21-stage and 51-stage ROs are simulated at 25 °C with 2% Tox, 5% Vth, and 5% L interdie and 1% Tox, 5% Vth, and 5% L intradie process variations (PV0 in Table I). Thousand chips are generated using MC simulation by HSPICE and the total aging time is set at 24 months with a 1-month step.

Fig. 12(a) shows the frequency difference F_{diff} range between the 21-stage reference and stressed ROs, where, in the legend, AT is aging time, M is month, and Y is years. From the figure, the frequency difference in new ICs (AT = 0) could be larger or smaller than 0, which is dependent on the process variations between the two ROs. In addition, the process variations of the CUTs are different from that of the 1000 sample new ICs, but the frequency differences still follow an identical distribution. The range of frequency differences in the new sample ICs is used as the fingerprint. After being used for 1 month, the stressed RO suffers from aging effects and its frequency became lower. The lowest frequency difference between the reference 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 1 month or longer is 100%. At 6 months, one year, and 2 years, the frequency difference between the reference and the stressed ROs becomes larger and larger. The variation of the frequency difference becomes larger as well. This is because the aging rate is different from chip to chip because of process variations; some ICs age faster and some others age slower.

RO-based sensors with 51-stage ROs are also implemented using the same temperature and the same process variations. Fig. 12(b) shows the simulation results. Comparing Fig. 12(a) with Fig. 12(b), the frequency difference between aged and new ICs is smaller when we use the larger stage ROs. The frequency difference variation, however, becomes smaller as well, which means that the RO-based sensor could still detect fully recycled ICs that has been used for 1 month with a 100% detection rate. If the RO-based sensor uses large-

TABLE I
PROCESS VARIATIONS

	Interdie			Intradie		
	V_{th} (%)	L (%)	Tox (%)	V_{th} (%)	L (%)	Tox (%)
PV0	5	5	2	5	5	1
PV1	8	8	3	7	7	2
PV2	20	20	6	10	10	4

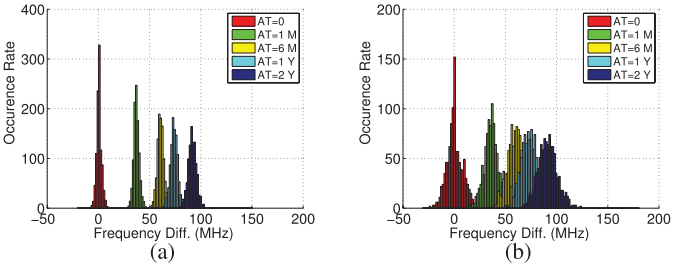


Fig. 13. Frequency difference distribution of RO-based sensor with 21-stage ROs with: (a) PV1 and (b) PV2.

stage ROs, it may impact the absolute value of the frequency difference between the reference and the stressed ROs, but the detection rate will not be impacted significantly. For different technologies, the stage count of the ROs could be adjusted based on the speed of the counter. In the following, we use RO-based sensors with 21-stage ROs according to the 90-nm technology for further analysis.

Process variations and temperature analysis: The effectiveness of the RO-based sensor is partly dependent on the variations between the reference and the stressed ROs. With lower rates of variation, the RO-based sensor could identify recycled ICs that age for a shorter period. The variations between the reference and the stressed ROs are, however, determined by intradie process variations. The smaller the intradie variations, the more effective the RO-based sensor will be. Table I shows the different process variation rates used in our simulation to analyze their impact on detection. Moving from PV0 to PV2, interdie and intradie variations both become larger. That is, because as feature size decreases and die size increases, process variations are increased significantly because of the complex semiconductor manufacturing process. RO-based sensors with 21-stage ROs are simulated at 25 °C using these process variation rates. PV1 are typical process variations for 90-nm technology [29], [34].

Through designing the sensor as a small module (hard macro), the reference and the stressed ROs are placed physically close and the variations between them are minimal. The simulation results of 1000 chips with PV1 and PV2 are shown in Fig. 13(a) and 13(b), respectively. Comparing Figs. 12(a), 13(a), and 13(b), the variation of the frequency differences between the reference and the stressed ROs in new ICs becomes larger with larger process variations. For the 1000 ICs with PV2, the detection rate of recycled ICs aged for 1 month is 95.2%. For recycled ICs that, however, age for 6 months, the detection rate is 100%. The RO-based sensor identifies shorter aged recycled ICs

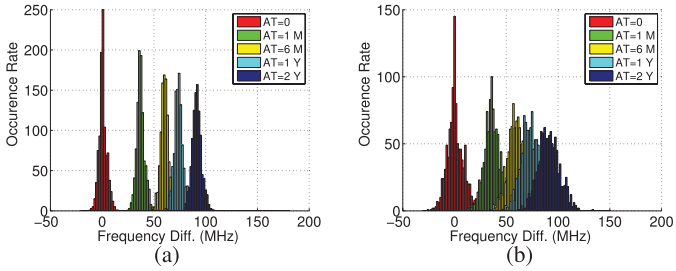


Fig. 14. Frequency difference distribution of RO-based sensor with: (a) PV1 and ±10 °C and (b) PV2 and ±20 °C.

with smaller intradie process variations as in PV0, PV1, and PV2.

The 1000 circuits generated using MC are also simulated with both process and temperature variations. Fig. 14(a) shows the frequency difference occurrence rate between the 21-stage reference and stressed ROs with process variations PV1 (shown in Table I) and temperature variations of ±10 °C around room temperature. Fig. 14(b) shows the simulation results with process variations PV2 and temperature variations of ±20 °C around room temperature. The results in Figs. 14(a) and 13(a) are from chips with the same process variations but different temperature variations. The frequency difference variations in Fig. 14(a) are slightly larger than those in Fig. 13(a) because of temperature variations. The same conclusion can be made by comparing Figs. 14(b) and 13(b). For the 1000 chips with PV2 and ±20 °C temperature variations, the detection rate of recycled ICs aged for 1 month is 92.3% but it is still 100% for recycled ICs aged for 6 months, demonstrating that our RO-based sensor is effective even with large process and temperature variations. We do not expect such a large variation in temperature and process in practice when authenticating a CUT. The temperature difference and process variations between the two ROs in RO-based sensor will be negligible as they are placed physically near each other.

From this analysis, the minimal usage time of recycled ICs that can be 100% detected using the RO-based sensor could be slightly different for different technologies. Process variations and temperature variations could impact the effectiveness of the RO-based sensor. Moreover, components used in the RO-based sensor play a significant role in determining the minimal usage time of recycled ICs that can be detected. For instance, a RO-based sensor composed of HVT cells can detect recycled ICs used for a shorter time with a 100% rate than a sensor composed of LVT cells does, that is, because the stressed RO with HVT cells will age faster than that with LVT cells.

2) Silicon Results: Our RO-based sensor is also verified through analysis of test chips fabricated using a 90-nm technology. The test chip is originally designed to verify the effects of aging on the frequency of ROs. In this paper, we use it to demonstrate the effectiveness of our RO-based sensor. In total, there are 96 delay chains in the chip that can work in RO mode by controlling different input signals [33]. Six of these ROs are selected to construct three RO-based sensors, as shown in Table II.

TABLE II
STRUCTURE OF RO-BASED SENSORS IN THE TEST CHIP

	ROs in RO-Based Sensors			
	Reference RO	Stressed RO	RO Structure	Vth
RO-based1	R_RO1	S_RO1	1 NAND + 200 BUFs	SVT
RO-based2	R_RO2	S_RO2	1 NAND + 200 BUFs	HVT
RO-based3	R_RO3	S_RO3	201 NANDs	HVT

1) RO-based1 contains two identical ROs (R_RO1 and S_RO1) with one SVT NAND gate and 200 SVT BUFs.
2) RO-based2 is composed of two identical ROs (R_RO2 and S_RO2) with one HVT NAND gate and 200 HVT BUFs.
3) RO-based3 includes ROs (R_RO3 and S_RO3) with 201 HVT NAND gates.

Therefore, R_RO1, R_RO2, and R_RO3 are Reference ROs, whereas S_RO1, S_RO2, and S_RO3 are Stressed ROs, respectively.

Comparing ROs included in the test chip with those used for HSPICE simulation, there are two main differences as follows.

1) The stage of ROs in the test chip is 201 whereas the stage of ROs used in MC simulation is much smaller (e.g., 21). The much larger number of stages in test chip is used to make the measurement and observation possible with low-end oscilloscopes;
2) The gates in ROs in the test chip are complex gates (BUFs, NANDs, etc.,) whereas inverter-based ROs are used in simulation.

That is, because we aim at analyzing the impact of aging on different types of gates in the test chip. According to our analysis in Section II, the number of stages and gate type of ROs, however, do not present a significant impact on the effectiveness of the RO-based sensor.

Now, we only have 15 test chips in our lab and all of them are used in this experiment to present the impact of process variations and aging. To replicate the RO-based sensor's stressed mode, S_RO1, S_RO2, and S_RO3 are enabled and experienced accelerated aging for 80 h at 135 °C with an elevated supply voltage (1.8 V instead of 1.2 V). The reason we use accelerated aging is that it takes a long time (usually weeks/months) to observe aging effects under normal conditions. The remaining three ROs are gated off and experienced no aging. In authentication mode, all of the ROs are enabled and the temperature is brought back to room temperature (around 25 °C). With the 15 new test chips, the average frequency of ROs is about 7.5 MHz. Fig. 15 shows the experimental results of the three RO-based sensors over the test chips. The red bars in the figure show the frequency difference between reference and stressed ROs in each RO-based sensor at time zero (new/unused ICs). Similarly, the yellow bars are the frequency difference between the two ROs after 80 h of aging.

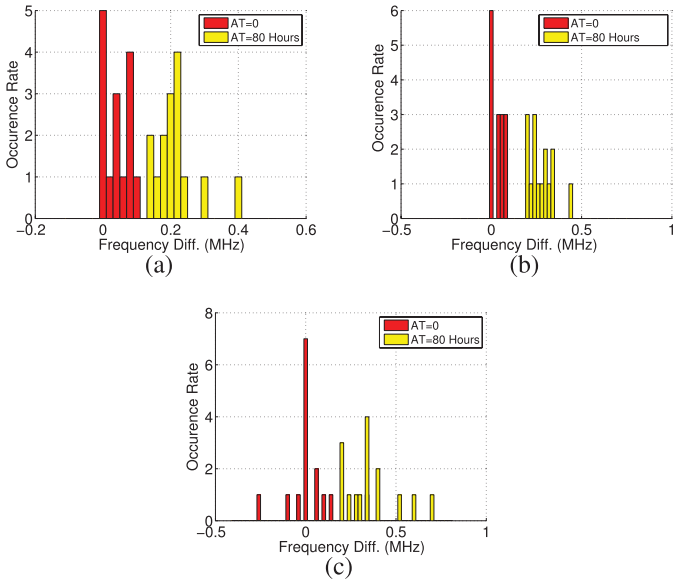


Fig. 15. Frequency difference distribution in: (a) RO-based1 (b) RO-based2 (c) RO-based3.

As a much larger number of stages are used in these sensors compared with those used in our simulations, the mean frequency of the ROs in the test chip and the frequency difference values are quite different from that in simulations. Even with 201 gates in these ROs, the detection rates of recycled ICs that aged 80 h using RO-based1, RO-based2, and RO-based3 are, however, all still 100%, which demonstrates that the RO stage count in RO-based sensor does not have a significant impact on the sensor's effectiveness in detecting recycled ICs.According to our detailed results, the average frequency degradation of the stressed ROs in RO-based1, RO-based2, and RO-based3 (shown in Fig. 15) is 3.2%, 4.0%, and 3.8%, respectively. Comparing Fig. 15(a) and (b), the frequency difference gap between new chips and aged chips in RO-based2 is larger than that in RO-based1. This is because RO-based sensors with HVT gates (RO-based2) will be more effective than those with SVT gates (RO-based1), which is also shown in Fig. 2(c) through simulation results. Comparing detection rates in Fig. 15(b) using RO-based2 (composed of HVT buffers) with Fig. 15(c) using RO-based3 (composed of HVT NAND gates), the gates used in the RO can slightly change the effectiveness of RO-based sensor but not significantly.

The ROs in the RO-based sensors in the test chip are not placed as close as they are supposed to. For instance, the results at time zero show that for RO-based1 and RO-based2, the R_ROs are faster than S_ROs in most cases whereas this is not the case for RO-based3. This could be because of the spatial variations that exist between the ROs not placed near each other, which made some ROs faster than others. For a RO-based sensor to be the most effective, it is recommended to place both ROs in a single localized module to reduce the variation between them. Limited by the amount and structure of the test chips, we cannot perform the same analysis with silicon data as we do with the MC simulations, however, the silicon results from these test chips demonstrate the effectiveness of the RO-based sensor.

TABLE III
AREA OVERHEAD CAUSED BY RO-, CAF-, AND SAF-BASED SENSORS ON CSAFTEST

Measurement		Area Overhead				Area
Scale (T_s)	Total Time (T_{total})	RO-based (%)	CAF-based (%)	SAF-based (%)	Reduction (%)	of CSAFTEST
1 min	1 month	–	7.37	3.72	49.5	500K gates and 12kB memory
1 h	one year	–	1.57	0.82	47.8	
one day	one year	–	0.18	0.12	33.3	
one day	4 years	–	0.37	0.21	43.2	
–	–	0.025	–	–	–	

B. AF-Based Sensors

From the above analysis, detection of a recycled chip depends on the amount of degradation caused by aging, workload, process, and environmental variations. If the chip is, however, used for a very short period or if the chip is designed and fabricated using an older technology node, it will not experience much degradation, thus negatively impacting the effectiveness of detection. For AF-based sensor, as the usage time of the ICs is calculated by counters and stored in the AF block, process and temperature variations cannot impact the data in AF cells. Therefore, the only step required to know how long the IC has been used to read the AF block by enabling authentication signal. A nonzero usage time from an AF-based sensor in a CUT does not suggest that it is a recycled IC because of the burn-in process. The CUT can be identified as a recycled one only if the usage time is longer than the time for burn-in process. Therefore, recycled ICs used for a very short period can still be detected by the AF-based sensors.

Area overhead analysis: To verify the effectiveness of AF-based sensors, we analyze the area overhead on the implementation of a design (named as CSAFTEST) with about 500-k gates and 12-kB in-system programmable memory. Table III shows the area overhead caused by RO-, CAF-, and SAF-based sensors with different measurement scales and total measurement time. From the table, the area overhead caused by AF-based sensors change with T_s and T_{total} as the structure of AF-based sensors change with measurement resolutions. For CAF-based sensor, the size of counter1 depends on T_s whereas the size of counter2 and the size of the AF memory block both depend on T_{total}/T_s. For SAF-based sensor, the area overhead is much smaller than that of CAF-based sensor because of the shifters. The reduction, calculated by {overhead(CAF-based)-overhead(SAF-based)}/overhead(CAF-based), is shown in the sixth column in Table III. For example, with $T_s = 1$ h and $T_{total} = 1$ year (8760 h), CAF-based sensor is designed with 20-bit counter1, 14-bit counter2, and 8760-bit AF memory block. The area overhead of this CAF-based sensor is 1.57% whereas the area overhead caused by SAF-based sensor is 0.82% and the reduction is 47.8%. If $T_s = 1$ min and $T_{total} = 1$ month and $T_s = 1$ day and $T_{total} = 1$ year, the area overhead of CAF-based sensor are, however, 7.37% and 0.18%, respectively.

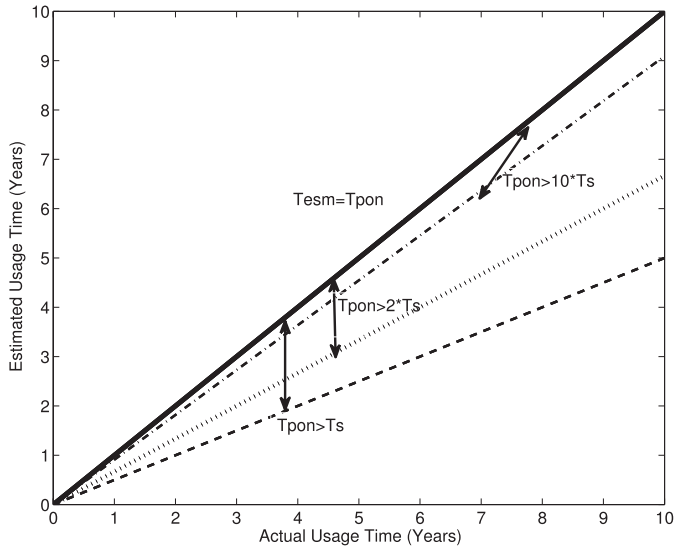
From this analysis, the area overhead caused by AF-based sensors depends on the application and specification of ICs. For example, if an IC is used in a system that requires a small T_s and a large T_{total}, the area overhead would be large. Otherwise, the overhead would be small (less than 1%). On the other hand, the time recorded by our AF-based sensors is power-on time and the intervals between power-on are not calculated. Therefore, the usage time stored in the sensor (T_{total}) is usually shorter than the time with power-off intervals. With a smaller T_{total}, the size of the AF memory block in our AF-based sensors will be smaller and accordingly the area overhead will be smaller.

Furthermore, comparing RO-based sensor with AF-based sensors, we can see that the following: 1) the area of RO-based sensor is much smaller than that caused by AF-based sensors and also stays constant because the number of gates used in RO-based sensor does not vary with designs. Here, the RO-based sensor is about 0.025% area overhead, which is negligible and 2) the accuracy of RO-based sensor is lower than that of AF-based sensors as it only provides an approximation of the usage time in a form of aging in the stressed RO.

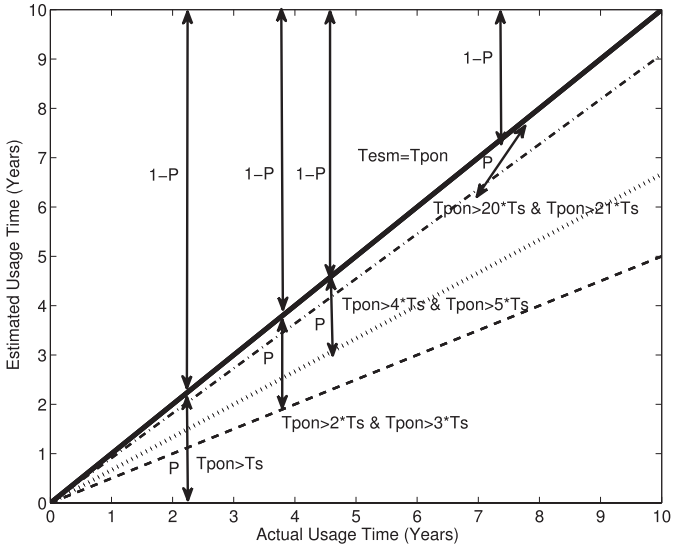
Usage time analysis: As the AF-based sensor only records usage time larger than T_s, if the power-on time of an IC is smaller than T_s, part of the usage time will be lost during the measurement. To verify the usage time, CAF- and SAF-based sensors are analyzed with different T_s. Consider the worst case, for example, if every time the IC is turned on, the power-on time (T_{pon}) is shorter than T_s, then the AF-based sensors will not record any usage time. The value stored in the AF memory will always be equal to the time for burn-in process. Our AF-based sensors will be ineffective in this case, which should be avoided when we design an AF-based sensor.

With appropriate T_s, $N = [T_{pon}/T_s]$ will be recorded in counter2 every time power is on and combined with previous usage time to be stored in the AF memory block in CAF-based sensor. Fig. IV-B shows the estimated usage time under different usage situations using CAF-based sensor. The X-axis represents the worst case when $T_{pon} < T_s$. In this case, the estimated usage time recorded by the sensor is always zero. Solid line: the ideal case when the estimated usage time (T_{esm}) is equal to the actual usage time. Range between the dashed and solid lines: the estimated usage time when $T_{pon} > T_s$. Range between the dash dotted line and solid line: the estimated time when $T_{pon} > 10 * T_s$. From this fig the longer the chip is used on each power-on, the more accurate estimated usage time will be recorded by CAF-based sensor.

For SAF-based sensor, the estimated usage time under different usage situations is shown in Fig. 16(b). Comparing Fig. 16(b) with 16(a), the accuracy of SAF-based sensor is slightly lower than that of CAF-based sensor. For example, when $T_{pon} > T_s$, the usage time recorded by CAF-based sensor would be $T_{est} = [T_{pon}/T_s] * T_s$ whereas the usage time recorded by SAF-based sensor would be $T_{est} = [T_{pon}/2T_s] * 2T_s$. In addition, as SAF-based sensor is based on the switching probability of several nets in the netlist, the estimated usage time shown in Fig. 16(b) is based on a probability. Assuming the output of the AND gate in SAF-based sensor (SS signal in Fig. 10) switches once during T_s with probability



(a)



(b)

Fig. 16. Usage time analysis using: (a) CAF-based sensor and (b) SAF-based sensor.

p, then SS will switch more than once with probability $1-p$. Note that SS does not switch during T_s will not be considered as this situation should be avoided when we design a SAF-based sensor. With this assumption, when $T_{\text{pon}} > 2 * T_s$, the estimated usage time will be in the range between the dashed and solid lines with probability p, shown in Fig. 16(b).

Even with time lost during the measurement using AF-based sensors, we can still identify a recycled IC as the usage time recorded by the AF memory block in used ICs will be longer than the time for burn-in process. After the burn-in process and before being sent to market, the AF-based sensor in all CUTs reports almost identical usage time. When ICs are, however, used in the field, the usage times recorded by the sensor in CUTs would be larger and different from each other based on the usage conditions before recycling. In addition, the usage times recorded by the AF-based sensors will not be impacted by aging recovery as the switching activity in a circuit will not be impacted by aging recovery.

C. Attack Analysis

Considering the capability of professional recyclers, we will discuss about a couple of attacks circumventing RO- and AF-based sensors. The first attack to RO-based sensor could be removal and tampering attacks. It is, however, inherently difficult for the recycler to remove the sensor, because of the expected measurement results from the two ROs. The second attack could be that the recycler tries to intentionally age the reference RO to mask the difference between the ROs in the RO-based sensor. Similarly, it is impossible to do that as reference RO cannot be gated on alone. The third attack could be that the attacker forces the sensor to work in authentication mode for a period under accelerated stress conditions. Simultaneously, with the accelerated aging, the frequency difference between the stressed and the reference ROs would shrink as both of them could asymptotically approach maximum degradation. This attack involves lots of time and effort, which makes it not economically viable. To carry out such attack, the attacker needs to know which pins are used as control pins, use a burn-in device, and force the chip to run in authentication mode for a certain time. The attacker could not then get much profit by going through this expensive and rather very slow and time-consuming process. We can, however, argue that attackers with unlimited resources may be able to remove the chip package, modify the original design, and tamper with the RO-based sensor. For such ICs where additional security is required, alterations could be made to the RO-based sensor to prevent these kinds of attacks. For example, to counter the third attack, a timer could be added to the control module to limit the running time for authentication. In addition, the RO-based sensor could be obfuscated inside the IC by multiplexing functional gates. This modification would make it more difficult for an attacker to analyze the IC, and make it more difficult to tamper with the sensor or modify it in any way.

For AF-based sensors, attackers would try to mask the usage time of ICs by disabling the sensor. The AF-based sensor, however, will automatically run whenever power is on and the usage time will be stored in the AF memory directly. Therefore, it is impossible for attackers to disable the sensor without removing the package and breaking the chip. The second attack could be erasing and alteration of AF cells; this is not possible because the memory used in our sensors is an AF OTP block. The most important advantage of AF OTP technique is its ability to resist all existing reverse engineering methods because the oxide breakdown in AF cells occurs in a random location within a bounded enclosure and is extremely small [30]. Therefore, the state of a bit cell stays well hidden in the silicon atoms, which makes it extremely difficult for attackers to tamper with the memory. The third attack could be modification of counters or signals connection in the sensor. With limited resources and without access to the original design, attackers, however, cannot modify the nets connection.

Decapping, professional cleaning, and remarking would not help attackers either.

V. Conclusion

In this paper, we proposed two techniques using lightweight on-chip sensors to detect recycled ICs. The frequency difference between the reference and the stressed ROs in the RO-based sensor made the easy identification of recycled ICs possible. The usage time stored in the AF memory using AF-based sensors could show how long an IC had been used and then identify a recycled IC. Experimental results and analysis demonstrated the effectiveness of these sensors. Our future work includes: 1) analyzing the impact of aging recovery on the effectiveness of the RO-based sensor; 2) implementing the AF-based sensors on test chip to further verify their effectiveness; and 3) developing on-chip sensors to detect recycled analog and RF devices.

VI. Acknowledgment

The authors would like to thank L. Winemberg of Freescale for providing the test chips for reliability analysis. This work is supported by Program for New Century Excellent Talents in University (NCET-12-0492), Zhejiang Provincial Natural Science Foundation of China (LR13F030001), the Fundamental Research Funds for the Central Universities (2012QNA5012), and the Foundation of Key Laboratory of System Control and Information Processing, Ministry of Education, China.

References

[1] (2010). Bureau of Industry and Security, U.S. Department of Commence. *Defense Industrial Base Assessment: Counterfeit Electronics* [Online]. Available: http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

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

[3] L. W. Kessler and T. Sharpe. (2010). *Faked Parts Detection* [Online]. Available: http://www.circuitsassembly.com/cms/component/content/article/159/9937-smt

[4] J. Stradley and D. Karraker, "The electronic part supply chain and risks of counterfeit parts in defense applications," *IEEE Trans. Compon. Packag. Technol.*, vol. 29, no. 3, pp. 703–705, Sep. 2006.

[5] Military Times. (2011). *Officials: Fake Electronics Ticking Time Bombs*, San Diego, CA, USA [Online]. Available: http://www.militarytimes.com/news/2011/11/ap-fake-electronics-ticking-time-bomb-110811/

[6] Tezzaron Semiconductor. (2008). *3D-ICs and Integrated Circuit Security*, Naperville, IL, USA [Online]. Available: http://www.tezzaron.com/about/papers/3D-ICs_and_Integrated_Circuit_Security.pdf

[7] (2011). *The Shocking Truth about Electronic Component Counterfeiting* [Online]. Available: http://www.combatcounterfeits.com/gallery.htms

[8] (2009). *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition* [Online]. Available: http://standards.sae.org/as5553/

[9] X. Zhang and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. Design Autom. Conf.*, 2012, pp. 703–708.

[10] X. Zhang and M. Tehranipoor, "Path-delay fingerprinting of identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, Oct. 2012, pp. 13–18.

[11] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*. New York, NY, USA: Springer-Verlag, 2011.

[12] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *IEEE Int. Solid-State Circuits Conf., Dig. Tech. Papers*, Feb. 2000, pp. 370–371.

[13] R. Pappu, "Physical one-way functions," Ph.D. dissertation, Dept. Media Arts Sci., Cambridge, MA, USA, 2001.

[14] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[15] E. Ozturk, G. Hammouri, and B. Sunar, "Physical unclonable function with tristate buffers," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2008, pp. 3194–3197.

[16] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *IACR J. Cryptol., Special Issue Secure Hardw.*, vol. 24, no. 2, pp. 375–397, 2011.

[17] (2011). F. Koushanfar. *Hardware Metering: A Survey* [Online]. Available: http://aceslab.org/sites/default/files/05-fk-metering.pdf

[18] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending piracy of integrated circuits," in *Proc. Proc. Conf. Design, Autom. Test Eur.*, 2008, pp. 1069–1074.

[19] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 66–75, Jan.–Feb. 2010.

[20] T. Kim, R. Persaud, and C. H. Kim, "Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits," *IEEE J. Solid-State Circuits*, vol. 43, no. 4, pp. 974–880, Apr. 2008.

[21] J. Keane, X. Wang, D. Persaud, and C. H. Kim, "An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB," *IEEE J. Solid-State Circuits*, vol. 45, no. 4, pp. 817–829, Apr. 2010.

[22] S. Mahapatra, D. Saha, D. Varghese, and P. B. Kumar, "On the generation and recovery of interface traps in MOSFETs subjected to NBTI, FN, and HCI stress," *IEEE Trans. Electron Devices*, vol. 53, no. 7, pp. 1583–1592, Jul. 2006.

[23] (2009). *Synopsys University Program* [Online]. Available: http://www.synopsys.com/Community/UniversityProgram/Pages/Library.aspx

[24] K. Uwasawa, T. Yamamoto, and T. Mogami, "A new degradation mode of scaled p^+ polysilicon gate P-MOSFETs induced by bias temperature instability," in *Proc. IEDM*, Dec. 1995, pp. 871–874.

[25] P. Heremans, R. Bellens, G. Groeseneken, and H. E. Maes, "Consistent model for the hot carrier degradation in N-channel and P-channel MOSFETs," *IEEE Trans. Electron Devices*, vol. 35, no. 12, pp. 2194–2209, Dec. 1988.

[26] H. Luo, Y. Wang, K. He, R. Luo, H. Yang, and Y. Xie, "Modeling of PMOS NBTI effect considering temperature variation," in *Proc. 8th Int. Symp. Quality Electron. Design*, Mar. 2007, pp. 139–144.

[27] R. Vattikonda, W. Wang, and Y. Cao, "Modeling and minimization of PMOS NBTI effect for robust nanometer design," in *Proc. 43rd Annu. Design Autom. Conf.*, 2006, pp. 1047–1052.

[28] Y. Wang, S. Cotofana, and L. Fang, "A unified aging model of NBTI and HCI degradation towards lifetime reliability management for nanoscale MOSFET circuits," in *Proc. IEEE Int. Symp. Nanoscale Archit.*, Jun. 2011, pp. 175–180.

[29] (2008). *Innovating Above and Beyond Standards* [Online]. Available: http://www.intel.com/technology/itj/2008/v12i2/3-managing/1-abstract.htm

[30] (2012). *Anti-fuse Memory Provides Robust, Secure NVM Option* [Online]. Available: http://www.eetimes.com/design/memory-design/4376742/Anti-fuse-memory-provides-robust–secure-NVM-option

[31] (2012). *NVM IP is an Antifuse-based, Embedded one-time programmable (OTP) Technology* [Online]. Available: http://www.sidense.com/technology.html

[32] (2012). *XPMâ Embedded NonâŁłVolatile Memory (NVM)* [Online]. Available: http://www.kilopass.com/products/otp-memory-ip/xpm-otp-nvm/

[33] N. Reddy, S. Wang, L. Winemberg, and M. Tehranipoor, "Experimental analysis for aging in integrated circuits," *presented at the IEEE North Atlantic Test Workshop*, Lowell, MA, USA, May 2011.

[34] B. NikoliÃ¼, and L. Pang, "Measurements and analysis of process variability in 90 nm CMOS," in *Proc. Int. Conf. Solid-State Integr. Circuit Technol.*, Oct. 2006, pp. 505–508.

Xuehui Zhang received the B.E.E. and M.E.E. degrees from the Department of Electronic and Information Engineering, Beihang University, Beijing, China, in 2006 and 2009, respectively, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA, in 2013.

She has developed several onchip structures and techniques to improve the security, trustworthiness, and reliability of a circuit. She has published many papers. Her current research interests include hardware Trojan detection, recycled IC identification, true random number generation, and IR-drop measurement.

Dr. Zhang received the First Prize in ESC Competition in 2010 and 2011.

Mohammad Tehranipoor (M'04–SM'07) is currently an Associate Professor of engineering innovation with the University of Connecticut, Storrs, CT, USA. He has published over 200 journal articles and refereed conference papers, 4 books, and 10 book chapters. His current research interests include computer-aided design and test for CMOS VLSI designs, reliable systems design at nanoscale, counterfeit electronics detection and prevention, supply chain risk management, and hardware security and trust.

Prof. Tehranipoor was a recipient of several Best Paper Awards as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, the 2009 UConn ECE Research Excellence Award, and the 2012 UConn SOE Outstanding Faculty Advisor Award. He serves on the program committee of more than a dozen leading conferences and workshops. He served as a Program Chair of the 2007 IEEE Defect-Based Testing workshop, a Program Chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, Co-Program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), General Chair for D3T in 2009 and DFTS in 2009, and Vice-General Chair for NATW in 2011. He co-founded a new symposium called the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), and served as host in 2008 and 2009, and General Chair and Chair of Steering Committee. He is currently serving as an Associate Editor-in-Chief for the *IEEE Design & Test*, an Associate Editor for *JETTA*, an Associate Editor for *Journal of Low Power Electronics*, an IEEE Distinguished Speaker, and an ACM Distinguished Speaker. He is a member of ACM and ACM SIGDA.