Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor

Xuehui Zhang, Nicholas Tuzzio and Mohammad Tehranipoor
ECE Department, University of Connecticut
xuehui.zhang, nicholas.tuzzio, tehrani@engr.uconn.edu

ABSTRACT

The counterfeiting and recycling of integrated circuits (ICs) have become major problems in recent years, potentially impacting the security of electronic systems bound for military, financial, or other critical applications. With identical functionality and packaging, it is extremely difficult to distinguish recovered ICs from unused ICs. A technique is proposed to distinguish used ICs from the unused ones using a fingerprint generated by a light-weight on-chip sensor. Using statistical data analysis, process and temperature variations' effects on the sensors can be separated from aging experienced by the sensors in the ICs when used in the field. Simulation results, featuring the sensor using 90nm technology, and silicon results from 90nm test chips demonstrate the effectiveness of this technique for identification of recovered ICs.

Categories and Subject Descriptors

B.8.0 [**Performance and Reliability**]: General

General Terms

Security

Keywords

Counterfeiting, Recovered ICs, Hardware security, and Circuit aging

1. INTRODUCTION

The counterfeiting of integrated circuits (ICs) has been 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]:

- is an unauthorized copy;
- does not conform to original component manufacturers design, model, and/or performance;
- is not produced by the original component manufacturers or is produced by unauthorized contractors;
- is an off-specification, defective, or used original component manufacturers product sold as "new" or working;
- 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 re-sale of used or defective ICs from 2005 to 2008 alone which is much more than other types of counterfeits [1]. Business Week published an investigative report in 2008 that traced recovered ICs found in U.S. military supplies back to their sources [3]. It is reported in [2] that used or defective products being sold as new or working account for 80 to 90% of all counterfeits being sold worldwide. With such estimate on the percentage of recovered ICs being sold, and the numbers relating to semiconductor sales and counterfeiting in general presented in [7], it could be possible that the intentional sale of used or defective chips in the semiconductor market could have accounted for between $9 billion and $15 billion USD of all semiconductor sales in 2008 alone; the trends shown in [1] suggest that this number is only going to increase over time.

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. The recycling process involves removing ICs from board or even dies in the ICs. The security issues associated with these ICs are: (1) a used IC can act as a ticking time bomb [4] since it does not meet the specification of the unused (fresh) ICs; (2) an adversary can include additional die on top of the recovered die carrying a back-door attack, sabotaging circuit functionality under certain conditions, or causing denial of service [5]. Note that in this paper, the terms *recovered IC* and *recovered die* are used interchangeably; these are the ICs/dies which have been removed from their original boards for the purpose of illicit re-sale. It is vital that we prevent these recovered ICs from entering critical infrastructures, aerospace, medical, and defense supply chains.

These recovered ICs can be classified into two categories: partially recovered ICs and fully recovered ICs. Partially recovered ICs will have the same external appearance as the IC they are meant to mimic, but do not contain the correct die internally—they were removed from their original board and remarked as a different IC. As such, decaping of randomly selected chips and careful inspection are effective at detecting partially recovered ICs. The more difficult class of recovered IC to detect would be the fully recovered ICs. These ICs have the original appearance, functionality, and markings as the devices they are meant to mimic, but they have been used for a period of time before they were re-sold. Even the best visual inspection techniques will have a difficult time identifying these fully recovered ICs with certainty [6]. Additionally, because fully recovered ICs contain the original, correct die internally, decaping technologies will provide no assistance in their detection. It is vital to develop new techniques to measure these ICs' specifications and compare them against the unused ones.

1.1 Previous Work

Physical unclonable functions (PUFs) implement challenge and response authentication for IC identification [9] [10] [11] [12] [13]. For each physical stimulus, the circuit will react in an unpredictable way due to 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) have been proposed in [14] [15] [16]. Metering techniques ensure that over pro-

DAC 2012, June 3-7, 2012, San Francisco, California, USA.

duction of integrated circuits will be prohibited. The above approaches are effective at authenticating ICs but not at identifying recovered ICs since they are expected to have the same IDs as the unused ICs.

Computer-aided design and reliability research community has also seen an extensive research on analyzing the aging of integrated circuits. In particular, ring oscillator based reliability analysis has become a common practice. For instance, a silicon odometer has been proposed to monitor different types of aging effects in [17] [18]; however, the objective was to improve the reliability of ICs, not to identify the recovered ICs. Such sensors will be ineffective if they were to be used in detecting recovered ICs due to the presence of process and environmental variations. We believe that no existing techniques are able to effectively address the IC/die recovery problem, and to the best of our knowledge this is the first paper to propose techniques to detect recovered ICs.

1.2 Contributions and Paper Organization

The major difference between fully recovered ICs and unused ICs is that fully recovered ICs have already experienced aging, as they were removed from their original boards and re-sold in the market. Aging effects, such as negative/positive bias temperature instability (NBTI/PBTI) and hot carrier injection (HCI), would have had an impact on the performance of the fully recovered ICs due to the change in the threshold voltage. In this paper, we propose a novel fingerprinting technique using a light-weight sensor based on ring oscillators, called combating die recovery (CDR) sensor, to help detection of recovered ICs.

Our CDR sensor is composed of a reference ring oscillator (Reference RO) and a stressed ring oscillator (Stressed RO) which is conceptually similar to [17] [18]. However, the Stressed RO is designed to age at a very high rate by using high threshold voltage (HVT) gates (to expedite aging so that ICs used even for a very short period of time can be identified) while the Reference RO is gated off from the power supply during chip operation, so that it experiences no stress. The frequency difference between the two ROs could denote the usage level of the chip under test (CUT) when compared against the fingerprints generated from fresh ICs; the larger the difference is, the longer the CUT has been used, and with a higher probability the CUT could be a fully recovered IC. With close placement of the two ROs in the CDR sensor, the impact of intra-die process variations could be minimized. Data analysis can effectively distinguish the frequency differences caused by aging from those of temperature and inter-die process variations, and then identify fully recovered ICs, which is demonstrated by our simulation and silicon results. In addition, partially recovered ICs would not report frequencies from the ROs since they were recovered from totally different ICs that most likely do not contain the CDR sensor. Thus, these partially recovered ICs could also be easily detected by our technique. The proposed CDR 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 CDR sensor proposed in the paper ensure that the Reference RO cannot be gated on alone, thus the frequency difference between the two ring oscillators cannot be changed to mask detection.

The rest of the paper is organized as follows. Section 2 outlines the necessary background and analyzes the impact of aging on different circuit elements and ring oscillators. Section 3 presents the CDR sensor architecture, and the measurement flow using CDR sensor for identifying recovered ICs is described in Section 4. Simulation results as well as silicon results from our 90nm test chip are presented in Section 5. Finally, our concluding remarks and future work are given in Section 6.

2. AGING ANALYSIS

In this section, we will briefly describe aging phenomenon in integrated circuits and present their impact on different circuit components and ring oscillators, which will be used in our CDR sensor.

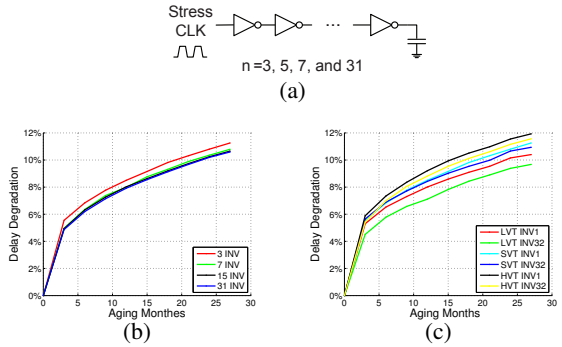

Figure 1: (a) Inverter chain structure, (b) Degradation of inverter chains with different lengths (stage count), and (c) Degradation of a 3-inverter chain with different inverter types.

When the chip operates in functional mode, the transistors age due mainly to NBTI and HCI. The aging effects of NBTI and HCI could cause parametric shifts and circuit failures, as demonstrated by reliability models [19] [21] [22]. NBTI can increase the absolute value of the PMOS threshold voltage, resulting in reduced transistor current and increased gate delay. HCI can create traps at the silicon substrate/gate dielectric interface, and can create dielectric bulk traps, and therefore impacts device parameters including threshold voltage. Since recovered ICs have been impacted by these aging effects when used in the field, the circuit parameters of recovered ICs would be different from those of fresh ICs. If a *fast-aging sensor* was embedded into the circuit to help detect its aging period, then recovered ICs could be identified.

In order to verify the effects of aging on a circuit's performance, several different inverter chains were simulated using Synopsys 90nm technology [20]. The delay of these inverter chains will represent the circuit's performance. The simulation was conducted using HSPICE MOSRA (Synopsys' reliability analysis tool) with combined NBTI and HCI aging effects at $25^{\circ}C$. Figure 1(a) shows the basic structure of the inverter chains with the same capacitive load and the same stress coming from a 500MHz clock. These chains are composed of 3, 7, 15, and 31 standard threshold voltage (SVT) inverters. Figure 1(b) presents the delay degradation of inverter chains under clock stress for up to 27 months with no interupt. From the figure, we can see that the number of inverters does not have a significant impact on the degradation of these chains since 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. There are three different threshold voltage models in the Synopsys 90nm technology: SVT, HVT, and low threshold voltage (LVT). The 3-inverter chains were simulated using these threshold voltages and two different size inverters (INVX1 and INVX32). Figure 1(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 were also simulated at $25^{\circ}C$ with a 500MHz 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. Figure 2 shows the simulation results. From the figure, we can see that the gate type does not impact the aging speed significantly. However, the inverter chain ages slightly faster than the others while NAND gate chain and 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 ring oscillators used to detect recovered ICs in our simulation analysis.

Figure 3(a) shows the frequency degradation of a 5-stage ring oscillator with HVT inverters after aging for 25 months. The frequency of the RO in a recovered IC will be smaller than in a fresh IC. If there are no environmental or process variations, we could easily identify recovered ICs by measuring the frequency of the RO

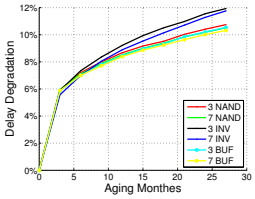

Figure 2: **Delay degradation of NAND, BUF, and INV chains.**

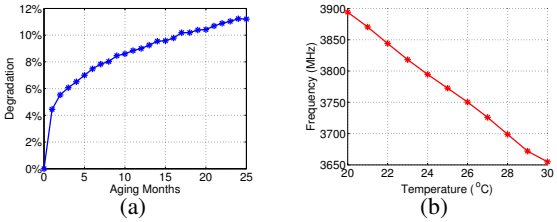

Figure 3: **(a) Frequency degradation of a 5-stage RO, and (b) Frequency of a 5-stage RO decreases with increasing temperature.**

embedded in the circuit. However, variations have a significant impact on the frequency of ROs. Figure 3(b) shows that the frequency of the 5-stage RO will decrease as we increase the temperature, and that the frequency variation could be very large. Note that increasing temperature can also increase the degradation of the circuit.

The 1000 Monte Carlo (MC) simulation results of the 5-stage RO are shown in Figure 4(a), at a temperature of $25°C$ with 2% Tox, 5% Vth, and 5% L inter-die variation and 1% Tox, 5% Vth, and 5% L intra-die variations. We can see that 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 Figure 4(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 recovered ICs can help separate them from those caused by process variations in fresh ICs if we are to try to use ROs to detect recovered ICs.

With a fixed stress, the number of inverters does not have a significant impact on an inverter chains' delay degradation. However, the frequency of an RO is related to the number of inverters, $f = \frac{1}{2*n*t_d}$, where n is number of stages in the RO and t_d is the delay of an inverter. Figure 4(c) shows the frequency shift of a 21-stage RO with HVT inverters. The frequency degradation is shown in Figures 4(d). Comparing the frequency degradation of the 5-stage and 21-stage ROs, we can see that the 5-stage RO experiences slightly more degradation since its oscillation frequency is higher than the 21-stage RO. However, a 5-stage RO may require a very fast counter which might be difficult to design to timing close. We will discuss this in detail in Section 5.

3. CDR SENSOR

Our main objectives in designing the CDR sensor are: (*i*) the sensor must age at a very high rate to help detect ICs used even for very short period of time, (*ii*) the sensor must experience no aging during manufacturing test, (*iii*) the impact of process variations and temperature on CDR sensor must be minimized, (*iv*) the sensor must be resilient to attacks, and finally (*v*) the measurement process must be done using a low-cost equipment and be very fast and easy.

As mentioned earlier, aging effects could slow down the frequency of the RO embedded into ICs. With an embedded RO, these recovered ICs could be identified based on its frequency, which will be smaller than that of a fresh IC. However, there are many parameters impacting the frequency of an RO, such as temperature and process variations. Our CDR sensor uses a Reference RO and a Stressed RO to separate the aging effects from process/environmental variations.

Figure 5 shows the structure of our CDR 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 time period, which is controlled by the timer.

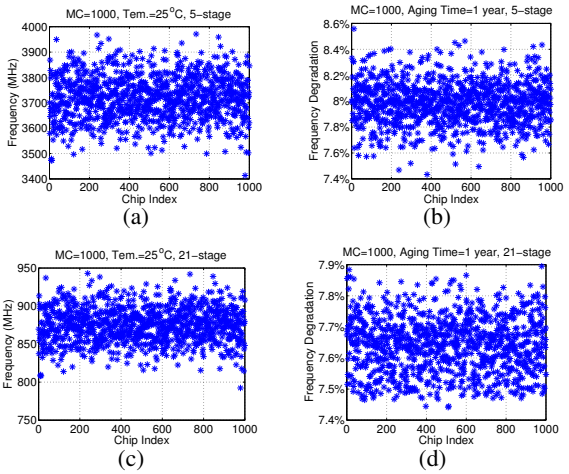

Figure 4: **(a) Frequency of a 5-stage RO varying with process variations, (b) Frequency degradation of a 5-stage RO aging for one year varying with process variations, (c) Frequency of a 21-stage RO varying with process variations, and (d) Frequency degradation of a 21-stage RO varying with process variations.**

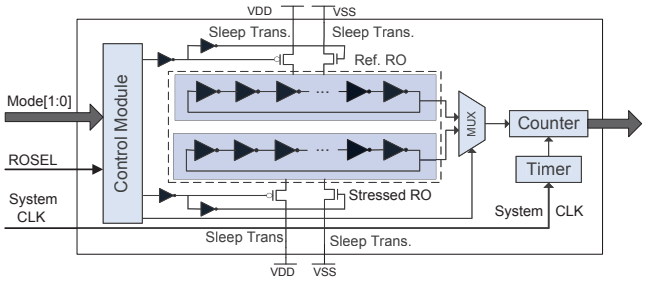

Figure 5: **The structure of the CDR sensor.**

System clock is used in the timer to minimize the measurement period variations due to circuit aging. The MUX selects which RO is going to be measured, and is controlled by the *ROSEL* signal. The Reference and Stressed ROs are identical, composed of HVT components. The inverters in Figure 5 could be replaced by any other types of gates (NAND, NOR, etc) only if they can construct a RO. It will not change the effectiveness of the CDR sensor significantly according to the analysis in Section 2. We use smaller-stage ROs in our CDR sensor considering the counter's measurement speed limits given a technology. For example, in our 90nm technology, a 16-bit counter can operate under frequency of up to $1GHz$; an inverter-based RO of at least 21 stages is required.

Sleep transistors are used to connect the ROs to the power supply in the CDR sensor; PMOS sleep transistors control the connection between VDD and the inverters and NMOS sleep transistors control the connection between VSS and the inverters. Both the Reference RO and the Stressed RO work in three modes, controlled by the *Mode* signal: (*i*) when the IC is in manufacturing test mode, the Reference RO and Stressed RO 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. (*ii*) 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 become smaller while the Reference RO will not change. ICs will spend most of their time in this mode. (*iii*) 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 RO and Stressed RO 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 *Model* signals and the authentication process takes a very short period of time. The three modes of operation ensure that (*i*) the frequency difference between the Reference RO and Stressed

RO will be larger over time since the Reference RO cannot be gated on alone, and (*ii*) it is extremely difficult for adversaries to force the CDR 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 CDR sensor module, which is impossible during simple recycling process.

The inverters of the Reference RO and the Stressed RO are placed physically next to each other, as Figure 5 shows, designed as a single small module. The process and environmental variations between them should be very small. Therefore, for a fresh IC, the frequency difference between the Reference RO and the Stressed RO would be within a certain small range. In a recovered IC, the Stressed RO will have suffered aging from its own oscillation since the chip has been working in normal functional mode for a long time. However, the Reference RO will not have experienced as much aging since it was gated off. The frequency difference between the Reference RO and the Stressed RO 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 fresh ICs' frequency difference range considering process variations, we can conclude with high confidence that the CUT was recovered from used boards.

The area overhead of our CDR sensor is negligible when compared to the millions of gates in modern ICs. With a 16-bit counter, the area overhead on the ISCAS'89 benchmark s38417, a DES implementation, and an implementation of the 8051 microprocessor is 0.16%, 0.09%, and 0.006%, respectively. Power consumption is also limited to that consumed by the Stressed RO in the CDR sensor. Furthermore, this CDR sensor is resilient to removal and tampering attacks. It is inherently difficult for the recycler to remove the sensor, due to the expected measurement results from the two ROs. This feature of the CDR sensor helps detect partially recovered ICs. In addition, one cannot intentionally age the Reference RO to mask the difference between the ROs in the CDR sensor, since Reference RO cannot be gated on alone. However, one can argue that attackers with unlimited resources may be able to remove the chip package, modify the original design, and tamper the CDR sensor. For such ICs where additional security is required, alterations could be made to the CDR sensor to prevent these kinds of attacks. The CDR 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, making it more difficult to tamper with the sensor or modify it in any way. Additional modifications for further security may be possible as well.

4. MEASUREMENT FLOW

Figure 6 shows the measurement flow for identifying recovered ICs. First, a certain number of random, fresh 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 fresh ICs with large process variations will be identified as recovered ICs. 1000 sample chips are tested in our simulation. In authentication mode, the Reference RO and Stressed RO's frequency is measured. The measurement environment should keep the temperature stable with as little variation as possible. However, we acknowledge that temperature variation should not impact the identification results significantly, since the Reference RO and Stressed RO will experience the same environmental temperature.

Once the sample chips have been measured, the frequency difference between the Reference RO and Stressed RO would be calculated, with $F_{diff} = F_{ref} - F_{str}$, 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 fresh ICs. If F_{diff} of the CUT is out of the range of the fresh ICs' fingerprint, there is a high probability that the CUT is a recovered IC. Otherwise, the CUT is assumed to be a fresh IC. The longer the CUT has been used, the more aging

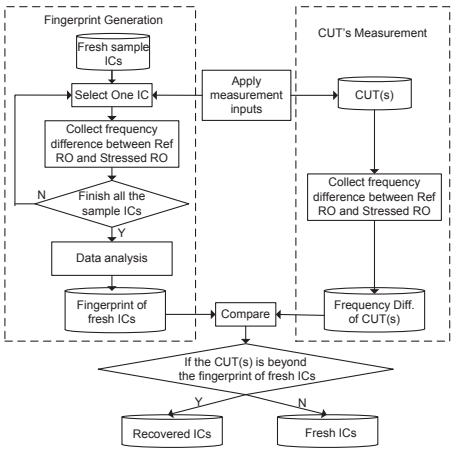

Figure 6: Measurement flow using CDR sensor for identifying recovered ICs.

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 30 seconds).

5. RESULTS AND ANALYSIS

5.1 Simulation Results

In order to verify the effectiveness of the CDR sensor, we implemented and simulated it using 90nm technology [20]. HSPICE MOSRA from Synopsys is used to simulate and measure the impact of aging on the CDR sensor. The nominal supply voltage is 1.2V. During simulation, in the stress phase, the Reference RO was gated off and the Stressed RO was gated on, experiencing NBTI and HCI aging. The stress for the Stressed RO comes from its own oscillation. In the authentication phase, the Reference RO and Stressed RO were both gated on and measured one by one, selected by the *ROSEL* signal. The measurement time was set up in the timer as $100\mu s$ in our simulation. Since the clock of the counter in the CDR 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 ring oscillators.

Stage Analysis: CDR sensors with 21-stage and 51-stage ROs were simulated at $25^{\circ}C$ with 2% Tox, 5% Vth, and 5% L inter-die and 1% Tox, 5% Vth, and 5% L intra-die process variations (PV0 in Table 1). 1000 chips were generated using Monte Carlo simulation by HSPICE and the total aging time was set at 24 months with a one month step.

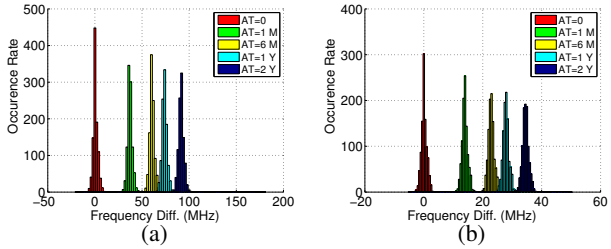

Figure 7: Frequency difference distribution of CDR sensor with PV0 using (a) 21-stage ROs, and (b) 51-stage ROs.

Figure 7(a) shows the frequency difference F_{diff} range between the 21-stage Reference RO and Stressed RO, where, in the legend, *AT* denotes aging time, *M* represents month, and *Y* represents years. From the figure, we can see that the frequency difference in fresh 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 were different from that of the 1000 sample fresh ICs, but the frequency differences still followed an identical distribution. The range of frequency differences in the fresh sample ICs is used as the fingerprint. After being used for

Table 1: Process variations.

	Inter-die			Intra-die		
	Vth	L	Tox	Vth	L	Tox
PV0	5%	5%	2%	5%	5%	1%
PV1	8%	8%	3%	7%	7%	2%
PV2	20%	20%	6%	10%	10%	4%

one month, the Stressed RO suffered from aging effects and its frequency became smaller. The smallest frequency difference between the Reference RO and the Stressed RO was larger than the largest frequency difference present in the fresh IC set. Therefore, the recovered IC detection rate for ICs aged for one month or longer is 100%. At 6 months, 1 year, and 2 years, the frequency difference between the Reference RO and the Stressed RO 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 due to process variations; some ICs aged faster and some others aged slower.

CDR sensors with 51-stage ROs were also implemented using the same temperature and the same process variations. Figure 7(b) shows the simulation results. Comparing Figure 7(a) and Figure 7(b), we observe that the frequency difference between aged and fresh ICs is smaller when we use the larger-stage ROs. However, the frequency difference variation becomes smaller as well, which means that the CDR sensor could still detect fully recovered ICs that had been used for one month with a 100% detection rate. If the CDR sensor uses large-stage ROs, it may impact the absolute value of the frequency difference between the Reference RO and the Stressed RO, 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 CDR sensors with 21-stage ROs according to our 90nm technology for further analysis.

Process Variations and Temperature Analysis: The effectiveness of our CDR sensor is partly dependent on the variations between the Reference RO and the Stressed RO. With lower rates of variation, the CDR sensor could identify fully recovered ICs that aged for shorter period of time. However, the variations between the Reference RO and the Stressed RO are determined by intra-die process variations. The smaller the intra-die variations, the more effective the CDR sensor will be. Table 1 shows the different process variation rates to analyze their impact on detection. Moving from PV0 to PV2, inter-die and intra-die variations both become larger. CDR sensors with 21-stage ROs were simulated at 25°C using these process variation rates.

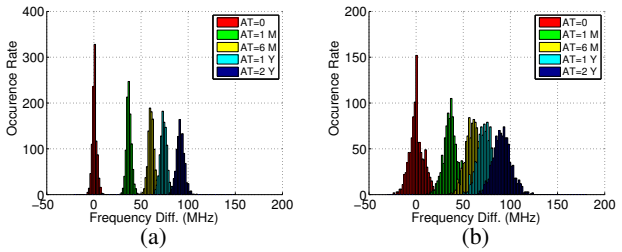

Figure 8: Frequency difference distribution of CDR sensor with 21-stage ROs with (a) PV1 and (b) PV2.

By designing the sensor as a small module (hard macro), the Reference RO and the Stressed RO are placed physically close and the variations between them will be minimal. The simulation results of 1000 chips with PV1 and PV2 are shown in Figure 8(a) and Figure 8(b), respectively. Comparing Figure 7(a), Figure 8(a), and Figure 8(b), we can see that the variation of the frequency differences between the Reference RO and the Stressed RO in fresh ICs becomes larger with larger process variations. For the 1000 ICs with PV2, the detection rate of recovered ICs aged for one month is 95.2%. However, for recovered ICs that aged for six months, the detection rate is 100% again. The CDR sensor identifies shorter-aged recovered ICs with smaller intra-die process variations as in PV0, PV1, and PV2.

Table 2: Structure of CDR sensors in the test chip.

	ROs in CDR sensors			
	Reference RO	Stressed RO	RO Structure	Threshold Voltage
CDR1	*R_RO*1	*S_RO*1	1 NAND + 200 BUFs	SVT
CDR2	*R_RO*2	*S_RO*2	1 NAND + 200 BUFs	HVT
CDR3	*R_RO*3	*S_RO*3	201 NANDs	HVT

The 1000 circuits generated using Monte Carlo were also simulated with both process and temperature variations. Figure 9(a) shows the frequency difference occurence rate between the 21-stage Reference and Stressed ROs with process variations PV1 (shown in Table 1) and temperature variations of $\pm 10°C$ around room temperature. Figure 9(b) shows the simulation results with process variations PV2 and temperature variations of $\pm 20°C$ around room temperature. The results in Figure 9(a) and Figure 8(a) are from chips with the same process variations but different temperature variations. We can see that the frequency difference variations in Figure 9(a) are slightly larger than those in Figure 8(a) due to temperature variations. The same conclusion can be made by comparing Figure 9(b) and Figure 8(b). For the 1000 chips with PV2 and $\pm 20°C$ temperature variations, the detection rate of recovered ICs aged for one months is 92.3% but it is still 100% for recovered ICs aged for six months, demonstrating that our CDR sensor is effective even with large process and temperature variations. Note that 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 CDR sensor will be negligible since they are placed physically near each other.

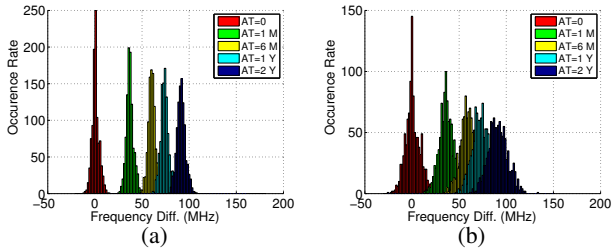

Figure 9: Frequency difference distribution of CDR sensor with (a) PV1 and $\pm 10°C$ and (b) PV2 and $\pm 20°C$.

5.2 Silicon Results

Our CDR sensor is also verified through analysis of test chips fabricated using a 90nm technology. The test chip was originally designed to verify the effects of aging on the frequency of ROs. In this work, we use it to demonstrate the effectiveness of our CDR sensor. Since most functionality in the test chip was designed for measuring different aging effects, here, we will not describe the entire test chip's structure in detail. In total, there are 96 delay chains in the chip which can work in ring oscillator mode by controlling different input signals. Six of these ring oscillators were selected to construct three CDR sensors as shown in Table 2.

- CDR1 contains two identical ROs (*R_RO*1 and *S_RO*1) with one SVT NAND gate and 200 SVT BUFs;
- CDR2 is composed of two identical ROs (*R_RO*2 and *S_RO*2) with one HVT NAND gate and 200 HVT BUFs
- CDR3 includes ROs (*R_RO*3 and *S_RO*3) with 201 HVT NAND gates.

where *R_RO*1, *R_RO*2, and *R_RO*3 are Reference ROs while *S_RO*1, *S_RO*2, and *S_RO*3 are Stressed ROs, respectively.

Comparing ROs included in the test chip with those used for HSPICE simulation, there are two main differences: (1) the stage of ROs in the test chip is 201 while the stage of ROs used in Monte Carlo simulation is much smaller (e.g. 21). The much larger number of stages in test chip was 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.) while inverter-based ROs were used in simulation. That is because we aim at analyzing the impact of aging on different types of gates in test chip. However, according to our analysis in Sections 2 and 5.1, the number of stages and gate type of ROs do not present a significant impact on the effectiveness of the CDR sensor.

Currently, 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 CDR sensor's stressed mode, *S_RO*1, *S_RO*2, and *S_RO*3 were enabled and experienced accelerated aging for 80 hours at 135°*C* with an elevated supply voltage (1.8V instead of 1.2V). The reason we used accelerated aging is that it takes a long time (usually weeks/months) to observe aging effects under normal conditions. The remaining three ROs were gated off and experienced no aging. In authentication mode, all of the ROs were enabled and the temperature was brought back to room temperature (around 25°*C*). With the 15 fresh test chips, the average frequency of ROs is about 7.5*Mhz*. Figure 10 shows the experimental results of the three CDR sensors over the test chips. The red bars in the figure show the frequency difference between Reference RO and Stressed RO in each CDR sensor at time zero (fresh/unused ICs). Similarly, the yellow bars are the frequency difference between the two ROs after 80 hours of aging.

Since a much larger number of stages are used in these sensors compared to those used in our simulations, the mean frequency of the ROs in test chip and the frequency difference values are very much different from that in simulations. However, even with 201 gates in these ROs, the detection rates of recovered ICs that aged 80 hours using *CDR*1, *CDR*2, and *CDR*3 are all still 100%, which demonstrates that the RO stage count in CDR sensor does not have a significant impact on the sensor's effectiveness in detecting recovered ICs. According to our detailed results, the average frequency degradation of the stressed ROs in *CDR*1, *CDR*2 and *CDR*3 (shown in Figure 10) is 3.2%, 4.0%, and 3.8%, respectively, Comparing Figure 10(a) and Figure 10(b), we can see that the frequency difference gap between fresh chips and aged chips in *CDR*2 is larger than that in *CDR*1. This is due to the fact that CDR sensors with HVT gates (*CDR*2) will be more effective than those with SVT gates (*CDR*1), which is also demonstrated in Figure 1(c) through simulation results. Comparing detection rates in Figure 10(b) using *CDR*2 (composed of HVT buffers) and Figure 10(c) using *CDR*3 (composed of HVT NAND gates), we can see that the gates used in the RO can slightly change the effectiveness of CDR sensor but not significantly.

Note that the ROs in the CDR sensors in the test chip were not placed as close as they were supposed to. For instance, the results at time zero show that for *CDR*1 and *CDR*2, the R_ROs are faster than S_ROs in most cases while this is not the case for *CDR*3. 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 CDR 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 did with the Monte Carlo simulations, however, the silicon results from these test chips demonstrate the effectiveness of our CDR sensor.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented the concept of IC/die recovery problem and proposed a technique using a light-weight on-chip sensor to detect recovered ICs. The fingerprint generated by the frequency difference between the Reference RO and the Stressed RO in the CDR sensor makes identification of fully recovered ICs easily possible. Simulation results using different process and temperature variations demonstrated its effectiveness. The silicon results further demonstrated that our CDR sensor can detect recovered ICs even used in the field for a very short period of time. In addition, our future work includes (i) using multiple CDR sensors to further improve detection resolution and capability, (ii) obfuscating the CDR sensor for further improvement of the security against tampering, and (iii) using other circuit parameters such as path-delay, leakage current, and switching power to detect recovered ICs.

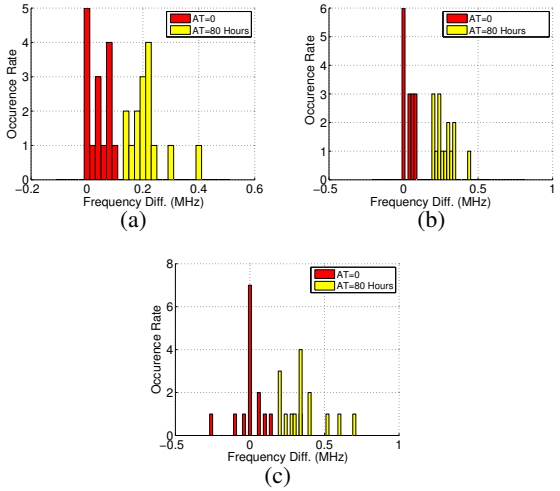

Figure 10: Frequency difference distribution in (a) *CDR*1, (b) *CDR*2, and (c) *CDR*3.

7. ACKNOWLEDGEMENT

The authors also would like to thank LeRoy Winemberg of Freescale for providing the test chips for reliability analysis.

8. REFERENCES

[1] "Defense Industrial Base Assessment: Counterfeit Electronics," Bureau of Industry and Security, U.S. Department of Commence, *http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf*, 2010.
[2] L. W. Kessler and T. Sharpe, "Faked Parts Detection," *http://www.circuitsassembly.com/cms/component/content/article/159/9937-smt,* 2010.
[3] Business Week, "Dangerous Fakes," *http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm,* 2008.
[4] Military Times, "Officials: Fake Electronics Ticking Time Bombs," *http://www.militarytimes.com/news/2011/11/ap-fake-electronics-ticking-time-bomb-110811/,* 2011.
[5] Tezzaron Semiconductor, "3D-ICs and Integrated Circuit Security," *http://www.tezzaron.com/about/papers/3D-ICs_and_Integrated_Circuit_Security.pdf*, 2008.
[6] *http://www.combatcounterfeits.com/gallery.htm*
[7] J. Stradley and D. Karraker, "The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications," *IEEE Transactions on Components and Packaging Technologies*, pp.703-705, Sept. 2006.
[8] M. Tehranipoor, and C, Wang "Introduction to Hardware Security and Trust," Springer, New York, USA, 2011.
[9] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC Identification Circuit Using Device Mismatch," in *Proc. ISSCC*, pp. 370-371, 2000.
[10] R. Pappu, "Physical One-way Functions," *Phd thesis, MIT*, 2001.
[11] G. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *Proc. DAC*, pp. 9-14, 2007.
[12] E. Ozturk, G. Hammouri, and B. Sunar, "Physical Unclonable Function with Tristate Buffers," in *Proc. ISCAS*, pp. 3194-3197, 2008.
[13] A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive," *IACR Journal of Cryptology, special issue on Secure Hardware*, 2011.
[14] F. Koushanfar "Hardware Metering: A Survey," *http://aceslab.org/sites/default/files/05-fk-metering.pdf*
[15] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending Piracy of Integrated Circuits," in proc. *DATE08*, pp. 1069-1074, 2008.
[16] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC Piracy Using Reconfigurable Logic Barriers," *IEEE Design & Test of Computers*, 2010.
[17] T. Kim, R. Persaud, and C. H. Kim, "Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits," *IEEE Journal of Solid-State Circuits*, pp. 974-880, 2008
[18] J. Keane, X. Wang, D. Persaud, and C.H. Kim, "An All-In-One Silicon Odometer for Separately Monitoring HCI, BTI, and TDDB," *IEEE Journal of Solid-State Circuits*, pp. 817-829, 2010
[19] 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. on Electron Devices,* vol. 53, no. 7, pp. 1583-1592, 2006.
[20] "http://www.synopsys.com/Community/UniversityProgram/Pages/Library.aspx".
[21] 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. Int. Electron Devices Meeting*, pp. 871-874, 1995.
[22] 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, 1988.
[23] H. Luo, Y. Wang, K. He, R. Luo, H. Yang, and Y. Xie "Modeling of PMOS NBTI Effect Considering Temperature Variation." in *Proc. ISQED*, pp. 139-144, 2007.
[24] R. Vattikonda; W. Wang; Y. Cao; "Modeling and Minimization of PMOS NBTI Effect for Robust Nanometer Design," in *Proc. DAC,* pp.1047-1052, 2006.