Low-cost On-Chip Structures for Combating Die and IC Recycling

Ujjwal Guin, Domenic Forte, and Mohammad (Mark) Tehranipoor
CHASE Center, ECE Department, University of Connecticut
Storrs, Connecticut, USA, 06269

Abstract: *The recycling of electronic components has become a major concern to industry and government as it potentially impacts the security and reliability of a wide variety of electronic systems. The sheer number of component types (analog, digital, mixed signal) and size (large or small) makes it challenging to find a one-size-fits-all solution. In this paper, we propose three light-weight, on-chip structures based on ring oscillators, anti-fuses and fuses for combating die and IC recycling. Each structure meets the unique needs and limitations of different part types and sizes. Taken together, the structures represent a suite of solutions that can provide excellent coverage of recycled parts.*

I. BACKGROUND

Counterfeit components pose a great threat to the global electronic component supply chain because of the lack of efficient, robust, and low-cost detection and avoidance technologies. The most recent data provided by IHS shows that reports of counterfeit parts have quadrupled since 2009 [1]. Presence of different types of counterfeits – recycled, remarked, cloned, overproduced, out-of-spec/defective, forged documentation, and tampered in the supply chain makes the detection process even more challenging [2] [3] [4] [5] [6] [7]. Today, the most widely discussed type of counterfeit components are recycled and remarked, which together make up more than 80% of the counterfeit instances reported [8]. In this work, we focus on detecting such recycled parts.

To prevent the recycled components from getting into the supply chain, we propose three different structures/designs that cover components of different types (digital, analog, and mixed-signal) and sizes (large and small). First, we propose an on-chip ring oscillator-based sensor to generate an age-based fingerprint for each IC. This structure is suitable for any digital IC manufactured using 90nm or below process technology. We also propose an on-chip antifuse-based structure to measure the actual usage time of an IC in the field [9] for larger digital ICs. Finally, we present near-zero cost fuse-based techniques to protect very small ICs from recycling and remarking. The output of all these structures can simply be read by a very low-cost piece of equipment to authenticate ICs under test.

The paper is organized as follows: in Section II we present our RO-based CDIR sensor. We describe AF-based CDIR structure in Section III. In Section IV, we present fuse-based CDIR structure. The simulation result for RO-based CDIR is shown in Section V. We conclude the paper in Section VI.

II. RO-BASED CDIR SENSOR (RO-CDIR)

The basic idea of the RO-CDIR is as follows. We exploit the changes of oscillation frequency of ring oscillators (ROs) over time due to well-known aging effects (negative bias temperature instability (NBTI) [10] and hot carrier injection (HCI) [11]). Our main objectives in designing the RO-CDIR sensor are: (i) the sensor must age at a very high rate to help detect ICs used even for very short period of time in the field, (ii) the sensor must experience no aging during manufacturing and burn-in tests, and (iii) the sensor must be resilient to attacks.

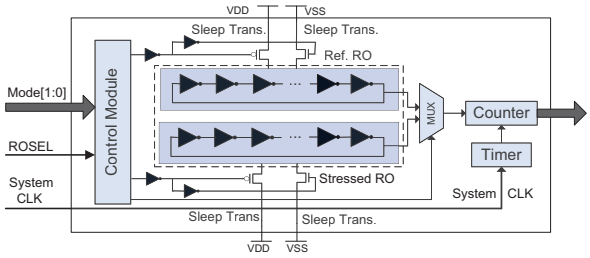


Figure 1. RO-CDIR Sensor.

Figure 1 shows the architecture of the proposed RO-CDIR, which is composed of a control module, a reference RO, a stressed RO, a MUX, a timer, and a counter. The reference RO is designed to age at a slow rate and the stressed RO is designed to age at a high rate. The counter measures the cycle count of the two ROs during a time period, which is controlled by the timer. 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 laid out identically and placed close to each other to minimize their difference in frequencies caused by process variation. In the 90nm technology, a 16-bit counter can operate under frequency of up to 1GHz which results in an inverter-based RO with at least 21 stages [12].

The frequency of the stressed RO decreases as it ages and the IC is used. The difference between the reference RO and stressed RO represent the amount of time used in the field. The larger the difference is, the longer the chip must have been used in the field. This sensor has been simulated and fabricated using 90nm technology. Our results demonstrate the effectiveness of the sensor in capturing usage time effectively and detect recycled ICs.

III. ANTIFUSE-BASED CDIR STRUCTURE (AF-CDIR)

In the RO-CDIR structure, the inverters of the reference RO and the stressed RO are placed physically next to each other to minimize the impact of intra-die process variations. However, it may still be difficult to completely exclude the impact of inter-die process variations. In addition, RO-CDIR structure 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) of the RO-CDIR

sensor is limited. For example, it may not identify recycled ICs used shorter than one month [9]. Finally, RO-CDIR relies on the aging in the ring oscillators. However, aging may not be as significant for older technology nodes ($>$ 90nm). Therefore, in order to provide a more accurate usage time, and identify recycled ICs that are only used for a very short period of time (e.g., 1 day), we have proposed an antifuse-based CDIR sensor called AF-CDIR.

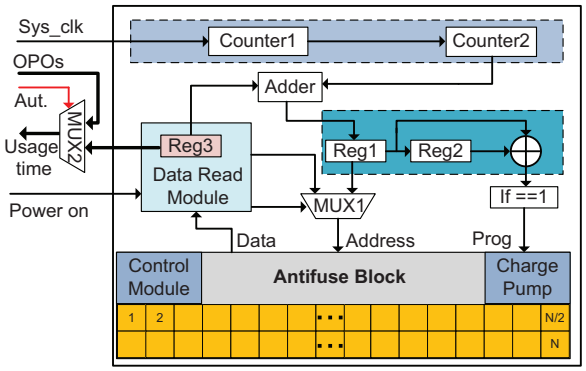


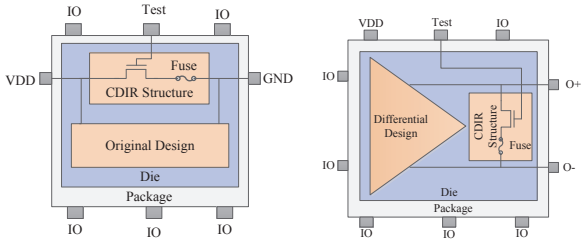
Figure 2. AF-CDIR.

Figure 2 shows the structure of the AF-CDIR sensor, which is composed of two counters, a data read module, an adder, and an antifuse OTP memory block. *Counter1* is used to divide the high frequency system clock to a lower frequency signal, as shown in Figure 2. *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: defined as the time unit reported by the sensor) and the total measurement time (T_{total}). Note that the fact that we can control this scale makes it more robust than the RO-CDIR but also increases its overhead.

An embedded antifuse 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 antifuse block, *Prog* is assigned to be 1'b1 if the value in *Counter2* increases by "1". By connecting the output of *Counter2* to *Address* in the antifuse block directly, the related antifuse 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*. Program and read operations share the same Address signals in antifuse block. Therefore, a MUX ($MUX1$ in Figure 2), controlled by data read module, is used to select the address (antifuse cell) to be read or programmed.

IV. Fuse-Based CDIR Structure (F-CDIR)

Both RO-CDIR and AF-CDIR sensors are suitable for large digital integrated circuits namely microprocessors, DSPs, microcontrollers, FPGAs, and large memories. However, a majority of the parts in the market today are smaller analog, digital, and mixed signal devices. Hence, the above structures are not well suited for such parts. In this section, we will propose a very low-cost design based on semiconductor fuse that can be implemented in any designs (except discrete components, such as, diodes, transistors, and passive components). This structure can be fabricated along with the original design and require only one extra $Test$ pin.



(a) F-CDIR implementation. (b) F-CDIR implemented in differential designs.

Figure 3. F-CDIR.

Figure 3(a) presents our proposed F-CDIR structure. F-CDIR consists of a switch and a fuse. The two terminals of this structure are connected to the VDD and GND pins. The control terminal is regulated by the $Test$ pin. The area overhead is only one transistor and a fuse, making it very low cost. The structure works as follows: during manufacturing test and burn-in test modes the $Test$ pin will always be "0" which will provide no current flowing through the structure. When the component is placed in printed circuit board (PCB) for normal operation the $Test$ pin will be connected to VDD. The MOS switch will become ON and a current will flow through the fuse which results in an open circuit inside the structure. The device will then operate normally as it was designed for. The detection of counterfeit component (used part) will be simply done by measuring the resistance between VDD and GND pins while setting $Test$ pin to VDD. The measured resistance between VDD and GND should be negligible for new component. This structure can also be implemented in differential designs such as the one shown in Figure 3(b). If the component is already used, the measured resistance will be very high (infinite).

V. Results

In this section, we will present the experimental results of the RO-based CDIR sensor. In order to verify the effectiveness of the RO-based sensor, we implemented and simulated it using 90nm technology [13]. HSPICE MOSRA from Synopsys is used to simulate and measure the impact of aging on the RO-based sensor. The nominal supply voltage is 1.2V. 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 effectiveness of the RO-based sensor is partly dependent on the variations between the Reference RO and the Stressed RO. With lower rates of variation, the RO-based sensor could identify recycled ICs that aged for a 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 RO-based sensor will be. Table I shows

Table I
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%

the different process variation rates used in our simulation to analyze their impact on detection. Moving from PV0 to PV2, inter-die and intra-die variations both become larger. That is because as feature size decreases and die size increases, process variations are increased significantly due to the complex semiconductor manufacturing process. RO-based sensors with 21-stage ROs were simulated at $25°C$ using these process variation rates. PV1 are typical process variations for 90 nm technology.

RO-based sensors with 21-stage and 51-stage ROs were simulated at PV0 constraints. 1000 samples were generated using Monte Carlo simulation by HSPICE and the total aging time was set at 24 months with a one month step. By designing the sensor as a small module (hard macro), the Reference RO and the Stressed RO were placed physically close and the variations between them were minimal. Figure 4(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. The range of frequency differences in the new sample ICs is used as the fingerprint. After being used for one month, the stressed RO suffered from aging effects and its frequency became much lower. RO-based sensors with 51-stage ROs were also implemented using the same temperature and the same process variations. Figure 4(b) shows the simulation results.

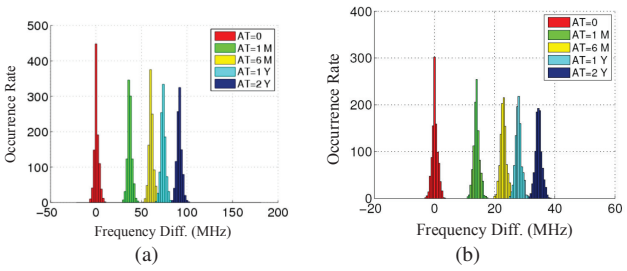


Figure 4. Frequency difference distribution of RO-based sensor with PV0 using (a) 21-stage ROs, and (b) 51-stage ROs.

The simulation results of 1000 chips with PV1 and PV2 are shown in Figure 5(a) and Figure 5(b), respectively. Comparing Figure 4(a), Figure 5(a), and Figure 5(b), we can see that the variation of the frequency differences between the Reference RO and the Stressed RO in new ICs becomes larger with larger process variations. For the 1000 ICs with PV2, the detection rate of recycled ICs aged for one month is 95.2%. However, for recycled ICs that aged for six months, the detection rate is 100%. The RO-based sensor identifies shorter-aged recycled ICs with smaller intra-die process variations as in PV0, PV1, and PV2.

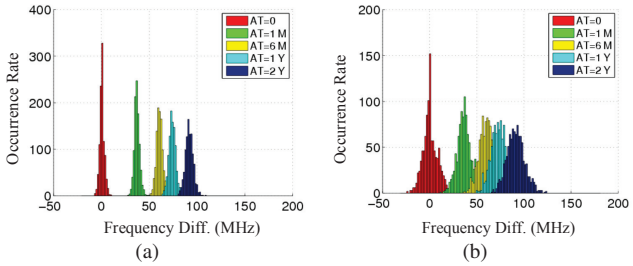


Figure 5. Frequency difference distribution of RO-based sensor with 21-stage ROs with (a) PV1 and (b) PV2.

VI. CONCLUSION

In this paper, we have presented three different structures – RO-CDIR, AF-CDIR, and F-CDIR – to detect recycled ICs of different types and sizes. RO-CDIR structure can be implemented in digital ICs with new technology nodes while the AF-CDIR structure can only be placed in large digital ICs of new and older technology nodes. Finally, the proposed low-cost fuse-based structure can be implemented in any components (small/large, analog/digital). These structures together make it possible to use a low-cost equipment to authenticate ICs very effectively.

REFERENCES

[1] J. Cassell, "Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defence Industry and National Security," April 2012, http://www.ihs.com/images/IHS-iSuppli-Reports-Counterfeit-Parts-Quadruple-Since-2009.pdf.

[2] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing: Theory and Applications (JETTA)*, 2014.

[3] U. Guin, D. Forte, and M. Tehranipoor, "Anti-Counterfeit Techniques: From Design to Resign," in *Microprocessor Test and Verification (MTV)*, 2013.

[4] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment," *Journal of Electronic Testing: Theory and Applications (JETTA)*, 2014.

[5] U. Guin and M. Tehranipoor and D. DiMase and M. Megrdichian, "Counterfeit IC Detection and Challenges Ahead ," *ACM/SIGDA E-NEWSLETTER*, vol. 43, no. 3, March 2013.

[6] U. Guin and M. Tehranipoor, "Counterfeit Detection Technology Assessment," in *GOMACTech*, 2013.

[7] U. Guin and M. Tehranipoor, "On Selection of Counterfeit IC Detection Methods," in *IEEE North Atlantic Test Workshop (NATW)*, May 2013.

[8] L. W. Kessler and T. Sharpe, "Faked Parts Detection," *Circuits Assembly, The Journal for Surface Mount and Electronics Assembly*, June 2010.

[9] X. Zhang and M. Tehranipoor, "Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs," *IEEE Transactions on VLSI Systems*, 2013.

[10] M. Alam and S. Mahapatra, "A comprehensive model of pmos nbti degradation," *Microelectronics Reliability*, vol. 45, no. 1, pp. 71 – 81, 2005.

[11] K.-L. Chen, S. Saller, I. Groves, and D. Scott, "Reliability effects on mos transistors due to hot-carrier injection," *Electron Devices, IEEE Transactions on*, vol. 32, no. 2, pp. 386 – 393, February 1985.

[12] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ics using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE-ACM Design Automation Conference*, June 2012, pp. 703 –708.

[13] Synopsys, "90nm Generic Library."