

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Recycled IC Detection Based on AF and RO Sensors for Security and Reliability

Bhuvaneshwari.M¹, Rajaramya.V.G², Yogananth.A³,Prabakaran.A.P⁴

P.G. Student, Department of ECE, Sembodai Rukmani Varatharajan Engineering College, Nagapattinam,
Tamilnadu, India¹

Associate Professor, Department of ECE, Sembodai Rukmani Varatharajan Engineering College,
Nagapattinam, Tamilnadu, India^{2,3}

Associate Professor, Department of ECE, A.V.C College of Engineering, Mayavaram, Tamilnadu, India⁴

ABSTRACT: The recycling of electronic components has become a major concern for the 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, and mixed-signal) and sizes (large or small) makes it extremely challenging to find a one-size-fits-all solution to detect and prevent recycled 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. These solutions include light-weight, on-chip structures based on ring oscillators (RO-CDIR), anti-fuses (AF-CDIR). Each structure meets the unique needs and limitations of different part types and sizes providing excellent coverage of recycled parts. 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 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.

KEYWORDS: Recycled Integrated Circuits (ICs), hardware security, Aging Effect, Temperature and Process Variation.

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. 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. 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, Business week published an investigation that traced recycled ICs found in U.S. military supplies back to their sources. It was reported 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, 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, 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.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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 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. 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 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. 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.

II. PROPOSED METHOD

A technique is proposed to distinguish used ICs from the unused ones using 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. 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 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 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. In this paper 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. By this way the Recycled IC's are detected from the unused IC's.

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. 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.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

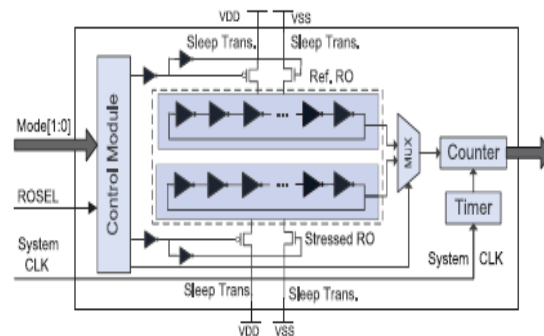


Fig 1 Structure of the RO-based sensor.

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.

In a recycled 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. 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.

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 intra die process variations. It may still be, however, difficult to completely exclude the impact of inter die 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.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

C.Modified Block Diagram

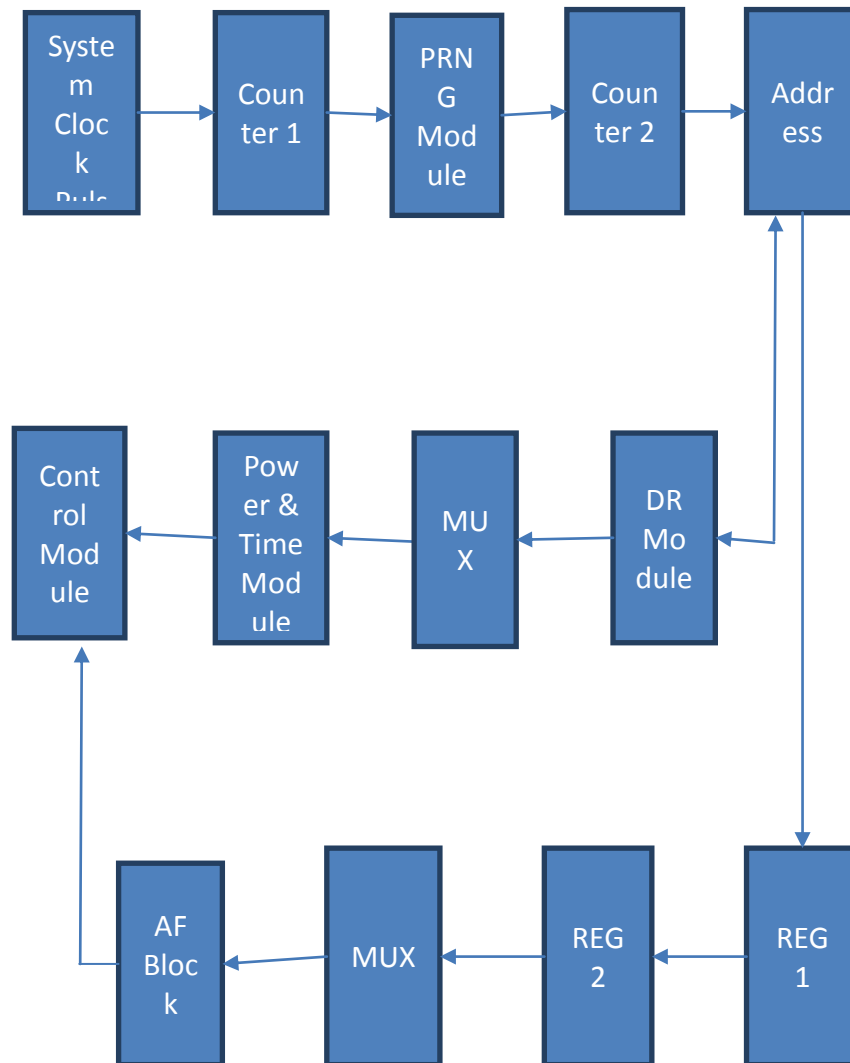


Fig 3. Block Diagram

Explanation:

System clock pulse generates a 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.The output of Counter 1 is given to PRNG Module(Pseudo-Random Number Generator) which gives the false output from which the true output is obtained. 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 (Ts : the time unit reported by the sensor) and the total measurement time (Ttotal). For example, if Ts is 1 h and Ttotal is one year based on the specification of an IC for a 38-bit counter1. 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 (FEPROM) to store the usage time information. In the AF block, prog is assigned to be 1_b1 if the value in counter2 increases by 1. Through connecting

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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. A MUX 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 MUX. 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 . 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.

III.RESULTS AND ANALYSIS

This section mainly deals with the simulation of signal- Antifuse based sensor as well as the RTL and Technological view of ICs.

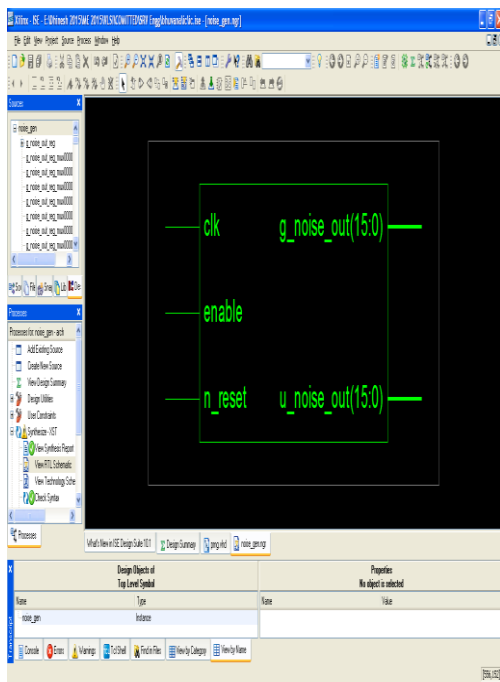


Fig4.RTLoutput of AF-Based sensor

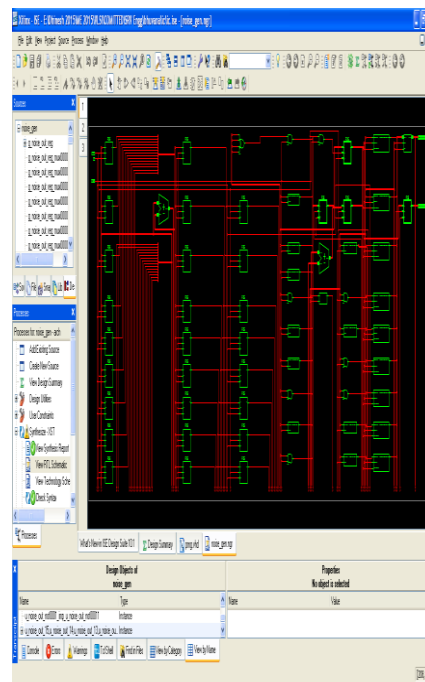


Fig 5.Technology view of AF-Based sensor

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

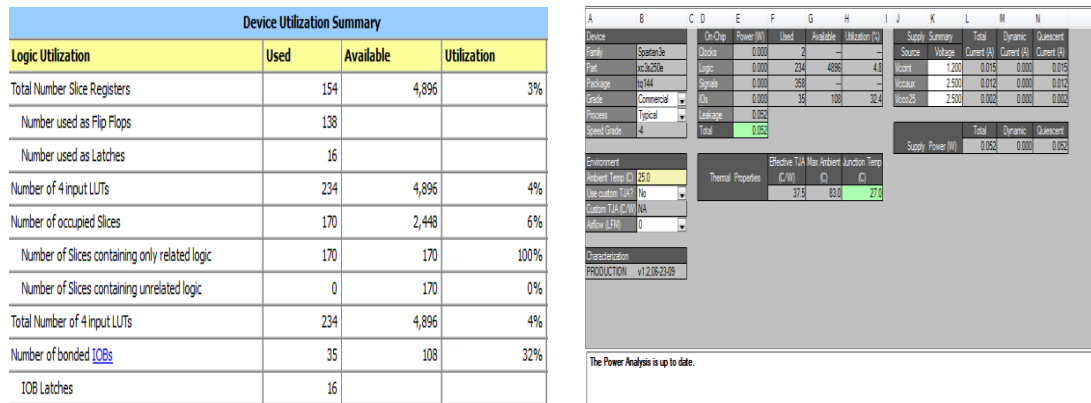


Fig 6.Area Report of the Processor Fig 7.Power Report&Temperature report

IV.CONCLUSION

An AF-based sensor using signal has been developed with low area overhead. 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. 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. Recycled ICs used for a very short period can be detected by the AF-based sensors. 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.

REFERENCES

- [1] X. Zhang and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in Proc. Design Autom. Conf., 2012.
- [2] 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.
- [3] Lu1, Li Shang2, Hai Zhou1,3, Hengliang Zhu1, Fan Yang1, XuanZeng,"Statistical Reliability Analysis Under Process Variation and Aging Effects",IEEEJ.Solid-State Circuits,May.2010.
- [4] "Compact modeling and simulation of circuit reliability for 65-nm CMOS technology" wenpingwang, vijayreddy, anand T. Krishnan,Dec 2007.
- [5] 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.
- [6] "Controlling Short-Channel Effects in Deep-Submicron SOI MOSFETs for Improved Reliability" AnuragChaudhry and M. JagadeshKumar, March 2004."