ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 1, Issue 4, December 2014

A Novel Technique for Effective Detection of Recycled ICs Using Joint Parameter Analysis

M.Maryam Sumayal[1], S.Meribha Sherin[2]

Assistant Professor, ECE, SCAD College Of Engineering and Technology, Tirunelveli, India[1]
Student, M.E. VLSI Design, SCAD College of Engineering and Technology, Tirunelveli, India [2]

Abstract: In recent years, the recycling of integrated circuits (ICs) have become major issues. It potentially impacts the security and reliability of electronic systems bound for critical applications. It would be highly difficult to detect the recycled ICs even using best visual inspection techniques as they have the original appearance, functions and packaging as the devices they are meant to mimic. This paper presents an efficient method to detect the recycled ICs. The technique proposed for recycled ICs detection when used in field is based on antifuse (AF-based). AF based method composed of counter and an embedded one-time programmable memory which is used to record the usage time of ICs. The analysis of usage time stored in AF-based method used to accurately identify the recycled ICs used for even a short period of time.

Keywords*:* counterfeiting recycled ICs, circuit aging reliable.

I. INTRODUCTION

An Integrated Circuits (IC) is a set of electronic circuits on one small plate of semiconductor material normally silicon. This can be made very compact. It may have up to several billion transistors and other electronic components in an area the size of a finger nail. ICs are used in virtually all electronic equipments today. They have revolutionized the world of electronics, computers, mobile phones and other digital home appliances are now inextricable parts of the structure of modern societies, made possible by the low cost of ICs. Microprocessors, digital memory chips and application specific integrated circuits (ASICs) are examples of most advanced ICs. ICs have two main advantages over discrete circuits: costs and performance. Cost is low because the chips, with all their components are printed as a unit by photolithography rather than being constructed one transistor at a time. Performance is high because the ICs components switch quickly and consume little power as a result of the small size and close proximity of the components.

In this paper, the term recycled ICs used to denote used ICs being sold as new or remarked as higher grades. These used or defective ICs enter the market when electronic recyclers divert scrapped circuit boards away from their original motherboard for the purpose of removing and reselling. As the recycling process usually involves a high-temperature environment to remove ICs from boards, there are several security issues associated with these ICs: a used IC can act as a ticking time bomb as it does not meet the specification of the unused ICs and an adversary can include additional die on top of the recycled die carrying a back-door, sabotaging circuit functionality under certain conditions, or causing denial of service.

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 which is much more 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 is reported in that used or defective products account for 80 to 90% of all counterfeits being sold worldwide. With such an estimate on the percentage of used ICs being sold, and the numbers relating to semiconductor sales and counterfeiting in general presented in, it could be possible that the intentional sale of used or defective chips in the semiconductor market could have accounted for about $15 billion USD of all semiconductor sales in 2008 alone. This number could actually be much larger since many of the counterfeit ICs go undetected and are being used in systems today. This number is only going to increase over time. Therefore, it is vital that we prevent these recycled ICs from entering critical infrastructures, aerospace, medical, and defense supply chains.

Usually the tests are performed in an ad-hoc fashion with no metrics based on real data from the test results to quantify effectiveness. Most of the tests are carried out without automation. The test results mostly depend on the subject matter experts (SMEs) and their subjective analysis. The decision making process becomes dependent on the SMEs, which can subject to interpretation. A chip can be considered as counterfeit in one lab while it could be very well marked as an authentic in another lab. Such inconsistency in detection of counterfeit parts can have catastrophic effects. Further, it is difficult to verify components as genuine for certain counterfeit types, such as overproduced, cloned, and tampered ICs. Test time and cost are major limiting factors for uniform implementation of detection methods. Finally, low-cost designs for counterfeit prevention approaches are needed to help prevent counterfeiters from shipping the counterfeited parts to the supply chain.

A. Previous Work

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. Physical unclonable functions implemented challenge and response authentication for IC identification. For each physical stimulus, the circuit may 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 using active and passive authentication and identification are known as hardware metering. 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.

Physical tests and inspections are often used to identify recycled ICs by visual inspection, blacktop testing, and scanning electron microscopy, scanning acoustic microscopy, X-ray imaging, X-ray fluorescence, 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.

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. Paper Organization

In the proposed system AF and RO is used to detect the recycled ICs. Therefore every recycled ICs should be identified even if it is used for a short period of time. Here any ICs which are recycled can be effectively detected. By using the AF one time programmable memory the area over head can be reduced. The paper is organized as follows: Section II explains about the antifuse memory. Section III describes about the main design. Results are discussed in Section IV and a conclusion is given in section V.

II. AF MEMORY

An antifuse is an electrical device that performs the opposite function to a fuse. Whereas a fuse starts with a low resistance and is designed to permanently break an electrically conductive path (typically when the current through the path exceeds a specified limit), an antifuse starts with a high resistance and is designed to permanently create an electrically conductive path (typically when the voltage across the antifuse exceeds a certain level). This technology has many applications.

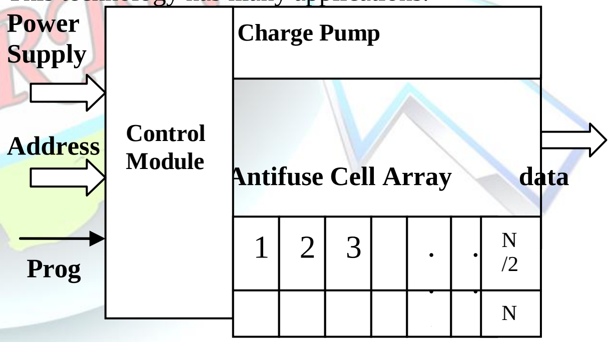


Fig.1 Typical Interface of AF memory

Antifuses are widely used to permanently program ICs. Antifuse PLDs are one time programmable in contrast to other PLDs that are SRAM based and which may be reprogrammed to fix logic bugs or add new functions. Antifuse PLDs have advantages over SRAM based PLDs in that like ASICs, they do not need to be configured each time power is applied. They may be less susceptible to alpha particles which can cause circuits to malfunction. Also circuits built via the antifuse's permanent conductive paths may be faster than similar circuits implemented in PLDs using SRAM technology. Quick Logic Corporation refers to their antifuses as "Via Links" because blown fuses create a connection between two crossing layers of wiring on the chip in the same way that a via on a printed circuit board creates a connection between copper layers. Antifuses may be used in programmable read-only memory (PROM). Each bit contains both a fuse and an antifuse and is programmed by triggering one of the two. This programming, performed after manufacturing, is permanent and irreversible.

Dielectric antifuses employ a very thin oxide barrier between a pair of conductors. Formation of the conductive channel is performed by a dielectric breakdown forced by a high voltage pulse. Dielectric antifuses are usually employed in CMOS and BiCMOS processes as the required oxide layer thickness is lower than those available in bipolar processes.

III. Main Design

The AF-based sensor is composed of counters with usage time of ICs when power-on stored in an embedded antifuse 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 antifuse block in the AF-based sensor are: it consumes less power to program or read compared with other types of OTP structures, such as electrical fuse or CMOS floating gate, the area of an antifuse is much smaller than an efuse, and 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 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 including power supply, address, prog, and data signals.

The synchronous design operates at highest frequency that derives a large load because it has to reach many sequential elements throughout the chip. Thus clock signals have been a great source of power dissipation because of high frequency and load. Clock signals do not perform any computation and mainly used for synchronization. Hence these signals are not carrying any information. So by using clock gating one can save power by reducing unnecessary clock activities inside the gated module. The circuit is based on a new clock gating flip flop approach to reduce the signal’s switching power consumption.

Clock signal is disabled when reset is 0 using clock gate techniques. In this, clock is selectively suspended without changing the functionality. Using this technique, clock is enabled and count starts only when IC is switched ‘on’. Thus this technique reduces time required. Thereby reduces the switching activity and the power consumption. Clock is enabled and count starts only when IC is switched ‘on’. Thus this technique reduces time required. Thereby reduces the switching activity and the power consumption.

Program and read operations, share the same address signals in AF block. Control signals are 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.

Once we get the previous usage time, it will be stored in register 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. Then the counter value is increased by one. 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 control signal and an authentication 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 reach the test_out. If the IC is in authentication mode by enabling the authentication signal, the data read module will set the AF IP in read mode. 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.

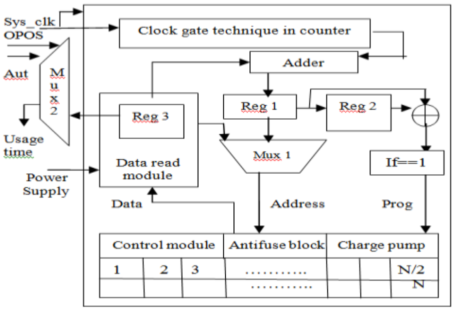


Fig.2 Structure of AF based method

The area overhead caused by AF-based sensors depends on the application and specification of ICs. The time recorded by 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.

As the AF-based sensor only records number of usage time the recycled ICs even turned on can be identified. With appropriate value recorded in counter every time power on is combined with previous usage time to be stored in the AF memory block in CAF-based sensor. 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.

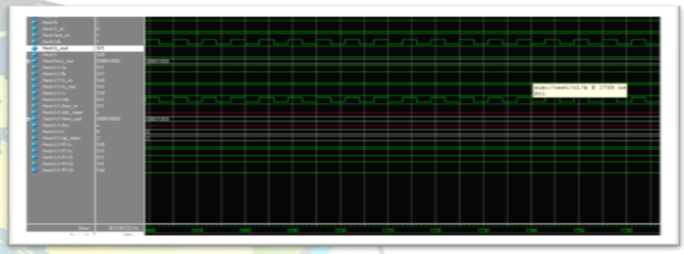
IV. Results

To verify the effectiveness of the AF-based and RO-based sensor, it can be simulated using Modelsim simulator. Here the recycled ICs used for even short period of time are detected. From the 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 is identified easily. test_out shows the usage time of the IC.

V. Conclusion

AF based method which uses counter and a one-time programmable memory to detect the recycled ICs even it is used for a very short time as the counter value is stored in the antifuse memory once the CUT is turned on. Experimental results and analysis demonstrated the effectiveness of these sensors.

Fig.3 Output of AF based method



References

[1]. 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.

[2]. 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.

[3]. 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.

[4]. 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.

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

[6]. 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.

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

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

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

[10]. *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