IJERST

International Journal of
Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 1
March 2015

National Conference on "Recent Prends in Communication & Information Technologies"NCRTCIT 2015

Organized by
Dept. of ECE, Indra Ganesan College of Engg., Trichy, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 1, March 2015
National Conference on "Recent Prends in Communication & Information Technologies" NCRTCIT 2015

Research Paper

RECYCLED IC DETECTION BASED ON AF AND RO SENSORS FOR SECURITY AND RELIABILITY

Bhuvaneswari M[1]*, Prabakaran A P[2] and Rajaramya V G[1]

*Corresponding Author: Bhuvaneswari M ✉

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-sizefits- 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, onchip 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 thatrecycled 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.

INTRODUCTION

The counterfeiting of integrated circuits (ICs) is on the rise, potentially impacting the security of a wide variety ofelectronic systems. A counterfeit componentis defined as an electronic part that is notgenuine.1) is an unauthorized copy; 2) doesnot conform to original component manufacturers design, model, orperformance or both; 3) is not produced bythe 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

[1] Sembodai Rukmani Varatharajan Engg. College, Nagapattinam.
[2] AVC College of Engg, Sembodai Rukmani Varatharajan, Mayavaram.

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 productsconsidered80%–90% of all counterfeitsbeing sold worldwide. With such estimateon the percentage of used ICs being sold,and the numbers relating to semiconductor sales and counterfeiting in generalpresented, it could be possible that theintentional sale of used or defective chips inthe semiconductor market could haveconsidered about $15 billion of allsemiconductor sales in 2008 alone. Thisnumber could actually be much larger asmany of the counterfeit ICs go undetectedand are being used in systems today. Inaddition, suggest that this number is onlygoing to increase over time. These used ordefective ICs enter the market whenelectronic recyclers divert scrapped circuitboards away from their designated place ofdisposal for the purposes of removing andreselling the ICs on those boards.

As the recycling process usuallyinvolves a high-temperature environment toremove ICs from boards, there are severalsecurity issues associated with these ICs: 1)a used IC can act as a ticking time bomb asit does not meet the specification of theunused (new) ICs and 2) an adversary caninclude additional die on top of the recycleddie carrying a back-door attack, sabotagingcircuit functionality under certainconditions, or causing denial of service.Therefore, it is vital that we prevent theserecycled ICs from entering critical infrastructures, aerospace, medical, anddefense supply chains. In this paper, theterm recycled ICs is used to denote used ICsbeing sold as new or remarked as highergrades. The terms unused ICs and new ICsrepresent the ICs that are brand new. On theother hand, most ICs used in the field are notturned on all the time. Consider an IC usedin a cell phone, for example; the cell phonemay only be powered on during the day forsome period. The real (power-on) usagetime of the IC would be much shorter thanthe usage time with power off intervals. Inthis paper, the term usage time is used torepresent the accumulated power-on timeeven if the IC is used intermittently. Ingeneral, the recycled ICs have the originalappearance, functionality, and markings asthe devices they are meant to mimic, butthey are used for a period before they areresold. Even the best visual inspectiontechniques will have difficulty in identifyingthese ICs with certainty. Additionally,because recycled ICs contain the originalcorrect die internally, decapping technologies will provide little assistance intheir detection. It is vital to develop newtechniques to help in measuring these ICs'specifications and effectively detect them ifthey are already used in the field even for ashort period.

PROPOSED METHOD

A technique is proposed to distinguish used ICs from the unused ones using light-weight on-chip sensor. Usingstatistical data analysis, process andtemperature variations' effects on the sensorscan 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 (RObased 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 thresholdvoltage (HVT) gates to expedite aging henceICs used for a period can be identified .Thereference RO is gated off from the powersupply during chip operation, hence itexperiences less stress. The frequencydifference between the two ROs coulddenote the usage time of the chip under test(CUT). The AF-based sensor, composed ofcounters and an embedded antifuse (AF)memory block, is also proposed to identifyrecycled ICs. The counters are used torecord the usage time of ICs and the value isdynamically stored in the AF memory blockby controlling the programming signal. Asthe AF memory block is one-timeprogrammable (OTP), recyclers could noterase the context during recycling process.Therefore, our AF-based sensor is resilientto removal and tampering attacks. In thispaper AF-based sensor using clock AF(CAF-based) records the cycle count of thesystem clock during the chip operation. Theusage time of recycled ICs can be reportedby this sensor and the measurement scaleand total measurement time could beadjusted according to the application of ICs.By this way the Recycled IC's are detectedfrom the unused IC's.

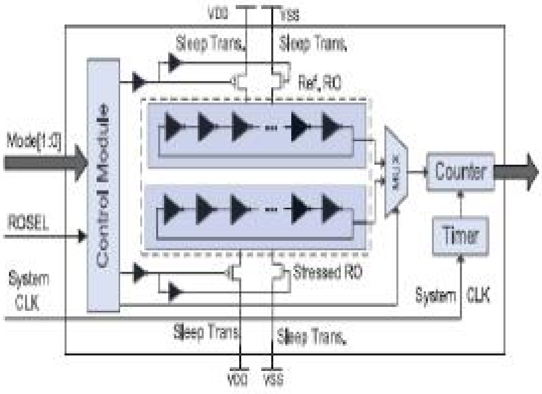
A. RO-Based Sensor

Our main objectives in designing theRO-based sensor are as follows: 1) thesensor must age at a very high rate to helpdetect ICs used for a short period; 2) thesensor must experience no aging ornegligible aging during manufacturing test;3) the impact of process variations andtemperature on RO-based sensor must beminimal; 4) the sensor must be resilient toattacks; and 5) finally, the measurementprocess must be done using low-costequipment and be very fast and easy. Asmentioned earlier, aging effects could slowdown the frequencies of ROs embedded intoICs. With an embedded RO, these recycledICs could be identified based on itsfrequency, which will be lower than that of anew IC. There are, however, manyparameters impacting the frequency of anRO, such as temperature and processvariations. Our RO-based sensor uses areference RO and a stressed RO to separatethe aging effects fromprocess/environmental variations. Thestructure of our RO-based sensor, which iscomposed of a control module, a referenceRO, a stressed RO, a MUX, a timer, and acounter.

The counter measures the cyclecount of the two ROs during a prespecifiedtime, which is controlled by the timer.System clock is used in the timer tominimize the measurement period variationsbecause of circuit aging. The multiplexer(MUX) selects which RO is going to bemeasured, and is controlled by the ROSELsignal. The reference and stressed ROs areidentical; both are composed of HVT components.

The inverters could be replaced byany other types of gates (NAND, NOR,etc.,) only if they can construct an RO. Itwill not change the effectiveness of the RO5based sensor significantly according to theanalysis. We use smaller stage ROs in ourRO-based sensor considering the counter'smeasurement speed limits given atechnology. For example, in our 90-nmtechnology, a 16-bit counter can operateunder frequency of up to 1 GHz; an inverterbasedRO of at least 21 stages is thenrequired. Sleep transistors are used toconnect the ROs to the power supply in theRO-based sensor; pMOS sleep transistorscontrol the connection between VDD andthe inverters and n-type MOS sleeptransistors control the connection betweenVSS and the inverters.

Figure 1: Structure of the RO-based Sensor



Both the reference and the stressedROs work in three modes that are controlledby the mode signal. 1) When the IC is inmanufacturing test mode, the reference andstressed ROs will be disconnected from thepower supply and experience no aging. Thismode only lasts a short time, depending onthe test procedures of the IC; 2) When theIC is in normal functional mode, thereference RO will be disconnected fromVDD and VSS but the stressed RO will begated on and will age. The frequency of thestressed RO will drop, whereas the referenceRO will not change a lot. ICs will spendmost of their time in this mode; 3) When theIC is in authentication mode (i.e., when anIC is taken from market and its authenticityis to be verified), both the reference andstressed ROs will be gated on by connectingto the power supply. The timer and counterwill be enabled to measure ROs' cycle countand ROSEL signal will select which RO tomeasure. The rest of the functionality of theIC would be turned off by mode signals andthe authentication process takes a very shortperiod. The three modes of operation ensurethat 1) the frequency difference between thereference and stressed ROs will be largerover time as the reference RO cannot begated on alone and 2) it is extremely difficult for adversaries to force the RO based sensor to operate in authentication mode when it is supposed to be in its normalfunctional mode, which would eliminate theaging difference. The only method to do thatwould be to modify the original RO-basedsensor module, which is impossible during asimple recycling process.

The inverters of the reference and thestressed ROs are placed physically next toeach other, designed as a single smallmodule. The process and environmentalvariations between them should be verysmall. Therefore, for a new IC, thefrequency difference between the referenceand the stressed ROs would be within acertain small range.

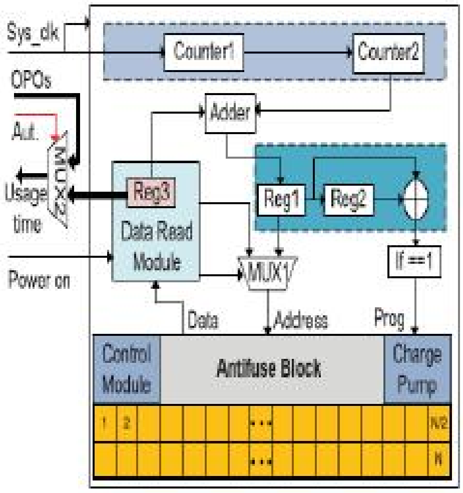
In a recycled IC, the stressed RO willhave suffered aging from its own oscillationsince the chip has been working in normalfunctional mode for a long time. Thereference RO, however, will not haveexperienced as much aging as it is gated off.The frequency difference between thereference and the stressed ROs will growlarger as the chip operates longer, which isdemonstrated by our simulation and siliconresults. If the frequency difference is outsideof the new ICs' frequency difference rangeconsidering process variations, we canconclude with high confidence that the CUTis recycled from used boards. The areaoverhead of our RO-based sensor isnegligible when compared with the millionsof gates in modern ICs.

Power consumption is also limited tothat consumed by the stressed RO in theRO-based sensor. Moreover, the testoverhead caused by the RO-based sensor isminimal as it is composed of such a smallnumber of standard gates. In addition, theRO-based sensor can be functional. We canargue that the starting time point of thesensors will be shifted from 0 to some agingtime (such as weeks), which makes itdifficult to distinguish used and new ICs. Asfor the impact of the testing process on thesensor, both ROs are kept in off mode usingthe sleep transistors thus the impact of agingand high temperature during test processwill be negligible. Therefore, the startingpoint will remain the same. In early lifefailure of the sensor, more than one sensorcan be added to the design. This will ensurethat one sensor is operating properly in thefield.

B. AF-Based Sensor

In the RO-based sensor, the invertersof the reference and the stressed ROs areplaced physically next to each other tominimize the impact of intra die processvariations. It may still be, however, difficultto completely exclude the impact of inter dieprocess variations on the sensor. In addition,RO based sensor provides only anapproximation of the usage time in a form ofaging in the stressed RO. Therefore, thesensitivity (the minimum usage time ofrecycled ICs detected by sensors) of the RObasedsensor is limited. For example, it maynot identify recycled ICs used shorter than 1month based on our simulation.

Figure 2: Structure of the CAF-based Sensor



To eliminate the issue of processvariations, provide a more accurate usagetime, and identify recycled ICs that are onlyused for a very short period for data read inCAF- and SAF-based sensors. we proposetwo AF-based sensors: CAF-based sensorand SAF-based sensor. 1) CAF-BasedSensor: the structure of the CAF-basedsensor, which is composed of two counters,a data read module, an adder, and an AFOTP memory block. Sys_clk is the highfrequencysystem clock, providing clock fordifferent modules including the data readmodule, the AF block, and registers. Counter1 is used to divide the highfrequencysystem clock to a lower frequencysignal, Counter2 is used to measure thecycle count of the lower frequency signal.

The size of the two counters can be adjustedaccordingly depending on the measurementscale (Ts : the time unit reported by thesensor) and the total measurement time(Ttotal). For example, if Ts is 1 h and Ttotalis one year based on the specification of anIC, a 38-bit counter1 will meet therequirement to count the usage time from 20ns (assume system clock = 50 MHz) to 1 hand a 14-bit counter2 will count the usagefrom 1 h to 8760 h (one year). As the datastored in registers (counters) could be lost orreset when power supply is off, non erasablememory is required in this sensor. Anembedded AF OTP block is used instead ofa field-programmable read-only memory(FPROM) to store the usage timeinformation because FPROM could betampered or altered by attackers. In the AFblock, prog is assigned to be 1_b1 if thevalue in counter2 increases by 1. Throughconnecting the output of counter2 to address8in the AF block directly, the related AF cellwill be programmed as 1.

Therefore, the largest address of thecell whose content is 1 will be the usagetime of CUT based on the measurementscale setup by counter1. From the abovedescription, the size of the AF block will bereduced using two counters. Program andread operations, however, share the sameaddress signals in AF block. Therefore, aMUX (MUX1 in Figure 8), controlled by dataread module, is used to select the address(AF cell) to be read or programmed. Everytime power supply is on, the AF block willwork in read mode for a short period.

During this time, the read address generatedby data read module will go through MUX1and all the AF cells will be traversed basedon the traversing binary tree principle. Thealgorithm for data read in an N-bit AFblock. There are log(N/2) loops in thealgorithm. The address is increased ordecreased by 2i"1[i = 0, . . . log(N/2)] forthe i th loop based on the value in theaddress. If the value stored in the address is1 ([address] == 1) and the value stored in thenext address is 0, the address will representthe usage time before power-on based on Ts.

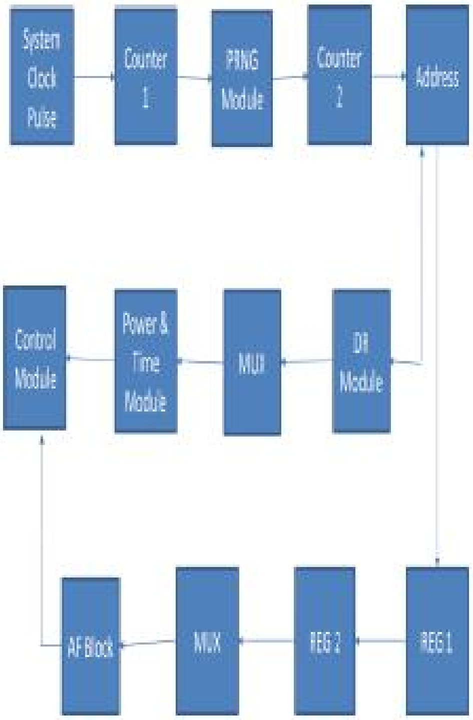
The read operation will last less thanlog(N/2) + 1 system clock cycles, dependingon the value stored in the AF block; thistime will be recorded by counter1, as well.Once we get the previous usage time, it willbe stored in register Reg3 and sent to theadder. The reason for using an adder here isthat counters start from 0 every time thepower is turned on and the previous usagetime must be considered when we calculatethe total usage time. In addition, Reg1 isused to sample the data in adder, Reg2delays the data in Reg1 with one systemclock, and XOR gates are used to comparethe data in Reg1 and Reg2. If they aredifferent (denoting the usage timeincreased), the AF OTP block will work inprogram mode and the data in Reg1 will gothrough MUX1 to the address in the AFblock. Therefore, combined with the valuein counter2 (the usage time after power-on),the new total usage time will be stored in theAF OTP block by programming a new AFcell with a larger address. From thisdiscussion, the AF OPT block isprogrammed internally. Through designingour sensor in this way, we can reduce theprobability of altering or tampering attackson the AF-based sensor.

To eliminate the need for additionalpins for authentication purposes on the chip,our CAF-based sensor uses a MUX (MUX2)and an authentication (Aut.) pin to send theusage time to the output pins of ICs. Thus, no extra output pins will be added to theoriginal design. When the IC works innormal functional mode, original primaryoutputs will go through MUX2. If the IC isin authentication mode by enabling the authentication signal, the data read modulewill set the AF IP in read mode and theusage time will go through MUX2. Inaddition, when the IC works inmanufacturing test mode, the functionalityof our CAF-based sensor will be disabledand structural fault test patterns will beapplied to the sensor.

C. Modified Block Diagram

Explanation: System clock pulse generatesa high frequency system clock, providingclock for different modules including thedata read module, the AF block andRegisters. Counter1 is used to divide thehigh- frequency system clock to a lowerfrequency signal.The output of Counter 1 isgiven to PRNG Module(Pseudo-Random Number Generator) which gives the falseoutput from which the true output isobtained. Counter2 is used to measure thecycle count of the lower frequency signal.

Figure 3: Block Diagram

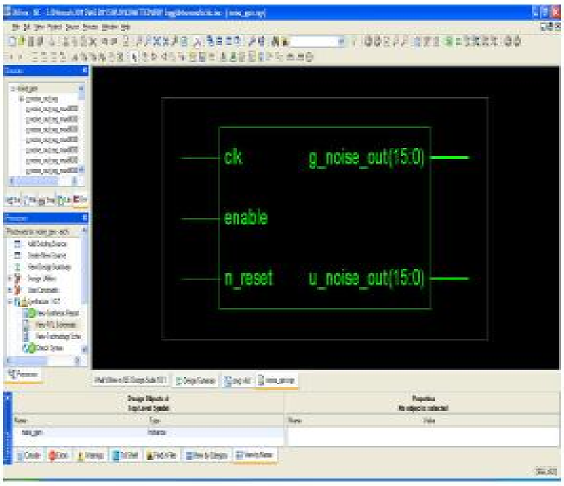


The size of the two counters can be adjustedaccordingly depending on the measurementscale (Ts : the time unit reported by thesensor) and the total measurement time(Ttotal). For example, if Ts is 1 h and Ttotalis one year based on the specification of anIC for a 38-bit counter1. As the data storedin registers (counters) could be lost or resetwhen power supply is off, nonerasablememory is required in this sensor. Anembedded AF OTP block is used instead ofa field-programmable read-only memory(FPROM) to store the usage timeinformation. In the AF block, prog isassigned to be 1_b1 if the value in counter2increases by 1. Through connecting theoutput of counter2 to address in the AFblock directly, the related AF cell will beprogrammed as 1. Therefore, the largestaddress of the cell whose content is 1 will be the usage time of CUT based on themeasurement scale setup by counter1. Fromthe above description, the size of the AFblock will be reduced using two counters. AMUX controlled by data read module, isused to select the address (AF cell) to beread or programmed. Every time powersupply is on, the AF block will work in readmode for a short period. During this time,the read address generated by data readmodule will go through MUX. If the valuestored in the address is 1 ([address] == 1)and the value stored in the next address is 0,the address willrepresent the usage timebefore power-on based on Ts. In addition,

Reg1 is used to sample the data in adder,Reg2 delays the data in Reg1 with onesystem clock, and XOR gates are used tocompare the data in Reg1 and Reg2. If theyare different (denoting the usage timeincreased), the AF OTP block will work inprogram mode and the data in Reg1 will gothrough MUX1 to the address in the AFblock. Therefore, combined with the valuein counter2 (the usage time after power-on),the new total usage time will be stored in theAF OTP block by programming a new AFcell with a larger address.

RESULTS AND ANALYSIS

This section mainly deals with thesimulation of signal- Antifuse based sensoras well as the RTL and Technological viewof ICs and also the Modelsim output.



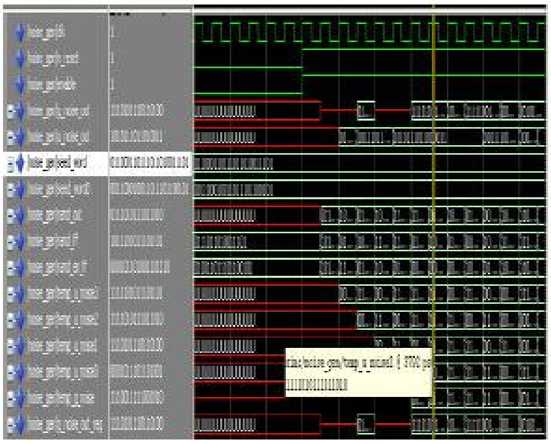


Figure 4: RTL Output of AF-Based Sensor

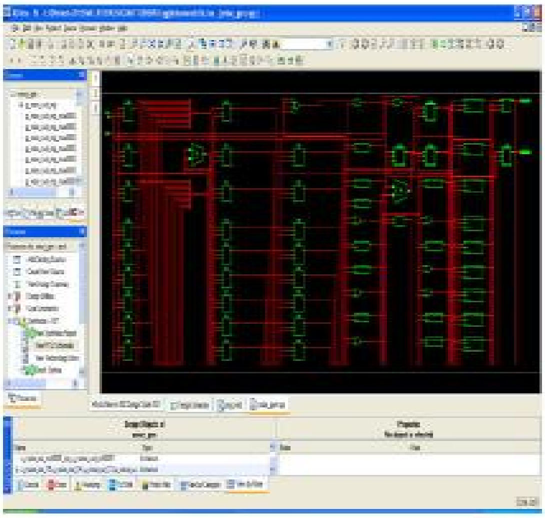


Figure 5: Technology View of AF-Based Sensor

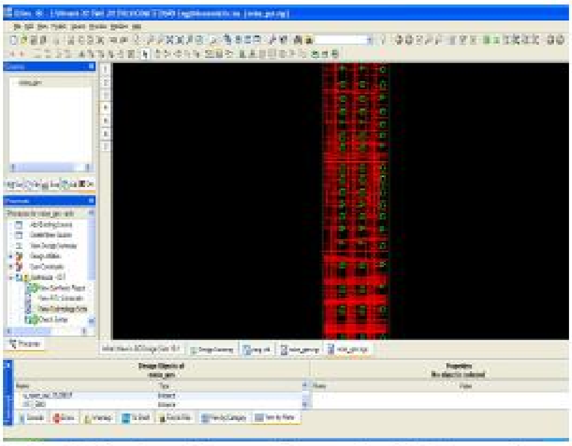
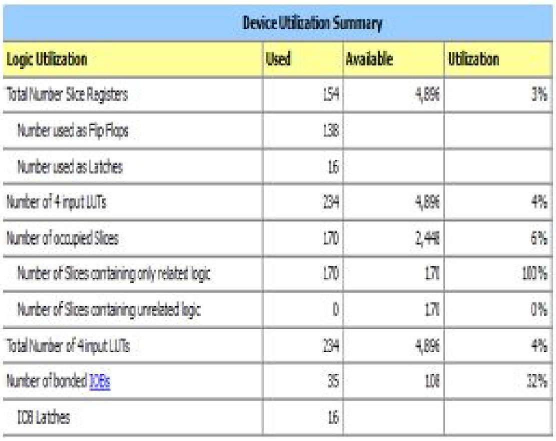
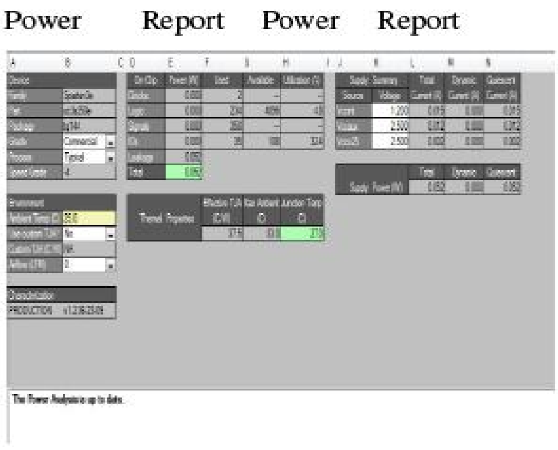


Figure 6: Area Report of the Processor



Device Utilization Summary			
Logic Utilization	Used	Available	Utilization
Total Number Slice Registers	154	4,896	3%
Number used as Flip Flops	138		
Number used as Latches	16		
Number of 4 input LUTs	234	4,896	4%
Number of occupied Slices	170	2,448	6%
Number of Slices containing only related logic	170	170	100%
Number of Slices containing unrelated logic	0	170	0%
Total Number of 4 input LUTs	234	4,896	4%
Number of bonded IOBs	35	108	32%
IOB Latches	16		

Figure 7: Power Report and Temperature Report



Power　Report　Power　Report

The Power Analysis is up to date.

CONCLUSION

An AF-based sensor using signal hasbeen developed with low area overhead. Theusage time stored in the AF memory usingAF based sensors could show how long anIC had been used and then identify arecycled IC. For AF-based sensor, as theusage time of the ICs is calculated bycounters and stored in the AF block, processand temperature variations cannot impactthe data in AF cells. Recycled ICs used for avery short period can be detected by the AF based sensors. For AF-based sensors,attackers would try to mask the usage timeof ICs by disabling the sensor. The AF based sensor, however, will automatically run whenever power is on and the usagetime will be stored in the AF memory directly. Therefore, it is impossible for attackers to disable the sensor withoutremoving the package and breaking the chip.

REFERENCES

1. “A Novel Gate-level NBTI DelayDegradation Model withStacking Effect”.
2. “Compact modeling andsimulation of circuit reliability for65-nm CMOS technology” wenping wang, vijay reddy, an and T. Krishnan,Dec 2007.
3. “Controlling Short-ChannelEffects in Deep-Submicron SOIMOSFETs for Improved Reliability” Anurag Chaudhry and M. Jagadesh Kumar,March 2004.”
4. Stradley J and Karraker D (2006), “The electronic part supply chainand risks of counterfeit parts indefense applications”, *IEEE Trans. Compon. Packag. Technol.*, Vol. 29, No. 3, pp. 703–705.
5. Lu1, Li Shang2, Hai Zhou1;3,Hengliang Zhu1, Fan Yang1, XuanZeng,”Statistical Reliability AnalysisUnder Process Variation and Aging Effects”, *IEEE J. Solid-State Circuits*, May. 2010.
6. “Modeling and Minimization ofPMOS NBTI Effect forRobust Nanometer Design”.
7. Zhang X and Tehranipoor M (2012), “Identification of recovered ICs using fingerprints from a lightweighton-chip sensor,” in Proc.Design Autom. Conf.
8. Zhang X and Tehranipoor M (2012), “Path-delay fingerprinting ofidentification of recovered ICs,” in Proc. IEEE Int. Symp. Defect FaultTolerance VLSI Nanotechnol. Syst.,*Oct.*

IJERST

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991
9 772319 599001 01