Path-Delay Fingerprinting for Identification of Recovered ICs

Xuehui Zhang, Kan Xiao and Mohammad Tehranipoor
ECE, University of Connecticut
{xuehui.zhang, kan.xiao, tehrani}@engr.uconn.edu

Abstract

The counterfeiting of integrated circuits (ICs) has been on the rise over the past decade, impacting the security and reliability of electronic systems. Reports show that recovered ICs contribute to about 80% of all counterfeit ICs in the market today. Such ICs are recovered from scrapped boards of used devices. Identification of such counterfeit ICs is a great challenge since these ICs have an identical appearance, functionality, and package as fresh ICs. In this paper, a novel path-delay fingerprinting technique is proposed to distinguish recovered ICs from fresh ICs. Due to degradation in the field, the path delay distribution of recovered ICs will become different from that found in fresh ICs. Statistical data analysis can effectively separate the impact of process variations from aging effects on path delay. Simulation results of benchmark circuits using 45nm technology demonstrate the efficiency of this technique for recovered IC identification.

I. Introduction

The counterfeiting of semiconductor components has been on the rise for many years, and recent increases in the counterfeiting of integrated circuits have been especially troubling. The number of microcircuit-related counterfeiting incidents reported by component manufacturers more than doubled over the period from 2005 to 2008 [1]. One subset of these counterfeits whose growth has been particularly fast are the “recovered” or “recycled” ICs. These recovered ICs enter markets when electronics “recyclers” divert old circuit boards from their proper place of disposal, strip the ICs from their boards, refine the ICs, and send the ICs back to the market. It is estimated that these “recovered” ICs- generically defined as used parts being sold as new or remarked as higher grades - account for 80% of all counterfeits being sold worldwide.

The growth of this type of counterfeit is worrisome for two reasons: the reliability and security concerns that these recovered ICs present, and the difficulties involved with detecting them. Recovered ICs are less reliable than their fresh counterparts. The stresses induced by the recovery process and the previous usage of the IC in the field will result in recovered ICs having reduced lifetimes, causing them to act like ticking time bombs in the systems using them [2]. Previous usage of the IC can result in degradation of performance-related parameters of the IC, causing recovered ICs to operate at lower performance (frequency and power). Recovered ICs may also have been further tampered with during the recycling process, and represent a general reliability and security risk.

Some recovered ICs may be detected through careful visual inspection, decaping, or X-ray photography, since the markings or parts of the package may have been damaged during the refining process. However, most recovered ICs are refined by professional remarking, packaging, and cleanup processes. It is very difficult to identify them, since they have the same appearance and functionality as their fresh counterparts.

Silicon physical unclonable functions (PUFs) have been developed to generate unique identifiers for each IC based on process variations [3] [4] [9]. Passive metering approaches uniquely identify each IC and register the IC using challenge-response pairs [10]. Active metering approaches lock each IC until it is unlocked by the IP holder [11]. Although extensive research exists in the domain of counterfeit detection and IC metering, not much research has yet to address the issue of recovered ICs. The only approach that has been proposed to identify recovered ICs is presented in [5] which uses a light-weight on-chip sensor. The simulation and silicon results demonstrated the effectiveness of this approach. However, this approach only works best for designs with this sensor but cannot address detection of existing and legacy ICs that have no such sensors embedded in them. We acknowledge that path-delay fingerprinting has already been used for detecting hardware Trojans [6]. The concept used in this paper is similar however we use clock sweeping techniques for fingerprint generation for the detection of used ICs impacted by aging.

Since recovered ICs have been used in the field before they were resold into the market, the performance of such ICs must have been degraded by aging effects, compared to fresh ICs. In this paper, we propose a path-delay based fingerprinting technique to identify recovered ICs. For fresh ICs, the delay distribution of paths will be within a certain range. The fingerprint of the fresh ICs can be generated during manufacturing test of these ICs and stored in a secure memory for future use when identifying recovered ICs. Due to aging effects, such as negative/positive bias temperature instability (NBTI/PBTI) and hot carrier injection (HCI), the path delays in recovered ICs will be larger than those in fresh ICs. For a chip under authentication (CUA), the larger the path delays are, the higher the probability there is that the CUA has been used and is a recovered IC. In this paper, we propose a fingerprinting and authentication flow for accurately identifying recovered ICs. Statistical data analysis is used to distinguish the path delay changes caused by process and temperature variations from those caused by aging. Since the path delay information is measured during the manufacturing test process, no extra hardware circuitry is required for this technique. In addition, there is no change required in current industrial design and test flows. Finally, this technique presents no area overhead, no power consumption, and is resilient to attacks.

The rest of the paper is organized as follows: Section II analyzes the effect of aging on different gates and paths. Section III presents our path-delay based fingerprinting technique and authentication flow. Statistical data analysis methods used in this paper are presented in Section IV. Simulation results and analysis are presented in Section V. Finally, concluding remarks are given in Section VI.

978-1-4673-3044-2/12/$31.00 © 2012 IEEE

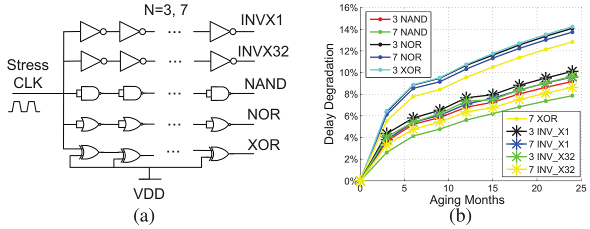


Fig. 1. (a) An illustrative circuit with NAND, NOR, XOR, and INV chains and (b) Delay degradation of the chains.

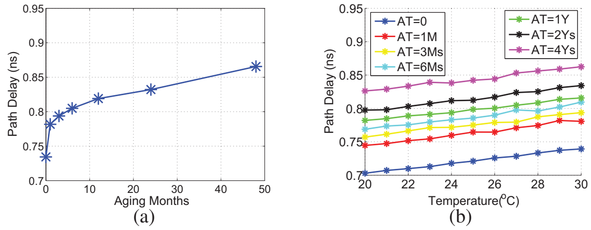


Fig. 2. (a) Delay degradation of path P_i and (b) P_i delay increases with increased temperature.

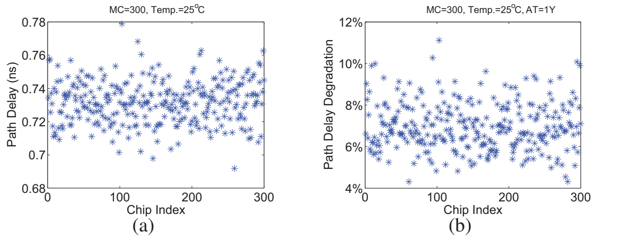


Fig. 3. (a) Delay of path P_i with process variations and (b) Delay degradation of path P_i changing with process variations.

II. Path-Delay Degradation Analysis

When a chip is used in the field, aging effects could cause some of its parameters to shift over time. NBTI increases the absolute value of the PMOS threshold voltage and results in decreasing transistor current and increasing gate delay [12] [13] [15]. HCI creates traps at the silicon substrate/gate dielectric interface, as well as dielectric bulk traps, and therefore degrades device characteristics including voltage threshold [12] [13] [15]. Since recovered ICs have been impacted by all of these aging effects, the path delay of recovered ICs will be different from those of fresh ICs.

In order to demonstrate the impact of aging on path delay in ICs, in a simple manner, different gate chains were simulated using a 45nm technology [7] as shown in Figure 1(a). The simulation was conducted by HSPICE MOSRA [8] with the built-in aging model [8] and combined NBTI and HCI aging effects at a temperature of 25°C. Standard threshold voltage (SVT) INVX1, INVX32, NAND, NOR, and XOR gate chains of different lengths were simulated for up to 2 years of usage. Figure 1(a) shows that all chains are experiencing stress from a 500MHz clock. Any other stress (e.g., DC stress which is a constant "0" or "1", or AC stress with different duty ratios) and usage time could be used in this simulation. Figure 1(b) presents the delay degradation caused by 2 years (24 months) of aging. From the figure, we can see that different gate chains age at slightly different rates, which depends on the structure of the gates. The XOR gate chain has the fastest aging rate amongst these chains. Comparing the delay degradation rates of the INVX1 and INVX32 chains, we can conclude that larger gates will age at a lower rate than smaller gates with the same stress. In addition, the workload (input value and the switching frequency of each gate) also has a significant impact on the aging rate. ICs may be recovered from different used boards from different users who may have applied different workloads to the IC at different times. It is practically impossible to know the exact input vectors applied by the user. We will discuss this and the impact workload has on a chip's path delay degradation in detail in Section III.

Figure 2(a) shows the delay of a randomly selected critical path P_i (this path includes 22 gates) from the ISCAS'89 benchmark s38417 with stress from a random workload (functional patterns) applied to the primary inputs. The path was aged for 4 years with NBTI and HCI effects at room temperature 25°C. From the figure, we can see that the degradation of path P_i used for 1 year is around 10% while if the circuit is used for 4 years, the degradation is about 17%, indicating that most aging occurred at the early usage phase of the design. Therefore, if there are no environmental or process variations, such degradation should provide great opportunities to identify recovered ICs by measuring one path delay from the circuit. However, these variations have a significant impact on the path delay. On the other hand, different paths age at different rates as demonstrated earlier in this section. Figure 2(b) shows the delay of path P_i under different temperatures at different aging times. In the figure, AT denotes aging time, M represent months, and Y denotes years. From Figure 2(b), we can see that the delay of path P_i increases as we increase the temperature and paths age at different speed under different temperature.

To analyze variations' impact on P_i's delay, we perform Monte Carlo simulation using HSPICE on s38417. 300 Monte Carlo simulation results of P_i at 25°C are shown in Figure 3(a), with 3-sigma 2% T_{ox}, 5% V_{th}, and 5% L inter-die and 1% T_{ox}, 5% V_{th}, and 5% L intra-die process variations. We can see that P_i's delay varies around 12% due to process variations. In addition, process variations also have a significant impact on the aging rate of path delay, as shown in Figure 3(b). P_i's delay degradation in the 300 ICs varied around 8% (4% $\sim$ 12%) for one year of aging. *These variations evidently make the detection difficult, thus, the path delay shifts caused by aging effects in recovered ICs must be separated from those caused by process variations in fresh ICs if we are to use path-delay fingerprints to identify recovered ICs.*

III. Path-Delay Fingerprinting Considering Aging

Figure 4 shows our flow for identifying recovered ICs using path-delay fingerprints and statistical analysis. The proposed flow is divided into three major steps. First, paths are simulated and selected according to their aging rate. Next, the delay information of these paths are measured by a clock sweeping technique in fresh ICs (either during manufacturing test on all ICs or during authentication on a sample of fresh ICs) and in any available CUAs. Finally, statistical analysis is used to decide whether the CUAs are recovered ICs or not.

• **Step 1. Path Selection:** Due to the large number of critical and long paths in a circuit, in this step, we select paths which age at faster rates by analyzing the gate types in different paths and simulating the circuit with different workloads. Paths with higher rates of aging are preferred for fingerprint generation, since the differences in the delay of those paths between recovered ICs and fresh ICs will be much larger than the differences in paths which degrade slower. Fingerprints generated by fast-aging paths could help identify recovered ICs used for a shorter time. However, there are several parameters impacting the aging rate of a path, including

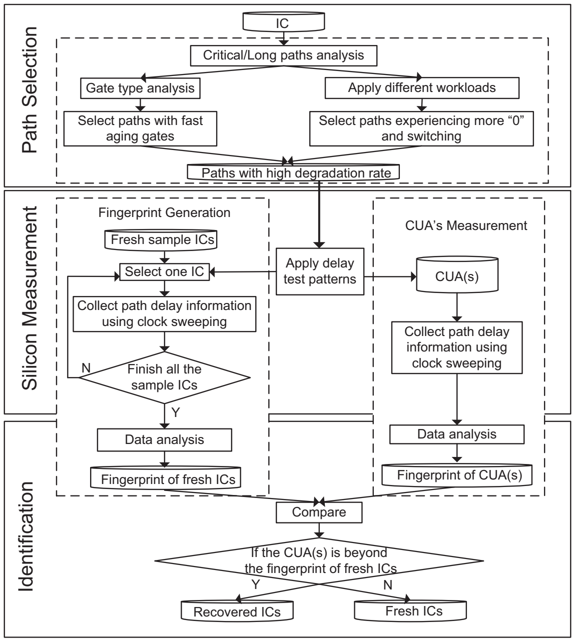

Path Selection
IC
Critical/Long paths analysis
Gate type analysis
Apply different workloads
Select paths with fast aging gates
Select paths experiencing more "0" and switching
Paths with high degradation rate
Silicon Measurement
Fingerprint Generation
Fresh sample ICs
Select one IC
Apply delay test patterns
CUA's Measurement
CUA(s)
Collect path delay information using clock sweeping
Collect path delay information using clock sweeping
N
Finish all the sample ICs
Y
Identification
Data analysis
Data analysis
Fingerprint of fresh ICs
Fingerprint of CUA(s)
Compare
If the CUA(s) is beyond the fingerprint of fresh ICs
Y
N
Recovered ICs
Fresh ICs

Fig. 4. Recovered IC identification flow.

the type of gates composing the path and the workload. Based on these parameters, and the observations made from simulation shown in Figure 1, we propose the following rules to select fast-aging paths: (i) paths with more fast-aging gates, such as NOR or XOR gates, will be selected, and (ii) paths that experience more zeros and more switching activity will be selected. More zeros in the path will increase the effect of NBTI on the PMOS transistors, and a high switching frequency will increase the HCI effects on gates, increasing the path delay degradation more significantly.

Paths with more fast-aging gates would be identified by analyzing the type of gates composing the paths. However, it is very difficult to identify paths that experience more zeros and more switching activity without knowing the specific workload. Therefore, in this work, different workloads (input combinations) are applied to ICs' primary inputs during logic simulation. For each gate on a critical path, the average switching activity and the zeros it has experienced are calculated. Paths with more switching activity and zeros are then selected using our flow. These paths, along with those composed of the more fast-aging gates, are used to generate fingerprints to identify recovered ICs. The number of selected paths could be adjusted according to the design and its testing procedure. In our simulation, we select the top 50 paths with fast-aging gates and the top 50 paths experiencing more switching activity and zeros in the benchmark circuit.

• **Step 2. Silicon Measurement:** The second step in Figure 4 is to collect the selected paths' delay from the ICs. Note that the fingerprint generation can be done during manufacturing test of a large sample of ICs before shipping them to the market or on a number of fresh ICs from each production kept by the design house for the purpose of authentication or recovered ICs identification. The larger the size of sample is, the wider of a range of process variations will be included in the fingerprint, reducing the probability that we identify fresh ICs with large process variations as recovered ICs. Path delay information from the fresh ICs is measured by performing test procedures on the ICs. Traditionally, test patterns are generated by ATPG before fabrication to detect path and transition delay faults. These patterns will be applied to all fresh ICs using clock sweeping techniques [14] to measure the path delay of the targeted paths. Note that using clock sweeping is a common practice in industry for speed binning of ICs [14].

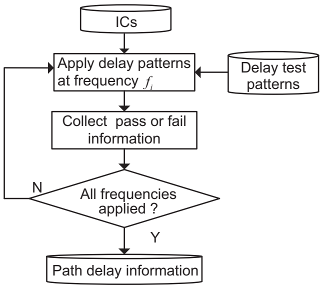

ICs
Apply delay patterns at frequency f_i
Delay test patterns
Collect pass or fail information
N
All frequencies applied ?
Y
Path delay information

Fig. 5. Clock sweeping flow.

Figure 5 shows the flow of the clock sweeping technique. The delay test patterns are applied to ICs at different clock frequencies (f_1, f_2, ... f_n). Under different frequencies, the paths could pass or fail. If the time period t_i of the frequency f_i ($t_i = \frac{1}{f_i}$) is larger than the path delay, the path will pass. Otherwise, the path will fail. When a path fails, the largest passing frequency will determine the path delay. The frequency step size ($\Delta f = f_i - f_{i-1}$), which depends on the tester, will determine the accuracy of path delay measurement results of silicon chips. For example, with the Ocelot ZFP tester [16], the main frequency is 400MHz and the frequency step size is 1MHz. In our simulation, a 5MHz step size around 1.0GHz circuit frequency is used for the clock sweeping technique. The measurement environment should keep the temperature as stable as possible, which can be controlled by the manufacturing test environment.

• **Step 3. Identification:** Once the path delay in all sample chips are measured, statistical data analysis will be used to generate a fingerprint for fresh ICs. The more the sample chips are, the more process variations will be covered, reducing the probability that fresh ICs with large process variations are identified as recovered ICs. For a circuit under authentication (CUA) taken from the market, the same test patterns will be applied in a near-identical environment. The path delay information of the CUA will be processed by the same statistical data analysis methods. In a simple analysis, if the fingerprint of the CUA is outside of the range of the fresh ICs' fingerprint, there is a high probability that the CUA is a recovered IC. Otherwise, the CUA is likely a fresh IC. The longer the CUA has been used, the more aging effects it will have experienced, making it easier to identify.

Without extra hardware circuitry embedded into the ICs, our recovered IC identification technique imposes no area or power overhead. It provides a negligible test time overhead during manufacturing test on a sample of ICs, since only a few patterns must be applied several times at different frequencies. Also, there is no change in the current IC design and test flow since there is no additional circuitry in the IC used for detection. In addition, this method is resilient to tampering attacks. It is inherently difficult for recyclers to mask the impact of aging on the recovered ICs' path-delay fingerprints during the recycling process. The only disadvantage of this technique is that the design must be known to get the path delay information.

IV. Statistical Data Analysis

Two statistical data analysis methods are used in this paper: simple outlier analysis (SOA), and principal component analysis (P-

CA) [17]. When performing SOA, we randomly select a single path from the selected path set, and use its delay range in fresh ICs to generate a fingerprint. The process variations of the CUA may or may not be the same as those within the sample ICs. The selected path delay of the CUA and sample ICs will follow the same distribution, which makes SOA effective in certain conditions. However, a single-path based analysis will not be very effective, due to the limited aging information collected. In general, this method is expected to be effective in distinguishing recovered ICs used for a long time from fresh ICs with small process variations, as demonstrated by our results in Section V.

As mentioned in Section I, using PCA has already been effectively used for detection of hardware Trojans [6]. In this work, in order to improve the effectiveness of our technique, we also use PCA to separate the aging effects on path delay from process variations. The path delay information of all selected paths, which have been measured by clock sweeping, will be processed by PCA. In our simulations, the top 100 paths with faster aging rates were selected to generate fingerprints. The delay of each path is one of the variables for PCA to use. Therefore, with N ICs, the dimension of the data set for PCA to generate fingerprint is N*100. The first three components of PCA in all fresh ICs were plotted, and a convex hull was created as the fingerprint for fresh chips. The path delay information of the CUA was also analyzed by the same process and plotted in the same figure. If the CUA is outside of the convex created by the fresh ICs, there is a high probability that the CUA is a recovered IC.

V. Results and Analysis

In order to verify the effectiveness of our recovered IC identification flow and data analysis methods, we implemented it using 45nm technology on a few benchmarks. HSPICE MOSRA [8] is used to simulate the effects of aging on the path delay of different benchmarks. The supply voltage of the 45nm technology is 1.1V. Random workloads (random functional input patterns) were applied to several ISCAS'89 benchmarks. Path delay information was collected using clock sweeping at different aging times. Different process and temperature variations were also simulated to analyze their impact on the effectiveness of our recovered IC identification method.

A. Process and Temperature Variations Analysis

Table I shows the three process variations rates we used in our simulations. Moving from PV0 to PV2, inter-die and intra-die variations both become larger. PV1 represents a realistic rate of process variations that a foundry might have. Four sets of Monte Carlo simulation (MCS) were run using different levels of variations, as shown in Table II. For each set of MCS, 300 Monte Carlo simulations were run to generate 300 chips. During the simulations, the aging effects of NBTI and HCI were simulated with random stress for the benchmark s38417. From the top 500 paths, the paths P_1, P_2,..., P_{50} with fast-aging gates and the paths $P_{51}, P_{52}, ..., P_{100}$ with more zeros and higher switching activities were selected to generate fingerprints as described in Section III.

Analysis using SOA: First, 300 Monte Carlo simulations were run in MCS1. The maximum aging time is 2 years. Here, SOA was used to process the path delay information. 3 paths (P_1, P_2, and P_{51}) were selected to show the results of SOA. Figures 6(a), 6(b), and 6(c) show the path delay distribution of the 3 paths from 300 ICs used for different aging times. Similar results were obtained for the other 97 paths as well. For each path, the range of the path delay at AT='0' is the fingerprint of the fresh ICs. If the path delay of the CUA is out of that range, there is a high probability that IC is a recovered one. Note the 300 different Monte Carlo simulations are used for recovered ICs from those used as sample fresh ICs. From these figures, we can see that the delay distribution of each path in recovered ICs shifts to the right, relative to the distribution of delays in fresh ICs. This is because path delay in recovered ICs increases due to aging. The longer the ICs have been used, the more path delay degradation they will have experienced. In addition, we see that the path delay variation increases as the aging time increases. The reason for this is that ICs with different process variations age at different speeds, and the path delay variations become larger as we increase the aging time.

TABLE I
Process variation rates.

	Inter-die (3σ)			Intra-die (3σ)		
	V_{th}	L	T_{ox}	V_{th}	L	T_{ox}
PV0	3%	3%	2%	2%	2%	1%
PV1	5%	5%	2%	5%	5%	1%
PV2	8%	8%	2%	7%	7%	2%

TABLE II
Simulation setup.

Experiments	Process Variations	Temperature
MCS1	PV0	25°C
MCS2	PV1	25°C
MCS3	PV2	25°C
MCS4	PV1	25°C ±10°C

Figure 6(a) shows the distribution of path P_1's delay, and we can see that the smallest delay of P_1 in recovered ICs used for 1 month is smaller than the largest delay in fresh ICs. Therefore, the detection rate of recovered ICs used for 1 month is less than 100% (98.3%) when we use the fingerprint generated by SOA from path P_1. However, the detection rate of recovered ICs used for 3 months or longer is 100%, which demonstrates that it is easier to detect recovered ICs that have been used for longer amounts of time. If we choose path P_2 to detect recovered ICs, the detection rate of ICs used for 1 month (95.7%) is slightly less than when using path P_1. However, if path P_{51} is used, which has the fastest aging rate among the 100 paths, the detection rate is 100% even if the ICs are only used for one month. P_{51} is the most effective path for identifying recovered ICs in this benchmark. From the above analysis, we can see that different paths generate different fingerprints due to their different aging speeds, which makes SOA slightly less effective.

Figures 7(a) and 7(b) show the delay distribution of path P_{51} across 300 Monte Carlo simulations in MCS2 and MCS3. Overall, Figures 6(c), 7(a), and 7(b) present the delay distribution of the same path (P_{51}) in ICs with different process variations. By comparing these figures, we can see that the larger the process variations are, the larger the path delay variations in fresh ICs will be, which makes it more difficult to detect recovered ICs. Even when using the most effective path P_{51}, the detection rates of ICs used for 1 month with PV1 and PV2 drop from 100% with PV0 to 78.0% and 50.7%, respectively. A 100% detection rate could be achieved if the ICs were used for 1 year or longer with PV1, or longer than 2 years with PV2.

300 Monte Carlo simulations were also run with ±10°C temperature variation during the aging process in MCS4 as shown in

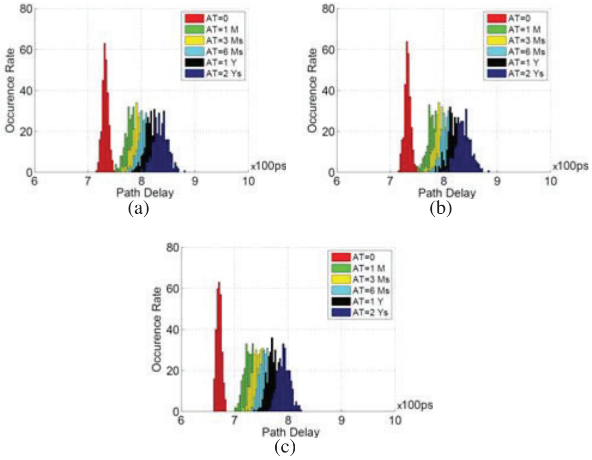


Fig. 6. Path delay distribution in ICs with PV0 in MCS1 at different aging times (a) Path P_1, (b) Path P_2, and (c) Path P_{51}.

Figure 7(c). The measurement temperature is 25°C. It shows the delay distribution of path P_{51} and the detection rate of ICs used for 1 month using it is 67.7%. Comparing Figure 7(c) and Figure 7(a), we can see that the larger the temperature variation is, the larger the path delay variation is, which makes it more difficult to detect recovered ICs.

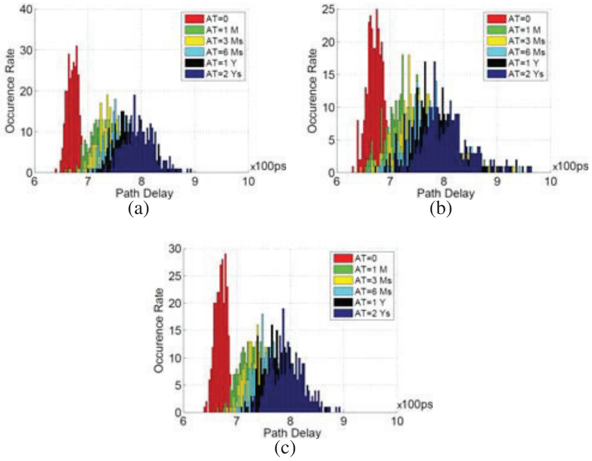


Fig. 7. Path P_{51} delay distribution in ICs at different aging times (a) in MCS2, (b) in MCS3, and (c) in MCS4.

Analysis using PCA: A similar analysis is done using PCA for different MCSs. Figure 8(a) shows the PCA results of the 100 paths in s38417 with 300 chips in MCS1. FC denotes the first component from PCA, SC represents the second component, TC is the third component, and DR denotes the detection rate. The convex is built up from fresh IC data, and represents the fingerprint for fresh ICs. The red asterisks represent chips used for 1 month. From the figure, we can see that the 300 used ICs were completely separated from the signature of the fresh ICs. Thus, the detection rate using path delay fingerprints generated by PCA is 100% for recovered ICs used for 1 month. For recovered ICs used for a longer time, the detection rate will obviously be 100% as well.

The path delay information from the remaining three sets of MCSs were also analyzed by PCA. Figure 8(b) shows the analysis results of fresh chips and recovered ICs used for 1 month in MCS2. From the 3-dimensional figure, we can see that some of the recovered ICs are close to the fresh ICs' fingerprint. The detection rate is 96.3%, which is much higher than using SOA. Comparing Figure 8(b) and Figure 8(a), we can see that (i) the convex hull built up from fresh ICs in MCS2 is much larger than that in MCS1 (note that the convex hull in MCS1 looks larger than MCS2 due to its small scale of axes), and (ii) the recovered ICs in MCS2 are closer to fresh ICs than those in MCS1, which makes the detection rate in MCS2 less than that in MCS1. The path delay information of 300 ICs used for 3 months in MCS2 were also processed, and the results are shown in Figure 8(c). Comparing Figures 8(b) and 8(c), we can see that the longer the chips have been used, the farther they will be from the fresh ICs' fingerprint. The detection rate of recovered ICs used for 3 months or longer with PV1 at 25°C is 100%.

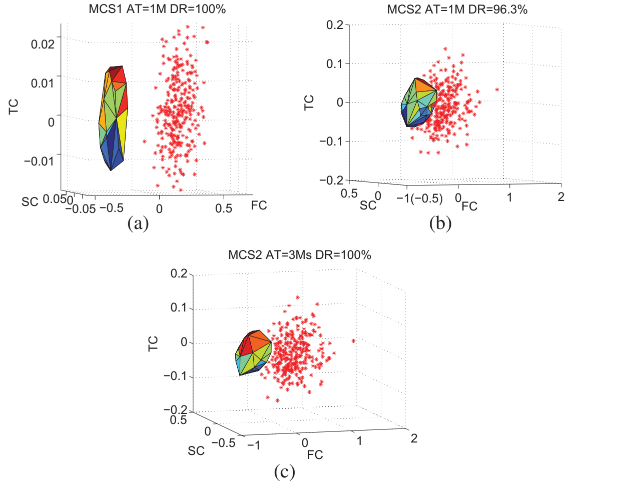


Fig. 8. PCA results of ICs under 25°C (a) used for 1 month with PV0 in MCS1, (b) used for 1 month with PV1 in MCS2, and (c) used for 3 months with PV1 in MCS2.

Figure 9 shows the PCA results of ICs in MCS3. The detection rate of recovered ICs used for 1 month, 3 months, 6 months, and 1 year are 72.7%, 89.3%, 99.3%, and 100%, respectively. The figures of PCA results of recovered ICs used for 1 month and 3 months are not shown here since the detection rates are so far from 100%. Figures 9(a) and 9(b) show the fresh ICs' fingerprint and the recovered ICs used for 6 months and 1 year, respectively. The recovered ICs used for longer times are easier to detect, as seen by comparing Figures 9(a) and 9(b). Comparing the detection rates in these simulations, we can see that it is more difficult to detect recovered ICs which have higher levels of process variations. The 99.3% detection rate of ICs used for 6 months and the 100% detection rate of ICs used for 1 year in MCS3 shows the effectiveness of our technique. We acknowledge that PV2 is an extremely high variation compared to what is expected in practice (e.g., PV1).

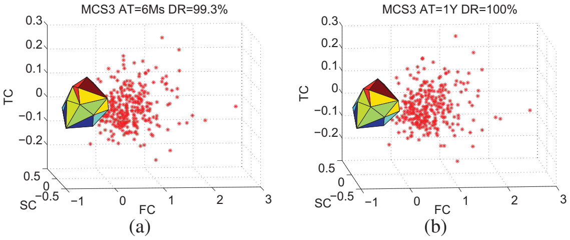


Fig. 9. PCA results of ICs with PV2 under 25°C in MCS3 used for (a) 6 months and (b) 1 year.

TABLE III

RECOVERED IC DETECTION RATES FOR S38417.

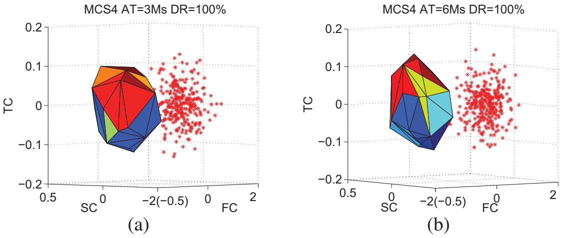
	SOA				PCA			
	1M	3M	6M	1Y	1M	3M	6M	1Y
MCS1	100%	100%	100%	100%	100%	100%	100%	100%
MCS2	78%	96.7%	99.7%	100%	96.3%	100%	100%	100%
MCS3	50.7%	76.3%	85.3%	95.6%	72.7%	89.3%	99.3%	100%
MCS4	67.7%	93.3%	98%	100%	90.6%	100%	100%	100%

TABLE IV

RECOVERED IC DETETION RATES - BENCHMARK COMPARISON UNDER MCS4 USING PCA.

Benchmark	1M	3M	6M	1Y
s9234	88%	100%	100%	100%
s13207	89.6%	100%	100%	100%
s38417	90.6%	100%	100%	100%

With the same measurement temperature 25°C, ±10°C temperature variation is used in MCS4 during the aging process. The detection rate of ICs used for 1 month, 3 months, and 6 months in MCS4 are 90.6%, 100%, and 100%, respectively. The fresh ICs' fingerprint and the detected recovered ICs used for 3 months and 6 months are shown in Figure 10. Comparing Figure 10(a) with Figure 8(c), we can see that the recovered ICs used for 3 months in MCS4 are closer to the fingerprint than recovered ICs used for 3 months in MCS2. This phenomenon demonstrates that temperature variations could increase the path delay variations in fresh ICs and make it more difficult to detect recovered ICs. However, the 100% detection rates of ICs used for 6 months in MCS4 demonstrates the effectiveness of our method with process and temperature variations.



(a) (b)

Fig. 10. PCA results of ICs with PV1 and ±10°C temperature variations in MCS4 used (a) 3 months, and (b) 6 months.

Figures 7 through 10 presented some detailed results relating to using this technique on s38417 with SOA and PCA. Table III, however, tabulates these results in addition to some other results obtained using both statistical analysis approaches. These results clearly demonstrate that PCA is more effective than SOA when it comes to identifying ICs used for shorter periods of time.

B. Benchmark Analysis

In addition to s38417, the ISCAS'89 benchmarks s9234 and s13027 were also simulated to demonstrate the efficiency of this technique on different designs. The process variation and temperature variation rates used in MCS4 were applied to these two benchmarks. The aging stress causing NBTI and HCI degradation in these benchmarks comes from random workloads. 300 MCS were run for each benchmark for a maximum 2 years of aging. The path selection method was also applied to these benchmarks, and 100 paths from each benchmark were used to run statistical data analysis using PCA.

Table IV shows the recovered IC detection rate for all three benchmarks under MCS4 for up to a year of aging. The detection rate for ICs used for 3 months in the benchmarks s9234 and s13207 is 100%, which matches the results obtained from s38417.

The results shown in this section clearly demonstrate that our recovered IC detection method using a path delay fingerprint generated by PCA is very effective, even in designs with large process and temperature variations.

VI. ACKNOWLEDGEMENT

This work was supported in part by the National Science Foundation (NSF) under grant CNS 0844995.

VII. CONCLUSION AND FUTURE WORK

We have presented a recovered IC identification method using path-delay fingerprinting in this paper. The path delay signatures from recovered ICs will be different from those from fresh ICs due to aging. With no additional hardware circuitry required, this method provides no overhead on area and power consumption. The simulation results of different benchmarks with different process and temperature variations demonstrated the effectiveness of our method. Our future work includes (i) implementation of this technique on FPGAs, (ii) implementation on designs with various clock gating and power switching techniques impacting the workload, and (iii) further improvement of detection rates for chips used for very short periods of time.

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* , Jan. 2010.
[2] Military Times, "Officials: Fake Electronics Ticking Time Bombs," *http://www.militarytimes.com/news/2011/11/ap-fake-electronics-ticking-time-bomb-1 10811/*, 2011.
[3] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," *Proceedings ISSCC 2000*, Feb. 2000.
[4] R. Pappu, "Physical one-way functions," *Phd thesis, Massachusets Instutute of Tecnhology*, 2001.
[5] X. Zhang, N. Tuzzio, and M. Tehranipoor , "Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor," in Proc. *Design Automation Conf. (DAC)*, 2012.
[6] Y. Jin, and Y. Makris, "Hardware Trojan Detection Using Path Delay Fingerprint," in Proc. *IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST)*, 2008.
[7] *http://www.nangate.com/?page_id=22*.
[8] *Synopsys, HSPICE user guide, 2010*.
[9] E. Ozturk, G. Hammouri, and B. Sunar, "Physical Unclonable Function with Tristate Buffers," in *Proc. ISCAS08*, pp. 3194-3197, 2008.
[10] F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual Property Metering, in *Proc. 4th Intl Workshop Information Hiding*, pp. 81-95, 2001.
[11] Y. Alkabani and F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security, *Proc. 16th USENIX Security Symp.*, Usenix Assoc., pp. 291-306, 2007.
[12] 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," *TED,* vol. 53, no. 7, pp. 1583-1592, July 2006.
[13] K. Uwasawa, T. Yamamoto, and T. Mogami, "A new degradation mode of scaled p+ polysilicon gate p-MOSFETs induced by bias temperature instability," in *IEDM Tech. Dig.*, 1995, pp. 871874.
[14] J. Lee, I. Park, and J. McCluskey "Error Sequency Analysis," *Proc. VLSI Test Symp.*, 2008
[15] 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, Dec. 1988.
[16] INOVYS, *http://www.etesters.com/listing/40e8f648-a2d6-23b8-949b-4b3c00 5c86fb/Ocelot_ZFP_-_Test_System_for_Complex_SOCs*.
[17] I. T. Jolliffe, "Principal Component Analysis (2ed Edition)," Springer, pp. 150-165, 2002.