Can EDA Combat the Rise of Electronic Counterfeiting?

Farinaz Koushanfar
Rice University,
Houston, TX

Saverio Fazzari
Booz Allen Hamilton, Inc.,
Arlington, VA

Carl McCants
Defense Advanced Research
Projects Agency, Arlington, VA

William Bryson
Analytical Solutions, Inc.,
Albuquerque, NM

Matthew Sale
U.S. Naval Surface Warfare
Center, Crane, IN

Peilin Song
IBM Research,
Yorktown Heights, NY

Miodrag Potkonjak
University of California,
Los Angeles, CA

ABSTRACT

The Semiconductor Industry Associates (SIA) estimates that counterfeiting costs the US semiconductor companies $7.5B in lost revenue, and this is indeed a growing global problem. Repackaging the old ICs, selling the failed test parts, as well as gray marketing, are the most dominant counterfeiting practices. Can technology do a better job than lawyers? What are the technical challenges to be addressed? What EDA technologies will work: embedding IP protection measures in the design phase, developing rapid post- silicon certification, or counterfeit detection tools and methods?

Categories and Subject Descriptors

B.7 [**Hardware**]: Integrated Circuits

General Terms

Design, Security

Keywords

Counterfeiting; Reliability; Device and IC aging

1. INTRODUCTION

A counterfeit (fake) product is an illegal forgery or imitation of an original design. The counterfeit parts intend to fraudulently deceive consumers by pretending to be genuine. A 2008 report by the US department of commerce estimated counterfeiting to account for about 8% of the global merchandize trade, equivalent to lost sales of as much as 600B in 2008, and expected to grow to 1.2T in 2009 [30]. Counterfeiting of microelectronics components, embedded systems, and computer peripherals is a common practice in many parts of the world.

Estimates for IC counterfeiting losses vary greatly depending on the source. One of the lowest estimates is provided by SIA at $7.5 B. Very recently, EE Times estimated that IC counterfeiting losses are as high as $ 169 B annually. Therefore, the fake parts are at least 2.5% of the annual IC sales and are significantly larger than the overall EDA revenues per year. Sources of fake products are diverse, ranging from re-labeling and using defective components to illegal overbuilding by manufacturers. Conventional chip identification methods such as printing serial numbers and burning fuses can be forged and thus, they have a limited effectiveness in preventing or detecting counterfeit chips.

Counterfeiting is a particularly important problem to address since it has at least four important ramifications: (i) the original IC part providers incur an irrecoverable loss due to the sale of often cheaper counterfeit components, (ii) low performance of counterfeit products (that are often of lower quality and/or cheaper older generations of a chip family) affects the overall efficacy of the integrated systems that unintentionally use them; this could in turn harm the reputation of authentic providers, (iii) unreliability of fake devices could render the integrated systems that unknowingly use the parts unreliable; this potentially affects the performance of weapons, airplanes, cars or other crucial applications that use the fake components [36], and (iv) untrusted fake components may have intentional malware or some backdoors for spying information or remotely controlling critical objects.

The rising trends in chip counterfeiting and its important consequences clearly motivate the urgent need for development of advanced IC anti-counterfeiting techniques. In this paper, we discuss the present state of IC anti-counterfeiting practice and research, technical challenges, and some potential EDA research and development directions for addressing the open problems.

2. PRESENT ANTI-COUNTERFEITING PRACTICES AND EFFORTS

Fake electronic parts have been a known issue since the early days of IC design and fabrication. The IC companies and government organizations have been aware of the occasional counterfeit incidents. Therefore, a preliminary set of guidelines and legal procedures are typically in place for handling the counterfeit subjects. The increasing growth of the number of counterfeit parts and the ascending potential risk of exploits have recently raised the awareness of this prevalent problem. In November 2011, the US Senate Armed

DAC 2012, June 3-7, 2012, San Francisco, California, USA.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Can EDA Combat The Rise Of Electronic Counterfeiting?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Advanced Research Projects Agency,Arlington,VA,Arlington**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at 49thThe Design Automation Conference (DACDAC 2012, June 3-7, 2012, San Francisco, California, 1/20

14. ABSTRACT
The Semiconductor Industry Associates (SIA) estimates that counterfeiting costs the US semiconductor companies $7.5B in lost revenue, and this is indeed a growing global problem. Repackaging the old ICs, selling the failed test parts, as well as gray marketing, are the most dominant counterfeiting practices. Can technology do a better job than lawyers? What are the technical challenges to be addressed? What EDA technologies will work: embedding IP protection measures in the design phase, developing rapid post-silicon certification, or counterfeit detection tools and methods?

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

Services Committee held a hearing to address the growing issue of counterfeit parts in the U.S. military supply chain. Senator John McCain of Arizona, the committeeŠs ranking Republican, and Senator Carl Levin of Michigan, committee chairman, were among the officials who investigated defense contractors about the rising number of detected counterfeits in the supply chain. The two senators have used the 2012 Defense Authorization Act to alter acquisition guidelines and make contractors responsible for the expenses of replacing the fake components.

Until now, only a handful of industrial/research labs, and government/military agencies and contractors have a set of more technical procedures for electronic counterfeit prevention and detection, which are often classified. In the remainder of this section, we briefly summarize four major industrial, research lab, government and defense agencies' anti-counterfeiting approaches and initiatives.

The Navy lab defines counterfeit parts in two broad categories: New parts that are misrepresented and old parts that are sold as new. One can envision testability and integrated identification methods and quantify them in terms of practicality, cost, and accessibility beyond factory production tests. The key challenge is to develop methods for at-speed functional test and parametric characterization available and easily implementable for non-factory test screeners as well as methods for better detecting aging and other usage/improper handling induced stresses in parts. One can point out that these challenges exist for digital, mixed-signal, and analog parts. It is important to identify perils from a security point of view of allowing the end user greater insight into the IC through testability.

A different path is taken by Analytical Solutions, Inc., an independent company which provides analyses of complex electronic devices related to commercial, military, medical, security, and space applications [38]. The company offers a "Five Tier Approach" to counterfeit detection to meet the specific needs of the customer, summarized in Table 1. This "Five Tier Approach" gives customers the options that may be required to evaluate and validate that the electronic part or device is not a counterfeit product and provide users the trust they need in the production or manufacturing of high reliability products.

Researchers at IBM have developed a new technique for detecting chip alterations using intrinsic light emission in combination with electrical tests. This method is based on the fact that any active device emits infrared light emission when it is powered on or operational. High sensitivity photon detectors can be employed to capture the weak emission while the chip under evaluation is powered on and electric stimuli are applied to it. In particular, two main families of electrical test modes, static and dynamic, can be applied. It has been demonstrated that combining the optical diagnostics and electrical tests significantly increases the delectability of the malicious circuits. The optical tool of choice that is used for this method is Picosecond Imaging Circuit Analysis (PICA), originally developed for diagnosing time-critical IC failures. This tool can measure time-resolved emission from switching gates, as well as time-integrated and time-resolved from gates in fixed logic state, also known as Light Emission from Off-State Leakage Current (LEOSLC). The approach resulted in many positive results, including high spatial resolution image processing and data interpretation.

IC anti-counterfeiting has been well recognized by DARPA as a strategically important and a necessary technology. For example, the original active hardware metering for IC piracy prevention and anti-counterfeiting was supported by a DARPA/MTO program [1]. As another example, the objectives of the ongoing DARPA/MTO Integrity and Reliability of Integrated Circuits (IRIS) program is to develop the technology to derive the functionality of an IC to determine unambiguously if malicious modifications have been made to that IC, and to accurately determine the IC's useful lifespan and reliability from a physical perspective [39]. While the IRIS program is still in an early phase, it is expected to provide new research results and advance the state-of-the-art of IC trust and anti-counterfeiting techniques.

3. RESEARCH CHALLENGES

Development of newer and more efficient IC anti-counterfeiting techniques is exceedingly interesting from scientific and engineering viewpoints. There are a number of challenging tasks that require not just implementation, design, algorithmic, and modeling innovations, but also conceptual breakthroughs that may greatly benefit future generations of ICs. This difficulty and richness is a consequence of the confluence of several technological, security, and design aspects, including:

- *Ultra large scale of integration.* Modern and future chips have a surprising number of subcomponents, in the order of billions. Failure or performance degradation of each subcomponent may result in an overall system failure. Although the need to simultaneously consider so many components is a nontrivial challenge, it may in some situations facilitate counterfeiting detection. For example, to show that a chip was already significantly used, it suffices to verify that any part of the chip was considerably used.

- *Limited controllability and observability.* It is well known that the ratio of the number of transistors vs. the number of inputs/outputs has been continuously increasing over time. For example, this ratio was around a hundred for the first generations of processors, while it is more than a million for contemporary processors. Thus, it is increasingly more difficult to organize any type of testing in modern ICs.

- *Identification and accessing System-on-a-Chip (SoC) subcomponents.* In case a complex SoC with multiple subcomponents is being investigated, typically optical investigations are needed for identifying and accessing the subparts to be individually tested. Most modern SoC designs are packaged using flip chip technology and a heat spreader which have to be removed for optical evaluations. There is a need to develop more advanced optical methods that not only identify the IP subparts, but also can classify the type of IP (e.g., RF front-end, A2D, memory, etc.) and find the test ports and scan chains to each subcomponent in an automated manner.

- *Functional identification and reverse engineering.* The effective lifetime of an airplane or a tank may span over several decades, while the average lifespan of the underlying electronic components is typically much

Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
External Visual Inspection	External Visual Inspection	External Visual Inspection		
Configuration Marking Permanency	Configuration Marking Permanency	Configuration Marking Permanency		
Lead Finish ID	Lead Finish ID	Lead Finish ID	Construction and Comparative Analysis	Die Analysis and Comparison "Trusted IC"
	X-Ray	X-Ray		
	CSAM	CSAM		
		Electrical Test		
		Internal Visual Inspection		

Table 1: "Five Tier Approach" to counterfeit detection from Analytical Solutions.

shorter. Therefore, to maintain the costly equipment or automotive/avionic systems, failed electronics must be replaced. A standing problem is the lack of sufficient documentation/description of the failed components. This may be because of the long supply chains, or part obsoleteness. In lieu of this information, one must reverse-engineer the target failed component using other working instances. Development of automated methods and tools for functional identification and IC reverse engineering is a major research challenge.

- *Interdisciplinary nature of problems.* Anti-counterfeiting requires knowledge and skills in several domains including IC technology, design, EDA, testing, security, statistical analysis, and game theory. Hence, continuous educational efforts are needed.
- *Variety of (unpredictable) attacks.* It is often not easy to develop sound, comprehensive, and practical defenses against known attacks. The situation becomes much more challenging when the attacks are difficult to predict.
- *Process variation and device aging.* Although the security aspects are obviously the most challenging and difficult to address, recent history teaches us that process variation and device aging models are critical for effective research and studies. On one side, they enable development of conceptually new security mechanisms such as physical unclonable functions (PUFs). On the other hand, they also directly invalidate numerous hardware security approaches that assume unform temporal and spacial characteristics of similar elements across one chip. Luckily, in terms of developing new anti-counterfeiting techniques, such imperfections can be essential and positive.

Furthermore, there is a large spectrum of IC counterfeiting and anti-counterfeiting problems. They are related to issues relevant to contracts between an IC seller and buyer and fulfillment of all contractual agreements, including ones that may not be explicitly stated. Currently popular exploits include reselling old ICs, selling lower performance chips as a higher performance model, and selling untested or defective ICs [30].

4. RELATED WORK

In this Section, we briefly summarize the related concepts which directly influence the research and development of advanced IC anti-counterfeiting methods. A closely related line of research is focused on detection of IC Trojans; such methods are exceptionally relevant when the counterfeit components introduce an exploit in the system. Due to space constraints, we do not discuss Trojan detection and prevention in this paper. Instead, we refer the interested readers to a comprehensive survey on this topic [28].

4.1 IP Watermarking

A watermark embeds a hidden signature in the chip at the design time [3, 29]. The signature is checked against its intended attributes for authenticity verification. Watermarking at different levels of design abstraction is useful and necessary, in particular for designs with multiple IPs where the IP infringement tracking is a challenging task. A watermark can identify a design, and not individual IC instances. It can become useful for tracking stolen design IPs in the supply chain.

4.2 Hardware Metering and Auditing

IC metering or hardware metering refers to tools, methodologies, and protocols that enable post-fabrication tracking of the ICs. Metering can differentiate legitimate hardware from pirated ones. Research efforts have been focused on how to generate a unique ID for a specific device. Hardware metering may be *passive*, or *active*. In passive metering, the ICs are specifically identified, either in terms of their functionality, or by other forms of unique identification [4]. The identified ICs may be matched against their record in a pre-formed database that could reveal unregistered ICs or overbuilt ICs (in case of collisions). In active metering, not only the ICs are uniquely identified, but also parts of the chipŠs functionality can be only accessed, locked (disabled), or unlocked (enabled) by the designer and/or IP rights owners using a high level knowledge of the design not transferred to the foundry [1].

Metering methods may also be classified as *intrinsic* or *extrinsic*: (i) Intrinsic hardware metering leverages process variation to create unique fingerprints by using the existing properties or side channels of the device, such as delay and power. Several approaches have been proposed to characterize the gate-level IC properties for hardware metering pur-

pose [5][6][7][8]. Intrinsic metering methods are inherently passive. (ii) Extrinsic hardware metering inserts additional hardware or software components to the device for ID generation [2][4]. The additional components can be configured to produce a unique, difficult to predict or clone fingerprint for each authentic device. Extrinsic metering methods may be passive or active.

There is a natural way to establish a connection between hardware metering and IC anti-counterfeiting techniques. The simple but powerful observation is that once a chip is identified by hardware metering techniques, then the foundry or other reliable sources can be contacted for obtaining more information about the IC such as the manufacturing date and the original buyer.

4.3 Physical Unclonable Functions (PUFs)

Physical unclonable functions (PUFs) are one potential candidate stricture for implementing the unique extrinsic IC identifiers. A PUF is a physical function that provides a mapping between its inputs and outputs based on the unique fluctuations in the unclonable device material properties such as timing or current. The PUF input vector is typically called a *challenge* and the PUF output vector is commonly called a *response*. To ensure security, the mapping should be such that responses can be rapidly evaluated, but they are hard to model, characterize, clone, or reproduce. PUFs have been proposed for both ASIC and FPGAs [22, 23, 26, 37, 27]. Comprehensive summaries and more detailed definition/classification of PUFs can be found in [31, 32]. Very little is known about industrial practices of authentic chip identification. An approach by Sun Microsystems was proposed where they use the unique EM radiation from each chip to establish its authenticity [24].

4.4 Device Aging Models

Natural phenomena such as negative bias temperature instability (NBTI) cause the aging of devices in form of threshold voltage increase. As a result, the IC structural properties such as delay and power would be impacted significantly, which cause degradation in the device lifetime. In order to evaluate and predict the increase of threshold voltages and, consequently the failure time, several quantitative models have been proposed. The time dependence of V_{th} shift follows fractional power law of the stress time [9], as shown in the following equation:

$$\Delta V_{th} = A \cdot exp(\beta V_G) \cdot exp(-E_\alpha / kT) \cdot t^{0.25} \qquad (1)$$

where V_G is the applied gate voltage; A and β are constants; E_α is the measured activation energy of the NBTI process; T is the temperature; and t is the stress time.

Due to the increase of threshold voltages, the aging process significantly impacts IC's structural properties. For example, the leakage energy of a logic gate exponentially decreases with the increase of threshold voltage, as indicated by the leakage current model [10]:

$$I_{leakage} = 2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot (\frac{kT}{q})^2 \cdot e^{\frac{\sigma \cdot V_{dd} - V_{th}}{n \cdot (kT/q)}} \qquad (2)$$

where L is effective channel length, V_{th} is threshold voltage, W is gate width, V_{dd} is supply voltage, n is subthreshold slope, μ is mobility, C_{ox} is oxide capacitance, ϕ_t is thermal voltage $\phi_t = kT/q$, and σ is drain induced barrier lowering (DIBL) factor.

On the other hand, delay of a logic gate increases in a close-to-linear manner with aging, as shown by the following delay model [10]:

$$Delay = \frac{k_{tp} \cdot k_{fit} \cdot L^2}{2 \cdot n \cdot \mu \cdot \phi_t^2} \cdot \frac{V_{dd}}{(ln(e^{\frac{(1+\sigma)V_{dd} - V_{th}}{2 \cdot n \cdot \phi_t}} + 1))^2} \cdot \frac{\gamma_i \cdot W_i + W_{i+1}}{W_i} \qquad (3)$$

where subscripts i and $i+1$ represent the the driver and load gates, respectively; γ is the ratio of gate parasitic to input capacitance; and k_{tp} and k_{fit} are fitting parameters.

4.5 Device Degradation

IC lifetime is influenced by a variety of phenomena that have been studied by the material science and semiconductor communities, including electromigration (EM) [11], stress migration (SM) [12], time dependent dielectric breakdown (TDDB) [13], thermal cycling (TC) [14], oxide breakdown [9], vertical interconnect access (VIA) [15][16], negative bias temperature instability (NBTI) [17], and hot-carrier injection (HCI) [18][19].

Electromigration is the transport of interconnect material (copper in modern designs) due to high density electric currents, i.e., movement of ions that alters the conductivity of an interconnect. The ramifications include physical disconnection of wires or failure of the overall IC to function correctly due to increase in wire delays. Closely related thermomigration has high impact on reliability of vias in particular in new technologies that do not use lead (Pb). Thermomigration moves metal material due to the underlying thermal gradient. Thermomigration is also related to stress migration where the difference in temperature creates thermo-mechanical stress due to different expansion rates of various materials in the IC.

Dielectric breakdown is a process where dielectric around wires develops cracks that drastically change its dielectric properties to the extent that it does not serve as an isolator anymore. Stress migration is a phenomenon where the metal atoms in the interconnects migrate due to mechanical stress, much like electromigration. Stress migration is caused by thermo-mechanical stresses which are caused by differing thermal expansion rates of different materials in the device. Thermal cycling is a phenomenon where the temperature of an IC or its parts is subject to high and rapid changes. It causes permanent damages that accumulate every time there is a cycle in the processor temperature, eventually leading to failures.

4.6 Aging Sensors

Accurate performance-degradation monitoring of CMOS circuits is one of the most critical issues for adaptive design techniques. Therefore, in addition to modeling and studies of aging, additional on-chip aging sensors can be implemented to monitor and report aging and reliability. Because of the increasing importance of this topic, various methods for realizing on-chip aging sensors have been recently proposed, including [33, 34, 35]: [33] proposed a technique to measure the beat frequency of two ring oscillators, one stressed and the other unstressed, to a very high delay sensing resolution for aging differentiation; [34] introduced two compact structures to digitally quantify the change in performance and power of devices undergoing NBTI and

defect-induced oxide breakdown. The small size of the sensors makes them amenable to use in a standard-cell design with low area and power overhead; [35] deployed a threshold voltage detector for monitoring the performance degradation of an aged MOSFET. Developing more sophisticated sensing methods with a higher resolution aging differentiation can directly advance the state-of-the-art anti-counterfeiting techniques. The relevant EDA research is to find the best placement of each sensor type on the chip to maximize age sensing coverage while minimizing the overall sensor overhead/cost.

4.7 System Failures

System failure has become a major concern in hardware-based system design, especially with the rapid growth in nanoscale technologies where power and temperature significantly increase due to the transistor scaling. Therefore, prediction and evaluation of system failure has drawn a great deal of attention from both industry and academic communities. Srinivasan et al. [20] introduced a reliability-aware microprocessor (RAMP) design model to predict and evaluate the mean time to failure resulting from different components of the system, such as applications, system architectures, and processor designs. They further extended the RAMP model to evaluate the system failure caused by technology scaling. In particular, estimates the mean times to failure (MTTF) of devices due to various aging phenomena can be found in [20].

5. IC ANTI-COUNTERFEITING TECHNIQUES: CASE STUDIES

Our goal in this section is to provide additional impetus for development of design automation techniques and tools for fighting counterfeiting techniques. While we do not discuss a detail presentation of any of the proposed techniques and do not show any security proofs, we believe that readers will find non-trivial IC counterfeiting ideas and starting points for the development of industrial-strength practical and fundamentally sound methods.

5.1 Techniques for Integrated Circuit Age Characterization

The threshold voltage of each CMOS transistor is a function of the number of dopants injected during manufacturing and the number of bonds that are broken during IC operation. The first component is subject to process variation and essentially follows an exponential distribution. The level of spatial correlation is exceedingly low to the extent that the threshold voltages of different transistors can be considered independent for any pair of transistors. The aging of PMOS transistors is due to chemical structure and is by an order of magnitude faster than the aging of their NMOS counterparts. There are three important observations. The first is that device aging is recoverable to a significant extent but not completely: when a transistor is not under stress or is only under stress for a small percentage of time, its threshold voltage reduces at an exponentially decreasing rate. The second is that a transistor ages when it is under stress, i.e., when its channel acts as an open switch. The third important piece of information is that although there are techniques for extraction of threshold voltage [8], such an extraction is a slow and expensive procedure unless it is restricted to a relatively few transistors.

A particularly important question is whether a chip is essentially new or has been used for a significant amount of time. If used, the distribution of threshold variations would be far from the expected foundry models. Noninvasive IC characterization methods can be used for determining the post-silicon distribution and correlations among the threshold voltages. Statistical outlier detection methods can determine if the measured distributions or correlations significantly deviate from the expected characteristics of new chips.

5.2 Design for Counterfeit Detection (DCD)

In testing and testing-related research and development fields, it is a standard practice that after each successful development of a set of techniques that utilize new technologies or new conceptual insights, the next phase is to develop approaches that incorporate these mechanisms into the design flow. We expect that a major rise of the practical importance of anti-counterfeiting techniques will be provided by the need for management of chips that use ultra-high levels of integration. Cutting edge ICs have already approached about 10 billion transistors per chip; it is unrealistic to expect high yields and long expected lifetimes. For example, one can easily envision that some types of maintenance will be required, at least in form of occasional adjustment of reverse and forward body biasing, to compensate for device aging or high operational temperatures. Thus, we anticipate that DCD approaches will share both the techniques and resources with IC characterization and maintenance methods.

An excellent example of one such maintenance technique has been developed by Mitra's research group at Stanford [25]. They have developed a low cost approach for measuring device aging and therefore slowdown of gates on the critical paths of an IC. This approach is also important because it uses only differential time measurements and induces very low hardware and energy overheads. It is relatively easy to re-target architectural primitives and measurements for detection of old chips using one of the techniques described in the previous subsection.

6. CONCLUSION

Counterfeiting of electronic components is a growing illegal business with important economical, military, governmental, and industrial ramifications. Repackaging the old ICs, selling the failed test parts, as well as gray marketing, are the most dominant counterfeiting practices. Surprisingly, although recently many aspects of hardware related security have been extensively studied, there has been very little IC counterfeiting research. Creation of IC anti-counterfeiting techniques poses numerous and diverse challenges while it also has the potential to address a spectrum of important IC design, management, and maintenance problems. We have analyzed the currently most popular IC counterfeiting attacks and identified the most important IC anti-counterfeiting desiderata. To make the paper self-contained, we presented the most relevant related technologies. The technical highlight of the paper are vignettes of two approaches for fighting IC counterfeiting using EDA techniques and a brief summary of presently available industrial and government methods.

7. REFERENCES

[1] Y. Alkabani and F. Koushanfar. "Active Hardware Metering for Intellectual Property Protection and Security" *USENIX Security*, pp. 291–306, 2007.

[2] A. Caldwell et al., "Effective iterative techniques for fingerprinting design IP," *IEEE T-CAD*, vol. 23, no. 2, pp. 208–215, 2004.

[3] A. Kahng et al., "Copy detection for intellectual property protection of VLSI designs," *ICCAD*, pp. 600–604, 1999.

[4] F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual property metering," *IH*, pp. 81–95, 2001.

[5] F. Koushanfar and M. Potkonjak, "CAD-based security, cryptography, and digital rights management," *DAC*, pp. 268–269, 2007.

[6] Y. Alkabani et al. "Trusted integrated circuits: a nondestructive hidden characteristics extraction approach," *IH*, pp. 102–117, 2008.

[7] S. Wei, S. Meguerdichian, and M. Potkonjak, "Gate-level characterization: foundations and hardware security applications," *DAC*, pp. 222–227, 2010.

[8] S. Wei, A. Nahapetian, and M. Potkonjak, "Robust passive hardware metering," *ICCAD*, pp. 802–809, 2011.

[9] R. Chau et al., "High-k/metal-gate stack and its MOSFET characteristics," *IEEE EDL*, vol. 25, no.6, pp.408–410, 2004.

[10] D. Markovic et al., "Ultralow-power design in near-threshold region," *Proc. of the IEEE*, vol. 98, no. 2, pp. 237–252, 2010.

[11] J. Black, "Electromigration - a brief survey and some recent results," *IEEE T-ED*, vol. 16, no. 4, pp. 338–347, 1969.

[12] A. Sekiguchi, J. Koike, and K. Maruyama, "Microstructural influences on stress migration in electroplated Cu metallization," *Appl. Phys. Lett.*, vol. 83, no. 10, pp. 1962–1964, 2003.

[13] J. Stathis, "Physical and predictive models of ultrathin oxide reliability in CMOS devices and circuits," *IEEE T-DMR*, vol. 1, no. 1, pp. 43–59, 2001.

[14] J. Pang, D. Chong, and T. Low, "Thermal cycling analysis of flip-chip solder joint reliability," *IEEE T-CPMT*, vol. 24, no. 4, pp. 705–712, 2001.

[15] K. Mistry et al., "A 45nm logic technology with high-k+metal gate transistors, strained silicon, 9 Cu interconnect layers, 193nm dry patterning, and 100% Pb-free packaging," *IEDM*, pp. 247–250, 2007.

[16] R. Havemann and J. Hutchby, "High-performance interconnects: an integration overview," *Proc. of the IEEE*, vol. 89, no. 5, pp. 586–601, 2001.

[17] S. Bhardwaj et al., "Predictive modeling of the NBTI effect for reliable design," *CICC* pp. 189–192, 2006.

[18] E. Takeda and N. Suzuki, "An empirical model for device degradation due to hot-carrier injection," *IEEE EDL*, vol. 4, no. 4, pp. 111–113, 1983.

[19] P. Heremans et al., "Consistent model for the hot-carrier degradation in n-channel and p-channel MOSFETs," *IEEE T-ED*, vol. 35, no. 12, pp. 2194–2209, 1988.

[20] J. Srinivasan et al., "The case for microarchitectural awareness of lifetime reliability," *ISCA*, 2004.

[21] E. Y. Wu et al., "Interplay of voltage and temperature acceleration of oxide breakdown for ultra-thin gate dioxides," *Solid-State Electronics Journal*, 2002.

[22] B. Gassend et al., "Silicon physical random functions," *ACM CCS*, pp. 148–160, 2002.

[23] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," *ACM T-RETS*, vol. 2, no. 1, pp. 1–33, 2009.

[24] K. Gross, R. C. Dhankula, and A. J. Lewis, "Detecting counterfeit electronic components using EMI telemetric fingerprints." US Patent Application US 2009/009830 A1, 2009.

[25] M. Agarwal et al., "Circuit failure prediction and its application to transistor aging," *IEEE VTS*, pp. 277–286, 2007.

[26] N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," *IH*, pp. 206–220, 2009.

[27] M. Potkonjak, S. Meguerdichian, and A. Nahapetian, "Differential public physically unclonable functions: architecture and applications," *DAC*, pp. 242–247, 2011.

[28] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE D & T of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[29] G. Qu and M. Potkonjak, "Intellectual Property Protection in VLSI Design," *Kluwer Academic Publisher*, 2003.

[30] Technical report by U.S. Department Of Commerce, Bureau Of Industry And Security, Office Of Technology Evaluation, "Defense industrial base assessment: Counterfeit electronics," 2010.

[31] U. Ruhrmair, S. Devadas, and F. Koushanfar, "Security based on Physical Unclonability and Disorder," Book Chapter in 'Introduction to Hardware Security and Trust', Editors: M. Tehranipoor and C. Wang, *Springer*, 2011.

[32] F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, and C. Wachsmann, "A formalization of the security features of physical functions," *IEEE S & P*, pp. 397–412, 2011.

[33] T. Kim, R. Persaud, and C. H. Kim, "Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits," *IEEE JSSC*, vol. 43, no. 4, pp. 874-Ű880, 2008.

[34] E. Karl et al., "Compact in-situ sensors for monitoring negative bias-temperature-instability effect and oxide degradation," *ISSCC*, pp. 410–411, 2008.

[35] K.K. Kim, W. Wang, and K. Choi, "On-chip aging sensor circuits for reliable nanometer MOSFET digital circuits," *T-CAS-II*, vol.57, no. 10, pp.798–802, 2010.

[36] F. Koushanfar, A-R. Sadeghi, and H. Seudie "EDA for Secure and Dependable Cybercars: Challenges and Opportunities," *DAC*, 2012.

[37] M. Majzoobi and F. Koushanfar, "Time-Bounded Authentication of FPGAs," *IEEEE T-IFS*, vol. 6 , no. 3, pp. 1123–1135 , 2011.

[38] Analytical Solutions Inc., *http://www.asinm.com/*.

[39] DARPA Microsystem Technology Office, *http://www.darpa.mil/Our_Work/MTO/*.