Efficient Strategies for Detection and Avoidance of Counterfeit ICs

Ujjwal Guin
Department of Electrical and Computer Engineering
Auburn University, AL, USA
ujjwal.guin@auburn.edu

***Abstract*—With the advent of globalization and the resulting horizontal integration, present-day electronic component supply chain has become extremely complex and calls for immediate solutions to eliminate counterfeit integrated circuits (ICs). Such counterfeit ICs – recycled, remarked, overproduced, defective, and/or cloned – have raised serious concerns regarding the safety and security of our critical infrastructures, such as, military systems, financial infrastructures, transportation, communication, medical systems, and many more applications. Due to the lack of efficient detection and avoidance techniques, many more instances of counterfeit ICs evade detection than those that are actually detected. One of the major concern is the reliability of such ICs, and their application in a critical infrastructure may result a catastrophic failure. In addition, the cloned ICs may have additional features that could provide additional capabilities to an adversary to gain control of a system by bypassing security modules. In this paper, two different solutions are presented for detecting the complete spectrum of these counterfeit ICs. These solutions are efficient, low cost and resistant to various known attacks.**

I. Introduction

The growing incidents of counterfeiting and piracy pose a great concern to the Government and Industry because of the substantial resources that are being channelled into the illegal activities by violating law and order to disrupt society, and impose a negative impact on innovation, economic growth, and competitiveness. In addition, the safety and security of our day-to-day lives are at stake as counterfeiting results in inferior quality (low reliability) products. It also results in the loss of business from the trade in counterfeit products [1]. International Chamber of Commerce estimated that the cost of counterfeiting and piracy for G20 nations was as much as US$775 billion every year. However, it will grow at an astonishing rate to $1.7 trillion in 2015 [2].

A report from the Information Handling Services Inc. (Englewood, CO, USA) shows that reports of counterfeit parts have quadrupled since 2009 [3]. This data has been compiled from two reporting entities - The Electronic Resellers Association International (ERAI) Inc. (Naples, FL, USA) and the Government-Industry Data Exchange Program, GIDEP (Corona, CA, USA). It is mentioned that the five most commonly counterfeited components (e.g., analog ICs, microprocessor ICs, memory ICs, programmable logic ICs, and transistors) represent $169 billion in potential annual risk for the global electronics supply chain based on all reported counterfeit incidents in 2011 [4].

The widespread incidents of counterfeiting and piracy of ICs are mainly due to the globalization of semiconductor industry and manufactured in places with limited trust and visibility [5], [6]. Because of the persistent trend of device scaling and the resulting increase in the complexity of the fabrication process, most companies designing system-on-chip (SoC) no longer maintain a fabrication unit (or foundry) of their own. Costs for building and maintaining such foundries are reported to be more than several billions of dollars [7]. This leads to the adaptation of horizontal integration in the semiconductor industry where the SoC designers provide contracts to the foundries and assemblies for production.

II. Threat Space

The US Department of Commerce first proposed the definition for a counterfeit part [8]. As the definition does not cover all counterfeit types, Guin et al. [5], [6], [9]–[13] developed a comprehensive taxonomy of counterfeit types, which is adopted by AS6171 Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts [14]. Figure 1 shows the entire threat space that leads to the counterfeiting and piracy. The figure does not include tampered type as the detection pose a different set of challenges and is not included in this paper.

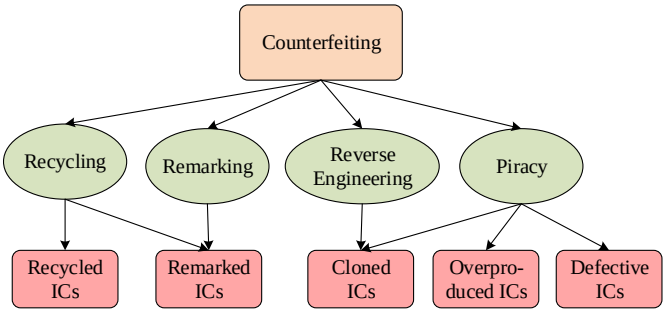


Figure 1: Threat space.

Recycling is a process by which the retired parts (may be functional, but, with reduced lifetime) are reclaimed from a discarded system. This rapid growth of IC recycling is due to the widely available electronic waste (e-waste). In the United States, only 25% of e-waste was properly recycled in 2009 [15]. However, this can be even worse for other countries. This huge resource of e-waste allows counterfeiters to pile

up an extremely large supply of counterfeit components. The reliability of recycled ICs is questionable as the reclaiming process (removal of ICs from a retired electronic system under a very high temperature, and then sanding, repackaging, and remarking) could damage the parts and produce many latent defects. On the other hand, a counterfeiter can remark a lower grade part to its higher grade counterpart mainly to gain larger profits. Similar to recycled parts, remarked ICs have reliability concerns as a space grade IC can withstand a wide range of temperatures, and radiation levels that would cause instant failure for a commercial grade component.

Reverse engineering (RE) is a process of extracting the design specification of the inner details of a product using advanced imaging instruments and powerful characterization tools. An untrusted foundry can extract gate-level netlist from the mask and layout information [16]. Once the foundry extracts the gate level netlist, it's a matter of time that full specification of an IC can be determined. In addition, untrusted foundries may sell illegal copies of the Graphic Database System II (GDSII) files that they receive from SoC designers for fabrication. A wide range of counterfeiters, from small entities to large organizations, can be involved in piracy in order to eliminate the large research and development (R&D) costs. A wide varieties of intellectual properties (IPs), such as register-transfer level (RTL) designs, netlists, and layouts can be pirated. The piracy leads to the cloning and overproduction of ICs. One can also source defective ICs in the market. In this paper, we describe a solution that enables forward trust between various entities in the semiconductor supply chain to prevent cloned, overproduced and defective ICs.

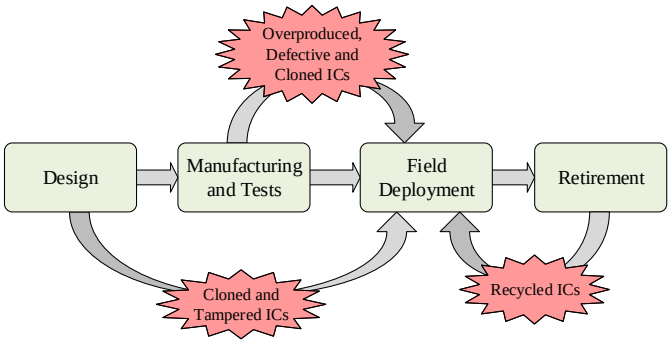


Figure 2: Supply chain vulnerabilities.

It is now important to analyze where these threats are originating from. In the design phase, complex integrated circuits are designed and assembled from RTL to GDSII, and the design steps are performed in many different places (even in different countries) mainly to reduce the development cost and time-to-market. Design reuse has also become an integral part of SoC design in the form of hard IPs (layout level designs), firm IPs (designers can optimize codes with parameterized constraints), and soft IPs (synthesizable RTL designs). In this stage, the counterfeiter can steal IPs to create clones, or tamper with codes to modify the functionality, create backdoors, etc., and sell in the open market (Field Deployment). During manufacturing, an untrusted foundry or assembly can illegally overproduce (more chips outside of the contract) ICs, sell defective chips, which should have been discarded, and manufacture clone ICs. Finally in the retirement stage, a counterfeiter can strip of parts from the retired electronic systems, and sell in the market as new.

III. Prior Approaches

A. Detection of Recycled and Remarked ICs

The detection and avoidance approaches are broadly classified into different categories. First, there are several standards [14], [17]–[19] in practice which recommend different physical and electrical tests to detect these ICs. The goal of these methods is to identify the defects and anomalies (see Chapter 3 of the book "Counterfeit Integrated Circuits: Detection and Avoidance" [6] for details) present in those recycled and remarked ICs, which are not typically present in authentic ones. However, prohibitively excessive test times, test costs, low detection capability and lack of automation make these test methods ineffective. Second, researchers have proposed several schemes based-on statistical data analysis [20]–[22]. Third, on-chip sensors have been proposed as an alternative to the conventional test methods [23]–[26]. Finally, DNA markings [27] are commercially available to provide traceability for electronic parts. Recycled and remarked ICs can be detected via fast or detailed authentication. In fast authentication, the marks fluoresce under UV light. A decision is taken regarding the authenticity of an IC based on the color produced. Detailed authentication is performed in specific laboratories, which is inefficient and costly [28]. Further, if counterfeiters add a different mechanism to the chip which can produce similar fluorescence, DNA marking will be ineffective for fast-authentication as it only observes the color. From the above discussion, it can be inferred that the on-chip sensors are the suitable candidates for detecting these ICs. In this paper, I will briefly describe different on-chip sensors that are proposed in [25], [26].

B. Avoidance of Overproduced, Cloned, and Defective ICs

The existing approaches aim to prevent IC piracy (see Figure 1) by attempting to give an SoC designer control over the number of ICs manufactured [29]–[35]. These approaches can be either passive or active. Passive approaches register all new authorized ICs by incorporating physically unclonable functions (PUFs) in each copy, and then storing their challenge-response pairs in a secure database. Later, any suspect ICs taken from the market can be checked for proper registration.

Active approaches are designed to automatically lock each new IC that is manufactured by a foundry until it is unlocked (activated) by the authorized SoC designers, which can be efficiently implemented though logic obfuscation [29]. This is a technique where a design is transformed to a different one to obfuscate the inner details of the original design. Only on the application of a programmed secret key is the transformation reversed, thus preserving the original functionality. Roy et

al. first proposed to obfuscate a netlist by using a set of XOR/XNOR gates (lock) which can only be unlocked by using a key. Unfortunately, this design is not resistant to reverse engineering as the key controlled gates are directly related to their key bits (XOR and XNOR gates indicate 0 and 1 at the key location, respectively) and vulnerable to key sensitization attacks [36]. Rajendran et al. addressed these problems by improving the original obfuscation technique [36]. However, Subramanyan et al. have shown that the key in an activated circuit can always be exposed using scan based manufacturing tests by SAT-based analysis, no matter what preventive measures one takes [37]. Different approaches have been proposed till date to mitigate SAT based attacks [38] [39] [40].

In this paper, I will briefly describe a technique to establish forward trust proposed in [35] to prevent overproduced, cloned, and defective ICs, getting into the electronic supply chain.

IV. On-Chip Sensors for Counterfeit Detection

On-chip sensors are used to detect recycled ICs, those have been used in the field. Recycled ICs are characterized by aging, i.e., prior usage has taken its toll on the components' life and performance. A shift in the components' parameters due to aging will occur when they are used in the field for some time, which leads to the development of parametric defects and anomalies in the component. Aging of a component used in the field can be attributed to two major, distinct phenomena (which are becoming more prevalent as the technology scales down). They are negative-bias temperature instability (NBTI) [41], [42] and hot carrier injection (HCI) [43], [44] which are prominent in PMOS and NMOS devices, respectively. NBTI occurs in p-channel MOS devices stressed with negative gate voltages and elevated temperatures due to the generation of interface traps at the $Si{-}SiO_2$ interface. Removal of the stress can anneal some of the interface traps, but not completely. As a result, it manifests as the increase in threshold voltage (V_{th}) and absolute off current (I_{off}) and the decrease of absolute drain current (I_{DSat}) and transconductance (g_m). HCI occurs in NMOS devices caused by the trapped interface charge at $Si - SiO_2$ surface near the drain end during switching. It results in non-recoverable V_{th} degradation. These two aging mechanisms lead to the increased delay in the components' internal paths, which ultimately reduces the component's operating speed.

To detect recycled ICs, we need to design a sensor that can take advantage of aging very efficiently. As we all know NBTI is one the major source of aging, our objective is to design a sensor that can expedite aging. The NBTI-aware on chip sensor [25] (see Figure 3 for details), can efficiently detect recycled ICs with little misprediction (predict a new IC as recycled and vice versa) when the chips are aged for a short period of time. We call this sensor as Combating Die and IC Recycling (CDIR) sensors. However, when the workload decreases, we require the chips to be used much longer for detection, which eventually results in a higher rate

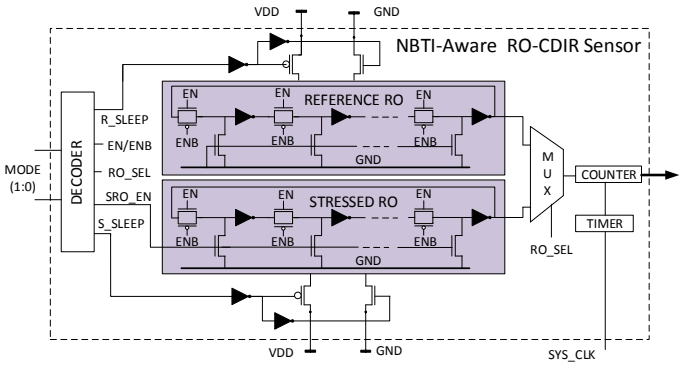


Figure 3: The NBTI-Aware RO-CDIR sensor [25]

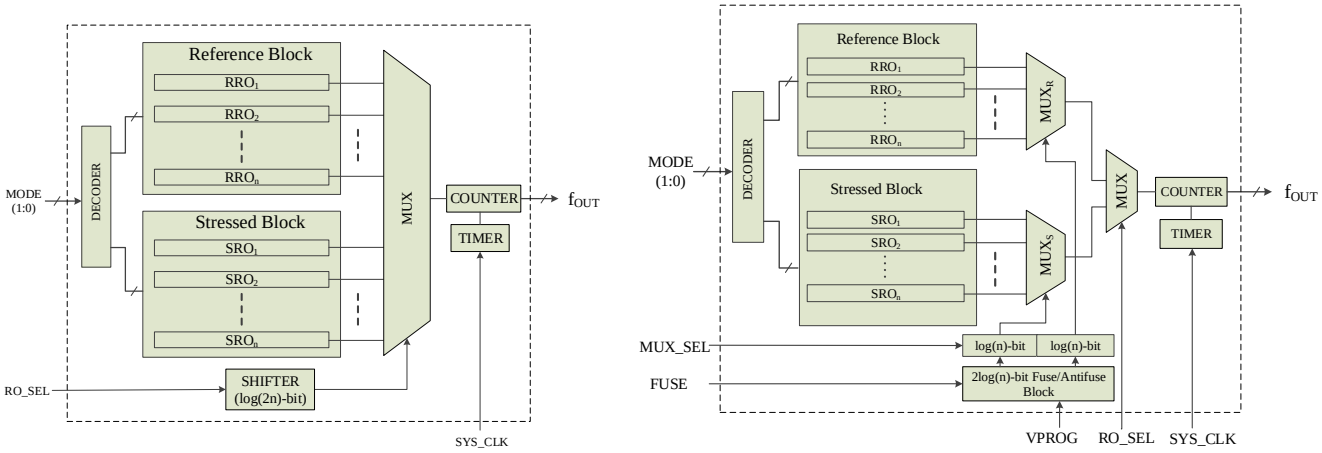
.

of misprediction. In addition, there may be a recycling activity from the overstock of electronic systems where the recyclers extract components from never used systems. The detection of these components can be performed with a CDIR that can detect a small amount of aging (for example, the amount of aging caused during the test of a system). When the application risk is critical [9] [6] [10], we do not have the luxury for any test escapes as the system failure due to using recycled chips could cause significant financial loss, as well as risks to safety and security. Thus, this necessitates further improvements of this simple CDIR.

To address these challenges, two different CDIR structures based on multiple ring oscillators have been proposed [26]. Here, we have multiple reference and stressed RO-pairs. An averaging approach was introduced to reduce the impact of process variations. This design provides a much better detection for ICs used for only few hours in the field with the cost of small misprediction. In addition, another modified design of multiple reference and stressed RO-pairs. In this case, a selection algorithm is used to find the best reference and stressed RO-pair. This CDIR with the best selected RO-pair, provides even better detection (no misprediction) of recycled ICs, even if they have been used only for a few hours, unlike the AN-CDIR. The details can be found in [26] [45].

V. Establishing Forward Trust for Counterfeit Avoidance

With increasing SoC design complexity, design reusability has become an integral part of the SoC design process, mainly to reduce manufacturing cost and time to market. Unfortunately, due to the lack of visibility and controllability of the manufacturing process, the trust becomes of the major concern among different entities in the semiconductor supply chain. An untrusted SoC designer can illegally use a third party IP in a different SoC and can also overuse it. In addition, SoC designers lose profits when an untrusted foundry or assembly overproduces chips and sells them under their name. Thus, forward trust is extremely important to the entities involved in the SoC design. Forward trust can be described as the trust on SoC designer from the IP owners, and foundry/assembly from the SoC designer/IP owners. Ensuring forward trust implies



(a) Multiple RO CDIR with averaging approach.

(b) Multiple RO CDIR with selection approach.

Figure 4: CDIR sensor with multiple ring oscillators [26].

that the IP owners does not need to trust the SoC designer, and SoC designers/IP owners to the foundries and assemblies. In this section, we present a comprehensive solution for establishing forward trust between the entities involved in SoC design and fabrication for protecting IPs and ICs.

Figure 5 shows the design flow for establishing forward trust between various entities involved with the SoC design process. The design flow is very similar to the existing IC design flow except for the lock insertion and functional activation steps. The design process starts with the insertion of locks by using a set of XOR/XNOR gates (we call them as key gates) using an existing secure logic encryption technique. The circuit produces functionally correct output when it receives a unlock key. The number of XOR or XNOR gates depends on the level of security one wants to achieve. It is important to enable manufacturing tests before the activation of chips.

Each 3PIP owner inserts key gates to lock their design and then generates test patterns. The SoC designer receives all these locked IPs and integrates them in the design. The SoC designer also inserts a lock in one of the in-house IP to protect against IC overproduction. The SoC designer collects all the test patterns from different IP owners and stores them in a pattern repository for future wafer and package tests.

The GDSII file corresponding to the SoC design is now sent to the foundry. The foundry first processes wafers, which generally contains hundreds of dies in a single wafer. Foundry then performs wafer test to inspect dies to find gross defects. If there are too many dies on a wafer that are defective, the foundry sometimes rejects the whole wafer. After wafer tests, the defect-free dies are sent to assembly for packaging. The good chips are then sorted out by using package tests and the chips that have been damaged during the packaging process are discarded. Finally, each chip is unlocked using the valid key by the entity who perform the final manufacturing test (foundry, assembly, or SoC designer) before supplied to the market. To protect this key from SoC designers, foundries and assemblies, a secure encrypted communication protocol is used. The interested readers can find more details in [35].

VI. Conclusion

Integrated circuits are becoming increasingly vulnerable to counterfeiting and piracy due to the lack of visibility and trust in the semiconductor manufacturing process. To address this trust issue, we have presented two different solutions for detecting the complete spectrum of counterfeit ICs to ensure the trustworthiness, security, and reliability of different ICs in the semiconductor supply chain.

References

[1] OECD, "The Economic Impact of Counterfeiting and Piracy," 2007, http://www.oecd.org/dataoecd/13/12/38707619.pdf.

[2] D. Chardonnal, "Impacts of counterfeiting and piracy to reach US$1.7 trillion by 2015," February 2011.

[3] J. Cassell, "Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defence Industry and National Security," April 2012.

[4] IHS iSuppli, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," 2011.

[5] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug 2014.

[6] M. M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.

[7] A. Yeh, "Trends in the global IC design service market," DIGITIMES Research, March 2012.

[8] U.S. Department Of Commerce, "Defense Industrial Base Assessment: Counterfeit Electronics," January 2010.

[9] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[10] ——, "A comprehensive framework for counterfeit defect coverage analysis and detection assessment," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[11] U. Guin, D. Forte, and M. Tehranipoor, "Anti-Counterfeit Techniques: From Design to Resign," in *Microprocessor Test and Verification (MTV)*, 2013.

[12] U. Guin, M. Tehranipoor, D. DiMase, and M. Megrdichian, "Counterfeit IC Detection and Challenges Ahead," *ACM/SIGDA E-NEWSLETTER*, vol. 43, no. 3, March 2013.

[13] U. Guin and M. Tehranipoor, "On Selection of Counterfeit IC Detection Methods," in *IEEE North Atlantic Test Workshop (NATW)*, May 2013.

[14] SAE, "Test methods standard; counterfeit electronic parts," Work In Progress, http://standards.sae.org/wip/as6171/.

[15] U.S. Environmental Protection Agency, "Electronic waste management in the united states through 2009," May 2011.

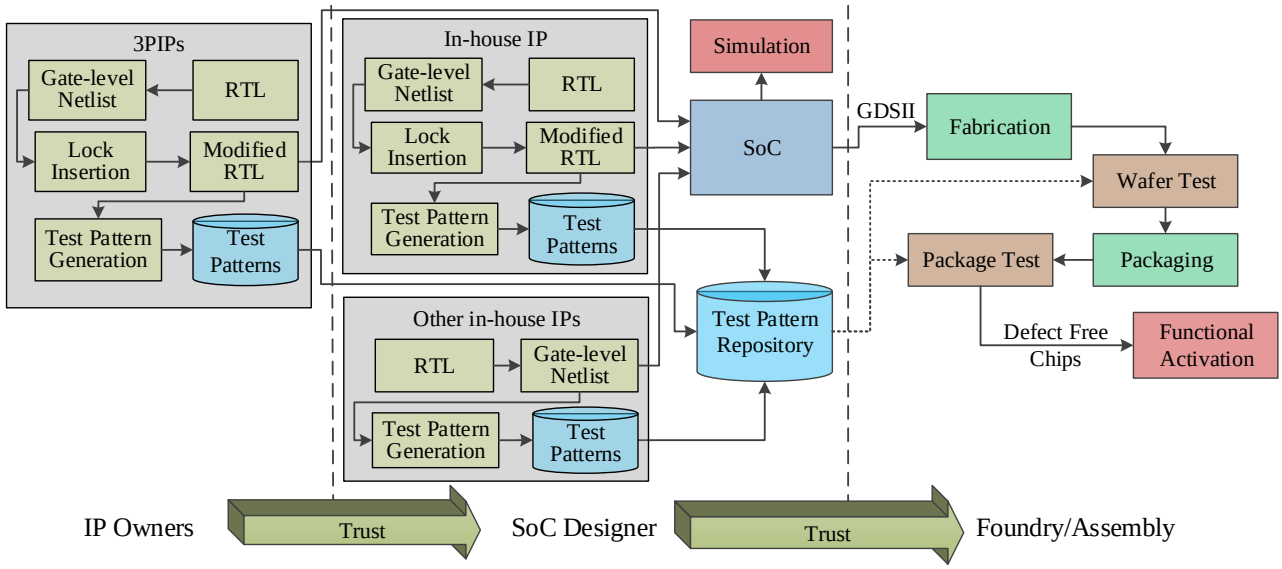


Figure 5: Flow for enabling forward trust in the SoC manufacturing process [35].

[16] R. Torrance and D. James, "The state-of-the-art in ic reverse engineering," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '09, 2009, pp. 363–381.

[17] SAE, "Counterfeit electronic parts; avoidance, detection, mitigation, and disposition," 2009, http://standards.sae.org/as5553/.

[18] CTI, "Certification for coutnerfeit components avoidance program," September 2011.

[19] IDEA, "Acceptability of electronic components distributed in the open market," http://www.idofea.org/products/118-idea-std-1010b.

[20] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ics," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, October 2012.

[21] K. Huang, J. Carulli, and Y. Makris, "Parametric counterfeit IC detection via Support Vector Machines," in *Proc. International Symposium on Fault and Defect Tolerance in VLSI Systems*, 2012, pp. 7–12.

[22] H. Dogan, D. Forte, and M. Tehranipoor, "Aging analysis for recycled fpga detection," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), IEEE International Symposium on*, Oct 2014, pp. 171–176.

[23] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ics using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE-ACM Design Automation Conference*, June 2012, pp. 703 –708.

[24] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ics," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 22, no. 5, pp. 1016–1029, May 2014.

[25] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost On-Chip Structures for Combating Die and IC Recycling," in *Proc. of ACM/IEEE on Design Automation Conference*, 2014.

[26] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233–1246, 2016.

[27] M. Miller, J. Meraglia, and J. Hayward, "Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts," in *SAE Aerospace Electronics and Avionics Systems Conference*, October 2012.

[28] Semiconductor Industry Association (SIA), "Public Comments - DNA Authentication Marking on Items in FSC5962," November 2012.

[29] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending Piracy of Integrated Circuits," in *Proc. on Design, Automation and Test in Europe*, March 2008, pp. 1069 –1074.

[30] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. of 16th USENIX Security Symposium on USENIX Security Symposium*, 2007, pp. 20:1–20:16.

[31] R. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," in *Proc. of IEEE/ACM International Conference on Computer-Aided Design*, November 2008, pp. 674 –677.

[32] Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote activation of ICs for piracy prevention and digital right management," in *Proc. of IEEE/ACM international conference on Computer-aided design*, 2007, pp. 674–677.

[33] J. Huang and J. Lach, "IC activation and user authentication for security-sensitive systems," in *Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust*, June 2008, pp. 76 –80.

[34] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC Piracy Using Reconfigurable Logic Barriers," *IEEE Design and Test of Computers*, vol. 27, no. 1, pp. 66 –75, Jan.-Feb. 2010.

[35] U. Guin, Q. Shi, D. Forte, and M. Tehranipoor, "FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2016.

[36] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in *Proc. of ACM/IEEE on Design Automation Conference*, June 2012, pp. 83–89.

[37] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on*, May 2015, pp. 137–143.

[38] U. Guin, Z. Zhou, and A. Singh, "A novel design-for-security (dfs) architecture to prevent unauthorized ic overproduction," in *IEEE VLSI Test Symposium (VTS)*, 2017.

[39] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Security analysis of anti-sat," in *ASP-DAC*, 2017.

[40] Y. Xie and A. Srivastava, "Mitigating sat attack on logic locking," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2016, pp. 127–146.

[41] M. Alam and S. Mahapatra, "A comprehensive model of pmos nbti degradation," *Microelectronics Reliability*, vol. 45, no. 1, pp. 71 – 81, 2005.

[42] V. Reddy, A. Krishnan, A. Marshall, J. Rodriguez, S. Natarajan, T. Rost, and S. Krishnan, "Impact of negative bias temperature instability on digital circuit reliability," in *Proc. on Reliability Physics*, 2002, pp. 248 – 254.

[43] K.-L. Chen, S. Saller, I. Groves, and D. Scott, "Reliability effects on mos transistors due to hot-carrier injection," *Electron Devices, IEEE Transactions on*, vol. 32, no. 2, pp. 386 – 393, February 1985.

[44] J. McPherson, "Reliability challenges for 45nm and beyond," in *Proc. of ACM/IEEE on Design Automation Conference*, 2006, pp. 176 –181.

[45] U. Guin, "Establishment of trust and integrity in modern supply chain from design to resign," 2016.