Ujjwal Guin *Auburn University, Auburn, AL*
Navid Asadizanjani and Mark Tehranipoor
University of Florida, Gainesville, FL

Editors: Michelle X. Gong and Shiwen Mao

PHoto, istockphoto.com

STANDARDS FOR HARDWARE SECURITY

Due to the globalization of design, manufacturing and distribution of integrated circuits (ICs), hardware underlying information systems have become increasingly vulnerable to a number of malicious attacks, primarily counterfeiting of ICs and piracy of intellectual properties (IPs). To ensure the security of our critical infrastructure, the use of trusted hardware is absolutely necessary. There are a handful of standards, either currently available today or in progress, that provide guidance to undertake hardware security issues. This article focuses on the standardization activity in the domain of hardware security.

DETECTION AND AVOIDANCE OF COUNTERFEIT ICS

Since the Senate Armed Service Committee hearing on counterfeit electronic parts in November 2011 [1], a significant amount of resources has been directed to detect these parts and prevent them from entering the supply chain. Numerous reports of counterfeit ICs can be found on the Internet by simply searching the term "counterfeit IC". For example, the U.S. Air Force reported in January 2012 that a company, Hong Dark Electronic Trade, based in Shenzhen, China, supplied approximately 84,000 suspect counterfeit parts to various Department of Defense (DoD) agencies [2].

The use of counterfeit parts in the critical infrastructures can lead to a system failure that might result in financial damages, risk of national security, and safety of human lives. For example, the counterfeit parts found on several essential military systems, such as high-altitude missiles, helicopters (SH-60B, AH-64 and CH-46), and aircrafts (C-17, C-130J and C-27J) could have serious consequences [3]. Army Lt. Gen. Patrick J. O'Reilly of the Missile Defense Agency (MDA) mentioned, "We do not want to be in a position where the reliability of a $12 million THAAD interceptor is destroyed by a $2 part" [4].

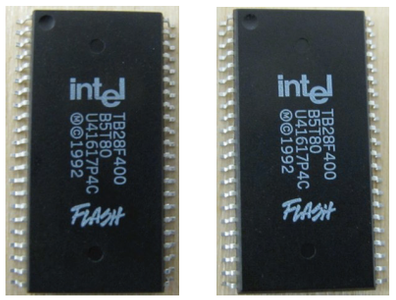
Why does this proliferation of counterfeit parts exists? The operational life of our critical infrastructure (e.g., various DoD applications, aerospace, etc.) is much higher than the lifetime of a part. For example, B52 bombers, which were first produced in 1940s, are still flying. The replacement electronic parts are no longer produced by the original component manufacturer (OCM). When the parts are no longer being manufactured, they are often supplied from less reliable third-party vendors and distributors. As a result, counterfeit ICs easily enter in the supply chain through these untrusted entities.

Information Handling Services (IHS) reported that the potential annual risk for the global supply chain is at $169 billion and is still increasing annually from the counterfeit ICs [5]. Reportedly, recycled ICs constitute almost 80% of all the reported counterfeiting incidents [6]. These chips are reclaimed from the old discarded electronics. Along with recycled ICs, other counterfeit IC types are remarked, overproduced, cloned, out-of-spec/defective, forge documentation and tamper types [6].

Since the rise of counterfeit parts in early 2000s, it was required to report these incidents so that overall size of the problem can be monitored and then controlled. National Defense Authorization Act (NDAA) for FY 2012 [7] established a process for mandating a personnel/test laboratory to report counterfeit electronic parts or suspect counterfeit electronic parts in writing within 60 days to appropriate government authorities and to the Government-Industry Data Exchange Program (GIDEP, http://www.gidep.org/) or a similar program, once they become aware of, or have reason to suspect, that any component or material contained in supplies are counterfeit.

On September 21, 2015, the DoD published a rule in the Federal Register to further implement Section 818 of the NDAA for FY 2012, which requires all DoD contractors and subcontractors, except in limited circumstances, to acquire electronic parts from trusted suppliers to avoid counterfeit electronic parts getting into the supply chain [8]. If a part is not available from any trusted supplier, it is mandatory to notify the contracting DoD officer.

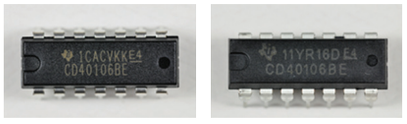
The rule imposed by the DoD allows more accountability and creates a proper database on parts entering from untrusted vendors to the defense applications. But the need for a proper detection standard has become significant as the rule also forces the contractors to be responsible for the proper testing of parts acquired from untrusted suppliers. The Society of Automotive Engineers (SAE) International is actively involved in developing or has developed a series of standards, such as, AS5553, AS6081, AS6496, and AS6171.



Authentic Recycled

Photos, University of Florida

FIGURE 1. A flash memory chip.



Authentic Clone

Photo, (left) SMT Corp

FIGURE 2. An inverter chip.

In April 2009, the SAE G-19CI committee issued AS5553 for providing guidance to the requirements, best practices and methods detecting counterfeit ICs. This document covers parts and supplier management, procurement procedure, test and evaluation methods and, finally, the action plan when a counterfeit or suspect counterfeit part is identified.

In December 2012, the SAE G-19D Distributor committee published AS6081 for helping part distributors to avoid, detect,

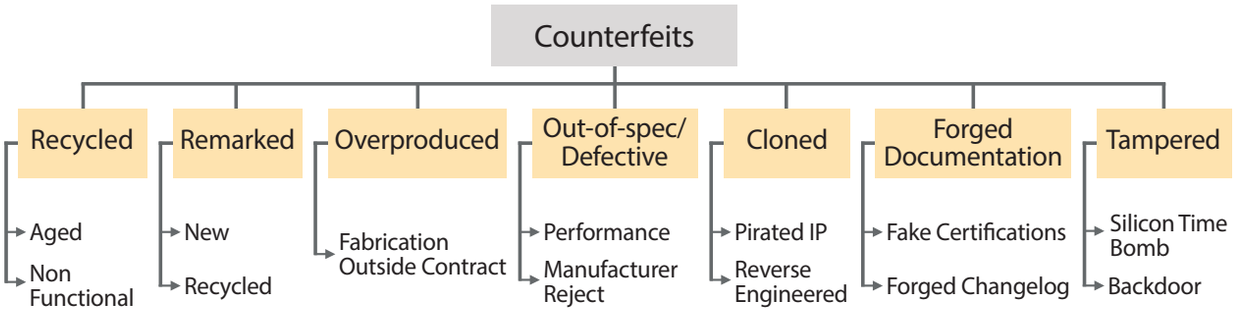
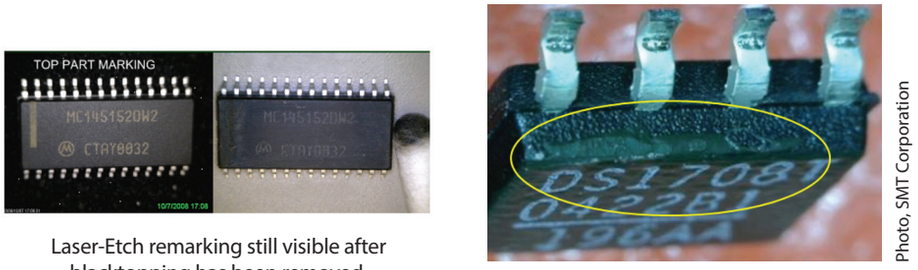


FIGURE 3. Taxonomy of different counterfeit types [6].



Laser-Etch remarking still visible after blacktopping has been removed.

Defective black-topping.

Photo, SMT Corporation

FIGURE 4. Defects and anomalies present in counterfeit parts.

(a) Optical imaging

(b) X-Ray imaging

(c) Scanning electron microcopy (SEM) imaging

Photos, University of Florida

FIGURE 5. Different visual inspection techniques commonly used for detecting counterefeit parts.

mitigate and then dispose counterfeit/ suspect counterfeit parts. This document standardizes the same objective as AS5553 only for the distributors. On August 2014, G-19AD Authorized Distributor Committee issued AS6496 to enhance the best practices and procedures in the authorized and franchised distribution channels to help mitigate counterfeit ICs. Note that all these standards (AS5553, AS6081 and AS6496) use AS6171 for developing a test plan for detecting these parts.

In October 2016, the SAE G-19A Test Laboratory Standards Development Committee issued AS6171 for developing test plans, which consist of a sequence of test methods. The standard adopts the taxonomy of counterfeit types and a model to evaluate the effectiveness of test methods from the work introduced in [9] and [10].

A comprehensive taxonomy of defects and anomalies present in the counterfeit parts is also introduced. The initial version of the standard does not include the assessment of tampered parts, those that are modified for malicious purposes. The G-19A group is currently working on adding tampered type, and the defects present in these parts, in revision of AS6171. An online version of the assessment process is also available and commonly referred to as the CDC Tool (http://cdctool.sae.org/), currently hosted by SAE, and acquired from University of Connecticut in 2016.

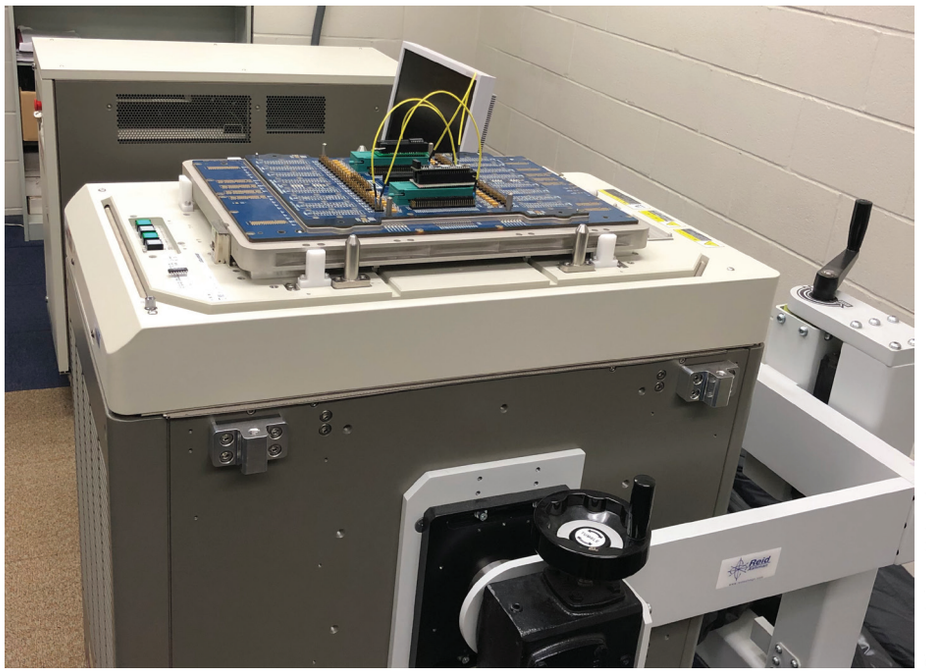
The defects and anomalies present in counterfeit parts can be broadly classified into three categories – defects related to the packaging, physical defects and electrical defects. Physical defects can be related to the part terminations (e.g., pins, balls and columns), surfaces and dies. Electrical defects are related to the DC, AC and functional parameters of the parts.

AS6171 introduces a set of test methods for detecting counterfeit parts. These tests can be broadly classified into two different classes – tests related to the physical properties and electrical properties of different parts. External visual inspection (EVI) consists of general inspection using different imaging techniques of all the incoming parts and then a detailed inspection of a selected sample. This is the first test to be performed, and then successive tests are carried out. These tests are radiological (X-Ray) inspection, decapsulation for internal inspection, material analysis (e.g., X-Ray Fluorescence (XRF) spectroscopy, Electron Dispersive Spectroscopy (EDS), Raman spectroscopy,

and/or Fourier Transform Infrared (FTIR spectroscopy), Acoustic Microscopy (AM), electrical tests (e.g., Curve Trace, tests for DC/AC parameters, functional tests, Burn-in, Temperature Cycling, and/or seal tests). AS6171 recommends a set of tests among this complete list based on the application risks. For example, if the parts are used in a critical application (e.g., aerospace) the testing must be comprehensive. On the other hand, if the application risk is low, simple EVI might be sufficient.

In addition to these standards developed by the G-19 Committee, two other standards – CTI CCAP-101 (http://www.cti-us.com/CCAP.htm) and IDEA-STD-1010 (https://www.idofea.org/idea-std-1010-inspection-standard) – are in practice, which provides guidance to detecting counterfeit ICs.

Is the electronic component supply chain safe from the counterfeit parts? It is actually the opposite. First, we still need a low-cost test method to efficiently detect these fake parts. Currently, we only apply visual inspection to all incoming parts. The accuracy of visual inspection is questionable as the counterfeiters are consistently evolving, and making their processes mature. The defects, which were easy to detect few years back may not be that easy to detect now. On the other hand, a handful of samples go through the actual test plan recommended by these standards. Second, enabling traceability of parts is challenging. A low-cost RFID-based solution can be a perfect candidate. Recently, DARPA launched Supply Chain Hardware Integrity for Electronics Defense (SHIELD, https://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense) program to protect the supply chain from the counterfeit parts. Third, there are a wide variety of parts already circulating in the supply chain, and for some of the cases there may not be any reference parts for comparison. Finally, we need automation in the test process. Currently most of the test methods are conducted in an ad-hoc fashion and the decisions are taken by the subject matter experts.



Photo, Auburn University

FIGURE 6. Advantest T2000 Automatic Test Equipment for electrical tests.

IP PIRACY

Along with counterfeit parts, piracy of intellectual properties (IPs) have been in the limelight in recent years. Cases on IP theft are being investigated, but only a small portion can be brought under jurisdiction. The Chinese smartphone manufacturing giant Huawei has been charged with IP piracy by the Department of Justice, New York [11]. The company is charged with stealing robotic technology necessary to test smartphones from T-Mobile. A widely cited U.S. Department of Commerce study states that IP-intensive industries comprised over 38% of the entire American economy [12]. According to a 2017 report by the United States Trade Representative, Chinese theft of American IP currently costs between $225 billion and $600 billion annually, a significant portion of which comes from IPs related to semiconductor design and software [13]. The Senate Judiciary Committee has recently created the IP Subcommittee to prevent IP piracy and theft [14].

Dire need to prevent IP piracy has led to research work on creating design standards by the Institute of Electrical and Electronics Engineers (IEEE). The standard IEEE Std. 1735 recommends the best practice to protect IPs. It provides a guideline on how to create designs in a secure way when encountering IP piracy. The standard is meant to be a good fit for designs where third-party IPs can be securely encrypted and be given to the IP users.

There are three primary stakeholders: the IP author, the IP user, and the tool vendor – in the trust model mentioned in Std. 1735 standard. IP authors are the creators and owners of IPs, who grant the right to use the IP in exchange for proper compensation.

TO ENSURE THE SECURITY OF OUR CRITICAL INFRASTRUCTURE, THE USE OF TRUSTED HARDWARE IS ABSOLUTELY NECESSARY

IP users are the receiving party, who get the right to use an IP. The tool vendors (e.g., Synopsys, Cadence and Mentor Graphics) provide EDA tools, which can be used by the IP users. In this model, the tool vendors are always trusted.

The IP protection is performed by encrypting the IP in such a way so that the IP user can only use an IP, which is compatible to one/multiple EDA tools. First, an IP author marks the IP design based on which blocks need to be encrypted and what remains visible to the user. Second, it chooses a set of vendor tools based on the requirement to enable access to the user through the tool. Each tool has its own public/private key pair that is used to encrypt the common session key, which is used to encrypt the IP.

The final protected IP has a key block for each vendor tool that contains the encrypted, common session key. The key block can only be decrypted by the specific tool vendor whose key was used to protect it. The tool can decrypt the protected IP using the recovered session key. In this way, the tools and encrypted IP together make IP functional, which enables it for simulation and verification. Recommendation for the interoperability among other hardware design standards (IEEE Std 1800, IEEE Std 1076) was made in Std. 1735. The standard has some recommendation on rights management programs that allow IP author control over IP use. The standard also provides enough control over the visibility of the IP. It fulfills an author's need to determine what is visible in a protected scheme.

Now, the same question comes - does the encryption proposed in Std. 1735 provide adequate security? Sadly, the answer is no. We first showed in 2015 that it cannot prevent an adversary adding malicious hardware to an encrypted IP [15]. Two years later, Chhotaray et al. showed that this standard is not secured after all [16]. IEEE 1735 standard does not specify the type of padding scheme to be used in its encryption, which leads to a possible Padded Oracle Attack (POA). It is also possible to launch Syntax Oracle Attack (SOA) due to error messages received from bad syntax. License violation can also occur despite following the standard. The standard does not provide protection against Hardware Trojans, malicious modifications in the netlist. ■

Ujjwal Guin received his PhD degree from the Electrical and Computer Engineering Department, University of Connecticut. He is currently an assistant professor in the Electrical and Computer Engineering Department of Auburn University, Auburn, AL. His research interests include hardware security and trust, supply chain security, and VLSI design and test. He is a co-author of the book Counterfeit Integrated Circuits: Detection and Avoidance (Springer, 2015), and was involved in developing a web-based tool, Counterfeit Defect Coverage Tool (CDC Tool), www.sae.org/standardsdev/cdctool/

Navid Asadizanjani received his PhD degree in Mechanical Engineering from the University of Connecticut. He is currently an assistant professor in the Electrical and Computer Engineering Department at the University of Florida, Gainesville, FL. His current research interest is primarily on physical attacks and inspection of electronics. This includes a wide range of products from electronic systems to devices.

Mark M. Tehranipoor is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity at the University of Florida, Gainesville, FL. His research projects include hardware security and trust, supply chain security, VLSI design, test and reliability. He has published more than 400 journal articles and refereed conference papers. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), and is currently serving as a founding EIC for the Journal on Hardware and Systems Security (HaSS) and associate editor for JETTA, JOLPE, IEEE TVLSI and ACM TODAES. He is a Fellow of the IEEE, and a Member of ACM and ACM SIGDA.

REFERENCES

[1] "The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain," Committee on Armed Services United States Senate, 2011. https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/pdf/CHRG-112shrg72702.pdf

[2] "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," U.S. Senate Committee on Armed Services Press Release, 2012. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

[3] R. McCormack, "Boeing's planes are riddled with chinese counterfeit electronic components," *Manufacturing and Technology News*, Vol. 19, June 2012.

[4] T. Kaiser, "SAS committee: Counterfeit electronics from China could be harmful to military," Online, *DailyTech*, November 2011.

[5] "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," https://technology.ihs.com/405654/top-5-most-counterfeited-parts-represent-a-169-billion-potential-challenge-for-global-semiconductor-market IHS iSuppli, 2011.4

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

[7] "National Defense Authorization Act (NDAA) for Fiscal Year 2012," 2012. Public Law 112-81, 112th Congress. https://www.congress.gov/112/plaws/publ81/PLAW-112publ81.pdf

[8] "Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts-Further Implementation (DFARS Case 2014-D005)," 2016. https://www.federalregister.gov/documents/2016/08/02/2016-17956/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic

[9] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead", *Journal of Electronic Testing: Theory and Applications (JETTA)*, 2014.

[10] U. Guin, D. DiMase, and M. Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment", *Journal of Electronic Testing: Theory and Applications (JETTA)*, 2014.

[11] "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice," U.S. Dept. of Justice https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade

[12] "Copyrights and patents, piracy and theft," The Washington Times. https://www.washingtontimes.com/news/2018/apr/24/copyrights-and-patents-piracy-and-theft/

[13] "2017 Special 301 Report," Office of the United States Trade Representative, 2017. https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF

[14] J. H. McQuade and D. M. S. Fassbender, "Senate Judiciary Committee Creates IP Subcommittee to Combat IP Theft," *Mondaq*. http://www.mondaq.com/unitedstates/x/781874/Trademark/

[15] 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.

[16] A. Chhotaray, A. Nahiyan, T. Shrimpton, D. Forte, and M. Tehranipoor. "Standardizing bad cryptographic practice: A teardown of the IEEE standard for protecting electronic-design intellectual property." In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1533-1546. ACM, 2017.