J Electron Test
DOI 10.1007/s10836-013-5430-8

Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead

Ujjwal Guin · Daniel DiMase · Mohammad Tehranipoor

Received: 6 August 2013 / Accepted: 19 December 2013

Abstract The counterfeiting of electronic components has become a major challenge in the 21st century. The electronic component supply chain has been greatly affected by widespread counterfeit incidents. A specialized service of testing, detection, and avoidance must be created to tackle the worldwide outbreak of counterfeit integrated circuits (ICs). So far, there are standards and programs in place for outlining the testing, documenting, and reporting procedures. However, there is not yet enough research addressing the detection and avoidance of such counterfeit parts. In this paper we will present, in detail, all types of counterfeits, the defects present in them, and their detection methods. We will then describe the challenges to implementing these test methods and to their effectiveness. We will present several anti-counterfeit measures to prevent this widespread counterfeiting, and we also consider the effectiveness and limitations of these anti-counterfeiting techniques.

Keywords Counterfeit ICs · Counterfeit detection and avoidance · Electronic component supply chain

Responsible Editor: M. Hsiao

U. Guin · M. Tehranipoor (✉)
ECE Department, University of Connecticut,
Storrs, CT 06269, USA
e-mail: tehrani@engr.uconn.edu

U. Guin
e-mail: ujjwal@engr.uconn.edu

D. DiMase
Honeywell Inc., Morristown, NJ, USA
e-mail: Daniel.DiMase@Honeywell.com

1 Counterfeit ICs: The Problem

Counterfeiting and piracy are longstanding problems growing in scope and magnitude. They are of great concern to government and industry because of (i) the negative impact they can have on innovation, economic growth, and employment, (ii) the threat they pose to the welfare of consumers, (iii) the substantial resources that they channel into criminal networks, organized crime, and other groups that disrupt and corrupt society, and finally, (iv) the loss of business from the trade in counterfeits [53]. Based on a 2008 report by the International Chamber of Commerce, it was estimated that the cost of counterfeiting and piracy for G20 nations was as much as US$775 billion every year and will grow to $1.7 trillion in 2015 [10].

Innovation in the business sector has always been the main driver of economic growth, through the development and implementation of ideas for new products and processes. These inventions are usually protected via patents, copyrights, and trademarks. However, without adequate protection of these intellectual property (IP) rights, the incentives to develop these new ideas and products would be considerably reduced, thereby weakening critical thinking and the innovation process [53]. These risks are particularly high for those industries in which the research and development (R&D) costs associated with the development of new products are very high compared to the cost of producing the resulting products. In the world of electronics, the R&D costs for the semiconductor industry are indeed extremely high, and protection of their IP rights is of the utmost importance.

Counterfeiting of integrated circuits has become a major challenge due to deficiencies in the existing test solutions and lack of effective avoidance mechanisms in place. Over the past couple of years, numerous reports [69] have pointed

Published online: 12 February 2014

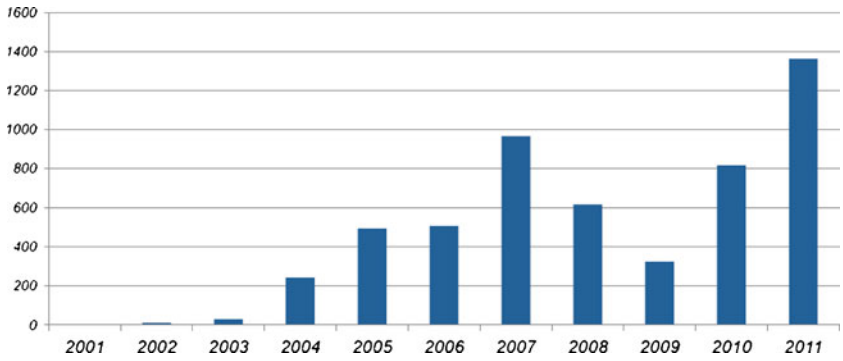

Fig. 1 Counterfeit incidents reported by IHS [7]

to the counterfeiting issues in the US electronics component supply chain. A Senate Armed Services public hearing on this issue and its later report clearly identified this as a major issue to address because of its significant impact on reliability and security of electronic systems [74, 75].

As the complexity of the electronic systems, along with the ICs used in them, has increased significantly over the past few decades, they are assembled (fabricated) globally to reduce the production cost. For example, large foundries located in different countries can offer lower prices to the design houses. This globalization leads to an illicit market willing to undercut the competition with counterfeit parts. If these parts end up in critical applications like defense, aerospace, or medical systems, the results could be catastrophic [71].

Just how big the market is remains a mystery. A study conducted from 2005–2007 reveals that 50 % of original component manufacturers (OCM) and 55 % of distributors (authorized and unauthorized) have encountered counterfeit parts [70]. The Electronic Resellers Association International [19] monitors, investigates, and reports issues that are affecting the global supply chain of electronics. ERAI, in combination with Information Handling Services Inc. [34], has been monitoring and reporting counterfeit component statistics dating back to 2001. The most recent data (Fig. 1) provided by IHS shows that reports of counterfeit parts have quadrupled since 2009.

With counterfeit incidents on the rise, it is increasingly important to analyze the vulnerabilities of the electronic component supply chain. Table 1 shows the five most commonly counterfeited components according to percentage of reported counterfeit incidents. They are as follows: analog ICs, microprocessor ICs, memory ICs, programmable logic ICs, and transistors. Together, these five component groups contribute around 68 %, slightly more than two-thirds, of all counterfeit incidents reported in 2011. Note that in this paper, we will use parts and components interchangeably to refer to semiconductor devices.

This steady increase of reported incidents reflects the need for effective methods of testing parts and for maintaining proper records as parts travel through the supply chain. There are a handful of standards that seek to do just this, with more being written and revised. The group responsible for many of these standards is the G-19 Counterfeit Electronic Parts Committee, set forth by SAE International [59]. Their standards target three different sectors of the industry: distributors, users, and test service providers (i.e., test laboratories). A collection of the standards that they have written or are currently working on is as follows: (i) $AS6081$ - Counterfeit Electronic Parts Avoidance, Distributors, (ii) $ARP6178$ - Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors, Distributors & Users, (iii) $AS5553$ - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, Users, and (iv) $AS6171$ - Test Methods Standard; Counterfeit Electronic Parts, Test Providers.

While SAE is the most prominent entity when it comes to standards, there are a couple of programs designed to help independent distributors gain customers' trust. Components Technology Institute, Inc. (CTI) [13] has created the Counterfeit Components Avoidance Program (CCAP-101) [15]. Independent distributors can be certified as CCAP-101 compliant, done by means of a yearly audit. Another program with similar goals has been developed by the Independent Distributors of Electronics Association (IDEA) [33]. A comparison of the SAE's AS5553, CTI's CCAP-101, and IDEA's STD-1010 is available in [14]. The main issue with many of these standards is that the "policy" and the

Table 1 Top-5 most counterfeited semiconductors in 2011 (Percentage of counterfeit part reports)

Rank	Commodity type	% of reported incidents
#1	Analog IC	25.2 %
#2	Microprocessor IC	13.4 %
#3	Memory IC	13.1 %
#4	Programmable logic IC	8.3 %
#5	Transistor	7.6 %
#6	Others	32.4 %

[1]Source: IHS parts management 2012 [35]

"regulations" are their main focus rather than the "technology". Thus it is easy for counterfeiters to adapt to the new regulations circumventing effective detection of counterfeit parts.

Detection and avoidance of counterfeit components are difficult challenges, partly because there are such a wide variety of counterfeit types impacting the supply chain. It is of the utmost importance to develop a taxonomy of defects and anomalies present in counterfeit components, to enable detection of these components with a group of test methods. In this paper, we have developed a comprehensive taxonomy of counterfeit types, defects and test methods. Our contributions include the development of:

(*i*) *Taxonomy of counterfeit types*: We develop a taxonomy of counterfeit types to analyze supply chain vulnerabilities.

(*ii*) *Taxonomy of counterfeit defects*: We develop a detailed taxonomy of the defects present in counterfeit ICs. To the best of our knowledge, this is the first approach to analyzing counterfeit components based on their defects and anomalies. This list of defects and anomalies is based on our detailed analysis of numerous counterfeit parts in collaboration with SAE G-19A, Test Laboratory Standards Development Subcommittee [58].

(*iii*) *Taxonomy of counterfeit detection methods*: Our counterfeit methods taxonomy describes all the test methods currently available for counterfeit detection. Test methods for counterfeit detection primarily target all the counterfeit parts already on the market (known as obsolete and active parts).

(*iv*) *Taxonomy of counterfeit avoidance methods*: The taxonomy of avoidance methods addresses how to prevent counterfeit parts from entering into supply chain and to identify counterfeit parts without performing the costly and time consuming detection methods.

The rest of the paper is organized as follows. In Section 2, we will describe different types of counterfeits and how they infiltrate the electronic component supply chain. Section 3 will present a detailed taxonomy of counterfeit defects. In Section 4, we will describe the taxonomy of counterfeit detection methods. The counterfeit avoidance techniques will be presented in Section 5. We will then discuss challenges to the implementation of current counterfeit detection and avoidance technologies. We will conclude the paper in Section 7.

2 Electronic Component Supply Chain Vulnerabilities

2.1 Counterfeit Types

A counterfeit component (*i*) is an unauthorized copy; (*ii*) does not conform to original OCM design, model, and/or performance standards; (*iii*) is not produced by the OCM or is produced by unauthorized contractors; (*iv*) is an off-specification, defective, or used OCM product sold as "new" or working; or (*v*) has incorrect or false markings and/or documentation [70]. Based on the definitions above and analyzing supply chain vulnerabilities, we classify the counterfeit types into seven distinct categories [25, 26, 28, 29] shown in Fig. 2.

1) **Recycled**: The most widely discussed counterfeit types at the present time are the recycled and remarked types. It is reported that in today's supply chain, more than 80 % of counterfeit components are recycled and remarked [38]. In the United States, only 25 % of electronic waste was properly recycled in 2009 [73]. That percentage might be lower for many other countries. This huge resource of e-waste allows counterfeiters to pile up an extremely large supply of counterfeit components. The components become recycled when they are taken from a used system, repackaged and remarked, and then sold in the market as new. These recycled parts either may be non-functioning or prior usage may have done significant damage to the part's life or performance.

2) **Remarked**: In remarking, the counterfeiters remove the old marking on the package (or even on the die) and mark them again with forged information. During the remarking process, the components' packages are sanded or ground down to remove old markings (part number, date code, country of origin, etc.). Then, to cover the sanding or grinding marks, a new coating is created and applied to the component. Components can also be remarked to obtain a higher specification than they are rated for by the original component manufacturer (OCM), e.g., from commercial grade to industrial or defense grade.

3) **Overproduced**: Today's high-density integrated circuits are mostly manufactured in state-of-art fabrication facilities. Building or maintaining such facilities for the present CMOS technology is reported to cost more than several billion dollars and this number is growing [51]. Given this increasing cost and the complexity of foundries and their processes, the semiconductor business has largely shifted to a contract foundry business model (horizontal business model) over the past two decades. This is also true for the assembly where the dies are packaged,

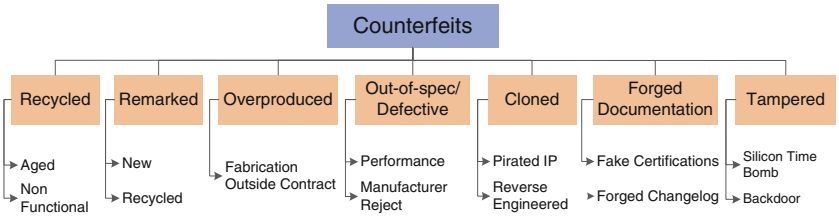

Fig. 2 Taxonomy of counterfeit types

tested, and shipped to the market. Any untrusted foundry/assembly that has access to a designer's IP, also has the ability to fabricate ICs outside of contract. They can easily sell excess ICs on the open market.

4) **Out-of-Spec/Defective**: The other variation of an untrusted foundry/assembly sourcing counterfeit components is out of specification or rejected components. They may either knowingly sell these components, or the components may be stolen and sold on open markets. During manufacturing tests, a component is considered defective if it produces an incorrect response to even one test vector. Sometimes, the probability of activating a component's defective node is extremely small. If these components make their way into the supply chain, detection will be extremely difficult as they produce correct responses in most of the test cases. These components can pose a serious threat to the quality and reliability of a system.
5) **Cloned**: Cloning is commonly used by a wide variety of adversaries/counterfeiters (from small entity to large corporation) to copy a design in order to reduce the large development cost of a component. A cloned component is an unauthorized production without a legal IP. Cloning can be done in two ways – by reverse engineering, and by obtaining IPs illegally. In reverse engineering, counterfeiters copy designs and then manufacture (fabricate) components which are the exact copy of their original counterpart. Sometimes cloning can be done by copying the – contents of a memory used in a tag for electronic chip ID, bitstream targeted to programmable gate arrays, etc.
6) **Forged Documentation**: Forged documentation may include certifications of compliance for some standards or programs, or a revision history or change-log of a component. Archived documentation for older designs and older parts may not be available at the OCM, making it difficult to verify their authenticity. In addition, many organizations have merged or have been acquired over the years, and information is often lost in the transition.
7) **Tampered**: Tampering can be done during any phase of the life cycle of a component. It can either be on the die level ("hardware Trojan") or package level. Such components can either act as a silicon time bomb where the device can behave differently under certain conditions or act as a backdoor where secret information from the chip can be sent out to an adversary. In both cases, the chip behaves outside of its specification, and thus we have included such ICs as counterfeit parts. A detailed taxonomy for tampering a device by hardware Trojans can be found in [68].

2.2 Supply Chain Vulnerability

Typically an electronic component will go through a process shown in Fig. 3. This process includes design, fabrication, assembly, distribution, usage in the system, and finally end of life. As seen, there are vulnerabilities associated with each step in this supply chain. In design stage, an IP may be stolen or a hardware Trojan may be inserted into the design. An untrusted foundry or assembly can insert a hardware Trojan or produce different types of counterfeits. The design house can use illegally obtained IPs in their designs. Overproduced and out-of-spec/defective parts can be entered into the supply chain in the fabrication stage. Untrusted foundries can potentially sell these parts in the open market. They can also tamper with the design to create a backdoor for getting secret information from the field.

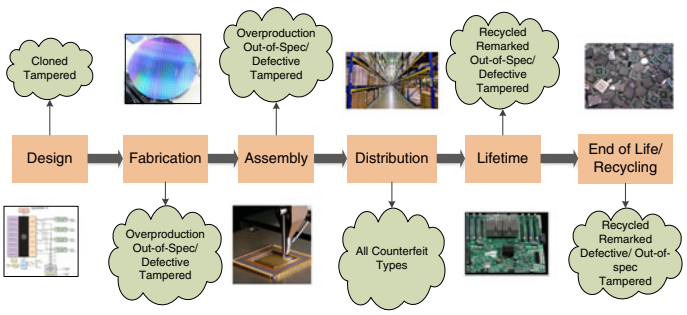

Fig. 3 Electronic components supply chain vulnerabilities

These parts also get into the supply chain in the assembly phase. An untrusted assembly can possibly sell these parts or tamper the designs. Illegal activities during distribution, in-the-system (lifetime), and end-of-life may bring different types of counterfeits back into the supply chain (recycled, remarked, etc.).

3 Counterfeit Defects

The detection of counterfeit components is a multifaceted problem. Different types of components (analog, digital, etc.) and counterfeits (discussed in Section 2.1) impact the detection results. Some counterfeits are easier to detect than others and some components are easier to test than others. To address this, it is of the utmost importance to develop a taxonomy of defects and anomalies present in the counterfeit components. By ensuring the detection of one or more defects, one can confidently detect counterfeit components. A counterfeit part may present anomalies on the leads/package, degradation in its performance, or a change in specification. Since we assume, the components are comprehensively tested by the assembly, any such anomalies and defective behavior by them can be attributed to being counterfeit. Figure 4 presents the classification of the defects present in the counterfeit components.

3.1 Physical Defects

Physical defects are directly related to the physical properties of the components. They can be classified as exterior and interior defects, depending on the location of the defects related to the packaging.

Exterior defects are related to packaging/shipping, leads/balls/columns, and package of a component. The most obvious defects will be ones that are associated with the packaging or shipping the parts arrived in. The leads/balls/columns of an IC can show how the part has been handled if it was previously used. Physically, they should adhere to datasheet specifications, including size and shape. The final coating on the leads should conform to the specification sheet. The package of an IC can reveal significant information about the chip. As this is the location where all model numbers, country of origin, date codes, and other information are etched, counterfeiters will try to be

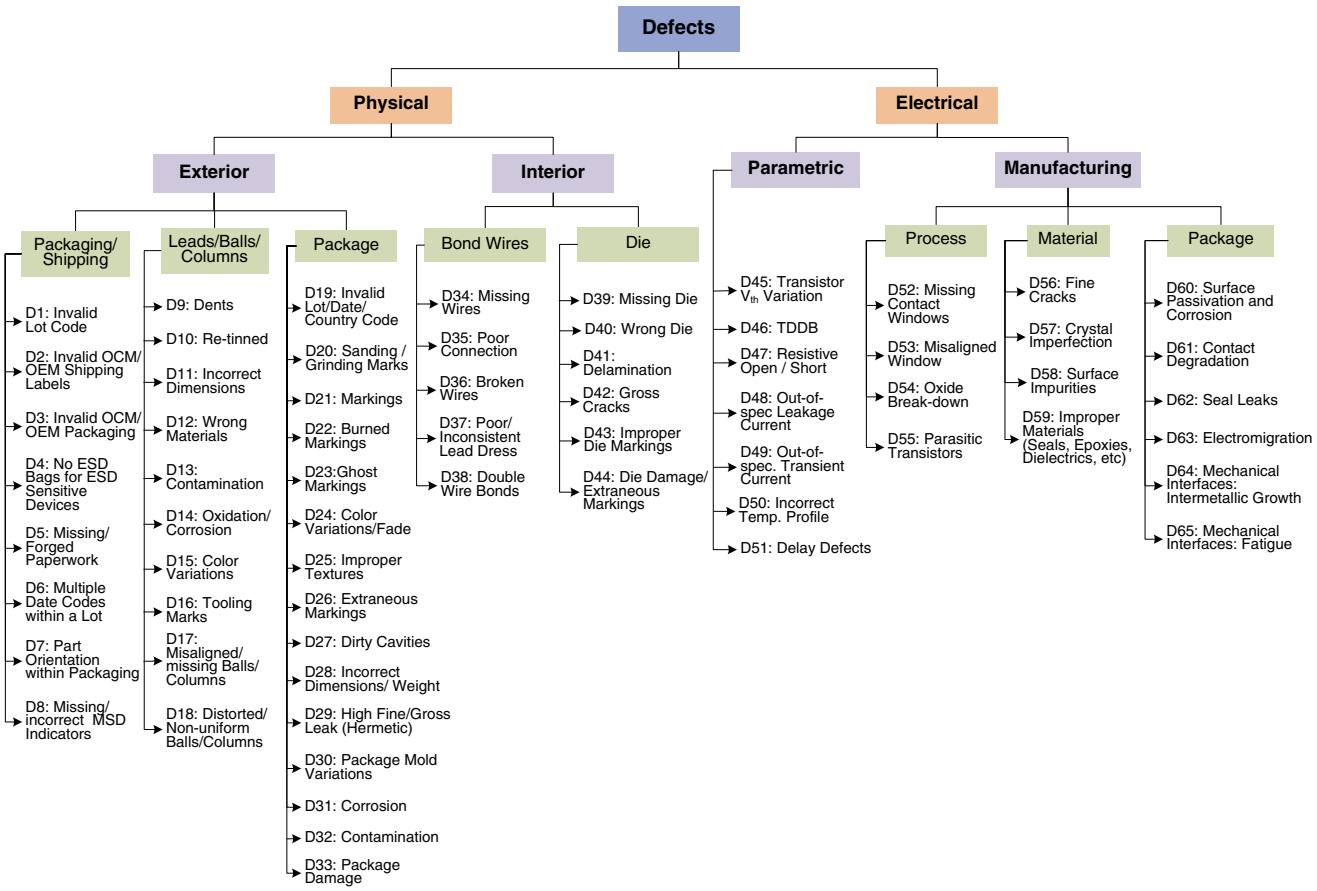

Fig. 4 A taxonomy of defects in counterfeit components

especially careful not to damage anything and to keep the package looking as authentic as possible.

Interior defects are mainly divided into two types: bond wire and die-related defects. Some common defects related to bond wires are missing/broken bond wires inside the package, a poor connection between the die and bond wire, etc. The die reveals a significant amount of relevant information regarding the component. Die-related defects include die markings, cracks, etc.

3.2 Electrical Defects

Typical electrical defects can be classified into two distinct categories, namely parametric defects and manufacturing defects. Parametric defects are shifts in component parameters due to prior usage or temperature. A shift in circuit parameters due to aging will occur when a chip is used in the field for some time. Manufacturing defects come from the fabrication process of components and are classified into three categories – process, material, and package. The defects under the process category come from the photolithography and etching processes during the fabrication. The defects related to material arise from impurities within the silicon or oxide layers. The passivation layer provides some form of protection for the die, but failure occurs when corrosion causes cracks or pin holes. The aluminum layer can easily be contaminated with the presence of sodium and chloride and results in an resistive open defect.

4 Counterfeit Detection Methods

It has become necessary for manufacturers, distributors, and users of electronic components to inspect all incoming electronic components for authenticity, especially with parts purchased outside of OCM-authorized distributors. It is absolutely necessary to analyze the current counterfeit detection methods for the inspection of such parts. In this section, we will describe these detection methods in detail. Figure 5 shows the detailed taxonomy of such methods.

4.1 Physical Inspections

Physical inspections are performed to examine the physical and chemical/material properties of the component's package, leads and die of a component mostly to detect the physical counterfeit defects (Section 3.1).

1) **Incoming Inspection**: When an order is received, it first goes through the incoming inspection. All the components under test (CUTs) are inspected thoroughly. In *low power visual inspection (LPVI)*, all the CUTs are strictly documented and inspected. LPVI requires a low power microscope (generally less than 10X magnification) to inspect the exterior of the CUT. The markings on genuine components tend to be clear and identical. The internal structure of the CUTs are analyzed using *X-Ray imaging*. If a known good component (golden model) is available, one can compare the images taken from the CUT with this golden model.
2) **Exterior Test**: The exterior part of the package and leads of the CUT are being analyzed by using exterior tests. In *package configuration and dimension analysis*, the physical dimensions of the CUTs are measured either by hand-held or automated test equipment. Any abnormal deviation of measurement from the specification sheet indicates that the CUT may be counterfeit. *Blacktop testing* is the procedure of testing the marking permanency of a CUT with various solvents. A non-epoxy blacktop coating should be dissolved in acetone, while a thermal or UV-cured epoxy will require the use of a much more aggressive solvent [45]. *Microblasting analysis* is a dry and superfine blasting process. Various blasting agents with proper grain sizes are bombarded on the surface (package) of the CUT, and the materials are collected for analysis. Some common blasting agents are aluminum oxide powder, glass beads, sodium bicarbonate powder, etc. *Hermiticity testing* is a special type of package analysis specific to hermetically sealed parts that tests the hermetic seal. The seal on such components ensures its correct operation in the environment that it was designed for. A break in this seal leads to the failure of the component. *Scanning acoustic microscopy (SAM)* is one of the most efficient, though expensive, ways of studying the structure of a component. This technology functions by using the reflection or the transmission of ultrasound waves to generate an image of the component based on its acoustic impedance at various depths. This is very useful in detecting delamination [37]. Cracks and voids in the die will also be detectable, as well as the structure of bond wires.
3) **Interior Test**: The internal structures, die and bond wires, of the CUTs are inspected by delid/decapsulation. There are three mainstream methods commercially available for decapsulation. These are chemical, mechanical, or laser-based products. Chemical decapsulation involves etching away the package with an acid solution. Newer laser-based techniques can remove an area of the package. Mechanical decapsulation involves grinding the part until the die is exposed. Once the part has been decapsulated and the required structures exposed, the following tests need to be performed:

   In *optical inspection*, all the related information regarding die and bond wires are properly documented.

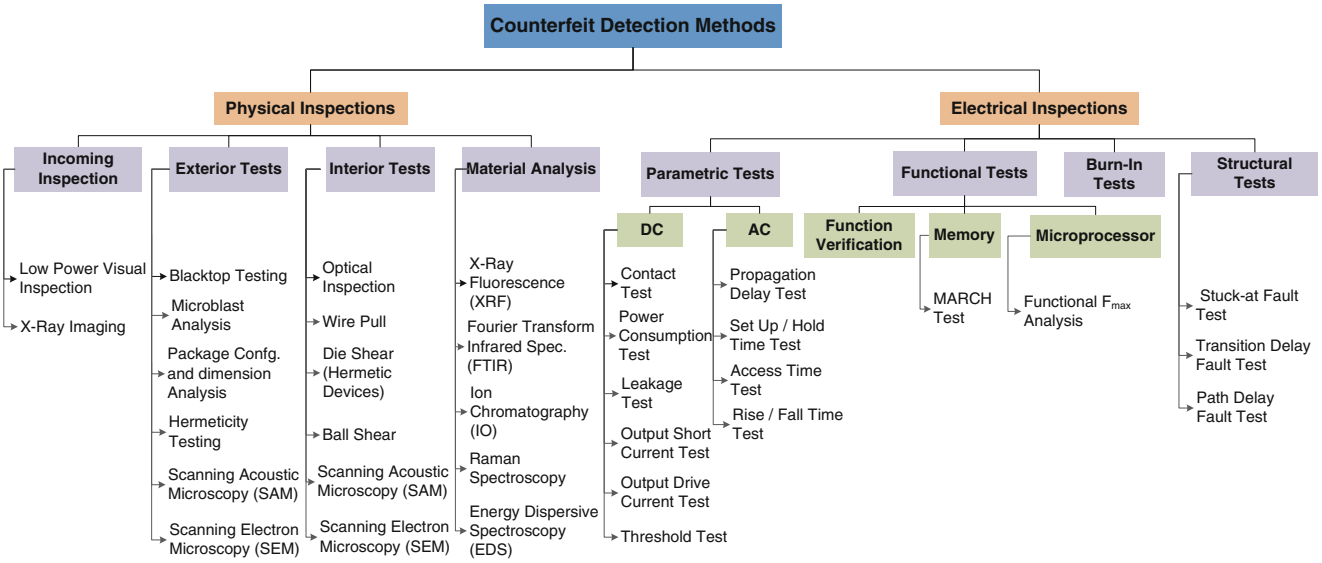

Fig. 5 A taxonomy of counterfeit detection methods

The relevant information regarding die markings (company logo, date code, chip ID, country of manufacturer, etc.), bond wire positions, bond types, etc. are to be documented. The integrity of the bonds with the die is tested using *wire pull*. The adhesiveness between die and bond wires degrades with time if the component is in the field. Comparison of the tension (pulling force) with the golden and test components determines whether it was used before or not. In *die shear*, die attach integrity is verified. This test is applicable to hermitic devices only. A *ball shear* test is applied to verify the ball bond integrity at the die. In *scanning electron microscopy (SEM)*, the images of die, package, or leads are taken by scanning it with a focused beam of electrons. If there is an anomaly present in it, it can easily be detected by SEM. It has an effective resolution up to a few nanometers which refers that the die can be analyzed down to its gate level. This is useful for a thorough analysis of the die.

4) **Material Analysis**: The chemical composition of the CUT is verified using material analysis. This is the only category of tests that can detect defects and anomalies related to materials. Defects such as wrong materials, contamination, oxidation of leads and packages, etc., can be detected. There are several tests that can perform material analysis. Some of the most popular tests are X-Ray fluorescence (XRF), fourier transform infrared spectroscopy(FTIR), ion chromatography (IO), Raman spectroscopy, and energy-dispersive X-ray spectroscopy (EDS).

4.2 Electrical Inspections

In this section, we will discuss various manufacturing tests suitable for detecting the defects and anomalies discussed in Section 3.2. An automatic test equipment (ATE) [23] may be required for some of these tests.

1) **Parametric Tests**: Parametric tests are performed to measure the parameters of a chip [52, 63]. If the chip has been used before, the DC and AC parameters may shift from their specified value (mentioned on the datasheet). After observing test results from a parametric test, a decision can be made as to whether or not a component is counterfeit. In *DC parametric tests*, the parametric measurement unit (PMU) of an ATE forces an I/O voltage and current to a steady state and measures the electrical parameters using Ohm's law. The operating conditions are set carefully during measurement. The DC parametric tests can be classified in different categories - contact test, power consumption test, output short current test, output drive current test, threshold test, etc. Detailed descriptions of each test can be found in [6]. In *AC parametric tests*, the measurement of AC parameters (terminal impedance, timing, etc.) is performed by using AC voltages with a set of frequencies. AC parametric tests can be classified as follows: rise and fall time tests, set-up, hold and release time tests, propagation delay tests, etc. A different set of parametric tests can also be applied to memories, as in [48]. DC parametric tests include voltage bump test, leakage tests, etc. AC parametric tests include set-up time sensitivity test, access time test, running time test, etc.

2) **Functional Tests**: Functional tests are the most efficient way of verifying the functionality of a component. A majority of the defects from the defect taxonomy (Fig. 4) can be detected by these tests. Any defects that impacts the functionality (from some easy defects such as missing or broken bond wires, missing or wrong dies, etc., to hard to detect defects related to process, material, and package) can be detected. In *function verification*, the functionality of a component is verified. It determines whether individual components, possibly designed with different technologies, function as a system and produce the expected response. In *memory tests*, read/write operations are performed on a memory to verify its functionality. MARCH tests [6, 48, 67] can be applied for counterfeit detection. Since the functions of memories are simple, exhaustive functional testing is possible and is normally used during manufacturing testing [6].
3) **Burn-In Test**: The reliability of a device is mainly ensured by burn-in [36]. In burn-in, the device is operated at an elevated temperature to simulate a stress condition in order to find infant mortality failures and unexpected failures, to assure reliability. Burn-in test methods are described in MIL-STD-883 for integrated circuits and MIL-STD-750 for other discrete components [16, 17]. The implementation of burn-in is very important as it can easily weed out the commercial grade components marked as military grade. It can also remove defective components or those components that were not designed to perform under these stress conditions.
4) **Structural Tests**: Over the past decade, there has been a major shift toward using structural tests [18, 20, 55, 62] to reduce the overall cost of manufacturing tests. Structural tests are very effective in detecting manufacturing defects (discussed in Section 3.2) for out-of-spec/defective counterfeit types. They can detect the cloned (reversed engineered) counterfeit components if there are some anomalies in the reverse engineering process. If the cloned netlist does not match with the genuine netlist for even few gates, some of the structural test vectors will produce an incorrect response and the CUT will be flagged as defective. It can also detect some of the delay defects due to aging in recycled and remarked counterfeit types.

5 Counterfeit Avoidance Methods

The avoidance of counterfeit components from entering the supply chain is a major challenge. One must consider all types of components, namely obsolete, active, and new while implementing anti-counterfeit measures. New mechanisms can be put in place during the design of new chips that could help to prevent counterfeiting. As obsolete parts are no longer being manufactured, and active parts are being fabricated based on previous designs and developed masks, the focus should be on the detection of such counterfeit components and the implementation of avoidance measures at the package level. As we described earlier, at this point, all the standards are in place simply for detection. In this section, we will briefly discuss various anti-counterfeit measures that can be implemented for new, active, and obsolete parts. Figure 6 shows the taxonomy of such anti-counterfeit measures.

5.1 Chip ID

Techniques to generate chip IDs are based on extracting unique features and parameters from a circuit to help uniquely identify each chip or embedding a unique ID into the chip during or after fabrication and test. They are described in the following:

1) **Physically Unclonable Functions**: PUFs have received much attention from the hardware security and cryptography communities as a new approach for IC identification, authentication, and on-chip key generation [5, 42, 43, 54, 64]. Silicon PUFs exploit inherent physical variations (process variations) that exist in modern integrated circuits. These variations are uncontrollable and unpredictable, making PUFs suitable for IC identification and authentication [1, 76]. These variations can help generate a unique signature for each IC in a challenge-response form, which allows later identification of genuine ICs. In recent years, various PUF architectures have been proposed. They are the arbiter PUF [21, 65], the ring oscillator PUF [21, 64], the SRAM PUF [24], etc.

PUFs can be used to detect cloned ICs as they generate unique IDs resulting from randomness in the IC

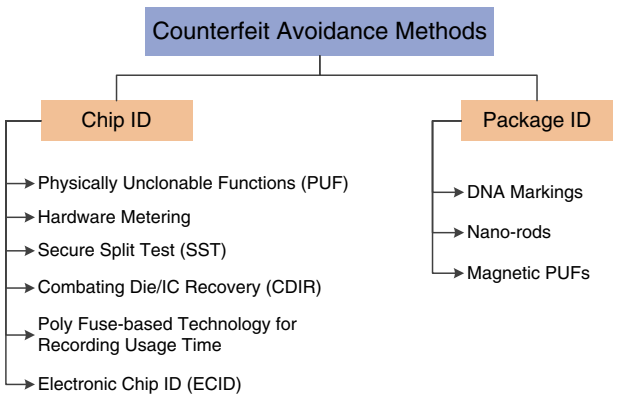

Fig. 6 A taxonomy of counterfeit avoidance techniques

manufacturing process that cannot be controlled or cloned. These unique IDs of the genuine ICs can be stored in a secured database for future comparison. Overproduced ICs can also be detected, by searching the chip IDs under authentication in these secured databases. If no match is found, there is a high probability that the IC is not registered and is a member of an overproduced type.

2) **Hardware Metering**: Hardware metering is a set of security protocols that enables the design house to achieve post-fabrication control of the produced ICs. The design house can distinguish different ICs produced with the same masks, as hardware metering provides a unique way to tag each chip and/or its functionality [39, 40]. Hardware metering approaches can be either passive or active. Passive approaches uniquely identify each IC and register the IC using challenge-response pairs. Later, suspect ICs taken from the market are checked for proper registration [39, 42, 46, 47, 64, 66]. Active metering approaches, however, lock each IC until it is unlocked by the IP holder [1, 2, 4, 8, 32, 57]. This locking is done in a variety of ways, including: (*i*) initializing ICs to a locked state on power-up [1], (*ii*) combinational locking by, for instance, scattering XOR gates randomly throughout the design [4, 32, 57], and (*iii*) adding a finite-state machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs [2, 9].

Figure 7 shows the design flow of hardware metering. The design house uses the high level design description to identify the best places to insert a lock. The design then passes subsequent design phases – synthesis, place, and route. The foundry receives the blueprint of the chip in the form of OASIS or GDSII files to fabricate the ICs. After manufacturing, the foundry scans the unique ID from each IC and sends it back to the design house. The design house then sends the unlock key to the foundry to unlock the IC. In this process, the design house keeps track of the number of activated ICs, which helps to prevent overproduction.

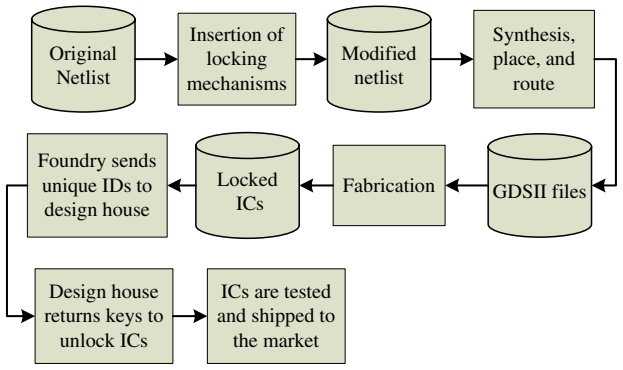

Fig. 7 IC enabling flow by active metering

3) **Secure Split Test**: Due to the globalization of the semiconductor industry and the prohibitively high cost of creating foundries and assembly companies for packaging, test, and burn-in processes, foundries now often fabricate the wafers/dies, test them, and ship them to the assembly. The assembly then packages the dies, tests them, and ships the ICs to the market. The foundry/assembly, however, can ship defective, out-of-spec, or even overproduced chips to the black market, as described in Section 2.1. Secure Split-Test (SST) secures the manufacturing test process to prevent counterfeits, allowing intellectual property (IP) owners to protect and meter their IPs [12]. SST introduces hardware components for cryptography and to block the correct functionality of an IC until it is activated by the IP owner. SST is designed to be resilient against different types of attacks to prevent the IC from being activated without IP owner's key. SST introduces the IP owner back into the manufacturing test process. SST is designed to prevent different types of counterfeited ICs such as cloned, overproduced, defective/out-of-spec ICs.

4) **Combating Die / IC Recovery (CDIR)**: The first CDIR to preventing parts from recycling has been presented in [79]. The technique in [79] inserts a lightweight sensor in the chip to capture the usage of the chip in the field and provides an easy detection capability. This type of sensor relies on the aging effects of MOSFETs to change a ring oscillator frequency in comparison with the golden one embedded in the chip. As a part used in the field ages because of the wearout mechanisms such as NBTI and HCI, the shift in the frequency of this sensor indicates the level of aging and provides a simple readout of the value.

5) **Poly Fuse-Based Technology for Recording Usage Time**: The antifuse-based sensor was first proposed for recycled IC detection [78]. It is composed of counters and an embedded antifuse memory block. The counters are used to record the usage time of ICs while its value is continuously stored in an antifuse memory block. Since the antifuse memory block is one-time programmable, counterfeiters cannot erase the context during the recycling process. Two different structures of the AF-based sensor have been proposed to measure the usage time of ICs. *CAF-based sensor* records the cycle count of the system clock during chip operation. The usage time of recycled ICs can be reported by this sensor, and the measurement scale and total measurement time could be adjusted according to the application of ICs. On the other hand, *SAF-based sensor* uses circuit activity as the trigger (clock) to the

counter. A number of signals with low switching probability are selected to calculate the usage time. This sensor generally requires less area overhead than the CAF-based sensor.

6) **Electronic Chip ID (ECID)**: To track ICs throughout the supply chain, each IC can be tagged with a unique ID. This ID can be easily read during the chip's lifetime. The conventional approach for writing the unique ID into a non-programmable memory (such as One-Time-Programmable [OTP], ROM, etc.) require post-fabrication external programming, such as laser fuses [3] or electrical fuses (eFuses) [56]. The eFuse is gaining popularity over laser fuses because of its small area and scalability [56].

5.2 Package ID

The anti-counterfeit avoidance measures discussed so far only target new ICs. However, a large portion of the supply chain is populated by active and obsolete components. There is no opportunity for adding any extra hardware to create a chip ID in those designs. For tagging such active and obsolete components, we need to create package IDs that do not require access to designs. No package modifications are allowed during the generation of package IDs. These IDs can be used for new components as well. DNA markings, nanorods, and magnetic PUFs are the viable options for creating package IDs.

1) **DNA Markings**: Plant DNA is scrambled to create new and unique genetic sequences, and these sequences of DNA are integrated with inks. These inks are then applied on the packages of the IC at the end of the packaging process. Once the ICs are received, then, authentication includes first checking whether the ink fluoresces under specific light, and second, sending a sample of the ink to a lab to verify that the DNA is in the database of valid sequences [49]. Recently, the DOD mandated [72] that DNA marking be placed on the components in order to track them throughout the supply chain. DNA markings have several limitations that introduce some serious concerns of their applicability in counterfeit avoidance. The fast authentication achieved by observing the fluorescence of the marking under specific light can be imitated by counterfeiters, either with invalid DNA or other materials. But detailed DNA validation is extremely time-consuming and costly [61].
2) **Nanorods**: In this technique, a microscopic pattern is created by growing an array of nanospheres into nanorods that are less than 100nm long [41]. Each time the process is repeated, the same pattern is created, but the exact angle and length of each individual nano-rod varies, so that each set of nanorods is distinct. After the array of nanorods is grown, it is applied to a chip using a specialized printer. The chip can be authenticated by comparing the overall pattern and visual properties of each nano-rod to a database.
3) **Magnetic PUFs**: A magnetic PUF uses the inherent characteristics of magnetic stripes for unique identification [30, 50]. Each magnetic stripe, due to the randomness of the creation process, has a noise-like component along with the data that is stored. This noise is unpredictable and difficult to clone, yet is consistent and repeatable, therefore acting as a PUF.

6 Detection and Avoidance Challenges

We believe that research in the detection and avoidance of counterfeit electronic components is still in its infancy. There are major challenges that must be overcome in the development of effective test methods. In this section, we will discuss the counterfeit detection and avoidance challenges that must be overcome in the near future.

6.1 Detection Challenges

The counterfeit detection standards [15, 33, 60] guide us to segregate the counterfeit components by recommending a set of detection methods. However, all these standards deal mainly with two types of counterfeits – recycled and remarked. In addition, they focus on existing test techniques which have proven to be ineffective as counterfeiters continuously improve their own skills and techniques. Further, there are currently no simple methods to verify components as genuine if they belong to the overproduced, cloned, or tampered categories. In the following, we will briefly discuss the implementation challenges of counterfeit detection methods.

1) **Physical Inspections**: Physical methods generally entail the inspection of the physical structure and the material analysis of a component. The major challenges for the implementation of physical inspections are:
   - (*i*) *Sampling*: Most of the physical tests are destructive. Sample preparation is extremely important as it directly relates to test confidence. If a few counterfeit components are mixed with a large batch, the probability of selecting the counterfeit one for test is extremely small.
   - (*ii*) *Test Time and Cost*: The test time and cost are major limiting factors in the use of physical tests for counterfeit detection. The equipment

used for physical inspections (e.g., scanning electron and acoustic microscopy [SEM or SAM]) are not custom-designed to detect counterfeit parts. It takes several hours (e.g., typically more than 8 hours for SEM analysis) to test a single component with good resolution.

(*iii*) *Automation*: These tests are done in an ad-hoc fashion with no metrics for quantifying against a set of counterfeit types, anomalies, and defects. Most of the tests are carried out without automation.

(*iv*) *Metrics*: Currently, there are no metrics to evaluate the effectiveness of physical inspections. The test results mostly depend on the subject matter experts (SMEs). The decision-making process is entirely dependent on the operator (or SMEs) – this is indeed error prone. A chip could be considered counterfeit in one lab while it could be marked as authentic in another lab. This was proven by a test run by G-19A group, where some labs reported a chip as counterfeit and others labeled it authentic [11].

2) **Electrical Inspections**: Electrical tests have the potential to be an efficient means of counterfeit detection, as they do not have the limitations of physical inspections. However, there are major challenges that are unique to electrical tests. In this section, we will briefly discuss the limitations of the electrical tests described in Section 4.2.

Parametric tests are generally very time efficient. However, due to increased process variations and environmental variations (temperature, noise, aging, etc.), the electrical parameters of a component vary significantly. It will be very difficult to conclude whether the variations in the parameters of a component are due to the aging (for recycled and remarked components) or to the process variations in the circuit. One can perform a statistical analysis based on the data observed from the parametric tests to determine the confidence level that a part is counterfeit with or without a golden IC. The efficiency of such analysis must be proven on a large number of golden and counterfeit parts.

For *functional tests*, test program generation for obsolete and active parts with limited knowledge of the part will be extremely difficult, if not impossible. The requirement of having a high-speed tester in order to apply functional test patterns to chips make it extremely expensive. It is nearly impossible to get the complete set of test vectors for an obsolete part from the OCM. In some cases, the OCM may no longer exist or the information required may no longer be available in archived records at the OCM. *Burn-in tests* are useful in detecting infant mortality failures of components. However, because of excessive test time and cost, these tests are only attractive and useful only for critical and high-risk applications. The implementation of *structural tests* in counterfeit detection is extremely challenging for several reasons. First, the structural tests require total access to the internal scan chains of a component. Sometimes, IP owners do not give permission to access their design and disable the internal scan chains with a fuse. Second, obsolete parts may not have design for testability (DFT) structures implemented. Finally, analog chips cannot be tested.

6.2 Avoidance Challenges

The techniques described in Section 5 pose several concerns for counterfeit avoidance. Table 2 presents the comparison study of all the different counterfeit avoidance technologies. We have assigned a score of high, medium, or low, depending on effectiveness.

1) **Reliability**: This is a major issue that must be overcome for many of these techniques. For example, the response of a PUF must be constant for a given challenge over a wide range of environmental variations, ambient noise, and aging. Active hardware metering does not have a reliability problem. However, its effectiveness for counterfeit avoidance is yet to be verified. There is a serious reliability concern on DNA marking as environmental conditions such as high temperatures can potentially damage the DNA and either make the sequence unreadable or change the sequence. The reliability of nanorods and magnetic PUFs have not yet been verified.

2) **Uniqueness**: This is a measure of uncorrelatedness between two chip IDs. Ideally, two IDs should differ with a probability of 0.5 under the same test conditions. Better uniqueness makes it difficult for counterfeiters to guess new IDs after obtaining a set of IDs. PUFs and magnetic PUFs produce responses nearly equal to the ideal case [31, 44, 77]. Any high-level language (C/C++, Java, Matlab etc.) can generate a true random number, which is generally used as the chip ID. Due to the huge number of base pairs in DNA, there are enough sequences to support billions of unique markings. However, fast authentication – observing the specific light – can be easily imitated. The uniqueness of the marking is based on the number of nanorods in the pattern and the sensitivity of the measuring device to color and intensity of light. Since the exact angle of each individual nano-rod is random, it is very unlikely

Table 2 Implementation challenges of counterfeit avoidance techniques

Avoidance techniques	Reliability	Uniqueness	Tamper resistance	Area overhead	Target counterfeit Types	Target component	Implementation cost
Physically unclonable functions (PUF)	Medium	High	High	Low	Remarked, overproduced, cloned	Digital ICs	Medium
Hardware metering	Medium	High	Medium	Low/medium	Overproduced, cloned	Digital ICs	High
Secure split test (SST)	NA	NA	Medium	Medium	Overproduced, out-of-spec/ defective, cloned	Digital ICs	High
Combating die/IC recovery (CDIR)	Medium	NA	High	Low	Recycled, remarked	Digital ICs	Low
Poly fuse-based technology for recording usage time	Medium	NA	High	Medium	Recycled, remarked	Digital ICs	Medium
Electronic chip ID (ECID)	High	High	Low	Low	Remarked	Digital ICs	Low
DNA markings	Medium	Medium	Medium	NA	Recycled, remarked	All (digital/analog/RF/etc.)	High
Nanorods	Not verified	Medium	Not verified	NA	Recycled, remarked	All (digital/analog/RF/etc.)	Not verified
Magnetic PUF	Not verified	High	High	NA	Remarked, cloned	All (digital/analog/RF/etc.)	Not verified

that the same process will produce the same result, and manually cloning the marking at a nano scale is not practical.

3) **Tamper resistance**: This is defined as the difficulties faced by the attacker/counterfeiter when attempting to disable the counterfeit avoidance system. It is extremely difficult to clone the IDs generated by PUFs and magnetic PUFs. The CDIR sensors also provide high tamper resistance because they use natural random process variation. As the poly fuse provides excellent resistance against tampering, it is hard to alter the contents in poly fuse-based sensors. It is easy to clone the ECID, as it static and readable. It is simple for counterfeiters to imitate the color generated by DNA markings, during fast authentication. The tamper resistance of nanorods has not yet been verified.

4) **Area overhead**: This is the area required on the die to implement a counterfeit avoidance measure. PUFs, CDIR sensors and ECID provide low area overhead whereas hardware metering, SST, and poly fuse-based sensors offer medium area overhead. DNA markings, nanorods, and magnetic PUFs do not require any area overhead.

5) **Target counterfeit types**: This represents the detectable counterfeit types (from the counterfeit taxonomy discussed in Section 2.1). PUFs and magnetic PUFs can detect remarked and cloned counterfeit types. SST can likely detect overproduced, out-of-spec/defective, and cloned component types. CDIR and poly fuse-based sensors are designed to target recycled and remarked types. ECID can potentially detect remarked type. DNA markings and nanorods may possibly be used to detect recycled and remarked counterfeit types.

6) **Target components**: This describes what type of components should be targeted for anti-counterfeiting. DNA markings, nanorods, and magnetic PUFs may be implemented in both analog and digital components, whereas the other anti-counterfeit measures can only target digital components.

7) **Implementation cost**: The cost of implementing a PUF would entail storing and maintaining the challenge-response pairs in a secure database, in addition to its area overhead. For hardware metering and SST, back-and-forth communication between the design house and foundry make it expensive to implement. For CDIR and poly fuse-based structures, the cost comes from the area overhead. To authenticate the ICs, low-cost equipment is required. We need only a secure database to store the ECID. Thus, the cost from area overhead is negligible. The detailed authentication for identifying the plant DNA applied to the IC is expensive.

6.3 Test Selection and Confidence Analysis

We must make every attempt to stay ahead of counterfeiters to prevent the widespread infiltration of counterfeit parts into our critical infrastructures. This should begin with a necessary comprehensive assessment of current detection technologies. A particular set of methods may be useful when applied to a specific type of components such as microprocessors, memories, etc., but the same set of methods may not extend to others such as analog ICs, transistors, etc. Physical methods, on the other hand, can be applied to all component types. However, some of the methods are destructive and take hours to implement. As a result, sampling is performed to certify a batch of parts by observing a small number of parts. Electrical methods, on the other hand, are non-destructive and time efficient, but very difficult to implement.

We need to develop a test selection technique [27] that will consider test time, test cost, and application risks while recommending a set of tests to detect the defects and anomalies present in counterfeit components with high confidence. While selecting a set of tests from the complete test set, one should first be chosen that detects all high frequency defects (those that occur most frequently in the counterfeit components), to reach a quicker decision as to a component being counterfeit. This technique should allow us to perform the following:

1) **Risk-Based Analysis**: The model should consider application risks while recommending a set of tests. The test set should be different for different risks. For critical applications we need to concentrate on obtaining the maximum test coverage of counterfeit defects irrespective of test time and cost. We should also focus on test time and cost while developing the test set for other application risks.
2) **Data-Driven Analysis**: The model should be developed on the data received from Government-Industry Data Exchange Program, GIDEP [22]. The decision that a component is counterfeit must be taken from data rather than from subject matter experts.

7 Conclusion

In this paper, we have presented all the counterfeit types currently corrupting the electronic component supply chain and the defects present in them. We have also presented a comprehensive taxonomy of the current counterfeit detection methods. We have described various types of anti-counterfeit measures that prevent counterfeit ICs from entering into the supply chain. We believe that current efforts to address the counterfeiting problem are clearly not sufficient. More research is needed to implement effective test methods that are adaptable, as the counterfeiting process will become more sophisticated over time. Finally, new, low-cost, and robust anti-counterfeit mechanisms must be developed.

Acknowledgments This work was supported in part by the National Science Foundation under grant CNS 1344271, Missile Defense Agency, and Honeywell. The authors would like to thank Steve Walters of Honeywell, and the G-19A group members for providing valuable feedback on the defect taxonomy.

References

1. Alkabani YM, Koushanfar F (2007) Active hardware metering for intellectual property protection and security. In: Proceedings of 16th USENIX security symposium on USENIX security symposium, pp 20:1–20:16
2. Alkabani Y, Koushanfar F, Potkonjak M (2007) Remote activation of ICs for piracy prevention and digital right management. In: Proceedings of IEEE/ACM international conference on computer-aided design, pp 674–677
3. Arndt K, Narayan C, Brintzinger A, Guthrie W, Lachtrupp D, Mauger J, Glimmer D, Lawn S, Dinkel B, Mitwalsky A (1999) Reliability of laser activated metal fuses in drams. In: Proceedings of IEEE on electronics manufacturing technology symposium, pp 389–394
4. Baumgarten A, Tyagi A, Zambreno J (2010) Preventing IC piracy using reconfigurable logic barriers. IEEE Des Test of Comput 27(1):66–75
5. Bolotnyy L, Robins G (2007) Physically unclonable function-based security and privacy in rfid systems. In: Proceedings of IEEE international conference on pervasive computing and communications, pp 211–220
6. Bushnell M, Agrawal V (2000) Essentials of electronic testing for digital, memory, and mixed-signal VLSI circuits. Springer
7. Cassell J (2012) Reports of counterfeit parts quadruple since 2009. Challenging US Defence Industry and National Security
8. Chakraborty R, Bhunia S (2008) Hardware protection and authentication through netlist level obfuscation. In: Proceedings of IEEE/ACM international conference on computer-aided design, pp 674 –677
9. Chakraborty R, Bhunia S (2009) HARPOON: an obfuscation-based SoC design methodology for hardware protection. IEEE Trans Comput Aided Des Integr Circ Syst 28(10):1493–1502
10. Chardonnal D (2011) Impacts of counterfeiting and piracy to reach US$1.7 trillion by 2015
11. CHASE (2013). http://www.chase.uconn.edu/arochase-special-workshop-on-counterfeit-electronics.php
12. Contreras G, Rahman T, Tehranipoor M (2013) Secure split-test for preventing IC piracy by untrusted foundry and assembly. In: Proceedings of international symposium on fault and defect tolerance in VLSI systems
13. CTI, Components technology institute, Inc. http://www.cti-us.com/
14. CTI (2010) Comparison of AS 5553, CTI-CCAP-101B, and IDEA-STD-1010-A
15. CTI (2011) Certification for coutnerfeit components avoidance program, http://www.cti-us.com/pdf/CCAP101Certification.pdf
16. Departnent of Defense (2010) Test method standard: microcircuits. Available: http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-883/std883.pdf

17. Department of Defense (2012) Test method standard: test methods for semiconductor devices. Available: http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-750/std750.pdf
18. Eldred RD (1959) Test routines based on symbolic logical statements. J ACM 6(1):33–37
19. ERAI, Electronic resellers association international (ERAI), http://www.erai.com/
20. Galey JM, Norby RE, Roth JP (1961) Techniques for the diagnosis of switching circuit failures. In: Proceedings of the second annual symposium on switching circuit theory and logical design, pp 152–160
21. Gassend B, Clarke D, van Dijk M, Devadas S (2002) Silicon physical random functions. In: Proceedings of the 9th ACM conference on computer and communications security, ser. CCS '02. ACM, New York, pp 148–160
22. GIDEP Government-industry data exchange program (GIDEP). http://www.gidep.org/
23. Grochowski A, Bhattacharya D, Viswanathan T, Laker K (1997) Integrated circuit testing for quality assurance in manufacturing: history, current status, and future trends. IEEE Trans Circ Syst II: Analog Digit Signal Process 44(8):610–633
24. Guajardo J, Kumar S, Schrijen G-J, Tuyls P (2007) Physical unclonable functions and public-key crypto for fpga ip protection. In: International conference onfield programmable logic and applications, pp 189–195
25. Guin U, Tehranipoor M (2013) Counterfeit detection technology assessment. In: GOMACTech
26. Guin U, Tehranipoor M (2013) On selection of counterfeit ic detection methods. In: IEEE north atlantic test workshop (NATW)
27. Guin U, DiMase D, Tehranipoor M (2014) A comprehensive framework for counterfeit defect coverage analysis and detection assessment. J Electron Test Theory Appl (JETTA) 30(1). doi:10.1007/s10836-013-5428-2
28. Guin U, Forte D, Tehranipoor M (2013) Anti-Counterfeit techniques: from design to resign. In: Microprocessor test and verification (MTV)
29. Guin U, Tehranipoor M, DiMase D, Megrdician M (2013) Counterfeit IC detection and challenges ahead. In: ACM SIGDA
30. Hart AD, Meyers LR, Hernandez C, Morley RE, Richter EJ, Indeck RS (2013) Card authentication system, Patent US8 447 991 B2. Available: https:patentimages.storage.googleapis.com/pdfs/US8447991.pdf
31. Hori Y, Yoshida T, Katashita T, Satoh A (2010) Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs. In: International conference on reconfigurable computing and FPGAs (ReConFig), pp 298–303
32. Huang J, Lach J (2008) IC Activation and user authentication for security-sensitive systems. In: Proceedings of IEEE international workshop on hardware-oriented security and trust, pp 76–80
33. IDEA, Acceptability of electronic components distributed in the open market. http://www.idofea.org/products/118-idea-std-1010b
34. IHS, Information handling services Inc. (IHS), http://www.ihs.com/
35. IHS iSuppli (2011) Top 5 most counterfeited parts represent a $169 billion potential challenge for global semiconductor market
36. Jensen F, Petersen NE (1982) Burn-in: an engineering approach to the design and analysis of burn-in procedures. Wiley
37. Jones J (2009) Counterfeit components and acoustic microscopy
38. Kessler LW, Sharpe T (2010) Faked parts detection. Circ Assemb J Surf Mt Electron Assemb. http://www.circuitsassembly.com/cms/component/content/article/159/9937-smt
39. Koushanfar F, Qu G, Potkonjak M (2001) Intellectual property metering. In: Information hiding. Springer-Verlag, pp 81–95
40. Koushanfar F, Qu G (2001) Hardware metering. In: Proceedings IEEE-ACM design automation conference, pp 490–493
41. Kuemin C, Nowack L, Bozano L, Spencer ND, Wolf H (2012) Oriented assembly of gold nanorods on the single-particle level. Adv Funct Materi 22(4):702–708
42. Kumar S, Guajardo J, Maes R, Schrijen G-J, Tuyls P (2008) Extended abstract: the butterfly puf protecting ip on every fpga. In: Proceedings of IEEE international workshop on hardware-oriented security and trust, pp 67–70
43. Kursawe K, Sadeghi A-R, Schellekens D, Skoric B, Tuyls P (2009) Reconfigurable physical unclonable functions—enabling technology for tamper-resistant storage. In: Proceedings of IEEE international workshop on hardware-oriented security and trust, pp 22–29
44. Maiti A, Gunreddy V, Schaumont P A systematic method to evaluate and compare the performance of physical unclonable functions. Available: http://eprint.iacr.org/2011/657.pdf
45. Marshall M (2011) Best detection methods for counterfeit components
46. Lee J, Lim D, Gassend B, Suh G, van Dijk M, Devadas S (2004) A technique to build a secret key in integrated circuits for identification and authentication applications. In: Proceedings of digest of technical papers on VLSI circuits, pp 176–179
47. Lofstrom K, Daasch W, Taylor D (2000) Ic identification circuit using device mismatch. In: Proceedings of IEEE international solid-state circuits conference, pp 372–373
48. Mazumder P, Chakraborty K (1996) Testing and testable design of high-density random-access memories. Springer
49. Miller M, Meraglia J, Hayward J (2012) 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
50. Morley RE, Richter EJ, Engel GL (2007) Method and apparatus for authenticating a magnetic fingerprint signal using an adaptive analog to digital converter. Patent US7 210 627 B2. Available: https://patentimages.storage.googleapis.com/pdfs/US7210627.pdf
51. Mouli C, Carriker W (2007) Future Fab: how software is helping Intel go nano—and beyond. IEEE Spectr 44(3):38–43
52. Nelson GF, Boggs WF (1975) Parametric tests meet the challenge of high-density ICs. Electronics 48(5):108–111
53. OECD (2007) The economic impact of counterfeiting and piracy. http://www.oecd.org/dataoecd/13/12/38707619.pdf
54. Pappu R (2001) Physical one-way functions. Ph.D. dissertation, Massachusetts Institute of Technology
55. Poage JF (1963) Derivation of optimal tests to detect faults in combinational circuits. In: Proceedings of the symposium on mathematical theory of automata, pp 483–528
56. Robson N, Safran J, Kothandaraman C, Cestero A, Chen X, Rajeevakumar R, Leslie A, Moy D, Kirihata T, Iyer S (2007) Electrically programmable fuse (eFUSE): from memory redundancy to autonomic chips. In: CICC, pp 799–804
57. Roy J, Koushanfar F, Markov I (2008) EPIC: ending piracy of integrated circuits. In: Proceedings on design, automation and test in Europe, pp 1069–1074
58. SAE, http://www.sae.org/works/committeeHome.do?comtID=TEAG19
59. SAE, SAE International, http://www.sae.org/
60. SAE (2009) Counterfeit electronic parts; avoidance, detection, mitigation, and disposition
61. Semiconductor Industry Association (SIA) (2012) Public comments—DNA authentication marking on items in FSC5962

62. Seshu S, Freeman DN (1962) The diagnosis of asynchronous sequential switching systems. IRE Trans Electron Comput EC-11(4):459–465
63. Soma M (1993) Fault coverage of dc parametric tests for embedded analog amplifiers. In: Proceedings on international test conference, pp 566–573
64. Suh G, Devadas S (2007) Physical unclonable functions for device authentication and secret key generation. In: Proceedings of ACM/IEEE on design automation conference, pp 9–14
65. Suh GE, Clarke D, Gassend B, van Dijk M, Devadas S (2003) Aegis: architecture for tamper-evident and tamper-resistant processing. In: Proceedings of the 17th annual international conference on supercomputing, ser. ICS '03. New York, ACM, pp 160–171
66. Su Y, Holleman J, Otis B (2007) A 1.6pj/bit 96 circuit using process variations. In: Proceedings of IEEE international on solid-state circuits conference, pp 406–611
67. Suk D, Reddy S (1981) A march test for functional faults in semiconductor random access memories. IEEE Trans Comput C-30(12):982–985
68. Tehranipoor M, Koushanfar F (2010) A survey of hardware trojan taxonomy and detection. IEEE Des Test Comput 27(1):10–25
69. trust-HUB http://trust-hub.org/home
70. US (2010) Department Of commerce, defense industrial base assessment: counterfeit electronics
71. US Congress (2011) Ike skelton national defense authorization act for fiscal year. Available: http://www.gpo.gov/fdsys/pkg/BILLS-111hr6523enr/pdf/BILLS-111hr6523enr.pdf
72. US Defense Logistics Agency (2012) Dna authentication marking on items in fsc 5962. Available: https://www.dibbs.bsm.dla.mil/notices/msgdspl.aspx?msgid=685
73. US Environmental Protection Agency (2011) Electronic waste management in the united states through 2009
74. US Senate Committee on armed services (2012) Inquiry into counterfeit electronic parts in the department of defence supply chain
75. US Senate Committee on armed services (2012) Suspect counterfeit electronic parts can be found on internet purchasing platforms, Available: http://www.gao.gov/assets/590/588736.pdf
76. Wang X, Tehranipoor M (2010) Novel physical unclonable function with process and environmental variations. In: Proceedings on design, automation test in europe conference exhibition (DATE), pp 1065–1070
77. Yu M-DM, Sowell R, Singh A, M'Rahi D, Devadas S (2012) Performance metrics and empirical results of a PUF cryptographic key generation ASIC. In: HOST, pp 108–115
78. Zhang X, Tehranipoor M (2013) Design of on-chip light-weight sensors for effective detection of recycled ICs. In: IEEE transactions on VLSI systems
79. Zhang X, Tuzzio N, Tehranipoor M (2012) Identification of recovered ICs using fingerprints from a light-weight on-chip sensor. In: Proceedings on IEEE-ACM design automation conference, pp 703–708

Ujjwal Guin is a doctoral student at the Electrical and Computer Engineering Department, University of Connecticut. He received his B.E. degree from Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, India and M.Sc. degree from Department of Electrical and Computer Engineering, Temple University in 2004 and 2010, respectively. He is an active participant in SAE International's G-19A Test Laboratory Standards Development Committee. His current research interests include counterfeit detection and avoidance, hardware security, VLSI testing, and reliability.

Daniel DiMase is the Director of Compliance and Quality at Honeywell International Inc, working in the counterfeit parts prevention team for the Aerospace Quality organization. He is involved in implementing policies and procedures to mitigate the counterfeit risk, and oversees customer and regulatory concerns. He participates in standards development activities to deploy industry best practices and procedures, and to create testing solutions for detection of suspect counterfeit electronic parts. He also contributes in site and supplier audits for Honeywell. He has worked on the NASA Contract Assurance Services team assisting NASA centers become compliant to NASA policy and the AS5553 standard for mitigating counterfeit electronic parts.

Mr. DiMase is an active participant in SAE Internationals G-19 Counterfeit Electronic Parts Document Development group. He is co-chairman of the Test Laboratory Standards Development committee, co-chairman of the Distributor Process Rating committee, and actively participates on the Counterfeit Electronic Parts standard development committee for distributors. Among other committees, has been active in the executive committee of the Aerospace Industry Associations Counterfeit Parts Integrated Projects Team. He is on the Department of Homeland Securitys Customs and Border Protection Advisory Committee on Commercial Operations of CBP in the Intellectual Property Rights subcommittee. He received a special recognition award at the DMSMS and Standardization 2011 Conference for his leadership role in mitigating counterfeit parts.

Dan DiMase has over 20 years of industry experience, previously serving in leadership positions as president of SemiXchange, Inc. and ERAI. He is a results-oriented leader proficient in supply-chain, operations and finance, with cross functional expertise in numerous areas, including international logistics, global sourcing, risk management, and strategic planning. He has a Six-Sigma Green Certificate from Bryant University. He received his Bachelor of Science degree in Electrical Engineering from The University of Rhode Island. He has an Executive MBA from Northeastern University.

Mohammad Tehranipoor is currently the F.L. Castleman Associate Professor in Engineering Innovation at the University of Connecticut. His current research projects include: computer-aided design and test for CMOS VLSI designs, reliable systems design at nanoscale, counterfeit electroincs detection and prevention, supply chain risk management, and hardware security and trust. Dr. Tehranipoor has published over 200 journal articles and refereed conference papers and has given more than 110 invited talks and keynote addresses since 2006. He has published four books and ten book chapters. He is a recipient of several best paper awards as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, the 2009 UConn ECE Research Excellence Award, and the 2012 UConn SOE Outstanding Faculty Advisor Award.

He serves on the program committee of more than a dozen of leading conferences and workshops. He served as Program Chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, Program Chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, Co-program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), General Chair for D3T-2009 and DFTS-2009, and Vice-general Chair for NATW-2011. He co-founded a new symposium called IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 General Chair and Chair of Steering Committee. He is currently serving as an Associate EIC for IEEE Design & Test, an Associate Editor for JETTA, an Associate Editor for Journal of Low Power Electronics (JOLPE), an IEEE Distinguished Speaker, and an ACM Distinguished Speaker. Dr. Tehranipoor is a Senior Member of the IEEE and Member of ACM and ACM SIGDA. He is currently serving as the director of CHASE center.