INVITED PAPER

Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain

This paper surveys the state of the art in counterfeiting and detection technologies.

By Ujjwal Guin, *Student Member IEEE*, Ke Huang, *Member IEEE*, Daniel DiMase, John M. Carulli, Jr., *Senior Member IEEE*, Mohammad Tehranipoor, *Senior Member IEEE*, and Yiorgos Makris, *Senior Member IEEE*

ABSTRACT | As the electronic component supply chain grows more complex due to globalization, with parts coming from a diverse set of suppliers, counterfeit electronics have become a major challenge that calls for immediate solutions. Currently, there are a few standards and programs available that address the testing for such counterfeit parts. However, not enough research has yet addressed the detection and avoidance of all counterfeit parts—recycled, remarked, overproduced, cloned, out-of-spec/defective, and forged documentation—currently infiltrating the electronic component supply chain. Even if they work initially, all these parts may have reduced lifetime and pose reliability risks. In this tutorial, we will provide a review of some of the existing counterfeit detection and avoidance methods. We will also discuss the challenges ahead for implementing these methods, as well as the development of new detection and avoidance mechanisms.

KEYWORDS | AC/DC parametric tests; counterfeit integrated circuits (ICs); electrical inspection; hardware security; machine learning; path-delay test; physical inspection

I. INTRODUCTION

Counterfeit integrated circuits (ICs), a major source of concern in the electronic component supply chain because of reliability and security issues, are impacting many industrial sectors, including computers, telecommunications, automotive electronics, and even military systems [1], [2]. The consequences can, obviously, be dramatic when critical systems begin to fail due to the use of counterfeit or low-quality components. According to [3], legitimate electronics companies miss out on about $100 billion of global revenue every year because of counterfeiting. Indeed, the hi-tech industry is significantly impacted by counterfeiting activity. Around 1% of semiconductor sales are estimated to be those of counterfeited units [4]. The tools and technologies utilized by counterfeiters have become extremely sophisticated and well financed [5]. In turn, this also calls for more sophisticated methods to detect counterfeit electronic parts that enter the market. Data provided by IHS (Englewood, CO, USA), shown in Fig. 1, shows that reports of counterfeit parts have quadrupled since 2009.

Counterfeit ICs pose a significant threat to the global electronics component supply chain and are becoming more difficult to detect as the counterfeiters increase their level of sophistication [7]. Counterfeiters are improving their technique and expertise, to an extent of successfully

Manuscript received October 16, 2013; revised April 22, 2014; accepted June 9, 2014. Date of publication July 15, 2014; date of current version July 18, 2014.
U. Guin and **M. Tehranipoor** are with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: ujjwal@engr.uconn.edu; tehrani@engr.uconn.edu).
K. Huang is with the Department of Electrical and Computer Engineering, San Diego State University, San Diego, CA 92115 USA (e-mail: k.h.huang@ieee.org).
D. DiMase is with Honeywell Inc., Providence, RI 02895 USA (e-mail: Daniel.DiMase@Honeywell.com).
J. M. Carulli, Jr. is with Texas Instruments, Dallas, TX 75243 USA (e-mail: j.m.carulli@ieee.org).
Y. Makris is with the Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: yiorgos.makris@utdallas.edu).
Digital Object Identifier: 10.1109/JPROC.2014.2332291

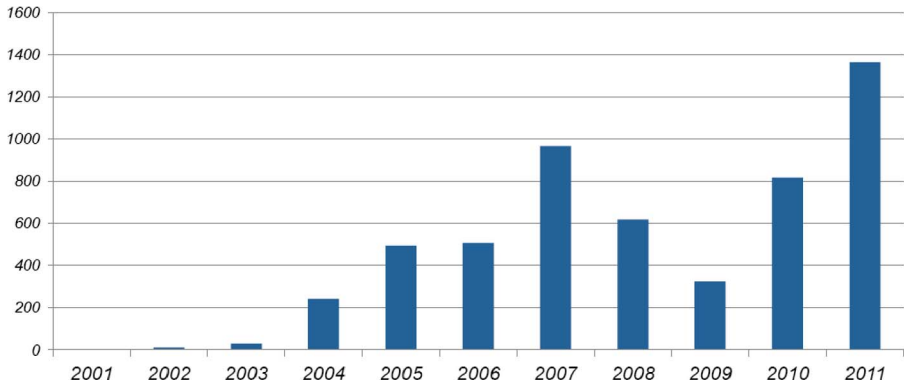


Fig. 1. ***Reported counterfeit parts have been quadrupled since 2009 [6].***

duplicating a company itself. Counterfeit ICs are of great concern to industry and government because a system malfunction can present situations that cause mission failures and health or safety concerns [8]. The potential for loss and tragedy caused by such devices could be significant for electronic systems supporting a number of sectors (e.g., medical, aerospace, defense, automotive, banking, energy/smart-grid, etc.).

Table 1 shows the top-5 most counterfeited semiconductors in 2011 according to data from ERAI (Naples, FL, USA). ERAI is a private organization that collects reported data on counterfeit incidents and reports the information to their members. As the table shows, the counterfeits with the most reported incidents impact affect both analog and digital ICs, as well as discrete components.

Contemporary advancements in very large scale integration (VLSI) have been accompanied by increasing variation in the performances of fabricated chips and concerns about the correctness of their operation. Indeed, failures can occur at any stage in the lifetime of an IC. During production, devices can fail due to design weaknesses, excessive process variations, or local spot defects. After production, devices can fail due to defects which are not detected by the production tests and manifest themselves later in the field of operation. These early life failures are caused by extrinsic process defects and are known as infant mortality. ICs can also fail during their lifetime due to aging, wear-and-tear, harsh environments, overuse, etc. These failures occur when a material or component exceeds its fundamental capability and are known as intrinsic reliability failure mechanisms.

Table 1 Top-5 Most Counterfeited Semiconductors in 2011 [10]

Ranks	Component 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%

Depending on the end-user application, ICs may go through burn-in tests, where they are exercised sufficiently long under stress conditions, in order to avoid early in-use system failures or to estimate the operating life of a particular device. Once the reliability issues of an IC are properly addressed, its lifetime can be estimated, and it can be shipped to customers. Fig. 2 illustrates typical device failure characteristics, often known as the bathtub curve [11]. The failure rate is defined as the probability that a device will fail in the time interval between t and $t + \delta t$, given that it has survived until time t [12]. As can be observed in Fig. 2, counterfeit devices are expected to have shorter time to failure compared to brand new devices. Table 2 summarizes the possible effects of counterfeit ICs for governments, industries, and consumers.

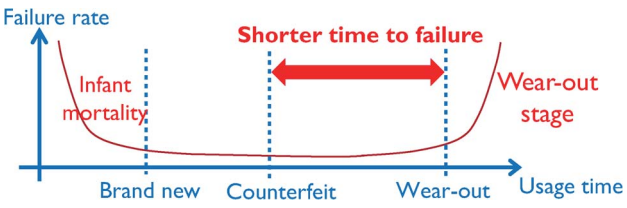


Fig. 2. ***The classical bathtub curve illustrating typical device failure characteristics.***

Table 2 Possible Effects of Counterfeit ICs [13]

Government	Industry	Consumer
National security or civilian safety issues	Costs to mitigate this risk	Costs when products fail due to lower quality and reliability of counterfeit parts
Costs of enforcement	Costs to replace failed parts	
	Lost sales	
Lost tax revenue due to illegal sales of counterfeit parts	Lost brand value or damage to business image	Potential safety concerns

As the IC supply chain has become globalized and thus more complex, additional sources of failure have become a concern. Specifically, the trustworthiness of IC supply chain is much harder to assess. Indeed, ICs provided by untrusted points in the supply chain could be intentionally relabeled, illegitimately replicated, or recycled from used or defective circuit boards. Even if these ICs work initially, they may have a reduced lifetime and can pose reliability risks.

A. Survey of Articles

It was pointed out by the Semiconductor Industry Association (SIA, Washington, DC, USA) in [8] that counterfeit devices can be avoided by exclusively buying semiconductor products either directly from the original component manufacturer (OCM) or directly from the OCM-authorized distributors/resellers. However, it is also reported by the SAE International (Washington, DC, USA) and the U.S. Department of Commerce that authorized distributors encounter counterfeit parts [2]. The problem is further compounded due to obsolescence and life cycles of piece parts which have much shorter life cycles than complex systems which the parts are incorporated within, requiring significant requalification. Several practices have been developed to identify counterfeit devices. They are broadly classified into counterfeit detection and counterfeit avoidance methods. For the purposes of this paper, counterfeit detection focuses on the detection of counterfeit parts in the supply chain whereas counterfeit avoidance concentrates on adding extra hardware in the circuit such that a suspect part is authenticated without costly and time-consuming detection methods (e.g., design for counterfeit avoidance, design for test, design for security).

In [14] and [15], Guin *et al.* 1) developed a comprehensive taxonomy of counterfeit types, counterfeit detection methods, and counterfeit defects; 2) presented assessment of all currently available counterfeit detection methods; and 3) proposed a method selection technique to maximize the test coverage specific to a set of tests. In [16], a statistical approach is used to distinguish recycled counterfeit ICs by training a one-class classifier using only new devices. The measurements used to build the classifier are typical test results from production early failure rate (EFR) analysis required to release most products, such as $V_{\min}$, $F_{\max}$, and I_{ddq}, thus no additional costs in terms of design, test, and area/power overhead are incurred to perform identification. The method is demonstrated using measurements from new and aged devices taken from actual chips in production. Path-delay fingerprinting, a method first introduced in [17] in the context of hardware Trojan detection, is adapted in [18] for detecting recycled ICs. This method also assumes that the recycled ICs have aged due to usage in the field, thus their path-delay distribution changes, providing opportunity for detection.

The most well-known counterfeit avoidance techniques include secure split test (SST), hardware metering, physical unclonable functions (PUFs), lightweight on-chip sensors, package ID, etc. SST attempts to prevent overproduced, out-of-spec/defective, and cloned ICs from entering into the supply chain. It enables the design house back into the manufacturing test process by placing a set of security measures in the design and controlling the test flow [19]. Hardware metering attempts to uniquely tag each chip produced from a certain design by active or passive methods to facilitate chip tracing [20], [21]. Similarly, part authentication tools [22] consist of providing an encrypted number for each device by a radio-frequency identification (RFID) tag in production. However, reverse-engineering tools have become very advanced and allow an attacker to read the stored encrypted number. To overcome this challenge, hardware intrinsic security (HIS) has been proposed as a mechanism that can provide security based on the inherent properties of an electronic device [23]. PUFs [24], for example, belong to the category of such HIS mechanisms. PUFs aim to measure the responses of hardware to certain given inputs, which depend on the unique physical properties of the device, since process variations affect each device in a unique and unclonable fashion. On-chip aging sensors and chip usage measurement structures have been proposed in an effort to detect recycled counterfeit devices [25]–[27]. Finally, package IDs have been proposed to track the components in the supply chain [28], [29].

B. Taxonomy of Counterfeit ICs

A counterfeit component 1) is an unauthorized copy; 2) does not conform to OCM design, model, and/or performance standards; 3) is not produced by the OCM or is produced by unauthorized contractors; 4) is an off-specification, defective, or used OCM product sold as "new" or working; or 5) has incorrect or false markings and/or documentation [2]. Based on the definition above and analyzing supply chain vulnerabilities, we classify the counterfeit types into seven distinct categories [7], [15], [30].

Fig. 3 shows the taxonomy of such counterfeit components. Recycled and remarked components draw much attention in the media, test labs, and industry, and they jointly contribute more than 80% of counterfeit incidents [31]. The recycled components are taken from used printed circuit boards (PCBs), repackaged and remarked, and then sold in the market as new. The remarking process includes the removal of markings on the package (or even on the die) and remarking with forged information. New components can also be remarked to obtain a higher specification, such as remarking from commercial grade part to industrial or defense grade. In overproduction, unauthorized actors in a foundry, assembly, or test site that have access to a designer's IP also have the ability to fabricate ICs outside contract. They can then sell excess ICs in the open market. The unauthorized actor may either knowingly sell out-of-spec/defective components, or they may be stolen and sold on open markets. Cloning is a process of copying a design by counterfeiters mainly to reduce the large development cost of a component. Cloning can be done in two ways: by reverse engineering,

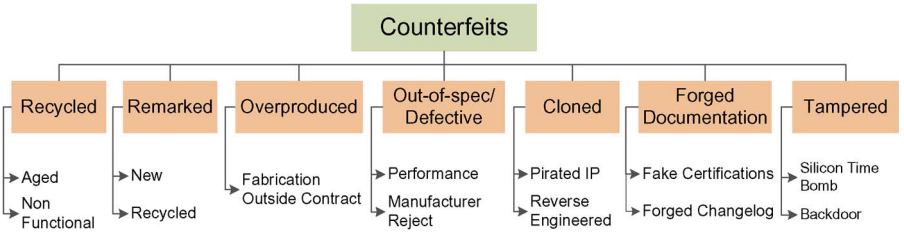


Fig. 3. ***Taxonomy of counterfeit types [7], [14], [30].***

and, by obtaining IPs illegally. Forged documentation may include the false certification of compliance for some standards or programs, or a falsified revision history or change log of a component. The final category of counterfeits is the tampered type. Tampering can occur at the die level ("hardware Trojan") or package level or in the software or firmware of the device. 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 [32].

C. Standardization Activities

Counterfeit prevention and detection require global recognition of the problem and a unified solution. Such a solution often comes in the form of international standards and may be verified through accredited conformity assessment programs. These programs may include key elements such as technical standard(s) recognized worldwide, competency-based training program(s), global supply chain certification system(s), certification bodies, and accreditation schemes. There are standards and command media in place or in development that includes guidance or requirements for detection of the counterfeit parts. One committee responsible for many of these standards is the G-19 Counterfeit Electronic Parts Committee, set forth by SAE International. Their standards target different sectors of the industry: independent distributors and brokers, authorized distributors, users and integrators (including government agencies), and test service providers. These standards are as follows:

1) AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition [33];
2) ARP6178: Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors [34];
3) AS6081: Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors [35] (intended for independent distributors and brokers);
4) AS6496: Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Authorized/Franchised Distribution [36];
5) AS6171: Test Methods Standard; Counterfeit Electronic Parts [37].

Components Technology Institute, Inc. (CTI, Huntsville, AZ, USA) has also created a Counterfeit Components Avoidance Program (CCAP-101) [38]. Independent distributors can be certified as CCAP–101 compliant, which is done by means of a yearly audit. Independent Distributors of Electronics Association (IDEA, West Baden Springs, IN, USA) has developed IDEA–STD–1010-B which mainly provides guidance for the visual inspection of electronic components [39].

Currently, the major issue with many of these standards is that they address the parts that are already circulating in the market, mainly, recycled and remarked parts. Any of the current counterfeit detection standards are not capable of addressing the detection of all types of counterfeits. Moreover, none of these standards are intended for developing avoidance mechanisms in ICs.

D. Taxonomy of Component Types

The type of components can significantly impact detection and avoidance. Components can be classified into three distinct types, namely, obsolete, active, and new. Components become obsolete when the OCM stops manufacturing them. The OCM may produce newer designs and no longer sell the previous generation. They may only be available through the electronic components distributors. Active parts are those that companies continue to fabricate, however, the design is congealed. In these cases, there may be a possibility of modifying the package instead of the die design of a component to address anti-counterfeit measures. New components are very flexible to implement any anti-counterfeit measures. The OCM can decide if one or more of these measures could be placed in the design depending on the area, power, and cost constraints.

II. COUNTERFEIT DETECTION

Over the past several years a specialized service of testing has been created for detecting counterfeit components. The components must be authenticated by these tests before being placed in systems. Fig. 4 shows a generalized taxonomy of counterfeit detection methods. The methods are broadly classified into physical and electrical inspections.

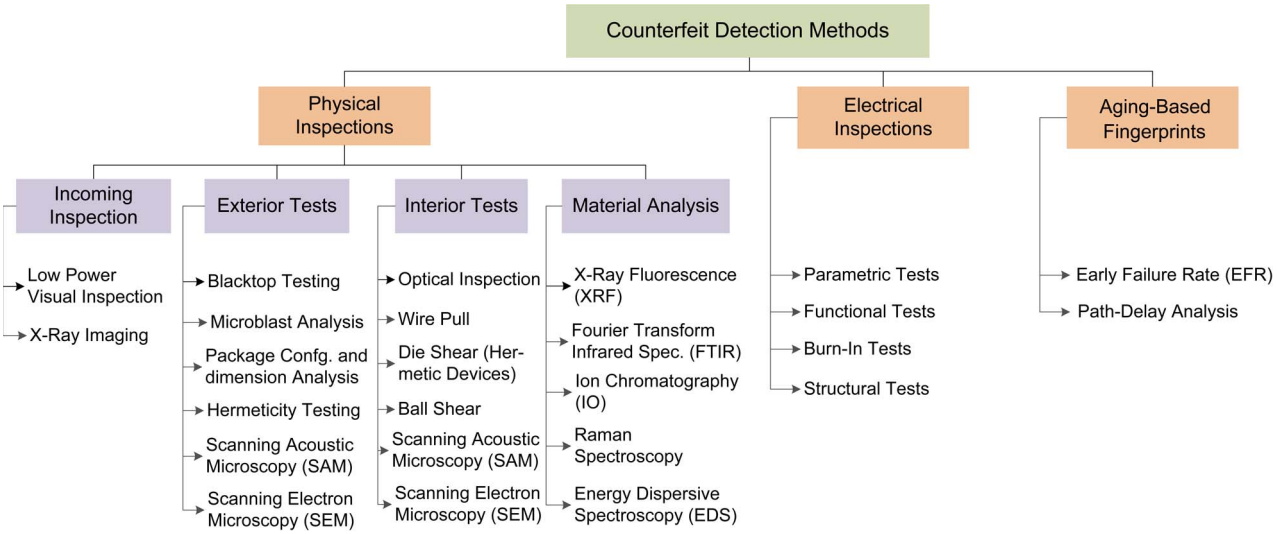


Fig. 4. ***Taxonomy of counterfeit detection methods [7], [14], [15].***

A. Physical Inspection for Counterfeit Detection

Such inspections are based on the physical properties of the component. These tests are grouped into four categories. In incoming inspection, all the components are inspected thoroughly. The external structure is observed carefully by low-power visual inspection (LPVI) while the internal structure is inspected by X-ray imaging. There are several external tests, such as blacktop testing, microblast analysis, hermiticity testing, scanning electron microscopy (SEM), scanning acoustic microscopy (SAM), and a variety of other test methods recommended to find the defects and anomalies present outside the package, inside the package, and on the leads of a component. For interior tests, one needs to decap the component first to expose the internal structure. Optical inspection, wire pull, die/ball shear, and SEM are a few of the tests that test labs generally perform for internal inspection. Material analysis methods are performed to find the defects related to the material composition of the package, leads, and die. X-ray fluorescence (XRF), Fourier transform IR spectroscopy (FTIR)", and energy dispersive spectroscopy (EDS), are a few material analysis methods.

Physical inspections are usually the first set of tests to be performed on the incoming components for authentication. The methodology and implementation of these tests apply uniformly on all types of components— obsolete, active, and new. These tests are based on the physical properties of leads, package, and die of components. In this section, we will describe some commonly used physical inspections used for the detection of counterfeit components.

1) Low-Power Visual Inspection (LPVI): LPVI is the first test usually performed on all the components. The leads and packages are carefully examined using a low-power microscope or magnification lamp, generally with less than 10X magnification. All the relevant information, packaging and shipping information, part number, lot/date/country code, etc., is documented in detail. Recycled parts, desoldered from the PCB, can sometimes be observed with deformed leads and extra material on them. Sometimes, a residual trace of the original marking exists below the new one. Scratches are often visible on the package as a sign of recycling.

Fig. 5 shows four counterfeit defects and anomalies detected by LPVI. Fig. 5(a) displays a peeled off plating layer from the leads. The leads in Fig. 5(b) clearly show a possible rework or reflow soldering. Ghost marking (residual marking

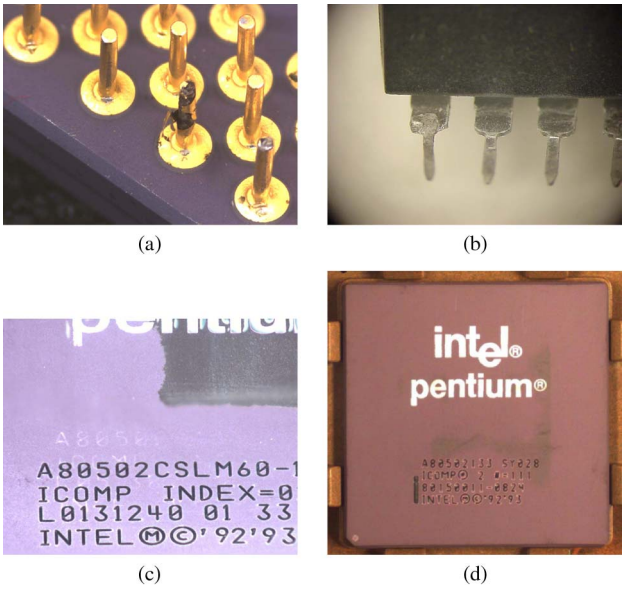


Fig. 5. ***Counterfeit defects detected by LPVI (source: Honeywell). (a) Fake plating on leads. (b) Residual materials on leads. (c) Ghost marking on the package. (d) Heat sink mark on the package.***

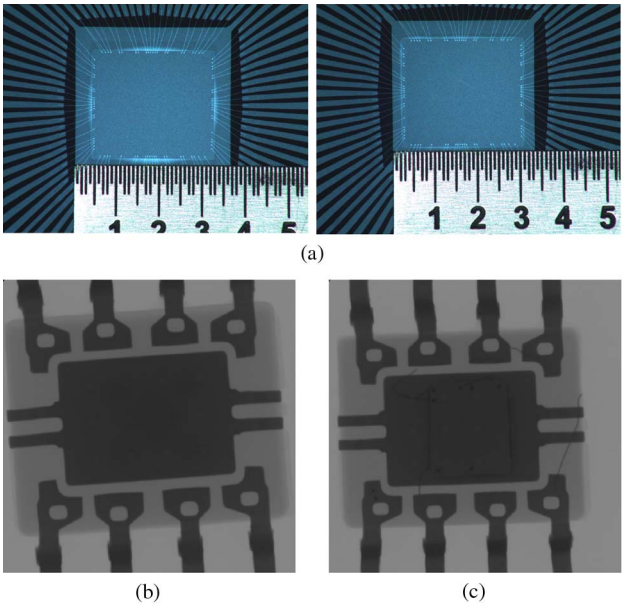


Fig. 6. ***Counterfeit defects detected by X-ray imaging (source: Honeywell). (a) Wrong Die. (b) Missing bond wires. (c) Broken bond wires.***

in white color below the new one) is clearly visible in Fig. 5(c). The heat sink mark in Fig. 5(d) indicates the prior usage of this Intel chip. These defects are easy to detect with LPVI.

2) X-Ray Imaging: X-ray imaging is a method of inspecting the internal structure of a component without performing the decapsulation. It generally belongs to the nondestructive category of tests. There are typically two types of X-ray imaging systems: film X-ray and real-time X-ray systems. In film X-ray systems, the images are formed on a radiographic film, whereas in real-time X-ray systems, a digital image is formed by digital sensors. The defects and anomalies related to die and bond wires such as missing or wrong die, cracks on the die, broken bond wires, etc., may be detected. Additional tests may be required to complete the authenticity of a component.

X-ray imaging is an important method used for counterfeit detection. It is performed on components to verify that the internal package, bond wires, and die construction are consistent with a golden (reference) part. If the golden part is not available, comparisons should be carried out within the same lot. Fig. 6 shows some typical counterfeit defects detected by X-ray imaging. Fig. 6(a) shows two different die sizes in the same lot. There are no bond wires inside the package that is shown in Fig. 6(b). Broken bond wires are presented in Fig. 6(c).

3) Microblast Analysis: Microblasting is a dry blasting counterfeit technique in which accurately defined blasting agents are bombarded on the surface of the target device in an effort to remove part markings and scratches from recycled and used parts or falsely represent new parts (e.g. upgrading temperature or speed-grade) by removing part markings prior to Counterfeit Electronic Partsly remarking devices. Compressed air is generally used to accelerate the blasting particles. Some popular blasting agents, such as aluminum oxide powder, sodium bicarbonate powder, and glass bead, are used, depending on the components' package type [such as dual in-line package (DIP), plastic leaded chip carrier (PLCC), etc.]. A variety of surface analysis techniques may be deployed to detect microblasting. Test methods include SEM, FTIR, RAMAN, and high-power microscopy, at typically more than 200x or greater.

4) Scanning Acoustic Microscopy (SAM): SAM is one of the efficient ways of studying the structure of a component without damaging it. This technology functions by utilizing the reflection and transmission of ultrasound waves to generate an image of the component based on its acoustic impedance at various depths. The component under test is submerged in either deionized water or isopropyl alcohol (IPA), which is used as a medium. Since air will have a much different acoustic impedance than any of the part's mediums, that section will appear much darker on the image produced. The resolution of SAM depends on the transducer frequencies. Lower frequencies provide higher penetration through the component at the cost of lower spatial resolution. SAM is very useful in detecting delamination, or, die attachment to the package. It can also detect the cracks and voids in the die and anomalies in the bond wires. SAM can also be useful for surface analysis and detecting ghost markings or sanding marks using reflective mode.

5) Scanning Electron Microscopy (SEM): SEM is a method of generating an image with a superfine resolution by using a focused electron beam. The image is formed by scanning the entire target area of the sample. SEM consists of two major components: the electron column and a control console. The column generates the focused electron beam for scanning the surface and the control console displays the image. When the high energetic electron beam interacts with the sample, it generates a secondary emission of backscattered electrons and X-rays. An electron detector detects these secondary electrons and an image is formed. A detailed description can be found in [40]. SEM is very useful for detecting many defects and anomalies present in counterfeit components. Using SEM to inspect the die requires decapsulation of the component. However, for external inspections, it is not necessary to decapsulate. The major issue associated with SEM is the long test time. Sometimes it requires several hours to inspect a single component in detail.

6) X-Ray Fluorescence (XRF) Spectroscopy: XRF is a nondestructive method for material analysis. The emission characteristics of a material are observed after heavy bombardment of high-energy X-rays. When the X-ray hits the surface of a material, the outer electrons obtain enough energy

Table 3 XRF Measurement Results (Source: Integra Technologies)

mil SnPb		% Sn		% Pb	
Row	Sample	Row	Sample	Row	Sample
1	0.193	1	100.000	1	0.000
2	0.243	2	100.000	2	0.000
3	0.351	3	100.000	3	0.000
4	3.495	4	99.876	4	0.124
5	0.853	5	99.829	5	0.171
6	0.030	6	100.000	6	0.000

* Part Number: TAJD476K020R and Pin Package: 2 CHIPCAP.

(ionization potential) to reach unstable higher outer orbits. The emission of radiation occurs when these high-energy electrons settle down to their original ground state. Each element produces a unique peak in the spectrum. A unique fingerprint is generated from the package of a component by XRF spectroscopy. A decision about a component's authenticity can be made upon comparison with a golden sample or the manufacturer data sheet if available. There are several X-ray fluorescence spectrometers with an automated sample feed that are available for material analysis. Table 3 shows the XRF measurement results. Rows 1–3 and 4–6 represent the known good and suspect samples, respectively. The suspect sample was a board pull, and shows higher lead coating thickness, and also some lead content in it.

7) Fourier Transform Infrared (FTIR) Spectroscopy: FTIR works based on infrared (IR) spectroscopy. A part of IR radiation is absorbed by the material under test and the other part is transmitted through it. The spectrum for molecular absorption and transmission is observed from the resultant IR radiation. The unique molecular fingerprint, created by FTIR, is compared to the fingerprint of the golden model for material comparison. FTIR is used to authenticate both organic and inorganic materials of a component. It is used to verify: 1) polymer, coating, etc., of the package; 2) residual foreign materials from the sand blasting process used to remove the old markings; and 3) residuals from chemical processing typical from counterfeits performing part removal from printed circuit boards and from the illicit refurbishment process.

8) Energy Dispersive Spectroscopy (EDS): EDS is used to chemically characterize a component using X-ray excitation. A high-energy beam of charged particles is bombarded on the surface, and the emitted X-ray spectrum is captured by an X-ray detector to form the EDS spectrum. A unique fingerprint of X-ray spectrum is generated by the materials used in the component's packaging. Fig. 7 shows the EDS spectrum generated from the leads of an IC. The material lead is detected on the leads of a counterfeit component during lead finish testing, shown in Fig. 7(a). The genuine component does not have the material lead on leads of the IC [Fig. 7(b)].

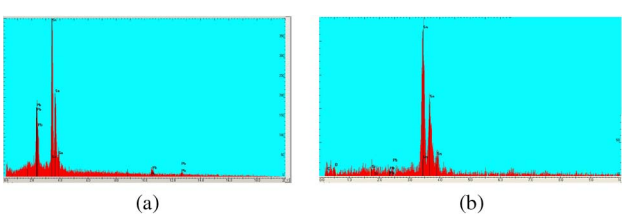


Fig. 7. *Counterfeit defects detected by EDS (source: Honeywell). (a) Counterfeit: element lead found in the leads of an IC. (b) Genuine: No lead found.*

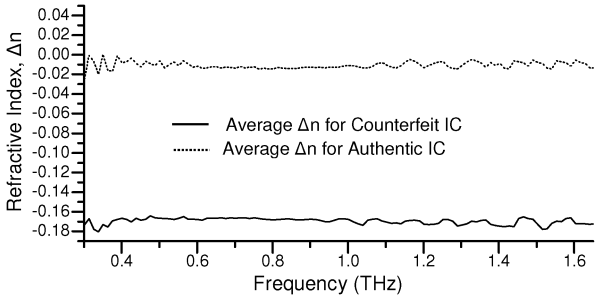


Fig. 8. *Difference in refractive index between top and bottom sides of ICs as a function of radiation frequency [42].*

9) Terahertz Time Domain Spectroscopy (THz–TDS): THz imaging [41] is used to inspect the internal structure of a component by using a pulsed laser operated in the THz frequency range. This technique does not require the application of any bias to the component during testing. There is also no need to decapsulate the component to observe the internal structure. Differential refractive indexes of component die and packaging allows the identification of counterfeit electronics [42]. THz spans the frequency region between 100 GHz and 30 THz. Three attributes make THz imaging useful for counterfeit detection: THz is 1) fully absorbed by metal; 2) partially absorbed by a doped semiconductor; and 3) transparent to plastics. Fig. 8 demonstrates that a counterfeit IC has a completely different refractive index than the a genuine one. The x-axis and the y-axis of the figure represent the frequency of the pulsed laser and differential refractive index (Δn), respectively. A large Δn has been observed in the counterfeit IC.

B. Electrical Inspection for Counterfeit Detection

These inspections are performed primarily to detect electrical defects and anomalies present in counterfeit components. These tests are grouped into four categories. Parametric tests [43]–[45] are efficient at verifying IC's direct current (dc) and alternating current (ac) parameters. They can reveal the shift in electrical parameters due to components' prior usage or out of specification conditions. The functionality of a component can be checked by using functional tests [45], [46]. The defects and anomalies

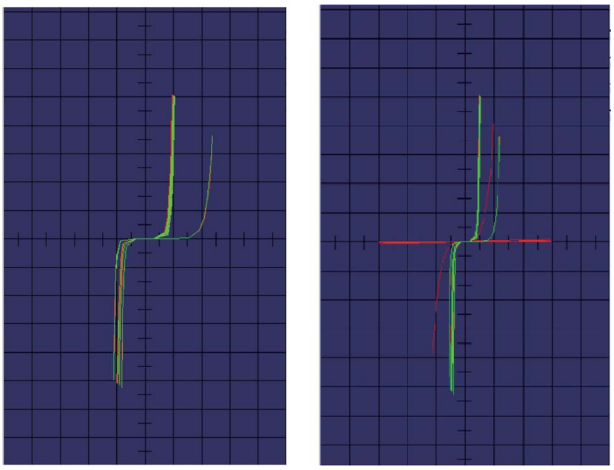


Fig. 9. ***Counterfeit identification using curve trace [52].***

which impact the functionality of a component, such as broken/missing bond wires, cracks, damaged die, open/short interconnect etc., can be detected. In burn-in tests, the component is operated at stressed conditions, such as elevated temperature, to find infant mortality failures in order to assure reliability [47], [48]. In structural tests [49]–[51], test patterns are applied to a chip through internal scan chains to find the defects and anomalies related to the internal structures, interconnects, and logic gates. In this section, we will briefly describe some of the popular electrical inspections.

1) Parametric Tests: Parametric tests are performed over a range of operating temperatures to measure dc and ac parameters of a chip. They include curve tracing test, contact test, power consumption test, output short current test, output drive current test, threshold test, rise and fall time tests, setup, hold and release time tests, propagation delay tests, etc. The objective of parametric testing is to determine the quality of each product to avoid counterfeit distribution and production. This is accomplished by running a suite of tests or as many vital tests as possible to check the dc, ac, and parametric performance of the component in question. The intricacies of these tests can easily give test engineers a robust data set that they can use to uncover a counterfeit component where other test methodologies fail to uncover any problems or anomalies.

Fig. 9 illustrates an example of counterfeit identification using curve trace, with the curve of a genuine device shown in Fig. 9(a), and the curve of a counterfeit device shown in Fig. 9(b). It can be readily observed that the curve of counterfeit device differs significantly from that of the genuine device. Curve trace is also useful in verifying the device pinout and determining circuit damage that may have been created due to poor handling and electro-static discharge. The datasheet of the device can be used when no genuine device is available for this test. We can further enhance the test capability by employing an automatic test equipment (ATE) to enable multiple parametric tests at one time, using automation to quickly perform measurements and evaluate the results.

Another form of proper parametric testing is to use an instrumentation board or instrumentation interface. These interfaces are used between the electronic component, standalone measurement equipment, and PC-based measurement equipment to provide specific parametric testing. These tests are either made available by the component manufacturer or are custom designed by the test lab with the end customer's review and approval.

2) Functional Tests: Functional tests are the most efficient way of verifying the functionality of a component and are perhaps one of the most expensive test methods available in the arsenal when testing complex devices. For instance, system memory chips will have to pass a series of functional tests exercising address, data lines, and bursting under various operating conditions (e.g., temperature, voltage, clock speed). A functional test could verify that all parts perform at specified higher frequencies and through the required temperature range using a functional baseline test. Testing over temperature or at room temperature (25 °C) are the industry standards for testing a circuit board design. This can be applied to the piece part(s) prior to manufacturing, but can be also used to test units on the manufacturing floor on assemblies to increase confidence that the assembled unit is free from faulty and counterfeit components, especially counterfeit components that were remarked as a higher performing part.

A counterfeit or substandard part may fail under a comprehensive functional test sequence. By checking that the device is functioning correctly, a whole range of other issues could be detected, e.g., wrong die, empty package, etc. The addition of a functional test process to current detection processes can be an effective way to increase counterfeit detection capability. A functional test will require a functioning system, most commonly a PCB-based system. For example, the system can be processor based with memory and a number of peripherals. The functional test is a software program with a series of algorithms that exercise and test specific elements of the design.

Several examples demonstrating the detection of counterfeit devices using functional tests under various operating conditions are shown in [53]. As an example, by lowering the ambient temperature in a temperature chamber while the device is repeatedly tested, failure was observed at very low temperature at −35 °C. However, the part was rated to operate at colder temperatures, indicating a defect in the device that could be counterfeit related.

C. Aging-Based Statistical Fingerprints

During the lifetime of an IC, performances continuously degrade due to aging mechanisms. Using recycled

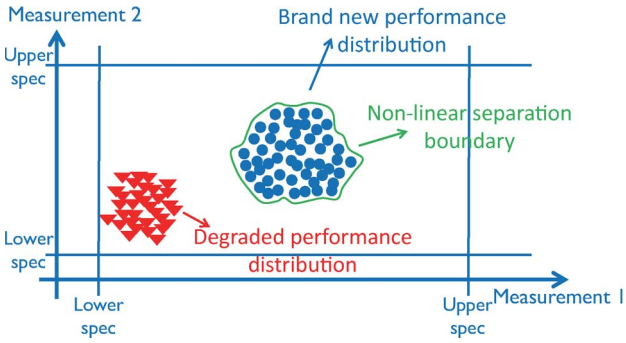


Fig. 10. ***Nonlinear separation boundary for counterfeit device detection [16].***

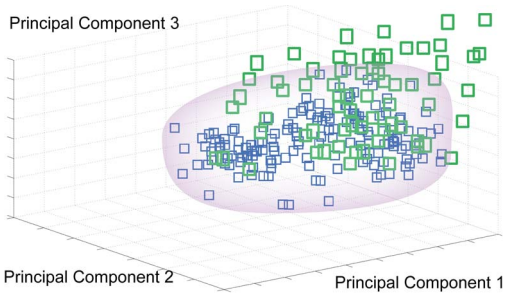


Fig. 11. ***Projection of devices at $t = t_0, t_1$, shown by blue and green squares, respectively.***

counterfeit ICs as brand new will significantly reduce the capability of a device to perform its required functions for prolonged period of time. The most common aging phenomena include electromigration, negative bias temperature instability (NBTI), hot carrier injection (HCI), and time-dependent dielectric breakdown (TDDB). The following two methods leverage the impact of these aging phenomena in order to detect recycled counterfeit ICs.

1) Early Failure Rate (EFR) Data Analysis: In [16], a low-cost statistical approach was discussed to detect recycled counterfeit ICs by training a one-class classifier using only brand new devices. The measurements used to build the classifier are typical test results from production early failure rate (EFR) analysis required to release most products, such as $V_{\min}$, $F_{\max}$, and I_{ddq}, thus no additional costs are incurred to perform identification. An overview of the one-class classifier, which is trained to separate new from aged devices in the space of such measurements, is illustrated in Fig. 10.

The first step involves collection of a set of parametric measurements, which can be taken from trustworthy provider across devices subject to process variations for the purpose of counterfeit IC detection. Then, using the parametric measurements of brand new devices, a one-class classifier is trained to distinguish counterfeit ICs from brand new ones. This approach is inspired by and resembles closely a machine-learning-based analog/RF IC test method [54].

The effectiveness of the approach is demonstrated on a microprocessor design, involving 49 parametric test measurements performed on 313 chips randomly chosen from different lots in production. These measurements are taken at five different time points for the same devices during burn-in test, in order to mimic the impact of aging degradation over time: t_0, t_1, t_2, t_3, t_4. Devices at $t = t_0$ are referred to as brand new, while devices at $t = t_i$, $i > 0$, are referred to as counterfeit. Since the data set has a relatively high dimensionality d for this case study ($d = 49$), a principal component analysis (PCA) [55] is performed in order to map the original 49 measurements onto vectors in a lower dimensional space with cardinality $d' < 49$. The structure of the data is maintained while only nine principal components are kept, i.e., $d' = 9$. Figs. 11 and 12 show the projection of devices at $t = t_0, t_1$ and $t = t_0, t_4$, respectively, onto the first three principal components. As can be clearly observed, performance degradation caused by aging mechanisms is accelerated during the burn-in test. Indeed, an support vector machine (SVM) trained with half of the devices at time $t = t_0$, achieves 100% correct group classification rate for classifying devices at $t = t_0, \ldots, t_4$, respectively, showing the excellent capability of detecting counterfeit devices using this approach [16].

2) Circuit Path-Delay Analysis: A path-delay fingerprinting technique, which was first introduced in [17] in the context of hardware Trojan detection, is adapted in [18] to distinguish recycled ICs from new ones. Due to degradation in the field, the path-delay distribution of recycled ICs will become different from that found in new ICs. Statistical data analysis can effectively separate the impact of process variations from aging effects on path delay. Simulation results demonstrate the efficiency of this technique for recycled IC identification.

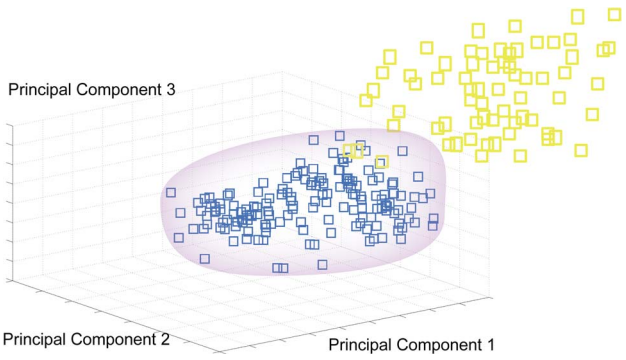


Fig. 12. ***Projection of devices at $t = t_0, t_4$, shown by blue and yellow squares, respectively.***

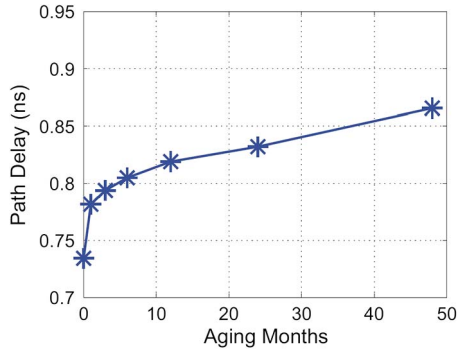


Fig. 13. *Degradation of a critical path due to aging in a digital circuit [18].*

Fig. 13 shows the delay degradation of a critical path from a random workload (functional patterns) applied to the primary input of a digital circuit. The path was aged for four years, using simulation, with NBTI and HCI effects at room temperature. We can observe from Fig. 13 that the degradation of the path used for one year is around 10% while if the circuit is used for four years, the degradation is about 17%, indicating that most aging occurred at the early usage phase of the circuit.

The approach in [18] consists of three major steps. First, paths are simulated and selected according to their aging rate. Next, the delay of these paths is measured by a clock sweeping technique in new ICs (either during manufacturing test on all ICs or during authentication on a sample of new ICs) and in any available devices under authentication.

Statistical analysis is used to decide whether the device under authentication is a recycled IC. The same test patterns will be applied to the circuit under authentication, taken from the market, in a near-identical environment. The path-delay information of the circuit will then be processed by the same statistical data analysis methods. In a simple analysis, if the fingerprint of the circuit is outside the range of the new ICs' fingerprint, there is a high probability that the circuit is a recycled IC. Otherwise, it is likely a new IC. The longer the circuit has been used in the field, the more aging effects it will have experienced, making it easier to identify.

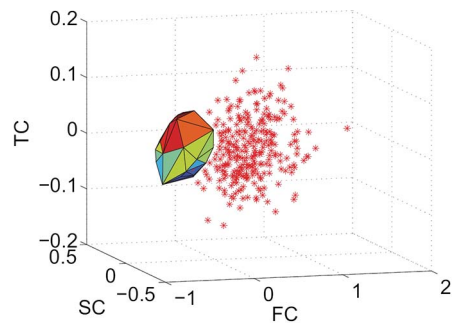


Fig. 14. *PCA results of the ICs used for three months with process variation [18].*

The recycled IC identification flow was demonstrated using 45-nm technology on a few benchmarks. HSPICE MOSRA [56] is used to simulate the effects of aging on the path delay of different benchmarks. Fig. 14 shows the PCA results of the ICs used for three months with process variation. The used ICs are represented by red dots; the convex hull is built up from new ICs' data, and represents the fingerprint for new ICs. It can be observed that the used ICs are completely separated from the signature of the new ICs, implying a 100% detection rate for recycled ICs.

We note that in cases where the counterfeit ICs are affected by large process variation, detecting these counterfeit ICs using statistical methods may be challenging, since patterns of counterfeit chips and golden chips tend to overlap in the space of parametric and side-channel measurements. To avoid/mitigate the impacts of large process variations, techniques proposed to detect hardware Trojans can be adopted for counterfeit detection purpose. In [57], advanced signal processing techniques based on Karhunen–Loève expansion are used to find a signal subspace from which the process noise is absent in order to identify Trojans that are well hidden within the variations of the signals generated by the process noise. In [58], it is shown that using postsilicon multimodal thermal and power characterization techniques, one can significantly improve the Trojan detection sensitivity, even under large process variations. In [59], it is demonstrated that measuring currents locally and from multiple power ports or pads can greatly enhance Trojan detection. A region-based transient-power signal analysis method to reduce the impact of increasing process variation in detecting hardware Trojans was discussed in [60]. It is shown that using signal calibration techniques, one can further increase the distance between Trojan-free and Trojan-infested circuits under different process parameters.

D. Counterfeit Detection Summary

The production and distribution of counterfeit parts are rising, and more of such parts are finding their way into consumer and military devices. As counterfeiters become more sophisticated, so must the methods used for detecting counterfeit parts. Over the last decade, multiple methods have been successfully utilized to detect counterfeit parts in an attempt to keep them from being used in final assemblies.

Table 4 summarizes different types of counterfeits and detection methods. As seen, there is no single test which can work to detect all counterfeit components. The parts themselves are different, the uses are varied, and, therefore the test plan for each component must be customized. A full suite of tests is required to identify counterfeit components. The functional and parametric tests have been vital in testing electronic components for over 40 years and are a

Table 4 Summary of Counterfeit Detection Methods

Detection Methods	Recycled	Remarked	Overproduced	Out-of-spec/Defective	Cloned
Low Power Visual Inspection (LPVI)	Low	Low	NA	NA	NA
X-Ray	Low	NA	NA	NA	NA
Microblast Analysis	Low	Medium	NA	NA	NA
Scanning Acoustic Microscopy (SAM)	Medium	NA	NA	NA	NA
Scanning Electron Microscopy (SEM)	Medium	Medium	NA	NA	Low
Material Analysis	Medium	Medium	NA	NA	NA
Parametric Tests	Medium	Low	Low	Medium	Low
Functional Tests	Medium	Low	Low	Medium	Low
EFR Analysis	Medium	Medium	Low	Low	Low
Path-Delay Analysis	Medium	Medium	Low	Low	Low

* Forged documentation and tampered types are not discussed here because of their unique detection challenges.

paramount tool for containing the counterfeit component epidemic plaguing our industry. However, in the electronics industry, it may not be practical cost-wise and time-wise to test every single functional and parametric requirement of the manufacturer. Proper strategic planning and outlining of tests between test lab and clients are important to establish an objective of performance measurement. Highly sophisticated counterfeit components may work under a subset of operating conditions but fail under others. Testing over a range of different test methods on the device will provide the highest level of assurance that electronic components are genuine. It is important to note that additional research is needed in early failure rate (EFR) data analysis and circuit path-delay analysis to verify the effectiveness of these methods for determining if a used part is sold as new. Preliminary analysis and results from these methods are encouraging.

III. COUNTERFEIT AVOIDANCE

Detection of counterfeit components is a major challenge because of the excessive test time, cost, and lack of metrics to evaluate the test confidence in evolving area of concern due to the rapidly changing threat environment. The issue urgently necessitates the development of innovative avoidance mechanisms to be incorporated in the design. These measures help detecting suspect parts without the need for aforementioned expensive detection methods. In this section, we will briefly describe some currently available avoidance methods.

A. CDIR Sensors

The combating die and IC recycling (CDIR) sensor was developed to prevent parts from recycling [26], [27]. The authors proposed three different structures to implement CDIR sensors. The first technique inserts a lightweight ring oscillator (RO)-based sensor in the chip to capture the usage of the chip in the field and provides an easy detection capability. Fig. 15 shows the structure for this RO-based sensor. This sensor is composed of a reference ring oscillator (reference RO) and a stressed ring oscillator (stressed RO). The sensor relies on the aging effects of MOSFETs to change the RO frequencies. The difference between the frequency of reference and stressed ROs gives the approximate usage time of the chip in the field.

The other two structures are antifuse-based sensors which are composed of counters and an embedded antifuse memory block. The counters are used to record the usage time of ICs while their values are continuously stored in an

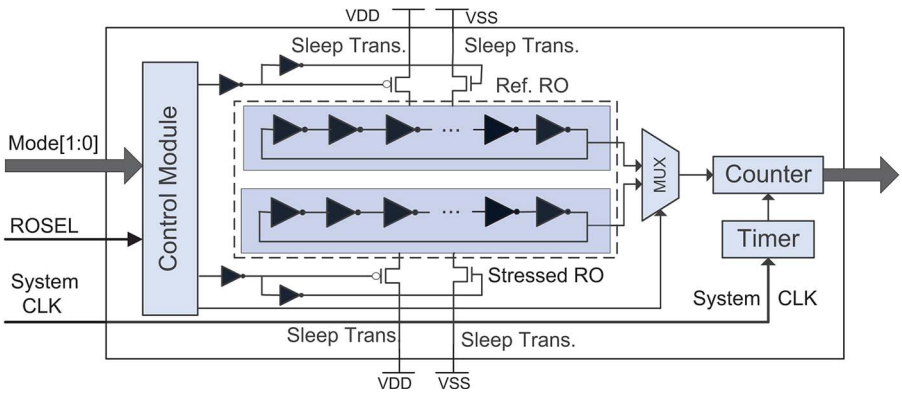


Fig. 15. *RO-based CDIR sensor [26].*

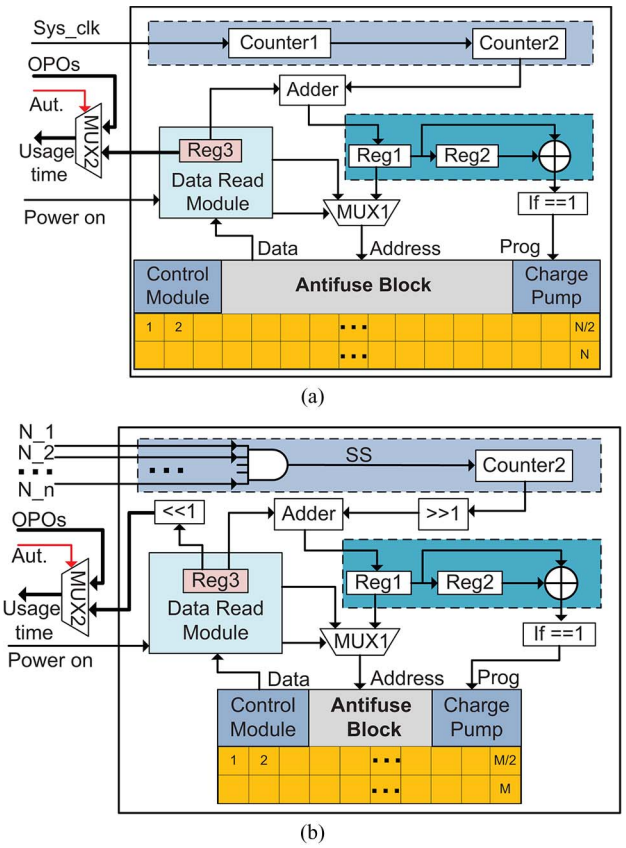


Fig. 16. ***Structure of the antifuse-based CDIR sensors [27]. (a) CAF-based CDIR sensor. (b) SAF-based CDIR sensor.***

antifuse memory block. Since the antifuse memory block is onetime programmable, the counterfeiters cannot erase the data during the recycling process. Two different structures of the antifuse-based sensors are shown in Fig. 16. These CDIR sensors use a MUX (MUX2) and an authentication (Aut.) pin to send the usage time to the output. Original primary outputs (OPOs) will go through MUX2 in the normal functional mode, while the data read module will set the antifuse IP in read mode, and the usage time will go through MUX2 in authentication mode. In manufacturing test mode, the functionality of these sensors will be disabled and structural fault test patterns will be applied to the sensor. A detailed description of these sensors is found in [27].

Fig. 16(a) shows the structure of the clock antifuse (CAF)-based sensor. It 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. Fig. 16(b) shows the structure of the signal antifuse (SAF)-based sensor. It uses circuit activity as trigger (clock) to the counter. A number of signals with low switching probability are selected to calculate the usage time. The SAF-based sensor generally requires less area overhead than the CAF-based sensor.

The area overhead of antifuse-based sensors is larger than the RO-based sensor because of the counters and the antifuse memory block. These antifuse-based sensors can be implemented in today's large VLSI chips as they result in negligible area overhead, whereas RO-based sensors can be placed in any digital chips. However, the major advantage of antifuse-based sensors is that the usage time stored in the memory to identify recycled ICs will not be impacted by technologies (i.e., older technology designs may not age as much as the new ones do), packages, assemblies, or process variations.

B. Secure Split Test (SST)

The high cost of creating a state-of-the-art manufacturing facility for high-density IC fabrication has led the semiconductor business model to grow horizontally across the globe [61]. This is also true for many assembly companies. The foundries fabricate wafers and dies, test them, and ship them to assemblies. The assemblies then package the dies, test, and ship them either to the design house (IP owners) or directly to the market. However,

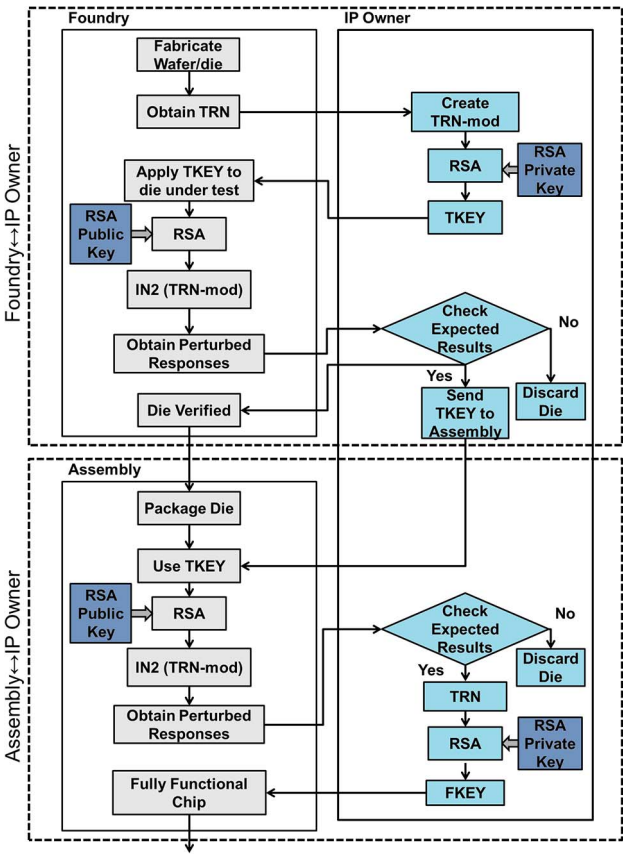


Fig. 17. ***Communication between IP owner, foundry, and assembly [19].***

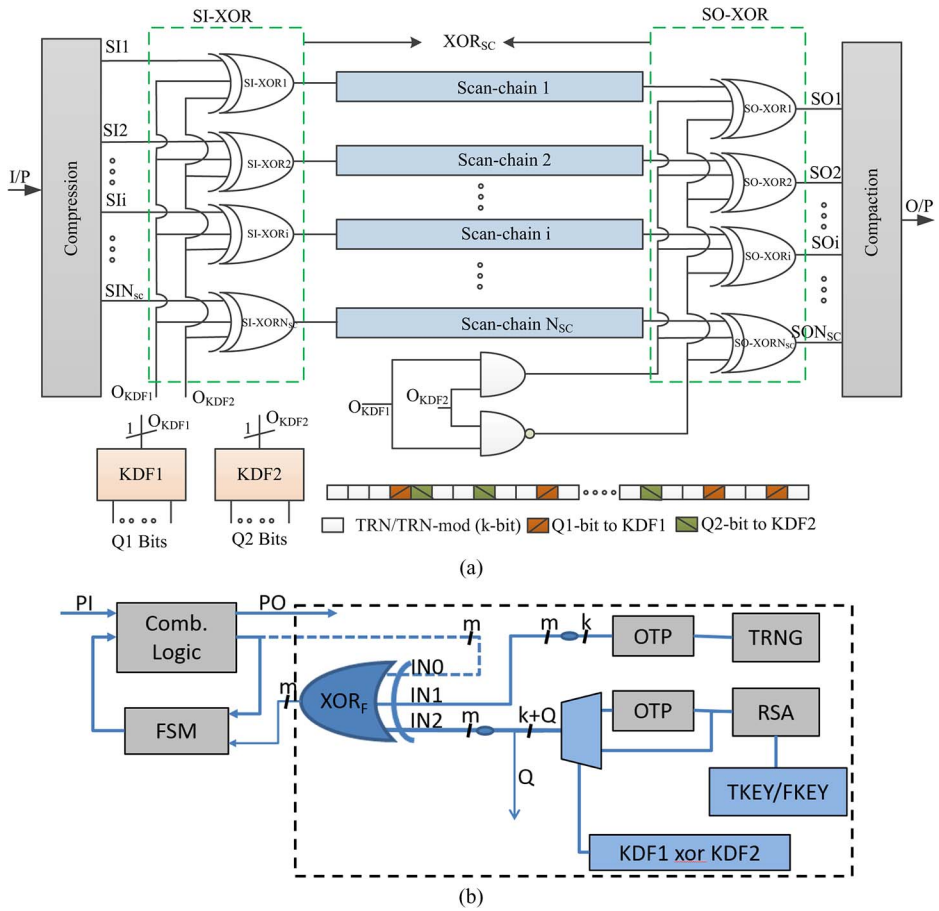


Fig. 18. ***Internal architecture of SST inside ICs [19]. (a) Scan locking block. (b) Functional-locking block with m = pk expansion.***

some untrusted foundries and assemblies can sell defective, out-of-spec, or even overproduced ICs on the open market. Secure split test (SST) secures the manufacturing test process to prevent counterfeits, allowing the design house to protect and meter their IPs [19]. SST introduces hardware components for cryptography and locking mechanisms to block the correct functionality of an IC until it is activated by the IP owner during or after the test. Thus, SST brings design houses back into the manufacturing test process.

Fig. 17 shows the communication flow between IP owner, foundry, and assembly. The IP owner first obtains a die's true random number (TRN) from foundry and modifies it in such a way that only he knows it. A test key (TKEY) is then generated from this modified TRN and the IP owner's private key. The IP owner sends the TKEY to the foundry for each die. The chip then encrypts the modified TRN by using a public key and tests the die using this modified TRN. It then sends the response back to the IP owner for the pass/fail decision. After verifying the die, the foundry sends it to the assembly. After packaging the die, the assembly tests the parts again. The assembly then sends the response to the IP owner. The IP owner then unlocks the good ICs using the final key (FKEY) and sends them to the market.

Fig. 18 shows the SST architecture. It secures the test processes of ICs by inserting scan locking block and functional-locking block in the design. The details of a scan-locking block are presented in Fig. 18(a). In scan-locking block, the inputs to some scan chains are inverted when FKEY is applied; the input bits are transparent when TKEY is applied. At the same time, the output from some of the scan chains can be inverted when TKEY is applied and transparent otherwise. This block is introduced so an attacker cannot extract any information from an unlocked IC. The scan-locking block consists of three-input XOR gates inserted at scan chain inputs (SI–XOR) and outputs (SO–XOR) and two key-determining functions (KDFs). Each KDF is composed of XOR gates forming an XOR odd-function circuit which outputs 1 if the input is odd (odd number of 1s) or 0 if it is even (even or zero number of 1s). Two KDFs, KDF1 and KDF2, are used to detect the type of key that has been provided by IP owner and determine the function of the scan-locking mechanism. The outputs of KDFs, OKDF1 and OKDF2, are fed to the three-input XOR gates through some logic gates to make the XORs

transparent (when KDF1= KDF2) or inverting (when KDF1 = KDF2). The Q bits needed to control each KDF are added to TRN and TRN-mod by the IP owner. Q is divided into two parts $Q1$ and $Q2$ as inputs for KDF1 and KDF2, respectively. The position of Q additional bits is random and known only by the IP owner since TRN-mod and TRN are encrypted and only TKEY and FKEY are visible by the foundry.

The functional-locking block's purpose is to ensure that only unlocked ICs will have the correct functionality. ICs will only function correctly when the IP owner sends the correct functional key. The functional-locking block is made up of three smaller hardware blocks, an XOR_F mask for functional locking, true random number generator (TRNG), and RSA decryption logic, as shown in Fig. 18(b). SST inserts the XOR_F mask on noncritical paths in the circuit. These XORs have three inputs connected to circuit paths (IN0), TRNG output (IN1), and RSA output (IN2). An XOR_F is transparent only when both inputs coming from the TRNG and RSA outputs are the same; otherwise it acts as an inverter. The TRNG output is different for each IC but it is constant throughout the IC's lifetime since it is stored in a onetime programmable (OTP) memory. The RSA component receives an encrypted key from the IP owner; this key is decrypted and connected to IN2. The circuit only becomes functional when the appropriate RSA input is applied; this gives the IP owner control over when/whether to activate the IC. The encryption and transmission of the key make up the communication component of SST. A server owned by the IP owner receives TRNs for each die and creates test keys (TKEYs); it then receives test outputs and compares them to the expected outputs to determine which dies have passed or failed. The same procedure is followed during assembly. The server decides whether an IC has passed the necessary tests after assembly, and only then, it sends the functional key (FKEY) to activate and unlock the IC.

Different types of attacks have been analyzed in [19]. SST is very efficient in preventing overproduced ICs as the design house unlocks the number of ICs they want. As the decision of the test process is taken by the design house, the foundry cannot source defective/out-of-spec ICs in the supply chain. Cloned ICs can also be detected by checking the registered ID of the IC in design house's secured database.

C. Hardware Metering

Hardware metering places a set of security protocols that enable the design house to achieve postfabrication control of the produced ICs. This method provides the design house with a unique way to identify each IC produced with the same masks [21], [62]. Hardware metering is broadly categorized into passive or active types. Early passive metering includes indented and digitally stored serial numbers on the ICs as a nonfunctional identification method. In functional identification, PUFs are introduced to uniquely identify each IC and register the IC using

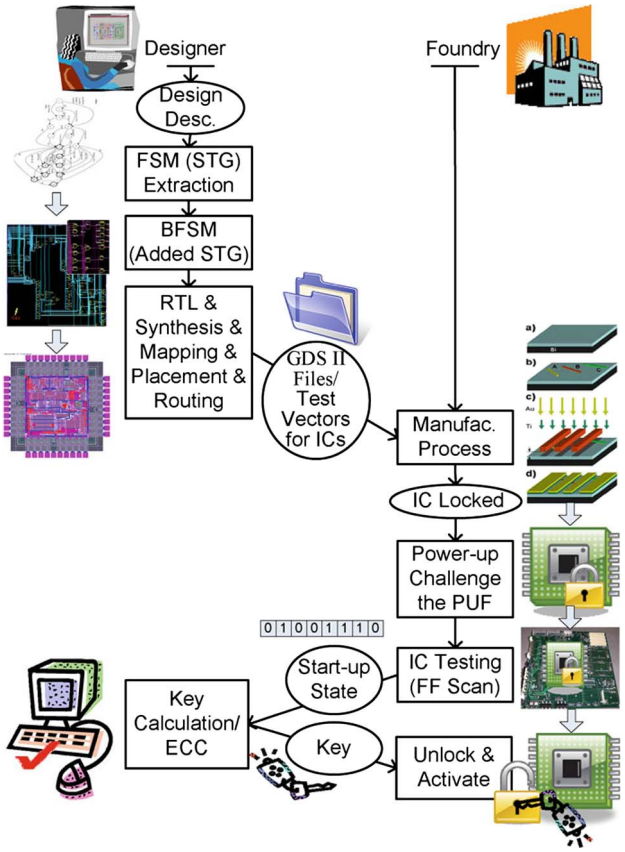


Fig. 19. *IC enabling flow by active metering [68].*

challenge–response pairs to prevent cloning and removal attacks. The ICs are authenticated by searching the response stored in the challenge–response pair database [62]–[67].

In addition to unique identification, active metering approaches lock each IC until it is unlocked by the IP holder [20], [69]–[73]. This locking is mostly done in three ways: 1) initializing ICs to a locked state on power-up [20]; 2) combinational locking by scattering XOR gates randomly throughout the design [71]–[73]; and 3) adding a finite-state machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs [70], [74].

In [75] and [76], a logic encryption technique is used to hardwire designs with built-in keys that are unique to each IC, and ensures that the application of any invalid key on the protected design forces the design to produce incorrect results. Logic encryption inserts additional circuit elements into the original design. It has been shown in [75] that testing concepts such as fault activation, propagation, and masking can be utilized to guide the insertion of key gates. This way, a perfect control over the functional corruption due to invalid key application can be achieved. The same concepts can not only be utilized by an attacker to leak the secret logic encryption key, but also by a

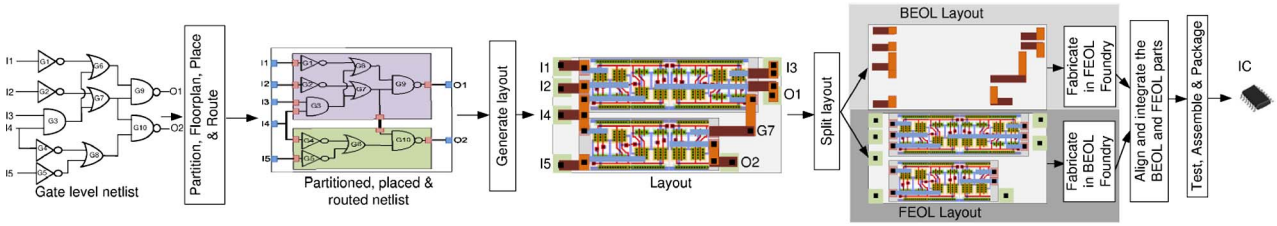


Fig. 20. *Split-manufacturing-aware design flow [80].*

designer to guide the insertion of key gates in attaining a hard-to-break logic encryption [76]. Fig. 19 shows an IC enabling flow by active metering [77].

In [78], Barak *et al.* lay the theoretical groundwork for adopting obfuscation as a means for protecting programs. An obfuscator $\mathcal{O}$ is defined as a "compiler" that takes as input a program (or circuit) P and produces a new program $\mathcal{O}(P)$ that has the same functionality as P yet is "unintelligible" in some sense. Obfuscators would have a wide variety of cryptographic and complexity-theoretic applications, ranging from software protection to homomorphic encryption. Most of these applications are based on an interpretation of the "unintelligibility" condition in obfuscation as meaning that $\mathcal{O}(P)$ is a "virtual black box," in the sense that anything one can efficiently compute given $\mathcal{O}(P)$, one could also efficiently compute given oracle access to P.

D. Split Manufacturing

Globalization of IC design flow has led to several security vulnerabilities. In order to mitigate the risks in manufacturing, split manufacturing approach has been proposed [79]. In this approach, the layout of the design is split into the front end of line (FEOL) layers and back end of line (BEOL) layers which are then fabricated separately in different foundries. The FEOL layers consist of transistors and other lower metal layers and the BEOL layers consist of the top metal layers. Postfabrication, the FEOL and BEOL wafers are aligned and integrated together using either electrical, mechanical, or optical alignment techniques. The final ICs are tested upon integration of the FEOL and BEOL wafers. The asymmetrical nature of the metal layers facilitates split manufacturing [80].

Fig. 20 shows an example of split-manufacturing-aware IC design flow, as depicted in [80]. A gate level netlist is partitioned into blocks which are then floorplanned and placed. The transistors and wires inside a block form the FEOL layers. The top metal wires connecting the blocks and the IO ports form the BEOL layers. The layout of the entire design is then split into FEOL and BEOL layers. The two layouts are then fabricated in two different foundries. Finally, FEOL and BEOL layouts are integrated by using electrical, mechanical, or optical alignment techniques and tested for defects.

E. IC Camouflaging

During the manufacturing, the chips can also be cloned in an unauthorized production by reverse engineering the original design or pirating the IP. In an effort to hamper an attacker from reverse engineering a chip, IC camouflaging has been proposed by introducing dummy contacts into the layout [81]. By using a mix of real and dummy contacts, one can camouflage a standard cell whose functionality can be one of many. If an attacker cannot resolve the functionality of a camouflaged gate, he/she will extract an incorrect netlist.

In one embodiment of IC camouflaging, the layouts of logic gates are designed to look identical, resulting in an incorrect extraction. To thwart reverse engineering of an

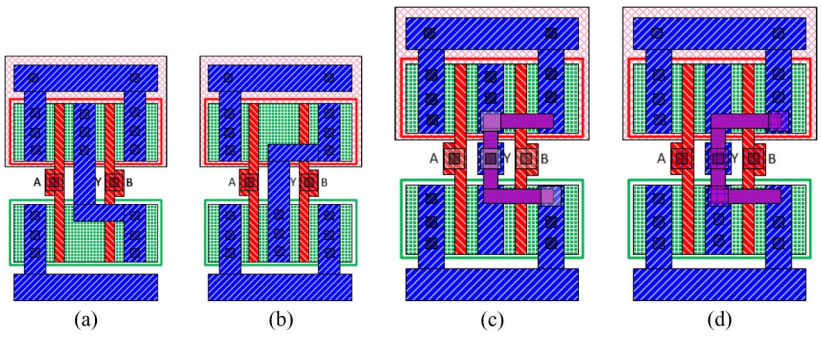


Fig. 21. *Example of IC camouflaging: standard cell layout of regular two-input (a) NAND and (b) NOR gates and camouflaged NAND (c) and NOR (d) gates [82].*

IC, any camouflaging technique has to provide resiliency to reverse engineering and corrupted outputs. The reverse engineer's inability to partially etch a layer is the basis for dummy contacts-based camouflaging. Contacts are conducting materials that connect two adjacent metal layers or a metal layer 1 and poly. They pass through the dielectric that separates the two connecting layers. While the true contact has no gap, a dummy contact has a gap in the middle and fakes a connection between the layers [82].

Fig. 21 shows an example of IC camouflaging as depicted in [82]. The layout of regular NAND and NOR cell shown in Fig. 21(a) and (b) looks different and is hence easy to reverse engineer. However, the layout of camouflaged NAND and NOR cell shown in Fig. 21(c) and (d) looks identical and is difficult to differentiate. When deceived into incorrectly interpreting the functionality of the camouflaged gate, the attacker may obtain a reverse-engineered netlist that is different from the original. The netlist obtained by an attacker is the deceiving netlist where the functionality of the camouflaged gates is arbitrarily assigned.

F. Hardware Watermarking

Hardware watermarking [83] has received much attention in the recent years to secure hardware intellectual properties (IPs) used in high-density ICs (e.g., system on chips). The reuse of these IPs poses a great concern to the industry as the infringement of IPs, e.g., trademark, copyright, or patent violation during the design. Hardware watermarking uniquely identifies an IP by creating a unique fingerprint in it. In recent years, different watermarking techniques have been proposed. Constraint watermarking affects the IP core at the GDSII level. The goal of constraint watermarking is to create a physical design pattern that can be demonstrated to but not be replicated purely by coincidence [84]. This is referred to as "proof of authorship," the probability that the occurrence of a watermark on a known nonwatermarked IP core is purely coincidental. Watermarks can be inserted into the bitstream of an IP core by injecting watermark bits into unused combinational logic block outputs. Another implementation of constraint watermarking involves breaking paths of logic into subpaths, each with unique timing constraints that add up to the timing constraint of the original path. In [85], Castillo *et al.* propose a hardware description language (HDL) level watermarking. They store the digital signature within memory structures or combinational logic that are part of the system, at the high level description of the design. In [86], Lach *et al.* propose a cryptographically encoded signatures to be placed in a field-programmable gate array (FPGA) design component to identify original recipient. Another watermarking method for IP protection was proposed at the combinational-logic-synthesis level [87].

G. Physical Unclonable Functions

Reverse-engineering tools such as microprobing, laser cutting, glitch attacks, and power analysis have become very advanced to date and allow an attacker to read and copy the stored encrypted information in a device. To overcome this challenge, hardware intrinsic security (HIS) has been proposed as a mechanism that can provide security based on inherent properties of an electronic device [23]. PUFs [24], for example, belong to the category of such HIS mechanisms. PUFs aim to measure the responses of hardware to certain given inputs, which depend on the unique physical properties of the device, since process variations affect each device in a unique and unclonable fashion.

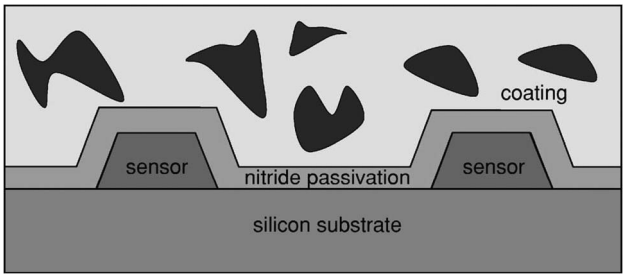


Fig. 22. ***Structure of a coating PUF [88].***

Rather than creating a single encrypted key, PUFs implement challenge–response authentication. When a stimulus is applied to the device, it reacts in an unpredictable (but repeatable) way due to the complex interaction of the stimulus with the physical structure of the device. This exact structure depends on physical factors introduced during manufacture which are unpredictable. The applied stimulus is called the challenge, and the reaction of the PUF is called the response [24]. A specific challenge and its corresponding response together form a challenge–response pair.

Various methods have been proposed to obtain this challenge–response pair. In [24], optical characteristics are exploited by using the speckle patterns of optical medium of laser light. The PUF consists of a transparent material that is doped with light scattering particles. When a laser beam shines on the material, a random and unique speckle pattern will arise. The placement of the light scattering particles is an uncontrolled process, and the interaction between the laser and the particles is very complex. Therefore, it is very hard to duplicate the optical PUF such that the same speckle pattern will arise.

A coating PUF was proposed in [88], where a network of metal wires is laid out in a comb shape in the top layer of an IC. The space between and above the comb structure are filled with an opaque material and randomly doped with dielectric particles. Fig. 22 illustrates the structure of a coating PUF, as proposed in [88]. The manufacture of the coating is an unpredictable mixing process, therefore, size and dielectric strength of the particles will be random up to a certain extent. Consequently, the measured capacitance values are unpredictable. This unique randomness can be used to obtain a unique identifier for the device carrying the coating PUF. Moreover, the placement of this

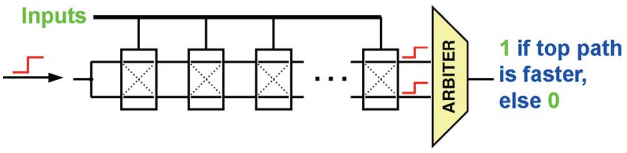


Fig. 23. *Delay PUF circuit: two delay paths with the same layout length for each input, and an output based on which path is faster [63], [91], [92].*

opaque PUF in the top layer of an IC protects the underlying circuits from being inspected by an attacker, e.g., for reverse engineering. When an attacker tries to remove (a part of) the coating, the capacitance between the wires is bound to change and the original unique identifier will be destroyed. In [89], an unclonable RFID tag is built using coating PUFs.

In [63], [90], and [91], a delay PUF exploiting the random variations in delays of wires and gates on silicon was proposed. Given an input challenge, a race condition is set up in the circuit, and two transitions that propagate along different paths are compared to see which comes first. An arbiter, typically implemented as a latch, produces a 1 or a 0, depending on which transition comes first. Fig. 23 illustrates the implementation of delay PUFs. The inputs determine the delay path of each switching block shown by rectangles in Fig. 23. The switching block is typically made by a pair of multiplexers controlled by the same input bit. The signal goes through only one path at a time in the block, which is controlled by the input bit. In this way, the circuit can create a pair of delay paths for each input combination.

The authentication of delay PUFs is illustrated in Fig. 24. As explained in [63], the PUF can have an exponential number of challenge–response pairs where the response is unique for each IC and each challenge. These unpredicted responses can be stored by a trusted party in a database for future authentication operations. To check the authenticity of an IC later, the trusted party selects a challenge that has been previously recorded but has never been used for an authentication operation, and obtains the PUF response from the IC. If the response matches the previous recorded one, the IC is then considered authentic.

A PUF based on ring oscillators was also discussed in [63]. A secure processor design using a PUF was shown in [93]. In [92], it was shown that the delay PUFs can be integrated into a small passive RFID tag for anticounterfeiting and secure access.

Other types of PUF implementation include SRAM PUFs [94], butterfly PUFs [64], and bistable ring PUFs [95], [96].

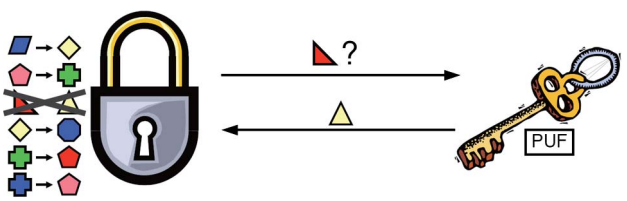


Fig. 24. *Delay PUF authentication [63], [91], [92].*

H. Package ID

The counterfeit avoidance measures discussed so far can only be implemented on dies that only target new large ICs. However, there is a wide variety of components that need to be addressed for counterfeit avoidance. These components mainly belong to: 1) large and small new analog; 2) small new digital; and 3) all active and obsolete categories. There are several challenges for the implementation of chip IDs in these designs. First, there is not enough space for adding any extra hardware to the designs. Second, one does not have the authority and option to make changes in the masks for active components. Finally, obsolete components are no longer manufactured. 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. DNA markings and nanorods are the viable options to create package IDs.

In DNA markings, a unique genetic sequence is generated by scrambling the plant DNA and mixing these new sequences with inks. These inks are then applied on the packages of the ICs at the end of the packaging process for new components. The active and obsolete components are authenticated first and then this DNA marking is placed on the package. 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 [28]. Recently, Department of Defense (DOD) mandated [97] that the DNA marking be placed on the components in order to track them throughout the supply chain. In nanorods, a microscopic pattern is created by growing an array of nanospheres to make nanorods that are less than 100 nm long [29]. Each time the process is repeated, the same pattern is created, but the exact angle and length of each individual nanorod 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 nanorod to a database.

I. Summary of Counterfeit Avoidance Methods

Table 5 shows the summary of counterfeit avoidance methods. The first column represents avoidance methods discussed in this paper. Columns 2–6 and 7–9 show counterfeit types and component types, respectively. Each entry in columns 2–6 represents how effective the methods are at detecting that counterfeit type. Each entry in columns 7–9 shows target component types with avoidance effectiveness. CDIR sensors can detect only recycled and remarked

Table 5 Summary of Counterfeit Avoidance Methods

Avoidance Methods	Counterfeit Types*					Component Types		
	Recycled	Remarked	Overproduced	Out-of-spec/ Defective	Cloned	Obsolete	Active	New
CDIR Sensors	High	High	NA	NA	NA	NA	NA	High
Secure Split Test (SST)	NA	NA	High	High	Medium	NA	NA	Medium
Hardware metering	NA	NA	Low	NA	Low	NA	NA	Medium
Split Manufacturing	NA	NA	Low	NA	Low	NA	NA	Medium
IC Camouflaging	NA	NA	NA	NA	Low	NA	NA	Medium
Hardware Watermarking	NA	NA	NA	NA	Medium	NA	NA	Medium
Physically Unclonable Functions (PUFs)	NA	NA	Low	NA	Low	NA	NA	Medium
Package ID	Medium	Medium	NA	NA	NA	High	High	High

* Forged documentation and tampered types are not discussed here because of their unique avoidance challenges.

new components. SSTs can target overproduced, cloned, and out-of-spec/defective parts. Hardware metering and PUFs can detect only cloned and overproduced components, while package ID can aim only for recycled and remarked types. IC camouflaging and hardware watermarking can be used to detect only cloned ICs. Overproduced and cloned ICs can be detected by split manufacturing. All these avoidance methods, except package ID, can target only new components. While many of the conterfeit avoidance methods could be useful for resolving the counterfeit problem, many of the techniques are not deployed in a production environment. Many of the techniques are promising, but need further research and development.

IV. DETECTION AND AVOIDANCE CHALLENGES

The limited research and development in the domain of counterfeit detection and avoidance has left major challenges to be addressed. In addition, the need to addressing this problem requires immediate action by industry, government, and academia since the impact of counterfeit electronics will not only be seen on business but also on our daily life. Lack of innovative and comprehensive solutions to detect counterfeit parts could be catastrophic.

The challenges we deal with today arise from the fact that: 1) the number of counterfeit parts entering the electronic component supply chain is increasing; 2) the sophistication of the techniques used by the counterfeiters is increasing; 3) there are different types of electronics components and one solution will not address this challenging problem for all types of counterfeit parts and types; 4) multiple test methods are required to detect the multiple known anomalies and are proven ineffective for detecting all types of counterfeit parts; 5) there is a lack of sufficient support to academia for developing innovative detection and avoidance solutions; and 6) there is a lack of sufficient amount of counterfeit data (types, defects, test cost, test time, etc.).

As a consequence, today, we cannot identify a part as counterfeit with a very high level of confidence without performing multiple test methods and/or receiving input from the original component manufacturer to assist in providing needed data, verifying the results and assisting in the final conclusion. There is clearly a need for the development of anticounterfeit mechanisms during design of the ICs. New methods are needed to allow track and trace of the components in the supply chain. Metrics are needed to evaluate the effectiveness of the existing test methods. New data collection mechanisms are needed to continuously monitor counterfeit activities and help the community understand the current trends and new threats. The processes defined must ensure detection, but must also balance the cost and lead-time issues associated with destruction of components, and nonrecurring engineering costs and testing. Sophisticated counterfeits may not be detected by a simple external, physical inspection process. New test techniques are needed to detect all defects and anomalies associated with counterfeit parts [15] in a comprehensive fashion.

A. Detection Challenges

Physical inspections suffer from several challenges. First, many of them are destructive; sample preparation is extremely important as it directly relates to the test confidence. The chance of selecting a counterfeit component from a lot is extremely small. Second, test time and cost are major limiting factors in the use of physical tests for counterfeit detection. For some tests, it may take up to several hours (e.g., typically more than eight hours for SEM analysis or to perform functional electrical tests that includes set-up) to test a single component. Third, most of the tests are carried out without automation and with no metrics for quantifying against a set of counterfeit types, anomalies, and defects. The test results are mostly dependent on the subject matter experts (SMEs) interpretation of results to distinguish between quality issues and counterfeit issues. The decision-making process is then error prone as it entirely depends on the operator or SMEs. It has been demonstrated by the G-19A group that a chip was marked as counterfeit in one lab while it was called authentic in another lab [98].

There are several limitations that make electrical tests ineffective. Increased process variations and environmental variations in lower technology nodes make the parametric test results indeterminate as the electrical parameters of a component vary significantly. Obsolete and active parts make the functional tests ineffective as test program generation for those parts with limited knowledge of functionality is extremely difficult if not impossible to obtain data or manufacturer test fixtures. The design and test information for the obsolete parts may be lost, or the OCM may no longer exist, as the design may have been sunset decades ago. Burn-in tests are helpful in detecting infant mortality failures of components, but are extremely expensive and time consuming. These tests are attractive and useful only for critical and high-risk, high-reliability applications where obtaining a high test coverage is of prime importance because of excessive test time and cost. Total access to the internal scan chains of a component is required for structural tests to be effective. Generally, IP owners disable the scan chains by using fuses to prevent the outside world from having access to their designs. Even if the scan is accessible, limited knowledge of the chip design and layout makes such test ineffective. Moreover, for obsolete parts, design for testability (DFT) may not even exist.

B. Avoidance Challenges

Counterfeit avoidance techniques, described in Section III, are still a work-in-progress and they pose unique challenges that must be addressed before deployment into the high-reliability systems. For instance, in the hardware metering technique, the untrusted foundry can fabricate more ICs while pretending the yield is low. That allows them to put more functioning chips into the market. A design house cannot prevent out-of-spec and defective ICs from entering the supply chain through an untrusted access point. As for PUFs, reliability is the major concern that must be addressed. PUFs are proven to be sensitive to a wide range of environmental variations (temperature, power supply noise), and aging.

DNA markings suffer from several limitations that introduce serious concerns about their applicability in counterfeit avoidance at the large scale. The fast authentication achieved by observing the fluorescence of markings under specific light can potentially be imitated by counterfeiters, either by invalid DNA or by other materials. The detailed DNA validation process is extremely time consuming and costly [99]. For fast authentication, nanorods must also deal with the same issues as in DNA markings. The reliability of the materials used by both methods cannot be completely verified.

The avoidance solutions must also consider the part types (analog, digital), the part size, the applications risks, cost of inserting the anticounterfeit measures, potential attacks, etc.

V. CONCLUSION

Detection and/or prevention of counterfeit electronic components have become a major challenge in the electronic component supply chain. In this paper, we first presented the various counterfeit types currently present in the supply chain, followed by a taxonomy of counterfeit detection methods which describes existing capabilities for counterfeit detection. We also briefly described some well-known physical and electrical inspection methods. We then presented counterfeit avoidance measures to emphasize what needs to be done in order to detect these counterfeit components in a proactive, rather than reactive manner, if such measures were to be in place. We presented the key challenges in counterfeit detection and avoidance, as well as contemporary research opportunities. ■

Acknowledgment

The authors would like to thank Steve Walters of Honeywell (Clearwater, FL, USA) and Sultan Lilani of Integra Technologies (Wichita, KS, USA) for providing their valuable feedback on physical inspection methods. They would also like to thank Prof. M. Anwar of the University of Connecticut (Storrs, CT, USA) for his comments on physical inspections.

REFERENCES

[1] U.S. Senate Committee on Armed Services, "Inquiry into counterfeit electronic parts in the Department of Defence supply chain," May 2012. [Online]. Available: http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf

[2] U.S. Department of Commerce, "Defense industrial base assessment: Counterfeit electronics," Jan. 2010.

[3] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectrum*, vol. 43, no. 5, pp. 37–46, May 2006.

[4] N. Kae-Nune and S. Pesseguier, "Qualification and testing process to implement anti-counterfeiting technologies into IC packages," in *Proc. Design Autom. Test Eur. Conf.*, 2013, pp. 1131–1136.

[5] S. Bastia, "Next generation technologies to combat counterfeiting of electronic components," *IEEE Trans. Compon. Packag. Technol.*, vol. 25, no. 1, pp. 175–176, Mar. 2006.

[6] IHS, "Reports of counterfeit parts quadruple since 2009, challenging U.S. Defence Industry and National Security," Apr. 2012. [Online]. Available: http://www.ihs.com/images/IHS-iSuppli-Reports-Counterfeit-Parts-Quadruple-Since-2009.pdf

[7] U. Guin, M. Tehranipoor, D. DiMase, and M. Megrdician, "Counterfeit IC detection and challenges ahead," in *ACM SIGDA E-Newslett.*, vol. 43, no. 3, Mar. 2013.

[8] Semiconductor Industry Association (SIA), "Winning the battle against counterfeit semiconductor products," Aug. 2013.

[9] S. Nevison, "Counterfeit parts infiltrate aerospace projects," *Industry Market Trends*, Apr. 2009.

[10] IHS Technology, "Top 5 most counterfeited parts represent a $169 billion potential challenge for global semiconductor market," Apr. 4, 2012. [Online]. Available: http://www.isuppli.com/Semiconductor-Value-Chain/News/pages/Top-5-Most-Counterfeited-Parts-Represent-a-$169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx

[11] D. Pantic, "Benefits of integrated-circuit burn-in to obtain high reliability parts,"

IEEE Trans. Reliab., vol. 35, no. 1, pp. 3–6, Apr. 1986.

[12] J. Carulli and T. Anderson, "Test connections—Tying application to process," in *Proc. IEEE Int. Test Conf.*, 2005, DOI: 10.1109/TEST.2005.1584030.

[13] Aerospace Industries Association, "Counterfeit parts: Increasing awareness and developing countermeasures," Special Rep., 2011.

[14] U. Guin, D. DiMase, and M. Tehranipoor, "A comprehensive framework for counterfeit defect coverage analysis and detection assessment," *J. Electron. Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[15] U. Guin and M. Tehranipoor, "On selection of counterfeit IC detection methods," in *Proc. IEEE North Atlantic Test Workshop*, May 2013.

[16] K. Huang, J. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, 2012, pp. 7–12.

[17] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardware-Oriented Security Trust*, 2008, pp. 51–57.

[18] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, 2012, pp. 13–18.

[19] G. Contreras, T. Rahman, and M. Tehranipoor, "Secure split-test for preventing IC piracy by untrusted foundry and assembly," in *Proc. Int. Symp. Defect Fault Tolerance VLSI Syst.*, 2013, pp. 196–203.

[20] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. USENIX Security Symp.*, Berkeley, CA, USA, 2007, pp. 20:1–20:16.

[21] F. Koushanfar and G. Qu, "Hardware metering," in *Proc. Design Autom. Conf.*, 2001, pp. 490–493.

[22] K. Chatterjee and D. Das, "Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Trans. Compon. Packag. Technol.*, vol. 30, no. 3, pp. 547–549, Sep. 2007.

[23] V. V. de Leest and P. Tuyls, "Anti-counterfeiting with hardware intrinsic security," in *Proc. Design Autom. Test Eur. Conf.*, 2013, pp. 1137–1142.

[24] R. Pappu, "Physical one-way functions," Ph.D. dissertation, Program Media Arts Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.

[25] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost on-chip structures for combating die and IC recycling," in *Proc. ACM/IEEE Design Autom. Conf.*, 2014, DOI: 10.1145/2593069.2593157.

[26] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICS using fingerprints from a light-weight on-chip sensor," in *Proc. IEEE Design Autom. Conf.*, Jun. 2012, pp. 703–708.

[27] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 5, pp. 1016–1029, May 2014.

[28] M. Miller, J. Meraglia, and J. Hayward, "Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts," in *Proc. SAE Aerosp. Electron. Avion. Syst. Conf.*, Oct. 2012, DOI: 10.4271/2012-01-2104.

[29] C. Kuemin, L. Nowack, L. Bozano, N. D. Spencer, and H. Wolf, "Oriented assembly of gold nanorods on the single-particle level," *Adv. Funct. Mater.*, vol. 22, no. 4, pp. 702–708, 2012.

[30] U. Guin, D. Forte, and M. Tehranipoor, "Anti-counterfeit techniques: From design to resign," in *Proc. Microprocessor Test Verif.*, 2013, to be published.

[31] L. W. Kessler and T. Sharpe, "Faked parts detection," 2010. [Online]. Available: http://www.circuitsassembly.com/cms/component/content/article/159/9937-smt

[32] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan./Feb. 2010.

[33] SAE International, "Counterfeit electronic parts; Avoidance, detection, mitigation, and disposition," 2009. [Online]. Available: http://standards.sae.org/as5553/

[34] SAE International, "Fraudulent/counterfeit electronic parts; Tool for risk assessment of distributors," 2011. [Online]. Available: http://standards.sae.org/arp6178/

[35] SAE International, "Fraudulent/counterfeit electronic parts: Avoidance, detection, mitigation, and disposition—Distributors counterfeit electronic parts; Avoidance protocol, distributors," 2012. [Online]. Available: http://standards.sae.org/as6081/

[36] SAE International, "Fraudulent/counterfeit electronic parts: Avoidance, detection, mitigation, and disposition—authorized/franchised distribution." [Online]. Available: http://standards.sae.org/wip/as6496/

[37] SAE International, "Test methods standard; Counterfeit electronic parts." [Online]. Available: http://standards.sae.org/wip/as6171/

[38] Components Technology Institute (CTI), "Certification for counterfeit components avoidance program," Sep. 2011. [Online]. Available: http://www.cti-us.com/pdf/CCAP101Certification.pdf

[39] Independent Distributors of Electronics Association (IDEA), "Acceptability of electronic components distributed in the open market." [Online]. Available: http://www.idofea.org/products/118-idea-std-1010b

[40] J. Goldstein *et al.*, *Scanning Electron Microscopy and X-ray Microanalysis*. New York, NY, USA: Springer-Verlag, 2003.

[41] B. Hu and M. Nuss, "Imaging with terahertz waves," *Opt. Lett.*, vol. 20, no. 16, pp. 1716–1718, 1995.

[42] H. C. Chou, J. Zeller, U. Guin, M. Tehranipoor, and M. Anwar, "Time-domain THz spectroscopy for counterfeit IC detection," in *Terahertz Physics, Devices, and Systems VII: Advanced Applications in Industry and Defense*, Apr. 2013.

[43] G. F. Nelson and W. F. Boggs, "Parametric tests meet the challenge of high-density ICs," *Electronics*, vol. 48, no. 5, pp. 108–111, Dec. 1975.

[44] M. Soma, "Fault coverage of dc parametric tests for embedded analog amplifiers," in *Proc. Int. Test Conf.*, Oct. 1993, pp. 566–573.

[45] M. Bushnell and V. Agrawal, *Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits*. New York, NY, USA: Springer-Verlag, Nov. 2000.

[46] P. Mazumder and K. Chakraborty, *Testing and Testable Design of High-Density Random-Access Memories*. New York, NY, USA: Springer-Verlag, Sep. 1996.

[47] U.S. Department of Defense, "Test method standard: Microcircuits," 2010. [Online]. Available: http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-883/std883.pdf

[48] U.S. Department of Defense, "Test method standard: Test methods for semiconductor devices," 2012. [Online]. Available: http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-750/std750.pdf

[49] R. D. Eldred, "Test routines based on symbolic logical statements," *J. Assoc. Comput. Mach.*, vol. 6, no. 1, pp. 33–37, Jan. 1959.

[50] J. M. Galey, R. E. Norby, and J. P. Roth, "Techniques for the diagnosis of switching circuit failures," in *Proc. 2nd Annu. Symp. Switching Circuit Theory Logical Design*, Oct. 1961, pp. 152–160.

[51] S. Seshu and D. N. Freeman, "The diagnosis of asynchronous sequential switching systems," *IRE Trans. Electron. Comput.*, vol. EC-11, no. 4, pp. 459–465, Aug. 1962.

[52] Retronix, "Retronix curve trace test capability." [Online]. Available: http://www.retronix.com/uploads/downloads/Curve

[53] Kozio, Inc., "A functional test approach for counterfeit, substandard, and high risk microcircuit detection." [Online]. Available: http://www.eejournal.com/archives/on-demand/2013021901-kozio/

[54] H.-G. Stratigopoulos and Y. Makris, "Error moderation in low-cost machine-learning-based analog/RF testing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 27, no. 2, pp. 339–351, Feb. 2008.

[55] I. Jolliffe, *Principal Component Analysis*. New York, NY, USA: Springer-Verlag, 1986.

[56] Synopsys, "HSPICE user guide," 2010.

[57] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 296–310.

[58] K. Hu, A. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity hardware Trojan detection using multimodal characterization," in *Proc. Design Autom. Test Eur. Conf.*, 2013, pp. 1271–1276.

[59] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, "Hardware Trojan detection and isolation using current integration and localized current analysis," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Syst.*, 2008, pp. 87–95.

[60] R. Rad, X. Wang, M. Tehranipoor, and J. Plusquellic, "Power supply signal calibration techniques for improving detection resolution to hardware Trojans," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, 2008, pp. 632–639.

[61] C. Mouli and W. Carriker, "Future FAB: How software is helping Intel go nano- and beyond," *IEEE Spectrum*, vol. 44, no. 3, pp. 38–43, Mar. 2007.

[62] F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual property metering," in *Information Hiding*. New York, NY, USA: Springer-Verlag, 2001, pp. 81–95.

[63] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. Design Autom. Conf.*, 2007, pp. 9–14.

[64] S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardware-Oriented Security Trust*, 2008, pp. 67–70.

[65] K. Lofstrom, W. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Proc. IEEE Int. Solid-State Circuits Conf.*, 2000, pp. 372–373.

[66] J. Lee *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Dig. Tech. Papers VLSI Circuits*, Jun. 2004, pp. 176–179.

[67] Y. Su, J. Holleman, and B. Otis, "A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2007, pp. 406–611.

[68] F. Koushanfar, "Integrated circuits metering for piracy protection and digital rights management: An overview," in *Proc. Great Lakes Symp. VLSI*, 2011, pp. 449–454.

[69] R. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, Nov. 2008, pp. 674–677.

[70] Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote activation of ICS for piracy prevention and digital right management," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, 2007, pp. 674–677.

[71] J. Roy, F. Koushanfar, and I. Markov, "Epic: Ending piracy of integrated circuits," in *Proc. Design Autom. Test Eur.*, Mar. 2008, pp. 1069–1074.

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

[73] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 66–75, Jan./Feb. 2010.

[74] R. Chakraborty and S. Bhunia, "HARPOON: An obfuscation-based SoC design methodology for hardware protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 28, no. 10, pp. 1493–1502, Oct. 2009.

[75] J. Rajendran, O. Sinanoglu, R. Karri, and Y. Pino, "Logic encryption: A fault analysis perspective," in *Proc. Design Autom. Test Eur. Conf.*, 2012, pp. 953–958.

[76] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis for logic obfuscation," in *Proc. Design Autom. Conf.*, 2012, pp. 83–89.

[77] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*. New York, NY, USA: Springer-Verlag, 2012.

[78] B. Barak *et al.*, "On the (im)possibility of obfuscating programs," in *Proc. 21st Annu. Int. Cryptol. Conf.*, 2001, pp. 1–18.

[79] R. Jarvis and M. G. McIntyre, "Split manufacturing method for advanced semiconductor circuits," U.S. Patent 7 195 931, 2004.

[80] J. Rajendran, O. Sinanoglu, and R. Karri, "Is split manufacturing secure?" in *Proc. Design Autom. Test Eur. Conf.*, 2013, pp. 1259–1264.

[81] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. ACM Conf. Comput. Commun. Security*, 2013, pp. 709–720.

[82] J. Rajendran, O. Sinanoglu, and R. Karri, "VLSI testing based security metric for IC camouflaging," in *Proc. IEEE Int. Test Conf.*, 2013, DOI: 10.1109/TEST.2013.6651879.

[83] E. Charbon, "Hierarchical watermarking in IC design," in *Proc. IEEE Custom Integr. Circuits Conf.*, May 1998, pp. 295–298.

[84] A. Kahng *et al.*, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001.

[85] E. Castillo, U. Meyer-Baese, A. Garcia, L. Parrilla, and A. Lloris, "Ipp@hdl: Efficient intellectual property protection scheme for IP cores," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 15, no. 5, pp. 578–591, May 2007.

[86] J. Lach, W. Mangione-Smith, and M. Potkonjak, "Fingerprinting techniques for field-programmable gate array intellectual property protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1253–1261, Oct. 2001.

[87] D. Kirovski, Y.-Y. Hwang, M. Potkonjak, and J. Cong, "Protecting combinational logic synthesis solutions," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 25, no. 12, pp. 2687–2696, Dec. 2006.

[88] B. Skoric, S. Maubach, T. Kevenaar, and P. Tuyls, "Information-theoretic analysis of capacitive physical unclonable functions," *J. Appl. Phys.*, vol. 100, no. 2, 2006, 024902.

[89] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Proc. Cryptographers' Track RSA Conf.*, 2006, pp. 115–131.

[90] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. Comput. Commun. Security Conf.*, 2002, pp. 148–160.

[91] D. Lim *et al.*, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[92] S. Devadas *et al.*, "Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, 2008, pp. 58–64.

[93] G. Suh, C. O'Donnell, and S. Devadas, "Aegis: A single-chip secure processor," *IEEE Design Test Comput.*, vol. 24, no. 6, pp. 570–580, Nov./Dec. 2007.

[94] D. Holcomb, W. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[95] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Ruhrmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proc. IEEE Int. Symp. Hardware-Oriented Security Trust*, 2011, pp. 134–141.

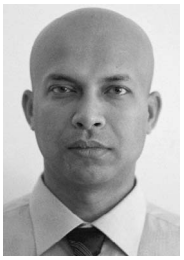
[96] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Ruhrmair, "Characterization of the ring PUF," in *Proc. Design Autom. Test Eur. Conf. Exhibit.*, 2012, pp. 1459–1462.

[97] U.S. Defense Logistics Agency, "DNA authentication marking on items in FSC 5962," Aug. 2012. [Online]. Available: https://www.dibbs.bsm.dla.mil/notices/msgdspl.aspx?msgid=685

[98] Center for Hardware Assurance, Security, and Engineering (CHASE), 2013. [Online]. Available: http://www.chase.uconn.edu/arochase-special-workshopon-counterfeit-electronics.php

[99] Semiconductor Industry Association (SIA), "Public comments—DNA authentication marking on items in FSC5962," Nov. 2012.

ABOUT THE AUTHORS



Ujjwal Guin (Student Member, IEEE) received the B.E. degree from the Department of Electronics and Telecommunication Engineering, Bengal Engineering and Science University, West Bengal, India, in 2004 and the M.Sc. degree from the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA, USA, in 2010. Currently, he is working toward the Ph.D. degree at the Electrical and Computer Engineering Department, University of Connecticut, Storrs, CT, USA.

His current research interests include counterfeit detection and avoidance, hardware security, very large scale integration (VLSI) testing, and reliability. He is an active participant in SAE International's G-19A Test Laboratory Standards Development Committee.

Mr. Guin received the Best Student Paper Award at the 2013 North Atlantic Test Workshop (NATW). He was awarded the SIGDA Ph.D. Forum scholarship at the 2014 Design Automation Conference (DAC).

Ke Huang (Member, IEEE) received the M.S. degree in electrical engineering from the Joseph Fourier University (Grenoble I University), Grenoble, France, in 2008 and the Ph.D. degree in electrical engineering from the University of Grenoble, Grenoble, France, in 2011.

After spending two years as a Postdoctoral Research Associate at the University of Texas at Dallas, Richardson, TX, USA, he joined San Diego State University, San Diego, CA, USA, as an Assistant Professor in 2014. His research focuses on applications of data mining and machine learning in hardware security, reliability, and analog/radio-frequency (RF) integrated circuit (IC) testing.

Dr. Huang was awarded a Ph.D. Fellowship from the French Ministry of National Education from 2008 to 2011. He was a recipient of the Second Place Winner Award at the IEEE Computer Society Test Technology Technical Council (TTTC) E.J. McCluskey doctoral thesis competition in 2013 and a recipient of the Best Paper Award from the 2013 Design Automation and Test in Europe (DATE'13) conference.

Daniel DiMase received a B.S. degree in electrical engineering from University of Rhode Island, Kingston, RI, in 1989, and an Executive M.B.A. from Northeastern University, Boston, MA, in 2010.

He is currently the Director of Compliance and Quality at Honeywell International Inc. (Providence, RI), working in the counterfeit parts prevention team for the Aerospace strategic business group. He has over 20 years of industry experience, previously serving in leadership positions as president of SemiXchange, Inc. and ERAI. His work and research includes mitigating counterfeit and cyber risks, standards development and industry best practices and procedures for avoidance and detection of suspect counterfeit electronic parts and cyber vulnerabilities, supply-chain management, operations and finance, international logistics, global sourcing, risk management, and strategic planning.

Mr. DiMase is an active participant in SAE International's G-19 Counterfeit Electronic Parts Document Development group. He is 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. He is on the Department of Homeland Security's 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. He has a Six-Sigma Green Certificate from Bryant University in 2008.

John M. Carulli, Jr. (Senior Member, IEEE) received the M.S.E.E. degree from the University of Vermont, Burlington, VT, USA, in 1990.

He is a Distinguished Member of the Technical Staff in the Analog Engineering Operations organization of Texas Instruments, Dallas, TX, USA. He was previously the manager of the product reliability and design reliability activities for new technology development in the External Development and Manufacturing division. His research interests include outlier analysis, product reliability modeling, performance modeling, and security.

Mohammad Tehranipoor (Senior Member, IEEE) received the M.Sc. degree in electrical engineering from University of Tehran, Iran, in 2000, and PhD degree in electrical and computer engineering from The University of Texas at Dallas, Richardson, TX, USA, in 2004.

He is currently the F.L. Castleman Associate Professor in Engineering Innovation at the University of Connecticut, Storrs, CT, USA. His current research projects include: computer-aided design and test for complementary metal–oxide–semiconductor (CMOS) very large scale integration (VLSI) designs, reliable systems design at nanoscale, counterfeit electronics detection and prevention, supply chain risk management, and hardware security and trust. He 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.

Dr. Tehranipoor 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 National Science Foundation (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 cofounded a new symposium called IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as 2008 HOST and 2009 HOST General Chair and Chair of Steering Committee. He is currently serving as an Associate Editor-in-Chief (EIC) for IEEE Design & Test, an Associate Editor for Journal of Electronic Testing: Theory and Applications (JETTA), an Associate Editor for *Journal of Low Power Electronics*, an IEEE Distinguished Speaker, and an Association for Computing Machinery (ACM) Distinguished Speaker. He is a Senior Member of ACM and ACM SIGDA. He is currently serving as the director of the Center for Hardware Assurance, Security, and Engineering (CHASE) center.

Yiorgos Makris (Senior Member, IEEE) received the Diploma of Computer Engineering from the University of Patras, Patra, Greece, in 1995 and the M.S. and Ph.D. degrees in computer engineering from the University of California at San Diego, La Jolla, CA, USA, in 1998 and 2001, respectively.

After spending a decade on the faculty of Yale University, New Haven, CT, USA, he joined the University of Texas at Dallas, Richardson, TX, USA, where he is now a Professor of Electrical Engineering, leading the Trusted and RELiable Architectures (TRELA) Research Laboratory. His research focuses on applications of machine learning and statistical analysis in the development of trusted and reliable integrated circuits and systems, with particular emphasis in the analog/radio-frequency (RF) domain.

Prof. Makris served as the Program Chair of the IEEE VLSI Test Symposium in 2013–2014 and of the Test Technology Educational Program (TTEP) in 2010–2012. He also served as a guest editor for the IEEE Transactions on Computers and as a topic coordinator and/or program committee member for several IEEE and ACM conferences. He is a recipient of the 2006 Sheffield Distinguished Teaching Award and a recipient of the Best Paper Award from the 2013 Design Automation and Test in Europe (DATE'13) conference. His research activities have been supported by the National Science Foundation (NSF), the U.S. Army Research Office (ARO), Semiconductor Research Corporation (SRC), the Defense Advanced Research Projects Agency (DARPA), Boeing, IBM, LSI, Intel, and Texas Instruments.