Review

Building Trust in Microelectronics: A Comprehensive Review of Current Techniques and Adoption Challenges

Kwame Nyako , Suman Devkota, Frank Li and Vamsi Borra *

Electrical and Computer Engineering Program, Rayen School of Engineering, Youngstown State University, Youngstown, OH 44555, USA
* Correspondence: vsborra@ysu.edu

Abstract: The field of microelectronics has experienced extensive integration into various aspects of our everyday lives, evident via its utilization across a wide range of devices such as cellphones, airplanes, computers, wristwatches, and other similar technologies. Microelectronics are vital to the healthcare and defense industries, making them vulnerable to counterfeit products. Currently, the complicated global microelectronics supply chain involves the production of varied components in multiple places, resulting in tremendous risk. In this scenario, it is possible for hostile or adversarial actors to exploit the situation by intentionally introducing counterfeit components. This hostile behavior could steal data or use these components as remote kill switches. To address these problems, enormous resources are being committed to research, innovation, and development to build trust in microelectronics. This research study provides a thorough analysis of the taxonomy associated with prominent attack, detection, and avoidance models in the realm of counterfeit microelectronics. This research aims to improve our understanding of dependable microelectronics. Prevention strategies like Physical Unclonable Functions (PUFs) and machine learning (ML), and detection methods like aging-based fingerprints are reviewed in this study. Finally, we underscore the significance of interdisciplinary cooperation, commitment to norms, and proactive methods.

Keywords: counterfeit; detection; trust; microelectronics

Citation: Nyako, K.; Devkota, S.; Li, F.; Borra, V. Building Trust in Microelectronics: A Comprehensive Review of Current Techniques and Adoption Challenges. *Electronics* **2023**, *12*, 4618. https://doi.org/10.3390/electronics12224618

Academic Editors: Wei Hu, Jiaji He and Haoqi Shan

Received: 13 October 2023
Revised: 7 November 2023
Accepted: 9 November 2023
Published: 11 November 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cybersecurity plays a pivotal and indispensable role in today's technological landscape. Yet, cybercriminal tactics continue to evolve, making their identification increasingly challenging. Phishing, IoT hacks, and ransomware have resulted in substantial losses in the tech industry. Thus, hardware security, which protects electronic gear throughout production, has grown in popularity. Hardware security, akin to other security domains, strives to shield hardware from threats that could compromise or obliterate it [1]. Ensuring 'Assurance' and 'Trust' in the context of securing hardware systems translates to the confidence that electronic equipment will perform as intended, free from the peril of compromised components [2].

As the global supply chain grows more intricate and the prevalence of counterfeit components surges, it becomes paramount to verify the authenticity of electrical chips. The infiltration of counterfeit components, potentially finding their way into electronic equipment, raises concerns as workers contend with mounting client demands [3]. National security, economic stability, and individual privacy hang in the balance when hardware systems lack adequate security. Reports from the Department of Defense reveal that over a million components in military aviation and combat missiles have been identified as counterfeit [4,5].

During the first Iraq War in 1991, fighter planes were disabled by a secret activation code embedded in the hardware [6]. Experts believe that the presence of a wicked electrical circuit that was remotely programmable and triggerable played a part in aiding such

a catastrophic catastrophe. The Semiconductor Industry Association (SIA) says that annual losses to manufacturers owing to counterfeits total USD 7.5 billion [7], amounting to around 11,000 job losses in the United States [8]. Other sources assert even higher losses, estimating annual sales losses of around USD 100 billion to counterfeiting [9,10].

To combat this menace, cutting-edge strategies for detecting and preventing counterfeits from infiltrating the market are of paramount importance [11]. Figure 1 illustrates the alarming increase in reported counterfeit components between 2021 and 2022, a period during which worldwide semiconductor sales remained relatively stable.

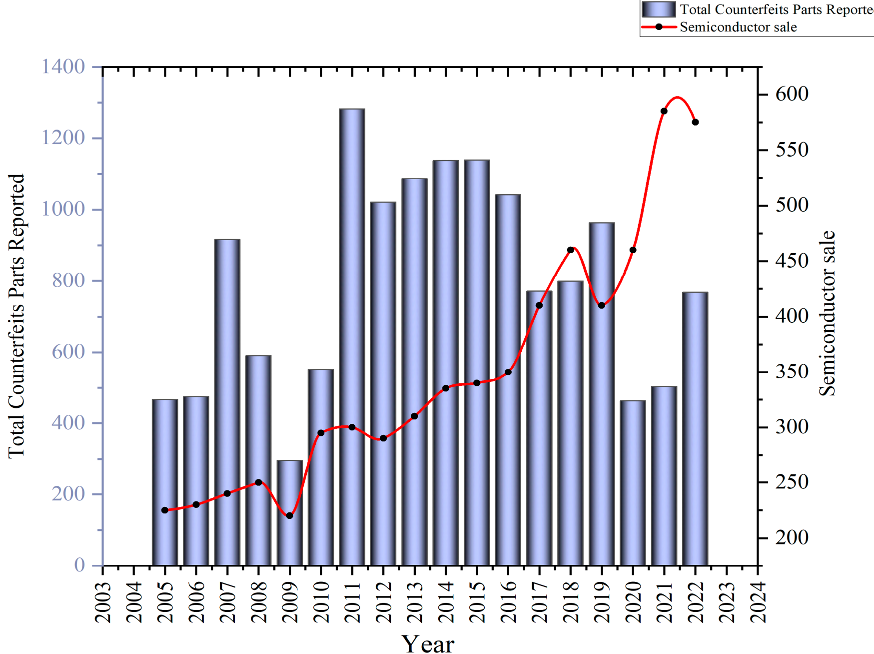

Figure 1. Reported counterfeits increased significantly between 2021 and 2022 [12].

Neglecting hardware security and component verification carries a spectrum of potential consequences, ranging from threats to national security to severe economic repercussions, underscoring the criticality of this facet of technology. The burgeoning presence of counterfeit components in the global supply chain mandates substantial investments in advanced detection technologies and concerted proactive initiatives. In this first section, we adopt a review-style approach to investigate the intricacies between semiconductor sales and the reporting of counterfeit parts in the industry. The aim is to understand if an increasing trend in semiconductor sales correlates with the rise in counterfeit parts. The objectives are to present the data, understand the underlying patterns, and provide insights on the significance of these trends.

Brief statistics below underscore the issues. Figure 1 below indicates that while global semiconductor sales remained steady from 2021 to 2022, reported counterfeit components surged by 35 percent. Over the years, semiconductor sales have shown a definitive upward trajectory. However, when juxtaposed with the total counterfeit parts reported, the relationship is not immediately apparent. While there is a spike observed between 2021 and 2022, a more substantial increase can be seen between 2010 and 2011. This suggests that drawing conclusions based solely on the 2021–2022 data might be premature.

To offer a more comprehensive view, we calculated the Pearson's r correlation between semiconductor sales and the total counterfeit parts reported. The results indicate a Pearson's r of 0.01366, which shows a positive correlation between semiconductor sales and counterfeit parts, albeit a weak one. The low correlation can also be attributed to the fact that the Pearson's r was computed from the average of yearly values. Other potential drivers for this trend deviation include the following.

The initial impact of the COVID-19 pandemic led to many businesses downsizing or suspending their operations, causing significant disruptions in global supply chains. However, as the global economy slowly rebounds, businesses are returning to their pre-pandemic activities, resulting in a surge in demand for electrical components. This heightened demand could create opportunities for counterfeiters to exploit weaknesses in the supply chain to meet the increased market needs. Additionally, as pandemic-related restrictions ease, global supply networks are gradually recovering and reopening, potentially enabling the cross-border spread of counterfeit parts. Moreover, the growing awareness of and reporting on counterfeit component issues likely contribute to the observed rise in reported instances of counterfeit electrical components infiltrating the market. To address the risks associated with counterfeit components, stakeholders should invest in advanced detection and prevention technologies, establish industry standards, and promote collaboration within the global supply chain.

Figure 2 is a trend analysis of the most frequently reported component types over the past decade, which reveals interesting information about the microelectronics market. One noteworthy tendency is the flattening of the capacitor spike, which could indicate either an advance in capacitor dependability and affordability or a shift in the counterfeiting community's focus. Since the Electronics Research and Analysis Institute (ERAI) began tracking this data, the demand for analog devices has expanded faster than any other type of component in the last year.

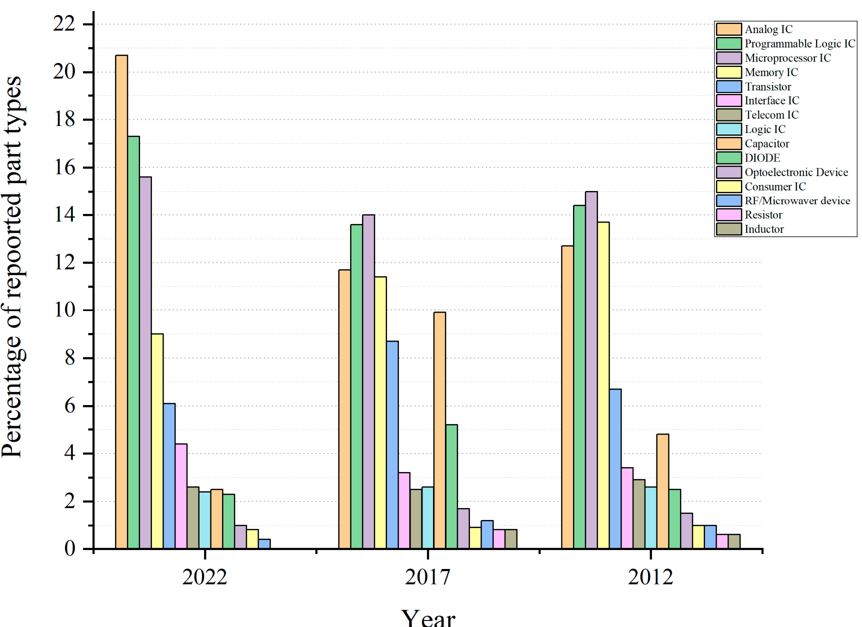

Figure 2. The most counterfeited semiconductors in 2022 compared with 10 and 5 years ago.

Other reasons for the recent rise of analog devices are likely to include growing prices, improving technology, and even sophisticated counterfeiting efforts. Stakeholders in the microelectronics sector would do well to keep an eye on these trends and determine their root causes; doing so would help in the creation of efficient methods for the identification, prevention, and avoidance of counterfeit products. In addition, having an awareness of these tendencies will aid in guaranteeing the security and dependability of microelectronic components.

Considering all the challenges above, we have adopted a review-style methodology, to meticulously examine the literature and advancements in the microelectronics domain. Additionally, we offer a thorough insight into the challenges and ever-changing threats and solutions concerning trusted microelectronics. The research aims to provide an in-depth understanding of the taxonomy of counterfeit attack, detection, and avoidance within the industry, articulating the complexities and current developments. The objectives en-

compass tracing microelectronics' evolution and its modern relevance, understanding external impacts like the COVID-19 pandemic on the sector's vulnerabilities, emphasizing the escalating sophistication of counterfeit threats, addressing ethical and security implications from technology convergence, and forecasting the future of microelectronics security with a focus on innovative solutions. These objectives lay the groundwork for the subsequent sections, ensuring readers receive a coherent and insightful exploration of the topic.

2. Counterfeit Attack Modes

As depicted in Figure 3, counterfeit integrated circuits (ICs) are primarily susceptible to four categories of attack mechanisms: software, hardware, network, and information security. In the subsequent sections, we delve into these potential attack techniques for counterfeit ICs, elaborating on the potential consequences they may entail.

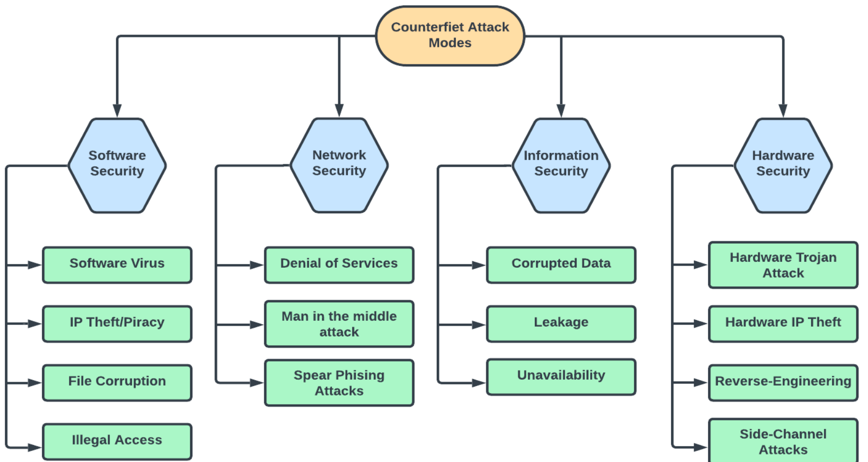

Figure 3. Chart showing counterfeit attack modes and the potential consequences of such attacks.

2.1. *Software Security*

As the significance of software security continues to escalate, the role of trusted microelectronics in fortifying software applications and ensuring their stability has gained paramount importance. Software security revolves around the safeguarding of software applications against vulnerabilities and attacks that could be exploited by counterfeit integrated circuits (ICs). Counterfeit ICs provide malicious actors with the means to inject malicious code, circumvent security protocols, or manipulate the functionality of software applications. They can also facilitate software-based side-channel attacks and privilege escalation, thereby granting unauthorized access to sensitive data or system resources.

Notably, the Plundervolt attack, elucidated by [13], exploits the dynamic frequency and voltage scaling features of modern CPUs, specifically targeting Intel SGX enclave operations. By manipulating the processor's voltage, attackers can induce known faults in the processor package, compromising security. This vulnerability can lead to the compromise of cryptographic keys and the introduction of memory-safety vulnerabilities. The repercussions, as outlined in [14], encompass unauthorized access to private data, system instability, software performance degradation, and reduced overall system security.

Furthermore, speculative execution, a form of software security attack that occurs when the CPU speculatively executes tasks it anticipates needing in the future without explicit instruction [15], introduces potential risks. This approach eliminates the need to await the completion of previous commands before executing new ones, thereby enhancing speed by reducing latency and increasing parallelism [16]. However, speculative execution can inadvertently execute potentially harmful programs, raising security concerns.

To enhance software security and instill trust, Physically Unclonable Functions (PUFs) have been proposed. PUFs are employed to generate unique and unpredictable cryptographic keys for authentication and encryption, constituting robust hardware-based secu-

rity mechanisms. Notable PUF projects include the Arbiter PUF, which leverages differing data-line delays [17], the Ring Oscillator PUF, which relies on variations in the frequencies of two-ring oscillators [18], the SRAM PUF, exploiting idiosyncrasies in SRAM-cell startup behavior [19], and the Memristor PUF, capitalizing on the resistance-changing properties of memristive devices [20]. It is worth noting that PUFs have faced attacks, as elucidated in [21], where modeling attacks seek to emulate a PUF's behavior through mathematical modeling. These attacks have been successfully executed with the aid of machine learning tools such as Support Vector Machines (SVMs) and neural networks.

2.2. Hardware Security

The embedding of Hardware Trojans, backdoors, and other malicious circuits within counterfeit integrated circuits (ICs) poses a significant threat, endangering the security, confidentiality, and availability of electronic systems [22]. This underscores the critical need for rigorous hardware security measures, including supply chain oversight, secure manufacturing processes, and state-of-the-art counterfeit detection technologies, to forestall unauthorized access [23], data breaches [24], or system malfunctions [25].

Hardware security presents multifaceted challenges, encompassing vulnerabilities to a range of attacks (e.g., side-channel or Trojan attacks) at various layers (e.g., chip or PCB), further complicating the landscape of hardware security. Concurrently, hardware trust concerns stem from interactions with untrustworthy third parties at any stage of a device's production and distribution, spanning from IP or CAD tool providers to manufacturing facilities and warehouses.

Among common hardware security breaches, Reverse Engineering Attacks, which aim to pilfer a device's intellectual property and design details for illicit purposes such as duplication or counterfeiting, are prominent [26]. These attacks can be executed through methods like deprocessing, optical imaging, and circuit extraction [27]. In contrast, fault injection attacks intentionally induce system malfunctions to gain access to or control over the targeted system [28], employing tools such as lasers, electromagnetic pulses, or temperature-dependent fault injections [29].

Side-channel attacks focus on unintentional data leakage from a device's physical implementation, encompassing aspects like power consumption, electromagnetic radiation, or timing data [30]. Techniques such as differential power analysis, simple power analysis, and correlation power analysis are employed to infer device behaviors and potentially extract sensitive information, such as encryption keys, from power consumption patterns [31].

Furthermore, Hardware Trojans represent malevolent hardware additions introduced during product assembly, serving as latent security or functionality vulnerabilities that can be activated at a later stage [32].

2.3. Network Security

Network attacks often manifest in the deployment of counterfeit network interface controllers or routers, potentially leading to the theft of sensitive information, service disruptions, or the illicit takeover of networked devices via unauthorized remote access [33].

In safeguarding critical infrastructure, the Internet of Things (IoT), and cloud-based services, trusted microelectronics play a central role [34]. These components are instrumental in ensuring the privacy, integrity, and authenticity of stored data [18], commonly relying on cryptographic primitives and secure key storage.

One particular area of scrutiny is spear-phishing, an exceptionally targeted and sophisticated form of phishing attack that surpasses conventional phishing attempts in terms of complexity and personalization. This issue is explored extensively in a research paper authored by a single individual [35]. The paper underscores the urgency for enterprises to proactively counter the escalating threat of spear-phishing. To fortify themselves against sophisticated cyberattacks, businesses are advised to prioritize user education, im-

plement robust security measures, and maintain a comprehensive and up-to-date incident response plan.

2.4. Information Security

In addition to bypassing security measures to gain unauthorized access to sensitive data, counterfeit cryptographic integrated circuits also have the potential to disrupt encryption or authentication methods. The advent of social media and cloud computing has necessitated a heavy investment by businesses in information security in order to safeguard data. The Federal Communications Commission offers tips to businesses for cybersecurity [36]. The CIA Triad, comprising of Confidentiality, Integrity, and Availability, serves as a fundamental framework within the field of information security. An all-encompassing information security strategy encompasses policies and security controls that effectively mitigate risks to these three essential components.

The CIA triad serves as a comprehensive framework for overseeing information security and is also valuable for effectively managing research products and data.

3. Counterfeit Detection Methods

Numerous previous research endeavors have conducted comprehensive analyses and comparisons of both destructive and non-destructive techniques employed for the identification of counterfeit integrated circuits (ICs) [37]. Destructive methods, including delayering and cross-sectioning, offer profound insights into the internal structure of ICs, uncovering potential anomalies or tampering. However, the use of these methodologies often results in the degradation of the examined components. Conversely, non-destructive techniques such as X-ray imaging, optical microscopy, and electrical testing provide the means to scrutinize integrated circuits without causing any harm to their structural integrity. Consequently, these approaches are better suited for conducting extensive screenings on a broader scale. This section underscores the importance of integrating multiple detection techniques to enhance the accuracy and effectiveness of counterfeit IC identification, thereby contributing to the overall enhancement of security and reliability in electronic systems. A concise overview of the taxonomy of counterfeit detection strategies, along with its subdivisions is provided. These are depicted in Figures 4 and 5.

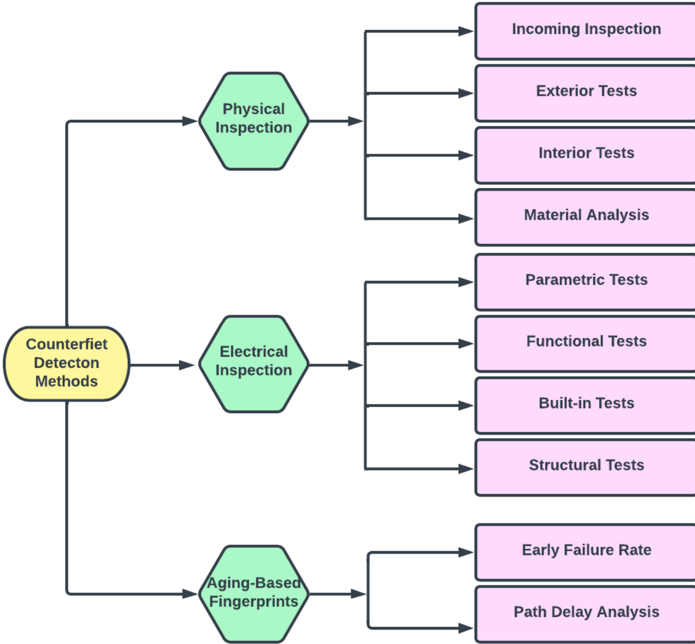

Figure 4. Counterfeit detection modes and subcategories [38].

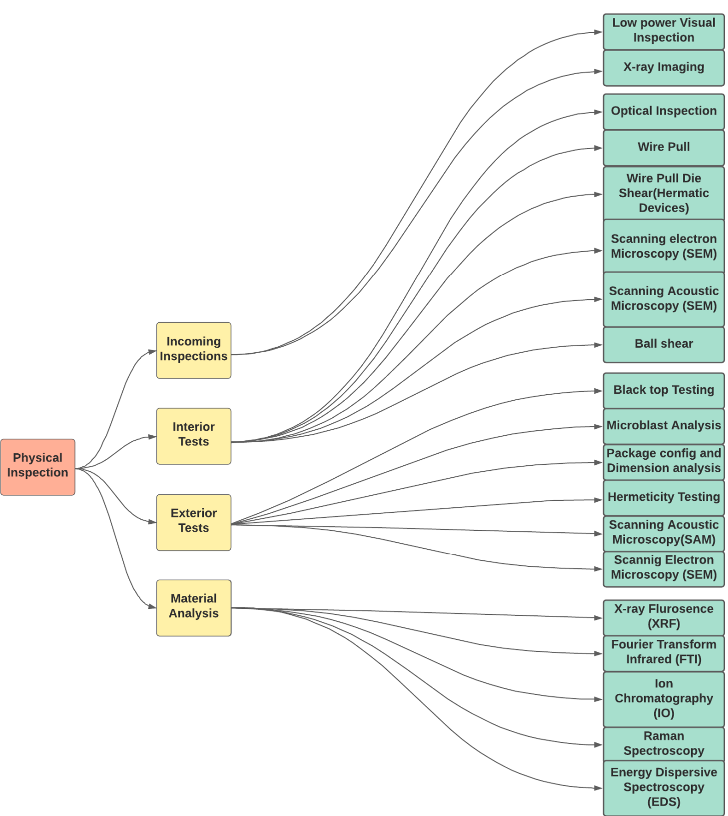

Figure 5. Subdivisions under physical inspection.

3.1. Physical Inspections

To identify imperfections, physical examinations involve a meticulous assessment of the components' external attributes. These examinations encompass both internal and external evaluations aimed at scrutinizing the component's construction, packaging, and leads. External tests, such as low-power visual inspection (LPVI) [39], blacktop testing [40–42], microblast analysis [43–45], hermiticity testing [46–48], scanning electron microscopy (SEM) [49–52], and scanning acoustic microscopy (SAM) [53–55], focus on assessing the component's exterior characteristics. The method of low-power visual examination (LPVI) uses tools like microscopes, digital cameras, or infrared light sources to inspect essential markings on package-level electronics and identify indications of previously used or recycled items, including marks on the package or leftover solder on IC connectors. Furthermore, X-ray visualization, which is a non-destructive testing technique, is applied to identify irregularities within the internal components, dies, and connecting wires by comparing them to a standard component. Microblast testing is used to determine if markings or scratches on reused or fake components have been intentionally erased using a dry sandblasting method. In contrast, internal assessments necessitate decapping the component to expose its internal structure, which can then be subjected to techniques like optical inspection [56–58], wire pull and die/ball shear [59–61]. Essential details about die markings, such as the company emblem, manufacturing date, chip identification, and origin country, among others, should be recorded. Wire pull is used to check the bond's consistency with the die. If the component has been used for an extended period, the bond between the die and bond wires may weaken. By comparing the tension (or pulling strength) between the standard and examined components, one can ascertain if the component had prior usage. The die shear method is employed to confirm the die attach's reliability, but it is relevant only for sealed devices. The ball bond's robustness at the die is assessed using a ball shear test. Scanning electron microscopy (SEM) captures images of the die, package, or leads by scanning them with a concentrated electron beam. This method is effective in detecting any irregularities present. With a resolution that can reach a few nanome-

ters, SEM allows for the detailed analysis of the die, even down to its gate level. For an examination of the material composition of the package, leads, and die, techniques such as X-ray fluorescence (XRF) [62–64], Fourier transform infrared spectroscopy [65–67], and energy-dispersive spectroscopy [68,69] are employed. XRF Spectroscopy is a non-invasive technique used for material analysis. When a material is subjected to intense X-rays, its outer electrons are energized to higher, unstable orbits. As these electrons revert to their original state, they emit radiation. This emission is specific to each element, resulting in a distinctive spectral peak. By using XRF, a unique signature from a component's package is obtained. The component's authenticity is ascertained by comparing this signature to a reference sample or, if accessible, the manufacturer's specifications. On the other hand, Energy Dispersive Spectroscopy (EDS) is a technique that determines the chemical properties of a component by stimulating it with X-rays. By directing a high-powered stream of charged particles onto the component's surface, X-rays are emitted. An X-ray detector then captures this emission to produce the EDS spectrum. This process yields a distinctive X-ray signature based on the materials present in the component's outer casing.

Lastly, Fourier Transform Infrared (FTIR) Spectroscopy leverages the principles of infrared (IR) spectroscopy. When subjected to IR radiation, a material will both absorb and transmit portions of it. The captured IR radiation provides insights into molecular behaviors, both in terms of absorption and transmission. Through this method, a specific molecular pattern is derived, which can then be compared to a known reference or "gold standard" for material verification. FTIR is versatile, suitable for examining both organic and inorganic substances in a component. It involves validating a component's specific materials, such as polymers or coatings; spotting remnants from procedures like sandblasting, which erase prior inscriptions; and detecting traces from chemical methods. These methods are commonly found in counterfeit parts, repurposed from circuit boards or resulting from unsanctioned refurbishing processes.

A comprehensive physical inspection constitutes the initial step in thwarting the infiltration of counterfeit components. This systematic examination is consistently applied to various categories of incoming components, regardless of their condition, encompassing new, used, or aged components. The security and reliability of electronic systems hinge upon this methodical approach to detecting counterfeit parts.

3.1.1. Incoming Inspections

For counterfeit integrated circuit (IC) detection, the physical inspection process initiates with inbound examinations. This procedure involves scrutinizing newly acquired components to ensure their authenticity and quality before their integration into electronic systems. Incoming inspections serve to identify anomalies, defects, or potential signs of counterfeiting through a careful examination of the components' physical attributes. Computer vision techniques play a pivotal role in addressing hardware security challenges. Techniques like Keypoint Extraction using SIFT and SURF, Image Segmentation, and Template Matching help in identifying and analyzing various elements of printed circuit boards (PCBs) and integrated circuits. With the evolution of deep learning and artificial neural networks (ANNs), feature extraction has become more efficient, particularly with models like AlexNet, ResNet, and Inception-v3. Despite these advancements, computer vision-based hardware security faces challenges, including the absence of large, labeled datasets and the inherent noise and clutter in imagery, especially in high-density PCBs. To address these challenges, future research can consider multi-modal imaging, develop publicly available datasets, and apply deep learning earlier in the computer vision pipeline. Collaborative efforts that combine hardware design, imaging, computer vision, and machine learning expertise are essential for more holistic solutions. The complexity of contemporary digital systems presents challenges in verifying chip authenticity, prompting the authors Akter et al. [70] to advocate for the use of terahertz (THz) and sub-terahertz (sub-THz) scanning combined with AI processing to detect counterfeit Integrated Circuits (ICs) and assess their reliability. This technology, tested on devices like the i7 microproces-

sor, uses unique THz signatures from circuit pins to distinguish genuine from counterfeit chips. Using MATLAB-based software, the THz response data undergoes a multi-step processing procedure, with techniques like Hough transform applied for image classification. The research suggests that this combined approach of THz scanning and AI processing can serve as a significant tool for cybersecurity, ensuring the reliability and genuineness of ICs in sectors vulnerable to counterfeit threats, such as defense and healthcare.

Another use of machine learning in counterfeit IC detection proposed by Sukhwan et al. [71] uses simulated circuits to pinpoint temperatures that best emphasize the disparities between genuine and counterfeit circuits. By using RLC circuits, non-inverting amplifier circuits, and the NSGA II algorithm, the research establishes optimal testing conditions, notably in extreme temperatures, that accentuate these differences. When tested on genuine Intel and counterfeit Soviet clone circuits, the counterfeit circuits exhibited significant output differences, especially in cold environments. This machine learning model is adaptable for industrial-grade counterfeit detection tools and offers a cost-efficient alternative. In a study by Lu et al. [67], the authors underscore the potential of X-ray imaging as a means to detect counterfeit and recycled ICs. They suggest using a method based on deep learning to analyze X-ray images of integrated circuits in order to spot fakes. The authors describe Hardware Trojans as malicious modifications in integrated circuits. These can include simple changes like adding, removing, or altering circuit cells (like gates) or their connections, as shown in Figure 6. When processing X-ray pictures, convolutional neural networks, also known as CNNs, are utilized, which enables the automatic extraction of distinguishing characteristics.

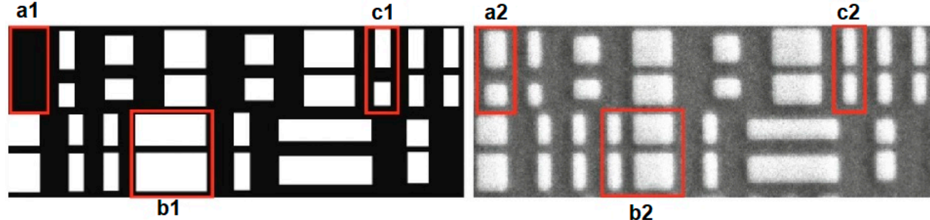

Figure 6. An SEM image of an IC layout showing **a2** being points of cell insertion, **b2** being points of cell deletion, and **c2** being points of cell replacement [67]. (Figure adopted with permission).

Consequently, these networks categorize integrated circuits as either authentic or counterfeit/recycled. The incorporation of deep learning in this technology holds the promise of surpassing current manual inspection procedures in terms of accuracy, speed, and scalability.

3.1.2. Exterior Tests

Blacktop testing, as defined by researchers in [38,72], involves inspecting the surface of the components for discrepancies, such as the existence of a blacktop coating intended to disguise remarking or other tampering, with the goal of discovering counterfeit ICs. The longevity of the parts under scrutiny is determined by subjecting them to a battery of different solvents. Hermeticity, as described in [73], necessitates a special method of package assessment, especially for hermetically sealed components. This evaluation ensures that the Hermetic Seal is intact and the product will work as expected in the designated setting. When the circuit's performance is at stake and great dependability is required, such as in the military or industry, hermetic enclosures for integrated circuit packages are commonly used. Examining a Fine Leak or a Gross Leak in a Hermetic Seal is a simple and low-cost approach to check for seal failure. To analyze a Fine Leak Hermetic Seal, one can use commercially available leak detection systems that use either helium or radioisotope tracer gases. A vacuum is applied, the integrated circuit is pressurized for a certain amount of time (allowing the gas to seep into the package cavity), and then the released gas is detected. Gross Leak Hermetic Seal assessments, on the other hand, may be readily carried out with just a bit of pressured air, a vacuum system, a pressure chamber, and

two liquids that will not interfere with any electronic devices [74–76]. Scanning electron microscopy uses a concentrated electron beam rather than light to create a high-resolution picture. The process begins when a beam of electrons is created by an electron cannon at the microscope's focal point. The extensive test time of SEM, since it might take several hours to analyze a single component, limits its applicability. However, SEM is particularly beneficial for identifying various faults and abnormalities prevalent in counterfeit components.

3.1.3. Interior Tests

The term "interior tests" describes the process of inspecting the inner workings of a gadget or product to ensure its legitimacy. The component's protective covering must be removed so that its internal structure may be examined for this test.

Bump connections, which are used in modern chip technologies instead of wire bonds, enhance the density and stress concentration on the connecting part by a substantial amount [77]. Ball shear testing has been created to examine the reliability of these bumps. To use this technique, one places an implement next to the base and presses down on the ball until it breaks. The idea behind both ball and die shear testing is quite similar. These experiments provide a direct measure of the interaction's trustworthiness; nonetheless, they call for the handling of the samples and a decapping procedure [78]. The electronic connections between various IC layers are critical to the reliability of the IC package as a whole. The quality and durability of bonding in microelectronic applications may be evaluated with tests like wire-pull testing. In this kind of testing, wires are subjected to an upward force applied by a hook, which is then used to draw the wire away from the substrate or die until the bond fails or the wire breaks. A tiny hook is inserted beneath the wire and pulled upwards to impart strain to the bond wire and determine its quality. In order to pass the standard non-destructive wire pull test used in the industry, all bonds must remain intact despite the light loading tension used [79]. The goals of wire pull testing are to assess the durability of the bond, investigate the causes of bond failure, and guarantee that the specified bond strength criteria are met. The die shear test is used in semiconductors and other microelectronic devices as a quality control measure to evaluate the adhesion and bonded area of bare die attached with media such as epoxy, solder, and sinter materials to substrate materials such as metal lead frames, ceramic packages, and printed circuit boards.

3.1.4. Material Analysis

The non-destructive qualities, rapidity, and compatibility of Raman spectroscopy with a diverse array of materials render it exceptionally well suited for implementation in hardware security applications [80]. This spectroscopic technique harnesses the scattering of light to provide valuable insights into the molecular composition and structure of materials. In the realm of hardware security, Raman-active compounds like nanotags play a pivotal role in the authentication and tracking of components [81]. Nanotags, infused with Raman-active materials can be affixed to integrated circuits or other hardware components, allowing for their secure identification and traceability. An exemplary illustration of Raman spectroscopy's efficacy in hardware security can be found in the work of Vaskova et al. [82], where it was employed to scrutinize the dielectric materials within electronic assemblies. The objective was to uncover instances of counterfeit capacitors, a prevalent concern in the electronics industry. By subjecting the components to Raman spectroscopic analysis, the researchers could non-destructively assess the molecular composition of the dielectric materials. Any disparities or inconsistencies in the spectral signatures could signify the presence of counterfeit or substandard components, thus enabling precise detection and mitigation of potential security threats. Raman spectroscopy's versatility and accuracy make it an invaluable tool in the ongoing efforts to enhance the security and reliability of electronic systems.

3.2. Electrical Inspections

Parametric, Burn-In, and Structural Tests

Sinanoglu et al. [83] introduced an innovative approach for detecting counterfeit integrated circuits (ICs) based on a two-dimensional space of parametric measurements. In their method, they employed a one-class support vector machine (SVM) trained using measurements obtained from a collection of new devices sourced from reputable suppliers. These devices naturally exhibit some degree of process variation. The one-class SVM, acting as a machine-learning model, establishes a nonlinear boundary within the parametric measurement space. This boundary effectively discriminates between genuine and counterfeit ICs.

The conventional one-class SVM, as described by Schölkopf [84] and colleagues, represent an objective function as:

$$\frac{1}{2}|w|^2 - \rho + C\sum_j \xi_j \quad (1)$$

Under the constraints, $w \cdot \phi(xj) \geq \rho - \xi j \; and \; \xi j \geq 0$. In this context, the equation $w \cdot \phi(x) = \rho$ identifies a hyperplane within the feature domain. The symbol $|\cdot|$ is representative of the Euclidean magnitude, while ξj are the slack variables. A pre-set parameter, C, determines the proportion of anomalies, as discussed by Müller et al. and Schölkopf et al. [84,85].

Another study by different authors [86] employed Support Vector Machines (SVMs) to detect counterfeit ICs, with a specific focus on distinguishing previously used ICs from unused ones. They accomplished this by training a one-class SVM classifier on a set of new devices that exhibit process variations. Notably, this approach obviated the need for prior knowledge concerning how transistor degradation may affect IC functionality. The classifier utilized straightforward parametric measurements and validation data from burn-in experiments simulating the aging process. This cost-effective method eliminated additional identification expenses and exhibited high effectiveness in identifying counterfeit ICs falsely represented as new. By incorporating various parametric measurements, this technique demonstrated exceptional precision in identifying used components falsely marketed as brand-new.

A recent study using SVM was performed by Kent et al. [87] and utilized a linear support vector machine (SVM), a supervised machine-learning model, to classify distinct categories. SVM works by creating a hyperplane that best separates data points from different categories, maximizing the margin between them. Its principle lies in ensuring the hyperplane is positioned to maximize the distance from the nearest data points of differing categories. The application of SVM extends beyond just this study; it has traditionally been employed for routine maintenance tasks like fault detection in hardware and software systems. For instance, SVM was applied to distinguish performance issues in heating ventilation air-conditioning and cooling chillers by categorizing the data into two classes: "fault detected" and "no fault detected". While machine learning techniques have been explored to address sensor location challenges for daylight harvesting, this particular study showcased SVM's distinct application in this context.

Furthermore, the impact of Negative Bias Temperature Instability (NBTI), a primary cause of circuit performance deterioration, can be assessed through a structural test to gauge the integrity of ICs. NBTI aging has been shown to influence the threshold voltage in PMOS devices [83,88–91]. As mathematically developed by Wang et al. [92] Equation (1) details the calculation for "ΔV_{th}" as influenced by NBTI for a given time "t". In this formula, "K_v" signifies the impact of the electric field, temperature, and carrier concentration. The time exponential constant is denoted as "n". The term "α" indicates the signal prob-

ability, representing the portion of time a transistor is under NBTI stress within a given period. "T" is the temperature,

$$\Delta V_{th} = \left(⟦ \sqrt{K_v^2 \times T_{clk} \times \frac{\alpha}{1 - \beta_t^{\frac{1}{2n}}}} ⟧ \right)^{2n} \quad (2)$$

In the realm of IC verification through structural tests, there is a noteworthy exploration of using ICs' distinctive timing path signatures, stemming from inherent process variations, as a basis for creating Physical Unclonable Functions (PUFs) for identification purposes. Structural tests encompass assessments like leakage, timing, and dynamic power measurements. These evaluations have the potential to uniquely identify the vast majority of ICs produced with cutting-edge technology, all without the need for additional chip components. Leveraging non-invasive gate-level characterization, this method derives continuous values capable of generating unique chip identifiers. The wealth of available test vectors enhances the diversity of challenge-response pairings, opening up new avenues for IC monitoring and security protocols [93–95]. This innovative approach holds promise for bolstering IC authentication and security measures while maintaining cost-efficiency and scalability.

3.3. Aging-Based Fingerprint Testing

Aging-based fingerprints are distinct characteristics that develop in electronic devices, such as integrated circuits, over time due to aging effects. These fingerprints offer valuable potential for enhancing hardware security by enabling the development of identification or authentication methods based on the natural wear and tear of these devices. Various factors, including Negative Bias Temperature Instability, Hot Carrier Injection, and Time-dependent Dielectric Breakdown, contribute to changes in the performance of transistors and other components as electronic devices undergo aging. These changes are unique to each device due to process variations and patterns of usage, resulting in the creation of individualized aging-based fingerprints [72,96].

In the context of this paper [97], a cost-effective approach is presented for safeguarding secret keys using Physical Unclonable Functions (PUFs), leveraging the unique hardware identity of sensor nodes. Additionally, a resource-efficient fingerprint recognition system is introduced, designed specifically for deployment in low-cost sensor nodes. PUFs are also employed for obfuscation to protect sensitive biometric data. The authors propose a two-factor authentication method to verify the source of collected data, relying on the unique physical identity of the trusted sensor node and the physical presence of an authorized individual overseeing data transfer. Experimental results indicate the feasibility of implementing the proposed PUF-based solution in the SRAMs of commercially available Bluetooth Low-energy chips within sensor nodes. The fingerprint identification technology is based on "QFingerMap16", utilizing unique texture-based features. The research further delves into the resilience, security, and privacy aspects of the suggested sensor nodes, drawing from experimental data involving PUFs and fingerprints sourced from public and standardized databases. This multifaceted approach offers promising implications for enhancing security and privacy in low-cost sensor node applications.

4. Counterfeit Avoidance Method

4.1. PUF-Based Avoidance Techniques

There are two main categories of Physical Unclonable Functions (PUFs): delay-based PUFs and memory-based PUFs. Each of these utilize different aspects of the underlying technology. These PUFs offer several advantages, including unpredictability, resistance to tampering, cost-effectiveness, and dynamic key generation. However, they also present challenges such as sensitivity to environmental factors, low entropy, and susceptibility to modeling attacks. Ongoing research and development in PUF design, error correction,

and countermeasures aim to address these issues, making PUFs a promising solution for hardware security.

One notable implementation is the Ring-Oscillator PUF, mentioned in article [98], which uses an oscillator with an odd number of gates to generate distinct signatures sensitive to manufacturing variations. However, delay-based PUFs suffer from spatial correlations in process parameters, limiting their uniqueness and making them susceptible to side-channel attacks.

To overcome these limitations, the authors of paper [22] introduce the Process and Environmental (PE)-PUF. This PUF design takes into account process and ambient variables like temperature, power supply noise, and crosstalk, enhancing the randomness and uniqueness of the generated signatures. The study employs a 90 nm-implemented seven-inverter ring oscillator with nearby interconnects, simulated using HSPICE.

In [99], researchers explore the application of deep learning techniques to model attacks on double arbiter PUFs. The results demonstrate that deep learning methods outperform conventional machine learning approaches like logistic regression and support vector machines in terms of predictive accuracy. The success rate in attacks against 3-1 DAPUFs exceeds 86%, surpassing the previous record of 76%. Similarly, the accuracy in attacks against 4-1 DAPUFs ranges from 71% to 81.5%, surpassing the prior high of 63%.

Finally, in [100], authors propose an innovative SRAM architecture that facilitates cost-effective and widespread key generation by integrating dynamic and multi-bit static entropy generation in memory. This design retains a commercial bitcell, a pitch-matched peripheral, and compatibility with memory compiler designs. Additionally, it incorporates a True Random Number Generator (TRNG) and a physically unclonable function (PUF) to enhance security.

4.2. Machine Learning and Artificial Intelligence

AI and machine learning (ML) approaches are increasingly being integrated into hardware design processes, providing a fresh approach to addressing various phases and layers of abstraction. By estimating hardware overhead [101], optimizing logic [102], routing [103], and introducing test points [104], these techniques address scalability difficulties and accelerate design completion. Using AI and ML in hardware design enables better optimization, more efficiency, and shorter development cycles.

The authors of the study [105] analyze the viability of repurposing an existing neural network to construct a robust Physically Unclonable Function in order to ensure safety and reliability in Internet of Things and smart sensor applications. The Multilayer Perceptron is the primary subject of this work. It is a feed-forward neural network with multiple layers of completely coupled neurons. They consider several network designs, each with its unique hidden layer depth and synaptic weight accuracy. PUF criteria such as uniformity, uniqueness, bit-aliasing, and reliability are used to assess the quality of the proposed solution. Another work [106] introduces "HW2VEC", a free and open source graph-learning tool developed to let researchers investigate hardware security applications using graph representations. HW2VEC is a tool that translates non-Euclidean hardware designs into an embedding in a Euclidean network and extracts graph representations from hardware designs at various abstraction levels.

4.3. Hardware Metering

Hardware metering, also referred to as integrated circuit metering, serves as a crucial mechanism for monitoring and safeguarding integrated circuits (ICs) once they have been manufactured. This becomes particularly significant as many businesses choose to outsource their IC manufacturing to companies located in different countries, exposing their designs to potential theft or replication risks. To address this challenge, experts have developed various methods for monitoring and managing ICs, with passive and active metering emerging as the two predominant approaches.

In passive metering systems, individual chips are initially identified separately to detect any unauthorized or counterfeit chips effectively. Active metering, on the other hand, provides designers with the capability to control specific chip operations, enhancing chip security. This article provides an overview of hardware metering, exploring its key concepts and diverse methodologies.

It is worth noting that hardware watermarking, while related, differs from hardware metering. While hardware metering involves actively or passively tagging individual chips, hardware watermarking embeds its mark within the design file rather than on the individual chips. Watermarking, however, has limitations in combatting counterfeiting as it cannot differentiate between chips of the same design. In contrast, hardware metering offers a more effective solution by assigning a unique identity to each chip or its functionality, enabling differentiation among chips with identical architectures.

Passive and Active IC Metering

Passive metering represents a method for the identification of counterfeit chips by monitoring and analyzing their operational data. In essence, this approach aims to distinguish genuine chips from counterfeits that replicate the control behaviors of legitimate chips. Passive metering proves particularly effective when dealing with a large number of chips that can be coupled, allowing for the examination of their individual control paths. This examination is achieved through techniques like XOR operations and additional parity tests [107].

However, as noted in [108], current passive metering methods suffer from various limitations, including challenges in quantifying chip IDs accurately, high associated costs, and issues related to scalability. To address these issues, the authors propose two significant changes as potential solutions. Firstly, they suggest utilizing manifestation properties to extract physical-level characteristics, such as gate threshold voltage, which remain independent of aging, temperature variations, and supply voltage. Secondly, to reduce expenses, expedite time-to-market, and enhance scalability, they advocate for IC segmentation. This segmentation involves selecting only a subset of gates for detailed characterization.

In [107], the authors delve into the horizontal semiconductor business model, which exposes designers' intellectual property (IP) to piracy and excessive production of integrated circuits due to the transparency prevalent across the production chain. To combat these challenges and enable chip-tracking post production, they introduce the concept of active hardware metering. The authors also discuss potential risks and countermeasures while presenting a low-overhead hardware solution based on an autonomous synthesis method.

Moreover, Ref. [109] introduces a novel approach to external active IC metering that utilizes a PUF (Physically Unclonable Function) design to generate keys. In contrast to traditional encryption modules, they employ a modified Finite State Machine (FSM) to protect PUF-based keys from unauthorized access. By integrating the retrieval method within the high-level design of the FSM, they significantly reduce the time and effort required to securely recover PUF-based keys, especially when the original FSM is reused.

4.4. Secure Split Testing

The "Secure Split-Test" (SST) is a newly introduced approach that restores testing authority to the owner of Intellectual Property (IP). With SST, chips are securely locked during the evaluation phase. Only the IP proprietor has the capability to decipher the locked test outcomes and grant access to the chips that meet the set criteria. SST's main objective is to halt the distribution of excess or flawed chips within the supply chain. Compared to its predecessor, this method streamlines the dialogue between the chip-making foundry and the IP owner. Evidence suggests that SST not only bolsters security but also mitigates communication obstacles. The researchers Contreras et al. [110] introduced a unique "SST Structure" to augment the protection of integrated circuits. This design incorporates a

locking mechanism known as the "XORF mask", which consists of three-way XOR gates situated in less crucial circuit routes. The XORF acts as a switch; it serves as a conduit when two inputs match, and as a converter when they differ. Placing these XORFs, especially near scan flip-flop entry points, can alter specific circuit feedback. True Random Number Generators (TRNGs) are employed to add an element of randomness, drawing from physical occurrences such as clock inconsistencies and temperature variations for entropy. TRNG outputs are saved in a non-reusable memory for consistency. The design also incorporates RSA encryption to fortify the IC's security, with a complex key system (TKEY and FKEY) governing the XORF operations. An additional "Scan-Locking Block", employing three-way XOR gates and key-driven functions (KDFs), has been integrated to enhance defenses against potential threats.

In the following sections, we present two comprehensive tables that encapsulate the myriad of challenges encountered in the realm of counterfeit electronics. Table 1, titled "Implementation Challenges of Counterfeit Detection Methods", delves into the obstacles faced when identifying fake components through various detection strategies. It outlines the practical difficulties and technical intricacies inherent to the current detection methodologies. Following this, Table 2, "Implementation Challenges of Counterfeit Avoidance Methods", shifts the focus to preventative strategies. It scrutinizes the hurdles in implementing effective systems designed to thwart the infiltration of counterfeit electronics into the supply chain, highlighting the proactive measures necessary to safeguard against such threats. Together, these tables provide a dual perspective on the fight against electronic counterfeiting, offering insights into both reactive detection and proactive prevention.

Table 1. Implementation challenges of counterfeit detection methods.

Detection Scheme	Dependability	Distinctiveness	Tamper Proofing	Chip Area Requirement	Target Component	Deployment Cost
Incoming Inspections	Varies	Moderate	Low	Low	Digital/Analog/RF, etc.	Low
Exterior Tests	Moderate	Moderate	Moderate	Low	Digital/Analog/RF, etc.	Moderate
Interior Tests	High	High	High	High	Digital/Analog/RF, etc.	High
Material Analysis	High	Moderate to High	High	Very High	Digital/Analog/RF, etc.	Very High
Parametric/Burn-in Test and Structural Tests	Very High	High	Very High	Moderate	Digital ICs	Moderate to High

Table 2. Implementation challenges of counterfeit avoidance methods.

Avoidance Scheme	Dependability	Distinctiveness	Tamper Proofing	Chip Area Requirement	Target Component	Deployment Cost
Physically Unclonable Functions (PUFs)	Moderate	High	High	Low	Digital ICs	Moderate
Passive Hardware Metering	Moderate to High	High	Moderate	Low	Digital ICs	Moderate
Active Hardware Metering	High to Very High	High	Moderate	Moderate	Digital ICs	Moderate
Machine Learning/Computer Vision	High	Moderate to High	Low	Varies	Digital ICs	Low
Secure Split Test (SST)	NA	NA	Moderate	Moderate	Digital ICs	High

(a) **Dependability:** Many of these methods grapple with the challenge of consistent performance. For instance, a PUF's reaction should remain unchanged across different environmental conditions, disturbances, and over time. Such issues do not plague active and passive hardware metering, though its ability to prevent counterfeiting is still under examination. Machine Learning, since the accuracy of its results depends on vast dataset, has a high reliability. Incoming Tests ensure initial quality but might vary in dependability based on the test's comprehensiveness.
(b) **Distinctiveness:** This evaluates the dissimilarity between chip identifications. Ideally, two identifiers should have a 50% probability of differing under identical conditions. Strong distinctiveness hinders the ability of counterfeiters to predict new IDs after obtaining a collection. PUFs and magnetic PUFs yield almost perfect results in this aspect. Common programming languages can produce truly random numbers, typically used for chip identification.
(c) **Tamper Proofing:** This gauges the challenges counterfeiters face in trying to bypass anti-counterfeit measures. The locked results of SSTs offer an appreciably high taper resistance to the chips. Material analysis imposes a high level of difficulty in detection because counterfeiting happens at the material composition level. Meanwhile, exterior tests detect tampering at the surface level. Machine Learning, combined with Material Analysis, can detect counterfeit actions at a compositional level.
(d) **Chip Area Requirement:** This represents the space required on the chip that is needed for anti-counterfeit tools. Machine Learning/Computer Vision, on the other hand, might demand significant computational resources but not necessarily chip space. In contrast, hardware metering, SST, and poly fuse-based sensors require more space.
(e) **Targeted Component Types:** This details the component kinds these anti-counterfeit tools are suited for. Parametric/Burn-in and Structural Tests are mostly targeted at digital components, while Incoming Tests can apply to both. PUFs can be used in both analog and digital parts while other tools are more suited for digital components.
(f) **Deployment Cost:** Setting up a PUF involves maintaining a secure challenge-response database, alongside the space it occupies. For hardware metering and SST, extensive communication between the designer and the manufacturer hikes up the price. Tools like CDIR come with their own spatial costs. Verifying integrated circuits demands affordable equipment, but the intricate verification for applied plant DNA on the IC as an interior test is high.

5. Challenges Facing the Microelectronics Industry in Adopting Trust

The COVID-19 pandemic has had a profound impact on the electronics industry, significantly increasing the prevalence and quality of counterfeit electronics. These attacks have grown more sophisticated over time, necessitating equally complex countermeasures in response. Traditional physical inspection countermeasures and confidence-building strategies are both expensive and risky, presenting substantial challenges. The time-consuming process of physically inspecting and testing counterfeit electronics further exacerbates the problem. Additionally, as commercial and military technologies converge, ethical concerns in the IT industry have arisen, prompting businesses to evaluate how their products' capabilities and applications, whether used by the Department of Defense or its adversaries, impact national security.

The growing reliance on microelectronics across various industries has heightened the demand for reliable and secure hardware solutions. In the realm of hardware security, verifying the authenticity and integrity of microelectronic components has become a daunting task. The intricacy of modern supply chains makes comprehensive monitoring from inception to final assembly challenging, increasing the risk of electronic equipment being composed of subpar materials, infected with malware, or subject to intellectual property (IP) theft.

Another challenge in the domain of trusted microelectronics is the ever-evolving landscape of threats and attack vectors. Hackers continuously devise new methods to exploit

hardware systems, necessitating ongoing vigilance from security researchers and designers. Side-channel attacks, for instance, rely on extracting sensitive data through the physical implementation of a system. Given these trends, microelectronics security remains a formidable challenge. As technology advances, physical components become increasingly complex and interconnected, making it challenging to defend against both existing and emerging threats. Consequently, it is evident that addressing these evolving dangers requires the integration of Physically Unclonable Functions (PUFs), robust design principles, and machine learning-based approaches to hardware security.

6. Conclusions

This comprehensive review underscores the significant challenges and threats con fronting the microelectronics industry, particularly from counterfeit components. As explored in Section 2, "Counterfeit Attack Modes", the industry is battling a range of sophisticated methods employed by malicious entities to introduce counterfeit components, undermining the integrity of both individual electronic units and larger systems. The vulnerabilities these attack modes present are not just technical but also ripple into economic, ethical, and security realms.

In response to these threats, Section 3, "Counterfeit Detection", delves into the multifaceted strategies and methods to identify and mitigate the presence of counterfeit components. These detection mechanisms are essential in ensuring the security, reliability, and efficiency of electronic systems. However, the ever-evolving nature of attack vectors demands ongoing research, innovation, and refinement in these detection methodologies.

Beyond the direct threats of counterfeiting, broader challenges have surfaced, such as the ethical dilemmas stemming from the overlap of commercial and military technologies and the heightened risks brought on by the COVID-19 pandemic. The complex interplay of these challenges necessitates a cohesive, interdisciplinary response, ranging from technological solutions like Physically Unclonable Functions (PUFs) and machine learning-based approaches to policy interventions and universally accepted industry standards.

Furthermore, a comparison of the implementation challenges involved in both the avoidance and detection techniques have been explored under the headings of dependability, distinctiveness, tamper proofing, chip area overhead and deployment costs. It must be noted, however, that this provides a generalized perspective. The actual dependability, distinctiveness, tamper proofing, chip area overhead, and ease of implementation may vary depending on the specific methodologies and tools used within each scheme.

In summary, the microelectronics industry is at a critical juncture. Trust and security are non-negotiable pillars for its sustained growth and evolution. By integrating insights from various sections, it is evident that proactive measures, collaborative efforts, and a commitment to continuous learning are vital to navigate the multifarious challenges and ensure a resilient future for microelectronics.

Author Contributions: Conceptualization, K.N., S.D. and V.B.; writing—original draft preparation, K.N.; writing—review and editing, V.B.; supervision, V.B.; funding acquisition, F.L. and V.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the U.S. Air Force via the Assured Digital Microelectronics Education and Training Ecosystem (ADMETE) grant (FA8650-20-2-1136).

Data Availability Statement: The datasets generated and/or analyzed during the current study are available in the "ERAI" repository at https://www.erai.com/ (accessed on 16 April 2022).

Conflicts of Interest: The authors declare no conflict of interest. Additionally, The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Bhunia, S.; Tehranipoor, M. Chapter 1—Introduction to Hardware Security. In *Hardware Security*; Bhunia, S., Tehranipoor, M., Eds.; Morgan Kaufmann: Burlington, MA, USA, 2019; pp. 1–20.
2. Fazzari Booz, S.; Hamilton, A.; Narumi, R. *New & Old Challenges for Trusted and Assured Microelectronics*; Booz Allen Hamilton: Arlington, VA, USA, 2019.
3. Shah, A. Europe, US Warn of Fake-Chip Danger to National Security, Critical Systems. The Register. 2022. Available online: https://www.theregister.com/2022/03/18/eu_us_counterfeit_chips/ (accessed on 13 April 2023).
4. Zeljka, Z. Supply Chain Compromise: Adding Undetectable Hardware Trojans to Integrated Circuits. Help Net Security. 2018. Available online: https://www.helpnetsecurity.com/2018/12/10/hardware-trojans/ (accessed on 19 March 2022).
5. Uppal, R. Threats to ICT Supply Chains including Counterfeit Electronic Components and Hardware Trojans Present Critical Risk to Military and Security Systems. International Defense Security & Technology Inc. 2020. Available online: https://idstch.com/threats/threats-to-ict-supply-chains-including-counterfeit-electronic-components-and-hardware-trojans-present-critical-risk-to-military-and-security-systems/ (accessed on 19 March 2022).
6. Hambling, D. Pentagon's "Kill Switch": Urban Myth? Wired. 2008. Available online: https://www.wired.com/2008/05/kill-switch-urb/ (accessed on 27 March 2023).
7. McKeefry, H. Counter the Counterfeiters. DigiKey. 2021. Available online: https://www.digikey.com/en/blog/counter-the-counterfeiters (accessed on 18 April 2022).
8. Brett, D. Counterfeit Electronic Parts: A Multibillion-Dollar Black Market. Trenton Systems. 2020. Available online: https://www.trentonsystems.com/blog/counterfeit-electronic-parts (accessed on 19 March 2022).
9. The Threat of Counterfeit Components to Electronic Supply Chains. Nanotech. Available online: https://www.nanosecurity.ca/counterfeit-electronic-components/ (accessed on 19 March 2022).
10. IEEE Transactions on Components and Packaging Technologies Publication Information. *IEEE Trans. Compon. Packag. Technol.* **2007**, *30*, C2. [CrossRef]
11. Bastia, S. Next generation technologies to combat counterfeiting of electronic components. *Compon. Packag. Technol. IEEE Trans.* **2002**, *25*, 175–176. [CrossRef]
12. Akhoundov, D. *2022 Annual Report*; ERAI, Inc.: Naples, FL, USA, 2022.
13. Murdock, K.; Oswald, D.; Garcia, F.D.; Van Bulck, J.; Gruss, D.; Piessens, F. Plundervolt: Software-Based Fault Injection Attacks against Intel SGX. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 1466–1482.
14. Tehranipoor, M.; Koushanfar, F. A Survey of Hardware Trojan Taxonomy and Detection. *IEEE Des. Test Comput.* **2010**, *27*, 10–25. [CrossRef]
15. Intel. Speculative Execution. 2018. Available online: https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/introduction-speculative-side-channel-methods.html (accessed on 16 March 2023).
16. Dewan, M.C. Study of Speculative Execution and Branch Prediction. 2006. Available online: https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=EBE980ABF71E4B8C0055F14D3DDAC3F2?doi=10.1.1.119.2934&rep=rep1&type=pdf (accessed on 16 March 2023).
17. Lee, J.W.; Lim, D.; Gassend, B.; Suh, G.E.; Van Dijk, M.; Devadas, S. A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In Proceedings of the 2004 Symposium on VLSI Circuits, Honolulu, HI, USA, 17–19 June 2004; Digest of Technical Papers (IEEE Cat. No.04CH37525). IEEE: Piscataway, PJ, USA, 2004; pp. 176–179.
18. Suh, G.E.; Devadas, S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In Proceedings of the 2007 44th ACM/IEEE Design Automation Conference, San Diego, CA, USA, 4–8 June 2007; pp. 9–14.
19. Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Silicon Physical Random Functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002.
20. Ranasinghe, C.; Engels, D.W.; Cole, P.H. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. Available online: https://www.semanticscholar.org/paper/Security-and-Privacy%3A-Modest-Proposals-for-Low-Cost-Ranasinghe-Engels/4c755bb9751f148a769737addc3e0fb14de42341 (accessed on 27 September 2023).
21. Rührmair, U.; Sehnke, F.; Sölter, J.; Dror, G.; Devadas, S.; Schmidhuber, J. Modeling Attacks on Physical Unclonable Functions. In Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; Association for Computing Machinery: New York, NY, USA, 2010; pp. 237–249.
22. Wang, X.; Tehranipoor, M. Novel Physical Unclonable Function with Process and Environmental Variations. In Proceedings of the 2010 Design, Automation & Test in Europe Conference & Exhibition (DATE 2010), Dresden, Germany, 8–12 March 2010; pp. 1065–1070.
23. Monjur, M.M.R.; Heacock, J.; Calzadillas, J.; Mahmud, M.; Roth, J.; Mankodiya, K.; Sazonov, E.; Yu, Q. Hardware Security in Sensor and its Networks. *Front. Sens.* **2022**, *3*, 850056. [CrossRef]
24. Shivakumara, T.; Patil, R.M.; Muneshwara, M.S. Review Paper on Dynamic Mechanisms of Data Leakage Detection and Prevention. *Int. J. Comput. Sci. Eng.* **2019**, *7*, 349–358.
25. Asadizanjani, N.; Rahman, M.T.; Tehranipoor, M. (Eds.) Package Security. In *Physical Assurance: For Electronic Devices and Systems*; Springer International Publishing: Cham, Switzerland, 2021; pp. 155–177.

26. Sharief, S.; Chahal, P.; Alocilja, E. Application of DNA sequences in anti-counterfeiting: Current progress and challenges. *Int. J. Pharm.* **2021**, *602*, 120580. [CrossRef]
27. Torrance, R.; James, D. The State-of-the-Art in IC Reverse Engineering. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 363–381.
28. Barenghi, A.; Breveglieri, L.; Koren, I.; Naccache, D. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. *Proc. IEEE* **2012**, *100*, 3056–3076. [CrossRef]
29. Balasch, J.; Gierlichs, B.; Verbauwhede, I. An In-Depth and Black-Box Characterization of the Effects of Clock Glitches on 8-Bit MCUs. In Proceedings of the 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, Tokyo, Japan, 29 September 2011; IEEE Computer Society: Washington, DC, USA, 2011; pp. 105–114.
30. Kocher, P.; Jaffe, J.; Jun, B.; Rohatgi, P. Introduction to differential power analysis. *J. Cryptogr. Eng.* **2011**, *1*, 5–27. [CrossRef]
31. Mangard, S.; Oswald, E.; Popp, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*; Springer: New York, NY, USA, 2007.
32. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems—CHES 2004*; Joye, M., Quisquater, J.-J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–29.
33. York, D. Chapter 3—Eavesdropping and Modification. In *Seven Deadliest Unified Communications Attacks*; York, D., Ed.; Syngress: Boston, MA, USA, 2010; pp. 41–69.
34. Alves, T.; Das, R.; Werth, A.; Morris, T. Virtualization of SCADA Testbeds for Cybersecurity Research: A Modular Approach. *Comput. Secur.* **2018**, *77*, 531–546. [CrossRef]
35. Parmar, B. Protecting against spear-phishing. *Comput. Fraud. Secur.* **2012**, *2012*, 8–11. [CrossRef]
36. Cybersecurity for Small Businesses. Federal Communications Commission. Available online: https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses (accessed on 7 September 2023).
37. Subramanyan, P.; Ray, S.; Malik, S. Evaluating the Security of Logic Encryption Algorithms. In Proceedings of the 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 5–7 May 2015; pp. 137–143.
38. Guin, U.; Huang, K.; DiMase, D.; Carulli, J.M.; Tehranipoor, M.; Makris, Y. Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proc. IEEE* **2014**, *102*, 1207–1228. [CrossRef]
39. Baldini, G.; Steri, G.; Dimc, F.; Giuliani, R.; Kamnik, R. Experimental Identification of Smartphones Using Fingerprints of Built-In Micro-Electro Mechanical Systems (MEMS). *Sensors* **2016**, *16*, 818. [CrossRef] [PubMed]
40. A Novel Technique for Effective Detection of Recycled ICs Using Joint Parameter Analysis. IJARTET Journal—Academia.edu. Available online: https://www.academia.edu/9939115/A_Novel_Technique_for_Effective_Detection_of_Recycled_ICs_Using_Joint_Parameter_Analysis (accessed on 27 October 2023).
41. Vosatka, J.; Stern, A.; Hossain, M.M.; Rahman, F.; Allen, J.; Allen, M.; Farahmandi, F.; Tehranipoor, M. Tracking Cloned Electronic Components using a Consortium-based Blockchain Infrastructure. In Proceedings of the 2020 IEEE International Conference on Physical Assurance and Inspection on Electronics, Washington, DC, USA, 28–29 July 2020; PAINE: Durham, NH, USA, 2020. [CrossRef]
42. Xiao, K. Techniques for Improving Security and Trustworthiness of Integrated Circuits. Ph.D. Thesis, University of Connecticut, Storrs, CT, USA, 2015.
43. Klocke, F.; Gorgels, C.; Bouzakis, E.; Stuckenberg, A. Tool life increase of coated carbide tools by micro blasting. *Prod. Eng.* **2009**, *3*, 453–459. [CrossRef]
44. Melentiev, R.; Kang, C.; Shen, G.; Fang, F. Study on surface roughness generated by micro-blasting on Co-Cr-Mo bio-implant. *Wear* **2019**, *428–429*, 111–126. [CrossRef]
45. Gadge, M.; Lohar, G.; Chinchanikar, S. A review on micro-blasting as surface treatment technique for improved cutting tool performance. *Mater. Today Proc.* **2022**, *64*, 725–730. [CrossRef]
46. Candler, R.N.; Park, W.T.; Hopcroft, M.; Kim, B.; Kenny, T.W. Hydrogen diffusion and pressure control of encapsulated mems resonators. In Proceedings of the International Conference on Solid State Sensors and Actuators and Microsystems, Seoul, Republic of Korea, 5–9 June 2005; Digest of Technical Papers, TRANSDUCERS '05. IEEE: Piscataway, NJ, USA, 2005; Volume 1, pp. 920–923. [CrossRef]
47. Ding, C.; Soni, G.; Bozorgi, P.; Piorek, B.D.; Meinhart, C.D.; MacDonald, N.C. A flat heat pipe architecture based on nanostructured titania. *J. Microelectromech. Syst.* **2010**, *19*, 878–884. [CrossRef]
48. Dandapat, N.; Ghosh, S. Interfacial and Cross-sectional Studies of Thermally Cycled Alumina-Monel Brazed Joint. *Trans. Indian Ceram. Soc.* **2020**, *79*, 152–157. [CrossRef]
49. Rahman, M.T.; Asadizanjani, N. Failure Analysis for Hardware Assurance and Security. *Electron. Device Fail. Anal.* **2019**, *21*, 16–24. [CrossRef]
50. Vashistha, N.; Lu, H.; Shi, Q.; Rahman, M.T.; Shen, H.; Woodard, D.L.; Asadizanjani, N.; Tehranipoor, M. Trojan Scanner: Detecting Hardware Trojans with Rapid SEM Imaging combined with Image Processing and Machine Learning. In *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis, Phoenix, AZ, USA, 28 October–1 November 2018*; ASM International. Available online: https://books.google.com/books?hl=en&lr=&id=Mx59DwAAQBAJ&oi=fnd&pg=PA256&dq=SEM+hardware+security&ots=-ibwWTUyG4&sig=l7llYBLLFmyYdJ6SbK-socj3Tx0#v=onepage&q=SEM%20hardware%20security&f=false (accessed on 27 October 2023).

51. Courbon, F.; Loubet-Moundi, P.; Fournier, J.J.A.; Tria, A. A high efficiency Hardware Trojan detection technique based on fast SEM imaging. In Proceedings of the 2015 Design, Automation and Test in Europe Conference & Exhibition (DATE), Grenoble, France, 9–13 March 2015; pp. 788–793. [CrossRef]
52. Rahman, M.T.; Shi, Q.; Tajik, S.; Shen, H.; Woodard, D.L.; Tehranipoor, M.; Asadizanjani, N. Physical inspection attacks: New frontier in hardware security. In Proceedings of the 2018 IEEE 3rd International Verification and Security Workshop, IVSW, Costa Brava, Spain, 2–4 July 2018; pp. 93–102. [CrossRef]
53. Thomas-Brans, F.; Heckmann, T.; Markantonakis, K.; Sauveron, D. New Diagnostic Forensic Protocol for Damaged Secure Digital Memory Cards. *IEEE Access* **2022**, *10*, 33742–33757. [CrossRef]
54. Xi, C.; Khan, A.A.; Jessurun, N.; Vashisthan, N.; Tehranipoor, M.M.; Asadizanjani, N. Physical Assurance for Heterogeneous Integration: Challenges and Opportunities. In Proceedings of the International Symposium on the Physical and Failure Analysis of Integrated Circuits, IPFA, Singapore, 18–20 July 2022. [CrossRef]
55. Klima, S.J.; Baaklini, G.Y.; Abel, P.B. *Nondestructive Evaluation of Structural Ceramics*; NASA: Washington, DC, USA, 1987.
56. Asadizanjani, N.; Rahman, M.T.; Tehranipoor, M. Optical Inspection and Attacks. In *Physical Assurance*; Springer: Cham, Switzerland, 2021; pp. 133–153. [CrossRef]
57. Kulkarni, A.; Xu, C. A Deep Learning Approach in Optical Inspection to Detect Hidden Hardware Trojans and Secure Cybersecurity in Electronics Manufacturing Supply Chains. *Front. Mech. Eng.* **2021**, *7*, 709924. [CrossRef]
58. Vashistha, N.; Rahman, M.T.; Shen, H.; Woodard, D.L.; Asadizanjani, N.; Tehranipoor, M. Detecting Hardware Trojans Inserted by Untrusted Foundry Using Physical Inspection and Advanced Image Processing. *J. Hardw. Syst. Secur.* **2018**, *2*, 333–344. [CrossRef]
59. van Gils, M.A.; van der Sluis, O.; Zhang, G.Q.; Janssen, J.H.; Voncken, R.M. Analysis of Cu/low-k bond pad delamination by using a novel failure index. In Proceedings of the 6th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Micro-Electronics and Micro-Systems, EuroSimE, Berlin, Germany, 18–20 April 2005; pp. 190–196. [CrossRef]
60. Viswanath, A.G.; Fang, W.; Zhang, X.; Ganesh, V.P.; Lim, L.A. Numerical analysis by 3D finite element wire bond simulation on Cu/low-K structures. In Proceedings of the 7th Electronics Packaging Technology Conference, EPTC, Singapore, 7–9 December 2005; Volume 1, pp. 215–220. [CrossRef]
61. Wang, C.; Sun, R. The Quality Test of Wire Bonding. *Mod. Appl. Sci.* **2009**, *3*, 50–56. [CrossRef]
62. Zamalloa Jara, M.A.; Luízar Obregón, C.; Araujo Del Castillo, C. Exploratory analysis for the identification of false banknotes using portable X-ray Fluorescence spectrometer. *Appl. Radiat. Isot.* **2018**, *135*, 212–218. [CrossRef] [PubMed]
63. Camp, D.C. K-Edge X-ray Fluorescence Analysis for Actinide and Heavy Elements Solution Concentration Measurements. *Adv. X-ray Anal.* **1984**, *28*, 91–98. [CrossRef]
64. Anceau, S.; Bleuet, P.; Clédière, J.; Maingault, L.; Rainard, J.L.; Tucoulou, R. Nanofocused X-ray beam to reprogram secure circuits. In Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, 25–28 September 2017; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 10529 LNCS. pp. 175–188. [CrossRef]
65. Chan, K.L.A.; Kazarian, S.G. Detection of trace materials with Fourier transform infrared spectroscopy using a multi-channel detector. *Analyst* **2006**, *131*, 126–131. [CrossRef] [PubMed]
66. Chen, H.; Ferrari, C.; Angiuli, M.; Yao, J.; Raspi, C.; Bramanti, E. Qualitative and quantitative analysis of wood samples by Fourier transform infrared spectroscopy and multivariate analysis. *Carbohydr. Polym.* **2010**, *82*, 772–778. [CrossRef]
67. Lu, H.; Capecci, D.E.; Ghosh, P.; Forte, D.; Woodard, D.L. Computer vision for hardware security. In *Emerging Topics in Hardware Security*; Tehranipoor, M., Ed.; Springer International Publishing: Cham, Switzerland, 2021; pp. 493–525. [CrossRef]
68. Huynh, N.; Cherian, H.; Ahn, E.C. Hardware security of emerging non-volatile memory devices under imaging attacks. In Proceedings of the International Conference on Applied Electronics, Pilsen, Czech Republic, 7–8 September 2021. [CrossRef]
69. Hadjikhani, A.; Rodzinski, A.; Wang, P.; Nagesetti, A.; Guduru, R.; Liang, P.; Runowicz, C.; Shahbazmohamadi, S.; Khizroev, S. Biodistribution and clearance of magnetoelectric nanoparticles for nanomedical applications using energy dispersive spectroscopy. *Nanomedicine* **2017**, *12*, 1801–1822. [CrossRef]
70. Akter, N.; Karabiyik, M.; Shur, M.; Suarez, J.; Pala, N. AI Powered THz VLSI Testing Technology. In Proceedings of the 29th North Atlantic Test Workshop, NATW 2020, Albany, NY, USA, 17–24 June 2020. [CrossRef]
71. Ishibuchi, H.; Kwoh, C.K.; Tan, A.H.; Srinivasan, D.; Miao, C.; Trivedi, A.; Crockett, K.; Institute of Electrical and Electronics Engineers. In Proceedings of the 2022 IEEE Symposium Series on Computational Intelligence (SSCI 2022), Singapore, 4–7 December 2022.
72. Xu, Z.; Cui, A.; Qu, G. A New Aging Sensor for the Detection of Recycled ICs. In Proceedings of the 2020 on Great Lakes Symposium on VLSI, Beijing, China, 8–11 September 2020; pp. 223–228.
73. Guin, U.; DiMase, D.; Tehranipoor, M. Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead. *J. Electron. Test.* **2014**, *30*, 9–23. [CrossRef]
74. Doyle, E.J. *Morris Bill Failure Analysis Techniques*; Rome Air Development Center: Oneida County, NY, USA, 1981.
75. Kim, B.; Park, W.-T. MEMS Packaging. In *Encyclopedia of Nanotechnology*; Bhushan, B., Ed.; Springer: Dordrecht, The Netherlands, 2012; pp. 1351–1359.
76. Davy, J. Calculations for Leak Rates of Hermetic Packages. *IEEE Trans. Parts Hybrids Packag.* **1975**, *11*, 177–189. [CrossRef]

77. Tu, K.N. Reliability challenges in 3D IC packaging technology. *Microelectron. Reliab.* **2011**, *51*, 517–523. [CrossRef]
78. Xi, C.; Jessurun, N.; Asadizanjani, N. A Framework to Assess the Security of Advanced Integrated Circuit (IC) Packaging. In Proceedings of the 2020 IEEE 8th Electronics System-Integration Technology Conference (ESTC), Tonsberg, Norway, 15–18 September 2020; pp. 1–7.
79. Fang, K. 3—Encapsulation Process Technology. In *Encapsulation Technologies for Electronic Applications*, 2nd ed.; Ardebili, H., Zhang, J., Pecht, M.G., Eds.; William Andrew Publishing: Norwich, NY, USA, 2019; pp. 123–181.
80. Zumbusch, A.; Holtom, G.R.; Xie, X.S. Three-Dimensional Vibrational Imaging by Coherent Anti-Stokes Raman Scattering. *Phys. Rev. Lett.* **1999**, *82*, 4142–4145. [CrossRef]
81. Sánchez-Purrà, M.; Roig-Solvas, B.; Rodriguez-Quijada, C.; Leonardo, B.M.; Hamad-Schifferli, K. Reporter Selection for Nanotags in Multiplexed Surface Enhanced Raman Spectroscopy Assays. *ACS Omega* **2018**, *3*, 10733–10742. [CrossRef]
82. Vaskova, H.; Neumann, P.; Kozubik, M.; Jelinek, K. Raman Spectroscopic Study of Counterfeit Electronic Components. *WSEAS Trans. Syst. Control* **2018**, *13*, 453–459.
83. Sinanoglu, O.; Karimi, N.; Rajendran, J.; Karri, R.; Jin, Y.; Huang, K.; Makris, Y. Reconciling the IC test and security dichotomy. In Proceedings of the 2013 18th IEEE European Test Symposium (ETS), Avignon, France, 27–30 May 2013; pp. 1–6.
84. Advances in Kernel Methods—Support Vector Learning. Available online: https://www.researchgate.net/publication/2346087_Advances_in_Kernel_Methods_-_Support_Vector_Learning (accessed on 28 October 2023).
85. Müller, K.R.; Mika, S.; Tsuda, K.; Schölkopf, K. An introduction to kernel-based learning algorithms. *IEEE Trans. Neural Netw.* **2001**, *12*, 181–201. [CrossRef] [PubMed]
86. Huang, K.; Carulli, J.M.; Makris, Y. Parametric counterfeit IC detection via Support Vector Machines. In Proceedings of the 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Austin, TX, USA, 3–5 October 2012; pp. 7–12.
87. Kent, M.; Huynh, N.K.; Schiavon, S.; Selkowitz, S. Using support vector machine to detect desk illuminance sensor blockage for closed-loop daylight harvesting. *Energy Build.* **2022**, *274*, 112443. [CrossRef]
88. Alam, M.A.; Mahapatra, S. A comprehensive model of PMOS NBTI degradation. *Microelectron. Reliab.* **2005**, *45*, 71–81. [CrossRef]
89. Bhardwaj, S.; Wang, W.; Vattikonda, R.; Cao, Y.; Vrudhula, S. Predictive modeling of the NBTI effect for reliable design. In Proceedings of the Custom Integrated Circuits Conference, San Jose, CA, USA, 10–13 September 2006; pp. 189–192. [CrossRef]
90. Kumar, S.V.; Kim, C.H.; Sapatnekar, S.S. An analytical model for negative bias temperature instability. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD, San Jose, CA, USA, 5–8 November 2006; pp. 493–496. [CrossRef]
91. Vattikonda, R.; Wang, W.; Cao, Y. Modeling and minimization of PMOS NBTI effect for robust nanometer design. *Proc. Des. Autom. Conf.* **2006**, 1047–1052. [CrossRef]
92. Wang, W.; Wei, Z.; Yang, S.; Cao, Y. An efficient method to identify critical gates under circuit aging. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD, San Jose, CA, USA, 4–8 November 2007; pp. 735–740. [CrossRef]
93. Rührmair, U.; Devadas, S.; Koushanfar, F. Security Based on Physical Unclonability and Disorder. In *Introduction to Hardware Security and Trust*; Springer: New York, NY, USA, 2012; pp. 65–102.
94. Alkabani, Y.; Koushanfar, F.; Kiyavash, N.; Potkonjak, M. Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. In *Information Hiding: 10th International Workshop, IH 2008, Santa Barbara, CA, USA, 19–21 May 2008*; Revised Selected Papers; Springer: Berlin/Heidelberg, Germany, 2008; pp. 102–117.
95. Gassend, B.; Lim, D.; Clarke, D.; Van Dijk, M.; Marten; Devadas, S. Identification and authentication of integrated circuits. *Concurr. Comput.* **2004**, *16*, 1077–1098. [CrossRef]
96. Zhang, X.; Xiao, K.; Tehranipoor, M. Path-delay fingerprinting for identification of recovered ICs. In Proceedings of the 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Austin, TX, USA, 3–5 October 2012.
97. Arjona, R.; Prada-Delgado, M.A.; Arcenegui, J.; Baturone, I. A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. *Sensors* **2018**, *18*, 2429. [CrossRef]
98. Chakraborty, R.S.; Narasimhan, S.; Bhunia, S. Hardware Trojan: Threats and emerging solutions. In Proceedings of the 2009 IEEE International High Level Design Validation and Test Workshop, San Francisco, CA, USA, 4–6 November 2009; pp. 166–171.
99. Khalafalla, M.; Gebotys, C. PUFs Deep Attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019; pp. 204–209.
100. Taneja, S.; Rajanna, V.K.; Alioto, M. In-Memory Unified TRNG and Multi-Bit PUF for Ubiquitous Hardware Security. *IEEE J. Solid-State Circuits* **2022**, *57*, 153–166. [CrossRef]
101. Servadei, L.; Zennaro, E.; Devarajegowda, K.; Manzinger, M.; Ecker, W.; Wille, R. Accurate Cost Estimation of Memory Systems Inspired by Machine Learning for Computer Vision. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019; pp. 1277–1280.

102. Neto, W.L.; Austin, M.; Temple, S.; Amaru, L.; Tang, X.; Gaillardon, P.E. LSOracle: A Logic Synthesis Framework Driven by Artificial Intelligence: Invited Paper. In Proceedings of the 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Westminster, CO, USA, 4–7 November 2019; pp. 1–6.
103. Xie, Z.; Huang, Y.H.; Fang, G.Q.; Ren, H.; Fang, S.Y.; Chen, Y.; Hu, J. RouteNet: Routability prediction for Mixed-Size Designs Using Convolutional Neural Network. In Proceedings of the 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Diego, CA, USA, 5–8 November 2018; pp. 1–8.
104. Ma, Y.; Ren, H.; Khailany, B.; Sikka, H.; Luo, L.; Natarajan, K.; Yu, B. High Performance Graph Convolutional Networks with Applications in Testability Analysis. In Proceedings of the 56th Annual Design Automation Conference 2019, Las Vegas, NV, USA, 2–6 June 2019.
105. Regazzoni, F.; Bhasin, S.; Pour, A.A.; Alshaer, I.; Aydin, F.; Aysu, A.; Beroulle, V.; Di Natale, G.; Franzon, P.; Hely, D.; et al. Machine Learning and Hardware Security: Challenges and Opportunities. In Proceedings of the 39th International Conference on Computer-Aided Design, San Diego, CA, USA, 2–5 November 2020.
106. Yu, S.Y.; Yasaei, R.; Zhou, Q.; Nguyen, T.; Al Faruque, M.A. HW2VEC: A Graph Learning Tool for Automating Hardware Security. In Proceedings of the 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), San Jose, CA, USA, 13–14 December 2021; pp. 13–23.
107. Koushanfar, F. Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 51–63. [CrossRef]
108. Wei, S.; Nahapetian, A.; Potkonjak, M. Robust passive hardware metering. In Proceedings of the 2011 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, 7–10 November 2011; pp. 802–809.
109. Cui, A.; Yang, Y.; Qu, G.; Li, H. A Secure and Low-overhead Active IC Metering Scheme. In Proceedings of the 2019 IEEE 37th VLSI Test Symposium (VTS), Monterey, CA, USA, 23–25 April 2019; pp. 1–6.
110. Contreras, G.K.; Rahman, M.T.; Tehranipoor, M. Secure Split-Test for preventing IC piracy by untrusted foundry and assembly. In Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems 2013, New York, NY, USA, 2–4 October 2013; pp. 196–203. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.