Physical Assurance for Heterogeneous Integration: Challenges and Opportunities

Chengjie Xi[1], Aslam A. Khan[1], Nathan Jessurun[1], Nidish Vashisthan[1], Mark M. Tehranipoor[1], Navid Asadizanjani[1],
[1]Florida Institute for Cyber Security Research, University of Florida, Gainesville, FL
Email : chengjiexi@ufl.edu, nasadi@ece.ufl.edu,

2022 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA) | 978-1-6654-9815-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/IPFA55383.2022.9915749

Abstract— **Integrated Circuit (IC) hardware assurance is an increasingly concerning topic for semiconductor industries. Because ICs are the industries' fundamental building blocks, they are consistently targeted for adversarial attacks. Physical inspection methods (i.e., Scanning Electron Microscopy (SEM), X-ray, and THz) are used to verify the IC hardware from the transistor to the device level. However, these inspection methods are difficult to apply to emerging packaging technologies and Heterogeneous Integration (HI) due to their inherent limitations and sample complexity. HI complex nature can provide some inherent features employable as countermeasures. For instance, the material and the structural fingerprints can be used to monitor, verify, and provide device assurance. This paper will introduce potential security vulnerabilities in HI hardware and review various physical inspection methods and their limitations surrounding comprehensive assurance. Both non-destructive and destructive methods will be discussed, ranging from material/structural analysis to transistor-level physical inspection. Insights to the MEMS&NEMS implantation into the package to secure the original design, will be also explored in this paper.**

Keywords—Heterogeneous Integration, Advanced Packaging, Hardware Assurance, Physical Inspection, MEMS

I. Introduction

Integrated Circuits (ICs) fabrication is currently heavily reliant on globalization of the semiconductor supply chain and outsourcing. This provides the opportunity to the adversaries to embed components or modify the original design in multiple points throughout the supply chain, resulting in hardware security threats. Detecting malicious changes necessitates the use of advanced inspection equipment and data analysis skills. Furthermore, as the IC packaging trend shifts from homogeneous to heterogeneous integration (HI), new threat models are emerged for hardware. HI has been established as one of the appealing alternatives to enable packaging more transistors in a constrained space following Moore's Law. As shown in Fig.1, HI, also known as chiplet integration, effectively integrates various dies into the same unit. This module-based design requires embedding several third-party chiplets, which also yields opportunities for attackers to embed malicious chips or hardware Trojans. Full reverse engineering could theoretically bring assurance to the end user by detecting any potential modifications [1]. However, this process is very expensive, time-consuming, and requires the involvement of subject matter experts. HI packaging also brings more challenges to the hardware system-level verification [2]. This is in particular very challenging for the case System in Packaging (SiP), which includes both passive and activate components. It is difficult for the end-user to authenticate all the finite elements comprehensively, such as passive and active chiplets, through-silicon vias (TSV), and C-4 bumps [3]. This can introduce both opportunities and challenges in leveraging 3D inspection technologies to auhenticate the system-levelhardware. Adversary such as an untrusted packaging facility can embed a malicious component at the system level resulting in "Big hack" [4] (more detailed threat models are introduced in Section 2) type threats. Therefore, research has developed to mitigate traditional and emerging hardware vulnerabilities. Several physical inspection methods have been adopted to authenticate the different components on an IC package to safeguard the IC without incurring extra costs [4]. These are outlined in Sections 4 & 5 as post-packaging hardware assurance methods.

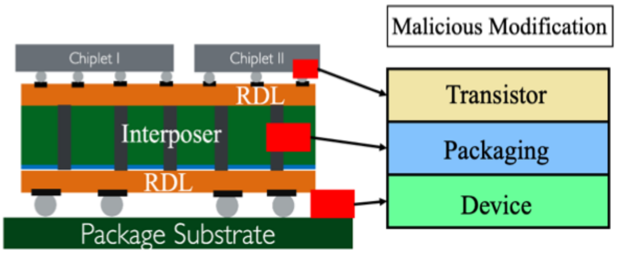

Fig. 1. An example of heterogeneous integration (HI) packaging and the potential malicious modification

Micro-electro-mechanical systems (MEMS) or Nano-electro-mechanical systems (NEMS) are potential solutions to provide security to the modern electronic systems. While providing security benefits, MEMS/NEMS-based active and passive protection enables high volume and inexpensive ASIC device production. Integration of MEMS primitives at the system level will result in significant advancements in semiconductor technology and core security objectives. MEMS devices are mass-produced and packaged in the same way as ICs, but they have unique process variations useful for identification [5] or physical unclonable function (PUF) [6][7]. PUFs can secure an electronic system from tampering in active or passive manner. MEMS integration meets a critically undeveloped aspect of electronic device security, specifically system-level safeguards against counterfeiting and reverse engineering.

II. Hardware-Level HI Packaging Vulnerabilities

The complexity and worldwide distribution of the IC supply chain has long been identified as a critical & concerning factor in hardware security. Different facilities worldwide participate in the IC design, manufacture, packaging, and testing process. As a result, it is prohibitively difficult to predict and control the entire semiconductor supply chain; adversaries can conduct malicious changes of the original design from transistor, packaging and device levels as shown in Fig.1. Severe security threats result when these counterfeit samples are integrated into critical applications such as aerospace, healthcare, transportation, and military domains.

During prominent discussions of hardware vulnerabilities, HI packaging was an emerging technology and did not draw much attention. In contrast, it is a significantly more relevant topic now since it continues scaling according to Moore's Law. Indeed, these improvements resulted in the new description, ‘more than Moore's Law’. Currently, HI packaging is prominently used in limited applications such as integrating high bandwidth memories (HBM) with CPUs or GPUs to achieve higher performance with high bandwidth and shorter interconnects. In the IEEE HI roadmap [8], researchers mentioned in the coming 5-10 years, more passive and active components will be integrated together, such as MEMS, sensors, radar, lidar, and more. HI can potentially contain a whole electronic system called System in Packaging (SiP). By involving more organizations in the supply chain, the introduction of complex HI packaging grows its attack surfaces while sidestepping existing countermeasures. These adversaries can include chiplet foundries or HI packaging outsourced semiconductor assembly and test (OSAT) facilities, as indicated in the HI packaging supply chain model Fig.2.

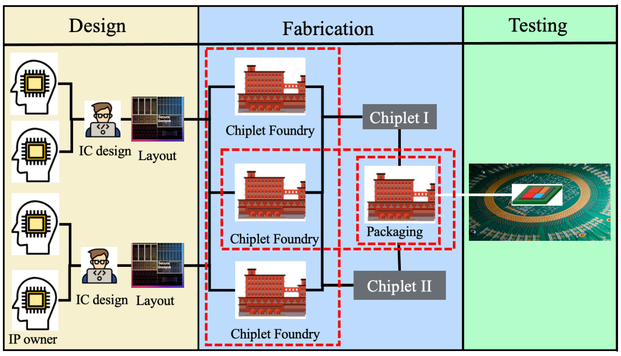

Fig. 2. Supply chain model and threat model of HI packaging. Red dashed boxes indicate potential adversarial entities.

III. Potential Hardware Attacks

As previously mentioned, various threats to hardware security can occur due to supply chain vulnerabilities associated with HI packaging. A comprehensive understanding of attacks, summarized in Fig. 3, yield key insights into these issues and aid in generating appropriate countermeasures. Finally, different physical inspection methods will be described which mitigate some of these concerns.

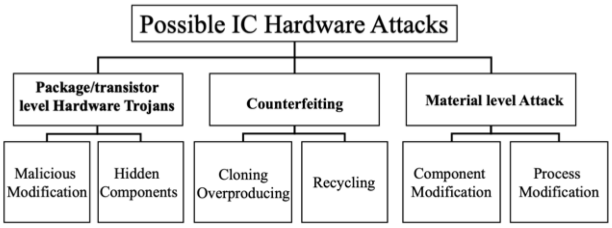

Fig. 3. Potential hardware attacks to HI packaging

A. Hardware Trojans

Hardware Trojans usually refer to modifications of the original IP design by either removing or adding logic gates. These adjustments are usually for adversarial purposes such as leaking data or compromising functionality. Currently, IC designs are highly dependent on third-party IPs, whose owners or foundries can add Trojans or modify the original design. These attacks are referred to as transistor-level hardware Trojans in this work. Different types of transistor-level hardware Trojans have been well summarized and classified in previous research [9]. Beyond this, emerging HI packaging enables actors to insert malicious active *and passive* components, which can be considered package-level hardware Trojans. This problem will compound as the complexity of the system increases, since HI packaging will adopt more third-party chiplets into the system.

Several countermeasures have been developed to protect ICs from the threats described above. IP owners can prevent hardware Trojans by securing the design through run-time monitoring, camouflage, obfuscation, etc. [10]. The IP owner can also use split manufacturing to prevent malicious foundries from having access to entire original design. They can also use pre-silicon verification to compare the received IC designs to their originals. However, the end-user can only verify the hardware design by using post-silicon physical inspection. Ideally, fully reverse engineering a sample using scanning electronic microscopy (SEM) imaging can provide this verification and prevent transistor/package level hardware Trojans. However, this is difficult in practice due to the small physical scale of hardware Trojans. In 2008, Samuel et al. demonstrated this by designing a small backdoor Trojan that could give the attacker complete high-level accessibility. The researchers took advantage of the original design to add 1341 gates which formed hardware Trojans [11]. To effectively detect these Trojans, machine learning-based computer vision methods have been developed without requiring human involvement [12]. Still, the limitation of physical inspection methods complicates the inspection of transistor- and package-level Trojans inside various categories of low technology node devices for ender users.

B. Counterfeit ICs

Guin et al. classified counterfeits into seven separate types: recycled, remarked, overproduced, out-of-spec/defective, cloned, forged documentation, and tampered [13]. These counterfeit samples will not only affect the reputation and profits of the IP owners, but also cause serious confidentiality and reliability issues such as data leakage or backdoors when these counterfeit samples are inserted into critical systems. When considering chip packaging, different physical inspection methods have been developed to verify the sample from different perspectives and make counterfeitting more cost prohibitive. These analyses include material characterization, texture analysis, structure analysis, and more [14]. However, detecting counterfeit samples is still highly challenging, since there is no certain feature which reliably identifies counterfeit samples. Also, the fast development of electronic components leaves numerous generations of IC on the market and makes it even harder to perform generalized counterfeit detection. Due to these challenges as listed above, 100% assurance requires novel advancements beyond current inspection capabilities.

C. Material Based Hardware Attacks

With the development of IC packaging, material innovation plays a more critical role in supporting high-performance devices. For instance, micro-bump material and fabrication processes have been designed to prevent defects or long-term electrical migration [15]. The fabrication process of the high aspect ratio TSV has been designed to achieve uniformity in filling without any defects [16]. In general, HI packaging innovation requires the packaging material to support long-term reliability in severe working environments. Due to the importance of IC packaging material, adversaries can potentially modify the material recipe and cause unwanted reliability problems. This is considered a material-level hardware attack. For instance, epoxy molding compound

(EMC) viscosity is designed to be low enough to fulfill the entire micrometer gap between the die and substrate [17]. Any unwanted change may lead to nonuniform underfilling and affect device reliability. However, altering this substance is relatively easy since it requires minimal advanced knowledge. Adversaries can randomly change the material composition or fabrication processes to achieve the desired effect.

IV. Post-packaging Assurance: Non-destructive Physical Inspections for HI

Various countermeasures have been developed in response to the attacks discussed above. Since end-users cannot easily embed pre-silicon assurance methods in the design, post-silicon methods such as electrical and physical inspection are the required alternative. While electrical testing can often spot anomalies inside the IC, adversaries can purposely design the components to bypass this standard electrical inspection [9]. To verify as many IC samples as possible, non-destructive testing (NDT) methods should be used to perform hardware assurance. Both academia and industry are using physical inspection to prevent extra or missing components & functionality from produced ICs. Several non-destructive physical inspection methods for structural and material characterization will be discussed in this section, which provide various measures of post-silicon hardware assurance.

A. *Structural Characterization*

NDT imaging modalities are mainly used to analyze the structural information such as surface, subsurface, and volumetric imaging of the sample under test. Using proper image processing and data analysis methods, suspicious components and features inside the ICs can be detected. Several IC structural analysis results are shown in Fig. 4.

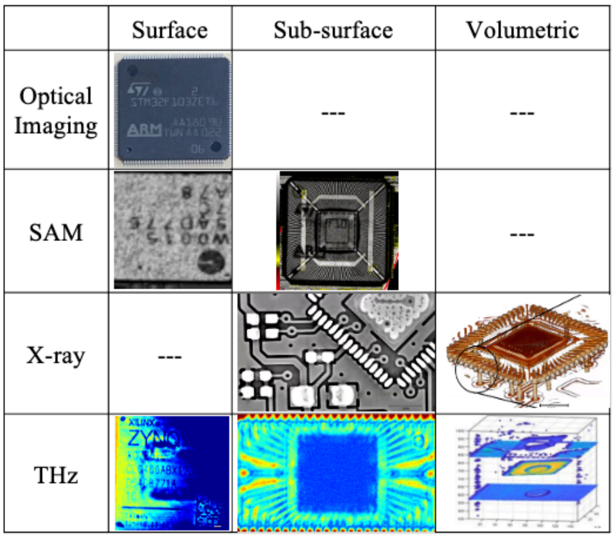

Fig. 4. Physical inspection for IC structural analysis

Optical cameras and microscopes are mainly used to analyze the surface texture, surface color, text, and scale of IC samples as show in Fig.4 [18]. It is easy, fast, and cheap to perform this type of characterization. However, optical imaging also carries some highly apparent drawbacks. These modalities can only characterize visible light information, which carries comparaitively few descriptive features. Also, optical imaging methods highly depend on the sight system, and different lighting setups such as color and intensity can lead to different results and will mislead the inspection process. These problems can often be solved through more robust image preprocessing.

Scanning acoustic microscopy (SAM) raster scans the sample with ultrasonic beams to form a high-resolution subsurface image down to several micrometers. As shown in Fig. 4, by selecting the suitable output signal waveform window, images of a certain sample layer can be characterized. SAM is a powerful tool in IC failure analysis that can detect small defects and delimitation [19]. SAM is also faster than similar approaches, taking minutes to characterize the IC sample on a centimeter scale. However, SAM requires the sample to submerge into liquid which might cause damage. Also, the high-frequency signals used to acquire high-resolution imaging limit its penetration depth and can only characterize a very shallow subsurface [20].

X-ray is adept at characterizing internal IC structure. Conventional 2D X-ray inspection can penetrate packaging substrate and detect internal defects such as cracks and voids for failure analysis. 2D X-ray can also provide top-down imaging of traditional IC samples, which is used to verify the lead frame structure and number of bond wires present. However, 2D X-ray is insufficient to characterize the HI packaging, which has more layers and requires a 3D view to verify the internal structure. Using computed tomography (CT), a 3D structure of the tested sample can be generated [21]. Laminography and digital tomosynthesis are also used for enhanced IC characterization capabilities. However, X-ray can be destructive to some samples such as storage devices, since the high-energy beams can corrupt memory information [22].

B. *Material Characterization*

The previous section mentioned adversaries can trigger hardware vulnerabilities by modifying material recipes. Therefore, characterizing IC packaging material helps prevent this type of attack. Material characterization has been listed as a viable counterfeit detection method since the early 2000s [13]. However, since then limited research has been performed to characterize IC packaging material for hardware assurance. The main reasons for this lack of development are as follows: first, there are currently limited non-destructive material characterization approaches, and the majority of methods suffer from low signal-to-noise ratio (SNR). Low SNR non-destructive material characterization requires a longer time of scanning to eliminate the environment and equipment noise, which can be very time-consuming and unsuitable for IC analysis. Second, current material-based counterfeit detection methods require a golden sample, or known authentic device, for comparison which is often difficult or impossible to obtain. Even with the golden sample, it is difficult to identify whether the difference that appears inside the material is from the magnification variance, environmental noise, malicious modification, or counterfeit samples. Thus, supplementary material characterization methods will be introduced here which overcome these limitations. When combined with data analysis and classification, material characterization can provide hardware assurance without using golden samples.

High SNR material characterization is usually achieved through leveraging a high energy source such as X-ray, electron beam, laser, etc. However, the downside of this approach is the potential to damage the samples under test. Fortunately, infrared (IR) laser sources located between the microwave and visible light break this pattern by exhibiting relatively high SNR for their beam energy among the material characterization resources. Also, IR is transparent to IC packaging material and can be used to characterize the subsurface material. Different IR spectrums with different wavelengths and bandwidths have been developed, such as near-infrared (NIR), mid-infrared (MIR), and Far-infrared (FIR) as shown in Fig.5(a). FIR, however, is not suitable for packaging due to its low energy and low SNR. Thus, it will not be discussed here.

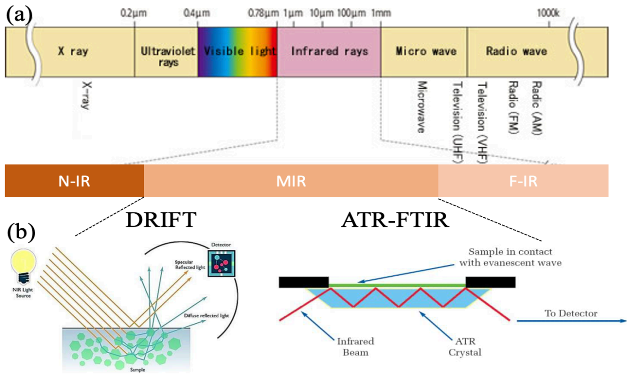

Fig. 5. (a) IR laser (b) Different type of M-IR spectroscopy: DRIFT, ATR- FTIR

NIR spectroscopy has the highest energy among IR material characterization mentioned above and can have high SNR with a relatively short characterization duration. NIR is also used to characterize wood, food, and pharmaceuticals non-destructively [23]. With different experiment setups, NIR methods can have reflection and transmission models for different applications. Portable NIR equipment also exists on the market at a low price, which can greatly increase the efficiency of IC packaging material characterization. Based on these facts, NIR is an ideal method as a hardware material characterization method. However, its high energy source and narrow bandwidth result in wave interference when imaging heterogeneous materials. The overlapping signals greatly complicate the material characterization process, limiting its application to hardware security.

Mid-IR is also used for material characterization and contains more information compared to NIR instruments. Two non-destructive MIR spectrum systems will be highlighted in particular: attenuated total reflection Fourier Transform Infrared (ATR-FTIR) and Diffuse Reflectance Infrared Fourier Transform (DRIFT) Spectroscopy as shown in Fig. 5(b). ATF-FTIR requires a tip to achieve perfect surface contact with the sample surface and collect the reflected information. However, due to the hardness and roughness of the package encapsulant material, it is very difficult to achieve perfect tip-to-surface contact, which will affect the test results [24]. Alternatively, DRIFT is a contactless material characterization without this issue. The DRIFT system can collect the surface and subsurface reflected signal in a contactless manner. The material composition can be characterized by comparing the signal intensity change between the input and output signals. Despite these benefits, the SNR of DRIFT is not high enough to provide qualitative and quantitative analysis of the IC packaging due to signal scattering caused by the rough surface and silica filter material underneath the surface. However, with the help of data analysis methods, it can be adapted to analyze the packaging material and review the material difference between different types of the samples. This can be used to provide hardware assurance through detecting suspicious counterfeit samples.

Raman spectroscopy is also used as an organic and inorganic material characterization method. Raman spectroscopy can use a near-IR (1064nm) laser source to achieve a lower fluorescent effect than the system that uses a visible laser source system [25]. However, it is insufficient to characterize package encapsulant material, which has a very strong photoluminescence effect. This makes Raman spectroscopy unable to detect the material difference inside the packaging and unreliable for hardware assurance purposes.

V. Post-packaging Assurance: Destructive Physical Inspections for HI

The most reliable and comprehensive countermeasure to provide full hardware assurance is to reverse engineer the whole IC design with the help of different imaging modalities and sample preparation [26]. Reverse engineering (RE) is performed to detect cloning of ICs and intellectual property (IP) piracy. It involves removing consecutive IC layers and taking periodic images to reconstruct a netlist. A precision milling machine is used to decapsulate a packaged IC with up to 2um of accuracy. Further device layers such as passivation, metal layers, vias, polysilicon, and active regions can be removed by CNC polishing with alternate SEM imaging after removing every layer. Since the silicon substrate is a thick layer, it is time-consuming to perform milling and polishing from the IC's backside.

Trojan Scanner (TS) is a hardware assurance framework that uses SEM images of logic cells from a backside thinned silicon die to detect hardware Trojans. These images of logic cells can be compared with golden (trusted) logic cells, or GDSII layout to detect Trojans[27]. A sample for TS can be prepared by milling an epoxy package to decapsulate the silicon die. Otherwise, a bare die or a flip-chip can be directly milled using a mechanical milling from the backside to remove the silicon substrate down to 10 um of remaining silicon thickness (RST). Finally, the silicon die can be polished to 1 um of RST to achieve a mirror finish. After polishing, silicon can be removed further using a plasma FIB followed by high-quality image acquisition using a SEM. TS requires an even polishing surface with less than a 100 nm gradient. Evenly polished surfaces ensure that SEM only captures logic cells, not the overlapping images from the underlying device layers such as polysilicon, vias, and metal. Overlapping images can cause errors in image analysis and hence false positives.

VI. Pre-packaging Assurance: MEMS & NEMS

The chips used in current electronic devices are largely produced and packaged by OSAT facilities, which are sometimes unreliable and prone to attacks. Due to the complexity of the global supply chain, it is impossible for individual trusted foundries or IP owners to control the whole fabrication and packaging process. Throughout various steps in the supply chain, the golden design of interposer I/O created by IP owners for fabrication and packaging of the chiplets stays visible. As a result, its design may be viewed by any entity in the supply chain using physical inspection techniques, making it vulnerable if any rogue entities are present. Potential adversaries such as end-users, reverse engineering entities, System on Chip (SOC) integrators, untrusted foundries, or interposer foundries may perform possible attacks such as IP piracy, overproducing, reverse engineering, and counterfeiting [28]. Many preventative approaches, including camouflaging, logic locking, and Finite State Machine (FSM), have been proposed against these threats and are commonly regarded to be secure [29][30]. However, because actual reverse engineering abilities and eventual modification are overlooked in security studies, the safety of these sequential obfuscation strategies is not certain.

The use of MEMS/NEMS in the system will result in a revolutionary and unique approach toward reconfigurable advanced packaging to conceal and logically lock the true golden design from attackers across the supply chain. The netlist/golden design will be hidden from hostile adversaries using this unique approach, and the IP creator will retain control of its design until it reaches the end-user. The primary advantage of this unique method is that the trusted designer or IP owner will be able to reconfigure and obfuscate the golden hardware design along the supply chain. Unlike typical obfuscation methods, the hardware connections will be modified and changed while the device is operational. In other words, the setup for interconnects and I/Os will have two states: ON-state and OFF-state architecture.

This technology would integrate existing active and passive protection into a low-cost MEMS device, allowing system designers to choose which IC connections should be secured. The MEMS device obscures connections between several integrated circuits, making effective non-destructive X-ray design derivation more difficult. Advanced generations might include passive X-ray absorption materials in the packaging and active internal devices to adaptively reorganize the circuitry, further obscuring the design.

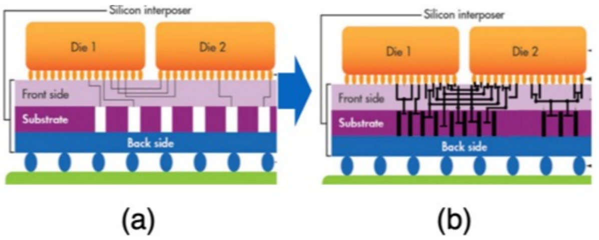

Fig. 6. (a) Existing IC packaging. (b) Reconfigurable IC packaging routed with NEMS array

VII. Discussion & conclusion

In this paper, conventional IC supply chain vulnerabilities are re-evaluated for modern HI packaging and new vulnerabilities to IC hardware security are considered. From this discussion, three different types of potential attacks on ICs (especially in HI packaging) are introduced: Trojans, counterfeit ICs, and material modifications. Traditional physical inspection methods used for material and volumetric characterization are introduced, along with their limitations at combatting emerging vulnerabilities. Globalization causes IC design, implementation, and manufacturing to include a plethora of untrusted suppliers and stakeholders. As a result, a designer's IP is visible to multiple parties which further complicates the process of hardware verification. Though various studies have presented threat mitigation strategies, a majority of the assurance techniques are in doubt since they lack comprehensive coverage. This study thoroughly examined the security and limitations of numerous cutting-edge assurance approaches for HI, especially utilizing MEMS/NEMS for customization, functional obfuscation, and reconfigurability before packaging.

References

[1] N. Vashistha, H. Lu, Q. Shi, M. T. Rahman, H. Shen, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, “Trojan Scanner: Detecting Hardware Trojans with Rapid SEM Imaging Combined with Image Processing and Machine Learning,” *ISTFA 2018 Conf. Proc. from 44th Int. Symp. Test. Fail. Anal.*, vol. 81009, no. January 2020, pp. 256–265, 2018, doi: 10.31399/asm.cp.istfa2018p0256.

[2] P. Gu, S. Li, D. Stow, R. Barnes, L. Liu, Y. Xie, and E. Kursun, “Leveraging 3D technologies for hardware security: Opportunities and challenges,” *Proc. ACM Gt. Lakes Symp. VLSI, GLSVLSI*, vol. 18-20-May-, pp. 347–352, 2016, doi: 10.1145/2902961.2903512.

[3] T. G. Lenihan, L. Matthew, and E. J. Vardaman, “Developments in 2.5D: The Role of Silicon Interposers,” pp. 53–55, 2013.

[4] D. Mehta, H. Lu, O. P. Paradis, M. A. Mukhil, M. T. Rahman, Y. Iskander, P. Chawla, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, “The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants,” *ACM J. Emerg. Technol. Comput. Syst.*, vol. 16, no. 4, 2020, doi: 10.1145/3401980.

[5] G. Baldini, G. Steri, F. Dimc, R. Giuliani, and R. Kamnik, “Experimental identification of smartphones using fingerprints of built-in micro-electro mechanical systems (MEMS),” *Sensors (Switzerland)*, vol. 16, no. 6, pp. 1–20, 2016, doi: 10.3390/s16060818.

[6] M. Martin and J. Plusquellic, “Notchpuf: Printed circuit board puf based on microstrip notch filter,” *Cryptography*, vol. 4, no. 2, pp. 1–20, 2020, doi: 10.3390/cryptography4020011.

[7] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, “A PUF taxonomy,” *Appl. Phys. Rev.*, vol. 6, no. 1, 2019, doi: 10.1063/1.5079407.

[8] “Heterogeneous Integration Roadmap 2021 Edition Chapter 11: MEMS and Sensor Integration,” 2021, [Online]. Available: https://eps.ieee.org/images/files/HIR_2021/ch11_MEMS.pdf.

[9] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, “Hardware trojan: Threats and emerging solutions,” *Proc. - IEEE Int. High-Level Des. Valid. Test Work. HLDVT*, pp. 166–171, 2009, doi: 10.1109/HLDVT.2009.5340158.

[10] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, “Hardware trojans: Lessons learned after one decade of research,” *ACM Trans. Des. Autom. Electron. Syst.*, vol. 22, no. 1, 2016, doi: 10.1145/2906147.

[11] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, “Designing and implementing malicious hardware,” *LEET 2008 - 1st USENIX Work. Large-Scale Exploit. Emergent Threat. Botnets, Spyware, Worms, More*, 2008.

[12] M. Tehranipoor and F. Koushanfar, “A survey of hardware trojan taxonomy and detection,” *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, 2010, doi: 10.1109/MDT.2010.7.

[13] U. Guin, K. Huang, D. Dimase, J. M. Carulli, M. Tehranipoor, and Y. Makris, “Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain,” *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014, doi: 10.1109/JPROC.2014.2332291.

[14] U. Guin and M. Tehranipoor, “Counterfeit detection technology assessment.” GOMACTech, 2013.

[15] B. Banijamali, S. Ramalingam, H. Liu, and M. Kim, “Outstanding and innovative reliability study of 3D TSV interposer and fine

pitch solder micro-bumps," *Proc. - Electron. Components Technol. Conf.*, pp. 309–314, 2012, doi: 10.1109/ECTC.2012.6248847.

[16] B. Banijamali, S. Ramalingam, K. Nagarajan, and R. Chaware, "Advanced reliability study of TSV interposers and interconnects for the 28nm technology FPGA," *Proc. - Electron. Components Technol. Conf.*, pp. 285–290, 2011, doi: 10.1109/ECTC.2011.5898527.

[17] J. H. Lau, M. Li, D. Tian, N. Fan, E. Kuah, W. Kai, M. Li, J. Hao, Y. M. Cheung, Z. Li, K. H. Tan, R. Beica, T. Taylor, C. T. Ko, H. Yang, Y. H. Chen, S. P. Lim, N. C. Lee, J. Ran, C. Xi, K. S. Wee, and Q. Yong, "Warpage and Thermal Characterization of Fan-Out Wafer-Level Packaging," *IEEE Trans. Components, Packag. Manuf. Technol.*, vol. 7, no. 10, pp. 1729–1738, 2017, doi: 10.1109/TCPMT.2017.2715185.

[18] P. Ghosh and R. S. Chakraborty, "Recycled and Remarked Counterfeit Integrated Circuit Detection by Image-Processing-Based Package Texture and Indent Analysis," *IEEE Trans. Ind. Informatics*, vol. 15, no. 4, pp. 1966–1974, 2019, doi: 10.1109/TII.2018.2860953.

[19] D. Johnson, P.-W. Hsu, C. Xi, and N. Asadizanjani, "Scanning Acoustic Microscopy Package Fingerprint Extraction for Integrate Circuit Hardware Assurance," *ISTFA 2021 Conf. Proc. from 47th Int. Symp. Test. Fail. Anal.*, vol. 84215, pp. 59–64, 2021, doi: 10.31399/asm.cp.istfa2021p0059.

[20] G. M. Zhang, D. M. Harvey, and D. R. Braden, "Microelectronic package characterisation using scanning acoustic microscopy," *NDT E Int.*, vol. 40, no. 8, pp. 609–617, 2007, doi: 10.1016/j.ndteint.2007.05.002.

[21] E. L. Principe, N. Asadizanjani, D. Forte, M. Tehranipoor, R. Chivas, M. DiBattista, S. Silverman, M. Marsh, N. Piche, and J. Mastovich, "Steps toward automated deprocessing of integrated circuits," *Conf. Proc. from Int. Symp. Test. Fail. Anal.*, vol. 2017-Novem, pp. 285–298, 2017, doi: 10.31399/asm.cp.istfa2017p0285.

[22] A. Ditali, M. K. Ma, and M. Johnston, "X-ray radiation effect in DRAM retention time," *IEEE Trans. Device Mater. Reliab.*, vol. 7, no. 1, pp. 105–111, 2007, doi: 10.1109/TDMR.2007.891530.

[23] C. Pasquini, "Near infrared spectroscopy: A mature analytical technique with new perspectives – A review," *Anal. Chim. Acta*, vol. 1026, pp. 8–36, 2018, doi: 10.1016/j.aca.2018.04.004.

[24] R. Karoui, G. Downey, and C. Blecker, "Mid-infrared spectroscopy coupled with chemometrics: A tool for the analysis of intact food systems and the exploration of their molecular structure-quality relationships-A review," *Chem. Rev.*, vol. 110, no. 10, pp. 6144–6168, 2010, doi: 10.1021/cr100090k.

[25] R. Gautam, S. Vanga, F. Ariese, and S. Umapathy, "Review of multidimensional data processing approaches for Raman and infrared spectroscopy," *EPJ Tech. Instrum.*, vol. 2, no. 1, p. 38, 2015, doi: 10.1140/epjti/s40485-015-0018-6.

[26] R. Wilson, H. Lu, M. Zhu, D. Forte, and D. L. Woodard, "REFICS: A Step Towards Linking Vision with Hardware Assurance," *Proc. - 2022 IEEE/CVF Winter Conf. Appl. Comput. Vision, WACV 2022*, pp. 3461–3470, 2022, doi: 10.1109/WACV51458.2022.00352.

[27] F. Courbon, P. Loubet-Moundi, J. J. A. Fournier, and A. Tria, "A high efficiency Hardware Trojan detection technique based on fast SEM imaging," *Proc. -Design, Autom. Test Eur. DATE*, vol. 2015-April, pp. 788–793, 2015, doi: 10.7873/date.2015.1104.

[28] M. Nabeel, M. Ashraf, S. Patnaik, V. Soteriou, O. Sinanoglu, and J. Knechtel, "An Interposer-Based Root of Trust: Seize the Opportunity for Secure System-Level Integration of Untrusted Chiplets," 2019, [Online]. Available: http://arxiv.org/abs/1906.02044.

[29] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *Integration*, vol. 72, 2020, doi: 10.1016/j.vlsi.2019.12.007.

[30] S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Clediere, R. Wacquez, J. Fournier, J. C. Souriau, G. Simon, and A. Merle, "A Novel Structure for Backside Protection Against Physical Attacks on Secure Chips or SiP," *Proc. - Electron. Components Technol. Conf.*, vol. 2018-May, pp. 515–520, 2018, doi: 10.1109/ECTC.2018.00081.