Editors: Jelena Mirkovic, mirkovic@isi.edu | Blair Taylor, btaylor@towson.edu

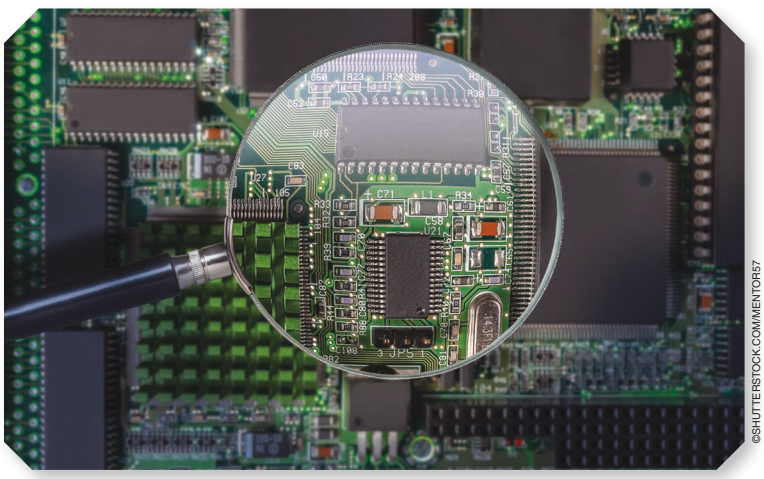
Physical Inspection and Attacks on Electronics

An Academic Course for the Hardware Cybersecurity Workforce

John True and Navid Asadizanjani | University of Florida

Many topics in the hardware security community, such as physical inspection and attacks, are still in early stages of research. As the semiconductor industry continues to advance towards higher volume production, there is an increasing demand to inspect and verify the functionality and security of these devices. This article aims to increase academic exposure to these research areas and raise awareness around educating the cybersecurity workforce.

The hardware security community has grown significantly over the past decade. However, many of the more advanced topics are still in the early stages of research and investigation, and some are only in the development phase. One topic, physical inspection and attacks on electronics (PHIKS), has received attention from the industry. Currently, the cost and expertise for the required equipment are prohibitive. At present, only well-funded university laboratories are likely to have the tools to study physical inspections and attacks. The advancements in the microscopy tools enable the imaging of emitted photons of a live transistor and measure its frequency using high-speed digitizers.[1] Such capabilities can be used to read data from a live chip before encryption and even extract a secret key without going through exhaustive electrical testing procedures. Books have been published[2] to help teach academic researchers, students, and practitioners the basic concepts of hardware security problems from intellectual property (IP) cores; to systems-on-chip; to integrated circuits (ICs);[3] to larger electronics systems, such as printed circuit boards (PCBs).[4,5] However, these educational activities still fail to improve students' understanding of physical inspections, attacks, reverse engineering (RE), and countermeasures and how to properly analyze their results.



©SHUTTERSTOCK.COM/MENTOR57

The University of Florida (UF) PHIKS course and curriculum have been established to prepare students, industry employees, and

Digital Object Identifier 10.1109/MSEC.2023.3236999
Date of current version: 15 March 2023

executives on the current landscape of hardware attacks and teach them how to effectively and efficiently prevent them. The goal of this article is to increase the academic exposure to these research areas and raise awareness around educating the cybersecurity workforce on the current attacks and state-of-the-art equipment used to mitigate them.

Motivation

There is a wide array of emerging attacks on hardware at different stages of its lifecycle (from design to resign).[6,7] The hardware "root-of-trust" assumption is rapidly becoming obsolete. Globalization of the electronics supply chain is one of the most prominent sources of hardware security threats today. Economic trends have shifted IC and PCB design, fabrication, assembly, and distribution to include third-party (and often offshore) entities, giving rise to a variety of threats.[8] Since hardware exists at the lowest abstraction level of a system, an attack on hardware can cripple everything, regardless of countermeasures employed at higher levels. Furthermore, since hardware often cannot be patched/fixed/updated as easily as software, most hardware vulnerabilities will require a complete replacement, making such issues expensive to deal with. We believe the effective education of the future workforce in the area of hardware supply chain cybersecurity is of the utmost importance. To develop countermeasures against such attacks, one requires a complete understanding of the attack itself as a first step. Computer system security engineers are lacking this knowledge in the area of physical inspection and attacks based on the lack of courses dedicated to this material. The UF PHIKS course has been established to train students with skills in various aspects of physical inspection and attacks, including counterfeit detection, RE, physical attacks using probing/photon emission (PE)/voltage imaging, anti-RE, and countermeasure against physical attacks.

In this article, we present the current hardware security challenges facing the semiconductor industry while exploring research areas where academia can contribute through learning and workforce training. The "Current Challenges" section establishes the most common challenges faced, the "Lab Equipment" section covers the curriculum and laboratory tools within the PHIKS course, and the "Research Solutions in the PHIKS Course" section highlights the research areas where academia has provided critical countermeasures for the hardware assurance industry. The "Experiences" section recounts experiences with teaching the PHIKS course. Finally, the final section highlights the future work for the course, research, and workforce development in the field of hardware assurance.

Since hardware exists at the lowest abstraction level of a system, an attack on hardware can cripple everything, regardless of countermeasures employed at higher levels.

Current Challenges

Counterfeit Detection

Counterfeit ICs have become a widespread problem due to the asymmetric challenge of verifying the authenticity of billions of various components before their final integration. These components integrated into critical systems, such as transportation, health care, or military applications, can lead to failure and loss of life. This has created a need to establish robust testing, detection, and avoidance techniques to mitigate the worldwide outbreak of counterfeit ICs.[9] Currently, regulatory procedures are in place, such as in the automotive and military sectors, to prevent gross penetration of counterfeit ICs into supply chains, but there is a lack of academic research areas in counterfeit IC detection.

The characterization and analysis of counterfeit electronics remain nontrivial and suffer from a variety of challenges:

- Modern ICs/PCBs are too complex to undergo exhaustive tests. Counterfeit tests are often performed by original equipment manufacturers, who do not have access to the original design and might not even have access to a working authentic component to compare results with.
- It is well known that semiconductor scaling of modern ICs has resulted in considerable process variation. Such variation makes it difficult to establish automated counterfeit detection thresholds for electrical anomalies. Authentic devices with variations can trigger false positives, increasing the difficulty of efficient counterfeit detection.
- Physical inspection is often considered one of the most effective methods for detection. In counterfeits, inspection is used to extract anomalies (defects) in the component's interior, exterior, and material composition that are consistent with counterfeiting. These tests are time-consuming and require expensive equipment (X-ray, optical microscopy, a scanning electronic microscope, etc.). Counterfeit detection is also performed manually

by subject matter experts (SMEs), a process that is often inconsistent and error prone.

Physical Attack and Detection

Attacks on electronics can be noninvasive, semi-invasive, and invasive. Noninvasive attacks involve protocol design flaws, side-channel attacks, and other vulnerabilities that manifest themselves externally. Such attacks are categorized as electrical testing attacks and are not the focus of our coursework. Our course focuses on semi-invasive and invasive attacks.

Semi-invasive attacks lie between invasive and noninvasive attacks: they employ depackaging to access the silicon chip, while the passivization layer is undamaged, limiting the time necessary to prepare the attack by removing microprobing requirements. These attacks can employ nondestructive tools, such as X-ray, laser, or other radiation-based techniques, to characterize and inject faults into the circuitry.

Invasive attacks are often the most complicated and time-consuming: an attacker uses chip testing equipment such as probing stations, focused ion beam (FIB)/electron beam workstations, or similar tools to extract data from the chip directly. Invasive attacks provide an almost unlimited capability to extract information from chips and understand their functionality. Such attacks are already exploited on chips to bypass security and extract data. For instance, data on Flash and electrically erasable programmable read-only memory cells were revealed by Courbon et al.[10] using FIB-scanning electron microscopy (FIB-SEM) systems. Such tools used to be very expensive and normally were available only to large labs and organizations; however, with advancements in the microscopy world, they are getting cheaper and more accessible to the public. Countermeasures and detection mechanisms, such as "active shield" or tamper detection, are discussed in the "Countermeasures for Probing Attacks."

RE

The globalization of IC and PCB industries has resulted in well-documented concerns, such as counterfeiting and hardware Trojans.[2,9] For such instances, physical inspection and RE represent important tools for validating the performance, quality, authenticity, and integrity of electronics. Physical inspection involves a visual examination of the PCB or IC interior and exterior. In the case of RE, many of the critical systems and infrastructures in use today are decades old. Maintaining them requires electronic components that are no longer available. Replacing or redesigning the entire system may be too time-consuming or expensive. However, through RE, one can study the particular component/board to reproduce it and/or replace it with an alternative in the legacy system. Our coursework teaches students how to apply image processing and pattern recognition to conduct RE.[4]

PHIKS Coursework

Lab Equipment

The Security and Assurance Lab (SCAN) at UF has a 2,500-ft^2 security research laboratory, housing more than US$7 million in advanced scientific equipment. Figure 1(a) shows our nondestructive and destructive imaging and circuit edit tools, which include the Leica MV6 optical microscope with 2D and 3D imaging capabilities and additional features to collect images in a semiautomated fashion; Bruker Skyscan 2211 Micro-computed tomography (CT) system; two TESCAN SEM-FIB systems (FERA and LYRA) with plasma and gallium ion columns; and the Zeiss Orion NanoFab with helium and neon beams for high-resolution edits down to fewer than 10 nm.

Figure 1(b) shows the Cascade Summit system, which was recently purchased, and is a microprobe station with a heating stage, with four positioners to measure current–voltage characteristics on samples after IC editing using any of our FIB systems. Figure 1(c) shows a new PE microscope from Hamamatsu, the Phemos-1000, capable of laser fault injection attacks. Finally, the lab also contains a wide array of bench equipment, such as power supplies, multimeters, oscilloscopes, waveform generators, and logic analyzers.

Course Modules

The focus of our PHIKS course is to introduce advanced techniques for physical inspection and attacks on electronic systems and components. Our recent research findings to automate the inspection approaches for RE and counterfeit detection are incorporated into the course modules.[11] More than 10 modules are discussed in this course to cover all aspects of this topic:

- Counterfeit Detection I and II
- Reliability Analysis
- Integrity Analysis
- PCB RE
- IC RE
- Anti-RE
- Invasive Physical Attacks on ICs
- Semi- and Noninvasive Physical Attacks on ICs
- Microprobing and Nanoprobing Attacks.

Throughout the course, both undergraduate and graduate students proceed through each module by first being presented with slides and then being given the opportunity to experiment with the related inspection equipment. It is important to ensure that they are able to perform complicated experiments safely and not damage the

equipment, and there are teaching assistants (TAs) available for students to observe and then repeat the process with a TA's help. This hands-on experimentation allows for a balance between theory and practice and allows students to gain a deeper understanding of the material through direct experience. This approach to learning can be more beneficial than simply seeing videos or slides of how something is done, as it allows students to actively engage with the material and apply their knowledge in a practical setting.

The most recent techniques for physical inspection and attacks are based on the tools and methodologies developed for failure analysis (FA) in electronics. FA tools are primarily developed to detect a defect during or after the fabrication process, but they have good enough resolution to detect Trojans, extract secret keys, or reverse engineer ICs. Such tools include different imaging modalities, such as an optical microscope, SEM, FIB, a PE microscope, X-ray microscopy, etc. as well as probe stations, all of which are part of our facilities at SCAN lab. It is worth mentioning that these attacks require a very sophisticated sample preparation process to expose a targeted area for RE or other measurements.

Research Solutions in the PHIKS Course

Automated Counterfeit Detection

Today, there are two main approaches for detecting counterfeit ICs: physical inspection and electrical tests. In our PHIKS course, we focus on the first approach. Physical inspection tests use high-tech imaging solutions (X-ray, SEMs, etc.) to determine interior and exterior defects associated with counterfeits. Figure 2 shows a few examples of counterfeit parts identified in our own lab and their defects. In Figure 2(a), X-ray CT has identified the remarking of components based on the presence of blacktop coating and differences in die orientation from authentic samples. Figure 2(b) shows several defects visible in optical images: earlier ("ghost") markings in a remarked chip, scratches on a recycled component's package, and retinned leads on a recycled chip. In Figure 2(c), SEM/elemental dispersive spectroscopy shows

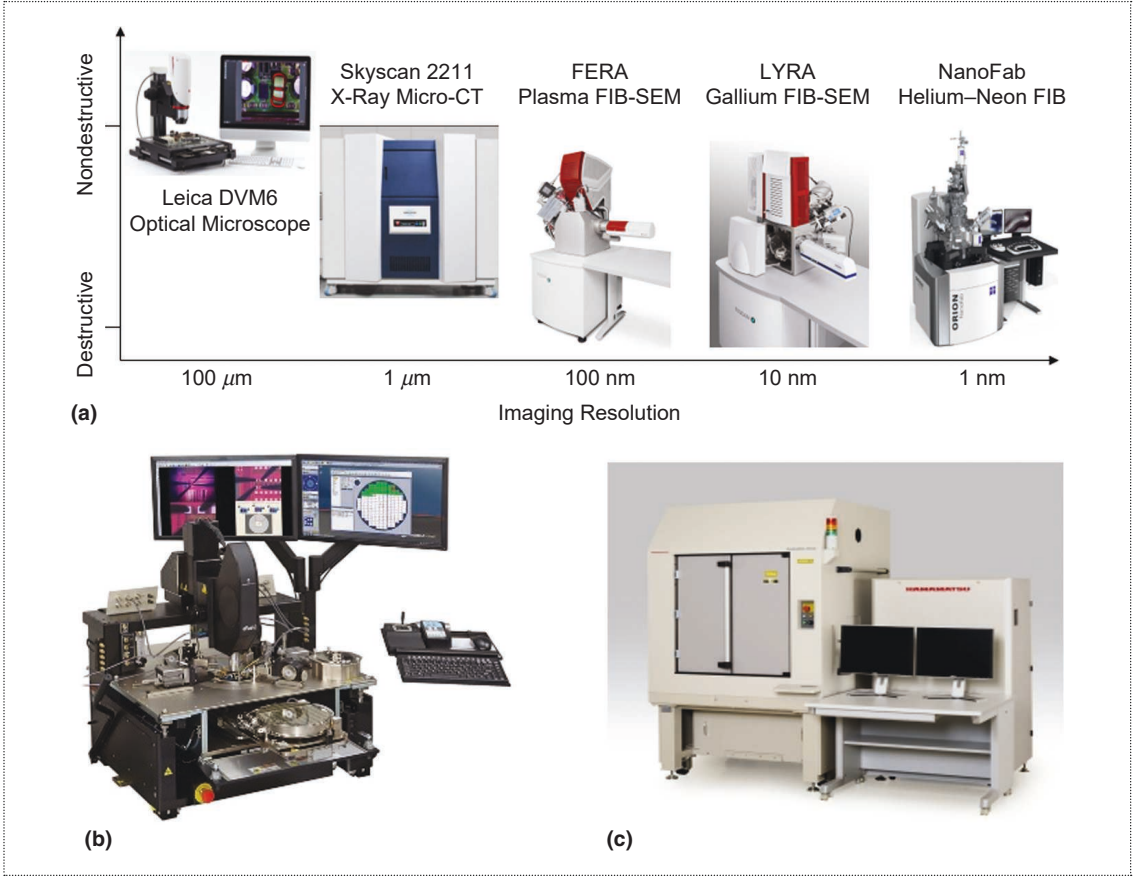


Figure 1. The SCAN lab advanced capabilities: physical inspection equipment includes (a) a Bruker Skyscan 2211 X-ray Micro-CT, TESCAN FERA and LYRA SEM-FIB systems, and a Zeiss Orion NanoFab; soon-to-be-added systems include (b) a Cascade Summit microprobe station and (c) a Hamamatsu Phemos-1000.

lead contamination on a recycled chip and differences in the marking texture of Intel Flash memory from authentic chips.

While physical inspection is applicable to a wide array of part types (analog, digital, and mixed) and sizes (large and small), it suffers from significant challenges as discussed earlier, high test time and costs, a destructive nature, a reliance on trained SMEs, and a lack of automation. Physical inspection can generate a large amount of characterization data from optical, X-ray, and SEM imaging tools. To process this information, image processing techniques are taught on how to perform filtering and edge detection. Students are tasked with analyzing data, such as markings on an IC, to perform identification of the text and logo.

Countermeasures for Probing Attacks

ICs host a series of security applications that are threatened by probing attacks; thus, attacks can directly probe the wires carrying sensitive information using FIB. Through the use of electronic design automation tools combined with equipment that can mill and deposit material with nanometer-level precision, an attacker can prevent damage to the sample and achieve access to critical signal wires. These signal wires can be carrying sensitive information, thereby presenting a vulnerability.

Various countermeasures, such as an active shield, an analog shield, a private circuit, etc. have been proposed to protect security-critical circuits against probing attacks. The active shield is the most common method; it detects milling by placing a dynamic signal-carrying wire mesh as a protective shield on the top-most metal layer.[12] To detect the attack, a digital pattern is transferred through the shield wires, and the received signals are compared with the same pattern from the lower metal layer. If a mismatch is detected, an alarm will be triggered, which results in a security action, such as the destruction of sensitive information. Florida Institute for Cybersecurity recently introduced a new holistic method[13] that is implementable into a traditional application-specific IC design flow, providing protection from FIB-based probing for security-critical circuits and nets. In the PHIKS course, we familiarize students with the most recent techniques for probing attacks and countermeasures.

Anti-RE Countermeasures

RE is used as a validation technique by manufacturers to detect faults, but it is can also be used with malicious intentions to duplicate or tamper with a design. Therefore, anti-RE mechanisms have been developed to provide the capability to detect and counteract attacks, such as RE.

PCB Anti-RE. In our prior research,[14] we introduced a new methodology to protect PCBs against nondestructive attempts for RE.[14] It aims at protecting PCBs against RE for malicious purposes—in particular, cloning and tampering. Our methods are based on the incorporation

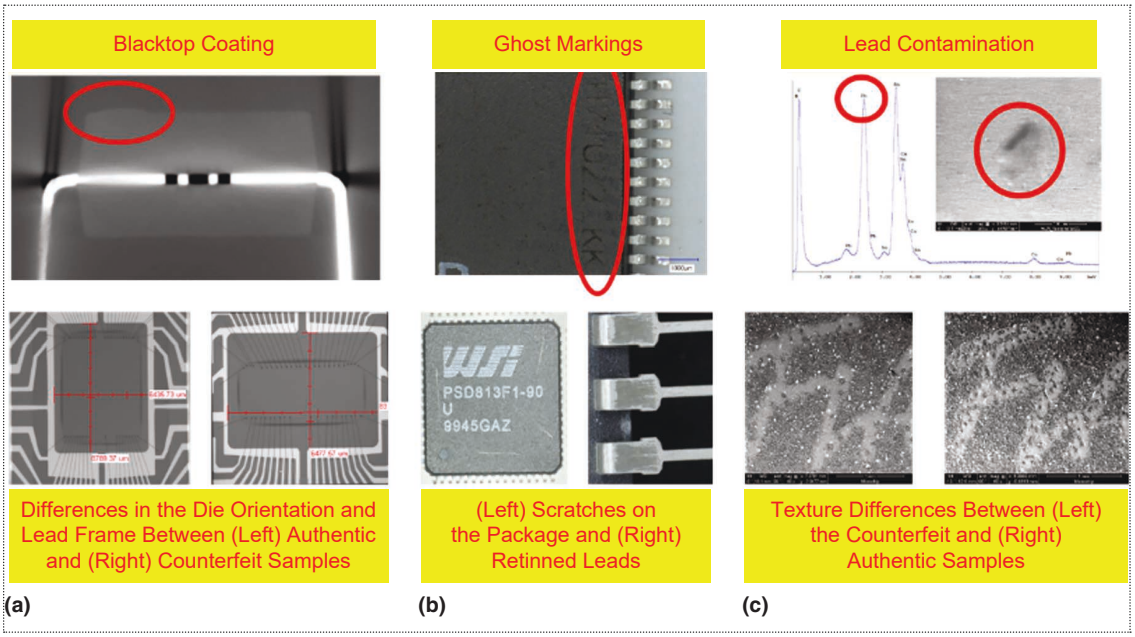


Figure 2. Sample images of defects found by (a) X-ray CT, (b) optical microscopy, and (c) SEM and elemental dispersive spectroscopy.

of high-Z material inside PCB layers that can create strong noise and artifacts in the reconstructed images in a destructive way, where the features can no longer be extracted after reconstructing the 3D image. Students in the PHIKS course have access to X-ray inspection tools in the lab, where they can view volumetric data from PCBs to analyze the impact on image processing techniques due to high-Z materials. In addition, the location of the high-Z material in PCB layers is also an important factor and should be optimized to achieve high enough noise and prevent RE without incurring unacceptable cost.

IC Anti-RE. To protect the design details in ICs, there are two different ways developed by instructors and taught within our PHIKS course. One method is to make device structures difficult to correctly image by microscopes. However, this is very difficult as RE techniques become more advanced. Another method is IC "camouflaging," which has been applied commercially and investigated by academic researchers to protect IP from attackers in the field. The main idea behind camouflaging is to remove recognizable patterns or distinguishable features from an IC, thereby making it more difficult to reverse engineer it with pattern recognition software. The most popular implementations of camouflaging occur at the gate level, where a camouflaged gate is one whose gate type cannot be determined by RE. That is, from the standpoint of an attacker who carries out RE, the gate may be any one of the possible gate types. When inputs are applied, however, a camouflaged gate still performs the function as intended by the designer.[15] It is important for IC designers to incorporate countermeasures and understand the impacts, such as the time, cost, and footprint or size, required to incorporate extra countermeasures. During the PHIKS course, students learn the two popular approaches for accomplishing this:

- Mix real contacts with dummy contacts within a standard cell. This approach relies on the attacker's inability to partially etch, which is the removal of material, and gain access to the contacts.
- Apply different doping steps or adjust the composition of dopants or atoms within the silicon to produce visually identical gates.

Experiences

The semiconductor cybersecurity workforce requires hands-on experience with design, manufacturing, and testing to be effective within the industry. While design and manufacturing have been researched extensively, testing and detection using industry inspection equipment have been less available for academia. A course such as PHIKS, which offers this rare hands-on access to inspection equipment through practical assignments, such as microscope data collection and counterfeit detection using image processing, meets the need for the workforce requirements. The course has been taught annually since the fall semester of 2018, with a class size of 15–20 undergraduate and graduate students per semester, totaling more than 100 students completing the curriculum. Students who have taken the course have gone on to graduate research studies and industry positions within the hardware security community.

Our PHIKS course has had a significant impact on cybersecurity workforce education through course slides, student data collection, and experimental modules dedicated to the topic of physical inspection and attacks and the countermeasures for that topic. The course material will hugely benefit the security, FA, and testing communities, as there is no comprehensive resource available with a focus on this topic. There is great interest from the hardware supply chain industry in learning more about this course and the material. For this reason, the PHIKS course material is available to all universities and community colleges nationwide through Trust-Hub[16] and our online database for counterfeit ICs, which are both developed by previous National Science Foundation support to faculty members to disseminate their courses and research artifacts. Additionally, to increase access to the course with UF students, we plan on expanding PHIKS to online students via the UF Electronic Delivery of Graduate Engineering program.

This article on the PHIKS course has highlighted the course material, its impact on the semiconductor industry's cybersecurity workforce development, and some of the research challenges for the community. As the cybersecurity workforce keeps expanding to meet the growing demand for designing, manufacturing, and inspecting semiconductors, there is a constant need to identify the challenges to the workforce through potential supply chain attacks. The development of a hardware-based curriculum focused on supply chain attacks will enable engineering students to begin to enter the workforce ready to make an impact. For advanced attacks on targets ranging from consumer electronics to military hardware, it is critical to have a course where students or current electronics workforce employees can learn the state of the art as well as research new attacks and countermeasures for hardware security. ■

References

1. F. Stellari, P. Song, M. Villalobos, and J. Sylvestri, "Revealing SRAM memory content using spontaneous photon emission," in *Proc. IEEE 34th VLSI Test Symp. (VTS)*, 2016, pp. 1–6, doi: 10.1109/VTS.2016.7477272.
2. M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*. New York, NY, USA: Springer Science & Business Media, 2011.
3. U. Guin, D. Forte, and M. Tehranipoor, "Anti-counterfeit techniques: From design to resign," in *Proc. 14th Int. Workshop Microprocessor Test Verification*, 2013, pp. 89–94, doi: 10.1109/MTV.2013.28.
4. N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, and D. Forte, "Non-destructive PCB reverse engineering using x-ray micro computed tomography," in *Proc. 41st Int. Symp. Testing Failure Anal.*, Nov. 2015, pp. 1–5, doi: 10.31399/asm.cp.istfa2015p0164.
5. D. Mehta et al., 2022, "Fics pcb x-ray: A dataset for automated printed circuit board inter-layers inspection," Cryptology ePrint Archive, https://eprint.iacr.org/2022/924
6. S. E. Quadir et al., "A survey on chip to system reverse engineering," *J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 1–34, Jan. 2017, doi: 10.1145/2755563.
7. M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan./Feb. 2010, doi: 10.1109/MDT.2010.7.
8. D. Mehta et al., "The big hack explained: Detection and prevention of PCB supply chain implants," *J. Emerg. Technol. Comput. Syst.*, vol. 16, no. 4, pp. 1–25, Aug. 2020, doi: 10.1145/3401980.
9. U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *J. Electron. Testing*, vol. 30, no. 1, pp. 9–23, Feb. 2014, doi: 10.1007/s10836-013-5430-8.
10. F. Courbon, S. Skorobogatov, and C. Woods, "Reverse engineering flash EEPROM memories using scanning electron microscopy," in *Smart Card Research and Advanced Applications*, K. Lemke-Rust and M. Tunstall, Eds. Cham, Switzerland: Springer International Publishing, 2017, pp. 57–72.
11. H. Lu, D. Mehta, O. Paradis, N. Asadizanjani, M. Tehranipoor, and D. L. Woodard, 2020, "FICS-PCB: A multi-modal image dataset for automated printed circuit board visual inspection," Cryptology ePrint Archive, https://eprint.iacr.org/2020/366
12. J.-M. Cioranesco et al., "Cryptographically secure shields," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, 2014, pp. 25–31, doi: 10.1109/HST.2014.6855563.
13. H. Wang, Q. Shi, A. Nahiyan, D. Forte, and M. M. Tehranipoor, "A physical design flow against front-side probing attacks by internal shielding," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2152–2165, Oct. 2020, doi: 10.1109/TCAD.2019.2952133.
14. N. Asadizanjani, "A new methodology to protect PCBS from non-destructive reverse engineering," in *Proc. Int. Symp. Test. Failure Anal.*, 2016, pp. 347–356.
15. M. E. Massad, S. Garg, and M. V. Tripunitara, "Integrated circuit (IC) decamouflaging: Reverse engineering camouflaged ICS within minutes," in *Proc. NDSS Symp.*, 2015. [Online]. Available: https://www.ndss-symposium.org/ndss2015/ndss-2015-programme/integrated-circuit-ic-decamouflaging-reverse-engineering-camouflaged-ics-within-minutes/
16. "FICS." TrustHub. Accessed: Nov. 25, 2022. [Online]. Available: https://trust-hub.org/

John True is a Ph.D. student in the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL 32611 USA. His research interests include X-ray CT reconstruction methods for reverse engineering semiconductors along with developing automated verification techniques of device designs. True received a B.S. degree in materials science and engineering from the University of Florida. He holds a certificate for semiconductor materials and has experience as a process engineer at Axcelis Technologies. Contact him at jtrue15@ufl.edu.

Navid Asadizanjani is an assistant professor in the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL 32611 USA. His research interests include novel techniques for integrated circuit counterfeit detection and prevention, system- and chip-level decomposition and security assessment, anti-reverse engineering, 3D imaging, invasive and semi-invasive physical assurance, and supply chain security. Asadizanjani received a Ph.D. in mechanical engineering from the University of Connecticut. He has received the National Science Foundation CAREER award; several best paper awards from the IEEE International Symposium on Hardware-Oriented Security and Trust and the American Society of Mechanical Engineers International Symposium on Flexible Automation; and the D.E. Crow Innovation award from the University of Connecticut. He is the cofounder and program chair of the IEEE Physical Assurance and Inspection of Electronics Conference. Contact him at nasadi@ufl.edu.