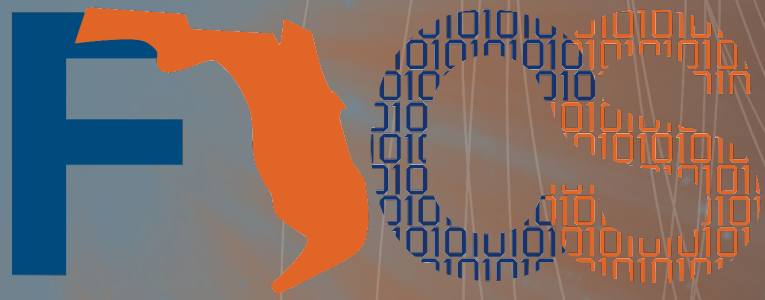


Research

The Florida Institute for Cybersecurity Research

PHYSICAL ASSURANCE AND INSPECTION OF ELECTRONICS

Physical Inspection and Assurance Tools for Electronics by FICS Research

Physical inspection of electronics has grown significantly over the past decade and is becoming a major focus for the chip designers, original equipment manufacturers, and system developers. The complex long life of the electronic devices coupled with their diverse applications are making them increasingly vulnerable to various forms of threats and inspection. Large industry and government efforts have been put in place across the globe to address related supply chain security problems to offer solutions, training and services. The number of programs introduced by US government have increased over the years to analyze and develop relevant solutions. Although much focus is given to digital domain, physical assurance and inspection of electronics as well as physical fingerprinting based on analog parameters are rapidly providing opportunities for unique countermeasures.

In spite of the significant attention research and development (R&D) resources invested in physical inspection and assurance research, there is much still required to provide comprehensive solutions for not just existing but emerging challenges and new-found vulnerabilities. Most importantly, we still lack tools and methodologies to support engineers and practitioners in the field to validate and verify the security and trustworthiness of the IPs, ICs, PCB, systems, and system of systems. We need a clear direction as to what the grand challenges facing the hardware security community are, especially with the current progress and emerging threats. The responses to the security threats remain reactive, rather than focusing on proactive or preventative solutions, and more robust technology.

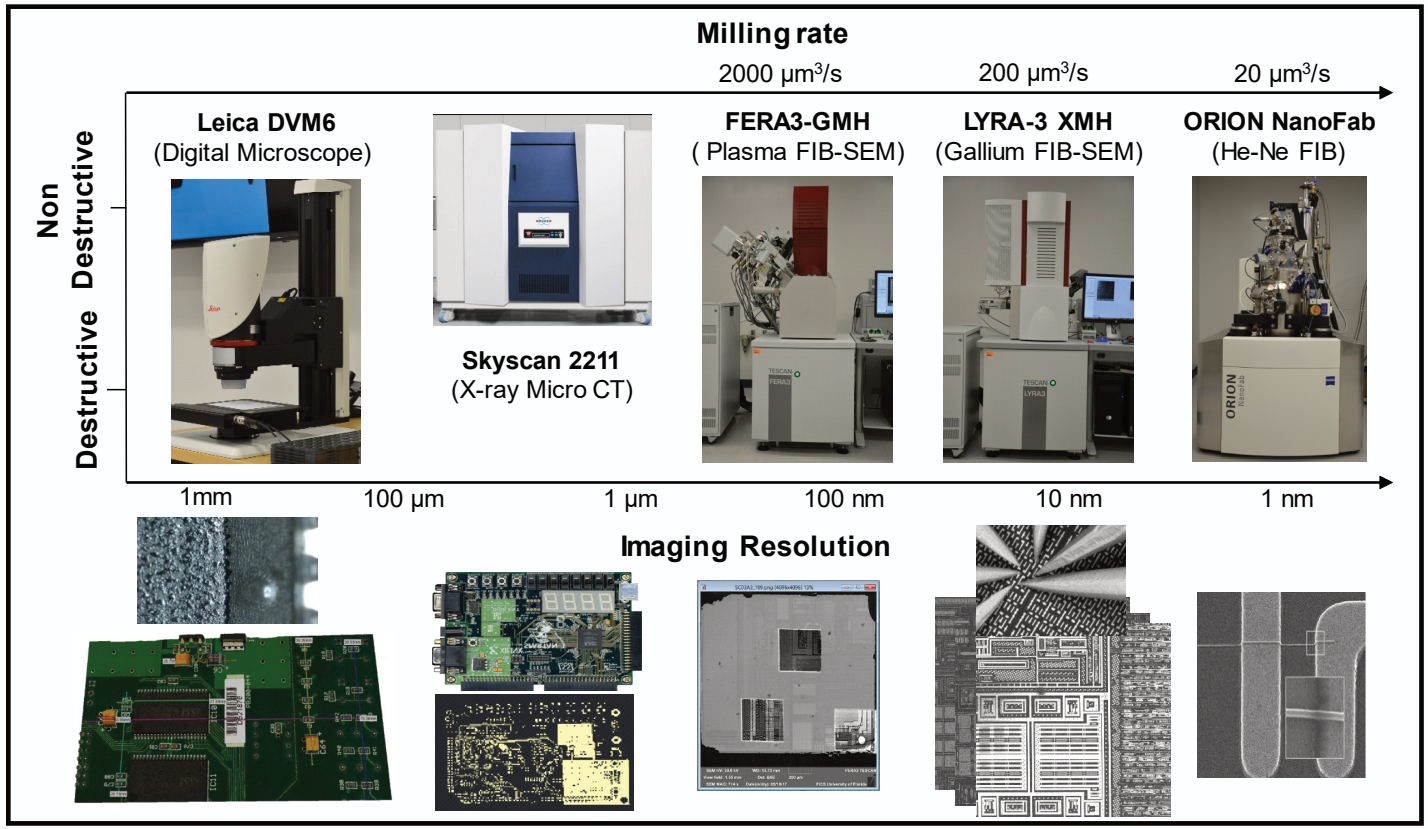
FICS Research Institute has been leading the charge in developing innovative tools and methodologies that bring together expertise in imaging, image analysis, inspection, assurance, machine learning, AI, and more, to build the most comprehensive set of automated tools to be used for ensuring security. This document provides a sample of tools developed by FICS researchers over the past several years.

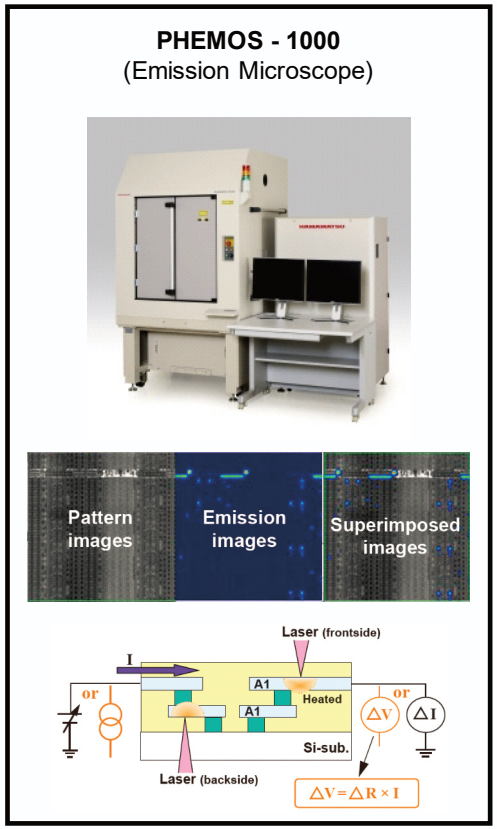
Please do not hesitate to contact us if you have any questions or are interested in learning more about each of the tools listed in this document.

Sincerely

Mark M. Tehranipoor, PhD
Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity
Director, Florida Institute for Cybersecurity (FICS) Research
Co-director, AFOSR/AFRL Center of Excellence, CYAN
Co-director, MEST Center
Phone: 352-392-2585
FICS Research: http://fics-institute.org/
MEST Center: https://mestcenter.org
Personal Page: http://tehranipoor.ece.ufl.edu/index.html

Selected SCAN Lab Facilities

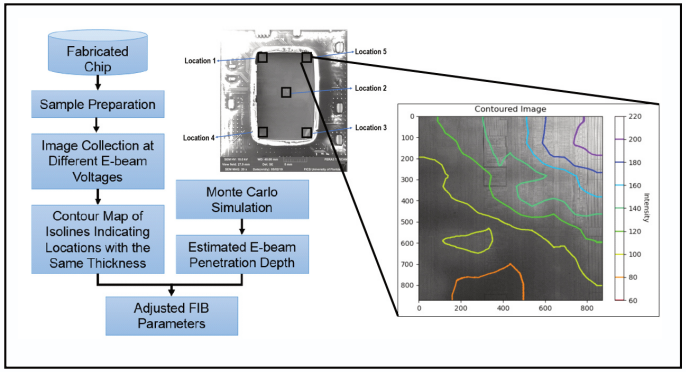


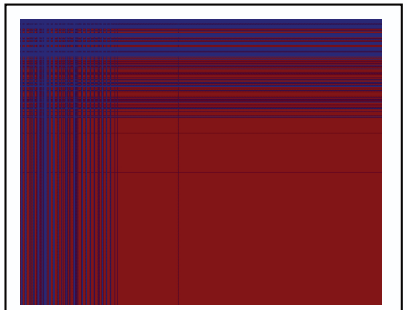


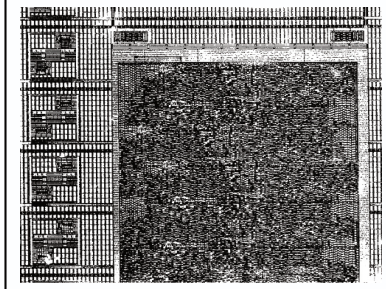
I. IC Assurance
   a. IC Backside Attack and Protection
      P1. SPARTA: Laser Probing Approach for Trojan Detection
      P2. Defense-in-depth: A Recipe for Protecting Logic Obfuscated Circuit
      P3. Protecting Microelectronics against Backside Attacks
      P4. Circuit-based Solution against Backside Attacks
   b. IC Reverse Engineering and Trojan Detection
      P5. Thickness measurement using the SEM Imaging
      P6. He-ion voltage imaging for Trojan Detection
      P7. Histogram-based Auto Segmentation (HAS) Algorithm for Reverse Engineering of Integrated Circuits
      P8. AutoMag: An unsupervised approach for estimating spatial magnification settings in Scanning Electron Microscopy for Reverse Engineering of Integrated Circuits
      P9. Unsupervised Automated Extraction of Standard Cell Library for Reverse Engineering of Integrated Circuits
      P10. Covert Gates: Protecting Integrated Circuits from Reverse Engineering with Undetectable Camouflaging
      P11. EMFORCED: EM-based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification
      P12. Trojan Scanner
      P13. Auto Delayering and SEM Imaging

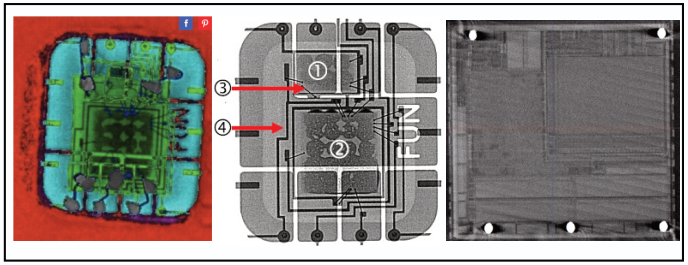
II. PCB ASSURANCE
      P14. AutoBoM: Statistical Image Analysis of PCB Components
      P15. AutoBoM: Superpixel Contour Refinement of PCB Component Estimates
      P16. 3D Stereo Photogrammetry for PCB Assurance
      P17. Annotator
      P18 Shadow-Based PCB Component Validation
      P19. PCB 3D Tomography
      P20. Auto3D
      P21. Automated Alignment and Sample Registration
      P22. Unsupervised and Semi-Supervised X-Ray CT Slice – to – Layer Identification.
      P23. Fully Automated Via Detection

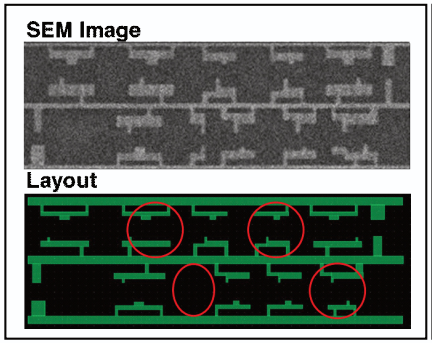
IC Assurance

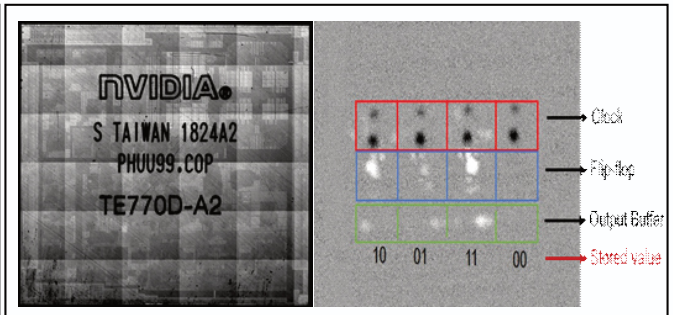


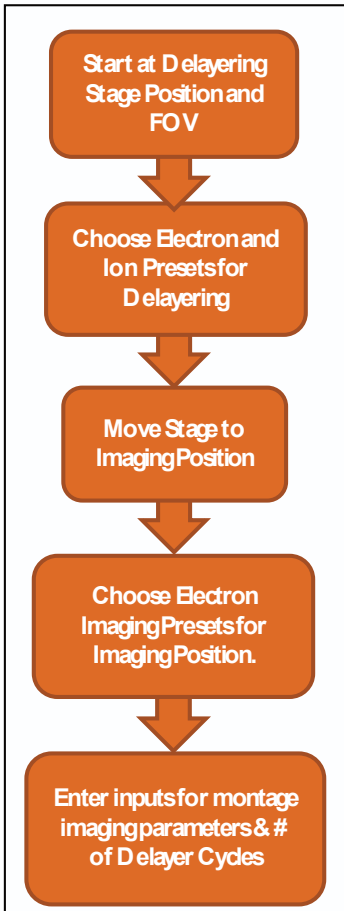


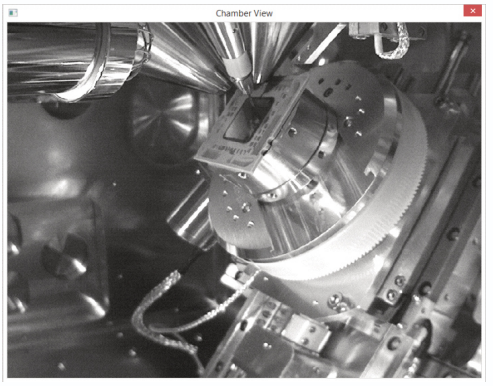


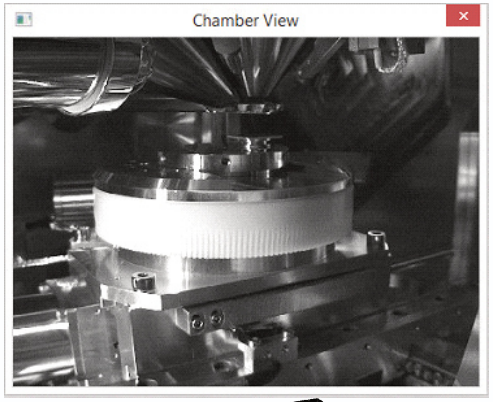


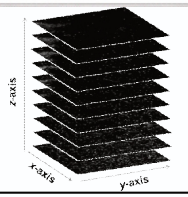












IC ASSURANCE

IC Backside Attack and Protection

P1. SPARTA: Laser Probing Approach for Trojan Detection

Integrated circuits fabricated at untrusted foundries are vulnerable to hardware Trojan insertion. Checking for the existence of Trojans usually requires a complex test process and design-level modifications. This results in low detection confidence and a significant increase in verification effort, making them inapplicable to complex circuits due to aggressive time-to-market constraints. On the other hand, for a high confidence detection of Trojans, an exhaustive inspection may be required using destructive reverse-engineering techniques. However, such methods are quite expensive, not applicable to all chips due to their destructive nature, and are very time-consuming. SPARTA, a non-destructive laser probing approach for Trojan detection, detects sequential hardware Trojans by comparing clock activity within the IC with the original clock tree created in the design phase. SPARTA does not need any golden samples, but rather the golden design. SPARTA is based upon creating a 2-dimensional frequency map of the backside silicon using electro-optical frequency mapping (EOFM), which extracts activity from clocked elements in the IC. The measurements are then compared with the expected sequential activity based on the clock tree identified in the IC design phase, and the differences in measured activity indicate circuit modifications and the presence of sequential hardware Trojans. SPARTA confidently identifies all additions, subtractions, or modifications to sequential elements with sub-micron spatial resolution and has been demonstrated on a 28nm device.

P2. Defense-in-depth: A Recipe for Protecting Logic Obfuscated Circuit

Logic locking has been proposed as an obfuscation technique to protect outsourced IC designs from IP piracy by untrusted entities in the design and fabrication process. In this case, the netlist is locked by adding extra key-gates, and will be unlocked only if a correct key is applied to the key-gates. Combinational locking and finite-state machine (FMS) based locking approached have been proposed for logic locking. In both locking approaches, the key is assumed to be written into a nonvolatile memory after the fabrication by the IP owner and only known to the IP owner. Therefore, the logic locking is considered as a broken scheme once the key value is exposed. In this project we analyze the vulnerability of the obfuscation techniques against different class of attacks, e.g., Oracle-guided, Oracleless and physical attacks. Leveraging the understanding about the susceptibility of logic obfuscation, we are investigating a multi-layer based defense mechanism. The multi-layer defense strategy, termed as defense-in-depth approach, implements several independent countermeasures in the device to provide aggregated protection against different attack vectors.

P3. Protecting Microelectronics against Backside Attacks

Modern computing systems are built around hardware roots of trust that safeguard cryptographic keys, enable secure boot, etc. However, physical security of the microelectronic system is still an open issue. Physical inspection techniques, developed for chip debugging and failure analysis (FA), can be used by an adversary for extracting the assets protected by the device. For example, In semi-invasive attacks, an adversary exploits the transparency of silicon backside for near-infrared light to stimulate the transistors in the device or detect light emitted from an IC. Therefore, a potential antagonist in the supply chain can use photonic emission analysis, and electro-optical frequency mapping (EOFM) for localizing CPU cores, cryptomodule, memory blocks or registers and initiate the extraction of chip assets through optical probing or laser fault injection. In this project we are investigating to develop metrics that that quantify the vulnerability of IC from backside to different class of probing and optical attacks. We are investigating circuit, device and material based solutions to detect or prevent optical and probing based attacks from chip backsides.

P4. Circuit-based Solution against Backside Attacks

A System-on-chip accommodates different security sensitive modules and information, collectively known as assets. Protecting the assets from a malicious entity is the key objective of the security architecture of the SoC. On the other hand, optical debugging and diagnosis based physical inspection methods are widely used for defect and failure localization in silicon implementation. Transparency of silicon to near-infrared (NIR) light is used for optical debugging methods, e.g., photon emission analysis, laser-voltage probing/imaging, laser stimulation. The semi-/non-invasive optical approaches allow runtime monitoring of the transistor through silicon substrate, i.e., chip backside. Besides, to facilitate the failure analysis, no protection scheme is implemented at the SoC backside. Therefore, an attacker can effortlessly track and extract the chip asset by optically attacking the security-sensitive modules. Therefore, we are investigating circuit-based solutions to protect the chip backside. Two approaches are adopted for developing the circuit-based protections against optical attacks; (a) developing sensors to detect optical attack attempts and (b) CMOS compatible preventive approaches. Our current work in this domain revolves around (i) developing vulnerability metric against backside attacks; (ii) developing CAD model to evaluate the sensor and device performance under optical analysis; (iiI) evaluating the proposed solutions based on vulnerability metrics. developing attacks. In this project, we shall leverage the laser scanning microscope (LSM), like PHEMOS-1000, capability available in UF/FICS Research's state-of-the-art SeCurity and AssuraNce (SCAN) lab facility.

IC Reverse Engineering and Trojan Detection

P5. Thickness measurement using the SEM Imaging

Hardware assurance of electronics is a challenging task and is of great interest to the government and the electronics industry. Physical inspection-based methods such as reverse engineering (RE) and Trojan scanning (TS) play an important role in hardware assurance. Therefore, there is a growing demand for automation in RE and TS. In practice, uniform delayering can be challenging if the thickness of the initial layer of material is non-uniform. Therefore, it is critical to evaluate the thickness of the layers to be removed in a real-time fashion. Our proposed method uses electron beam voltage imaging, image processing, and Monte Carlo simulation to measure the thickness of remaining silicon to guide a uniform delayering process. SEM images at different accelerating voltages are used to create the contour maps using image processing as different voltage beam energy has different penetration depths. Once the contour map is created, Monte Carlo simulation was performed at different accelerating voltages which showed the direct correlation between accelerating voltage and interaction volume. This information was used to estimate the approximate thickness of leftover silicon over the sample surface. The predicted thickness map will then be used as online feedback to adjust FIB parameters for automated, uniform delayering for physical assurance and inspection of electronics.

P6. He-ion voltage imaging for Trojan Detection

Due to the complexity of modern IC chips and the stealthy nature of HTs, the former HT detection techniques available in the market and studied by researchers usually lack the coverage, speed and/or confidence of detection. The imaging-based solution developed recently (Trojan Scanner), supported by modern microscopies and AI-enhanced image analysis, is practically capable of detecting all the stealthy HTs. Firstly, SEM images were employed to record the sample surface information during the imaging which includes silicon with different dopants and doping concentration along with the micro filler cells. As the filler cells and the heavily doped silicon regions present close characters and thus difficult to differentiate them from each other in SEM Imaging. We proposed a method of using He-Ion imaging as the filler cells and the lightly doped silicon are not grounded. The positive charges from the ion beam accumulate on the surface, build up positive surface potential and trap the electrons. Therefore, the secondary electron emission is prohibited on these regions, which makes these regions appear dark. Therefore, the He-Ion imaging can effectively be used in determining any trojan present in the filler cells as they will show up in He-imaging. It will also efficiently prohibit the appearance of passive regions in the obtained images for the Trojan Scanner model, enabling accurate detection and reducing the time in image analysis.

P7. Histogram-based Auto Segmentation (HAS) Algorithm for Reverse Engineering of Integrated Circuits

The increasing complexity of advanced integrated circuit (IC) chips has rendered optical imaging obsolete for efficient reverse engineering. Computer vision algorithms now expedite reverse engineering of present-day integrated chips by processing higher-resolution Scanning Electron Microscopy (SEM) images of the densely packed chips in order to automate structural component segmentation. However, available segmentation algorithms only work on higher-quality SEM images, which take a very long time to acquire and require human interaction to optimize image parameters. This image-processing algorithm, called Histogram-based Auto Segmentation (HAS), segments the structural elements of integrated circuits in SEM images to enable reverse engineering and failure analysis. The algorithm processes the low magnification and/or poor quality SEM image through a series of stages in which it extracts the histogram of the image, corrects it, and segments the histogram based on its number of peaks. The algorithm does not try to model noise sources, and does not require parameter fine-tuning. The segmentation algorithm simply relies on the working principles of scanning electron microscopy imaging to produce high-contrast between different materials in the integrated circuit image. This greatly simplifies the traditionally lengthy and expensive integrated circuit reverse engineering workflow.

P8. AutoMag: An unsupervised approach for estimating spatial magnification settings in Scanning Electron Microscopy for Reverse Engineering of Integrated Circuits

Imaging is an integral part of reverse engineering of integrated circuits. Modalities such as Scanning Electron Microscope require fine tuning of various parameters to acquire reliable images. Such fine tuning is a laborious task especially in case of full-scale reverse engineering and typically results in severe time delays in image acquisition if not done correctly. This algorithm assists in the fine tuning of one such parameter, the magnification. It goes through a fast-acquired image and assigns varying degrees of magnification to it. This map (as shown in figure above) can be used to change magnification settings with respect to the content in the image and automate the entire image acquisition workflow.

P9. Unsupervised Automated Extraction of Standard Cell Library for Reverse Engineering of Integrated Circuits

The availability of standard cell libraries is taken for granted in the reverse engineering workflow. Being confidential information, the library might not be available for typical off the shelf components. However, the library is essential in converting the acquired images of integrated circuits into useful and understandable logic circuits. This algorithm assists in the automated extraction of the standard cell library from just the images of the contact layer of the integrated circuit. The extracted logic cells can be presented to a Subject Matter Expert for decoding and identification.


BRUKER

P10. Covert Gates: Protecting Integrated Circuits from Reverse Engineering with Undetectable CamouflagingP11. EMFORCED: EM-based

Existing methods of camouflaging are based on logic gates that assume one of many Boolean functions, either through variation of threshold voltage or contact configurations. Unfortunately, such methods lead to high overheads, and are vulnerable to invasive as well as non-invasive functional attacks. We have developed a new camouflaging strategy, termed as 'covert gate', that leverages doping and dummy contacts to create camouflaged gates that are indistinguishable from regular gates under modern imaging techniques. The technique allows a designer to introduce arbitrary dummy inputs to logic gates, so that the netlist retrieved by the attacker during reverse engineering is functionally incorrect. Since covert gates are indistinguishable from regular gates, attack complexity is significantly increased and with very low overheads. In preliminary work, we have fabricated and imaged test structures to show the indistinguishability of the channel and contact regions that are modified to create covert gates. Our empirical results show that covert gate indistinguishability can make SAT attacks exponentially more complex and prevent gate identification by ATPG-based attacks even under pessimistic assumptions. We have also developed models to characterize gate-level overheads, and netlist modification tools for camouflaging designs. In the future, we plan to fabricate prototype devices to validate our models, estimated overheads, and indistinguishability of gates in silicon. We also plan to improve our covert gate insertion methods to meet different objectives (minimize area, performance, or power overheads, maximize security, etc.).

P11. Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification

Electronics supply chain vulnerabilities have broadened in scope over the past two decades. With nearly all IC design companies relinquishing their fabrication, packaging, and test facilities, they are forced to rely upon companies from around the world to produce their ICs. This dependence leaves the electronics supply chain open to counterfeiting activities. EMFORCED, an electromagnetics-based fingerprinting framework, is designed to detect remarked and cloned counterfeit ICs. Benefiting from naturally occurring electromagnetic second order effects to identify the IC design layout without decapsulating the chip under test. Enabling only the clock, power, and ground pins allows us to generate a design-specific fingerprint which is dependent upon the physical parameters of the chip under test. Leveraging the emissions from the clock distribution network creates a holistic, design-level, fingerprint including both temporal and spatial information. Statistical analysis and machine learning techniques are used to demonstrate reference-free and reference-inclusive classification methods based on EMFORCED measurements, providing various scenarios for this low-cost, fast, and zero design overhead solution.

P12. Trojan Scanner

Hardware Trojans are malicious changes to the design of integrated circuits (ICs) at any stage of the IC design cycle. Different approaches have been developed to detect Trojans namely non-destructive (electrical tests like run-time monitoring, functional and structural tests) and destructive (full chip reverse engineering). However, these methods cannot detect all types of Trojans and they suffer from a number of disadvantages such as slow speed of detection and lack of confidence in detecting all types of Trojans. Majority of hardware Trojans implemented in an IC will leave a footprint at the doping (active) layer. In this research project, we are developing a physical inspection based Trojan detection framework called “Trojan Scanner” for the untrusted foundry threat model, where a trusted GDSII layout (golden layout) is available. Advanced image analysis vision algorithms in combination with the supervised machine-learning model are used to classify different features of the golden layout and SEM images from an IC under authentication. Our results demonstrate that Trojan Scanner is more reliable than electrical testing and faster than full chip reverse engineering. Trojan Scanner does not rely on the functionality of the circuit rather focuses on the real physical structure to detect malicious changes done by the untrusted foundry.

P13. Auto Delayering and SEM Imaging

Plasma FIB (Focussed Ion Beam) delayering followed by SEM (Scanning Electron Microscopy) imaging is an important step for physical inpsection and assurance of integrated circuits. This step requires a considerable time and a need of skilled SEM engineer to finish deprocessing and imaging of integrated circuits. In this project we are automating the deprocessing and imaging of semicondcutor device layers for hardware trojan detection and anti reverse engineering purposes. We are developing a python based scripting to automate the FIB-SEM delayering-imaging process and a combined with a feedback based image analysis engine. The feedback engine automatically directs the SEM to take images at optimum parameters (dwelling time, magnification and resolution etc.) to speed up the hardware assurance with high confidence level. This technique will improve accuracy of detection and save human hours spent on FIB plasma delayering and SEM imaging.

PCB ASSURANCE

P14. AutoBoM: Statistical Image Analysis of PCB Components

The goal of AutoBoM is to automatically extract a Bill of Materials (BoM), the list of all components on a PCB, given an image of the board. The extracted BoM can then be used for reverse engineering and hardware assurance purposes. “Statistical Image Analysis of PCB Components” is a subproject of AutoBoM. This subproject involves taking images of various PCBs under different imaging conditions (e.g. lighting, camera type, and camera position) and manually annotating each. Then, component features (shape, color, and texture) are extracted and analyzed. Here, the purpose is twofold. First, to gain insight on the image representations of common PCB components. This will inform later AutoBoM methodologies (e.g. component detection, classification, and identification). Second, to evaluate the effects of different imaging conditions. This will lay the groundwork necessary for a more robust design.

P15. AutoBoM: Superpixel Contour Refinement of PCB Component Estimates

The goal of AutoBoM is to automatically extract a Bill of Materials (BoM), the list of all components on a PCB, given an image of the board. The extracted BoM can then be used for reverse engineering and hardware assurance purposes. “Superpixel Contour Refinement of PCB Component Estimates” is a subproject of AutoBoM. This subproject involves pixel-level contour refinement, given a rough, initial component estimate. The goal is to extract more informative shape and texture information to improve later AutoBoM methodologies (e.g. component detection, classification, and identification).

P16. 3D Stereo Photogrammetry for PCB Assurance

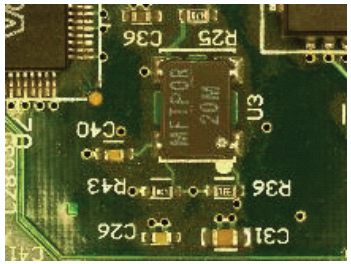
PCB Assurance and Authentication requires thorough analysis of microelectronic components for malicious tampering and modifications. The current method of using 2D Images is insufficient and misses essential information that 3D Imaging provides. Trojans have been known to be different in dimensions in addition to differences in look and texture , so metrology is essential in such a process. 3D Imaging can provide not just the same information as 2D, but also the surface height of components and also around 4x more surface data to compare with. Our goal is to use a Robotic arm with a mounted camera to image at various angles and distances to build a dense 3D model of the PCB. This model is analyzed in 3D space and processed to segment, identify and locate microelectronics components and produce a 3D CAD model. Later the implementation will be extended to handheld camera imaging that is robust to handheld capture noise. With primary focus on improving the Imaging speed to provide near realtime Vulnerability Assessment and Quality Assurance for PCBs, Photogrammetry is an approach to provide detailed surface analysis of PCBs with affordable means of imaging such as cameras, instead of restrictive and expensive approaches like Interferometry systems.

PCB Assurance

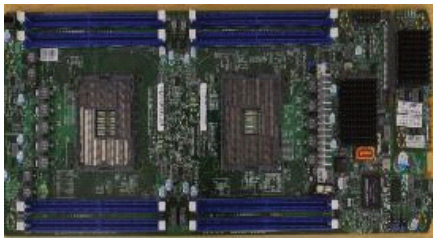
Surface Level Imaging

Reflective Surface Imaging

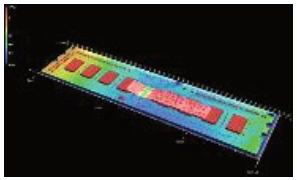
Digital Optical Microscope



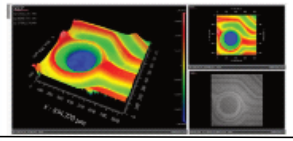
Cameras



Patterned Light

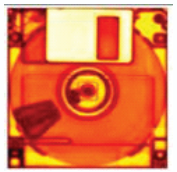


White Light / Laser Interferometry

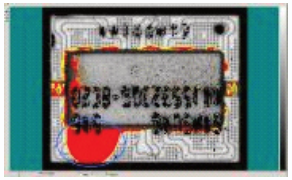


Penetrative Surface Imaging

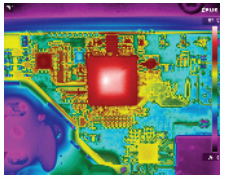
Terahertz Imaging



Scanning Acoustic Imaging

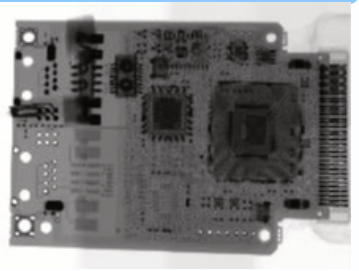


Thermal Imaging

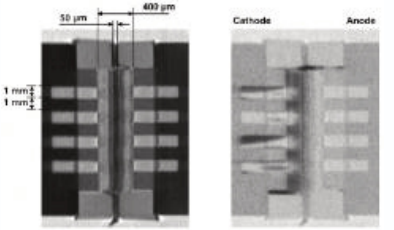


Volumetric Imaging

X ray Imaging



Neutron Imaging



P17. Annotator

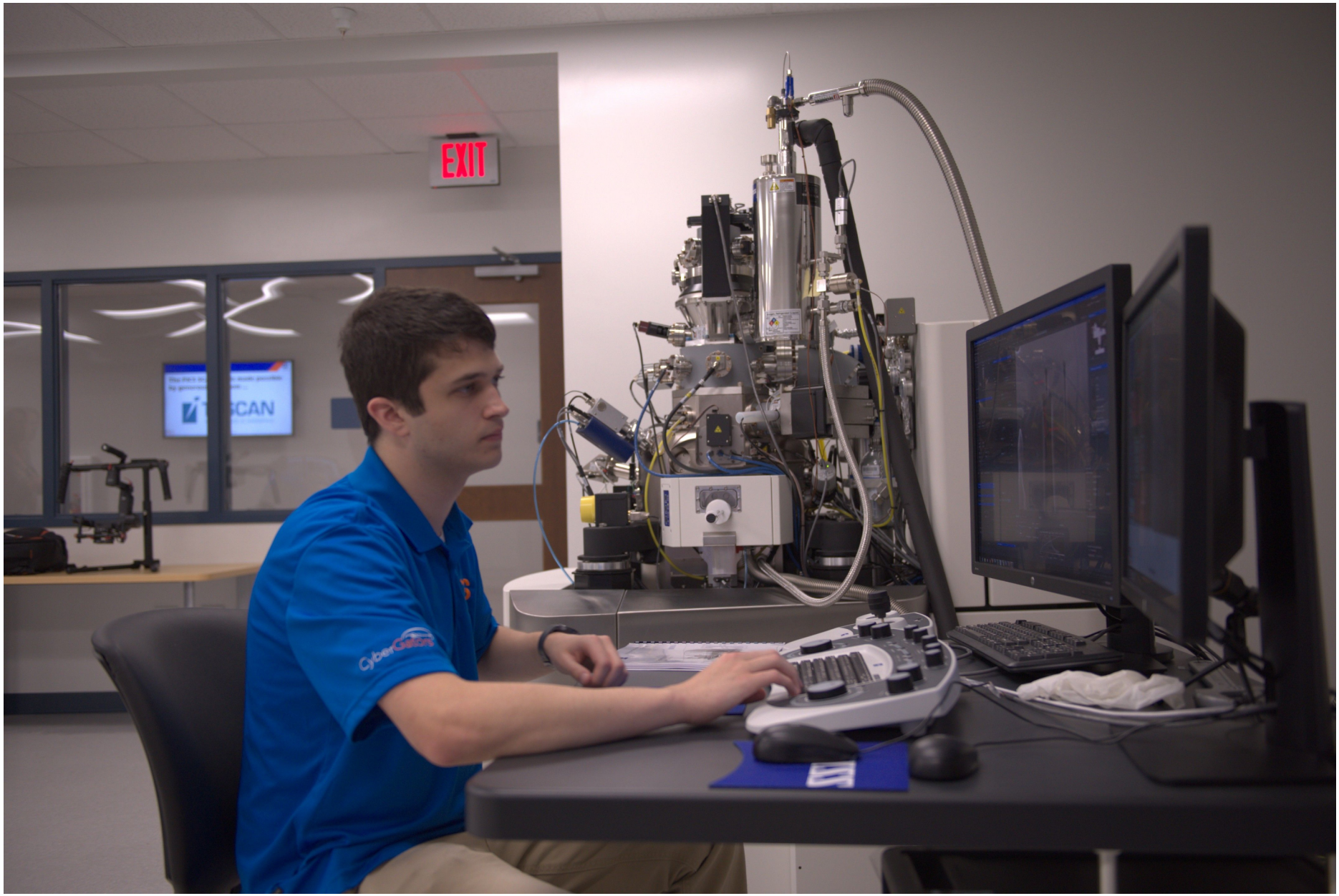
Machine learning solutions are often used to locate specific objects within an input image. This usually requires significant amounts of training data, which is typically generated in a lengthy manual process. Our goal in the automatic semantic annotator project is to reduce the manual labor burden of this task. Moreover, we aim to provide seamless integration between the annotation and detection processes by combining the front-end of both processes. This allows us to dynamically improve our detection process through real-time output correction and ground-truth feedback.

P18. Shadow-Based PCB Component Validation

A substantial portion of the AutoBoM project involves detecting surface-mount devices (SMDs) on the PCB in question. Currently, this entails making an initial estimate of where components might exist and progressively refining that estimation. Once the existence of a component is verified, that component is considered validated. One such method, shadow-based component validation, produces a 2D output after synthesizing images with various illumination angles. When a light source is placed on one side of the PCB, each component casts a shadow. However, board text, contact pads, and vias do not. By locating shadows and correlating them with an initial background subtraction process, we can effectively discriminate surface-mounted components from silkscreen or via elements.

P19. PCB 3D Tomography

In order to verify PCB design and final functionality, it is necessary to perform this in depth analysis via x-ray CT. X-Ray CT is a time consuming process that collects 2D images from various angles around a sample, and then a reconstruction of these images is transformed into a 3D image. The interpreted 3D image is heavily impacted by errors and noise in the 2D collected images.
The signal to noise ratio and the time required to process the data-set can be minimized by selecting collection parameters that provides adequate spatial resolution for advanced machine learning and processing techniques to be performed. By training a neural network on previously captured and processed x-ray data, this network's prior knowledge can be used to reconstruct a PCB's structural fidelity more rapidly and accurately than compared to traditional algorithms for reconstruction. This decreased post processing time, can lead to reduced collection times due to dynamically selecting collection parameters related to the PCB's atomic density, number of layers, minimum feature size, and component density. This will enable design verification specific to each PCB with a high level of confidence using the least amount of x-ray collection and processing time compared to current collection and reconstruction standards


EXIT

P20. Auto3D

IIn the modern globalized supply chain, reverse engineering (RE) is needed to validate the performance, quality, authenticity, and integrity of electronics, e.g., detection of counterfeits and hardware Trojans. In the case of legacy systems, RE can be an invaluable tool for recovering original design files in order to evaluate, reproduce, and/or redesign them. The goal of this project is to develop an entirely automated and non-destructive process for the reverse engineering of printed circuit boards (PCBs). X-Ray computed tomography is used to capture a 3- dimensional scan of the entire depopulated

P21 Automated Alignment and Sample Registration

Project Description: The initial step for Reverse Engineering of PCBs using X-ray CT is referred to as sample acquisition. This stage focuses on the actual imaging in the X-ray CT machine producing a 3-D point cloud of the sample followed by reconstruction to produce the respective 3-D volume representation of the PCB. During sample acquisition it is important to slightly misalign/angle a PCB sample in the X-Ray chamber in both the x and y direction to maximize the amount of information retrieved used to create the 3-D point cloud during the scan and resultant reconstruction. However, while this produces a 3-D reconstruction of the sample at a high quality it also creates challenges with post imaging analysis. Therefore, it is important to properly align and register these samples in order to facilitate later stages of analysis. Not to mention automate this stage of analysis to reduce the strain on resources such as time or reliance upon subject matter experts. This tool uses only the 3-D reconstruction data to accurately align and register the 3-D volume in order to facilitate high quality analysis and results in later stages of the Reverse Engineering process.

P22. Unsupervised and Semi-Supervised X-Ray CT Slice – to – Layer Identification

Project Description: Once a sample has been properly aligned and registered the data is ready for analysis to retrieve necessary design info for reproduction. One of the key pieces of information in the reproduction of a design is the number of layers and what the layout design at each layer is composed of. From the perspective of Reverse Engineering with X-ray CT what slices of the 3-D volume belong to what layers is necessary information for later stages of reverse engineering. Such as via or trace detection since these are key components of a design that can be unique to individual layers in a design. Furthermore, it is important to account for the amount of prior knowledge regarding a design one may be in possession of. For example, it is not unheard of for designs to be lost during company migrations or attrition but a reproduction of a device is necessary for obsolescence management. Or perhaps, one does possess prior design information in the form of a layout or manufacturing data. In either case it is important to be able to address this challenge regardless the amount of a priori knowledge. This tool is able to determine the number of layers and how many/what slices correspond to what layers in an unsupervised fashion(no reference information provided), as well as improve upon those results if the user has reference information available(in the form of a digital or X-ray CT image for each layer).

P23. Fully Automated Via Detection

Project Description: One of the key pieces of design information for a PCB design are typically its Vias (electrical conductivity interconnects between layers) and traces (electrical conductivity interconnects within layers). With the correspondence between slices of a 3-D X-ray CT imaged PCB and its layers known the next stage is to retrieve the vias and traces for each respective layer. A key challenge with this task is the variability across designs with regards to scale, noise, and complexity/density. It is important that the detection of the vias and traces be able to account for all these challenges and do so in a generalizable manner across a vast variety of designs. Therefore, this tool accurately detects and localizes vias and traces in a design in an automated and unsupervised fashion.

Navid Asadi
Phone: 352-294-1075
Email: nasadi@ece.ufl.edu
fics.institute.ufl.edu

Domenic Forte
Phone: 352-392-1525
Email: dforte@ece.ufl.edu
fics.institute.ufl.edu

Mark Tehranipoor
Phone: 352-392-2585
Email: tehranipoor@ece.ufl.edu
fics.institute.ufl.edu

Mailing Address: P.O. Box 116200, Gainesville Florida 32611-6200
Physical Address:601 Gale Lemerand Dr. 226 Materials Engineering (MAE) Gainesville FL 32611
http://fics-institute.org