Physical Inspection & Attack: New Frontier in Hardware Security

M Tanjidur Rahman[1], Qihang Shi, Shahin Tajik, Haoting Shen, Damon L. Woodard,
Mark Tehranipoor and Navid Asadizanjani

Abstract— **Due to globalization, the semiconductor industry is becoming more susceptible to trust and security issues. Hardware Trojans, i.e., malicious modification to integrated circuits (ICs), can violate the root of trust when the devices are fabricated in untrusted facilities. Literature shows as the microscopy and failure analysis tools excel in the resolution and capability, physical inspection methods like reverse engineering and photonic emission become attractive in helping verify such trust issues. On the contrary, such physical inspection methods are opening new capabilities for an adversary to extract sensitive information like secret keys, memory content or intellectual property (IP) from the chip compromising confidentiality and integrity. Different countermeasures have been proposed, however, there are still many unanswered questions. In this paper, we discuss physical inspection/attack methods using failure analysis tools and analyze the existing countermeasures and security/trust issues related to them. Next, we will introduce challenges related to the development of new countermeasures and trust verification. Finally, we present research roadmap for this emerging field.**

Index Terms— **Physical Inspection/attacks, Invasive attacks, Reverse Engineering, Probing, Optical Attacks.**

1. INTRODUCTION

Modern embedded devices and internet of things (IoT) have become an indispensable part of our life. Although benefits of such advancements are indisputable, the concern regarding security and trust is also on the rise. Outsourcing design and fabrication, invites vulnerability to malicious activities and alterations. Any malicious modification to the structure and function of a chip can be identified as hardware Trojan. More than a decade of research in this field has produced a number of approaches to detect Trojans [1], [2]. These inserted circuits or modifications cannot be easily detected because of stealthy nature of Trojans. Besides, these approaches require functionality analysis from a golden IC to define authenticity of ICs under authentication (IUA). Some prior work suggested inspection methodologies like reverse engineering and photonic emission analysis as an emerging solution to verify and assess the root of trust [3], [4]. Such methodologies can be identified as physical inspection where physical access to the chip/system is required.

The physical inspection methods such as reverse engineering, electrical and optical probing, photonic emission analysis, fault injection techniques and side-channel analysis are developed to support failure analysis (FA) of the chip at post-silicon stage. Besides, FA tools like chip polishing, microscopy, probing, focus ion Beam (FIB), X-ray imaging, laser voltage probing etc. have experienced significant advancement to facilitate these techniques. Demand for higher yield and faster failure analysis and fault localization at smaller technology nodes also catalyzed the progress and revolution in FA techniques and tools. However, an adversary can use such FA methods and tools to attack a chip and compromise security through exposing assets – sensitive information, intellectual property, firmware, cryptographic keys etc. [5]. Researchers showed that such physical inspection methods, when used for physical attacking of a chip, are capable of compromising the confidentiality and integrity provided by modern cryptography and security measures through observation of a chips silicon implementation [6]–[11]. So, a skilled attacker can analyze a single chip and use the extracted information to inject fault or denial of service (DoS) to a system remotely. So, a detailed understanding of different physical inspection/attack methods is required to use such methods as trust verification tools as well as protect assets inside the chip.

In recent years, there has been extensive analysis on different physical inspection/attack processes and countermeasures [5], [12]–[15]. To develop effective countermeasures and trust verification techniques a taxonomy (fig. 1) of physical inspection/attacks is presented based on sample preparation and nature of inspection/attack processes. Physical inspection/attacks can be performed in non-invasively, semi-invasively and invasively. In the past, when compared to non-invasive attacks, invasive and semi-invasive attacks were considered as a less concerned threat to security due to the requirement of equipment, expertise, and execution time. But in the recent years, even though new features are added, the FA equipment are becoming cheaper and easily accessible. Further, FIB and SEM imaging systems are accessible in many academic/industry labs and can be rented for only few hundreds of dollars per hour. Therefore, it is expected to see major growth in physical attacks in near future. Equally important, we also expect growth in physical inspection based techniques to provide effective means for security and trust verification.

In this paper, we perform a comprehensive study of the state of knowledge in the field of physical inspection/attacks research and the existing countermeasures. We present a number of challenges for developing trust verification techniques based on invasive and semi-invasive physical inspection methods. We discuss the shortcomings of recent

[1] Authors are with Florida Institute For Cybersecurity (FICS) Research, Electrical & Computer Engineering Department, University of Florida, Gainesville, FL, USA. Contact: mir.rahman@ufl.edu, {nasadi,tehranipoor}@ece.ufl.edu

countermeasures and present research directions to develop more effective approaches. The paper is organized as follows, in Section 2, we discuss different types of non-invasive attacks. Invasive and semi-invasive attacks are briefly analyzed in Sections 3 and 4. In Section 5, we present future research opportunities in computer vision and machine learning in the field of hardware security. Finally, we conclude the paper in Section 6.

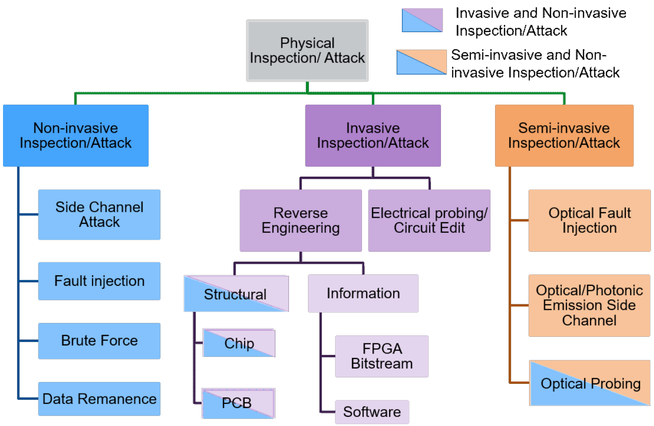

Invasive and Non-invasive Inspection/Attack
Semi-invasive and Non-invasive Inspection/Attack
Physical Inspection/ Attack
Non-invasive Inspection/Attack
Invasive Inspection/Attack
Semi-invasive Inspection/Attack
Side Channel Attack
Fault injection
Brute Force
Data Remanence
Reverse Engineering
Electrical probing/ Circuit Edit
Structural
Chip
PCB
Information
FPGA Bitstream
Software
Optical Fault Injection
Optical/Photonic Emission Side Channel
Optical Probing

Fig. 1: Taxonomy of physical inspection/attacks.

2. Non-Invasive Inspection/Attacks

A non-invasive attack attempts to extract assets without tampering with the packaging or structure of the chip/printed circuit board (PCB). Non-invasive attacks are executed both actively or passively. Example of active non-invasive attacks are fault-injection techniques, brute force, and data remanence. Passive attacks like side channel analysis have been studied extensively for exposing cryptographic keys or sensitive information. In addition, using side channel signal analysis using transient and quiescent power, delay, and electromagnetic (EM) have been widely proposed for trust verification against Trojans [1], [2]. In recent years, non-destructive reverse engineering and optical probing attacks have also been investigated extensively as both defensive and offensive mechanisms. Such attacks are discussed in later section.

3. Invasive Inspection/Attacks

Invasive attacks require access to internal components of a chip or PCB. Hence, depackaging and decapsulation are the two common initial steps taken to prepare the sample. However, the chip is destroyed after such type of attacks. Prevalent forms of invasive inspection/attacks are reverse engineering, electrical probing and circuit edit. For a successful invasive attack, a facility with IC soldering/desoldering station, polisher, simple chemical lab, X-ray, high-resolution optical microscope, FIB and scanning electron microscope (SEM) workstation, photonic emission microscope, microprobing station, logic analyzer, signal generator and laser cutting system may be required depending on the nature of the sought-after attack and inspection.

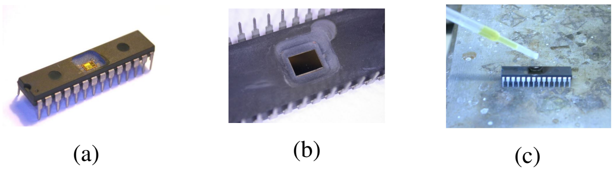

(a) (b) (c)

Fig. 2: (a) Chip decapsulated from frontside (b) Chip decapsulated from backside (c) Selective acid decapsulation of the chip [5].

2.1 Reverse Engineering

Reverse Engineering of an IC is the process of analyzing the internal structure, connection for extracting design, stored information and functionality of the chip. The subsystem level reverse engineering comprises hardware and firmware extraction (fig. 1).

2.1.1 Chip Reverse Engineering: IC reverse engineering comprises of 5 steps [16].

a) Decapsulation: Decapsulation exposes the internal die, lead frame and die connecting components - bond wire, ball grid arrays. Decapsulation can be completed from frontside (fig. 2a) or backside (fig. 2b). Mechanical polishing and computer numerical control (CNC) multi-tool milling are non-selective means of decapsulation. Wet chemical etching and plasma etching are two common selective approaches of decapsulation. Fig. 2c shows the selective decapsulation using acid etching.

b) Delayering: Delayering is the process of removing materials layer by layer for imaging and analysis. Delayering done with wet/dry plasma etching, FIB or polishing.

c) Imaging: After exposing a new layer, high-resolution images are collected, and stitched together for extracting netlist. Commonly, an optical microscope or SEM is used for imaging. In recent years, X-ray synchrotron and ptychography have been used to extract circuit connection information of a 14 nm node IC [17]. Although the technique is claimed to be non-destructive but the samples for this type of imaging need to be as small as few tens of microns which would really make it a destructive technique.

d) Annotation: All features in images like active region, gates, capacitors, inductors, resistors, vias, contacts, and metal lines are annotated manually or using image processing software.

e) Netlist and Functionality Extraction: Different components of the circuit layout are identified, and interconnection between the components are obtained to fully extract the netlist. Software like ICworks [14], Pix2Net [18], Degate [19] can extract the complete netlist and functionality of the chip. Fig. 3 shows the steps involved in chip reverse engineering.

2.1.2 PCB Reverse Engineering: PCB reverse engineering focuses on identifying all components on the board and the interconnection between them. PCB reverse engineering can be destructive or non-destructive. In a destructive method, delayering, removal of components, and imaging is performed iteratively layer by layer [14]. In destructive delayering, it is important to collect information about material thickness, composition and characteristics of each layer. X-ray tomography is used for non-invasive imaging and extracting internal structure of a PCB [20]. During X-ray imaging, material composition, filter, source power, source/detector distance to object, exposure time, imaging artifact and tomography algorithm influences the image quality and netlist extraction process.

2.1.3 Bitstream and Firmware Reverse Engineering: Bitstream is a file that contains configuration data for FPGA. SRAM-programmed FPGA requires an external non-volatile memory (NVM). When power is applied, the bitstream is loaded into the SRAM FPGA. A flash-programmed FPGA uses internal flash memory to hold the bitstream data. Firmware reverse engineering is the process of converting the machine code into a human-readable format. Both bitstream and firmware are stored in non-volatile memory (NVM) like read-only memory (ROM), electrically erasable programmable ROM (EEPROM) or flash memory. The information is stored in the memory cell transistors as electrons. The challenge for reverse engineering memory cells is that any source of energy can disturb the charge distribution and erase the memory content. The known prominent NVM extractor tools are scanning probe microscopy, scanning Kelvin probe microscopy, passive voltage contrast (PVC) and scanning capacitance microscopy (SCM) [14], [16], [21]. Probe microscopy uses the direct probing method to extract the charge information. PVC probing applies primary electron beam using SEM and detects modified secondary beam. Presence of electric field at different location of die is the source of such beam modification. The area with lower/zero charge density appear brighter in the image. Then image processing techniques are used to identify the bit value. SCM uses high sensitive capacitance sensor to identify charge in memory cells. As bitstream and firmware are encrypted with encryption standards like 3DES and AES, decryption is required once extracted.

2.1.4 Trust Verification and Security Threat with Reverse Engineering: The purpose of reverse engineering could be divided into two main goals namely:

1) Extracting IP Blocks, Netlist and Functionality: Such knowledge can verify the root of trust of a chip and impose security threat, simultaneously. Modern semiconductor industry heavily relies on third-party resources, that is third-party IP, fabrication facility, that has triggered the concern for hardware Trojan insertion and introduce trust issues. Hardware Trojan is considered a malicious change in functionality or parametric change of an IC. Such changes include addition and deletion of transistors, gates, interconnects etc.. Parametric changes consist of thinning interconnects, weakening flip-flops and increasing susceptibility to aging. This can reduce the yield and reliability and make it susceptible to attack [22]. Hardware Trojan are expected to be activated under very specific/rare conditions, which make it difficult to activate and detect them using random input patterns. Test approaches based on functional testing and side channel fingerprinting have been widely proposed to detecting hardware Trojans at post-silicon stage [23]–[26] . Functionality or side-channel information of IUA are compared with a golden IC to detect hardware Trojans. The main challenge to these methods is that the 'golden chip' is not available for setting the benchmark to test IUA. The authors assumed that reverse engineering can provide such golden chip [1]. If such golden chips are available, then the logic test responses and side-channel information gathered from those reverse-engineered Trojan-free chips can be used to authenticate the IUA.

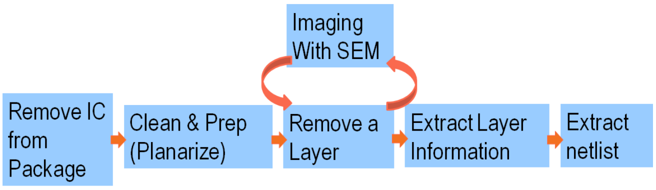


Fig. 3: IC reverse engineering process.

Reverse engineering has been gaining more attention in recent years and experiencing community-wide acceptance as an effective approach for hardware Trojan detection. Assuming a golden layout of the chip is available, machine learning approach has been used to compare SEM images of IC internal layers/components with the chip layout. For this technique, decapsulating, delayering and imaging are required to detect hardware Trojans [4]. In [27], a high-quality SEM image from a backside thinned golden IC is compared with low-quality SEM image of an IUA. The objective is to identify malicious changes performed by the foundry. Such method can equally be applicable for detecting hardware Trojans in PCBs.

Reverse engineering attack is associated with various threats such as IP piracy, cloning, counterfeiting and hardware Trojan insertion. To perform the aforementioned attacks an adversary is required to perform partial or complete reverse engineering to extract the netlist followed by identification and disabling of built-in protection mechanisms. However, for decades, reverse engineering has been used as a valuable tool to identify IP and patent infringement cases by organizations like Tech insider, Micronet Solutions.

2) Extracting Location of Sensitive Wire or IP Blocks: An attacker can extract the layout and netlist of ICs through reverse engineering. Such information can expose the location of security-critical modules, memory blocks or sensitive wires of the chip, hence, significantly reduce the cost and time required for probing attacks, [13], optical fault injection attacks [7] or remote attacks. The layout and netlist information of a chip and PCB can be deduced non-destructively using X-ray ptychography and

X-ray tomography, respectively. So, the adversary can now learn about the security measures or cryptographic key implemented in the chip and perform a more accurate and less time-consuming attack on the rest.

2.1.5 Existing Countermeasures Against Reverse Engineering

Different passive and active countermeasures against reverse engineering have been proposed. The aim of these existing countermeasures against reverse engineering is to increase the required execution time, expertise and equipment prohibitively higher. Passive countermeasures like Protecting service manuals and documentation, hardware watermarking, split manufacturing, hardware metering have been proposed as a possible solution to prevent foundry to clone devices [28]. Obfuscation, camouflaging, tamper protection layers etc. are well-known countermeasures against reverse engineering.

Obfuscation is a powerful tool to hide design secrets from a potential adversary. The objective of obfuscation is to obscure a design through modification while allowing the system or design to maintain the same functionality as the original. Obfuscation to protect against reverse engineering can be classified into two techniques system-level and circuit level obfuscation [29]. Finite state machine (FSM) modification by adding extra FSM node, logic encryption by adding gates, physically unclonable function (PUF) obfuscation are example of System-level obfuscation [30]–[32]. All these techniques require certain input sequence to unlock the circuit functionality.

Circuit-level obfuscation includes cell camouflage and dummy contacts to protect chip layout from reverse engineering attack [33], [34]. In the camouflage technique, the layout of standard cells with different functionalities is made to appear identical by using real and dummy contacts. Position of real contact can enable the exact functionalities of the cell. Such camouflage significantly increases the effort for reading chip layout and memory cells. Filler cells are inserted into the layout and sometimes connected with metal layers to create a dense network to increase complexity of layer [29].

A tamper-proof fitting enclosure like torx and custom screws shapes, adhesively bonded enclosures are widely used for protection against physical attack on PCB. Using spare inputs and outputs from processors to route signals which are not timing critical, but which are functionally critical could be used for raising confusion in PCB reverse engineering. Meanwhile, IEEE1149.1 JTAG and debugging port elimination can make the firmware extraction more difficult. Deposition of high-Z material like tantalum and tungsten, on PCB board prevents PCB reverse engineering by introducing inevitable imaging artifacts during non-destructive X-ray tomography [35].

2.1.6 Challenges and Research Opportunity: Challenges involve with reverse engineering are two folds 1) to develop reverse engineering as an effective tool for trust verification and failure analysis 2) Countermeasures to protect chip/pcb/software/bitstream from reverse engineering. Each has its own difficulties and challenges.

The most prevalent challenge in reverse engineering is automation at different stages, as shown in fig. 3, for complete chip reverse engineering. Although delayering and imaging tools have developed to capture submicron level features, human operator involvement is required for operating those tools due to a wide range of fabrication process, layer thickness, material and device structure. Considering the recent advancements in automating the imaging and delayering tools [36] the concept of Intelligent Microscopy is of interest of many in this community. An intelligent microscope to delayer and image ICs automatically, stores images and recollect images with low resolution without spending a lot of time on the areas of IC where the features are larger can save the time hugely for imaging and delayering during reverse engineering. In addition, image post-processing like image compression, stitching, annotation, etc. are not been fully automated yet although lots of progress is seen in this domain. Efficient and reliable package removal and delayering are also necessary for the subsequent imaging step. The challenge of exposing the die or PCB evenly at each layer is required to be addressed to mitigate the imaging and feature extraction challenges. To achieve this, research groups and companies are combining chemical and physical polishing/etching techniques according to the different properties of materials in devices, and have made progresses [27], [36]. FIB is also used as an alternative technique for delayering. Compared to traditional polishing/etching, FIB delayering is generally slower but allows an in-situ examining by SEM, making it convenient for small volume materials removing.

For imaging, because of the very small scale of modern IC chips node technology, automatic imaging and image stitching are required to finish the reverse engineering in reasonable period. From the imaging point of view, IC chips can be divided in two parts: routing part that includes metals layers and vias, and active layer that includes gates, contacts and doped region. Different parameters such as SEM beam energy, probe size, magnification, dwelling time and pixel size, should be chosen accordingly to collect desired information while minimizing the time consumption [27]. Currently, automation can be achieved through the predefining imaging parameters [36]. The imaging time can be reduced with compressed sensing the process of reconstructing a image from a series of random sampling. Meanwhile, multi-beam SEM system is recently introduced, which greatly speeds up the imaging by using tens of parallel beams to scan multiple areas simultaneously, however the tool is very expensive that makes it difficult to many to get access [37]. Once the images are taken, it is required to create a photomosaic to extract the netlist. Such panorama of adjoining images is challenging due to repetitive features and lacks automation. Besides the SEM, non-destructive X-ray tomography has been used to extract circuit connection in PCB [20] and a 14 nm node technology chip [17]. But the requirement for IC reverse engineering with X-ray ptychography is the smaller sized sample.

Netlist and circuit extraction were manual during the early stage of hardware reverse engineering [16]. Decades of research has developed different methodology for chip/PCB/FPGA reverse engineering. All such methods require operator involvement at different stages to identify the gate. It has been quantitatively showed that methods with higher positive feature like reliability, robustness, accuracy, efficiency etc. may not be suitable for industrial implementation due to higher negative features like complexity, cost and lack of automation [38]. Addressing the issues like complexity and automation in reverse engineering are required to develop this technique as a effective trust verification tool.

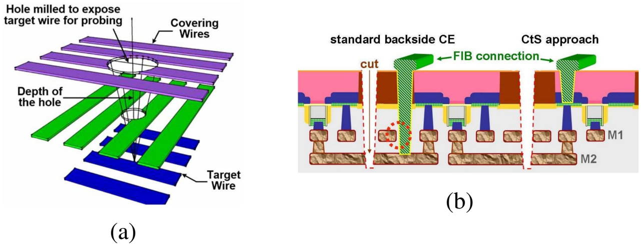
To protect the IP theft and counterfeiting different anti-reverse engineering technology has been developed. The existing countermeasures on reverse engineering, such as camouflaging and logic locking [14], focus on increasing the time, cost, expertise and equipment. Literature does not suggest any benchmark or matrix for analyzing the strength and applicability of existing countermeasures in reverse engineering. Implementing anti-reverse engineering would increase the area overhead, power consumption, fault analysis cost and introduce complication in trust and patent verification. Besides, backside of the chip remains defenseless and offer direct accesses to active region of the chip. Such accesses allow direct electrical measurement via probing [11] or device status observation via microscopy measurement [15], [14], facilitating the reverse engineering. The challenges for developing required countermeasure to protect backside will be discussed in later sections.

2.2 Electrical Probing and Circuit Edit

Electrical probing inspection/attack is a kind of invasive physical analysis to directly probe a signal wire for extracting information e.g. plaintexts or encryption keys from a chip/PCB/FPGA. The circuit edit is permanently modifying the connection in the chip layout using FIB for injecting fault or probing.

2.2.1 Electrical Probing and Circuit Editing Fundamentals: A silicon die can be accessed through frontside or backside depackaging. This leads to the dichotomy between frontside and backside probing. Frontside probing exposes devices starting from passivation layer of the IC and usually target metal interconnects that are located in higher metal layers [5], while backside probing exposes devices starting from the substrate of the IC and usually target transistor channels, diffusion contacts, and interconnects in low metal layers [12].

The wire that the probing attack targets is called a target wire. The physical point on a target wire chosen to serve as connection between target wire and deposited metal contact during probing is called a point of interest (PoI). Attacker can identify desirable PoI by reverse engineering. Partial reverse engineering to extract the data path is sufficient for this purpose. PoI can also be identified from backside through PE analysis during operation of chip.



(a)

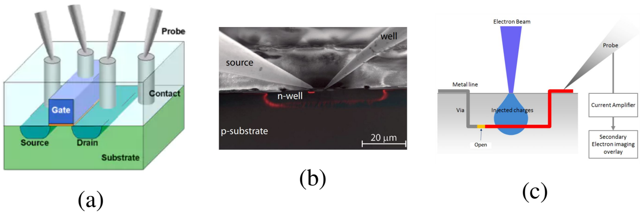
(b)

Fig. 4: (a) Frontside milling- milling from back end of line through covering wires (purple and green) to reach target wires (blue) [39] (b) Back side milling comparison between standard backside circuit edit and CtS approach [12].

A probing attacker needs to identify the absolute coordinate of the point to mill. The signal of the wire can be buried beneath several metal layers. A hole is milled with state-of-the-art FIB, as shown in fig. 4a, to expose PoI for frontside probing. FIB can deposit material at nanometer resolution to produce required conducting path for probing. In backside probing, the silicon material can be polished down to 30 μm. Advance node technology uses shallow trench isolation (STI). STI generally reached by creating a wide trench till n-well level and then milling a local trench. This reduction can reduce the device material to 300-400 nm. Now milling narrow trench and depositing conductive material can generate contact holes. Contacts to silicide (CtS) method has also been developed for probing drain and source of a FET [6]. From fig. 4b it is clear that CtS can avoid the probability of short-circuit (red circle area) which is present in standard backside probing [12].

Conventional electrical probing is also called microprobing after minimum precision it is able to reach. Nano-probing is also providing the capability to probe at submicron level with the probe tip size as small as 5 nm, this allows to directly probe every terminal of a transistor (fig. 5a) where conventional microprobing cannot.

2.2.2 Existing Countermeasures : Existing countermeasures focus on two types of countermeasures: 1) Fully prevent probing physically 2) encrypting information [39]. Countermeasures based on probing attempt detection are two types - active and passive shields. Active shields



(a)

(b)

(c)

Fig. 5: Fig. 5: (a) Cross sectional view of nanoprobing a MOS [40] (b) EBIC imaging: The two probes are connecting respectively the right transistor source and the well. The red color represents the intensity of the EBIC induced current generated along the p-n junction depletion regions (c) Schematic of the EBAC characterization principle [41].

are signal carrying interconnects/metal mesh sensors placed as a top-most metal layer. The signals in interconnects are compared continuously to verify the integrity of the chip. These signals may use ring oscillator, RC delay, block cypher, random number [42]–[44]. Passive shields are kind of analog shield based on parametric data like capacitance [45]. Any variation in signal or parameter can initiate reset signal for ICs. In addition to hardware based approaches, one cryptographical method called t-private circuits proposed to modify the security-critical circuit so that at least t + 1 probes are required by an attacker to extract one bit of information [46]. Here, signal is encoded by XORing the signal with t number of independently generated random signal. Obfuscation can be used to encrypt the layout to make the extracted information analyze difficult.

2.2.3 Security Threats and Research Opportunities: Probing allows extraction of information from physical circuit devices that carries information and allows an attacker to extract security assets such as encryption keys [13]. Depending on the direction milling is performed to expose targeted device of the probing - frontside or backside of the IC - each target different categories of devices, leading to different capabilities and challenges. A number of protective mechanisms have been developed to detect or deter frontside milling, which can be used against probing, circuit editing, among other invasive attacks [47].

A few weaknesses remain to be secured in existing protective designs. Existing designs require high area overhead and, occupy a number of routing layers to detect milling with a shield, which is expensive on state-of-art IC designs while prohibitive on cost-sensitive and layers-limited technologies; their implementation is limited to top layers which may be sub-optimal, and do not properly protect key signals of the shield itself against circuit editing attacks; none considered protecting against backside attacks; none considered protecting against frontside attacks at an angle; some designs leave weaknesses for the attacker to exploit, such as not secured against replay attack [43], not secured against rerouting of shield wires [44], only protecting certain wires, leaving protected information to be probed from logically related signals and reconstructed [48], or incurring large area overhead while relying on other methods to protect its security primitives [46] ask. Improving upon existing frontside protection mechanisms in these aspects can be very useful for designs where backside attack is made infeasible, for example on back-to-back 3D ICs. In particular, shield-based detection of tampering attempts could be improved in terms of maximum secure aspect ratios, protection against circuit edits and protection against angled milling by undergoing computer-aided design (CAD) based evaluations and optimizations.

Although currently less vulnerable than backside protections, frontside protections will likely remain vulnerable due to the simple fact that tools used in invasive attacks are the same tools necessary in IC failure analysis and diagnosis; it is less difficult for an attacker to acquire a state-of-art FIB, than for technology node the protection designs are fabricated on to remain state-of-art. A more advanced FIB has a higher aspect ratio, which enables the attacker to leave a smaller footprint when milling through the shield layers, therefore less likely to trigger detection. This situation is particularly relevant for cost-limited ICs such as smartcards, which are unlikely able to afford state-of-art technology nodes to begin with. It remains to be shown whether protection against probing attacks can be expected for devices fabricated under legacy technology nodes, or a more practical metric of protection should be used instead.

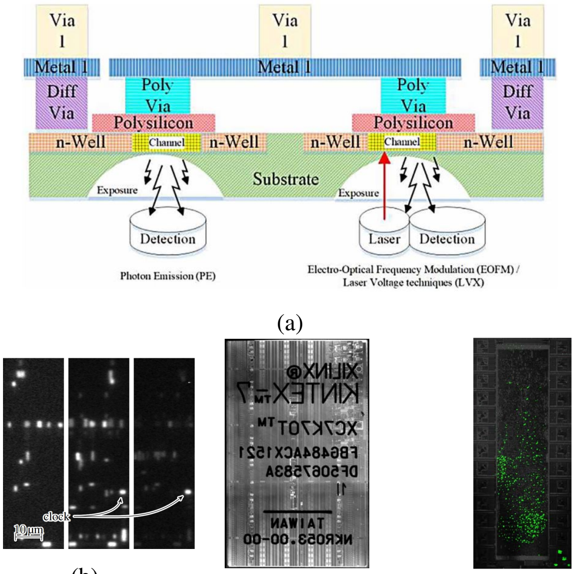
Backside attacks present a direr threat. This category of probing attacks includes passive attacks such as photon emission, semi-invasive attacks such as laser voltage techniques (LVX), and fully invasive CtS deposition as well as circuit editing on lower level interconnects [15]. More recent technology nodes typically employ STI technique to reduce latch-up faults, which makes backside probing easier since STI spares probing attackers the trouble to insulate contacts to wires they intend to probe at [11]. Probing attacks from the backside are more difficult to protect against since they dont require high aspect ratio FIB as in frontside attacks [49], typical technology nodes do not support adding metal interconnects below substrates, and in the case of PE attacks the circuit has no way of detecting a completely passive observer. Due to these difficulties, protection mechanism dedicated against backside probing has yet been proposed. Among existing protection mechanisms, only the Probe Attempt Detector (PAD) [11] and t-private circuit [50] can be expected to remain effective against backside probing attacks, although their respective weaknesses continue to prevent them from becoming complete solutions.

Conventional FA tools cannot meet with the nanometer resolution required for current 14 nm node technology due to non-uniformity in dopant implants, structural defects and processing conditions [51]. For this reason, Nanoprobing is emerging as a solution. As depicted in fig. 5a, characterizing the transistor or any sensitive wire is possible using nanoprobe. The probe can be assembled on any SEM or FIB stage and can be used for extracting the information from devices fabricated at newer technology node. In addition, electron beam induced current (EBIC) (fig. 5b) and electron beam absorbed current (EBAC) (fig. 5c) are two emerging techniques to measure the signal passing through a p-n junction [52]. So, at submicron level, combination of EBIC/ EBAC and nanoprobing can be a powerful tool for extracting the signal form a wire or transistor.

In summary, extensive research in protection against tampering attacks is necessary to answer some fundamental questions in the field, particularly in developing dedicated solutions against backside attacks, proposing practical security metrics for ICs fabricated under legacy technology nodes, optimizing existing protective designs, and eliminating their existing weaknesses.

4. Semi-Invasive Inspection/Attacks

Semi-invasive attacks lie in the gray zone of the non-invasive and invasive attacks. Semi-invasive attacks were first used to flip a bit in microcontroller SRAM cell using a photoflash lamp [9]. These inspection/attacks are mostly based on optical techniques, i.e., attacks based on UV light, laser and X-ray. Semi-invasive attacks impose greater threat towards the security of the chip due to their low cost and less evaluation time. In most cases, the semi-invasive attacks require decapsulating the chip. The internal structure of the chip remain intake as access to direct contact with metal layers and transistors are not needed. The IUA must stay functional after the decapsulation.



(a)

(b)

(c)

(d)

Fig. 6: (a) Photon emission and optical probing - electro-optical frequency modulation or laser voltage techniques are used for passive and active measurements [13]. (b) Various logic elements implementing combinational (left) and sequential logic (center and right) on a MAX V complex programmable logic device from Altera.. Inactive clock input implies the combinational logic blocks [50] (c) Reflected light overview image of a complete Xilinx Kintex 7 FPGA die during optical probing [8] (d) activity during FPGA bitstream decryption in the dedicated AES core inside the FPGA [8].

3.1 Optical Fault Injection Attack: It has been reported that, if photon energy is higher than silicon bandgap energy i.e., 1.1 eV electron-hole pairs can be generated in the silicon [9]. Later this principle is used for injecting faults in an embedded device, such as microcontrollers and FPGAs and even in the physically unclonable function [10], [53], [54]. In optical fault injection inspection/attack techniques, after decapsulation the chip is mounted on a PCB to facilitate fault injection attack. Fault injection is possible from both frontside and backside. As the number of interconnect layers at the frontside of modern chip is increasing, optical path of photons get obstructed. Such an obstruction is avoided by injecting fault form backside. In backside fault injection technique the die is thinned using polisher down to 10 μm. The position of the target can be selected using reverse engineering [7] or photonic emission analysis [10] which will be discussed briefly in Section 3.2. To inject a fault in a circuit by flipping a bit, a precisely focus light source with a photonic energy higher than silicon bandgap energy is required. Photocurrent laser stimulation is used to introduce bit flips whereas thermal laser stimulation introduce timing fault in system [12].

3.2 Optical/Photonic Emission Side Channel Analysis: At static state, CMOS circuit operates at the linear region of MOSFET. During a switching event, transistors enter into operation mode termed as saturation for a short period of time. The transistors release hot carriers as a form of photon emission. Due to the higher mobility of electrons, the n-type transistors emit significantly more photons as compared to p-type transistors as shown in fig. 6a. The near-infrared region photons can penetrate silicon and can be used as side channel information when observed from IC backside [10], [55]. As photonic emission analysis is performed from the backside, the sample is prepared by polishing the backside using instruments like Ultratech ASAP-1. To increase surface quality, an anti-reflective coating (ARC) is applied. Then the chip is assembled in a custom PCB for photonic emission analysis. Spatial and temporal variation in photonic emission can be captured with CCD camera and an avalanche photodiode, respectively [55]. As shown in fig. 6b Such information expose the logic blocks and functionality of the chip. Photonic emission analysis can be utilized to attack AES, attack delay-based PUFs, extracting functional state machine, identifying sequential, combinational logic, memory arrays, reverse engineering memory cells [6], [50], [55].

3.3 Optical Probing: Electrical probing requires FIB for circuit editing to place the contact with PoI. However, as silicon is transparent for NIR photons, the analysis is possible using optical probing. Electro-optical probing (EOP) and Electro-optical frequency mapping (EOFM) probs electrical signals on transistors and creates an activity map of the active circuit, respectively. Incoherent light source is used in EOP/EOFM. Apart from the difference that laser source is used in laser voltage probing (LVP)/laser voltage imaging (LVI); these two methods are equivalent of EOP/EOFM. [8]. The sample is decapsulated and placed in a custom PCB for analysis. But if the IUA is a flip-chip no decapsulation is required because the active region is directly accessible for optical probing. As no decapsulation is required when a flip-chip is used for optical probing, this technique then can also be classified as non-invasive attack. As shown in fig. 6c the die is visible at the wavelength to which silicon is transparent. Using optical probing the AES block of Xilinx Kintex 7 FPGA has been identified [8].

3.4 Security Threat and Trust Verification: To safeguard sensitive information inside the chip different countermeasures are placed at the frontside of the chip.

However, semi-invasive attacks have imposed a threat towards the confidentiality and integrity of the chip from both backside and frontside. Optical fault injection and photonic emission attacks were used for exposing the keys for cryptographic ciphers like AES, RSA [54], [56], [57]. Combination of spatial information from photonic emission analysis and temporal information from picosecond imaging circuit analysis (PICA) enables an adversary to extract memory location, logic location and executed logic in microcontroller [58]. A Similar attack has been performed on AES block of FPGA [50]. Similarly information like Locating the secured circuitry and extracting sensitive design information are also possible with optical probing as shown in fig. 6d. Exposure of functionality, firmware and cryptography key enables an adversary to analyze IP, locate the security measures and exploit cryptomodule. Regardless of the security threats imposed by semi-invasive attacks, photonic emission analysis [59] and optical probing can facilitate the reverse engineering for trust verification and identifying any suspicious activity in the chip.

3.5 Existing Countermeasures and Research Opportunity: Countermeasures against semi-invasive attacks can be categorized into two classes of detection and prevention schemes. To detect active optical attacks, such as laser fault injection, silicon light sensors are conventional solutions to detect the photons of the light beam. However, if the deployed laser beam has a larger wavelength than the silicon band gap, as in the case of optical probing, the light sensors are only stimulated thermally. As a result, no electron-hole pairs are generated, and therefore, a silicon photosensor is not triggered. Hence, silicon light sensors cannot be used to detect optical probing attempts, where the photons have less energy than silicon bandgap.

However, the thermal stimulation during optical probing attempts can lead to immediate local disturbances in temperature and current of the transistors on the chip. Temperature and current variations affect the signal propagation delays of timing-dependent circuits, such as ring-oscillator Physically Unclonable Functions (PUFs). Thus, one potential countermeasure [60] could be using a ring-oscillator PUF and distributing its ring-oscillators close to the security related-part of the chip. In this case, any optical probing attempt would influence the behavior of the PUF with a high probability.

Another approach would be to prevent optical access from the backside of the chip. For instance, adding an entirely opaque layer to the backside of the chip, which is actively monitored, can detect unauthorized optical access to the backside of the chip. Such a scheme has been proposed in [15], where particular layers are coated on the silicon substrate. This multilayer coating layer reflects the incoming lights from a set of LEDs to a set of light detectors. If an attacker removes the coating layers to interact optically with transistors, the reflection characteristics of the IC backside are changed, and therefore, attack attempts can be detected. Besides, adding irregualr and fabrication-compatible particles such as nano-scale pyramids in the silicon oxide layer can scatter the photons emitted from transistors. Such a protection layer is a cheaper and more promising method against LVP [61].

While there are experimentally verified concepts available to either detect or prevent optical access to the IC backside, further research is required to validate their mass production compatibility. However, there are also other conceivable countermeasure schemes, which are worthy to be considered by the research community. For instance, similar to power side-channel analysis countermeasures, adding gates carrying an inverted signal could make optical probing ineffective, since they cancel the data-dependent modulation of the reflected light from transistors. However, this would need development and verification of proper structures and ASIC design tools. Another potential countermeasure would be the deployment of an unstable clock source in the chip to randomize the relation of the processed data and probed signal over multiple integrations.

5. Application of Computer Vision and Machine Learning in Physical Inspection/Attack

Because of the advances in computer vision and machine learning, researchers are now considering the use of this method on the IC images for different purposes in particular for reverse engineering and hardware Trojan detection. Unlike other means, methods involving computer vision and machine learning may be capable of detection features that are undetectable by other means, are significantly faster, and can be largely automated. The pipeline for this purpose in general includes image preprocessing, feature extraction, and classification. The image preprocessing step involves the use if image processing techniques to remove as much noise as possible to make the presence of the features of interest more prominent. The feature extraction step comprises of the use of computer vision method to extract salient features of the images objects. The final step consists of using the extracted features as input to machine learning algorithms for determining the presence of the features of interest or annotating them in the image. To date, relatively little research has been performed on the use of computer vision and machine learning methods for reverse engineering or to detect hardware Trojans. Therefore, important research challenges are still unaddressed and provide a roadmap for future research efforts.

Critical challenges to the development of automated computer vision/machine learning based methods include noisy images, unoptimized feature representation, and a lack of training data for machine learning algorithms. SEM imagery typical contains a considerable amount of noise which can affect the reliable extraction of object features. The common techniques used for noise removal in digital images may not be suitable for this application. The development of noise removal techniques specific to SEM imagery would be an important research contribution. The number of objects within an SEM image may be in the order of billions. Therefore, extraction features not only should be robust to noise, capture relevant information about the object but must also be computed quickly. Feature extraction methods and feature representations specific to the problem of hardware Trojan detection or reverse engineering in SEM imagery are necessary to meet these requirements. There have many advances in the area of machine learning as it applies to classification. However, to leverage advances in machine learning, large sets of data which represents the problem space is required for training machine learning algorithms. Certain types of machine learning algorithms, such as deep learning, require on the order of millions of data points to achieve good classification performance. One possible approach would include techniques to synthesize realistic training data using machine learning methods such has generative adversal networks (GAN). Meeting the discussed challenges is a requirement to the goal of an automated reverse engineering and Trojan detection tool based upon SEM imagery.

6. Conclusion

Physical inspection/attack techniques are becoming a growing concern in semiconductor industry. Physical attack combined with SAT or remote attack impose greater security threat. In this work we have analyzed the techniques for invasive, semi-invasive, and non-invasive physical inspection/attack methods followed by the state-of-the-art countermeasures against each physical attacks. Later, we presented the security threats coming with the advancements of physical inspection tools which are mainly for failure analysis purposes but can be used for trust verification or maliciously for physical attacks. We have also reviewed the challenges for existing countermeasures and scope of research opportunities. Systematic approach for developing countermeasures, lead a new direction towards hardware security. Addressing the challenges of automation can lay the foundation for trust verification tools for hardware Trojan detection.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, 2010.

[2] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[3] "Trusted integrated circuits (trust)." [Online]. Available: https://www.darpa.mil/program/trusted-integrated-circuits

[4] C. Bao, D. Forte, and A. Srivastava, "On application of one-class svm to reverse engineering-based hardware trojan detection," in *Quality Electronic Design (ISQED), 2014 15th International Symposium on*. IEEE, 2014, pp. 47–54.

[5] S. Skorobogatov, "Hardware security of semiconductor chips: Progress and lessons."

[6] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2012, pp. 41–57.

[7] F. Courbon, P. Loubet-Moundi, J. J. Fournier, and A. Tria, "Increasing the efficiency of laser fault injections using fast gate level reverse engineering," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2014, pp. 60–63.

[8] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1661–1674.

[9] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 2–12.

[10] S. Tajik, H. Lohrke, F. Ganji, J.-P. Seifert, and C. Boit, "Laser fault attack on physically unclonable functions," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2015 Workshop on*. IEEE, 2015, pp. 85–96.

[11] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, "Breaking and entering through the silicon," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 733–744.

[12] C. Boit, C. Helfmeier, and U. Kerst, "Security risks posed by modern ic debug and diagnosis tools," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*. IEEE, 2013, pp. 3–11.

[13] H. Wang, D. Forte, M. M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Design & Test*, vol. 34, no. 5, pp. 63–71, 2017.

[14] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM journal on emerging technologies in computing systems (JETC)*, vol. 13, no. 1, p. 6, 2016.

[15] C. Boit, S. Tajik, P. Scholz, E. Amini, A. Beyreuther, H. Lohrke, and J.-P. Seifert, "From ic debug to hardware security risk: The power of backside access and optical interaction," in *Physical and Failure Analysis of Integrated Circuits (IPFA), 2016 IEEE 23rd International Symposium on the*. IEEE, 2016, pp. 365–369.

[16] R. Torrance and D. James, "The state-of-the-art in ic reverse engineering," in *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, 2009, pp. 363–381.

[17] M. Holler, M. Guizar-Sicairos, E. H. Tsai, R. Dinapoli, E. Müller, O. Bunk, J. Raabe, and G. Aeppli, "High-resolution non-destructive three-dimensional imaging of integrated circuits," *Nature*, vol. 543, no. 7645, p. 402, 2017.

[18] [Online]. Available: http://micronetsol.net/pix2net-software/

[19] [Online]. Available: http://www.degate.org/

[20] N. Asadizanjani, M. Tehranipoor, and D. Forte, "Pcb reverse engineering using nondestructive x-ray tomography and advanced image processing," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 7, no. 2, pp. 292–299, 2017.

[21] F. Courbon, S. Skorobogatov, and C. Woods, "Reverse engineering flash eeprom memories using scanning electron microscopy," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2016, pp. 57–72.

[22] Y. Shiyanovskii, F. Wolff, A. Rajendran, C. Papachristou, D. Weyer, and W. Clay, "Process reliability based trojans through nbti and hci effects," in *Adaptive Hardware and Systems (AHS), 2010 NASA/ESA Conference on*. IEEE, 2010, pp. 215–222.

[23] X. Zhang and M. Tehranipoor, "Case study: Detecting hardware trojans in third-party digital ip cores," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 67–70.

[24] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards trojan-free trusted ics: Problem analysis and detection scheme," in *Proceedings of the conference on Design, automation and test in Europe*. ACM, 2008, pp. 1362–1365.

[25] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "Mero: A statistical approach for hardware trojan detection," in *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, 2009, pp. 396–410.

[26] S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, "Tesr: A robust temporal self-referencing approach for hardware trojan detection," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 71–74.

[27] N. Asadijanzani, "Detecting hardware trojans inserted by untrusted foundry using physical inspection and advanced image processing techniques," June, 2018.

[28] 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," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[29] A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar, and S. Kundu, “Physical design obfuscation of hardware: A comprehensive investigation of device and logic-level techniques,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 64–77, 2017.

[30] Y. Alkabani and F. Koushanfar, “Active hardware metering for intellectual property protection and security.” in *USENIX security symposium*, 2007, pp. 291–306.

[31] J. A. Roy, F. Koushanfar, and I. L. Markov, “Epic: Ending piracy of integrated circuits,” in *Proceedings of the conference on Design, automation and test in Europe*. ACM, 2008, pp. 1069–1074.

[32] R. S. Chakraborty and S. Bhunia, “Harpoon: an obfuscation-based soc design methodology for hardware protection,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493–1502, 2009.

[33] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, “Security analysis of integrated circuit camouflaging,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 709–720.

[34] L.-W. Chow, J. P. Baukus, and W. M. Clark Jr, “Integrated circuits protected against reverse engineering and method for fabricating the same using vias without metal terminations,” Sep. 14 2004, uS Patent 6,791,191.

[35] Z. Guo, B. Shakya, H. Shen, S. Bhunia, N. Asadizanjani, M. M. Tehranipoor, and D. Forte, “A new methodology to protect pcbs from non-destructive reverse engineering,” 2016.

[36] E. L. Principe, N. Asadizanjani, D. Forte, M. M. Tehranipoor, R. Chivas, M. DiBattista, S. E. Silverman, M. Marsh, N. Piché, and J. T. Mastovich, “Steps toward automated deprocessing of integrated circuits,” 2017.

[37] “Multisem 505/506.” [Online]. Available: https://www.zeiss.com/microscopy/int/products/scanning-electron-microscopes/multisem.html/Overview

[38] G. Rematska and N. G. Bourbakis, “A survey on reverse engineering of technical diagrams,” in *Information, Intelligence, Systems & Applications (IISA), 2016 7th International Conference on*. IEEE, 2016, pp. 1–8.

[39] Q. Shi, N. Asadizanjani, D. Forte, and M. M. Tehranipoor, “A layout-driven framework to assess vulnerability of ics to microprobing attacks,” in *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*. IEEE, 2016, pp. 155–160.

[40] “Nanoscale Device Characteristics Analysis System Nano-Prober NP6800.” [Online]. Available: https://www.hitachi-hightech.com/global/science/products/microscopes/electron-microscope/nano-probing-system/np6800.html

[41] “Imina.ch. (2018). EBIC / EBAC Techniques for Semiconductor Failure Analysis — Imina Technologies SA.” [Online]. Available: https://www.imina.ch/applications/ebic-ebac-nanoprobing-failure-analysis-sem

[42] S. Manich, M. S. Wamser, and G. Sigl, “Detection of probing attempts in secure ics,” in *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 134–139.

[43] J.-M. Cioranesco, J.-L. Danger, T. Graba, S. Guilley, Y. Mathieu, D. Naccache, and X. T. Ngo, “Cryptographically secure shields,” in *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 25–31.

[44] S. Briais, J.-M. Cioranesco, J.-L. Danger, S. Guilley, D. Naccache, and T. Porteboeuf, “Random active shield,” in *Fault Diagnosis and Tolerance in Cryptography*, 2012, pp. 11–pages.

[45] P. Laackmann and H. Taddiken, “Apparatus for protecting an integrated circuit formed in a substrate and method for protecting the circuit against reverse engineering,” Sep. 28 2004, uS Patent 6,798,234.

[46] Y. Ishai, A. Sahai, and D. Wagner, “Private circuits: Securing hardware against probing attacks,” in *Annual International Cryptology Conference*. Springer, 2003, pp. 463–481.

[47] “Tarnovsky Deconstruct Processor - YouTube.” [Online]. Available: https://www.youtube.com/watch?v=w7PT0nrK2BE

[48] S. Skorobogatov, “How microprobing can attack encrypted memory,” in *2017 Euromicro Conference on Digital System Design (DSD)*. IEEE, 2017, pp. 244–251.

[49] R. Schlangen, P. Sadewater, U. Kerst, and C. Boit, “Contact to contacts or silicide by use of backside fib circuit edit allowing to approach every active circuit node,” *Microelectronics Reliability*, vol. 46, no. 9-11, pp. 1498–1503, 2006.

[50] S. Tajik, D. Nedospasov, C. Helfmeier, J.-P. Seifert, and C. Boit, “Emission Analysis of Hardware Implementations,” in *2014 17th Euromicro Conference on Digital System Design*. IEEE, aug 2014, pp. 528–534. [Online]. Available: http://ieeexplore.ieee.org/document/6927287/

[51] S. Toh, Z. Mai, P. Tan, E. Hendarto, H. Tan, Q. Wang, J. Cai, Q. Deng, T. Ng, Y. Goh *et al.*, “Use of nanoprobing as the diagnostic tool for nanoscaled devices,” in *Physical and Failure Analysis of Integrated Circuits, 2007. IPFA 2007. 14th International Symposium on the*. IEEE, 2007, pp. 53–58.

[52] S. Kleindiek, K. Schock, A. Rummel, M. Zschomack, P. Limbecker, A. Meyer, and M. Kemmler, “Combining current imaging, ebic/ebac, and electrical probing for fast and reliable in situ electrical fault isolation,” in *Physical and Failure Analysis of Integrated Circuits (IPFA), 2016 IEEE 23rd International Symposium on the*. IEEE, 2016, pp. 231–234.

[53] J.-M. Schmidt and M. Hutter, *Optical and em fault-attacks on crt-based rsa: Concrete results*. na, 2007.

[54] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, “Simple photonic emission analysis of aes,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2012, pp. 41–57.

[55] S. Tajik, E. Dietz, S. Frohmann, J.-P. Seifert, D. Nedospasov, C. Helfmeier, C. Boit, and H. Dittrich, “Physical characterization of arbiter pufs,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2014, pp. 493–509.

[56] J.-M. Schmidt, M. Hutter, and T. Plos, “Optical fault attacks on aes: A threat in violet,” in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*. IEEE, 2009, pp. 13–22.

[57] J. Krämer, D. Nedospasov, A. Schlösser, and J.-P. Seifert, “Differential photonic emission analysis,” in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2013, pp. 1–16.

[58] D. Nedospasov, J.-P. Seifert, A. Schlösser, and S. Orlic, “Functional integrated circuit analysis,” in *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 102–107.

[59] F. Stellari, P. Song, A. J. Weger, J. Culp, A. Herbert, and D. Pfeiffer, “Verification of untrusted chips using trusted layout and emission measurements,” in *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 19–24.

[60] S. Tajik, J. Fietkau, H. Lohrke, J.-P. Seifert, and C. Boit, “Pufmon: Security monitoring of fpgas using physically unclonable functions,” in *On-Line Testing and Robust System Design (IOLTS), 2017 IEEE 23rd International Symposium on*. IEEE, 2017, pp. 186–191.

[61] H. Shen, “Nanopyramid An optical scrambler against backside probing attacks,” Presentation, June, 2018.