Is Backside the New Backdoor in Modern SoCs?

(Invited Paper)

Nidish Vashistha†, M Tanjidur Rahman†, Olivia P. Paradis, and Navid Asadizanjani
Florida Institute for Cybersecurity (FICS) Research, Department of Electrical & Computer Engineering,
University of Florida, Gainesville, 32611, FL, USA
†Both authors have contributed equally to this paper.

***Abstract*—Modern integrated circuits (ICs) possess several countermeasures to safeguard sensitive data and information stored in the device. In recent years, semi-invasive physical attacks based on optical debugging techniques have proven to be capable of easily bypassing these security measures implemented in the chip. Optical attacks can reveal the data stored in memory, cache and register through various methods such as photon emission analysis, laser fault injection, laser voltage probing, and thermal laser stimulation. The above-mentioned methods, which employ laser scanning microscopy and photon emission microscopy, are effective because the silicon substrate is transparent to near-infrared (NIR) photons. Therefore, the most vulnerable part of an IC to optical attacks is the backside, where the chip's transistors can be accessed and probed with a NIR laser beam. Although different optical attack detection and avoidance mechanisms have been proposed, many can be circumvented and none are universal solutions for all types of optical attacks. In this study, we present a taxonomy of the different types of optical attacks and the security threats posed by each type. Then we discuss the existing prevention-detection based solutions to optical probing attacks which will set the future research direction.**

***Index Terms*—Hardware Security, Optical Attacks, Backside Protection of IC, Photon Emission Analysis**

I. Introduction

Presently, system-on-chips (SoCs) are designed for various applications from high-performance servers to low power computers in outer space to internet-of-things (IoT). These SoCs consist of tens of millions of transistors, several intellectual property (IP) cores, complex on-chip busses, and protocols to meet the current, all-encompassing technological demands. For instance, the new 10nm FinFET A11 bionic chip has approximately four billion transistors [1]. Due to the sheer complexity of the designs, SoCs are subject to rigorous testing and physical inspection procedures for detection of manufacturing and packaging defects [2]–[4]. Optical debugging methods, such as photonic emission analysis (PEA), laser fault injection (LFI), electro-optical probing (EOP), optical beam induced resistance change (OBIRCH), etc. are commonly used for yield analysis, probe testing, and failure analysis (FA). These debugging methods are feasible because silicon is transparent to near-infrared (NIR) photons. However, in recent decades, researchers have shown that the aforementioned optical inspection methods can also be used to compromise the confidentiality and integrity of assets stored inside the ICs [5]–[8]. Metal layers and protective meshes located at the frontside of the SoC obstruct the path of incident photons, protecting the ICs from optical attacks. However, no such protections are present in the device's backside, i.e., silicon substrate. Simply exposing the backside by de-packaging or de-lidding is shown to be sufficient for deployment of optical attacks [6], [9]. As a result, an attacker can use the silicon die's backside as a backdoor to access the back-end-of-line (BEOL) implementation of the device, exposing the assets within the chip. In addition, the recent shift toward flip-chip packaging exposes the silicon substrate, as compared to DIP packaging. In flip-chip package the attacker only requires IC de-lidding to access the substrate. The simple sample preparation approach for flip-chips renders them vulnerable targets for optical attacks.

The objectives of this paper are threefold. First, to provide an in-depth analysis of the security vulnerabilities caused by backside optical attacks. Second, to outline a variety of optical attack techniques and identify the potential targets for each method. Third, to analyze the benefits and constraints of several countermeasures against optical attacks that have been proposed so far.

This paper is organized as follows: The basics of flip-chip packaging and assets stored in the SoCs are discussed in section II. Different optical attack methodologies as well as the security threats imposed by each are introduced in section III and IV, respectively. In section V, we present the threat model. Section VI investigates the existing countermeasures against backside optical attacks. Finally, we conclude our study in section VII with a focus on the future direction of optical attack detection and avoidance methods.

II. Background and Motivation

A. Flip - Chip

The concept of connecting integrated circuits on a silicon die to a package in an upside flipped orientation was invented for military and civil aviation purposes [10]. Since then, packaging for consumer electronics has developed from dual in-line packaging (DIP) to ball grid array (BGA) packaging. Recently, IC vendors have switched to bare die flip-chip packaging to enable a thermal interface for fast cooling and easy access for reliability and failure analysis. Many of the major players in semiconductor market, such as Samsung Group (South Korea), Intel Corporation (U.S.), Global Foundries (U.S.), TSMC (Taiwan), UMC (Taiwan), Amkor Technology (U.S.), ST Microelectronics (Switzerland), and Texas Instruments (U.S.) are using flip-chips in their SoC segments and this market is expected to increase exponentially in upcoming years

978-1-7281-4823-6/19/$31.00

[11]. Although flip-chip packaging offers thermal venting and simplified failure analysis, it also introduces vulnerabilities in SoCs to physical attacks such as fault injection, partial reverse engineering, and optical probing which are discussed in more detail in section IV.

B. Assets on an SoC

Modern SoCs store sensitive data such as encryption keys, soft IP (FPGAs and programmable SoCs), biases or weights of neural networks, and proprietary algorithms to perform specialized tasks such as artificial neural networks, machine vision, and machine learning. The objective of SoC security architecture is to protect sensitive information, collectively known as assets, from unauthorized entities [12]–[14]. The nature of assets present in an SoC differs with the field of application and security architecture. Thus, a generalized taxonomy to classify all types of assets cannot be created. In general, essential assets include:

a) Digital Rights and Checking Code: In an SoC, the digital right management (DRM) policy defines the access rights for a different class of users to protect security-critical contents from piracy [12]. DRM, in a device, can be defined by either a firmware (software) or circuit (hardware) based approach. Unlike software based DRM, hardware based DRM provides better performance in terms of speed, power, memory usage, and security features. However, both hardware and software-based DRM execution can be monitored in real-time using optical analysis. Such monitoring can be used for injecting fault into the access control module, modifying the user privileges in the DRM policy, or bypassing the several protection mechanisms implemented in the chip.

b) Device Key: A device key is used to authenticate firmware and hardware, as well as grant access rights to an end user. Device keys may include cryptomodule keys, e-fuse configurations for silicon validation, or firmware authentication keys from the original equipment manufacturers (OEMs), etc. Lack of security against undesired monitoring of these device keys compromises the confidentiality of the assets and the root-of-trust.

c) On-Chip Protected Data: The security of on-chip protected information is associated with the integrity, confidentiality, and availability issues in the device. User information (e.g. login credentials or bio-metric data), protected firmware, and bitstream are examples of protected data on-chip. This information is appealing to malicious entities seeking to gain economic or competitive advantage. Therefore, it is vital to protect such information from possible attacks.

Various security policies and protection schemes have been developed to protect the aforementioned assets from different kinds of attacks. Still, the assets have been shown to be vulnerable against physical attacks such as PEA, LFI, and optical probing [2], [15]. Therefore, asset identification, threat model development, and attack surface detection can facilitate in developing impeccable countermeasures against semi-invasive/non-invasive optical attacks.

III. Optical Attack Techniques

In this section, we discuss a taxonomy of different optical attack methodologies and provide an in-depth assessment for each method. Depending on the stimulation techniques and detection methods, optical analysis can be classified under three major categories: a) photon emission (PE), b) electro-optical probing, and c) laser stimulation.

A. Photon Emission Analysis (PEA)

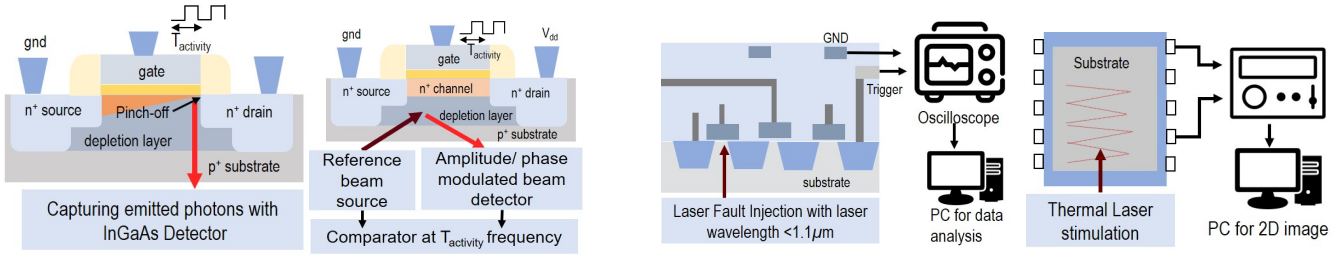
PEA is primarily developed for functional analysis and fault localization on silicon die without any external stimuli. During IC operation, hot-carrier luminescence coincides with the switching activities of the logic gates, which are directly related to their respective logic states. The current carriers gain kinetic energy when the MOSFET transistor's operation region switches to a saturated state. Then, the energy of the carriers is released in the form of emitted photons at the drain edge of the transistor, i.e., the pinch-off region of the transistor's space-charge region. In PEA, photons are collected with a detector and a 2D image mapping the locations of the emitted photons is produced for analysis (see Fig. 1a). In addition, temporal information of the signal propagating through the chip can be detected if PEA is incorporated with picosecond image circuit analysis (PICA) [7], [16].

The photon emission (PE) intensity depends on the applied voltage and switching frequency of the transistor. Since hot-carrier luminescence is best detected when switching activity occurs in transistors with a high electron mobility, PE is more prominent in n-type transistors than p-type transistors [7], [17]. Such data-dependency in emission can be a source of side-channel information for an adversary to extract the assets outlined in section II-B.

B. Electro-Optical Probing Techniques

Electro-optical probing (EOP) and electro-optical frequency mapping (EOFM) are two major electro-optical analysis techniques used for optical contact less probing and defect detection for ICs [2], [6], [18]. EOP involves probing electrical signals on the transistor with an incoherent light source whereas EOFM creates an activity map of the circuitry operating at a certain switching frequency. Laser-voltage analysis is another form of electro-optical probing. Apart from the difference in the laser source used, laser-voltage analysis and electro-optical analysis are equivalent. The measurement principle of laser-voltage probing (LVP) and laser voltage imaging (LVI) techniques are similar to EOP and EOFM, respectively [2], [19]. A laser beam with wavelength of 1.3 μm is used for EOP/EOFM due to the high absorption coefficient and refractive index of silicon.

In EOP, the laser can be focused on a single transistor from the backside of an SoC. Photons with NIR wavelengths can pass through the substrate, causing partial absorption and reflection in the active region or first metal layer. Since the absorption coefficient and refractive index of silicon are dependent on the space-charge densities caused by the time-varying electric field, the amplitude and phase of the laser beam are



(a) (b) (c) (d)

Fig. 1: (a) Setup used for photon emission analysis. During N-type MOSFET switching, emitted photons are captured using an InGaAS detector and a 2D mapping of the device is generated, (b) Optically probing a transistor operating at T_{active} frequency using EOFOM/EOP, (c) Laser fault injection setup using photo-current stimulation and oscilloscope and (d) Setup for thermal laser stimulation to observe OBIRCH or Seebeck effect.

modulated by the electrical parameters of the transistor. The optical detector measures the intensity of the modulated light and, hence, probes the transistor's electrical parameters.

In EOFM, the laser scans the region of interest (RoI) on the device under test (DUT) and the reflected light is evaluated by a spectrum analyzer, which acts as a narrow-band frequency filter [20]. The frequency-filtered values are then sampled for every scanned pixel and used to construct a 2D image using a grayscale or false-color representation [6]. If a node operates at the frequency of interest, it will modulate the incident light with the same frequency. The locations of the nodes operating at the same frequency are identified as a bright spot when the signal is evaluated by the spectrum analyzer. The optical probing setup is shown in Fig. 1b.

C. Laser Stimulation (LS)

Scanning a RoI with an infra-red (IR) laser can inject thermal or photoelectric energy inside the device under test (DUT), which locally perturbs the device's parameters or electrical signals. LS techniques use these circuitry perturbations to flip data stored in memory, inject fault in the circuit, or measure device parameters such as the logical state of gates. The effects of laser stimulation are related to the wavelength of the laser and the silicon band gap energy. Therefore, depending on the wavelength of laser used, the effect of LS can be divided into two major classes:

a) Laser Fault Injection (LFI): Lasers with a photon energy greater than or equal to the silicon band-gap energy, 1.1 eV, generate electron-hole pairs in the silicon. This effect is commonly referred to as photoelectric laser stimulation (PLS) [5], [16]. Lasers with a wavelength less than $1100nm$ can introduce PLS in the device. The logic state of a CMOS circuit can be flipped if the PLS is focused on a transistor drain or source terminal [5], [19], thus injecting a fault into the circuitry. The success of laser fault injection depends on several factors such as the wavelength, power, and exposure time of the incident photons [21].

b) Thermal Laser Stimulation: Methods that use thermal laser stimulation (TLS) are widely used for defect localization. TLS can occur when laser photons with wavelengths greater than $1100nm$ are incident on a device. Local heating caused by TLS introduces variations in resistance and generates an electromotive force (EMF) due to the Seebeck effect, which causes variations in device parameters such as voltage and current. These variations can be probed with techniques such as OBIRCH and thermally induced voltage alteration (TIVA) [8], [16]. During TLS, a voltage is supplied to bias the device and the current between the supply pins is monitored with a current pre-amplifier. The current between the supply pins is sampled and a computer generates a 2D map of device response by localizing the current variations in the circuit (see Fig. 1d).

Tab. I summarizes different optical attack methods and their objectives.

D. The Chip Backside Accessibility

In modern SoCs, the optical path of photons are obstructed at the front side of the die due to the presence of a large number of interconnecting metal layers. The backside, which lacks such metal layers, is extremely vulnerable to optical attacks on the die or exposed silicon chip. In a normal packaged chip (DIP or BGA), the packaging polymer or ceramic prevents access to the backside of the chip. and also a presence of heat sink copper shield makes the sample preparation (wet etching or mechanical polishing) more challenging. Nonetheless, the flip-chip substrate is typically covered with a metallic lid, which can be easily removed to expose the silicon die.

E. Necessary Equipment

A successful optical attack requires a laser source with variable wavelengths for laser stimulation and an InGaAs detector for photon emission analysis. Recent advancements in FA instruments have increased the availability of various microscopes to facilitate optical analysis techniques. Laser scanning microscope (LSM) and photon emission microscope (PEM) are used for laser stimulation analysis and PEA. In addition, several FA instruments have incorporated the LSM and PEM to provide a single solution for all optical debugging techniques. These microscopes are available in different industrial/academic labs and an adversary can rent them for a few hundred dollars per hour.

TABLE I: Techniques, measurable units, and objectives of different optical attack methodologies

Type of Optical Attack		Technique	Source	Observable Parameter	Objective
Photon Emission Microscopy		Photon emission analysis (PEA)	Transistor switching activity	Emitted photons from transistor	Probing/Activity of transistor
Electro-Optical Analysis		EOFM/EOP	1.3 μm laser stimulation	Modulation in laser amplitude/phase	Optical Probing
Laser Stimulation	PLS & TLS	Laser fault injection	$\lambda <$ 1.1μm laser stimulation	Change in voltage/current	Bit flip
	TLS	OBIRCH,TIVA, SDL,RIL,etc.	$\lambda >$ 1.1µm laser stimulation	Voltage/Current variation: 1. Resistance change 2. Seebeck effect	Short/open localization

IV. Security Threats of Optical Attack

An SoC must adhere to information security requirements which includes protecting the availability, confidentiality, and integrity of the assets [22]. The confidentiality and integrity of the assets can be considered compromised, since the information on the IC can be raided from the chip's backside with the attacks described in section III. Therefore, ignoring the threat from optical attacks, leave a wide attack surface for an adversary to reveal the assets stored in the SoC.

For example, cryptographic cipher keys such as AES, RSA etc. stored in Flash and EEPROM have been exposed by attacking the control circuitry or memory cells using LFI and PEA [5], [23], [24]. Flash and EEPROM are widely used as on-chip memory to store other types of sensitive information as well such as soft IP, algorithms, and authentication keys. Similarly, the contents of battery backed RAM (BBRAM), an NVM widely used in FPGA, can be read by applying TLS from the backside of the chip [8]. Furthermore, volatile memory such as static random access memory (SRAM) is also susceptible to attacks such as PEA, LFI and TLS [7], [8], [25]. In SoC architecture, SRAM is the cache memory, which stores the immediately-used data. Cache can therefore be considered a main point of interest (PoI) for attackers and all security developers.

Protecting Key-storage from optical attacks is another security challenge in ICs. One time programmable (OTP) memory, such as electrical fuse (efuse) and anti-fuse, is implemented as a secured key-storage method. An adversary can localize the efuse by using OBIRCH or scanning electron microscopy [26] and then expose the key value [27]. Physical unclonable functions (PUFs), are another method for secure key-storage in modern SoCs. PUF generates keys from intrinsic device properties. Although PUF is tamper-evident against invasive physical attacks, it is vulnerable to non- and semi-invasive attacks such as PEA and LFI [19], [28].

Recent studies have shown that logic gates and registers can be optically probed in a contact-less manner [6], [6], [9], [9]. The values stored in the logic gates can be revealed with PEA and even changed with a laser beam with energy greater than the band gap energy of silicon [17]. For example, optical methods can be used to localize the flip-flops in the chip by using the clock frequency from the data-sheet (see Fig.2a). Once the flip-flops are localized, an adversary can extract the stored values or change the logic state of the logic gates of a modern AI or neural network chip to manipulate the weights or biases [21], [29]. Similarly, PEA and EOFM can also be used to locate AES modules [6], cores, cache locations (see Fig. 2b) [30], and signal propagation paths [6], [25]. In addition, reflected light image from the backside of the chip makes it easier to differentiate between distinct modules on the chip (see Fig. 2c).

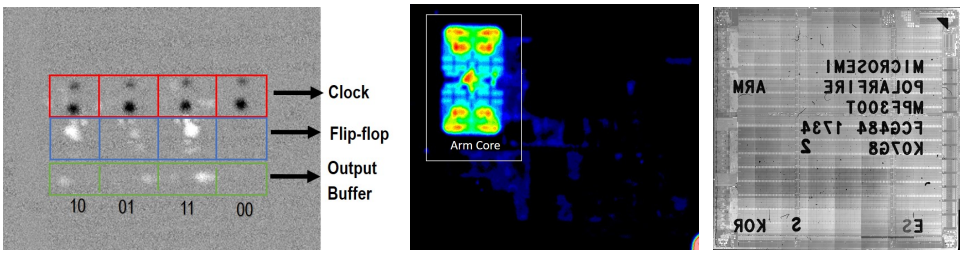
Since such semi-invasive attacks extract assets through run-time monitoring of silicon implementation, optical attacks are effective against the standard security policies meant to protect the assets. For example, in a modern processor, a secured communication environment between software and hardware is developed through a "secure boot-up" policy. Since hardware is considered root-of-trust, security assets such as efuse configuration, cryptographic keys, post-silicon observability information, etc. are initiated from embedded memory during the secured boot-up [31], [32]. However, embedded memory, cache, and registers used for storing information can be probed even during the secure boot-up process. Hence the security mechanism of the entire device is compromised. In summary, sensitive information protected by "secured" embedded memory can no longer be considered "read-proof" against optical attacks.

V. Threat Model and Attack Approach

In this section, we present the threat model and attack approach for various optical attacks. A comprehensive threat model identifies the assets of the device; objective, capabilities, and information available to an attacker; and the attack approach adopted by an adversary. The objective of an adversary is to acquire the assets described in II-B. Although an attacker may adopt any asset extraction approach, e.g., side-channel analysis, electrical probing etc., optical attacks allow direct access to sensitive information through the backside of the chip.

For successful asset extraction using an optical attack, an adversary must complete the following steps ;

a) Acquiring the target device and defining the asset: In optical asset extraction methodologies, the attacker needs



(a) (b) (c)

Fig. 2: (a) Localizing the flip-flop location using clock frequency and optically probing the stored values; (b) the ARM core in a commercially available chip localized from PEA [30]; (c) The internal structure of a Microsemi FPGA collected with a 1.3μm laser.

physical access to the chip. Often, the chip can be easily acquired from the open market or any untrusted entity in the semiconductor supply chain. Depending on the objective of the attack, an adversary can target the assets on the chip as well as the associated IP.

b) Localizing the Point of interest (PoI): The PoI localization approach is defined by the capabilities and information available to the adversary. If the attacker is an untrusted foundry that has access to the GDSII file, reverse engineering the netlist is sufficient for target localization. An end user with full-blown reverse engineering capabilities, e.g., a reverse engineering entity such as TechInsights (formerly ChipWorks), would adopt an invasive reverse engineering approach to find the PoI. In a non-reverse engineering approach, an attacker can analyze the chip with laser scanning microscope (LSM) or photonic emission microscope (PEM) and then localize the assets with EOFM or PEA. Such an approach is faster, more accessible, and less expensive than a reverse engineering approach because it only requires access to a few FA instruments.

c) DUT Preparation and Optical Attack Approach Selection: Sample preparation of flip-chips is relatively easy as it only requires lid removal and surface cleaning with a reagent such as iso-propyl alcohol (IPA) while sample preparation of regular DIP/BGA chips requires package removal by mechanical polishing or acid etching [15]. The resolution of laser stimulation and photon emission can be improved by further thinning the substrate with mechanical polishing. Depending on the PoI, e.g., cache or register, and available information, an attacker can then choose the appropriate approach.

VI. Countermeasures against Backside Optical Attacks

At present, there are two main approaches in the literature to protect the IC backside from optical probing: prevention and detection. The preventive strategy hinders asset extraction from adversaries by methods such as offering a protective shield at the RoI, hiding the parameters of circuit (e.g. clock randomization, obfuscation, etc.), and/or offering error correction techniques against fault injection attacks. The detection strategy monitors for attacks (e.g. by sensing disturbances such as photons, current and temperature etc.) and raises an alarm (e.g. by register zeroization, device reset, or shut down) to safeguard the system under attack. If the the prevention mechanisms are circumvented, attackers can readily probe the contents of the IC, as the detection mechanisms merely raise the alarm after the chip has been compromised. As a result, a stand-alone strategy is not sufficient to protect assets within an IC. Several countermeasures against backside optical probing have been developed over the past few years. These solutions can be classified into three categories, based on the level of abstraction: 1) material based solutions, which involve protection mechanisms such as incorporating a protective shield on the silicon die or altering the characteristics of the backside silicon to make it opaque to laser attacks. 2) device layer (or devices) based security techniques, which use existing CMOS process to implement an electrically or optically active device layer to obstruct or detect any physical attacks. 3) circuit-based solutions, detect probing attacks by monitoring the electrical parameters of the circuits such as delay, glitch, current, or temperature. Additionally, circuit-based solutions can also prevent attacks by obfuscating circuit parameters such as clock frequency. The coverage region of these anti-probing solutions on different types of ICs is summarized in Table II.

TABLE II: Anti-Probing Solutions for Different Types of IC Types.

Types of Circuits	Type of Anti-Probing Solution		
	Material	Devices	Circuits
ASIC / Digital ICs	Yes	Yes	Yes
Memories	Yes	Yes	Maybe
FPGAs / Prog. SoC	Yes	Yes	Yes

A. Material Based Protection Mechanism

Material-based protection mechanisms block or detect infrared laser probing to safeguard the backside transistors. The practice of material-based protection of sensitive information within ICs is not new. Historically, its origins can be traced back to almost half a century ago when the first on-chip, material based countermeasure was proposed by Keister et. al for the protection of electronics used in the US Navy weapons and systems [33]. Keister's invention involved the use of a thin film of perfluoropolymer and metal, which

produced a pyrotechnic reaction when adversaries attempted to de-package the chip [33]. This self-destructing mechanism prevented reverse engineering, recycling, and repair by enemy forces. Keister solution was appropriate for electronics used in war but not for commercial applications because of its violent nature. Hence,in 1993, Camilletti et. al developed a less violent alternative using a tamper-proof coating [34]. Camilletti utilized a silica resin layer, which is a hyper-oxidizing material on the substrate, to protect the IC as a strong shield. The silica is oxidized when the circuit is analyzed during reverse engineering processes such as decapsulation, cross-sectioning, wet (acid/base) etching, or dry etching (plasma, reactive ion, or focused ion beam [35]). The oxidized fillers release heat, which destroys the substrate and prevents further attacks.

Due to the self-destructive nature of the above-mentioned countermeasures, their application in consumer electronics are restricted. As a result, researchers have shifted to less disruptive methods. For example, in 1993, Byrne introduced a tamper-resistant structure that protects the active circuitry from disassembly and only damages the underlying IC layers when an adversary attempts to remove it [36]. Similarly, in 1997, Candelore proposed an anti-tamper shield that physically separates the electrically active parts (such as the bond wire) from important circuit modules (such as memory and CPU) [37]. An effort to remove this shield will harm the wire connections, which results in open circuits that prevent the chip from working. Most of the above methods have concentrated on protecting the overall chip, with a significant focus on metal layers, in order to avoid any type of electrical testing or reverse engineering. In 1999, Kommerling et. al suggested a low frequency sensor to protect smart card processors from laser interferometer guided focused ion beam attacks [38]. In 2006, Kommerling also proposed an encapsulation circuit utilizing a light source that creates a distinctive interference pattern on the chip material, which is further used to produce a unique cryptographic key [39]. Any efforts to tamper with the package will alter the interference pattern, which changes the key. The drawback of this method is that it requires a transparent encapsulant that is further enclosed with a reflective exterior package. Thus, Kommerling's light source method cannot be implemented in flip chip based FPGAs and programmable SoCs. Also in 2006, Tuyls et. al proposed a read-proof protective coating consisting of TiO_2 and TiN particles in an aluminophosphate matrix [40]. The protective coating makes the IC opaque to laser light, hardens the exterior structure to prevent wet etching attacks on the silicon die, and also introduces randomness in the layers similar to PUFs (see Fig. 3). Such randomness can be used to create a unique fingerprint, which can then be used by a cryptography module to generate a unique key, which is never stored on the chip itself. Their countermeasure is immune to the backside physical attacks electrical probing using FIB, but this cannot prevent optical attacks.

Material-based security solutions involve a physical protective shield. This makes it difficult to implement in a compact electronics system (e.g. smart cards), systems that require extra cooling (e.g. graphic cards and CPUs), and in next generation packaging methods such as flip chips. As the semiconductor technology advances toward smaller feature size, low power designs, and compact IC packages, standard material based countermeasures are becoming obsolete and must be updated. To fill the technological gap created by materials based backside protection countermeasures, device layer based protection methods have been developed.

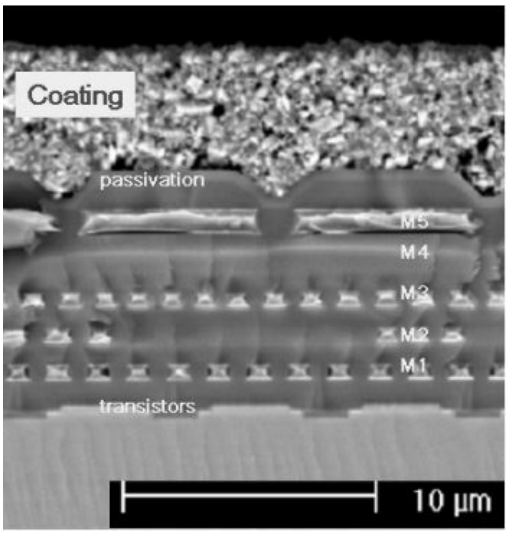


Fig. 3: Cross-sectional SEM image of a coating PUF IC. The sensors are located underneath the passivation layer i.e. M5 [40]

.

B. Device Layer Based Protection Mechanism

Device layer based solutions involve using existing semiconductor process and device layers to protect the backside of the IC. Since no extra material or shield is required outside the IC. In this manner, ordinary circuit applications are preserved and the device layers remain accessible for failure analysis.

Integrated circuit structures include multiple layers, the diffusion region to create circuit elements such as transistors, the first highly conductive metal layer connected to diffusion regions to interconnect transistors, a distribution of power and clock across the chip. Metal layers past the first layer are used to connect other components on the chip, depending on the CMOS process used for design. In 1989, Gilberg et. al proposed the idea of using device layers to safeguard an IC [41]. They proposed the idea of secured circuit areas by defining them with diffusion and the first metal layer to route, store and process secure data, while the second metal layer at the top provides a shield for secured areas by carrying a pre-determined signal that is essential for normal working of protected secured areas. For example, in the case of volatile random access memory (RAM), metal layer-2 acts as a shield to the first conductive layer and carries power as a predetermined signal. when an adversary removes this shield, the power supply is also removed, triggering the deletion of

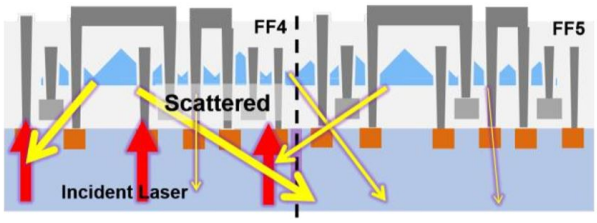


Fig. 4: Incident laser beam is scrambled by nanopyramids to disturb the LVP signal for optical probing. [46]

the secure data. Gilberg's approach prevents the inspection of circuits with failure analysis instruments such as scanning electron microscope (SEM) and physical probing, but with the advancement of a focused ion beam, the adversary can dig a trench to access the metal layer-1 or diffusion layer and reconnect the second metal layer by deposition. Hence this approach has overlooked backside attacks and can be circumvented with in-situ plasma FIB and probing techniques.

In 2012, Zachariasse proposed a protection method against backside attacks that utilizes the p-n junction of the diffusion regions located at the backside of the chip [42]. In accordance with semiconductor physics, forward-biased p-n junctions can illuminate (light-emitting diode-LED mode) the backside silicon whereas reverse-biased p-n junctions can detect (photodiode mode) any light reflected from the backside substrate. At the end of the substrate, a light modulating structure was added to detect signal changes due to tampering from the backside. Thus, Zachariasse's counter-measure can protect the backside from physical tampering, but it does not protect the chip from contact-less optical attacks, which do not require sample preparation. To improve Zachasiasse's detection mechanism, Amini et. al [43], [44] proposed adding an optically active layer. This layer is coated with ITO-Ag-ITO, which introduces angle-dependent reflection for backside attack detection. The properties of the optically active layer and the reflecting state of the coated layer depend on the coating process. Such layers are difficult to circumvent if the properties are unknown by the attackers. Amini also added an extra layer, which is opaque lasers, to increase robustness against backside optical attacks. In 2018, Shen et. al suggested an approach to prevent LVP attacks by scrambling the reflected laser signal with a nanopyramid type structure silicon layer (Figure 4). These structures can be placed in Fin-FETs or planar transistors and the fabrication is compatible with existing CMOS process without the addition of an extra mask. Also in 2018, Borel et. al proposed a packaging method that includes a backside shield with deeply-etched blind holes and a metal lining [45]. The etched holes weaken the chip, leading to damage if mechanical stress is introduced by polishing or plasma FIB. The metal layer, which is opaque to IR, which prevents the laser fault injection attacks. There is no discussion about the shield's resistance to acid etching or its applicability to flip chips.

C. Circuits Based Protection Mechanism

So far, several material and device layer based solutions have been presented, but many can be readily circumvented and have drawbacks such as the need for an external enclosure. Thus, the field of IC asset protection had advanced toward circuits based protection mechanisms, which are integrated during the IC design process. Such early integration of the protection mechanisms are more cost-effective and secure from an informed attackers such as untrusted foundries, which have control over the fabricated process and have access to the design layout and test vectors [47].

The possible ways of implementing a countermeasure that satisfies the above described requirements are to design circuits that are resilient and tolerant to fault injection, or to introduce a circuit level primitive / sensor to detect disturbances caused by optical attacks. For example, in TLS and EOP attacks, laser photons can cause local temperature increases at probed regions and, in fault injection (LFI) attacks, current and clock variations can cause timing delays. In 2011, Jagannathan et. al proposed a Single event upset (SEU) tolerant flip-flop circuit design approach [48]. The 8-transistor SEU-hardened storage cell, known as the Quatro latch, is resistant to faults caused by heavy ions, neutrons, and alpha particles . In 2014, Han et. al introduced a Quadded logic (QL) technique based on a redundancy approach using backup transistors [49], [50]. This solution can correct the injected faults by switching them from critical to sub-critical status. Further, in 2016, Dierickx proposed a transistor-level fault tolerant design that can resist radiation [51]. Also in 2016, He et.al proposed an attack detection method using the digital logic design of the ring oscillator to detect frequency disturbances triggered by LFI attacks [52]. They used a phased locked loop (PLL) circuit to monitor the RO output ripples, if there is a change beyond a set threshold detected, it can raise raise the 'alarm' signal to activate the defense reaction. In 2017, Tajik et. al introduced another circuit based countermeasure using PUF (physically unclonable function) based security monitoring (PUFMon) to detect laser attacks [53]. The PuFMon uses a combination of RON (ring oscillator networks) and RO sum PUFs to detect change in frequency of ring oscillators by monitoring the state of counters of two adjacent ROs and RO sum PUFs (see Fig.5). Tajik's study demonstrated the effectiveness of the sensor module on backside probing attacks and other fault injection attacks such as clock manipulations and reconfiguration in Altera FPGA.

In 2015, Manich et. al proposed a circuit-based countermeasure that detects backside polishing attempts [54]. Backside polishing is a sample preparation step commonly used before low power laser attacks and FIB attack, which can disable/tamper a sensor circuit in a passive state or circumvent any device layer based countermeasures [43], [46]. Manich's backside polishing detector (BPD) utilizes through silicon vias (TSV) to monitor their parasitic capacitance, assuming that the circuit is designed to operate on the MHz frequency range so that other parasitic effects such as resistive and

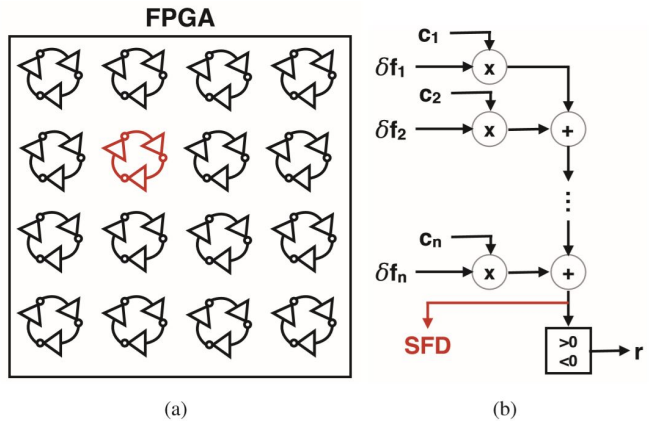


Fig. 5: (a) Ring oscillator network to detect LVP attacks (b) The modied architecture of the RO sum PUF network uses PUF output to detect optical attack. [53]

.

inductive effects are negligible. The capacitance of the TSV decreases when the substrate is thinned (due to polishing attempts) and can be monitored with a delta meter to create a unique signature of the unpolished chip (see Fig. 6). Though this countermeasure is a relatively robust solution for an electrical probing attacks, but a backside optical probing can be performed in most of the flip chip IC without any polishing. Also, the TSV process is very complicated and costly for low cost, bulk manufacturing of ICs like smart cards, low end FPGAs that are still fabricated in big transistor technology nodes.

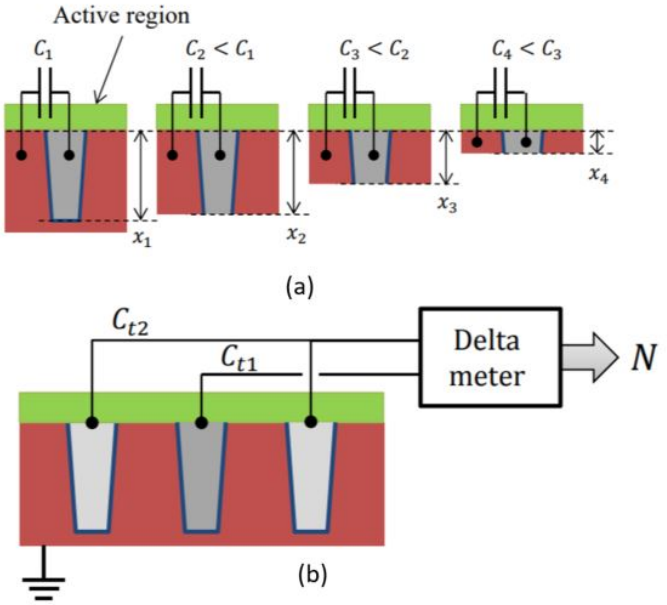


Fig. 6: (a) Parasitic capacitance of TSVs is proportional to the thickness of the silicon substrate. (b) Principle of BPD: Thickness detection by comparing capacitance [54]

.

VII. Conclusion and Future direction

We analyzed several different countermeasures to protect chip assets from optical backside attacks and conclude that there is no universal method. Thus, it is vital to develop an attack vs. countermeasure matrix to assist IC designers to incorporate more robust IC security measures without impacting the cost, applicability, and reliability of the device. Table III summarizes the different types of optical attacks and the suggested countermeasures. Materials based methods, which involve protective shields, can be circumvented. Moreover, protective shields are incompatible with modern IC packaging techniques and compact systems such as IoT devices. Device layers based protection can prevent photon emission up to a certain extent by photo-sensing diodes or doping the backside with an optically inactive device layer, but these countermeasures can be bypassed with mechanical polishing or dry etching (Plasma FIB). Circuit-based countermeasures use diffusion area elements (transistors and logic gates) to detect/prevent optical attacks and are difficult to circumvent without impacting the normal functionality of the circuit. However, such countermeasures may introduce additional timing delays and consume additional resources such as silicon area, power, and cost.

TABLE III: Backside Optical Attacks and Countermeasures .

Type of Optical Attack		Countermeasure		
		Protective Shield	Device Layers	Circuits Sensors
Photon Emission Microscopy		No	Yes	Yes
Electro-Optical Probing		Partially	No	Yes
Laser Stimulation	PLS & TLS	No	Partially	Yes
	TLS	No	Partially	Yes

As semiconductor technology progresses, circuit-based countermeasures are becoming more appealing to the secure IC design community for optical attack detection and prevention, as compared with materials and device layer based methods. An experienced designer must strategically determine the locations and the activation timing (start-stop and duration) of the sensors in order to account for trade-offs such as increased cost and reduced circuit performance. This practice is consistent with the notion of design for security and opens new avenues for research.

References

[1] R. Zafar, "Apple A11 Bionic Chip Has 6 Cores 4 Billion Transistors And 70% Faster Multi-Thread Workloads."

[2] M. T. Rahman, Q. Shi, S. Tajik, H. Shen, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, "Physical inspection & attacks: New frontier in hardware security," in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*. IEEE, 2018, pp. 93–102.

[3] G. K. Contreras, A. Nahiyan, S. Bhunia, D. Forte, and M. Tehranipoor, "Security vulnerability analysis of design-for-test exploits for asset protection in socs," in *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2017, pp. 617–622.

[4] Y. Chen, H. Chen, X. Zhang, and P. Lai, "Failure localization methods for system-on-chip (soc) using photon emission microscopy," in *Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE, 2013, pp. 591–594.

[5] 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.

[6] 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.

[7] 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.

[8] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, "Key extraction using thermal laser stimulation," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 573–595, 2018.

[9] M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, and N. Asadizanjani, "The key is left under the mat: On the inappropriate security assumption of logic locking schemes," Cryptology ePrint Archive, Report 2019/719, 2019, https://eprint.iacr.org/2019/719.

[10] ""flip-chip" interconnections," Sep 1963. [Online]. Available: https://archive.org/stream/Aviation_Week_1963-09-23#page/n47/mode/1up

[11] By, "Flip chip technology market 2019 global analysis, industry growth, sales revenue, competitive landscape, future trends and comprehensive research study till 2023," Apr 2019. [Online]. Available: https://www.marketwatch.com/press-release/flip-chip-technology-market-2019-global-analysis-industry-growth-sales-revenue-competitive-landscape-future-trends-and-comprehensive-research-study-till-2023-2019-04-15

[12] A. Arm, "Security technology-building a secure system using trustzone technology," *ARM Technical White Paper*, 2009.

[13] S. Ray, S. Bhunia, and P. Mishra, "Security validation in modern soc designs," in *Fundamentals of IP and SoC Security*. Springer, 2017, pp. 9–27.

[14] A. P. D. Nath, S. Bhunia, and S. Ray, "Artifact: Architecture and cad flow for efficient formal verification of soc security policies," in *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2018, pp. 411–416.

[15] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *arXiv preprint arXiv:1907.08863*, 2019.

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

[17] 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, 2014, pp. 528–534.

[18] W. M. Yee, M. Paniccia, T. Eiles, and V. Rao, "Laser voltage probe (lvp): A novel optical probing technology for flip-chip packaged microprocessors," in *Proceedings of the 1999 7th International Symposium on the Physical and Failure Analysis of Integrated Circuits (Cat. No. 99TH8394)*. IEEE, 1999, pp. 15–20.

[19] S. Tajik, H. Lohrke, F. Ganji, J.-P. Seifert, and C. Boit, "Laser fault attack on physically unclonable functions," in *2015 workshop on fault diagnosis and tolerance in cryptography (FDTC)*. IEEE, 2015, pp. 85–96.

[20] H. Photonics, "Emission Microscopy: Phemos-1000," https://www.hamamatsu.com/resources/pdf/sys/SSMS0003E_PHEMOS1000.pdf, accessed:2018-04-26.

[21] 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.

[22] S. J. Greenwald, "Discussion topic: what is the old security paradigm?" in *Proceedings of the 1998 workshop on New security paradigms*. ACM, 1998, pp. 107–118.

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

[24] S. Skorobogatov, "Using optical emission analysis for estimating contribution to power analysis," in *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2009, pp. 111–119.

[25] F. Stellari, P. Song, M. Villalobos, and J. Sylvestri, "Revealing sram memory content using spontaneous photon emission," in *2016 IEEE 34th VLSI Test Symposium (VTS)*. IEEE, 2016, pp. 1–6.

[26] N. Vashistha, M. T. Rahman, H. Shen, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, "Detecting hardware trojans inserted by untrusted foundry using physical inspection and advanced image processing," *Journal of Hardware and Systems Security*, vol. 2, no. 4, pp. 333–344, 2018.

[27] H. C. Chen, C. Y. Tsai, S. Y. Liu, Y. P. Chang, and J. C. Lin, "Defect localization and root cause analysis on e-fuse read reliability failure," in *ISTFA 2014: Conference Proceedings from the 40th International Symposium for Testing and Failure Analysis*. ASM International, 2014, p. 304.

[28] 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.

[29] J. Breier, X. Hou, D. Jap, L. Ma, S. Bhasin, and Y. Liu, "Practical fault attack on deep neural networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 2204–2206.

[30] M. Dhwani, S. Tajik, D. Woodard, N. Asadi, and M. Tehranipoor, "On the physical security of ai accelerators," International Conference on Physical Assurance and Inspection of Electronics, 2019.

[31] A. Mundra and H. Guan, "Secure boot on embedded sitara™ processors," http://www.ti.com/lit/wp/spry305a/spry305a.pdf, accessed: 2018-09-30.

[32] B. V. Patel, "Method for securing communications in a pre-boot environment," Dec. 4 2001, uS Patent 6,327,660.

[33] F. Keister and J. Rust, "Pyrotechnic eradication of microcircuits," Apr. 3 1973, uS Patent 3,725,671.

[34] R. C. Camilletti, L. A. Haluska, and K. W. Michael, "Tamper-proof electronic coatings," Oct. 17 1995, uS Patent 5,458,912.

[35] M. Rahman, M. Dewan, A. Ahmed, and M. Chowdhury, "A time-dependent collisional sheath model for dual-frequency capacitively coupled rf plasma," *IEEE Transactions on Plasma Science*, vol. 41, no. 1, pp. 17–23, 2012.

[36] R. C. Byrne, "Tamper resistant integrated circuit structure," Nov. 29 1994, uS Patent 5,369,299.

[37] B. Candelore, "Anti-tamper bond wire shield for an integrated circuit," Jan. 19 1999, uS Patent 5,861,662.

[38] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors." *Smartcard*, vol. 99, pp. 9–20, 1999.

[39] O. Kömmerling and F. Kömmerling, "Anti tamper encapsulation for an integrated circuit," Feb. 28 2006, uS Patent 7,005,733.

[40] P. Tuyls, G.-J. Schrijen, B. Škorić, J. Van Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2006, pp. 369–383.

[41] R. C. Gilberg, R. M. Knowles, P. Moroney, and W. A. Shumate, "Secure integrated circuit chip with conductive shield," Jun. 12 1990, uS Patent 4,933,898.

[42] F. Zachariasse, "Semiconductor device with backside tamper protection," Jun. 12 2012, uS Patent 8,198,641.

[43] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, B. Szyszka, and C. Boit, "Assessment of a chip backside protection," *Journal of Hardware and Systems Security*, vol. 2, no. 4, pp. 345–352, 2018.

[44] E. Amini, R. Muydinov, B. Szyszka, and C. Boit, "Backside protection structure for security sensitive ics," in *Proceedings from the 43rd international symposium for testing and failure analysis*, 2017, pp. 279–284.

[45] S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Cledière, R. Wacquez, J. Fournier, J.-C. Souriau, G. Simon, and A. Merle, "A novel structure for backside protection against physical attacks on secure chips or sip," in *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)*. IEEE, 2018, pp. 515–520.

[46] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An optical scrambler against backside probing attacks," in *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*. ASM International, 2018, p. 280.

[47] Q. Shi, N. Vashistha, H. Lu, H. Shen, B. Tehranipoor, D. L. Woodard, and N. Asadizanjani, "Golden gates: A new hybrid approach for rapid hardware trojan detection using testing and imaging," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2019, pp. 61–71.

[48] S. Jagannathan, T. Loveless, B. Bhuva, S.-J. Wen, R. Wong, M. Sachdev, D. Rennie, and L. Massengill, "Single-event tolerant flip-flop design in

40-nm bulk cmos technology," *IEEE Transactions on Nuclear Science*, vol. 58, no. 6, pp. 3033–3037, 2011.

[49] J. Han, E. Leung, L. Liu, and F. Lombardi, "A fault-tolerant technique using quadded logic and quadded transistors," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 8, pp. 1562–1566, 2014.

[50] P. Schiefer, R. McWilliam, and A. Purvis, "Fault tolerant quadded logic cell structure with built-in adaptive time redundancy," *Procedia CIRP*, vol. 22, pp. 127–131, 2014.

[51] B. Dierickx, "Radiation hard design in cmos image sensors," in *Workshop on CMOS active pixel sensors for particle tracking. CPIX*, vol. 14, 2014.

[52] W. He, J. Breier, S. Bhasin, N. Miura, and M. Nagata, "Ring oscillator under laser: potential of pll-based countermeasure against laser fault injection," in *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2016, pp. 102–113.

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

[54] S. Manich Bou, D. Arumi Delgado, R. Rodríguez Montañés, J. Mujal Colell, and D. Hernández García, "Backside polishing detector: a new protection against backside attacks," in *DCIS'15-XXX Conference on Design of Circuits and Integrated Systems*, 2015.