BackMon: IC Backside Tamper Detection using On-Chip Impedance Monitoring

Tahoura Mosavirik and Shahin Tajik

Department of Electrical and Computer Engineering,
Worcester polytechnic Institute, Worcester, MA, USA
{tmosavirik,stajik}@wpi.edu

Abstract.
The expansion of flip-chip technologies and a lack of backside protection make the integrated circuit (IC) vulnerable to certain classes of physical attacks mounted from the IC's backside. Laser-assisted probing, electromagnetic, and body-basing injection attacks are examples of such attacks. Unfortunately, there are few countermeasures proposed in the literature, and none are available commercially. Those that do exist are not only expensive but are incompatible with current IC manufacturing processes. They also cannot be integrated into legacy systems, such as field programmable gate arrays (FPGAs), which are integral parts of many of the industrial and defense systems. In this paper, we demonstrate how the impedance monitoring of the printed circuit board (PCB) and IC package's power distribution network (PDN) using on-chip circuit-based network analyzers can detect IC backside tampering. Our method is based on the fact that any tampering attempt to expose the backside silicon substrate, such as the removal of the fan and heat sinks, leads to changes in the equivalent impedance of the package's PDN, and hence, scanning the package impedance will reveal whether the package integrity has been violated. To validate our claims, we deploy an on-FPGA network analyzer on an AMD Zynq UltraScale+ MPSoC manufactured with 16 nm technology, which is part of a multi-PCB system. We conduct a series of experiments at different temperatures, leveraging the difference of means as the statistical metric, to demonstrate the effectiveness of our method in detecting tamper events required to expose the IC backside silicon.

Keywords: Anti-Tamper · Flip-Chip Technology · IC Backside · Impedance Characterization · Physical Attacks · Physical Layer Security

1 Introduction

With the ubiquity of digital electronics in our daily lives, integrated circuits (ICs) now have access to more sensitive information and assets than ever before. The threats to the physical security of computer chips and countermeasures have been widely researched. However, the security of the system is still threatened by sophisticated physical attacks relying on failure analysis (FA) tools, which exploit the lack of protection on the chip's package backside to probe the data or interfere with the computation. The increase in the number of metal layers on the frontside of ICs, as well as the advent of new packaging concepts like ball grid arrays and flip-chip technologies, have triggered a paradigm shift in mounting these attacks from the IC backside. Photon emission analysis [TNH+14], laser fault attacks [TLG+15], laser-assisted probings [TLSB17, CCT+18, KKTS21, KGM+21], Electromagnetic (EM) fault injection [HMW+24], and body biasing injection (BBI) [TMOL12] are examples of such backside attacks, which could bypass the conventional algorithmic countermeasures for recovering the secret.

In the early days of the IC backside attacks, silicon substrate polishing was the main requirement to perform both semi-invasive and fully-invasive attacks. While silicon removal is still required for fully-invasive attacks (e.g., microprobing [HNT+13] or e-beam probing [AKR+23]), many semi-invasive attacks have become non-invasive due to the expansion of the flip-chip packages (FCPs) as well as the availability of better light sensors, moving to longer laser wavelengths, and higher power laser or EM sources. As a result, the adversary only needs to detach the existing heat sink on the silicon substrate to access the backside silicon to perform the attack. The fact that the heat sink and other cooling components are usually not electrically connected to the chip has made detection of their removal challenging. Detecting silicon polishing has also been challenging, as no active electrical signal is available on the silicon substrate to monitor the IC's backside.

A few on-chip self-monitoring schemes have been introduced in the literature to either prevent or detect tampering with the IC's backside. The prevention schemes are usually based on distorting the optical path between a laser/emission microscope and transistors on the chip using laser engraved marks or opaque layers. However, similar to the detachment of the heat sink, such passive layers can be removed without any consequences. The detection-based solutions, on the other hand, attempt to detect the attack by creating interactions between the protection structure and electrical signals on the chip or printed circuit board (PCB) to detect removal. Due to the lack of electrical signals on the silicon backside, one class of solutions utilizes the optical interaction between transistors and an opaque layer [ABH+18, HAL+22]. Other solutions are based on tamper-sensitive secure enclosures to cover and prevent access to the IC package. Examples include optical waveguide physically unclonable functions (PUFs) [VWN+16], capacitive PUF enclosures [IOK+18], and anti-tamper radio enclosures[STZP22].

While these detection-based methods have been shown to be very effective against any backside tamper event, they are very costly and need a highly customized design, making them inappropriate for legacy systems. Moreover, they might be unusable for edge devices with small size, weight, and power matters (SWaP) requirements. Therefore, we ask the following research question: *Is it possible to have a legacy-compatible on-chip circuit-based sensor capable of monitoring the physical integrity of the IC backside without using any external sensors or enclosures?*

Our Contribution. Inspired by recently introduced power distribution network's (PDN) impedance monitoring solutions [MGST22, ZSS+23, MMST23, SMT23, MST23], we answer the above question positively. We rely on the fact that the functionality of network analyzers (the tools used for PDN impedance characterizations) can be emulated on FPGAs [Ior18, ZAB+18, MST23] by electrically stressing the PDN of the system with various frequencies and simultaneously measuring voltage drops for impedance estimation. As tampering activity on the backside of the IC's package will lead to changes in the equivalent impedance of the system's PDN, the continuous physical scanning of PDN at certain frequency bands will reveal whether the chip backside integrity has been violated. In [MST23], it was demonstrated that polishing the plastic QFP package of an FPGA from the frontside has an impact on the PDN's impedance. However, while the frontside tampering could have an impact on the power interconnects, it is not clear if tampering with disconnected components on the IC's backside has any impact on the PDN's impedance.

The primary goal of this work is to investigate the possibility of detecting backside tampering with cooling components before the adversary can access the silicon substrate and launch the attack. First, we will explain why tampering with existing components (e.g., fan, fin, and heat spreader) on the backside of the IC's package, despite not being connected to the IC's PDN, can affect the PDN's impedance profile. Moreover, we discuss in which frequency band impedance variations, caused by tampering, are expected. To monitor the PDN's impedance, we will realize a network analyzer on the FPGA fabric of a flip-chip packaged AMD Zynq UltraScale+ MPSoC manufactured with 16 nm technology, which

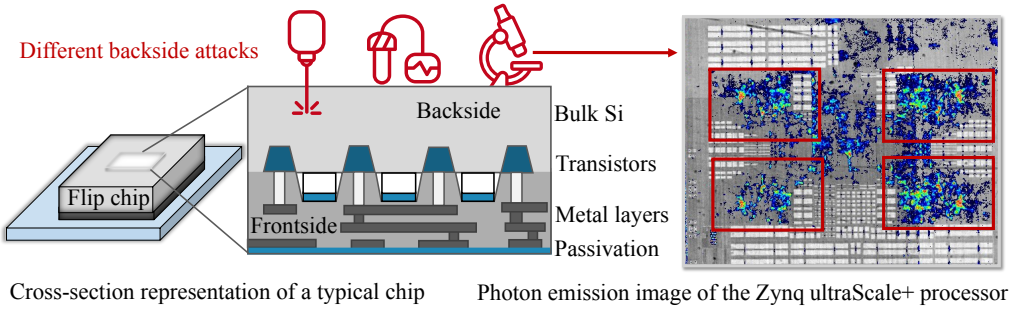


Figure 1: Illustration of how the silicon backside in FCP can be used as an attack medium.

is part of a multi-PCB system. After performing extensive tampering experiments (i.e., step-by-step removal of the components from the IC's backside) at various temperatures using a thermal chamber and deploying difference of means as a metric, we will validate our claims that impedance monitoring at specific frequency bands could reveal tamper events to the IC's backside.

Remark. The primary contribution of this work is the exploration of the impact of the package's backside on the PDN's impedance profile. On-chip (-FPGA) impedance monitoring has already been introduced in [Ior18, ZAB+18, MST23], and is not the main contribution of this work.

2 Technical background

In this section, we elaborate on silicon backside security, the system's PDN equivalent circuit model and its characteristics for a multi-PCB system to explain how different steps needed to access the IC backside would affect the impedance of the PDN at distinct frequencies. We also explain how backside tamper attempts impact the power and ground plane's equivalent impedance.

2.1 Silicon Backside Security

The IC backside is open for adversarial attempts on the silicon substrate, as conceptually depicted in Figure 1 in FCP. This figure shows the cross-section view of a typical flip-chip IC and possible backside attacks, including side-channel analysis (SCA) and optical attacks. The active side of the chip, which contains the electrical connections and metal layers, is flipped downward and directly attached to the silicon substrate. As seen in the figure, bulk silicon is the only medium between the IC backside and the transistors on the die. Passivation is a thin protective layer applied to the active region of the chip to prevent damage/interference and ensure long-term reliability. FCP configuration provides several benefits, such as shorter electrical paths, better thermal management, and higher packaging density compared to traditional wire bonding methods. However, it allows attackers to directly access the target core from the outside of the chip and conduct non-invasive SCAs and semi- or fully-invasive optical attacks to extract the cryptographic key through the silicon substrate [NMM21, MNS+20].

Although optical attacks can be performed from both the frontside and backside of the IC, the existing multiple interconnected layers on the IC frontside obstruct the optical paths from transistors to the surface of the chip. This makes the analysis of the target IC from its frontside more difficult, and therefore, attackers are more inclined to the IC backside to launch successful SCA/optical attacks. Therefore, it is of great importance to actively monitor the chip environment and verify if there has been an attempt to make unauthorized changes to the IC package medium in FCP. In the next subsection, we

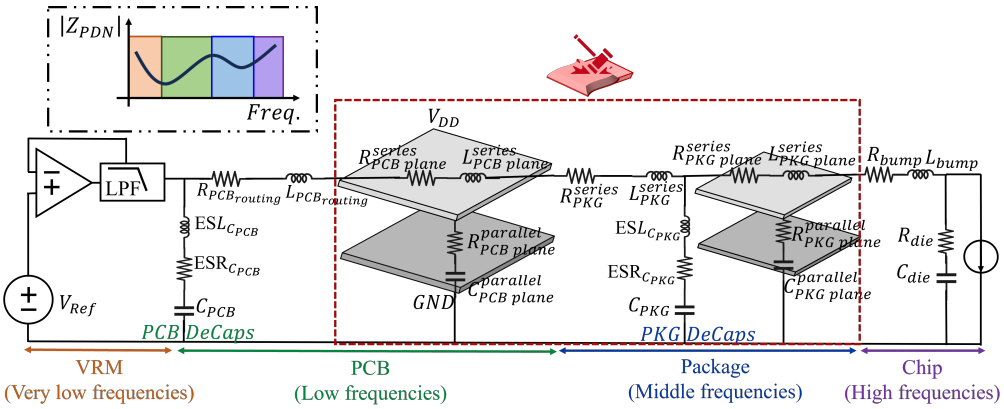


Figure 2: (a) Equivalent RLC circuit model of the power distribution network (PDN) of the system and the contribution of different parts of the PDN to the impedance over frequency. The area shown in dashed red color shows the circuit elements that IC backside tamper attempts will affect.

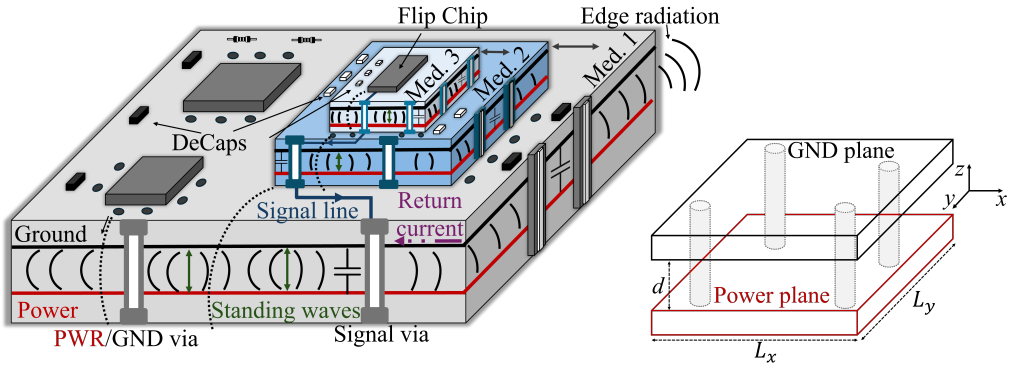
elaborate on how leveraging the cavity resonance model helps us to understand the PDN impedance behavior of a complex system when an adversary tries to gain unauthorized access to the IC backside.

2.2 Power Distribution Network (PDN)

The primary role of the PDN is to deliver a stable supply voltage to different components on the PCB, from the voltage regulator module (VRM) and passive networks to the power rails on each chip. In general, a typical PCB may have several voltage domains (i.e., VRMs) to support different supply voltage levels, load currents, and various chips/components [ZSS+23]. Each VRM is connected to its respective PDN by a passive distribution network comprising PCB traces, PCB planes (i.e., power and ground planes), and board-level decoupling capacitors. Power and ground planes (PGPs) act as low-impedance paths for the flow of current, effectively minimizing voltage fluctuations and ensuring stable power distribution to the components on the PCB. Overall, the PDN consists of interconnections in the PCB, package, and chip, which together provide the required target impedance over a specified frequency range. Each PDN component has a distinct contribution to the physical signature of the PDN at different frequency bands.

The PDN comprises off-chip and on-chip components, including bulk capacitors, PCB routing, ceramic capacitors, PCB planes, vias, package bumps, on-chip power planes, and transistor capacitance. The impedance contribution of these components to the overall PDN's impedance is different at various frequency bands. The voltage regulator's and off-chip components' impedance dominate the PDN's impedance at lower frequencies, while on-chip components contribute mostly to the impedance at higher frequencies, as shown in the upper left graph of Figure 2. The parasitic inductance on each capacitor is the primary cause of this impedance behavior. At high frequencies, an ideal capacitor behaves like a short circuit. However, the parasitic inductance on the capacitor's metals results in resonance at a particular frequency, causing it to become an open circuit at very high frequencies. Smaller capacitors have less parasitic inductance and resonate at higher frequencies. As a result, as the frequency increases, all capacitors, from large to small, become open circuits and have less impact on the PDN impedance. The on-chip structures dominate the PDN impedance at higher frequencies due to their smaller dimensions.

Every element in the PDN contributes to the impedance profile, with some elements dominating the PDN's performance in certain frequency ranges [SB17]. The package circuit components are closer to the IC and are effective in the middle-frequency range [ZBC+19].



(a) (b)

Figure 3: (a) Simplified illustration of a multi-PCB system (the heatsinks and fan module are not shown in this figure for simplicity); (b) Power and ground plane (PGP) pair isometric view.

In case of an IC backside tamper event, we can expect a change in the impedance value in the middle-frequency ranges, and thus, scanning the impedance of this region can reveal the backside tamper events with more confidence. The area shown in dashed red color in Figure 2 shows the equivalent circuit elements that will be impacted by possible tamper attempts when an adversary tampers with the IC backside silicon. As seen in this figure, there would also be an impact on PGPs equivalent series/parallel resistance, capacitance, and inductance, as well as package parasitics.

2.3 Power and Ground Planes (PGPs)

Systems that incorporate FCP can be composed of multiple PCBs where each PCB can host different subsystems, and they are interconnected to form a complete system as depicted in Figure 3a. Assuming a thermal management module exists on the flip-chip in Figure 3a, there would be multiple mediums (i.e., PCBs). Each medium has its own application-specific voltage domain, and consequently, its own PDN. Generally, each PDN is composed of multilayer parallel PGP layers. These layers are connected to the power/ground pins of IC chips and decoupling capacitors pads through vias in each medium as depicted in Figure 3a.

Signal routings/vias (signal, power, and ground) create discontinuity return paths throughout the PGPs. These return paths (an example of such return path is shown in purple color in Figure 3a) create a strong electric field that propagates along the edges of the PGPs [SZW+14]. A major effect of the PGPs is their behavior as EM resonant cavities, where the insulator's dielectric constant and the cavity's dimensions determine the resonance frequency [LTH+95]. When excited at the resonance frequency, the planes become a significant source of resonance peaks in the package and the board and also can act as a source of edge-radiated field emission [SPK+14], which would result in the coupling between the PGPs and their surrounding medium. To be more specific, the created standing waves in the cavity at resonance can produce significant coupling to neighboring circuits and transmission lines [SKNL04, PLKK03]. Any tampering attempt on the IC backside silicon (e.g., heatsink removal) would impact this coupling and, consequently, affect the impedance profile at the resonance peaks.

The behavior of the multi-PCB system shown in Figure 3a can be explained using the cavity model, particularly if the interaction between the PCBs and their environment in case of the IC's backside tampering attempts needs to be analyzed. This model can be employed to understand the behavior of enclosed structures with EM waves. In the case of a multi-PCB system, each pair of PCB's PGP can be considered a separate cavity within

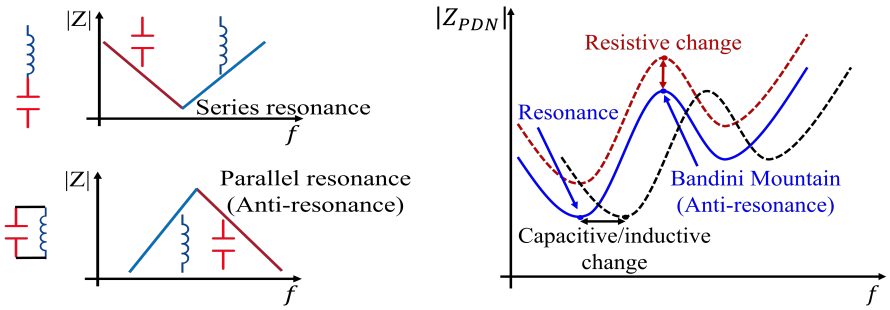
the overall enclosure. The cavity model can be leveraged to trace back the root cause of the impedance profile behavior of each medium individually, as well as the interactions between them. The cavity geometry can be modeled as a planar circuit based on the cavity model with dimensions of L_x and L_y along the x and y directions [KSF+11, RKF+09]. The spacing between the plane pair is d along the z direction and is filled with a dielectric layer with a relative permittivity and permeability of ε_r and μ_r, respectively. The following equation refers to the frequency of the resonances/anti-resonances generated on the PGPs for an open-ended PCB of size $L_x \times L_y$ [LTH+95]:

$$(f_{res})_{mn} = \frac{1}{2\pi\sqrt{\varepsilon_r \mu_r}} \sqrt{\left(\frac{m\pi}{L_x}\right)^2 + \left(\frac{n\pi}{L_y}\right)^2}, \tag{1}$$

where c is the speed of light in free space and m and n refer to integers representing the mode numbers along the x and y directions, respectively. Please note that modes refer to the different patterns of EM waves that can exist within the cavity. Multilayer PGPs can be decomposed into blocks so that each block contains a pair of parallel planes. Figure 3b shows a pair of each medium PGPs where these two thin metal layers separated by an electrically small distance (d) form a cavity.

As seen in equation 1, these modes are determined by the geometry and dimensions of the cavity. Each mode corresponds to a specific resonance frequency at which the cavity can efficiently store and exchange energy with the EM field [RWVD94]. The system impedance peaks depend on the resonance mode, and the resonance frequency is determined by the mode number, dielectric constant of the insulator, and physical size of the planes [RWVD94]. At the plane resonance frequency, the power distribution impedance reaches its highest value, with the maximum value dictated by the losses in the structure. When the adversary intends to access the IC backside, he/she should take some preliminary steps, such as removing the fan and/or heatsink module. These changes to the surrounding environment of the IC backside would impact the material's EM properties such as ε_r and μ_r (typically due to the increase in the IC's temperature as a result of fan and/or heatsink removal) and geometrical features of the cavities formed inside each PGP pair, resulting in a change in the overall impedance especially at PDN resonance frequencies. External package-level tamper attempts can also change the propagating modes inside each pair of PCB's PGPs, as any tamper event can introduce disturbances in the EM environment surrounding the system, leading to alterations in the impedance profile and propagation characteristics of the PGPs.

Cavity resonance frequencies can lead to a change in the magnitude and frequency of the impedance resonance maxima and minima. In some cases, including in a multi-PCB system, the impedance maxima has a significantly large impedance magnitude. These large PDN impedance peaks may not be present in a single-PCB PDN profile but arise due to the resonant behavior of the cavity formed by the multi-PCB system as there are multiple transitions between medium 1, 2, and 3 as depicted in Figure 3a. The heatsink/heat spreader structure can couple with the PDN, affecting its impedance characteristics. This coupling can result in a change in the impedance maxima and minima at frequencies corresponding to the resonant modes of the heatsink/heat spreader and their interaction with the PDN at different transitions between the media. Removing the heatsink can also lead to increased electromagnetic interference (EMI) radiations, which can induce currents in the PGPs, leading to changes in the resonance magnitude and frequency.



(a) (b)

Figure 4: (a) Series and parallel resonant components illustration ; (b) Frequency-domain impedance profile indicating resonance, anti-resonance, resistive, and capacitive/inductive changes.

3 Methodology

3.1 Threat Model

For our threat model, we assume that a security-critical IC (e.g., a root-of-trust, cryptographic chip, etc.) is being used in an untrusted field, and the attacker can physically tamper with its package. We aim to identify the IC's backside tamper attempt before the attacker can perform backside attacks. We further assume that the impedance profiles of genuine PDN samples at different temperatures have been acquired during an enrollment phase in a trusted field and stored on the same chip used for impedance monitoring. The attacker is interested in the secrets and assets stored on the IC. This IC is presumed to contain an embedded network analyzer circuit designed for impedance characterization of the PDN. If the security-critical IC is an FPGA, the network analyzer can be programmed as a soft IP into it along with other existing IP cores. Therefore, no additional modification is needed, and the golden impedance signature of the package remains intact. In a hostile environment, impedance characterization can be carried out before or during the runtime to validate the package's integrity and detect potential tamper events. Upon detection of a discrepancy between the measured and the golden impedance profiles, an anti-tamper response (e.g., key zeroization) will be executed. Furthermore, this self-contained impedance monitoring technique only works on powered-on systems.

3.2 Bandini Mountain

As discussed in section 2.2, PDN consists of different components in the PCB, package, and chip level, which forms an RLC equivalent circuit shown in Figure 2. Although the PDN RLC model is complex, traditional series and parallel circuit models can still be utilized to analyze PDN characteristics. A series-resonant circuit is defined by a capacitor and inductor that are connected in series. When the capacitive and inductive reactances are equal in magnitude and opposite in phase, the current is at maximum, resulting in an impedance minimum illustrated in Figure 4a. On the other hand, a parallel anti-resonant circuit is created when a capacitor and inductor are connected in parallel. In this case, however, it results in generating the minimum current throughout the parallel circuit, and an impedance maxima is created at the corresponding parallel resonance frequency. The frequencies at which these conditions occur are called the series and parallel (anti-resonance) resonance frequencies, respectively [FCAF12].

One of the important anti-resonance frequencies of PDN occurs at the parallel resonance of the on-die capacitance (C_{ODC}) and the package inductance (L_{PKG}). If we look at the PDN impedance profile from the die's perspective, the parallel resonance peak impedance

looks like a mountain, as shown in Figure 4b. This particular peak in the PDN impedance profile is called "Bandini Mountain" [SB17]. The frequency of the Bandini Mountain peak impedance is derived from the parallel resonant frequency as follows

$$f_{Bandini} = \frac{1}{2\pi\sqrt{L_{PKG}C_{ODC}}} \tag{2}$$

This feature is generally the most significant peak in the impedance profile and is also referred to as the PDN resonance noise, where the on-die capacitance resonates with package inductance [LSXR12, FCAF12]. The Bandini Mountain frequency is common in the MHz regime up to 100 MHz range. In this work, we leverage this undesirable but unique feature of the PDN to characterize IC's backside tampering activities. We later discuss the obtained results in Sect. 5, confirming that Bandini Mountain peak impedance can serve as a powerful distinguisher to differentiate between a tampered and genuine sample.

The value of the Bandini Mountain frequency depends on the value of on-die decoupling capacitance and package loop inductance. These values vary depending on the specific chip and package technology. Bandini Mountain's most important figures of merit (FOMs) are its characteristic impedance and peak frequency. The changes in these two FOMs can be used to explain the PDN impedance behavior when different layers on top of the IC's package get disconnected/removed to expose the silicon. The peak impedance value of the Bandini Mountain is mostly related to the quality factor of the C_{ODC} and L_{PKG} resonator, which is related to the equivalent series resistance (ESR) of the C_{ODC} and L_{PKG}. The package leads' ESR and the on-die capacitor's ESR often contribute to a high-quality factor (sharp and large impedance peak) for the resonant peak impedance with values approaching 1 Ω [SB17].

When the adversary disconnects/removes different layers of the cooling modules on top of the IC's package, there will be both resistive (along the impedance-axis) and capacitive/inductive (along the frequency-axis) changes at the resonance and anti-resonance frequency regions as shown in Figure 4b. While disconnecting/ removing the active part of the IC's backside cooling module has a significant contribution to the value of the Bandini impedance (the resistive part), removing the passive part of it would affect the combination of resistive, capacitive, and inductive parts of the PDN impedance profile. In the next section, we elaborate on how temperature influences different factors that contribute to the proposed method's detection confidence.

3.3 Thermal Effects on PDN Impedance

FCPs have high power densities due to the proximity of the active components, leading to significant heat generation. Heatsink structures dissipate heat generated by the electronic components, influencing the temperature distribution within the system. Generally, there are two types of heatsinks: passive (Fin) and active (Fan). Passive heatsinks rely on thermal radiation to dissipate heat, typically featuring a large surface area and fins to increase heat transfer with no power consumption. These heatsinks are made of materials with high thermal conductivity, such as aluminum or copper. They help spread the heat away from the flip chip, reduce localized hotspots, and maintain a uniform temperature distribution across the package. In FCPs with particularly high power dissipation, passive heatsinks alone may not be sufficient to adequately cool the components. Thus, active heatsinks are used in conjunction with passive ones to enhance heat dissipation by providing forced airflow over the fins, increasing heat transfer, and improving thermal performance. Active heatsinks need additional power to generate air/fluid flow and absorb heat. Combining both types of heatsinks ensures optimal thermal management and helps prevent overheating, ensuring the reliability of FCPs.

The impact of temperature on PDN impedance and loss is frequency-dependent. At higher frequencies, the "skin effect" becomes more significant, causing the current to concentrate near the surface of conductors. Elevated temperatures can exacerbate this effect, leading to changes in effective resistance and impedance at higher frequencies. As the temperature of the flip chip increases, localized hotspots may develop due to variations in thermal conductivity, power dissipation, and thermal management within the chip. These hotspots can create nonuniform temperature distributions across the chip surface and within the PDN. The non-uniform thermal distribution can also degrade the performance of the PDN by exacerbating losses in the system. Higher temperatures can increase resistive losses in the conductive elements of the PDN, leading to higher power dissipation and decreased efficiency. Additionally, elevated temperatures can affect the dielectric properties of materials in the PDN, potentially increasing dielectric losses.

Looking at the thermal management system from a security perspective, the first step that an attacker takes to launch an attack on the backside of the IC in a typical FCP is to disconnect/remove the fan. As a result, there will be nonuniform thermal distribution in the horizontal and vertical directions in the PDN. Thermal coupling and low vertical heat transferability would result in heat accumulation inside each block of the PGP pair on the die [SKP+22]. This increased temperature on the die will propagate through the entire system and, consequently, affect the electrical properties of the PDN, such as the resistance and capacitance of the PGPs and decoupling capacitors. Changes in temperature can alter the resonant frequencies of the PGP pair cavities, impacting PDN impedance at the Bandini Mountain frequency. Removing the fan may allow mechanical vibrations to propagate more freely, potentially inducing resonant frequencies in the system. Resonance effects and increased local temperature can increase "crosstalk" in the PDN by causing additional coupling between adjacent traces or components, which can perturb the impedance profile of the PDN [RWVD94]. It is worth mentioning that the phenomenon of crosstalk refers to the EM coupling between signal traces, power planes, ground planes, or other conductive elements within the PDN. When signals propagate along traces or planes, they generate EM fields that can induce voltages or currents in nearby conductors.

Temperature variations can affect parasitic elements within the PDN of the package, such as parasitic capacitance and inductance as well. However, temperature influences the resistive part of the impedance profile depicted in Figure 4b more significantly at "Bandini Mountain" frequency. After removing the active part of the heatsink, the attacker will proceed to get access to the IC backside silicon by removing the passive part of the heatsinks. This part of the heatsink is often attached to the component using thermal interface materials (TIMs), which can influence the electrical properties of the PDN, such as the effective relative permittivity (i.e., dielectric constant). Removing the fin heatsink/heat spreader can further change the electrical connectivity between the chip and the PCB, affecting the distribution of power and return currents and altering the impedance characteristics of the PGPs. Heatsink structures can also mitigate mechanical vibrations and resonance within the system.

3.4 Embedded Impedance Measurements

The VNA functionality can be implemented on the chip to enable self-contained monitoring of the system-level physical integrity [MST23]. A VNA on an FPGA consists of both active and passive modules, as shown in Figure 5. The active module stimulates the PDN of the system by drawing electrical current with different frequencies using power waster circuits (e.g., an array of interconnected configurable logic blocks (CLBs) [Ior18, ZAB+18], ring-oscillators (ROs) [GOKT18, PHT20], or Dual RAM collisions [ATG+19]). The activation frequency and consumed current of power waster circuits are controlled by a sinusoidal current modulator. The passive module, on the other hand, measures the voltage drops using on-die voltage sensors and other analog-to-digital (ADC) circuits, such as ROs or

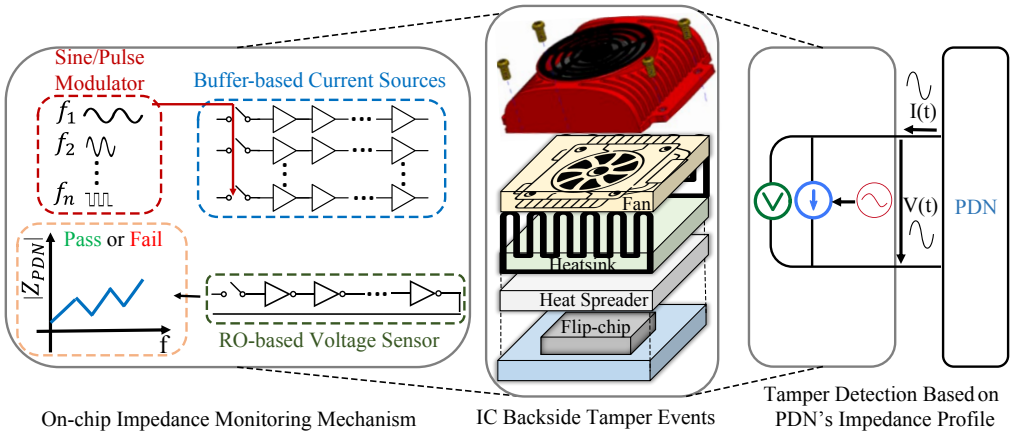


Figure 5: Block diagram of an embedded VNA on FPGA and "BackMon" tamper detection methodology (the red fan cover figure is taken from the Kria K26 SOM thermal design guide document in [Xila]).

Time-to-Digital converters (TDCs), utilizing the FPGA's resources [MLS+20]. Having the amount of current consumption and voltage drop at hand, the impedance value of the PDN seen by the logic circuits of the FPGA fabric at a specific frequency can be obtained.

Existing FPGA-based VNA variants employ similar power-wasting circuits based on buffer/inverter chains [ZAB+18, Ior18]. However, they use different voltage drop measurement circuits, namely TDC-based ADCs [ZAB+18] and RO-based ADCs [Ior18]. We use an RO-based ADC in this work, and thus, focus on how the frequency changes in a RO, measured by on-chip binary counters, can be converted to impedance values. Activating the power-wasting circuit on the core voltage plane at frequency f_i generates a sinusoidal current over time ($I = I_0 e^{j2\pi f_i t}$) through the PDN, which causes sinusoidal voltage variation ($V = V_0 e^{j2\pi f_i t + \phi}$) on the PDN with lagging in the phase. In this case, the impedance of the PDN at frequency f_i in the Polar coordinate representation is given by Ohm's law as $Z_{PDN} = V/I = (|V|/|I|)e^{\phi}$. Using the Cartesian representation, the impedance can be written as a complex number as $Z_{PDN} = R_{PDN} + jX_{PDN}$, where the real part R_{PDN} of impedance is the resistance and the imaginary part X_{PDN} is the reactance caused by the capacitance and inductance of the system. While R_{PDN} is frequency-independent, X_{PDN} is a function of frequency. The magnitude of the PDN impedance is $|Z_{PDN}| = \sqrt{R_{PDN}^2 + X_{PDN}^2}$. The magnitude of the PDN impedance can be approximated by considering only the difference in values of voltage and current when the power wasters are activated (V_{ON} and I_{ON}) or deactivated (V_{OFF} and I_{OFF}), cf. [Ior18, ZS18]

$$|Z_{PDN}| \approx \left|\frac{\Delta V}{\Delta I}\right| = \left|\frac{V_{OFF} - V_{ON}}{I_{OFF} - I_{ON}}\right| \tag{3}$$

On FPGAs, I_{ON} and I_{OFF} are constants and can be estimated either during the synthesis using the FPGA power estimators or using off-chip power monitoring modules. V_{OFF} equals the supply voltage of the FPGA V_{SUPPLY}. However, the V_{ON} is dynamic and approximated using the frequency of the RO-based sensor during the measurement. The frequency of an RO is proportional to the voltage drop on the FPGA, i.e., $f_{RO_{OFF}} \approx kV_{OFF} = kV_{SUPPLY}$ and $f_{RO_{ON}} \approx kV_{ON}$, where k is a constant. In this case, based on equation 5, the impedance magnitude at a given frequency can be written as follows, cf. [Ior18]

$$|Z_{PDN}| \approx \left|\frac{(\frac{f_{RO_{OFF}} - f_{RO_{ON}}}{f_{RO_{OFF}}})V_{SUPPLY}}{I_{OFF} - I_{ON}}\right| \tag{4}$$

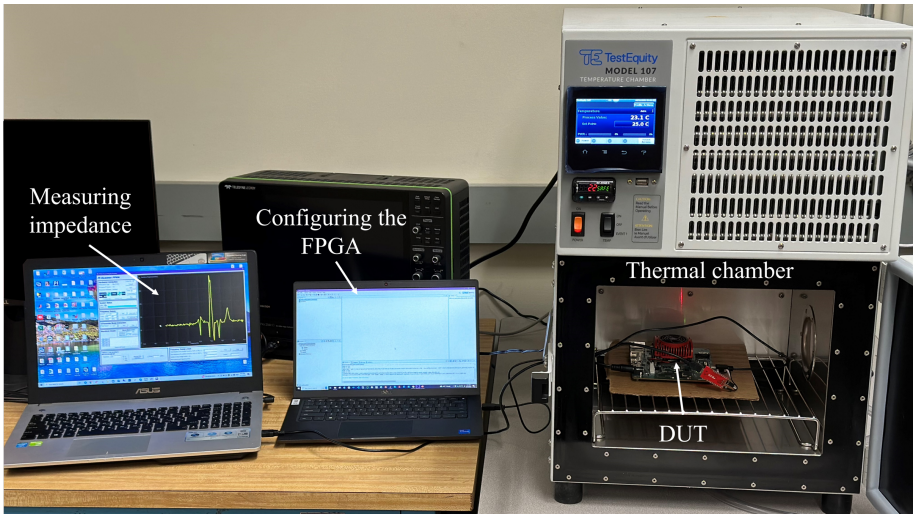


Figure 6: "BackMon" experimental setup.

where $f_{RO_{OFF}}$ and $f_{RO_{ON}}$ are the RO frequencies when the power-waster circuits are deactivated and activated, respectively. To characterize the complete profile $|Z_{PDN}|$ over a frequency range, the $f_{RO_{ON}}$ should be measured under different activation frequencies of power-wasting circuits.

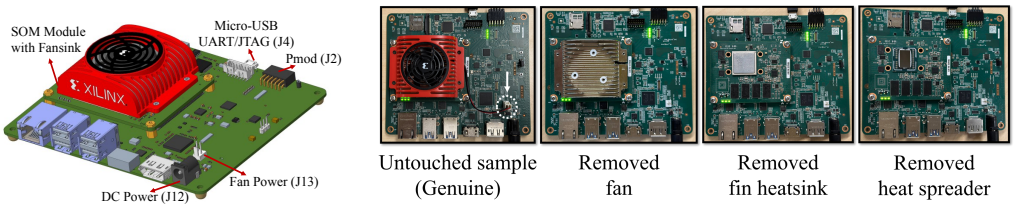
Ideally, the activation signal for the power-wasting circuits should be a sinusoidal wave, not a pulse wave, to prevent total harmonic distortion (THD). While sinusoidal waves at a specific frequency have a single harmonic, pulse waves at the same frequency contain the sinusoidal frequency and harmonics at the higher frequencies. To generate sinusoidal wave signals on FPGAs, one can use either Coordinate Rotation Digital Computer (CORDIC) algorithms or a lookup table that stores amplitude samples of a sinusoidal function over time. However, these methods cannot generate sinusoidal waves higher than a few tens of megahertz using the fastest clocks on FPGAs. At higher frequencies, the practical choice is to utilize pulse waves for activating power-wasting circuits. While these may not offer the same precision as sinusoidal waves, they are a reliable alternative that can be effectively used in such scenarios. For tamper detection purposes, we are only interested in detecting changes in impedance values, not their absolute physical values. Therefore, as long as the impedance characterization for a specific frequency is performed consistently using sinusoidal or pulse waves, we still can rely on the measured $|Z_{PDN}|$ for tamper detection.

3.5 Statistical Analysis

We define $\mathfrak{Z}_{PDN_i}^{Genuine}$ and $\mathfrak{Z}_{PDN_i}^{Tampered}$ as random variables corresponding to measured impedance values of the PDN at the frequency f_i for the genuine and tampered case studies, respectively. The number of measurement repetitions for frequency f_i is represented by N. We use the difference of means (DOM) as a standard statistical metric that measures the absolute difference between the mean values of $\mathfrak{Z}_{PDN_i}^{Genuine}$ and $\mathfrak{Z}_{PDN_i}^{Tampered}$ for each f_i. DOM is utilized to quantitatively differentiate between genuine and tampered experiments and can be calculated as follows

$$DOM(f_i) = \left|\mu(|\mathfrak{Z}_{PDN_i}^{Genuine}|) - \mu(|\mathfrak{Z}_{PDN_i}^{Tampered}|)\right|, \tag{5}$$

where, $\mu(.)$ refers to the mean function.



(a) (b)

Figure 7: (a) Kria KV260 vision AI starter kit description[Xilb]; (b) Each step of tampering attempts to expose the IC backside.

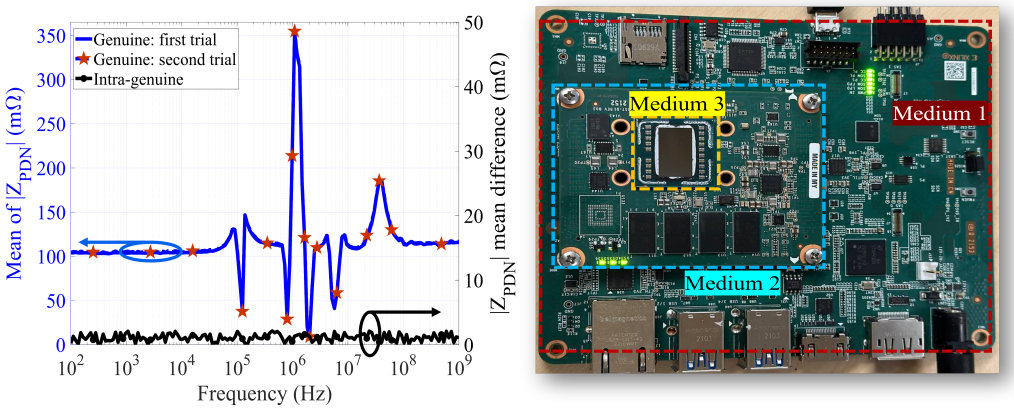
4 Experimental Setup

4.1 Device under Test

To experimentally validate the proposed method, we used Kria KV260 vision AI starter kit [Xilb], which contains AMD Zynq UltraScale+ MPSoC manufactured with 16 nm technology. Our experimental setup is shown in Figure 6, which includes the DUT, thermal chamber, and two desktop computers for configuring the PI Scanner IP and measuring the impedance. Jumper"J2" was utilized to configure the PI Scanner IP on the FPGA, and jumper "J4" was used to communicate between the chip and PI Scanner software (see Figure 7(a)). This board has several power domains, namely, a 5 V domain supplying the K26 system-on-module (SOM) ($V_{CC_{SOM}}$), a 3.3 V domain supporting the Raspberry Pi camera interface and Pmod connector, and a 1.8 V, 1.2 V, and 2.75 V domains for image access system (IAS) interface connectors. We performed our measurements on $V_{CC_{SOM}}$ PDN for the chip's backside tamper detection experiments. Figure 7(a) shows the Kria KV260 board used in our experiments. Jumper "J13" (it is marked as fan power in Figure 7(a)) was initially used for powering on the fansink module(here, the term "fansink" refers to the combination of the fan, finned heatsink, and the heat spreader sheet).

4.2 On-FPGA Network Analyzer

We have used PI Scanner IP [PIS, Ior18] for realizing a VNA on the FPGA. This IP generates current on the FPGA using configuration logic blocks by sequencing multiple transient switching currents to superimpose an overall constant current. The design can measure the impedance with a resolution of 1 mΩ over 0 - 1 GHz. However, we performed the impedance measurements within 100 Hz - 1 GHz. The purpose of this paper is to identify IC's backside tampering attempts, which are related to PDN's package impedance changes. The Package circuit components are closer to the IC and are effective in the middle-frequency range [ZBC+19]. Therefore, there was not much useful information in very low-frequency ranges between 0 - 100 Hz for our experiments. Moreover, due to large wavelengths between 0 - 100 Hz, the integration time increases significantly. Impedance characterization beyond 1 GHz requires conventional VNAs. The IP generates sinusoidal activation waves using the Lookup Table method for lower frequencies and pulse activation waves for higher frequencies using the Mixed-Mode Clock Manager (MMCM) of AMD FPGAs [Ior16, Ior20]. Moreover, it uses RO and IOBUF ROs [BEG+21] for measuring the voltage drop on the core and I/O banks of the FPGA, respectively. The time needed to scan the entire frequency band is in the order of seconds. There is a trade-off between detection accuracy and scan time that can be controlled by tuning the number of frequency points measured. We communicated with the FPGA from our laptop using a UART communication link. After loading the VNA bitstream to FPGA, we could send commands to the FPGA and receive measurement data from it using the same serial link.



(a) (b)

Figure 8: (a) The mean (left y-axis) and mean difference (right y-axis) of 110 impedance profiles of two trials of the genuine sample measurements (Intra-genuine) over the 100 Hz - 1 GHz frequency band at 25°C; (b) The multi-PCB device under test after the heat spreader removal, where every highlighted medium corresponds to a PCB in the system.

4.3 Thermal Chamber

We used a TestEquity Chambers TE-107 [Tes] as the thermal chamber for testing our approach at various frequencies. The TE-107 supports temperatures in the range of -42 to +130°C. The chamber includes 7.62 cm access ports on the left and right sides, enabling users to attach cables to test samples. Foam plugs are used to isolate the chamber from the outside environment.

5 Results

In this section, we show how "BackMon" can detect various levels of IC backside tampering attempts at different temperatures. To this end, we systematically performed the experiments at different stages, ranging from the attacker's first attempt, powering off the fan, to his/her last steps, which would be removing the fin heatsink and heat spreader and exposing the chip to the external environment. When the attacker reaches the last stage (i.e., the heat spreader is removed), the chip is prepared to conduct the backside attack. Therefore, one of the important experiments to which we should pay attention is the impedance profile distribution between this experiment and the genuine sample experimental results at various temperatures.

We start with the experiment in which the chip's fan is powered on and connected to the J13 jumper (we used this case as the reference measurement for all experiments). We continue the experiments to observe the impact of tampering by powering off the fan, removing it, removing the finned heatsink, and the heat spreader at different temperatures (see Figure 7(b) for illustration of the different steps taken to expose the IC backside). To have enough data for statistical analysis, the PDN impedance signatures have been measured 110 times in each experiment. The measurements were carried out within the 100 Hz - 1 GHz frequency band with logarithmic steps using the PI Scanner default setting with 157 frequency points. We performed the experiments in a controlled-temperature environment to analyze the robustness of the proposed tamper detection method at different temperature conditions. To be more specific, we carried out the experiments at -5°C, 5°C, 25°C, and 45°C.

Our first experiment is dedicated to studying the consistency of PDN impedance profiles for the untouched sample experiment over time to investigate to what extent we can rely on

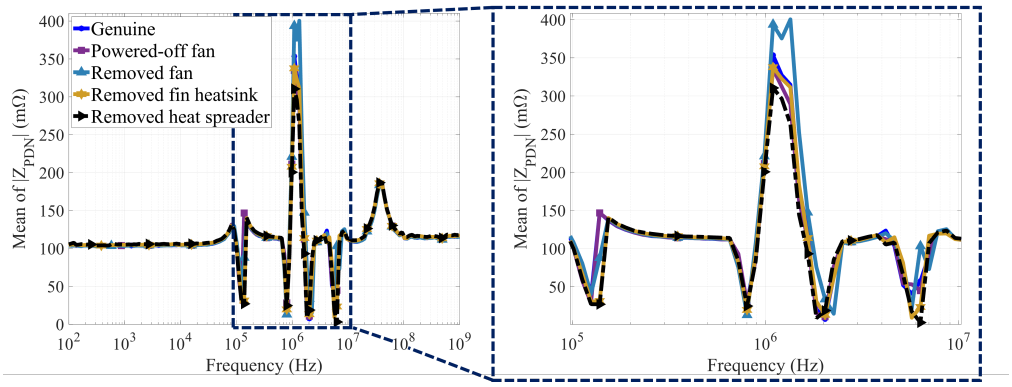


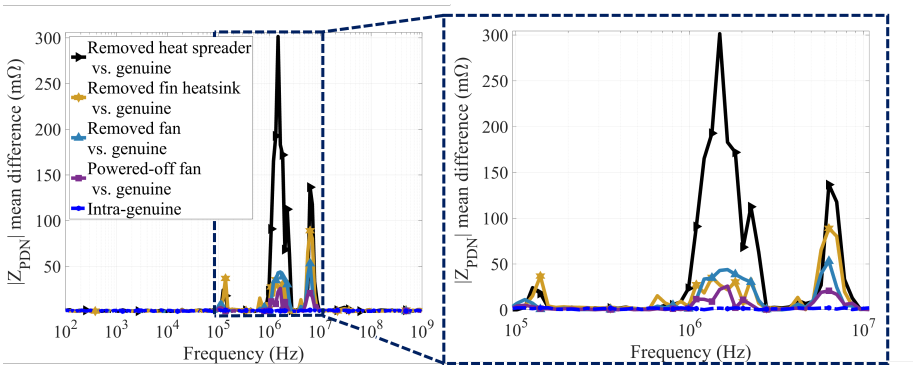
Figure 9: The mean of the impedance profile within the frequency band of 100 Hz - 1 GHz at 25°C. The right-side figure shows the zoomed-in view of the bandwidth with the most deviation from the impedance mean of the genuine sample.

a golden impedance signature. For this reference experiment, we performed two sets of 110 measurements in two different trials for the same genuine sample (the untouched sample with the fan powered on) on different days. Figure 8a illustrates the mean (left y-axis - blue curves) and mean difference (right y-axis - black curve) of the collected impedance traces for two trials of measurements on the same board over the frequency band of 100 Hz - 1 GHz at 25°C. It can be observed that the impedance profiles (left y-axis curves) are well-matched to each other, and no significant difference of more than 2.12 $m\Omega$ (at 1.09 MHz) is seen in the results. Therefore, we can detect tamper events if the detection threshold is set to a value of slightly more than 2.12 $m\Omega$. The mean difference of two trials of genuine measurements (black curve in Figure 8a) shows the noise floor for this experiment, and it can be used as the threshold in the next experiments to see if a tamper attempt has occurred or not. This intra-genuine impedance signature is calculated for all experiments at different temperatures, and the verifier can used it to differentiate between tampered and untouched samples (see Figure 10).

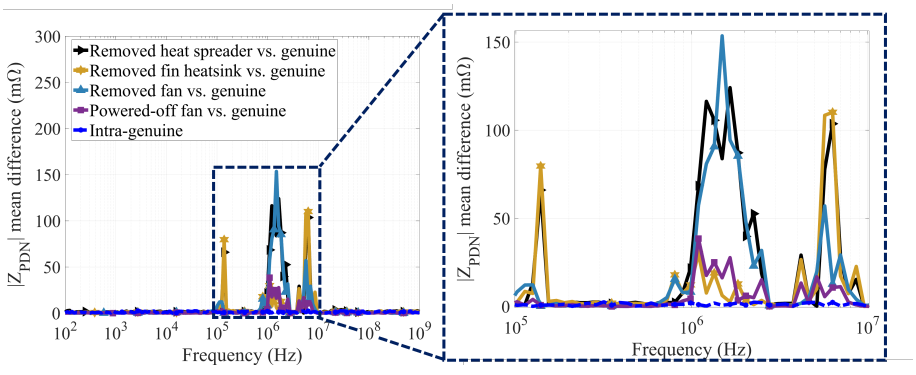
Then, we start tampering with the IC's backside by powering off the active part of the heatsink (fan). We disconnected the fan power (jumper "J13"), which is highlighted by the dashed white line in the first step of tampering attempts shown in Figure 7(b). In the next experiment, the fan is removed, and lastly, we removed the passive heatsink (fin heatsink) and heat spreader to expose the IC backside to the external environment. At each stage, the impedance profiles over the frequency band of 100 Hz - 1 GHz are measured 110 times before going to the next step.

The mean of the impedance profiles measured at 25°C is shown in Figure 9 where the right-side figure shows the zoomed-in view of the bandwidth with the most deviation from the impedance mean of the genuine sample. As expected, higher differences are seen in the frequency (x-axis) and impedance (y-axis) values at the resonance and anti-resonance frequency regions, indicating higher capacitive/inductive and resistive changes at these frequencies. The mean of the impedance profiles at other temperatures is not shown for brevity, as the main goal is to compare the mean difference graphs of the impedance traces. The mean difference of the impedance traces for intra-genuine and tampered cases are shown in Figure 10 at different temperatures. These results confirm the method's effectiveness in detecting different stages of backside tamper events at different temperatures from -5°C to 45°C.

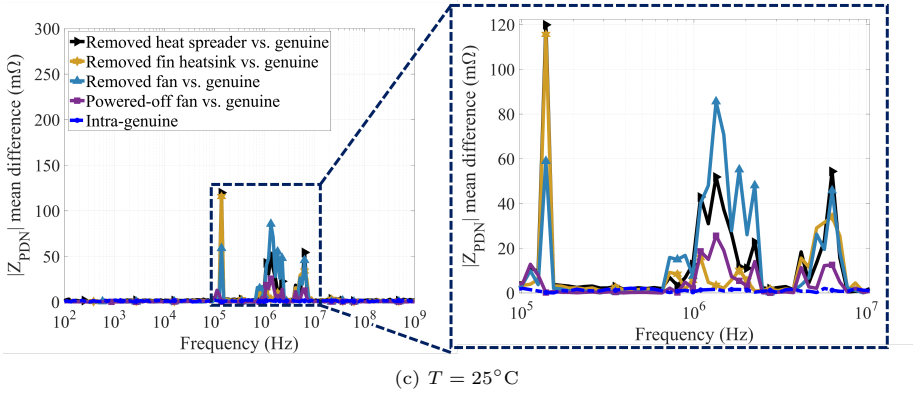
In all four measured temperatures, the difference between intra-genuine signatures is significantly lower than between the genuine and tampered sample signatures within the 100 kHz - 10 MHz band. Therefore, it is conceivable that every step of tamper attempts can be detected with high confidence at PDN's resonance and anti-resonance frequency



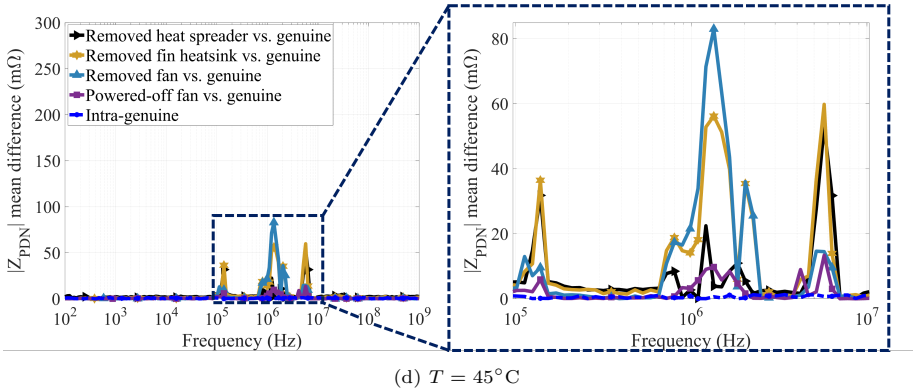
(a) $T = -5°\mathrm{C}$



(b) $T = 5°\mathrm{C}$



(c) $T = 25°\mathrm{C}$



(d) $T = 45°\mathrm{C}$

Figure 10: The mean difference between the intra-genuine and the tampered sample's impedance profiles within the 100 Hz - 1 GHz frequency band at different temperatures.

regions in the aforementioned bandwidth. On the contrary, higher levels of overlap between tampered and genuine case studies are observed in lower frequency regimes and very high frequencies. While we expect to see the effect of VRM and larger decoupling capacitors at lower frequencies, on-die impedance dominates the impedance profile at very high frequencies. This confirms the agreement between the theory and experimental results for detecting the impact of package-level tamper events in the middle-range frequencies.

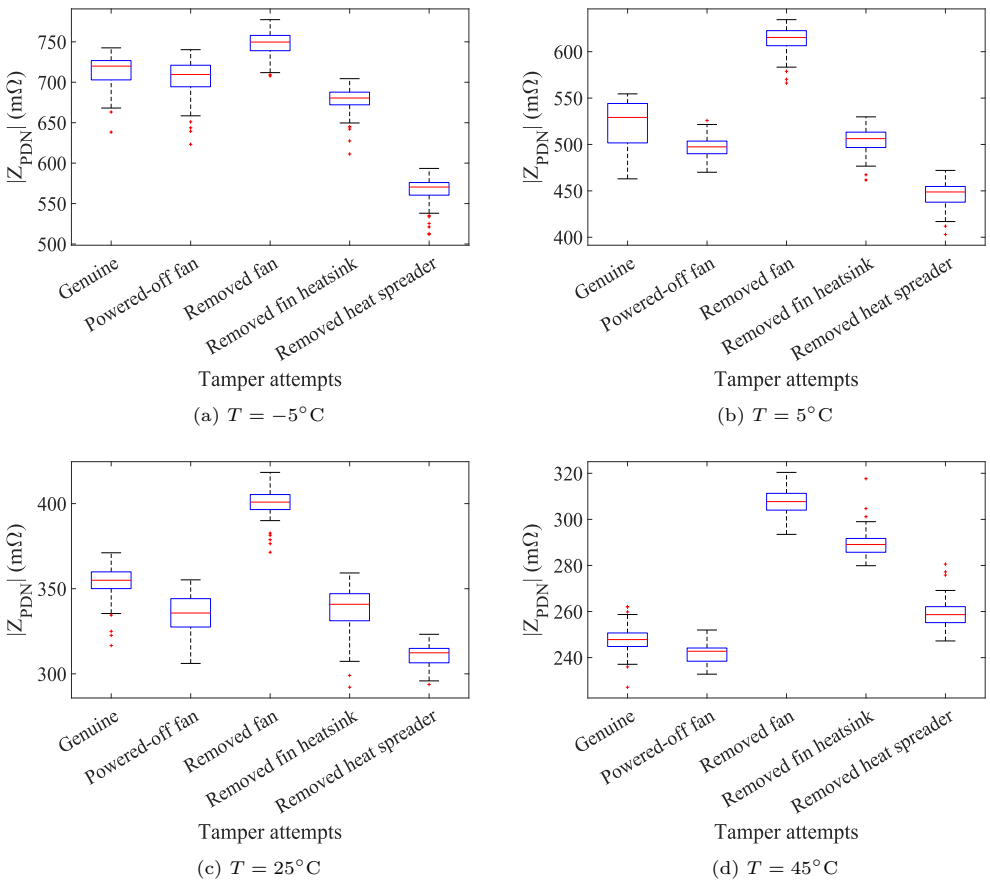
It can be seen that every step of the IC's backside tampering activities can be detected at PDN's resonance and anti-resonance frequencies, while higher levels of overlap between tampered and genuine cases are observed in lower frequency regimes (where we expect to see the effect of VRM and PCB components) and very high frequencies (where we expect to see the effect of on-die impedance). This confirms the agreement between the theory and experimental results for detecting the impact of package-level tamper events in the middle-range frequencies. We also can observe three regions of maximum difference between genuine and tampered cases, which correspond to the three transitions we have in our multi-PCB DUT. These three transitions between media are shown in different colors in Figure 8b.

It is interesting to observe that although IC's backside cooling components (e.g., fan, fin, and heat spreader) are connected to the IC's power domain (even the fan power domain is different from the IC's PDN), tampering with them can affect the PDN's impedance profile within these three transition regions. This is due to the fact that tampering with IC's backside cooling module would make the chip and its surrounding environment hotter, and this higher temperature would cause a change in the PDN impedance in the resonance and anti-resonance frequency regions of the spectrum (100 kHz - 10 MHz).

Figure 8b demonstrates our DUT after the heat spreader removal, where every highlighted medium corresponds to a PCB in the system. When transitioning from one medium to another, the impedance profile changes due to discontinuities seen in the signal path and the changes in the dimensions of the PGPs. The discontinuities include vias or connectors between PCBs that can introduce reflections and alter the impedance profile at transition points. The dimensions of the PGPs may change at transition points due to variations in layer stackup, signal routing, and component placement. Each of these media (PCBs) has different numbers of layers, thicknesses, and materials, all affecting the dimensions and impedance of the PGPs. The heat spreader removal is the last stage of the tampering attempts, and it is expected that it will have a more significant impact on the impedance profile. However, the mean difference between the heat spreader removal and intra-genuine experiments is higher at $-5°$C compared to the same value at $45°$C at the three transition regions. This indicates that the detection confidence will decrease as the temperature increases. An increase in temperature leads to decreased mean difference values in PDN impedance peaks due to changes in the electrical properties of the materials involved. To be more specific, the electrical properties of materials, i.e., dielectric constant and loss tangent, can be temperature-dependent. As temperature increases, these properties may change, affecting the overall impedance of the PDN.

We further performed a detailed statistical analysis at the Bandini Mountain frequency, where we can observe the maximum difference between impedance values measured for the genuine and tampered cases. We plotted impedance distributions over 110 measurements using boxplots in Figure 11 for different temperatures. This provides a comprehensive visualization of the impedance distribution at the Bandini Mountain frequency. The central box in each plot indicates the inter-quartile range, highlighting the middle 50% of the data, with the median value depicted by the red line within each box. Whiskers are the straight lines extending from the ends of the box to the maximum and minimum impedance values. Whiskers indicate the range of the impedance data over 110 measurements, with outliers plotted individually beyond the whiskers in red color.

It can be seen that different tampering attempts on the IC's backside environment would



(a) $T = -5°\mathrm{C}$ (b) $T = 5°\mathrm{C}$

(c) $T = 25°\mathrm{C}$ (d) $T = 45°\mathrm{C}$

Figure 11: Impedance distribution at the Bandini Mountain frequency for different backside tamper events at different temperatures.

impact the impedance distribution remarkably. Therefore, Bandini Mountain impedance can serve as a powerful distinguisher between tampered and genuine (untouched) samples at different temperature conditions, from low to high temperatures. There is also consistency in the impedance data distribution for various temperature conditions. In the case of the experiment where the fan is completely removed, we can see an increase in the impedance values at all four temperature conditions. The fan provides forced airflow over the heatsink fins, enhancing heat dissipation and affecting the PDN impedance. When it is removed, the resistive part of the impedance increases significantly. Furthermore, the rotating component of the fan can exhibit inductive behavior due to its motion.

When the passive parts of the heatsinks (the fin heatsink and the heat spreader) are removed, we detect a decrease in the impedance values. Passive heatsinks dissipate heat away from the chip, and by removing them, the overall system runs hotter, which can affect its electrical properties. Increased temperature can lead to higher resistive losses in the conductive elements of the PDN, resulting in lower impedance. Heatsink structures can also mitigate mechanical vibrations and resonance within the system. Removing heatsinks may allow mechanical vibrations to propagate more freely, inducing resonant frequencies in the system. Resonance effects can increase crosstalk by causing additional coupling between adjacent traces or components, which can impact the impedance.

Generally, dielectric constant and loss increase when temperature increases, but the loss tangent increases more inconspicuously. As a result, as we increase the temperature from $-5°\mathrm{C}$ to $45°\mathrm{C}$, the overall impedance values decrease due to the increase in the dielectric

Table 1: The Comparison Between IC Backside Tamper Detection Methods.

IC Backside Defense Mechanism	Measured Parameters	Requirement of Extra Fabrication Steps	Method's Abstraction Level		
			Circuit-level	Package-level	PCB-level
Backside Coating [ABH+18]	Light Intensity	Yes	-	✓	-
Protection Wafer [HAL+22]	Light Intensity	Yes	-	✓	-
Optical Waveguide PUF [VWN+16]	Light Intensity	Yes	-	-	✓
Capacitive PUF Enclusure [IOK+18]	Capacitance	Yes	-	-	✓
Anti-Tamper Radio [STZP22]	Radio Signal	Yes	-	-	✓
BackMon	Impedance	No	✓	-	-

constant, which causes an increase in the distributed capacitance of the PDN. Furthermore, an increase in temperature can lead to higher dielectric losses, which can contribute to a decrease in impedance at certain frequencies. Also, higher temperatures can increase the resistance of conductive materials. This change in resistance can impact the impedance of the PDN, especially at higher frequencies. The characteristics of the distributed capacitance and inductance of the chip's package can be temperature-dependent, affecting the overall impedance of the PDN in the middle-frequency range where Bandini Mountain frequency is.

6 Discussion

6.1 Comparison with Related Work

Table. 1 qualitatively compares existing IC backside tamper detection techniques with the proposed method, "BackMon," in terms of measured parameters, the requirement of extra fabrication steps, and the abstraction level at which the method is implemented. The backside defense methods in [ABH+18, HAL+22] are implemented at package level, and the one in [VWN+16] is implemented at PCB-level. All three methods in [ABH+18, HAL+22, VWN+16] leverage the optical interaction between transistors and an opaque layer (light intensity). On the other hand, the methods in [IOK+18, STZP22] use secure enclosures to prevent access to the IC package and are implemented at the PCB level. While the methods presented in [ABH+18, HAL+22, VWN+16, IOK+18, STZP22] necessitate additional manufacturing steps, "BackMon" is implemented at the circuit level and provides compatibility with legacy systems as it does not require extra fabrication steps. Therefore, the proposed method in this work is considered a cost-effective solution that removes the need for external sensors or components.

6.2 Success Rate for Reversing Backside Tampering

The attacker might remove components from a powered-off device for backside imaging purposes. In such cases, a question arises about the feasibility of undoing the tampering effect on the impedance before powering up the device. The adversary is theoretically required to equalize the two-dimensional impedance curve by re-gluing the removed components, which is a hard, if not impossible, task due to the following reasons. Reattaching the same removed component to the package or PCB will not deliver the same parasitic signature as the glue distribution on the surfaces, and the placement of the component will be changed. Components' parasitics cause the most local maxima and minima of the

impedance curve over the frequency, and hence, reattaching components even in identical locations demonstrates different parasitics.

Second, in our threat model, the golden impedance signature is stored on the chip, and hence, the attacker does not have access to it for analysis and equalization. We assume that the golden signatures can only be recovered using semi- or fully-invasive techniques, which will already change the package's PDN characteristics. Even if the attacker extracts golden signatures from another training sample, it will differ from the target's signature due to the variations in the manufacturing process and parasitics. Consequently, the adversary cannot observe the exact same impedance signature that has been used during the enrollment phase.

6.3 Robustness to Voltage Variations

Voltage variations could have an adverse influence on the RO sensor behavior. The behavior of the RO sensor inside the FPGA could be distorted if other ICs sharing the same PDN cause voltage drops due to their activities. In such a scenario, the PDN's impedance should be measured when other active ICs are idle. Another option would be to take the maximum voltage variations as additive noise into account during the enrollment phase and later tune a detection threshold accordingly. In other words, if impedance characterization should be performed when other ICs are causing voltage ripple, we should consider the worst-case scenario, i.e., the maximum possible voltage ripple of different components and, therefore, their impact on the RO sensor frequency. Increased voltage ripple would require a higher detection threshold and, therefore, could decrease the system's detection confidence.

The changes in the voltage could also be induced by the attacker to deceive the sensor with the intention of masking the effect of backside tampering. First, as mentioned in the previous subsection (Sect. 6.2), the attacker does not have access to the device's golden impedance signature, and thus, she does not know the exact amount of equalization needed to recreate the golden impedance profile. Second, an attacker should bypass the voltage regulator to connect her voltage supply or function generator to the main PDN to change the voltage. As shown in [MST23], such tamper events can be detected by impedance sensing at lower frequency bands using the same sensor. Furthermore, the dedicated on-die voltage sensors on ASICs and FPGAs can also detect such voltage variations.

6.4 Detecting Silicon Polishing

Based on the results reported in [SLL+08, LXH+12], polishing of the silicon has an impact on the package-die stress level, which has an influence on the switching delay of transistors. The changes in the delay have been measured using delay-based circuits, such as ROs and inverter chains [SLL+08, LXH+12]. Hence, such changes at the transistor level alone can influence the behavior of the sensor part of the FPGA-based network analyzer. In addition, thinning the silicon substrate changes the resistance of the package, which further affects the PDN's impedance. As a result, silicon removal is expected also to be detected using our proposed approach. In future work, we intend to systematically explore the impact of backside silicon substrate polishing on the PDN's impedance. Unfortunately, a backside polishing machine was not available to us during the writing of this paper.

7 Conclusion

This work presented a self-contained IC backside tamper detection method based on characterizing the device's PDN impedance profile. We first provided the technical details about why various components used on flip-chip packages, including heat sinks,

fins, and fans, contribute to the PDN's impedance at resonance and anti-resonance points. Based on this foundation, we argued that tampering activity on an IC package's backside should lead to changes in the PDN's impedance at these frequency bands. Inspired by [Ior18, ZS18, MST23], we deployed an on-FPGA network analyzer for integrity monitoring. We further validated our claims by emulating a backside tampering attack, in which we detached cooling components from the IC's package. We demonstrated that each preparation step an attacker takes to access the IC backside would influence the system's electromagnetic environment and impedance profile at middle-frequency ranges. We performed the experiments at various temperatures and deployed the difference of means as a statistical metric to differentiate the genuine and attacked samples. The methodology presented in this work not only offers a reliable approach to verifying the IC's backside integrity and detecting various forms of tamper events but also proves to be a cost-effective solution, eliminating the need for external sensors or components.

Acknowledgment

This work was sponsored by NSF under the grant number 2338069. We thank William L. Appleyard at Worcester Polytechnic Institute for helping prepare the samples for experiments. We gratefully thank Saleh Khalaj Monfared for taking the photon emission image.

References

[ABH+18] Elham Amini, Anne Beyreuther, Norbert Herfurth, Alexander Steigert, R Muydinov, Bernd Szyszka, and Christian Boit. IC security and quality improvement by protection of chip backside against hardware attacks. *Microelectronics Reliability*, 88:22–25, 2018.

[AKR+23] Elham Amini, Tuba Kiyan, Lars Renkes, Thilo Krachenfels, Christian Boit, Jean-Pierre Seifert, Jörg Jatzkowski, Frank Altmann, Sebastian Brand, and Shahin Tajik. Electrons vs. photons: Assessment of circuit's activity requirements for e-beam and optical probing attacks. In *ISTFA 2023*, pages 339–345. ASM International, 2023.

[ATG+19] Md Mahbub Alam, Shahin Tajik, Fatemeh Ganji, Mark Tehranipoor, and Domenic Forte. RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions. In *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 48–55. IEEE, 2019.

[BEG+21] Julia Burgiel, Daniel Esguerra, Ilias Giechaskiel, Shanquan Tian, and Jakub Szefer. Characterization of IOBUF-based ring oscillators. In *2021 International Conference on Field-Programmable Technology (ICFPT)*, pages 1–4, 2021.

[CCT+18] Samuel Chef, Chung Tah Chua, Jing Yun Tay, Yu Wen Siah, Shivam Bhasin, J Breier, and Chee Lip Gan. Descrambling of embedded SRAM using a laser probe. In *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–6. IEEE, 2018.

[FCAF12] Hany Fahmy, Jack Carrel, Ray Anderson, and Harry Fu. Simulating FPGA power integrity using S-Parameter models. 2012.

[GOKT18] Dennis RE Gnad, Fabian Oboril, Saman Kiamehr, and Mehdi B Tahoori. An Experimental Evaluation and Analysis of Transient Voltage Fluctuations in

FPGAs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 26(10), 2018.

[HAL+22] Norbert Herfurth, Elham Amini, Marco Lisker, Jean-Pierre Seifert, and Christian Boit. A scalable & comprehensive resilience concept against optical & physical IC backside attacks. In *2022 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pages 1–6. IEEE, 2022.

[HMW+24] Rikuu Hasegawa, Kazuki Monta, Takuya Wadatsumi, Takuji Miki, and Makoto Nagata. On-chip evaluation of voltage drops and fault occurrence induced by Si backside EM injection. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pages 22–37. Springer, 2024.

[HNT+13] Clemens Helfmeier, Dmitry Nedospasov, Christopher Tarnovsky, Jan Starbug Krissler, Christian Boit, and Jean-Pierre Seifert. Breaking and entering through the silicon. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 733–744, 2013.

[IOK+18] Vincent Immler, Johannes Obermaier, Martin König, Matthias Hiller, and Georg Sig. B-trepid: batteryless tamper-resistant envelope with a PUF and integrity detection. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 49–56. IEEE, 2018.

[Ior16] Cosmin Iorga. Method and system for measuring the impedance of the power distribution network in programmable logic device applications, April 12 2016. US Patent 9,310,432.

[Ior18] Cosmin Iorga. Solve Power Integrity Problems in FPGA Systems Using an Embedded Vector Network Analyzer. *Signal Integrity Journal*, 2018.

[Ior20] Cosmin Iorga. FPGA configured vector network analyzer for measuring the Z parameter and S parameter models of the power distribution network in FPGA systems, February 11 2020. US Patent 10,560,075.

[KGM+21] Thilo Krachenfels, Fatemeh Ganji, Amir Moradi, Shahin Tajik, and Jean-Pierre Seifert. Real-world snapshots vs. theory: Questioning the t-probing security model. In *2021 IEEE symposium on security and privacy (SP)*, pages 1955–1971. IEEE, 2021.

[KKTS21] Thilo Krachenfels, Tuba Kiyan, Shahin Tajik, and Jean-Pierre Seifert. Automatic extraction of secrets from the transistor jungle using laser-assisted side-channel attacks. In *30th USENIX security symposium (USENIX security 21)*, pages 627–644, 2021.

[KSF+11] Jingook Kim, Ketan Shringarpure, Jun Fan, Joungho Kim, and James L Drewniak. Equivalent circuit model for power bus design in multi-layer PCBs with via arrays. *IEEE Microwave and Wireless Components Letters*, 21(2):62–64, 2011.

[LSXR12] Zhe Li, Hong Shi, John Xie, and Arif Rahman. Development of an optimized power delivery system for 3D IC integration with tsv silicon interposer. In *2012 IEEE 62nd Electronic Components and Technology Conference*, pages 678–682. IEEE, 2012.

[LTH+95] Guang-Tsai Lei, Robert W Techentin, Paul R Hayes, Daniel J Schwab, and Barry K Gilbert. Wave model solution to the ground/power plane noise problem. *IEEE Transactions on Instrumentation and Measurement*, 44(2):300–303, 1995.

[LXH+12] Gerald S Leatherman, Jessica Xu, Jeffrey Hicks, Bahattin Kilic, and Daniel Pantuso. Die-package stress interaction impact on transistor performance. In *2012 IEEE International Reliability Physics Symposium (IRPS)*, pages 2E.4.1–2E.4.6. IEEE, 2012.

[MGST22] Tahoura Mosavirik, Fatemeh Ganji, Patrick Schaumont, and Shahin Tajik. Scatterverif: Verification of electronic boards using reflection response of power distribution network. *ACM Journal on Emerging Technologies in Computing Systems*, 18(4):1–24, October 2022.

[MLS+20] Shayan Moini, Xiang Li, Peter Stanwicks, George Provelengios, Wayne Burleson, Russell Tessier, and Daniel Holcomb. Understanding and Comparing the Capabilities of On-Chip Voltage Sensors against Remote Power Attacks on FPGAs. In *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 941–944. IEEE, 2020.

[MMST23] Tahoura Mosavirik, Saleh Khalaj Monfared, Maryam Saadat Safa, and Shahin Tajik. Silicon Echoes: Non-invasive Trojan and tamper detection using frequency-selective impedance analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–261, 2023.

[MNS+20] Takuji Miki, Makoto Nagata, Hiroki Sonoda, Noriyuki Miura, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, and Katsuya Kikuchi. Si-backside protection circuits against physical security attacks on flip-chip devices. *IEEE Journal of Solid-State Circuits*, 55(10):2747–2755, 2020.

[MST23] Tahoura Mosavirik, Patrick Schaumont, and Shahin Tajik. Impedanceverif: On-chip impedance sensing for system-level tampering detection. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 1:301–325, 2023.

[NMM21] Makoto Nagata, Takuji Miki, and Noriyuki Miura. Physical attack protection techniques for IC chip level hardware security. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 30(1):5–14, 2021.

[PHT20] George Provelengios, Daniel Holcomb, and Russell Tessier. Power distribution attacks in multitenant FPGAs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 28(12):2685–2698, 2020.

[PIS] PIScanner. PIScanner – FPGA Configured Vector Network Analyze. URL: https://storage.googleapis.com/wzukusers/user-29188536/documents/5c12c1352367bAich15I/datasheet_piscanner.pdf.

[PLKK03] Jun So Pak, Junwoo Lee, Hyungsoo Kim, and Joungho Kim. Prediction and verification of power/ground plane edge radiation excited by through-hole signal via based on balanced TLM and via coupling model. In *Electrical Performance of Electrical Packaging (IEEE Cat. No. 03TH8710)*, pages 181–184. IEEE, 2003.

[RKF+09] Liehui Ren, Jingook Kim, Gang Feng, Bruce Archambeault, James L Knighten, James Drewniak, and Jun Fan. Frequency-dependent via inductances for accurate power distribution network modeling. In *2009 IEEE International Symposium on Electromagnetic Compatibility*, pages 63–68. IEEE, 2009.

[RWVD94] Simon Ramo, John R Whinnery, and Theodore Van Duzer. *Fields and waves in communication electronics*. John Wiley & Sons, 1994.

[SB17] Larry D Smith and Eric Bogatin. *Principles of power integrity for PDN design–simplified: robust and cost effective design for high speed digital products*. Prentice Hall, 2017.

[SKNL04] Madhavan Swaminathan, Joungho Kim, Istvan Novak, and James P Libous. Power distribution networks for system-on-package: Status and challenges. *IEEE Transactions on Advanced Packaging*, 27(2):286–300, 2004.

[SKP+22] Keeyoung Son, Seongguk Kim, Hyunwook Park, Taein Shin, Keunwoo Kim, Minsu Kim, Boogyo Sim, Subin Kim, Gapyeol Park, Shinyoung Park, et al. Thermal and signal integrity co-design and verification of embedded cooling structure with thermal transmission line for high bandwidth memory module. *IEEE Transactions on Components, Packaging and Manufacturing Technology*, 12(9):1542–1556, 2022.

[SLL+08] Rudolf Schlangen, Rainer Leihkauf, Ted Lundquist, Peter Egger, Uwe Kerst, and Christian Boit. Trimming of IC timing and delay by backside FIB processing-comparison of conventional and strained technologies. In *2008 IEEE International Electron Devices Meeting*, pages 1–4. IEEE, 2008.

[SMT23] Maryam Saadat Safa, Tahoura Mosavirik, and Shahin Tajik. Counterfeit chip detection using scattering parameter analysis. In *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, pages 99–104. IEEE, 2023.

[SPK+14] K Shringarpure, S Pan, J Kim, B Achkir, B Archambeault, J Drewniak, and J Fan. Formulation and network reduction to a physics based model for analysis of the power distribution network in a production level multi-layered printed circuit board. *IEEE Transactions on Electromagnetic Compatibility*, 2014.

[STZP22] Paul Staat, Johannes Tobisch, Christian Zenger, and Christof Paar. Anti-tamper radio: System-level tamper detection for computing systems. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1722–1736. IEEE, 2022.

[SZW+14] Ketan Shringarpure, Biyao Zhao, Leihao Wei, Bruce Archambeault, Albert Ruehli, Michael Cracraft, Matteo Cocchini, Edward Wheeler, Jun Fan, and James Drewniak. On finding the optimal number of decoupling capacitors by minimizing the equivalent inductance of the PCB PDN. In *2014 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 218–223. IEEE, 2014.

[Tes] TestEquity. TestEquity Model 106 and 107 Temperature Chamber Operation and Service Manual. URL: https://www.testequity.com/UserFiles/documents/pdfs/106-107.pdf.

[TLG+15] Shahin Tajik, Heiko Lohrke, Fatemeh Ganji, Jean-Pierre Seifert, and Christian Boit. Laser Fault Attack on Physically Unclonable Functions. In *2015 workshop on fault diagnosis and tolerance in cryptography (FDTC)*, pages 85–96. IEEE, 2015.

[TLSB17] Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, and Christian 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*, pages 1661–1674, 2017.

[TMOL12] K TOBICH, P MAURINE, T Ordas, and PY Liardet. Yet another fault injection technique: by forward body biasing injection. In *YACC: Yet Another Conference on Cryptography*. Citeseer, 2012.

[TNH+14] Shahin Tajik, Dmitry Nedospasov, Clemens Helfmeier, Jean-Pierre Seifert, and Christian Boit. Emission analysis of hardware implementations. In *2014 17th Euromicro Conference on Digital System Design*, pages 528–534, 2014.

[VWN+16] Michael Vai, David J Whelihan, Benjamin R Nahill, Daniil M Utin, Sean R O'Melia, and Roger I Khazan. Secure embedded systems. *Lincoln Laboratory Journal*, 22(1):110–122, 2016.

[Xila] Xilinx. Kria K26 SOM Thermal Design Guide. URL: https://docs.xilinx.com/r/en-US/ug1090-k26-thermal-design/Thermal-Solution-Installation-Examples.

[Xilb] Xilinx. Kria KV260 Vision AI Starter Kit Data Sheet. URL: https://docs.xilinx.com/r/en-US/ds986-kv260-starter-kit/Summary.

[ZAB+18] Shuze Zhao, Ibrahim Ahmed, Vaughn Betz, Ashraf Lotfi, and Olivier Trescases. Frequency-domain Power Delivery Network Self-characterization in FPGAs for Improved System Reliability. *IEEE Transactions on Industrial Electronics*, 65(11), 2018.

[ZBC+19] Biyao Zhao, Siqi Bai, Samuel Connor, Wiren Dale Becker, Matteo Cocchini, Jonghyun Cho, Albert Ruehli, Bruce Archambeault, and James L Drewniak. Physics-based circuit modeling methodology for system power integrity analysis and design. *IEEE Transactions on Electromagnetic Compatibility*, 62(4):1266–1277, 2019.

[ZS18] Mark Zhao and G Edward Suh. FPGA-based Remote Power Side-channel Attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 229–244. IEEE, 2018.

[ZSS+23] Huifeng Zhu, Haoqi Shan, Dean Sullivan, Xiaolong Guo, Yier Jin, and Xuan Zhang. PDNPulse: Sensing PCB anomaly with the intrinsic power delivery network. *IEEE Transactions on Information Forensics and Security*, 2023.