IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2023, No. 1, pp. 301–325. DOI:10.46586/tches.v2023.i1.301-325

ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection

Tahoura Mosavirik, Patrick Schaumont and Shahin Tajik

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

Abstract. Physical attacks can compromise the security of cryptographic devices. Depending on the attack's requirements, adversaries might need to (i) place probes in the proximity of the integrated circuits (ICs) package, (ii) create physical connections between their probes/wires and the system's PCB, or (iii) physically tamper with the PCB's components, chip's package, or substitute the entire PCB to prepare the device for the attack. While tamper-proof enclosures prevent and detect physical access to the system, their high manufacturing cost and incompatibility with legacy systems make them unattractive for many low-cost scenarios. In this paper, inspired by methods known from the field of power integrity analysis, we demonstrate how the impedance characterization of the system's power distribution network (PDN) using on-chip circuit-based network analyzers can detect various classes of tamper events. We explain how these embedded network analyzers, without any modifications to the system, can be deployed on FPGAs to extract the frequency response of the PDN. The analysis of these frequency responses reveals different classes of tamper events from board to chip level. To validate our claims, we run an embedded network analyzer on FPGAs of a family of commercial development kits and perform extensive measurements for various classes of PCB and IC package tampering required for conducting different side-channel or fault attacks. Using the Wasserstein Distance as a statistical metric, we further show that we can confidently detect tamper events. Our results, interestingly, show that even environment-level tampering activities, such as the *proximity of contactless EM probes* to the IC package or *slightly polished IC package*, can be detected using on-chip impedance sensing.

Keywords: Anti-Tamper · Power Distribution Network · Physical Attacks · Physical Layer Security · PCB Verification

1 Introduction

Strong cryptography is required to maintain the secrecy and integrity of processed data in embedded systems. However, even in the existence of such cryptographic primitives, attackers who obtain physical access to these devices can perform physical attacks to break the security of the entire system. Mounting physical attacks (e.g., Side-Channel Analysis (SCA) and Fault-Injection (FI)) usually requires adversaries to tamper with the system and prepare it for such attacks. Depending on the attack requirements, tampering at different abstraction levels of the system, from the printed circuit board (PCB) to integrated circuits (ICs), is desired by the attacker. For instance, in case of power analysis attacks, an adversary might need to solder or replace a shunt resistor on the PCB's power rails or remove decoupling capacitors from the PCB to amplify leakage through power consumption [DCEM18, LBS19]. Another example includes the polishing or removing the integrated circuit (IC) package to carry out semi- or fully-invasive

Received: 2022-07-15 Accepted: 2022-09-15 Published: 2022-11-29

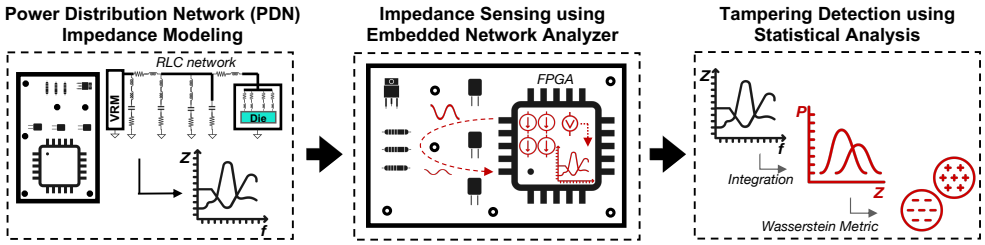


Figure 1: The concept of the ImpedanceVerif framework: (i) Modeling the PDN impedance as an RLC circuit, (ii) Characterizing the impedance of this RLC network using an embedded network analyzer on FPGAs, and (iii) performing statistical analysis for detecting tamper events using Wasserstein metric.

attacks [HMH+12, KGM+21, Sko17]. In extreme cases, the attacker might even desolder the chip from its original PCB and mount it on custom boards or sockets optimized for attacks. However, in most non-invasive attacks, the adversary might only create connections between her probes and PCB or place electromagnetic probes in a contactless fashion close to the IC package without any physical modifications to the system.

Several anti-tamper solutions are based on tamper-evident secure enclosures to cover the entire system and realize hardware security modules (HSMs). These envelopes detect changes in the physical characteristics of the environment, such as the enclosure's capacitance or the envelope's internal electromagnetic field.

While such secure enclosures shield the system against several classes of tampering and modifications, they are very costly and need a highly customized design making them unusable for legacy systems. Therefore, we seek anti-tamper schemes, which on the one hand, cover different abstraction levels of the system from PCB to chip level, and on the other hand, require minimal changes to the conventional electronic boards. Ideally, a security-critical chip holding secret keys and other assets should be able to physically sense its environment to detect any unauthorized changes in the system and react accordingly.

There have been a few attempts in the literature to include such self-contained sensors into system security-critical ICs to detect physical anomalies, including PCB-level Trojans [FNH+18], counterfeit boards [ZRS21, WHT19, GXTF17], or removal of components [BEG+21]. On digital ICs and field-programmable gate arrays (FPGAs), these sensors take the form of timing circuits such as on-chip [GXTF17, BEG+21] and PCB trace-based ring-oscillators [ZRS21]). If all goes well, any PCB anomalies will then affect the sensitive timing behavior of these sensors.

However, such passive sensing methods have led to low-precision measurements and noisy behavior. Therefore, advanced signal processing and machine learning methods are needed to obtain acceptable classification accuracy. On the other hand, active sensing methods, such as time-domain reflectometry (TDR), have shown a high precision in detecting malicious implants on the I/O signal traces of PCB. However, they need custom analog circuits inside the chips [FNH+18]. Moreover, all these solutions only demonstrate the detection of specific modifications to the system (e.g., removal/insertion of a component to an I/O signal trace). It remains open how these solutions apply to multiple classes of tampering. Therefore, we ask the following research question: *Is it possible to have an on-chip circuit-based sensor that is capable of monitoring the physical integrity of its environment beyond its die, from its package to PCB, in a unified manner?*

Our Contributions: In this work, we indeed positively answer the above question and solve the puzzle of why existing on-chip sensors have limited applicability and poor performance when sensing tampering of the environment beyond the chip itself. Inspired by novel insights in power integrity analysis and its application to physical integrity, we introduce a self-contained tamper-evident sensor. The sensor characterizes the impedance

of the power distribution network (PDN) and can verify the physical integrity of the system from board to chip level, see Figure.1. As any tampering attempt on the PCB will lead to changes in the equivalent impedance of the PDN, the continuous physical scanning of PDN will reveal whether the PCB's integrity has been violated [MGST22, ZSS+22]. In this regard, we will explain how the functionality of network analyzers, the traditional tools to perform such impedance characterizations, can be emulated on FPGAs without any extra component or modification to the system [Ior18, ZAB+18]. We demonstrate that electrically stressing the PDN of the system with various frequencies and simultaneously measuring voltage drop for impedance estimation is the key to detecting various tamper events. We further show that the impact of different classes of tampering on the magnitude of PDN impedance is higher at certain frequency bands. After performing extensive experiments on a commercial FPGA board and deploying Wasserstein distance as a metric, we discovered that such a wideband impedance characterization could surprisingly reveal very sophisticated tampering/modifications to the system, namely, (i) the addition/removal of PCB components, (ii) the connection of a probe/wires to the PCB, (iii) the presence of an EM probe close to the IC package, (iv) and modifications to the IC package.

Remark. In this work, we are taking only the first steps toward understanding the applicability of power integrity solutions to the problem of physical verification and tamper detection. Therefore, we do not claim that the proposed sensing mechanism provides a complete or error-free security solution. More research is required to explore the strengths and limitations of the proposed solution in real-world scenarios. FPGA-based network analyzers have been previously reported in the power integrity literature [Ior18, ZAB+18] to achieve system reliability during PCB design. Hence, their design is not the main contribution of this work. Our primary intention in this paper is to draw attention to the potential of this known but not well-researched sensing mechanism in hardware security.

2 Technical Background

2.1 PDN Characterization

A PDN handles the system's power delivery from the external power regulator down to the transistors on the chip. Figure. 2(a) demonstrates a PDN model for a typical PCB. The equivalent circuit of a PDN is an RLC network [ZHS+15, ZAB+18]. The PDN connects the VRM to every power-sinking component on the PCB, and every component has specific power and voltage requirements. The PDN covers off-chip components such as bulk capacitors, PCB routing, multilayered ceramic capacitors (MLCCs), spreading, and vias. The PDN also covers on-chip components such as IC packaging, bonding wires, on-chip power grid, etc. The contribution of each component to the PDN's impedance is distinct at different frequencies; see Figure. 2(b). While at lower frequencies, the equivalent impedance of the PDN is dominated by the voltage regulator's characteristics, at higher frequencies, the off-chip and on-chip components contribute most to the impedance [LFH10, ZAK+17, ZAB+18]. The main reason for such an impedance behavior is the existing parasitic inductance on each capacitor [FCAF12]. An ideal capacitor behaves as a short-circuit at high frequencies. However, the parasitic inductance causes the capacitor to resonate at a particular frequency depending on its capacitance and inductance values. Smaller capacitors have smaller parasitic inductance due to their smaller physical dimensions; therefore, they resonate at higher frequencies. In this case, the capacitor's impedance for frequencies higher than its resonance frequency increases, and thus, at very high frequencies, the capacitor behaves like an open circuit. Consequently, by moving to higher frequencies, each set of capacitors, from the large to small ones, become open circuits, and their effect on the PDN impedance diminishes.

To characterize the PDN impedance over different frequency bands, Z (impedance) and

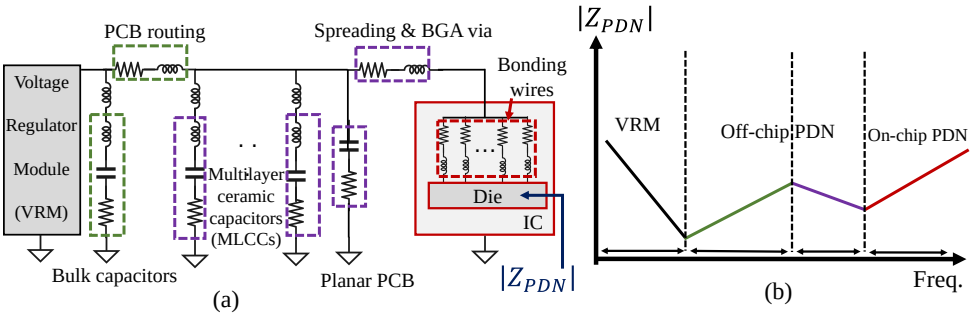


Figure 2: (a) The equivalent RLC circuit of the system's PDN (b) Contribution of different parts of the PDN to the magnitude of the PDN impedance over frequency.

S (scattering) parameters are used [Bog10, Pup20]. These parameters are usually employed in RF/Microwave engineering and in power/signal integrity analysis of electronic systems to describe the electrical properties of linear RLC electrical networks. S- and Z-parameters are complex numbers (including the voltage amplitude and the phase of traveling waves) and are frequency-dependent. The number and organization of the parameters depend on the available electrical ports on the RLC circuit. S-parameters directly represent the signal's attenuation and reflection/transmission at each port of network. On the other hand, Z-parameters can be used to derive the observed impedance at each port of the network. S-parameters and Z-parameters represent comparable data, but measuring one or the other may be more convenient depending on the measurement conditions. Network analyzers are the primary instruments for measuring these parameters. They contain both a source used to stimulate the PDN of the system by injecting sine waves with different frequencies into the network and receivers, used to measure the amount of signal reflection and transmission at each frequency. The resulting measurements reveal *the system's frequency response*. We distinguish scalar network analyzers (SNAs) and vector network analyzers (VNAs). While SNAs can only measure the magnitude of the signal, VNAs can measure both the amplitude and the phase of the traveling wave. VNAs have been utilized in the literature for detecting counterfeit and tampering activities at the PCB level using both scattering [MGST22] and impedance parameters [ZSS+22]. There also exist similar commercial products that characterize the V/I signatures of the ICs (e.g., SENTRY [ABIa]) and PCBs (e.g., AMS [ABIb]) in a frequency range.

2.2 Challenges with Current On-Chip Circuit-based Sensors

A few on-chip circuit-based sensors have been proposed in the literature to indirectly sense the changes in the impedance of the PDN due to different anomalies. Virtually all these circuit-based sensors are based on various analog to digital converters (ADCs). Ring-oscillators (ROs) are a popular example of such ADCs due to their sensitivity, simplicity, and compatibility with digital circuits. The main hope has been that modifications in part of the system's board or package lead to changes in the behavior of these ROs, and consequently, the attacks would be detected. For instance, on-chip RO-based sensors have been proposed to detect counterfeit PCBs and hardware Trojan implants on PCBs by monitoring the PDN [LML12, WHT19] or traces of the PCB [GXTF17, ZRS21, BEG+21]. While in the former case, a network of ROs is realized on the chip to sense the PDN modifications, in the latter schemes, either extended ROs between chips and off-chip PCB traces or I/O bank-based ROs are deployed to monitor the physical integrity of connected traces to the chip. Such on-chip RO-based sensors have also been proposed to measure the impact of die-package stress interaction on transistor performance [LXH+12]. In more ambitious attempts, it has even been tried to detect the effect of non-invasive attacks on

the system. A prime example is the integration of a custom LC oscillator into the front side of the IC package to detect the approach of an EM probe [HHM+14]. Another example is the measurement of the voltage drop caused by the inclusion of the shunt resistor into the PCB using an on-chip RO [LML12].

By taking a careful look at the outcomes of these sensors, it becomes evident that the changes in the behavior of RO sensors in some tampering scenarios are not distinguishable from changes resulting from the noise (i.e., thermal noise, process variation, etc.). Moreover, they have been designed only for specific system modifications, and therefore, do not cover a wide range of tampering scenarios. The main reason behind such weak performance of virtually all these solutions is their *passive* sensing mechanism. As described in the previous subsection, each component on an electronic board contributes to the overall PDN impedance in different frequency bands. To measure the PDN impedance at different frequencies, *each* discrete frequency needs to be measured by *actively* stimulating the system and measuring each response using RO sensors. If the system is stimulated using always-on stressor circuits or not stressed at all, the RO sensors can only measure the DC characteristics of the PDN, namely the resistance. Even if we consider the generated pulses by switching transistors in an RO sensor as stressors, the switching frequency and its harmonics are constant, and thus, the system is stimulated at only a few frequency points. Some PCB modifications might lead to resistance variations, and therefore, such passive sensors can detect them. However, many tamper events (as will be shown in this paper) lead to changes in the capacitance and inductance at specific frequencies, which are not measurable using passive sensors.

3 Methodology

3.1 Threat Model

This section reviews our threat model with the presumption of having an on-chip network analyzer capable of measuring the core and I/O PDN impedance profiles. For our threat model, we assume that the victim's electronic board is operated in an untrusted field and the attacker has physical access to it. The goal is to detect the attacker's tampering attempt on the system before she can mount SCA or FI attacks. The attacker is interested in the secrets and assets stored on a security-critical IC (e.g., a root-of-trust, cryptographic chip, etc.) soldered on a PCB. We assume that this security-critical IC contains an embedded network analyzer circuit 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 PCB remains intact. For non-FPGA systems, the system should be redesigned to include an FPGA-based or ASIC network analyzer. We assume that the PDN's impedance profiles of genuine samples have been collected in an enrollment phase in a trusted environment and stored on the same chip, which performs the impedance characterization. Later in the hostile environment, the impedance characterization can be performed before boot or during runtime to verify the system's integrity for possible tampering attempts. Upon detection of a discrepancy between the measured impedance profile and the golden impedance profile, an anti-tamper response (e.g., key zeroization) will be executed.

We assume that the adversary can physically tamper with all components on the core and I/O PDNs of the board connected to the victim chip, including adding/removing/replacing other components. Moreover, she can make physical connections with the core and I/O PDNs of the system to run measurements or communicate with the victim chip. She also can tamper with the IC package and pins and even place probes in the proximity of the package. However, we assume that she cannot tamper with the running impedance

characterization IP during the design phase (e.g., using hardware Trojan insertion) or operation phase (e.g., using remote fault injection attacks). Furthermore, the proposed sensing countermeasure only works on powered-on systems. Attacks on powered-off devices for netlist reverse-engineering purposes or non-volatile memory (NVM) content readouts using techniques such as scanning electron microscopy are out of the scope of this work.

3.2 Embedded Network Analyzers

The VNA functionality needs to be realized on one or multiple chips of an electronic board to enable self-contained monitoring of the physical integrity from PCB to chip level. In the field of power integrity, RF, and microwave engineering, there have been a few attempts to miniaturize VNAs for embedded systems. One prominent example is the open-source NanoVNA kits [Edy], which utilize off-the-shelf analog and digital chips (e.g., audio codec, microcontrollers, mixers, and oscillators) to realize small-size and portable VNAs. It is conceivable that small devices, such as NanoVNA, can be integrated into large electronic boards to stimulate the PDN and collect scattering/impedance traces during runtime. VNA can even be constructed from single-chip solutions such as the ADL5960 chip from Analog Devices [Ana], Inc. or custom analog designed chips [YHN11]. While such analog technologies provide high-resolution PDN characterizations, they are incompatible with many legacy and low-cost systems. Therefore, there have been parallel efforts [Ior18, ZAB+18, GOKT18, OBDS+19] to emulate the functionality of VNAs using the available digital resources on FPGAs for power integrity purposes.

A VNA on an FPGA consists of an active and a passive module, see Figure. 3. The active module needs to stimulate 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]). A sinusoidal current modulator controls the activation frequency and amount of consuming current of power waster circuits. The passive module, on the other hand, needs to measure the voltage drops using on-die voltage sensors and other analog-to-digital (ADC) circuits, such as ROs or Time-to-Digital converters (TDCs), using the available resources on FPGAs [MLS+20]. Knowing the amount of current consumption and voltage drop can reveal the approximate impedance value of the PDN seen by the logic circuits of the FPGA fabric at a specific frequency. Here we elaborate more on how such circuits approximate the impedance.

Currently, the two proposed FPGA-based VNA variants in the literature [Ior18, ZAB+18] use similar power wasting circuits based on buffer/inverter chains, but they use different sensing circuits for measuring the voltage drop, namely TDC-based ADCs [ZAB+18] and RO-based ADCs [Ior18]. As we use an RO-based ADC in this paper, we focus on how the frequency changes in a RO, measured by on-chip binary counters, can be converted to the 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:

$$Z_{PDN} = R_{PDN} + jX_{PDN} \tag{1}$$

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

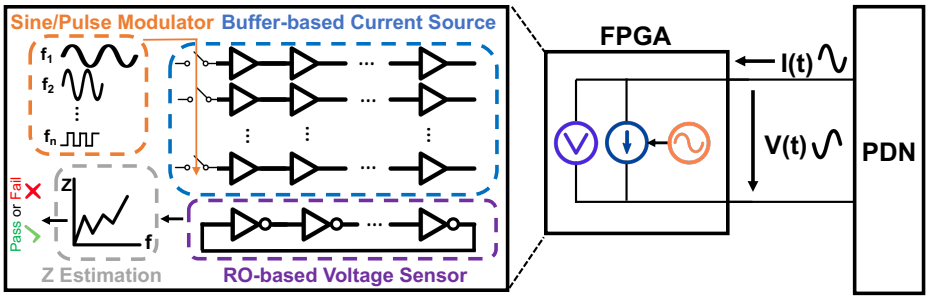


Figure 3: Main building blocks of an embedded VNA on FPGA.

when the power wasters are activated (V_{ON} and I_{ON}) or deactivated (V_{OFF} and I_{OFF}), cf. [Ior18, ZS18]

$$|Z_{PDN}| \approx \left|\frac{\Delta V}{\Delta I}\right| = \left|\frac{V_{OFF} - V_{ON}}{I_{OFF} - I_{ON}}\right| \tag{2}$$

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]

$$|Z_{PDN}| \approx \left|\frac{(\frac{f_{RO_{OFF}} - f_{RO_{ON}}}{f_{RO_{OFF}}})V_{SUPPLY}}{I_{OFF} - I_{ON}}\right| \tag{3}$$

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. Note that in the ideal case, the activation signal for the power wasting circuits should be a real sinusoidal wave, not a pulse wave. While sinusoidal waves at a given frequency have a single harmonic, pulse waves at the same frequency contain the sinusoidal frequency and several harmonics at the higher frequencies. This phenomenon is called total harmonic distortion (THD). Hence, to generate such sinusoidal wave signals on FPGAs, one can use either Coordinate Rotation Digital Computer (CORDIC) algorithms or Lookup-Table methods to store amplitude samples of a sinusoidal function over time. Such techniques, unfortunately, cannot generate sinusoidal waves higher than a few tens of megahertz using the fastest clocks on modern FPGAs. Therefore, at higher frequencies (e.g., higher than 100 MHz), we should inevitably use pulse waves to activate power-wasting circuits. Naturally, this causes inaccuracies in the estimation of the impedance. However, for tampering detection purposes, we are only interested in detecting changes in impedance values, not their absolute physical values. Thus, as long as the measurements for a specific frequency are performed consistently using sinusoidal or pulse waves, we still can rely on the estimated $|Z_{PDN}|$ for tampering detection.

3.3 Statistical Analysis on Noisy Measurements

Voltage and temperature variations can affect the behavior of the RO sensor on the chip, leading to noisy measurements. In this case, measurement repetition at each frequency point can provide us with a probability distribution for impedance values. Here, we provide the preliminary information required for the statistical analysis and comparison of these probability distributions. In our notation, m is the number of frequency points,

where the impedance of the PDN is measured using the embedded VNA. The number of measurement repetitions for frequency f_i is denoted by n. We define $\mathcal{Z}_i$ as a random variable corresponding to the impedance of the PDN at the frequency f_i. More precisely, we define $\mathcal{Z}_i^G$ and $\mathcal{Z}_i^T$ as random variables corresponding to the impedance of the PDN at the frequency f_i in the genuine and tampered system, respectively. The realization (i.e., the measured values) of the $\mathcal{Z}_i^G$ and $\mathcal{Z}_i^T$ in the j^{th} measurement are denoted by $z_{i_j}^G$ and $z_{i_j}^T$, respectively. We show the empirical cumulative distribution function (ECDF) of $\mathcal{Z}_i^G$ and $\mathcal{Z}_i^T$ with $\mathcal{G}_i$ and $\mathcal{T}_i$, respectively. Finally, we denote the probability density function (PDF) of $\mathcal{Z}_i^G$ and $\mathcal{Z}_i^T$ with γ_i and τ_i, respectively.

3.3.1 Wasserstein Metric

In order to quantify the difference between $\mathcal{Z}_i^G$ and $\mathcal{Z}_i^T$, we will use the Wasserstein metric [ACB17]. The Wasserstein metric is a function that gives a distance between two probability distributions. The p^{th} ($p \geq 1$) Wasserstein distance between γ_i and τ_i is given by

$$W_p(\gamma_i, \tau_i) = [\inf \mathbb{E}(d(\mathcal{Z}_i^G, \mathcal{Z}_i^T))^p]^{(1/p)} \tag{4}$$

where $\mathbb{E}(\mathcal{Z})$ is the expected value of a random variable $\mathcal{Z}$, d is the Euclidean distance between two points, and the infimum is taken over all joint distributions of the random variables $\mathcal{Z}_i^G$ and $\mathcal{Z}_i^T$ with PDFs γ_i and τ_i, respectively.

3.3.2 Empirical Distribution Function Tests

$\mathcal{Z}_i^G$ follows a Gaussian distribution with the mean μ_i^G and the deviation σ_i^G due to the existence of thermal noise, which has the characteristics of a white additive Gaussian process. However, $\mathcal{Z}_i^T$ does not necessarily follow a Gaussian distribution. In some cases (as we will see in Sect. 5), the tampering can indirectly contribute to unknown disturbances in the impedance measurement, which makes $\mathcal{Z}_i^T$ non-Gaussian. To compare $\mathcal{Z}_i^T$ and $\mathcal{Z}_i^G$, we can use empirical distribution function tests, which can also be applied to non-Gaussian distributions. We deploy two non-parametric statistical tests on samples $z_1, z_2, \cdots, z_n$ to detect the tamper events, namely Shapiro-Wilk (SW) and Kolmogorov-Smirnov (KS) tests. The SW test is a test for normality, testing whether measurement samples follow a normal distribution. The KS test is a *supremum*-based statistical testing, which is based on the largest vertical difference between two ECDFs. We refer the reader to the [RW11] for more information. KS test can be used to test whether two data samples come from the same distribution.

4 Experimental Setup

For our experiments, we used Digilent Arty S7 development boards [Diga] which contain AMD/Xilinx Spartan-7 FPGAs manufactured with a 28 nm technology. These boards have multiple power domains, namely, a 1 V domain supplying the core (V_{CCINT}) and Block RAMs (BRAMs) (V_{CCBRAM}) of FPGA, a 3.3 V domain supplying the FPGA I/O banks (V_{CCO}), and a 1.8 V domain as the auxiliary supply voltage (V_{CCAUX}). In this paper, we perform our measurements on V_{CCINT} and V_{CCO} PDNs as they are the main media for SCA/FI attacks. Figure. 4 shows the front and backside of the Arty S7 development boards used in our experiments. In Figure. 4a, the area in red color shows the jumper "JP3" used for bypassing the 10 mΩ shunt resistor, and in Figure. 4b, the areas in red and blue color show 47 nF and 470 nF decoupling capacitors, respectively.

We have used PIscanner IP [PIS, Ior18] for realizing a VNA on the FPGA. This IP generates current on the FPGA using configuration logic blocks (for the core voltage PDN) and I/O blocks (for I/O voltage PDN) by sequencing multiple transient switching currents

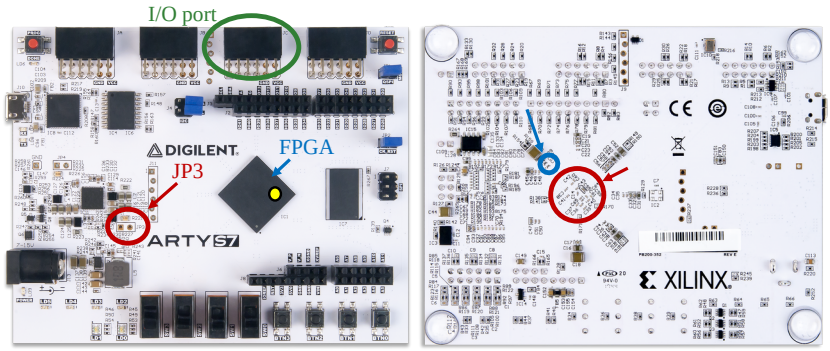


Figure 4: Digilent FPGA development kit. (a) Front side of the board. The area in red color shows the jumper used for bypassing the 10 mΩ shunt resistor. The highlighted area in green color shows one of the I/O ports. The highlighted point in yellow color on the FPGA shows the approximate location for the EM probe measurements with maximum coupling. (b) The backside of board. The areas in red and blue color show 47 nF and 470 nF decoupling capacitors, respectively.

to superimpose to an overall constant current. The design can measure the impedance with a resolution of 1 mΩ over 0 - 588 MHz. However, we performed the impedance measurements within 100 Hz - 588 MHz for this specific FPGA board since there was not much useful information between 0 - 100 Hz for our experiments. Moreover, due to large wavelengths between 0 - 100 Hz, the integration time is increased significantly. Impedance characterization beyond 1 GHz requires analog 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 Xilinx 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. Such a resolution is sufficient to detect permanent tamper events (e.g., capacitor removal) and temporary tampering (e.g., connecting probes) occurring in order of minutes/hours for a practical SCA/FI. More specifically, there is a trade-off between detection accuracy and scan time that can be controlled by tuning the number of frequency points measured. The IP occupies 963 FFs and 1459 LUTs. The cost of the IP is $2000. It is a one-time payment for all FPGAs of the same family. 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. Finally, we carried out offline statistical analyses (see Sect. 3.3) on the impedance signatures collected from the experimental setup mentioned above using MATLAB [Mat22]. We calculated Wasserstein distance in Sect. 5.3 using Python's scipy.stats library.

5 Results

This section presents our impedance characterization results for various classes of tamper events and physical conditions. There are probably unlimited tamper events that can occur to a sample, and naturally, we cannot cover all of them. However, to show the sensor's capability in covering different threats, we select a set of few tamper events, which can represent virtually all possible modifications. Therefore, we prioritize our experiments based on the physical distance of the tamper event to the chip's die, from the maximum to the minimum distance. Moreover, we make sure that we cover the entire frequency band by tampering with the resistive, capacitive, and inductive portion of the PDN impedance.

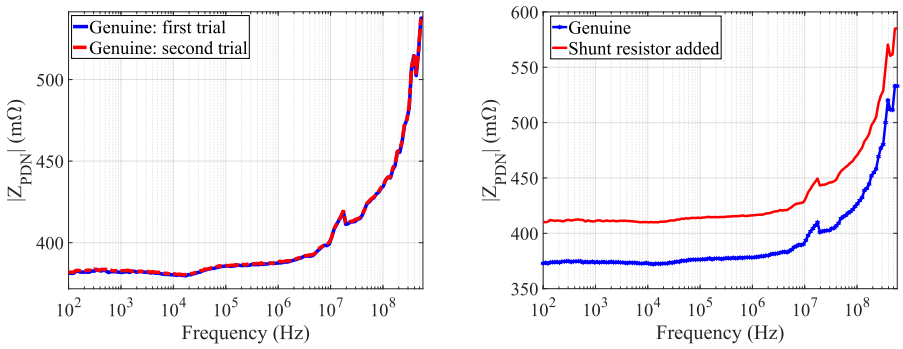


Figure 5: The mean of 105 impedance measurements over the frequency band of 100 Hz - 588 MHz (a) An untouched sample (intra-genuine measurements). (b) The board with added 10 mΩ shunt resistor.

Hence, we start by experimenting on a shunt resistor, which has the maximum distance from the FPGA chip, and we continue the experiments to observe the impact of tampering on the FPGA chip itself.

Since some of our performed modifications to the FPGA boards are irreversible (e.g., polishing a package), we had to use different boards from the same family for each tampering experiment. The Digilent Arty S7 kits have a 10 mΩ shunt resistor [Diga, Digb] with the possibility of bypassing it using a jumper (see JP3 jumper in Figure. 4a). We used the boards in the bypassed mode for our reference measurements for all experiments, except for the experiment in Sect. 5.2.2. To have enough data for statistical analysis, the PDN impedance profiles of all FPGA boards have been measured 105 times (for obtaining statistically significant results [DW09]) using the FPGA impedance characterization method described in Sect. 3.2 before any tampering. The measurements were carried out within the frequency band of 100 Hz - 588 MHz with logarithmic steps. The total number of frequency points was 152. After changing the physical condition of the boards or tampering with them, we repeated the impedance characterization 105 times over the same frequency range. It should be noted that all experiments were conducted at room temperature. Finally, we calculated the Wasserstein distance (WD) between the genuine and tampered samples' impedance signatures over the entire frequency band (i.e., between 100 Hz - 588 MHz) to quantitatively distinguish between legitimate and tampered samples.

5.1 Tamper Events not Causing External Disturbances

Here, we consider tamper events that do not cause further external disturbances on the sensor, and therefore, all the measurements on modified samples are mainly influenced by the thermal noise.

5.1.1 Intra-genuine Signature Consistency

In the first step, we wanted to assess the consistency of PDN impedance signatures for the same board over time. This is of great importance as it shows to what extent we can rely on a golden impedance signature. In this regard, we performed two sets of 105 measurements in two different trials for the same samples on different days and times. Figure. 5a illustrates the mean of the collected impedance traces for two trials of measurements on the same board, over the frequency band of 100 Hz - 588 MHz. According to Figure. 5a, it can be observed that the mean of impedance magnitudes are well-matched to each other. Figure. 11a shows the histograms for the intra-genuine measurements' trials at $f = 315.97$ MHz, where the maximum distance between the mean of two trails of the genuine boards'

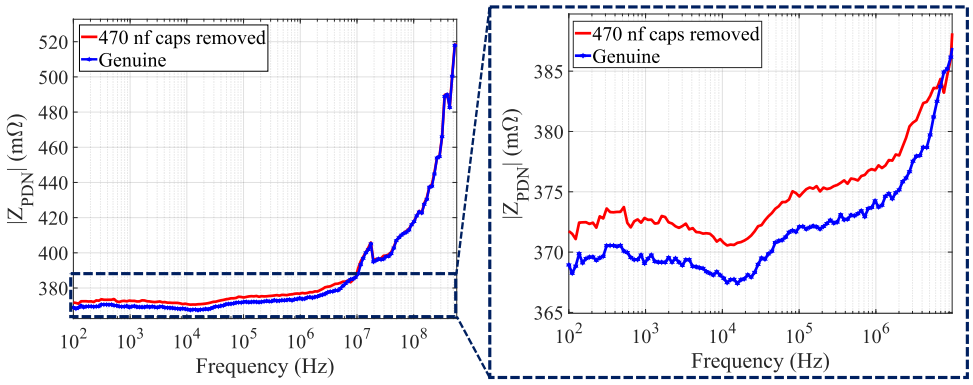


Figure 6: The mean of 105 impedance profile measurements for removing 470 nF decoupling capacitors over the frequency band of 100 Hz - 588 MHz. The right-side figure shows the zoomed-in view of the bandwidth with the most deviation from the mean graph.

measurements occurs. Form Figure. 11a, it can be seen that the maximum deviation between the mean of the measurements is 1.67 $m\Omega$.

5.1.2 Adding a Shunt Resistor

First, we emulated the primary preparation step for power analysis attacks, adding a shunt resistor on the victim PCB's power rails to enable the measurement of current fluctuations. Even if such shunt resistors exist on a genuine PCB, adversaries might want to replace them with other resistors to externally-amplify couplings of shares in protected cryptographic implementations [DCEM18, LBS19]. As we had bypassed the existing shunt resistor of the FPGA boards for all of our golden signature extractions, we just needed to remove the jumper to emulate the inclusion of a shunt resistor (see Figure. 4 (a)). The existing shunt resistor on samples has a 10 mΩ resistance[Diga, Digb]. The means of PDN impedance measurements for both genuine and tampered samples for 105 measurements are shown in Figure. 5b. As it can be observed, there is a considerable shift in the magnitude of the PDN impedance in the entire spectrum. This shift looks constant until the system's resonance frequency and starts to change in higher frequencies. For this case, the maximum deviation takes place at $f = 587.80$ MHz. Form Figure. 11b, it can be seen that the maximum deviation between the mean of the measurements is 52.08 $m\Omega$, which is 31.18 times the maximum deviation of the intra-genuine measurements (1.67 $m\Omega$). **Interpretation.** As described in Sect. 3.2, the impedance magnitude of the PDN can be written as $Z_{PDN} = R_{PDN} + jX_{PDN}$. The primary contributor to the shift in Figure. 5b is the resistance portion of the impedance R_{PDN}, which is independent of the frequency. However, resistors used on PCBs are not ideal, and thus, they contain parasitic capacitance and inductance and can show much higher impedance magnitudes at higher frequencies. Therefore X_{PDN} of the PDN impedance also plays a role in this shift.

5.1.3 Removing Decoupling Capacitors

We performed two independent sets of tampering on two different samples to observe the sensor's sensitivity to the decoupling capacitors' removal. First, we removed three 470 nF decoupling capacitors on one of the FPGA boards and measured the impedance profile over frequency. Second, we removed eight 47 nF decoupling capacitors on another FPGA board and measured the impedance profile to check their effect on the physical behavior of the system as well. The location of these two sets of capacitors is shown in Figure. 4(b). As decoupling capacitors behave as low-pass filters, the adversary usually removes these decoupling capacitors in real-world scenarios to amplify leakage through

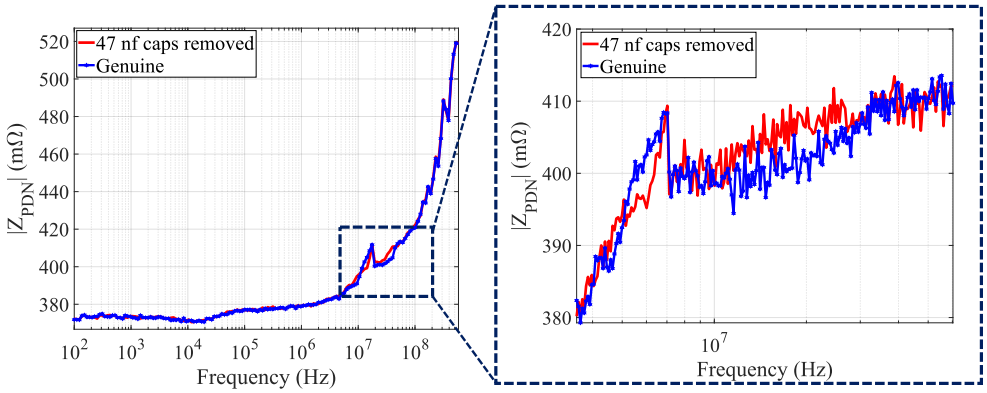


Figure 7: The mean of 105 impedance profile measurements for removing 47 nF capacitors from the board over the frequency band of 100 Hz - 588 MHz. The right-side figure shows the zoomed-in view of the bandwidth with the most deviation from the mean graph.

power consumption.

Figure. 6 and 7 demonstrate the mean of $|Z_{PDN}|$ profiles of 105 measurements for the genuine sample and the samples from which 470 nF and 47 nF decoupling capacitors have been removed, respectively. According to these results, it is observable that each set of decoupling capacitors contributes to a particular portion of the impedance spectrum. In Figure. 6 and 7, the right-side graphs show the zoomed-in view of the bandwidth where the most significant deviation from the genuine $|Z_{PDN}|$ signatures occurs.

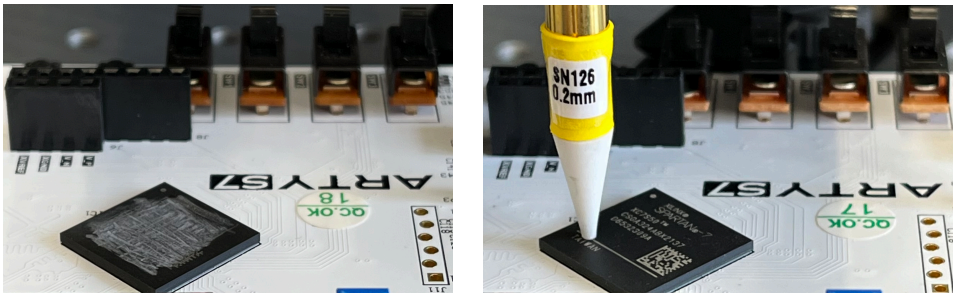
By removing 47 nF and 470 nF decoupling capacitors, the maximum deviation happens at $f = 39.90$ MHz and $f = 1.57$ kHz, respectively. Based on Figure. 11d and 11c, the maximum deviation between the mean of the measurements is $5.95m\Omega$ and 3.83 $m\Omega$ for 47 nF and 470 nF capacitors removal, respectively. It is observable that the maximum deviation for 47 nF and 470 nF capacitors removal cases is 3.5 and 2.29 times the maximum deviation of the intra-genuine measurements (1.67 $m\Omega$).

Interpretation. While 47 nF capacitors affect the frequency band of 3.69 - 60.36 MHz, 470 nF capacitors directly impact the lower frequency band below 9.4 MHz. This is in line with the theoretical expectations presented in Sect. 2.1, where the effect of smaller capacitors on the impedance is significant at higher frequencies due to their smaller physical dimensions, causing a resonance at higher frequencies.

5.1.4 Proximity of an EM Probe

Our next experiment analyzes the influence of placing a high-precision EM probe in the vicinity of the FPGA surface. The interesting fact about this experiment is that there is no physical connection between the probe's tip and the system. The hope is that a coupling between the EM probe and the metal layers of the chip affects the PDN impedance at high frequencies [HHM+14]. We used an EM probe station from Riscure with HP EM probe 125 SN126 0.2 mm to emulate this class of non-invasive attack [Ris].

We scanned the surface of the FPGA by placing the EM probe in the vicinity of the FPGA package surface in different locations to evaluate the effect of impedance coupling between the probe and the metal lines of the FPGA. The sensor and stressor circuits were implemented on the X0/Y0 bank of the Spartan 7 FPGA. While the physical location of metal lines can differ from the location of the utilized logic blocks on the FPGA, we still found the strongest coupling effect when the probe was located on top of the X0/Y0 bank (Figure. 8b. The mean of 105 measured impedance signatures for this attack can be seen in Figure. 9. The maximum deviation takes place at $f = 284.92$ MHz. Form Figure. 11e, the maximum deviation between the mean of the measurements is 13.65 $m\Omega$, which is 8.17 times the maximum deviation between the mean of the intra-genuine measurements.



(a) (b)

Figure 8: Devices under attack (a) Polished FPGA package (b) Placing an EM probe on top of the FPGA package.

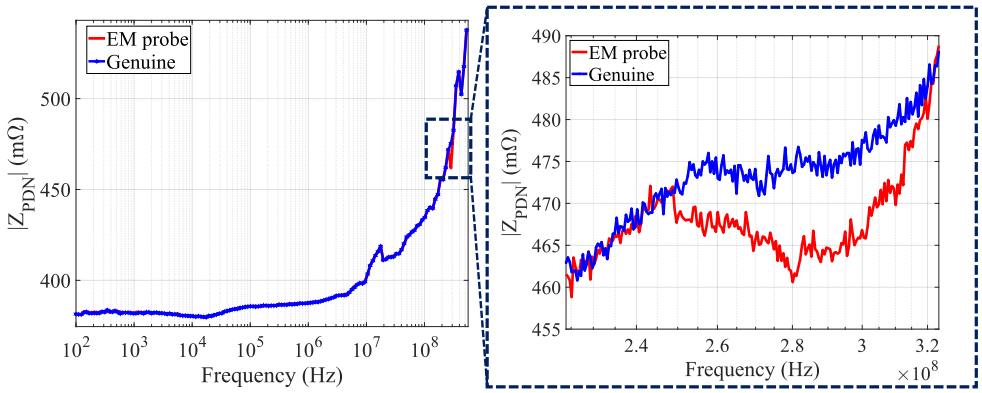


Figure 9: The mean of 105 impedance profile signatures when the EM probe is positioned over the left corner of the FPGA.

Interpretation. The observable effect can be explained using the cavity perturbation theory [Poz11]. According to this theory, when a small sample (here, the small cross section of the EM probe) is exposed to electric and magnetic fields of a structure (here, the FPGA), the sample perturbs the field distribution that causes a change in the resonant frequency of the structure. This coupling results in the field perturbation of the circuit and creates this added resonance frequency to the impedance profile as seen in Figure. 9.

5.1.5 IC Package Polishing

The goal of this experiment is to find out whether IC package polishing/removing has an impact on the PDN impedance. Package polishing is the main preparation step for carrying out semi- or fully-invasive attacks. To emulate this attack, we partially polished the surface of the FPGA package and measured the impedance profile magnitudes, see Figure. 8a. During the polishing of the IC package on the IC frontside, a small area of metal layers were exposed. The exposure of the die to the ambient light photons can disturb the measurements. Therefore, we carried out these measurements in an isolated dark room. Figure. 10 illustrates the mean of 105 impedance profile signatures for the genuine sample and the FPGA, whose package is partially polished and is placed in a dark room during the measurements. For this case, the maximum deviation of the mean graph occurs at $f = 430.96$ MHz. Form Figure. 11f, it can be seen that the maximum deviation between the mean of the measurements is 18.49 $m\Omega$, which is 11.07 times the maximum deviation of the intra-genuine measurements (1.67 $m\Omega$).

Interpretation. The plastic package behaves as a dielectric material contributing to on-chip PDN capacitance [Inc96]. Thus, polishing the package affects the system's PDN

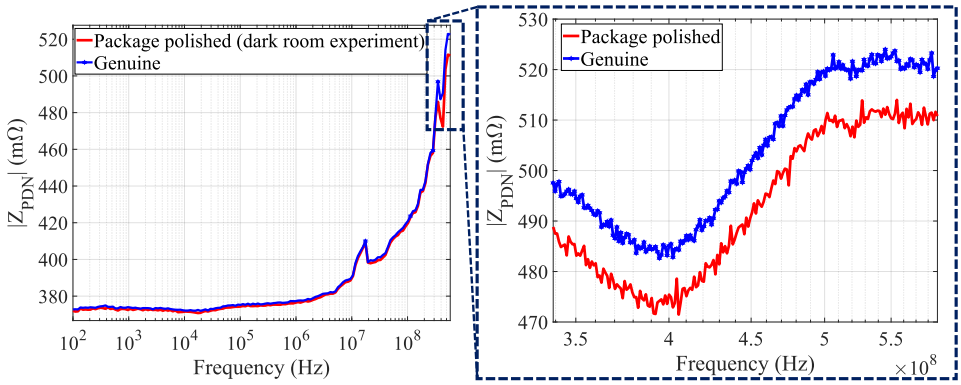


Figure 10: The mean of 105 impedance profile signatures when the surface of the FPGA package is polished.

impedance. Its effect is observable at high frequencies due to the smaller dimensions of IC structures. Note that we did not de-solder the FPGA for polishing.

5.2 Tamper Events with External Disturbances

Here, we present two sets of experiments where tampering causes extra environmental disturbances on the sensor. In these cases, thermal noise is not the only noise source for the measurements, and we observe an irregular non-Gaussian impact on the impedance measurement distribution of tampered samples.

5.2.1 IC Package Polishing with Exposure to Light

As mentioned in Sect. 5.1.5, the exposure of the die to the ambient light photons can disturb the measurements. As such a scenario still can occur in a real-world attack, we decided to perform the impedance characterization in this physical condition as well. Therefore, we conducted the measurements in a room where the board was exposed to the room light. Figure. 12a illustrates the mean of 105 impedance profile signatures for this set of measurements. As seen per results, there exists an unusual behavior in the impedance signatures for this case. Careful investigation of the results showed a significant fluctuation in impedance signatures in frequencies above the resonance frequency, where the overall impedance is dictated by the IC package and die. For this case, the maximum deviation takes place at $f = 388.61$ MHz. Form Figure. 12b, the maximum deviation between the mean of the measurements is 19.39 $m\Omega$, which is 11.61 times the maximum deviation between the mean of the measurements between the intra-genuine measurements (1.67 $m\Omega$). Figure. 12b shows that after such tampering, the data distribution is divided into two bell curves. This was not the case for the previous results where we investigated other classes of tamper events.

Interpretation. The unusual impedance signature in Figure. 12a could be due to the interaction of photons with metal layers and the active region of the chip, leading to local temperature variations, which affect both the sensor and on-chip impedance.

5.2.2 Connecting an Oscilloscope Probe

In this experiment, we connected an oscilloscope probe to the jumper "JP3" pins to analyze the impact of connecting a measurement device without any other physical modifications to the system. Figure. 12c shows the impedance profile of 105 measurements conducted using the proposed verification method for this case. Note that connecting an oscilloscope probe necessitates removing the jumper "JP3" from the PCB's PDN. Therefore, the golden

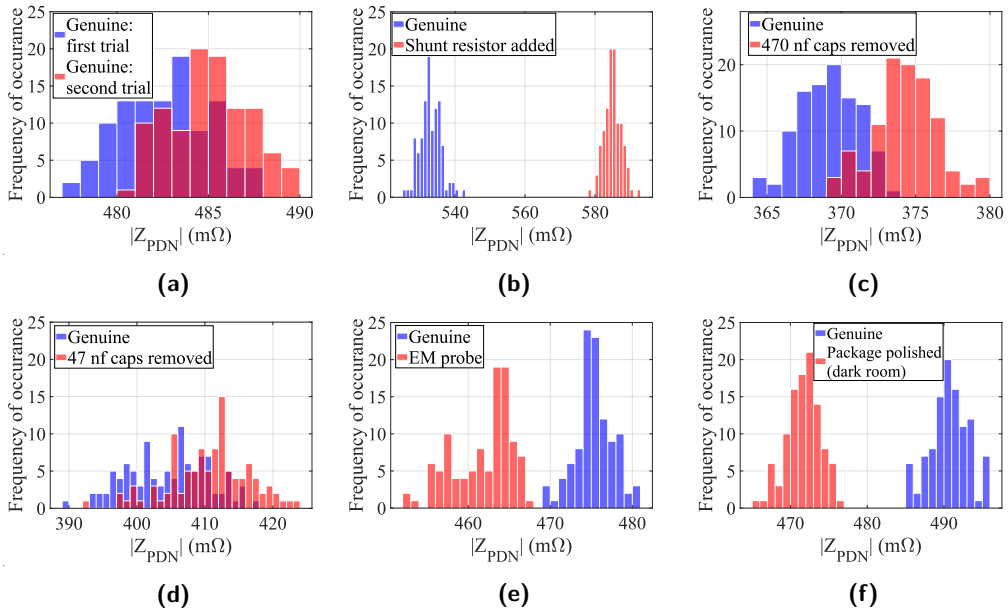


Figure 11: Impedance histogram representations. All histograms are plotted at the frequency point where the distance between the mean of the measurements is maximum. (a) Intra-genuine measurements at $f = 315.97$ MHz. (b) Adding shunt resistor ($f = 587.80$ MHz). (c) 470 nF capacitors removed ($f = 1.57$ kHz). (d) 47 nF capacitors removed ($f = 39.90$ MHz). (e) EM probe on the location showed in Figure. 4(a) in yellow color ($f = 284.92$ MHz). (f) FPGA package polished (not exposed to light, $f = 430.96$ MHz).

sample for this experiment would be the FPGA board without bypassing the shunt resistor. We did not have complete control over external disturbances during the measurements in this attack. An example of such disturbances is slight probe movements that can happen during the measurements. Moreover, the unshielded cable and probe connector can behave like an antenna injecting EM interference to the power rails of the chip, which influences the sensor response. The maximum deviation between the mean of the measurements takes place at $f = 53.15$ kHz. From Figure. 12d, the maximum distance between the mean of the measurements is 6.05 $m\Omega$, which is 3.62 times the maximum distance for intra-genuine measurements (1.67 $m\Omega$).

Interpretation. Adding the oscilloscope probe caused a shift to lower impedance values since the oscilloscope's output resistance would be in parallel with the shunt resistor, and as a result, the overall Z_{PDN} will be shifted to a lower value (the shift is around 4 $m\Omega$). Moreover, the oscilloscope cable can create an inductance, which further affects the impedance at higher frequencies. Due to the slight local movements of the oscilloscope probe during the measurements, the shape of the distribution is deviated from normal, as seen in the histogram representation in Figure. 12d.

5.3 Statistical Analysis of Impedance Traces

In this section, we present the statistical analyses conducted for our experiments. According to the experimental results presented in subsections 5.1, and 5.2, a single measurement can successfully detect some tamper events (e.g., a shunt resistor addition or package polishing). However, for some other tamper events, the impedance measurements of genuine and tampered samples overlap. In these cases, integration is necessary to obtain the measurement's statistics and, thus, compare the statistical features of the data. Furthermore, based on the results presented in Figure. 11, tamper events can change not

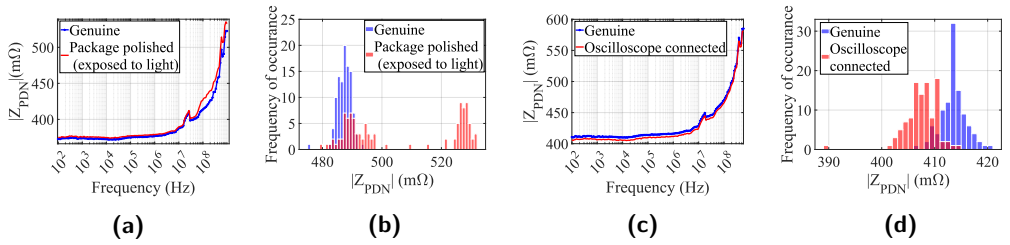


Figure 12: (a) The mean of 105 impedance profile signatures for polishing the FPGA package and measuring impedance profile in a room exposed to light. (b) Histograms at $f = 388.61$ MHz for polishing the FPGA package in a room exposed to light. (c) The mean of 105 impedance profile signatures for connecting the oscilloscope probe to the DUT. (d) Histograms at $f = 53.15$ kHz for connecting the oscilloscope probe to the DUT.

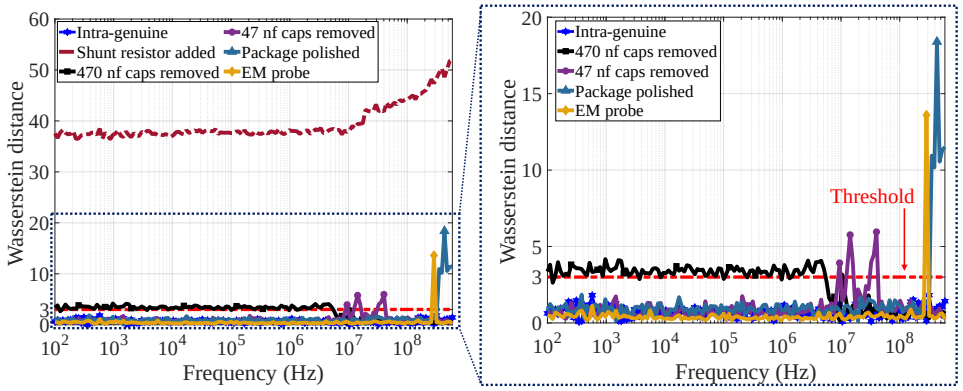
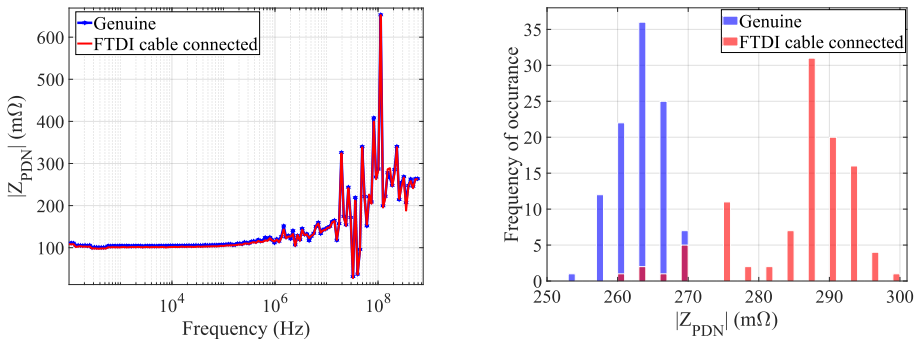


Figure 13: The Wasserstein distance profile for intra-genuine measurements and different attacks over 100 Hz - 588 MHz band (core voltage PDN). The figure on the right shows the zoomed-in view of the left-side figure, excluding the shunt resistor added experiment.

only the mean of the measurements but also the variance or the entire shape of the PDF. Therefore, we deploy the Wasserstein distance (WD) metric (explained in Sect. 3.3.1) to quantify the dissimilarities between the collected impedance traces of genuine and tampered samples. We computed the WD for intra-genuine measurements as well as tamper events performed throughout this work. As the disturbances in some tampering experiments are not systematic and repeatable, they cannot be directly compared with other results. Hence, we excluded these particular experiments from the WD analysis. The WD distance profile is given in Figure. 13 within the frequency band of 100 Hz - 588 MHz. As it can be observed, the WD for various tamper events and physical conditions is frequency-dependent. Note that the frequency axis of Figure. 13 is scaled logarithmically. Thus, the effects of tamper events on WD in higher frequency bands are seen as narrow peaks.

The magnitude of the WD metric shows that all tamper events performed in this paper can be distinguished if we use the sensor at the right frequency. Moreover, the detection thresholds for different tamper events, and their corresponding frequency bands, can be selected differently. However, we still can define a global threshold at $WD = 3$ for the tampering experiments presented in this work without causing any false alarms. Naturally, this threshold should be adjusted for different systems and possible tamper events. Moreover, more research is probably required to consider a broader range of tamper events and their influence on the WD metric.



(a) (b)

Figure 14: Connecting the FTDI cable to one of the I/O ports. (a) The mean of 105 impedance profile signatures. (b) Histogram representation ($f = 169.85$ MHz).

6 Discussion

6.1 Coverage and Comparison of the Sensor

Spatial Coverage: A high spatial coverage sensor ensures that most physical locations of the system can be sensed. To increase the spatial coverage of the proposed on-chip impedance sensing method, one can realize multiple RO or TDC sensors and distribute them around the core and I/O PDNs of the chip. In this case, the sensed values of multiple sensors can be compared and analyzed. Distributing sensors on the FPGA has been shown to increase the spatial coverage of the embedded network analyzer for power integrity purposes [ZAB+18]. For instance, in our case, it can improve the detection of a close-distant EM probe at various locations of the IC package. Note that on larger systems with multiple PDNs, each power domain requires such embedded network analyzers for impedance characterization. For instance, in case of the deployed FPGA board in this work, the I/O PDN is separate from the core PDN of the FPGA. Therefore, any modification to I/O PDN will be hidden from the core PDN sensor.

Realizing a network analyzer for other PDNs might be challenging as enough required logic resources might not be available to realize the sensor circuits. For I/O PDN sensing on FPGAs, IOBUF ROs [BEG+21] can be deployed as the sensor to monitor the voltage drop on I/O banks. We performed an experiment using the IOBUF ROs to assess the feasibility of detecting a physical connection to I/O ports. We connected an FTDI chip through three wires (TX, RX, and GND) to one of the I/O ports of the FPGA board (see Figure. 4 (a)) and measured the impedance profile of the I/O voltage PDN. The mean of 105 measurements is depicted in Figure. 14a. In this figure, the maximum deviation is detected at 169.85 MHz, in which the shift in the impedance magnitude is 22.42 $m\Omega$. There also exists a shift between 3-7 $m\Omega$ at lower and middle range frequencies. More fluctuation in the impedance profile is observed at higher frequencies. However, these variations were consistent in all measurements, and the detected changes at different portions of the spectrum are reliable.

Comparison with Related Work: Table 1 compares the proposed VNA sensing method in this work with other on-chip sensing methods in the literature in terms of FPGA compatibility and detection capability. The proposed method enables the detection of resistive, capacitive, and inductive tamper events in both PCB/IC core PDNs as well as I/O PDNs, which makes it superior to other related works. Unfortunately, the overhead of these solutions cannot be compared fairly due to the deployment of different IC platforms for sensing and the lack of reported resource utilization for some of these sensors.

Table 1: The comparison between embedded sensing methods.

Sensing Method	FPGA Compat.	Detection capability					
		Resistive Tamp.	Inductive Tamp.	Capacitive Tamp.	PCB PDN Covg.	IC PDN Covg.	I/O PDN Covg.
RO Array[LML12]	✓	✓	×	×	✓	✓	×
RO Array[WHT19]	✓	✓	×	×	✓	✓	×
IOBUF RO[BEG+21]	✓	✓	×	×	×	×	✓
Trace-based RO[GXTF17]	✓	✓	×	×	✓	✓	✓
Trace-based RO[ZRS21]	✓	✓	×	×	✓	✓	✓
Trace ADC[PHB16]	×	✓	×	×	×	×	✓
ASIC RO Array[LXH+12]	×	✓	×	×	?	✓	×
LC Oscillator[HHM+14]	×	×	✓	✓	×	✓	×
TDR[FNH+18]	×	✓	✓	✓	×	×	✓
VNA (ImpedanceVerif)	✓	✓	✓	✓	✓	✓	✓

✓: Yes, ×: No, ?: Unknown **Compat.**: Compatible, **Tamp.**: Tampering, **Covg.**: Coverage

6.2 Success Rate for Reversing Physical Tampering

In some attack scenarios, the adversary might physically tamper (i.e., add, remove, or replace components) with the powered-off device or during a period of time where the sensor is inactive. In such scenarios, a question arises about the feasibility of undoing the tampering effect on the impedance before the activation of the sensor. Here we should elaborate on a couple of points. First, note that the proposed sensor in this work senses a two-dimensional parameter, i.e., the magnitude of the impedance, which itself is a function of frequency. Each physical tamper event affects the PDN impedance magnitude over the entire spectrum. Therefore, the adversary is theoretically required to equalize the impedance curve using electrical components, which is a hard, if not impossible, task due to the following reasons. Components' parasitics cause the most local maxima and minima of the impedance curve over the frequency, and hence, replacing components even with identical samples demonstrates different parasitics. Furthermore, even re-soldering the same removed component to the system or desoldering an added component will not deliver the same signature as the solder wire or flux characteristics will be changed. However, reversing physical tampering might still be feasible if the tampering impact on the entire spectrum is less than the detection threshold of the sensor.

Second, the tamper events can cause changes to the shape of impedance traces distribution, which are hard to hide or reverse. We performed empirical distribution function tests (see Sect. 3.3.2) on some of our tamper events to see such changes. The first row of Table. 2 (SW test) shows the percentage of the number of the frequency points where impedance distributions deviate from the normal distribution. The second row (KS test) shows the percentage of the number of the frequency points where the impedance distribution of the modified sample is different from the impedance distribution of the genuine sample to the total number of frequency points. As it can be observed from the SW test, because of the external disturbances during or after tampering, the distributions are deviated from normal (compare with Figure. 12b and 12d). Also, from the KS test results, we can conclude that the distributions of the samples under attack are different from the genuine ones depending on the type of modifications. As a result, the attacker needs to correct all these discrepancies in all frequency points to be able to undo the tampering.

Third, in our threat model, the genuine impedance signature is stored on the chip, and thus, the adversary does not have access to it for analysis and equalization. We assume that the signature can only be read out using semi- or fully-invasive techniques, which will already change the PDN characteristics. Even if the adversary recovers a genuine signature from another training sample, it will differ from another sample's signature due to the process variations and existing parasitics. As a result, the attacker cannot observe the same impedance that has been used during the enrollment phase.

Table 2: Dissimilarity ratio percentage based on statistical test results for different attacks.

Test result	Intra-Genuine	47 nF caps removed	Oscilloscope connected	Package polished (exposed to light)
SW test	N/A	5.92 %	13.81 %	33.55 %
KS test	0 %	11.18 %	100 %	100 %

6.3 Robustness to Environmental and Malicious Noise

Voltage and Temperature Variations: As mentioned in Sect. 3.3, the RO sensor's output (here $f_{RO_{ON}}$) can suffer from temperature variations. Naturally, measurement repetition and averaging can minimize the effect of noise. In addition to integration, to compensate for the thermal drift, we consider the relative (and not the absolute) frequency values of RO in both the idle and active states of the measurements at each frequency point. Therefore, we always measure the current reference point (i.e., $f_{RO_{OFF}}$) of the idle state of the FPGA and then activate the stressor and measure the $f_{RO_{ON}}$. In this case, the reference point is updated for each measurement, and the effect of the temperature on the sensor is minimized. Note that temperature can also have a direct systematical impact on the impedance of the PDN [BFGG16]. In this case, the impedance signatures of a few temperature points should be collected in the enrollment phase. In the verification phase in the field, based on the system's temperature (e.g., using the die temperature sensor), the associated golden signature can be used to compare the measurements and golden signature.

Voltage variations can also have an adverse impact on the RO sensor behavior. If other active ICs share the same PDN, their activity might cause severe voltage drops, and thus, distort the RO sensor inside the FPGA. In this case, the impedance can be measured when other active components are idle (e.g., before booting). Another option is to take the maximum voltage drop of other components as additive noise into account during the enrollment phase and later adjust a detection threshold accordingly. To be more specific, if impedance characterization should be performed when other components are switching, we should consider the worst-case scenario, i.e., maximum possible voltage ripple of different components and, consequently, their impact on the RO sensor frequency. Increased voltage ripple will require a higher detection threshold and hence can decrease the detection confidence of the system.

The changes in the voltage and temperature can also be induced by the adversary to fool the sensor with the intention of masking the effect of the tamper event. In this case, we elaborate on a couple of points. First, as mentioned in the previous subsection (Sect. 6.2), the adversary does not have access to the golden impedance signature of the device, and hence, she does not know the exact required amount of equalization to reconstruct the golden impedance profile. Second, an adversary should bypass the voltage regulator and connect her voltage supply or function generator to the board to change the voltage. As shown in Sect. 5, such connections can be detected by impedance sensing. Moreover, most voltage variations can also be detected using on-die voltage sensors. Finally, the temperature has a global effect on the impedance curve, and its impact at different frequency bands is different. Thus, it is challenging to mask the effect of a tamper event in a single frequency band using a global parameter such as temperature.

EM/RF Noise: There might be some confusion if one compares impedance sensing with side-channel sensing methods (e.g., [PKR20, PSK+22]) for verification purposes. One might think that similar to the susceptibility of side-channel signals to EM/RF noise, impedance values might also suffer from the same adverse effect. However, in contrast to side-channel signals, the overall impedance of the system is constant and determined by the amount of materials (i.e., the dielectric) and their geometry used in fabricating PCBs and ICs. Naturally, while the impedance value might be affected under extreme mechanical stress or temperature/humidity variations, it is not impacted by electromagnetic interference.

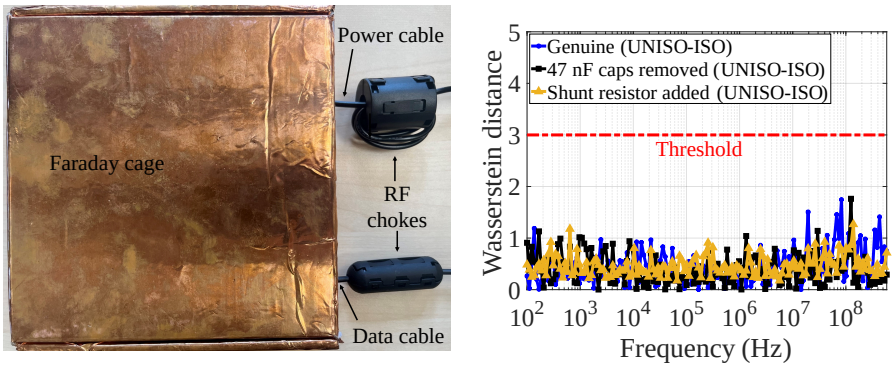


Figure 15: (a) The Faraday cage setup used for isolated measurements. (b) Wasserstein distance between isolated (ISO) and unisolated (UNISO) measurements for the genuine board, removing 47 nF capacitors, and adding shunt resistor experiments.

However, as mentioned earlier in this subsection, the behavior of the impedance sensing circuit (here, the on-chip RO) might be sensitive to such noise on the power line. However, because of the existence of the voltage regulator on the board, such noise is usually filtered before reaching the IC. Furthermore, it is very unlikely that the existing radio waves in the room are strong enough to cause any disturbance to the implemented RO on the chip. We conducted extra experiments to validate our assumption about the minimal impact of RF noise on our measurements. To make a comparison, we isolated the experiment condition using a Faraday cage and RF noise suppressor chokes for the cables, see Figure. 15a. As it can be observed in Figure. 15b, the maximum WD over various frequencies for a genuine board in an unisolated and isolated environment is less than 1.7, which is comparable to the measured WD between two genuine samples in an unisolated environment (see Figure. 13). Moreover, $WD = 1.7$ is smaller than the threshold (i.e., $WD = 3$) required to detect tamper events. Figure. 15b also shows WD for the tampered PCB (the 47 nF capacitors removal and addition of the 10 mΩ shunt resistor experiments) between unisolated and isolated environments. Similar to the obtained WD for the genuine sample between unisolated and isolated environments, the maximum WD for tamper events is very small and falls below the defined threshold of $WD = 3$. This confirms that there is no significant difference in the measurement outcomes, and hence, EM/RF noise is not a relevant factor for ImpedanceVerif.

6.4 ImpedanceVerif as PUF?

During our experiments, we have observed that different genuine samples demonstrate slight PDN impedance differences compared to each other due to the process variation. Therefore, there might be a potential to deploy such impedance variations to construct seamless tamper-evident PUFs for the entire system. Moreover, it might be feasible to realize the concept of *Virtual Proofs of Reality* [RMHX+15] for the entire system. However, to meet the PUF requirements, the inter-distance of impedance variations between genuine boards should be large enough to uniquely identify each board. Estimating the inter-distance requires extensive measurements on a large number of boards, which was beyond the scope of this work. If the inter-distance requirements are met, then it is also conceivable to apply PUF key derivation techniques proposed in [IU19, GXKF22] to extract high-entropy keys from PDN impedance measurements.

7 Conclusion

In this work, we presented a self-contained physical verification framework, *ImpedanceVerif*, which is based on the impedance characterization of the system's power distribution network (PDN). We first explained that various components of an electronic board have a distinct contribution to the PDN's impedance signature at different frequency bands. Hence, any tampering activity on the board will lead to changes in PDN's impedance. We further demonstrated that the functionality of embedded network analyzers can be realized on commercial FPGAs without any extra components and modifications to monitor the integrity of the PDN impedance. To experimentally validate our claim, we implemented an embedded network analyzer on commercial FPGAs and conducted extensive experiments for various classes of attack conditions for PCBs and IC packages required for conducting different physical attacks. We showed that by choosing the Wasserstein distance as a statistical metric, we were able to detect various classes of tamper events (e.g., the inclusion of a shunt resistor, proximity of an EM probe to the IC, or a polished IC package) at distinct frequency bands with high confidence. Finally, we expect that embedded network analyzers on ASICs will achieve higher precision and higher bandwidth in the future using appropriate analog technologies (e.g., see [Ana]). Such future technologies enable a high-confidence detection of more sophisticated tamper events.

Acknowledgment

This effort was sponsored in part by Cisco Research program and in part by NSF under the grant number 2117349. In addition, we gratefully thank William L. Appleyard at Worcester Polytechnic Institute (WPI) for preparing the samples, Faraday cage, and cables. We would also like to thank Prof. Fatemeh (Saba) Ganji at WPI for her valuable insights into the selection of statistical metrics. Finally, we would also like to thank Stephen Bitar and Prof. Sergey Makarov at WPI for their helpful comments about the RF shielded enclosures.

References

[ABIa] ABI Electronics. SENTRY Counterfeit IC Detector. URL: https://www.abielectronics.co.uk/Products/SENTRYCounterfeitICDetector.php.

[ABIb] ABI Electronics. SYSTEM 8 Advanced Matrix Scanner (AMS). URL: https://www.abielectronics.co.uk/Products/SYSTEM%208%20AMS.php.

[ACB17] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *International conference on machine learning*, pages 214–223. PMLR, 2017.

[Ana] Analog Devices. ADL5960 – 10 MHz to 20 GHz, Integrated Vector Network Analyzer Front-End. URL: https://www.analog.com/media/en/technical-documentation/data-sheets/adl5960.pdf.

[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.

[BFGG16] Nestor Berbel, Raúl Fernández-García, and Ignacio Gil. Modeling technique of the conducted emission of integrated circuit under different temperatures. *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, 29(2):291–300, 2016.

[Bog10] Eric Bogatin. *Signal and Power Integrity–Simplified*. Pearson Education, 2010.

[DCEM18] Thomas De Cnudde, Maik Ender, and Amir Moradi. Hardware masking, revisited. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, page 123–148, May 2018.

[Diga] Digilent. Arty S7™ FPGA Board Reference Manual. URL: https://digilent.com/reference/_media/reference/programmable-logic/arty-s7/arty-s7_rm.pdf.

[Digb] Digilent. Arty S7™ FPGA Board Schematic. URL: https://digilent.com/reference/_media/arty:arty_sch.pdf.

[DW09] Scott DW. Sturges' rule. *Wiley Interdiscip Rev Comput Stat*, 1(3):303–06, 2009.

[Edy] Edy555. NanoVNA. URL: https://nanovna.com/.

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

[FNH+18] Daisuke Fujimoto, Shota Nin, Yu-Ichi Hayashi, Noriyuki Miura, Makoto Nagata, and Tsutomu Matsumoto. A demonstration of a ht-detection method based on impedance measurements of the wiring around ics. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 65(10):1320–1324, 2018.

[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.

[GXKF22] Kathrin Garb, Marvin Xhemrishi, Ludwig Kürzinger, and Christoph Frisch. The wiretap channel for capacitive puf-based security enclosures. *arXiv*, 2022.

[GXTF17] Zimu Guo, Xiaolin Xu, Mark M Tehranipoor, and Domenic Forte. MPA: Model-assisted PCB attestation via board-level ro and temperature compensation. In *2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pages 25–30. IEEE, 2017.

[HHM+14] Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki. Em attack is non-invasive? - design methodology and validity verification of em attack sensor. *Cryptographic Hardware and Embedded Systems*, 8731:1–16, 2014.

[HMH+12] Johann Heyszl, Dominik Merli, Benedikt Heinz, Fabrizio De Santis, and Georg Sigl. Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis. In *International Conference on Smart Card Research and Advanced Applications*, pages 248–262. Springer, 2012.

[Inc96] Intel Inc. Intel packaging databook. https://www.intel.cn/content/dam/www/public/us/en/documents/packaging-databooks/packaging-chapter-04-databook.pdf, 1996.

[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.

[IU19] Vincent Immler and Karthik Uppund. New insights to key derivation for tamper-evident physical unclonable functions. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 30–65, 2019.

[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)*. IEEE, 2021.

[LBS19] Itamar Levi, Davide Bellizia, and François-Xavier Standaert. Reducing a masked implementation's effective security order with setup manipulations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 293–317, 2019.

[LFH10] Sungkeun Lim, Jiwei Fan, and Alex Q Huang. Transient-voltage-clamp Circuit Design based on Constant Load Line Impedance for Voltage Regulator Module. *IEEE Transactions on Industrial Electronics*, 57(12):4085–4094, 2010.

[LML12] Adrien Le Masle and Wayne Luk. Detecting power attacks on reconfigurable hardware. In *22nd International Conference on Field Programmable Logic and Applications (FPL)*, pages 14–19. IEEE, 2012.

[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.

[Mat22] MathWorks Inc. MATLAB - Statistical and Machine Learning Toolbox. url: https://www.mathworks.com/products/statistics.html, 2022.

[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.

[OBDS+19] Sergei Odintsov, Ludovica Bozzoli, Corrado De Sio, Luca Sterpone, and Artur Jutman. A new FPGA-based detection method for spurious variations in PCBA power distribution network. In *2019 IEEE 22nd International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, pages 1–6. IEEE, 2019.

[PHB16] Steven Paley, Tamzidul Hoque, and Swarup Bhunia. Active protection against PCB physical tampering. In *2016 17th International Symposium on Quality Electronic Design (ISQED)*, pages 356–361. IEEE, 2016.

[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.

[PKR20] Gor Piliposyan, Saqib Khursheed, and Daniele Rossi. Hardware trojan detection on a PCB through differential power monitoring. *IEEE Transactions on Emerging Topics in Computing*, 2020.

[Poz11] David M Pozar. *Microwave engineering*. John wiley & sons, 2011.

[PSK+22] Hammond Pearce, Virinchi Roy Surabhi, Prashanth Krishnamurthy, Joshua Trujillo, Ramesh Karri, and Farshad Khorrami. Detecting hardware trojans in PCBs using side channel loopbacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2022.

[Pup20] Peter J Pupalaikis. *S-parameters for Signal Integrity*. Cambridge University Press, 2020.

[Ris] Riscure. EM probe station. Riscure. URL: https://getquote.riscure.com/en/quote/2101064/em-probe-station.htm.

[RMHX+15] Ulrich Rührmair, JL Martinez-Hurtado, Xiaolin Xu, Christian Kraeh, Christian Hilgers, Dima Kononchuk, Jonathan J Finley, and Wayne P Burleson. Virtual Proofs of Reality and their Physical Implementation. In *2015 IEEE Symposium on Security and Privacy*, pages 70–85. IEEE, 2015.

[RW11] Nornadiah Mohd Razali and Yap Bee Wah. Power comparisons of shapiro-wilk , kolmogorov-smirnov , lilliefors and anderson-darling tests. *Journal of Statistical Modeling and Analytics*, 2(1):21–33, 2011.

[Sko17] Sergei Skorobogatov. How microprobing can attack encrypted memory. In *2017 Euromicro Conference on Digital System Design (DSD)*, pages 244–251. IEEE, 2017.

[WHT19] Xiaoxiao Wang, Yueying Han, and Mark Tehranipoor. System-Level Counterfeit Detection Using On-Chip Ring Oscillator Array. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12):2884–2896, 2019.

[YHN11] Kumpei Yoshikawa, Takushi Hashida, and Makoto Nagata. An on-chip waveform capturer for diagnosing off-chip power delivery. In *2011 IEEE International Conference on IC Design & Technology*, pages 1–4. IEEE, 2011.

[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.

[ZAK+17] Shuze Zhao, Ibrahim Ahmed, Armina Khakpour, Vaughn Betz, and Olivier Trescases. A robust dynamic voltage scaling scheme for FPGAs with ir drop compensation. In *2017 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pages 2939–2944. IEEE, 2017.

[ZHS+15] Biyao Zhao, Chenxi Huang, Ketan Shringarpure, Jun Fan, Bruce Archambeault, Brice Achkir, Samuel Connor, Michael Cracraft, Matteo Cocchini, Albert Ruehli, et al. Analytical PDN Voltage Ripple Calculation using Simplified Equivalent Circuit Model of PCB PDN. In *2015 IEEE Symposium on Electromagnetic Compatibility and Signal Integrity*, pages 133–138. IEEE, 2015.

[ZRS21] Dongrong Zhang, Qiang Ren, and Donglin Su. A novel authentication methodology to detect counterfeit PCB using PCB trace-based ring oscillator. *IEEE Access*, 9:28525–28539, 2021.

[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+22] Huifeng Zhu, Haoqi Shan, Dean Sullivan, Xiaolong Guo, Yier Jin, and Xuan Zhang. PDNPulse: Sensing PCB anomaly with the intrinsic power delivery network. pages 1–17. arXiv, 2022.