LeakyOhm: Secret Bits Extraction using Impedance Analysis

Saleh Khalaj Monfared
Worcester Polytechnic Institute
Worcester, MA, USA
skmonfared@wpi.edu

Tahoura Mosavirik
Worcester Polytechnic Institute
Worcester, MA, USA
tmosavirik@wpi.edu

Shahin Tajik
Worcester Polytechnic Institute
Worcester, MA, USA
stajik@wpi.edu

ABSTRACT

The threats of physical side-channel attacks and their countermeasures have been widely researched. Most physical side-channel attacks rely on the unavoidable influence of computation or storage on current consumption or voltage drop on a chip. Such data-dependent influence can be exploited by, for instance, power or electromagnetic analysis. In this work, we introduce a novel non-invasive physical side-channel attack, which exploits the data-dependent changes in the impedance of the chip. Our attack relies on the fact that the temporarily stored contents in registers alter the physical characteristics of the circuit, which results in changes in the die's impedance. To sense such impedance variations, we deploy a well-known RF/microwave method called scattering parameter analysis, in which we inject sine wave signals with high frequencies into the system's power distribution network (PDN) and measure the echo of the signals. We demonstrate that according to the content bits and physical location of a register, the reflected signal is modulated differently at various frequency points enabling the simultaneous and independent probing of individual registers. Such side-channel leakage challenges the t-probing security model assumption used in masking, which is a prominent side-channel countermeasure. To validate our claims, we mount non-profiled and profiled impedance analysis attacks on hardware implementations of unprotected and high-order masked AES. We show that in the case of the profiled attack, only a single trace is required to recover the secret key. Finally, we discuss how a specific class of hiding countermeasures might be effective against impedance leakage.

KEYWORDS

Impedance Analysis, Side-Channel Attack, Scattering Profiling, Masked Implementation, Template Attacks

ACM Reference Format:
Saleh Khalaj Monfared, Tahoura Mosavirik, and Shahin Tajik. 2023. LeakyOhm: Secret Bits Extraction using Impedance Analysis. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3548606.3560649

1 INTRODUCTION

Physical side-channel leakages can compromise the security of cryptographic implementations on integrated circuits (ICs). Such leakages exist due to the inevitable impact of computation and storage on current consumption or voltage drop on a chip. These data-dependent fluctuations reveal themselves through various measurable quantities, such as power consumption [47], electromagnetic emanation [45], acoustic waves [28], photon emission [27], and thermal radiation [37]. Over the last decades, these quantities have been exploited in different classes of side-channel analysis (SCA) attacks for breaking the security of various cryptographic implementations. At the same time, various countermeasures (e.g., hiding and masking) have been developed to defeat these attacks.

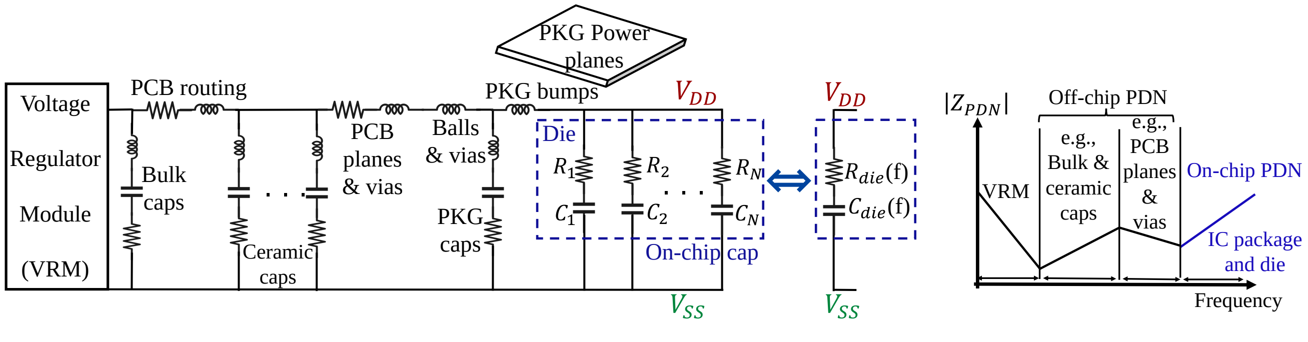
While current and voltage alterations have been considered the root cause of side-channel leakages, the data-dependent variation of the parameter relating current and voltage to each other via Ohm's law, i.e., impedance, has always been ignored. The primary assumption has been that impedance is a constant parameter that is determined by the materials used in the fabrication of the PCB, chip's die, and package. Hence, it is defined by the physical structure and size of the chip rather than the running computation on a system or stored content on a chip. For instance, adding/removing a circuit to/from a chip can cause changes in the impedance of the die. Such changes have been the basis of some hardware Trojan and tamper detection methods (on both chips [60, 64, 65] and PCBs [59, 61, 86]), where the malicious circuits modify the impedance of the system and, thus, can be detected. However, the effect of the circuit state or content of memory elements inside the chip on information leakage through the die's impedance has not been studied so far.

The contribution of impedance to side-channel leakage could be implicitly observed in a specific class of SCA attacks, namely static power analysis [58]. For this attack, the adversary halts the circuit and exploits the data-dependent static current consumption of transistors in steady states. It was shown that the state of flip-flops on a chip lead to static current variations leading to successful key recovery using differential power analysis (DPA). The fluctuation in the static current is indeed caused by changes in the overall impedance of the die; however, the focus in static SCA attacks [11, 55, 58] has been on the measurable quantity, i.e., the static current and the role of the impedance has never been discussed.

Driven by the fact that impedance is also affected by the stored content on a chip, the following research questions arise: *(1) Is it possible to measure the information leakage through the impedance directly? (2) What would be the consequence of impedance analysis for prominent side-channel countermeasures, i.e., masking?*

Our Contribution. To answer the above questions, we present a novel non-invasive SCA attack based on directly characterizing the chip's impedance. Our method relies on a known RF/microwave impedance characterization technique called scattering parameter

CCS '23, November 26–30, 2023, Copenhagen, Denmark
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9450-5/22/11…$15.00
https://doi.org/10.1145/3548606.3560649



(a)

(b)

Figure 1: (a) Equivalent RLC circuit model of the power distribution network of the PCB and chip [60]. (b) Contribution of different parts of the PDN to the impedance over frequency [60].

analysis, in which we inject electrical sine waves with different frequencies into the power delivery network (PDN) of the chip and measure the echoes of the signals. We demonstrate that the reflected signals are modulated uniquely at various frequency points based on the register contents and physical location of a register on the chip. The transistor's imperfections, asymmetric logic gates, and interconnects with various lengths contribute to impedance variations and, consequently, to the modulation of the reflected signals. We show that analyzing these echoes at different frequencies enables the adversary to profile register contents and read them out simultaneously in the attack phase. Therefore, such analyses provide a large number of virtual probes for different locations of the chip in the frequency domain during a time period, which challenges the central underlying assumption of the t-probing security model for masking schemes. To validate our claims, we launch impedance-based SCA attack on unmasked and masked AES designs implemented on a Field Programmable Gate Array (FPGA) manufactured with a 28 nm technology. As a result, we successfully break the security of the targeted implementations by recovering their keys.

Remark. The primary contribution of this work is the introduction of a new physical side-channel based on impedance analysis. A comparative experimental study between impedance analysis and other side-channels, specifically power side-channels, requires a unified setup[22] and deserves a future study.

Availability. We publicly publish our measurement traces and make the source code of our attacks open source to foster the security research:
https://github.com/Hidden_For_DoubleBlindReview

2 TECHNICAL BACKGROUND

2.1 Power distribution network (PDN)

The PDN is responsible for delivering low noise and constant voltage supply to the electronic components on the PCB, from the voltage regulator module (VRM) to the power rails on the chip. Each component has a distinct contribution to the physical signature of the PDN at different frequency regimes. The system's PDN is represented by an equivalent circuit model shown in Figure 1a. The PDN comprises both 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 Figure 1b. The parasitic inductance present 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 PDN impedance at higher frequencies is dominated by the on-chip structures due to their smaller dimensions, as shown in Figure 1b.

The dashed blue region in Figure 1a shows the equivalent RC model of the on-chip capacitance. To model the wideband on-chip behavior of the circuit, multiple narrowband parallel RC circuits (N in total) are connected to V_{DD} and V_{ss}. The succeeding subsection provides further details on the origins of on-chip PDN impedance.

2.2 Sources of On-die Impedance

On-die capacitance C_{die} and resistance R_{die} are the dominant features of the on-chip impedance in high-frequency bands [75]. The ranges of such frequency bands are determined based on the chip's technology and size. Here, we explain the sources of on-die capacitance using the physical structure of a CMOS inverter. Figure 2 shows the cross-sectional view of an inverter, metal power grid layers, and the locations of the corresponding on-die capacitors. According to Figure 2, an inverter comprises a PMOS and an NMOS transistor. These transistors serve as switches, with the NMOS having an infinite off-resistance and a finite on-resistance. Meanwhile, the PMOS has a positively doped source, drain, and gate region in the form of an n-well. The On-die capacitance C_{die} is affected by several elements, including the metal layers grid network, non-switching gate, and p-n diode junction diffusion [75]. Resistance in

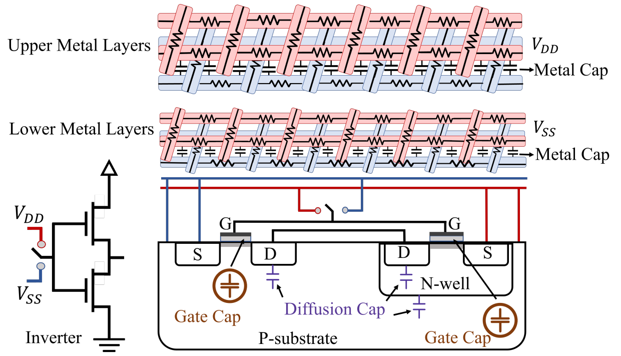


Figure 2: The physical representation of a CMOS inverter cross section and the locations of different types of on-die capacitors. The black capacitors show the capacitance of metal lines, the blue ones show the p-n diode junction diffusion capacitance and the capacitance shown in green color corresponds to non-switching gate capacitance.

the power net, transistor channel, transistor gate, and contacts of n-well and P-substrate contribute to R_{die} [51].

The location of each capacitance that contributes to C_{die} is shown in Figure 2 using different colors. The black color represents the metal capacitance, C_m, which pertains to the power/ground metallization grid network located on the die. The size of C_m is affected by the density of the grid network, the width and distance of metal layers, and the permittivity of materials. Typically, C_m is larger in upper metal layers due to denser power and ground meshes, while it is slightly smaller in lower metal layers because the power traces are less dense and thinner. The purple color corresponds to the diffusion capacitance, C_d, which relates to the p-n diode junctions. It is essential to note that C_d and C_m only contribute to a small portion of the total C_{die}, while the non-switching gate capacitance, C_g, is the main contributor.

On the chip's PDN, all non-switching and powered-on circuits contribute to C_g. This is because when a transistor is powered on, it has a channel underneath the gate, contributing to C_{die}. On the other hand, when a transistor is powered off, its channel is inactive and does not significantly contribute to on-die capacitance. Initially, when the device is not powered on, the decoupling capacitance effect of the gates is negligible. However, when the device is turned on, the channels start to form, and as a result, C_g becomes the dominant contributor to C_{die}. If the chip's design is modified, different parts of C_{die} (particularly C_g) would change based on the size, location, and nature of the tamper event. This modification changes the equivalent circuit of the on-chip PDN and affects the measured signatures from the chip.

2.3 Non-invasive Impedance Characterization

To characterize the impedance of the PDN in different frequencies, S (Scattering) or Z (Impedance) parameters are deployed [4, 71]. Every circuit/electronic component can be described as a one or multi-port network. S parameters directly represent the attenuation, reflection transmission ratio of the signal at each port of such network over the frequency domain to the applied electromagnetic field [69]. For instance, S_{11} quantifies how much power is reflected from the the port 1 if the EM field is transmitted from port 1. In frequency domain analysis, waveforms are represented by sine waves. Frequency, amplitude, and phase are the three terms that can fully characterize a sine wave. Thus, we utilize both the amplitude and phase response in the frequency domain to accurately characterize the chip at each frequency point. A Vector Network Analyzer (VNA) is an instrument that measures the transmitted and/or reflected power of a signal that goes into and comes back from a component. We use a VNA to inject sine waves into the chip at every frequency point to record the chip's PDN's reflected response . The impedance profile can be easily derived from the reflection coefficient. Equation 1 expresses the relationship between the input impedance of the device under test (DUT) and the reflection coefficient:

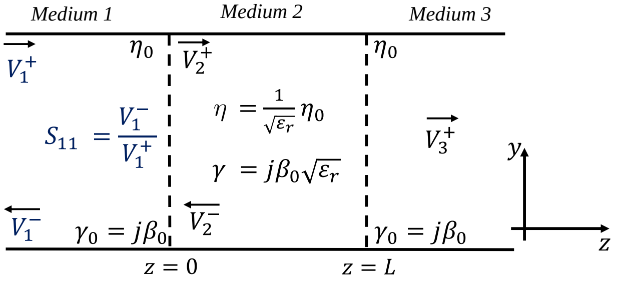


Figure 3: The simplified (ideal) transmission line model for normal uniform plane wave incidence on different media (the characteristic impedance of medium 2 is different from medium 1 and 3) [60].

$$Z_{DUT} = Z_0 \frac{1 + S_{11}}{1 - S_{11}}, \tag{1}$$

where S_{11} is the reflection coefficient, Z_0 represents the reference impedance of the VNA which is 50 Ω, and Z_{DUT} corresponds to the impedance obtained from S_{11}. We only deploy S_{11} in our proposed method as the VNA can directly measure it from the chip. However, based on Equation 1, it is observable that the reflection coefficient is another representation of the impedance.

We further explain the changes that occur to the injected voltage wave by the VNA into the chip by analyzing the ideal transmission line model. This model is the backbone of more complex circuits, and understanding its theoretical foundation clarifies our methodology's mechanism. Figure 3 shows an ideal transmission line model where there is a change in the characteristic impedance and propagation constant of medium 2 that are represented by η and γ, respectively. For simplicity, we assume that medium 1 and medium 3 are lossless, thus giving a characteristic impedance of η_0 and a corresponding propagation constant of $\gamma_0 = j\beta_0$. We consider medium 2 a non-magnetic ($\mu_r = 1$) medium with a relative permittivity of ε_r. Noting that ε_0 and μ_0 are the permittivity and permeability of the free space, respectively, and β_0 denotes the free space wave number, we can consider $\beta_0 = 2\pi f\sqrt{\varepsilon_0\mu_0}$ and rewrite the second medium's propagation constant as $\gamma = j\beta_0\sqrt{\varepsilon_r}$. Considering $\eta_0 = \sqrt{\mu_0/\varepsilon_0}$, we can rewrite the characteristic impedance

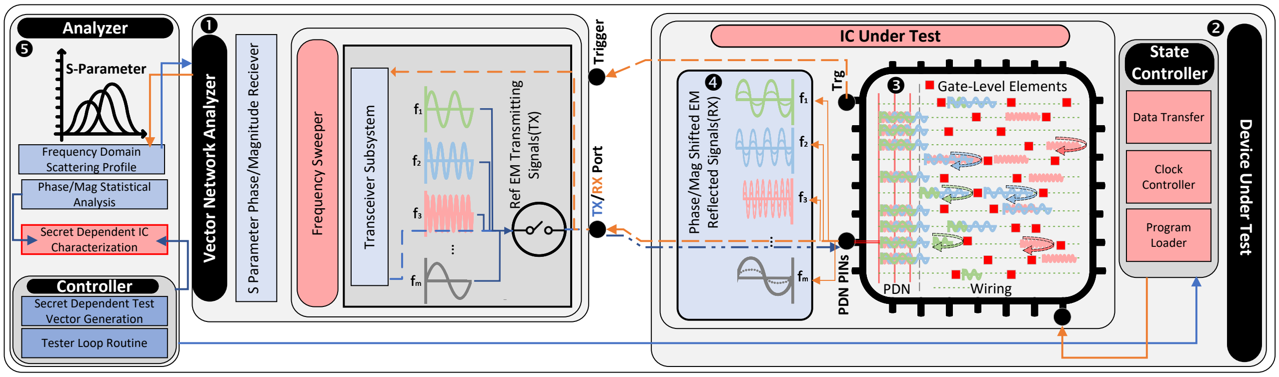


Figure 4: High-level overview of LeakyOhm's methodology and attack flow

of medium 2 as $\eta = \sqrt{1/\varepsilon_r}\eta_0$. The VNA injects a voltage wave with the known amplitude of V_1^+ in medium 1, and the reflected voltage wave has an amplitude of V_1^-. After V_1^+ is injected, multiple reflections and transmissions occur in the lines. Based on the model in Figure 3, the lines' voltages can be written as [69]: $V_1(z) = V_1^+ e^{-j\beta_0 z} + V_1^- e^{+j\beta_0 z}$, $V_2(z) = V_2^+ e^{-\gamma z} + V_2^- e^{+\gamma z}$, and $V_3(z) = V_3^+ e^{-j\beta_0 z}$, where V_i^+ and V_i^- ($i = 1, 2, 3$) are forward and backward voltage waves through/from the medium i; however, we assume that there exists no backward voltage wave in medium 3, for simplicity.

V_1^+ is a known parameter (injected by VNA), whereas V_1^-, V_2^+, V_2^-, and V_3^+ are unknown values. We apply the boundary conditions on the voltage wave components at the interfaces of the media and find all these four unknowns. We are interested in obtaining the S_{11} in medium 1 which can be derived as

$$S_{11}(f, \varepsilon_r, L) = \frac{V_1^-}{V_1^+} = \frac{(\eta^2 - \eta_0^2)(1 - e^{+2j\gamma L})}{(\eta_0 + \eta)^2 - (\eta - \eta_0)^2 e^{+2j\gamma L}} \tag{2}$$

where L is the length of the path that the injected wave voltage travels. From Equation 2, it can be concluded that the reflection coefficient depends on three parameters: the frequency band of interest, the relative permittivity of the sample, and the length of the wave's traveling path. On the other hand, the dependence of S_{11} on the frequency has another aspect: frequency and wavelength are inversely proportional to each other. This explains why we can detect smaller size changes in the chip's configuration at higher frequencies. When registers with different placement and routing are exposed to the incident wave injected from the VNA, the changes occurring in Equation 2 parameters will result in a change in the S_{11} profile at distinct frequencies. For example, when the placement and routing of the circuit is altered, L is changed, and this would cause the chip's reflection response to be different for different placements and routings.

2.4 Masking and *t*-Probing Model

Masking is the prominent countermeasure against SCA attacks due to its sound theoretical and mathematical foundations. In masking schemes, the computation on a chip is distributed between a couple of shares (multi-party computation) and the intermediate computations dealing with the secrets (secret sharing). The number of shares defines the order of the masking and its resiliency against SCA and probing attacks. For cryptographic implementations, the key and plaintext should be represented in a shared form, and the entire computations are performed on shares. At the end of the computation, the ciphertext should be obtained by recombining the output shares. The main advantage of masking is that it can be evaluated in formal security models. For instance, in Boolean masking schemes, every random bit x is represented by $(x_0, \ldots, x_d)$ in such a way that $x = x_0 \oplus \ldots \oplus x_d$. According to [13], an adversary who is limited to the d^{th} order SCA or the number of probes can be defeated by a secret sharing with $d + 1$ shares. Moreover, it was shown that measurements of each share x_i are adversely influenced by Gaussian noise, and thus, the number of noisy traces needed to extract x grows exponentially with the number of shares [70].

On the other hand, the t-probing model, which was first introduced in the seminal work of Ishai et al. [39] can be deployed for the security analysis of masking schemes. In this model, it is assumed that the attacker is limited to at most t physical probes to observe the computation on wires of the circuit at each time period (e.g., one clock cycle). In such a case, at least $t + 1$ shares are needed to prevent the attacker from learning any sensitive information from t observations. It has been demonstrated that the two aforementioned leakage models are related by reducing the security in one model to the security of the other to unify the leakage models and so simplify the analysis of SCA countermeasures [23]. In other words, placing $t = d$ physical probes on the wires of the target circuit is equivalent of d^{th}-order noisy SCA attack. While there have been some sophisticated SCA attacks violating this assumptions [48], for most practical SCA attacks, it is reasonable to assume that the adversary has a limited number of probes due to practical issues due to, for instance, the lack of spatial space [43, 76] to accommodate several physical probes or increased noise in the case of higher-order power analysis. As a result, several constructions, security proofs, and multiple implementations have been reported.

Note that, in several countries, protection against SCA attacks is one of the criteria defined by certification bodies. Among various SCA countermeasures, masking schemes have been widely in use for more than a decade in many secure ICs, such as smartcard chips.

3 SYSTEM-LEVEL IMPEDANCE ANALISYS

In this section, we propose and describe a systematic approach to analyze and interpret impedance profiles as new side-channel leakage criteria for integrated circuits.

3.1 High-Level Representation

Although the nature of the back-scatter analysis is entirely non-invasive, the proposed SCA involves active measurements. Specifically, as indicated earlier, a series of test electromagnetic signals are generated in a tester device (e.g., VNA) and transmitted through the output port directly to the DUT's PDN. Consequently, the signals are collected as input at the tester's receiver, which can then be used to characterize the impedance of the DUT. Figure 4 depicts a high-level overview of the workflow, setup, and approach of our attack.

As indicated, in ❶, VNA generates the test signals over a particular frequency band by employing an embedded programmable *Frequency Sweeper*. During the experiments, these signals are selected in the *Transceiver Subsystem* and are sent through the *TX* port of the VNA. At the same time in ❷, DUT is equipped with a *State Controller* that preserves the target IC in a specific state. *TX* signals are received at IC's PDN interface. As shown in ❸, based on the frequency of the transmitted signal, each test signal propagates differently throughout the chip's PDN, and hence, different propagation behavior of each of them yields in certain *Magnitude* and *Phase* when they are reflected back to the PDN pins (❹). Then, VNA detects and measures the reflected signal (*RX*) at each frequency and estimates scattering parameters (S-Parameters) as the final measurement. In ❺, measurement data are sent to the analyzer for characterization. Analyzer performs an iterative profiling procedure to exploit the variations of reflected *RX* signals in both *Magnitude* and *Phase* at each selected frequency ($f(|S_{11}|, \angle S_{11})$).

3.2 Systematic Impedance Analysis

In order to apply the proposed attack as an end-to-end SCA, here we present an abstract and systematic definition of impedance analysis. Inspired by telecommunication methodologies and terminologies, we can consider a communication system to describe the workflow of our attack.

At the high-level, test signals at different frequencies, which are generated by the VNA, could be treated as data *carries*. The DUT is the noisy communication *channel*, and the received signals are the measurements that are to be analyzed and decoded. As depicted in Figure 5, a series of signals on pre-determined frequencies are transmitted with reference *Magnitude* and *Phase* of $|0dB|\angle 0^{\circ}$. The test signals are represented in a polar coordinate system in Figure 5. On the other hand, the received signals which are attenuated and distorted can also be represented as polar coordinate $|M_{Rx}dB|\angle P_{Rx}{}^{\circ}$. The high-level goal here is to characterize the communication channel based on a set of received signals of *RX*. In the realm of telecommunications, the problem at hand here is categorized in the well-known sub-field of *Channel Characterizations* [85]. Although similar measurement methodologies seek to characterize the wireless channels [12, 16, 68], we apply the same measuring methodology in the context of IC characterization to extract information. In other words, the channel characterization, in this case, yields information about the internals of the IC (specifically the contents of the registers). Hence, a systematic SCA could be accomplished by analyzing the set of $|M_{Rx}dB|\angle P_{Rx}{}^{\circ}$ with respect to the target state of the DUT during the measurements.

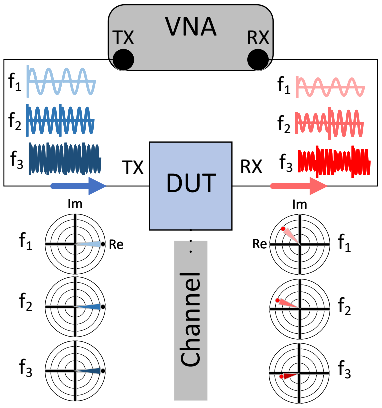


Figure 5: Systematic representation of impedance analysis inspired by communication systems.

4 PHYSICAL-LEVEL ANALYSIS OF IMPEDANCE LEAKAGE

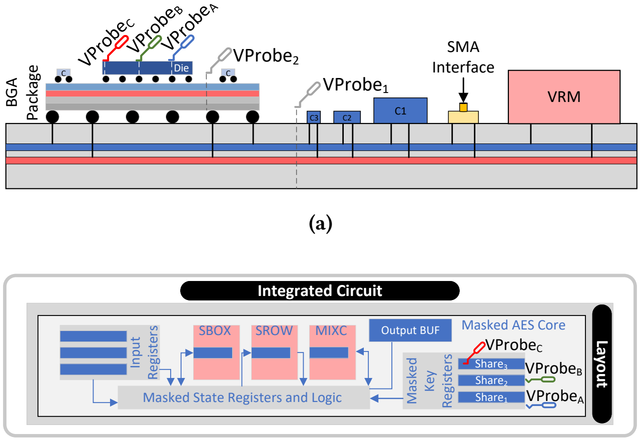
To perform SCA on the reflected signals from the chip's die, it is vital to understand how the transmitted carrier signals are modulated based on the physical characteristics (and specifically the contents of the registers) on the chip. As described earlier, the system's PDN (to and from the chip) can be considered a communication channel in high frequencies between a transmitter and a receiver. The VNA in our system is both the transmitter and the receiver on this channel. Therefore, the channel model is analogous to a RADAR channel model [26]. In this case, the transmitted signal $x(t)$ from the VNA at frequency f_i can be written as follows:

$$x(t) = A \sin(2\pi f_i t) \tag{3}$$

where A is the amplitude of the transmitted signal. Considering the PDN of the chip as the entity that applies the desired information to the carrier $x(t)$, the amplitude and phase of $x(t)$ are reshaped. Thus, the modulated signal $\tilde{x}(t)$, received at the VNA can be described [79]:

$$\tilde{x}(t) = \alpha_i A \sin(2\pi f_i (t - 2T) + \phi_i) + n(t) \tag{4}$$

where α is the attenuation or fading factor, ϕ is the phase shift, $2T$ is the round-trip time of the signal, and $n(t)$ is a Gaussian noise added to the signal. In our case study, we experimentally show that the characterization of the PDN, which contains a data-dependent leakage, could be observed in the amplitude, phase, and round-trip time variations. However, since our analyzes in this paper are confined within the frequency domain data, we do not consider the round trip time as a leakage parameter.



(a)

(b)

Figure 6: (a) Realization of virtual probes with the use of VNA and (b), Applying virtual probes on a masked AES implementation on a chip.

4.1 Realization of Virtual Probes

As indicated in our approach, the transmit carrier signals $x(t)$ are injected on a wide range of frequencies f_i. As covered in Section 2.3, well-studied back-scattering PDN profiling confirms that even in nanometer-scale characterization, different circuit elements (i.e., inductors and capacitors) reflect (and forward) different portions of input energy in accordance with carrier frequency [38] due to nonlinearity in their frequency response [3]. This frequency-dependent behavior of the elements in the microscopic scale is affected by physical and intrinsic (such as dimensions) features, which determines the resonate frequency of the elements [72]. Hence, exploiting the same observation in our scenario, different input frequencies (f_i) yield capturing the response of different elements on the DUT. In accurate terms, the reflected signal at a particular frequency contains a dominant response of specific elements.

To illustrate this, Figure 6a shows a high-level cross-section block diagram of a simple PDN and a target IC. Here, an adversary generates $(x(t), f_i)$ using a VNA and injects the signals via the SMA interface. Based on the selected f_i multiple *Virtual Probes* could be deployed to characterize the board. For instance, on-board capacitors (e.g., $C1$ and $C2$) are large elements, and their dominant response could be observed in $\tilde{x}(t)$ with low-frequencies (MHz). This indicates that any modification on these elements could be observed in $\tilde{x}(t)$ with those frequencies. In other words, by knowing those exact frequencies f_{Probe_1}, the adversary can place a *Virtual Probe* on $C1$ and $C2$. Sweeping to higher frequencies (GHz), the adversary will have multiple *VProbes*, on different elements (physical locations) on the chip to perform a powerful SCA. This capability is granted by the fact that IC-level elements are physically asymmetric and placed and routed uniquely on the die. Figure 6b depicts the utilization of *VProbes* to effectively disable a *Masked AES* implementation on a target chip. We show that, with a proper profiling process, an attacker can precisely determine frequencies for each share of the masked key to extract all secret values simultaneously.

It is also noteworthy to mention that in Figure 6b, each target key register shows a dominant response on a specific frequency set, leading the adversary to distinguish the leakages.

4.2 Effects of Parallel Computation and Masking Schemes

Cryptography implementations in software fundamentally suffer from time-domain leakage caused by the serialized execution model. Many researchers have shown that even secured masking implementations could be easily broken by template attacks on software [66, 80]. In the case of masking implementations on hardware, with the assumption of parallel computing on shares, the data-dependent power leakage is experimentally shown to be reduced significantly [21]. The CMOS power consumption model in masking schemes assumes that expected power consumption P for a masked secret bit $c = (m, c \oplus m) = (s_1, s_2)$ hold the following condition [20]:

$$\begin{aligned} &P(c = 0) = P(c = 1) \\ &P(s_1 = 0, s_2 = 0) + P(s_1 = 1, s_2 = 1) = \\ &P(s_1 = 1, s_2 = 0) + P(s_1 = 0, s_2 = 1) \end{aligned} \tag{5}$$

Although decoupling effects [20] and higher order attacks [78] can exploit the aforementioned condition, considering the CMOS *Hamming Weight* model and as long as s_1 and s_2 computations are performed simultaneously at t_1 this constraint in Equation 5 is believed to be maintained. Compared to 1-d scalar power consumption measurements, impedance leakage is measured over set of N samples of frequencies, making the leakage variable a 2-d parameter.

By applying the same condition on *Impedance* leakage, an ideal one-bit masking rules the following:

$$\forall f_i \in F = \{BW\} : \mathcal{Z}_{f_i}(c = 0) = \mathcal{Z}_{f_i}(c = 1) \tag{6}$$

As thoroughly investigated in Section 4.1, constraints indicated in Equation 6 could not be trivially held by first order boolean masking, as the unique physical realizations, corresponding wiring and required routing for s_1 and s_2 computations yield in frequency-dependant measurements. Here in contrast to scalar power leakage model, impedance profile in Equation 6 should be satisfied for all frequency stamps to ensure the security. For instance, if $N = 100$ impedance measurements are conducted from the bandwidth $F = BW = \{1GHz - 2GHz\}$, Equation 6 should be held. In such strong constraint, one can derive $\exists f_\alpha \in F$, where $\mathcal{Z}_{f_\alpha}(c = 0) \neq \mathcal{Z}_{f_\alpha}(c = 1)$ and therefore impedance of masks values could be distinguished effectively.

5 PROPOSED ATTACK SCENARIOS

In this section, we will elaborate on multiple attack scenarios based on the developed scatter profile of the DUT. Ultimately, here we showcase that the proposed methodology could challenge t-probe security model. Based on our findings we exhibit that unlike power consumption side channels, impedance leakage collected from scattering profiles does not scale down exponentially [13, 40] by increasing the number of shares. On the contrary, we showcase that the impedance leakages of *t-share* operands are leaked through distinguishable frequencies and do not cause significant additive noise to leakage measurement. In other words, although state-of-the-art masking schemes, such as Threshold Implementation [73] and Domain-Oriented Masking [31], are highly effective in mitigating time-domain SCA (i.e., DPA on power consumption), they will not suffice against proposed frequency-domain impedance SCA. As thoroughly described in Section 4.1, this is due to the fact that the physical characteristics of gate-level elements are scattered over a frequency bandwidth that can be captured by impedance profiling. Here, we exploit this fact to exhibit that the aforementioned characteristic is indeed data-dependent and can be used to reveal secrets.

We start off with simple case studies to verify scattering leakage is exploitable, and then we move toward realistic scenarios where sensitive data are protected by higher-order well-known masking schemes. First, we describe how adversaries can mount conventional non-profiled attacks via impedance analysis. Particularly we develop *Differential Impedance Analysis* (DIMA) to break unprotected cryptographic implementations. Furthermore, a non-profiled *Correlation attack* is also presented to illustrate conventional leakage models (i.e., Hamming Weight) are also effective in impedance analysis.

After verifying the applicability of naive non-profiling scenarios, we specifically aim to sidestep protected hardware implementations by exploiting on-die location-based profiling. As our main attack, we present *Template Impedance Attack (TIMA)* to extract time-constant high-order masked operations. We showcase that *TIMA* effectively breaks state-of-the-art masking schemes.

5.1 Threat Model

DIMA and CIMA attacks are performed in known plaintext scenarios. For TIMA, we also assume the access to profile the random shares (i.e., all key shares). Building templates for mask registers plays a crucial role in mounting a successful template attack which is usually not taken into account. For a thorough discussion, please refer to [7].

On the execution level, since our method aims to extract data directly from the DUT, we assume that the measurements are performed when target data remain unchanged in some registers on DUT. This consideration makes our treat model very similar to static power side-channel analysis [22, 56–58] and LLSI attack [48, 49], where instead of performing the measurements during the secret-dependant operations, adversary snapshots at timestamps where secret-dependant data are stored in some form (i.e., in Flip-Flops) on the DUT. In this regards, TIMA does not apply any time-series multi-variant analysis on the target like the works in [22, 25]. and the measurements are captured on a single clock-cycle. Here, we make use of multivariate frequency analysis which exploits the frequency-dependent leakage on the same time-stamp. Hence, our threat model requires a clock-controlled environment for high-speed DUT during the measurement. However, this limitation might be resolved by iterating the measurements without clock halting. (For more discussion please see Section 7.3)

5.2 Naive Impedance Attacks

In order to showcase the exploitability of impedance side-channel leakage, we demonstrate that conventional power-side channel attacks could be easily modified to be applied to impedance measurements. Here, we describe two high-level attacks useful for unprotected cryptographic algorithms. Namely, in the following, we describe impedance-based DPA and CPA.

5.2.1 *Differential Impedance Analysis.*

Differential Power Analysis [45] on cryptography implementation exploits the variations of dynamic power consumption of DUT by employing hypothesis-based differential measurements of traces. For correct hypothetical secrets, the differential analysis maximizes a secret-dependant intermediate operation over time-domain measurement. We inspire the same methodology to deploy Differential Impedance Analysis (DIMA) over the frequency domain. In other words, for a correct hypothesis of a secret, the absolute difference of impedance measurements of a secret-related intermediate value should be maximized at some frequency stamp. This frequency stamp is physically related to the characteristics of the element that somehow(i.e., stores or transfers) intermediate value. The routine for DIMA is mostly similar to conventional DPA. The adversary could follow the same algorithmic process in DPA [46]. However, instead of calculating differential measurement on time stamps, the attacker performs the differential analysis on frequency stamps. Algorithm 1 illustrates a high-level description of DIMA. In Algorithm 1, $Trc_a[]$ represents the array of all measured traces for the attack and $Inp(Trc_a[i])$ shows the associated input with trace $Trc_a[i]$. Furthermore, $Int_v(key = k, input = i)$ depicts the result value of a selected intermediate bit value in the targeted cipher where key and input of the cipher are k and i, respectively.

Algorithm 1 Differential Impedance Analysis

```
function DIMA ATTACK($Trc_a[]$)
    for $k \in K = \{0, 1, ..., 2^m\}$ do          ▷ $K$ is set of key values
        for $i = 0, 1, ..., |Trc_a|$ do
            $H \leftarrow Int_v(k, Inp(Trc_a[i]))$    ▷ intermediate value
            if $H = 1$ then
                $One_{Trc} \leftarrow Append(Trc_A[i])$
            else
                $Zero_{Trc} \leftarrow Append(Trc_A[i])$
            end if
        end for
        $Diff_k \leftarrow DOM_{freq}(Zero_{Trc}, One_{Trc})$
    end for
    return $ArgSort(Mean(Diff, freq))$
```

As indicated in Algorithm 1, the Difference Of Mean (DOM_{freq}) is performed element-wise on each frequency stamp of impedance traces. Finally, we apply a simple averaging on each candidate to represent each guess key with a single score. Then an *Argument Sort* on frequency-normalized $Diff_k$ values are performed and target key is extracted. On the algorithmic level, the frequency indices of maximum values of $Diff_{Key=k}$ indicates the frequencies at which the intermediate value's physical deployment on the die leaks the most. Particularly, the same frequencies could be considered independently and be used as a profile to reveal this specific intermediate value's content. We take advantage of similar behavior to put together a powerful profiling attack which will be elaborated later on.

5.2.2 Correlation Impedance Attacks. As another well-established power side-channel attack, Correlation Power Analysis (CPA) [6] is also used, and they mitigate some drawbacks of DPA [50]. CPA uses a power consumption model on the hardware to establish a correlation between the secret-dependent operation and inputs over power measurement. For instance, a famous metric assumes that power consumption of operands on the circuits tracks a linear trend with respect to its Hamming Weight (HW). Here, the same approach is utilized for the adversary to attack an unknown secret. We use frequency-stamped impedance traces to mount a Correlation Impedance Attack (CIMA). Although different leakage models for impedance traces could be employed as a proper candidate, we use a simple HW model to develop our attack. In CIMA attacker executes Pearson Correlation [15] over frequency-domain impedance values. Hence, target intermediate content leaks on a specific frequency stamp that is indicated by CIMA. Armed with an HW model, we launch CIMA on the first round of AES's S-Box output to showcase a successful correlation impedance attack. It is noteworthy to mention that based on our evaluations (in Section 6.4.1), the HW model shows a near-linear leakage trend over impedance's phase ($\angle S_{11}$) on the target frequency stamp.

Although CIMA successfully breaks the hardware realization of a prominent cryptographic algorithm (i.e., AES) with a much less number of measurements, it is not effective against masking schemes. This is due to the fact that CIMA like other correlation attacks, strives to discover the likelihood of a single secret-dependant intermediate value, which is largely diminished by masking [21]. In the following, we propose an attack that builds upon frequency-spanned leakage of impedance measurements enabling us to extract masked secrets through frequency analysis in hardware implementations.

5.3 Template Impedance Attacks

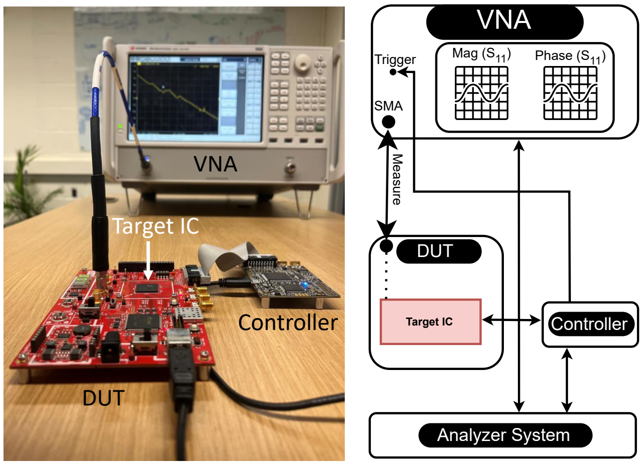
Template attack proposed by Chari et.al. [14], provides a strong attack methodology where the adversary can profile a target hardware of her choosing with an arbitrary cryptographic implementation (e.g., protected) and break similar hardware using a limited number of power consumption measurements. In contrast to non-profiling methods which strive to eliminate noise by averaging over large measurement traces, template attack utilizes multi-variant characterization of points of interest (including the noise) by employing the identical target hardware, making it extremely powerful during attack phase [14]. Owing to the nature of the impedance measurements, we believe a similar Template Impedance Attack (TIMA) is the most powerful attack that can be performed using impedance analysis. TIMA follows the same algorithm as a regular template attack while performing on frequency stamps. Algorithm 2 depicts the high-level flow of TIMA.

In Algorithm 2, each profile trace $Trc_p[key = k, Inx = i]$, is a collection of measurements associated with the impedance of the target at frequencies $\{fr_0, fr_1, ..., fr_f\}$, where the k and i refers to the cipher's key and trace index, respectively. Moreover, $Mean(.)$ and $Cov(.)$ are *Average* and *Covariance* calculation functions. As demonstrated, the TIMA Profile phase is performed on the DUT controlled by the adversary. As highlighted, Points Of Interest (POIs) in this attack are determined by averaging measurement values over a frequency band. Hence, frequency stamps that cause maximum difference for all the possible target $\mathcal{K}$ are selected using the Difference in Means (*DOM*) metric. Moreover, we apply *TopK*, a localized Top-K [2] with empirically set smoothing factor α to select final POIs. Note that as collected scattering measurements are complex numbers, TIMA Profile could be applied to $\angle S_{11}$ or $|S_{11}|$ or even $f(|S_{11}|, \angle S_{11})$. As discussed earlier in this article, we mainly focus on $\angle S_{11}$ profiling since it is more resilient to additive noise compared to $|S_{11}|$. Nevertheless, one could deploy an iterative estimation [74] or optimization [5] procedure to find near-optimal parameters for $f(|S_{11}|, \angle S_{11})$ leakage profiling kernel to enhance the attack success rate.

Algorithm 2 Template Impedance Attack

```
function TIMA Profile(.)
    for $k \in K = \{0, 1, ..., 2^m\}$ do                ▷ $K$ is set of key values
        for $i = 0, 1, ..., N_p$ do
            $Trc_p[k, i] \leftarrow Measure(\{Z_{fr_0}, Z_{fr_1}, ..., Z_{fr_f}\})$
        end for
        $AVTrc_p[k] \leftarrow Mean(Trc_p[k], N_p)$
    end for

        $DM \leftarrow DOM(AVTrc_p[k], freq)$
        $POI[p] \leftarrow TopK(DM, p)$

    for $k \in K = \{0, 1, ..., 2^m\}$ do
        $Mean_p[k] \leftarrow Mean(Trc_p[k], POI)$
        $Cov_p[k] \leftarrow Cov(Trc_p[k], POI)$
    end for
    return $Mean(Trc_p), Cov(Trc_p)$
function TIMA Attack($Trc_a[], Mean_p[], Cov_p[]$)
    for $k \in H = \{0, 1, ..., 2^m\}$ do                ▷ $H$ is set of guess target
values
        $Dis_k \leftarrow MultivarGaussian(Mean_p[k], Cov_p[k])$
    end for
    for $i = 0, 1, ..., N_p$ do

            $STrc_a[] \leftarrow Select(Trc_a[], POIS)$

    for $k \in H = \{0, 1, ..., 2^m\}$ do
        $P[k] \leftarrow PDF_{eval}(Dis_k, STrc_a[j])$
    end for
    $Res[k] \leftarrow Acc(P[k])$
end for
return $ArgMax(Res[])$
```

In the second phase, the attacker has limited access to the target DUT and captures a small number of measurement traces of impedance $Trc_a[]$. Consequently, TIMA Attack routine is executed. As highlighted, measurements on pre-determined frequency



(a) (b)

Figure 7: Measurement setup. (a) VNA capturing S_{11} traces from the DUT and (b) Experimental setup diagram.

stamps (POIs from the profiling phase) are selected first ($STrc_a[]$). Then probability evaluation (PDF_{eval}) of each measured attack trace is computed for each key hypothesis based on its Gaussian multi-variant distribution (Dis_k) extracted during TIMA Profile phase. Lastly, probabilities are accumulated for all captured traces to indicate the final candidate.

As will be explored, TIMA can be successfully applied in multiple attack scenarios and particularly on masked implementation. Specifically, we exercise a single bit TIMA on masked AES implementation (in Section 6.5) to recover all masked shares of the key, bit by bit. On the algorithmic level, the advantage of TIMA comes from the fact that every single bit on DUT contributes to a unique set of *POIs* over the frequency band, and consequently, forms a (fairly) distinguishable Gaussian multi-variant distribution that can be estimated with a fair amount of profiling measurements.

6 EVALUATION

6.1 Experimental Setup

6.1.1 Measurement Equipment. We utilized a Keysight ENA Network Analyzer E5080A[42], which enables RF/microwave scattering measurements and operates on 9KHz - 6 GHz frequency bandwidth. We used Minicircuit CBL-2FT-SMNM+ characterization shielded cables [54] suitable for scattering measurements which are also operable in the same frequency bandwidth. The used VNA ports have internal capacitors to filter out the DC voltage on the V_{CCINT}, and therefore, no Bias Tee is needed.

6.1.2 Device Under Test. For our experiments, we used NewAE CW305 board (NAE-CW305) [62], which is equipped with an AMD/Xilinx Artix-7 FPGA [81] (XC7A100T), built with a 28 nm technology, see Figure 7a. CW305 board provides direct access to the FPGA's PDN network, which was the main reason for the selection of this board. Moreover, while the FPGA contains multiple PDN domains (e.g., V_{CCINT}, V_{CCO},) a 1V domain supplying the core (V_{CCINT}, V_{CCAUX}, etc.), for our evaluations, V_{CCINT} power domain is our primary target PDN as it is connected the FPGA registers. Furthermore, CW305 has multiple SMA (SubMiniature version A) connectors that enable access to a shunt resistor, as well as a 20 dB low-noise amplified low-side signal suitable for power analysis. However, our experiments are carried out by the SMA port on the low side of the shunt resistor X3 port on the board, which gives us direct access to the PDN of the FPGA.

6.1.3 Analyzer and Controller Configuration. To control the state of the target FPGA chip, we have utilized a NewAE CW-Lite board [63], which provides serial communication with the DUT and could be used as an intermediate controller to transfer plaintext and receive ciphertext from the target IC. Furthermore, to conduct measurements, the CW305 board is configured to synchronize IC's clock once the controller receives the trigger signal (e.g., CW-Lite). Specifically, for our clock controlled experiments (e.g. TIMA), target's clock signal is generated via PLLs on CW305 and a feedback is sent to the controller at the same time. Based on the received and synchronous clock signal of the target and upon reaching to the desired time-stamp, a mask signal is sent by the controller and target's clock signal is masked and computation is halted. During this idle status, although the PLL clock on the board is oscillating but the target clock on the IC is gated. Consequently, a trigger signal is sent to the VNA for the measurement during this period. In our experiments, PLL board clock is set to $100MHz$.

In order to schedule and prepare the input data for the IC and also analyze measurements and conduct our attacks, we employed *Python 3.7* scripts. We used *PyVisa* [18] and *Scipy.Stat* [19] to communicate with the instruments and perform statistical analysis, respectively. Furthermore, hardware designs are written in Verilog, and synthesizes are carried out by Xilinx Vivado [84]. The *Analyzer System* is a machine with an Intel XEON E5 2697 V3 CPU clocked at 2.6 GHz, equipped with 128 GB of DDR3 RAM, and runs an Ubuntu 20.04.6 LTS.

6.1.4 Measurement Procedure. Figure 7b depicts our experiment diagram. Our experiments process could be described as follows:

- ■ As the initial step, The desired hardware design of the *Target IC* (e.g., a masked AES) as a bitstream is programmed using a JTAG connection.

(1) Arbitrary input data (i.e., masked plaintext, masked keys, etc.) are prepared in the *Analyzer System* and are sent to the *Controller*.
(2) Using a serial interface *Controller*, sends the data to the *Target IC* and collects timing stamps (Clock triggers) from *Target IC* during its operation. At a desired time stamp, it triggers the VNA for the measurement.
(3) VNA performs a measurement upon getting triggered and sends back the measured traces to the *Analyzer System*.
(4) Once the execution on the *Target IC* is finished, output is received by the controller and is sent to *Analyzer System* via UART connection for verification purposes.

For the suitable profiling procedure required for our proposed attacks, we developed an iterative and automated process to capture the traces. Furthermore, note that in accordance with our threat model, our attacks require time-constant measurements as it exploits the physical characteristics of the die. Hence, synchronization and clock control are vital in our measurements, handled via *Controller* in our attack scenarios.

6.2 Target Implementation and Configuration

VNA Configurations and Frequency bands. On each set of experiments, based on the target implementation different frequency target band is selected. Based on our experiments, different implementations on the FPGA results in different leakage on each narrow-band frequency. This is due to the variations in physical realization of components on the target which effects the impedance profile. We indicate that different target frequency band might result in different (maybe superior) attack success rate. Our targeted bands are selected naively and experimentally. Furthermore, *IF Bandwidth* and *Averaging* factors, used for adjusting the VNA measurement quality are set experimentally in our attacks. IF Bandwidth is set to *500 Hz* in our experiments to reliably filter out unwanted responses such as higher frequency spectral noise [41] and Averaging factor is selected to be $AV_{idx} = 200$ in TIMA attack to reduce measurement noise floor.

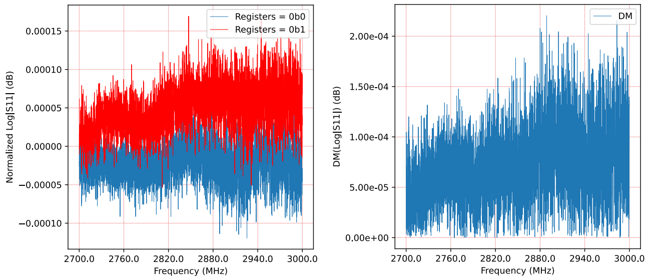
Implementation of AES S-box. Unprotected AES targeted for CIMA and DIMA in our experiments is implemented with a fully pipelined architecture using Canright's S-box [9]. These attacks are carried out at the first clock-cycle (first round S-box's output).

Implementation of Masked AES. Ultimately we deploy experiments with TIMA, targeting AES DOM implementation for FPGA [32] with 3 shares (masking order of 2). We mount two attacks on different scenarios. 1) The measurements are performed on the first round's key-share byte registers of extended Canright's masked S-box[10] which is the underlying S-box circuitry used in AES DOM. This attack targets the first byte of the key and is carried out when three key-share registers are loaded in the core before the execution of the first masked S-box (clock-cycle 1) 2) We target the full key extraction during the initialization process and once key values (3×128 bits) are loaded into the registers. We deploy TIMA before starting AES-DOM is executed (Where *aes_start* signal is set at clock-cycle 0).

Complex Number Analysis. Although the impedance values (alternatively S_{11}) are complex values which are usually represented by magnitude and phase numbers, our main attacks (i.e., CIMA, DIMA, and TIMA) are only carried out on the phase ($\angle S_{11}$) part of the measurements.

6.3 Attacking Fan-out Registers

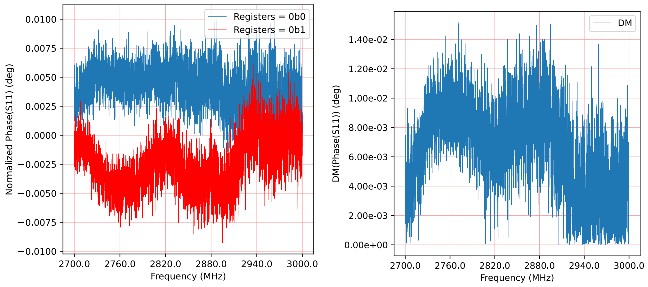
We start off with a simple profiling analysis of a design with fan-out registers. The same methodology is used by Moradi et al. [58] and similar research scenario [56] to analyze the leakage of static power consumption. Here, we cascaded two 1024 sets of FDCEs (D Flip-Flop with Clock Enable and Asynchronous Clear) [83]. In contrast with static-based power SCA [58], we explicitly specified the location [82] of the register sets for the implementation phase as different locations of registers yield different results in our evaluation. In this experiment, the wiring and locations are manually specified to deploy two connected register sets on two adjacent FPGA slices [81].



(a)

(b)

Figure 8: $|S_{11}|$ leakage on fan-out register. (a) Normalized and averaged comparison (b) Differential analysis of leakage.



(a)

(b)

Figure 9: $\angle S_{11}$ leakage on fan-out register. (a) Normalized and averaged comparison (b) Differential analysis of leakage.

High Fan-out Binary Registers In the first experiments, we program the DUT to set all 2048 registers to either **`0b0`** or **`0b1`**. This setting is done via deploying a control register on the FPGA configured by the *Controller*. Upon receiving the *run* command from the *Controller*, values on the registers are set. For each case, we collect the total number of *600* traces in the frequency range of $F = 2.7GHz - 3GHz$, with 5000 linearly spanned frequency stamps. In other words, $((3 - 2.7)/1000) \times 10^9 Hz = 300kHz$ is set as the frequency resolution. To minimize temperature-induced drifts, we follow a normalization process where we perform a reference measurement (e.g. a FPGA register fan-out program where all registers are cleared.) after each measurement and store the difference as the final trace. Note that since our attack is a differential attack, normalized values do not affect the final outcome.

Figure 8a depicts average values of S_{11} magnitude for each case of the experiment over the selected frequency band. The difference (*DM*) between the two groups is illustrated in Figure 8b. As shown in this figure, the difference exists over the entire selected frequency band, however, at some stamps, it is larger compared to others. This indicates that at certain frequency stamps, the magnitude of the impedance differs based on the content of the registers and their corresponding wiring on specific positions on the die.

Similarly, Figure 9 details the average difference of $\angle S_{11}$ for each group of traces. Note that $\angle S_{11}$ and $|S_{11}|$ are uniquely different metrics with completely different behavior. Consequently, each case in Figure 8a and Figure 9a follow different pattern. For instance,

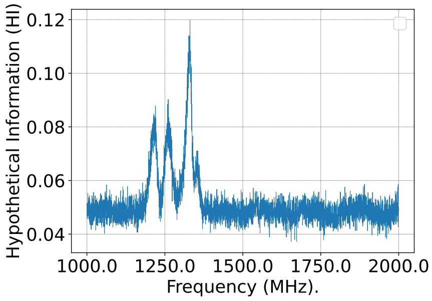


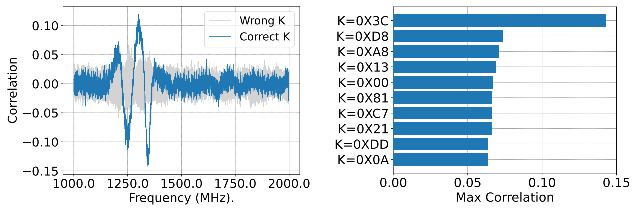
Figure 10: Hypothetical Information (HI) the impedance leakage for the presented S-box attack.

normalized $\angle S_{11}$ for case `0b1` is less than `0b0` traces for most of the selected frequency band, where for $|S_{11}|$ opposite behavior is observed. Also, the absolute difference at some frequencies is larger compared to the magnitude DM. This can be justified as often RF *Phase* measurements are known to be more resistant to noise compared to magnitude.

To validate that the SNR level in the experiments is exploitable, we organize a simple profiling attack, where we use 600 (out of 1200) traces to determine *POI* frequencies (We refer to them as *Train Data*) and then read out values of other 600 traces (e.g., *Test Data*) at selected *POI* based on each case. The details of these experiments are provided in Appendix 8.

6.4 Attacking AES S-BOX

As the next step, we advance our target to attack AES S-BOX. We consider first-round S-BOX with a known plain-text scenario. In the following, we apply CIMA and DIMA attacks to an unprotected AES S-BOX implementation (derived from ProjectVault [17]). Also, note that S-BOX's output $Tar = S - BOX(K_{in}, P_{in})$ is considered as the target intermediate value in our attacks, and the goal is to find the first byte of the secret key value. In order to verify the leakage for our captured traces, we first demonstrate an information leakage analysis. Figure 10 shows the Hypothetical Information (HI) [8] of impedance leakage for the S-box target in frequency domain. It shows that the some frequency sub-bands are more exploitable compared to others.



(a)

(b)

Figure 11: *CIMA* on 1200 samples (a) Correlation index over selected frequency band and (b) Top correlated keys and the maximum value of correlation (the selected frequency for keys are not necessarily the same).

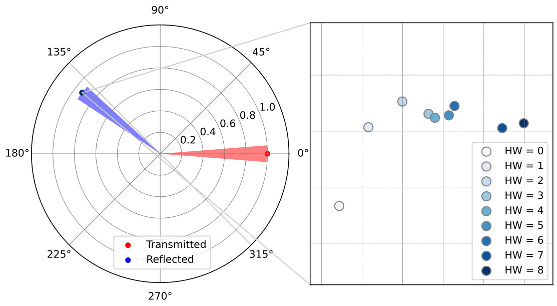
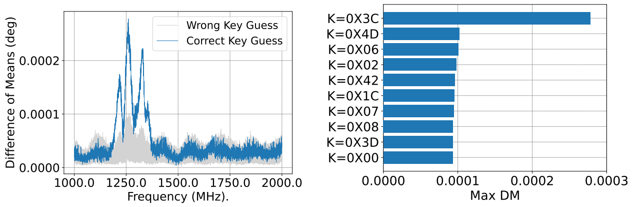


Figure 12: Polar representation of each *HW* group of the reflected traces at $Freq = 1328MHz$, where CIMA score is maximized. Near-linear trend of HW leakage is visible for $\angle S_{11}$.

6.4.1 CIMA. As our first attempt to break AES using impedance data, we deploy *CIMA* based on a conventional HW model. In this experiment, we mount our attack on 1200 measurement traces. Furthermore, we select the frequency range of $F = 2GHz - 3GHz$, with 3000 linearly spanned stamps. Figure 11 depicts the results of CIMA in terms of correlation index.

Furthermore, to verify that the chosen model in our attack successfully distinguishes on *Magnitude* and *Phase*, Figure 12 represents the polar distribution of the collected measurements with respect to the *HW* of the chosen intermediate value. As shown, we grouped up and averaged the traces in their corresponding *HW* class. The distribution of reflected signals (indicated in blue) shows that groups could be effectively distinguished.

6.4.2 DIMA. Our next attack scenario is to perform impedance differential analysis (namely *DIMA*) on an AES S-Box. For this attack, we employ $N = 3000$ traces on the frequency band of $F = 1GHz - 2GHz$, with 3000 frequency samples at each measurement. Figure 13 shows the final differential results for the possible key space using a multi-bit DIMA analysis.



(a)

(b)

Figure 13: *DIMA* on 3000 samples (a) Differential results over the key space (b) Keys with the maximum value of multi-bit differences.

As another analysis, we investigated and measured the leakage of each individual intermediate bit as our indicator. Figure 14 depicts the leakage for different bits of the target intermediate value. Although some bits are potentially more exploitable for the attack, it is clearly observed that each individual bit leaks in a distinguishable set of frequency samples.

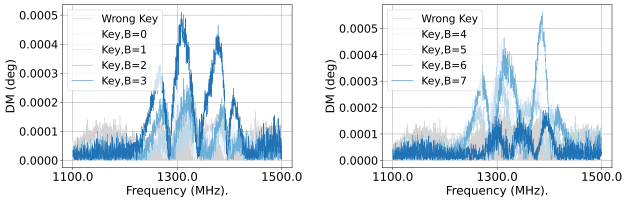


Figure 14: DIMA leakage analysis of different bits of the intermediate value

6.5 Attacking DOM AES

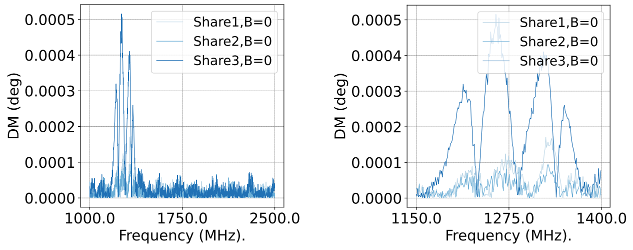
As our ultimate experiment, we prepare an attack on a protected AES implementation. In this scenario, we target a 3-Share AES DOM hardware core. To ensure that random generator execution does not incur additional leakage, we consider an off-chip TRNG, which feeds in the masked operands into the FPGA target. As explained, we consider the attack in two scenarios.

6.5.1 Attacking Key Register Byte. Here, we perform the attack at the first clock-cycle where shares of the first key byte (as well as first input byte shares) are loaded into the target. Hence, regardless of the masked operations on the upcoming clocks, TIMA attacks the key (share) registers directly. We carry out the *Profiling Stage* with $N = 20,000$ number of traces to template masked key registers. Specifically, we execute *TIMA* profiling for each bit of all key shares independently ($8 \times 3 = 24$ for each byte of the master key). It is also worth noting that shares are generated uniformly random and each trace is used to template for all target bits. More specifically, for each template target bit, we would have roughly $N_0 = 10,000$ traces where a target bit of the target share is **0b0**.

Figure 15 and Figure16 show the bit leakage model among bits on different shares and on the same share, respectively. Note that DM metric is shown here to highlight that distinguished POIs on different frequency points for each individual bit of each share enables *TIMA* to effectively extract the master key.

After *Profiling Phase*, we perform a single trace attack on the DUT with unknown shares. In order to reduce the noise we carried out VNA-enabled averaging of $AV_{idx} = 200$ on the the attack trace. *TIMA* successfully recovers all the bits of each share individually. Figure 17 serves as an example to showcase the key extraction based on template scores of each target bit after attack stage. Combining extracted share bits could then be used to reconstruct the first byte of the master key as shown in Figure 17.

6.5.2 Analysing Full-length Key. We further focus on the key registers on the FPGA at the time before the AES-DOM is initiated. As random shares are stored on FPGA registers before loaded into the AES core (i.e., DOM core), we target the time-stamp where *aes_start* signal is set. Note that although DOM execution is byte-wise and shares are randomize in the key registers for each byte execution, original shares are loaded from other locations (additional wires and registers) into the core. These registers are targeted in this attack.



(a) (b)

Figure 15: Leakage measurement of *Inter-Share* bits based on DM. (a) Wide frequency plot and (b) frequency zoomed-in plot.

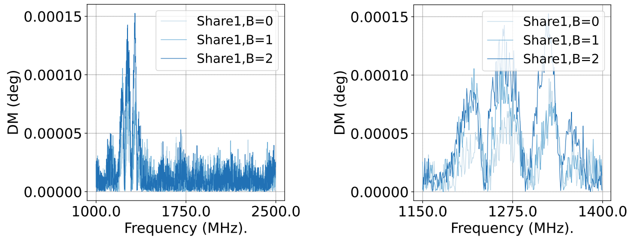


Figure 16: Leakage measurement of *Intra-Share* bits based on DM. (a) Wide frequency plot and (b) frequency zoomed-in plot.

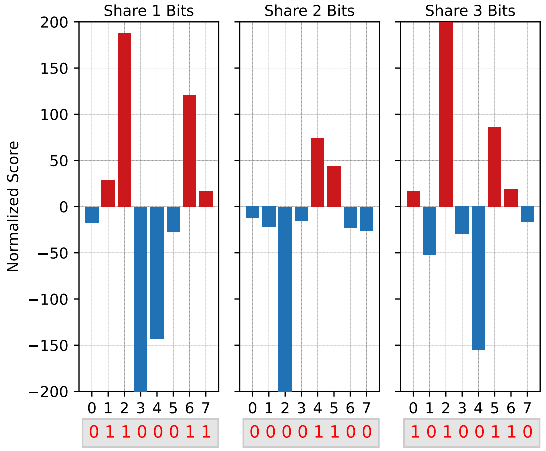


Figure 17: Extracting the bit values of all three shares for the first key byte, the first byte of master key can be computed as $K = S_1 \oplus S_2 \oplus S_3 =$ 0xC6 $\oplus$ 0x30 $\oplus$ 0x65 = 0x93

We profile TIMA on full-length keys with 50,000 traces and follow the same procedure explained in the previous attack. Figure 18 shows the DM metric over frequency domain for different bits on all three shares of the target key during TIMA *Profiling Phase.* Note that similar to the previous experiment, DM is plotted for the averaged

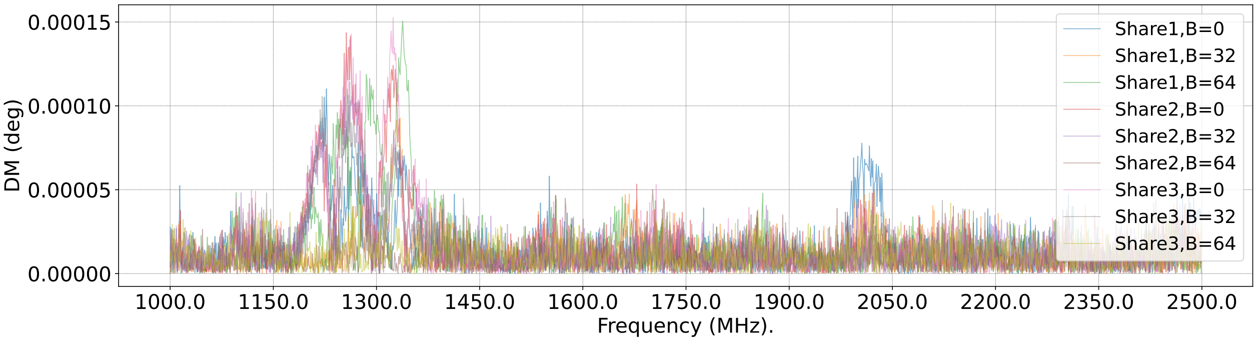


Figure 18: illustration of full-length key leakage through frequency of AES-DOM using TIMA

trace of approximately 25,000 traces for $b_t = 0b0$ and 25,000 traces for $b_t = 0b1$ ($DM_{b_t} = Abs(Mean(Tr|b_t = 0b0) - Mean(Tr|b_t = 0b1))$). As shown, each individual bit could visually be distinguished by DM metric.

7 DISCUSSIONS

7.1 Comparison with Power SCA

There has been a numerous efforts to provide fair metrics [67] and methodologies [8, 22, 52] to compare and analyze the leakage of various power analysis attacks. It is shown that time-series multivariate leakage in dynamic power attacks could be considered to improve attack success rate [33]. Impedance leakage is multivariate by nature but in contrast to dynamic leakage is time-constant. Although, dimension reduction techniques such as Principal Component Analysis (PCA) combined with leakage metrics such as Perceived Information (PI) [77] could be used to provide fair comparison with uni-variate leakage [22] (e.g. averaged static traces), further extensive experiments and modeling are required.

Moreover, the threat model assumptions, experimental conditions, and setup highly contributes to the SNR and success rate of the attack. Impedance attack presented in this work is somehow similar to static-side channels but differs in experimental details. Moradi [58] and Moos [55] use climate chambers and full board clock halt (for noise reduction) to perform static SCA. Cassiers et al. [11] removed the need for a climate chamber in a later work, but the attack still requires a low-noise amplifier, the control of the power supply and the source clock of the target, whereas impedance analysis utilizes only clock gating with no control over power supply or environment temperature. We believe that an accurate experimental comparison among static, dynamic, and impedance SCA should be under the same threat model, conditions, and target and deserves a future study. Another interesting course of research could be the leakage analysis of time-variant impedance profiles which could introduce time-frequency multivariate impedance attacks.

7.2 Possible Countermeasures

As investigated throughout the paper, the nature of impedance leakage is directly caused by the physical placements of secret-dependant registers. Hence, a fundamental approach to resolve these leakages is real-time refreshing of the secret-dependant registers and/or routing. A series of hardware randomization solutions [34, 44, 53] present methods including partial reconfiguration as *Moving Target Defense*, to secure FPGA against SCA. Similar methodologies [35], if deployed in an online manner, could be used to prevent impedance analysis. Alternatively, system level approaches to detect clock-control on the device [24] could also be deployed as countermeasure to those impedance attacks which are performed in clock-controlled environment.

7.3 Clock control and impedance measurements

A clock controller is deployed in our measurement setup to ensure an accurate time stamp for our measurements. However, compared to static power side-channel where static snapshots without halted clocks could lead to an increase of the noise (due to additive noise caused by dynamic power consumption) [22], impedance analysis is not susceptible to time-varying measurements as long as the target intermediate values are stored (i.e., in Flip-Flops) in the circuit. This is mainly due to the unique and non-additive leakage of each individual (bit of) intermediate value through the frequency domain, which relaxes the clock control constraints in our threat model. On the other hand, as indicated by prior works [48, 56], in many real-world cryptographic masked hardware and software implementations [1, 36], masked state/key registers are not overwritten every clock-cycle and are maintained for tens of clock cycles. Consequently, it is possible for the adversary to perform an iterative measurement without clock control to capture properly time-stamped measurements.

Furthermore, we stress that if target frequencies are known by the adversary (i.e., in the case of template attack), considering the typical VNA capabilities [41], frequency sweep could be done up-to two orders of magnitude faster, giving the adversary the advantage to perform multiple measurements during a single MHz clock execution of DUT.

7.4 Effects of Wiring

Previous researchers have shown that long wires in FPGA implementations could potentially increase the leakage for power side-channel attacks [29, 30]. On the other hand, very close wiring between sensitive operands could also result in coupling effects [20] that leak sensitive data. Hence, hardware routing and wiring should be done exceedingly carefully when it comes to implementing protected crypto-systems. Our experiments show that long wiring of secret dependant registers increases impedance leakages as well. Specifically, the deployment of long routing on the FPGA die realizes a series of buffers and intermediate elements that contributes to target impedance which could be exploited to reveal data.

8 CONCLUSION

In this paper, we presented a novel non-invasive physical side-channel attack exploiting the data-dependent changes in the impedance of the chip. We demonstrated that the temporarily stored contents in registers of an IC alter the die's impedance, which can be measured using scattering parameters commonly deployed in RF/microwave engineering. Since registers at different locations affect the impedance profile of the system at various frequency bands, the content of these registers can be probed simultaneously by identifying the frequencies of interest. To assess the threat of our discovered side-channel, we mounted several impedance analysis attacks against unprotected and protected hardware AES-128 implementations on an FPGA and showed that secret key bits could be recovered confidently. In the case of the profiled attack, only a single trace was required to recover the secret key. Our results challenged the effectiveness of masking schemes as side-channel countermeasures, and hence, we believe that the integration of specific hiding countermeasures in addition to masking is required to mitigate our attack.

REFERENCES

[1] ANSSI-FR. 2023. ASCAD masked implementation of AES. https://github.com/ANSSI-FR/ASCAD. Accessed: 2023-04-26.

[2] Benjamin Arai, Gautam Das, Dimitrios Gunopulos, and Nick Koudas. 2007. Anytime measures for top-k algorithms. In *Proceedings of the 33rd international conference on Very large data bases.* 914–925.

[3] Stephen A Billings. 2013. *Nonlinear system identification: NARMAX methods in the time, frequency, and spatio-temporal domains.* John Wiley & Sons.

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

[5] Léon Bottou. 1998. Online algorithms and stochastic approxima-p tions. *Online learning and neural networks* (1998).

[6] Eric Brier, Christophe Clavier, and Francis Olivier. 2004. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6.* Springer, 16–29.

[7] Olivier Bronchain, Gaëtan Cassiers, and François-Xavier Standaert. 2021. Give me 5 minutes: Attacking ASCAD with a single side-channel trace. *Cryptology ePrint Archive* (2021).

[8] Olivier Bronchain, Julien M Hendrickx, Clément Massart, Alex Olshevsky, and François-Xavier Standaert. 2019. Leakage certification revisited: Bounding model errors in side-channel security evaluations. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I 39.* Springer, 713–737.

[9] David Canright. 2005. A very compact S-box for AES. In *International Workshop on Cryptographic Hardware and Embedded Systems.* Springer, 441–455.

[10] David Canright and Lejla Batina. 2008. A very compact "perfectly masked" S-box for AES. In *Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings 6.* Springer, 446–459.

[11] Gaëtan Cassiers, Loïc Masure, Charles Momin, Thorben Moos, and François-Xavier Standaert. 2023. Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023), 482–518.

[12] Hasna Chaibi, Mostafa Belkasmi, and Z Mohammadi. 2015. UWB outdoor channel characterization and modeling based on measurements. In *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM).* IEEE, 1–5.

[13] Suresh Chari, Charanjit S Jutla, Josyula R Rao, and Pankaj Rohatgi. 1999. Towards sound approaches to counteract power-analysis attacks. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19.* Springer, 398–412.

[14] Suresh Chari, Josyula R Rao, and Pankaj Rohatgi. 2003. Template attacks. In *Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4.* Springer, 13–28.

[15] Israel Cohen, Yiteng Huang, Jingdong Chen, Jacob Benesty, Jacob Benesty, Jingdong Chen, Yiteng Huang, and Israel Cohen. 2009. Pearson correlation coefficient. *Noise reduction in speech processing* (2009), 1–4.

[16] Duška Čoja, Nataša Nešković, and Aleksandar Nešković. 2017. Channel impulse response estimation using vector network analyzer. In *2017 25th Telecommunication Forum (TELFOR).* IEEE, 1–4.

[17] Open Source Community. 2023. Github, Project Vault. https://github.com/ProjectVault/orp/tree/master/hardware. Accessed: 2023-04-26.

[18] PyVisa Community. 2023. PyVISA: Control your instruments with Python. https://pyvisa.readthedocs.io/en/latest/. Accessed: 2023-04-26.

[19] Scipy Community. 2023. Scipy Statistical Functions. https://docs.scipy.org/doc/scipy/reference/stats.html. Accessed: 2023-04-26.

[20] Thomas De Cnudde, Begül Bilgin, Benedikt Gierlichs, Ventzislav Nikov, Svetla Nikova, and Vincent Rijmen. 2017. Does coupling affect the security of masked implementations?. In *Constructive Side-Channel Analysis and Secure Design: 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers 8.* Springer, 1–18.

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

[22] Santos Merino Del Pozo, François-Xavier Standaert, Dina Kamel, and Amir Moradi. 2015. Side-channel attacks from static power: When should we care?. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE).* IEEE, 145–150.

[23] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. 2019. Unifying leakage models: From probing attacks to noisy leakage. *Journal of Cryptology* 32 (2019), 151–177.

[24] Robert Dumitru, Andrew Wabnitz, and Yuval Yarom. 2023. On Borrowed Time–Preventing Static Power Side-Channel Analysis. *arXiv preprint arXiv:2307.09001* (2023).

[25] François Durvaux and François-Xavier Standaert. 2016. From improved leakage detection to the detection of points of interests in leakage traces. In *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I 35.* Springer, 240–262.

[26] RAM Fens, Mayazzurra Ruggiano, and Geert Leus. 2008. Channel characterization using radar for transmission of communication signals. In *2008 European Conference on Wireless Technology.* IEEE, 127–130.

[27] Julie Ferrigno and M Hlaváč. 2008. When AES blinks: introducing optical side channel. *IET Information Security* 2, 3 (2008), 94–98.

[28] Daniel Genkin, Adi Shamir, and Eran Tromer. 2017. Acoustic cryptanalysis. *Journal of Cryptology* 30 (2017), 392–443.

[29] Ilias Giechaskiel and Ken Eguro. 2016. Information leakage between FPGA long wires. *arXiv preprint arXiv* 1611 (2016).

[30] Ilias Giechaskiel, Ken Eguro, and Kasper B Rasmussen. 2019. Leakier wires: Exploiting FPGA long wires for covert-and side-channel attacks. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)* 12, 3 (2019), 1–29.

[31] Hannes Groß, Stefan Mangard, and Thomas Korak. 2016. Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order. *Cryptology ePrint Archive* (2016).

[32] Hannes Gross, Stefan Mangard, and Thomas Korak. 2016. Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. *Cryptology ePrint Archive* (2016). https://eprint.iacr.org/2016/486

[33] Vincent Grosso and François-Xavier Standaert. 2015. ASCA, SASCA and DPA with enumeration: which one beats the other and when?. In *Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21.* Springer, 291–312.

[34] Tim Güneysu and Amir Moradi. 2011. Generic side-channel countermeasures for reconfigurable devices. In *Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13.* Springer, 33–48.

[35] Benjamin Hettwer, Johannes Petersen, Stefan Gehrer, Heike Neumann, and Tim Güneysu. 2019. Securing cryptographic circuits by exploiting implementation diversity and partial reconfiguration on FPGAs. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE).* IEEE, 260–263.

[36] hgrosz. 2023. Verilog Implementation of DOM AES. https://github.com/hgrosz/aes-dom. Accessed: 2023-04-26.

[37] Michael Hutter and Jörn-Marc Schmidt. 2014. The temperature side channel and heating fault attacks. In *Smart Card Research and Advanced Applications: 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013.*

Revised Selected Papers 12. Springer, 219–235.

[38] Masahiro Ichihashi and Haruichi Kanaya. 2019. A simple methodology for on-chip transmission line modeling and optimization for high-speed clock distribution. *Japanese Journal of Applied Physics* 58, SB (2019), SBBC06.

[39] Yuval Ishai, Amit Sahai, and David Wagner. 2003. Private circuits: Securing hardware against probing attacks. In *Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23*. Springer, 463–481.

[40] Akira Ito, Rei Ueno, and Naofumi Homma. 2022. On the success rate of side-channel attacks on masked implementations: Information-theoretical bounds and their practical usage. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 1521–1535.

[41] keysight. 2023. E5080A ENA Documentation Manual. https://www.keysight.com/us/en/library/manuals/help-file/e5080a-ena-network-analyzer-pdf-help-for-firmware-rev-a110x-2651497. Accessed: 2023-04-26.

[42] Keysight. 2023. Keysight Documentations. https://www.keysight.com/us/en/product/E5080A/e5080a-ena-vector-network-analyzer.html. Accessed: 2023-04-26.

[43] Kleindiek Nanotechnik GmbH. 2020. Prober Shuttle (PS8). https://www.nanotechnik.com/ps8.html

[44] David S Koblah, Fatemeh Ganji, Domenic Forte, and Shahin Tajik. 2022. Hardware Moving Target Defenses against Physical Attacks: Design Challenges and Opportunities. In *Proceedings of the 9th ACM Workshop on Moving Target Defense*. 25–36.

[45] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential power analysis. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*. Springer, 388–397.

[46] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. 2011. Introduction to differential power analysis. *Journal of Cryptographic Engineering* 1 (2011), 5–27.

[47] Paul C Kocher. 1996. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*. Springer, 104–113.

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

[49] Thilo Krachenfels, Tuba Kiyan, Shahin Tajik, and Jean-Pierre Seifert. 2021. Automatic Extraction of Secrets from the Transistor Jungle using {Laser-Assisted}{Side-Channel} Attacks. In *30th USENIX Security Symposium (USENIX Security 21)*. 627–644.

[50] Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson, Christine Servière, and Jean-Louis Lacoume. 2006. A proposition for correlation power analysis enhancement. In *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*. Springer, 174–186.

[51] Leonard MacEachem, Xin Jie Wang, and Tad Kwasniewski. 2017. On-die power grid broadband model determination using a priori narrowband measurements. *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)* (2017), 1493–1496.

[52] Loïc Masure, Gaëtan Cassiers, Julien Hendrickx, and François-Xavier Standaert. 2023. Information bounds and convergence rates for side-channel security evaluators. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023), 522–569.

[53] Nele Mentens. 2017. Hiding side-channel leakage through hardware randomization: A comprehensive overview. In *2017 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS)*. IEEE, 269–272.

[54] MiniCircuits. 2023. MiniCircuits Datasheets. https://www.mouser.com/datasheet/2/1030/CBL_2FT_SMNM_2b-2303455.pdf. Accessed: 2023-04-26.

[55] Thorben Moos. 2019. Static Power SCA of Sub-100 nm CMOS ASICs and the Insecurity of Masking Schemes in Low-Noise Environments. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2019, 3 (2019), 202–232.

[56] Thorben Moos. 2019. Static power SCA of sub-100 nm CMOS asics and the insecurity of masking schemes in low-noise environments. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), 202–232.

[57] Thorben Moos, Amir Moradi, and Bastian Richter. 2019. Static power side-channel analysis—An investigation of measurement factors. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28, 2 (2019), 376–389.

[58] Amir Moradi. 2014. Side-Channel Leakage through Static Power: Should We Care about in Practice?. In *Cryptographic Hardware and Embedded Systems–CHES 2014: 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings 16*. Springer, 562–579.

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

[60] Tahoura Mosavirik, Saleh Khalaj Monfared, Maryam Saadat Safa, and Shahin Tajik. 2023. Silicon Echoes: Non-Invasive Trojan and Tamper Detection using Frequency-Selective Impedance Analysis. *Cryptology ePrint Archive* (2023).

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

[62] NewAE. 2023. CW305 Artix FPGA Target. https://rtfm.newae.com/Targets/CW30520Artix20FPGA. Accessed: 2023-04-26.

[63] NewAE. 2023. NewAE Hardware Product. https://rtfm.newae.com/Capture/ChipWhisperer-Lite/. Accessed: 2023-04-26.

[64] Luong N Nguyen, Chia-Lin Cheng, Milos Prvulovic, and Alenka Zajić. 2019. Creating a Backscattering Side Channel to Enable Detection of Dormant Hardware Trojans. *IEEE transactions on very large scale integration (VLSI) systems* 27, 7 (2019), 1561–1574.

[65] Luong N. Nguyen, Baki Berkay Yilmaz, Milos Prvulovic, and Alenka Zajic. 2020. A Novel Golden-Chip-Free Clustering Technique Using Backscattering Side Channel for Hardware Trojan Detection. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 1–12.

[66] Elisabeth Oswald and Stefan Mangard. 2006. Template attacks on masking—resistance is futile. In *Topics in Cryptology–CT-RSA 2007: The Cryptographers' Track at the RSA Conference 2007, San Francisco, CA, USA, February 5-9, 2007. Proceedings*. Springer, 243–256.

[67] Kostas Papagiannopoulos, Ognjen Glamočanin, Melissa Azouaoui, Dorian Ros, Francesco Regazzoni, and Mirjana Stojilović. 2023. The side-channel metrics cheat sheet. *Comput. Surveys* 55, 10 (2023), 1–38.

[68] Bile Peng, Sebastian Rey, and Thomas Kürner. 2016. Channel characteristics study for future indoor millimeter and submillimeter wireless communications. In *2016 10th European Conference on Antennas and Propagation (EuCAP)*. IEEE, 1–5.

[69] David M Pozar. 2011. *Microwave engineering*. John wiley & sons. 299 pages.

[70] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan. 2009. Statistical analysis of second order differential power analysis. *IEEE Transactions on computers* 58, 6 (2009), 799–811.

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

[72] Li Chuang Quek, Ming Dak Chai, and Heng Chuan Shu. 2015. Characterization of on die capacitance and silicon measurement correlation. In *2015 International Conference on Electronics Packaging and iMAPS All Asia Conference (ICEP-IAAC)*. IEEE, 739–742.

[73] Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, and Ingrid Verbauwhede. 2015. Consolidating masking schemes. In *Advances in Cryptology–CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I 35*. Springer, 764–783.

[74] Richard J Rossi. 2018. *Mathematical statistics: an introduction to likelihood based inference*. John Wiley & Sons.

[75] Larry D. Smith, Shishuang Sun, Mayra Sarmiento, Li Zhe, and Karthik Chandrasekar. 2011. On-Die Capacitance Measurements in the Frequency and Time Domains. *DesignCon, Santa Clara, CA* (2011).

[76] Robert Specht, Vincent Immler, Florian Unterstein, Johann Heyszl, and Georg Sig. 2018. Dividing the threshold: Multi-probe localized EM analysis on threshold implementations. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 33–40.

[77] François-Xavier Standaert, Tal G Malkin, and Moti Yung. 2009. A unified framework for the analysis of side-channel key recovery attacks. In *Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings 28*. Springer, 443–461.

[78] F-X Standaert, Eric Peeters, and J-J Quisquater. 2005. On the masking countermeasure and higher-order power analysis attacks. In *International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II*, Vol. 1. IEEE, 562–567.

[79] HL van Trees, KL Bell, and Z Tian. 2013. Detection estimation and modulation theory, part I: Detection, estimation, and filtering theory. *A Papoulis Probability Random Variables & Stochastic Processes* 8, 10 (2013), 293–303.

[80] Lichao Wu, Guilherme Perin, and Stjepan Picek. 2022. The best of two worlds: Deep learning-assisted template attack. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022), 413–437.

[81] Xilinx. 2023. Xilinx 7 Series FPGAs Configurable Logic Block. https://www.eng.auburn.edu/~nelson/courses/elec4200/FPGA/ug474_7Series_CLB.pdf. Accessed: 2023-04-26.

[82] Xilinx. 2023. Xilinx Constraints Guide. https://www.xilinx.com/htmldocs/xilinx14_7/cgd.pdf. Accessed: 2023-04-26.

[83] Xilinx. 2023. Xilinx Documentation. https://docs.xilinx.com/r/en-US/ug974-vivado-ultrascale-libraries/EFUSE_USR. Accessed: 2023-04-26.

[84] Xilinx. 2023. Xilinx Vivado Toolkits. https://www.xilinx.com/products/design-tools/vivado.html. Accessed: 2023-04-26.

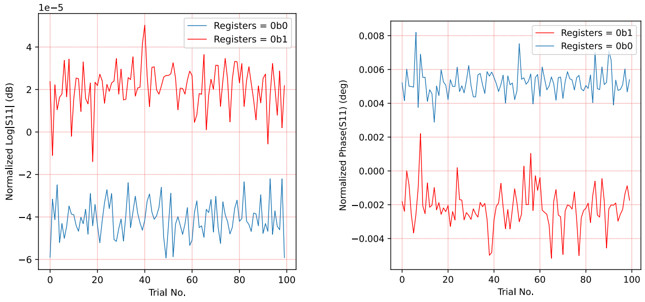
[85] Xuefeng Yin and Xiang Cheng. 2016. *Propagation channel characterization, parameter estimation, and modeling for wireless communications*. John Wiley &

Sons.
[86] Huifeng Zhu, Haoqi Shan, Dean Sullivan, Xiaolong Guo, Yier Jin, and Xuan Zhang. 2022. PDNPulse: Sensing PCB Anomaly with the Intrinsic Power Delivery Network. (2022), 1–17.

APPENDICES

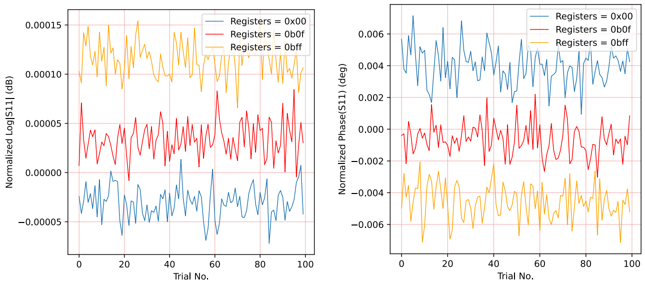
A. Validation Tests For Bit Extractions

Figure 19 shows the results of the aforementioned verification process (described in Section 6.3) for 100 random trials. More specifically, at each trial, POI is calculated as in Equation 7:



(a) **(b)**

Figure 19: Profiled testing on single bit fan-out register implementation (a) $|S_{11}|$ and (b) $\angle S_{11}$.



(a) **(b)**

Figure 20: Profiled testing on multi-bit fan-out register implementation (a) $|S_{11}|$ and (b) $\angle S_{11}$.

$$
\begin{aligned}
DM_{trial} &= DM(Rnd(Trace|R = 0b0), Rnd(Trace|R = 0b1)) \\
POI_{trial} &= ArgMax(DM_{trial}(S_{11}))
\end{aligned}
\tag{7}
$$

Where *DM* is calculated over two 300 sets of randomly picked traces from each case. Then, the normalized and averaged S_{11} value for each case is plotted at the chosen POI_{trial}.

Multi-Valued Registers For more advanced attacks, we also implement a similar scenario for a 2-threshold fan-out register layout. We set 4096 FDCEs to be configured as 1) all zeros (**`0x00`**), or 2) all ones (**`0xff`**), or 3) balanced zeroes and ones (**`0x0f`**). Figure 20 illustrates phase and magnitude test results for a 2-threshold distinguisher. In this scenario, the POI frequency for each trial is selected based on an additive DM of each case:

$$
\begin{aligned}
&For : a, b \in \{0x00, 0xff, 0x0f\}, a \neq b \\
&DM_{trial} = \sum_{a,b} (DM(Rnd(Tr|R = a), Rnd(Tr|R = b)))
\end{aligned}
\tag{8}
$$

As depicted in Figure 20, both S_{11} magnitude and phase could be used to distinguish and mount a successful analysis to discover registers' contents.