LeakyOhm: Secret Bits Extraction using Impedance Analysis

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

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

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

ABSTRACT
The threat of physical side-channel attacks and their countermeasures is a widely researched field. Most physical side-channel attacks rely on the unavoidable influence of computation or storage on voltage or current fluctuations. 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 temporally 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 violates 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 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

Reference Format:

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 [41], electromagnetic emanation [39], acoustic waves [23], photon emission [22], and thermal radiation [31]. Over the last three 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 [54, 58, 59] and PCBs [52, 55, 78]), 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 [51]. 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 [48, 51] 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) Does impedance analysis provide any advantages over conventional SCA attacks (e.g., power or EM) in terms of granularity or number of traces? (3) 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 single-trace non-invasive SCA attack based on direct characterization of the chip’s impedance. Our method relies on a known RF/microwave impedance characterization technique called scattering parameter analysis, in which we inject sine waves with different frequencies into the power delivery network (PDN) of the chip and measure the echo 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. We will discuss how the transistor’s imperfections, asymmetric logic gates, and interconnects with various lengths contribute to
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 wide-band on-chip behavior of the circuit, multiple narrow-band 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 \( C_{\text{die}} \) and resistance \( R_{\text{die}} \) are the dominant features of the on-chip impedance in high-frequency bands [68]. 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 \( C_{\text{die}} \) is affected by several elements, including the metal layers grid network, non-switching gate, and p-n diode junction diffusion [68]. Resistance in the power net, transistor channel, transistor gate, and contacts of n-well and P-substrate contribute to \( R_{\text{die}} \) [45].

The location of each capacitance that contributes to \( C_{\text{die}} \) is shown in Figure 2 using different colors. The black color represents the metal capacitance, \( C_m \), which pertains to the power/grid 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 \( C_{\text{die}} \), 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 \( C_{\text{die}} \). 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 inverter is not powered on, the decoupling capacitance effect of the gates is negligible. However, when the element is turned on, the channels start to form, and as a result, \( C_g \) becomes the dominant contributor to \( C_{\text{die}} \). If the element’s design is modified, different parts of \( C_{\text{die}} \) (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, 64]. \( S \) parameters are spectrally measured over the frequency domain and are typically used in RF/microwave engineering to obtain the reflection/transmission properties of the circuit to the applied electromagnetic field [62]. 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 in this regard. 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:

\[
\begin{align*}
S_{11} & = \frac{V_1^+}{V_1^-} \\
\eta & = \frac{1}{\sqrt{\epsilon_r}} \eta_0 \\
y & = j\beta_0 \sqrt{\epsilon_r} \\
y_0 & = j\beta_0
\end{align*}
\]

where \( S_{11} \) is the reflection coefficient, \( Z_0 \) represents the reference impedance of the VNA which is 50 \( \Omega \), and \( Z_{\text{DUT}} \) 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 a change in the characteristic impedance and propagation constant of medium 2 are represented by \( \eta \) and \( \gamma \), respectively. For simplicity, we assume that medium 1 and medium 3 are lossless, thus giving a characteristic impedance of \( \eta_0 \) and a corresponding propagation constant of \( y_0 = j\beta_0 \). We consider medium 2 as a non-magnetic (\( \mu_r = 1 \)) medium with a relative permittivity of \( \epsilon_r \). Considering \( \beta_0 = \omega \sqrt{\mu_r \epsilon_r} \), we can rewrite the second medium’s propagation constant as \( \gamma = j\beta_0 \sqrt{\epsilon_r} \). Considering \( \eta_0 = \sqrt{\mu_0 / \mu_0} \), we can rewrite the characteristic impedance of medium 2 as \( \eta = \sqrt{1 / \eta_0} \). \( \epsilon_0 \) and \( \mu_0 \) are the permittivity and permeability of the free space, respectively, and \( \beta_0 \) denotes the free space wave number. The VNA injects a voltage wave with the known amplitude of \( V_1^+ \) (in medium 1), and the reflected voltage wave is denoted with 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 [62]:

\[
V_1(z) = V_1^+ e^{-j\beta_0 z} + V_1^- e^{j\beta_0 z} \\
V_2(z) = V_2^+ e^{-\gamma z} + V_2^- e^{\gamma z} \\
V_3(z) = V_3^+ e^{-j\beta_0 z} \\
\end{align*}
\]

and \( V_1^+ \) is injected, multiple reflections and transmissions occur in the lines. Based on the model in Figure 3, the lines’ voltages can be written as [62]:

\[
V_1^+ \text{ (injected by VNA), whereas } V_1^-, V_2^+, V_3^+ \text{ and } V_3^- \text{ are unknown values. We apply the boundary conditions on the voltage wave components at the interfaces of the media and find all these four unknowns. We are interested in obtaining the}
\]

\[
Z_{\text{DUT}} = Z_0 \frac{1 + S_{11}}{1 - S_{11}},
\]

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) [53].
S\textsubscript{11} in medium 1 which can be derived as

\[ S_{11}(f, \epsilon, \Lambda) = \frac{V^{-}}{V^{+}} = \frac{(\eta^2 - \eta_0^2)(1 - e^{2j\Lambda L})}{(\eta_0 + \eta)^2 - (\eta - \eta_0)^2 e^{2j\Lambda L}} \] (2)

In Equation 2, \( L \) is the length of the path that the injected wave voltage travels. From the Equation, 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 smaller size changes in the chip’s configuration at higher frequencies are inversely proportional to each other. This explains why smaller size changes in the chip’s configuration at higher frequencies can be detected. 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 routing.

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 among multiple number of shares (multi-party computation) and the intermediate computations of the original secrets are dealt with these shares. 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 [9], an adversary who is limited to the \( d\)-th order SCA (or \( t \) 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 unfavorably influenced by Gaussian noise, and thus, the number of noisy traces needed to extract \( x \) grows exponentially with the number of shares [63].

On the other hand, the \( t \)-probing model, which was first introduced in the seminal work of Ishai et al. [33] 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 [20]. 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 these assumptions [42], for most practical SCA attacks, it is reasonable to assume that the adversary has a limited number of probes due to practical issues such as the lack of spatial space [37, 69] 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 smart-card chips [16, 28].

3 SYSTEM-LEVEL IMPEDANCE ANALYSIS
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 (i.e., VNA) and are transmitted through the output port directly to the DUT’s PDN. Consequently, the reflected 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 the approach of our attack.

As indicated, in 1, 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 2), 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 3, 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 signal yields in certain Magnitude and Phase when they are reflected back to the PDN pins (4). Then, VNA detects and measures the reflected signal (on RX) at each frequency and estimates scattering parameters (S-Parameters) as the final measurement. In 5 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 (f1, f2, f3).

3.2 Systematic Impedance Analysis

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

At the higher level, generated test signals at different frequencies could be treated as data carriers. 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 0 dB, 0°. The test signals are represented in a polar coordinate system in Figure 5. On the other side, the received signals which are attenuated and distorted can also be represented as polar coordinates $|M_{RX} dB| \angle P_{RX}$. 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 [77]. Although similar measurement methodologies seek to characterize the wireless channels [8, 12, 61], we apply the same measuring methodology in the context of IC characterization to extract information. In other words, the channel characterization in this case, results in recovering 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 $|M_{RX} dB| \angle P_{RX}$ with respect to the target state of the DUT.

4 PHYSICAL-LEVEL ANALYSIS OF IMPEDANCE LEAKAGE

To perform SCA on the reflected signals from the chip’s die, it is vital to interpret 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 at high level [21]. In this case, the transmitted signal $x(t)$ from the VNA at frequency $f_i$ can be written as follows:

$$x(t) = A \sin(2\pi f t)$$

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(modulated) upon interaction of the carrier signals. Thus, the modulated signal $\tilde{x}(t)$, received at the VNA can be described [71]:

$$\tilde{x}(t) = aA \sin(2\pi f_i t - 2T) + \phi + n(t)$$

where $a$ is the attenuation or fading factor, $\phi$ 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.

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 (e.g., inductors and capacitors) reflect (and transmit) different portions of input energy in accordance with carrier frequency [32] due to non-linearity in their frequency response [3]. This frequency-dependent behavior of the elements in the microscopic scale is affected by physical and intrinsic features, which determines the resonate frequency of the elements [65]. 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.
with the assumption of parallel computing on shares, the data-
physical locations) on the chip to perform a powerful SCA. This
masking schemes assumes that expected power consumption
$P$ significantly [18]. The CMOS power consumption model in boolean
dependent power leakage is experimentally shown to be reduced
tacks [60, 72]. In the case of masking implementations on hardware,
implementation on a target chip. In Figure 6b, each target
depicts the utilization of $V$Probes
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 (i.e., 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 $\tilde{x}(t)$ within those frequency bands. In other words, by knowing those exact frequencies $f_{\text{Probe}}$, the adversary can place a Virtual Probe on C1 and C2. Sweeping to higher frequencies(GHz), the adversary will have multiple $V$Probes, 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 $V$Probes to effectively attack a Masked AES implementation on a target chip. In Figure 6b, each target masked key register would show a dominant response on a unique frequency set, leading the adversary to distinguish the leakages. 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.

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 implementa-
tions on software could be easily broken by template at-
tacks [60, 72]. 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 [18]. The CMOS power consumption model in boolean
masking schemes assumes that expected power consumption $P$ for

\begin{align*}
\forall f_1, f_2 \in F &= \{BW\}:
\quad \text{Im}(f_1(c = 0) = \text{Im}(f_1(c = 1))
\quad \text{Im}(f_2(s_1 = 0, s_2 = 0) + \text{Im}(f_2(s_1 = 1, s_2 = 1))
\quad \text{Im}(f_2(s_1 = 1, s_2 = 0) + \text{Im}(f_2(s_1 = 0, s_2 = 1))
\end{align*}

Although decoupling effects [17] and higher order attacks [70] 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 time-stamp $t_1$, this constraint in Equation 5 is believed to be satisfied. 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 boolean masking, rules the following:

\begin{align*}
P(c = 0) &= P(c = 1)
\quad P(s_1 = 0, s_2 = 0) + P(s_1 = 1, s_2 = 1) =
\quad P(s_1 = 1, s_2 = 0) + P(s_1 = 0, s_2 = 1)
\end{align*}

As thoroughly investigated in Section 4.1, constrains indicated in Equation 6 could not be held, as the unique physical realizations, corresponding wiring and required routing for $s_1$ and $s_2$ computations yield in frequency-dependant impedance traces. More specifically, one can derive $\exists f_1, f_2 \in F = \{BW\}$, where Equation 6 is not satisfied 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 effectively chal-
lenge 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 exponen-
tially [9, 34] 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 signif-
ificant additive noise to leakage measurement. In other words, al-
though state-of-the-art masking schemes, such as Threshold Imple-
mentation [66] and Domain-Oriented Masking [26], are highly effec-
tive in mitigating time-domain SCA (i.e., DPA on power consump-
tion), they will fail 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 leak-
age 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. Particu-
larly we develop Differential Impedance Analysis (DIMA) to break

\begin{align*}
\forall f_1, f_2 \in F &= \{BW\}:
\quad \text{Im}(f_1(c = 0) = \text{Im}(f_1(c = 1))
\quad \text{Im}(f_2(s_1 = 0, s_2 = 0) + \text{Im}(f_2(s_1 = 1, s_2 = 1))
\quad \text{Im}(f_2(s_1 = 1, s_2 = 0) + \text{Im}(f_2(s_1 = 0, s_2 = 1))
\end{align*}
unprotected cryptographic implementations. Furthermore, a non-profiled Correlation attack is also presented to illustrate conventional leakage models (e.g., Hamming Weight) could also be 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 plain-text scenarios. For TIMA, we also consider known masked shares in our profiling stage. Templating 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 threat model analogous to static power side-channel analysis [19, 49–51] and LLSI attack [42, 43], where instead of performing the measurements during the secret-dependant operations, adversary snapshots at timestamps where secret-dependant data are stored in some form (e.g., in Flip-Flops) on the DUT. Hence, our threat model requires a clock-controlled environment for high-speed targets during the measurement. However, this limitation could be resolved by iterating the measurements without clock halting. (For more discussion please see Section 7.2)

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 attacks aiming unprotected cryptographic implementations. Namely, in the following, we describe impedance-based DPA and CPA.

5.2.1 Differential Impedance Analysis

Differential Power Analysis [39] 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 traces. 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 interacts with (e.g., stores or transfers) the intermediate value. The routine for DIMA is mostly similar to conventional DPA. The adversary could follow the same algorithmic process in DPA [40], but instead of time stamps, on frequency-domain measurements. Specifically, 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.

Algorithm 1 Differential Impedance Analysis

```
function DIMA ATTACK(Tr, in)
    for i ∈ K = \{k_m\} do \(\triangleright\) K is set of possible target values
        for j < |Tr| do \(\triangleright\) H is guess intermediate value
            H ← Int(val(i, inj)) \(\triangleright\) H is guess intermediate value
            if H = 1 then
                One.freq ← Append(Tr[j])
            else
                Zero.freq ← Append(Tr[j])
            end if
        end for
        Diff.freq ← DOM(freq(Zero.freq, One.freq))
    end for
    return ArgSort(Mean(Diff.freq))
```

As indicated in Algorithm 1, the Difference Of Mean (DM) is performed element-wise on each frequency stamp of impedance traces. On the algorithmic level, the index of maximum values of Diff.freq 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 mitigates some drawbacks of DPA [44]. CPA uses a power consumption model on the hardware to establish a correlation between the secret-dependant 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 content’s 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 [11] over frequency-domain impedance values. Hence, target intermediate content leaks on a specific frequency stamp that is indicated by CIMA. Arm with an HW model, we lunch 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 6.3.1), the HW model shows a near-linear leakage trend over impedance’s phase (\(\angle S_{11}\)) on the target frequency time-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 [18].
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. [10], 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 attempt 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 [10]. 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.

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 metric. Moreover, we apply \( \text{LOCTopk} \), a localized Top-K [2] with empirically set smoothing factor \( \alpha \). Note that as collected scattering measurements are complex numbers, TIMA PROFILE could be applied to \(|\mathcal{S}_{11}| \) or |\(\mathcal{S}_{11}\)| or even \( f(|\mathcal{S}_{11}|, \mathcal{S}_{11}) \). As discussed earlier in this article, we mainly focus on \( |\mathcal{S}_{11}| \) profiling since it is more resilient to additive noise compared to |\(\mathcal{S}_{11}\)|. Nevertheless, one could deploy an iterative estimation [67] or optimization [5] procedure to find near-optimal parameters for \( f(|\mathcal{S}_{11}|, \mathcal{S}_{11}) \) leakage profiling kernel to enhance the attack success rate.

In the second phase, the attacker has limited access to the target DUT and captures a small number of measurement traces of impedance \( Trc_{attc}[] \). Consequently, TIMA ATTACK routine is executed. As highlighted, measurements on pre-determined frequency stamps (from the profiling phase) are selected over collected \( Trc_{attc}[] \). Then probability evaluation of a measured trace is computed for each hypothesis based on its profiled Gaussian multi-variant distribution (\( \text{Disk} \)). 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 6.4) 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. Compared to other SCAs, TIMA significantly outperforms any other

### Algorithm 2 Template Impedance Attack

```plaintext
// Template Impedance Attack

function TIMA_PROFILE() for i ∈ K = \{k_{2^m}\} do if \( N_{prof} < j \) then \( Trc_{prof}[i, j] \leftarrow \text{Measure}(\{Z_{f_{r}}, Z_{f_{r}^{1}}, \ldots, Z_{f_{r}^{N}}\}) \) end for

\( AVT_{prof}[i] \leftarrow \text{Mean}(Trc_{prof}[i, j], N_{prof}) \)

end for

\( DM \leftarrow \text{DM}(AVT_{prof}[i], Freq) \)

\( POI[p] \leftarrow \text{LOCTopK}(DM, p) \)

end for

// Template Impedance Attack

function TIMA_ATTACK(Trc_{attc}[], Mean_{prof}[], Cov_{prof}[]) for k ∈ H = \{k_{2^m}\} do \( Mean_{prof}[i, j] \leftarrow \text{Mean}(Trc_{prof}[i, j], POI) \)

\( Cov_{prof}[i] \leftarrow \text{Cov}(Trc_{prof}[i], POI) \)

end for

for j < N_{attc} do

\( STrc_{attc}[j] \leftarrow \text{Select}(Trc_{attc}[i], \text{POIS}) \)

end for

for k ∈ H = \{k_{2^m}\} do

\( Pr[k] \leftarrow \text{PDF}_{\text{equal}}(\text{Disk}, STrc_{attc}[j]) \)

end for

\( Res[k] \leftarrow \text{Acc}(Pr[k]) \)

end for

return \( \text{ArgMax}(Res[i]) \)
```

static and dynamic power consumption attacks and circumvents \( d^{th}\)-order masking schemes.

### 6 EVALUATION

#### 6.1 Experimental Setup

6.1.1 Measurement Equipment. We utilized a Keysight ENA Network Analyzer E5080A [36], which enables RF/microwave scattering measurements and operates on 9KHz - 6 GHz frequency bandwidth. We used Minicircuit CBL-2FT-SMNM+ characterization shielded cables [47] 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) [56], which is equipped with an AMD/Xilinx Artix-7 FPGA [73] (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, 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 [57], which provides serial communication with the DUT and could be used as an intermediate controller to transfer plain text and receive cipher text 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.

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 [14] and Scipy.Stat [15] 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 [76]. 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., the masked AES) as a bitstream is programmed using a JTAG connection.
- (1) Arbitrary input data (i.e., masked plain-text, masked keys, etc.) are prepared in the Analyzer System and are sent to the Controller.

6.2 Attacking Fan-out Registers

We start with a simple profiling analysis of a design with fan-out registers. The same methodology is used by Moradi et al. [51] and similar research scenarios such as [49], 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) [75]. In contrast with static-based power SCA [51], we explicitly specified the location [74] 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 [73].

6.2.1 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 FF 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, $((3 - 2.7)/1000) 	imes 10^9 Hz = 300kHz$ is set as the frequency resolution. Furthermore, the IF bandwidth of VNA for this experiment is set to 500 Hz. To minimize thermal noise, we follow a normalization process where we perform a normalization reference measurement after each measurement (e.g., the case where FPGA_ref_program as reference) 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 $S_{11,θ}$ for each group of traces. Note that $ΔS_{11}$ and $|S_{11}|$ are uniquely different...
metrics with completely different behavior. Consequently, each case in Figure 8a and Figure 9a follow different patterns. For instance, normalized $|S_{11}|$ 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.

Figure 10 shows the results of the aforementioned process for 100 random trials. More specifically, at each trial, POI is calculated as in Equation 7:

$$DM_{trial} = DM(Rnd(\text{Trace}|R = 0b0), Rnd(\text{Trace}|R = 0b1))$$

$$POI_{trial} = \text{ArgMax}(DM_{trial}(S_{11}))$$ (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$\_trial$.

6.2.2 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 11 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:

$$DM_{trial} = \sum_{a,b} (DM(Rnd(\text{Tr}|R = a), Rnd(\text{Tr}|R = b)))$$ (8)

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

6.3 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 [13]). Also, note that S-BOX’s output $Tar = S - BOX(Key,P_{in})$ is considered as the target intermediate value in our attacks, and the goal is to find the first byte of the secret key value.

6.3.1 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.
Figure 12: 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 13: Polar representation of each HW group of the reflected traces.

Furthermore, we select the frequency range of $F = 2\text{GHz} - 3\text{GHz}$, with 3000 linearly spanned stamps. Figure 12 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 13 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.

6.3.2 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 $F = 1\text{GHz} - 2\text{GHz}$, with 3000 frequency samples at each measurement. Figure 14 shows the final differential results for the possible key space using a multi-bit DIMA analysis.

As another analysis, we investigated and measured the leakage of each individual intermediate bit as our indicator. Figure 15 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 on 3000 samples (a) Differential results over the key space (b) Keys with the maximum value of multi-bit differences.

Figure 15: DIMA leakage analysis of different bits of the intermediate value

6.4 Attacking Masked AES

As our ultimate experiment, we prepare an attack on a protected AES implementation. In this scenario, we target a 3-Share AES hardware core. To ensure that random generator execution does not incur additional leakage, we consider an off-chip TRNG, which feeds the masked operands into the FPGA target. We apply TIMA and 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 ($8 \times 3 = 24$ profiles for each byte of the master key). It is also worth noting that shared keys are generated randomly and are used to template all the targets in each trace (out of our $N = 20,000$ data set). 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 16 and Figure 17 show the bit leakage model among bits on different shares and on the same share, respectively. We reiterate that highlighting distinguishable POIs over different frequencies for every individual bit of each share enables TIMA to effectively extract the master key.

After Profiling Stage, we perform a single trace test attack on the DUT with unknown shares. In order to reduce the noise we carried out VNA-enabled averaging index of $AV_{\text{idx}} = 200$ on the same trace. TIMA successfully recovers all the bits of each share individually. Figure 18 serves as an example to showcase how the first byte of the master key could be extracted.
Figure 16: Leakage measurement of Intra-Share bits based on DM.

Figure 17: Leakage measurement of Inter-Share bits based on DM.

Figure 18: Extracting the bit values of all three shares for the first key byte, the first byte of master key can be computed as $K = S_1 + S_2 + S_3 = \text{0xC6} \oplus \text{0x48} \oplus \text{0x65} = \text{0xEB}$

7 DISCUSSIONS

7.1 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 the employment of a real-time refreshing of the secret-dependant registers and/or routing. A series of hardware randomization solutions [27, 38, 46] present methods including partial reconfiguration as Moving Target Defense, to secure FPGA against SCA. Similar methodologies [29], if deployed in an online manner, could be used to prevent impedance analysis.

7.2 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) [19], 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 [42, 49], in many real-world cryptographic masked hardware and software implementations [1, 30], 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 [35], frequency sweep could be done in orders of $\text{ps}$ which gives the adversary the advantage to perform multiple measurements during a single MHz clock execution of DUT.

7.3 Effects of Wiring

Previous researchers have shown that long wires in FPGA implementations could potentially increase the leakage for power side-channel attacks [24, 25]. On the other hand, very close wiring between sensitive operands could also result in coupling effects [17] 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

Although power consumption-based side-channel attacks have been widely studied and well-established methods (e.g., DPA, CPA, etc.) are provided to systematically attack cryptographic implementations, they mostly rely on leakage of dynamic power consumption of secret-dependant operations which are significantly reduced by masking methods and they often require a large number of measurement traces. This paper presents the very first side-channel attacks based on IC back-scattering characterization and establishes a methodology to acquire a data-dependent model based on IC’s impedance measurements. We show that impedance leakage of hardware circuits not only is data-dependent and exploitable but
also spanned through the frequency domain where state-of-the-art masking schemes are ineffective. The method proposed in this article challenges the t-probe security model by mounting a fully non-invasive profiling attack.

In spite of the sophisticated measurement setup and analysis used in this article, we believe that the current work highlights a new physical side-channel leakage that could effectively be exploited by various methods.

REFERENCES


[64] Nele Mentens. 2017. Hiding side-channel leakage through hardware randomiza-
tion: A comprehensive overview. In 2017 International Conference on Embedded 
272.
[66] Thorben Moos. 2019. Static Power SCA of Sub-100 nm CMOS ASICs and the 
insecurity of masking schemes in low-noise environments. IACR Trans. Cryptog 
[67] Thorben Moos. 2019. Static Power SCA of Sub-100 nm CMOS ASICs and the In-
security of Masking Schemes in Low-Noise Environments. IACR Trans. Cryptogr 
[68] Thorben Moos. 2019. Static Power SCA of Sub-100 nm CMOS ASICs and the In-
security of Masking Schemes in Low-Noise Environments. IACR Trans. Cryptogr 
[69] Thorben Moos. 2019. Static Power SCA of Sub-100 nm CMOS ASICs and the In-
security of Masking Schemes in Low-Noise Environments. IACR Trans. Cryptogr 
[70] Thorben Moos, Amir Moradi, and Bastian Richter. 2019. Static power side-channel 
analysis—An investigation of measurement factors. IACR Transactions on Very 
[71] 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 Spring, 562–579.
ScatterVerif: Verification of Electronic Boards Using Reflection Response of Power 
Distribution Network. ACM Journal on Emerging Technologies in Computing 
[73] Tahoura Mosavirik, Saleh Khalaj Monfared, Maryam Saadat Safa, and Shahin 
[74] Tahoura Mosavirik, Tahoura Mosavirik, Saleh Khalaj Monfared, Maryam Saadat 
actions on Cryptographic Hardware and Embedded Systems 1 (2023), 301–325.
[78] Luong N Nguyen, Chia-Lin Cheng, Mâlos Pruvolvic, and Alenka Zajić. 2019. Cre-
ating a Backscattering Side Channel to Enable Detection of Dormant Hardware 
Trojans. IEEE transactions on very large scale integration (VLSI) systems 27, 7 
[79] Luong N Nguyen, Baki Berkay Yilmaz, Mâlos Pruvolvic, and Alenka Zajić. 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.
[80] Elisabeth Oswald and Stefan Mangard. 2006. Template attacks on mask-
ing—resistance is futile. In Topics in Cryptology–CT-RSA 2007: The Cryptographers’ 
[81] Bile Peng, Sebastian Rey, and Thomas Künzer. 2016. Channel characteristics 
study for future indoor millimeter and submillimeter wireless communications. In 
[83] 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.
Press.
[85] 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.
[86] Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, and Ingrid Ver-
CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 
[88] Larry D. Smith, Shishuang Sun, Mayra Sarmiento, Li Zhe, and Karthik Chan-
drasekhar. 2011. On-Die Capacitance Measurements in the Frequency and Time 
Domains. DesignCon. Santa Clara, CA (2011)
[89] Robert Specht, Vincent Immel, Florian Unterstein, Johann Heyssel, and Georg Sig. 
2018. Dividing the threshold: Multi-probe localized EM analysis on threshold 
implementations. In 2018 IEEE International Symposium on Hardware Oriented 
[90] F-X Standaert, Eric Peeters, and J-J Quisquater. 2005. On the masking counter-
measure and higher-order power analysis attacks. In International Conference on 
Information Technology: Coding and Computing (ITC’05)-Volume II, Vol. 1, IEEE, 
562–567.
[91] HL van Trees. KL Bell, and Z Tian. 2013. Detection estimation and modulation 
theory, part I. Detection, estimation, and filtering theory. A Papoulis Probability 
[92] Lichao Wu, Guilherme Perin, and Stejpan Pickel. 2022. The best of two worlds: 
Deep learning-assisted template attack. IACR Transactions on Cryptographic 
[97] Xiaofeng Yin and Xiang Cheng. 2016. Propagation channel characterization, pa-
parameter estimation, and modeling for wireless communications. John Wiley & 
Sons.
[98] Huifeng Zhu, Haoqi Shan, Dean Sullivan, Xiaolong Guo, Yier Jin, and Xuan 
Zhang. 2022. PDPulse: Sensing PCB Anomaly with the Intrinsic Power Delivery 