Impedance vs. Power Side-channel Vulnerabilities: A Comparative Study

Md Sadik Awal, Buddhipriya Gayanath, and Md Tauhidur Rahman
Security, Reliability, Low-power, and Privacy (SeRLoP) Research Lab
ECE Department, Florida International University, Miami, Florida, USA
E-mail: {mawal003, bgaya003 and mdtrahma}@fiu.edu

***Abstract*—In recent times, impedance side-channel analysis has emerged as a potent strategy for adversaries seeking to extract sensitive information from computing systems. It leverages variations in the intrinsic impedance of a chip's internal structure across different logic states. In this study, we conduct a comparative analysis between the newly explored impedance side channel and the well-established power side channel. Through experimental evaluation, we investigate the efficacy of these two side channels in extracting the cryptographic key from the Advanced Encryption Standard (AES) and analyze their performance. Our results indicate that impedance analysis demonstrates a higher potential for cryptographic key extraction compared to power side-channel analysis. Moreover, we identify scenarios where power side-channel analysis does not yield satisfactory results, whereas impedance analysis proves to be more robust and effective. This work not only underscores the significance of impedance side-channel analysis in enhancing cryptographic security but also emphasizes the necessity for a deeper understanding of its mechanisms and implications.**

***Index Terms*—Impedance side-channel, side-channel analysis, impedance leakage, key extractions, side-channel attack**

I. Introduction

In cybersecurity, side-channel attacks have long been recognized as potent threats, exploiting unintended information leakage to compromise the security of cryptographic systems and electronic devices. Traditional side channels, such as power, electromagnetic (EM) emissions, and timing variations, have received significant attention in academia and industry due to their ability to leak sensitive information from cryptographic devices and systems [1], [2], [2]–[6]. For instance, power side-channel attacks leverage fluctuations in the power consumption of cryptographic devices across different operations, such as encryption and decryption processes. Similarly, EM emissions arise from the electrical operations within cryptographic devices, leading to unintentional radiations that attackers can intercept and analyze [4], [5]. Usually, the vulnerabilities in the hardware implementation or the physical characteristics of the encryption systems facilitate these unintended physical side channels, which are then exploited to extract confidential information from cryptographically secure algorithms [1], [2], [2]–[6].

Recently, impedance analysis has found applications across various domains, including radio frequency (RF) related fields [7], counterfeit chip detection [8] and tempering detection [9]. It has also been discovered that impedance can inadvertently leak sensitive information related to the computations and data being processed within a system. Our research demonstrates the potential of the runtime impedance of a device as a side-channel, unveiling software instructions through distinct impedance profiles generated by each operation [10], [11]. Subsequent studies have exploited impedance as a side channel to extract the AES key from the register of an FPGA [12]. These approaches to leveraging impedance marks a significant shift in the perception of impedance within the cybersecurity domain. Impedance analysis, while it remains an important tool for enhancing hardware security, it also presents a novel vulnerability that adversaries can exploit to their advantage.

Although studies demonstrate the extraction of the cryptographic key, such as the AES key, using power and impedance side channels, there remains a gap in the literature regarding the comparative evaluation of these two side channels. This study endeavors to bridge this gap by providing a detailed comparative analysis of the performances of impedance and power side channels in the extraction of the AES key. The primary contributions of this paper are,

- Exploring the source of impedance side-channel leakage and the extraction of AES keys using it. This includes scenarios with and without countermeasures.
- Performing a comparative analysis of the performances of impedance and power side channels.

The structure of this paper is organized as follows: Section II discusses the background of power and impedance side channels, including a discussion on correlation analysis and the existing research on the extraction of encryption keys using physical side channels. Section III presents the proposed method to compare the power and impedance side channels. Section IV details the experimental setup. We present and compare the findings of AES key extraction using power and impedance side channels in Section V. Section VI concludes the work.

II. Background and Related Work

This section covers the basics of the cryptographic algorithm targeted in this study, explores power and impedance side channels, and outlines the attack methodology used. Furthermore, it reviews recent literature on existing power and impedance side channel-based work.

A. Advanced Encryption Standard

This study focuses on the advanced encryption standard (AES), a commonly used symmetric block cipher algorithm that encrypts and decrypts data using the same key. Figure. 1 presents the overview of AES encryption steps for r rounds. Each round involves a key-dependent substitution step using the Rijndael S-BOX [13], [14], a step that shifts rows, a step that mixes columns, and a step that adds a round key [15]. The Rijndael S-BOX is a lookup table and is critical for the security of the algorithm. It changes an 8-bit input to an 8-bit output, making the encryption stronger by ensuring that a small change in the input significantly affects the output. This study considers the AES-128 algorithm to compare how well impedance and power side channels can be used to analyze it.

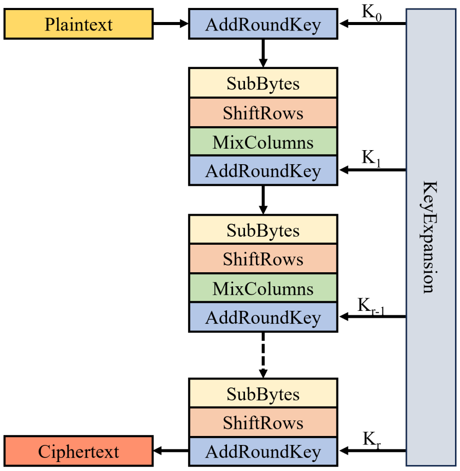


Fig. 1: Overview of AES Encryption.

B. Power Side Channel

The power side channel focuses on the power consumption of the target devices and is a well-studied area [1]. It originates from the fact that, in digital circuits, the execution of operations depends on the switching activities of the transistors. These switching activities lead to voltage and current fluctuations across digital components, resulting in power consumption variations. These fluctuations can be captured by measuring the voltage changes across the power supply pins of the target component using an oscilloscope. The resultant measurements can be subsequently used in further analysis and processing to extract information related to the operation being executed. This poses a security and privacy issue as it can be exploited to obtain sensitive credentials.

This work focuses on using power side channels to extract the AES key. We explore a scenario within an embedded system that requires the implementation of AES. We study the internal memory modules to be read and written with the intermediate values of the computations performed in the encryption process. The dynamic power consumption of these memory modules, corresponding to read and write operations, is intrinsically linked to the changes in the logic states of the transistors. During the write operation, we focus on the state transitions of the transistors, either transitioning from ON to OFF or vice versa. By measuring and analyzing these power consumption patterns, we aim to recover the AES encryption key.

C. Impedance Side Channel

In contrast to the power side channel, the impedance side channel utilizes changes in the intrinsic impedance variation of the system based on different logic states. The logic state of the device represents various transistor configurations, resulting in impedance variations [10], [16]. The impedance variation due to stored binary values in memory cells exhibits distinct differences. This variation is evident when writing specific data to the memory across different clock cycles, where the number of transistors in the ON and OFF states varies and remains constant until the next clock signal. By exploiting this phenomenon, our focus shifts to the impedance variations resulting from the storage of intermediate values of AES encryption in the memory chip. We explore the use of impedance measurements to extract the encryption key, leveraging these variations.

To measure the impedance, we use a Vector Network Analyzer (VNA). VNA is widely used to characterize multi-port networks. The VNA operates by injecting a known test signal and analyzing the reflected and transmitted signals from the device under test (DUT). This process allows the VNA to calculate the DUT's scattering parameters, commonly referred to as S-parameters, which are widely used in the fields of radio frequency (RF) and microwave systems. A key focus of our analysis is the input port reflection coefficient, S_{11}, from which we derive the supply side impedance of the DUT, Z_i, using 1. Here, Z_{ref} represents the reference impedance.

$$Z_i = \frac{1 + S_{11}}{1 - S_{11}} \times Z_{ref} \tag{1}$$

D. Correlation Analysis

Recent works use different types of analytical methods to signals in physical side channels. One popular analysis method is correlation-based analysis. This analysis is considered powerful in unmasking the relationships of the secret information hiding inside the noisy measurements using the Pearson correlation coefficient as a statistical test [17]. Furthermore, instead of focusing on only a single measurement point, it adopts a multivariate approach by analyzing multiple points within the measurement trace [1].

$$\rho(x_s, h_k) = \frac{M \sum_{m=1}^{M} x_{s,m} h_{k,m} - \sum_{m=1}^{M} x_{s,m} \sum_{m=1}^{M} h_{k,m}}{\sqrt{D_x D_h}} \tag{2}$$

$$D_x = M \sum_{m=1}^{M} x_{s,m}^2 - (\sum_{m=1}^{M} x_{s,m})^2$$

$$D_h = M \sum_{m=1}^{M} h_{k,m}^2 - (\sum_{m=1}^{M} h_{k,m})^2$$

In cryptography, correlation-based analysis starts with the collection of leakage responses generated by known plaintext operations. Each measurement is synchronized with the cryptographic encryption operation performed in the device over the plaintext. The next step involves selecting a leakage model that represents hypothesized side-channel leakages. This leakage model is then correlated with the actual observed leakage to find the leaked information. To facilitate this analysis, let M represent the total number of measurements, S the total number of sampling points per measurement, $x_{s,m}$ the actual leakage at the s'th sample point of the m'th measurement, and $h_{k,m}$ the hypothesized leakage for a guessed key k at the m'th measurement. The relationship between the actual and hypothesized leakages is quantified by the Pearson correlation coefficient $\rho(x_s, h_k)$, calculated as presented in 2.

The correct key from the leakage is identified by finding the guessed key for which the maximum absolute correlation occurs within the full sampling point S. We use this correlation-based analysis method for both the power and impedance side channels to extract the cryptographic key.

E. Related Work

Power side-channel analysis on both the hardware and software implementations of cryptographic algorithms has been extensively researched over the past few decades. Authors in [18] present one of the earliest power side-channel attacks to extract the AES key from smart cards. In [19], the authors discuss a detailed explanation of step-wise differential power analysis (DPA) attacks over AES implementation. In [20], three attack scenarios are presented: single-bit DPA, multi-bit DPA, and a correlation analysis. The authors implement AES in two platforms. The study concludes by proposing an enhanced DPA approach that strategically organizes plaintext inputs to maximize the leakage. Additionally, [21], [22] present AES key extraction attacks using power analysis on the ATmega328P microcontroller. Further, [23] presents a power analysis attack specifically targeted against ASIC implementations of the AES. The authors in [24], [25] present their findings on power side-channel attacks targeting the advanced modes of AES.

Impedance is a recent addition to the field of side-channel analysis [10], [11], [16], [26], [26], [27]. Before its application to cryptographic key recovery, numerous studies focused on using impedance for hardware security. Authors in [28] introduce a detection technique using board level impedance to detect physical modifications of the board. The study in [26] explores a method for non-destructively detecting hardware Trojans through internal impedance variations. The authors in [29], study a clustering method to classify ICs into Trojan-free and Trojan-infected groups. In addition to the usage of impedance in physical modification detection, it is recently attracting the focus of device switching activities. Authors in [16] use impedance measurements to disassemble software instruction types for anomaly monitoring and software integrity verification. The study of impedance changes induced by the switching activities is used to detect and identify the firmware in [11]. The authors in [30] use the impedance of digital circuits to introduce a novel RFID tag design. These works present the run-time impedance variations of the devices as the side-channel.

III. Power vs Impedance: Key Extraction

This section discusses the attack methodology performed against the AES implementation utilizing power and impedance side channels. We present the threat model, the leakage model used in the attack, and the metrics to evaluate the power and impedance side channels.

A. Source of Impedance Side-channel

Impedance side-channel analysis introduces a novel approach to probing the intricate and often overlooked behaviors of electronic circuits, particularly in memory chips. This investigative technique methodically explores memory operations, revealing how variations in electrical impedance could potentially disclose information about the data being processed and stored. At the core of this analysis lies the understanding that various physical and architectural factors within a circuit influence its overall impedance characteristics [16], [26]. These factors include parasitic elements inherent to physical implementations, interconnection structures, transistor property variations across the silicon substrate, and the distinct semiconductor material properties of the transistor configurations.

Within memory chips, such as Static Random Access Memory (SRAM) and Dynamic Random Access Memory (DRAM), the control circuit manages memory access and data read/write operations. The memory array, organized in rows and columns, stores data at specific address locations. Three primary components define the impedance profile of memory: the architecture and layout of the memory array, the cell type, and the related data and control logic circuitry. Manufacturers tailor the arrangement of memory cells in rows and columns, as well as the cell type (e.g., four-transistor (4T) or six-transistor (6T) cell structures in SRAM), based on factors such as performance requirements, power consumption, and area constraints, thereby influencing the impedance characteristics.

However, in accordance with our study, we focus on the impedance changes corresponding to the memory content. The process of writing data to or reading from memory cells initiates a series of events that create unique impedance profiles for the stored bit sequences within the memory array. Specifically, the activation of transistors, fabrication process variations, and the specific data retention logic employed contribute to these distinctive impedance profiles. Furthermore, the impedance profiles are influenced by factors such as the data stored inside the memory cells, the different locations of the cells in terms of rows and columns within the array, and the varying lengths of connections for each cell. Thus, the impedance measurements should reflect these variations and can be vulnerable to data leakage.

B. Attack against AES

In this subsection, we describe the target intermediate of AES encryption, as well as the hypothetical leakage model.

1) Target Intermediate: The key extraction of the AES encryption using physical side-channel analysis usually targets the first or final round of the algorithm. The targeted round is used to model the leakage signal. In our work, we target the first round of the AES algorithm. The AES encryption begins with performing the bitwise XOR operation on the plaintext and the secret key, and the resulting product is used in the substitution step. The output value of the substitution step is stored in memory, and it is our targeted computational intermediate value. The steps of AES encryption are illustrated in 1.

We use the plaintext in our hypothetical leakage model. With the known plaintext p_i, and the corresponding round subkey k_j, the targeted computational intermediate m_i can be represented as in 3. This intermediate value depends on both the input plaintext and the secret cryptographic key. Thus, the corresponding side-channel leakages are correlated with the secret key information. The attackers can exploit the statistical properties of the leakage traces to extract the cryptographic key.

$$m_i = SBOX(p_i \oplus k_j) \tag{3}$$

2) Leakage Model: We perform correlation analysis-based attacks against the AES implementation using both power and impedance side channels and evaluate their results. We use the hamming weight (HW) leakage model [31]–[33]. The HW refers to the total number of set bits (number of '1's) in the data. This HW leakage model is predicated on the assumption that the power consumed by the cryptographic device—or the impedance variations [31], [33] observed—is directly correlated with the HW of the processed data. As the hamming weight increases, more transistors switch, leading to higher leakage.

The HW leakage model considers the HW of the targeted intermediate value as the leakage source. It assumes a linear relationship between the HW and the observed leakage. Let L be the observed leakage, $HW(m)$ be the hamming weight of the targeted intermediate m, a and b be the constant coefficients, and n be the noise in the leakage measurement. The observed leakage, L, can be expressed as in 4. The fundamental assumption here is that variations in the physical properties observed through side channels during cryptographic operations can reveal information about the internal data being processed.

$$L = a \times HW(m_i) + b + n \tag{4}$$

The effectiveness of the HW model in side-channel attacks lies in its ability to exploit the statistical correlation between the measured leakages and the HW of the secret data being processed. We can make informed guesses about the secret key by analyzing these correlations.

C. Threat Model

During the experiment, we write the intermediate values to the memory. It is assumed that the attacker possesses physical access to the system and can control the input plaintexts to the system. The assumptions for the experiment are as follows.

- In the power side channel case, the attacker can access the PDN of the memory module and measure the power signals when the data is written to the memory using an oscilloscope.
- In the impedance side channel case, the attacker can connect a VNA to the PDN of the memory module and measure the impedance after each intermediate value corresponding to each plaintext is written to the memory.

D. Evaluation Metric

To compare the performance of the power and impedance side channels, we use three comprehensive metrics. These metrics assist in the systematic analysis of the effectiveness of both power and impedance side channels in recovering the AES key.

In the evaluation of the two targeted side channels, we use correlation ratio (CR) 5 as a confidence metric for correct key recovery. It is calculated as the ratio between the correlation coefficient for the correct key and the highest correlation coefficient observed for the wrong keys. It can assess the confidence of the correct key guess with respect to other wrong key guesses. A higher ratio indicates a strong level of confidence in precisely guessing the correct value for the key. Let k_c and k_w denote the correct subkey and the wrong guessed subkey, respectively, from K key space. We use 2 to develop 5 and compute the CR as of the confidence score of each subkey.

$$CR = \frac{\max_{m \in M}(\rho(x_m, k_c))}{\max_{m \in M}(\rho(x_m, k_w)) \text{ for } k_w \in K} \tag{5}$$

As for the second metric, we use the minimum traces to key disclosure (MTD) metric to evaluate which side channel will result in early identification of the correct key with respect to the minimum number of traces. The significance of MTD lies in its ability to quantify the data complexity of side-channel attacks, assessing the practical feasibility and security implications of such attacks. A lower MTD value indicates more efficient and effective side-channel attacks, as it requires fewer traces to extract the secret information. On the other hand, a higher MTD value suggests a less efficient side channel, requiring more traces to extract the subkey and, consequently, may be less practical in real-world scenarios. Thus, MTD can be used to compare the efficacy of the power and impedance side-channel attacks.

In the evaluation for assessing the effectiveness of side-channel attacks, we utilize the interquartile range (IQR) as our third metric. The IQR serves as a robust measure for outlier detection within datasets, which is essential for ensuring the integrity of the data under analysis. The IQR, as defined in 6, calculates the difference between the 75th percentile (Q3) and the 25th percentile (Q1) of the observed data points. This calculation focuses on the variability within the central 50% of the data and renders the IQR a pivotal tool in identifying significant deviations in the correlation coefficients calculated using the hypothetical keys to find the correct key.

The outliers of the correlation coefficient distribution formed by all guessed keys represent the potential correct key candidates. Let x be the calculated correlation coefficient using 2 due to the guessed subkey K_x. By establishing lower and upper bounds for outlier detection, a correlation coefficient x outside these thresholds is flagged as an outlier, as presented in 7. These outliers represent the potential correct subkey candidates that do not follow the distribution of the wrong subkeys. The incorporation of the IQR metric enhances the evaluation process by facilitating the identification of the correct subkey candidate. This, in turn, allows for a more accurate assessment of side-channel vulnerabilities.

$$\text{IQR} = Q3 - Q1 \tag{6}$$

$$\text{Outliers} = \begin{cases} x < Q1 - 1.5 \times \text{IQR} \\ x > Q3 + 1.5 \times \text{IQR} \end{cases} \tag{7}$$

IV. Experimental Setup

In this section, we describe the hardware setup and data collection steps for each power and impedance side channel.

A. Hardware Setup

The hardware setup is illustrated in Figure 2. We use an oscilloscope and a vector network analyzer (VNA) to measure the power and impedance signals, respectively. For power measurements, we employ the SIGLENT SDS5104X oscilloscope with a 5 Giga sample per second rate, enabling us to collect 2501 voltage sample points for each measurement. We utilize the Rigol RSA5032N spectrum analyzer for impedance measurements in VNA mode. We select a frequency range from 100 kHz to 3.2 GHz, allowing us to measure impedance at 10,001 linearly distributed frequency points.

Regarding the memory component, we use the FM18W08 FRAM (Ferroelectric Random Access Memory) [34] from Infineon Technologies in this experiment. The FM18W08 is a $32K \times 8$ nonvolatile memory capable of read and write operations like a standard SRAM. It consists of 32,768 memory locations, each with 8 data bits, which can be accessed through a parallel interface. The FRAM array is structured into 4092 rows, each comprising 8 bytes, with addresses of a 15-bit length. We use the Alchitry Au with an Artix 7 FPGA [35] to develop the memory controller to control the FRAM read and write operations. The Alchitry Au operates with a clock frequency of 100 MHz.

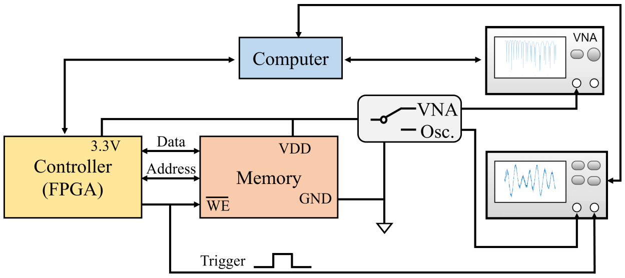


Fig. 2: Experimental setup diagram.

Power Side-Channel Attack: During the measurement, we connect a probe of the oscilloscope to the 3.3V PDN of the memory chip. We use different plaintext to perform AES encryption and record the voltage fluctuations. We achieve synchronization of our measurements through the write-enable signal of the memory chip. We use an 8-bit plaintext and an 8-bit AES subkey in each experiment to compute an intermediate value. We record the voltage fluctuations at the time of writing the intermediate value of the first round of AES to the memory. This enables us to collect the necessary traces to extract all 16 subkeys of the 128-bit AES encryption.

Impedance Side-Channel Attack: For the impedance side-channel analysis, we connect the VNA to the 3.3V PDN of the memory chip via a coaxial cable. Unlike in the power side-channel analysis, we collect impedance measurements after the intermediate values have been written to the memory. The VNA measures the reflection coefficient parameters (S_{11}), which we convert to impedance values using 1. Although impedance includes both phase and magnitude, we focus solely on the magnitude in our analysis as it carries the most information [9].

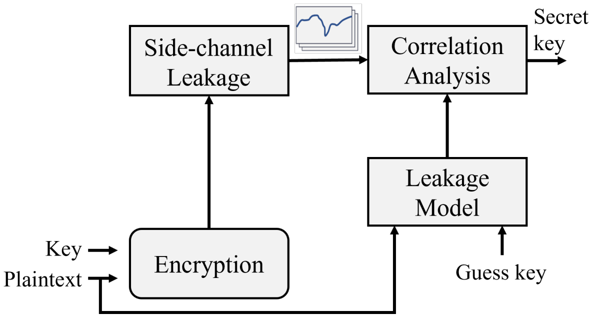


Fig. 3: AES key extraction method.

B. Data Collection and Analysis

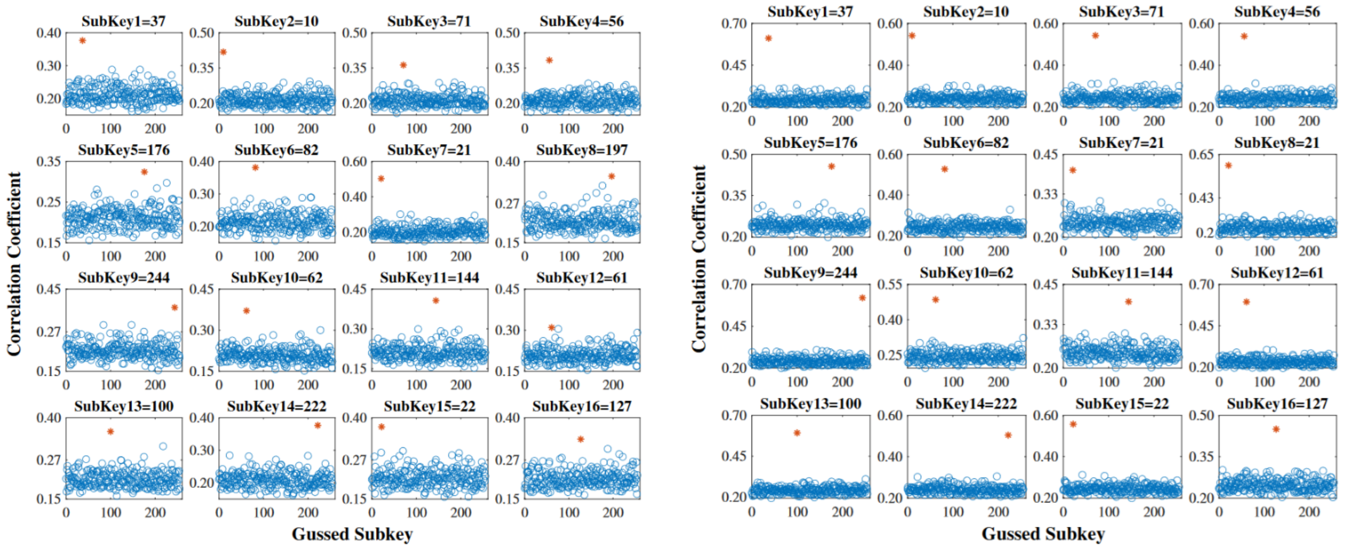
For power side-channel measurements, we automate the data collection process by utilizing the write-enable signal of the memory as a trigger. This trigger signal initiates the oscilloscope measurement. We develop a custom Python script incorporating Standard Commands for Programmable Instruments (SCPI) commands to transfer the measured traces to a computer. To mitigate noise, we take each measurement trace as an average of 128 measurements. We use these averaged traces for the power side-channel analysis.

During the impedance side-channel measurements, a similar automated setup is implemented. Python scripts with SCPI commands facilitate the transfer of measured traces from the VNA to the computer. Similar to the power side-channel measurements, we take the average of 100 measurements as each measurement trace to reduce noise.

We perform correlation analysis with the collected measurement traces by comparing the actual leakages with hypothetical leakages. Figure 3 illustrates the analysis steps. We recover the correct key as the key value corresponding to the maximum correlation coefficient observed during the analysis.

V. Results and Analysis: Power vs. Impedance

We use the AES-128 encryption and follow the evaluation metrics described in Section III-D to conduct a comprehensive comparison of the performance of power and impedance side



(a) Power side-channel

(b) Impedance side-channel

Fig. 4: Results of 8-bit subkey extraction for 128-bit AES.

channels. Additionally, in a subsequent scenario, we evaluate the resilience of these side channels in a noise-injected environment. In every scenario, we target the first round of the AES encryption process. We adopt a divide-and-conquer approach by dividing the full 128-bit AES key into 16 subkeys and focus our efforts on recovering each subkey individually.

A. Baseline Side-channel Analysis

To initiate our analysis, we perform the correlation analysis described in Section II-D for all possible 8-bit guessed subkeys and plot the findings in Figure 4. Since we use the 128-bit AES encryption, our analysis involves 16 subkeys. Maximum correlation values in Figure 4 are represented by asterisk ($*$) for visual clarity. Figure 4a represents the results obtained from the power side-channel analysis, while Figure 4b depicts the results of the impedance side-channel analysis. The results demonstrate the vulnerability of the 128-bit AES implementation to both the power and impedance side-channel attacks.

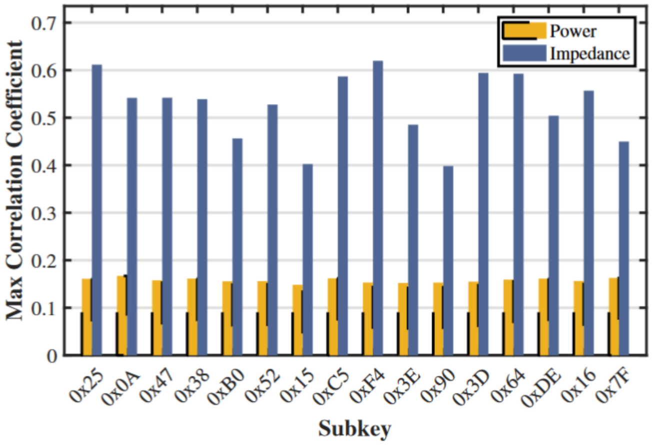


Fig. 5: Maximum correlation coefficient without noise.

Subkey	0x25	0x0A	0x47	0x38	0xB0	0x52	0x15	0x15
Power	0.37	0.41	0.36	0.38	0.32	0.38	0.50	0.35
Impedance	0.61	0.54	0.54	0.53	0.45	0.52	0.40	0.58
Subkey	**0xF4**	**0x3E**	**0x90**	**0x3D**	**0x64**	**0xDE**	**0x16**	**0x7F**
Power	0.34	0.37	0.40	0.30	0.35	0.37	0.37	0.33
Impedance	0.61	0.48	0.39	0.59	0.59	0.50	0.55	0.44

TABLE I: Maximum correlation coefficients observed.

Table I provides a summary of the maximum correlation coefficient observed in both side channels for each individual subkey. Additionally, we compare the maximum correlation coefficient values obtained in Figure 4 for each subkey. Figure 5 presents a visual representation of Table I. The findings show that the maximum correlation values obtained through impedance side channels are consistently higher than those of the power side channels. This suggests a potential superiority of the impedance side channel in information leakage over the power side channel.

Correlation Ratio: We proceed to compare and analyze the results obtained from the two side channels using the metrics discussed in Section III-D. First, to assess the discriminability level of the recovered correct key concerning other key candidates, we calculate the correlation ratio for each subkey using 5. The resulting graph is presented in Figure 6. The findings further suggest that the correct subkeys can be identified with a higher discriminability level most of the time when using the impedance side channel compared to the power side channel.

MTD: As the second evaluation metric, we use the MTD in recovering the 128-bit AES key. The MTD represents the min-

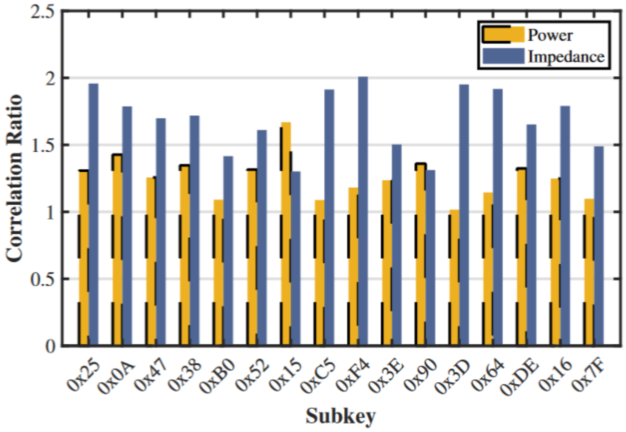


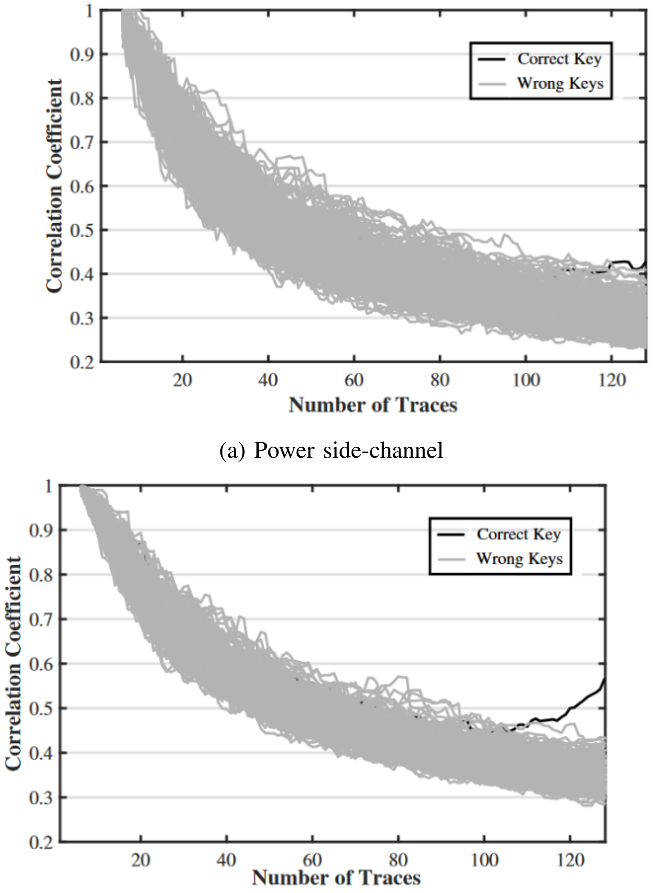
Fig. 6: Correlation ratio without noise.

imum number of side-channel traces required to successfully recover the secret key or a part of it, such as a subkey. When comparing the performance of the two side channels for AES-128 subkey extraction, the MTD metric aids in determining which side channel is more effective. The side channel with a lower MTD value is considered more potent, as it can recover the subkey using fewer traces, posing a higher security threat to the cryptographic system.

Our observations indicate that the MTD performs better in the impedance side-channel than the power side-channel. We present the MTD for subkey-1 in Figure 7 for only 128 traces. We find that with this limited number of traces, the correlation coefficient of the correct key is distinctly identified from the wrong key guesses using the impedance side-channel. In contrast, in the case of the power side-channel, the correlation coefficient of the correct key falls within the range of correlation coefficients of the wrong key guesses. We observe similar findings for other subkeys as well. The results suggest that the correct key can be recovered with fewer measurements using the impedance side channel compared to the power side channel.

IQR: To better understand the results and quantify the confidence in the recovered keys, we employ the IQR method on the highest five correlation coefficients obtained from Figure 4. This approach helps us identify the guessed key for which the corresponding correlation coefficient is an outlier. Such an outlier indicates that the correlation coefficient can be statistically distinguished due to that guessed key, making it a potential correct subkey candidate. In scenarios where we find multiple outliers, all of them are considered potential correct subkey candidates. However, the absence of outliers implies that we cannot reliably identify the correct key based on the correlation coefficient values, indicating poor performance.

Table II presents the correlation coefficients that lie outside the first and third quartile range. The entry ‘F’ in the table signifies a failure to distinguish the correct subkey from the wrong ones. The findings suggest that the impedance side channel provides more distinct outliers compared to the power side channel, further corroborating the superiority of the impedance side channel in extracting the correct subkeys.



(a) Power side-channel

(b) Impedance side-channel

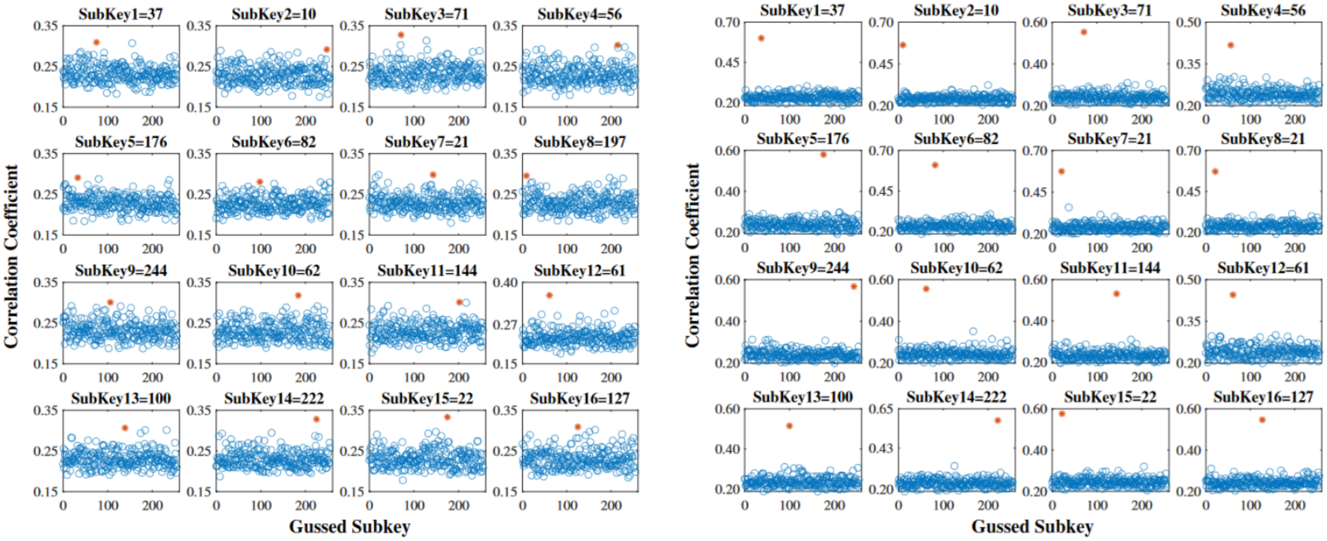
Fig. 7: Subkey-1 recovery with 128 traces.

Subkey	**0x25**	**0x0A**	**0x47**	**0x38**	**0xB0**	**0x52**	**0x15**	**0x15**
Power	1	1	1	1	F	1	1	F
Impedance	1	1	1	1	1	1	1	1
Subkey	**0xF4**	**0x3E**	**0x90**	**0x3D**	**0x64**	**0xDE**	**0x16**	**0x7F**
Power	F	F	1	F	F	1	1	F
Impedance	1	1	1	1	1	1	1	1

TABLE II: Number of outliers using the highest five correlation coefficients.

B. *Noise-Injected Side-channel Analysis*

In the second phase of the experiment, we introduce noise into the measurement traces by executing background activities in the memory controller while collecting power and impedance measurements. To implement these background activities, we use ten 5-bit linear feedback shift registers (LFSRs). Each of these LFSRs is designed to shift bits to the left. Each LFSR operates by shifting bits to the left and uses XOR logic to generate an input bit at each clock cycle. In our implementation, we tap the fourth and fifth bits of the LFSR to generate the new input bit. The use of LFSRs ensures



(a) Power side-channel

(b) Impedance side-channel

Fig. 8: Results of 8-bit subkey extraction for 128-bit AES with noise.

the generation of a sequence of bits that appears random. Moreover, the parallel use of ten such left-shift LFSRs allows us to generate the background activities efficiently.

Following the LFSR implementation, we collect the same number of traces as previously for each power and impedance side channel setup and repeat the correlation analysis for AES-128 key extraction. Figure 8 presents the subkey extraction results of each side channel with the LFSR implemented in the background. As illustrated, the performance of the power side channel in extracting the subkeys degrades significantly in the presence of noise. However, even under noisy conditions, the impedance side channel can successfully extract all the 8-bit subkeys of AES-128.

Considering the results of the second attack scenario after introducing additional noise to the measurements, we find that the impedance side channel can still recover all the subkeys correctly, in contrast to the power measurements. These background activities result in power consumption variations due to increased internal switching activities.

C. Summary of Results

In synthesizing the findings from this comparative analysis, several key insights emerge regarding the efficacy and implications of impedance and power side-channel attacks in cryptographic systems.

- Impedance side-channel analysis demonstrates superior efficacy in key extraction, both in the presence and absence of noise, suggesting its potential as a significant security and privacy threat surpassing that of power leakage.
- Some countermeasures effective against power side-channel attacks may not offer the same level of protection against impedance side-channel attacks. However, we need further example cases and analysis to generalize such a statement.

VI. Conclusion

This study provides a comprehensive comparative analysis between impedance and power side-channel analysis techniques, focusing specifically on their efficacy in extracting cryptographic keys. Contrary to the common perception that views impedance side-channel analysis merely as an alternative to power analysis, our findings reveal that impedance analysis holds superior potential in decrypting AES keys where power analysis proves inadequate.

The findings demonstrate the robustness and effectiveness of impedance analysis, challenging its often-overlooked significance. Additionally, the results of this study serve as a compelling motivation for further exploration into the underlying mechanisms of impedance analysis and their implications for hardware security. Furthermore, our findings underscore the need to incorporate impedance side-channel analysis into the standard evaluation protocols for cryptographic systems. By doing so, we can ensure a more comprehensive and robust assessment of potential vulnerabilities, thereby enhancing the overall security posture.

References

[1] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[2] S. M. Del Pozo, F.-X. Standaert, D. Kamel, and A. Moradi, "Side-channel attacks from static power: When should we care?" in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2015, pp. 145–150.

[3] N. Gattu, M. N. I. Khan, A. De, and S. Ghosh, "Power side channel attack analysis and detection," in *Proceedings of the 39th International Conference on Computer-Aided Design*, 2020, pp. 1–7.

[4] D. Das, M. Nath, S. Ghosh, and S. Sen, "Killing em side-channel leakage at its source," in *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2020, pp. 1108–1111.

[5] N. Sehatbakhsh, B. B. Yilmaz, A. Zajic, and M. Prvulovic, "Emsim: A microarchitecture-level simulation tool for modeling electromagnetic side-channel signals," in *2020 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 2020, pp. 71–85.

[6] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4*. Springer, 2003, pp. 29–45.

[7] Z. Hameed and K. Moez, "Design of impedance matching circuits for rf energy harvesting systems," *Microelectronics Journal*, vol. 62, pp. 49–56, 2017.

[8] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *Journal of Electronic Testing*, vol. 30, pp. 9–23, 2014.

[9] M. S. Awal, A. Madanayake, and M. T. Rahman, "Nearfield rf sensing for feature-detection and algorithmic classification of tamper attacks," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 490–499, 2022.

[10] M. S. Awal and M. T. Rahman, "Impedance leakage vulnerability and its utilization in reverse-engineering embedded software," 2023.

[11] M. S. Awal, C. Thompson, and M. T. Rahman, "Utilization of impedance disparity incurred from switching activities to monitor and characterize firmware activities," in *2022 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. IEEE, 2022, pp. 1–7.

[12] S. K. Monfared, T. Mosavirik, and S. Tajik, "Leakyohm: Secret bits extraction using impedance analysis," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 1675–1689.

[13] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact rijndael hardware architecture with s-box optimization," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2001, pp. 239–254.

[14] A. Barrera, C.-W. Cheng, and S. Kumar, "A fast implementation of the rijndael substitution box for cryptographic aes," in *2020 3rd International Conference on Data Intelligence and Security (ICDIS)*. IEEE, 2020, pp. 20–25.

[15] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (aes)," 2001-11-26 2001.

[16] M. S. Awal and M. T. Rahman, "Disassembling software instruction types through impedance side-channel analysis," in *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2023, pp. 227–237.

[17] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," vol. 3156, 08 2004, pp. 16–29.

[18] S. Mangard, "A simple power-analysis (spa) attack on implementations of the aes key expansion," in *Information Security and Cryptology — ICISC 2002*, P. J. Lee and C. H. Lim, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 343–358.

[19] J. A. Ambrose, N. Aldon, A. Ignjatovic, and S. Parameswaran, "Anatomy of differential power analysis for aes," in *2008 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, 2008, pp. 459–466.

[20] Y. HAN, X. Zou, L. Zhenglin, and Y.-c. CHEN, "The research of dpa attacks against aes implementations," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, pp. 101–106, 12 2008.

[21] O. Lo, W. J. Buchanan, and D. Carson, "Power analysis attacks on the aes-128 s-box using differential power analysis (dpa) and correlation power analysis (cpa)," *Journal of Cyber Security Technology*, vol. 1, no. 2, pp. 88–107, 2017.

[22] F. R. Nuradha, S. D. Putra, Y. Kurniawan, and M. A. Rizqulloh, "Attack on aes encryption microcontroller devices with correlation power analysis," in *2019 International Symposium on Electronics and Smart Devices (ISESD)*, 2019, pp. 1–4.

[23] S. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an asic aes implementation," in *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.*, vol. 2, 2004, pp. 546–552 Vol.2.

[24] D. Jayasinghe, R. Ragel, J. A. Ambrose, A. Ignjatovic, and S. Parameswaran, "Advanced modes in aes: Are they safe from power analysis based side channel attacks?" in *2014 IEEE 32nd International Conference on Computer Design (ICCD)*, 2014, pp. 173–180.

[25] S. Fahd, M. Afzal, H. Abbas, W. Iqbal, and S. Waheed, "Correlation power analysis of modes of encryption in aes and its countermeasures," *Future Generation Computer Systems*, vol. 83, pp. 496–509, 2018.

[26] L. N. Nguyen, C.-L. Cheng, M. Prvulovic, and A. Zajić, "Creating a backscattering side channel to enable detection of dormant hardware trojans," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 7, pp. 1561–1574, 2019.

[27] K. Okamoto, T. Amano, K. Iokibe, and Y. Toyota, "Identification of equivalent current source of cryptographic circuit based on impedance and current measurements at board level," in *2012 Proceedings of SICE Annual Conference (SICE)*. IEEE, 2012, pp. 73–78.

[28] H. Zhu, H. Shan, D. Sullivan, X. Guo, Y. Jin, and X. Zhang, "Pdnpulse: Sensing pcb anomaly with the intrinsic power delivery network," *IEEE Transactions on Information Forensics and Security*, 2023.

[29] L. N. Nguyen, B. B. Yilmaz, M. Prvulovic, and A. Zajic, "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)*, 2020, pp. 1–12.

[30] C.-L. Cheng, S. Sangodoyin, L. N. Nguyen, M. Prvulovic, and A. Zajić, "Digital electronics as rfid tags: Impedance estimation and propagation characterization at 26.5 ghz and 300 ghz," *IEEE Journal of Radio Frequency Identification*, vol. 5, no. 1, pp. 29–39, 2020.

[31] E. Peeters, F.-X. Standaert, and J.-J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration*, vol. 40, no. 1, pp. 52–60, 2007.

[32] S. Kumar, V. A. Dasu, A. Baksi, S. Sarkar, D. Jap, J. Breier, and S. Bhasin, "Side channel attack on stream ciphers: A three-step approach to state/key recovery," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2022, no. 2, pp. 166–191, 2022.

[33] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[34] *FM18W08 256-Kbit (32 K × 8) Wide Voltage Bytewide F-RAM Memory*, Infineon Technologies, 9 2015, 001-86207 Rev. *E.

[35] "Alchitry au product page," https://alchitry.com/boards/au/, (Accessed: 3 April 2024).

Md Sadik Awal (S'17) received his B.Sc. degree in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology, Bangladesh in 2021. Since 2022, he has been a Graduate Research Assistant in the SeRLoP Lab while pursuing a Ph.D. at Florida International University's School of Electrical and Computer Engineering. His current research interests span the areas of hardware security, side-channel analysis, embedded systems, and signal processing.

Buddhipriya Gayanath is a graduate student at the Department of Electrical and Computer Engineering at Florida International University. He earned his B.Sc. degree from University of Sri Jayewardenepura in 2022. His current research focuses on radio frequency, analog and mixed-signal circuits, and signal processing.

Md Tauhidur Rahman (S'12–M'18-SM'21) is an Assistant Professor in the Department of Electrical and Computer Engineering at Florida International University (FIU). He received his Ph.D. degree in Computer Engineering from the University of Florida in 2017. His current research interests include hardware security and trust, side-channel analysis, memory systems, embedded security, and privacy. He is one of the recipients of the 2019 NSF CRII Award.