chips

MDPI

Article

PreSCAN: A Comprehensive Review of Pre-Silicon Physical Side-Channel Vulnerability Assessment Methodologies

Md Kawser Bepary, Tao Zhang *, Farimah Farahmandi and Mark Tehranipoor

Department of ECE, University of Florida, Gainesville, FL 32603, USA; mdkawser.bepary@ufl.edu (M.K.B.); farimah@ece.ufl.edu (F.F.); tehranipoor@ece.ufl.edu (M.T.)

* Correspondence: tao.zhang@ufl.edu (T.Z.)

Abstract: Physical side-channel attacks utilize power, electromagnetic (EM), or timing signatures from cryptographic implementations during operation to retrieve sensitive information from security-critical devices. This paper provides a comprehensive review of these potent attacks against cryptographic hardware implementations, with a particular emphasis on pre-silicon leakage assessment methodologies. We explore the intricacies of cryptographic algorithms, various side-channel attacks, and the latest mitigation techniques. Although leakage assessment techniques are widely adopted in the post-silicon phase, pre-silicon leakage assessment is an emerging field that addresses the inherent limitations of its post-silicon counterpart. We scrutinize established post-silicon techniques and provide a detailed comparative analysis of pre-silicon leakage assessment across different abstraction levels in the hardware design and verification flow. Furthermore, we categorize and discuss existing pre-silicon power and electromagnetic modeling techniques for leakage detection and mitigation that can be integrated with electronic design automation (EDA) tools to automate security assessments. Lastly, we offer insights into the future trajectory of physical side-channel leakage assessment techniques in the pre-silicon stages, highlighting the need for further research and development in this critical area of cybersecurity.

Keywords: hardware security; side-channel analysis; pre-silicon leakage assessment; power analysis; electromagnetic analysis; security metrics

Citation: Bepary, M.K.; Zhang, T.; Farahmandi, F.; Tehranipoor, M. PreSCAN: A Comprehensive Review of Pre-Silicon Physical Side-Channel Vulnerability Assessment Methodologies. *Chips* **2024**, *3*, 311–333. https://doi.org/10.3390/chips3040016

Academic Editor: Gaetano Palumbo

Received: 1 July 2024
Revised: 10 September 2024
Accepted: 22 September 2024
Published: 2 October 2024

1. Introduction

Over the past decades, the exponential growth and evolution of cyberspace have not only revolutionized communication and commerce but have also resulted in cyberspace becoming integral to every aspect of modern life, highlighting its profound importance in shaping contemporary society. Therefore, cybersecurity has attracted an ever-increasing amount of attention regarding the protection of users and nations from malicious activities. Significant success has been accomplished by cryptographic algorithms for encryption and authentication to preserve confidentiality, integrity, and availability of data such as passwords, credentials, and secret keys. However, most efforts have until now focused on the mathematic robustness and resilience of these algorithms against cryptanalysis at a high abstraction level. This is reasonable but disregards the fact that the actual computation is essentially operated by underlying hardware devices, which may unintentionally serve as the backdoor leaking security assets.

In the ever-evolving landscape of cybersecurity, side-channel attacks have emerged as a significant threat [1–3]. Unlike traditional attacks that target the algorithm or key directly, side-channel attacks exploit information leaked during the execution of cryptographic algorithms [1,4]. This information leakage can occur through various channels such as power consumption, EM radiation, or even acoustic signature [1,2]. The insidious nature of these attacks, exploiting unintended information leakage, makes them particularly challenging to predict and prevent, with the use of conventional security measures. As our

reliance on cryptographic systems continues to grow, spanning from online banking to secure military communications, the potential impact of successful side-channel attacks also escalates [2,3]. Despite the increasing threat, there is a noticeable gap in the literature reviewing the diverse types of side-channel attacks and the techniques used to assess leakage in the early design stage [5,6]. This gap hinders the development of robust defenses and a broader understanding of this critical issue.

This review paper aims to bridge this gap by providing a comprehensive overview of side-channel leakage assessment techniques at the post-silicon and pre-silicon abstraction levels. It will delve into the various types of side-channel attacks and leakage assessment techniques, including but not limited to power-monitoring attacks and EM attacks [1,2]. The paper will also explore the different leakage assessment methodologies at post-silicon and pre-silicon abstraction levels, such as Welch's *t*-test and KL divergence [5,7]. By offering a thorough investigation of existing pre-silicon power and electromagnetic leakage modeling and assessment techniques, this paper aims to serve as a valuable resource for researchers and practitioners in the field. It will foster a greater understanding of side-channel attacks and leakage assessment techniques, ultimately contributing to the development of more secure systems.

The structure of this paper is designed to systematically guide readers through the complex landscape of side-channel security in cryptographic systems. The main contributions of this review are as follows:

- We provide an overview of the prevalent side-channel attacks and their countermeasures. This background information establishes the necessary foundation to understand the vulnerabilities and protection strategies in modern cryptographic systems (Section 2).
- We compare post-silicon leakage assessment techniques with pre-silicon simulation approaches, analyzing different abstraction levels of the hardware design cycle. Additionally, we discuss various leakage quantification metrics, offering a clearer understanding of how leakage can be effectively measured and mitigated (Section 3).
- We present recent advancements in pre-silicon power and electromagnetic modeling and leakage assessment techniques. This includes a critical evaluation of these methodologies based on their applicability, accuracy, and limitations, offering a practical framework for researchers and practitioners who aim to enhance hardware design security (Section 4).
- We conclude by summarizing the key findings and proposing future research directions. This discussion emphasizes the gaps in the current literature and suggests promising areas for further exploration in pre-silicon side-channel assessment and mitigation strategies (Section 5).

Overall, this survey aims to provide a cohesive framework for understanding the existing methodologies in side-channel leakage assessment, with a special focus on pre-silicon techniques. It highlights the strengths and weaknesses of various approaches while offering guidance on future research avenues that could enhance the security of cryptographic hardware.

2. Physical Side-Channel Background

In the realm of digital security, understanding side-channel attacks and their respective countermeasures is essential. While traditional side-channel attacks predominantly target cryptographic implementations like AES [8] and RSA algorithm [9], which serve as root-of-trust in electronic systems and safeguard explicit security assets such as secret keys, increasing attention is also being paid to non-cryptographic components. These include communication buses and computing units in modern computer architectures [10], which are now recognized as potential targets. This section explores various types of side-channel attacks, particularly focusing on those exploiting power and electromagnetic emissions, which pose significant threats to cryptographic systems. Additionally, we discuss a range of strategies developed to mitigate these threats, each offering unique advantages to enhance

system resilience. This comprehensive background is crucial for grasping the nuances of leakage assessment techniques applied in both post-silicon and pre-silicon stages of cryptographic device development. Understanding these elements is fundamental to developing effective strategies for detecting and enhancing cryptographic security against side-channel attacks.

2.1. Side-Channel Attacks

Side-channel attacks (SCA) exploit the physical characteristics of cryptographic devices to extract sensitive information, primarily focusing on power consumption and EM emissions during cryptographic operations. These attacks are noted for their practicality in breaching security without needing to break the cryptographic algorithm mathematically. This subsection details the spectrum of side-channel attacks, with particular emphasis on power and electromagnetic analyses due to their widespread use, cost-effectiveness, and significant potential for revealing critical security information.

- Simple Side-Channel Attack: Simple Power Analysis (SPA) and Simple Electromagnetic Analysis (SEMA) involve direct observation of power or EM emissions to identify operational patterns such as key loading or algorithmic execution. These techniques do not require statistical analysis but rely on the clear visibility of patterns in the data traces [11,12].
- Differential and Correlation Side-Channel Attacks: Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) use statistical techniques to analyze variations in power consumption or electromagnetic emissions, as shown in Figure 1. DPA focuses on differences in power use between different operations, while CPA correlates these variations with predicted models based on cryptographic keys or operations [4,13]. Both methods aim to exploit the side-channel data collected across multiple operations to deduce secret information.
- Static Power Side-Channel Attacks: Static power side-channel attacks (S-PSCA) exploit the static power consumption of a device to extract sensitive information. Unlike dynamic power side-channel attacks, which focus on power consumption during active operations, S-PSCA analyzes the power consumption when the device is in a steady state. This can reveal information about the internal state of the device, such as values stored in registers or memory cells, potentially exposing cryptographic keys [2,14].
- Mutual Information Analysis: Mutual Information Analysis (MIA) employs a general statistical method that does not assume a specific leakage model, making it effective across diverse device architectures and operational modes. MIA assesses the mutual information between the guessed states of a cryptographic key and the measured side-channel signals to identify dependencies that may reveal sensitive data [15,16].
- Template Attack: Template attacks model the statistical distribution of side-channel leakage from a cryptographic device. By establishing a "template" based on a known operation, these attacks can predict the device's behavior during cryptographic operations, allowing for efficient extraction of secrets from minimal data samples [17,18].
- Deep-Learning-Based Side-Channel Attack: Deep-Learning-Based Side-Channel Attacks (DL-SCA) apply neural network architectures to detect and exploit patterns in side-channel data that might be less apparent through conventional statistical methods. This approach is particularly effective against devices with complex or unknown protection mechanisms, as it can learn to identify subtle vulnerabilities from large datasets of power or EM traces [19,20].

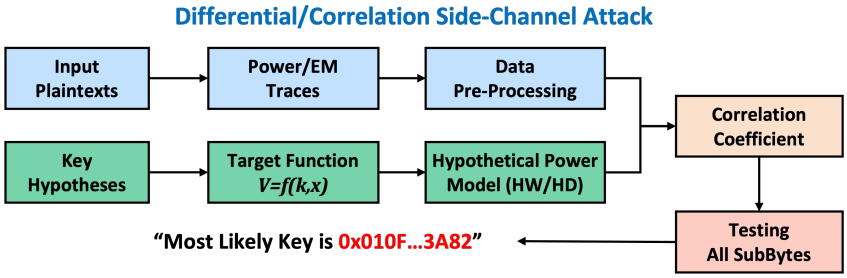


Figure 1. Overview of the differential/correlation-based side-channel attack.

2.2. Side-Channel Mitigation

This subsection discusses key strategies designed to protect cryptographic systems against side-channel attacks, focusing specifically on hiding, masking, and dual rail logic techniques. These methods enhance the security of systems by making it difficult for attackers to extract useful information from side-channel leakages.

2.2.1. Hiding

Hiding techniques aim to obscure the side-channel signatures that could be exploited by attackers. These methods include introducing noise into power consumption profiles, randomizing execution flows, or applying advanced masking schemes. The goal is to reduce the correlation between the observable leakages and the sensitive data being processed, thereby complicating the efforts of attackers to decipher cryptographic keys or other secret information [21,22].

2.2.2. Masking

Masking techniques involve altering the sensitive data by combining it with random values, thus obscuring the original information during processing. This section briefly outlines different masking approaches:

- Boolean Masking: This common technique involves splitting sensitive data into multiple shares and combining them with random masks during different computation stages. It effectively conceals the data by requiring all random masks to be known for successful extraction [23].
- Threshold Implementation (TI): TI divides computations into multiple shares that are processed separately. This method ensures that no single share reveals any critical information about the original data, enhancing security [24].
- Affine Masking: Affine masking utilizes linear transformations combined with constant shifts, providing robust protection, particularly against higher-order attacks. It randomizes intermediate values during cryptographic computations [25].
- Domain Oriented Masking (DOM): DOM applies masking at a domain level rather than individually for bits. This approach masks groups of related bits collectively, reducing the overhead and increasing resilience against side-channel attacks [24].

2.2.3. Dual Rail Logic

Dual Rail Logic enhances security by using complementary values across two physical signals, or "rails", for each logical bit. This redundancy ensures that leakage from a single rail does not disclose sensitive data, significantly increasing the complexity of side-channel attacks [26,27]. Additionally, Delay-Based Dual-Rail Precharge Logic (DB-DPL) introduces delay elements to equalize the power consumption of different logic paths [28]. TEL Logic Style uses a secure cell library to enhance resistance against side-channel attacks [29].

These mitigation techniques are vital for designing cryptographic systems that can withstand side-channel attacks, thus preserving the confidentiality and integrity of sensitive data.

3. Pre-Silicon Side-Channel Leakage Assessment

This section explores side-channel leakage assessment techniques in both post-silicon and silicon stages, which involves evaluating the potential for cryptographic systems to inadvertently disclose sensitive data through observable physical channels. Initially, Section 3.1 explores motivations, trade-offs between post-silicon and pre-silicon assessments, and scopes of these methodologies. We then detail quantification metrics and challenges in post-silicon leakage assessment, along with their implications for side-channel countermeasures. This narrative helps set the stage for a deep dive into pre-silicon leakage assessment in Section 3.2, where we assess leakage across various abstraction levels and highlight the crucial role of quantification metrics. Through this discussion, we aim to provide readers with a comprehensive understanding of side-channel leakage assessment and underscore the importance of precise leakage quantification.

3.1. Motivations for Pre-Silicon Leakage Assessment

With the rise of Internet-of-Things (IoT) devices, the threat landscape for side-channel attacks has significantly expanded, presenting new challenges due to the increased attack surface and ease of access for adversaries. This amplifies the importance of assessing side-channel leakage to detect potential vulnerabilities in cryptographic implementations before chip fabrication. Security experts have employed various methodologies, including evaluation and conformance testing, by analyzing post-silicon power and EM traces for side-channel leakage assessment [5,30,31]. Despite the high accuracy and rapid processing of post-silicon evaluation techniques, they do not allow for design modifications to address detected vulnerabilities [32,33]. Consequently, embedding resistance to side-channel attacks during the design phase has emerged as a critical challenge. Figure 2 illustrates the scope of post-silicon and pre-silicon leakage assessments in the microelectronic chip design and development workflow.

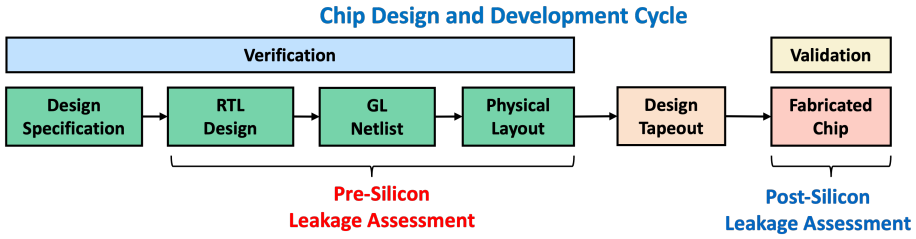


Figure 2. Post-silicon and pre-silicon side-channel leakage assessment techniques in the chip design flow.

Performing side-channel leakage assessments during the pre-silicon stages is crucial for designers to identify and mitigate vulnerable designs based on established evaluation criteria. Computer-aided design (CAD) technologies, which incorporate various tools throughout the chip design process, are becoming increasingly important in addressing these challenges. Assessing side-channel leakage at different pre-silicon abstraction levels involves balancing time, accuracy, and flexibility. Table 1 highlights the differences between pre-silicon and post-silicon side-channel leakage assessments. Pre-silicon evaluations provide more flexibility in identifying and mitigating potential vulnerabilities, though this often results in lower accuracy and longer evaluation times [32,33]. These methods are essential for designers to refine their designs and incorporate security countermeasures. However, during the design phase, there are always trade-offs to balance, including considerations of circuit area, power consumption, speed, and security.

Table 1. Comparison of pre-silicon and post-silicon side-channel leakage assessment [32].

	Pre-Silicon Assessment			**Post-Silicon Assessment**
	RTL	**Gate Level**	**Layout Level**	
Time	Medium	High	Very high	Low
Accuracy	Low	Medium	High	Very high
Flexibility	High	Medium	Low	Not feasible (ASIC); challenging (FPGA)

3.1.1. Conventional Post-Silicon Leakage Assessment

Two prevalent security certification programs, Common Criteria (CC) and FIPS, employ distinct testing methodologies—evaluation-style and conformance-style, respectively [30]. Evaluation-style testing, exemplified by CC, involves a comprehensive evaluation of cryptographic implementations against various attack strategies, demanding knowledge of the threat model. This method is thorough but criticized for its high cost, reliance on specific leakage models, and potential to overlook vulnerabilities [30]. In contrast, FIPS employs conformance-style testing that checks compliance with security standards rather than performing in-depth vulnerability assessments. It efficiently detects any leakage presence but does not quantify the vulnerability, which is a limitation also found in Test Vector Leakage Assessment (TVLA), a conformance-style tool that detects but does not measure the extent of side-channel vulnerability [30]. Wang and Tang [34] highlight the limitations of both methods and call for hybrid approaches that combine early detection with detailed leakage analysis, addressing the gaps in current pre-silicon and post-silicon assessments.

Subsequently, we explore several quantification metrics used in post-silicon assessments, such as signal-to-noise ratio (SNR), measurement to disclose (MtD), and test vector leakage assessment (TVLA), to address the complexities of evaluating side-channel threats effectively.

- Signal-to-Noise Ratio (SNR): The Signal-to-Noise Ratio (SNR) plays a crucial role in side-channel assessments. In the context of side-channel analysis, the signal represents the exploitable information for an attack, while the noise encompasses all other information [35]. The SNR is computed as the variance of the signal divided by the variance of the noise.

$$SNR = \frac{Var(P_{signal})}{Var(P_{noise})} \quad (1)$$

  A higher SNR means the signal stands out more distinctly from the noise, which is critical for evaluating the vulnerability of cryptographic systems to side-channel attacks. The variability of SNR across different leakage models underscores its adaptability to various attack scenarios [35].
- Measurement to Disclose (MTD): MTD evaluates the security of cryptographic implementations by quantifying the number of traces required to recover a key [36,37]. It begins by collecting side-channel measurements under known key conditions to build statistical models of the device's leakage and noise. Effective use of MTD demands engineering expertise, comprehensive knowledge of cipher design, and familiarity with the hardware and trace measurement techniques [37]. MTD serves as an essential metric for assessing the vulnerability of cryptographic systems to side-channel attacks.
- Test Vector Leakage Assessment (TVLA): The Test Vector Leakage Assessment (TVLA) evaluates cryptographic implementations for susceptibility to side-channel attacks (SCA) and determines the effort needed to extract sensitive information. TVLA employs Welch's *t*-test to quantify side-channel vulnerabilities [5]. This method employs Welch's *t*-test to analyze power consumption across two distinct datasets: one with a

static key and fixed plaintexts and another with the same key but varying plaintexts. The *t*-test is computed as follows:

$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{\sigma_0^2}{N_0} + \frac{\sigma_1^2}{N_1}}} \quad (2)$$

Here, μ_0 and μ_1 represent the means of the fixed and random sets respectively, σ_0 and σ_1 are their standard deviations, and N_0 and N_1 represent the number of observations in each set. A *t*-test result falling outside the predetermined confidence interval suggests a significant leakage risk, indicating a failure in the cryptographic implementation's security. Beyond the standard fixed-vs-random test, TVLA can also be adapted to include random-vs-random scenarios, where both key and plaintext are varied to detect otherwise obscured leakages, and semifixed-vs-random key tests, where keys are partially fixed [38]. These variations contribute to a more comprehensive evaluation of a system's vulnerability to side-channel attacks.

3.1.2. Limitations of Post-Silicon Assessment

Evaluating post-silicon side-channel leakage poses numerous challenges and limitations. As per the study conducted by Kiaei et al. [39], forecasting the degree and exploitability of side-channel leakage from intricate System-on-Chip (SoC) designs is a daunting task. While the post-silicon environment offers more detailed side-channel leakage data than the pre-silicon environment, the latter significantly improves test resolution and support for root cause analysis. This implies that pre-silicon side-channel leakage assessment could be a crucial instrument for the security analysis of contemporary Security SoC. Nevertheless, the focus on post-silicon stages by most existing power side-channel assessment techniques significantly limits the flexibility to alter designs once leakage is detected [40], highlighting several key issues:

- Delayed Interventions: Post-silicon assessments typically identify vulnerabilities too late in the development cycle, making subsequent modifications costly and time-consuming.
- Limited Flexibility: Once a chip is fabricated, addressing detected vulnerabilities often requires starting a new development cycle, which can be prohibitively expensive and complex.
- Need for Early Assessment: There is a growing demand for side-channel leakage assessments to be conducted earlier in the design cycle to maximize the flexibility in applying countermeasures effectively.

These challenges underscore the importance of developing and integrating pre-silicon side-channel assessment techniques early in the design process to ensure security measures are both effective and economical.

3.2. Pre-Silicon Leakage Assessment Overview

Assessing side-channel leakage across different abstraction levels, such as RTL, gate level, and layout level, is crucial for securing cryptographic hardware designs. At the RTL level, power side-channel leakage is evaluated by estimating the power profile of a hardware design through functional simulation. Tools like RTL-PSC [7] and RTL-PAT [41] facilitate this process by using evaluation metrics to measure the design's susceptibility to power side-channel leakage. These frameworks provide an early-stage security assessment, allowing for the implementation of countermeasures before the design is finalized. At the gate level, methodologies such as Architecture Correlation Analysis [42] are employed to prioritize gates within a design according to their impact on side-channel leakage. This ranking involves logic synthesis, logic simulation, gate-level power estimation, and assessment of gate leakage. By identifying the gates that significantly contribute to side-channel leakage, these methodologies facilitate the deployment of specific countermeasure implementation [42,43]. Side-channel leakage assessment at the layout level is very costly and

time-consuming. The layout level offers the most precise representation of a hardware design and could potentially uncover side-channel leakages that are not detectable at higher abstraction levels. Nonetheless, the complexity of layout-level designs renders side-channel leakage assessment at this level a formidable task. Table 2 presents a comparative analysis of leakage assessment in different pre-silicon abstraction levels.

Table 2. Comparison of RTL, gate, and layout-level side-channel leakage assessment [43].

Properties	RTL	Gate-Level Netlist	Layout-Level
Available information	Switching activity	Switching activity	Switching activity
	Register counts	# of fanouts (approx. Load capacitance: $C_{gate} + C_{wire} + C_{diffusion}$)	Load capacitance ($C_{gate} + C_{wire} + C_{diffusion} + C_{parasitic}$), resistance
	Submodules (hierarchy)	Library definition	Library, parasitics, geometry, metal layers
	Functional testbench	Functional and parametric testbench	Functional and parametric testbench
Simulation granularity	Transition of each clock cycle	n-time samples per clock cycle	Transistor level SPICE simulation
	For each submodule	For each node	For each transistor
Tool	Synopsys VCS (SAIF), Cadence Incisive (VCD)	Synopsys VCS (SAIF), Cadence Incisive (VCD)	Ansys Redhawk, Cadence Voltus, Spectre, Synopsys HSPICE
Side-channel metric	TVLA, KL divergence	TVLA, KL divergence	TVLA, KL divergence
Accuracy	Low	Medium	High
Complexity	Medium	High	Very high

3.2.1. Leakage Quantification in Pre-Silicon

Test vector leakage assessment (TVLA/Welch's *t*-test) and KL divergence are common metrics to quantitatively assess the side-channel resiliency of design if the two sets of leakage traces significantly differ from each other [5,7]. This subsection discusses the existing side-channel leakage assessment metrics that are employed in the pre-silicon abstraction levels.

- Test Vector Leakage Assessment (TVLA): In the pre-silicon phase, TVLA requires thoughtful adaptation due to the absence of physical noise in simulated environments. Traditional post-silicon methods, like fixed vs. random trace comparisons, are less effective here because simulations inherently lack the electrical noise that actual hardware would introduce [44]. This discrepancy necessitates alternative approaches, such as the use of random vs. semifixed datasets, where part of the key or data remains constant while the rest varies. This approach helps in highlighting potential leakage paths that might be obscured in entirely random setups due to the uniform distribution of simulated noise.
  The *t*-test, employed in this context, adapts as follows:

$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{\sigma_0^2}{n_0} + \frac{\sigma_1^2}{n_1}}} \tag{3}$$

  Here, μ_0 and μ_1 are the means of the outputs from two different simulation setups—one with semifixed and one with fully varied inputs—while σ_0^2, σ_1^2, n_0, and n_1 denote their variances and sample sizes. By tailoring the analysis to the unique characteristics of pre-silicon simulations, TVLA not only becomes feasible but also provides

a critical tool for preemptively identifying and mitigating side-channel vulnerabilities, ensuring that security is built into the hardware design from the ground up.

- Kullback-Leibler (KL) Divergence: KL divergence measures the statistical difference between probability distribution functions. In the context of power side-channel analysis, KL divergence assesses design vulnerabilities by comparing the probability density functions (PDFs) of power/EM traces assuming a Gaussian distribution. It quantifies the likelihood of an attacker correctly inferring the key by evaluating how distinct these distributions are between different keys [7]. The formula for KL divergence is given by Equation (4):

$$D_{KL}(k_i||k_j) = \int f_{T|k_i}(t) \log \frac{f_{T|k_i}(t)}{f_{T|k_j}(t)} \, dt \tag{4}$$

where $f_{T|k_i}(t)$ and $f_{T|k_j}(t)$ represent the PDFs of the switching activities associated with keys k_i and k_j, respectively. The normalized form of KL divergence under the assumption of normal distributions is expressed as:

$$D_{KL}(k_i||k_j) = \frac{(\mu_i - \mu_j)^2 + \sigma_i^2 - \sigma_j^2}{2\sigma_j^2} + \ln \frac{\sigma_j}{\sigma_i} \tag{5}$$

Here, μ_i, σ_i^2 denote the mean and variance of the EM traces for key k_i, and μ_j, σ_j^2 denote those for key k_j. Higher KL divergence values indicate more distinguishable probability distributions of leakage traces, increasing the risk of successful differential or correlation attacks. KL divergence also provides insights into the probability of an attacker failing to extract the correct key, thereby influencing the security requirements of a cryptographic design. For instance, achieving a 90% attack failure probability may necessitate keeping KL divergence below 0.03 [45].

- Side-Channel Vulnerability (SCV): The Side-Channel Vulnerability (SCV) metric, although conceptually similar to the widely used Signal-to-Noise Ratio (SNR), provides unique benefits. Unlike the SNR, which necessitates analyzing thousands of silicon traces, SCV can be effectively employed in formal methods utilizing information flow tracking (IFT) to evaluate side-channel vulnerabilities using a limited number of simulated traces during the pre-silicon design phase [32,40]. The SCV is defined as:

$$SCV = \frac{P_{\text{signal}}}{P_{\text{noise}}} = \frac{P_{T.hi} - P_{T.hj}}{P_{\text{noise}}} \tag{6}$$

Here, $P_{T.hi}$ and $P_{T.hj}$ represent the average power consumption of the target function when the Hamming Weight (HW) of the output is $hi = HW(Ti)$ and $hj = HW(Tj)$ for the ith and jth input patterns, respectively. In this context, the difference between $P_{T.hi}$ and $P_{T.hj}$ serves as the signal power used for the side-channel vulnerability assessment.

3.2.2. Challenges in Pre-Silicon Assessment

Pre-silicon assessment of side-channel leakage plays a crucial role in identifying hardware vulnerabilities during the design phase, yet it encounters significant challenges. Despite the advantages of conducting these assessments in System-on-Chip (SoC) environments, where they provide detailed and noise-free analyses, they often fall short in delivering the necessary resolution and root cause analysis capabilities that are more readily available in post-silicon settings [31,39,46]. This discrepancy implies that while pre-silicon assessments can comprehensively reveal potential vulnerabilities, pinpointing the exact causes of these vulnerabilities remains difficult. Additionally, challenges in pre-silicon side-channel leakage assessment include:

- High Simulation Costs: The need for numerous high-resolution power/EM traces significantly raises the simulation costs, especially for complex designs with many components.

- Resolution and Analysis Limitations: Pre-silicon environments often lack the resolution and root cause analysis capabilities, limiting their effectiveness in identifying precise vulnerability causes.
- Ubiquitous Vulnerabilities: Vulnerabilities related to data-dependent power dissipation are prevalent across all levels of the system stack, necessitating comprehensive verification of leakage characteristics at every abstraction level [39].
- Complexity of Modern Designs: The intricate and diverse nature of modern hardware designs adds another layer of complexity, making thorough assessments more challenging.

Addressing these challenges is crucial for enhancing the effectiveness of pre-silicon side-channel leakage assessments and ultimately strengthening hardware security.

4. Review of State-of-the-Art Pre-Silicon Leakage Assessment Techniques

This section provides a comprehensive review of state-of-the-art power and electromagnetic leakage modeling and assessment techniques. Section 4.1 delves into the intricacies of power side-channel leakage assessment, encompassing key aspects such as leakage detection and mitigation techniques. This section aims to provide a thorough understanding of the various strategies employed to assess and mitigate side-channel leakages in power models. Moving forward, Section 4.2 shifts the focus to electromagnetic leakage modeling and assessment. It covers a range of topics, including white box analysis, layout-level EM simulation, and leakage mitigation techniques. This section aims to explain the complexities of electromagnetic leakage and the methodologies used to model, assess, and mitigate such leakages. Through this section, we aim to provide readers with a robust understanding of both power and electromagnetic side-channel leakages, their assessment, and mitigation techniques.

4.1. Advancements in Power Modeling and Leakage Assessment Techniques

Pre-silicon side-channel leakage assessment is pivotal for ensuring the security of new chip designs against various side-channel threats. It involves simulating the implementation of cryptographic ciphers to analyze power consumption patterns, which can reveal vulnerabilities to power-based side-channel attacks. While pre-silicon tools have made significant strides in providing early assessment results during chip design [47], challenges persist when transitioning from simulated environments to real-world implementations where measurements are susceptible to noise and distortions. This section delves into cutting-edge methodologies for pre-silicon power modeling and assessment, discussing their strengths and limitations. These advancements are crucial for identifying and mitigating hardware vulnerabilities at the design stage, thereby enhancing the overall security posture of new chip designs [47,48].

4.1.1. Leakage Detection Techniques

The following subsection delves into the methodologies and tools used in pre-silicon power side-channel leakage detection, highlighting their significance in the broader context of hardware security.

- NCSIM [49]/PLAN/PARAM [50]: Accelerating power trace simulation involves estimating power consumption across different levels of abstraction. NCSIM [49], a white-box simulator, focuses on DPA resistance at the gate level (see Figure 3a). While it does not account for static power consumption, NCSIM can model glitches and early propagation with added timing information. The tool supports various power estimation techniques, including transition counting and random transition weighting, and can annotate transition weighting by extracting parasitic data from the full-chip layout. However, transistor-level simulation for operations like internal MOV with core initialization in NCSIM can take up to 10 h, contrasting with a logic simulation that completes in minutes.
  Another tool, PLAN/PARAM [50] (see Figure 3b), estimates power by aggregating consumption from all signals within a module. This method assumes the power

consumption of a k-bit signal correlates with its Hamming weight. Evaluating the entire Shakti-C processor using PLAN/PARAM takes approximately 5 h, significantly faster than the month-long requirement for post-and-place route simulations.

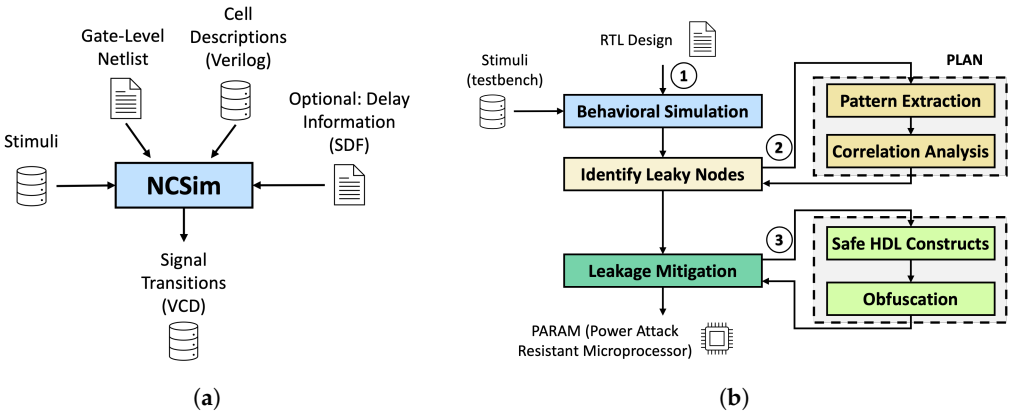


Figure 3. (**a**) Architecture of simulation environment using cadence NCSIM/Incisive [49], (**b**) Architecture of PLAN/PARAM leakage simulator [50].

- Architecture Correlation Analysis (ACA) [51]: The growing complexity of contemporary systems, fueled by System-on-Chip (SoC) integration, complicates the task of accurately pinpointing the origins of side-channel leakage. Consequently, secure SoC designers are compelled to proactively deploy costly countermeasures to protect subsystems like encryption modules, leading to increased chip design expenses. To address this issue, a new methodology known as Architecture Correlation Analysis (ACA) [51] has been introduced, presented in Figure 4. ACA enables the accurate identification of side-channel leakage sources at the granularity of a single cell during the design phase. By leveraging a leakage model typically used in differential side-channel analysis techniques, ACA ranks cells within a netlist based on their individual contributions to side-channel leakage. This strategy allows designers to apply countermeasures selectively where they are most effective, thereby reducing the need for expensive blanket countermeasure application. The effectiveness of the ACA methodology is showcased through its application to an AES coprocessor within an SoC design. By employing ACA, researchers successfully pinpoint sources of side-channel leakage at both the gate level within the AES module and within the overarching SoC [51]. Moreover, the efficacy of ACA is confirmed through its integration into an optimized hiding countermeasure.

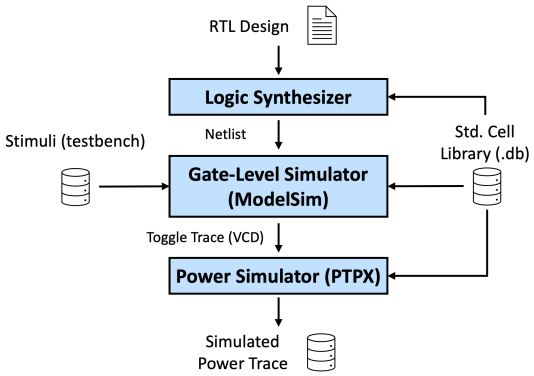


Figure 4. Simulation procedure of architecture correlation analysis (ACA) [51].

- RTL-PSC [7,41]: RTL-PSC [7,41] is one of the pioneers in RTL power side-channel evaluation of cryptographic cores, checking security vulnerabilities much earlier than the typical post-silicon evaluation in the entire development cycle. This method employs functional

simulation at the RTL to estimate the power consumption profile of a hardware design, utilizing the Synopsys VCS tool to count transitions, as shown in Figure 5. RTL-PSC distinguishes itself from other methods with two notable advantages: precise quantitative analysis of power side-channel leakage and exceptional efficiency. For instance, the evaluation time for AES-GF is approximately 43.6 min, while for AES-LUT, it varies between 24 and 44 min [7]. In contrast, gate-level and layout-level evaluations would take approximately 31 h and over a month, respectively.

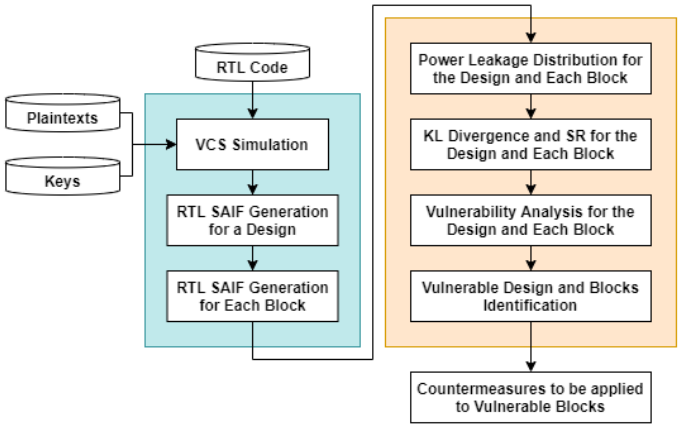


Figure 5. High-level flow of RTL power side-channel vulnerability assessment [7].

More specifically, RTL-PSC aims at quantifying the RTL power side-channel leakage in terms of KL divergence. KL divergence, as detailed in Section 3.2.1, measures the statistical distance between two probabilistic distributions. As for RTL-PSC methodology evaluating side-channel leakage, the distributions are generated with the simulated design switching activities (toggle counts in dumped SAIF files) by fitting them into the Gaussian distribution model. For each set of switching activities, the security analyzer will pick a different cryptographic key with random plaintexts (messages). Given the huge search space of key guesses (e.g., full key guess of a typical AES-128 calls for 2^{128} which is computationally intractable), a critical assumption of RTL-PSC is the hamming distance between selected key values is positively correlated with the resulting leakage. As such, RTL-PSC can excel in conventional post-silicon methodology in assessing design vulnerabilities without sacrificing accuracy while preserving the maximum flexibility in countermeasure deployment [7].

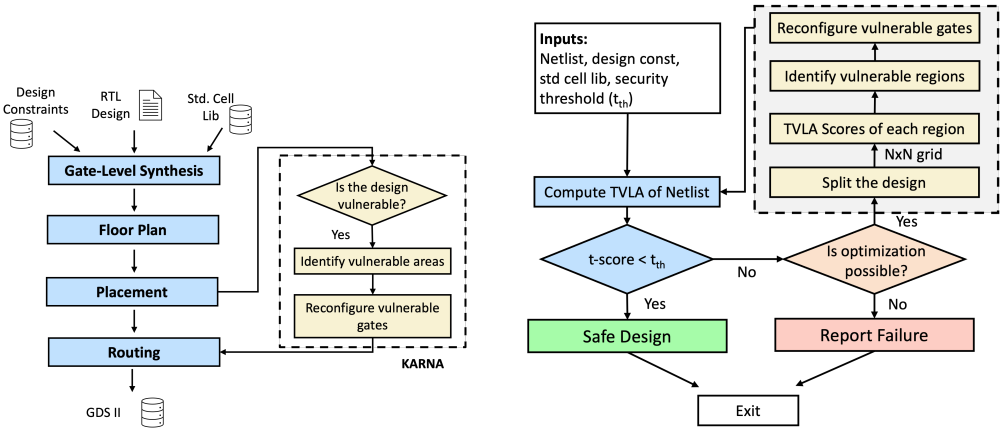
- PSC-TG [40]: The PSC-TG framework [40] represents an innovative approach for predicting power side-channel leakage at the RTL. This method enhances flexibility in implementing countermeasures against power side-channel attacks (SCAs), which exploit cryptographic implementation leaks to extract sensitive information. Unlike many existing techniques focused on post-silicon stages, PSC-TG initiates with RTL information flow tracking to pinpoint the most vulnerable variables. Formal assertions are then developed based on these variables and an assumed attack model to generate test patterns [32,40]. The side-channel vulnerability (SCV) metric is derived from estimated power using as few as two patterns, quantifying initial side-channel leakage. For higher-order assessments in masked implementations, PSC-TG employs a *t*-test to provide a pass/fail outcome [40]. Experimental evaluations across RTL, gate-level, and FPGA implementations validated PSC-TG's efficacy. Specifically, *t*-test results for masked Simon implementations aligned closely with post-silicon findings.
- Micro-Architectural Power Simulator (MAPS) [52]: Corre et al. introduce MAPS (Micro-Architectural Power Simulator), a novel tool designed to assess power side-channel leakage in cryptographic software running on ARM Cortex-M3 processors [52]. Power side-channel attacks exploit power consumption patterns during cryptographic algorithm execution to extract sensitive data. Creating a properly masked version of a

block cipher involves iterative and time-intensive processes, each requiring costly leakage assessments. MAPS aims to streamline this process with a fast and user-friendly simulator that models Cortex-M3 pipeline leakages, particularly those introduced by pipeline registers. The leakage characteristics of the Cortex-M3 series are derived directly from its HDL source code, eliminating the need for complex and expensive profiling phases [52]. As a case study, first-order masked Assembler implementations of the lightweight cipher Simon are analyzed to understand pipeline leakages and provide mitigation strategies. This tool represents a significant advancement in cryptographic software development, offering an efficient approach to evaluate and mitigate power side-channel leakage at the micro-architectural level [52].

4.1.2. Leakage Mitigation Techniques

Now, we will discuss about automated EDA tools that are designed to detect power side-channel leakage and apply mitigations.

- KARNA [53]: Karna [53] introduces an innovative methodology aimed at fortifying the side-channel security of devices within the Electronic Design Automation (EDA) flow. Unlike traditional countermeasures that often impose significant overheads, potentially compromising low-power, high-performance, and compact design requirements, Karna takes a unique approach. It operates without introducing additional logic, instead focusing on identifying and reconfiguring vulnerable gates within the design to enhance side-channel resistance. Notably, Karna utilizes standard cell library gates, foregoing the need for specialized gate libraries [53]. The overview of the framework and leakage mitigation flow is illustrated in Figure 6.
  The verification and mitigation flow of Karna has been seamlessly integrated into the Synopsys Design Compiler. Its effectiveness is demonstrated through significant reductions in side-channel leakage in implementations of AES, PRESENT, and Simon block ciphers synthesized for a 28 nm technology node. Remarkably, Karna achieves these enhancements by optimizing the available space around existing gates, thereby avoiding any additional area overheads. The authors validated the improved side-channel resilience of these optimized designs against Differential Power Analysis attacks [53]. This approach successfully mitigates power side-channel vulnerabilities without introducing delays, increasing power consumption, or escalating gate counts, underscoring Karna's potential as a pivotal tool for enhancing device security.



(**a**) (**b**)

Figure 6. (**a**) Overview of Karna framework integration into the standard EDA flow, (**b**) Leakage verification and mitigation using KARNA [53].

4.1.3. Comparison of Power Leakage Assessment Techniques

Pre-silicon side-channel leakage assessment plays a vital role in identifying vulnerabilities in cryptographic hardware early in the design process, primarily by simulating

power consumption patterns to assess the risk of side-channel attacks. Tools and methodologies have evolved significantly to facilitate early detection of power-based leakage, yet challenges persist, particularly when transitioning from simulated environments to real-world applications. Noise and measurement distortions in physical environments often introduce discrepancies, making it difficult to replicate the precision of pre-silicon models in post-silicon scenarios.

Despite these limitations, the current methodologies for pre-silicon power leakage assessment have made substantial progress. Techniques like NCSIM [49]/PLAN/PARAM [50] and ACA [51] are effective for early-stage design, with a particular focus on gate-level resistance to differential power analysis (DPA). Tools such as RTL-PSC [7] offer quick feedback, especially useful during the early design stages when designers are focused on making rapid iterations. However, the complexity and computational costs of generating high-resolution power traces remain a significant obstacle, as the simulation times can be prohibitively long, particularly for more detailed evaluations. PSC-TG [40] and KARNA [53] stand out in later design stages for providing more detailed vulnerability analyses and enhancing security within the electronic design automation (EDA) flow. These methodologies also address specific design complexities but may still struggle to accurately locate the sources of leakage. Table 3 provides an overview of the techniques, their strengths, and their limitations. As pre-silicon techniques evolve, further advancements in computational efficiency and the integration of automated security evaluation metrics will be necessary to mitigate these challenges effectively.

Table 3. Comparison of Pre-Silicon Power Modeling and Leakage Assessment Techniques

Technique	Description	Applicability	Evaluation Time	Complexity	Accuracy	Technology Dependency
NCSIM [49]/ PLAN/ PARAM [50]	Estimates power consumption at various abstraction levels. Focuses on gate-level DPA resistance.	Best for early-stage design and DPA resistance	Hours to days	High	Moderate to high	Low (Generic simulation tools)
ACA [51]	Identifies leakage sources at cell granularity using a differential leakage model.	Complex SoC designs	Moderate	Moderate to high	High	Medium (Specific IC designs)
RTL-PSC [7,41]	Assesses power side-channel leakage via RTL simulation, using transition counts to estimate power profiles.	Early design stages	Minutes to hours	Low to moderate	Moderate	Low (RTL design stages)
PSC-TG [40]	Uses RTL information flow tracking to predict vulnerabilities, employing formal assertions to develop test patterns.	Early and middle design phases	Minutes to hours	Moderate	High	Medium (Depends on RTL info)
MAPS [52]	Assesses leakage in cryptographic software on specific processors, focusing on pipeline leakages.	Software on ARM Cortex-M3	Fast (seconds to minutes)	Low	High	High (Specific to ARM Cortex)
KARNA [53]	Enhances side-channel security within the EDA flow by reconfiguring vulnerable gates to enhance resistance, using standard cell library gates without extras.	Final design stages, before manufacturing	Hours	Moderate to high	High	Medium (Depends on EDA tools)

4.2. Electromagnetic Modeling and Leakage Assessment Techniques

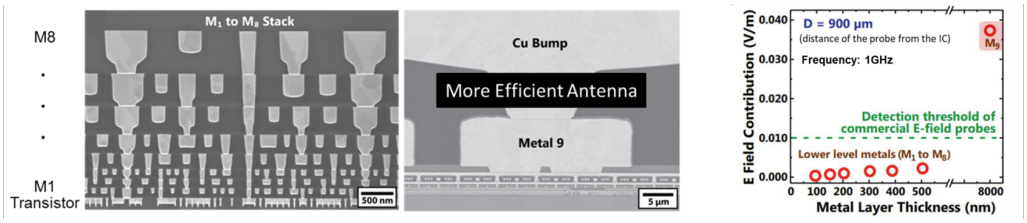
The origin of EM side-channel leakage lies in the distinct logic transition patterns exhibited by CMOS gates, which directly influence the observable side-channel trace patterns [54,55]. Evaluating EM side-channel leakage during integrated circuit (IC) design necessitates a comprehensive system-level multiphysics simulation approach. This ap-

proach considers crucial factors such as the design library, physical design parameters, placement of the power grid, and integration plans within the system. Accurate simulation tools capable of modeling IC EM emissions at the layout level are essential for understanding EM side-channel emissions and implementing effective countermeasures. These tools utilize high-performance solvers to simulate EM radiation accurately. They enable designers to analyze and optimize designs to mitigate EM side-channel vulnerabilities. Researchers have conducted numerous studies employing various methodologies and strategies to simulate EM radiation and develop countermeasures for different ICs. For instance, studies have focused on analyzing EM radiation from CMOS ICs, performing EM emanation simulations to analyze side-channel vulnerabilities in AES implementations, and developing techniques and tools to suppress EM radiation or enhance circuit resistance against localized EM attacks [54–57]. These efforts collectively contribute to a comprehensive understanding of ongoing research in EM emanation from cryptographic ICs. The goal is to effectively mitigate the challenges posed by EM leakage in cryptographic implementations through advanced simulation and optimization techniques.

4.2.1. Leakage Detection Techniques

The following subsection delves into the methodologies and tools used in pre-silicon electromagnetic side-channel leakage detection, highlighting their significance in the broader context of hardware security.

- White-Box Analysis [54,55]: Electromagnetic emissions in integrated circuits (ICs), caused by data-dependent current consumption passing through different metal layer interconnects, pose a significant security risk. In response to the growing threat of EM side-channel attacks on internet-connected devices, a novel approach called STELLAR has been introduced [54,55]. STELLAR provides a detailed analysis of the EM leakage in the context of side-channel security, focusing on its origin within CMOS-based ICs. The study reveals that EM radiation primarily stems from the metal layer routings within CMOS integrated circuits. Simulations are employed to explore the contributions of individual metal layers to the radiated electric field (E-field), demonstrating that the highest metal layers, such as Metal 9 (M9), play a significant role in EM radiation, illustrated in Figure 7. Commercially available E-field probes are used to assess the sensitivity and detectability of the EM leakage from different metal layers. The results show that for the specific example of Intel's 32 nm technology, the radiation from M9 can be detected, while lower-level metal layers do not exceed the detection threshold of E-field probes. This underscores the importance of minimizing EM radiation from top-level metal layers and provides insights into designing countermeasures against EM side-channel attacks [54,55].



(**a**) (**b**)

Figure 7. (**a**) Cross-Section of the metal-interconnect stack (Intel 32 nm), and (**b**) E-field contributions of the metal stack [54].

The STELLAR countermeasure involves routing the cryptographic core within lower-level metal layers, making EM leakage undetectable to external attackers with EM probes. Additionally, a Signature Attenuation Hardware (SAH) is employed to suppress the encryption signature before it reaches the highly radiating top-level metal layers, ensuring security against EM side-channel attacks [54,55,58]. Real-world testing with a 128-bit AES engine demonstrates the effectiveness of STELLAR, with no secret

key disclosure even after 1 million encryptions, minimal area and power overhead, and no performance penalties.

- Efficient DEMA Simulation [56]: Kumar et al. [56] present an efficient simulation flow at the layout level aimed at evaluating the susceptibility of integrated circuits (ICs) to electromagnetic side-channel attacks (EM SCA). The flow consists of three key steps: circuit analysis, model simplification, and EM radiation, and incorporates strategies to reduce computational costs without sacrificing predictive accuracy [56,59]. Figure 8 provides an overview of the entire process.

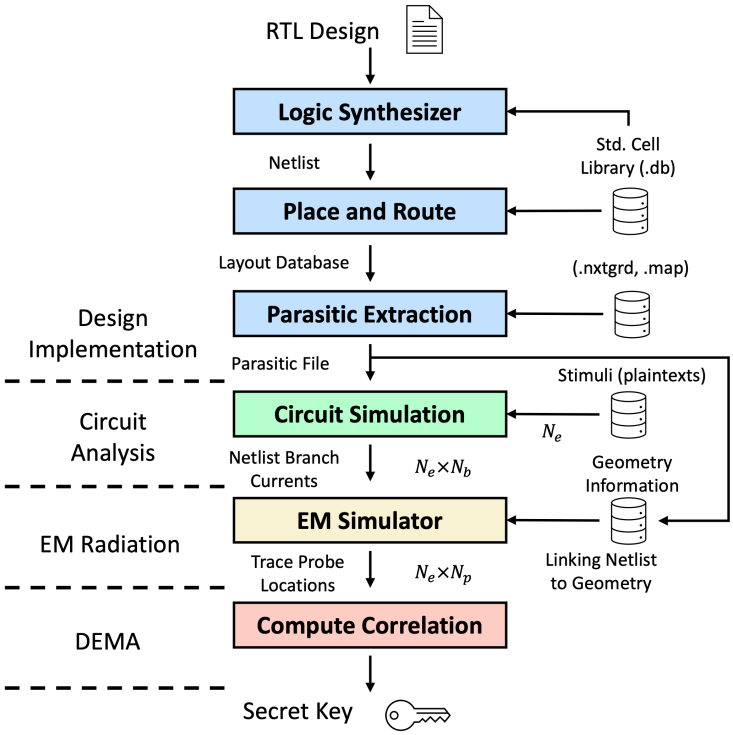


Figure 8. Efficient EM side-channel vulnerability simulation flow at layout level [56].

The circuit analysis step involves acquiring critical traces using industry-standard CAD tools, focusing on high-accuracy transient-circuit simulations exclusively during the cipher-execution phase. A hybrid approach that combines gate-level and transistor-level simulations is proposed, with transistor-level simulations using SPICE reserved for the critical last round. Model simplification aims to mitigate computational complexity by restricting the simulation of radiation to a reduced set of currents, specifically focusing on currents within the top metallization layers of the on-chip power-delivery network. The EM radiation step calculates the transient fields that would be received by a probe at different positions near the chip's surface, given the distribution of transient currents on the chip. EM traces are generated for various probe positions, orientations, and times. This step entails substantial computational complexity but can be effectively parallelized to reduce simulation times [56,59].

The proposed simulation flow, applied to an AES ASIC implementation, provides insights into electromagnetic side-channel attacks (EM SCA). The process involves circuit analysis for 5000 different encryptions and EM simulations. The analysis shows that probe proximity and noise significantly influence attack success. Furthermore, early-stage design choices, particularly the on-chip power distribution network design, can impact EM attack vulnerability. These findings emphasize the need for careful consideration during implementation [56,59].

- Multi-Physics EM Simulation [57]: Lin et al. [57] present an innovative pre-silicon EM side-channel simulation framework, illustrated in Figure 9, with three key contributions. Firstly, it provides an efficient pre-silicon EM side-channel simulation method powered by a machine learning-driven auto-Point-of-Interest (POI) detection algorithm. Secondly, the framework's accuracy is validated using a 130 nm AES128 test chip, effectively identifying EM leakage locations and the number of traces required for complete key disclosure. Lastly, the framework demonstrates versatility by handling EM leakage simulations from both the front and back sides of a design. The study identifies unexpected power ring structure leakage as a significant source of data exposure from the substrate side, endorsing the value of the auto-POI approach in guiding EM measurements [57].

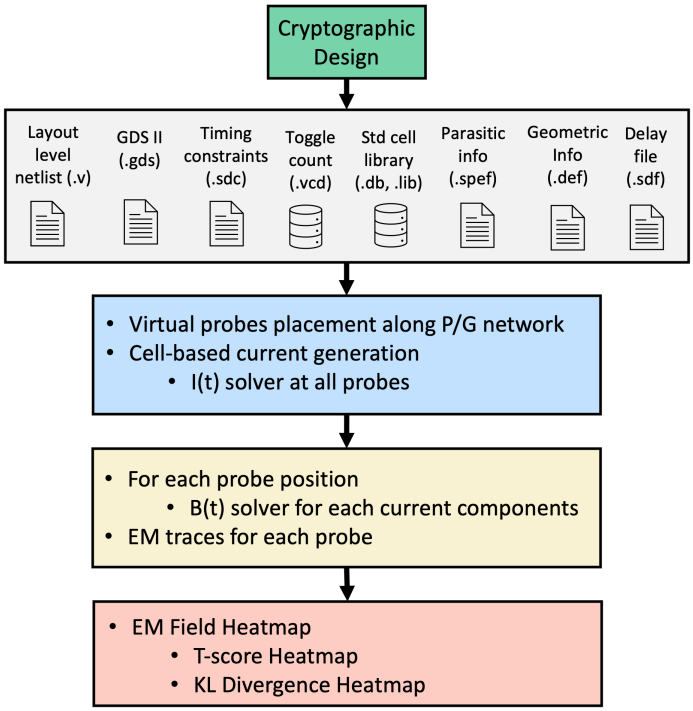


Figure 9. Overview of Multiphysics EM Leakage Simulation Flow [57].

The multiphysics simulation methodology encompasses layout-level power simulation, near-field EM modeling, and side-channel leakage analysis, with machine learning facilitating critical POI identification. The research also discusses potential design countermeasures to mitigate EM side-channel vulnerabilities, such as optimizing power grids, using shielding cans, and considering backside protection [57]. Overall, this paper presents a comprehensive framework for pre-silicon EM side-channel simulation, promising advancements in hardware security.

4.2.2. Leakage Mitigation Techniques

The following subsection discusses about automated EDA tools that are designed to detect EM side-channel leakage and apply mitigations in pre-silicon.

- CAD4EM-P [60]: Ma et al. [60] propose CAD4EM-P, an automated computer-aided design (CAD) tool designed to fortify circuits against EM side-channel attacks (SCA). Unlike traditional countermeasures that often impose significant overheads and demand specialized expertise from integrated circuit (IC) designers, CAD4EM-P integrates seamlessly into modern IC design flows. This tool focuses on enhancing circuit resistance to EM SCA by implementing security-oriented placement and routing strategies. The resulting IC designs are fortified against SCA attacks while incurring minimal area and power overheads [60,61].

CAD4EM-P's development involves investigating the root causes of EM leakage at the layout level and validating the effectiveness of security-driven placement and routing through mathematical modeling. This approach includes data-dependent register reallocation and adjustments to wire lengths to significantly reduce the correlation between protected data and EM leakage. Experimental simulations on cryptographic circuits demonstrate the efficacy of the developed EM leakage model and the CAD tool in enhancing EM side-channel security [60,61].

4.2.3. Comparison of EM Leakage Assessment Techniques

Pre-silicon EM side-channel leakage assessment is crucial for safeguarding new chip designs from EM-based side-channel threats. Simulating cryptographic processes to evaluate EM emission patterns allows developers to identify vulnerabilities prone to EM side-channel attacks. Despite significant advancements in simulation technology, the transition from theoretical models to practical applications is fraught with challenges due to the noise and distortions typical in real-world environments. These methodologies are vital for uncovering and mitigating hardware vulnerabilities early in the design process, substantially enhancing the security integrity of new chip designs.

Table 4 offers a comparative overview of various pre-silicon EM modeling and leakage assessment techniques. It illustrates their key attributes, advantages, limitations, and specific application contexts, providing a clear perspective on each method's utility and implementation scope. Techniques like STELLAR white box analysis [54,55] are critical for high-level integrated circuits vulnerable to EM attacks, focusing on leakage detection from upper metal layers. Conversely, multi-physics simulation [57] provides a more comprehensive solution for complex designs by integrating front and back-side EM analysis, along with layout-level power simulation. However, challenges remain in terms of computational cost and simulation accuracy, as generating EM traces is resource-intensive. Current tools also lack systematic approaches to quantitatively assess security during pre-silicon design and often fail to pinpoint the exact sources of leakage. Techniques such as CAD4EM-P [60] seek to enhance circuit resistance by employing security-driven design strategies, yet further advancements in automated and scalable methodologies are necessary to meet real-world demands. The comparative analysis in Table 4 helps guide designers in selecting the most suitable methods for robust EM leakage mitigation, emphasizing the need for continuous improvements in modeling efficiency and security evaluation.

Table 4. Comparison of Pre-Silicon Electromagnetic Modeling and Leakage Assessment Techniques

Technique	Description	Applicability	Evaluation Time	Complexity	Accuracy	Technology Dependency
White-Box Analysis [54,55]	Focuses on detecting EM leakage from higher metal layers using detailed analysis and specific countermeasures.	High-level ICs susceptible to EM attacks	Hours to days	High	High	High (Specific IC designs)
DEMA Simulation [56]	Utilizes a hybrid simulation approach combining gate-level and transistor-level analyses to identify EM vulnerabilities.	Early to mid-stage design phases	Hours to days	Moderate to high	High	Medium (Specific IC layouts)
Multi-Physics Simulation [57]	Integrates layout-level power simulation with EM modeling and leakage analysis, enhanced by machine learning for POI detection.	Complex IC designs considering both front and back side emissions	Hours to days	High	Very high	High (Advanced IC designs)
CAD4EM-P [60]	Enhances circuit resistance to EM SCA via security-oriented placement and routing within modern IC design flows.	Late-stage design phases focusing on EM SCA resistance	Hours	Moderate	High	Medium (Depends on EDA tools)

5. Conclusions and Future Directions

This comprehensive review has delved into the fundamental aspects of physical side-channel analysis, focusing on both pre-silicon and post-silicon side-channel leakage assessment techniques across various abstraction levels. By critically evaluating the advantages and disadvantages of these techniques, we provide a foundation for future research and a roadmap for researchers and practitioners navigating the evolving cybersecurity landscape. Our exploration of pre-silicon power and electromagnetic side-channel leakage modeling represents a critical frontier, promising detailed insights into vulnerabilities at a granular level. Understanding potential side-channel risks before physical fabrication allows designers to implement countermeasures early in the design process. Additionally, the quest for efficient EM leakage simulation aligns with the need for streamlined assessment processes that are practical for real-world implementation. Effective EM leakage simulation techniques are essential for preemptively identifying and mitigating security flaws, thus reducing the risk of costly post-silicon revisions.

Beyond traditional realms, system-on-chip (SoC) level assessment is crucial for a comprehensive understanding of side-channel risks in complex integrated circuits [31]. As SoCs become more prevalent in modern electronic devices, evaluating their side-channel vulnerabilities at this holistic level is increasingly important. Another intriguing domain is the early-stage EM leakage simulation, particularly at the gate level. Gate-level EM simulation can provide valuable insights early in the design process, though it presents significant challenges due to the lack of physical geometry information, which is crucial for accurate leakage estimation [43]. The rise of machine learning-assisted leakage methodologies represents a promising advancement in the field. These techniques enhance the efficiency and accuracy of leakage modeling, enabling more robust side-channel attack defenses. As these methodologies mature, they are likely to become more integrated into standard design practices, providing designers with powerful tools to anticipate and counteract side-channel vulnerabilities [62]. Furthermore, recent years have seen the development of commercial tools by companies such as Ansys and Rambus, which facilitate side-channel leakage modeling during the design stages. These tools are instrumental in bridging the gap between theoretical research and practical application.

Despite the progress made in side-channel leakage assessment, several areas require further exploration to enhance both pre-silicon and post-silicon methodologies:

- Machine Learning in Pre-Silicon Assessments: While machine learning techniques have shown promise in post-silicon leakage detection, their application in pre-silicon assessments remains underexplored. Future research could focus on developing machine learning models tailored for pre-silicon environments to improve the accuracy and efficiency of early-stage leakage assessments.
- Cross-Abstraction Leakage Correlation: There is a need for research that bridges the gap between different levels of abstraction (e.g., RTL, gate level, and layout level) in pre-silicon assessments. Establishing a robust correlation between leakage models across these abstractions could lead to more accurate and reliable leakage predictions, enabling designers to make informed decisions early in the design process.
- Automation and Scalability: The current methodologies for pre-silicon side-channel analysis are often manual and resource-intensive. Developing automated frameworks that can scale to handle large and complex designs is essential. These frameworks should also be adaptable to various design paradigms and technologies, ensuring their relevance across different hardware architectures.
- Countermeasure Evaluation: Most pre-silicon assessments focus on identifying potential vulnerabilities, but few consider the effectiveness of side-channel countermeasures at these early stages. Future research should aim to integrate the evaluation of countermeasures into pre-silicon tools, providing a holistic approach that not only identifies vulnerabilities but also assesses the potential impact of countermeasures before they are implemented in silicon.

- Emerging Threats and Standards: As cryptographic standards evolve and new threats emerge, there is a continuous need to update and refine side-channel leakage assessment methodologies. Future research should stay aligned with these evolving standards and threats, ensuring that assessment techniques remain robust and relevant in the face of new challenges.
- Heterogeneous Computing and IoT: The proliferation of heterogeneous computing platforms and IoT devices introduces new complexities in side-channel leakage assessment. Research should focus on developing tailored assessment methodologies for these platforms, considering their unique architectural features and constraints.

By addressing these areas, the field of side-channel leakage assessment can continue to advance, providing more effective tools and techniques to safeguard hardware implementations from potential side-channel attacks. Our paper aims to inspire collaborative efforts and propel advancements in the field, contributing to the ongoing dialogue on robust cybersecurity measures and encouraging the development of innovative solutions to address the ever-evolving challenges posed by side-channel attacks.

Author Contributions: Conceptualization, M.K.B. and M.T.; methodology, M.K.B.; investigation, M.K.B. and T.Z.; resources, F.F. and M.T.; writing—original draft preparation, M.K.B.; writing—review and editing, T.Z.; visualization, M.K.B. and T.Z.; supervision, F.F. and M.T.; funding acquisition, F.F. and M.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Randolph, M.; Diehl, W. Power side-channel attack analysis: A review of 20 years of study for the layman. *Cryptography* **2020**, *4*, 15. [CrossRef]
2. Socha, P.; Miškovskỳ, V.; Novotnỳ, M. A Comprehensive Survey on the Non-Invasive Passive Side-Channel Analysis. *Sensors* **2022**, *22*, 8096. [CrossRef] [PubMed]
3. Spence, A.; Bangay, S. Security beyond cybersecurity: Side-channel attacks against non-cyber systems and their countermeasures. *Int. J. Inf. Secur.* **2022**, *21*, 437–453. [CrossRef]
4. Kocher, P.; Jaffe, J.; Jun, B.; Rohatgi, P. Introduction to differential power analysis. *J. Cryptogr. Eng.* **2011**, *1*, 5–27. [CrossRef]
5. Schneider, T.; Moradi, A. Leakage Assessment Methodology: A Clear Roadmap for Side-Channel Evaluations. In Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2015: 17th International Workshop, Saint-Malo, France, 13–16 September 2015; pp. 495–513.
6. Gao, S.; Oswald, E. A Novel Framework for Explainable Leakage Assessment. In *Cryptology ePrint Archive*; IACR: Bellevue, WA, USA, 2022.
7. He, M.; Park, J.; Nahiyan, A.; Vassilev, A.; Jin, Y.; Tehranipoor, M. RTL-PSC: Automated Power Side-Channel Leakage Assessment At Register-Transfer Level. In Proceedings of the 2019 IEEE 37th VLSI Test Symposium (VTS), Monterey, CA, USA, 23–25 April 2019; pp. 1–6.
8. Dworkin, M.; Barker, E.; Nechvatal, J.; Foti, J.; Bassham, L.; Roback, E.; Dray, J. Advanced Encryption Standard (AES). 2001. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (accessed on 1 September 2024).
9. Easttom, C. Asymmetric Algorithms. In *Modern Cryptography: Applied Mathematics for Encryption and Information Security*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 233–252.
10. Rodrigues, C.; Oliveira, D.; Pinto, S. BUSted!!! Microarchitectural Side-Channel Attacks on the MCU Bus Interconnect. In Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2024; pp. 3679–3696.
11. Clavier, C.; Marion, D.; Wurcker, A. Simple power analysis on AES key expansion revisited. In Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2014: 16th International Workshop, Busan, Republic of Korea, 23–26 September 2014; pp. 279–297.
12. Bhunia, S.; Tehranipoor, M. *Hardware Security: A Hands-On Learning Approach*; Morgan Kaufmann: San Francisco, CA, USA, 2018.

13. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis With A Leakage Model. In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop, Cambridge, MA, USA, 11–13 August 2004; pp. 16–29.
14. Bhandari, J.; Nabeel, M.; Mankali, L.; Sinanoglu, O.; Karri, R.; Knechtel, J. Lightweight Masking Against Static Power Side-Channel Attacks. *arXiv preprint* **2024**, arXiv:2402.03196.
15. Gierlichs, B.; Batina, L.; Tuyls, P.; Preneel, B. Mutual information analysis: A generic side-channel distinguisher. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Washington, DC, USA, 10–13 August 2008; pp. 426–442.
16. Batina, L.; Gierlichs, B.; Prouff, E.; Rivain, M.; Standaert, F.X.; Veyrat-Charvillon, N. Mutual information analysis: A comprehensive study. *J. Cryptol.* **2011**, *24*, 269–291. [CrossRef]
17. Chari, S.; Rao, J.R.; Rohatgi, P. Template attacks. In *Cryptographic Hardware and Embedded Systems—CHES 2002: 4th International Workshop, Redwood Shores, CA, USA, 13–15 August 2002*; Revised Papers 4; Springer: Berlin/Heidelberg, Germany, 2003; pp. 13–28.
18. Gierlichs, B.; Lemke-Rust, K.; Paar, C. Templates vs. stochastic methods: A performance analysis for side channel cryptanalysis. In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, 10–13 October 2006; pp. 15–29.
19. Maghrebi, H. *Deep Learning based Side Channel Attacks in Practice*; IACR: Bellevue, WA, USA, 2020.
20. Wu, L.; Perin, G.; Picek, S. Deep Learning on Side-Channel Analysis. In *Security and Artificial Intelligence: A Crossdisciplinary Approach*; Springer International Publishing: Cham, Switzerland, 2022; Volume 13211, pp. 48–71.
21. De Mulder, E.; Eisenbarth, T.; Schaumont, P. Identifying and Eliminating Side-Channel Leaks in Programmable Systems. *IEEE Des. Test* **2018**, *35*, 74–89. [CrossRef]
22. Salomon, D.; Weiss, A.; Levi, I. Improved Filtering Techniques for Single-and Multi-Trace Side-Channel Analysis. *Cryptography* **2021**, *5*, 24. [CrossRef]
23. Biryukov, A.; Dinu, D.; Le Corre, Y.; Udovenko, A. Optimal first-order boolean masking for embedded iot devices. In *Smart Card Research and Advanced Applications: 16th International Conference, CARDIS 2017, Lugano, Switzerland, 13–15 November 2017*; Revised Selected Papers; Springer: Berlin/Heidelberg, Germany, 2018; pp. 22–41.
24. Groß, H.; Mangard, S.; Korak, T. Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. In *Cryptology ePrint Archive*; IACR: Bellevue, WA, USA, 2016.
25. Fumaroli, G.; Martinelli, A.; Prouff, E.; Rivain, M. Affine Masking against Higher-Order Side Channel Analysis. In *International Workshop on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 262–280.
26. Bhasin, S.; Guilley, S.; Souissi, Y.; Danger, J.L. Efficient FPGA Implementation of dual-rail countermeasures using Stochastic Models. In Proceedings of the Non-Invasive Attack Testing Workshop (NIAT 2011), Nara, Japan, 26–27 September 2011; Volume 10.
27. Nawaz, K.; Kamel, D.; Standaert, F.X.; Flandre, D. Scaling Trends For Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study. In *Constructive Side-Channel Analysis and Secure Design: 8th International Workshop, COSADE 2017, Paris, France, 13–14 April 2017*; Revised Selected Papers 8; Springer: Berlin/Heidelberg, Germany, 2017; pp. 19–33.
28. Bucci, M.; Giancane, L.; Luzzi, R.; Scotti, G.; Trifiletti, A. Delay-based dual-rail precharge logic. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2010**, *19*, 1147–1153. [CrossRef]
29. Bellizia, D.; Scotti, G.; Trifiletti, A. TEL logic style as a countermeasure against side-channel attacks: Secure cells library in 65 nm CMOS and experimental results. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65*, 3874–3884. [CrossRef]
30. Roy, D.B.; Bhasin, S.; Guilley, S.; Heuser, A.; Patranabis, S.; Mukhopadhyay, D. CC meets FIPS: A hybrid test methodology for first order side channel analysis. *IEEE Trans. Comput.* **2018**, *68*, 347–361. [CrossRef]
31. Ahmed, B.; Bepary, M.K.; Pundir, N.; Borza, M.; Raikhman, O.; Garg, A.; Donchin, D.; Cron, A.; Abdel-moneum, M.A.; Farahmandi, F.; et al. Quantifiable assurance: From ips to platforms. *arXiv preprint* **2022**, arXiv:2204.07909.
32. Nahiyan, A.; Park, J.; He, M.; Iskander, Y.; Farahmandi, F.; Forte, D.; Tehranipoor, M. Script: A cad framework for power side-channel vulnerability assessment using information flow tracking and pattern generation. *ACM Trans. Des. Autom. Electron. Syst. (TODAES)* **2020**, *25*, 1–27. [CrossRef]
33. Farahmandi, F.; Rahman, M.S.; Rajendran, S.R.; Tehranipoor, M. CAD for Power Side-Channel Detection. In *CAD for Hardware Security*; Springer International Publishing, Cham, Switzerland, 2023; pp. 123–147.
34. Wang, Y.; Tang, M. A Survey of Side-Channel Leakage Assessment. *Electronics* **2023**, *12*, 3461. [CrossRef]
35. Yano, Y.; Iokibe, K.; Toyota, Y.; Teshima, T. Signal-to-Noise Ratio Measurements Of Side-Channel Traces For Establishing Low-Cost Countermeasure Design. In Proceedings of the 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Seoul, Republic of Korea, 20–23 June 2017; pp. 93–95.
36. Mangard, S. Hardware Countermeasures Against DPA–a Statistical Analysis of Their Effectiveness. In Proceedings of the Topics in Cryptology–CT-RSA 2004: The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, 23–27 February 2004; pp. 222–235.
37. Šijačić, D.; Balasch, J.; Yang, B.; Ghosh, S.; Verbauwhede, I. Towards efficient and automated side-channel evaluations at design time. *J. Cryptogr. Eng.* **2020**, *10*, 305–319. [CrossRef]

38. Becker, G.; Cooper, J.; De Mulder, E.; Goodwill, G.; Jaffe, J.; Kenworthy, G. Test Vector Leakage Assessment (TVLA) Derived Test Requirements (DTR) with AES. In Proceedings of the International Cryptographic Module Conference, Gaithersburg, MD, USA, 24–26 September 2013.
39. Kiaei, P.; Liu, Z.; Eren, R.K.; Yao, Y.; Schaumont, P. Saidoyoki: Evaluating Side-Channel Leakage In Pre-And Post-Silicon Setting. In *Cryptology ePrint Archive*; IACR: Bellevue, WA, USA, 2021.
40. Zhang, T.; Park, J.; Tehranipoor, M.; Farahmandi, F. PSC-TG: RTL Power Side-Channel Leakage Assessment With Test Pattern Generation. In Proceedings of the 2021 58th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 5–9 December 2021; pp. 709–714.
41. Pundir, N.; Park, J.; Farahmandi, F.; Tehranipoor, M. Power side-channel leakage assessment framework at register-transfer level. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2022**, *30*, 1207–1218. [CrossRef]
42. Kiaei, P.; Yao, Y.; Liu, Z.; Fern, N.; Breunesse, C.B.; Van Woudenberg, J.; Gillis, K.; Dich, A.; Grossmann, P.; Schaumont, P. Gate-level side-channel leakage assessment with architecture correlation analysis. *arXiv preprint* **2022**, arXiv:2204.11972.
43. Bepary, M.K.; Zhang, T.; Azar, K.Z.; Rahman, F.; Farahmandi, F.; Tehranipoor, M. EMSC-GL: Security Assessment and Modeling of Electromagnetic Side-channel Leakage at Gate-level. In Proceedings of the Annual Government Microelectronic Applications and Critical Technology Conference (GOMACTech), San Diego, CA, USA, 20–23 March 2023.
44. He, J.; Ma, H.; Guo, X.; Zhao, Y.; Jin, Y. Design for EM Side-Channel Security Through Quantitative Assessment of Rtl Implementations. In Proceedings of the 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC), Beijing, China, 13–16 January 2020; pp. 62–67.
45. Park, J.; Tyagi, A. Security Metrics For Power Based SCA Resistant Hardware Implementation. In Proceedings of the 2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), Kolkata, India, 4–8 January 2016; pp. 541–546.
46. Kiaei, P.; Liu, Z.; Schaumont, P. Leverage the average: Averaged Sampling in Pre-Silicon Side-Channel Leakage Assessment. In Proceedings of the Proceedings of the Great Lakes Symposium on VLSI 2022, Irvine, CA, USA, 6–8 June 2022; pp. 3–8.
47. Liu, Z.; Schaumont, P. Root-Cause Analysis of Power-Based Side-Channel Leakage in Lightweight Cryptography Candidates. In Proceedings of the NIST 5th Lightweight Cryptography Workshop (2022), Virtual, 9–11 May 2022.
48. Shanmugam, D.; Schaumont, P. Improving Side-channel Leakage Assessment Using Pre-silicon Leakage Models. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design, Munich, Germany, 3–4 April 2023; pp. 105–124.
49. Fadl, O.S.; Abu-Elyazeed, M.F.; Abdelhalim, M.B.; Amer, H.H.; Madian, A.H. Accurate dynamic power estimation for CMOS combinational logic circuits with real gate delay model. *J. Adv. Res.* **2016**, *7*, 89–94. [CrossRef] [PubMed]
50. KF, M.A.; Ganesan, V.; Bodduna, R.; Rebeiro, C. PARAM: A Microprocessor Hardened for Power Side-Channel Attack Resistance. In Proceedings of the 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), San Jose, CA, USA, 7–11 December 2020; pp. 23–34.
51. Yao, Y.; Kathuria, T.; Ege, B.; Schaumont, P. Architecture Correlation Analysis (ACA): Identifying the Source of Side-Channel Leakage at Gate-Level. In Proceedings of the 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), San Jose, CA, USA, 7–11 December 2020; pp. 188–196.
52. Le Corre, Y.; Großschädl, J.; Dinu, D. Micro-Architectural Power Simulator for Leakage Assessment of Cryptographic Software on ARM Cortex-M3 Processors. In Proceedings of the Constructive Side-Channel Analysis and Secure Design: 9th International Workshop, COSADE 2018, Singapore, 23–24 April 2018; pp. 82–98.
53. Slpsk, P.; Vairam, P.K.; Rebeiro, C.; Kamakoti, V. Karna: A Gate-Sizing Based Security Aware EDA Flow for Improved Power Side-Channel Attack Protection. In Proceedings of the 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Westminster, CO, USA, 4–7 November 2019; pp. 1–8.
54. Das, D.; Nath, M.; Chatterjee, B.; Ghosh, S.; Sen, S. STELLAR: A generic EM Side-Channel Attack Protection Through Ground-Up Root-Cause Analysis. In Proceedings of the 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 5–10 May 2019; pp. 11–20.
55. Das, D.; Sen, S. Electromagnetic and power side-channel analysis: Advanced attacks and low-overhead generic countermeasures through white-box approach. *Cryptography* **2020**, *4*, 30. [CrossRef]
56. Kumar, A.; Scarborough, C.; Yilmaz, A.; Orshansky, M. Efficient Simulation of EM Side-Channel Attack Resilience. In Proceedings of the 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, USA, 13–16 November 2017; pp. 123–130.
57. Lin, L.; Zhu, D.; Wen, J.; Chen, H.; Lu, Y.; Chang, N.; Chow, C.; Shrivastav, H.; Chen, C.W.; Monta, K.; et al. Multiphysics Simulation of EM Side-Channels From Silicon Backside with ML-Based Auto-POI Identification. In Proceedings of the 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 13–14 December 2021; pp. 270–280.
58. Das, D.; Nath, M.; Ghosh, S.; Sen, S. Killing EM Side-Channel Leakage At Its Source. In Proceedings of the 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, 9–12 August 2020; pp. 1108–1111.
59. Wang, M.; Iyer, V.V.; Xie, S.; Li, G.; Mathew, S.K.; Kumar, R.; Orshansky, M.; Yilmaz, A.E.; Kulkarni, J.P. Physical Design Strategies For Mitigating Fine-Grained Electromagnetic Side-Channel Attacks. In Proceedings of the 2021 IEEE Custom Integrated Circuits Conference (CICC), Virtual, 25–30 April 2021; pp. 1–2.

60. Ma, H.; He, J.; Liu, Y.; Zhao, Y.; Jin, Y. CAD4EM-P: Security-Driven Placement Tools For Electromagnetic Side Channel Protection. In Proceedings of the 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Xi'an, China, 16–17 December 2019; pp. 1–6.
61. Ma, H.; He, J.; Liu, Y.; Liu, L.; Zhao, Y.; Jin, Y. Security-Driven Placement And Routing Tools For Electromagnetic Side-Channel Protection. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *40*, 1077–1089. [CrossRef]
62. Gao, Y.; Ma, H.; Kong, J.; He, J.; Zhao, Y.; Jin, Y. EMSim+: Accelerating Electromagnetic Security Evaluation with Generative Adversarial Network. In Proceedings of the 2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD), San Francisco, CA, USA, 28 October–2 November 2023; pp. 1–8.