JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 02
2024
Research Article
https://doi.org/10.56979/702/2024

Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities

Muhammad Kaleem[1], Muhammad Azhar Mushtaq[1*] , Sadaqat Ali Ramay[2], Aamir Mahmood[3], Tahir Abbas Khan[2], Sayyid Kamran Hussain[2], Adeel Anwar[4], and Hassnain Abdullah Bhatti[5]

[1]Department of IT, Faculty of Computing & IT , University of Sargodha, Pakistan.
[2]Department of Computer Science Times institute, Multan, Pakistan.
[3]Sr. Cyber Security Specialist, Jazan Integrated Gasification and Power Company, Riyadh, Saudi Arabia.
[4]Director of IT (pre-opening), Jumeirah Hotels and Resorts, Kingdom of Saudi Arabia.
[5](Telecom Engineer) Director Sales and Partnership,ABCC - Abdullah Bhatti Construction Company PVT Ltd. Multan, 60000, Punjab, Pakistan.
[*]Corresponding Author: Muhammad Azhar Mushtaq. Email: azhar.mushtaq@uos.edu.pk

Received: April 12, 2024 **Accepted:** August 19, 2024 **Published:** September 01, 2024

Abstract: Side-channel attacks have become increasingly important in the dynamic field of cybersecurity, posing a challenge to the security paradigms of cryptographic systems and implementations. The goal of this thorough review paper is to give a thorough understanding of side-channel assaults by examining the various kinds, subtypes, and difficulties that they present for modern security solutions. Understanding the taxonomy of side-channel attack vulnerabilities is essential for creating effective defense methods because these assaults target a wide range of vulnerabilities, from power consumption patterns to acoustic emanations.

Keywords: Side-channel; Cybersecurity; Paradigms.

1. Introduction

In the current digital era, technology has assimilated into our daily lives, bringing convenience and innovation. However, side-channel assaults (SCA) are a possible threat that come along with this improvement [1].

A more complex kind of security breach known as side-channel attacks concentrates on the inadvertent disclosure of data during the physical application of cryptographic algorithms rather than taking advantage of software flaws. These attacks identify critical data by analyzing seemingly innocuous side-channel data, such as power consumption, electromagnetic emissions, or timing variations.

Side-channel attacks fall into two broad categories: passive attacks, in which the attacker does nothing more than watch the information that has been spilled and examine it, and active assaults, in which the attacker modifies the device's functionality. These assaults can also be categorized as Non-Invasive (not tampering with the device's packaging), Semi-Invasive (making certain changes without fully opening the device), or Invasive (opening or removing the device's protection) [2].

This overview of the literature examines the spectrum of side-channel attacks, classifying and elucidating different kinds and variations to offer a comprehensive comprehension of their influence on cryptographic implementations. It also tackles issues raised by these attacks, like reducing power usage weaknesses and thwarting the use of electromagnetic emission. To help with the review, a structured table with a taxonomy of side-channel assaults is included. The methodology section covers methods for analyzing side-channel attack performance and offers insights into the instruments, methods, and metrics researchers use to gauge the efficacy of countermeasures and the resilience of cryptographic systems. This methodical investigation opens the door for thoughtful debates and further study by bridging theoretical comprehension with real-world applications.

In the future, the evaluation takes into account new developments, possible lines of inquiry, and technical breakthroughs that may influence side-channel attack research. The final round of the conversation evaluates the knowledge acquired, points out any inadequacies, and explores the wider cybersecurity ramifications. To sum up, protecting cryptographic infrastructures from side-channel assaults is essential to maintaining the robustness of our digital age secure communication systems.

2. Materials and Methods

2.1. Resources of Search

Using reputable search engines such as IEEE Xplore, ACM, Springer, and Google Scholar, we conducted our study to gather information onside channel attacks and its types. Root research materials relevant to the primary topic were not included in the first search. The selected research articles and conference proceedings underwent additional analysis in compliance with the evaluation criteria.

2.2. Initial Stage Selection Criteria

The selection of research publications and conference papers was initially conducted using a range of predetermined criteria, such as the language used in the paper, the year of publication, and the topic's relevance to the selected field. Only academic publications written in English were taken into consideration in this study. We focused on studies published between 2019 and 2023 in our review article. The selected articles had to be relevant to the search hierarchy's keywords.

2.3. Selection and Evaluation Process

There were 1150 research articles and conference reports found using the basic search parameters. Out of the papers found, we selected 95 publications with titles that we felt would be relevant to our research. From those publications, 64 research articles were chosen. after carefully assessing the abstracts of those studies for significance. The research articles that met the abstract criteria-based screening strategy were subjected to in-depth analyses. After a comprehensive evaluation of the research articles' quality, 48 were selected for the final analysis. 25% of the articles from Science Direct and 21% of the papers from Springer were included in the final selection, while 12% of the papers.

Table 1. Search Outcomes

No.	Platform	Early Search	Selection based on Abstract Final Paper for study
1	IEEE	2818	13
2	SPRINGER	105	3
3	SENSORS	1510	8
4	MDPI	107	4
5	USENIX Association	52	2
6	Other	205	2
	Total No. of paper	8047	32

2.4. Challenges of side channel attack

Side-channel assaults present significant issues in the field of cybersecurity that require thoughtful analysis and smart countermeasures. These attacks provide a complex threat to the security of cryptographic systems and sensitive data because they take advantage of unintentional information leakage through a variety of routes, such as power consumption, electromagnetic emanations, or timing patterns. In order to tackle the intricacies involved in side-channel attacks, it is imperative to comprehend the principal obstacles that cybersecurity experts and investigators encounter while striving to strengthen systems against these covert dangers.

- Hardware Trojans—unauthorized components or modifications to circuits—provide a significant issue since they can compromise circuit dependability, cause functionality to be disrupted, and reveal confidential information [3].
- Using CAD and third-party intellectual property raises security concerns since these tools could contain harmful or unreliable code, which could compromise security and cause data leaks [4].
- Using full cryptographic algorithm masking presents implementation issues and requires a large amount of resources because it requires a large number of random values and constant mask updating[5].

- It can be difficult to balance heat production and electricity consumption, especially in data Centre settings [6].
- Draws attention to the challenges associated with internal hardware-based techniques that need modifications to the original design, making them unfeasible for usage in legacy devices [7].
- One of the main challenges is modifying traditional side-channel analysis techniques to address the complexity of AI models, which are known for their complex structures, large number of parameters, and stringent precision requirements [8].

2.5. Taxonomy of side channel attack

We create a taxonomy of side-channel assaults by grouping them into several kinds, each of which represents a particular set of features. One common kind is timing attacks, which take advantage of differences in execution time to extract confidential data. Attacks known as "Power Analysis" concentrate on power usage trends, extracting cryptographic secrets from variations in power consumption. Unintentional radiation is the target of electromagnetic emanation attacks, which gather data from electromagnetic fields that are emitted. The aforementioned hierarchical classification presents an organized framework for comprehending the varied terrain of side-channel attacks and their intricate variants, hence furnishing a fundamental comprehension for subsequent investigation and study.

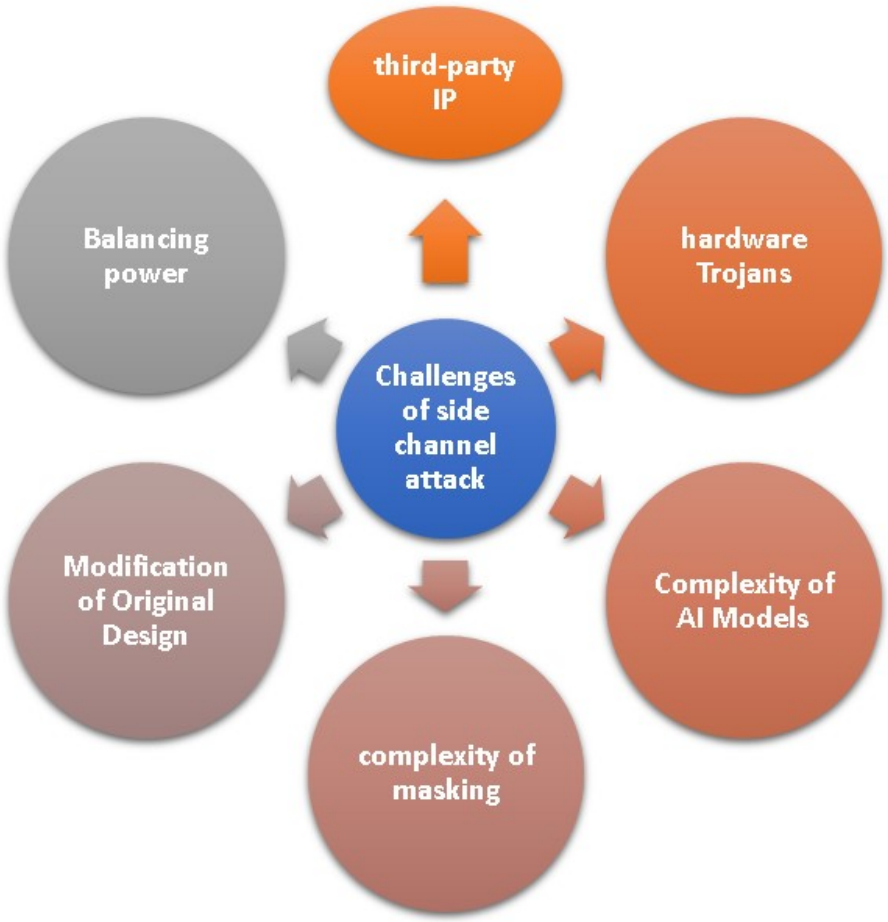

Figure 1. Challenges of side channel attack

2.6. Power Analysis Attack (PAA)

The term "Power Analysis Attack" (PAA) describes a class of side-channel attacks that take advantage of data that is exposed through a cryptographic device's operational power consumption trends. Hardware security modules and smart cards are examples of cryptographic devices that frequently display noticeable power consumption changes that correlate to various internal operations, including encryption or decryption procedures .Using advanced tools, the attacker examines variations in the device's power usage while cryptographic algorithms are being executed. An attacker can deduce sensitive information—such as secret keys or intermediate values—used in cryptographic processes by examining these patterns. Power

Analysis Attacks are a concern for secure cryptographic method implementations since they can be non-intrusive, meaning they don't involve physically altering the device.

The demand for improvements in food production has been driven by the projected peak of 10.9 billion people on Earth by 2100. This has led to advances in genetic engineering that improve crop quality and yield [1]. Digital agriculture has become a crucial component of sustainable food production in this regard. But as recent cyberattacks on vital infrastructure like the Florida water system and large agribusinesses show, it confronts serious cybersecurity challenges. These occurrences draw attention to digital agriculture's vulnerabilities, which could have an impact on labor costs, food supply, and labor expenses. This study examines side-channel attacks (SCAs) on digital agriculture in a way never seen before in order to allay these worries. It does this by critically assessing the body of research on cyber threats and by offering in-depth analyses of SCA threats and their ramifications. By starting this important discussion.

2.7. Simple Power Analysis (SPA)

The vital requirement for reliable user identification in wired and wireless access for corporate applications is addressed by RSA Security. Countermeasures are essential to the security of RSA-based devices because cryptanalysis techniques, in particular side-channel attacks like Differential Power Analysis (DPA) and Simple Power Analysis (SPA), are constantly evolving. Modular exponentiation is the target of SPA and DPA attacks, which are the main topic of this study. The work presents a low-cost exponent-randomizing method, in contrast to previous remedies that frequently result in decreased speeds or higher prices. This approach strikes a balance between security and efficiency, and it stands up well against a variety of power threats. The real-world crypto-system model emphasizes how crucial it is to comprehend electromagnetic radiation and power usage in order to secure cryptographic algorithms. The suggested method attempts to overcome the difficulties brought forth by developing cryptanalysis tools by improving security without compromising efficiency. [9].

Traditional security methods for hardware are increasingly vulnerable in the face of growing security issues in hardware design, especially with the globalization of production and the incorporation of third-party IP cores [10]. Logical locking and camouflage are examples of conventional hardware design-for-trust (DFT) methods that are vulnerable to sophisticated attack vectors, such as Boolean Satisfiability (SAT) assaults. Reconfigurable obfuscation techniques, such those based on Look-Up Tables (LUTs) and Magneto-Electric Spin-Orbit (MESO) devices, are intended to counteract SAT assaults; however, they come with built-in overheads. In this regard, the LOCK&ROLL approach effectively mitigates Machine Learning-assisted Power Side-Channel Attacks (P-SCAs) by introducing Symmetrical MRAM-based LUT (SyM-LUT). When used in conjunction with a Scan Enable Obfuscation Mechanism (SOM), SyM-LUT provides strong defense against ML-assisted P-SCAs and SAT attacks while requiring little overhead.

Boolean masking, which represents an n-bit secret variable Z as the sum of d random integers across F_n/2, is an essential defense mechanism against side-channel attacks on symmetric cyphers [11]. The number of masking shares, or parameter d, has a significant impact on installation and security expenses. Although (d-1)-th order masking is widely used and considered secure, this study investigates the need to measure the difficulty of a d-th order assault relative to its (d-1)-th order counterpart. The paper explores the exponential and quadratic patterns in attack and implementation costs that are increasing with d. A measurable assessment of assault expenses is presented via the success rate (SR), a presentation upper-bound measure associated with the necessary quantity of traces for success [11].

2.8. Correlation Power Analysis (CPA)

A specific type of Power Analysis Attack (PAA) known as Correlation Power Analysis (CPA) focuses on finding relationships between power usage patterns and the internal states that a cryptographic device experiences during operation. In a CPA, the attacker examines the power usage logs that are obtained from the targeted device as it performs cryptographic operations such as encryption and decoding. The core idea underlying CPA is to find relationships between power consumption variations and particular operations or intermediate values that are part of the cryptographic process. An attacker can gain insight into the internal states of the device by carefully matching power traces with the relevant operations or data-dependent fluctuations. This could reveal sensitive information like secret keys. .

This study introduces MW-FF as a novel countermeasure to mitigate the growing threat of Side-Channel Attacks (SCAs) that target the growing number of IoT edge devices, specifically the vulnerability

of encryption key exposure. In contrast to traditional methods, MW-FF recognizes the trade-offs involved in obtaining complete protection and places a higher priority on strengthening tamper resistance while minimizing the related implementation area overhead. MW-FF attempts to thwart Power Analysis Attacks (PAAs), such as Correlation Power Analysis (CPA), by incorporating a tiny circuit that manages random values into the original combinational circuit without making any changes. The assessment of MW-FF includes a study of its tamper resistance and implementation space for ASICs and FPGAs. This offers a flexible solution that can be used with a range of cyphers and can coexist with existing countermeasures. Essentially, the intended methodology seeks to [12]

2.9. Differential Power Analysis (DPA)

A side-channel attack technique called Differential Power Analysis (DPA) looks at variations in power consumption while cryptographic algorithms are operating. In simpler terms, DPA monitors power changes during different computational processes and uses the unique power consumption patterns of a device to extract sensitive data, such as cryptographic keys.

The vital requirement for reliable user identification in wired and wireless access for corporate applications is addressed by RSA Security. Countermeasures are essential to the security of RSA-based devices because cryptanalysis techniques, in particular side-channel attacks like Differential Power Analysis (DPA) and Simple Power Analysis (SPA), are constantly evolving. Modular exponentiation is the target of SPA and DPA attacks, which are the main topic of this study. The real-world crypto-system model emphasizes how crucial it is to comprehend electromagnetic radiation and power consumption in order to secure cryptographic algorithms. The suggested method attempts to overcome the difficulties brought about by developing cryptanalysis techniques by improving security without compromising performance [9].

The increasing demand for machine learning (ML) models, along with their considerable development costs, has given rise to a market where ML models are offered as services [13]. It is now essential to protect the intellectual properties (IPs) of machine learning (ML) models, since these models are increasingly being used on edge devices for increased privacy and performance. This change, however, leaves ML models open to possible extraction attacks via physical side-channel vulnerabilities, like those that take advantage of electromagnetic emissions and power consumption. This study highlights how vulnerable edge-based ML accelerators are to these kinds of attacks, highlighting how important it is to have strong defenses. The study expands on existing cryptographic countermeasures by focusing on Boolean masking and introducing improvements such as a shuffle countermeasure for improved side-channel resilience, a masked Kogge-Stone architecture for reduced latency, and an alternate implementation with a masked LUT. The results demonstrate increased security against power-based side-channel attacks and validate the effectiveness of these measures.

2.10. Physical side-channel attacks

In physical side-channel attacks, attackers use measurements of the cryptographic device's physical properties in an effort to infer relationships between these properties and the internal states of the system. The goal is to use accidental emissions or changes in physical parameters to extract useful information. Implementing secure cryptographic algorithms, using randomization techniques, and putting in place physical safeguards to reduce the amount of sensitive data that leaks through unintentional channels are all examples of countermeasures against physical side-channel attacks. The following is a list of physical side channel subtypes:

2.11. Information Leakage Exploitation

Information Violation In the context of physical side-channel attacks, "exploitation" refers to the act of taking advantage of inadvertent information leaks from the physical attributes of a cryptographic system, such as timing variations, power consumption, or electromagnetic emissions. The attacker's goal is to use these unintentional signals to infer important details, such as secret keys or the cryptographic device's internal states. In this type of attack, adversaries use the physical side-channel information that can be observed to deduce correlations between the cryptographic operations that are being performed and the unintentional emissions. The objective is to retrieve sensitive data from the target system by taking advantage of the inadvertent leak.

The increasing integration of artificial intelligence (AI) models in the intelligent Internet of Things (IoT) has raised security concerns, specifically regarding potential side-channel attacks (SCAs) [8]. When

AI models are used on a variety of IoT-enabled smart devices, they can be physically altered, providing attackers with the chance to take advantage of side channels and extract vital data such as model structures, hyper parameters, and exact weights. Effective methodologies for measuring and analyzing information leakage resulting from SCAs on AI models are lacking in current research. By utilizing information theory and presenting a fuzzy grey correlation-based extraction algorithm, this work fills in these gaps. The integrated framework investigates hierarchical weight extraction, met parameter extraction, and power trace-based structure extraction. The analysis method based on information theory provides a theoretical framework to understand the amount of leakage through side channels. An algorithm for multiple-micro space parallel SCA is developed to enable the extraction of AI weights with high precision. The suggested analysis approach and SCA algorithm's viability and effectiveness are confirmed by simulations and experiments, which offer important insights for creating safe AI model extraction algorithms for the intelligent IoT. Physical side-channel attacks are the subtype of side-channel attacks that are used here, with a focus on power traces to extract sensitive data from AI models installed in Internet of Things smart devices.

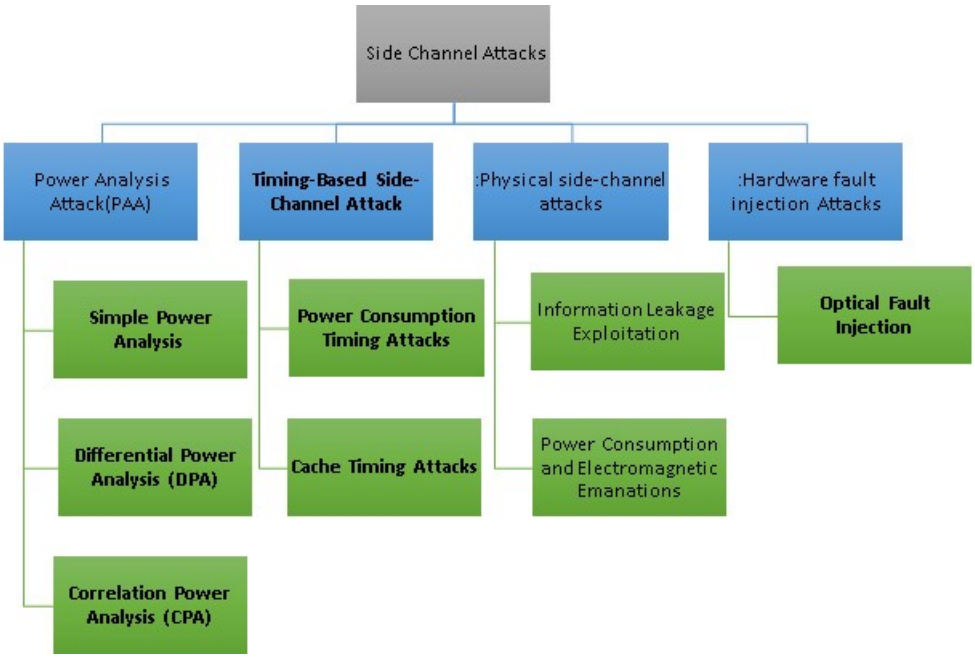

Figure 2. Taxonomy of side channel attack

2.12. Power Consumption and Electromagnetic Emanations

In the context of physical side-channel attacks, power consumption and electromagnetic emissions relate to two distinct categories of observable physical attributes that might be used to leak information. Power Consumption: This entails keeping an eye on changes in a cryptographic device's power usage habits while it's operating. Variations in power consumption may be associated with particular cryptographic processes, which could disclose details about the inner workings or secret keys. Electromagnetic Emanations: This refers to the inadvertent electromagnetic radiation that a device releases while it is operating. Adversaries may be able to extract sensitive data by intercepting and examining these emissions to learn more about the cryptography procedures.

The increasing demand for machine learning (ML) models, along with their considerable development costs, has given rise to a market where ML models are offered as services [13]. It is now essential to protect the intellectual rights (IPs) of machine learning (ML) models, since these models are increasingly being used on edge devices for increased privacy and performance. This change, however, leaves ML models open to possible extraction attacks via physical side-channel vulnerabilities, like those that take use of electromagnetic emissions and power usage. This study highlights how vulnerable edge-based ML accelerators are to these kinds of attacks, highlighting how important it is to have strong defences. The study expands on existing cryptographic countermeasures by focusing on Boolean masking and introducing improvements such as a shuffle countermeasure for improved side-channel resilience, a masked Kogge-Stone architecture for reduced latency, and an alternate implementation with a masked

LUT. The results demonstrate increased security against power-based side-channel attacks and validate the effectiveness of these solutions, taking into.

Cryptographic systems are vulnerable to Deep-learning Side-Channel Attacks (DL-SCAs), especially in hardware environments where parallel calculations introduce additional complexity. Previous studies explore the effects of different boards on DL-SCA accuracy, model tweaking, and hyperparameter modifications. Nevertheless, hardware implementations continue to be extremely difficult for DL-SCAs, particularly in advanced technologies. This study presents a new method based on the AdaBoost ensemble learning technique: a tandem deep-learning side-channel assault. Using several independently trained deep learning models, the tandem model outperforms single models, averaging 33.5% fewer traces required for a successful assault. Promising attacks on AES-128 executed on Xilinx Artix-7 FPGAs using a 28 nm technology highlight the efficacy of the suggested technique. Additionally, the study investigates how various classifier combinations affect the effectiveness of the tandem model. [14].

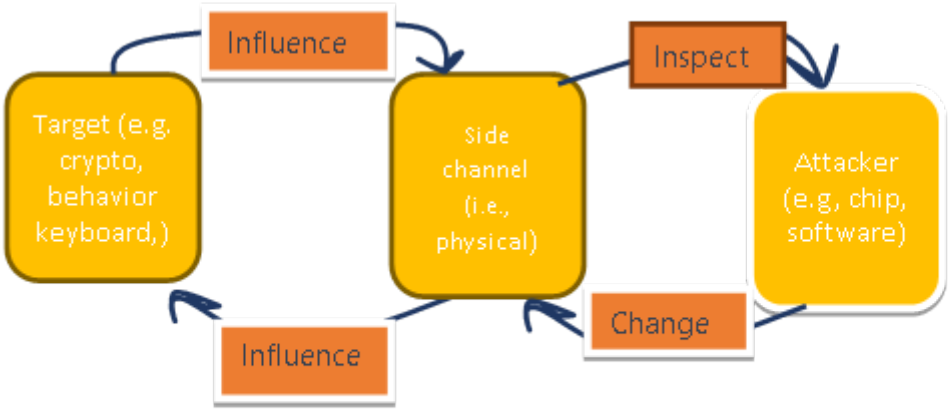

Figure 3. General notion of passive (−→) and active (←) side-channel

2.13. Hardware fault injection Attacks(HFIA)

A class of security risks known as Hardware Fault Injection Attacks (HFIA) involves purposefully introducing faults into the hardware components of a cryptographic device in order to exploit weaknesses. These attacks' main objective is to introduce malfunctions or mistakes into the device's functionality and track how these flaws impact its behaviour, sometimes resulting in the leak of private data like cryptographic keys. Attackers in HFIA employ a variety of techniques, including clock glitching, voltage manipulation, and laser-induced defects, to undermine the hardware's integrity. Adversaries try to obtain insight into the cryptography processes by strategically inserting defects into the device's operation, which ultimately compromises the system's security.

Ensuring strong security is crucial in the continually expanding realm of the Internet of Things (IoT), particularly when confronted with possible side-channel assaults (SCAs). The use of cryptographic methods in IoT devices presents difficulties despite current security precautions, necessitating careful attention to avoid vulnerabilities. Paper [15]introduces the Trusted Hardware-based Scalable Secure Architecture (THASSA), a flexible platform that can be used to create new secure IoT systems or as an additional security layer for existing ones. THASSA utilizes a combination of hardware and software solutions to address information flow vulnerabilities within Internet of Things edge devices. By using robust message exchange, dynamic key rolling, and a Commercial Off-The-Shelf (COTS) Trusted Platform Module (TPM) for enhanced security, it stops attackers from taking advantage of system flaws. THASSA seeks to offer security, scalability, and configurability, greatly advancing the continuous endeavours to strengthen the networked world of IoT devices [16].

2.14. Optical Fault Injection

A particular kind of Hardware Fault Injection Attack (HFIA) known as Optical Fault Injection (OFI) entails intentionally creating faults in a cryptographic device's hardware by manipulating it optically. In this attack, adversaries expose the device to laser or light pulses in order to take advantage of vulnerabilities in it. The aim is to interfere with the hardware's regular operation and see how induced faults affect cryptographic functions, possibly resulting in the extraction of private data such as cryptographic keys. Attackers employ precise optical signal targeting in Optical Fault Injection to undermine the integrity of the cryptographic device. Adversaries aim to cause deliberate errors through

optical manipulation in order to take advantage of weaknesses and obtain unauthorised access to private information.[17].

New techniques for defect localization have been developed as a result of the shift in Microelectronics Failure Analysis (FA) towards interconnects with multiple layers, especially when conventional Silicon Debugging and Diagnosis (SDD) techniques are no longer directly applicable [18]. Thanks to packaging techniques like flip-chip that expose the bulk silicon, FA methods from the chip backside have surfaced. But using silicon's transparency to Near-Infrared (NIR) photons has led to the development of optical fault injection (FA) methods like Photon Emission Analysis (PEA) and Laser Fault Injection (LFI). Although these methods improve the speed of FA, they also pose security risks because they allow an attacker to optically probe confidential data that is stored in the Integrated Circuit (IC). Logic locking, designed to safeguard intellectual property, is susceptible to optical attacks, as demonstrated by the disclosure of locking keys that are reachable from the rear of the chip. This paper addresses concerns about the confidentiality, availability, and integrity of optical attacks by providing a taxonomy of optical attacks, identifying approaches against logic locking, and evaluating countermeasures to mitigate backside optical attacks[19].

2.15. Timing-Based Side-Channel Attack

Timing-Based Side-Channel Attacks (TBSCA) are a class of security threats that take advantage of differences in how long cryptographic algorithms take to execute in order to retrieve confidential data. In these attacks, adversaries examine a cryptographic device's timing patterns while it is in use with the goal of inferring information about internal workings and possibly locating cryptographic keys or other sensitive information. Timing-Based Side-Channel Attacks concentrate on timing the duration of various cryptographic operations, allowing the attacker to identify minute differences that could be impacted by the algorithms being run or the data being processed. Through a thorough analysis of these timing differences, adversaries try to deduce information about the cryptographic device's internal states.

2.16. Cache Timing Attacks

In Side-Channel Analysis (SCA), the term "cache attacks" refers to a group of security risks that take advantage of data leaks from a device's cache memory when performing cryptographic operations. In these attacks, adversaries try to deduce sensitive information, like cryptographic keys, by examining the timing or access patterns to the cache. In SCA, cache attacks entail observing and deciphering the communications that take place between a cryptographic device and its cache memory. Attackers can use discrepancies in access times or patterns to their advantage, deriving information about the device's internal workings from this data. Through the use of side-channel information related to caches, attackers hope to undermine the cryptographic system's security [20].

The need for advanced detection mechanisms is growing due to the growing threat of sensitive data leaks through cache side channels, which primarily affect cryptographic systems. Developers find it difficult to implement the current detectors because of their limitations with regard to scalability, automation, and accurate vulnerability localization. This paper presents CACHEQL, a comprehensive detector for production software that satisfies eight important requirements, such as automation and scalability. By using mutual information and a novel formulation based on conditional probability, CACHEQL improves computing efficiency in a novel way when quantifying information leakage. The detector treats side channel traces like a cooperative game and has a precise vulnerability localization method based on Shapley values. Thorough tests on real-world cryptosystems show that CACHEQL is capable of locating known vulnerabilities, measuring leaks [21].

2.17. Power Consumption Timing Attacks

In the evolving landscape of information security, the integrity of cryptographic algorithms has become a paramount concern[22]. While modern cryptographic methods are theoretically robust against brute-force attacks, recent research highlights vulnerabilities arising from the hardware on which these algorithms operate. Side-channel attacks (SCAs) exploit these physical weaknesses, leveraging parameters like power consumption and timing patterns. A specific subtype, Cache-based Side-Channel Attacks (CSCAs), capitalizes on cache timing and access patterns. authorpresents WHISPER, a runtime detection tool utilizing a machine learning ensemble to proactively identify CSCAs on Intel's x86 architecture. WHISPER exhibits noteworthy precision, minimal overhead, and resilience under diverse system load conditions. Importantly, the tool's versatility extends to detecting other attacks, such as Spectre and

Meltdown, making it a comprehensive solution against various side-channel threats, with a particular focus on cache access patterns[23].

3. Classification of Side Channel Attack

Understanding the various tactics adversaries use to compromise cryptographic systems requires examining the field of side-channel attacks. Here, we describe and group different kinds of side-channel attacks, offering a well-organized synopsis that forms the basis for comprehending their unique traits and possible danger. We also discuss critical performance measures for side-channel attacks in this section, which are important to assess the effectiveness of countermeasures in strengthening the resilience of cryptographic systems. Enhancing digital security is greatly aided by the key matrices that have been outlined. They offer valuable insights into the effectiveness and durability of defences. The comprehensive classification provided by the following table sheds light on the subtle techniques used in these attacks and provides insights into the vulnerabilities they exploit.

It is concluded and investigated into side-channel attacks by classifying and organizing the various attack kinds. This group aids in the comprehension of the cunning tactics employed by malevolent actors to undermine cryptographic systems. Examining key performance indicators yields useful data to evaluate defenses' efficacy in fortifying cryptographic systems. In addition to showing how well defenses function, the comprehensive charts also significantly contribute to improving digital security. The generated table provides a clear picture of the intricate strategies these attacks employ, exposing the vulnerabilities they exploit. For researchers and practitioners, this section is a helpful resource that can help them better understand side-channel attacks and support ongoing efforts to fortify our digital defenses.

Table 2 (a). Classification of Attacks

Attack	Sub Type	Full Name	Citation
Physical side channel attack	Power Consumption and Electromagnetic Emanations	Guarding Machine Learning	GML[13]
		Tandem Deep Learning	TDL[14]
		Embedded Neural Networks	ENN [24]
		Random Number Generators	RNG[25]
	Information Leakage Exploitation	RASCv2 Remote Access	RASCv2[7]
		Side channel fuzzy analysis	ScFA[8]
	Differential Side channel	Masked Implementations	MI [5]
		LOCK&ROLL	LeL[10]
		Side-Channel Resistant	ScR[26]

		Segmented Modular Exponent	SME [9]
		Guarding Machine Learning	GML[13]
		Side-Channel Power Acquisition	ScPA[27]
	Correlation Power Analysis (CPA	Decentralized Blockchain Network	DBN [28]
		Stratifcation of Hardware	SoH[4]
Hardware fault injection Attacks	Optical Fault Injection	Volt Pillager	VoP[29]
		Plundervolt	PoV[6]
		Fault-Assisted Side-Channel	FASc[5]
		Neural Networks from Hardware	NNoH[30]
		Novel Trusted Hardware-based	NTHB [15]
		Hertzbleed	HTPSc[31]
	Cache Timing Attacks	Turning Power Side-Channel A Optical Attacks	OAML [18]
Timing-Based Side-Channel Attack		Making Logic Obfuscation Fragile	FTSC [32]
	Power Consumption Timing Attacks	Frequency Throttling Side-Channel	
		Side-Channel Fuzzy Analysis-Based	ScFA [8]

Table 2 (b). Classification of Attacks

Technique	Performance	Method	Weakness

Boolean Masking	Latency Reduction	Shuffle CountermeasureTop of Form	Leakage (Alternative Implementation)
Tandem-AdaBoost	Efficiency	Ensemble	Device-Dependency
Side-Channel Analysis (SCA)	Embedded DNN Vulnerability	Taxonomy and Classification	Lack of Mitigation Techniques
Quantum-enhanced RoTs	Quantum random number generation	Method: Survey and analysis	Limited understanding of quantum impact on physical security
RASCv2	Sampling Speed Enhancement	AES Key Extraction	Missed Range
Side-channel analysis	Theoretical and Experimental Validation	Fuzzy gray correlation-based multiple-microspace parallel SCA algorithm	Complexity
Fault Injection	Full key recovery	SC analysis on masked algorithms	Vulnerability of random number generation
Technique: LOCK&ROLL) Top of Form	Near-zero power variation	Symmetrical MRAM-based	Not specified
RSA Implementation	Fast	Combination of acceleration techniques	No specified

Boolean Masking	Latency Reduction	Shuffle CountermeasureTop of Form	Leakage (Alternative Implementation)

Side-channel power analysis	Visual analysis, Capture-the-flag scenario	In-depth analysis Reverse engineering	Not specified in the provided text.
Decentralized blockchainnetwork	Efficiency Improvement	Branching and Decentralized Blockchain	Unknown and Heterogeneous Adversaries
fault injection attacks Top of Form	Data leakage, secret key recovery	Backdoor entries, hardware Trojans	Design vulnerabilities, untrustworthy third-party IP,
Hardware-based voltage glitching	SGX key-recovery attacks,	VoltPillager hardware device injecting messages	ineffective, challenges SGX's threat model
Plundervolt Attack	Corruption of Intel SGX enclave	Exploitation of privileged dynamic	, challenging to fully mitigate

	computations, key recovery	voltage scaling interfaces	
Fault Injection	Full key recovery	SC analysis on masked algorithms	Vulnerability of random number generation
Hardware-based attacks	Security vulnerabilities	Survey and analysis	Underdeveloped security solutions
Trusted	Secure		Not specified
" Hardware-Based Security Framework	Communication, Dynamic Key Rolling	Cryptographic methods	
Turning Power	Side-channel analysis	Experimental evaluation	Not specified
Side-Channel A side-channel attack	AES key recovery	Experimental evaluation	Not specified
Frequency throttling side-channel attack	AES key recovery	Experimental evaluation	Not specified
Side-channel analysis	Side-channel analysis	Theoretical and Experimental Validation	Fuzzy gray correlation-based multiple-microspace parallel SCA algorithm

4. Discussion and Future work

Further investigation is required to fully understand power side-channel vulnerabilities across a larger spectrum of CPU architectures. This entails a thorough analysis of the special features of the AMD leakage model. Further attention should be paid to improving the real-world application of fully homomorphic encryption (FHE) in cryptographic software to effectively isolate operands from secrets and allay worries about power leakage.Sustaining current masking and blinding techniques in order to prevent practical leakage through power side channels requires constant refinement and improvement. A way to diversify defense mechanisms against power side-channel attacks is to investigate alternative defense strategies, such as the integration of unrelated loops, vectoring operations, and investigating the interleaving of complementary kernels. The goal of this ongoing research project is to support the ongoing creation of efficient mitigation techniques in the field of CPU security..

Regarding the necessity of protecting against fault injection, the planned future work centers on investigating and putting preventive measures directly in the enclave code to lessen possible risks associated with injected faults. The plan is to test whether it is feasible to replicate potentially weak instructions inside the enclave and then analyses the results to find errors. Although adding these types of checks by hand might be possible for smaller, more crucial code segments, like memory management or cryptography, protecting a whole existing codebase is considered impossible without automated support. Future research should explore existing approaches from previous studies, such as compiler-level automatic instruction duplication, and modify them for x86 architectures, especially in the context of the SGX framework.Maintaining the security and performance goals of SGX enclaves while integrating these preventive measures seamlessly presents a challenge. It is emphasized that SGX enclaves are constrained in that they cannot rely solely on mitigations associated with measuring CPU voltage because SGX does not have a reliable way to access Model-Specific Registers (MSRs), which makes it susceptible to attempts at circumvention by an infected operating system. Thus, future efforts in this field are anticipated to focus on the creation of automated and effective fault injection defenses that are customized for the SGX enclave.

5. Conclusion

This comprehensive analysis of side-channel attacks (SCA) went deep into the complex state of cryptography vulnerabilities, explaining the diverse array of forms, subtypes, and obstacles presented by these devious security breaches. The well-structured categorization scheme offered functions as a valuable reference for scholars and professionals. The research on how we assess cryptographic systems' resilience to side-channel attacks has revealed the various instruments and defenses employed. Future research directions are being discussed in order to further the ongoing discussion about strengthening the security of our digital systems against emerging cyber threats. This review informs us about the current state of side-channel attack research and motivates further efforts to strengthen cryptographic systems against the constantly evolving challenges of technology.

Referencess

1. A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," Sensors, vol. 22, no. 9, p. 3520, May 2022, doi: 10.3390/s22093520.
2. R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices," IEEE Commun. Surv.Tutor., vol. 20, no. 1, pp. 465–488, 2018, doi: 10.1109/COMST.2017.2779824.
3. A. Rehman, I. Razzak, and G. Xu, "Federated Learning for Privacy Preservation of Healthcare Data From Smartphone-Based Side-Channel Attacks," IEEE J. Biomed. Health Inform., vol. 27, no. 2, pp. 684–690, Feb. 2023, doi: 10.1109/JBHI.2022.3171852.
4. S. Kaur, B. Singh, and H. Kaur, "Stratification of Hardware Attacks: Side Channel Attacks and Fault Injection Techniques," SN Comput. Sci., vol. 2, no. 3, p. 183, May 2021, doi: 10.1007/s42979-021-00562-3.
5. Y. Yao, M. Yang, C. Patrick, B. Yuce, and P. Schaumont, "Fault-assisted side-channel analysis of masked implementations," in 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC: IEEE, Apr. 2018, pp. 57–64. doi: 10.1109/HST.2018.8383891.
6. K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens, "Plundervolt: Software-based Fault Injection Attacks against Intel SGX," in 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA: IEEE, May 2020, pp. 1466–1482. doi: 10.1109/SP40000.2020.00057.
7. Y. Bai, A. Stern, J. Park, M. Tehranipoor, and D. Forte, "RASCv2: Enabling Remote Access to Side-Channels for Mission Critical and IoT Systems," ACM Trans. Des. Autom.Electron. Syst., vol. 27, no. 6, pp. 1–25, Nov. 2022, doi: 10.1145/3524123.
8. Q. Pan, J. Wu, A. K. Bashir, J. Li, and J. Wu, "Side-Channel Fuzzy Analysis-Based AI Model Extraction Attack With Information-Theoretic Perspective in Intelligent IoT," IEEE Trans. Fuzzy Syst., vol. 30, no. 11, pp. 4642–4656, Nov. 2022, doi: 10.1109/TFUZZ.2022.3172991.
9. Yiwei Zhang, Xinjian Zheng, and Bo Peng, "A side-channel attack countermeasure based on segmented modular exponent randomizing in RSA cryptosystem," in 2008 11th IEEE Singapore International Conference on Communication Systems, Guangzhou, China: IEEE, Nov. 2008, pp. 148–151. doi: 10.1109/ICCS.2008.4737161.
10. G. Kolheet al., "LOCK & ROLL: Deep-Learning Power Side-Channel Attack Mitigation Using Emerging Reconfigurable Devices and Logic Locking," 2022.
11. A. Ito, R. Ueno, and N. Homma, "On the Success Rate of Side-Channel Attacks on Masked Implementations: Information-Theoretical Bounds and Their Practical Usage," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles CA USA: ACM, Nov. 2022, pp. 1521–1535. doi: 10.1145/3548606.3560579.
12. Y. Koyanagi and T. Ukezono, "A Cost-Sensitive and Simple Masking Design for Side-Channels," in TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON), Chiang Mai, Thailand: IEEE, Oct. 2023, pp. 732–737. doi: 10.1109/TENCON58879.2023.10322358.
13. A. Dubey, R. Cammarota, V. Suresh, and A. Aysu, "Guarding Machine Learning Hardware Against Physical Side-channel Attacks," ACM J. Emerg. Technol. Comput. Syst., vol. 18, no. 3, pp. 1–31, Jul. 2022, doi: 10.1145/3465377.
14. H. Wang and E. Dubrova, "Tandem Deep Learning Side-Channel Attack on FPGA Implementation of AES," SN Comput. Sci., vol. 2, no. 5, p. 373, Sep. 2021, doi: 10.1007/s42979-021-00755-w.
15. M. Khan, M. Hatami, W. Zhao, and Y. Chen, "A Novel Trusted Hardware-based Scalable Security Framework for IoT Edge Devices," In Review, preprint, Oct. 2023. doi: 10.21203/rs.3.rs-3417345/v1.
16. Y. Zhang, C. Slocum, J. Chen, and N. Abu-Ghazaleh, "It's all in your head(set): Side-channel attacks on AR/VR systems".
17. J. Breier and X. Hou, "How Practical Are Fault Injection Attacks, Really?," IEEE Access, vol. 10, pp. 113122–113130, 2022, doi: 10.1109/ACCESS.2022.3217212.
18. L. Lavdas, M. T. Rahman, M. Tehranipoor, and N. Asadizanjani, "On Optical Attacks Making Logic Obfuscation Fragile," in 2020 IEEE International Test Conference in Asia (ITC-Asia), Taipei, Taiwan: IEEE, Sep. 2020, pp. 71–76. doi: 10.1109/ITC-Asia51099.2020.00024.
19. B. Hettwer, S. Gehrer, and T. Güneysu, "Applications of machine learning techniques in side-channel attacks: a survey," J. Cryptogr. Eng., vol. 10, no. 2, pp. 135–162, Jun. 2020, doi: 10.1007/s13389-019-00212-8.
20. Y. Guo, A. Zigerelli, Y. Zhang, and J. Yang, "Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks," in 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA: IEEE, May 2022, pp. 1458–1473. doi: 10.1109/SP46214.2022.9833692.

21. A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, "AlphaLogger: detecting motion-based side-channel attack using smartphone keystrokes," J. Ambient Intell. Humaniz.Comput., vol. 14, no. 5, pp. 4869–4882, May 2023, doi: 10.1007/s12652-020-01770-0.
22. M. Mushtaqet al., "WHISPER: A Tool for Run-Time Detection of Side-Channel Attacks," IEEE Access, vol. 8, pp. 83871–83900, 2020, doi: 10.1109/ACCESS.2020.2988370.
23. M. M. Ahmadi, L. Alrahis, O. Sinanoglu, and M. Shafique, "DNN-Alias: Deep Neural Network Protection Against Side-Channel Attacks via Layer Balancing." arXiv, Mar. 12, 2023. Accessed: Jan. 09, 2024.[Online]. Available: http://arxiv.org/abs/2303.06746
24. M. Méndez Real and R. Salvador, "Physical Side-Channel Attacks on Embedded Neural Networks: A Survey," Appl. Sci., vol. 11, no. 15, p. 6790, Jul. 2021, doi: 10.3390/app11156790.
25. S. Chowdhury, A. Covic, R. Y. Acharya, S. Dupee, F. Ganji, and D. Forte, "Physical Security in the Post-quantum Era: A Survey on Side-channel Analysis, Random Number Generators, and Physically Unclonable Functions." arXiv, Feb. 08, 2021. Accessed: Jan. 15, 2024.[Online]. Available: http://arxiv.org/abs/2005.04344
26. U. Gulen and S. Baktir, "Side-Channel Resistant 2048-Bit RSA Implementation for Wireless Sensor Networks and Internet of Things," IEEE Access, vol. 11, pp. 39531–39543, 2023, doi: 10.1109/ACCESS.2023.3268642.
27. D. Lightbody, D.-M. Ngo, A. Temko, C. C. Murphy, and E. Popovici, "Attacks on IoT: Side-Channel Power Acquisition Framework for Intrusion Detection," Future Internet, vol. 15, no. 5, p. 187, May 2023, doi: 10.3390/fi15050187.
28. R. F. Olanrewaju, B. U. I. Khan, M. L. M. Kiah, N. A. Abdullah, and K. W. Goh, "Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT," Electronics, vol. 11, no. 23, p. 3982, Dec. 2022, doi: 10.3390/electronics11233982.
29. Z. Chen, G. Vasilakis, K. Murdock, E. Dean, D. Oswald, and F. D. Garcia, "VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface".
30. Q. Xu, M. T. Arafin, and G. Qu, "Security of Neural Networks from Hardware Perspective: A Survey and Beyond," in Proceedings of the 26th Asia and South Pacific Design Automation Conference, Tokyo Japan: ACM, Jan. 2021, pp. 449–454. doi: 10.1145/3394885.3431639.
31. Y. Wang, R. Paccagnella, E. T. He, H. Shacham, C. W. Fletcher, and D. Kohlbrenner, "Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86," IEEE Micro, vol. 43, no. 4, pp. 19–27, Jul. 2023, doi: 10.1109/MM.2023.3274619.
32. C. Liu, A. Chakraborty, N. Chawla, and N. Roggel, "Frequency Throttling Side-Channel Attack," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles CA USA: ACM, Nov. 2022, pp. 1977–1991. doi: 10.1145/3548606.3560682.