ISSN 2007-9737

A Look at Side Channel Attacks on Post-quantum Cryptography

Kevin A. Delgado-Vargas[1], Cuauhtemoc Mancillas-López[2], Gina Gallegos-García[1,*]

[1] Instituto Politécnico Nacional,
Centro de Investigación en Computación, Mexico City,
Mexico

[2] Instituto Politécnico Nacional,
Centro de Investigación y de Estudios Avanzados, Mexico City,
Mexico

{kdelgadov2019, ggallegos}@cic.ipn.mx, cuauhtemoc.mancillas@cinvestav.mx

Abstract. Post-quantum cryptography (PQC) is designed to be secure against attacks from quantum computers, yet it remains vulnerable to classic side-channel attacks (SCAs), which exploit physical implementation leaks. This manuscript examines the various SCAs used to evaluate PQC schemes, focusing on non-invasive techniques such as timing, power, and electromagnetic analysis. We provide a detailed account of the execution of these attacks against diverse PQC algorithms and identify common vulnerabilities and weaknesses. Our study reveals that, while various countermeasures have been proposed to protect PQC implementations, they are not entirely effective against sophisticated attacks. Stronger and more resilient countermeasures are needed, especially in IoT environments. The review highlights the weaknesses in the current defenses, including the necessity for more robust masking techniques, adequate security countermeasures tailored to IoT constraints, and methods to generalize SCAs across diverse hardware platforms. These issues must be addressed to enhance the practical security of PQC schemes in real-world scenarios.

Keywords. Post-quantum cryptography (PQC), side-channel attacks (SCAs), countermeasures, non-invasive attacks.

1 Introduction

Analyzing a cryptographic primitive can be viewed from two distinct perspectives. On the one hand, it can be viewed as an abstract mathematical entity or a black box (i.e., a transformation, possibly parameterized by a key that transforms an input into an output), commonly called ”classical cryptanalysis”.

On the other hand, this primitive must be implemented in a program that will run on a specific processor in a specific environment and, therefore, will present specific characteristics. In this case, we talk about *physical security* [48].

Physical attacks take advantage of the physical vulnerabilities generated in the implemented primitive on the devices to recover the used secret key. These kinds of physical attacks are called Side-Channel Attacks (SCA). SCA tends to be less general, i.e., the attack depends entirely on the implementation’s characteristics.

Physical security concerns the development of measures to meet the needs of the cryptographic primitives in practice. The measures must reduce the gap between the characteristics of an implemented cryptographic primitive and what is assumed about it [57]. The executions of the cryptographic implementations were assumed to be secure until numerous attacks refuted this. This made the developers focus on researching how to ensure the implementation minimizes side-channel leakages, which led to an understanding of

the mathematical algorithms employed in the side-channel analysis.

Compared to cryptographic attacks, SCA can observe and analyze the internal physical quantities for the key (or other secret quantities) extraction [53]. SCA is performed in two steps. First, the physical leakage of each query performed on cryptographic implementations is turned into probability and score vectors. With this information, the key extraction can be performed. The second step is to sort the information and search over every individual key until the entire key is completed and extracted [84].

2 Side Channel Attacks

SCAs can be conducted by analyzing one of the many physical leak devices produced while executing cryptographic schemes. These leaks represent a vulnerability that an attacker can exploit to analyze and break the security of cryptographic algorithms [69]. SCA on embedded devices first appeared in 1996 with a Timing Attack [47]. In this, the secret key is assumed to be correlated to the time fluctuations of the executions of a secure algorithm.

Applying a statistical analysis, it may be possible to select the correct key. In 1999, another side-channel attack based on the device's power consumption came up [46]. We can classify the type of attack depending on what the adversary can do with the device. On one hand, the active attacks may change the conditions under which the device used to work.

On the other hand, the passive attacks only observe the physical leakage of the device. It is said that these are more dangerous kinds of attacks because they leave no damage to the device that can be detected later on. These attacks exploit the fact that the device itself leaks physical information while performing the related operations to the secret information of the cryptographic algorithm, which can be measured externally [69]. Similar to the previous classification, SCAs can be categorized based on the characteristics of the attack to be executed and its potential invasiveness for the device.

This classification can be divided into invasive, semi-invasive, and non-invasive attacks. Each of them is dependent on how the attacker obtains information from the device or how the attack is performed. Invasive attacks focus on destroying the physical packaging of the integrated circuit while it maintains its functionality.

Usually, they involve accessing the silicon to observe, manipulate, and interfere with the system internals. Semi-invasive attacks require depackage, but unlike invasive attacks, they do not require direct electrical contact with a chip surface. In this kind, the attacker can perform photonic analysis, optical contactless probing, or laser stimulation [91, 92, 55] or even induce faults in the device.

Non-invasive attacks do not require opening the device to perform the attack. However, the attacker must know the system and observe specific physical parameters produced by the device while the algorithm runs. The main purpose of non-invasive attacks is to determine the secret key of a cryptographic device by measuring its execution time, power consumption, or electromagnetic field.

Since the beginning of this century, SCA has been studied, primarily in modern cryptography, with the RSA scheme or the standard AES. However, with the emergence of the quantum computer and Grover and Shor's algorithms, the physical security of modern cryptography is at risk, and the main problem is where its security relies.

Due to this, post-quantum cryptography has emerged as a safer alternative to these algorithms and quantum computing. In 2016, the National Institute of Standards and Technology (NIST) initiated a standardization process to standardize one or more quantum-resistant schemes. One of the main factors in this process is the resistance to SCA. Figure 1 provides a representation of the classification of non-invasive SCA in modern cryptography, with a taxonomy based on the work in [21]. It also shows the attacks reported to focus on post-quantum cryptography. These attacks are in the white boxes.

3 Non-invasive Attacks

So many studies exist in every classification, invasive, semi-invasive, and non-invasive attack, as seen in Section 2. In this work, we focus on the physical no-invasive classification. As we discussed before, non-invasive attacks are mainly those where we can only observe the device's behavior while it is working with the algorithm.

Those attacks are timing analysis, power analysis, electromagnetic emission analysis, fault analysis, and, in rare cases, light analysis and acoustics analysis.

The power analysis (PA), analyses the power traces measured over time. These traces are related to the computation of the algorithm since each operation of it has its power signature [36]. Depending on the way that the power traces are analyzed, it can be a Simple Power Analysis (SPA), Differential Power Analysis (DPA), Correlation Power Analysis (CPA), or Template.

Electromagnetic emission attack (EMA), this technique is related to the PA, but the main difference is how the traces are acquired because of the different tools used. In this, the challenge is to recognize the data leakage.

In the **Timing Analysis (TA)**, the attacker analyzes the time the device takes to compute the algorithm's operations. The time required to perform each operation differs based on the input.

Fault analysis (FA), studies the computational errors that may or may not be provoked. This can be because of the device itself. However, faults can be induced too, which can make the device work incorrectly and the attacker observes the result of the execution and compares it with the correct behavior.

In this work, we mainly review only the non-invasive attacks described in this section due to their capability to be applied to modern cryptography and post-quantum cryptography.

4 Side Channel Attacks to Modern Cryptography

Our work is focused on noninvasive attacks. We first examine some of these attacks made on modern cryptography. Over the past 20 years, the non-invasive SCA has been investigated [53]. All the primary schemes and standards we routinely employ, such as RSA, AES, and DES, have been subjected to non-invasive SCA.

Numerous studies have examined the SCA methodology, which breaks the schemes. Figure 2 shows some examples of attacks on modern cryptography, sorted by type of attack related to the non-invasive SCA. All of them are executed on embedded devices, including but not limited to NFC and RFID tags, smart cards, FPGAs, and Android devices.

Table 1 represents all works based on the literature and their relationship to the specific SCA they perform. The initial column in the table pertains to the research cited in the literature, followed by the type of non-invasive attack. The attacks are categorized as TA, FA, and PA, further subdivided into SPA with the S, DPA with the D, CPA with the C, Template with the T, and finally EMA.

Beginning from left to right, as we established in the last section, in the **TA**, the attacker analyzes the time the device takes to compute the algorithm's operations. Depending on the target scheme to attack, RSA or AES, the attacks exploit some of the operations in the process [4, 101, 16].

In the RSA-CRT implementation, the target is the Montgomery multiplication process, and the Chinese Remainder Theorem is used for optimization [4]. In the case of the OpenSSL AES implementation, the attack focuses on the timing data generated by cache collisions; the attack is performed on various processors [16].

In **FA**, the errors may or may not be induced by the attacker. The main target schemes are HC-128, AES, and RSA [45, 60, 18]. The faults go from inducing random words in the inner cipher state to exploiting the fault to recover the internal state, modify the public modulus, and observe the resultant faults to get the private exponent.

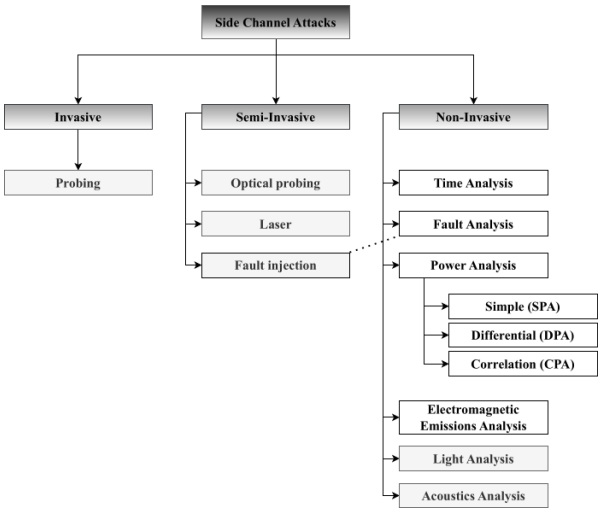

Fig. 1. Taxonomy of SCA to modern cryptography, the SCA to post-quantum cryptography is shown in the white boxes

PA are separated depending on the type and the way that the traces are analyzed, SPA [66, 1, 27], DPA [94, 15, 56, 96, 72], CPA [19, 14, 52], and Template [25, 67, 3, 30]. These attacks added to the schemes under study, the CLEFIA and Camelia ciphers, the Alternating Step Generator (ASG) cipher, and RC4, as well as the substitution blocks (SB). Here the attacker uses primarily chosen plaintext to exploit the produced leakage, while the encryption process is working, in this way, the attacker can deduce the key from the acquired traces.

The way that the **EMA** is performed is similar to the PA, but how the attacker can get the traces is the main difference because, in this case, a special probe is needed. A framework for side-channel attacks on stream ciphers was introduced in [50], which complemented previous work by Sim, Bhasin, and Jap.

This framework combines automated tools such as machine learning and mixed integer linear programming to achieve effective attacks on stream ciphers, including TRIVIUM. The framework supports noisy data and provides key recovery during initialization and when the cipher reaches its pseudo-random state. Most of the PA can also be done in EMA just by changing the traces, but some attacks only focus on the EM leakage [96, 10, 49, 37, 101, 30, 52]. Other attacks rely on the non-invasive attacks [85, 71, 29, 35, 64, 11, 58, 86, 38, 87]; in these, the authors focus on exploiting the cache-based attacks, providing theoretical models and some methodologies that can be used with the side-channel leakages, some models can be adapted depending on the leakage model and the noise distribution [35].

5 Side Channel Attacks to Post-quantum Cryptography

As in modern cryptography, SCA on post-quantum cryptography also has been a field of study. Both have received non-invasive attacks, mainly on embedded devices like ARM-based processors or FPGAs. However, in the post-quantum, the attacker must first find the function that will lead to retrieving the key from the leakage of the device.

Figure 3 shows some SC non-invasive attacks made to post-quantum cryptography and sorted by type of exploited leakage. Due to the NIST standardization process, the main schemes that have received attention are those participating. Figure 3 shows that each type has received many attacks.

Table 2 summarizes the attacks made to PQ schemes, where all are sorted by type of SCA. Beginning with the TA and ending with the EMA. In a few cases, the attack can be done using two techniques. However, the ✓ stands for the main SCA, and a – represents the SCA that can be applied with the same procedure.

TA: Some attacks done to post-quantum schemes can be seen in [90, 88, 82, 5, 89, 79, 24, 83, 23]. The TA has been done to some schemes. McEliece received a theoretical analysis in [90], where the time needed to perform the decryption is exploited on the degree of error locator polynomial algorithm.

This attack received further analysis in [88], where the private key is related to the error locator polynomial in the Patterson algorithm, and the time needed to perform the operations leaks information about the polynomials.

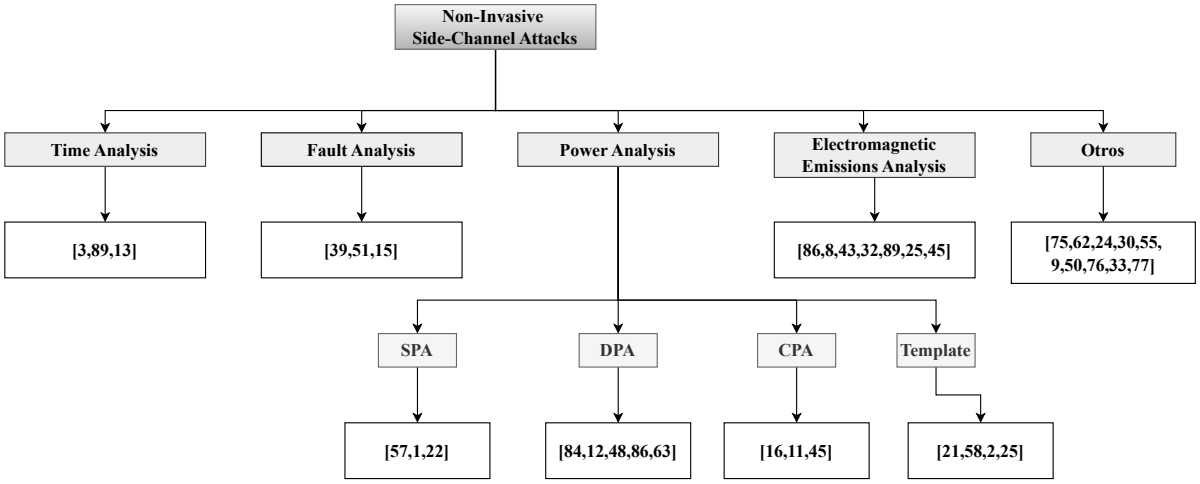

Fig. 2. Side channel attacks performed against modern cryptography schemes arranged according to the taxonomy shown in figure 1

This attack was expanded using the syndrome inversion with the previous leakage [89]. A few years later, this analysis was improved in [5]. The same attack in [23] attacked two schemes, LAC and Ramstake, where it is possible to distinguish between ciphertexts that produce errors before decoding due to the execution time of the ECC decoding algorithm.

FA: Even when the Code-based post-quantum algorithms are ”protected” by their error correction codes. Attackers find a way to induce some errors in the McEliece scheme that lead to the leak of information that gives an understanding of how the scheme works when the plaintext is corrupted [20].

UOV and Rainbow, two schemes of multivariable public key cryptography, received a theoretical analysis to recover partially the secret key [34]. In [73] it is demonstrated that lattice-based cryptography is vulnerable to FA. They showed that it is possible to exploit algorithmic properties in the Number-Theoretic Transform to construct chosen inputs. The presented attack was made against the Kyber and Dilithium schemes.

SPA: This attack is used mostly when the signal-to-noise ratio is high enough; else, DPA is a better option to make the attack [48].

There are so many works in the literature that do SPA like those seen in [36, 62, 68, 75, 81, 97, 41, 13]. Some implementations of McEliece have received this kind of SCA. An extraction of the secret key from the analysis of the Goppa polynomials is presented in [36]. Likewise in [62] XGCD algorithm used by the McEliece scheme is analyzed, resulting in the recovery of the ciphertext.

From NewHope and Frodo, it is possible to recover the secret key by choosing a ciphertext and performing the decryption. Then, by analyzing the performed operations related to the secret key, especially the modular addition, and if the addition is larger than the modulus it can lead to recovering the secret key [68]. HQC algorithm is analyzed in [75], specifically in the decoding of a vector during the decryption phase.

The main idea is to perform a chosen ciphertext attack to determine the parts of the secret key. Another attack over the same scheme is seen in [81], where a chosen-ciphertext attack is performed to exploit the decoding algorithm to retrieve a large part of the secret key through an oracle. Then, the remaining part is determined using an algorithm based on linear algebra. Even when Kyber is the winner scheme in the NIST standardization process, it has been the target

Table 1. Research on SCA to modern cryptography found in the literature. The works are related to the type of SCA. TA is for time analysis. FA for failure analysis. SPA for simple power analysis. DPA for differential power analysis. CPA for correlation power analysis. Temp for template power attacks. And EMA for analysis of electromagnetic emissions. SC indicates the cryptographic schemes that have been successfully targeted by the SCA

Work	TA	FA	PA				EM	SC
			S	D	C	T		
[4]	✓	×	×	×	×	×	×	RSA
[101]	✓	×	×	×	×	×	×	RSA
[16]	✓	×	×	×	×	×	×	AES
[45]	×	✓	×	×	×	×	×	HC-128
[60]	×	✓	×	×	×	×	×	RSA
[18]	×	✓	×	×	×	×	×	AES
[66]	×	×	✓	×	×	×	×	SB
[1]	×	×	✓	×	×	×	×	RC4
[27]	×	×	✓	×	×	×	×	RSA
[94]	×	×	×	✓	×	×	×	DES
[15]	×	×	×	✓	×	×	×	AES
[56]	×	×	×	✓	×	×	×	AES
[96]	×	×	×	✓	×	×	×	AES
[72]	×	×	×	✓	×	×	×	AES
[19]	×	×	×	×	✓	×	×	AES
[14]	×	×	×	×	✓	×	×	ChaCha20
[52]	×	×	×	×	✓	×	×	AES
[25]	×	×	×	×	×	✓	×	AES
[67]	×	×	×	×	×	✓	×	AES
[3]	×	×	×	×	×	✓	×	AES
[30]	×	×	×	×	×	✓	×	AES
[96]	×	×	×	×	×	×	✓	AES
[10]	×	×	×	×	×	×	✓	RSA
[49]	×	×	×	×	×	×	✓	AES
[37]	×	×	×	×	×	×	✓	AES
[101]	×	×	×	×	×	×	✓	RSA
[30]	×	×	×	×	×	×	✓	AES
[52]	×	×	×	×	×	×	✓	AES
[50]	×	×	×	×	×	×	✓	TRIVIUM

of some attacks and analyses. But it has also received some protection against SCA. There are some exploitable leakages like those presented in [97] where the attacker can recover the original message from masked message encoding, which leads to performing a chosen-chiphertext attack to recover the secret key using deep learning techniques.

It is possible to perform a SPA on post-quantum schemes like those mentioned before, that is why in [41] a platform to perform a PA based on Test Vector Leakage Assessment (TVLA) is developed. This platform works with both software and hardware implementations of the schemes.

In this way, the platform can show the leakage of the implementation on the obtained traces, which leads to identifying the specific source of the leakage. Further work on masked polynomial comparison for lattice-based cryptography is discussed in [13]. This study identifies critical weaknesses in two algorithms used to mask lattice-based schemes.

It demonstrates that the claimed security of these algorithms fails to hold up, even when faced with higher-order threats. The work proposes a framework to evaluate for information leakage during the re-encryption steps, thereby providing a practical approach to enhance the robustness of implementations against side-channel attacks.

DPA: Usually, to perform a DPA, the attacker selects an intermediate value; this is a function in which the secret key is related to some data the attacker knows. It also uses a model to predict power consumption, usually the Hamming Weight (HW) or the Hamming Distance (HD), depending on the implementation. Several studies from this kind of attack on the PQC can be seen in [70, 42, 7, 8, 76, 17, 44, 99].

In the case of McEliece in [70], the attack was on a bit permutation of the ciphertext, then the HW was applied to individual bits of the leakage. This way, the permutation matrix is recovered by applying a correlation analysis between the permuted ciphertext and each measurement.

The hash-based scheme, SPHINCS, received a theoretical partial secret key recovery [42]. The attack consists of finding a function related to the secret key and the known data, and then it is

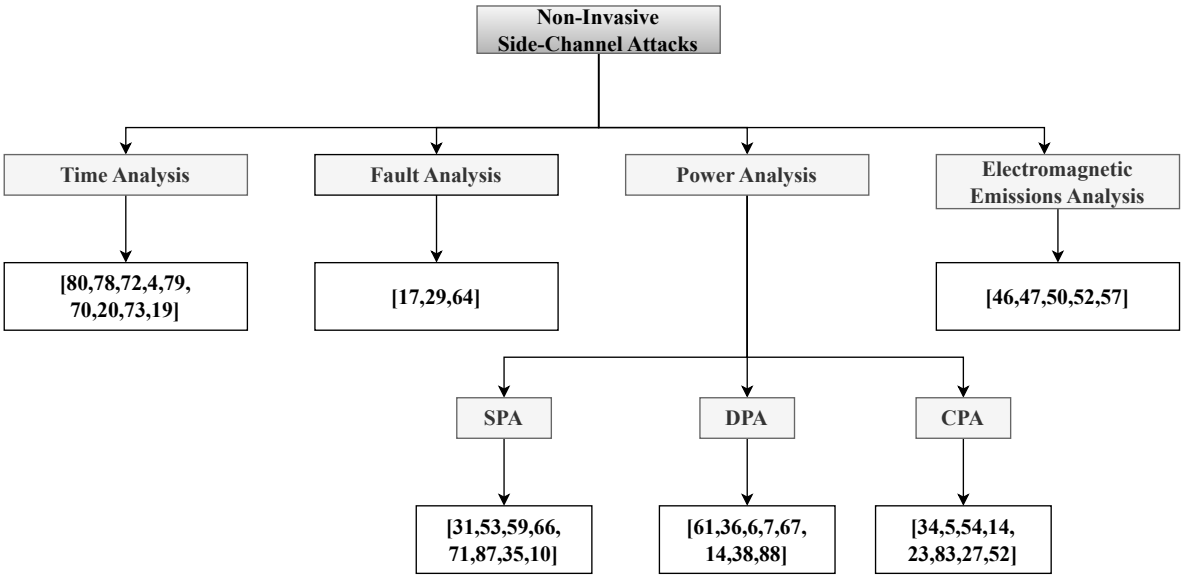

Fig. 3. Side channel attacks performed against post-quantum cryptography schemes arranged according to the taxonomy shown in figure 1

called twice in key and signature generations. This attack uses a simulated implementation. NewHope and Frodo, due to their similarities, a single attack works in both. The attack on them is in the intermediate states of matrix-polynomial multiplication related to the subkeys.

The attack observes the intermediate results and key bit a bit, and after this, it is possible to recover the full secret key with a 99% success rate [7]. Kyber was used to analyze the performance of the SC countermeasures by attacking the FO transform. But the countermeasures can also be applied to signature schemes like Dilithium and Falcon [8].

An attack on the polynomial multiplier in the signing function of Dilithium can retrieve a part of the secret key. Then, it is possible to forge signatures with the knowledge of the partial key. In the case of Dilithium, an attack on the polynomial multiplier used in the signing function could reveal part of the secret key, allowing forgery of signatures with partial key knowledge [76]. Furthermore, recent advances in side-channel analysis have led to numerous significant findings.

A comprehensive analysis of Dilithium's polynomial multiplication operations focused on DPA side-channel attacks. The study demonstrated that by profiling power traces and isolating polynomial coefficient multiplications, attackers were able to exploit these traces to recover the secret key successfully [17].

Using deep learning for side-channel attacks on lattice-based KEM such as Frodo and NewHope has demonstrated promising outcomes. This approach significantly exceeds traditional approaches, such as horizontal differential power analysis and template attacks [44].

The side-channel analysis conducted in [99] on the SIKE (Supersingular Isogeny Key Exchange) scheme has revealed weaknesses in ARM-based implementations. The analysis centered on developing efficient countermeasures to address these vulnerabilities, encompassing diverse attack techniques and mitigation strategies.

CPA: CPA is similar to DPA, but in this kind of attack, some other techniques are applied to perform a correlation analysis and retrieve the secret key like those seen in [39, 6, 63, 17, 28, 93, 32, 61].

Table 2. Research on SCA to post-quantum cryptography found in the literature (Part 1). The jobs are related to the type of SCA. TA is for time analysis. FA for failure analysis. SPA for simple power analysis. DPA for differential power analysis. CPA for correlation power analysis. And EMA for analysis of electromagnetic emissions. SC indicates the cryptographic schemes that have been successfully targeted by the SCA

Work	TA	FA	PA			EM	SC
			S	D	C		
[90]	✓	×	×	×	×	×	McEliece
[88]	✓	×	×	×	×	×	McEliece
[5]	✓	×	×	×	×	×	McEliece
[89]	✓	×	×	×	×	×	McEliece
[79]	✓	×	×	×	×	×	McEliece
[24]	✓	×	×	×	×	×	QC-MDPC
[83]	✓	×	×	×	×	×	ntruencrypt
[23]	✓	×	×	×	×	×	LAC, Ramstake
[20]	×	✓	×	×	×	×	McEliece
[34]	×	✓	×	×	×	×	UOV, Rainbow
[73]	×	✓	×	×	×	×	Kyber, Dilithium
[36]	×	×	✓	×	×	×	McEliece
[62]	×	×	✓	×	×	×	McEliece
[68]	×	×	✓	×	×	×	NewHope, Frodo
[75]	×	×	✓	×	–	×	HQC
[81]	×	×	✓	×	×	×	HQC
[97]	×	×	✓	×	×	×	Kyber
[41]	×	×	✓	×	×	×	Kyber
[13]	×	×	✓	×	×	×	NTRU
[70]	×	×	×	✓	×	×	McEliece
[42]	×	×	×	✓	×	×	SPHINCS
[7]	×	×	×	✓	×	×	NewHope, Frodo
[8]	×	×	×	✓	×	×	Falcon, Dilithium
[76]	×	×	×	✓	×	×	Dilithium
[17]	×	×	×	✓	×	×	Dilithium
[44]	×	×	×	✓	×	×	NewHope, Frodo
[99]	×	×	×	✓	×	–	SIKE
[39]	×	×	×	×	✓	×	NTRU
[6]	×	×	×	×	✓	×	NewHope, Frodo
[63]	×	×	×	×	✓	×	Kyber, Saber
[17]	×	×	×	–	✓	×	Dilithium
[28]	×	×	×	×	✓	×	Kyber
[93]	×	×	×	×	✓	×	Kyber
[32]	×	×	×	×	✓	×	Kyber
[61]	×	×	×	×	✓	×	Kyber
[78]	×	×	×	×	×	✓	Kyber, NTRU
[43]	×	×	×	×	×	✓	Falcon
[65]	×	×	×	–	×	✓	Kyber, NTRU
[95]	×	×	×	–	×	✓	Kyber, NTRU, ...
[31]	×	×	×	×	×	✓	HQC
[33]	×	×	×	×	×	✓	Kyber
[77]	×	×	×	×	×	✓	Kyber
[74]	×	×	×	×	×	✓	Kyber, NTRU

In the NTRU Prime scheme, the intermediate function selected is the multiplication of ciphertext and the secret key in the decryption phase. Then the HW is used to determine the expected power consumption and make the correlation with the measured power values [39].

Frodo and NewHope are shown to be vulnerable to CPA in [6]. With deep learning, they demonstrate that the attack can be generalized to noisy implementations with better results compared to classical techniques. NTRU, Kyber, and Saber have similarities, such as the Toom-Cook-based multiplication and the NTT.

These algorithms were selected as intermediate values in [63], using the HW to recover the secret key. The attack can be applied to other schemes that use polynomial multiplications.

Dilithium has been analyzed in its signature generation, specifically the polynomial multiplication operation used during the algorithm's sample rejection loop. This attack uses traces collected from a COTS-embedded device.

Kyber and Saber are analyzed through a multi-platform setup, with protected and unprotected implementations using the TVLA with an oscilloscope and the ChipWhisperer tool. The attack focuses on the inverse-NTT. Another example of attacks against Kyber is in [32], where the decapsulation phase is the intermediate value. However, in this case, the attack was unsuccessful.

An implementation of Kyber on ARM and RISC-V MCU received an attack in [61]. The attack requires less than 100 traces to recover the full key at the Montgomery reduction procedure.

Dilithium was investigated in [17], in the context of signature generation, specifically targeting polynomial multiplication during the sample rejection loop. Power traces collected from a Commercial Off-The-Shelf (COTS) embedded device were used in the attack.

In [28], the authors demonstrate the effectiveness of template-based attacks for recovering secret keys in the Kyber scheme. [93] explores the CPA attacks on the Kyber cryptographic algorithm by analyzing the inverse-NTT operation. The study examines the effectiveness of various power analysis techniques in unraveling the security of Kyber. The research evaluates different implementations to determine their vulnerability to CPA attacks.

EMA: The electromagnetic analysis (EMA) method is similar to power analysis (PA), but it collects traces differently. EMA analysis identified vulnerabilities in six cryptographic schemes participating in the standardization process. These vulnerabilities primarily pertain to the error-correcting procedures employed in these schemes and the Fujisaki-Okamoto transform (FO).

Specifically, the information leaked by these components in the output of the decryption algorithm can lead to the full recovery of the secret key [78]. For example, the Falcon scheme was studied and revealed that the Fast Fourier Transform (FFT) leaks less data than the Number Theoretic Transform (NTT) when subjected to EMA.

The analysis demonstrated that it is more straightforward to eliminate incorrect guesses using FFT than with NTT [43]. Furthermore, research has revealed that Saber and Kyber exhibit information leakage through EMA, which can be exploited by employing a multi-bit error-injection technique to retrieve the secret key [65]. Power/EM side-channel attacks have been elucidated in [95], affecting several post-quantum cryptographic schemes based on the FO transform using the MV-PC oracle with deep learning techniques. The re-encryption function was chosen as an intermediate value for all examined schemes. A new key recovery side-channel attack was proposed in [31], targeting the Hamming Quasi-Cyclic (HQC) code-based cryptosystem, a candidate in the NIST post-quantum standardization process.

This attack exploits the Reed-Muller decoding step in the decapsulation process, particularly the Hadamard transform, known for its diffusion property. The attack effectively uses side-channel information to construct an oracle that distinguishes between decoding patterns. It requires fewer than 20,000 electromagnetic traces to recover the entire static secret key.

In [33], research on CRYSTALS-Kyber revealed vulnerabilities in the polynomial multiplication between the secret key and ciphertext. To mitigate the detected leakages, the study suggested two masking countermeasures, additive and multiplicative. For example, multiplicative masking was introduced as a novel countermeasure for CRYSTALS-Kyber.

An analysis, in [77], of low-cost countermeasures such as ciphertext sanity checks and decapsulation failure checks revealed their vulnerability to chosen-ciphertext attacks. The secret key was retrieved from linear inequalities derived from side-channel leakage using an improved solver, demonstrating its superiority and simplicity over previous approaches.

Practical side channel and fault attacks targeting lattice-based cryptographic schemes are discussed in [74]. These attacks highlight the vulnerability of lattice-based cryptography to both side channel and fault attacks, highlighting the need for robust countermeasures.

6 Open Problems

Post-quantum cryptography (PQC) schemes are intended to safeguard information against quantum computer threats. However, they still encounter significant obstacles from classical side-channel attacks (SCAs). These challenges arise from information leakage through the physical implementation of cryptographic algorithms.

Addressing these issues requires understanding the limitations of current countermeasures, exploring specific vulnerabilities in Internet of Things (IoT) environments, and dealing with SCAs across diverse devices. The literature review showed that the secret keys can be retrieved if the leakage analysis is the right one. Due to this, there are some open problems like the ones listed next:

Countermeasures: To counteract the vulnerability of PQC schemes to SCAs, various techniques have been proposed, including masking and hiding [51, 9, 40, 12, 22]. Masking introduces random values to obscure sensitive data during computation, while hiding aims to reduce leakage visibility by adding noise or using complex data manipulation processes.

Nonetheless, these safeguards are not entirely impenetrable. Even with the use of some defenses, some studies prove that SCAs are still capable of compromising the secret keys. It is necessary to provide a detailed characterization of leakage patterns specific to PQC schemes.

Current models are often inadequate for predicting how different PQC algorithms leak information through various channels. Comprehensive models must be developed to better understand and analyze these leakage patterns. Their inherent resilience constrains the efficacy of masking and concealment techniques.

Research is required to develop more resilient masking techniques and identify scenarios where current techniques fail, enabling more robust defenses. Practical implementation issues frequently arise with theoretical countermeasures. Research into the impact of these measures on performance, usability, and integration is imperative for practical applications.

SCA on IoT: The rapid expansion of IoT devices presents various security challenges, especially when protecting these devices from SCAs. Because IoT devices are interconnected and have diverse applications, they are susceptible to various side-channel vulnerabilities [2, 54, 59]. Research conducted by [100, 2] highlights the significance of implementing effective security measures in this setting. Securing PQC implementations in IoT environments, which often have resource constraints and high connectivity, is challenging. The development of lightweight and efficacious countermeasures that are tailored to these constraints is an ongoing challenge. As new hardware and architectures for the Internet of Things emerge, SCAs must adapt to these changes.

Research is needed to develop effective attack techniques across evolving hardware platforms, including custom accelerators. A dearth of uniform frameworks exists for evaluating the security of PQC implementations in IoT settings. The development of consistent and comprehensive assessment frameworks would facilitate improved evaluation and comparison of countermeasures.

SCA on different devices: SCAs have been extensively studied concerning specific devices and operating systems. However, applying a single type of SCA across multiple devices with varying characteristics remains challenging. Research by [26, 98, 80] has extensively explored Side-Channel Attacks (SCAs) across various devices and operating systems.

Despite these studies, applying a single SCA type uniformly across devices with differing characteristics remains a significant challenge. [26] and [98] suggest that certain SCAs may be generalized. However, significant research is required to address several issues:

– Cross-Scheme Vulnerabilities:
  It is limited to understanding how vulnerabilities may be shared across different PQC schemes. Identifying common weaknesses and developing countermeasures that apply across various schemes to enhance overall security is essential.
– Cross-Device Attack Adaptation:
  Adapting SCAs to target a diverse range of devices without modifying the attack to cater to each device's distinct characteristics presents a challenge. Research is required to devise effective comprehensive attack strategies and countermeasures across various devices.
– New Device Categories:
  Emerging devices, such as wearable devices, present additional security challenges.

It is necessary to conduct extensive research to understand how SCAs can be applied to these new categories and to develop appropriate defenses.

7 Conclusion and Future Work

This paper provides a detailed account of the execution of side-channel attacks against diverse PQC algorithms. Our manuscript reveals that significant advancements have been made in developing PQC schemes, which are essential for protecting against the threat of quantum computers. However, these advances also present new challenges, requiring innovative physical security approaches.

Non-invasive attacks, which do not necessitate physical access to the device, are becoming increasingly sophisticated and efficacious in detecting potential leakage patterns. These advancements are crucial for safeguarding cryptographic systems in real-world applications where physical security may be challenging to maintain.

The intersection of PQC and SCAs presents a complex landscape that requires continued research and development. To ensure the security of post-quantum cryptographic systems, it is imperative to develop robust algorithms and implement effective defenses against side-channel attacks.

It is imperative to maintain a balanced focus on both the advancement of cryptographic techniques and the fortification of defenses against SCAs as we transition into a post-quantum era. This dual-focus approach will be essential for developing secure, reliable, and resilient cryptographic systems that deal with quantum and side-channel threats.

Future, it is proposed that side-channel attacks in post-quantum schemes and their applications in various cryptographic protocols utilized in multiple scenarios, such as medicine, be investigated.

Similarly, research on a security model that focuses on protecting implementations of post-quantum schemes considers the different vulnerabilities found in this work.

These models should consider side-channel resistance's theoretical and practical aspects, considering various attack vectors and implementation scenarios.

Acknowledgments

The authors thank CONAHCyT for funding this research under grants CONAHCYT 321068 and SIP 20240654. Cuauhtemoc Mancillas López thanks CYTED for funding this research under the project *NEW CRYPTO TOOLS - Nuevas herramientas criptográficas para la e-comunidad (522RT0131)*.

References

1. **Agrawal, D., Rao, J. R., Rohatgi, P. (2003).** Multi-channel attacks. Cryptographic Hardware and Embedded Systems - CHES 2003, Springer Berlin Heidelberg, pp. 2–16. DOI: 10.1007/978-3-540-45238-6_2.
2. **Ali, S., Hussain, M. M., Ali, F., Taimoor, S. (2023).** Mitigating side-channel attacks in the IoT ecosystem: A comprehensive review. ACM Computing Surveys, Vol. 56, No. 1, pp. 1–35.
3. **Archambeau, C., Peeters, E., Standaert, F. X., Quisquater, J. J. (2006).** Template attacks in principal subspaces. Cryptographic Hardware and Embedded Systems - CHES 2006, pp. 1–14. DOI: 10.1007/11894063_1.
4. **Arnaud, C., Fouque, P. A. (2013).** Timing attack against protected RSA-CRT implementation used in PolarSSL. Topics in Cryptology – CT-RSA 2013, Springer Berlin Heidelberg, pp. 18–33. DOI: 10.1007/978-3-642-36095-4_2.
5. **Avanzi, R., Hoerder, S., Page, D., Tunstall, M. (2011).** Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. Journal of Cryptographic Engineering, Vol. 1, pp. 271–281. DOI: 10.1007/s13389-011-0024-9.

6. **Aydin, F., Kashyap, P., Potluri, S., Franzon, P., Aysu, A. (2020).** DeePar-SCA: Breaking parallel architectures of lattice cryptography via learning based side-channel attacks. Embedded Computer Systems: Architectures, Modeling, and Simulation, pp. 262–280. DOI: 10.1007/978-3-030-60939-9_18.
7. **Aysu, A., Tobah, Y., Tiwari, M., Gerstlauer, A., Orshansky, M. (2018).** Horizontal side-channel vulnerabilities of post-quantum key exchange protocols. 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 81–88. DOI: 10.1109/HST.2018.8383894.
8. **Azouaoui, M., Kuzovkova, Y., Schneider, T., van-Vredendaal, C. (2022).** Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks. eprint.iacr.org/2022/916.
9. **Bangerter, E., Blom, R., Malkin, T., Tuchman, L. (2022).** Effective masking techniques for post-quantum cryptographic implementations. IEEE Transactions on Information Forensics and Security, Vol. 17, No. 4, pp. 945–957.
10. **Bauer, A., Jaulmes, E., Prouff, E., Wild, J. (2013).** Horizontal and vertical side-channel attacks against secure RSA implementations. Topics in Cryptology – CT-RSA 2013, pp. 1–17. DOI: 10.1007/978-3-642-36095-4_1.
11. **Becker, G. T., Kumar, R. (2014).** Active and passive side-channel attacks on delay based puf designs. eprint.iacr.org/2014/287.
12. **Bertoni, G., Daemen, J., Peeters, M., Assche, G. V. (2023).** Advancements and limitations of masking techniques in side-channel attack mitigation.
13. **Bhasin, S., D'Anvers, J. P., Heinz, D., Pöppelmann, T., Van Beirendonck, M. (2021).** Attacking and defending masked polynomial comparison for lattice-based cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2021, No. 3, pp. 334–359. DOI: 10.46586/tches.v2021.i3.334-359.
14. **Biryukov, A., Dinu, D., Le Corre, Y. (2017).** Side-channel attacks meet secure network protocols. Applied Cryptography and Network Security, Springer International Publishing, pp. 435–454. DOI: 10.1007/978-3-319-61204-1_22.
15. **Bogdanov, A. (2007).** Improved side-channel collision attacks on AES. Selected Areas in Cryptography, pp. 84–95. DOI: 10.1007/978-3-540-77360-3_6.
16. **Bonneau, J., Mironov, I. (2006).** Cache-collision timing attacks against AES. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 201–215. DOI: 10.1007/11894063_16.
17. **Bouvet, A., Guilley, S., Vlasak, L. (2021).** First-order side-channel leakage analysis of masked but asynchronous AES. Security and Privacy, Springer International Publishing, pp. 16–29. DOI: 10.1007/978-3-030-90553-8_2.
18. **Brier, E., Chevallier-Mames, B., Ciet, M., Clavier, C. (2006).** Why one should also secure RSA public key elements. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 324–338. DOI: 10.1007/11894063_26.
19. **Carlet, C., Heuser, A., Picek, S. (2017).** Trade-offs for S-Boxes: Cryptographic properties and side-channel resilience. Applied Cryptography and Network Security, Springer International Publishing, pp. 393–414. DOI: 10.1007/978-3-319-61204-1_20.
20. **Cayrel, P. L., Dusart, P. (2010).** McEliece/Niederreiter PKC: Sensitivity to fault injection. 2010 5th International Conference on Future Information Technology, pp. 1–6. DOI: 10.1109/FUTURETECH.2010.5482663.

21. **Chowdhury, S., Covic, A., Acharya, R. Y., Dupee, S., Ganji, F., Forte, D. (2020).** Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. Journal of Cryptographic Engineering, pp. 1–37. DOI: 10.1007/s13389-021-00255-w.

22. **Cohen, L., Daemen, J., Assche, G. V. (2023).** Practical challenges in deploying post-quantum cryptography countermeasures. IEEE Security & Privacy, Vol. 21, No. 3, pp. 52–61.

23. **D'Anvers, J. P., Tiepelt, M., Vercauteren, F., Verbauwhede, I. (2019).** Timing attacks on error correcting codes in post-quantum schemes. Proceedings of ACM Workshop on Theory of Implementation Security Workshop, Association for Computing Machinery, pp. 2–9. DOI: 10.1145/3338467.3358948.

24. **Eaton, E., Lequesne, M., Parent, A., Sendrier, N. (2018).** QC-MDPC: A timing attack and a CCA2 KEM. Post-Quantum Cryptography, Springer International Publishing, pp. 47–76. DOI: 10.1007/978-3-319-79063-3_3.

25. **Elaabid, M. A., Guilley, S. (2010).** Practical improvements of profiled side-channel attacks on a hardware crypto-accelerator. Progress in Cryptology – AFRICACRYPT 2010, Springer Berlin Heidelberg, pp. 243–260. DOI: 10.1007/978-3-642-12678-9_15.

26. **Foley, D., Korkishko, M., Scott, M. (2023).** Exploring side-channel attacks on emerging wearable devices. Journal of Hardware and Systems Security, Vol. 7, No. 1, pp. 57–72.

27. **Fouque, P. A., Kunz-Jacques, S., Martinet, G., Muller, F., Valette, F. (2006).** Power attack on small RSA public exponent. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 339–353. DOI: 10.

28. **Fournaris, A. P., Dimopoulos, C., Koufopavlou, O. (2020).** Profiling dilithium digital signature traces for correlation differential side channel attacks. Embedded Computer Systems: Architectures, Modeling, and Simulation, Springer International Publishing, pp. 281–294. DOI: 10.1007/978-3-030-60939-9_19.

29. **Genelle, L., Prouff, E., Quisquater, M. (2010).** Secure multiplicative masking of power functions. Applied Cryptography and Network Security, pp. 200–217. DOI: 10.1007/978-3-642-13708-2_13.

30. **Gierlichs, B., Lemke-Rust, K., Paar, C. (2006).** Templates vs. stochastic methods: A performance analysis for side channel cryptanalysis. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 15–29. DOI: 10.1007/11894063_2.

31. **Goy, G., Loiseau, A., Gaborit, P. (2022).** A new key recovery side-channel attack on HQC with chosen ciphertext. Post-Quantum Cryptography, Springer International Publishing, pp. 353–371. DOI: 10.1007/978-3-031-17234-2_17.

32. **Grünfeld, J. M. H. (2023).** Side-Channel Attacks on CRYSTALS Kyber: An analysis of a post-quantum algorithm and its vulnerabilities to sidechannel attacks. Master's thesis, NTNU.

33. **Hamoudi, M., Bel-Korchi, A., Guilley, S., Takarabt, S., Karray, K., Souissi, Y. (2021).** Side-channel analysis of CRYSTALS-Kyber and a novel low-cost countermeasure. Security and Privacy, Springer International Publishing, pp. 30–46. DOI: 10.1007/978-3-030-90553-8_3.

34. **Hashimoto, Y., Takagi, T., Sakurai, K. (2013).** General fault attacks on multivariate public key cryptosystems. Post-Quantum Cryptography: 4th International Workshop, PQCrypto, Vol. 96, No. 1, pp. 1–18.

35. **Heuser, A., Rioul, O., Guilley, S. (2014).** Good is not good enough.

Cryptographic Hardware and Embedded Systems – CHES 2014. Lecture Notes in Computer Science, Vol. 8731, pp. 55–74. DOI: 10.1007/978-3-662-44709-3_4.

36. **Heyse, S., Moradi, A., Paar, C. (2010).** Practical power analysis attacks on software implementations of McEliece. Post-Quantum Cryptography, Springer Berlin Heidelberg, pp. 108–125. DOI: 10.1007/978-3-642-12929-2_9.
37. **Homma, N., Hayashi, Y., Miura, N., Fujimoto, D., Tanaka, D., Nagata, M., Aoki, T. (2014).** EM attack is non-invasive? - design methodology and validity verification of EM attack sensor. Cryptographic Hardware and Embedded Systems-CHES 2014, Springer Berlin Heidelberg, pp. 1–16. DOI: 10.1007/978-3-662-44709-3_1.
38. **Homma, N., Nagashima, S., Imai, Y., Aoki, T., Satoh, A. (2006).** High-resolution side-channel attack using phase-based waveform matching. Cryptographic Hardware and Embedded Systems-CHES 2006, Springer Berlin Heidelberg, pp. 187–200. DOI: 10.1007/11894063_15.
39. **Huang, W. L., Chen, J. P., Yang, B. Y. (2019).** Power analysis on NTRU prime. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2020, No. 1, pp. 123–151. DOI: 10.13154/tches.v2020.i1.123-151.
40. **Hülsing, A., Cid, C. M., Gerbush, B. K. V., van-der-Meer, J. (2023).** Leakage models for post-quantum cryptographic algorithms. International Conference on Cryptographic Hardware and Embedded Systems (CHES).
41. **Kamucheka, T., Fahr, M., Teague, T., Nelson, A., Andrews, D., Huang, M. (2021).** Power-based side channel attack analysis on PQC algorithms. https://eprint.iacr.org/2021/1021.
42. **Kannwischer, M. J., Genêt, A., Butin, D., Krämer, J., Buchmann, J. (2018).** Differential power analysis of XMSS and SPHINCS. Constructive Side-Channel Analysis and Secure Design, Springer International Publishing, pp. 168–188. DOI: 10.1007/978-3-319-89641-0_10.
43. **Karabulut, E., Aysu, A. (2021).** FALCON down: Breaking FALCON post-quantum signature scheme through side-channel attacks. 2021 58th ACM/IEEE Design Automation Conference (DAC), pp. 691–696. DOI: 10.1109/DAC18074.2021.9586131.
44. **Kashyap, P., Aydin, F., Potluri, S., Franzon, P. D., Aysu, A. (2021).** 2Deep: Enhancing side-channel attacks on lattice-based key-exchange via 2-D deep learning. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 40, No. 6, pp. 1217–1229. DOI: 10.1109/TCAD.2020.3038701.
45. **Kircanski, A., Youssef, A. M. (2010).** Differential fault analysis of hc-128. Progress in Cryptology – AFRICACRYPT 2010, Springer Berlin Heidelberg, pp. 261–278.
46. **Kocher, P., Jaffe, J., Jun, B. (1999).** Differential power analysis. Advances in Cryptology-CRYPTO' 99, Springer Berlin Heidelberg, pp. 388–397.
47. **Kocher, P. C. (1996).** Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. Advances in Cryptology-CRYPTO '96, Springer Berlin Heidelberg, pp. 104–113. DOI: 10.1007/3-540-68697-5_9.
48. **Koeune, F., Standaert, F. X. (2005).** A tutorial on physical security and side-channel attacks. Springer Berlin Heidelberg, pp. 78–108. DOI: 10.1007/11554578_3.
49. **Korak, T., Plos, T. (2013).** Applying remote side-channel analysis attacks on a security-enabled NFC tag. Topics in Cryptology-CT-RSA 2013, Springer Berlin Heidelberg, pp. 207–222. DOI: 10.1007/978-3-642-36095-4_14.
50. **Kumar, S., Dasu, V., Baksi, A., Sarkar, S., Jap, D., Breier, J., Bhasin, S. (2022).** Side channel attack on stream

ciphers: A three-step approach to state/key recovery. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2022, No. 2, pp. 166–191. DOI: 10.46586/tches.v2022.i2.166-191.

51. **Kurtz, A., Liu, H. H., Moreno, F. V., Wu, L. Z. (2023).** Advanced countermeasures for side-channel attacks in post-quantum cryptography. Journal of Cryptography, Vol. 34, No. 2, pp. 205–228.

52. **Le, T. H., Clédière, J., Canovas, C., Robisson, B., Servière, C., Lacoume, J. L. (2006).** A proposition for correlation power analysis enhancement. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 174–186. DOI: 10.1007/11894063_14.

53. **Li, Y., Chen, M., Wang, J. (2016).** Introduction to side-channel attacks and fault attacks. Proceedings of the 2016 Asia-Pacific Microwave Conference (APMC), pp. 573–575. DOI: 10.1109/APEMC.2016.7522801.

54. **Liu, Y., Zhang, T., Chen, L. (2024).** Adaptation of side-channel attacks to emerging hardware platforms. IEEE Transactions on Computers.

55. **Lohrke, H., Tajik, S., Krachenfels, T., Boit, C., Seifert, J. P. (2018).** Key extraction using thermal laser stimulation: A case study on xilinx ultrascale FPGAs. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2018, No. 3, pp. 573–595. DOI: 10.13154/tches.v2018.i3.573-595.

56. **Lu, J., Pan, J., den-Hartog, J. (2010).** Principles on the security of AES against first and second-order differential power analysis. Applied Cryptography and Network Security, Springer Berlin Heidelberg, pp. 168–185.

57. **Maes, R. (2013).** Physically unclonable Functions: Constructions, properties and applications. Vol. 9783642413957. DOI: 10.1007/978-3-642-41395-7.

58. **Maghrebi, H. (2019).** Deep learning based side channel attacks in practice. https://eprint.iacr.org/2019/578.

59. **Martin, J., Lioy, A., Teixeira, J. (2024).** Standardized frameworks for security assessment of post-quantum cryptographic implementations. IEEE Transactions on Information Forensics and Security.

60. **Medwed, M., Standaert, F. X., Großschädl, J., Regazzoni, F. (2010).** Fresh re-keying: Security against side-channel and fault attacks for low-cost devices. Progress in Cryptology – AFRICACRYPT 2010, Springer Berlin Heidelberg, pp. 279–296.

61. **Meijer, J. (2023).** Towards future proof cryptographic implementations: Side-channel analysis on post-quantum key encapsulation mechanism CRYSTALS-kyber. Master's thesis, University of Twente.

62. **Molter, H. G., Stöttinger, M., Shoufan, A., Strenzke, F. (2011).** A simple power analysis attack on a McEliece cryptoprocessor. Journal of Cryptographic Engineering, Vol. 1, pp. 29–36. DOI: 10.1007/s13389-011-0001-3.

63. **Mujdei, C., Wouters, L., Karmakar, A., Beckers, A., Bermudo-Mera, J. M., Verbauwhede, I. (2024).** Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication. ACM Transactions on Embedded Computing Systems, Vol. 23, No. 2. DOI: 10.1145/3569420.

64. **Neve, M., Tiri, K. (2007).** On the complexity of side-channel attacks on AES-256 – methodology and quantitative results on cache attacks. eprint.iacr.org/2007/318.

65. **Ngo, K. (2023).** Side-channel analysis of post-quantum cryptographic algorithms. Ph.D. thesis, KTH Royal Institute of Technology.

66. **Novak, R. (2003).** Side-channel attack on substitution blocks. Applied Cryptography

and Network Security, pp. 307–318. DOI: 10.1007/978-3-540-45203-4_24.

67. **Oren, Y., Weisse, O., Wool, A. (2014).** A new framework for constraint-based probabilistic template side channel attacks. Cryptographic Hardware and Embedded Systems-CHES 2014, pp. 17–34. DOI: 10.1007/978-3-662-44709-3_2.
68. **Park, A., Han, D. G. (2016).** Chosen ciphertext simple power analysis on software 8-bit implementation of ring-LWE encryption. 2016 IEEE Asian Hardware-Oriented Security and Trust, pp. 1–6. DOI: 10.1109/AsianHOST.2016.7835555.
69. **Peeters, E. (2013).** Side-channel cryptanalysis: A brief survey. Springer New York, pp. 11–19. DOI: 10.1007/978-1-4614-6783-0_2.
70. **Petrvalsky, M., Richmond, T., Drutarovsky, M., Cayrel, P. L., Fischer, V. (2016).** Differential power analysis attack on the secure bit permutation in the McEliece cryptosystem. 2016 26th International Conference Radioelektronika, pp. 132–137. DOI: 10.1109/RADIOELEK.2016.7477382.
71. **Pietrzak, K. (2009).** A leakage-resilient mode of operation. Advances in Cryptology - EUROCRYPT 2009, Springer Berlin Heidelberg, pp. 462–482. DOI: 10.1007/978-3-642-01001-9_27.
72. **Prouff, E., Giraud, C., Aumônier, S. (2006).** Provably secure S-Box implementation based on fourier transform. Cryptographic Hardware and Embedded Systems - CHES 2006, pp. 216–230. DOI: 10.1007/11894063_17.
73. **Ravi, P. (2023).** Implementation attacks on post-quantum lattice-based cryptography. Doctoral thesis, Nanyang Technological University, Singapore.
74. **Ravi, P., Chattopadhyay, A., Bhasin, S. (2021).** Practical side-channel and fault attacks on lattice-based cryptography. 2021 IFIP/IEEE 29th International Conference on Very Large Scale Integration, pp. 1–2. DOI: 10.1109/VLSI-SoC53125.2021.9607000.
75. **Ravi, P., Jhanwar, M. P., Howe, J., Chattopadhyay, A., Bhasin, S. (2018).** Side-channel assisted existential forgery attack on dilithium - a nist pqc candidate. https://eprint.iacr.org/2018/821.
76. **Ravi, P., Jhanwar, M. P., Howe, J., Chattopadhyay, A., Bhasin, S. (2018).** Side-channel assisted existential forgery attack on dilithium - A NIST PQC candidate. eprint.iacr.org/2018/821.
77. **Ravi, P., Paiva, T., Jap, D., D'Anvers, J. P., Bhasin, S. (2024).** Defeating low-cost countermeasures against side-channel attacks in lattice-based encryption: A case study on crystals-kyber. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2024, No. 2, pp. 795–818. DOI: 10.46586/tches.v2024.i2.795-818.
78. **Ravi, P., Sinha Roy, S., Chattopadhyay, A., Bhasin, S. (2020).** Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2020, No. 3, pp. 307–335. DOI: 10.13154/tches.v2020.i3.307-335.
79. **Santini, P., Battaglioni, M., Chiaraluce, F., Baldi, M. (2019).** Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes. Code-Based Cryptography, Springer International Publishing, pp. 115–136. DOI: 10.1007/978-3-030-25922-8_7.
80. **Schaefer, C., Müller, T., Böhme, S. (2024).** Cross-scheme vulnerabilities in post-quantum cryptography: A survey. Journal of Computer Security.
81. **Schamberger, T., Renner, J., Sigl, G., Wachter-Zeh, A. (2021).** A power side-channel attack on the CCA2-Secure HQC KEM. Smart Card Research and Advanced Applications, pp. 119–134. DOI: 10.1007/978-3-030-68487-7_8.

82. **Shoufan, A., Strenzke, F., Molter, H. G., Stöttinger, M. (2010).** A timing attack against patterson algorithm in the McEliece PKC. Information, Security and Cryptology - ICISC 2009, pp. 161–175.

83. **Silverman, J. H., Whyte, W. (2006).** Timing attacks on NTRUEncrypt via variation in the number of hash calls. Topics in Cryptology - CT-RSA 2007, pp. 208–224. DOI: 10.1007/11967668_14.

84. **Standaert, F. X. (2010).** Introduction to Side-Channel Attacks. pp. 27–42. DOI: 10.1007/978-0-387-71829-3_2.

85. **Standaert, F. X., Malkin, T. G., Yung, M. (2009).** A unified framework for the analysis of side-channel key recovery attacks. Advances in Cryptology - EUROCRYPT 2009, pp. 443–461. DOI: 10.1007/978-3-642-01001-9_26.

86. **Standaert, F. X., Peeters, E., Archambeau, C., Quisquater, J. J. (2006).** Towards security limits in side-channel attacks. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 30–45. DOI: 10.1007/11894063_3.

87. **Stebila, D., Thériault, N. (2006).** Unified point addition formulæ and side-channel attacks. Cryptographic Hardware and Embedded Systems - CHES 2006, Springer Berlin Heidelberg, pp. 354–368. DOI: 10.1007/11894063_28.

88. **Strenzke, F. (2010).** A timing attack against the secret permutation in the McEliece PKC. Post-Quantum Cryptography, pp. 95–107. DOI: 10.1007/978-3-642-12929-2_8.

89. **Strenzke, F. (2011).** Timing attacks against the syndrome inversion in code-based cryptosystems. eprint.iacr.org/2011/683.

90. **Strenzke, F., Tews, E., Molter, H. G., Overbeck, R., Shoufan, A. (2008).** Side channels in the mceliece PKC. Post-Quantum Cryptography, pp. 216–229. DOI: 10.1007/978-3-540-88403-3_15.

91. **Tajik, S., Dietz, E., Frohmann, S., Dittrich, H., Nedospasov, D., Helfmeier, C., Seifert, J. P., Boit, C., Hübers, H. W. (2017).** Photonic side-channel analysis of arbiter pufs. Journal of Cryptology, Vol. 30, pp. 550–571. DOI: 10.1007/s00145-016-9228-6.

92. **Tajik, S., Lohrke, H., Seifert, J. P., Boit, C. (2017).** On the power of optical contactless probing: Attacking bitstream encryption of FPGAs. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1661–1674. DOI: 10.1145/3133956.3134039.

93. **Teague, T. (2022).** Side-channel analysis on post-quantum cryptography algorithms. Computer Science and Computer Engineering Undergraduate Honors Theses.

94. **Tu, C., Zhang, L., Liu, Z., Gao, N., Ma, Y. (2017).** A practical chosen message power analysis approach against ciphers with the key whitening layers. Applied Cryptography and Network Security, Springer International Publishing, pp. 415–434. DOI: 10.1007/978-3-319-61204-1_21.

95. **Ueno, R., Xagawa, K., Tanaka, Y., Ito, A., Takahashi, J., Homma, N. (2021).** Curse of re-encryption: A generic Power/EM analysis on post-quantum KEMs. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2022, No. 1, pp. 296–322. DOI: 10.46586/tches.v2022.i1.296-322.

96. **Veyrat-Charvillon, N., Standaert, F. X. (2010).** Adaptive chosen-message side-channel attacks. Applied Cryptography and Network Security, Springer Berlin Heidelberg, pp. 186–199.

97. **Wang, J., Cao, W., Chen, H., Li, H. (2022).** Practical side-channel attack on masked message encoding in latticed-based kem. eprint.iacr.org/2022/859.

98. **Wang, L., Zhang, Y., Liu, X. (2024).** Cross-device side-channel attack techniques: A survey. IEEE Transactions on

Dependable and Secure Computing, Vol. 21, No. 2, pp. 453–466.

99. Zhang, F., Yang, B., Dong, X., Guilley, S., Liu, Z., He, W., Zhang, F., Ren, K. (2020). Side-channel analysis and countermeasure design on ARM-Based quantum-resistant SIKE. IEEE Transactions on Computers, Vol. 69, No. 11, pp. 1681–1693. DOI: 10.1109/TC.2020.3020407.

100. Zhang, H., Wang, X., Chen, R. (2022). Securing IoT devices against side-channel attacks: Challenges and solutions. IEEE Internet of Things Journal, Vol. 9, No. 2, pp. 1245–1258.

101. Zhou, Y., Feng, D. (2005). Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing. eprint.iacr.org/2005/388.

Article received on 20/08/2024; accepted on 04/11/2024.
**Corresponding author is Gina Gallegos-García.*