Scientific Research Publishing

Journal of Information Security, 2023, 14, 227-249
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Hardware Security for IoT in the Quantum Era: Survey and Challenges

Doudou Dione*, Boly Seck, Idy Diop, Pierre-Louis Cayrel, Demba Faye, Ibrahima Gueye

IT Engineering Department, Cheikh Anta Diop University, Dakar, Senegal
Email: *doudou.dione@esp.sn

How to cite this paper: Dione, D., Seck, B., Diop, I., Cayrel, P.-L., Faye, D. and Gueye, I. (2023) Hardware Security for IoT in the Quantum Era: Survey and Challenges. *Journal of Information Security*, **14**, 227-249.
https://doi.org/10.4236/jis.2023.144014

Received: April 21, 2023
Accepted: August 5, 2023
Published: August 8, 2023

Abstract

The Internet of Things (IoT) has become a reality: Healthcare, smart cities, intelligent manufacturing, e-agriculture, real-time traffic controls, environment monitoring, camera security systems, etc. are developing services that rely on an IoT infrastructure. Thus, ensuring the security of devices during operation and information exchange becomes a fundamental requirement inherent in providing safe and reliable IoT services. NIST requires hardware implementations that are protected against SCAs for the lightweight cryptography standardization process. These attacks are powerful and non-invasive and rely on observing the physical properties of IoT hardware devices to obtain secret information. In this paper, we present a survey of research on hardware security for the IoT. In addition, the challenges of IoT in the quantum era with the first results of the NIST standardization process for post-quantum cryptography are discussed.

Keywords

IoT, Hardware Security, Side-Channel Attacks, Post-Quantum Cryptography, NIST

1. Introduction

The strong growth of the Internet of Things is facilitated by the availability of low-cost hardware. This hardware consists of routing, sensing, actuating, computing and other devices. These IoT devices handle tasks such as system activation, security, communication, object detection and specific actions. Whether in smart cities, modern agriculture, industry or even healthcare, the applications of the IoT are almost similar in their operation. First there is the object in the physical world, then the acquisition, processing and communication module. To take full advantage of all these potentialities, this technological revolution needs

to be secured in order to protect the sensitive data they store and exchange, particularly in the medical field [1]. Security schemes are nowadays applied in several embedded technologies such as the IoT which is a collection of hardware and software components. However, the hardware part became the target of several attacks that can affect an entire system, such as Side-Channel Attacks (SCAs), Fault Injection Attack (FIA), hardware Trojans, counterfeit chips and reverse engineering are all threats to hardware security in the IoT environment [2]. For example, a SCA can be carried out on the power consumption, the sound that the device can emit, or even on the electromagnetic (EM) emissions. Currently, these security threats are serious problems for IoT systems, which are increasingly present in our daily lives, especially in the medical field [3].

Sangodovin *et al.* [4] showed that information about IoT devices and FPGA modules can be collected from a distance of about 200 m outdoors through side channel EM signal leakage. They predict the received power of EM signals and determine the proximity ranges from which leakage from an IoT device can be monitored. Duan *et al.* [5] presented the flaws in the PRESENT ultralight algorithm by disclosing some of its vulnerabilities using SCA in resource-constrained devices such as IoTs. The identification of side-channel leakage based on synchronisation has been carried out by Prates *et al.*, revealing new vulnerabilities associated with response time [6]. Other attacks can be carried out during the IC manufacturing process. The latter can fall victim to a slight modification that can compromise the security of an entire system: this is the case of hardware Trojans as described Guo *et al.* in [7].

As a result of all these threats, it is important to focus on these attacks by identifying the technical challenges in order to propose countermeasures to defend against them.

Contribution:

We analyse the vulnerabilities of IoT systems to physical attacks, in order to find better approaches to security while taking into account the resource issues associated with IoTs. We also examine the challenges of quantum IoT systems and the NIST standardisation process for post-quantum cryptography.

Organization:

Section 2 is dedicated to IoT devices. Section 3 presents the most common hardware attacks in IoT. Section 4 analyses post-quantum IoT systems and cryptosystems. Section 5 reviews IoT security challenges and provides guidance for future research on hardware security in IoT. Finally, Section 6 is devoted to the conclusion.

2. Hardware in IoT

The IoT environment consists of software and hardware part that work together. The components such as communication media, microcontrollers, and sensors are connected via the internet in the IoT. The information is collected from the physical world through the sensors and then processed, analyzed, and stored either in the cloud or locally as shown in **Figure 1**.

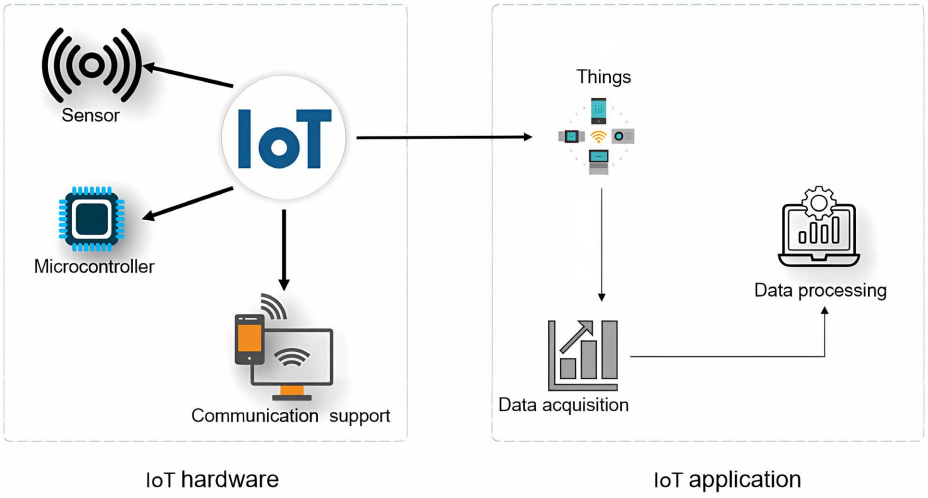


Figure 1. IoT system components.

The hardware sub-modules such as sensors, signal conditioning circuits and analog-to-digital converters are used to capture the often analog signal and transform it into a digital signal, but also to measure the time signal using time-to-digital converters. The actuators are used with signal conditioning circuits and digital to analog converters to convert the digital signal into analog provided by microprocessor [8]. The microcontroller is the main component of the IoT system. It is an integrated circuit, also called a microchip, which is dedicated to the execution of a single task.

To ensure security in IoT devices, it is essential to guarantee the reliability of the chips (SoC). These SoCs are widely used in IoT technology [9]. Indeed, chips are the target to many security threats in the IoT due to their manufacturing process. Hardware Trojans and reverse engineering are among the threats that can affect the security of these chips. For example, a hardware Trojan is a type of hardware threat that modifies the original system, the attacker may add an extra circuit or gate. These types of threats are difficult to detect because they are in hibernation most of the time and are activated by rare events that may occur inside the system.

From the design to the application of integrated circuits, several parties are involved in this process, ranging from the semiconductor manufacturer to the end user, the SoC designer, the intellectual property vendor and the EDA tool vendor [10]. Printed circuit boards, also known as PCBs, consist of microchips, transistors, diodes, resistors, capacitors, and inductors, etc. In each part of this process, an attack can be implemented, for example, a hardware Trojan inserted in the semiconductor manufacturing by acting on the transistors by changing the polarity of the dopants or on the RTL manipulation. Some can increase the power consumption of the circuit, such as the counter-based Trojan. Others can increase the overall temperature of the system and can cause premature aging, as in the case of an FPGA. In general, Trojans are designed to leak information such as secret keys [11].

3. Hardware Attacks on IoT Devices

IoT devices increasingly contain dense systems-on-chip (SoC) with high-frequency multicore processors and complex pipelines. As a result, sophisticated security mechanisms must be developed to protect SoCs while executing secret data, such as full disk and file encryption. Unfortunately, researchers and hardware developers in the IoT space primarily focus on designs that have low latency and require fewer hardware resources. As a result, their implementations often lack techniques to protect against various hardware attacks. These attacks exploit physical vulnerabilities in the hardware implementation rather than flaws in the mathematical structure of the cryptographic algorithm.

3.1. Fault Injection Attacks

The FIAs are active attacks that directly impact IoT hardware devices to recover cryptographic keys and other secret data or access restricted code areas and functions. This causes abnormal behavior at the software level, which the attacker can exploit for various purposes. These include obtaining personal information, bypassing a security check, and illegally accessing and controlling the system. FIAs have a long history and have been analysed in detail in the literature, especially for smart cards and other embedded MCUs [12]-[17].

The FIAs are divided into two categories: transient and permanent, and invasive and non-invasive. Transient faults are temporary faults that can be recovered after a system reset or shutdown of the fault source. Permanent faults, on the other hand, change the state of the target components indefinitely, with the effects persisting even after a reboot or reset of the device. Clock glitches, voltage glitches, and electromagnetic fault injections (EMFIs) are examples of non-invasive transient FIAs, and laser fault injections and ion-based fault injections are invasive FIAs.

3.1.1. Invasive FIAs

The invasive FIAs involve a major modification of DUT, whether during the preparation or execution of an attack. Preparation techniques include removing protective layers in the SoC or IC, called decapsulation, to directly induce faults in the internal components. These processes may cause irreparable damage or destruction of the target under evaluation, which could lead to permanent data loss.

Laser FIAs

Optical FIA [18] used a torch to induce faults in a microcontroller. However, this technique proved ineffective. Another technique of optical fault attacks using laser is adopted due to its effectiveness. Laser FIA systems disrupt integrated circuits. These attack techniques use a laser source, connected to a microscope. Thus the laser beam is fixed on the local tissue of the chip or circuit by approaching it from the front or from the back [19] [20]. However, physical countermeasures can be made on both sides which can make these attacks difficult to

implement. Nevertheless, there are ways of circumventing them, as proposed in [21]. Here, the authors presented a variant of laser-based attacks by attacking from the side of the chip and focusing the beam on this area. This provided another angle of attack. However, their technique shows that more energy is needed on the sides than on the faces for a faulty execution. This energy difference can be explained by the attack distance. Kathrin *et al.* [22] proposed a temporary laser FIA on flash memory. Their method allowed to adjust some laser parameters in order to obtain faults on the microcontroller. The authors [23] used laser beam injection to assess vulnerabilities in machine learning or deep learning based implementations for embedded system security. The work of Olivier *et al.* [24] demonstrated three vulnerabilities on a secure ATECC608B circuit, widely used in Internet of Things devices. This attack allows to retrieve secret masking keys from the EEPROM but also to disable the access to the memories by using a long laser pulse.

Ion-based FIAs

These types of attacks are very expensive and require extensive knowledge. Carlton *et al.* in [25], state that there are no known attacks against mobile SoCs using ions. However, other ion-based FIAs have been successfully carried out. For example, in [26], Li *et al.* succeeded in exploiting flaws in an RSA implementation on an FPGA board that allowed them to recover the key.

3.1.2. Non-Invasive FIAs

Non-invasive attack techniques are among the most widely used due to their ease of implementation with little financial resources. Therefore, these attacks are a serious threat to easily accessible IoT devices. The attacker uses environmental parameters, such as voltage or clock, to cause faulty behaviour that can lead to erroneous calculations. The attacker can take advantage of these faults to extract secret information [17].

Clock glitches

This is one of the most commonly used methods, due to its simplicity. In this type of attack, the attacker generates problems in the device's clock, which can cause desynchronization in the device. In the clock signal, an extra edge is produced at the output [27] as shown in **Figure 2**.

Unlike some attacks like laser fault injection, clock glitching does not destroy the device and is very effective for cryptographic implementations especially in IoT devices. The authors [29] proposed a clock glitching scheme on an AES implementation. Using an external clock generator, they found an appropriate frequency of clock glitching. Thus, their method succeeded in recovering the secret key with six faulty chiphertext. But first the right frequency has to be found. Another low cost and open method, called HackMyMCU Framework is proposed by *et al.* [30] which is an extension of [31] that targets clock glitching and electromagnetic attacks. Both modules of the clock fault injection system are evaluated on a microcontroller that runs the AES AddroundKey operation showing that the types of attacks can induce specific faults.

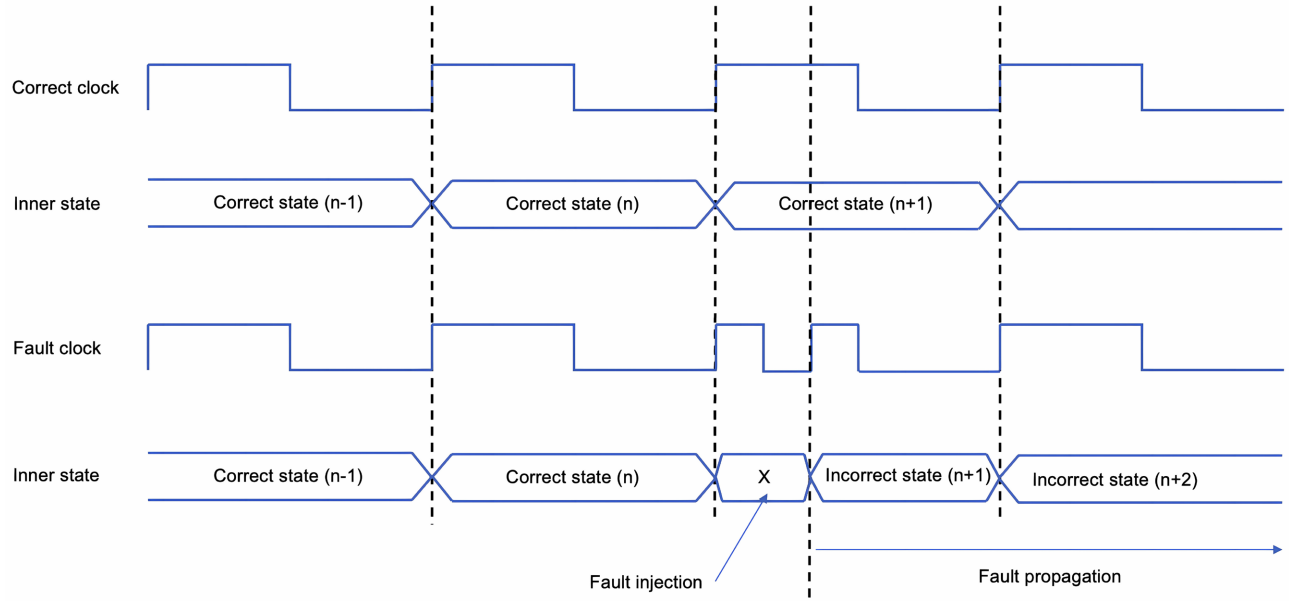


Figure 2. Clock glitch and fault injection representation [28].

Voltage glitches

The attacker tries to disrupt the normal execution cycle by acting on the supply voltage of a device. Injecting a high voltage on the device's power supply at a specific time during its operation can compromise the safety parameters of the entire system. This is helped by the fact that voltage regulators cannot filter out all input faults and noise, which is often the cause of voltage fault attacks [32]. The authors of [33] studied the effect of these attacks on the D flip flop (DFF) of a CMOS-based circuit. They proved that negative voltage glitch fault injections are due to timing constraints because the power supply cannot induce faults on the DFFs.

The attack may be positive or negative, as in the figure below, depending on the supply voltage Vdd and the circuit will give a faulty output. This causes some instructions to jump during the execution of the code, leading to the recovery of the secret key as shown in **Figure 3**.

To protect against these types of attacks, Rafid Muttaki *et al.* [35] proposed a universal fault detection sensor that can detect invasive and non-invasive FIAs such as voltage glitching.

Electromagnetic fault injection (EMFIs)

FIAs differ from other attacks on IoT systems because they involve multiple layers of the system. The attack occurs at the physical layer of the IoT hardware devices but affects the operation of software components and programs at the other layers of the system. The types of software that can be affected by fault injection include device drivers, operating systems, and application software [36]. For example, the authors in [17] analyzed how FIAs are performed on cryptographic devices to trick the encryption algorithm by using a secret null key. The attacker can then use this null key to decrypt and steal sensitive data. These types

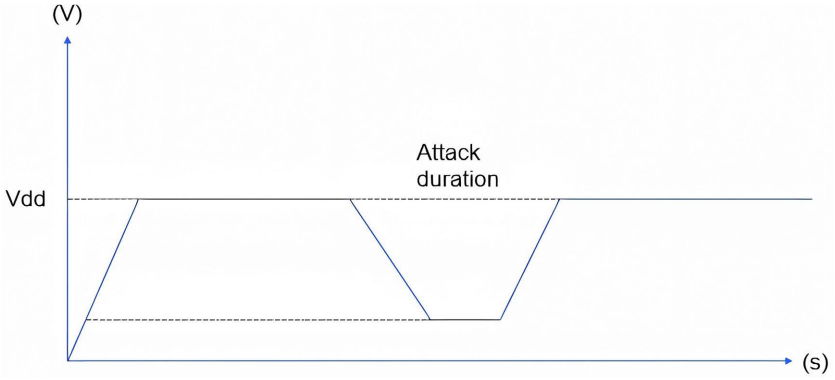


Figure 3. A negative supply voltage glitch attack model [34].

of attacks pose a significant threat to IoT devices because they are carried out at the physical layer and compromise the softwares at other layers. Work has shown the effectiveness of electromagnetic FIAs on IoT SoCs against an AES implementation [37]. The Thumb instruction set is commonly used for data processing in the arithmetic and logic unit of embedded systems and is the target of many FIAs. The single-bit or dual-bit fault model is a very powerful model that allows an attacker to perform efficient attacks [38]. While these can be performed using global fault injection techniques, such as under-powering [39], further analysis is required to filter out the exploitable faults. While it is possible to execute a one-bit error at an unselected position, it is much more complicated to target a bit specifically. Therefore, a more accurate fault injection technique is required. Laser fault injection is a well-suited method. As shown in [40], it is possible to inject a single-bit error into the data retrieved from the flash memory. This allows the instruction to be corrupted while it is being fetched, before it is executed by the processor. The corruption is temporary and affects only the fetched instruction. The contents of the flash memory are not affected. Thus, if the instruction is fetched again from flash memory without a laser fault injection, it will execute normally. This attack allowed authors Cayrel *et al.* to find the message in the encryption of a NIST finalist for standardization of post-quantum cryptography.

3.2. Side-Channel Attacks

The SCAs are first introduced by Kocher in [41]. These attacks represent one of the non-invasive passive attacks that are of great interest to researchers. The attackers attempt to exploit the timing, the power consumption, the electromagnetic radiation of the attacked IoT devices (see **Figure 4**). A non-invasive passive attack means that the attacker does not act directly on the target victim, unlike an invasive attack such as fault injection, making it difficult or nearly impossible to detect. It takes only a small amount of information per side channel to find the secret key.

3.2.1. Power Analysis

The integrated circuits are becoming more powerful and sophisticated. They

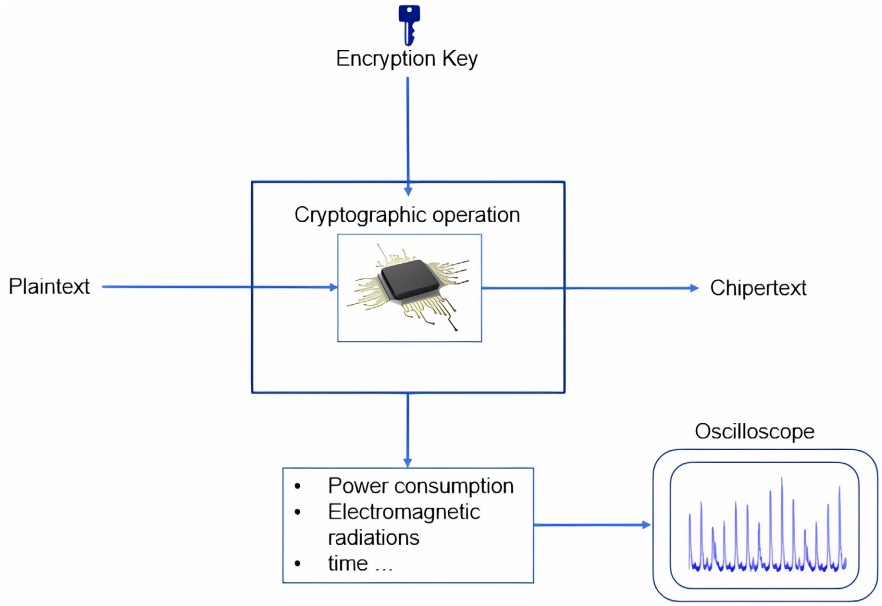
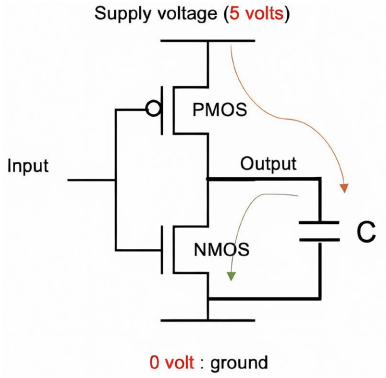


Figure 4. Side-channel attacks.

contain millions of transistors, mostly CMOS, which act as switches with high (1) and low (0) states, performing particular functions as shown in **Figure 5**. The voltage variations associated with the operations of these can be important elements in revealing information about the system in operation, by attempting to analyze the power measurements of the device. This attack technique, called power analysis, is a SCA. These power analysis attacks have been the subject of several studies due to their powerful nature. They are dominant in SCAs. There are three categories of power analysis attacks used.

Simple power analysis (or SPA): This attack uses power traces collected during the operations of cryptographic devices performing cryptographic functions. Analysis of these electrical signals for an IoT hardware device can provide a lot of information about the encryption code used [42] [43]. It is difficult in practice to retrieve the value of the key using only this technique. Nevertheless, it can help to know the running cryptographic algorithm.

Differential power analysis (or DPA): This is a much more powerful power analysis attack than the SPA. The DPA attack tries to identify differences in the power traces that can reveal the secret key [44]. Unlike SPA attack, DPA attack does not require detailed knowledge of the cryptographic device, but of the cryptographic algorithm executed by the device. In these types of attacks, everything depends on the power consumption data of the cryptographic device. Trace shifting is used to analyze the power consumption at a fixed time based on the data being processed [45]. Currently, most of the integrated circuits are based on CMOS technology. These CMOS transistors switch from high to low or from low to high. From these transitions, a correlation can be made between the current consumed by the circuit and the operations taking place within it. In other words, the power consumption during the calculation of the function is



Input	Output	Current
$0 \rightarrow 0$	$1 \rightarrow 1$	Low
$0 \rightarrow 1$	$1 \rightarrow 0$	Discharge
$1 \rightarrow 0$	$0 \rightarrow 1$	Charge
$1 \rightarrow 1$	$0 \rightarrow 0$	Low

Figure 5. Simplified schematic of a CMOS inverter and a transition table.

related to the secret key of the encryption algorithm. Published by Paul Kocher in 1999, the DPA is an attack known to be very effective in hardware implementations to recover the secret key. This attack has been applied to several encryption algorithms such as DES [44] or AES [38] which has replaced it and is now the most widely adopted global standard for data security. On the latter, the attack targets the first output of the S-Box (AddRoundKey and SubBytes). Indeed, for AES 128, the value of the encryption key is 128 bits and it would be impossible to test all the key values directly. However, each key can be divided into bytes, 16 per key. The DPA attack tries to resolve the bytes individually, which would constitute 256 possibilities or subkeys. So to recover the entire key, it takes 4096 attempts.

At the output of the S-Box, we have $y = SBox\left(k_n \oplus x_n\right)$ with d_i (LSB) a selection function to select a bit of *y*, k_n (256 subkeys) the estimated key ($n \in \{0,15\}$). The S-BOX is the fixed substitution table of 128-bit AES and x_n is the known input parameter as shown in **Figure 6**.

To find K_n, we proceed by key assumptions. The function d_i sorts the consumption traces ti of the plaintext and classifies them according to the value of the LSB (0 or 1) for example. This results in two groups P_0 and P_1 as shown in **Figure 7**. The difference of averages of each group is then computed using the Equation (1). In this case, the good hypothesis would correspond to a significant difference (most significant peak in the average traces). Otherwise, the hypothesis is wrong.

$$\Delta k = \frac{\sum_{i=1}^{n}\left(1-d_i\right)\cdot t_i\left(j\right)}{\sum_{i=1}^{n}\left(1-d_i\right)} - \frac{\sum_{i=1}^{n} d_i \cdot t_i\left(j\right)}{\sum_{i=1}^{n} d_i} \tag{1}$$

Correlation power analysis (or CPA)

The CPA is another SCA attack that is a variant of the DPA attack but even more powerful. This type of attack is increasingly used against hardware implementations and can directly target a byte of the encryption key. The CPA attack tries to match two variables, namely power and data (see **Figure 8**). Indeed, a strong correlation exists between power and the cryptographic algorithm in a

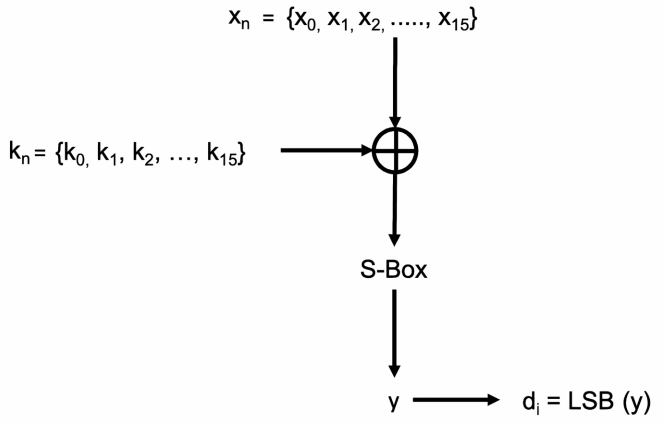


Figure 6. S-Box output.

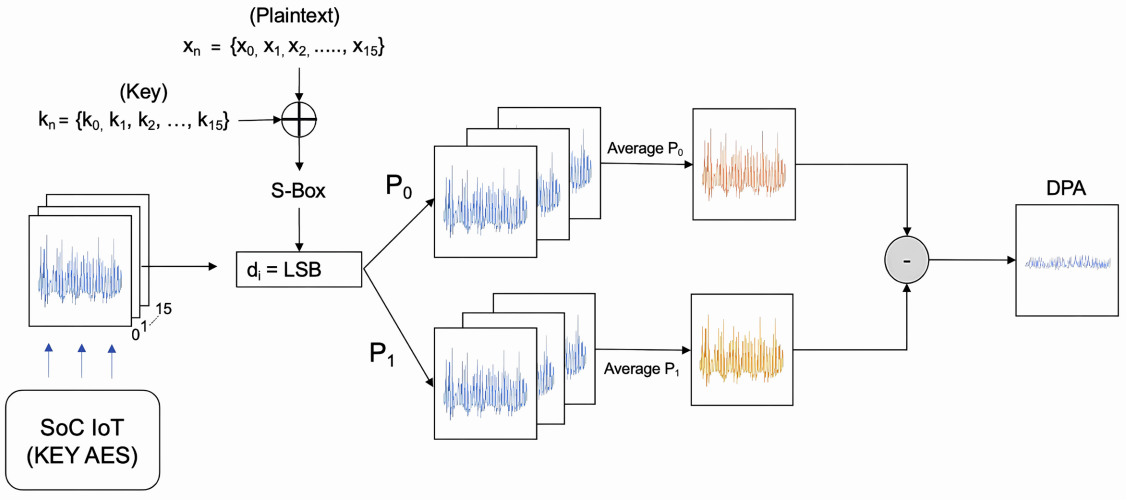


Figure 7. DPA attacks.

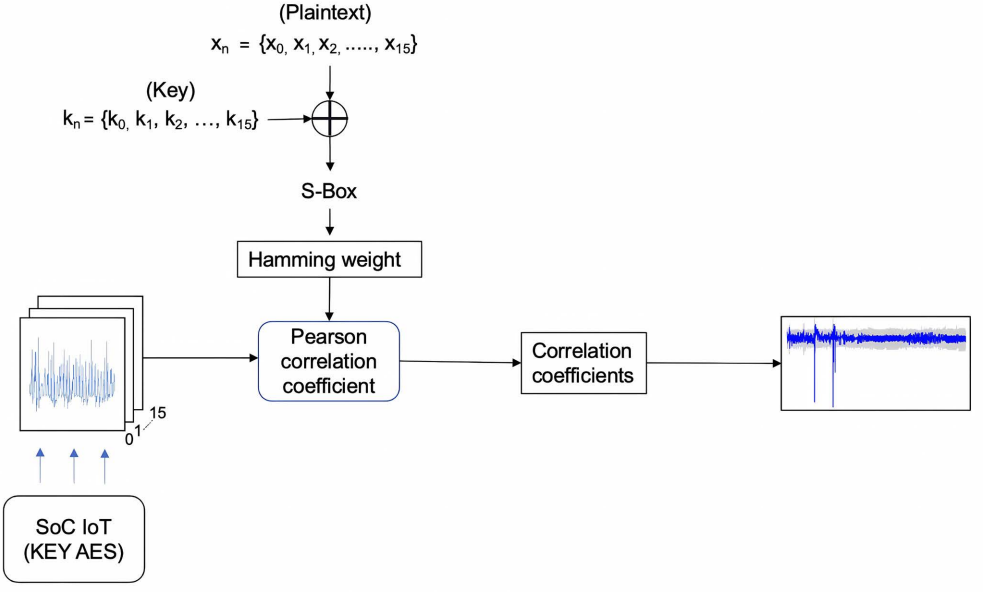


Figure 8. CPA attacks.

running device. In other words, the power consumption is proportional to the data (Hamming weight). Thus, finding a good correlation can help to recover all key values [46]. An empirical coefficient, also known as the Pearson coefficient ($r_{H,V}$) is used to calculate the correlation. This coefficient has the expression:

$$r_{H,V} = \frac{\sum_{i=1}^{N}\left(h_i - \overline{h}\right)\left(v_i - \overline{v}\right)}{\sqrt{\sum_{i=1}^{N}\left(h_i - \overline{h}\right)^2}\sqrt{\sum_{i=1}^{N}\left(v_i - \overline{v}\right)^2}} \tag{2}$$

with v_i and h_i the respective values of the consumption (voltage) at point i and the hamming weight. $\overline{v}$ and $\overline{h}$, their means and N the number of traces. Ba-Anh Dao *et al.* in [47] discussed a body of work on SCA with a focus on SoCs before conducting a CPA attack against an AES 128 implementation on an FPGA board. This same type of attack was carried out by the authors of [48] in 2012 to recover the final tower key RK24L.

Recently the rise of new technologies such as Machine Learning or Deep Learning, has opened the way to other types of attacks using fewer traces compared to the long-used statistical methods. This is illustrated by the work of [49] which uses the support vector machine (SVM) to predict the Hamming weight from power traces. Convolutional neural networks (CNNs) are also used in [50] [51] for SCAs. For example in [52], Zhe Wang *et al.* used Deep Learning on SM4 algorithms with and without protection implemented on an FPGA board. The results obtained, they claim, are significantly better compared to classical attacks such as DPA. Other algorithms are also being studied against SCAs such as Xboost, Random Forest, k-Nearest Neighbour, etc.

3.2.2. Electromagnetic Emission Analysis

This type of attack uses the measurement of electromagnetic waves emitted by operating integrated circuits. These EM waves are defined as synchronized oscillations of electric and magnetic fields that propagate at the speed of light through a vacuum [53]. Due to the difficulty of acquiring data from IoTs, the approach using side channels such as electromagnetic emissions was used. Observing or even acquiring electromagnetic emanations in an IoT device can allow an attacker to understand the relationship between it and the cryptographic algorithms. As demonstrated by Karin *et al.* in [54], electromagnetic attacks can be performed on IoT SoCs due to voltage fluctuations between the digital part and the analogue circuit. These electromagnetic attacks (EMA) are divided into two categories: electromagnetic analysis and differential electromagnetic analysis [55].

This part is only a preparation step consisting in obtaining information about the device in question. The attacker observes a trace of the electromagnetic signal of the device and knows its architecture or even the security scheme applied in order to hope to retrieve information about the encryption key based on the transitions at system start-up. This step is a starting point for further analysis

with other techniques such as DEMA.

Differential electromagnetic analysis (DEMA)

Work has shown the effectiveness of electromagnetic FIAs on IoT SoCs against an AES implementation. The authors of [56] used a DPA technique based on electromagnetic emissions to attack a Texas instruments ARM cortex-A8 SoC system with an AES 128 implementation. The authors succeeded in conducting an attack with only 10,000 traces for the SoC without a masking system. Other approaches such as deep learning are increasingly used against IoT SoCs to recover the AES key implemented in them through electromagnetic signals [57].

3.2.3. Timing Attacks

This type of attack exploits the time channel by measuring the time required to execute operations, either in real time from the clock or from the monotonically increasing counter [58]. The first work on the time attack was carried out by Tsunoo *et al.* [59], breaking a DES algorithm, thus opening up a new area of research on SCA. The temporal attack is often used against weak devices like smart cards or the Internet of Things. The author of [60] also used this type of attack against an AES implementation. The authors of [61] present timing attacks on a network-on-chip. They attack the communication between shared memory and an ARM cortex-A9 core.

3.3. SCA Countermeasures on SoC-IoT

Several research papers have proposed techniques for countermeasures of invasive and non-invasive hardware attacks. Techniques to make the processed data power independent for power analysis attacks (non-invasive attack) or even to make the metal protection layer of the chips more resistant (invasive attack) are proposed. Some of these techniques often consist of increasing the noise when data is processed and others can be included in the cryptographic module to monitor the supply voltage (voltage glitches) or even the clock frequency (clock glitches) in an attempt to stop operation if an attack is detected. Error-correcting codes are also used against FIAs in order to prevent the analysis of faulty outputs by suppressing the execution of the algorithm if an error is detected [62] [63] [64]. Xiaomin and proposed a masking method to attenuate the current difference by superimposing a metal-insulator-metal capacitor over the critical modules of the chip [65]. Their technique stands up well against DPA attacks. However, their work is limited to the critical modules of the chip.

In order to protect the information that may be contained in a signal captured from a device performing a cryptographic function, it is essential to put in place systems that can scramble the signal, making it difficult to process. Processing operations randomly in a processor is a good way of doing this. Both DPA and CPA are based on correlation, and signal desynchronisation can complicate these SCA-based attack methods.

4. Post-Quantum Cryptography in IoT

4.1. NIST PQC Standardization and Result

As mentioned in the previous sections, the IoT environment is resource constrained, which requires the implementation of lightweight cryptographic algorithms. Modern security protocols in most of our systems rely mainly on three basic cryptographic functions: Public Key Encryption (PKE), digital signature, and key establishment algorithm or Key Encapsulation Mechanism (KEM). Unfortunately, Shor has shown in [66] that there are quantum algorithms that can solve the difficult problems of integer factorization (currently RSA for signature) and discrete logarithm (Diffie-Hellman for key exchange) in polynomial time. Thus, the threat to the security protocols currently in use is real. For this reason, the NIST (National Institute of Standards and Technology) standardization process has been launched since 2017 to find replacements for these current systems. This has given a significant boost to research in post-quantum cryptography over the last five years.

The main goal of the process started in 2017 by NIST is to replace three standards that are considered the most vulnerable to quantum attacks, *i.e.*, FIPS 186-4[1] (for digital signatures), NIST SP 800-56A[2], and NIST SP 800-56B[3] (both for keys establishment in public-key cryptography). For the first round of this competition, 69 candidates met the minimum criteria and the requirements imposed by NIST. 26 out of 69 were announced on January 30, 2019, for moving to the second round. Of these, 17 are public-key encryption and/or key-establishment schemes and 9 are digital signature schemes. In July 2020, NIST started the third round of this process where only seven finalists were admitted (four PKE/KEM and three signature schemes). In addition to the finalists, eight alternate candidates were selected.

On July 5, 2022, NIST published the first four winning algorithms from this campaign to standardize post-quantum cryptographic algorithms. These future standards will be default options for selecting post-quantum algorithms in the majority of security products. These post-quantum algorithms will also be combined with proven classical algorithms through hybrid mechanisms. The first four algorithms selected are a key establishment algorithm named CRYSTALS-Kyber; and three digital signature algorithms named CRYSTALS-Dilithium, FALCON, and SPHINCS+. The first three of these algorithms are based on structured lattices; the last one, SPHINCS+ is a hash-based signature scheme. These four algorithms will therefore be used as the basis for writing U.S. federal standards. The scope of the NIST announcement is international with strong involvement of the cryptography research community, which will make the future US standards also used as de facto international industry standards. Beside the four winners, an extension of the NIST PQC standardization campaign (4th round) is planned for

[1]https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[2]https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf
[3]https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf

four key establishment algorithms: BIKE [67], HQC [68], *Classic McEliece* [69] (all three based on error-correcting codes), and SIKE [70] (isogeny graphs-based). *Classic McEliece* was the first selected finalist as a key encapsulation mechanism, while BIKE and HQC were alternative candidates. The latter two use special codes to reduce the size of the public key, which is considered the main drawback of code-based cryptosystems.

Recently, NIST issued a call for additional digital signature proposals for June 2023 to be considered in the PQC standards process. For certain applications, such as certificate transparency, NIST is now interested in signature schemes other than structured lattice that have short signatures and fast verification to diversify post-quantum signature standards. As such, any structured lattice-based signature proposal will need to significantly outperform CRYSTALS-Dilithium and FALCON in the relevant applications and/or guarantee substantial additional security properties to be considered for standardization.

The main question is how to use these new post-quantum cryptography standards in the resource-constrained IoT environment. This necessarily requires the implementation of lightweight algorithms taking into account the vulnerability of IoT devices to SCAs and FIAs for better security.

4.2. Applications in IoT

The new NIST standards for post-quantum cryptography (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+) will bring many advantages, especially for the integrity of data exchanged in an IoT network. However, the implementation of these post-quantum algorithms requires a good knowledge of IoT systems as well as the security issues that can arise. Securing an IoT system is essentially about protecting the IoT device-to-device communication, sensing/actuating, and information exchange.

In [71], Xie *et al.* present a comprehensive design flow for implementation based on high-level synthesis (HLS) of NIST PQC candidates and standards. HLS has become a popular method of hardware accelerator design and is used in areas such as deep learning, cryptography, and image processing. This method takes a high-level C/C++ implementation and translates it into a hardware implementation. The same C/C++ code can be used to generate multiple RTLs, each with a different area and latency. Another advantage of using HLS is the ease of verification. HLS uses the classic Finite State Machine with data (FSMD) to design the hardware components, which are arranged hierarchically, according to the different function calls in the C design specification. The main commercial tools are Xilinx Vivado HLS and Mentor Catapault. HLS for designing post-quantum cryptography accelerators was first proposed by Soni *et al.* in [72] [73] to map high-level C specifications of the second round NIST PQC candidates into both FPGA and ASIC implementations. They showed that the maximum latency reduction achieved was 45× with a maximum increase in area overhead was 12×. The authors further improved on their approach to have

power, area, speed, and security (PASS) tradeoffs using a C to ASIC design flow [74]. The authors developed ASIC designs for two lattice-based digital signature schemes PQC: qTESLA and the future candidat winner CRYSTALS-Dilithium. They also showed that for both algorithms, a higher security level (level 3 or 5) results in a power, area, and time overhead. In addition, the memory requirements for both algorithms account for nearly 50% of the total ASIC area. As discussed in the previous section, *Classic McEliece* is a candidate for extension in the NIST PQC standards campaign. However, due to the large size of the public key, its computational cost and time poses significant challenges, especially for embedded devices. In [75], the authors used HLS-based HW/SW co-design acceleration on the *Classic McEliece*. They achieved significant maximum speedups of up to 55.2×, 3.3×, and 8.7× in the key generation, encapsulation, and decapsulation algorithms, respectively, compared to a SW-only scalar implementation.

Ring-Learning With Errors (LWE) lattice-based cryptography is one of the most promising approaches for NIST PQC standardization (three of the four winners are lattice-based) due to the relatively low computational complexity and ease of hardware implementation [76] [77]. Aysu *et al.* describe the first hardware implementation of a quantum-secure encryption scheme along with its low-cost power side-channel countermeasures. The encryption uses an implementation-friendly Binary Ring Learning with Errors (BRLWE) problem with binary errors that can be efficiently generated in hardware. Unlike the Ring-LWE method, where the errors are based on a Gaussian distribution, the BRLWE scheme uses binary errors to obtain a much lower computational complexity [78]. This approach provided a high-speed PQC platform to ensure security for the applications and has strong potential for use in IoT servers and edge computing devices. However, a direct implementation of BRLWE has a vulnerability to power SCAs, even with a SPA, due to the nature of the binary coefficients. To protect against SPA and DPA respectively, they performed a redundant addition in plus the memory update and B-RLWE specific opportunity to construct a lightweight countermeasure based on randomization of intermediate states and masked threshold decoding. Their result is an interesting trade-off between side channel security and the cost of the B-RLWE hardware surface on a SAKURA-G FPGA board. In [77], the authors proposed the inverted BRLWE, an optimized variant for the BRLWE scheme that is proven to be secure against quantum attacks and is highly efficient for hardware implementations. They presented two variants of inverted BRLWE: a high-speed architecture targeting edge and powerful IoT devices, and an ultralightweight architecture, which can be implemented on resource-constrained nodes in IoT. Their two different ASIC implementations showed improvement in terms of speed, area and power. This is the first implementation of LWE lattice-based cryptosystems on the ASIC platform.

In [79], Mustafa *et al.* proposed a post-quantum lattice-based RSA (LB-RSA) for IoT-based cloud applications to secure shared data and information.

Among all the studied post-quantum cryptographic schemes, the lattice-based scheme is mainly used in IoT due to its simplicity and scalability compared to other cryptographic schemes, as shown in the initial NIST results for PQC standardization. Therefore, in the near future, a more elaborate study will be conducted on the secure implementation of these future new post-quantum standards in constrained environments.

5. Research Challenges and Orientations

With the increase in IoT devices, security needs are also increasing. The main challenge for these devices is primarily related to resource issues that can make it difficult to implement security algorithms. However, lightweight algorithms developed under the NIST program have solved some of these problems, but not all of them. Indeed, these devices in operation can leak information from their auxiliary channels which can sometimes be very sensitive. More and more these flaws are exploited by attackers with powerful techniques to find the keys that allowed the encryption of the IoT SoC. To counter these attacks, countermeasures are proposed as described in Section 1. Nevertheless, as we mentioned earlier, these low-cost devices are resource-limited, which may impact the implementation of adequate countermeasures for these objects.

PQC is an entirely modern field that industries and academics are studying to prepare for the quantum era especially in IOT. However, the post-quantum IoT cryptosystems developed are not guaranteed against physical attacks. IoT device designers need to take a closer look at the world of quantum computing and its threats to minimize these risks. Although most modern public key cryptography systems use relatively large key sizes, these are sometimes much larger in post quantum algorithms. This poses a major challenge for implementations on resource-constrained devices. For example, it is essential to deploy post-quantum cryptography systems based on lighter lattices to handle the processing and use of large keys on increasingly powerful IoT devices. One of the biggest challenges is that the current choice of IoT platforms is not obvious because these devices will be noticeably less powerful than the devices that will exist in the future in the quantum era. In addition, with recent advances in the growth of cloud computing, large-scale IoT applications are enabling correct and timely execution. Privacy issues related to cloud computing can interrupt the execution of these applications, which is one of the main research areas.

In a connected thing system, identifying a valid verifier in an authentication scheme requires too many resources for IoT devices, to the point of being impractical. In addition, implementing classical random functions and selecting pseudo-random functions are very complex tasks. Thus, in the quantum domain, the implementation of such a protocol requires either external quantum servers equipped with the adequate capacity and to determine the exact quantity of services of the PQC necessary. Concerning code-based post-quantum cryptography, one of the main directions of research is to analyze variants of the origi-

nal McEliece scheme with different codes. From this survey, it is clear that there is still room for improvement in the design of these systems with the extension of the NIST PQC standardization campaign.

Overall, we notice that the existing schemes in the PQC use lattice-based cryptosystems. The private and public key sizes used by these schemes are more optimal compared to other post-quantum cryptosystems. These lattice-based schemes and other existing post-quantum schemes should be based on finding an optimal trade-off between performance, security and memory cost in the IOT era. With the growth of cloud computing, the challenges are even greater when communication takes place between IoT devices. The design of future IOT devices must take into account these new constraints related to confidentiality, integrity and availability in an increasingly close quantum era.

6. Conclusion

In this article, we have examined the challenges of IoT systems in the face of hardware attacks. The strong growth of IoTs needs to be accompanied by security measures on the software and hardware side to ensure their sustainability. After a detailed study on the different physical attacks that can be made against IoT systems, we have projected ourselves into the quantum era and the problems linked to low-resource systems. Indeed, it is important to find lightweight post-quantum cryptographic systems capable of adapting to resource-constrained environments such as the IoT with the NIST standardisation process. Finally we proposed some research directions after showing some challenges related to these types of attacks and post-quantum cryptography.

Acknowledgements

This work is supported by the African Centre for Technology Studies (ACTS) and the International Development Research Centre (IDRC)/Swedish International Development Cooperation Agency (SIDA).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Conti, M., Losiouk, E., Poovendran, R. and Spolaor, R. (2022) Side-Channel Attacks on Mobile and IoT Devices for Cyber-Physical Systems. *Computer Networks*, **207**, Article ID: 108858. https://doi.org/10.1016/j.comnet.2022.108858

[2] Dofe, J., Frey, J. and Yu, Q. (2016) Hardware Security Assurance in Emerging IoT Applications. *IEEE International Symposium on Circuits and Systems* (*ISCAS*), Montreal, 22-25 May 2016, 2050-2053. https://doi.org/10.1109/ISCAS.2016.7538981

[3] Hong, S. (2019) Special Issue on "Side Channel Attacks". *Applied Sciences*, **9**, Article No. 1881. https://doi.org/10.3390/app9091881

[4] Sangodoyin, S., Werner, F.T., Yilmaz, B.B., Cheng, C.-L., Ugurlu, E.M., Sehat-

bakhsh, N., Prvulovic, M. and Zajic, A. (2020) Side-Channel Propagation Measurements and Modeling for Hardware Security in IoT Devices. *IEEE Transactions on Antennas and Propagation*, **69**, 3470-3484. https://doi.org/10.1109/TAP.2020.3037659

[5] Duan, X., Cui, Q., Wang, S., Fang, H. and She, G. (2016) Differential Power Analysis Attack and Efficient Countermeasures on PRESENT. 2016 8*th IEEE International Conference on Communication Software and Networks* (*ICCSN*), Beijing, 4-6 June 2016, 8-12. https://doi.org/10.1109/ICCSN.2016.7586627

[6] Prates, N., Vergutz, A., Macedo, R.T., Santos, A. and Nogueira, M. (2020) Defense Mechanism for Timing-Based Side-Channel Attacks on IoT Traffic. *GLOBECOM* 2020-2020 *IEEE Global Communications Conference*, Taipei, 7-11 December 2020, 1-6. https://doi.org/10.1109/GLOBECOM42002.2020.9322070

[7] Guo, S., Wang, J., Chen, Z., Li, Y. and Lu, Z. (2020) Securing IoT Space via Hardware Trojan Detection. *IEEE Internet of Things Journal*, **7**, 11115-11122. https://doi.org/10.1109/JIOT.2020.2994627

[8] Tudosa, I., Picariello, F., Balestrieri, E., De Vito, L. and Lamonaca, F. (2019) Hardware Security in IoT Era: The Role of Measurements and Instrumentation. *Workshop on Metrology for Industry* 4.0 *and IoT*, Naples, 4-6 June 2019, 285-290. https://doi.org/10.1109/METROI4.2019.8792895

[9] Ahmed, A., Farahmandi, F., Iskander, Y. and Mishra, P. (2019) Security and Trust Verification of IoT SoCs. In: Chakraborty, R.S., Mathew, J. and Vasilakos, A.V., Eds., *Security and Fault Tolerance in Internet of Things*, Springer, Berlin, 1-19. https://doi.org/10.1007/978-3-030-02807-7_1

[10] Li, H., Liu, Q., Zhang, J.L. and Bertozzi, L. (2016) A Survey of Hardware Trojan Threat and Defense. *Integration*, **55**, 426-437. https://doi.org/10.1016/j.vlsi.2016.01.004

[11] Jacob, N., Merli, D., Heyszl, J. and Sigl, G. (2014) Hardware Trojans: Current Challenges and Approaches. *IET Computers & Digital Techniques*, **8**, 264-273. https://doi.org/10.1049/iet-cdt.2014.0039

[12] Anderson, R. and Kuhn, M. (1998) Low Cost Attacks on Tamper Resistant Devices. *Security Protocols*: 5*th International Workshop*, Paris, 7-9 April 1997, 125-136. https://doi.org/10.1007/BFb0028165

[13] Bao, F., Deng, R.H., Han, Y.F., Jeng, A., Narasimhalu, A.D. and Ngair, T. (1998) Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults. *Security Protocols*: 5*th International Workshop*, Paris, 7-9 April 1997, 115-124. https://doi.org/10.1007/BFb0028164

[14] Boneh, D., DeMillo, R.A. and Lipton, R.J. (2001) On the Importance of Checking Cryptographic Protocols for Faults. *Advances in Cryptology—EUROCRYPT*'97: *International Conference on the Theory and Application of Cryptographic Techniques*, Konstanz, 11-15 May 1997, 37-51. https://doi.org/10.1007/3-540-69053-0_4

[15] Yen. S.-M. and Joye. M. (2000) Checking before Output May Not Be Enough against Fault-Based Cryptanalysis. *IEEE Transactions on Computers*, **49**, 967-970. https://doi.org/10.1109/12.869328

[16] Hemme, L. (2004) A Differential Fault Attack against Early Rounds of (Triple-)DES. *Cryptographic Hardware and Embedded Systems-CHES* 2004: 6*th International Workshop*, Cambridge, 11-13 August 2004, 254-267. https://doi.org/10.1007/978-3-540-28632-5_19

[17] Barenghi, A., Breveglieri, L., Koren, I. and Naccache, D. (2012) Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. *Proceed-*

ings of the IEEE, **100**, 3056-3076. https://doi.org/10.1109/JPROC.2012.2188769

[18] Skorobogatov, S.P. and Anderson, R.J. (2003) Optical Fault Induction Attacks. *Cryptographic Hardware and Embedded Systems-CHES* 2002: 4*th International Workshop*, Redwood Shores, 13-15 August 2002, 2-12. https://doi.org/10.1007/3-540-36400-5_2

[19] Roscian, C., Dutertre, J.-M. and Tria, A. (2013) Frontside Laser Fault Injection on Cryptosystems—Application to the AES' Last Round. 2013 *IEEE International Symposium on Hardware-Oriented Security and Trust* (*HOST*), Austin, 2-3 June 2013, 119-124. https://doi.org/10.1109/HST.2013.6581576

[20] He, W., Breier, J. and Bhasin, S. (2016) Cheap and Cheerful: A Low-Cost Digital Sensor for Detecting Laser Fault Injection Attacks. *Security, Privacy, and Applied Cryptography Engineering*: 6*th International Conference*, *SPACE* 2016, Hyderabad, 14-18 December 2016, 27-46. https://doi.org/10.1007/978-3-319-49445-6_2

[21] Rodriguez, J., Baldomero, A., Montilla, V. and Mujal, J. (2019) LLFI: Lateral Laser Fault Injection Attack. 2019 *Workshop on Fault Diagnosis and Tolerance in Cryptography* (*FDTC*), Atlanta, 24 August 2019, 41-47. https://doi.org/10.1109/FDTC.2019.00014

[22] Garb, K. and Obermaier, J. (2020) Temporary Laser Fault Injection into Flash Memory: Calibration, Enhanced Attacks, and Countermeasures. 2020 *IEEE* 26*th International Symposium on On-Line Testing and Robust System Design* (*IOLTS*), Napoli, 13-15 July 2020, 1-7. https://doi.org/10.1109/IOLTS50870.2020.9159712

[23] Dumont, M., Moëllic, P.-A., Viera, R., Dutertre, J.-M. and Bernhard, R. (2021) An Overview of Laser Injection against Embedded Neural Network Models. 2021 *IEEE* 7*th World Forum on Internet of Things* (*WF-IoT*), New Orleans, 14 June-31 July 2021, 616-621. https://doi.org/10.1109/WF-IoT51360.2021.9595075

[24] Hériveaux, O. (2022) Triple Exploit Chain with Laser Fault Injection on a Secure Element. 2022 *Workshop on Fault Detection and Tolerance in Cryptography* (*FDTC*), 16 September 2022, 9-17. https://doi.org/10.1109/FDTC57191.2022.00011

[25] Shepherd, C., Markantonakis, K., van Heijningen, N., Aboulkassimi, D., Gaine, C., Heckmann, T. and Naccache, D. (2021) Physical Fault Injection and Side-Channel Attacks on Mobile Device : A Comprehensive Analysis. *Computers & Security*, **111**, Article ID: 102471. https://doi.org/10.1016/j.cose.2021.102471

[26] Li, H.Y., Du, G.H., Shao, C.P., Dai, L., Xu, G.Q. and Guo, J.L. (2021) Heavy-Ion Microbeam Fault Injection into SRAM-Based FPGA Implementations of Cryptographic Circuits. *IEEE Transactions on Nuclear Science*, **62**, 1341-1348. https://doi.org/10.1109/TNS.2015.2423672

[27] Kazemi, Z. (2022) Fault Injection Attacks on Embedded Applications: Characterization and Evaluation. Université Grenoble Alpes, Saint-Martin-d'Hères.

[28] Potestad-Ordóñez, F.E., Jiménez-Fernández, C.J. and Valencia-Barrero, M. (2017) Vulnerability Analysis of Trivium FPGA Implementations. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, **25**, 3380-3389. https://doi.org/10.1109/TVLSI.2017.2751151

[29] Liu, H.L., Liu, Z.L., Qiao, Y.F., Lu, Z.J., *et al.* (2017) Clock Glitch Fault Injection Attacks on an FPGA AES Implementation. *Journal of Electrotechnology, Electrical Engineering and Management*, **1**, 23-27. https://doi.org/10.23977/jeeem.2017.11005

[30] Kazemi, Z., Papadimitriou, A., Souvatzoglou, I., Aerabi, E., Ahmed, M.M., Hely, D. and Beroulle, V. (2019) On a Low Cost Fault Injection Framework for Security Assessment of Cyber-Physical Systems: Clock Glitch Attacks. 2019 *IEEE* 4*th International Verification and Security Workshop* (*IVSW*), Rhodes, 1-3 July 2019, 7-12.

https://doi.org/10.1109/IVSW.2019.8854391

[31] Kazemi, Z., Papadimitriou, A., Hely, D., Fazcli, M. and Beroulle, V. (2018) Hardware Security Evaluation Platform for MCU-Based Connected Devices: Application to Healthcare IoT. 2018 *IEEE* 3*rd International Verification and Security Workshop* (*IVSW*), Costa Brava, 2-4 July 2018, 87-92. https://doi.org/10.1109/IVSW.2018.8494843

[32] Yanci, A.G., Pickles, S. and Arslan, T. (2009) Characterization of a Voltage Glitch Attack Detector for Secure Devices. 2009 *Symposium on Bio-Inspired Learning and Intelligent Systems for Security IEEE*, Edinburgh, 20-21 August 2009, 91-96. https://doi.org/10.1109/BLISS.2009.18

[33] (2006) Effets des problèmes de tension d'alimentation sur les circuits CMOS. *Conférence internationale sur la conception et le test de systèmes intégrés dans la technologie à l'échelle nanométrique*, 257-261.

[34] Béringuier-Boher, N., Beroulle, V., Hély, D., Damiens, J. and Candelier, P. (2016) Clock Generator Behavioral Modeling for Supply Voltage Glitch Attack Effects Analysis. *Microprocessors and Microsystems*, **47**, 37-43. https://doi.org/10.1016/j.micpro.2016.02.014

[35] Muttaki, M.R., Zhang, T., Tehranipoor, M. and Farahmandi, F. (2022) FTC: A Universal Sensor for Fault Injection Attack Detection. 2022 *IEEE International Symposium on Hardware Oriented Security and Trust* (*HOST*), McLean, 27-30 June 2022, 117-120. https://doi.org/10.1109/HOST54066.2022.9840177

[36] Yuce, B., Schaumont, P. and Witteman, M. (2018) Fault Attacks on Secure Embedded Software: Threats, Design, and Evaluation. *Journal of Hardware and Systems Security*, **2**, 111-130. https://doi.org/10.1007/s41635-018-0038-1

[37] Majéric, F., Bourbao, E. and Bossuet, L. (2016) Electromagnetic Security Tests for SoC. *International Conference on Electronics*, *Circuits and Systems* (*ICECS*), Monte Carlo, 11-14 December 2016, 265-268. https://doi.org/10.1109/ICECS.2016.7841183

[38] Giraud, C. (2005) DFA on AES. *Advanced Encryption Standard—AES*, 4*th International Conference*, *AES* 2004, Bonn, 10-12 May 2004, 27-41. https://doi.org/10.1007/11506447_4

[39] Barenghi, A., Bertoni, G.M., Breveglieri, L., Pellicioli, M. and Pelosi, G. (2010) Fault Attack on AES with Single-Bit Induced Faults. 6*th International Conference on Information Assurance and Security*, Atlanta, 23-25 August 2010, 167-172. https://doi.org/10.1109/ISIAS.2010.5604061

[40] Cayrel, P.-L., Colombier, B., Dragoi, V.-F., Menu, A. and Bossuet, L. (2020) Message-Recovery Laser Fault Injection Attack on Code-Based Cryptosystems.

[41] Kocher, P., Jaffe, J. and Jun, B. (1999) Differential Power Analysis. 19*th Annual International Cryptology Conference*, Santa Barbara, 15-19 August 1999, 388-397. https://doi.org/10.1007/3-540-48405-1_25

[42] Lo, O., Buchanan, W.J. and Carson, D. (2017) Power Analysis Attacks on the AES-128 S-Box Using Differential Power Analysis (DPA) and Correlation Power Analysis (CPA). *Journal of Cyber Security Technology*, **1**, 88-107. https://doi.org/10.1080/23742917.2016.1231523

[43] Gamaarachchi, H. and Ganegoda, H. (2018) Power Analysis Based Side Channel Attack.

[44] Messerges, T.S., Dabbish, E.A. and Sloan, R.H. (1999) Investigations of Power Analysis Attacks on Smartcards. *Proceedings of the USENIX Workshop on Smart-*

card Technology on USENIX Workshop on Smartcard Technology, Chicago, 10-11 May 1999, 151-161.

[45] Mangard, S., Oswald, E. and Popp, T. (2008) Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer Science & Business Media, Berlin, 31.

[46] Nuradha, F.R., Putra, S.D., Kurniawan, Y. and Rizqulloh, M.A. (2019) Attack on AES Encryption Microcontroller Devices with Correlation Power Analysis. 2019 *International Symposium on Electronics and Smart Devices* (*ISESD*), Badung, 8-9 October 2019, 1-4. https://doi.org/10.1109/ISESD.2019.8909447

[47] Dao, B.-A., Hoang, T.-T., Le, A.-T., Tsukamoto, A., Suzaki, K. and Pham, C.-K. (2021) Correlation Power Analysis Attack Resisted Cryptographic RISC-V SoC with Random Dynamic Frequency Scaling Countermeasure. *IEEE Access*, **9**, 151993-152014. https://doi.org/10.1109/ACCESS.2021.3126703

[48] Wang, C.X., Xie, X.J., Yu, M.Y., Wang, J.X. and Tang, X.C. (2012) A CPA Attack against Round Based Piccolo-80 Hardware Implementation. 2012 5*th International Congress on Image and Signal Processing*, Chongqing, 16-18 October 2012, 1735-1740. https://doi.org/10.1109/CISP.2012.6470033

[49] Heuser, A. and Zohner, M. (2012) Intelligent Machine Homicide: Breaking Cryptographic Devices Using Support Vector Machines. *Constructive Side-Channel Analysis and Secure Design*: *Third International Workshop*, *COSADE* 2012, Darmstadt, 3-4 May 2012, 249-264. https://doi.org/10.1007/978-3-642-29912-4_18

[50] Maghrebi, H., Portigliatti, T. and Prouff, E. (2016) Breaking Cryptographic Implementations Using Deep Learning Techniques. *Security*, *Privacy*, *and Applied Cryptography Engineering*: 6*th International Conference*, *SPACE* 2016, Hyderabad, 14-18 December 2016, 3-26. https://doi.org/10.1007/978-3-319-49445-6_1

[51] Picek, S., Samiotis, I.P., Kim, J., Heuser, A., Bhasin, S. and Legay, A. (2018) On the Performance of Convolutional Neural Networks for Side-Channel Analysis. *Security*, *Privacy*, *and Applied Cryptography Engineering*: 8*th International Conference*, *SPACE* 2018, Kanpur, 15-19 December 2018, 157-176. https://doi.org/10.1007/978-3-030-05072-6_10

[52] Wang, Z., Wang, H., Yang, Y.N., Li, D.J., Zhang, Z. and Wu, T.T. (2022) The Research of the Side-Channel Analysis Method Based on Deep Learning for Trusted Platform Module. *Journal of Physics*: *Conference Series*, **2358**, Article ID: 012016. https://doi.org/10.1088/1742-6596/2358/1/012016

[53] Sangodoyin, S., Werner, F.T., Yilmaz, B.B., Cheng, C.-L., Ugurlu, E.M., Sehatbakhsh, N., Prvulović, M. and Zajic, A. (2020) Side-Channel Propagation Measurements and Modeling for Hardware Security in IoT Devices. *IEEE Transactions on Antennas and Propagation*, **69**, 3470-3484. https://doi.org/10.1109/TAP.2020.3037659

[54] Gandolfi, K., Mourtel, C. and Olivier, F. (2001) Electromagnetic Analysis: Concrete Results. *Cryptographic Hardware and Embedded Systems—CHES* 2001: 3*rd International Workshop*, Paris, 14-16 May 2001, 251-261. https://doi.org/10.1007/3-540-44709-1_21

[55] Tudosa, I., Picariello, F., Balestrieri, E., De Vito, L. and Lamonaca, F. (2020) Hardware Security in IoT Era: The Role of Measurements and Instrumentation. *Workshop on Metrology for Industry* 4.0 *and IoT*, Naples, 4-6 June 2019, 285-290. https://doi.org/10.1109/METROI4.2019.8792895

[56] Balasch, J., Gierlichs, B., Reparaz, O. and Verbauwhede, I. (2015) DPA, Bitslicing and Masking at 1 GH. *Cryptographic Hardware and Embedded Systems—CHES* 2015: 17*th International Workshop*, Saint-Malo, 13-16 September 2015, 599-619.

https://doi.org/10.1007/978-3-662-48324-4_30

[57] Wang, R., Wang, H.Y. and Dubrova, E. (2020) Far Field EM Side-Channel Attack on AES Using Deep Learning. *Proceedings of the* 4*th ACM Workshop on Attacks and Solutions in Hardware Security*, Orlando, 13 November 2020, 35-44. https://doi.org/10.1145/3411504.3421214

[58] Ge, Q., Yarom, Y., Cock, D. and Heiser, G. (2018) A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware. *Journal of Cryptographic Engineering*, **8**, 1-27.

[59] Tsunoo, Y., Saito, T., Suzaki, T., Shigeri, M. and Miyauchi, H. (2003) Cryptanalysis of DES Implemented on Computers with Cache. *Cryptographic Hardware and Embedded Systems-CHES* 2003: 5*th International Workshop*, Cologne, 8-10 September 2003, 62-76. https://doi.org/10.1007/978-3-540-45238-6_6

[60] Bernstein, D.J. (2005) Cache-Timing Attacks on AES.

[61] Reinbrecht, C., Susin, A., Bossuet, L., Sigl, G. and Sepúlveda, J. (2017) Timing Attack on NoC-Based Systems: Prime+ Probe Attack and NoC-Based Protection. *Microprocessors and Microsystems*, **52**, 556-565. https://doi.org/10.1016/j.micpro.2016.12.010

[62] Kömmerling, O. and Kuhn, M.G. (1999) Design Principles for Tamper-Resistant Smartcard Processors. *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, Chicago, 10-11 May 1999, 9-20.

[63] Yamaguchi, M., Toriduka, H., Kobayashi, S., Sugawara, T., Hommaa, N., Satoh, A. and Aoki, T. (2010) Development of an On-Chip Micro Shielded-Loop Probe to Evaluate Performance of Magnetic Film to Protect a Cryptographic LSI from Electromagnetic Analysis. 2010 *IEEE International Symposium on Electromagnetic Compatibility*, Fort Lauderdale, 25-30 July 2010, 103-108. https://doi.org/10.1109/ISEMC.2010.5711255

[64] Skorobogatov, S.P. (2005) Semi-Invasive Attacks—A New Approach to Hardware Security Analysis. University of Cambridge, Cambridge.

[65] Cai, X.M., Xie, G.Q., Kuang, S.J., Li, R.F. and Li, S.Q. (2021) Efficient DPA Side Channel Countermeasure with MIM Capacitors-Based Current Equalizer. *Journal of Systems Architecture*, **118**, Article ID: 102146. https://doi.org/10.1016/j.sysarc.2021.102146

[66] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings* 35*th Annual Symposium on Foundations of Computer Science*, Santa Fe, 20-22 November 1994, 124-134.

[67] Melchor, C.A., Aragon, N., Barreto, P., Bettaieb, S., Bidoux, L., *et al.* (2020) BIKE: Bit Flipping Key Encapsulation, NIST Post-Quantum Cryptography Standardization Project (Round 3).

[68] Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Persichetti, E., Zémor, G. and Bourges, I.C. (2018) Hamming Quasi-Cyclic (HQC, NIST PQC Round).

[69] Albrecht, M.R., Bernstein, D.J., Chou, T., Cid, C., Gilcher, J., *et al.* (2020) Classic McEliece. Tech. Rep., National Institute of Standards and Technology, Gaithersburg.

[70] Azarderakhsh, R., Campagna, M., Costello, C., Feo, L., Hess, B., Jalali, A., *et al.* (2017) SIKE—Supersingular Isogeny Key Encapsulation. https://sike.org

[71] Xie, J.F., Basu, K., Gaj, K. and Guin, U. (2020) Special Session: The Recent Advance in Hardware Implementation of Post-Quantum Cryptography. 2020 *IEEE* 38*th*

VLSI Test Symposium (*VTS*), San Diego, 5-8 April 2020, 1-10. https://doi.org/10.1109/VTS48691.2020.9107585

[72] Soni, D., Basu, K., Nabeel, M. and Karri, R. (2019) A Hardware Evaluation Study of NIST Post-Quantum Cryptographic Signature Schemes. 2*nd PQC Standardization Conference*.

[73] Basu, K., Soni, D., Nabeel, M. and Karri, R. (2019) NIST Post-Quantum Cryptography—A Hardware Evaluation Study. Cryptology ePrint Archive.

[74] Soni, D., Nabeel, M., Basu, K. and Karri, R. (2019) Power, Area, Speed, and Security (PASS) Trade-Offs of NIST PQC Signature Candidates Using a C to ASIC Design Flow. 2019 *IEEE* 37*th International Conference on Computer Design* (*ICCD*), Abu Dhabi, 17-20 November 2019, 337-340. https://doi.org/10.1109/ICCD46524.2019.00054

[75] Kostalabros, V., Ribes-González, J., Farràs, O., Moretó, M. and Hernandez, C. (2021) HLS-Based HW/SW Co-Design of the Post-Quantum Classic Mceliece Cryptosystem. 2021 31*st International Conference on Field-Programmable Logic and Applications* (*FPL*), Dresden, 30 August-3 September 2021, 52-59. https://doi.org/10.1109/FPL53798.2021.00017

[76] Aysu, A., Orshansky, M. and Tiwari, M. (2018) Binary Ring-LWE Hardware with Power Side-Channel Countermeasures. 2018 *Design*, *Automation & Test in Europe Conference & Exhibition* (*DATE*), Dresden, 19-23 March 2018, 1253-1258. https://doi.org/10.23919/DATE.2018.8342207

[77] Ebrahimi, S., Bayat-Sarmadi, S. and Mosanaei-Boorani, H. (2019) Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT. *IEEE Internet of Things Journal*, **6**, 5500-5507. https://doi.org/10.1109/JIOT.2019.2903082

[78] Buchmann, J., Göpfert, F., Güneysu, T., Oder, T. and Pöppelmann, T. (2016) High-Performance and Lightweight Lattice-Based Public-Key Encryption. *Proceedings of the* 2*nd ACM International Workshop on IoT Privacy*, *Trust*, *and Security*, Xi'an, 30 May-3 June 2016, 2-9. https://doi.org/10.1145/2899007.2899011

[79] Mustafa, I., Khan, I.U., Aslam, S., Sajid, A., Mohsin, S.M., Awais, M. and Qureshi, M.B. (2020) A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications. *Proceedings of the* 2*nd ACM International Workshop on IoT Privacy*, *Trust*, *and Security*, Vol. 8, 99273-99285. https://doi.org/10.1109/ACCESS.2020.2995801