Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective

Javier Oliva del Moral, Antonio deMarti iOlius, Gerard Vidal, Pedro M. Crespo, *Senior Member, IEEE*, and Josu Etxezarreta Martinez

***Abstract*—The machinery of industrial environments was connected to the Internet years ago with the scope of increasing their performance. However, this change made such environments vulnerable against cyber-attacks that can compromise their correct functioning resulting in economic or social problems. Moreover, implementing cryptosystems in the communications between operational technology (OT) devices is a more challenging task than for information technology (IT) environments since the OT networks are generally composed of legacy elements, characterized by low-computational capabilities. Consequently, implementing cryptosystems in industrial communication networks faces a tradeoff between the security of the communications and the amortization of the industrial infrastructure. Critical infrastructure (CI) refers to the industries which provide key resources for the daily social and economical development, e.g., electricity. Furthermore, a new threat to cybersecurity has arisen with the theoretical proposal of quantum computers, due to their potential ability of breaking state-of-the-art cryptography protocols, such as RSA or elliptic curve cryptography. Many global agents have become aware that transitioning their secure communications to a quantum secure paradigm is a priority that should be established before the arrival of fault-tolerance. In this article, we aim to describe the problematic of implementing post-quantum cryptography (PQC) to CI environments. For doing so, we describe the requirements for these scenarios and how they differ against IT. We also introduce classical cryptography and how quantum computers pose a threat to such security protocols. Furthermore, we introduce state-of-the-art proposals of PQC protocols and present their characteristics. We conclude by discussing the problematic of integrating PQC in industrial environments.**

***Index Terms*—Communication system security, cryptographic protocols, hardware security, industrial communication, Internet of Things, quantum cryptography.**

I. Introduction

THE EXPONENTIAL development of communication technologies in the late 20th century and, specially, in the early 21^{st} century has resulted in a contemporary society that exists in a hyperconnected world. In this paradigm, communications do not only refer to the actions of texting, phone (video) calls, social media or news media but also to the control of industrial machines, bank transfers, stock acquisitions, control of unmanned aerial vehicles (UAVs) or managing automated houses (domotics), to name a few. Furthermore, strongly tangled concepts, such as Smart Cities, Industry 4.0, or the Internet of Things (IoT) are currently being investigated for their convergence with other advanced technologies, such as artificial intelligence (AI) or quantum computing (QC) on a historical inflection point in the form of a fourth industrial revolution [1].

In this sense, relying on communications for executing the critical tasks involved in such hyperconnected paradigm requires that those transmissions of information are secure and private. Cyber vulnerabilities in the control systems of a smart city or an automated industry may lead to catastrophic consequences. For example, in a possible future where the transport of people and cargo is exclusively done by autonomous vehicles which rely on the communications among them and some central control stations to move around, the intrusion of a malicious entity on the system to disturb it would lead to fatal consequences economically and socially (casualties). Hence, modern crime and war is heavily based on hacking activities with the scope of manipulating critical infrastructures (CIs), to produce economical or social losses by interrupting their production or by decreasing the life-time of their devices, or obtaining sensitive information regarding state, industrial or personal secrets (banking information or sensitive images, for example). This paradigm of cybercrime and cyberwar is present nowadays with an estimated amount of 2200 known cyberattacks per day in 2022, posing a threat to the business' infrastructure every 39 s [2]. Indeed, awareness on cyberattacks among Nation-state actors is increasing due to current geopolitical tensions, as seen recently [3]. It is due to all these factors that concepts, such as the cyber apocalypse, are being coined to describe the fear that a cyberattack to CI's

Manuscript received 22 January 2024; revised 13 April 2024 and 16 May 2024; accepted 1 June 2024. Date of publication 6 June 2024; date of current version 6 September 2024. This work was supported in part by the Spanish Ministry of Economy and Competitiveness through the MADDIE Project under Grant PID2022-137099NB-C44, and in part by the Gipuzkoako Foru Aldundia through the "Post-Quantum Cryptographic Strategies for Critical Infrastructures" Project under Grant IS172551022. *(Corresponding author: Javier Oliva del Moral.)*

Javier Oliva del Moral is with the Department of Basic Sciences, Tecnun-University of Navarra, 20018 Donostia-San Sebastian, Spain, and also with Donostia International Physics Center, 20018 Donostia-San Sebastian, Spain (e-mail: jolivam@unav.es).

Antonio deMarti iOlius, Pedro M. Crespo, and Josu Etxezarreta Martinez are with the Department of Basic Sciences, Tecnun-University of Navarra, 20018 Donostia-San Sebastian, Spain (e-mail: ademartio@unav.es; pcrespo@unav.es; jetxezarreta@unav.es).

Gerard Vidal is with Opscura, 20018 Donostia-San Sebastian, Spain (e-mail: gerard@opscura.io).

Digital Object Identifier 10.1109/JIOT.2024.3410702

systems and networks of a country would led to shutting down their capabilities regarding civilian and military services. It is important to state that the possibility of major devastation in the CI of a nation does not have to imply that all the systems consisting it should be attacked, the failure of parts of the structure may lead to a catastrophic propagation of failures through the whole network due to the interconnection among the elements. This effect is known as cascading effect [4].

All of these vulnerabilities make cybersecurity and cryptography to be the pillars to erect the previously described paradigmatic society in a security way. Cybersecurity is defined as the practice of protecting important systems and confidential information from cyberattacks. In this sense, many methods and elements are used for the sake of protecting communication and computer networks, but the algorithms that are employed to cipher sensitive data being communicated in such meshes relate to the field of cryptography. Hence, in this society where the quote "Information is power" is getting more and more relevant, the use of such practices is of capital relevance. Importantly, the proposal of the RSA or elliptic curve cryptography (ECC) asymmetric cryptographic systems has maintained the security of communication systems for over 40 years [5], [6], [7]. The core of those protocols resides in the fact that they are based on hard problems that cannot be solved in a practical time frame by classical computing methods, i.e., thousands of years of computing are required to extract the plain text from the ciphertext if the key is unknown. Unluckily, quantum computers have posed a threat to the security of those asymmetric cryptography protocols. Shor's algorithm is a theoretical quantum algorithm that provides an exponential speedup for solving prime number factorization and the computation of discrete logarithms, respectively, which are the hard problems in which the security of the previously commented protocols relies upon [8]. At the current time, quantum computers that can execute such algorithm efficiently and correctly only exists as a theoretical promise. Nonetheless, the past years, QC has proven to be a rapidly evolving field with the achievement of milestones, such as the first experimental realizations of quantum advantage [9], [10], [11], [12], [13] or quantum error correction [14], [15]. Such tremendous advancements have made educated voices to estimate the appearance of efficient quantum computers able to make state-of-the-art asymmetric protocols to be deprecated to be within the range of one to two decades [16]. Hence, many have raised the alarm of a possible "Quantum Apocalypse" that would result in sensitive data and systems to become completely vulnerable.

Fortunately, there is hope for making the computer and machine networks of the future to be secure in the fault-tolerant QC era due to the proposals of QKD and post-quantum cryptography (PQC). The first refers to using the properties of quantum mechanics in order to secure and transmit information [17]. This paradigm includes important protocols for QKD, such as BB84 [18] or E91 [19]. Although being a very promising candidate for a quantum-safe future, QKD is still a nascent technology posing many challenges that include technical complexity and cost as well as the requirement of sophisticated infrastructure. This comes with the added requirement of still needing to deal with the noise, loss and decoherence that limit the performance of quantum communication systems, e.g., quantum repeaters are being investigated for solving such problem [20]. Hence, PQC has been proposed as the paradigm of classical cryptography schemes that are secure against attackers that have access to fault-tolerant quantum computers [21]. Quantum computers do not provide an exponential speedup to solve every computer science problem [22] and, therefore, the main idea in PQC would be to find hard problems that cannot be efficiently tackled by such technology, even if it is fully operational. Obviously, this should be done in conjunction with security against classical attacks, since PQC protocols would be useless if they were still vulnerable to traditional hacking. The importance of migrating to quantum-secure cryptography has not gone unnoticed for many countries with an open PQC protocol standardization process like the U.S. National Institute of Standards and Technology (NIST) [23] or like Europe with the quantum cybersecurity agenda by the European Policy Centre (EPC) [24]. Several PQC protocols, such as hash-, lattice- or code-based cryptography, have been proposed as a way of allowing secure communications on the networks of the future. Interestingly, even Google has decided to introduce PQC protocols in their Chrome browser [25], announcing that they will admit the use of the X25519Kyber768 protocol to encrypt transport layer security (TLS) connections. Such protocol is a combination of a classical ECC-based protocol and the lattice-based CRYSTALS-Kyber [26] PQC algorithm, which is one of the algorithms selected at this point by the NIST for standardization.

Each PQC protocol has its own benefits and disadvantages in terms of security levels, ciphertext size or speed, among other benchmarks. This implies that the selection of PQC protocols is very application-dependent in the sense that as a function of the requirements of a specific system, an approach could be valid or not. Following this logic, PQC protocols are usually proposed for systems in which the cybersecurity is the most critical requirement (information technology (IT) services), while the latency because of the introduction of those cryptography protocols can be deemed as not too important. However, latency is a key performance parameter in industrial control systems (ICSs) and CI, where introducing a delay over the system requirements can imply a failure that cannot be tolerated in such environments [27]. This should obviously be done maintaining a certain level of security on the system. Additionally, it is important to state that implementing cryptography in such networks is done by means of processors that are not powerful enough to manage huge key sizes, mainly because the introduction of such systems should be somehow seamless to the existing communication infrastructure and cheap.[1] It is in this sense that, the inclusion of PQC in industrial and critical environments poses an interesting tradeoff between the benchmarks of those protocols. As mentioned previously, protecting ICS and CI from possible cyberattacks

[1]We can speculate that QKD will not be a major player to secure such networks due the fact that they are very costly as well as they require significant infrastructure to be deployed.

is fundamental due to the immense impact that those systems have in society and industry, making their failure to cause intolerable economic losses and, in the worse scenario, injuries and even casualties. Interestingly, this systems have shown to be vulnerable in the recent times with several hacking proposals [28], [29], [30], [31]. Therefore, the necessity of transitioning the security of industrial and CI to PQC is central to keep all those systems secure against a possible quantum threat, as it has been recently noted by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the NIST [32].

A. Motivation and Related Work

Due to the global security threat posed by the possibility of a fault-tolerant quantum computer, PQC is one of the most important topics in cryptography at the moment. Thus, there are many works pointing out the importance and the lack of cybersecurity in operational technology (OT) environments as well as surveys about PQC cryptosystems. Specifically, there are many theoretical and experimental references regarding PQC cryptosystems, such as [33], [34], [35], and [36]. However, there is a gap in the literature regarding the merge of both problems. Since OT environments are a clear and critical target for cybercriminals, it is of the most importance to protect those scenarios from quantum attacks as well. In comparison with previous works about PQC cited before, this manuscript aims to provide a perspective on the problem of implementing PQC algorithms in CI and OT environments. In the literature there are many works regarding the importance of cybersecurity and cryptography in OT [27], [28], [31], [37], [38], [39], [40], [41], [42]. As PQC algorithms were traditionally conceived from the point of view of IT communications, there are some requirements in industrial environments that are usually not fulfilled by those. Therefore, we want to emphasize the necessity of more research in PQC algorithms from the point of view of OT communications and, at the same time, more test benches implementing PQC algorithms in industrial environments. This comes with the objective of assessing their reliability for OT communications while providing information for cryptography researchers in order to develop new PQC algorithms that are tailored to fulfill those requirements. Papers, such as [34], [43], and [36], provide a good introduction of the problem and a survey for NIST PQC algorithms, *while [44] gives a good introduction to PQC cybersecurity in OT*. In the context of industrial scenarios it is common to underestimate the importance of cybersecurity as well as to consider it as a toll to productivity due to the additional costs. Moreover, each global agent is aiming to standardize PQC protocols in an independent manner, requirements that will be necessary to all vendors to fulfill once established. The NIST standardization process stands as one of the first efforts for PQC standardization and, while followed by a considerable amount of occidental countries, it is not the only one in the world, where countries, such as France [45] or Germany [46], are also following different processes. Thus, it is very unlikely that a global adoption of the same standard will happen for this new field of cryptography, as it happened for the widespread RSA and ECC cryptographic schemes.

B. Outline and Contribution

In this context, the principal objective of this contribution is to stress out the necessity of the integration of new generation PQC protocols to industrial and CI environments as well as to discuss the state of affairs and challenges regarding such integration. Specifically, we aim to the following.

1) Provide an introduction to traditional cryptography in OT environments for industry experts for providing them the basic knowledge of the problem. As mentioned before, many industrial players may be unaware of the importance of integrating cryptography in their environments and, thus, it is our intention to provide them with the basic concepts. Also, this serves to introduce the challenges and requirements of integrating cybersecurity, in general, to CI and industrial environments.
2) Discuss how QC can pose a threat to OT communications and show how this risk fundamentally differs from the one that IT communications may experience. This is aimed to show industrial players why transitioning to quantum secure cryptography will be critical as well as to show PQC developers how those networks should be protected.
3) Describe the state-of-the-art PQC families and protocols being considered, not only within the NIST standardization process but also within other processes around the world. This serves as an introduction of PQC cryptography for newcomers. Additionally, we intend to show that due to the uncertainty regarding the PQC algorithms that will be implemented (some strong candidates are being questioned or have been recently broken) and the fact that it seems that many global agents will adopt their own methods, PQC integration in OT environments will require a great degree of flexibility regarding implementation.
4) Provide a discussion of the state-of-affairs regarding PQC implementation in OT environments. Specifically, we want to pose the main challenges when integrating those quantum secure protocols in such scenarios. Finally, to show the necessity of more active research on this topic both by cryptographers and industrial players.

The manuscript is organized as follows: in Section II we provide a review of the communication systems in industrial environments as well as of the stringent requirements for integrating cybersecurity in them. We follow, in Section III, with a short review on cryptography and the threat that quantum computers pose to traditional ciphering schemes. Existing proposals of PQC algorithms are surveyed in Section IV presenting several protocols proposed by many worldwide agents. In addition, the performance benchmarks of those PQC candidates are presented. An overview of the state of PQC in industrial and CI environments is finally presented in Section V, were we speculatively discuss which existing protocols may be the ones for integration in those scenarios.

C. Review Methodology

The methodology regarding the literature review conducted was as follows. An exhaustive online search was conducted in order to identify key works reviewing classical cryptography and PQC algorithms. For such initial search, the traditional databases for classical cryptography were explored, i.e., IEEE Xplore, ACM and the Cryptology ePrint Archive. Many references regarding PQC were found in those sources, but the review by Bernstein and Lange was specially useful to identify many lines and references regarding such field [21]. Furthermore, the NIST standardization process was also an starting point to identify many of the methodologies that present the potential to be implemented. Since the NIST standardization stands as the mainstream process in this line, it was the starting point to identify PQC protocols that go beyond the basic theory for PQC families. Once studied, we followed to other standardization efforts since one of the points of this perspective is to show that many global agents are independently doing such process and we wanted to show the heterogeneous nature of this field. Moreover, (post-quantum) cryptography is a dynamic field so many related blogs, e.g., Cloudflare[2] or Google Bughunters,[3] were regularly read in order to follow developments of those fields at the time of writing this article. Regarding industrial cryptography, we based on the knowledge of one of the authors (G. Vidal) in order to identify a preliminary batch of relevant literature regarding this topic. Afterwards, we complemented such literature by means of IEEE Xplore and ACM databases as well as by getting references from such initial set of articles. Last but not least, some missing references were pointed by the referees, which were discussed for completeness of the work.

Once the literature was collected and understood, all the information was used to make discussions regarding the implementation of PQC in industrial networks as well as to identify which are the challenges associated to it. This has been done by comparing the core problem of IT cryptography in contrast to OT cryptography, which is the one tackled in this perspective. In this way, it has been seen that most of the PQC protocols that have been proposed would have difficulties to be integrated in industrial networks as they have been constructed from the IT point of view. Finally, future work has been pointed out in order to make such scenarios quantum secure.

II. Industrial Environments

ICS are the components of the industrial sector and infrastructures, from essential services, such as energy, water, transportation systems to manufacturing plants, agricultural systems, building automation systems, etc. In these infrastructures we will always find complex components that share a common denominator: physical processes that are modified by logical computation or viceversa. These components are called cyber–physical systems (CPSs). In Fig. 1, we show an example of ICS. In this example, in short, the instrumentation sensors measure physical variables, programmable logic controllers (PLCs) implement a control loop and send signals to the actuators. All the process is controlled and monitored by the supervisory control and data acquisition (SCADA) and the operator interacts via the human–machine interface (HMI) or the Engineering Work Station (EWS).

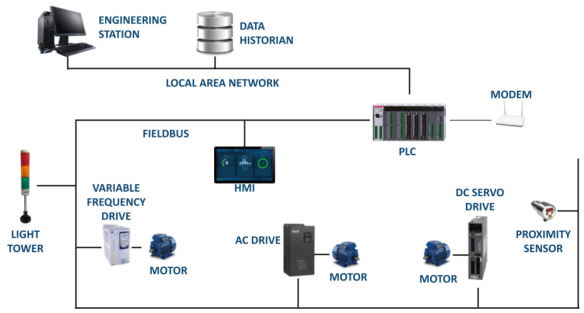


Fig. 1. Example of ICS network diagram.

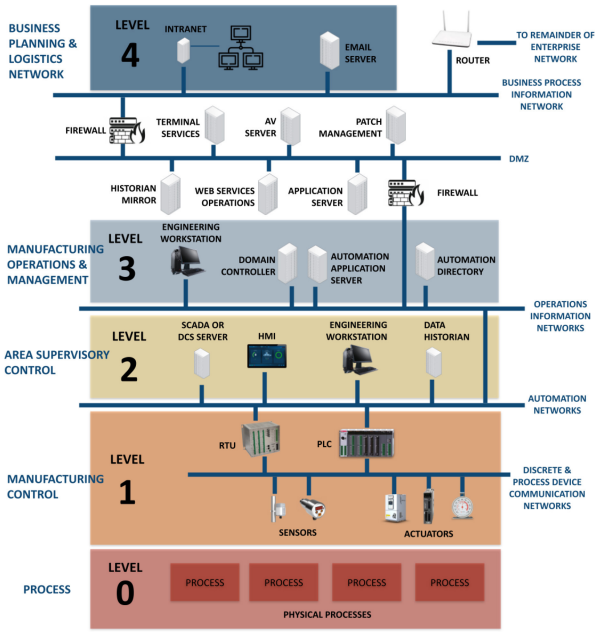


Fig. 2. Purdue model of interaction between IT and OT services.

Since these systems control real world processes, any potential cyberattack impact on them could imply a physical effect in the real world. Hence, cyber-risks could turn not only into production downtimes but also physical damage to operators or users. A good survey of different objectives and techniques used to attack ICS networks has been collected in MITRE ATT&CK.[4]

ICS and CPS are a part of larger infrastructures which interact with IT systems at certain point. In Fig. 2, we show how IT and OT interact in this type of infrastructures according to the Purdue model, even though there are several models, such as RIA 4.0 and others.

The mitigation of these risks is challenging since the security mechanisms and techniques that are suitable for IT do not match the needs in OT.

[2]https://blog.cloudflare.com/

[3]https://bughunters.google.com/blog

[4]https://attack.mitre.org/

A. Differences Between IT and OT

Understanding the inner differences between IT and OT communications are essential in the realm of cybersecurity, particularly when safeguarding CI like energy systems. First, one of the most prominent distinctions lies in their component lifetimes. OT systems often rely on hardware with a lifespan of up to 20 years, whereas IT systems typically have a significantly shorter lifespan of 3 to 5 years. This variance makes it challenging for OT systems to stay updated with the latest security measures, as their components may become outdated and incompatible with newer cybersecurity technologies over time.

Second, availability requirements vary significantly. OT systems demand extremely high levels of availability since any downtime can have severe consequences. In contrast, IT systems usually have more moderate availability requirements. This discrepancy emphasizes the need for robust cybersecurity measures in OT to prevent disruptions that could impact critical operations.

Moreover, real-time requirements diverge between the two domains. OT systems often require real-time responsiveness, with certain elements in the energy sector requiring millisecond-level reactions to commands [27], [47]. This real-time demand can make it challenging to introduce comprehensive cybersecurity measures in OT systems due to the need for rapid response, whereas in IT systems, real-time requirements are typically less stringent, allowing for more deliberate and thorough security implementations.

Additionally, the approach to patching and security standards differs significantly. In IT, security standards are generally more mature, and patching can be executed relatively quickly. In contrast, the OT sector faces slower patching processes often constrained by regulations. This slow pace can leave OT systems vulnerable to emerging threats for extended periods. Lastly, while both domains attend to data integrity, OT systems typically emphasize data integrity as a top priority, while confidentiality is considered a lower to medium priority. In contrast, IT systems prioritize confidentiality as a must, alongside integrity and availability.

Also, we need to remark an additional issue: the cybersecurity generational gap. From a cybersecurity perspective, the age of an industrial plant can significantly impact the cost and complexity of achieving a high level of cybersecurity. Let's delve into this scenario:

When starting a new company or building a modern industrial plant today, you have the advantage of being able to incorporate cybersecurity measures from the very beginning. Many modern components and systems are designed with cybersecurity in mind, often featuring embedded security features and protocols. This not only simplifies the process of implementing cybersecurity but also reduces the overall cost. It is essentially a proactive approach that builds security into the infrastructure from the ground up.

However, the challenge arises when dealing with older industrial plants, where the components and systems were likely not designed with cybersecurity in mind. These legacy systems may lack modern security features, making them vulnerable to cyber threats. Retrofitting these older components with cybersecurity measures can be a complex and costly endeavor. It may involve upgrading or replacing outdated hardware and software, implementing security protocols, and training personnel to operate in a more secure manner.

Furthermore, integrating cybersecurity into an older plant often requires a careful balance between maintaining operational continuity and enhancing security. Downtime can be expensive and disruptive, so the process must be meticulously planned and executed.

In summary, the cost of achieving a high level of cybersecurity can be much higher in older industrial plants due to the need for retrofitting and upgrading legacy systems. In contrast, new companies and modern facilities have the advantage of incorporating cybersecurity measures at a lower cost from the outset, due to the availability of cyber-embedded components and systems. However, it is crucial for all organizations, regardless of age, to prioritize cybersecurity to protect CI and assets from evolving cyber threats.

B. Industrial Cybersecurity Standards and Mechanisms

Industrial vendors, recognizing the pressing need for enhanced cybersecurity, are taking significant steps to fortify their products and services [37]. This involves developing and implementing robust security measures throughout their supply chains and lifecycles. Governments worldwide are also taking an active role in formulating regulations and guidelines to address these challenges [48], [49]. They are working to create a secure environment for CI sectors, including energy, water, and transportation, by establishing cybersecurity frameworks and compliance mandates.

In parallel to the IT sector, where standards like ISO 27001 serve as well-established benchmarks, industrial sectors adhere to their specific standards, with IEC-62443 being the primary global reference [47]. This standard offers a comprehensive framework for ICSs' cybersecurity. It defines guidelines for secure design, deployment, and maintenance, providing a roadmap for organizations to bolster their security posture. Additionally, various countries, such as the U.S., the European Union, and China, have crafted regional regulations tailored to their specific requirements, reflecting the nuances of their industrial landscapes [48], [49], [50].

Furthermore, sector-specific regulations address the unique cybersecurity concerns within industries like water and electricity. These regulations take into account the distinct OT challenges that may not align perfectly with traditional IT standards. By tailoring security measures to the particularities of each sector, these regulations help bridge the gap between the IT and OT worlds, ensuring the protection of critical systems.

In addition to broader standards and regulations, there are specific standards for components and systems used in industrial environments. These may include industrial communication protocols and HW requirements. By adhering to these standards, organizations can ensure compatibility and security among different components and systems

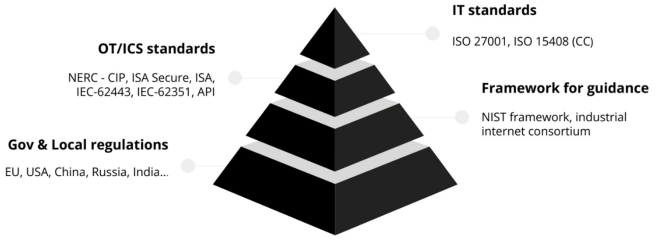


Fig. 3. This pyramid shows how standards are organized according to their level of definition in ICS.

within their infrastructure. The interoperability provided by these specific standards is crucial for maintaining a secure and efficient industrial ecosystem. Fig. 3 summarizes these interdependencies.

It is also worth mentioning that many of these legacy protocols were designed without strong security considerations, making them vulnerable to cyberthreats [as shown many times (pipedream [51], goose attacks [52], rogue7 [53], etc]. The introduction of virtual private networks (VPNs) into these setups helps create a secure tunnel for data transmission, adding an extra layer of protection. However, this adaptation does come with its own set of latency concerns, further highlighting the ongoing struggle to balance security with operational efficiency.

Additionally to the encryption challenges in industrial cybersecurity, recent regulations have begun mandating the use of VPNs in inherently insecure industrial protocols [50].

Moreover, the emergence of post-quantum encryption technologies has added a new dimension to the regulatory landscape. As QC capabilities continue to advance, traditional encryption methods may become vulnerable to rapid decryption, posing a significant threat to data security as we will discuss in the next section. In response, regulators are intensifying efforts to mandate the adoption of post-quantum encryption techniques in CI sectors. This drive for post-quantum encryption standards underscores the necessity for constant adaptation in the industrial cybersecurity field, where maintaining the integrity and confidentiality of data remains paramount, even in the face of evolving threats and technological advancements.

III. Prequantum Cryptography and Quantum Apocalypses

A. Overview on Cryptography

Cryptography is the study of algorithms which are able to make some information unintelligible to a third party (providing confidentiality), to protect it under changes from a third party (providing integrity) and to prevent that a third party masquerades as one of the trusted communication parties (providing authenticity). Mathematical tools for encrypting valuable information have been developed since the dawn of civilizations, with notorious examples, such as the Caesar cipher (a shift cipher where each letter is substituted by another letter in a fixed number of positions down the alphabet), used by the Roman Emperor Julius Caesar.[5] New encryption algorithms were discovered since those primitive days of cryptography because they had been cracked by other entities trying to obtain the protected information. For example, one of the most important events of World War II was breaking the Enigma code used by Nazi Germany to protect commercial, diplomatic and military communication. The digital revolution brought the possibility of evolving cryptographic techniques by means problems that are harder to solve, but, at the same time, it provided an additional tool for hackers to crack those codes.

Modern cryptography distinguishes two types of cryptosystems depending on how a message is encrypted: 1) symmetric and 2) asymmetric key schemes. Symmetric key schemes make use of the same key for encryption and decryption algorithms. For example, the advanced encryption standard (AES) proposed by J. Daemen and V. Rijmen in 1998, also known as Rijndael scheme, is the most implemented symmetric cryptosystem scheme [54]. On the other hand, asymmetric key schemes or public key schemes consist of two different algorithms and keys for each of the parties sharing secrets: 1) each of the parties use their public key (generated by the other party) to encrypt messages and 2) their private key (generated by itself) for decrypting the received messages. One of the most famous and most used asymmetric key cryptosystem scheme is the RSA cryptosystem, developed by Rivest, Shamir and Adleman [5].

In the ensuing paragraphs, we provide a comprehensive explanation of both schemes based on a network composed of three parties: 1) a server; 2) a user who wants to have a secure connection with it; and 3) an eavesdropper who wants to obtain information about the message. In cryptography those are usually referred to as Alice, Bob and Eve, respectively.

1) Symmetric Key Schemes: Symmetric key schemes are cryptosystems where both parties, Alice and Bob, share the same key, i.e., they use the same bit string to cipher and to decipher the message. The security of a symmetric scheme relies on the length of the key and on the fact that the key keep its secret to other parties. In this schemes, the key exchange is the most important process since all the security relies on the privacy of such key. If an eavesdropper, Eve, is able to obtain information about the key, the communication is not secure anymore. The most popular symmetric key scheme is the previously mentioned AES [54], Blowfish [55] and its more recent version Twofish [56] are also relatively popular open access schemes. To discuss the basic operation of a symmetric key exchange protocol, we begin by explaining how confidentiality and integrity/authenticity are achieved in the communication between the parties:

1) *Confidentiality:* The confidentiality in a symmetric scheme cryptosystem relies on the secrecy of the key. Eve knows how the algorithms which encrypt and decrypt the message work and she could perform a brute force attack by trying all possible key combinations to decipher the message. This, however, is a very inefficient attack. Assuming a key length of n, Eve has to try

[5]This fact was stated by Roman historian Suetonius in *Vita Divi Julii*, 56.6.

2^{n-1} possibilities in average, which may take several years if the value of n is sufficiently large, even having access to the most powerful computers. Therefore, if the secret key is regularly changed, this type of attack is impossible.

2) *Integrity and Authenticity:* symmetric key exchange algorithms do not only cipher the plaintext (message), but they also create a message-authentication code (MAC) by means of the message and an authentication key, k_{auth}, in order to protect the integrity of the message and verify the identity of Bob. Alice can check this information with the decryption algorithm for deciding if Bob has been the sender or not.

Following our discussion, a symmetric key exchange cryptosystem has three steps for protecting a plaintext message:

1) *Key Exchange:* Alice and Bob exchange a secret key and an authentication key, (k_{sym} and k_{auth}, respectively), which usually are two bit strings, in a secure way. If Eve, an adversary, gets information about the keys, the communication will not be secure. An important challenge is how to do this key exchange using a telecommunication channel certifying that Eve do not get any information about the keys, whose solution will be explained in the next section.
2) *Encryption Algorithm (Enc) and Signature Algorithm (Sgn):* Bob, by means of the symmetric key (k_{sym}) encrypts the plaintext (Msg) generating the ciphertext (Ct). At the same time, he generates the MAC with making use of the authentication key (k_{auth}) and the message (Msg). Then, he broadcasts the ciphertext and the MAC, implying that both Alice and Eve have access to them. The broadcasted information would be

$$(\text{Enc}(\text{Msg}, k_{\text{sym}}), \text{Sgn}(\text{Msg}, k_{\text{auth}})) = (\text{Ct}, \text{MAC}).$$

3) *Decryption Algorithm (Dec) and Verification Algorithm (Vry):* Alice decrypts the ciphertext using the shared secret key, (k_{sym}), and recovers the message. Also, she checks if the MAC corresponds to the k_{auth}, she obtains a boolean value, b, i.e., $b = 1$ if it is correct or $b = 0$ if not

$$(\text{Dec}(\text{Ct}),\text{Vry}(\text{MAC}, \text{Msg}, k_{\text{auth}})) = (\text{Msg}, b).$$

Note that Eve will not be able to recover the message if she is not able to obtain information about the secret key or makes a brute force attack, which would take a lot of computational time.

2) Asymmetric Key Schemes: As defined above, asymmetric key or public key schemes are defined as cryptosystems where each of the parties involved in the communication use their own key to secure the information, the private key and the public key. Each of those are usually employed to share a secret between two parts and, therefore, this encryption schemes may be used for the confidential key exchange required in symmetric schemes, called key encapsulation mechanism (KEM). In this sense, this could refer to the transmission of the bit string used as the input of an algorithm which can be used by Alice and Bob to generate the same symmetric key. Otherwise, if it is used to encrypt the message it is called public key encapsulation (PKE). In asymmetric key schemes confidentiality, integrity and authenticity are achieved in the following ways.

1) *Confidentiality:* The confidentiality relies in the hardness of finding the solution of the mathematical problem that Eve, the eavesdropper, has to solve in order to obtain the secret key or recover the plaintext. The problems used in public key schemes are computationally hard problems that cannot be efficiently solved. Thus, with no additional information, Eve cannot obtain the information about the message that has been encrypted or the private key.
2) *Integrity and Authenticity:* The integrity and authenticity of the message is achieved by means of a digital signature. Digital signatures are based on a hard problem so that the algorithm makes use of a message and a private key as an input for providing a unique output which identifies the party and the message. Any change in the signed ciphertext produces a totally different output providing a way to protect the integrity of the message. The authenticity of the message is determined by the secret key and it can be checked by using the public key, i.e., all parties can check the authenticity of a message but it only can be signed by the owner of the private key.

Regarding the general operation of a public key cryptosystem, those are based on the following three algorithms.

1) *Key Generator Algorithm (Gen):* Alice creates her private key (Sk). By means of it and the selected asymmetric cryptography algorithm, she generates the public key (Pk) and sends it to Bob. Note that by sending the key to Bob, Alice broadcasts it as public information and, hence, anyone in the network can access to that information. A potential eavesdropper, Eve, can get and store such key to try to decrypt the message but she will no be able to crack it due to the complexity of the problem she has to solve as we will explain below, she will require an unreasonable amount of time to obtain the plaintext.
2) *Encryption Algorithm (Enc):* Bob with the public key encrypts the plaintext (the message Msg) generating the ciphertext (Ct). He then proceeds to communicate publicly the protected message

$$\text{Enc}(\text{Msg}, \text{Pk}) = \text{Ct}.$$

3) *Decryption Algorithm (Dec):* Alice uses her own private key and the decryption algorithm to obtain the message that Bob wanted to provide in a secure manner

$$\text{Dec}(\text{Enc}(\text{Msg}, \text{Pk}), \text{Sk}) = \text{Msg}.$$

This is the general scheme of an asymmetric key cryptosystem, the security of which relies on the assumption that Eve is not able to recover the original plaintext by just using the public key and the ciphertext. Such thing relies on a mathematical problem that is hard to solve but for which it is easy to prove if a given solution is correct or not. Those are usually referred as one-way functions. They are designed in such a way that Eve can not decipher the message in

reasonable time without the private key and she can not get any information about the private key by means of the public information. The most famous, and widely used, scheme is the RSA cryptosystem, developed by Rivest et al. [5]. Its security is based on the factorization of large numbers in their prime factors. Other used schemes are based on ECC, such as the elliptic curve Diffie–Hellman (ECDH) scheme [57].

3) Security Notion: Proving the security of a cybersecurity scheme is not a trivial problem, i.e., mathematically proving that a function is indeed an One-Way function is not a simple task. In fact, one of the "Millenium Prize Problems," known as the $P \stackrel{?}{=} NP$ problem [58], involves to prove if the set of the problems whose solution is hard to find is the same to the set of problems whose solution is easy to check. However, the security of cryptosystems can be studied by means of some security notions. There are three cases which have to be taken into account to study a cryptosystem's security. In all of them, the adversary who wants to break the security is modeled by a probabilistic polynomial time algorithm. The scheme is secure if the algorithm has no advantage for discovering the secret over a random guesser algorithm, i.e., it is said Eve has a negligible advantage if she guess the correct answer with probability $1/2 + \epsilon(k)$, where k is a security parameter and $\epsilon(k)$ is a negligible function. Following this logic, the three security notions considered are as follows.

1) *Ciphertext-Indistinguishability Under Chosen Plaintext Attacks (IND-CPAs):* Refers to the property where Eve is not able to distinguish a random ciphertext from an actual ciphertext whose plaintext is known by herself.
2) *One-Wayness Under Chosen Plaintext Attacks (OW-CPAs):* Refers to the property where Eve is not able to recover the plaintext, even when she has the ability to choose and encrypt any plaintext of her choice and observe the corresponding ciphertext.
3) *Key-Indistinguishability Under Chosen Ciphertext Attacks (IND-CCAs):* refers to the property where Eve can call the decryption algorithm as many times she needs for an arbitrary ciphertext but she is not able to guess the key.

4) Digital Signatures: Digital signatures allow to sign a message in such a way that the origin of a message can be verified and ensure that the message has not been altered. They are used to verify the authenticity and ensure the integrity of a message in a public key cryptosystem. In order to sign a message, the signer has to generate a private and a public key, the private key is used to sign the message and the public key is needed to verify if a message has been signed by the true party. This process is also done by three polynomial-time algorithms: 1) the key-generation algorithm (Gen), which generates the public (Pk) and the private keys (Sk); 2) the signing algorithm (Sign), which uses the secret key to sign a message; and 3) the verification algorithm which checks by means of the Pk if a message has been signed by the party who generated the public key.

The security of a Digital Signature resides in the probability that a malicious party is able to sign a message without having access to the Sk and it can be verified satisfactorily. It is worth to say that the security of digital signatures resides on the computational complexity of an algorithm to solve the hard problem in which signature security relies on. Therefore, the same security notions in public key schemes explained above are applied to digital signatures. Nonetheless, in this case the adversary is interested in signing a message. I.e., Eve wants to masquerade as a trusted party, rather than acquiring information about a protected message. One of the most used digital signature scheme is the Elliptic Curve Digital Signature Algorithm (ECDSA) [59] based on ECC.

B. Quantum Apocalypses

Quantum computers promise to be huge step forward in computation as a result of being able to reduce significantly (exponentially for some algorithms) the number of operations an algorithm needs to solve some computational problems. There are two important quantum algorithms which will compromise the security of the current computer network security systems: 1) Grover's algorithm [60] and 2) Shor's algorithm [8].

Grover's algorithm provides a quadratic speedup for searching the secret key in symmetric key cryptosystems [21]. As said before, the security in these schemes relies on the key's secrecy and its length since a brute force attack consists in searching the n-bit combination. Therefore, the complexity of a classical brute force attack is bounded by 2^{n-1} on average, while a quantum computer could run Grover's algorithm to reduce the maximum number of steps to $2^{n/2}$, on average. This algorithm does not compromise the symmetric cryptography paradigm since the qudaratic boost can be compensated by doubling the key size and increasing the computational cost of the key exchange and encrypt and decrypt algorithms, but as it is just doubling down the key size, the extra costs are rarely noticeable [21]. There are other quantum attack proposals to symmetric cryptography, such as variational quantum attack algorithms (VQAAs) [61], [62], but they do not compromises its security.

As explained before, the key exchange algorithm for establishing the secret key of a symmetric protocol is done with a public key (asymmetric) cryptosystem. In this sense, doubling the size of the key to be shared increments the complexity of the key generation algorithm of the public key scheme. However, increasing the computational cost is feasible in order to hold the security in almost all the cases and, hence, this is not problematic. Nonetheless, the security of a public key cryptosystem relies on the complexity of the hard problem which has to be solved to get the private key. For example, a brute force attack to RSA consists in trying all primes p and checking whether p is a factor of N, requiring $\sqrt{N}$ attempts in the worst case scenario, which is exponential in the digits of N (d) and, thus, is an unfeasible task for any classical computer. The most efficient classical algorithm to solve such problem, known as the general number field sieve [63], achieves a complexity of $\mathcal{O}(e^{\sqrt{\ln(n)\ln(\ln(n))}})$ asymptotically [64], using this method up to RSA-250 (250 digits) have been factorized satisfactorily [65].

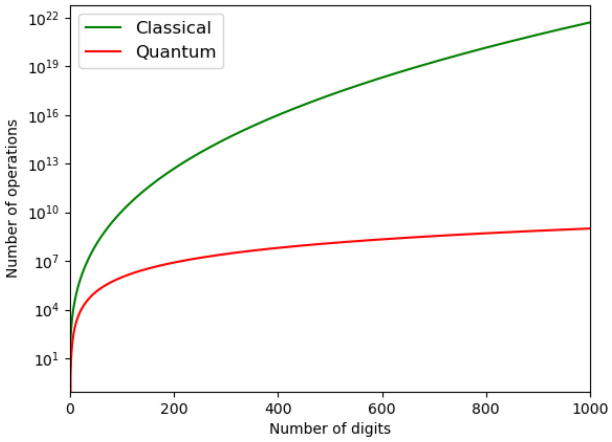


Fig. 4. Comparison between the operation's number of the general number field sieve and the Shor's algorithms to break RSA cryptography.

A large enough fault-tolerant quantum computer could run Shor's algorithm, which is able to factor a number in its primes taking advantage of the laws of quantum mechanics. The first large enough quantum computer will be able to solve factorization problem using $10d$ logical qubits,[6] where d is the number of digits, with a complexity of $\mathcal{O}(d^3)$ [64]. A comparison between both algorithms, in terms of their bounds in number of steps, is represented in Fig. 4, where the huge difference (exponential speedup) between both algorithms when the number of digits increases can be easily observed.

Therefore, Shor's algorithm is a potential threat to the security of all communications over the world, and will be a real problem in the near future since it is able to break most used public key cryptosystems, RSA and ECC schemes. As a result, governments and private companies, such as technological giants IBM, Google, and Microsoft, to cite some of them; are dedicating an immense amount of economical and human resources to develop a large enough functional quantum computer (fault-tolerant) able to compute Shor's algorithm and break the current cybersecurity. Hence, new cryptography schemes are required in order to protect our communications and documents in the post-NISQ[7] quantum era. Another issue to take into account is the fact that some people speculate about the possibility that some global agents are storing encrypted communications for decrypting it in the future once fault-tolerant quantum computers are available. Thus, finding an alternative to RSA and ECC cryptography resistant to quantum attacks is a very relevant problem nowadays. Moreover, it is estimated that a secret holds its value for 15 years [16] and, thus, it is necessary to consider public key cryptosystems based on hard problems that can not be solved efficiently by quantum computers as soon as possible, i.e., it is necessary to implement quantum resistant algorithms 15 years before the first functional quantum computer is available. Google, IBM, China and Xanadu have shown quantum advantage using their computers and they expect a huge increase in their quantum computer capability during the following years [9], [10], [11], [12], [13]. To sum up, we are at a critical moment for cryptography.

It is in this paradigm that the most promising technologies for the future quantum-safe cryptography are QKD and PQC. QKD takes advantage of quantum superposition and the no-cloning theorem [69] to exchange a pair of symmetric keys in such a way that Eve is not able to achieve any information of the key, since if she tries to get it Alice and Bob are able to detect such an attempt and discard the exchanged key. Alice and Bob are able to do such things due to the properties of quantum mechanics (no-cloning, entanglement). This proposal is a good candidate for establishing future secure communications, but it is still a nascent technology with many problems as well as requiring a huge investment in infrastructure. Also, QKD is pretty susceptible to DDoS attacks since it can be done just by adding photons to the optical fiber or by measuring the emitted photons, since measuring a quantum state destroys the quantum information inside it. On the other hand, PQC is a family of different asymmetric key schemes which are secure against classical and quantum attacks. This proposals are based on hard problems for which quantum computers do not offer a substantial (not to say any) speedup. In this article we will focus on the PQC solution, specially since the objective of the present manuscript is to understand how quantum secure cryptography can be integrated in industrial and CI networks. As reviewed before, those networks pose some stringent conditions, such as low latencies or adaptability, to legacy devices implying that the integration of cryptography to such scenarios must be almost seamless. Hence, it seems straightforward to discard QKD as a realistic candidate for the transition to quantum secure communications in ICS/CI as a results of the high cost and infrastructure need that the technology requires, also because DDoS attacks are very harmful to CI due to the reduction of the availability.

IV. Post-Quantum Cryptography

PQC refers to classical cryptographic methods based on hard problems whose solution cannot be found in polynomial time by neither classical nor quantum computers. The hardness of the problem is defined by the computational complexity of an algorithm capable to solve it. In this sense, a quantum computer should not provide any advantage (or such should be almost negligible) in solving the hard problem that stands at the core of a PQC protocol. Note that, as we commented in Section III-B for the case of symmetric cryptography, doubling the key length seems to be enough to keep the security level of classical methods against Grover search attacks. However, CI networks present strong latency requirements implying that doubling the key length could not be an acceptable solution. In this context, there are some proposals for lowering the computational and memory requirements of symmetric key cryptosystems, named lightweight cryptography

[6]Note that this number refers to logical or "noiseless" qubits [66]. For quantum computers to work, quantum error correction is required implying that many more physical or "noisy" qubits will be required for an implementation of the Shor algorithm that cracks RSA [67].

[7]Noisy intermediate-scale quantum era: Refers to time scale in which quantum advantage has been firmly proven, but the quantum computers available are still small and too noisy to offer the full potential of QC [68]. NISQ is where we stand right now.

(LWC) [70]. LWC reduces the required data to achieve secure communication channels and, thus, reduces the needed device computational resources [71], [72]. Furthermore, it is applicable to networks with legacy and computationally limited devices, including CI networks. Recently, the NIST has finished its standardization process for LWC [73], including some quantum resilient methods, such as Ascon-80pq [74]. In this work we will focus on the key agreement processes (asymmetric key schemes), which stand as more problematic in the context of industrial OT communications due to their latency and computational requirements.

In the following section we will introduce the different hard problems in which PQC methods are based. It is believed that such hard problems are secure against classical and quantum attacks. However, as explained earlier, the security of a cryptosystem is based on some assumption instead of mathematical proofs, hence, it is not possible to assure that any new proposed cryptosystem is secure. Hybrid cryptosystems were proposed in order to keep the current cybersecurity and add quantum resilient protocols, if the PQC protocol is proven to be insecure under classical and quantum attacks in the future the communication protocol would maintain the current security. Hybrid cryptosystems were also conceived to help to the transition from classical to quantum cryptography [75]. Despite of being a very active field and a good proposal to OT cybersecurity, we will not talk about hybrid solutions. Nonetheless, we encourage the interested reader to read the following papers [75], [76], [77].

PQC algorithms emerge as a consequence of assuming that a possible attacker has, or will have, a large and reliable enough quantum computer to break classical algorithms. Therefore, the new cryptography algorithms have to be hard to solve for classical and quantum computers implying security in the quantum era. These algorithms are usually divided into seven different families based on the hard problem in which their security relies on: 1) hash-based; 2) code-based; 3) lattice-based; 4) multivariate; 5) isogeny-based; 6) multiparty computation (MPC); and 7) graph-based cryptography. A diagram of the different families with the most important proposed schemes is represented in Fig. 5. In the following sections we will review the basic operation of such schemes, including an enumeration for each family of the different implementations, proposed to be standardized in the future. Several global entities, such as the U.S., China, or the European Union, have started own PQC standardization processes considering different candidates of each family. In this sense, we also provide an overview of those processes around the world. We encourage the interested reader in this topic to read the review made by Bernstein and Lange [21] and by Bavdekar et al. [78], based on PQC families proposed to NIST standardization process.

A. Hash-Based Cryptography

Hash-based cryptography was first proposed by Ralph. Merkel in the 70s [79]. The security of this cryptosystem relies on hash functions. A hash function (H_M) is a mathematical function that compresses an input string of bits of arbitrary length to a string of fixed length, i.e., it maps an input of an undetermined length into an output of fixed length m, which appears to be random but is deterministic. Formally, a hash function is defined as

$$H_m : \{0, 1\}^* \rightarrow \{0, 1\}^m.$$

Hash functions are usually employed to create digital signatures, deemed as hash-based signatures (HBS), providing authenticity and integrity to the communication. The first signature scheme using hash-functions was introduced by Lamport [80]. Those functions can be classified into one way hash functions (OWHFs), collision resistant hash functions (CRHFs) and Universal OWHFs (UOWHF). The general scheme of a hash function cryptosystem is composed by three algorithms, Gen, Enc, and Dec in the case of encryption or Gen, Sign, and Vry in the case of a digital signature scheme.

1) *Gen:* The key generation algorithm generates a public key (Pk) and private key (Sk). In general, this is done by choosing a private random seed, seed(n), i.e., a random bit string. A key (k) is derived from the seed by setting it as the input of a hash chain, which is a sequence of hash functions where the output of one hash becomes the input of the next one and it may involve other private functions, $f_i(x_i)$. Usually, the Sk is composed by the key, the seed and the parameters of the hash chain. Finally, the public key (Pk) is a parameter of the entire hash chain, but it does not reveal the individual hash values

$$\begin{aligned} \text{Sk} &\leftarrow \{H(x_n), n, f(x_i)\} \\ \text{Pk} &\leftarrow x'_m | m \leq n. \end{aligned}$$

2) *Enc/Vry:* Bob can use the public key to encrypt messages, recreating the hash chain to generate the ciphertext (Ct) or to verify the signature of Alice ($b = 1$ if Alice is the emitter or $b = 0$ if not)

$$\begin{aligned} \text{Ct} &\leftarrow \text{Enc(H, Pk, msg)} \\ b = 0, 1 &\leftarrow \text{Vry(H, Pk, sig)}. \end{aligned}$$

3) *Dec/Sign:* Alice is able to decrypt the message of Bob with the private key and to sign her messages by means of the private key

$$\begin{aligned} \text{msg} &\leftarrow \text{Dec(H, Sk, Ct)} \\ \text{Sig} &\leftarrow \text{Sign(H, Sk, msg)}. \end{aligned}$$

1) Security Notion: The security notion of a hash function resides in three characteristics that must have in order to be secure: 1) preimage resistance; 2) second-preimage resistance; and 3) collision resistance. These can be formally defined as follows.

1) *Preimage Problem:* Given the output of the hash function, $H_m(x)$, find the input x (One-wayness function).
2) *Second Preimage Problem:* Given the output of the hash function, $H_m(x)$, and the input x, find another input, y, that fulfills $H_m(x) = H_m(y)$ with $y \neq x$ (Weak collision resistance).
3) *Collision Problem:* Find two inputs, x and y, which fulfill $H_m(x) = H_m(y)$ (strong collision resistance). If a

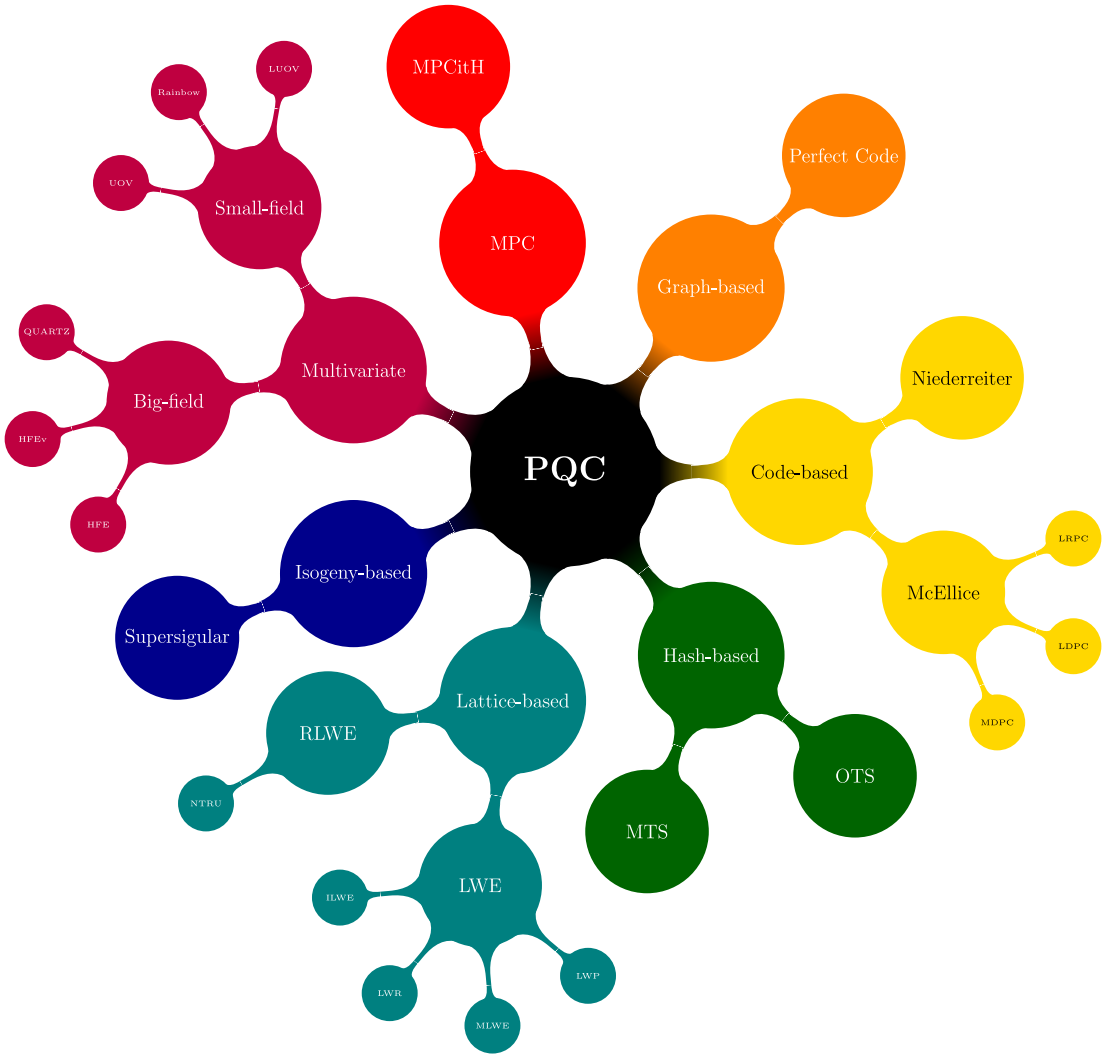


Fig. 5. Diagram of the different PQC algorithm families and the most important proposed cryptosystems.

Hash-function has collision resistance it implies second preimage resistance.

A hash function takes an input of arbitrary length and gives an output of a fixed length, as we said above. For being a "good" hash function it has to give completely different outputs for two random inputs. This characteristic it is guaranteed if the hash function has the following properties.

1) *Strong Avalanche Effect:* A small change in the input of the Hash function produces a huge change in the output.
2) *Completeness:* Each bit of the input string has an effect on all the output bits.

The collision problem is the problem whose solution is found with less computational complexity for both classical and quantum computers, hence, its security is bounded by the resilience of a hash function to this attacks, i.e., it has to be collision resistant. A classical algorithm finds the solution with a complexity of $\mathcal{O}(2^n/2)$ and a quantum computer is able to solve it more efficiently with a computational cost of $\mathcal{O}(2^n/3)$ but without compromising its security [81].

2) PQC Protocols: There are two types of hash-based digital signatures (HBS): 1) the one-time signature (OTS) scheme and 2) the multitime signature (MTS) scheme, sometimes called statefull HBS and stateless HBS, respectively. The principal difference between them is the times that a secret key can be used without losing the security assumption. Only Europe, Japan and the U.S. have a HBS algorithm in their standardization process, SPHINCS+ [82], which is a MTS signature scheme. The parameters of such algorithm is available in Table II. SPHINCS+ has been implemented on an Artix-7 FPGA [83] and on an ARM CortexM3 [84].

B. Lattice-Based Cryptography

Lattice-based cryptography is based on hard problems involving lattices. It is a special case of the subset sum problem-based cryptography proposed by Merkle and Hellman [85]. Generally, a lattice is defined as an infinity grid of points represented by a linear combination of linearly independent vectors, called basis, $B = b_1, b_2, \ldots, b_n$

$$\mathcal{L}(B) = \left\{ \sum_i c_i b_i : c_i \in \mathbb{Z} \right\}.$$

Thus, any point of the lattice is represented by an unique combination of the vectors of B. It is by definition a discrete subgroup of $\mathbb{R}^n$, since $\mathcal{L}$ spans $\mathbb{Z}^n$ which is a subgroup of $\mathbb{R}^n$.

Hoffstein, Pipher, and Silverman proposed a lattice-based cryptosystem based on polynomial rings called "NTRU" in the 1990s [86]. The polynomial ring is defined as $\mathcal{R}_q = \mathcal{Z}_q[x]/(f(x))$, where $f(x) = x^n - 1$ if n is prime, or $f(x) = x^n + 1$ if n is a power of two. The NTRU cryptosystem depends on three integers (N, p, q) and four sets of polynomials $(\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\phi, \mathcal{L}_m)$, and it is composed by the following algorithms.

1) *Gen:* Alice gets two random polynomials (f, g) from $\mathcal{L}_g$, under the condition that f has inverses modulo q, F_q, and modulo p, F_p. The secret key (Sk) is the polynomial f and the public key is defined by $\text{Pk} \equiv h = F_q \cdot g \bmod q$.
2) *Enc/Vry:* To encrypt a message m chosen from the polynomial set $\mathcal{L}_m$, Bob has to choose a random polynomial ϕ from $\mathcal{L}_\phi$

$$\text{Ct} \leftarrow \text{Enc}(\text{Pk}, \phi, m) \equiv p\phi \cdot h + m \bmod q.$$

3) *Dec/Sign:* Alice uses the Sk to decrypt the message computing

$$\begin{aligned} a &\equiv f \cdot \text{Ct} \mod q \\ \text{msg} &\leftarrow F_p \cdot a \mod p \end{aligned}$$

where the coefficients of a are selected between $-q/2$ and $q/2$.

Another lattice-based cryptosystem is based on the learning with errors (LWEs) problem, which was proposed by Regev [87] and which will be later described. The three algorithms involving such cryptography scheme are as follows.

1) *Gen:* Given the dimension, n, of the lattice, the key generator algorithm generates the public and the private key as

$$\begin{aligned} \text{Sk} &\equiv s^t \leftarrow \mathbb{Z}_q^n \\ \text{Pk} &\equiv b^t = s^t A + e^t \end{aligned}$$

where A is a $n \times m$ modulo q random matrix and e^t is a random error vector, both of them selected from a probabilistic distribution.
2) *Enc/Vry:* Bob encodes the message, a bit string (msg), by using a secret vector $x \leftarrow \{0, 1\}^m$ and the public key

$$\text{Ct} \equiv (u, u') \leftarrow \left(Ax, b^t x + \text{msg} \cdot q/2\right).$$

3) *Dec/Sign:* Alice is able to decrypt the Ct using the Sk by computing

$$\text{msg} \cdot q/2 \approx u' - s^t u.$$

1) Security Notion: The security of Lattice-based cryptography relies on the following worst-case problems.

1) *Shortest Vector Problem (SVP):* Given a lattice $\mathcal{L}$ find a nonzero vector $\vec{v} \in \mathcal{L}$, whose norm $|\vec{v}|$ is minimized.
2) *Closest Vector Problem (CVP):* Given a lattice $\mathcal{L}$ and a vector $\vec{u}$ find vector $\vec{v} \in \mathcal{L}$ such that the distance between $\vec{u}$ and $\vec{v}$ is shorter or equal to the distance between $\vec{u}$ and the lattice $\mathcal{L}$, i.e., the problem involves minimizing the norm $|\vec{v} - \vec{u}|$.

Despite of the existence of an algorithm which finds the nonzero vector of the SVP in time $\mathcal{O}(2^n)$ [88], there is no quantum algorithm providing an exponential speedup. Indeed, it is worth noting that the SVP problem can be reduced to the CVP problem. Ajtai et al. [89] showed that there is a connection between the worst-case problems and the average-case problems in lattice-based cryptography and explain how to construct hard lattice instances from random instances. This connection implies that if there is a probabilistic algorithm that solves the hard problems in the average-case, then there exists a solution for the worst-case scenario. However, it has been proven that there is no probabilistic algorithm in polynomial time for the worst-case scenario. Finally, they conclude that a lattice-based cryptography scheme based on average-case problems can be designed with the security of the worst-case problems. The average-case problems related with lattices are as follows.

1) *Short Integer Solution (SIS):* Given a set of m vectors $\vec{a}_i \in \mathbb{Z}_q^n$ as the columns of a matrix $A_{n\times m}$, where q is a prime number and q define the modulus of the lattice, find a nonzero integer vector $\vec{v} \in \mathbb{Z}^m$ which fulfills $A \cdot \vec{v} = 0 \in \mathbb{Z}_q^n$.
2) *LWEs:* Given a set of pairs $(\vec{a}_i, b_i)$, where $\vec{a}_i$ and b are sampled from a certain distribution, find a secret vector $\vec{s}$ such that $\vec{s} \cdot a_i \text{mod} e_i = b_i$ and e_i is sampled from a Gaussian distribution over $\mathbb{Z}$.

Both problems are considered to be computationally hard for classical and quantum computers giving the security notion to lattice-based cryptography schemes. Specifically, the security of NTRU cryptography relies on the ring-LWE (RLWE) problem, a variant of LWE problem where the secret vector is an unknown polynomial $s(x)$ in $\mathbb{R}_q$ and is faster than LWE-based cryptography [90].

2) PQC Protocols: Lattice-based cryptography can be splitted in two different algorithms: 1) NTRU, developed by mathematicians Hoffstein et al. [86] and 2) LWEs first introduced by Oded Regev [87]. Lattice-based cryptography is the most promising quantum resistant cryptosystem, for encryption and signatures. This can be seen as different countries are proposing a large amount of lattice-based protocols to be standardized. The NTRU encryption protocols that have been proposed to be standardized are: NTRU [91], NTRU-HRSS [92], NTRU-Prime [93], and NTRU+ [94]. The following NTRU protocols have been also proposed to generate signatures: Falcon [95], FatSeal [96], Peregrine [97], and SOLMAE [98]. On the other hand, the LWE encryption protocols proposed to be standardized are: CRYSTALS-Kyber [26], Saber [99], FrodoKEM [100], LAC PKE [101], Aigis-Enc [102], AKCN-MLWE [103], TALE [104], AKCN-E8 [105], SCloud [106], and SMAUG-T, which is a merge of SMAUG [107] and [108]; and the following LWE protocols have been also proposed to generate signatures: CRYSTALS-Dilithium [109], Aigis-Sig [102], Mulan [110], NCC-Sign [111], and HAETAE [112].

The following lattice-based PQC protocols have been implemented in HW devices, some of them in devices with low-computational resources: NTRU, NTRU-HRSS, and NTRU-Prime on an Artix-7 and on aZynq UltraScale+ [113];

TABLE I
PERFORMANCE OF LATTICE-BASED PQC PROTOCOLS. CIPHERTEXT (CT) AND KEYS LENGTH ARE EXPRESSED IN BYTES. ALL VALUES ARE TAKEN FROM THE LEVEL I SECURITY DEFINED BY NIST: "ANY ATTACK THAT BREAKS THE RELEVANT SECURITY DEFINITION MUST REQUIRE COMPUTATIONAL RESOURCES COMPARABLE TO OR GREATER THAN THOSE REQUIRED FOR KEY SEARCH ON A BLOCK CIPHER WITH A 128-BIT KEY (E.G., AES128)" [176]

Lattice-based	Public Key	Private key	Ct/Signature
NTRU [168], [133]	930	1234	930
NTRU-HRSS [169], [133]	1 138	1 450	1 138
NTRU-Prime [169], [170], [133]	994	15 158	897
NTRU+ [94], [171]	864	1 728	864
Falcon citeFalconPerf,NIST3	897	7 553	666
FatSeal [96]	2 321	385	2 048
Peregrine [97], [171]	897	7 553	666
SOLMAE [98], [171]	897	7 553	666
CRYSTALS-Kyber [172], [133]	800	1 632	768
Saber [169], [133]	672	832	736
FrodoKEM [100], [133]	9 619	19 888	9 720
LAC PKE [101]	544	1 056	704
Aigis-Enc [102], [173]	672	1 568	672
AKCN-MLWE (AES256) [103]	10 560	10 560	8 610
TALE [104], [174]	736	1 504	704
AKCN-E8 (AES256) [105]	928	928	896
SCloud (AES256) [106]	98 800	19 800	82 300
TiGER [171], [108]	480	177	640
SMAUG [171], [107]	174	672	768
CRYSTALS-Dilithium(AES192) [133]	1 312	2 528	2 420
Aigis-Sig [102]	672	1 568	672
Mulan [110]	1 312	2 528	2 420
GCKSign [175], [171]	1 760	288	1 952
NCC-Sign [111], [171]	1 440	2 400	2 529
HAETAE [112], [171]	992	1 376	1 463

NTRU+ on a Xilinx Zynq-7000 [114]; Falcon on an ARM Cortex-A53 [115] and on an ARM CortexM3 [84]; CRYSTALS-Kyber on a Xilinx Artix-7 [116], on a Xilinx Artix-7 and on a Virtex-7 FPGAs [117] and on 64-bit ARM Cortex-A processors [118] using number-theoretic transform (NTT) optimization [119], [120], Saber on a Xilinx UltraScale+ [121] and on an Artix-7 and on a Zynq UltraScale+ [113]; and LAC on a Xilinx Zynq-7000 [122] and CRYSTALS-Dilithium in [123] on Virtex UltraScale+ and on an ARM Cortex-M4 [123].

The parameters of those algorithms are available in Table I. In [124] they give a good survey explaining different aspects of lattice-based cryptography as their theory, security and performance. They include NIST and Chinese standardization processes.

C. Code-Based Cryptography

The first instance of a code-based cryptosystem was conceived by McEliece [125], which consisted in using the complexity of decoding a syndrome within code theory in order to encrypt messages with a high level of security. While proving a fine level of security, the McEliece cryptosystem usually suffers from excess in memory since it precises large ciphertexts and key pairs. Given this backdrops, a second version introduced by Niederreiter [126] proposed a variation that allowed faster key generation and message sending while preserving the security given by the McEliece cryptosystem [127].

TABLE II
PERFORMANCE OF HASH-BASED PQC PROTOCOLS. CIPHERTEXT (CT) AND KEYS LENGTH ARE EXPRESSED IN BYTES. ALL VALUES ARE TAKEN FROM THE LEVEL I SECURITY DEFINED BY NIST: "ANY ATTACK THAT BREAKS THE RELEVANT SECURITY DEFINITION MUST REQUIRE COMPUTATIONAL RESOURCES COMPARABLE TO OR GREATER THAN THOSE REQUIRED FOR KEY SEARCH ON A BLOCK CIPHER WITH A 128-BIT KEY (E.G., AES128)" [176]

Hash-based	Public Key	Private key	Ct/signature
SPHINCS+ [82], [172], [133]	32	64	7 856

The McEliece cryptosystem requires being able to generate a random t-correctable (n, k)-code, that is, a k-dimensional code composed of n bits able to correct all errors of weight equal or less than t. Given this condition the key generation goes as follows.

1) *Gen:* a t-correctable (n, k)-code with generator matrix G and parity check matrix H is randomly generated altogether with a random nonsingular binary matrix S of size $k \times k$ and a random permutation matrix P of size $n \times n$. Finally, the matrix product $G' = SGP$ is computed, which is itself a new code. The key pair can now be introduced
$$\text{Sk} \equiv G \in \mathbb{F}_2^{k\times n}, S \in \mathbb{F}_2^{k\times k}, P \in \mathbb{F}_2^{n\times n}$$
$$\text{Pk} \equiv G' \in \mathbb{F}_2^{k\times n}.$$
2) *Enc:* the plaintext that is to be encrypted must be presented as a k-dimensional binary vector $\mathbf{m} \in \mathbb{F}_2^k$. The message is encoded within the public key code, G', as $\mathbf{m}G'$. Additionally, an n-dimensional random error $\mathbf{e} \in \mathbb{F}_2^n$ of Hamming weight equal or lower than t must be introduced. The encryption process consists in adding the error $\mathbf{e}$ to the encoded message as: $\mathbf{c} = \mathbf{m}G' + \mathbf{e}$.
3) *Dec:* The private key owner can decipher a ciphertext by first computing $CP^{-1} = \mathbf{m}SGPP^{-1} + \mathbf{e}P^{-1} = \mathbf{m}SG + \mathbf{e}P^{-1}$. Afterwards, one can follow by computing $\mathbf{e}P^{-1}H^T = \mathbf{m}SGH^T + \mathbf{e}P^{-1}H^T = \mathbf{e}P^{-1}H^T = \mathbf{z}$, where $\mathbf{z} \in \mathbb{F}_2^{n-k}$ is the syndrome. Given that one knows H and $\mathbf{z}$, the error $\mathbf{e}P^{-1}$ can be obtained through decoding, which allows the private key holder to find $\mathbf{m}SG$. Furthermore, $\mathbf{m}SGG^T = \mathbf{m}S$ and, finally, by computing $\mathbf{m}SS^{-1} = \mathbf{m}$, one can reach the plaintext.

The Niederreiter cryptosystem builds upon the McEliece one by encrypting the plaintext through the error $\mathbf{e}$. In other words, the cryptosystem is slightly modified into the following.

1) *Gen:* a t-correctable (n, k)-code with parity check matrix H is randomly generated altogether with a random nonsingular binary matrix S of size $n-k \times n-k$ and a random permutation matrix P of size $n \times n$. Finally, the matrix product $K = SHP$ is computed. The key pair can now be introduced
$$\text{Sk} \equiv H \in \mathbb{F}_2^{n-k\times n}, S \in \mathbb{F}_2^{n-k\times n-k}, P \in \mathbb{F}_2^{n\times n}$$
$$\text{Pk} \equiv K \in \mathbb{F}_2^{k\times n}.$$
2) *Enc:* the plaintext which is to be encrypted must be presented as an n-dimensional error vector $\mathbf{e} \in \mathbb{F}_2^n$ of Hamming weight less or equal to t. Now, the message is

encrypted through the product $\mathbf{z} = \mathbf{e}K^T$, where $\mathbf{z} \in \mathbb{F}_2^{n-k}$ is the outcoming syndrome, which is the ciphertext.

3) *Dec:* The ciphertext can be decrypted by the key pair owner by first operating $\mathbf{z}(S^{-1})^T = \mathbf{e}P^T H^T S^T (S^{-1})^T = \mathbf{e}P^T H^T$, the result is a decodable syndrome given that we know the parity check matrix H. After decoding, one recovers $\mathbf{e}P^T$, upon applying $\mathbf{e}P^T(P^T)^{-1} = \mathbf{e}P^T P = \mathbf{e}$, which returns the plaintext. Note that permutation matrices are always orthogonal.

The Niederreiter cryptosystem allows for a code based-cryptosystem to happen without the requirement of storing the plain text within the code, which yields a time improvement. Nevertheless, this is done at the expense of the dimensionality change within the two cryptosystems. While the dimension of the plaintext of a McEliece cryptosystem using a t-correctable (n, k)-code is k, for a Niederreiter cryptosystem it is correspondent to the dimension of the space of n-dimensional binary error vectors of Hamming weight less or equal to t, which may be lower. This translates to the fact that less possible plaintexts can be ciphered.

1) Security Notion: Attacking either code-based cryptosystems may be done in two different ways. The first consists in attempting to separate the public key into the private key, which has been proved to be unfeasible [128]. The second one consists in attempting to decode the syndrome given K.[8] This problem is defined as the computation syndrome decoding problem, which is proven to be NP-complete [129], [130].

1) *Computing the Syndrome Decoding Problem:* given a binary linear t-correctable code of parity check matrix K and a syndrome $\mathbf{z} \in \mathbb{F}_2^{n-k}$ produced by the summation of a code word $\mathbf{x} \in \mathbb{F}_2^n$ with and an error $\mathbf{e}\mathbb{F}_2^n$ of weight equal or less than t by $\mathbf{z} = (\mathbf{x} + \mathbf{e})K^T$, find the error $\mathbf{e}$.

The best known generic attack on both cryptosystems is the Lee–Brickell attack [131], which sets the security of the code and proves that both the McEliece and the Niederreiter cryptosystem have the same level of security [127].

2) PQC Protocols: Two Niederreiter protocols have been proposed to be standardized: 1) BIKE [132], proposed to the NIST standardization process [133] and 2) PALOMA [134], proposed to the Korea PQC standardization process [135]. In the case of McEllice protocols, NIST process is considering Classical McEllice [125] and Hamming quasi-cyclic (HQC) protocols [136] and South Korea is considering REDOG [137].

The parameters of those algorithms are available in Table III. The following code-based PQC protocols have been implemented on a Xilinx Artix-7: BIKE [138], the classic McEliece [139] and HQC [140].

TABLE III
PERFORMANCE OF CODE-BASED PQC PROTOCOLS. CIPHERTEXT (CT) AND KEYS LENGTH ARE EXPRESSED IN BYTES. ALL VALUES ARE TAKEN FROM THE LEVEL I SECURITY DEFINED BY NIST: "ANY ATTACK THAT BREAKS THE RELEVANT SECURITY DEFINITION MUST REQUIRE COMPUTATIONAL RESOURCES COMPARABLE TO OR GREATER THAN THOSE REQUIRED FOR KEY SEARCH ON A BLOCK CIPHER WITH A 128-BIT KEY (E.G., AES128)" [176]

Code-based	Public Key	Private key	Ct/Signature
BIKE [133]	1 540	280	1 572
PALOMA [134], [171]	319 488	7 808	32
Cl. McEllice [133]	261 129	6 492	128
HQC [133]	2 249	40	4 481
Piglet-1 [177]	1 212	32	1 801
ROLLO-I [178], [171]	1 240	120	620
REDOG [137], [171]	14 250	1 450	830
Enhanced PQsigRm [179], [171]	2 000 000	✗	1 032

D. Multivariate Cryptography

Multivariate cryptography is a public-key cryptography scheme based on a multivariate and nonlinear polynomial map of a field $\mathbb{F}$. It was first proposed by Matsumoto and Imai [141]. In this scheme, a vector $x \in \mathbb{F}^q$ is mapped to a vector $x' \in \mathrm{F}^q$ through a map P composed of a set of nonlinear polynomials $p_1, p_2, \ldots, p_m$

$$P : \mathbb{F}^q \to \mathbb{F}^q \tag{1}$$

$$x = (x_1, \ldots, x_n) \to x' = (p_1(x), \ldots, p_m(x)). \tag{2}$$

The secret key is a nonlinear map P, and two affine maps S and T. An affine map is a linear map which connected two different affine spaces. The public key is the composition of the map with the affine maps S and T: $P_k = T \circ P \circ S$, which looks like a random map. Multivariate cryptosystems are composed by the following algorithms.

1) *Gen:* Alice generates an easily invertible quadratic map $P : \mathbb{F}^q \to \mathbb{F}^p$ and composes it with two affine maps, $S : \mathbb{F}^q \to \mathbb{F}^q$ and $T : F^p \to \mathbb{F}^p$

$$\mathrm{Sk} \leftarrow P, S, T$$
$$\mathrm{Pk} = P' \leftarrow T \circ P \circ S.$$

2) *Enc:* Bob uses the Pk to encrypt a message $m \in \mathbb{F}^q$ getting the ciphertext (Ct) and sends it to Alice

$$\mathrm{Ct} \leftarrow P'(m) \in \mathbb{F}^q.$$

3) *Dec:* Alice, by means of the Sk, decrypts the ciphertex obtaining the message

$$\mathrm{Ct} \leftarrow P(m) \in \mathbb{F}^q.$$

1) Security Notion: The security notion in multivariate cryptography relies on the NP-hard problem of finding preimages of multivariate polynomial maps. This is defined as follows.

1) *The Multivariate Quadratic (MQ) Problem:* Given a system of polynomials p_1, p_2, ..., and p_m, where each p_i is a nonlinear polynomial in n variables whose coefficients and variables are defined over F^q, find a solution $x = (x_1, \ldots, x_n)$ that satisfies $p_1(x) = p_2(x) = \cdots = p_m(x) = 0$.

The computational complexity to solve the MQ problem depends on the degree of the polynomials, the number of variables n and polynomials m and the field $\mathbb{F}$. The best classical algorithm to solve this problem is based on Gröbner bases, known as F5 [142], and there is not a known quantum algorithm which solves MQ problem faster than F5 algorithm [143].

[8] For the McEliece case, K can be obtained through G'.

TABLE IV
PERFORMANCE OF MULTIVARIATE PQC PROTOCOLS. CIPHERTEXT (CT) AND KEYS LENGTH ARE EXPRESSED IN BYTES. ALL VALUES ARE TAKEN FROM THE LEVEL I SECURITY DEFINED BY NIST: "ANY ATTACK THAT BREAKS THE RELEVANT SECURITY DEFINITION MUST REQUIRE COMPUTATIONAL RESOURCES COMPARABLE TO OR GREATER THAN THOSE REQUIRED FOR KEY SEARCH ON A BLOCK CIPHER WITH A 128-BIT KEY (E.G., AES128)" [176]

Multivariate	Public Key	Private key	Ct/Signature
GeMSS [172], [133]	352 168	16	33
Rainbow [144], [133]	157 800	611 300	164
MQ-Sign [147], [171]	328 441	15 561	134

2) PQC Protocols: There are two multivariate cryptosystems proposed to be standardized: 1) rainbow [144] and 2) GeMSS [145]. An implementation on an ARM CortexM3 of Rainbow and GeMSS is done in [84]. Both of them have been proposed in the NIST standardization process. However, recently, a new paper has been published claiming that the Rainbow protocol can be broken in just one weekend by means of a laptop [146]. On the other hand, South Korea has proposed a multivariate cryptography protocol called MQ-sign [147].

The parameters of those algorithms are available in Table IV. Rainbow has been implemented in a HW device in [148].

E. Isogeny-Based Cryptography

ECC is a public key cryptosystem developed in the 1980s by Koblitz [6] and Miller [7], who suggested separately in the same year to use elliptic curves in the Diffie–Hellman cryptography protocol. Hasse (1936) discovered supersingular elliptic curves during his work on the Riemann hypothesis for elliptic curves [149]. Since quantum attacks based on Shor's algorithm break ECC relying on the discrete-logarithm problem [8], this field was deemed as not secure. However, the interest in elliptic-curves for PQC was recovered due to the work in Supersingular-Isogeny Diffie–Hellman (SIDH) published by Jao and de Feo [150] and the work of Rostovtsev and Stolbunov [151]; and in Hard Homogeneous Spaces [152] protocols, both of them are based on random walks in graphs of horizontal isogenies.

An elliptic curve is a projective curve defined over a field k. Specifically, it composed by the set of points that fulfill the following equation:

$$E : y^2z = x^3 + axz^2 + b^3 \quad a, b \in k \quad \text{and } 4a^3 + 27b^2 \neq 0$$

where the point at infinity is $(0 : 1 : 0)$, when $z = 0$. In the affine space it is defined as

$$y^2 = x^3 + ax + b$$

with $\mathcal{O} = (0 : 1 : 0)$ as the point at infinity.

Following such definition, an isogeny is a map between two elliptic curves $\phi : E \rightarrow E'$, such as ϕ is a surjective group morphism, that preserves its identity $\phi(\mathbb{O}) = \mathbb{O}'$. Two curves are called isogenous if there exists an isogeny between them and, there is a isogeny if and only if $\#E(k) = \#E'(k)$, where # is defined as the cardinality of the elliptic curve. An elliptic curve defined over a field $\mathbb{F}_p$ has an invariant, called the j-invariant of a Montgomery curve, which determines the isomorphism class. It is defined by

$$j(E_{a,b}) = \frac{256(a^2-3)^3}{a^2-4}.$$

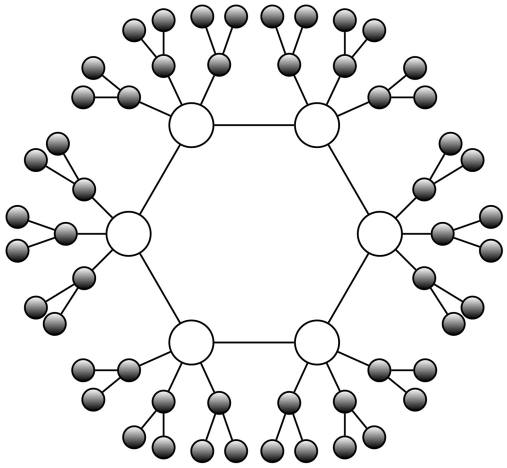


Fig. 6. Graphical representation of a graph of isogenies, where each node is a elliptic curve and each edge connect two elliptic curves if there exits an isogeny between them.

Two isogenous elliptic curves have different j-invariants, $j(E) \neq j(E')$ if they can be mapped by an isogeny ϕ, hence, an isogeny maps one isomorphism to another.

A graph of isogenies is a collection of elliptic curves, i.e., isomorphisms, connected by isogenies, where the elliptic curves are the nodes and the isogenies are the edges. An example is represented in Fig. 6.

Isogeny-based PQC protocols are based on random walks in isogeny graphs, obtaining a shared secret to be used as symmetric key between Alice and Bob. Isogeny-based protocols are only composed by the key exchange algorithm.

1) *Key Exchange:* The key exchange algorithm consists on random walks taken by Alice and Bob from the same Elliptic Curve E_0 along the graph. They publish the EC they have reached, E_A and E_B, and they repeat exactly the same random walk they followed before but from the EC the opposite party have published, reaching the same secret EC, E_S. It is easy to see that both paths have to commute: $P_A(P_B(E_0))$ has to be equal to $P_B(P_A(E_0)$, where P_i is the secret path they followed. Alice and Bod end the algorithm in the same elliptic curve with the same j-invariant, i.e., in the same isomorphism.

A singular EC is an EC with singular points, which are defined as points within the EC and in the curves defined by the two partial derivatives of the EC, known as the Jacobi criterion. Supersingular-Isogeny Diffie–Hellman (SIDH) cryptography is a special case of Isogeny-based cryptography whose security against classical and quantum attacks has been proved [153].

1) Security Notion: The security of Isogeny-based cryptography against classical and quantum attacks relies on the Supersingular Isogeny problem (SSIP).

1) *SSIP:* Given a prime p and two supersingular elliptic curves over $\mathbb{F}_{p^2}$, E and E' find an isogeny $\phi : E \to E'$.

The best algorithm to solve the SSIP and, hence, that breaks isogeny-based cryptography, is based on meet-in-the-middle attack and its complexity is $\mathcal{O}(p^{1/4})$, which requires $\mathcal{O}(p^{1/4})$ storage capability [153], or, in the case of Supersingular Isogeny key encapsulation (SIKE), its security is based on van Oorschot-Wiener (vOW) golden collision finding algorithm [154]. The best quantum algorithm is able to find the secret with $\mathcal{O}(p^{1/6})$, which is not a notorious advantage and does not compromise isogeny-based cryptography [153].

2) PQC Protocols: SIKE [155] is an encryption scheme based on Supersingular Isogeny Diffie–Hellman protocol proposed for the NIST standardization process. On the other hand, FIBS is a signature scheme based on the same protocol proposed in the South-Korean standardization process [156]. A compressed alternative of SIKE was proposed in 2016 by Axzarderakhsh et al. [157], requiring to transmit half of the data. This compressed SIKE was implemented in an ARM Cortex-M4 processor [158] and on a Xilinx Virtex-7 [159], the authors claimed that it is the algorithm which introduces the lowest latency to communications due to its low-computational requirements and the extremely compact key sizes. There are also works that try to speed-up the algorithm proposed by Jao and de Feo [150], such as the work of Koziel et al. [160].

The parameters of those algorithms are available in Table V.

F. Multiparty Computation Protocol and Graph-Based Cryptography

In the PQC standardization processes around the word only South Korea is still considering a protocol based on one of these problems as we will see in the next section [135].

1) Multiparty Computation Protocol: MPC Protocol cryptography is used in scenarios where several parties P_i want to make some data available keeping its confidentiality. As an example, we could imagine two different countries which wants to keep the trajectory of its spy satellite secret but they want to be sure that they have different trajectory in order to avoid collisions. Therefore, each party has a secret x_i, the trajectory of their satellite, which has to remain secret but they want to share some confidential information making sure they will not collide. This is known as the MPC problem. In this sense, the MPC paradigm relates with the interest of allowing some party to do some computations to extract some conclusions using some protected data without actually having access to the raw data. The zero-knowledge proof allows the entities to convince the other ones about something without making the data public. The first MPC scheme was proposed by Ishai et al. [161], known as MPC-in-the-head paradigm. The first application proof of this paradigm was presented by Giacomelli et al. [162] and protocols based on this paradigm can be used to generate signatures. Picnic [163] is a PQC signature scheme that has been proposed for the NIST standardization process, but that was rejected in the third round [133]. However, AIMer [164] PQC algorithm based on MPC-in-the-head paradigm had been selected for the second round in the South Korea PQC standardization process.

TABLE V
PERFORMANCE OF ISOGENY-BASED PQC PROTOCOLS. CIPHERTEXT (CT) AND KEYS LENGTH ARE EXPRESSED IN BYTES. ALL VALUES ARE TAKEN FROM THE LEVEL I SECURITY DEFINED BY NIST: "ANY ATTACK THAT BREAKS THE RELEVANT SECURITY DEFINITION MUST REQUIRE COMPUTATIONAL RESOURCES COMPARABLE TO OR GREATER THAN THOSE REQUIRED FOR KEY SEARCH ON A BLOCK CIPHER WITH A 128-BIT KEY (E.G., AES128)" [176]

Isogeny-based	Public Key	Private key	Ct/Signature
SIKE [133]	330	374	346
FIBS [156]	32	64	17 088

TABLE VI
PERFORMANCE OF MULTIPARTY COMPUTATION AND GRAPH-BASED PQC PROTOCOLS. CIPHERTEXT (CT) AND KEYS LENGTH ARE EXPRESSED IN BYTES. ALL VALUES ARE TAKEN FROM THE LEVEL I SECURITY DEFINED BY NIST: "ANY ATTACK THAT BREAKS THE RELEVANT SECURITY DEFINITION MUST REQUIRE COMPUTATIONAL RESOURCES COMPARABLE TO OR GREATER THAN THOSE REQUIRED FOR KEY SEARCH ON A BLOCK CIPHER WITH A 128-BIT KEY (E.G., AES128)" [176]

Others	Public Key	Private key	Ct/Signature
IPCC (AES80)[167]	4 800	400	92 000
AIMer [164]	32	16	5 904

2) Graph-Based Cryptography: Graph-based cryptography refers to perfect code cryptosystems (PCCs) proposed by Fellows and Koblitz [165]. The study of perfect codes (PCs) emerged in the field of information theory, since PCs over graphs corresponds to PCs over structured alphabets [166]. Despite of having its origin in the study of codes, we separate this cryptography from code-based cryptography explained in Section IV-C since the hard problem to be solved in order to break each of the cryptosystems is different. A graph is a mathematical object formed by a set of edges and vertices, where each vertex is connected to other vertices through edges. A PC in a graph is defined as the set of vertices A such that every vertex not included in A is connected to only one element in A. A graph is defined as $G = V, E$, where V is a set of vertices and E is a set of edges. Therefore, $A \subseteq V$ and for every $v \in V$, $N[v]$ contains only one element of A, where the set $N[v]$ is formed by the vertices connected by an edge to v. The security of this cryptosystem relies on the hardness of knowing if a graph has PCs or not, which is a hard problem by itself (NP-complete problem) [166], as well as on the hardness of finding the vertices which form the PC, which is conjectured to be a hard problem (NP-complete problem). IPCC [167] is a graph-based PQC protocol proposed to be standardized in the South-Korean standardization process, which improves the original ideas proposed by Koblitz.

G. Performance of PQC Algorithms

The NIST has defined 5 security levels to compare the performance of the different PQC algorithms when the security they provide is the same [176]. Some metrics on the performance of the different PQC algorithms proposed to be standardized to achieve first level of security are presented in: Table I (lattice-based), Table II (hash-based), Table III (code-based), Table IV (multivariate cryptography), Table V

TABLE VII
ADEQUACY OF PQC PROTOCOLS TO CI IN TERMS OF THEIR KEY AND CIPHERTEXT/SIGNATURE LENGTHS, THE NUMBER OF PQC ALGORITHMS PROPOSED TO BE STANDARDIZED AND THE AVERAGE COMPUTATIONAL TIME. THE LETTERS AND THE COLORS DEFINE THE SUITABILITY OF THE PQC FAMILY, BEING THE MOST SUITABLE (A/GREEN), MODERATELY SUITABLE (B/YELLOW), HARDLY SUITABLE (C/ORANGE), AND NOT SUITABLE (D/RED)

PQC family	Key lengths	Ct/Signature length	Number of PQC algorithms	Time*	Appropriate for CI
Hash-based	A	D	C	D	D
Lattice-based	B	B	A	A	A
Code-based	C	B	B	D	D
Multivariate	D	A	B	D	C
Isogeny-based	A	B	C	C	B
Multiparty	A	C	D	D	D
Graph-based	C	D	D	C	D

(isogeny-based), and Table VI (MPC and graph-based). In general terms their performance in OT communications can be briefly discussed as follows.

1) *Lattice-Based (Table I):* Lattice-based cryptography requires relatively small public and private keys as well as ciphertexts while showing a lower computational cost compared to other PQC families [180]. Hence, it is the most promising candidate to be implementable in ICS/CI scenarios.
2) *Hash-Based (Table II):* There is only one hash-based PQC protocol, Sphincs+, proposed along the world, and its problems are the large ciphertext and the lengthy signing time [172], which could make it not suitable for ICS/CI.
3) *Code-Based (Table III):* Their public and private keys' length are longer than for other PQC families implying that more memory is required. Also, the fact that deciphering the ciphertext requires a high-computational cost makes code-based not to be the best option to be deployed in an ICS/CI environment a priori [133].
4) *Multivariate-Based (Table IV):* Multivariate-based cryptosystems require large keys while their ciphertext lengths are the same as for other PQC families, or even shorter. Nonetheless, due to the high computational and memory resources requirements [180] multivariate cryptography is not the best option to be used in CI.
5) *Isogeny-Based (Table V):* Isogeny-based cryptography presents keys of moderate length, however, FIBS has a large signature, making it unappealing to be implemented in CI. Although isogeny-based protocols have small key sizes, the computational cost is a great disadvantage due to the low-computational requirements in ICS/CI.
6) *Graph-Based and MPC Cryptography (Table VI):* These are the least used PQC algorithms along the world. They are not receiving a lot of attention and, thus, their security against classical and quantum attacks are not as studied as for other PQC families. Due to the nature of ICS/CI is not in principle recommended to use protocols based on these hard problems for such contexts.

The result of this high-level comparison among PQC algorithms implies that, a priori, the most suitable protocols for its integration in ICS/CI networks are those that belong to the lattice-based cryptography family. It is important to note that during the writing of this perspective, a new preprint was posted proposing a quantum algorithm that solves LWE problem with a polynomial complexity [181]. While the method proposed does not break NIST PQC candidates, developments in this field may lead to such outcome. Thus, even if out speculative comparison leans toward them, this advances in quantum algorithms should be taken into account. The comparison is summarized in Table VII. However, and as discussed before, this conclusion is rather speculative and, thus, an actual comparison in the conditions of those scenarios should be done for obtaining accurate results and conclusions because it is probably that any of them satisfies all industrial infrastructure communication's constrains.

H. PQC Standardization Processes Around the World

Despite of the global concern regarding the cybersecurity threat posed by the possibility of constructing fault-tolerant quantum computers, not every country/entity has started a standardization process by their own, or if they has started they do not publish this information. In this context, the U.S. is the pioneer by means of the NIST PQC standardization process, which started in 2017 and is yet unfinished (at the moment they are conducting the fourth round [23]). Even if it stands as the largest standardization process, not all countries will adopt NIST recommendation and standardized PQC algorithms as a result of economical and political differences. Countries not aligned with the North Atlantic Treaty Organization (NATO) and the USA foreign policy are developing their own algorithms, such as, for example, China. However, even EU countries that belong to such alliances are developing PQC protocols and requirements by their own, e.g., Germany and France. There are other countries which are investing in quantum technologies but they do not have published a PQC standardisation process. However, by comparing Table VIII with Table IX it can be inferred that it is quite probable that they are making their own efforts to be quantum secure.

The main issue with the adoption of PQC schemes for cryptography tasks resides on the youth of most of the proposals. More concretely, there is not a wide experience in the integration of the schemes in real systems implying that the security of the experimental implementation of PQC

TABLE VIII
DATA HAVE BEEN OBTAINED FROM EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI) IN THE CASE OF EUROPE [182]; FROM CHINESE ASSOCIATION FOR CRYPTOLOGIC RESEARCH (CACR) IN THE CASE OF CHINA [183]; FROM NIST IN THE CASE OF U.S. OF AMERICA [133]; FROM BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI) IN THE CASE OF GERMANY [46]; FROM CRYPTOGRAPHY RESEARCH AND EVALUATION COMMITTEES (CRYPTRECS) IN THE CASE OF JAPAN [184]; FROM AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI) IN FRANCE [45]; AND FROM KOREAN PQC (KPQC) IN THE CASE OF SOUTH KOREA [135]. A DISCUSSION COMPARING THEIR PERFORMANCES IS GIVEN IN SECTION IV-G, WHILE A SET OF TABLES PRESENTING THE PERFORMANCE IS GIVEN IN SECTION IV

PQC Algo.	**Europe (ETSI)**	**China (CACR)**	**USA (NIST)**	**Germany (BSI)**	**Japan (CRYPTREC)**	**France (ANSSI)**	**South Korea (KpqC)**
Code-based	✓	✓	✓	✓	✓	✗	✓
Niederreiter	BIKE [132]	-	BIKE [132]	-	BIKE [132]	-	PALOMA [134]
McEllice	Cl. McEllice [125] HQC [136]	Piglet-1 [177]	Cl. McEllice [125] HQC [136]	Cl. McEllice [125]	Cl. McEllice [125] HQC [136]	-	REDOG [137]
Signature	-	-	-	-	-	-	
Lattice-based	✓	✓	✓	✓	✓	✓	✓
LWE	CRYSTALS-Kyber [26] Saber [99]	Aigis-Enc [102] AKCN-MLWE [103] SCloud [106]	CRYSTALS-Kyber [26] Saber [99]	FrodoKEM [100]	CRYSTALS-Kyber [26] Saber [99]	CRYSTALS-Kyber [26] FrodoKEM [100]	-
LWE Signature	CRYSTALS-Dilithium [109]	Aigis-Sig [102] Mulan [110]	CRYSTALS-Dilithium [109]	-	CRYSTALS-Dilithium [109]	CRYSTALS-Dilithium [109]	HAETAE [112]
RLWE	NTRU [91] NTRU-HRSS [92] NTRU-Prime [93]	TALE [104] LAC PKE [101] AKCN-E8 [105]	NTRU [91] NTRU-HRSS [92] NTRU-Prime [93]	-	NTRU [91] NTRU-HRSS [92] NTRU-Prime [93]	NTRU+ [94]	NTRU+ [94] SMAUG+TiGER(merged) [107], [108]
RLWE Signature	Falcon [95]	FatSeal [96]	Falcon [95]	-	Falcon [95]	Falcon [95]	NCC-Sign [111]
Hash-Based	✓	✗	✓	✗	✓	✗	✗
MTS	SPHINCS+ [82]	-	SPHINCS+ [82]	-	SPHINCS+ [82]	-	-
Multivariate	✓	✗	✓	✗	✓	✗	✓
Small-Field	-	-	-	-	-	-	-
Big-Field	GeMSS [145]	-	GeMSS [145]	-	GeMSS [145]	-	-
Signatures	-	-	-	-	-	-	MQ-Sign [147]
Isogeny	✓	✗	✓	✗	✓	✗	✓
Supersingular	SIKE [155]	-	SIKE [155]	-	SIKE [155]	-	-
Signatures	-	-	-	-	-	-	-
MPC	✗	✗	✗	✗	✗	✗	✓
Signatures	-	-	-	-	-	-	AIMer [164]
Graph-based	✗	✗	✗	✗	✗	✗	✓
Perfect Code	-	-	-	-	-	-	-

TABLE IX
GLOBAL DISTRIBUTION OF THE PUBLIC INVESTMENT IN QUANTUM TECHNOLOGIES IN [185] AND IN [186]. THE TOTAL INVESTMENT WAS AROUND 27 BILLION EUROS IN 2022 AND INCREASED A 33% IN 2023, TO 36 BILLION EUROS

Country	Quantum Public Spend 2023 (Million €)	(Million $)	Quantum Public Spend 2022 (Million €)
China	13 500 (+0%)	15 000	13 500
UK	3 600 (+200%)	4 300	1 200
USA	3 000 (+172.73%)	3 750	1 100
Germany	3 000 (+13.33%)	3 300	2 600
South Korea	2 000 (+56143%)	2 350	35
France	1 800 (+0%)	2 200	1 800
Russia	1 250 (+119.3%)	1 450	570
Europe	1 000 (+0%)	1 100	1 000
Canada	1 000 (+0%)	1 100	1 000
India	630 (−30%)	735	900
Japan	600 (+0%)	700	600
Others	4 620 (+71.1%)	5 100	2 700
Total	36 000 (+33%)	40 000	27 000

schemes is still a question to be deeply explored. Due to the criticality of cybersecurity regarding the security of national secrets, most governments are still skeptical of completely relying on those novel methods. This is also a result of the fact that many of the cryptography protocols proposed in the past were proved to be insecure years later of their proposal. This is somehow result of the fact that some of the hard problems in which cryptography is based on rely on mathematical assumptions regarding their hardness, which is a evolving science. Obviously, this problem is exacerbated when PQC security proofs are considered, mainly because the class of problems that are solvable by quantum computers and its relationship to other complexity classes is still a question under research. Also, even with formal proofs of the hardness, the actual implementations of the protocols are not guaranteed to be safe. Therefore, due to the early stage of PQC proposals, many countries are exploring different possibilities as a function of their own analyses and interests rather than relying on the recommendations by a single entity, such as the NIST. In Tables VIII and IX, we present the global efforts regarding PQC integration in their communications and public investments, respectively, in quantum technologies as a way of showing a picture of the state of affairs at the time of writing.

Recently, South Korea has finished round 1 of their PQC Standardisation process [135]. After the whole process that has taken almost one year, they have decided to discard ROLLO-1 [178], Enhanced pqsigRm [179], SMAUG [107], GCKSign [175], TiGER [108], Peregrine [97], SOLMAE [98],

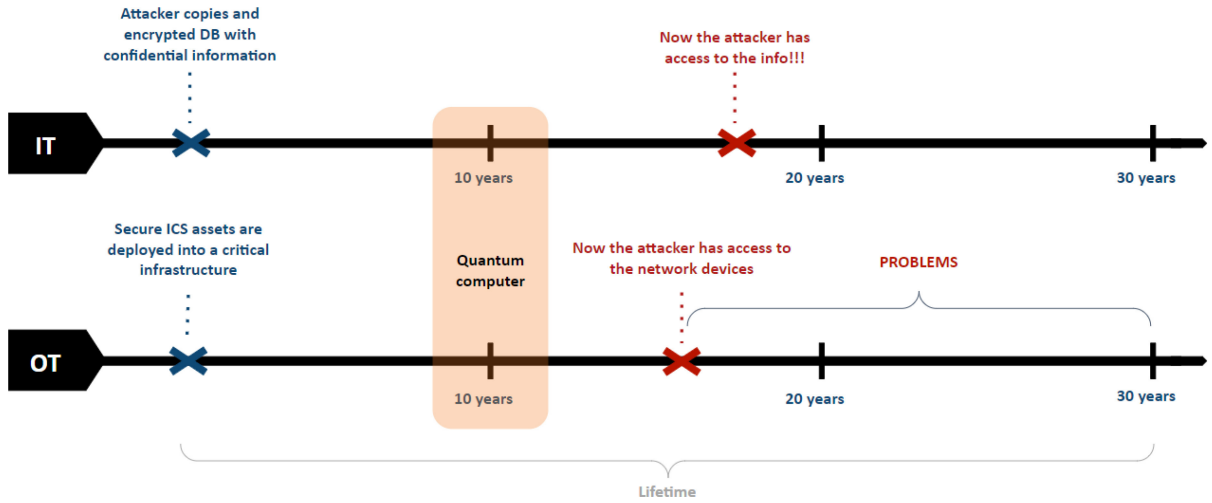


Fig. 7. Comparison of the lifespan of secrets in IT environments and the lifespan of devices in OT environments reveals significant differences. In IT communications, security must withstand quantum attacks several years prior to the advent of fault-tolerant quantum computers. This preemptive security measure is essential due to the risk of intercepting and storing communications today for decryption at a later time, known as "Harvest now, decrypt later" attack. Conversely, in OT communications, this particular issue is less pressing. However, cybersecurity in OT environments must still be quantum resilient, primarily because OT devices have long lifespans.

FIBS [156] and IPCC [167]. On the contrary, the signature algorithms AIMer [164] as a MPC signature; HAETAE [112] and NCC-Sign [111] as lattice-based signatures; and MQ-Sign [147] as Multivariate signature have been maintained as candidates for the second round. Regarding PKE/KEM algorithms they have selected NTRU+ and a merge of SMAUG [107] and TiGER [108] as lattice-based; and PALOMA [134] and REDOG [137] as code-based for the second round.

V. Post-Quantum Cryptography in Critical Infrastructure

Providing cybersecurity resources to CIs is an indispensable task due to the fact that their constituting elements are interconnected among them and with other CI industries, implying that a weakness in any point of the network could produce a cascading effect that would result in a large economical, social and human cost, as we have explained in Section II. An adversary with the computational power of a quantum computer could take advantage of weakness in a concrete part of CI's communications to launch a fatal quantum attack that could potentially affect several urban centers, industrial and state infrastructures. Therefore, integrating classical cryptographic methods in CI networks will provide security nowadays, but since the life-time span of OT devices is longer than the time scale estimated for the construction of the first fault tolerant quantum computer,[9] such solution can be deemed as a patch in the goal of protecting CI networks. Fig. 7, shows the essential difference of the problems of securing IT and OT environments. The main point in trying to accelerate the integration of PQC in IT networks is the "harvest now, decrypt later" paradigm, i.e., possible attackers store encrypted data for decrypting it once a quantum processor is available. Therefore, a fast integration is required for IT from the point of view of confidentiality, since the attackers are interested in the actual content of the encrypted data. On the other hand, in OT environments a possible attacker is not interested in reading the content of the information being communicated, but it is interested in being able to violate the system, i.e., to break data authenticity and integrity to attack the CI. Thus, the harvest now, decrypt later paradigm is not very relevant in this scenario. The big problem lays in the lifespan of the devices. As discussed before, industrial networks are assumed to last many decades and consist of legacy equipment, so integrating a secure solution against classical attacks may not be useful once quantum attacks can be realized, putting the entire system into a high degree of vulnerability. Protecting CI networks with quantum resilient solutions should aim to make them secure over the whole lifespan of the system. Consequently, PQC solutions for CI are a crucial necessity and, hence, it is necessary to target PQC from the point of view of CIs, fulfilling the required stringent communications requirements with the low-computational resources/legacy devices and testing the proposed solutions in real environments.

One of the main issues with implementing PQC in communication networks, both in OT and IT, is the increased duration of the handshake between parties. This is primarily due to the larger key length of PQC cryptosystems compared to traditional protocols. The handshake between parties typically occurs by means of the TLS protocol. There are experiments documented in the literature that compare the handshake times between PQC cryptosystems and classical ones, as noted in [188]. The latency increase in IT communications poses a significant challenge, especially when there is a high volume of communication relying on this protocol. However, in the case of OT communications, an increase in latency is not merely an optimization concern; it could potentially result in fatal errors. Therefore, the most important characteristic

[9]Note that it is projected that, at the current pace, IBM quantum processors could crack RSA by 2040 [187].

a PQC algorithm should present in order to be suitable for its implementation in CI, in combination with security (data integrity and authenticity), is a low-computational time (as this relates to the latency added to the system). This comes from the fact that some controlling operations in OT require latencies of the order of milliseconds, as in IEC-62443 [47], failing to satisfy such latency constraints may cause failures on the system.

Another important concern in OT cybersecurity are the side-channel attacks (SCAs). A SCA is a type of security breach that involves analyzing patterns of information leakage from a system to gain unauthorized access to sensitive data. Instead of directly attacking the cryptographic algorithm itself, SCAs exploit unintended side channels, such as power consumption, electromagnetic emissions, acoustic emanation, or timing information, to infer secret information, such as encryption keys. A comprehensive analysis and definition of each type of SCA is provided in [189].

By observing these side channels, attackers can deduce valuable information about the internal operations of a system and potentially compromise its security. While SCAs are a crucial consideration in IT cybersecurity, they are less of a concern in OT environments. This is because conducting a SCA in OT environments typically requires physical access to the devices or prior infection with malware. However, nowadays physical access is not always necessary to conduct a SCA. Some attacks can be executed remotely or with limited physical proximity to the target system, assuming that the device has been priory infected by a malware which send enough information to the attacker for doing a SCA. However, the feasibility and effectiveness of a SCA may vary depending on the specific type of attack and the level of access to the target device. Although physical access may facilitate certain types of SCAs on ICS, it is not always a strict requirement for successful attacks. For example, in [190] they perform a SCA to a infected PLC knowing its cache behavior. This article contributes to a better understanding of the risks posed by SCA in industrial control environments and emphasize the need for robust countermeasures to protect CI against this kind of attacks. Another important issue related to SCA is error and fault detection [191]. An error in the PQC algorithm could leak enough information to enable a SCA attack. For instance, some research focuses on enhancing the NTT [120], [192], which can reduce the computation time of lattice-based algorithms [193], but it may also leak information. A good review of NTT and its applications in PQC is given in [119]. Error and fault detection present a significant challenge not only in lattice-based cryptography but also in other PQC families, such as hash-based algorithms [194], [195].

Many research efforts aiming the implementation of PQC algorithms in HW are being conducted by the community, as pointed out in Section IV-G, and examples of these implementations are given in the section "PQC protocols" for each PQC family (Sections IV-A2, IV-B2, IV-C2, IV-D2, IV-E2, and IV-F. However, since each of the discussed PQC protocols has not been tested under the same conditions (processor, benchmark, security level, ...), performing a high-level comparison by means of the provided latencies would be inaccurate. Thus, the conclusions would not be relevant for the application of the protocols in ICS/CI. This also comes in hand with the fact that since such implementations have not been realized from the point of view of ICS/CI, i.e., trying to fulfill the stringent conditions imposed by such systems, the obtained conclusions would only be partially true. Recently, a study on implementing CRYSTALS-Kyber and CRYSTALS-Dilithium in IoT environments, meaning environments with limited computational resources, has been published [196]. These PQC algorithms were selected in the NIST standardization process [23]. The study pointed out the challenges of implementing PQC algorithms in IoT environments and presented an efficient and innovative lattice-based cryptography processor to make them suitable for IoT environments. However, more studies and implementations of PQC algorithms in IoT infrastructures are needed, particularly concerning SCA and the potential delay they could introduce to communication processes. Despite of the lack of such benchmark, it is possible to somehow bound the performance of PQC families in order to select which of them could be a potentially good option to be deployed in an ICS system. We have done this by using the tables in Section IV-G, where we compare the keys and ciphertext length of each PQC algorithm and their computational cost, characteristics that, in the end, are related with the latency introduced to the communications and the requirements of the hardware used in the network. However, the lack of actual fair comparative metrics for PQC in industrial and CI networks urges for performing such comparison in the same conditions and from the point of view of the necessities of such scenarios. In this way, the selection of PQC protocols for deployment in ICS/CI will be actually possible, feature that has recently been pointed out by the CISA, NSA and NIST to be of critical importance [32].

Another challenge in implementing any new cryptosystem into a standardized communication protocol is that it may require changes across all systems [33]. All systems must adopt the same cryptosystem for a successful handshake initiation, necessitating a migration of all systems from the classical TLS protocol to a quantum-secure protocol. However, not all systems are prepared to incorporate PQC in their current state. Some are old and lack the resources, while others may not be designed to accommodate this type of cryptography, even in IT communication [197]. In the context of OT communications, the fact that all devices have to adopt the same PQC protocol is less problematic due to the confined nature of communications within an industry. Communication between devices typically occurs only within the same industrial setting, necessitating standardization only within that specific industry. For instance, a PLC primarily communicates with other devices within the manufacturing control layer or the Area Supervisory Control layer (refer to Fig. 2), rather than with devices outside of this network. In order to communicate with elements outside this network, the protocols used are IT standards and, thus, do not concern the discussions presented here.

Another important issue for integrating PQC in ICS/CI infrastructure is that it is also necessary to think about a resiliency solution, with the capability to adapt for different

TABLE X
IN THIS TABLE WE PRESENT THE MOST VALUABLE INSIGHTS AND PROBLEMS FOR IMPLEMENTING PQC SECURITY IN CI

Problems	Importance	Section
Latency	OT protocols require low latency communications [47], [27], [192]	II-A
Legacy devices	PQC require a great amount of memory and computational resources [51], [53], [52]	II-A
Data integrity and availability	Data integrity and availability are the most important characteristics in OT cryptography	II-A
Regulation	The solution has to be resilient to fulfill the regulations of the different countries [48], [49], [50]	IV-H
Agility	PQC primitives security are not proved and HW solutions are not flexible	IV
Theory	There are not theoretical PQC specific proposals for OT protocols	V
Experiments	More tests of PQC algorithms in CI environments have to be done	V

cryptography algorithms, since it is not exactly known if they would be secure against quantum attacks[10] or specific cybersecurity requirements could be imposed by different countries and OT environments. Note also the recent controversy regarding the calculations of the security level of Kyber-512 posed by Daniel Bernstein et al. [198] and the recently proposed method for breaking the Rainbow PQC cryptosystem in one weekend requiring a single laptop [146]. In principle, it seems rather difficult that such flexibility can be achieved by implementing those cryptographic protocols with a hardware solution, which is the most explored one for low-latency solutions as shown in Section IV. As an example, if the network of a electricity provider is secured by integrating a specific PQC protocol in hardware, were the case that such method is not reliable anymore, then all those chips introduced in the network should be substituted by new ones that implement the alternative. It is straightforward to see that such scenario would lead to a high cost in terms of money and man power. Hybrid cryptography could be a good solution for maintaining classical cybersecurity even if the implemented PQC algorithm is proven to be insecure, but it will not be secure against quantum computers until the industry upgrade its PQC communication protocol. Furthermore, as we exposed before, there are many PQC standardisation processes along the word. The generalized increment in the public investment in quantum technologies, Table IX, is a signal that countries consider their development a priority. Moreover, this table refers only to public expend and it does not show private and/or military investment in quantum technology. It is a signal that in the near future each country could adopt their own PQC cryptosystem protocols and will require to fulfill their cybersecurity requirements to companies that operate/sell in their territory. Note that France has recently established a normative requiring cybersecurity for the communication protocols within CIs [50] and, even if no specifics on PQC are required yet, it is a matter of time that they will. Hence, having flexible PQC solutions would allow fulfilling the specific requirements imposed by these global agents.

Moreover, it is important to note that the PQC solutions integrated in this networks should be low-power and autonomous in terms of energy. This is related with the previous discussion on the required flexibility. Note that if the power of the PQC solutions require to be changed regularly (for example by using batteries), such requirement would also result in huge costs for the industry. Therefore, it is essential that the solutions are powered by in the same way as the other elements of the network. This is why they should be low-power as not to make the power system to be saturated, i.e., they should not be a problem for the power system of the network [199]. Also, some environments are more challenging than other (e.g., an oil extraction plant), so self powering methods may also be required as a function of the ICS to secure. For example, energy harvesting methods could be required to power some of the devices as in some IoT sensor networks [200], implying low-power consumption requirements.

Regarding current PQC algorithms, those mainly focus on achieving quantum security to provide confidentiality, integrity and authenticity, being the first one the most important characteristic; due to the fact that they are thought mainly from the point of view of IT. For those to be implemented in OT, they should assure high availability and adaptability as discussed in Section II-B. Several countries are trying to standardize PQC algorithms taking only into account the perspective of IT systems, nonetheless, considering also the OT context is of pivotal importance for the security and safety of the industry.

Subsequently, since ICS/CIs have to be secure under quantum attacks as well, it is necessary to study how those algorithms work on OT networks and see which of them achieve all the requirements. Despite of the fact that there are many PQC families and many different protocols for each family, it is probable that none of them fulfill all the demanding requirements in CI environments. So, there could not be only a lack of PQC experimental work in OT environments, but also a lack of theoretical framework. If such were the case, cryptography should urge cryptographers to find other possible families or protocols that fit those conditions before a future comes in which operational technologies have no protection to quantum attacks. The Table X summarizes everything presented in this section in a schematic manner.

VI. CONCLUSION AND GUIDELINES

In this article we have provided a comprehensive review of the state-of-the-art of PQC from the perspective of industrial and CI networks. For doing so, we defined what are ICSs specifying its different layers and their communication protocols. Among the ICSs and different industries, we have focused on CI networks, which provide goods and services that are indispensable for providing social and economical necessities on a day-to-day basis. In this sense, the stringent conditions that the communication network of a CI should meet have

[10]Recall the new proposal for solving LWE with quantum computers in polynomial time [181].

been presented. Therefore, the integration of cybersecurity in such OT systems is much more difficult than for IT services, but protecting them is of vital importance as cyberattacks on CI may lead to unbearable economical and social losses. Thus, we have provided a comprehensive overview of cryptography, the mathematical tool to maintain information secure, and discussed why quantum technologies can make state-of-the-art classical cryptography methods deprecated in a timescale of around 20 years, imposing a threat to ICS/CI components whose lifetimes are deemed to be of around 40 years. Hence, the paradigm of PQC has arised as the possible solution to such quantum apocalypse, and it consists in designing cryptographic methods that rely on hard problems for which QC does not provide exponential speedups. Thus, we have given a review of the state-of-the-art of PQC families and protocols. We have also discussed that PQC development is being done by different global agents in an somehow independent way, implying that the near future will probably see many protocols operating at distinct industries or countries around the world, different to what happened with the widespread RSA and ECC protocols. Finally, we have discussed the current state of affairs regarding the integration of such families in ICS/CI networks.

We have concluded that although there are many different PQC alternatives that seem to provide good security against quantum attacks for IT services in the near-future, their implementation in CI is not a trivial problem. The lack of security notions for the PQC families, the long lifetime span of OT devices, the fact that the communications within ICS have stringent requirements and that those are mainly composed of legacy elements of little computational capabilities imply that there is a current gap in terms of PQC protocols that can be seamlessly adapted to such scenarios. Moreover, the absence of a general benchmark of PQC algorithms under the same conditions (e.g., same processor for latency tests) makes it hard to make a top view comparison among them to conclude which could be well suited for implementation in CI networks. This is really important since cryptosystems that introduce too much latency reduce the availability of communication protocols, which could produce fatal consequences not only to the specific industry which suffers the shutdown, but also to all the interconnected industrial chain due to cascade effects. Therefore, we consider that the following points stand as some of the most relevant future research lines regarding this topic.

1) Conduct experimental studies comparing different PQC families under the same conditions. As explained through this article, the latency of PQC protocols is provided for specific scenarios and implementations (e.g., different processors), implying that a straight comparison by means of the literature data would not be accurate. This type of studies would clarify which protocols could be more suitable for integration in industrial networks as well as providing information to the community.
2) Optimized PQC implementations for OT networks should be investigated in order to understand the capabilities of current proposals. As stated before, there are not many fair comparisons of state-of-the-art PQC protocols to understand which could be potentially implementable in industrial networks. However, the optimization of those existing protocols to be dedicated to such scenarios should also be investigated. Those could be candidates for OT communication systems would there be any successful protocols to fill all the conditions required.
3) Propose PQC protocols from the point-of-view of the stringent conditions of OT services. As discussed, the problem of securing industrial networks is fundamentally different to the one of protecting IT systems. For example, in OT the aim should be authenticity/integrity rather than confidentiality. This with the very important requirement of low latency. In this sense, researcher on PQC proposals could think of their methods to target this problematic instead of protecting confidentiality, which is the usual target.
4) Propose flexible solutions for PQC integration in ICS/CI networks. In Section V, we discussed that PQC solutions for ICS/CI networks should be flexible in order to avoid huge economic and manpower costs if the implemented protocol results to be deprecated or if new governmental requirements are imposed since, for example, hardware solutions would imply the substitution of a humongous amounts of elements introduced in different points of a network that could be enormous in terms of space, i.e., in of the order of hundred of kilometers. Thus, proposing, for example, programmable methods that are flexible enough to change protocols if required is important for this post-quantum transition.
5) Standardization processes for PQC implementations in industrial environments should be conducted. Through this document, many PQC standardization efforts around the world have been discussed, but those are oriented toward IT communications. As commented before, both communication scenarios are very different in the requirements for cryptography, indicating that the IT and OT implementations will diverge. Therefore, efforts regarding PQC implementations for OT networks should be pushed worldwide. Importantly, this should be done with a fast pace since, as discussed before, equipment that is not quantum secure could be vulnerable through their lifetime.

COMPETING INTERESTS

The authors declare no competing interests.

ACKNOWLEDGMENT

The authors want to acknowledge Reza Dastbasteh for fruitful discussions regarding code-based cryptography.

REFERENCES

[1] T. Philbeck and N. Davis, "The fourth industrial revolution: Shaping a new era," *J. Int. Affairs*, vol. 72, no. 1, pp. 17–22, 2018. [Online]. Available: https://www.jstor.org/stable/26588339

[2] (Packetlabs, Toronto, ON, USA). *Cybersecurity Statistics*. (2023). Accessed: 3, 2024. [Online]. Available: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/

[3] (CISA, Washington, DC, USA). *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities*. (2023). [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[4] V. R. Palleti, S. Adepu, V. K. Mishra, and A. Mathur, "Cascading effects of cyber-attacks on interconnected critical infrastructure," *Cybersecurity*, vol. 4, no. 1, p. 8, Mar. 2021. [Online]. Available: https://doi.org/10.1186/s42400-021-00071-z

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[6] N. Koblitz, "Elliptic curve Cryptosystems," *Math. of Computation*, vol. 48, no. 177, pp. 203–209, 1987. [Online]. Available: http://www.jstor.org/stable/2007884

[7] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. CRYPTO*, 1986, pp. 417–426.

[8] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[9] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019. [Online]. Available: https://doi.org/10.1038/s41586-019-1666-5

[10] H.-S. Zhong et al., "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, pp. 1460–1463, 2020. [Online]. Available: https://www.science.org/doi/abs/10.1126/science.abe8770

[11] Y. Wu et al., "Strong quantum computational advantage using a Superconducting quantum processor," *Phys. Rev. Lett.*, vol. 127, Oct. 2021, Art. no. 180501. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.127.180501

[12] H.-Y. Huang et al., "Quantum advantage in learning from experiments," *Science*, vol. 376, no. 6598, pp. 1182–1186, 2022. [Online]. Available: https://www.science.org/doi/abs/10.1126/science.abn7293

[13] L. S. Madsen et al., "Quantum computational advantage with a programmable photonic processor," *Nature*, vol. 606, no. 7912, pp. 75–81, Jun. 2022. [Online]. Available: https://doi.org/10.1038/s41586-022-04725-x

[14] S. Krinner et al., "Realizing repeated quantum error correction in a distance-three surface code," *Nature*, vol. 605, no. 7911, pp. 669–674, May 2022. [Online]. Available: https://doi.org/10.1038/s41586-022-04566-8

[15] R. Acharya et al., "Suppressing quantum errors by scaling a surface code logical qubit," *Nature*, vol. 614, no. 7949, pp. 676–681, Feb. 2023. [Online]. Available: https://doi.org/10.1038/s41586-022-05434-1

[16] M. Mosca and M. Piani (Global Risk Instit., Toronto, ON, USA). *Quantum Threat Timeline Report 2022*. Accessed: 3, 2024. [Online]. Available: https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.74.145

[18] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241

[19] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661

[20] K. Azuma et al., "Quantum repeaters: From quantum networks to the quantum Internet," 2022, *arXiv:2212.10820*.

[21] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017.

[22] T. Vidick and J. Watrous, "Quantum proofs," *Found. Trends® Theor. Comput. Sci.*, vol. 11, nos. 1–2, pp. 1–215, 2016. [Online]. Available: http://dx.doi.org/10.1561/0400000068

[23] (NIST, Gaithersburg, MD, USA). *Post-Quantum Cryptography Standarization*. (2017). [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[24] A. Rodriguez (European Policy Centre, Brussels, Belgium). *A Quantum Cybersecurity Agenda for Europe*. (2023). [Online]. Available: https://www.epc.eu/en/publications/A-quantum-cybersecurity-agenda-for-Europe 526b9c

[25] D. O'Brien. "Protecting chrome traffic with hybrid Kyber KEM." 2023. [Online]. Available: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

[26] J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Eur. Symp. Security Privacy*, 2018, pp. 353–367.

[27] E. Korkmaz, M. Davis, A. Dolgikh, and V. Skormin, "Detection and mitigation of time delay injection attacks on industrial control systems with PLCs," in *Computer Network Security*, J. Rak, J. Bay, I. Kotenko, L. Popyack, V. Skormin, and K. Szczypiorski, Eds. Cham, Switzerland: Springer Int. Publ., 2017, pp. 62–74.

[28] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, 2015, pp. 1–8.

[29] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *Proc. IEEE Globecom Workshops*, 2012, pp. 1508–1513.

[30] N. Kush, M. Branagan, E. Foo, and E. Ahmed, "Poisoned GOOSE: Exploiting the GOOSE protocol," in *Proc. 12th Aust. Inf. Secur. Conf.*, vol. 149, 2014, pp. 17–22.

[31] E. D. Knapp and J. T. Langill, "Chapter 7—Hacking industrial control systems," in *Industrial Network Security*, 2nd ed., E. D. Knapp and J. T. Langill, Eds. Boston, MA, USA: Syngress, 2015, pp. 171–207. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780124201149000071

[32] (NISA, Hyderabad, India, NSA, Fort Meade, MD, USA, and NIST, Gaithersburg, MD, USA). *Quantum-Readiness: Migration To Post-Quantum Cryptography*. (2023). [Online]. Available: https://www.cisa.gov/sites/default/files/2023-08/Quantum

[33] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *Proc. 7th Int. Conf. Mobile Secure Services (MobiSecServ)*, 2022, pp. 1–8.

[34] K. Kan and M. Une, "Recent trends on research and development of quantum computers and standardization of post-quantum cryptography," *Monetary Econ. Stud.*, vol. 39, pp. 77–108, Nov. 2021. [Online]. Available: https://ideas.repec.org/a/ime/imemes/v39y2021p77-108.html

[35] M. Alvarado, L. Gayler, A. Seals, T. Wang, and T. Hou, "A survey on post-quantum cryptography: State-of-the-art and challenges," 2023, *arXiv:2312.10430*.

[36] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, 2023. [Online]. Available: https://www.mdpi.com/2410-387X/7/3/40

[37] "The state of industrial security in 2022." 2022. Accessed: 3, 2024. [Online]. Available: https://www.barracuda.com/reports/iiot-2022-report

[38] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, Dec. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361518303658

[39] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101677. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819302172

[40] H. M. H. Uchenna P. Daniel Ani and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2017. [Online]. Available: https://doi.org/10.1080/23742917.2016.1252211

[41] M. Krotofil and D. Gollmann, "Industrial control systems security: What is happening?" in *Proc. 11th IEEE Int. Conf. Ind. Inform. (INDIN)*, 2013, pp. 664–669.

[42] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for Industrial Internet of Things: Research challenges and opportunities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3567–3569, Aug. 2018.

[43] A. K. Pandey, A. Banati, B. Rajendran, S. D. Sudarsan, and K. K. S. Pandian, "Cryptographic challenges and security in post quantum cryptography migration: A prospective approach," in *Proc. IEEE Int. Conf. Public Key Infrastruct. Appl. (PKIA)*, 2023, pp. 1–8.

[44] S. Paul, "On the transition to post-quantum cryptography in the Industrial Internet of Things," Ph.D. dissertation, Dept. Comput. Sci., Technische Universität Darmstadt, Darmstadt, Germany, 2022. [Online]. Available: http://tuprints.ulb.tu-darmstadt.de/21368/

[45] (French Cybersecurity Agency, Paris, France). *French National Agency for the Security of Information Systems*. Accessed: 3, 2024. [Online]. Available: https://www.ssi.gouv.fr/en/

[46] "Federal office for information security." Accessed: 3, 2024. [Online]. Available: https://www.bsi.bund.de/EN/Home/home_node.html

[47] *The WorldŠs Only Consensus-Based Automation and Control Systems Cybersecurity Standards*, ISA/IEC Standard 62443. Accessed: 3, 2024.

[Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[48] R. Mattioli and K. Moulinos (ENISA, Athens, Greece). *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*. (2015). [Online]. Available: https://www.enisa.europa.eu/publications/maturity-levels
[49] (CISA, Washington, DC, USA). *Industrial Control Systems*. Accessed: 3, 2024. [Online]. Available: https://www.cisa.gov/topics/industrial-control-systems
[50] (Agence nationale de la sécurité des systèmes d'information, Paris, France). *La cybersécurité des systèmes Industriels*. Accessed: 3, 2024. [Online]. Available: https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels
[51] R. Ramirez, C.-K. Chang, and S.-H. Liang, "PLC Cyber-security challenges in industrial networks," in *Proc. 18th IEEE/ASME Int. Conf. Mechatron. Embed. Syst. Appl. (MESA)*, 2022, pp. 1–6.
[52] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," in *Proc. 6th Int. Conf. Inf. Technol. Multimedia*, 2014, pp. 5–10.
[53] E. Biham, S. Bitan, A. Carmel, A. Dankner, U. Malin, and A. Wool, "Rogue7: Rogue engineering-station attacks on S7 simatic PLCs," presented at Black Hat USA, 2019, pp. 1–21.
[54] J. Daor, J. Daemen, and V. Rijmen. "AES proposal: Rijndael." Oct. 1999. [Online]. Available: https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf
[55] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," in *Fast Softw. Encrypt.*, R. Anderson, Ed. Berlin, Gerrmany: Springer, 1994, pp. 191–204.
[56] B. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. "Twofish: A 128Bit block cipher." Jan. 1998. [Online]. Available: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf
[57] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[58] (claymath, Providence, RI, USA). *Millenium Prize Problems*. Accessed: 3, 2024. [Online]. Available: https://www.claymath.org/millennium-problems/
[59] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)," Dept. Combinator., Optim., Univ. Waterloo, Waterloo, ON, Cannada, Rep. CORR 99-33, 1999. [Online]. Available: https://books.google.es/books?id=gAPeMwEACAAJ
[60] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.
[61] Z. Wang, S. Wei, G.-L. Long, and L. Hanzo, "Variational quantum attacks threaten advanced encryption standard based symmetric cryptography," *Sci. China Inf. Sci.*, vol. 65, no. 10, Jul. 2022, Art. no. 200503. [Online]. Available: https://doi.org/10.1007/s11432-022-3511-5
[62] B. Aizpurua, P. Bermejo, J. Etxezarreta Martinez, and R. Orus, "Hacking cryptographic protocols with advanced variational quantum attacks," 2023, *arXiv:2311.02986*.
[63] J. P. Buhler, H. W. Lenstra, and C. Pomerance, "Factoring integers with the number field sieve," in *The Development of the Number Field Sieve*, A. K. Lenstra and H. W. Lenstra, Eds. Berlin, Germany: Springer, 1993, pp. 50–94.
[64] K. K. Soni and A. Rasool, "Cryptographic attack possibilities over RSA algorithm through classical and quantum computation," in *Proc. Int. Conf. Smart Syst. Invent. Technol. (ICSSIT)*, 2018, pp. 11–15.
[65] (Inria, Paris, France). *Factorization of RSA-250*. Accessed: 3, 2024. [Online]. Available: https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;dc42ccd1.2002
[66] A. deMarti iOlius, P. Fuentes, R. Orús, P. M. Crespo, and J. Etxezarreta Martinez, "Decoding algorithms for surface codes," 2023, *arXiv:2307.14989*.
[67] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, Apr. 2021. [Online]. Available: https://doi.org/10.22331/q-2021-04-15-433
[68] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018. [Online]. Available: https://doi.org/10.22331/q-2018-08-06-79
[69] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
[70] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, vol. 1, nos. 3–4, pp. 187–201, 2017.
[71] J. Kaur, A. Sarker, M. M. Kermani, and R. Azarderakhsh, "Hardware constructions for error detection in lightweight Welch-Gong (WG)-oriented streamcipher WAGE benchmarked on FPGA," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 2, pp. 1208–1215, Apr.–Jun. 2022.
[72] J. Kaur, M. M. Kermani, and R. Azarderakhsh, "Hardware constructions for lightweight cryptographic block cipher QARMA with error detection mechanisms," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 1, pp. 514–519, Jan.–Mar. 2022.
[73] M. S. Turan et al., "Status report on the final round of the NIST lightweight cryptography standardization process," US Dept. Commer., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NIST IR 8454, 2023.
[74] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight authenticated encryption and hashing," *J. Cryptol.*, vol. 34, no. 3, p. 33, 2021. [Online]. Available: https://doi.org/10.1007/s00145-021-09398-9
[75] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *Proc. 8th Int. Conf. Post-Quant. Cryptogr. (PQCrypto)*, 2017, pp. 384–405.
[76] H. Seo and R. Azarderakhsh, "Curve448 on 32-bit ARM cortex-M4," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2021/1355, 2021. [Online]. Available: https://eprint.iacr.org/2021/1355 s
[77] M. Bisheh-Niasar, R. Azarderakhsh, and M. Mozaffari-Kermani, "Cryptographic accelerators for digital signature based on Ed25519," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 29, no. 7, pp. 1297–1305, Jul. 2021.
[78] R. Bavdekar, E. Jayant Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: A review of techniques, challenges and Standardizations," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2023, pp. 146–151.
[79] R. C. Merkle, "Secrecy, authentication, and public key systems," Ph.D. dissertation, Dept. Electr. Eng., Stanford Univ., Stanford, CA, USA, 1979. [Online]. Available: https://www.proquest.com/dissertations-theses/secrecy-authentication-public-key-systems/docview/302984000/se-2
[80] L. Lamport, "Constructing digital signatures from a one way function," Dept. Comput. Sci. Lab., SRI Int., Menlo Park, CA, USA, Rep. CSL-98, Oct. 1979, 2010. [Online]. Available: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/
[81] G. Brassard, P. HØyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," in *Proc. 3rd Latin Am. Symp.*, 1998, pp. 163–169. [Online]. Available: https://doi.org/10.1007
[82] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ signature framework," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 2129–2146. [Online]. Available: https://doi.org/10.1145/3319535.3363229
[83] D. Amiet, L. Leuenberger, A. Curiger, and P. Zbinden, "FPGA-based SPHINCS+ implementations: Mind the glitch," in *Proc. 23rd Euromicro Conf. Digit. Syst. Design (DSD)*, 2020, pp. 229–237.
[84] R. Gonzalez et al., "Verifying post-quantum signatures in 8 kB of RAM," in *Post-Quantum Cryptography*, J. H. Cheon and J.-P. Tillich, Eds. Cham, Switzerland: Springer Int. Publ., 2021, pp. 215–233.
[85] R. Merkle and M. Hellman, "Hiding information and signatures in trapdoor knapsacks," *IEEE Trans. Inf. Theory*, vol. 24, no. 5, pp. 525–530, Sep. 1978.
[86] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*, J. P. Buhler, Ed. Berlin, Germany: Springer, 1998, pp. 267–288.
[87] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, Sep. 2009. [Online]. Available: https://doi.org/10.1145/1568318.1568324
[88] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, Dec. 1982.
[89] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108. [Online]. Available: https://doi.org/10.1145/237814.237838
[90] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2010, pp. 1–23.
[91] W. Whyte and J. Hoffstein, "NTRU," in *Encyclopedia of Cryptography and Security*, Boston, MA, USA: Springer, 2011, pp. 858–861. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_464

[92] A. Hülsing, J. Rijneveld, J. Schanck, and P. Schwabe (NIST, Gaithersburg, MD, USA). *NTRU-HRSS-KEMx—Submission to the NIST Post-Quantum Cryptography Project*. (2017). [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/NTRU_HRSS_KEM.zip

[93] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "NTRU prime: Reducing attack surface at low cost," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2016/461, 2016. [Online]. Available: https://eprint.iacr.org/2016/461

[94] J. Kim and J. H. Park, "NTRU+: Compact construction of NTRU using simple encoding method," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1664, 2022. [Online]. Available: https://eprint.iacr.org/2022/1664

[95] P.-A. Fouque et al., "Falcon: Fast-fourier lattice-based compact signatures over NTRU," *NISTŠs Post Quantum Cryptogr. Stand. Process*, vol. 36, no. 5, pp. 1–75, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:231637439

[96] T. Xie, H. Li, Y. Zhu, Y. Pan, Z. Liu, and Z. Yang, "FatSeal: An efficient lattice-based signature algorithm," *J. Electron. Inf. Technol.*, vol. 42, no. 2, pp. 333–340, 2020. [Online]. Available: https://jeit.ac.cn/cn/article/doi/10.11999/JEIT190678

[97] E.-Y. Seo, Y.-S. Kim, J.-W. Lee, and J.-S. No, "Peregrine: Toward fastest FALCON based on GPV framework," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1495, 2022. [Online]. Available: https://eprint.iacr.org/2022/1495

[98] K. Kim. "How SOLMAE was designed." Accessed: Mar. 2024. [Online]. Available: https://ircs.re.kr/wp-content/uploads/2023/06/40CISC_S23_2col_final.pdf

[99] J.-P. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren, "Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2018/230, 2018. [Online]. Available: https://eprint.iacr.org/2018/230

[100] E. Alkım et al. "FrodoKEM learning with errors key encapsulation algorithm specifications and supporting documentation." 2019. [Online]. Available: https://frodokem.org/

[101] X. Lu et al., "LAC: Practical ring-LWE based public-key encryption with byte-level modulus," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2018/1009, 2018.

[102] J. Zhang, Y. Yu, S. Fan, Z. Zhang, and K. Yang, "Tweaking the asymmetry of asymmetric-key cryptography on lattices: KEMs and signatures of smaller sizes," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2019/510, 2019. [Online]. Available: https://eprint.iacr.org/2019/510

[103] Z. Jin and Y. Zhao, "Optimal key consensus in presence of noise," 2017, *arXiv:1611.06150*.

[104] Y. Zhu, Z. Liu, and Y. Pan, "When NTT meets Karatsuba: Preprocess-then-NTT technique revisited," in *Proc. 23rd Int. Conf. Inf. Commun. Security*, 2021, pp. 249–264.

[105] Z. JIn and Y. Zhao, "AKCN-E8: Compact and flexible KEM from ideal lattice," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2020/056, 2020. [Online]. Available: https://eprint.iacr.org/2020/056

[106] Z. Zheng, A. Wang, H. Fan, C. Zhao, C. Liu, and X. Zhang, "SCloud: Public key encryption and key encapsulation mechanism based on learning with errors," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2020/095, 2020. [Online]. Available: https://eprint.iacr.org/2020/095

[107] J. H. Cheon, H. Choe, D. Hong, and M. Yi, "SMAUG: Pushing lattice-based key encapsulation mechanisms to the limits," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2023/739, 2023. [Online]. Available: https://eprint.iacr.org/2023/739

[108] S. Park, C.-G. Jung, A. Park, J. Choi, and H. Kang, "TiGER: Tiny bandwidth key encapsulation mechanism for easy miGration based on RLWE(R)," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1651, 2022. [Online]. Available: https://eprint.iacr.org/2022/1651

[109] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS—Dilithium: Digital signatures from module lattices," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2017/633, 2017. [Online]. Available: https://eprint.iacr.org/2017/633

[110] J. Zheng, F. He, S. Shen, C. Xue, and Y. Zhao, "Parallel small polynomial multiplication for dilithium: A faster design and implementation," in *Proc. 38th Annu. Comput. Security Appl. Conf.*, 2022, pp. 304–317. [Online]. Available: https://doi.org/10.1145/3564625.3564629

[111] K.-A. Shim, J. Kim, and Y. An. "NCC-sign: A new lattice-based signature scheme using non-cyclotomic polynomials." Accessed: 3, 2024. [Online]. Available: https://www.kpqc.or.kr/images/pdf/NCC-Sign.pdf

[112] J. H. Cheon et al., "HAETAE: Shorter lattice-based fiat-Shamir signatures," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2023/624, 2023. [Online]. Available: https://eprint.iacr.org/2023/624

[113] V. B. Dang, K. Mohajerani, and K. Gaj, "High-speed hardware architectures and FPGA benchmarking of CRYSTALS-Kyber, NTRU, and saber," *IEEE Trans. Comput.*, vol. 72, no. 2, pp. 306–320, Feb. 2023.

[114] Z. Qin, R. Tong, X. Wu, G. Bai, L. Wu, and L. Su, "A compact full hardware implementation of PQC algorithm NTRU," in *Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE)*, 2021, pp. 792–797.

[115] S. Paul and P. Scheible, "Towards post-quantum security for Cyber-physical systems: Integrating PQC into industrial M2M communication," in *Proc. 25th Eur. Symp. Res. Comput. Secur.*, 2020, pp. 295–316.

[116] W. Guo, S. Li, and L. Kong, "An efficient implementation of KYBER," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 3, pp. 1562–1566, Mar. 2022.

[117] Y. Huang, M. Huang, Z. Lei, and J. Wu, "A pure hardware implementation of CRYSTALS-KYBER PQC algorithm through resource reuse," *IEICE Electron. Exp.*, vol. 17, no. 17, 2020, Art. no. 20200234.

[118] P. Sanal, E. Karagoz, H. Seo, R. Azarderakhsh, and M. Mozaffari-Kermani, "Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM cortex-a processors," in *Security Privacy Communication Netw.*, J. Garcia-Alfaro, S. Li, R. Poovendran, H. Debar, and M. Yung, Eds. Cham, Switzerland: Springer Int. Publ., 2021, pp. 424–440.

[119] A. Satriawan, I. Syafalni, R. Mareta, I. Anshori, W. Shalannanda, and A. Barra, "Conceptual review on number theoretic transform and comprehensive review on its implementations," *IEEE Access*, vol. 11, pp. 70288–70316, 2023.

[120] A. Sarker, M. Mozaffari-Kermani, and R. Azarderakhsh, "Hardware constructions for error detection of number-theoretic transform Utilized in secure cryptographic architectures," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 3, pp. 738–741, Mar. 2019.

[121] S. Sinha Roy and A. Basso, "High-speed instruction-set coprocessor for lattice-based key encapsulation mechanism: Saber in hardware," *Proc. IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2020, 2020, pp. 443–466. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8690

[122] R. Tong et al., "High-speed hardware implementation of PQC algorithm LAC," in *Proc. IEEE 14th Int. Conf. Anti-Counterfeit., Secur., Identif. (ASID)*, 2020, pp. 104–108.

[123] L. Beckwith, D. Nguyen, and K. Gaj, "High-performance hardware implementation of CRYSTALS-Dilithium," *Proc. Int. Conf. Field-Program. Technol. (ICFPT)*, 2021, pp. 1–10.

[124] A. Wang, D. Xiao, and Y. Yu, "Lattice-based cryptosystems in standardisation processes: A survey," *IET Inf. Secur.*, vol. 17, no. 2, pp. 227–243, 2023. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/ise2.12101

[125] R. J. McEliece, "A public-key Cryptosystem based on algebraic coding theory," *Deep Space Netw. Prog. Rep.*, vol. 44, pp. 114–116, Jan. 1978.

[126] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Probl. Control Inf. Theory*, vol. 15, no. 2, pp. 157–166, 1986.

[127] Y. X. Li, R. Deng, and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 271–273, Jan. 1994.

[128] N. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2001/010, 2001. [Online]. Available: https://eprint.iacr.org/2001/010

[129] R. Overbeck and N. Sendrier, *Code-Based Cryptography*. Berlin, Germany: Springer, 2009, pp. 95–145. [Online]. Available: https://doi.org/10.1007/978-3-540-88702-7_4

[130] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 384–386, May 1978.

[131] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key Cryptosystem," in *Proc. Workshop Theory Appl. Cryptogr. Techn.*, 1988, pp. 275–280.

[132] N. Aragon et al. "Bike: Bit flipping key encapsulation." 2017. Accessed: 3, 2024. [Online]. Available: https://bikesuite.org/

[133] G. Alagic et al., "Status report on the third round of the NIST post-quantum cryptography Standardization process," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR-8413, 2022. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458

[134] D.-C. Kim, C.-Y. Jeon, Y. Kim, and M. Kim. "PALOMA: Binary separable goppa-based kem." Accessed: 3, 2024. [Online]. Available: https://www.kpqc.or.kr/images/pdf/PALOMA.pdf

[135] "Korean post-quantum cryptography." Accessed: 3, 2024. [Online]. Available: https://www.kpqc.or.kr/

[136] C. Aguilar-Melchor et al. "Hamming quasi-cyclic (HQC)." 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:127090340

[137] J.-L. Kim, J. Hong, T. S. C. Lau, Y. Lim, and B.-S. Won, "REDOG and its performance analysis," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1663, 2022. [Online]. Available: https://eprint.iacr.org/2022/1663

[138] J. Richter-Brockmann, J. Mono, and T. Güneysu, "Folding BIKE: Scalable hardware implementation for reconfigurable devices," *IEEE Trans. Comput.*, vol. 71, no. 5, pp. 1204–1215, May 2022.

[139] "Complete and improved FPGA implementation of classic McEliece," vol. 2022, pp. 71–113, Jun. 2022. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/9695

[140] S. Deshpande, C. Xu, M. Nawan, K. Nawaz, and J. Szefer, "Fast and efficient hardware implementation of HQC," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1183, 2022. [Online]. Available: https://eprint.iacr.org/2022/1183

[141] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *Proc. Workshop Theory Appl. Cryptogr. Techn.*, 1988, pp. 419–453.

[142] J. C. Faugère, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, 2002, pp. 75–83. [Online]. Available: https://doi.org/10.1145/780506.780516

[143] T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi, and K. Sakurai, "A multivariate quadratic challenge toward post-quantum generation cryptography," *ACM Commun. Comput. Algebra*, vol. 49, no. 3, pp. 105–107, Nov. 2015. [Online]. Available: https://doi.org/10.1145/2850449.2850462

[144] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2005, pp. 164–175.

[145] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, "GeMSS: A great multivariate short signature." 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:8432066

[146] W. Beullens, "Breaking rainbow takes a weekend on a laptop," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/214, 2022. [Online]. Available: https://eprint.iacr.org/2022/214

[147] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkĺorper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung," *J. flur die reine und angewandte Mathematik*, vol. 1936, no. 175, pp. 193–208, 1936, doi: 10.1515/crll.1936.175.193.

[148] A. Ferozpuri and K. Gaj, "High-speed FPGA implementation of the NIST round 1 rainbow signature scheme," in *Proc. Int. Conf. ReConFigur. Comput. FPGAs (ReConFig)*, 2018, pp. 1–8.

[149] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper III. die Struktur des Meromorphismenrings. die Riemannsche Vermutung," *J. für die reine und angewandte Mathematik*, vol. 175, pp. 193–208, 1936. [Online]. Available: http://eudml.org/doc/149968

[150] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Proc. 4th Int. Workshop Post-Quantum Cryptogr.*, 2011, pp. 19–34.

[151] A. Rostovtsev and A. Stolbunov, "Public-key cryptosystem based on isogenies," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2006/145, 2006. [Online]. Available: https://eprint.iacr.org/2006/145

[152] J.-M. Couveignes, "Hard homogeneous spaces," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2006/291, 2006. [Online]. Available: https://eprint.iacr.org/2006/291

[153] S. Tani, "Claw finding algorithms using quantum walk," *Theor. Comput. Sci.*, vol. 410, no. 50, pp. 5285–5297, Nov. 2009. [Online]. Available: https://doi.org/10.1016

[154] P. C. Oorschot and M. J. Wiener, "Parallel collision search with cryptanalytic applications," *J. Cryptol.*, vol. 12, no. 1, pp. 1–28, Jan. 1999. [Online]. Available: https://doi.org/10.1007/PL00003816

[155] B. Koziel, A.-B. Ackie, R. E. Khatib, R. Azarderakhsh, and M. Mozaffari-Kermani, "SIKE'd up: Fast and secure hardware architectures for supersingular isogeny key encapsulation," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2019/711, 2019. [Online]. Available: https://eprint.iacr.org/2019/711

[156] S. Kim, Y. Lee, and K. Yoon, "Fibs: Fast isogeny based digital signature." Accessed: 3, 2024. [Online]. Available: https://www.kpqc.or.kr/images/pdf/FIBS.pdf

[157] R. Azarderakhsh, D. Jao, K. Kalach, B. Koziel, and C. Leonardi, "Key compression for isogeny-based cryptosystems," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2016/229, 2016. [Online]. Available: https://eprint.iacr.org/2016/229

[158] M. Anastasova, R. Azarderakhsh, and M. M. Kermani, "Fast strategies for the implementation of SIKE round 3 on ARM cortex-M4," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 10, pp. 4129–4141, Oct. 2021.

[159] R. Elkhatib, B. Koziel, R. Azarderakhsh, and M. Mozaffari Kermani, "Cryptographic engineering a fast and efficient SIKE in FPGA," *ACM Trans. Embed. Comput. Syst.*, vol. 23, no. 2, pp. 1–25, Mar. 2024. [Online]. Available: https://doi.org/10.1145/3584919

[160] B. Koziel, A. Jalali, R. Azarderakhsh, M. M. Kermani, and D. Jao, "NEON-SIDH: Efficient implementation of supersingular isogeny Diffie–Hellman key-exchange protocol on ARM," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2016/669, 2016. [Online]. Available: https://eprint.iacr.org/2016/669

[161] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Zero-knowledge from secure multiparty computation," in *Proc. 39th Annu. ACM Symp. Theory Comput.*, 2007, pp. 21–30. [Online]. Available: https://doi.org/10.1145/1250790.1250794

[162] I. Giacomelli, J. Madsen, and C. Orlandi, "ZKBoo: Faster zero-knowledge for boolean circuits," in *Proc. 25th USENIX Conf. Secur. Symp.*, 2016, pp. 1069–1083.

[163] M. Chase et al., "Post-quantum zero-knowledge and signatures from symmetric-key primitives," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2017/279, 2017. [Online]. Available: https://eprint.iacr.org/2017/279

[164] S. Kim et al., "AIM: Symmetric primitive for shorter signatures with stronger security (full version)," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1387, 2022. [Online]. Available: https://eprint.iacr.org/2022/1387

[165] M. Fellows and N. Koblitz, "Kid krypto," in *Proc. CRYPTO*, 1993, pp. 371–389.

[166] J. Kratochvíl, "Perfect codes over graphs," *J. Combinat. Theory, Ser. B*, vol. 40, no. 2, pp. 224–228, 1986. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0095895686900791

[167] J. Ryu, Y. Kim, S. Yoon, J.-S. Kang, and Y. Yeom. "Ipcc—Improved perfect code cryptosystems." Accessed: 3, 2024. [Online]. Available: https://www.kpqc.or.kr/images/pdf/IPCC.pdf

[168] I. Upasana, N. Nandanavanam, A. Nandanavanam, and N. Naaz, "Performance characteristics of NTRU and ECC Cryptosystem in context of IoT environment," in *Proc. IEEE Int. Conf. Distrib. Comput.*, 2020, pp. 23–28.

[169] Z. Liang, B. Fang, J. Zheng, and Y. Zhao, "Compact and efficient KEMs over NTRU lattices," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/579, 2022. [Online]. Available: https://eprint.iacr.org/2022/579

[170] "NTRU prime speed." Accessed: 3, 2024. [Online]. Available: https://ntruprime.cr.yp.to/speed.html

[171] H. Kwon, M. Sim, G. Song, M. Lee, and H. Seo, "Evaluating KpqC algorithm submissions: Balanced and clean benchmarking approach," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2023/1163, 2023. [Online]. Available: https://eprint.iacr.org/2023/1163

[172] K. Bürstinghaus-Steinbach, C. Krauß, R. Niederhagen, and M. Schneider, "Post-quantum TLS on embedded systems," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2020/308, 2020. [Online]. Available: https://eprint.iacr.org/2020/308

[173] Y. Hu, S. Dong, and X. Dong, "Analysis on Aigis-enc: Asymmetrical and symmetrical," *IET Inf. Security*, vol. 15, pp. 1–15, Mar. 2021.

[174] S. Zhou et al., "Preprocess-then-NTT technique and its applications to KYBER and NEWHOPE," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2018/995, 2018. [Online]. Available: https://eprint.iacr.org/2018/995

[175] J. Woo, K. Lee, and J. H. Park, "GCKSign: Simple and efficient signatures from generalized compact knapsacks," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1665, 2022. [Online]. Available: https://eprint.iacr.org/2022/1665

[176] *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. (2016). Accessed: 3, 2024. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[177] L. Wang and J. Hu, "Two new module-code-based KEMs with rank metric," in *Proc. 24th Aust. Conf. ACISP*, 2019, pp. 176–191.

[178] C. Kim, Y.-S. Kim, and J.-S. No, "Layered ROLLO-i: Faster rank-metric code-based KEM using ideal LRPC codes," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1572, 2022. [Online]. Available: https://eprint.iacr.org/2022/1572

[179] J. Cho, J.-S. No, Y. Lee, Z. Koo, and Y.-S. Kim, "Enhanced pqsigRM: Code-based digital signature scheme with short signature and fast verification for post-quantum cryptography," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2022/1493, 2022. [Online]. Available: https://eprint.iacr.org/2022/1493

[180] Y.-A. Chang, M.-S. Chen, J.-S. Wu, and B.-Y. Yang, "Postquantum SSL/TLS for embedded systems," in *Proc. IEEE 7th Int. Conf. Service-Orient. Comput. Appl.*, 2014, pp. 266–270.

[181] Y. Chen, "Quantum algorithms for lattice problems," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2024/555, 2024. [Online]. Available: https://eprint.iacr.org/2024/555

[182] "European telecommunications standards institute." Accessed: 3, 2024. [Online]. Available: https://www.etsi.org/

[183] "Chinese association for cryptologic research." Accessed: 3, 2024. [Online]. Available: https://www.cacrnet.org.cn/

[184] "Cryptography research and evaluation committees." Accessed 3, 2024. [Online]. Available: https://www.cryptrec.go.jp/en/

[185] "Overview of quantum initiatives worldwide 2023." Accessed: 3, 2024. [Online]. Available: https://qureca.com/es/overview-of-quantum-initiatives-worldwide-2023/

[186] (Qureca, Glasgow, Scotland). *Overview Of Quantum Initiatives Worldwide 2022*. (2022). (Accessed: 3, 2024). [Online]. Available: https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/

[187] "How quantum computers can break the Internet··· starting now no secret is safe." Accessed: 3, 2024. [Online]. Available: https://www.veritasium.com/videos/2023/4/14/how-quantum-computers-break-the-internet-starting-now/

[188] "The TLS post-quantum experiment." Accessed: 3, 2024. [Online]. Available: https://blog.cloudflare.com/the-tls-post-quantum-experiment

[189] N. Tsalis, E. Vasilellis, D. Mentzelioti, and T. Apostolopoulos, "A taxonomy of side channel attacks on critical infrastructures and relevant systems," in *Critical Infrastructure Security and Resilience* (Advanced Sciences and Technologies for Security Application). Cham, Switzerland: Springer, 2019.

[190] D. Tychalas and M. Maniatakos, "Special session: Potentially leaky controller: Examining cache side-channel attacks in programmable logic controllers," in *Proc. IEEE 38th Int. Conf. Comput. Design (ICCD)*, 2020, pp. 33–36.

[191] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Reliable and error detection architectures of Pomaranch for false-alarm-sensitive cryptographic applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 12, pp. 2804–2812, Dec. 2015.

[192] K. Ahmadi, S. Aghapour, M. M. Kermani, and R. Azarderakhsh, "Efficient algorithm level error detection for number-theoretic transform assessed on FPGAs," 2024, *arXiv:2403.01215*.

[193] T. Yu, C. Cheng, Z. Yang, Y. Wang, Y. Pan, and J. Weng, "Hints from Hertz: Dynamic frequency scaling side-channel analysis of number theoretic transform in lattice-based KEMs," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2024/070, 2024. [Online]. Available: https://eprint.iacr.org/2024/070

[194] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 2, pp. 1–19, Dec. 2016. [Online]. Available: https://doi.org/10.1145/2930664

[195] M. Mozaffari-Kermani and R. Azarderakhsh, "Reliable hash trees for post-quantum stateless cryptographic hash-based signatures," in *Proc. IEEE Int. Symp. Defect Fault Toler. VLSI Nanotechnol. Syst. (DFTS)*, 2015, pp. 103–108.

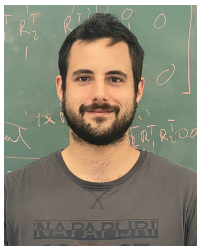
[196] H. N. S. Aldin, M. R. Ghods, F. Nayebipour, and M. N. Torshiz, "A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology," *Sens. Int.*, vol. 5, Jan. 2024, Art. no. 100258, doi: 10.1016/j.sintl.2023.100258.

[197] M. Campagna et al., "Quantum safe cryptography and security: An introduction, benefits, enablers and challengers," ETSI, Sophia Antipolis, France, White Paper, Jun. 2015. [Online]. Available: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

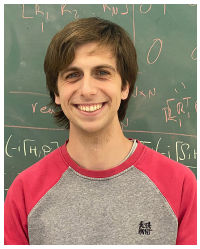
[198] D. Bernstein, "NSA, NIST, and post-quantum cryptography." Accessed: 3, 2024. [Online]. Available: https://www.muckrock.com/foi/united-states-of-america-10/nsa-nist-and-post-quantum-cryptography-126349/

[199] M. Yoshikawa and Y. Nozaki, "Electromagnetic analysis method for ultra low power cipher Midori," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, 2017, pp. 70–75.

[200] H. N. S. Aldin, M. R. Ghods, F. Nayebipour, and M. N. Torshiz, "A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology," *Sens. Int.*, vol. 5, 2024, Art. no. 100258. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666351123000323



Javier Oliva del Moral received the B.S. degree in telecommunications engineering from the Polytechnic University of Madrid, Madrid, Spain, in 2019, and the M.Sc. degree in astrophysics, cosmology and high energy physics from the Autonomous University of Barcelona, Bellaterra, Spain, in 2022. He is currently pursuing the Ph.D. degree in quantum dots, quantum error mitigation and post-quantum cryptography with the Quantum Information Lab, Tecnun-University of Navarra, Donostia-San Sebastian, Spain, and with the Donostia International Physics Center, Donostia-San Sebastian.



Antonio deMarti iOlius received the B.Sc. degree in physics from the University of Barcelona, Barcelona, Spain, in 2020, and the M.Sc. degree in physics from King's College London, London, U.K., in 2021. He is currently pursuing the Ph.D. degree in quantum error correction with the Quantum Information Lab, Tecnun-School of Engineering, Tecnun-University of Navarra, Donostia-San Sebastian, Spain.

His research interests include quantum error correcting codes, decoding algorithms, and post-quantum cryptography.

Gerard Vidal received the M.Sc. degree in complex systems, the M.Sc. degree in EE engineering, and the Ph.D. degree in physics from the Universidad de Navarra, Pamplona, Spain.

He is the Founder of Opscura, Donostia-San Sebastian, Spain, an industrial cybersecurity company. He is an Associate Professor with the Universidad de Navarra and Mondragon University, Mondragón, Spain.

Dr. Vidal received more than 25 prizes and awards, including the Alexander Fleming Award from London Business School. He is the Founding Member of the European CyberSecurity Organization, which reports to the European Commission. He is the Board Member of Spanish Standard Organization.

Pedro M. Crespo (Senior Member, IEEE) received the M.Sc. degree in applied mathematics and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1983 and 1984, respectively, and the engineering degree in telecommunications from the Universidad Politécnica de Catalunya, Barcelona, Spain, in 1987.

From September 1984 to April 1992, he was a member of the Technical Staff with the Signal Processing Research Group, Bell Communications Research, Chester Springs, NJ, USA, where he worked in the areas of data communication and signal processing. He actively contributed in the definition and development of the first prototypes of xDigital Subscriber Lines transceivers. From May 1992 to August 1999, he was a District Manager with the Telefónica Research and Development, Madrid, Spain. From 1999 to 2002, he was the Technical Director of Spanish Telecommunication Operator, Jazztel, Alcobendas, Spain. In 2009, he became the Director of the Electronics and Communication Department, Research and Development Center CEIT, Donostia-San Sebastian, Spain. He is currently a Professor with the TECNUN-School of Engineering, University of Navarra, Donostia-San Sebastian. He holds seven patents in the areas of digital subscriber lines and wireless communications. His research interests include the area of information and signal processing with a focus on wireless communications and networks. More recently, his interests also include quantum information theory and coding.

Dr. Crespo was a recipient of the Bell Communication Research's Award of Excellence.

Josu Etxezarreta Martinez received the B.S. (Hons.) and M.S. degrees in telecommunications engineering and the Ph.D. degree (summa cum laude) in quantum information theory from the TECNUN-School of Engineering, University of Navarra, Donostia-San Sebastian, Spain, in 2016, 2018, and 2022, respectively.

He is currently a Researcher with the Quantum Information Lab, Tecnun-University of Navarra, where he conducts research in topics related with quantum error correction, quantum information theory, error mitigation, open quantum systems, and post-quantum cryptography.

Dr. Etxezarreta Martinez received the Extraordinary Ph.D. Prize by the University of Navarra as a result of his dissertation.