Quantum Computing-Resistant Cryptography

Bruno Santos, *Student Member, IEEE,* and José Areia *Student Member, IEEE*

***Abstract*—Quantum computing is undoubtedly a hot topic in the research community, attracting considerable attention due to the latest advancements in technology. With that in mind, this paper aims to clarify the implications of quantum computing in contemporary cryptography and familiarise the reader with fundamental post-quantum algorithms, modern cryptographic principles, and the basics of quantum computing. The reader can explore the following subjects within the scope of this paper: cryptographic schemes (both symmetric and asymmetric), challenges inherent in quantum computing, quantum algorithms, affected public key encryption schemes, impacted symmetric schemes, the repercussions on hash functions, and the domain of post-quantum cryptography. Additionally, relevant open challenges and future work will be presented.**

***Index Terms*—Asymmetric Cryptography, Hash Functions, Post-Quantum Computing, Quantum Computing, Symmetric Cryptography.**

I. Introduction

There is no doubt that the advancement of technology indisputably serves as a cornerstone of the modern era [1]. However, a more substantial technological breakthrough has already been discovered, but it is yet to realise its full potential. In the early 1980s, Richard Feynman [2] proposed that certain quantum mechanical effects cannot be efficiently simulated on a classical computer. Consequently, he introduced the concept of simulating quantum physics using what he termed a "quantum computer". This observation prompted speculation that computation, in general, might be executed more efficiently by leveraging these quantum effects [3].

Constructing quantum computers with the available resources at that time posed a significant challenge. Furthermore, not only was the construction of quantum computers challenging given the available resources, but there was also uncertainty regarding how to harness quantum effects to expedite computation [4]. Consequently, progress in the field unfolded gradually. It was only in 1994, with the presentation of a polynomial time quantum algorithm for factoring integers by Peter Shor [5], [6], that the field of quantum computing truly came into prominence. While quantum computing is capable of solving n-time calculations in a brief time-frame [4], concerns are emerging about cryptography that is resistant to this advancing technology [5].

Cryptography is recognised as the practice and study of techniques for ensuring secure communication in the presence of adversarial behaviour [7]. These techniques often represent an intersection of various disciplines, including mathematics [8], computer science [9], information security [10], and more [11]. Mathematics plays a crucial role in this field, as robust algorithms are essential for deploying a secure cryptographic scheme [8]. However, quantum computing has the capability to comprehend and break algorithms in the blink of an eye. Consequently, many authors [12], [10], [11], [9] delve into this theme to understand which cryptographic algorithms are resistant to the potential threats posed by quantum computing [13]. In the context of these works, this paper aims to elucidate the concepts of quantum computing and cryptography. Subsequently, it endeavours to present solutions and viable approaches for cryptography that can withstand the challenges posed by quantum computing.

The paper is organised as follows. Section II will provide a concise background on quantum computing, modern cryptography, and include a literature review. Following that, Section III will delve into the post-quantum cryptography era. In doing so, vulnerable systems to quantum attacks will be outlined, and algorithms to mitigate these vulnerabilities will be presented. Finally, Sections IV and V will address some open challenges related to this theme and offer conclusions based on the outcomes of this work.

II. Background

This section is dedicated to the examination of crucial background information related to the paper's central theme. We will begin by evaluating quantum computing, delving into a comprehensive understanding of this technology, with a specific emphasis on the latest advancements. Furthermore, an overview of modern cryptography and its relevance to the paper's theme will be presented. Finally, a literature review will be provided to distinguish this work from other pertinent studies.

A. Quantum Computing

By definition, quantum computing refers to a computational paradigm that leverages quantum mechanical phenomena [5], [4]. These phenomena constitute a mathematical theory, governed by a set of axioms [2], [14]. The consequences of these axioms describe the behaviour of quantum systems [3]. Frequently, quantum calculations involve quantum states [10], which bear resemblance to probabilistic states [14], as these systems are represented by a column vector:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

where $|0\rangle$ read as "ket 0" and represents a quantum bit, or a qubit [3]. As mentioned, column vectors can be analogous to probabilistic states. Consider, for example, a bit. It can be in a state of 0 or 1. In a classical state, the probability of the bit being 0 is $\frac{1}{2}$, as it can either be 0 or not. However, if we

Both authors were with the School of Management and Technology, Polytechnic of Leiria, Portugal.
E-mail: {2230455, 2230456}@my.ipleiria.pt
José Areia are with Computer Science and Communication Research Centre, Polytechnic of Leiria, Portugal.

take into consideration a previous experience X, where we observe that 0 occurs $\frac{3}{4}$ of the time, and 1 occurs $\frac{1}{4}$ of the time, we realise that at present, unlike the simple 50% chance we typically have, we are dealing with a probabilistic state. This state can be expressed as follows:

$$\text{PR}(X = 0) = \frac{3}{4} \text{ and } \text{PR}(X = 1) = \frac{1}{4} \tag{2}$$

This type of representation can be succinctly expressed as follows, in conjunction with the "ket" notation:

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4} |0\rangle + \frac{1}{4} |1\rangle \tag{3}$$

Quantum states possess two essential characteristics: (a) the entries of a quantum state vector are complex numbers [5], and (b) the sum of the absolute values squared of the entries of a quantum state vector is 1 [3]. These simple changes, in contrast with probabilistic state vectors [4], can significantly enhance the efficiency of quantum computers [3] and communication protocols [15]. The mathematical expression that represents these changes follows the Euclidean norm of a column vector [16]. It is denoted and defined as follows:

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \Leftrightarrow \|v\| = \sqrt{\sum_{k=1}^{n} |a_k|^2} \tag{4}$$

For a single system, these operations are trivial, as we only need to consider the existence and the probability state of one system, e.g., the probability state of a single bit. However, when extended to multiple systems, the operations tend to become more challenging [4]. For the classical state, we can use the Cartesian product [16], which precisely captures the mathematical notion of viewing an element of one set and an element of a second set together, as if they form a single element of a combined set [17]. For the sake of notation, a probabilistic state of multiple states is represented as follows:

$$\frac{1}{2} |00\rangle + \frac{1}{2} |11\rangle \tag{5}$$

where "ket" is now represented by the column vector of the two systems, i.e., two bits that can be both 0 or 1. However, as mentioned earlier, the probabilistic state that forms the basis for quantum logic implies the necessity of a prior experience X. With multiple systems, we must have experiences X and Y for each system [3] (in this case, we only have two systems, so we only need an X and Y). The question is: What if we have the experience X but not the Y one? Quantum knowledge answers this question by stating that "when only X is measured, the results must be consistent with the probabilities we would obtain under the assumption that Y was also measured" [4]. This give us the so-called reduced probabilistic state of X alone:

$$\text{PR}(X = a) = \sum_{b \in \Gamma} \text{PR}((X, Y) = (a, b)) \tag{6}$$

With this formula, we can now comprehend the probabilistic state of Y. However, multiple systems do not consist of just two bits, as we have been illustrating. Multiple systems are defined with n-systems, each having its own probability state. This implies that simple Cartesian products are insufficient to resolve the calculations for a single combined set [15]. Instead, all the probability states of the different systems are arranged in their own matrices, and then the probability of that matrix is calculated in conjunction with the other states. The following calculation shows a summary of the calculations mentioned:

$$\begin{pmatrix} 1 & \frac{1}{2} & 0 \\ 1 & 1 & 0 \\ 1 & 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \tag{7}$$

As we are currently considering two systems, these conditions naturally extend for further calculations in the case of multiple systems.

Since quantum computing involves multiple systems that can be infinite, a circuit is necessary to understand them [4]. In a quantum circuit model, wires represent qubits, and gates represent operations acting on these qubits [3], [16]. Figure 1 illustrates a quantum circuit on the qubit X in which operations HTH were performed.

Fig. 1. Quantum circuit diagram depicting the operations on a single X qubit, including the application of H, T, and H gates in sequence.

To enhance coherence and improve readability, we can design the output of the operation at the end of the circuit. For example, for the state $|0\rangle$ with the operation TSH the result is $\frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle$, so we can represent this as follows:

Fig. 2. Quantum circuit diagram depicting the operations on a single $|0\rangle$ qubit, including the application of T, S, and H gates in sequence with a representative output.

It is possible to represent multiple systems in the same diagram. Figure 3 represents a multiple system with both states $|a\rangle$ and $|b\rangle$. First, the state $|a\rangle$ is affected by the Hadamard operation. Then, the controlled-NOT operation is performed, where $|a\rangle$ is the controller, and $|b\rangle$ is the target.

Finally, the junction between classical bits and qubits is also possible, i.e., a qubit can, in space and time, be transformed into a classical bit [12]. These types of transformations can also be represented in a diagram. Figure 4 represents the two previous qubit states $|a\rangle$ and $|b\rangle$, and then the two classical bits c and d.

The classical bits are represented by two parallel lines, and the transformation that can occur when a qubit is transformed into a classical bit is represented by the measurement gate. In

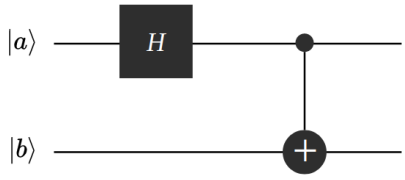

Fig. 3. Multiple systems quantum circuit with both $|a\rangle$ and $|b\rangle$ states, affected by Hadamard operation and a NOT gate.

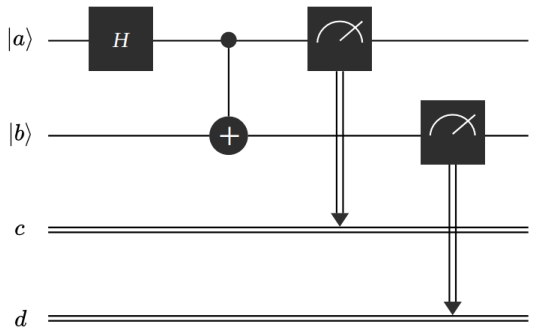

Fig. 4. Multiple systems quantum circuit with both $|a\rangle$ and $|b\rangle$ states, affected by Hadamard operation, a NOT gate, and a measurement gate that change their post-measurement states to classic bits c and d.

Figure 4 both states $|a\rangle$ and $|b\rangle$ are measured and are changed into their post-measurement states, while the measurement outcomes are overwritten onto the classical bits c and d respectively, as indicated by the arrows.

Despite being highly valuable for high-speed calculations, quantum systems can indeed present difficult challenges to overcome. Quantum computers are primarily probabilistic [18]. This implies that in one operation, many solutions can be generated, but only one is correct. In fact, this trial and error weakens the advantage of quantum computing [10]. These systems are susceptible to errors, especially qubits [18]. They can be affected by heat [13], noise in the environment [14], as well as stray electromagnetic couplings [17]. They also happen to have not only bit-flips, like classical computers, but also phase errors [18].

In 2017, Bishop *et al.* introduced the definition of "Quantum Volume", which is a metric to measure how powerful a quantum computer is based on the number of qubits it has, the quality of error correction on these qubits, and the number of operations that can be performed in parallel. Conclusions were drawn that an increase in the number of qubits does not improve a quantum computer if the error rate is high. However, improving the error rate would result in a more powerful quantum computer [19].

B. Modern Cryptography

Cryptography is the art of securing communication and information [20]. It uses techniques to protect data from unauthorised access [20], manipulation [21], and interception [22]. This field has evolved significantly, moving from simple methods to advanced algorithms. The goals of cryptography can be summarised into four main objectives. The first objective is confidentiality, which ensures that only authorised recipients can access information through data encryption. The second objective is integrity, which guarantees that information remains unaltered during transmission or storage, thus increasing the reliability of data. The third objective is authentication, which verifies the identities of communicating parties, establishing trust and preventing impersonation. Finally, non-repudiation provides indisputable proof of message origin, limiting the ability to deny sending a message [20].

Cryptography algorithms are vast [21] and can be grouped into three different cryptography systems [20]. These systems are designed to accomplish the goals of cryptography, but not all of them can accomplish all four by design [23].

The first system is symmetric-key cryptography, also known as "secret key" [22]. This system uses a shared secret key between the sender and receiver to encrypt and decrypt messages. Additionally, this system primarily provides confidentiality, but it does not inherently offer integrity, authentication, or non-repudiation [20]. This system can be represented by two functions [22]. The first function takes place on the sender and it is the encryption (E) of the message (M) with the secret key (k) - that results in the cipher text (CT):

$$E_k(M) = CT \tag{8}$$

The second function takes place on the receiver and it is the decryption (D) of the cipher text (CT), using the secret key (k), to obtain the original message (M):

$$D_k(CT) = M \tag{9}$$

On the other hand, asymmetric-key cryptography uses two different keys - one public and one private. These keys are mathematically related to each other and form a pair. When using asymmetric cryptography, the sender uses the recipient's public key to encode the message, which can only be decoded using the recipient's private key. This means that if a message is stolen, it will be useless to the thief without the corresponding private key. The sender can also use his private key to encode the message, which can only be decoded using the sender's public key. This method doesn't provide confidentiality but it provides authentication, integrity and non-repudiation on the sender's end.

The whole system alone, despite being slower than the previous one, can provide confidentiality [23], integrity [20], authentication and non-repudiation [21]. This system can be represented by at least four functions: two in the sender and two in the receiver [22]. In the functions, the sender will be represented by the letter A and the receiver by the letter B. The first function will take place on the sender and will use the receiver's public key (PUB) to cipher the message:

$$E_{PUB_B}(M) = CT \tag{10}$$

This message can only be decoded by the recipient using its own private key PR:

$$D_{PR_B}(CT) = M \tag{11}$$

This method only assures confidentiality and non-repudiation on the receiver's end. The other method, in asymmetric encryption, is to encrypt the message on the sender's end with its own private key:

$$E_{PR_A}(M) = CT \tag{12}$$

On the receiver's end, the ciphertext can be decoded using the sender's public key:

$$D_{PR_A}(CT) = M \tag{13}$$

This method, also known as digital signature, does not assure confidentiality because everyone can decode the ciphertext. However, it does assure authentication, integrity and non-repudiation on the sender's end. These two methods can also be put to work together to get the best of both.

The last system of cryptography is a cryptographic hash function. A hash function is a one-way mathematical function [23] that converts data of any length into a hashed output of a fixed length [21]. A one-way function means that the hashed output cannot be reverted to the initial input [20]. This system, by design, primarily provides integrity and can be represented by a single function [22]. The hash function (H) will take the message (M) as its input and output the hashed version of the message (Z):

$$H(M) = Z \tag{14}$$

It is important to note that neither of these systems is better than the other, each having its specific use and advantages. Cryptographic algorithms can also be divided into classical cryptography, post-quantum cryptography or quantum cryptography [24]. Classical cryptography employs complex mathematical problems to safeguard data from non-quantum threats. On the other hand, post-quantum cryptography utilises even more complex mathematical problems that can withstand quantum attacks [25]. Meanwhile, quantum cryptography utilises the properties of quantum mechanics to secure data from quantum threats, rather than relying on difficult mathematical problems [24], [25].

C. Literature Review

Numerous researchers have devoted their efforts to comprehending the capabilities of quantum computing and identifying the requirements necessary to establish and/or validate the resistance of specific cryptographic algorithms to quantum computing. This subsection aims to present some of works related to this topic.

Mavroeidis *et al.*, in their work titled "The Impact of Quantum Computing on Present Cryptography" [26], endeavoured to elucidate the implications of quantum computing on current cryptography and introduce the reader to basic post-quantum algorithms. Interestingly, their paper diverges from the conventional mathematical algorithms of Shor [5] and Grover [27]. Instead, it delves into various quantum key distribution methods and mathematical-based solutions, including the BB84 protocol, lattice-based cryptography, multivariate-based cryptography, hash-based signatures, and code-based cryptography. The authors concluded that quantum computing poses a substantial risk to both traditional public key algorithms and symmetric key algorithms. One of the proposed solutions is to adopt the quantum key distribution methods and mathematical-based solutions presented in their work.

In 2017, Aumasson published an article titled "The Impact of Quantum Computing on Cryptography" [10]. In his work, he explores various aspects of cryptography, quantum computing, and the algorithms [5], [6], [27] that undermine the traditional cryptographic algorithms in use today. The author concludes, and we quote, "There is no need to panic, though – in my opinion, the quantum computers that will break RSA won't come this year, very likely not this decade, and probably not this century". This statement indicates that, from the perspective of the author, advancements are being made in the field of quantum computing, but we are still considerably distant from achieving practical and meaningful utilisation of this technology.

In an intriguing perspective, Fernández-Caramés and Fraga-Lamas presented their work on blockchain cryptography designed to withstand quantum computing attacks [9]. Because blockchain uses public-key cryptography and hash functions, the technology can be affected by quantum computing attacks. The authors analysed the impacts of quantum computing attacks, specifically based on Grover's and Shor's algorithms, on blockchain technology. The study focused on exploring the application of post-quantum cryptosystems to mitigate the potential threats posed by these quantum algorithms. The authors concluded that certain enhancements are imperative for the future of quantum computing in the context of blockchain. These enhancements encompass the aggregation of signatures, ring signatures, identity-based encryption (IBE), secret sharing, homomorphic encryption, zero-knowledge proofs, and secure multi-party computation (SMPC).

Malviya *et al.*, in their work titled "Quantum Cryptanalytic Attacks of Symmetric Ciphers: A Review" [28], provide a comprehensive review of various quantum attacks on symmetric cryptography. In contrast to other works, the primary objective of this work is to furnish valuable information for cryptologists, enabling them to incorporate new quantum crypt-analysis techniques into their toolbox and leverage them in the development of post-quantum symmetric ciphers. The authors present various quantum attacks, hitherto unique in the literature, including the quantum differential attack, quantum truncated differential attack, quantum impossible differential attack, quantum linear crypt-analysis, Simon's algorithm attack, Quantum DS Meet-in-the-Middle, Quantum Related Key attacks, and Quantum collision search. In addition to detailing the utility and application of these attacks, the authors propose countermeasures against them.

All the works presented in this literature review aimed to contribute to the community's understanding in the fields of cryptography, quantum computing, and post-quantum computing. They not only provided essential information for compre-

hending the concepts but also offered potential solutions for future mitigation's within the respective themes.

III. Quantum Computing-Resistant Cryptography

The impact of quantum computers on modern cryptography is notable [26]. Since quantum computers represent a distinct and potentially more powerful paradigm for computing [13] than classical computers, cryptographic security needs to keep pace with developments in the quantum domain to remain resistant to this technology [10]. To address this challenge, a new area of study has emerged. The goal of this study area, known as post-quantum cryptography or quantum-resistant cryptography, is to develop cryptographic systems that are secure against both quantum and conventional computers while maintaining interoperability with existing communication protocols and networks [29], [26]. To enhance security in these terms, the first step is to understand which systems are vulnerable to quantum algorithms.

A. Cryptosystems Vulnerable to Quantum Algorithms

Both symmetric [12] and asymmetric [5], [6] cryptography exhibit vulnerabilities in the face of quantum computing advancements. As previously mentioned, in 1994, Peter Shor [5] demonstrated that the factorisation of large integers would undergo fundamental changes when addressed using quantum computers. Asymmetric algorithms are commonly referred to as one-way functions due to their ease of computation in one direction, while the inversion process proves to be challenging [1]. This is attributed to the fact that asymmetric algorithms, exemplified by RSA, leverage the computational challenge associated with the factorisation of bi-prime numbers. Nevertheless, Kirsch and Chow [18] posited that RSA is theoretically susceptible in the event of the introduction of a rapid factorisation algorithm or a substantial increase in computational power. The latter could be realised through the application of quantum mechanics in computing, commonly referred to as quantum computers.

Additionally, asymmetric cryptographic algorithms, such as Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC), rely on addressing the Discrete Logarithm Problem (DLP) [26]. This problem is challenging to solve as it involves determining the integer a in the equation $g^a \equiv x \mod p$. The integer a is denoted as the discrete logarithm problem of x to the base g, expressed as $a = \log_g x \mod p$. The discrete logarithm problem proves to be difficult to compute when the parameters are sufficiently large, as recommended in recent advisories. This is particularly relevant when employing algorithms like Diffie-Hellman, where key sizes are advised to be 2048 bits or larger [8].

On the contrary, for symmetric algorithms, quantum computing poses a relatively minor threat, as the computational speed does not compromise their security significantly [10]. The sole known concern related to symmetric algorithms is Grover's algorithm, which provides a square root speed-up over classical brute force algorithms [27]. For instance, for a n-bit cipher the quantum computer operates on $\sqrt{2^n} = 2^{n/2}$, implying that a symmetric cipher with a key length of 128 bits, such as AES-128, would offer a security level equivalent to 64 bits [26]. Nevertheless, a report by NIST [29] emphasised that if key sizes are adequate, symmetric cryptographic schemes, particularly the Advanced Encryption Standard (AES), exhibit resistance to quantum computers.

Table I provides a comparative yet simple analysis of classical and quantum security levels in prominent cryptographic schemes aforementioned, based on the research conducted by Mavroeidis *et al.* [26].

TABLE I
Comparative Analysis of Classical and Quantum Security Levels in Prominent Cryptographic Schemes, based on the research by Mavroeidis *et al.* [26].

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		Classical Computing	Quantum Computing
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

Lastly, the family of hash functions faces a challenge similar to symmetric algorithms, as their security is contingent upon a fixed output length. Attacks such as pre-image and collision attacks can be employed against this category of algorithms [8]. However, in the realm of quantum computing, it is feasible to utilise Grover's algorithm to find a collision in a hash function within square root steps of its original length [26], [10]. Brassard *et al.* [30] additionally demonstrated that, to ensure a b-bit security level against Grover's quantum algorithm, a hash function must furnish at least a $3b$-bit output. Consequently, numerous existing hash algorithms are deemed unsuitable for use in the quantum era. However, both SHA-2 [13] and SHA-3 [18], with extended output lengths, persist as quantum-resistant options.

Table II summarises the algorithms considered throughout the extensive content of this article. The table also includes information on functionality, security strength, affected cryptographic protocols, and associated mitigation measures.

TABLE II
Exploring the Influence of Quantum Algorithms on Cryptography Protocols and Strategies for Mitigation

Quantum Algorithm	Functionality	Impacted Algorithms	Mitigation
Shor [5]	Factoring	RSA	Migrate to QSC
Shor [6]	Discrete logarithm	DF, DSA, ECC	Migrate to QSC
Grover [27]	Key search	**Symmetric key algorithms (e.g., AES)**	**Sufficient key length**
Grover [27]	Pre-image attack	**Hash functions (e.g., SHA-256)**	**Sufficient hash length**

B. Quantum-Resistant Cryptographic Algorithms

It has been established that modern cryptography poses a threat to quantum computing. With this consideration, this subsection introduces algorithms designed to mitigate these threats. There are numerous alternatives to mathematical problems that have already been implemented as public key

cryptographic schemes, which the Hidden Subgroup Problems (HSP) - that includes the factorising integers or computing discrete logarithms - does not encompass [31]. Hence, they are quantum resistant. The alternatives are the following: (1) Lattice-based cryptography [32], (2) Hash-based signatures [33], (3) Code-based cryptography [34], and (4) Multivariate-based cryptography [35].

1) Lattice-based Cryptography: This represents a form of public-key cryptography [26]. Of crucial significance are two computational problems associated with lattices, namely the shortest vector problem [32] and the learning with errors problem [36]. However, this cryptographic approach avoids the vulnerabilities associated with RSA. Instead of multiplying primes, this method involves the multiplication of matrices. Consequently, it does not fall to the vulnerabilities exploited by Shor's algorithm. To accomplish this, numerous candidates [37] attempted to implement a Lattice-based algorithm with the goal of finding the shortest non-zero vector, which is considered optimal [32], and to be part of NIST's quantum-safe cryptographic standard. Three algorithms were chosen: (a) CRYSTALS-Kyber, among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation, (b) CRYSTALS-Dilithium which has high efficiency and it is recommend has the primary algorithm, and (c) FALCON which has high efficiency too, but it is recommend for applications that need smaller signatures than Dilithium can provide.

Departing from NIST's quantum-safe cryptographic standards, an older algorithm presented in 1998 by Hoffstein *et al.* is NTRU [38]. NTRU can be employed for both encryption and digital signatures. Its resistance to Shor's algorithm is attributed to the challenge of factorising specific polynomials. In both 2013 [39] and 2016 [40], newer versions of NTRU were published, enhancing the algorithm's security through the implementation of more secure ring structures. As of today there is not any known attack for NTRU [13]. Therefore, we can conclude that NTRU, despite not being part of the NIST's standards, can be considered a viable candidate for the post-quantum era.

2) Hash-based Signatures: This type of signature scheme was initially invented by Leslie Lamport in 1979. Subsequently, in 2009, Bernstein [41] succinctly introduced the scheme. In simple terms, hash-based signatures articulate the problem by specifying a parameter a that delineates the desired security level for our system [33]. For a 128-bit a security level, a secure hash function is required, capable of accepting arbitrary-length input and generating a 256-bit output [26]. Consequently, SHA-256 is regarded as an optimal solution that can accommodate our message m.

To complete the signature scheme, a pair of keys — private and public — is utilised. For the private key, a random number generator is employed to produce 256 pairs of random numbers. Subsequently, for the public key, all the generated numbers from the private key are independently hashed, resulting in the creation of 512 different hashes (256 pairs) of 256-bit length each.

The subsequent step is to sign the message. To achieve this, for each bit of the message digest, one number is selected from each pair that constitutes the private key [33]. With this approach, a sequence of 256 numbers is obtained. This sequence of numbers constitutes the digital signature, which is then published along with the plaintext message. In accordance with the "Lamport one-time signature," the private key should never be used again, and the remaining 256 numbers from the pairs should be destroyed.

Supported by Buchmann *et al.* [41], the authors explain that in the scenario where signing multiple messages is desired, chaining can be introduced. Witernitz developed a one-time signature (WOTS) that he proved to be more efficient than Lamport's, as the signature size and the keys are smaller [42]. Later, Merkle introduced a new approach that combines Witernitz's OTS with binary trees, known as the Merkle Signature Scheme [43]. Presently, two hash-based signature schemes are being considered for standardisation: the eXtended Merkle Signature Scheme (XMSS) [44] and Stateless Practical Hash-based Incredibly Nice Collision-resilient Signatures (SPHINCS) [45].

3) Code-based Cryptography: Code-based cryptography pertains to cryptographic systems that utilise error-correcting codes [34]. These types of algorithms rely on the challenge of decoding linear codes. Therefore, they are considered resistant to quantum attacks when the key sizes are increased by a factor of 4 [45]. Furthermore, Buchmann *et al.* [44] assert, with the usage of McEliece's original public-key code-based scheme, that the optimal approach to address the decoding problem is to transform it into a Low-Weight-Code-World Problem (LWCWP). However, solving a LWCWP in large dimensions is regarded as infeasible [28].

For every cryptographic system, the application of code-based cryptography represents a trade-off between efficiency and security. McEliece's cryptosystem exhibits fast encryption and decryption processes with very low complexity, but it necessitates the use of large public keys (ranging from 100 kilobytes to several megabytes) [26].

4) Multivariate-based Cryptography: By definition, this type of cryptography involves the simultaneous observation and analysis of more than one outcome variable, i.e., multivariate random variables [35]. The security of this public key scheme relies on the challenge of solving systems of multivariate polynomials over finite fields. Multivariate systems can be used for both digital signatures and encryption [46]. However, researchers [47], [46] have presented various attempts to construct asymmetric public key systems based on multivariate polynomials. However, many of them are considered insecure due to the fact that certain quadratic forms associated with their central maps have low rank. The most promising signature schemes include Unbalanced Oil and Vinegar (based on multivariate quadratic equations) [47] and Rainbow [13]. UOV has larger signatures and public key sizes due to a 3:1 ratio of variables to equations, while Rainbow is more efficient with smaller ratios, resulting in shorter signatures and key sizes [48].

IV. Open Challenges & Future Work

The emergence of quantum computers, capable of breaking most traditional cryptography algorithms, necessitates the migration to quantum-safe cryptography, particularly asymmetric key systems. Quantum computers are still in their early stage, presenting a lot of problems for them to be used for decrypting data. In symmetric and hash cryptosystems, while being theoretically possible to obtain the full quadratic speedup using Grover's algorithm, all the steps of the algorithm must be performed in series. In the real world, where attacks on cryptography use massively parallel processing, the advantage of Grover's algorithm will be way smaller than expected. In 1999, Christof Zalka had already shown the limitations of paralleling Grover's algorithm in the paper "Grover's quantum searching algorithm is optimal" [49]. The most vulnerable cryptosystem, the asymmetric, is highly vulnerable to quantum computing due to Shor's algorithm. However, the feasibility of running this algorithm on today's quantum computers is still in question. Quantum computers still produce a lot of errors and some succumb to them. To get closer to the theoretical potential of Shor's algorithm, a quantum computer with error tolerance is necessary [50], [51]. These are some of the challenges that quantum researchers still have to face. For future work, there is a need for further research and practical applications in the areas of quantum error correction and quantum-resistant asymmetric cryptography.

V. Conclusion

In the modern world, where information holds a crucial role, it is imperative to ensure maximum security during data transmission and storage. Quantum computers are in their early stage of development and will not be a problem for cryptography for some years. However, with the use of Grover's and Shor's algorithms, quantum computers will pose a significant threat to modern cryptography systems in the future. These future attacks can be used in the data that is being transmitted now – this is known as harvest now and decrypt later. This means that is not sufficient to wait until quantum computing becomes a problem, but to prevent it now. The most affected cryptosystem is the asymmetric key cryptography which will need to be replaced with quantum-safe cryptography. Mathematical-based cryptosystems like lattice-based cryptography, hash-based signatures and code-based cryptography are the potential candidates for the migration. As for the rest of the cryptosystems, there is no need to replace the modern cryptography algorithms for the post-quantum ones. However, an increase in the key length and hash length will be needed.

Acknowledgment

This research received support during the Secure Computer Systems Administration course, instructed by Professor Patrício Domingues (0000-0002-6207-6292) at the School of Management and Technology, Polytechnic of Leiria.

References

[1] M. Dusek, N. Lutkenhaus, and M. Hendrych, "Quantum Cryptography," in *Quantum Cryptography*, 2006, vol. 49, pp. 381–454, arXiv:quant-ph/0601207. [Online]. Available: http://arxiv.org/abs/quant-ph/0601207

[2] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467–488, Jun. 1982. [Online]. Available: https://doi.org/10.1007/BF02650179

[3] E. G. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," 2000.

[4] J. Preskill, "Quantum computing 40 years later," arXiv, Tech. Rep., Feb. 2023, arXiv:2106.10522 [quant-ph] type: article. [Online]. Available: http://arxiv.org/abs/2106.10522

[5] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, pp. 124–134. [Online]. Available: https://ieeexplore.ieee.org/document/365700

[6] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, arXiv:quant-ph/9508027. [Online]. Available: http://arxiv.org/abs/quant-ph/9508027

[7] M. Bellare and P. Rogaway, *Introduction to Modern Cryptography*. Boca Raton, FL: CRC Press, 2005.

[8] R. L. Rivest, "CHAPTER 13 - Cryptography," in *Handbook of Theoretical Computer Science*, ser. Handbook of Theoretical Computer Science, J. Van leeuwen, Ed. Amsterdam: Elsevier, Jan. 1990, pp. 717–755. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780444880710500187

[9] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8967098

[10] J.-P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, Jun. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372317300519

[11] S. B. Sadkhan, "Key note lecture multidisciplinary in cryptology and information security," in *2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE)*, Dec. 2013, pp. 1–2. [Online]. Available: https://ieeexplore.ieee.org/document/6998773

[12] Z. Liu, K. Nguyen, G. Yang, H. Wang, and D. Wong, "A lattice-based linkable ring signature supporting stealth addresses," 2019.

[13] D. B. S. Solanki, A. Saini, and A. Saini, "Review paper on quantum computing and quantum cryptography," 2023.

[14] R. Liboff, *Introductory Quantum Mechanics*. Pearson Education, 2003. [Online]. Available: https://books.google.pt/books?id=xMIlAgQSRUsC

[15] C. R. García, S. Rommel, S. Takarabt, J. V. V. Olmos, S. Guilley, P. Nguyen, and I. T. Monroy, "Quantum-resistant transport layer security," 2024.

[16] J. L. Brien, "Optical quantum computing," *Science*, vol. 318, no. 5856, p. 1567–1570, Dec. 2007. [Online]. Available: http://dx.doi.org/10.1126/science.1142892

[17] S. Simonović, "On Photonic Implementation of Quantum Computers," *Advanced Technologies and Materials*, vol. 48, no. 2, pp. 61–68, Dec. 2023. [Online]. Available: http://atm-journal.uns.ac.rs/index.php/atm/article/view/1192

[18] Z. J. Kirsch and M. Chow, "Quantum Computing: The Risk to Existing Encryption Methods," in *Quantum Computing: The Risk to Existing Encryption Methods*, 2015.

[19] L. Bishop, S. Bravyi, A. W. Cross, J. Gambetta, J. Smolin, and March, "Quantum Volume," in *Quantum Volume*, 2017. [Online]. Available: https://www.semanticscholar.org/paper/Quantum-Volume-Bishop-Bravyi/650c3fa2a231cd77cf3d882e1659ee14175c01d5

[20] A. J. Menezes, P. C. v. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Dec. 2018, google-Books-ID: YyCyDwAAQBAJ.

[21] "What is Cryptography?" Sep. 2023. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

[22] A. Salomaa, *Public-Key Cryptography*. Springer Science & Business Media, Oct. 1996.

[23] "What is cryptography?" 2023. [Online]. Available: https://www.iso.org/information-security/what-is-cryptography

[24] "Classical cryptography and quantum cryptography," 2023. [Online]. Available: https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/

[25] R. Copil, "Classical vs. Quantum vs. Post-Quantum Cryptography," Jul. 2020. [Online]. Available: https://www.quantropi.com/differences-between-classical-quantum-post-quantum-cryptography/

[26] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018, arXiv:1804.00200 [cs]. [Online]. Available: http://arxiv.org/abs/1804.00200

[27] L. K. Grover, "A fast quantum mechanical algorithm for database search," arXiv, Tech. Rep., Nov. 1996, arXiv:quant-ph/9605043 type: article. [Online]. Available: http://arxiv.org/abs/quant-ph/9605043

[28] A. K. Malviya, N. Tiwari, and M. Chawla, "Quantum cryptanalytic attacks of symmetric ciphers: A review," *Computers and Electrical Engineering*, vol. 101, p. 108122, Jul. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790622003743

[29] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," 2016-04-28 2016.

[30] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," *ACM SIGACT News*, vol. 28, no. 2, pp. 14–19, Jun. 1997. [Online]. Available: https://dl.acm.org/doi/10.1145/261342.261346

[31] J. Lomonaco and L. H. Kauffman, "Quantum Hidden Subgroup Problems: A Mathematical Perspective," arXiv, Tech. Rep., Jun. 2002, arXiv:quant-ph/0201095 type: article. [Online]. Available: http://arxiv.org/abs/quant-ph/0201095

[32] D. Micciancio and O. Regev, "Lattice-based Cryptography," in *Lattice-based Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer, 2009, pp. 147–191. [Online]. Available: https://doi.org/10.1007/978-3-540-88702-7_5

[33] C. Dods, N. P. Smart, and M. Stam, "Hash Based Digital Signature Schemes," in *Hash Based Digital Signature Schemes*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and N. P. Smart, Eds., vol. 3796. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 96–115. [Online]. Available: http://link.springer.com/10.1007/11586821_8

[34] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Code-based cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 95–145. [Online]. Available: http://link.springer.com/10.1007/978-3-540-88702-7_4

[35] J. Ding and B.-Y. Yang, "Multivariate Public Key Cryptography," in *Multivariate Public Key Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer, 2009, pp. 193–241. [Online]. Available: https://doi.org/10.1007/978-3-540-88702-7_6

[36] Y.-K. Liu, V. Lyubashevsky, and D. Micciancio, "On Bounded Distance Decoding for General Lattices," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, ser. Lecture Notes in Computer Science, J. Díaz, K. Jansen, J. D. P. Rolim, and U. Zwick, Eds. Berlin, Heidelberg: Springer, 2006, pp. 450–461.

[37] NIST, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," *NIST*, Jul. 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[38] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*, ser. Lecture Notes in Computer Science, J. P. Buhler, Ed. Berlin, Heidelberg: Springer, 1998, pp. 267–288.

[39] D. Stehlé and R. Steinfeld, "Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices," 2013, publication info: Published elsewhere. Submitted. Some of the results in this paper have been presented in preliminary form at Eurocrypt 2011. [Online]. Available: https://eprint.iacr.org/2013/004

[40] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "NTRU Prime: Reducing Attack Surface at Low Cost," in *Selected Areas in Cryptography – SAC 2017*, ser. Lecture Notes in Computer Science, C. Adams and J. Camenisch, Eds. Cham: Springer International Publishing, 2018, pp. 235–260.

[41] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Introduction to post-quantum cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer, 2009, pp. 1–14. [Online]. Available: https://doi.org/10.1007/978-3-540-88702-7_1

[42] A. Hülsing, "W-ots+ - shorter signatures for hash-based signature schemes," in *Progress in Cryptology–AFRICACRYPT 2013*, ser. Lecture Notes in Computer Science (LNSC), A. Youssef, A. Nitaj, and A. Hassanien, Eds. Germany: Springer, 2013, pp. 173–188, 6th International Conference on the Theory and Application of Cryptographic Techniques in Africa (Africacrypt 2013), Africacrypt 2011 ; Conference date: 22-06-2013 Through 24-06-2013.

[43] R. C. Merkle, "A Certified Digital Signature," in *Advances in Cryptology — CRYPTO' 89 Proceedings*, ser. Lecture Notes in Computer Science, G. Brassard, Ed. New York, NY: Springer, 1990, pp. 218–238.

[44] J. Buchmann, E. Dahmen, and A. Hülsing, "Xmss - a practical forward secure signature scheme based on minimal security assumptions," Cryptology ePrint Archive, Paper 2011/484, 2011, https://eprint.iacr.org/2011/484. [Online]. Available: https://eprint.iacr.org/2011/484

[45] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn, "SPHINCS: Practical Stateless Hash-Based Signatures," in *Advances in Cryptology – EUROCRYPT 2015*, ser. Lecture Notes in Computer Science, E. Oswald and M. Fischlin, Eds. Berlin, Heidelberg: Springer, 2015, pp. 368–397.

[46] W. Buchanan and A. Woodward, "Will quantum computers be the end of public key encryption?" *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 1–22, Jan. 2017. [Online]. Available: https://doi.org/10.1080/23742917.2016.1226650

[47] C. Tao, A. Diene, S. Tang, and J. Ding, "Simple Matrix Scheme for Encryption," in *Post-Quantum Cryptography*, ser. Lecture Notes in Computer Science, P. Gaborit, Ed. Berlin, Heidelberg: Springer, 2013, pp. 231–242.

[48] B. Rawal and A. Peter, "Quantum-Safe Cryptography and Security," in *Quantum-Safe Cryptography and Security*, ser. Blockchain Technologies, B. S. Rawal, G. Manogaran, and M. Poongodi, Eds. Singapore: Springer Nature, 2022, pp. 35–51. [Online]. Available: https://doi.org/10.1007/978-981-16-3412-3_2

[49] C. Zalka, "Grover's quantum searching algorithm is optimal," *Physical Review A*, vol. 60, no. 4, pp. 2746–2751, Oct. 1999, arXiv:quant-ph/9711070. [Online]. Available: http://arxiv.org/abs/quant-ph/9711070

[50] M. Amico, Z. H. Saleem, and M. Kumph, "An Experimental Study of Shor's Factoring Algorithm on IBM Q," *Physical Review A*, vol. 100, no. 1, p. 012305, Jul. 2019, arXiv:1903.00768 [quant-ph]. [Online]. Available: http://arxiv.org/abs/1903.00768

[51] J.-Y. Cai, "Shor's Algorithm Does Not Factor Large Integers in the Presence of Noise," arXiv, Tech. Rep., Jun. 2023, arXiv:2306.10072 [quant-ph] type: article. [Online]. Available: http://arxiv.org/abs/2306.10072

Bruno Santos Bruno Santos (Student Member, IEEE) received a bachelor's degree in Computer Engineering, from Polytechnic of Leiria, Portugal, in 2023. He is currently taking a master's degree in Cybersecurity and Digital Forensics, from Polytechnic of Leiria, Portugal.

José Areia José Areia (Student Member, IEEE) obtained his bachelor's degree in Computer Engineering from Polytechnic of Leiria, Portugal, in 2023. Currently pursuing a master's degree in Cybersecurity and Digital Forensics at Polytechnic of Leiria, he is actively engaged in the research project "Secure and Privacy-Preserving Machine Learning" at the Computer Science and Communication Research Centre. Additionally, he serves as an assistant professor at the School of Management and Technology at Polytechnic of Leiria.