Communication

Impact of Quantum Computing on Asymmetric Cryptography Infrastructures: Prospective Study and Post-Quantum Transition Roadmap

João Lucas *, Carlos Caleiro, António Gonçalves, Laercio Cruvinel

Posted Date: 29 December 2025

doi: 10.20944/preprints202512.2449.v1

Keywords: quantum computing; asymmetric cryptography; post-quantum transition; resilience of digital infrastructures

 doi:10.20944/preprints202512.2449.v1

Communication

Impact of Quantum Computing on Asymmetric Cryptography Infrastructures: Prospective Study and Post-Quantum Transition Roadmap

João Lucas [1,*], Carlos Caleiro [1], António Goncalves [2] and Laercio Cruvinel [3]

[1] Instituto Superior Técnico (IST), Universidade de Lisboa, Av. Rovisco Pais 1, 1049-001 Lisboa, Portugal
[2] Instituto Universitário Militar (IUM) / Centro de Investigação Naval (Portuguese Naval Academy) (CINAV), 2810-001 Almada, Portugal
[3] Universidade Autónoma de Lisboa (UAL), Palácio Dos Condes Do Redondo, R. de Santa Marta 56, 1169-023 Lisboa, Portugal
* Correspondence: joao.m.lucas@tecnico.ulisboa.pt

Abstract

The evolution of quantum computing represents one of the most significant technological transforma- tions of this century, with direct implications for cryptographic systems currently in use, especially in the field of asymmetric cryptography. This article develops a prospective study on the impact of quantum computing on asymmetric cryptographic infrastructures, presenting the central problem and proposing the implementation of a structured solution in the form of a transition roadmap. This approach enables the anticipation of technological scenarios and the identification of appropriate miti- gation strategies, based on scientific evidence and expert projections. The results obtained highlight the vulnerability of classical cryptographic algorithms, based on complex mathematical problems, such as RSA and ECC, demonstrating that the technological and cryptographic transition is inevitable. However, this transition should not be exclusively algorithmic, it must integrate technical training policies, regulatory compliance, interoperability between hybrid systems, and continuous monitor- ing mechanisms. The proposed solution stands out from the others due to its methodological and operational approach, offering a dynamic, detailed, and adaptable model applicable to different organi- zational and sectoral contexts. The proposed roadmap is structured in sequential and interdependent phases, allowing for practical and strategic guidance of the transition process. The contributions of this research include the systematization of the phases of the post-quantum transition process, the introduction of a resilient and evolutionary model capable of responding to technological uncertainty, and the consolidation of an integrated approach that combines academic, scientific, organizational, and technical rigor. Planning and adopting a proactive stance are crucial factors in ensuring the operational continuity and resilience of digital infrastructures in a potential quantum era. The article therefore constitutes a relevant contribution to the academic debate on post-quantum information security, offering practical guidance and concepts applicable to the protection of digital infrastructures in the context of profound technological transformation.

Keywords: quantum computing; asymmetric cryptography; post-quantum transition; resilience of digital infrastructures

1. Introduction

The potential development of quantum computing has raised concerns in the scientific and technological community, as the foundations of digital security could be compromised.

 doi:10.20944/preprints202512.2449.v1

Quantum technology emerges as a paradigm that surpasses the limits of classical computing, thanks to its computational data processing capabilities, leveraging principles of quantum mechanics, which enables the execution of highly complex and high-speed parallel operations.

Asymmetric cryptography, which forms the basis of modern digital security and is based on highly complex mathematical problems, has proven, based on results obtained to date, to be potentially vulnerable to quantum algorithms, as is the case with the impact of Shor's algorithm on the RSA cryptographic system.

The potential vulnerabilities of asymmetric cryptography, in relation to quantum computing and its algorithms, have implications that extend far beyond the technical domain. Critical digital infrastructures are found in a wide range of sectors, from governments to businesses, which depend on encryption systems such as PKI (Public Key Infrastructure), authentication systems, and sensitive information protection systems such as MFA.

Faced with this problem, several international organizations, such as the National Institute of Standards and Technology (NIST), the EU (European Union), Canada (Cybersecurity Center), and the Post-Quantum Cryptography Coalition (PQCC), have been working to achieve an appropriate PQC transition.

This study fits within this framework, aiming to analyze a problem and a central question in detail and then present a proposed solution that addresses the central question.

The study's theoretical methodology allows for a connection between the theoretical approach to the quantum threat and the formulation of a practical, structural, and operational response.

1.1. Objectives

The main objective of this article is, first, to prospectively analyze the impact of quantum comput- ing on asymmetric digital infrastructures, identifying the problem and developing a central question associated with it, resulting from existing technological advances.

Second, it seeks to present a proposed solution that allows for the central question to be answered, promoting an adequate adaptation of quantum computing and its algorithms to digital infrastructures. Specifically, the study in question aims to:

- To introduce the theoretical concepts of quantum computing;
- To introduce asymmetric cryptography;
- Address the existing problem associated with quantum computing and cryptography, as well as the central issue arising from quantum algorithmic development;
- Present a proposed applied solution;
- Present the conclusions and limitations of the study;
- Promote a prospective methodological approach that allows for the anticipation of risk scenarios, combining academic rigor with practical applicability;
- Promote a prospective methodological approach that allows for the anticipation of risk scenarios, combining academic rigor with practical applicability;
- Contribute to the scientific advancement of information security by providing a conceptual and operational framework that supports decision-making in contexts of technological uncertainty;
- Contribute to the scientific debate regarding the post-quantum transition.

2. Theoretical Methodology of Work

The methodological decision regarding the literature review (theoretical methodology) that guides this article arises from the uncertainty regarding the progress of quantum computing, as an evolving scientific domain.

There is "*no clear demonstration yet that it is possible to develop quantum computers with the necessary size to be useful.*" [1]. Thus, a prospective review (technology foresight review) was adopted, complemented by elements of guided narrative review.

 doi:10.20944/preprints202512.2449.v1

Through this combination, it is possible to ensure a balance between the anticipation of possible scenarios and the narrative structuring that ensures the cohesion and consistency of the investigative path.

Prospective review is particularly appropriate in contexts where technological evolution may be accelerated, with high uncertainty regarding its development. Thus, it seeks to identify emerging signs of progress, as well as technological trends and potential disruptions that could impact the cryptographic paradigm.

On the other hand, the introduction of guided narrative review elements ensures greater thematic delimitation, with the narrative being constructed with a focus on the central research question, avoiding unnecessary distractions. In concrete terms, the methodological choice allows:

- Defining the most relevant thematic areas for study, ensuring that the study remains focused on fundamental aspects;
- Mapping adaptation and transition strategies for post-quantum algorithms (PQC);
- Building a prospective framework that is not limited to the current state of the art but seeks to provide strategic solutions.

This methodological choice is directly aligned with the objectives proposed in this study. Regard- ing the methodological evaluation criteria, to ensure rigor and scientific consistency, the following criteria are used:

- Relevance: Pertinence of the study;
- Applicability.

2.1. Eligibility Criteria

The eligibility criteria are defined in order to ensure the quality and transparency of the sources present in the theoretical basis of the study, through the specification of the inclusion and exclusion criteria of the literature review.

These criteria determine the studies and documents that are considered relevant for investigative analysis, with inclusion criteria being defined according to the following parameters:

- Thematic scope: Works directly related to quantum computing, asymmetric cryptography, PQC, information security and technological transition;
- Scientific nature of the study: Scientific articles, technical reports, institutional documents, books, and scientific conferences;
- Methodological relevance: Studies that present an empirical, prospective, analytical, or conceptual approach, with applicable contributions to risk analysis and the formulation of post-quantum transition strategies.

Regarding the exclusion criteria, publications that presented at least one of the following characteristics were excluded:

- Deviation from thematic scope: Studies unrelated to the research topic;
- Insufficient relevance: Publications that address the topic merely speculatively, without proven technical or scientific contributions;
- Content duplication: Repeated versions of content in different works.

2.2. Information Sources and Validation Mechanisms

The information sources for this study were selected to ensure comprehensiveness, currency, and scientific credibility. These sources were databases, academic repositories, and institutional portals of high recognition, ensuring the inclusion of the most relevant studies for the thematic area under analysis.

Therefore, the following databases (scientific and technical) were used ACM Digital Library, Collective Catalog of the University of Lisbon and IEEE Xplore Digital Library. Regarding source selection and validation mechanisms, they are based on three fundamental criteria:

 doi:10.20944/preprints202512.2449.v1

- Thematic relevance: Inclusion of studies and case studies related to the thematic area under study;
- Credibility and scientific review: Prioritization of information published by highly recognized bodies and institutions, such as NIST, IEEE and EU;
- Temporal relevance: Selection of documents and information that are preferably recent, avoiding the use of obsolete literature.

In order to guarantee the credibility of the information, the validation of the sources was carried out in different ways, in order to confirm the consistency of the contents.

2.3. Bias Considerations

Recognizing the prospective nature and the thematic area of the present study, the risk of bias is a reality, in terms of temporal bias and thematic bias, resulting from the existing technological uncertainty and the scope of the technological area in question.

In order to mitigate this risk, the interpretations were based on a technical basis and validation from various sources (previous subchapter), avoiding unverifiable speculative extrapolations.

Thus, the methods for assessing risk of bias were based on triangulation of recognized sources, critical analysis of evidence, and interpretation of studies. These mechanisms ensured that the results and conclusions were interpreted in a balanced and consistent manner.

3. Theoretical and Technical Background

Quantum computing consists of a computational model that differs from classical computing in its logical mode of operation and is based on the theoretical and practical applications of the properties of quantum mechanics and quantum physics in relation to computer science.

Research and development in quantum computing began in the 1950s, when scientists decided to apply the laws of quantum physics and quantum mechanics to computers. Quantum computing is based on three fundamental phenomena of quantum mechanics: quantum superposition, quantum entanglement, and quantum interference.

Quantum computers offer unprecedented computational capabilities and can perform exponentially faster calculations, solving complex mathematical problems that form the basis of protocols used in asymmetric cryptography, such as factoring large integers into prime numbers and discrete logarithms of elliptic curves.

These protocols emerged in the 1970s with the creation of DES, RSA, and the PKI public/private key model, evolving into AES and ECC for reasons of security and efficiency.

Although there are already demonstrations of breaking the aforementioned figures by quantum computers, it is important to note that they do not represent an immediate threat, but rather a potential future threat, with the improvement of quantum technology.

3.1. Asymmetric Cryptography

Asymmetric cryptography has as its main basis, the concept of a public key, which plays a fundamental role in the information security of digital infrastructures. It applies to a system of key pairs, where one key is considered the public key and the other the corresponding private key [2].

Key pairs are generated through cryptographic algorithms based on mathematically complex problems, defined as one-way functions. The cryptographic security of the public key depends on the private key, since the public key is publicly shared [3].

There are different types of public-key cryptosystems with different objectives, including digital signatures, DHKE [4], public-key encapsulation, and public-key cryptography. The robustness of asymmetric cryptography is based on the computational mathematical difficulty of solving certain problems, such as the large number factorization problem (2,048 bits) [5] and the discrete logarithm problem (associated with DHKE).

 doi:10.20944/preprints202512.2449.v1

This type of cryptography underpins several internet standards, such as SSH and PGP. Applications of asymmetric cryptography include several internet standards such as SSH, web server authentication with TLS, digital money, password-authenticated key agreements, email content authentication and masking with PGP or S/MIME, time services, and non-repudiation protocols.

An important aspect is ensuring that a given public key is authentic, proving that it belongs to the person or entity claiming it and has not been altered or replaced by third parties. PKI is a possible solution to be applied in this situation, being used for the certification of key pairs, where one or more entities, known as certification authorities, verify the authenticity.

3.2. History of Asymmetric Cryptography

During the initial phase of cryptography, two parties exchanged a key as a security method. This same key was used for both encryption and decryption and had to be kept absolutely secret.

In 1874, William Stanley Jevons, through his book *The Principles of Science* [6], considered it unlikely that any reader could know the numbers multiplied to produce the number *8616460799*. Indirectly, he analyzed the relationship between one-way functions and cryptography.

In 1996, mathematician Solomon W. Golomb considered that Jevons had anticipated the main characteristic of the public key, which is the basis of the RSA system, although he did not invent the concept [7].

In 1970, British cryptographer James H. Ellis, working at Government Communications Headquarters, conceived the possibility of implementing public-key cryptography [8], but did not know how to do it.

Back in 1973, his colleague, Clifford Cocks, implemented what became known as RSA. Because computing power was quite limited at the time, these new systems could not be implemented on a large scale.

Only after the design of the open internet architecture, associated with Berners-Lee, did public-key cryptography reach its full potential.

3.3. Asymmetric Cryptography - RSA

Created in 1978 by three MIT researchers, namely Ronald Rivest, Adi Shamir, and Leonard Adleman [9], RSA has become one of the most widely used cryptographic systems in the world. This system is based on a key relationship (public/private). Among these keys, the following dependencies exist:

- Information encoded with the public key can only be read with the corresponding private key;
- Information encoded with the private key can only be read with the public key;
- There is no obvious relationship between the two, in the sense that it is possible to discover the private key in polynomial time from the public key.

Due to the high computational cost of the processes inherent in this type of information encoding/decoding, this type of scheme is normally used in conjunction with asymmetric cryptography.

3.4. Symmetric Cryptography and Asymmetric Cryptography

Before the 1970s, all cryptographic systems used symmetric key algorithms, where the same key was used by both the sender and the receiver.

To exchange the key, a secure channel known to all communicating parties had to be used. This process proved outdated and uncontrollable as the number of participants increased, in situations where secure channels were unavailable, or when keys were frequently changed.

In contrast, in an asymmetric cryptosystem, public keys could be publicly disseminated, since only the corresponding private keys needed to be protected.

 doi:10.20944/preprints202512.2449.v1

3.5. Weaknesses of Asymmetric Cryptography

As with all technological systems, asymmetric cryptography has vulnerabilities. The wrong choice of asymmetric key algorithm (few are considered satisfactory), short key length, and the possibility of private key discovery are some of the risks associated with asymmetric cryptography.

Due to these risks, all the security associated with information can be lost. With the advent of quantum computing, several asymmetric algorithms may be more vulnerable to attacks (the subject area of this study).

In addition to the weaknesses mentioned, some studies observe risks regarding the provision of the private key to third parties. Research on the implementation of PKI by Uruguay found that centralized custody by TSPs could weaken the principle of private key secrecy, increasing the exposure of the key system to attacks such as MITM and raising concerns about legal non-repudiation [10].

3.6. Public Key Infrastructure (PKI)

Although already mentioned, public key infrastructure is an approach that prevents cyberattacks. A certificate authority, which issues the certificate of compliance, must properly verify the identity of the sender and receiver.

Web browsers, for example, are provided with a long list of self-signed identity certificates from PKI providers and certificates from potential communicators. Public key infrastructure is widely used, including examples such as TLS and SSL, providing security for transactions occurring in the web browser (most websites use TLS for HTTPS).

It is important to note that public key digital certificates are typically valid for several years at a time, and therefore the associated private keys must be kept secure during that period. When a private key used to create certificates related to the PKI server is compromised or accidentally disclosed, attacks such as *man-in-the-middle* become possible, making a given certificate insecure.

3.7. Quantum Computing and Cryptanalytic Implications

Quantum computing emerged in the 1980s, based on new paradigms associated with computational power and information transmission. Both have the potential to revolutionize the most diverse areas of society.

Currently, with the imminent realization of quantum technologies on a large scale, there is massive interest from various organizations worldwide, with particular attention from large multinational technology companies, investing heavily in specialized personnel capable of handling the new methods and techniques involved.

3.8. Quantum Entanglement

Entanglement is one of the main concepts of quantum computing, being the most mysterious and powerful phenomenon in quantum mechanics, where two or more qubits are somehow interconnected to the point that they cannot be correctly described without each other, even if they are separated.

No matter how far apart they are, if we measure the state of one qubit, we will instantly know the state of the other. In the context of computing, this is a crucial feature, allowing complex correlations between qubits, and is essential in quantum algorithms.

It is "*precisely the mysterious phenomenon of entanglement that underlies the development of quantum computing. The idea is that it should be possible to manipulate a set of entangled particles so that they perform, in parallel, an exponentially large number of calculations.*" [1].

This concept is at the heart of the disparity between classical physics and quantum physics, being a fundamental characteristic [11]. Although measurements of physical properties, such as polarization, momentum, and position, may show perfect correlation, paradoxical effects are

 doi:10.20944/preprints202512.2449.v1

generated, resulting in an apparent and irreversible collapse of a particle's wave function, altering its original quantum state. Such measures could affect the system.

Quantum entanglement was the subject of a significant scientific paper in 1935, which described what became known as the EPR paradox [12], in which it was considered that there was a violation of the realism of causality, arguing that the accepted formulation, referring to quantum mechanics, should therefore be incomplete.

Later, it was discovered that the correlations produced by quantum entanglement cannot be explained by the properties inherent in the individual particles themselves. Scientific articles related to Erwin Schrödinger's short theory [13] were also quite relevant to the development of this thematic area.

The demonstration of this quantum phenomenon has already been carried out by Griffith Univer- sity, using a technique that allows the division of a single photon between two laboratories, verifying whether one part altered the state of the other [14].

3.9. Quantum Interference

Just as light and sound waves can be associated with the interference process, the same happens with quantum states, where this phenomenon can be exhibited.

Quantum algorithms, as a rule, are designed to manipulate the phase of superimposed states, so that computational paths leading to incorrect answers suffer interference and are canceled out. On the other hand, paths leading to the correct answer should suffer interference, to the point of being amplified. It is important to note that, in the calculation, the measure used has a high probability of collapsing to the state that represents the correct solution.

3.10. Quantum Circuits

Just as in classical computing, quantum computing uses circuits to describe a sequence of operations. A quantum circuit is simply a computational model that describes a (quantum) algorithm step by step. The components of a quantum circuit diagram are:

- Input: The input qubits are in an initial state, usually $|0\rangle$ for each qubit. The combined state of multiple qubits is mathematically described by their tensor product;
- Horizontal lines: Each line represents the temporal evolution level of a single qubit.
- These are not necessarily made of wires, and may simply represent a passage process for a trapped ion or the spatial displacement of a photon;
- Direction: The circuit is read from left to right, describing the evolution of the quantum system in relation to time;
- Quantum gates: Blocks of lines that represent unitary operations applied to the qubits;
- Vertical lines: Vertical segment connecting multiple lines of qubits, as happens in a CNOT gate, where it acts simultaneously on these qubits. The vertical line represents the synchronization of the operation, but not the transmission of information;
- Control: In a controlled gate, such as CNOT, a solid point on a line indicates that the qubit represented on that line is a control qubit. If in state $|1\rangle$, the gate performs the operation on the target qubit. If in state $|0\rangle$, the gate performs no operation. If the control qubit is in a superposition state or if two qubits are entangled, it will not be possible to understand the individual behavior of the control qubit and the target qubit. One must always consider simultaneously the unitary operator, which represents the entire circuit, acting simultaneously on the combined state of the qubits;
- Output: At the end of the circuit, the qubits that make up the output can be measured. The measurement collapses the superposition of each qubit to a classic result of 0 or 1.

 doi:10.20944/preprints202512.2449.v1

3.11. Quantum Algorithms

The process for finding quantum algorithms is usually based on the quantum circuit model. Certain quantum algorithms could be roughly categorized by the amount of increase in processing speed achieved. Regarding the fundamental pillars of quantum algorithms, these are:

- Quantum Fourier Transform: This is a quantum analog based on the classical discrete Fourier transform and is fundamental in algorithms such as Shor's algorithm. This pillar performs transformations of data encoded in amplitudes of quantum states for a given frequency space, being an example of how certain linear transformations can be performed in an exponentially more evolved way;
- Amplitude Amplification: A general technique, applicable in quantum algorithms such as Grover's algorithm. It is used to increase the probability of measuring one or more states corresponding to the solution of a given problem. It works iteratively, rotating the state vector towards the desired state;
- Quantum Interference: As previously discussed, quantum interference works in conjunction with amplitude amplification, being a fundamental mechanism for quantum algorithms to function. The operations are carefully orchestrated so that unwanted states cancel each other out through destructive interference, while the solution state is reinforced by constructive interference, leaving it as the most probable result in the final measurement;
- Hamiltonian Simulation: Inspired by Feynman's original idea, it involves using a quantum computer to simulate the evolution of another quantum system. This is done by mapping the Hamiltonian (an operator that describes the total energy) of the system to be simulated onto a sequence of quantum logic gates;
- Heisenberg's Uncertainty Principle: Quantum mechanics is fundamentally probabilistic. The outputs of the algorithms will not return a single, determined result, but rather a probability distribution in relation to the possible outcomes. By running the algorithms multiple times, the statistics of the results will be analyzed to infer the solution.

3.12. Shor's Algorithm

Among the main quantum algorithms, proven to be effective, the Shor Algorithm stands out, due to its usefulness and way of working. This was developed in the 1990s by mathematician Peter Shor and presented in the article Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [15], showing practical evidence of polynomial acceleration.

Still on quantum algorithms, due to the potential applicability of Shor's algorithm, "*(...) the quantum paradigm implies that essentially all implemented public key cryptography will be completely broken by a quantum computer and that brute force attacks on symmetric ciphers can also be accelerated by approximately a quadratic factor.*" [5].

3.13. Post-Quantum Cryptography (PQC)

With the potential impact of quantum computing on current cryptographic systems, post-quantum cryptography emerges as a solution, containing a set of options based on alternative mathematical problems, different from those employed in asymmetric cryptography, these being:

- Lattice-based cryptography: Construction of cryptographic primitives involving lattices. This type of construction has proven resilient in both classical and modern computing. In 2024, NIST announced the Module-Lattice-Based Digital Signature Standard referring to PQC;
- Code-based cryptography: Code-based cryptography, which allows the construction of quantum- resistant public-key cryptographic systems. This process involves the use of error correctors to protect data, based on the difficulty of decoding random linear codes. The McEliece cryptosystem [16] is widely regarded in this context for its properties, although its application results in high- dimensional keys;

 doi:10.20944/preprints202512.2449.v1

- Hash-based cryptography: Construction of cryptographic primitives based on hash functions, applying to the construction of digital signatures, with proof of computational integrity [17] and proofs of reach of issued credentials (HashWires protocol) [18]. In public key authentication environments, cryptographic keys are unbreakable, if the hash function is not broken at the time, it is established;
- Multivariate cryptography: Asymmetric cryptographic primitives based on multivariate polyno- mials. This cryptographic concept has been widely used in the field of cryptanalysis [19] often linked to the theory of NP-completeness.

3.14. Post-Quantum Cryptography Algorithms

There are several initiatives underway that seek to implement post-quantum cryptography, culminating in an evaluation and selection process that began in 2016. Of these, three PQC standards stand out, in which the algorithms in question are as follows:

- ML-KEM;
- CRYSTALS-Dilithium (or ML-DAS);
- Sphincs+ (or SLH-DAS).

ML-KEM focuses on the secure exchange of keys between two entities over public communication channels. Its original name is CRYSTALS-Kyber, and it was standardized by NIST as FIPS 203, making it resistant to quantum computers.

ML-DSA has applications in post-quantum digital signatures and has been standardized by NIST under the FIPS 204 standard. It was developed from CRYSTALS-Dilithium and seeks to replace RSA and ECDSA using lattice-based mathematical problems, offering different levels of security (ML-DSA-44, ML-DSA-65 and ML-DSA-87).

SLH-DAS, also known as Sphincs+, can be used primarily for integrity (hashing) functions. It consists of a digital signature scheme based on cryptographic hash functions, providing security against quantum computing attacks.

One of its main features is that it doesn't have a sender to track which private keys were used. Instead, a unique signature key tree is constructed, based on randomization to select the key to be used for each signature. Companies like Google and Microsoft have already begun adopting these protocols in their products.

3.15. Comparative Analysis of PQC Algorithms

Among the post-quantum algorithms mentioned (ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DAS), namely by NIST, structural, functional and operational differences are observed, which reflect the diversity of cryptographic approaches, in response to possible quantum threats.

ML-KEM and ML-DAS constitute preferred solutions for an operational and institutional transition, being widely applicable in network, authentication and communication protocols.

SLH-DAS is more conservative in terms of digital security, although it presents inferior performance when compared to ML-KEM or ML-DAS, due to the larger signature size and greater computational demand.

Still, its purely hash-based nature makes it a reliable and resilient option, particularly suited to long-term integrity and authentication applications where performance is not a critical factor.

Thus, the coexistence of these algorithms, with distinct characteristics and purposes, reflects the need for a hybrid and adaptive cryptographic approach, based on resilience and continuity, in the face of the inevitable progression of quantum computing.

4. Problem Statement and Central Question

The transition to Post-Quantum Cryptography (PQC) is driven by an operational problem that is fundamentally time-asymmetric: sensitive data and trust relationships protected today may be compromised retroactively once quantum capabilities reach a cryptographically relevant threshold.

 doi:10.20944/preprints202512.2449.v1

This risk is amplified by the fact that public-key cryptography is not deployed in isolation; it is embedded in Public Key Infrastructure (PKI) ecosystems (certificates, trust anchors, key lifecycles, protocol stacks, hardware modules, and third-party dependencies), where change is slow, coordinated, and operationally constrained.

4.1. Problem Statement

Due to the uncertainty regarding the development of quantum computing, the central question is associated with a problem, verifying its relevance and potential impact, based on three fundamental questions (Mosca's theorem) [5]:

- "*How long have the cryptographic keys remained secure, containing this personal, health, professional, business, and national security information?*". The value of X represents this value;
- "*How long will it take to implement quantum security tools?*". There may be a simple automatic implementation that replaces a fully controlled system, or we may have an encryption method that needs to be adapted to a restricted environment. The value of Y represents that period of time;
- "*How long will it take for a quantum computer to break the encryption systems currently used?*". *Z*represents this metric.

The operational risk emerges when the required confidentiality horizon plus the organisational migration lead time exceeds the estimated time-to-capability:

If $X + Y > Z$, then the organisation faces material risk, because data protected today may become decryptable (or signatures forgeable) before migration is completed.

According to Post-Quantum World, a possible decline in RSA (2048 bits) is estimated, with a percentage probability of 14.28%, by 2026, and 50%, by 2031 [20].

4.2. Central Question

This article largely addresses a central question associated with the aforementioned problem. This question then emerges as a synthesis of the identified problem and is based on the conceptual framework of the thematic area.

The question's formulation also reflects existing concerns regarding the potential vulnerabilities of digital infrastructures in the face of the advance of quantum computing. Thus, the central question defined is the following:

> *How could the evolution of quantum computing compromise the security of asymmetric cryptography, and what strategy could be adopted to ensure a safe and resilient transition to the post-quantum era?*

The central question plays a structuring role, guiding the entire theoretical foundation of the study. Its relevance goes beyond the scientific dimension, as it has organizational, economic, and social implications, given that the breach of asymmetric cryptography could jeopardize existing infrastructure in key sectors such as healthcare, defense, banking, and telecommunications. The definition of the issue arises from two complementary dimensions:

- Prospective dimension: Assessment of the impact of quantum computing on digital infrastruc- tures (asymmetric cryptography), envisioning possible temporal scenarios;
- Technical dimension: Preparation of a technical plan of measures and solutions that can be applied, to guarantee adequate risk mitigation and a gradual transition.

5. Proposed Solution: A Five-Phase Transition Roadmap

The proposed solution consists of the presentation of a post-quantum transition roadmap, supported by the knowledge acquired throughout the research process, aiming to support the migration process.

 doi:10.20944/preprints202512.2449.v1

The aim of this presentation is to ensure that it is applicable globally to different organizational and institutional contexts. It is important to distinguish experimental efforts that aim to achieve large-scale quantum computing from those that seek to capture the computational power of quantum mechanics and quantum physics while ignoring the steps necessary to achieve a scalable, fault-tolerant design.

With the materialization of the proposed solution, related to the construction of a strategic roadmap, this is divided into five phases, reflecting the inherent importance and complexity, these being the following phases:

5.1. Phase 1 - Initial Process and Awareness Raising

- Raising awareness of the risks of quantum computing;
- Inventory of assets and infrastructure that rely on asymmetric encryption technology processes.

5.2. Phase 2 - Assessment, Training, and Alignment

- Formation of teams specialized in implementing post-quantum cryptography;
- Performance and interoperability assessment of hybrid systems;
- General alignment and training.

5.3. Phase 3: Transition and Integration

- Gradual replacement of infrastructure, prioritizing critical infrastructure;
- Adopting hybrid architectures;
- Performing performance, compatibility, and security tests;
- Validing PQC protocols in strategic sectors.

5.4. Phase 4: Widespread Implementation and Standardization

- Global implementation of PQC algorithms;
- Implementation and standardization of strategic policies;
- Dissemination of applicable technical roadmaps.

5.5. Phase 5: Consolidation, Monitoring, and Continuous Resilience

- Search for mechanisms for continuous updating of algorithmic processes;
- Preparation of contingency plans;
- Ongoing review of legal requirements that depend on cryptography;
- Continuous monitoring of implemented algorithms;
- Continuation of the investigative process.

5.6. Roadmap Summary

Table 1. Post-Quantum Transition Roadmap: Phases.

Phase	
1.	Initial Process and Awareness Raising
2.	Assessment, Training, and Alignment
3.	Transition and Integration
4.	Widespread Implementation and Standardization
5.	Consolidation, Monitoring, and Continuous Resilience

 doi:10.20944/preprints202512.2449.v1

6. Application Perspective in Critical Sectors

6.1. Healthcare Sector

The healthcare sector is one of the most sensitive areas in the context of the quantum transition, given the highly confidential nature of clinical, genetic and biomedical data circulating between medical institutions, insurers and government entities.

With sectoral application, the continuity and confidentiality of medical services are guaranteed, as well as compliance with standards and guidelines of international organizations, namely the European Health Data Space.

Currently, computational data security is ensured by PKI infrastructures and TLS, HTTPS and VPN protocols.

6.2. Financial Sector

The financial sector is considered one of the most sensitive sectors in the context of the quantum threat, due to its dependence on authentication and digital signature systems, based on asymmetric cryptography, which are fundamental in processes such as electronic transactions, blockchain, payment systems and bank authentication.

By implementing the proposed solution, a structured transition can be ensured, ensuring the resilience of the economic ecosystem in the face of emerging threats from the quantum era.

7. Operationalization of the Proposed Solution

Operationalizing the proposed solution is an essential process, moving from a theoretical context to practical application, and is fundamental to the credibility of the study.

The operational examples presented demonstrate that the PQC transition is not a singular event, but a complex sequence of interconnected measures. Pilot projects are necessary to ensure a valid approach, in line with the imminent costs related to the quantum challenge.

7.1. Operationalization of the Proposed Solution in the Healthcare Sector

The healthcare sector is fundamentally characterized by the need to guarantee the confidentiality and longevity of medical data, since clinical information, such as genetic data, must remain protected for a long period of time.

Thus, by delving deeper into concrete examples that demonstrate the operationalization of the quantum transition proposal in this sector, operational measures should be implemented, such as:

- Launching comprehensive audits aimed at identifying all TLS certificates and all digital signatures with a validity period exceeding five years;
- Certificates of compliance with a validity that exceeds the projected horizon for the quantum threat should be marked;
- Use of QC frameworks, creating simulated clinical data testing environments that simulate the time required to break asymmetric cryptographic systems;
- Implementation of pilot projects for VPN connection and remote access, where DHKE is replaced by hybrid encapsulation ECC + ML-KEM;
- Use of the hybrid encryption protocol, selected as a mandatory standard for all new confidential data flows.

7.2. Operationalization of the Proposed Solution in the Financial Sector

The financial sector operates based on high operational resilience, using regulations such as DORA [21] or NIS2 [22] and relying on the integrity of digital signatures for high-level transactions. Its operation focuses on minimizing latency during cryptographic transformation.

Thus, by delving deeper into concrete examples that demonstrate the operationalization of the quantum transition proposal in this sector, operational measures should be implemented, such as:

 doi:10.20944/preprints202512.2449.v1

- Conducting audits on all systems using ECDSA, focusing on interbank transaction protocols and customer authentication mechanisms;
- Inventory of assets, according to their vulnerability exposure and operational frequency;
- Creation of dedicated areas for performance overload testing hybrid systems on high-frequency platforms and payment gateways. The two main metrics should be transaction latency and the increase in signature key size when migrating from ECDSA to a hybrid system (ECDSA + ML-DSA);
- Implementation of pilot projects related to interbank communications, signed by hybrid algo- rithms. This approach ensures that transactions remain valid while offering protection against future quantum breakdowns;
- Implementation of internal mandates that explicitly integrate the use of hybrid cryptography into industry compliance frameworks, including NIST FIPS standards, as a minimum requirement.

8. Formal Review Protocol

Although this study adopts a prospective review (technology foresight review) complemented by elements of guided narrative, it seeks to ensure the transparency and reproducibility of the information contained herein.

The formal review protocol defines the procedures and methods used, preventing the introduction of study bias. A predefined protocol ensures the objectives, search strategy, and selection criteria are defined a priori.

8.1. Queries and Search Terms

Regarding the consultations, these are combined with three thematic axes in order to ensure the traceability, reproducibility, and transparency of the study, which are as follows:

- Quantum computing/Quantum cryptography;
- Asymmetric cryptography/Public key infrastructure/RSA/ECC;
- Post-Quantum/PQC/Transition roadmap/Migration strategy.

8.2. Filters and Dates

The research was conducted between September and December 2025. References from 2016 to the present date were prioritized, except for fundamental works, such as the scientific article by Peter Shor (1997).

Only references with academic and scientific recognition, whose documentation was in English or Portuguese, were selected.

8.3. Qualitative Nature of the Synthesis

To clarify, explicitly, the qualitative nature of the synthesis, it is important to note that the results obtained in the review are not aimed at statistical analysis, but rather at qualitative and prospective synthesis.

The qualitative nature of the synthesis aims at conceptual consolidation and the identification of existing gaps, allowing the construction of a model and the comparison of the developed cryptographic transition proposal with other existing ones.

The prospective approach aims at the analysis of data and projections, justifying the formulation of future scenarios and relying on time horizons and technological milestones.

 doi:10.20944/preprints202512.2449.v1

9. Conclusions and Limitations

9.1. Response to the Study's Central Question

Answering the central question under study, "*How could the evolution of quantum computing compromise the security of asymmetric cryptography, and what strategy could be adopted to ensure a safe and resilient transition to the post-quantum era?*", associated with the existing problem, through the development of a proposed solution, asymmetric cryptography will be (prospectively) compromised, since the mathematical problems that support it will be solved by quantum computing, as seen in the case of Shor's algorithm in relation to RSA (large number factorization).

Regarding the second aspect of the central issue, the implementation of the proposed roadmap should be adopted as a strategy to ensure a safe and resilient transition to the post-quantum era, allowing for an adequate transition without high associated risks.

9.2. General Research Conclusions

This work was developed based on the identification of an emerging problem. In this sense, a central question was outlined, serving as a guideline for the work carried out.

The study's theoretical foundation was initially established using a methodology based on a prospective review (technology foresight review), complemented by elements of a guided narrative review.

This methodological approach enabled, in addition to a state-of-the-art analysis, the projection of trends and the identification of relevant gaps.

Subsequently, a proposed solution was developed, embodied in the construction of a roadmap, contributing technically, scientifically, organizationally, and temporally. The research process reaffirmed the following initially defined objectives:

- Prospective analysis of the impact of quantum computing on asymmetric cryptography;
- Direct contribution to the scientific and organizational debate, providing practical guidance to support the transition of digital infrastructures to the quantum era.

9.3. Limitations of the Study and Research

Given the insufficient computational capacity for the widespread application of quantum algorithms in large-scale cryptanalytic operations, a limitation is found that conditions the present study, not deriving from the theoretical foundation or valid references, but from the impossibility of fully proving the usefulness of the area in question.

Quantum computing is currently in the *Noisy Intermediate-Scale Quantum* (NISQ) phase. This requires the development of higher-capacity quantum processors and a larger storage capacity for qubits, given that most qubits are lost due to circumstances such as thermal fluctuations, radiation, or electromagnetism.

Quantum Error Correction (QEC) aims to combat this fact, being able to reduce the effects of noise on stored quantum information. In this way, a quantum correction would allow low-fidelity quantum computers to execute high-complexity or circuit-depth algorithms [23].

The interconnection between qubits, the standardization of their development and noise control are considered the main barriers to the expansion of quantum computing technology. There remains, therefore, a high level of skepticism regarding the practical and widespread development of this scope of study.

According to Professor Arlindo Oliveira, "*(...) there is still no clear demonstration that it is possible to develop quantum computers with the necessary size to be useful.*" [1].

Thus, this research adopted a prospective approach, focusing on exploring scenarios related to the post-quantum transition, supported by scientific evidence and technological projections.

The decision to develop a dynamic and flexible roadmap stems precisely from the uncertainty surrounding the progress of quantum computing, as it depends on variables that cannot be directly controlled.

 doi:10.20944/preprints202512.2449.v1

9.4. Reflective Closure

Although there is uncertainty regarding the development of quantum computing, the evidence presented so far in this study indicates that organizations should prepare for a possible technological change, so that the transition is carried out progressively.

Thus, through this article, we seek to strengthen the adoption of a proactive and prospective stance, ensuring the robustness of digital infrastructures in scenarios of technological uncertainty.

Funding: This research received no external funding.

Acknowledgments: The authors acknowledge the support of Instituto Superior Técnico and the academic supervision provided within the master's programme context.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Oliveira, A. Estratégia europeia para as tecnologias quânticas: visão ou FOMO? *PÚBLICO* **2025**.
2. Bernstein, D., L.T. Post-Quantum cryptography. *Nature* **2017**, *549*, 188–194. https://doi.org/10.1038/nature23461.
3. Stallings, W. Cryptography and Network Security: Principles and Practice. *Prentice Hall* **1990**, p. 165.
4. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory* **1976**, *22(6)*, 644–654. https://doi.org/10.1109/tit.1976.1055638.
5. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE, Security Privacy* **2018**, *16(5)*, 38–41. https://doi.org/10.1109/msp.2018.3761723.
6. Jevons, W.S. The Principles of Science: A Treatise on Logic and Scientific Method. *Macmillan Co* **1874**, p. 141.
7. Golomb, S.W. On Factoring Jevons' Number. *Cryptologia* **1996**, *20(3)*, 243–246. https://doi.org/10.1080/0161-119691884933.
8. Ellis, J.H. The Possibility of Secure Non-secret Digital Encryption. *CryptoCellar* **1970**.
9. Rivest, R. L., S.A..A.L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Mas- sachusetts Institute of Technology* **1978**.
10. A. Sabiguero, A.V.; Esnal, G. Let There Be Trust. *IEEE URUCON* **2024**, pp. 1–5. https://doi.org/10.1109% 2FURUCON63440.2024.10850093.
11. Horodecki, R., H.P.H.M..H.K. Quantum entanglement. *Reviews of Modern Physics* **2007**, *81(2)*, 865–942. https://doi.org/10.1103/revmodphys.81.865.
12. Einstein, A., P.B..R.N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review* **1935**, *47(10)*, 777–780. https://doi.org/10.1103/physrev.47.777.
13. Schrödinger, E. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society* **1936**, *32(3)*, 446–452. https://doi.org/10.1017/S0305004100019137.
14. Fuwa, Maria; Takeda, S.Z.M.W.H.M.F.A. Experimental proof of nonlocal wavefunction collapse for a single particle using homodyne measurements. *Nature Communications* **2015**. https://doi.org/10.1038/ncomms7 665.
15. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing, Quantum Physics, SIAM* **1997**, *26*. https://doi.org/10.1137/s0097539 795293172.
16. of Electrical, I.; Engineers, E. Code-Based Cryptography: state of the art and perspectives, 2017.
17. Ben-Sasson, E.; Bentov, I.; Horesh, Y.; Riabzev, M. Scalable, transparent, and post-quantum secure computa- tional integrity. *Cryptology Archive* **2018**, *2018/046*.
18. Chalkias, Konstantinos; Cohen, S.L.K.M.F.R.Y. HashWires: Hyperefficient Credential-Based Range Proofs. *Privacy Enhancing Technologies Symposium* **2021**.
19. Garey, Michael R., J.D.S. Computers and intractability: a guide to the theory of NP-completeness. *San Francisco: W.H. Freeman* **1979**.
20. of Standards, N.I.; Technology. NIST Workshop on Cybersecurity in a Post-Quantum World, 2015.

 doi:10.20944/preprints202512.2449.v1

21. Digital Operational Resilience Act. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), 2022.
22. European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), 2022.
23. W. Cai, Y. Ma, W.W.C.L.Z.L.S. Bosonic quantum error correction codes in superconducting quantum circuits. *Fundamental Research* **2020**. https://doi.org/10.1016/j.fmre.2020.12.006.