UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingenieros Informáticos

Quantum Cryptographic Primitives

D O C T O R A L T H E S I S

Submitted for the degree of Doctor by:

Marta Irene García Cid
Master Degree in Chemical Science and Technology

Madrid, 2024


UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingenieros Informáticos

Doctoral Degree in Software, Systems and Computing

Quantum Cryptographic Primitives

D O C T O R A L T H E S I S

Submitted for the degree of Doctor by:

Marta Irene García Cid
Master Degree in Chemical Science and Technology

Under the supervision of:
Dr. Vicente Martín Ayuso
Dra. Laura Ortiz Martín

Madrid, 2024

Title: Quantum Cryptographic Primitives

Author: Marta Irene García Cid

Doctoral Programme: Software, Systems and Computing

Thesis Supervision:

Dr. Vicente Martín Ayuso, Professor, Universidad Politéctica de Madrid (Supervisor)

Dra. Laura Ortiz Martín, Assistant Professor, Universidad Politéctica de Madrid

External Reviewers:

Thesis Defense Committee:

Thesis Defense Date:

This thesis has received funds from Indra Sistemas S.A.; EIT Digital co-funded by the European Institute of Innovation and Technology (EIT), a body of the European Union; EuroQCI Spain project supported by the European Commission through the Europe Digital program, under the grant number DIGITAL-2021-QCI-01-DEPLOY-NATIONAL; and PQREACT project supported by the European Union's Horizon Europe research and innovation programme under grant agreement N° 101119547.

A la abuela Cristina

Acknowledgement

Son muchas las personas a las que tengo que agradecer por estos años en los que me han formado, guiado y apoyado. En primer lugar, agradecer a mis directores de tesis Vicente y Laura que, sin conocerme me aceptaron en el grupo de investigación con los brazos abiertos y con los que he aprendido a investigar. Me han ido abriendo las puertas al mundo de las comunicaciones cuánticas y la criptografía, y me han apoyado y aconsejado en cada decisión. Agradecer a Indra, concretamente a Isabel, que me dio la oportunidad de proponer un doctorado industrial sobre una tema que en su momento conllevaba mucha incertidumbre. Aún así se arriesgó y me apoyó. A Sebas quien me acompañó a la primera reunión con el que, más tarde, iba a ser mi director de tesis. Él junto con Jorge Maestre, han sido los que más me animaron para empezar esta aventura. Agradecer a Jorge Manzanares que siempre ha estado disponible para ayudar en lo que necesitara. Gracias a David y a Paco, el primero por la guía científica y técnica, y el segundo por la guía en desarrollo de negocio, que han críticos en los ultimos años de la tesis. Aunque ya no forme parte de la empresa, tengo que agradecer a Raquel porque sin ella esta tesis se habría ahogado en un mar de burocracia y no habría salido adelante. Por supuesto, agradecer a mis compañeros de trabajo que hacen cada día ameno y que siempre están dispuestos a ayudar. Para que una tesis de estas características haya podido salir adelante ha sido tan importante la direccion científica como el apoyo familiar. Por eso, en lo personal quiero agradecer a mis padres por su apoyo constante, por animarme cuando no me veía capaz y por aconsejarme sabiamente como siempre hacen. A mis hermanos Alex, Álvaro y Sophie, porque sin saberlo me alegran los días malos cuando nos juntamos. A Óscar porque me ha sufrido en todo el proceso, y aun así ha sido mi alegría diaria. Y a la abuela Cristina, Doctora en Química por la Universidad Complutense de Madrid, que ha sido mi inspiración, mi guía y mi ejemplo a seguir en todo momento. Por último quiero agradecer a un grupo heterogéneo de personas, todos ellos amigos, que ya sea en largos viajes, excursiones por la montaña o sesiones de cotilleos, me han ayudado a desconectar y a centrarme: Margarita, Patri, Ani, Sergio, Jaime, Roberto, Rodri, Dileep, Javier, Aurora y Pati. Para terminar quiero dejar una reflexión personal. La vida se compone de buenos y malos momentos. No sabemos que estamos en un buen momento hasta que llega lo malo. Es ahí cuando nos entristecemos, agobiamos, confundimos y no vemos la luz al final del túnel. Sin embargo, si logramos tener fe, paciencia, seguimos trabajando y nos apoyamos en buenas personas, es de esos malos momentos de los que más aprendemos y en los que más maduramos.

Abstract

The main motivation of this thesis is the uncertain panorama of cybersecurity risks and threats, accentuated by the arrival of the quantum computer. This type of computer is completely disruptive, since its operation is governed by quantum mechanical phenomena. The implementation of Shor's algorithm in a quantum computer with relevant size and performance will allow breaking the security of the most currently used pre-quantum asymmetric algorithms. This panorama makes it necessary to research new cryptographic paradigms that are resistant to quantum threats. Thus, quantum and post-quantum cryptography emerge. Several national security agencies are recommending the immediate migration to quantum-resistant solutions of vulnerable critical cryptosystems, mainly by implementing post-quantum algorithms, some of them recently standardized.

PQC bases its security on the difficulty of solving mathematical problems, just like conventional pre-quantum algorithms. In the different rounds of the NIST competition, PQC algorithms have been discarded, even discovering critical vulnerabilities in some algorithms that had managed to reach advanced rounds. The main algorithms selected to be standardized (CRYSTALS-KYBER as a key encapsulation mechanism and CRYSTALS-Dilithium as a digital signature algorithm) are based on learning-with-error problems, so finding a vulnerability to this problem would put at risk the PQC solutions chosen for the migration of current cryptosystems. For its part, quantum cryptography bases its security on the same physical foundations as quantum computers, being independent of the computational capacity of an adversary. The implementation of solutions based on quantum cryptography still requires greater technological maturity, development of standards and certification of devices. In addition, the infrastructures necessary for these networks are expensive and difficult to scale, in their current conception, due to the need to have trusted intermediate nodes. However, the rapid advances in this field allow to further research quantum communications networks to be a reality for daily operations where a high level of security is required.

The main objective of this thesis is to **investigate quantum cryptography-based solutions that go beyond quantum key distribution (QKD)**. The thesis has focused on proposing two novel cryptographic mechanisms ensuring that the new protocols are comparable in efficiency with pre-quantum and post-quantum algorithms. Furthermore, it has been taken into account that these protocols are implementable in current quantum communications infrastructures (QCI) to maximize the technical benefit of the investments carried out for these deployments.

As a result, **a quantum-assisted digital signature protocol (Q-DS) and a quantum zero-knowledge proof (QZKP) have been proposed, analyzed and implemented**, which combine symmetric pre-quantum mechanisms with QKD.

The proposed quantum-assisted digital signature protocol avoids the use of vulnerable pre-quantum public-key cryptosystems, using symmetric keys generated by QKD and using them with widely known NIST-approved hash functions, giving rise to a composite cryptosystem whose security against various attacks is demonstrated. This composite approach allows signing messages of arbitrary length with efficient signature generation and verification processes,

in some cases over-performing pre-quantum DSA and the most efficient post-quantum DSA *CRYSTALS-Dilithium*.

For its part, the proposed quantum zero-knowledge proof allows the authentication of users in a QCI without revealing personal information during the process. The proposal of a quantum version of ZKP has been done in this thesis for the very first time, without precedent in the literature. The QZKP is a step further to fully exploit the advantages of a QCI to guarantee an end-to-end security of communications by using the same physical infrastructure than QKD and Q-DS, optimizing the resources allocated in the deployment of these networks and the development of quantum cryptographic devices. A theoretical study as well as experimental tests have been carried out, resulting in a secure and efficient authentication mechanism.

Finally, given the industrial nature of this thesis, the evolution of the political panorama regarding quantum technologies and PQC have been closely followed, including the positions of relevant security-oriented organizations and economic investments for project funding. In order to promote research in quantum cryptography in a coherent manner, not only investments for the development of technologies and proofs of concept are required, but also international coordination to optimize the available funding. Recently, the EuroQCI programme has been launched for the deployment of QCI in Europe, with the aim of having in the future an integrated European network with terrestrial links based on optical fibre, as well as, satellite links. These advances, added to the development of quantum repeaters and quantum memories, will provide a step forward towards the future Quantum Internet. These issues, although not technical, have influenced the design of the cryptographic protocols proposed in this thesis.

Resumen

La motivación principal de esta tesis es el panorama incierto de los riesgos y amenazas de ciberseguridad, acentuado por la llegada del ordenador cuántico. Este tipo de ordenadores son completamente disruptivos, ya que su funcionamiento está gobernado por fenómenos mecano cuánticos sin equivalente en el mundo macroscópico. La implementación del algoritmo de Shor en un ordenador de estas características permitirá romper la seguridad de los algoritmos asimétricos pre-cuánticos más utilizados en la actualidad. Este panorama hace necesaria la investigación en nuevos paradigmas criptográficos que sean resistentes ante las nuevas amenazas. De este modo, surgen la criptografía cuántica y la post-cuántica (PQC). Varias agencias nacionales de seguridad están recomendando la rápida migración a soluciones resistentes a la computación cuántica de los criptosistemas críticos vulnerables, principalmente implementando los algoritmos post-cuánticos, actualmente en proceso de estandarización.

PQC basa su seguridad en la dificultad de resolver problemas matemáticos, al igual que los algoritmos pre-cuánticos. En las distintas rondas del concurso del NIST, se han ido descartando algoritmos de PQC, llegando a descubrir vulnerabilidades críticas en algunos algoritmos que habían logrado llegar a rondas avanzadas. Los principales algoritmos seleccionados para ser estandarizados (CRYSTALS-KYBER como mecanismo de encapsulación de claves y CRYSTALS-Dilithium como algoritmo de firma digital) se basan en problemas de aprendizaje por errores, por lo que encontrar una vulnerabilidad a este problema pondría en riesgo las soluciones PQC elegidas para la migración de los criptosistemas actuales. Por su parte, la criptografía cuántica basa su seguridad en los mismos fundamentos físicos que la computación cuántica, siendo independiente de la capacidad computacional de un adversario. La implementación de soluciones basadas en criptografía cuántica aún requiere de una mayor madurez tecnológica, desarrollo de estándares y certificación de dispositivos. Además, las infraestructuras necesarias para estas redes son costosas y de baja escalabilidad, en su concepción actual, debido a la necesidad de tener nodos intermedios de confianza. Sin embargo, los rápidos avances que se están logrando en este campo permiten visualizar un futuro en el que las redes de comunicaciones cuánticas serán una realidad para las operaciones diarias donde se requiere un alto nivel de seguridad.

El objetivo principal de esta tesis es el de **investigar soluciones basadas en criptografía cuántica que vayan más allá de la distribución cuántica de claves (QKD)**. La tesis se ha centrado en proponer dos mecanismos criptográficos novedosos asegurando que los nuevos protocolos sean comparables en eficiencia con los algoritmos pre-cuánticos y post-cuánticos. Además, se ha tenido en cuenta que estos protocolos sean implementables en las infraestructuras de comunicaciones cuánticas (QCI) actuales para maximizar el beneficio técnico de las inversiones en este tipo de despliegues.

Como resultado, **se han propuesto, analizado e implementado un protocolo de firma digital asistida por claves QKD y una prueba de conocimiento cero cuántica**, que combinan mecanismos pre-cuánticos simétricos con QKD.

Por un lado, el protocolo de firma digital asistida evita el uso de criptosistemas pre-cuánticos de clave pública vulnerables, utilizando claves generadas por QKD y utilizándolas con funciones

hash ampliamente conocidas y aprobadas por el NIST, dando lugar a un criptosistema compuesto cuya seguridad frente a diversos ataques ha sido analizada y demostrada. Este enfoque compuesto permite firmar mensajes de longitud arbitraria mediante procesos de generación y verificación de firmas altamente eficientes, en algunos casos hasta superando los algoritmos de firma digital pre-cuánticos y post-cuánticos más eficiente *CRYSTALS-Dilithium*.

Por su parte, la prueba de conocimiento cero cuántica propuesta permite la autenticación de usuarios en una QCI sin revelar información personal durante el proceso. La propuesta de una versión cuántica de ZKP se ha realizado en esta tesis por primera vez, sin precedentes en la literatura. La QZKP supone un paso más para aprovechar al máximo las ventajas de una QCI que garantice la seguridad de extremo a extremo de las comunicaciones. Esto es así, puesto que la QZKP utiliza la misma infraestructura física que QKD y Q-DS, optimizando los recursos asignados en el despliegue de estas redes y el desarrollo de dispositivos de criptografía cuántica. Se ha llevado a cabo un estudio teórico así como pruebas experimentales, dando como resultado un mecanismo de autenticación seguro y eficiente.

Por último, dado el carácter industrial de la tesis, ha sido necesario seguir de cerca los desarrollos en PQC y la evolución del panorama político respecto a las tecnologías cuánticas, incluyendo las posturas de las organizaciones relevantes en materia de seguridad y las inversiones económicas para financiación de proyectos. Y es que, para promover la investigación en criptografía cuántica de manera coherente, se requiere no solo inversiones para el desarrollo de tecnologías y pruebas de concepto, sino también coordinación internacional para optimizar esa financiación disponible. Actualmente, el programa EuroQCI se ha lanzado para el despliegue de QCI en Europa, con el objetivo de tener en el futuro una red europea integrada con enlaces terrestres basados en fibra óptica y enlaces satelitales. Estos avances, sumados al desarrollo de repetidores y memorias cuánticas, proporcionarán un paso adelante hacia el futuro Internet Cuántico. Estas cuestiones, aunque no técnicas, han influido en el diseño de los protocolos criptográficos propuestos en esta tesis.

Table of Contents

List of Figures

List of Tables

Abbreviations and acronyms

2PR Second Preimage Resistant

AES Advanced Encryption Standard

ANSSI Agence nationale de la sécurité des systèmes d'information

AP Application Plane

B2B Back-to-Back

BDExp Business Development Experience

BSI Bundesamt für Sicherheit in der Informationstechnik

CAGR Compound Annual Growth Rate

CAMM Crypto-Agility Maturity Model

CC Classic Channel

CCC Computing Community Consortium

CCN Centro Criptologico Nacional

CISA Cybersecurity and Infrastructure Security Agency

CP Control Plane

CPU Central Processing Units

CR Collision Resistant

CRQC Cryptographically-Relevant Quantum Computer

CV Continuous Variable

CVP Closest Vector Problem

CWDM Coarse Wavelength Division Multiplexing

DEP Digital Europe Program

DFB Distributed-FeedBack

DoS Denial of Service

DP Data Plane

DSA Digital Signatures Algorithms

DV Discrete Variable

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

EDDSA Edwards-curve Digital Signature Algorithm

EDF European Defence Fund

EDIDP European defence Industrial Development Program

EIT European Institute of Technology

EPR Einstein–Podolsky–Rosen

ER Extinction Ratio

ESA European Space Agency

ESP European Space Program

ETSI European Telecommunications Standards Institute

EWBI East-West Bound Interface

FIPS Federal Information Processing Standards

GDP Gross Domestic Product

GeMSS Great Multivariate Short Signature

GEO Geostationary Orbits

GERD Gross Domestic Expenditure on R&D

GPON Gigabit-capable Passive Optical Network

GPU Graphics Processing Units

GPV Gentry–Peikert–Vaikuntanathan

GSM Global System for Mobile

H2020 Horizon 2020

HE Horizon Europe

HSM Hardware Security Module

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

ISO International Organization for Standardization

ISP Internet System Providers

ITS Information-Theoretic Secure

ITU International Telecommunication Union

KDF Key Derivation Function

KEM Key Encapsulation Mechanisms

KGR Key Generation Rate

KMS key management systems

LDPC Low-Density Parity Check

LEO Low Earth Orbits

LWE Learning with Errors

MDI Measure-Device-Independent

MLWE Module Learning With Errors

MLWR Module Learning With Rounding

MPC Multi Party Computation

NATO North Atlantic Treaty Organisation

NBI North Bound Interface

NCCoE National Center of Cybersecurity Excellence

NCSC National Cyber Security Center

NFV Network Function Virtualization

NISQ Noisy Intermediate Scale Quantum

NIST National Institute of Standards and Technology

NLNCSA Netherlands National Communications Security Agency

NMR Nuclear Magnetic Resonance

NSA National Security Agencies

NTT Number Theoretic Transformation

NV Nitrogen Vacancy

OLT Optical Line Termination

ONT Optical Network Terminal

OQS Open Quantum Safe

OS Optical Switches

OTP One-Time Pad

P&M Prepare and Measure

PBS Polarization Beam Splitter

PDM Polarization-Division Multiplexers

PKE Public Key Encryption

PKI Public Key Infrastructure

PNS Photon-Number Splitting

PQC Post-Quantum Cryptography

PR Preimage Resistant

Q-DS Quantum-assisted Digital Signature

QBER Quantum Bit Error Rate

QC Quantum Channels

QCI Quantum Communications Infrastructures

QCN Quantum Communication Networks

QDS Quantum Digital Signatures

QI Quantum Internet

QKD Quantum Key Distribution

QM Quantum Memories

QN Quantum Nodes

QPU Quantum Processing Unit

QR Quantum Repeaters

QRNG Quantum Random Number Generator

QSS Quantum Secret Sharing

QuAI Quantum Abstraction Interface

QZKP Quantum Zero-Knowledge Proofs

R&D Research and Development

RNG Random Number Generator

ROADM Reconfigurable Optical Add-Drop Multiplexer

RSA Rivest-Shamir-Adleman

SAGA Security And cryptoGrAphic

SBI South Bound Interface

SDN Software-Defined Network

SDNC Software-Defined Network Controller

SIDH Supersingular Isogeny Diffie-Hellman

SIKE Supersingular Isogeny Key Encapsulation

SIPRI Stockholm International Peace Research Institute

SIS Short Integer Solution

SME Medium-Sized Enterprises

SPAD Single-Photon Avalanche Detectors

SSMF Standard Single-Mode Fiber

SVP Shortest Vector Problem

SWaP-C Size, Weight, Power and Cost

TDM Time-Division Multiplexers

TETRA Terrestrial Trunked Radio

TLS Transport Layer Security

UPM Universidad Politécnica de Madrid

WDM Wave-Division Multiplexers

XOF eXtendable Output Functions

ZKP Zero-Knowledge Proof

zkSNARK Zero-knowledge succinct non-interactive argument of knowledge

"And if I fly or if I fall, at least I can say I gave it all..."
RuPaul

Chapter 1

Introduction

1.1 Motivation

The main motivation for this thesis is the uncertain panorama of cybersecurity risks and threats that currently governs due to the alarm caused by the arrival of the quantum computer. The operation of a quantum computer is disruptive in the sense that it is governed by quantum phenomena that have no equivalent in the macroscopic world. Furthermore, Shor's algorithm, published in 1994, is widely known algorithm that implemented on a quantum computer with the necessary requirements, is capable of breaking the security of pre-quantum asymmetric algorithms [Shor, 1994]. On the other hand, in 1996, Grover published another algorithm to be implemented on this type of computers [Grover, 1996]. In this case, it is a search algorithm that, used to carry out a brute force attack, reduces the number of operations required to break a symmetric algorithm by approximately half.

New cryptographic paradigms that are being investigated as potential solutions, i.e. quantum and post-quantum cryptography (PQC), both of them facing security challenges. Specifically, the implementation of quantum cryptographic solutions still requires technological maturity, development of standards and device certification. Furthermore, given the infrastructure requirements of the networks needed for the deployments, they are high-cost and low-scalability solutions in their current state, due to the need to have trusted intermediate nodes [Mehic et al., 2020]. For its part, post-quantum cryptography bases its security on the difficulty of solving a mathematical problem, as it is the case with conventional pre-quantum algorithms. Several PQC algorithms in the different rounds of the National Institute of Standards and Technology (NIST) process [NIST, 2016] have failed due to the discovery of critical vulnerabilities [Beullens, 2022; Castryck and Decru, 2023]. Furthermore, the algorithms that have been selected to be standardized are mainly based on Learning with Errors (LWE). Finding a way to break this problem would mean the violation of the PQC solutions chosen for the migration of actual cryptosystems.

Currently, several National Security Agencies (NSA) are recommending the rapid migration of vulnerable critical cryptosystems to quantum-resistant solutions, mainly by implementing standardized post-quantum algorithms (CRYSTAL-KYBER as a key encapsulation mecha-

nism and CRYSTAL-Dilithium, FALCON and SPHINCS+ as digital signature algorithms) [Cybersecurity et al., 2023; French Cybersecurity Agency (ANSSI) and Swedish National Communications Security Authority, 2024; Nacional, 2022]. However, it should be noted that this type of PQC solutions so far have focused on being resistant to Shor's algorithm, but it is possible that at any time new methods will be found to break cryptographic solutions using a quantum computer, which have not yet been imagined. Therefore, it is natural to think about cryptographic alternatives that are based on the same physical foundations as the quantum computer, these are the principles of quantum mechanics. With the aim of ensuring that its security does not depend on the computational capabilities of the adversaries, either because they have a supercomputer or because they have access to a relevant quantum computer.

To promote research in the field of quantum cryptography in a coherent way, it requires not only investments for the development of the technologies and execution of proofs of concept, but also international coordination to maximize the profit of the available financing. Currently, the EuroQCI program [Commission, 2019] has been launched for the deployment of Quantum Communications Infrastructures (QCI) in Europe, with the aim of having in the future an integrated European network that has both terrestrial fiber optic-based links and space-to-ground links. Given the effort put from a research, economic and industrial point of view to achieve this objective, it is advisable to maximize the result in such a way that these quantum communications infrastructures provide many services apart from the quantum key distribution. In addition, these advances, added to the integration of QCI with conventional communications networks, will provide a step forward towards the future Quantum Internet (QI).

1.2 Objectives of the Thesis

Based on the situation of the security panorama described in the previous section, for the development of this thesis a main objective was established, which was to **investigate solutions that use QCI to propose protocols that go beyond quantum key distribution.** The temporal evolution of the work carried out over the years is shown in Figure 1.1.

To fulfill this general objective, the first specific objective (**O1**) was defined, being this to carry out a state of the art of quantum communications networks and the cryptographic panorama, identifying a series of challenges and opportunities. The general challenges aforementioned lead us to establish the following starting requirements:

- the proposal of cryptographic mechanisms resistant to a relevant quantum computer to replace pre-quantum mechanisms considered vulnerable;
- the new cryptographic protocols are, at least, comparable in efficiency with pre-quantum and post-quantum algorithms;
- the protocols are implementable in current quantum communications infrastructures to maximized the technical profit from the investments made in current deployments.

Based on the main objective and the starting requirements, the second specific objective (**O2**) was defined to be covered in the first part of the thesis, that is, "*Design, analyze and*

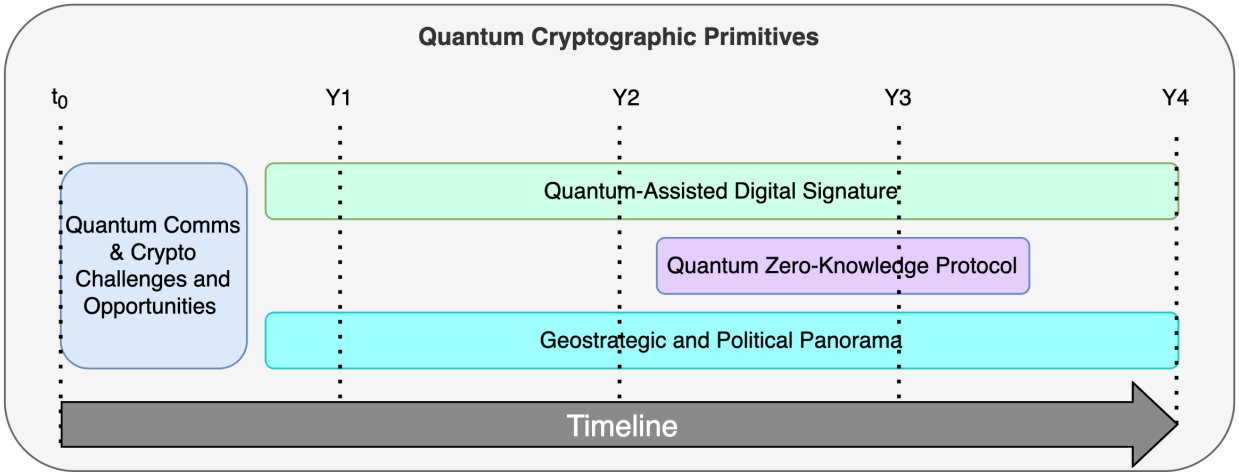


Figure 1.1: Temporal evolution of the work carried out in this thesis over the years, with t_0 being the starting time and YX being the end of each year.

implement a new quantum digital signature protocol". Broken down as:

- **O2.1** *Design a new quantum digital signature protocol*, taking as a starting point the previous studies available in the literature. Current digital signatures use vulnerable pre-quantum algorithms.
- **O2.2** *Analyze the security of the novel quantum digital signature protocol proposed*, demonstrating its robustness against attacks on the integrity of the message, signature forgery attacks and repudiation attacks by the signer of the message.
- **O2.3** *Implement the proposed quantum digital signature protocol*, to demonstrate the feasibility of implementation and compare its efficiency against other pre-quantum and post-quantum solutions.

In a second part of the thesis, which was executed in parallel with the first, the migration of the concept of classical Zero-Knowledge Proof (ZKP) to the quantum paradigm was investigated. The opportunity to execute the protocol was possible thanks to the availability of experimental Quantum Key Distribution (QKD) devices during the international stay at Politecnico di Milano, in Italy. Thus, the third specific objective (**O3**) of "*design, analyze and implement a new quantum zero-knowledge protocol*" was defined. This is broken down in a similar way to O2, that is:

- **O3.1** *Design a new quantum zero-knowledge protocol*, as a cryptographic mechanism for user authentication in a quantum communications infrastructure. Current zero-knowledge proofs are mostly based on pre-quantum asymmetric algorithms and are therefore vulnerable.
- **O3.2** *Analyze the security of the proposed quantum zero-knowledge protocol*, demonstrating that it meets the properties of completeness, soundness and zero-knowledge.
- **O3.3** *Implement the proposed quantum zero-knowledge protocol*, to demonstrate the feasibility of implementation in experimental setup and the agreement with the theoretical

results.

Finally, to fulfill these specific objectives, it has also been necessary to monitor developments in the field of post-quantum cryptography, the evolution of the geostrategic and political landscape, and the positioning of the different relevant organizations in terms of security, for the identification and addressing of the concerns raised by the last ones. These types of issues, even though they are non-technical, have influenced the design of the cryptographic protocols that are addressed in this thesis.

1.3 Thesis Structure

The structure of the document is organized as follows:

- Chapter 2 provides foundational knowledge relevant to this thesis, including an introduction to cryptography, the threat of quantum computers, the new quantum-resistant cryptographic paradigms that aim to solve this threat (PQC and quantum cryptography), and the quantum communication infrastructure needed to support quantum cryptography, laying the groundwork for the subsequent chapters.
- Chapter 3 presents the first result of the thesis, which is the novel quantum-assisted digital signature proposed. This section includes: i) the designed protocol, ii) the security analysis carried out, and iii) the implementation and experimental results.
- Chapter 4 details the second result of the thesis, which is the novel quantum zero knowledge proof proposed. As in the previous chapter, this section includes: i) the designed protocol, ii) the security analysis, and iii) the implementation and experimental results.
- Chapter 5 explores more business-oriented aspects as part of the industrial nature of the thesis. Specifically, the technological challenges that these solutions are still facing and that will define the lines of research for the coming years. As an example, the strategies to integrate isolated quantum communication infrastructures have been analyzed. From a political point of view, the positioning of the different national security agencies and the proposed migration plans are also covered, in addition to the market perspectives and the funding opportunities to address the identified challenges.
- Chapter 6 concludes the thesis by summarizing the main findings and suggesting future research directions that emerge from this work, as well as the main academic results and industry-oriented activities.

Chapter 2

Quantum-Resistant Cryptographic Paradigms

2.1 Conventional Cryptography

Cryptography is an art that has existed practically since the emergence of writing, and its purpose is to prevent the information transmitted from being read by unauthorized individuals. This art has existed practically since the existence of writing and throughout history different mechanisms have been used such as substitution cipher in ancient Egypt, Spartan scytale in the 5th century BC and, more recently, the Enigma machine during the Second World War. Over the years, methods for sending information in a secure way have become increasingly sophisticated thanks to technological advances in the field of communications and, especially, with the emergence of computer systems. However, just as cryptographic methods have evolved and benefited from new technologies to provide increasingly greater information security, these advances have brought with them new ways of attacking transmitted information by malicious actors. Thus, historically, cryptographic solutions have evolved as new ways to violate them appeared, and vice versa.

In general, cryptography has three main objectives [Forouzan, 2007], which are illustrated in Figure 2.1. The first is to protect the information that is sent so that an unauthorized actor who intercepts the message is not able to interpret it, this is called **confidentiality**. The second is to demonstrate that someone is who they say they are and is not impersonating another person or to demonstrate the authorship of certain information, which is achieved through **authentication** mechanisms. The third major objective is to guarantee the **integrity** of the information, that is, to be certain that a message that has been sent has not been modified during transmission.

The first two objectives are achieved through encryption mechanisms, while the integrity of a message and the identification of its author are achieved through signature mechanisms, thus, the recipient of the message can be sure that it was written by the person who signed it and that information is true.

Since the beginning of the digital age, the previous main objectives regarding cryptography

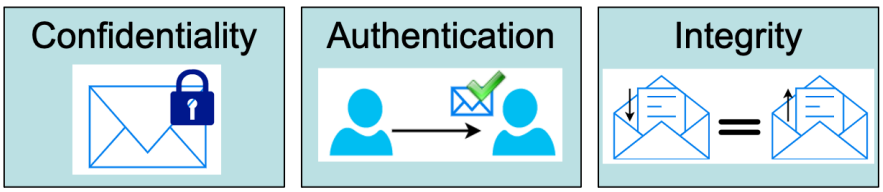


Figure 2.1: Objectives of cryptography: Confidentiality, authenticity and integrity of information.

have been the same, but now trying to prove the identity of users, network nodes, clients and servers; ensure confidentiality through different communication channels and environments such clouds, satellites, etc.; integrity of the information from text to streaming video. With that, new needs have arisen such as the rights for privacy of the users or the exchange of just partial information for collaborative applications. The main difference is the appearance or conception of cyberspace as a new environment in which information currently travels.

Given these objectives within the cyberspace, great efforts have been made related to secure communication and cybersecurity by standardization bodies [ETSI, 2024; ISO, 2024; NIST, 2024d]. These are of special importance in environments that handle sensitive information such as critical infrastructures, public administrations and banking entities, and military headquarters and bases.

As historically, despite all these efforts over the years, new high-profile cyber-attacks are strongly targeting communication networks and data centres handling critical information. Moreover, cybercriminals become more and more experts, sometimes managing to cause great damage without even detecting the origin of the attack [Alshamrani et al., 2019].

Even using all the security measures and cryptographic protocols, the communication and critical infrastructures have been and are the victim of multiple cyberattacks every day. Several examples can be found in the news, such as the one occurred in Iran in July 2021, which caused the delay and cancellation of hundreds of trains, sowing chaos in the country [Guardian, 2021]. In April 2022 where the French hospital group 'GHT Coeur Grand Est' was forced to disconnect its services from the network [HTCoeurGrandEst, 2022]. Or more recently, in July 2024 CrowdStrike company suffered an incident where a cryptographic vulnerability was exploited, causing significant disruptions to their endpoint protection services [Cybersecurity and (CISA), 2024]. This event clearly shows the need for cryptoagility, as its absence hindered CrowdStrike's ability to promptly replace the compromised cryptographic algorithms, experiencing an extended downtime followed by a challenging recovery process.

To protect against these threats and meet the objectives of cryptography, the following two cryptographic paradigms are used:

- **Symmetric cryptography**. In which the parties involved in the process share the same secret key that they will use to, for example, encrypt the information. Examples of this paradigm include symmetric encryption, such as the one shown in diagram (a) in Figure 2.2, or message authentication codes, among others. The most widely used symmetric algorithm in communications today is the Advanced Encryption Standard (AES) [NIST, 2001], although there are many more such as, for example, Blowfish

[Alabaichi et al., 2013].

- **Asymmetric cryptography**. In this case, each of the parties involved have a pair of keys, one of which will be public and the other private, and will remain secret. Furthermore, this pair of public-private keys are related to each other through a mathematical problem such as one way functions, for example, the product of two large prime numbers. This paradigm allows the development of various cryptographic primitives such as asymmetric encryption, as the one shown in diagram (b) of Figure 2.2, digital signature or key negotiation, among others. The most relevant asymmetric algorithms today are Rivest-Shamir-Adleman (RSA) [Rivest et al., 1978], Elliptic Curves [NIST, 2023a] or Diffie–Hellman [NIST, 2023b], among others.

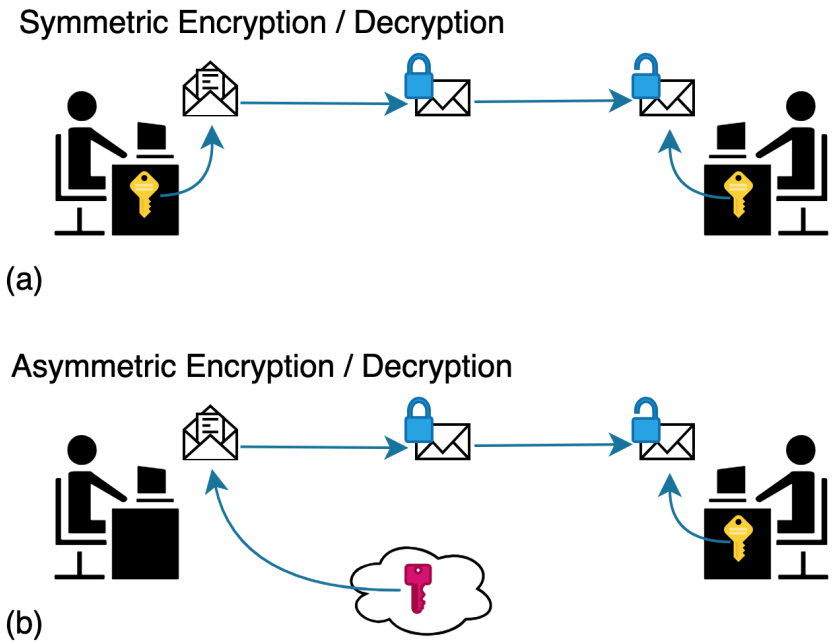


Figure 2.2: (a) Mechanism based on the use of a symmetric key to encrypt and decrypt information. (b) Asymmetric mechanism for the encryption of the information using the public key of the receiver and the decryption using the private key.

All of these currently used cryptographic solutions will be included within a group called classic or pre-quantum cryptography, to differentiate them from the solutions discussed later in this section.

2.2 The disruption of quantum computers

The discovery and recent advances in quantum physics have had a great impact on various areas of science and technology. One of the areas that has been influenced by these physical systems is computing. It was during lectures in 1981 that physicist Richard Feynman suggested that quantum systems could be used to simulate quantum phenomena more efficiently than classic computers [Feynman, 1985]. Just four years later, physicist David Deutsch proposed a

theoretical model of a universal quantum computer [Deutsch, 1985], laying the theoretical foundations for the development of quantum computing.

These types of systems are based on the ability to manipulate quantum states of nature and their interactions, taking advantage of the corresponding phenomena of superposition, entanglement and tunneling, which have no equivalent in the macroscopic world, as we will see later in this chapter. These features become the building blocks of a novel computing paradigm, which can address complex computing problems with potentially better performance, accuracy and computing time.

A key application of computing has been the simulation of natural processes to study the behavior of physical, chemical and biological systems in order to better understand nature, predict its behavior and be able to manipulate it to, for example, design new drugs or new materials. However, the study of these systems implies the presence of relevant quantum phenomena whose complexity imposes practical limitations when simulating them on conventional computers, making it necessary to make approximations and reductions of the problem to simpler systems [Rosales-Pelaez et al., 2019]. These approaches do not always allow obtaining accurate results in a reasonable execution time. Despite efforts through approximation models and specialized hardware, no classic computational paradigm has provided a fully-efficient and accurate solution to problems of many particles interacting with each other.

This is where quantum computers offer a solution. To make the calculations, a system with the same properties as those that are intended to be simulated is used as physical support. Quantum computers are expected to excel in simulating quantum phenomena, with the number of variables needed growing linearly in contrast to the classic counterpart [Courtland, 2017]. This recognition of quantum effects as computational tools can maintain the pace described by Moore's law [Schaller, 1997], even imagining transistors at the atomic scale.

In this way, the impact of quantum computing is expected to be as radically disruptive as the beginning of classic computing in the mid-20th century. Although it is important to note that quantum computing will complement conventional computing, giving rise to hybrid environments. This is because quantum processing units will be particularly efficient and cost-effective for solving certain problems, but not necessarily all of them. This coexistence and complementarity is similar to the coexistence of CPUs and GPUs in today's computers and mobile devices.

2.2.1 Features of a quantum computer

In quantum computers, the minimum unit is the Quantum Processing Unit (QPU), which are physical chips containing qubits, i.e. the quantum equivalent of a bit. The way to program on a quantum computer is by assigning degrees of freedom of the problem to a qubit to perform the calculations. Therefore, the greater the complexity of the problem, in terms of the number of variables, the greater the number of qubits needed.

When operating with these systems it is found that, on the one hand, to preserve their quantum properties, the qubits cannot interact freely with each other, nor with the environment, since

any disturbance leads to errors that affect the calculation of the solution to the problem. Thus, the system has to be isolated from the environment to reach long coherence times, i.e. a measure of how long a quantum system can remain in a superposition. While on the other hand, it is necessary to manipulate these qubits to perform calculations, which automatically implies coupling with the environment, causing decoherence [Nielsen and Chuang, 2010]. Therefore, another big challenge lies in finding a system that balances the aforementioned requirements.

Among all the proposed quantum computing models, one paradigm mainly stands out, the so-called digital or gate-based model [Michielsen et al., 2017]. This model encodes problems using quantum logic gates, so that any quantum problem can be encoded in a sequence of said gates.

Any sequence of gates applied to a set of qubits forms quantum circuits. The application of each of the logic gates introduces errors into the system, so the more complex a circuit is, the greater the impact of the error on the final state. Currently, methods to mitigate or correct these errors are being investigated. Error correction codes require great control over the qubits [Gaitan, 2008]. There are other approaches such quantum computers based on analog or adiabatic computing models [Albash and Lidar, 2018]. Instead of encoding the problem in a circuit of logic gates, a Hamiltonian is designed whose fundamental state encodes the solution of the problem to be solved. Until now, fault-tolerant quantum computers have not yet been achieved, and thus error is one of the major bottlenecks to scaling current digital quantum computers.

2.2.2 Physical Implementation

Although the theory of quantum mechanics has been understood for a couple of decades, the qubits, quantum chips and the complementary hardware technologies required are stil evolving in laboratories. The industry is in its infancy, with a strong link to the research laboratories of academia and a rapid transfer to startups, which will reach a higher maturity in the next decade.

The technologies that allow the implementation of a quantum computer can be of different types depending on the physical system used as a base. Mainly, systems based on superconductors, solid state, nuclear magnetic resonance (NMR) and photonics stand out. Superconducting qubit quantum computers [Ang, 2014] are one of the most widely used platforms today. These systems at cryogenic temperatures allow the flow of electricity without friction, giving rise to measurable macroscopic quantum effects. Regarding solid state systems, we highlight on the one hand the ion traps [Kielpinski et al., 2002], where a small number of ions are confined in an isolated space by electromagnetic fields. Initialization is performed by cooling the system to its ground state using optical pumping and the state is measured using state-dependent fluorescence techniques which provide high fidelities. On the other hand, in solid state systems based on diamond lattices [Weimer et al., 2012] the qubit is encoded in the spin associated with a nitrogen vacancy (NV) center in a carbon lattice (diamond). In this type of platforms the spin state of the NV center can be controlled at room temperature and has long coherence times i.e. on the order of seconds. This technology is also used for certain types of high

precision quantum sensors [Ho et al., 2021]. For their part, NMR-based processors [Nielsen and Chuang, 2010] trap the molecules and align or anti-align their nuclear spins by applying a strong magnetic field with coherence times ranging from milliseconds to seconds. Finally, it is possible to encode the qubits into photons, giving rise to optical quantum computers [Takeda and Furusawa, 2019]. These particles are very resistant to decoherence and can be controlled at room temperature. Furthermore, its degrees of freedom allow not only qubits to be encoded but also qudits, which are n-level quantum systems.

Although each quantum computing system has its advantages and disadvantages, in general all of them face the challenge of scalability of the solution, given the intrinsic complexity of these technologies.

Finally, it is worth mentioning an important metric in quantum computing called Quantum Volume. This metric was proposed by IBM in order to quantify the general capacity of a quantum computer to solve problems [Bishop, 2017], regardless of the technology used (NRM, photonic, etc.). To know the quantum volume of a quantum computer it has to be measured experimentally, implementing a quantum circuit with a certain number of qubits and operations that have to be executed (i.e. depth of the circuit) without losing the coherence. The variables that affect the quantum volume are the number of qubits and their quality in terms of fidelity, error rate and decoherence, the parallelism to perform multiple simultaneous operations, and the depth of the circuit, i.e. the number of operations that can be executed before the system loses coherence. All this allows the comparison of the different current quantum computers.

2.2.3 Impact of quantum computers on current cryptographic systems

As we have seen, the arrival of the quantum computer represents a paradigm shift in computing that has opened a whole panorama of challenges and opportunities for the coming decades. Specifically, given the leap in performance that quantum computers will bring, a great boost is expected in areas such as molecular simulation, materials science or biology. However, in technological areas such as artificial intelligence, cybersecurity or cryptocurrencies, these new capabilities can pose a new threat. The latter being the reason why quantum technologies have become of great geostrategic importance [Krelina, 2021].

As commented before, Peter Shor published an algorithm that, implemented on a Cryptographically-Relevant Quantum Computer (CRQC), is capable of factoring large integers in polynomial time, making asymmetric cryptography used in current communications, such as RSA or ECC, vulnerable [Shor, 1994]. In addition, Grover's quantum search algorithm is quadratically faster than any equivalent classic algorithm [Grover, 1996]. In this case, Grover's algorithm does not directly violate a cryptographic mechanism as Shor's does, but it is capable of reducing the security of symmetric cryptography systems by half. As stated in the ETSI standard EG 203 310 [ETSI, 2016]: *"Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength (in other words to retain 128 bit security will require to implement 256 bit keys). Elliptical curve cryptography will offer no security. RSA based public key cryptography will offer no security...*

The Diffie-Helman-Merkle key agreement protocol will offer no security."

Therefore:

- In symmetric cryptography, the impact of quantum computing (at least, as far as is known) is not devastating, since it does not rule the primitives currently used as invalid, but it does reduce their security, with a term of at least half. Despite this, and due to the nature of symmetric cryptographic primitives, the increase in key size, output result size, etc., makes it unnecessary to create or design new cryptographic primitives.
- Regarding the current pre-quantum asymmetric cryptographic standards (RSA, Diffie-Hellman, ECC), they base their security on mathematical problems of computational cost that are impracticable for classic computing, but that can be solved in acceptable time once a CRQC is available. This fact forces the need to develop new cryptography resistant to quantum computing.

Given that all modern communications and current digital platforms base their security on pre-quantum cryptographic mechanisms, the arrival of a CRQC could lead to the destabilization of the global economy, not to mention the implications at the security and defense levels for the nations where the confidentiality of classified information is critical [Krelina, 2021]. As concrete examples, in mobile communications such as Global System for Mobile (GSM) or Terrestrial Trunked Radio (TETRA), there are billions of devices in the world whose security is based on symmetric encryption with encryption keys of length 128 *bits* or less [ETSI, 2017]. In this framework, vulnerability analysis such as the one published by ETSI for TETRA [ETSI, 2006] will no longer be valid as well as the current definitions of risk, impact and likelihood of an attack.

2.2.4 Temporal Horizon of the Quantum Computer Threat

As commented previously, for the threat of the quantum computer to become a reality, a CRQC is required. Today these technologies are in what is called the era of Noisy Intermediate Scale Quantum (NISQ), as is the example of IBM's *Condor* processor that is capable of handling up to 1121 *qubits* [Gambetta, 2023]. However, the aforementioned attacks on current cryptographic systems will require a greater number of qubits and greater control over them. Although they are not CRQC, these quantum computers already surpass the best classic supercomputers in solving certain mathematical problems.

Therefore, although quantum technologies are maturing rapidly, with an increasing number of governments and companies launching Research and Development (R&D) programs, the technology is still in the research, development and demonstration phases, making it difficult to predict the future time horizons and the exact capabilities that these computers will have, which generates various beliefs and bets in the market.

However, although a CRQC will not be available until the medium or long term, it is critical that the migration to cryptographic systems that are resistant to quantum computers be carried out as soon as possible. This is mainly due to what is known as the "Harvest (or Store) now, decrypt later" attack [Cho, 2019]. The attack consists of confidential information encrypted using current cryptographic methods that may be intercepted and stored by attackers, waiting

for a CRQC to be available to decrypt it. This type of attack has implications such as that represented by Mosca's theorem [Mosca, 2015], which is illustrated in the diagram in Figure 2.3.

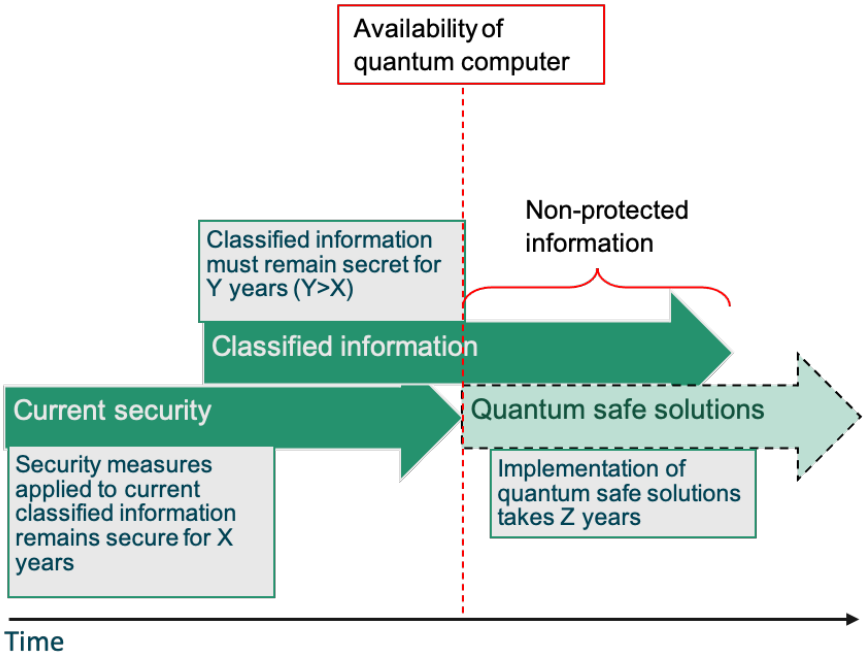


Figure 2.3: Mosca's theorem [Mosca, 2015], by which we assume that a CRQC will not be available for X years, but we have classified information that has to remain in that state for Y years. The migration process from pre-quantum cryptographic systems to quantum-resistant ones takes Z years to complete. The theorem tells us that if $Y + Z > X$, we are in trouble.

We assume that a CRQC will not be available for X years, but we have classified information that has to remain in that state for Y years. Furthermore, the process of migrating cryptographic systems to quantum-resistant systems takes Z years to complete. What Mosca's theorem tells us is that if $Y + Z > X$, we are in trouble.

This is why national security agencies, such as the Spanish National Cryptological Center (CCN), have proposed migration calendars for cryptographic systems to secure against the quantum computer threat with the aim of completing the migrations in 2030 [Nacional, 2022].

2.3 Quantum-resistant cryptographic paradigms

In view of the threat of the quantum computer and the growing need to protect cryptographic systems, great efforts are being invested in two types of solutions to make a system "quantum-resistant", that is, resistant to attacks perpetrated by a CRQC. The two new paradigms that are under research are quantum cryptography and post-quantum cryptography (PQC).

2.3.1 Post-Quantum Cryptography

The future availability of a CRQC will be critical, as we have seen, for most of current cryptographic standards. Regarding symmetric cryptography, the National Institute of Standards and Technology (NIST) [NIST, 2024d] has already launched a series of initiatives to deal with these vulnerabilities taking into account the risks posed by quantum computers. But the biggest threat that a quantum computer presents, at least in the medium term, is against asymmetric cryptography. It is important to remember that the keys used for symmetric cryptography procedures are often generated through asymmetric key negotiation procedures. To address this risk posed by quantum computers, NIST began a project in 2016, based on a series of competitive rounds, aimed at defining new asymmetric cryptographic standards based on alternative mathematical problems to those already known, with the ability to be robust against Shor's algorithm implemented in a quantum computer [NIST, 2016]. These algorithms are known as post-quantum cryptography (PQC). After several rounds of the competition in which all the proposals received were successively evaluated, in July 2022 the 3rd round of standardization of this process was completed. This round was of special relevance because it evaluated 7 algorithms selected as "Finalists" after which the first post-quantum cryptography standards were chosen. In addition to the "Finalist" candidates for this 3rd round, and in an attempt to propose alternative promising candidates, NIST also selected 8 remaining algorithms as "Alternative" candidates. This candidates require more study time than the finalists. The completion of this 3rd round has additional relevance in the announcement made by the NIST organization of the opening of a new competition, focused on digital signatures, to enhance the diversity of mathematical problems of the schemes received. This new competition takes advantage of the years of knowledge that this first competition would have provided.

The evaluated algorithms are divided into Public Key Encryption/Key Encapsulation Mechanisms (PKE/KEM) and Digital Signatures Algorithms (DSA). A **Public Key Encryption** scheme uses two keys, a private key and a public key, which are mathematically related. The encryption algorithm takes the plain message and generates an encrypted message using the public key. The decryption algorithm uses the private key to obtain the clear message from the encrypted message. For its part, **Key Encapsulation Mechanisms** also use two keys, a public key and a private key. The difference with the previous one is that the algorithm generates a random value and then derives a symmetric key from this value. It then uses the public key to generate an encapsulation (ciphered text) of that random value. The decapsulation algorithm takes the generated encapsulation and the private key to obtain the random value generated by the other party during encapsulation and then derive the same session key.

Both paradigms have, conceptually, different objectives, i.e., PKE schemes aim to cover the ability to perform asymmetric key encryption while KEM schemes aim to cover the need to establish a shared symmetric key. The NIST PQC standardization process has as its main focus the study of KEM paradigms to establish keys with which to encrypt asymmetrically. This is despite the performance advantage of symmetric ciphers over asymmetric ones. However, it should be taken into account that most of KEM solutions are based on a PKE scheme, since there is a series of established transformations, known as Fujisaki-Okamoto transformations

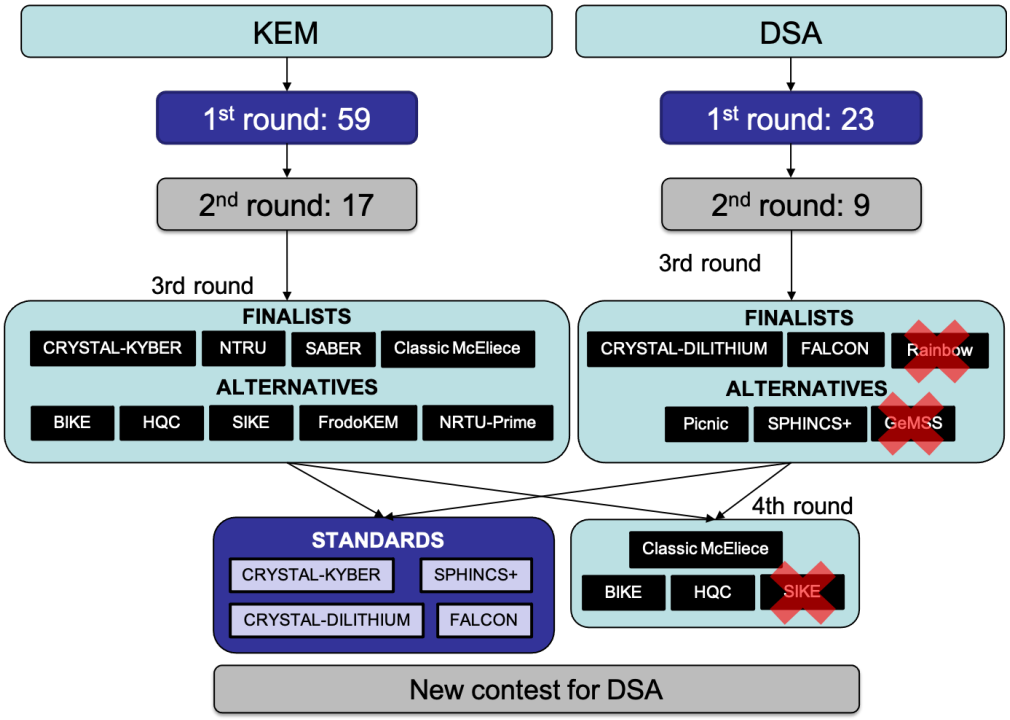


Figure 2.4: Rounds and candidates of the NIST's standardization processes for new Post-Quantum Cryptographic solutions.

[Hofheinz et al., 2017], that allow transforming PKE schemes with weak security conditions to KEM schemes with robust security conditions.

Finally, **Digital Signatures Algorithms** based on asymmetric or public key cryptography also use two related keys, a public key and a private key. The signing process uses the private key to generate the signature of a message. The verification algorithm takes as inputs the signature and the public key and, performing the corresponding public key operations, which are dependent on each algorithm, validates the veracity of the signature received.

It is important to clarify the different use of the cryptographic schemes presented above. DSA are used for authentication purposes, one of the objective of cryptography. KEM are primarily used to establish a key between two users and use that key to encrypt with a symmetric or asymmetric algorithm.

Among the different paradigms that we have just discussed, NIST has actively promoted diversity among the proposals received so that they were based on a heterogeneous set of mathematical problems. For that reason, there are several alternatives available in case some of the schemes are subject to some attacks or weaknesses not yet known. The main families of algorithms, divided into the different types of complex mathematical problems on which they are based, are the following:

- Code-based Cryptography. Based on the decoding of linear random error correcting codes.

- Multivariate-based Cryptography. Based on the resolution of systems of equations in several nonlinear variables on finite bodies.
- Lattice-based Cryptography. Based on difficult problems about the mathematical concept of a lattice, such as finding the smallest vector of a lattice or the closest to one within a lattice.
- Isogeny-based Cryptography. Generalization of the discrete logarithm problem on elliptic curves, this family is based on the search of elliptic curves in a graph defined on their space.
- Symmetric-based Cryptography. Based on the robustness of the cryptographic primitives used in symmetric cryptography. This includes block ciphers or cryptographic hash functions, among others.

Currently, NIST is involved in 3 parallel post-quantum algorithm standardization processes. Following the completion of the third round of the original NIST competition, four algorithms were selected for standardization. Two algorithms have been chosen as the main ones: *CRYSTALS-Kyber* (KEM) and *CRYSTALS-Dilithium* (DSA). Furthermore, it was also decided to proceed with further standardization of the *FALCON* and *SPHINCS+* signature schemes. Regarding this process, the first standards proposals for *CRYSTALS-Kyber* (FIPS 203), *CRYSTALS-Dilithium* (FIPS 204) and *SPHINCS+* (FIPS 205) were published in August 2023, to receive suggestions and comments from the cryptographic community. to the details of the standardization proposals carried out by NIST. In December 2023, NIST announced the compilation of the modification proposals received for study and the final standards were published in August 2024 [NIST, 2024a, 2024b, 2024c]. NIST also announced that the *FALCON* standard would be proposed later. Late publication of the *FALCON* standard compared to the rest is due to the complexity of the scheme.

In addition to the algorithms selected for standardization at the end of the third round, a fourth round was announced for a more in-depth study of 4 candidates qualified as 'Alternatives', in order to standardize at least one more KEM scheme. The selected algorithms were: *BIKE*, *Classic McEliece*, *HQC* and *SIKE*. NIST announced that unless an uncontrolled vulnerability is found in *HQC* or *BIKE* schemes, one of them will be selected for further standardization, along with *CRYSTALS-Kyber* within the category of key encapsulation mechanisms. Furthermore, given the security of the *Classic McEliece* scheme, NIST was not asking for further analysis in this regard but rather with respect to possible use cases where this scheme could fit, due to its excessive key size, which makes it not suitable for general purpose encapsulation mechanisms. Regarding the candidate *SIKE*, an unrecoverable vulnerability with respect to this scheme was discovered shortly after the announcement of the fourth round. This fact forced NIST to declare *SIKE* an invalid scheme and discard it from the competition for this fourth round [Castryck and Decru, 2023].

Finally, due to the great focus put on encapsulation mechanisms (KEM) throughout the standardization contest, NIST announced in July 2022 the creation of an additional standardization contest dedicated exclusively to asymmetric digital signatures. This would be possible thanks to the experience added after more than 6 years since the candidates that were originally presented in the first post-quantum standardization competition. Figure 2.4

shows a summary of the whole NIST process. Among the objectives of this call are:

1. **Diversify the family** of PQC digital signature algorithms;
2. Obtain schemes with **shorter signatures** and **faster verification** to be used in certain applications; and
3. Find candidates based on proposals **other than structural lattices**.

The deadline for submitting proposals closed in June 2023, and at the end of July 2023 it was announced that, of the 50 proposals received, 40 were considered 'correct and complete' and would be the ones that would make up this digital signature contest. Within the proposals, there is the following division:

- Code-based Cryptography: 5 candidates
- Multivariate-based Cryptography: 11 candidates
- Lattice-based Cryptography: 7 candidates
- Isogeny-based cryptography: 1 candidate
- Symmetric-based cryptography: 4 candidates
- MPCith-based Cryptography: 7 candidates
- Others: 5 candidates

It is of particular interest to see that, in connection with the creation of this additional signature contest, the consideration of a new paradigm, called *MPCith*, has been formalized. This paradigm builds zero-knowledge protocols from Multi Party Computation (MPC) protocols. In MPC, the prover runs a series of calculations with information from multiple parties, committing to the result of each party independently. In turn, the verifier requests verification of the result of a subset of the total participating parties. This paradigm is used in conjunction with the Fiat-Shamir transformation, under which zero-knowledge protocols are transformed into digital signatures, for the generation of this type of protocols from MPC. This is specially relevant in this thesis since we propose a quantum version of the zero-knowledge protocols.

Standardized PQC Algorithms

An overview of the algorithms that have ultimately been chosen for standardization so far is shown in this section. This shows NIST's interest in standardizing schemes based on different mathematical problems to avoid the risk that future attacks or weaknesses could lead to a lack of standardized secure cryptographic schemes.

Regarding the mathematical problem underlying each DSA PQC algorithm:

- *CRYSTALS-Dilithium.* Its security is based on the lattice-based Module Learning With Errors (MLWE) problem. This scheme is very efficient due to the use of the Number Theoretic Transformation (NTT), which allows multiplying polynomials over finite fields more efficiently than traditional methods. With respect to the underlying probability distribution, it is uniformly distributed. Dilithium is a signature scheme with high

efficiency, easy implementation, and strong theoretical and analyzed security. It is the main digital signature algorithm selected to be standardized (FIPS 204 [NIST, 2024b]) due to its wide range of applications, derived from the performance and key sizes it generates.

- *FALCON*. The "Fast Fourier lattice-based compact signatures over NTRU" design, from which it takes its name, is based on the Gentry–Peikert–Vaikuntanathan (GPV) model for lattice-based signatures using 'trapdoor' functions. The mathematical strength of *FALCON* is based on the complexity of the Short Integer Solution (SIS) problem on the rings known as NTRU. *FALCON* was chosen for standardization because NIST is confident in its security. Despite this, it is considered an extremely complex scheme, which is why its standardization is being carried out at a different pace than the rest of the standardization selections.
- *SPHINCS+*. This scheme combines the use of One Time Signatures, Few Times Signatures, Merkle Trees, and Hypertrees to construct a general-purpose digital signature scheme. *SPHINCS+* was selected for standardization (FIPS 205 [NIST, 2024c]) because it provides a viable signature scheme which is based on a completely different set of assumptions than the other signature schemes that will be standardized. The underlying difficulty of this scheme is the robustness of the cryptographic hash functions used, therefore it is considered a conservative scheme at the security level.

Regarding the key encapsulation mechanism (KEM) *CRYSTALS-Kyber*, the underlying problem is based on the MLWE problem, as CRYSTALS-Dilithium, based on the difficulty of solving linear matrix systems when they are modified with a random error term. The security of this lattice-based scheme has been strongly analyzed theoretically and under specific parametrizations. Kyber also provides very good software and hardware performance. Some important reason to standardize *CRYSTALS-Kyber* (FIPS 203 [NIST, 2024a]) among the three finalist lattice-based schemes is that the performance of NTRU is not as good as Kyber. Another decision factor is that there is more evidence about the strength of the MLWE problem than the Module Learning With Rounding (MLWR), the underlying problem of *SABER*.

Security of PQC algorithms

The main national security agencies (NSA) in Europe, as well as the North Atlantic Treaty Organisation (NATO) itself, have recommended the migration of vulnerable cryptographic systems to PQC solutions. However, it should be taken into account that: 1) the underlying mathematical problems are difficult to solve, but they are not Information-Theoretic Secure (ITS), as happened with pre-quantum algorithms; 2) given that they are recent algorithms, they still have to undergo several years of cryptanalysis to consider them truly robust; 3) the two main KEM and DSA algorithms relies on a single solution (MLWE).

Throughout the NIST competition, several candidates that were progressing in successive rounds had to be discarded because critical vulnerabilities were found. Examples of this are:

- DSA *Rainbow*, which was broken by a brute force attack carried out with a conventional computer [Beullens, 2022]. *Rainbow* is a signature based on systems of equations in

several variables proposed by Ding and Schmidt. Rainbow relies on the Oil-and-Vinegar method, by which two sets of variables are defined, each playing a role in the constitution of the system of equations, but with defined rules for the interaction between these variables. This scheme was the only one of the finalist signature schemes that is not based on lattices.

- *Great Multivariate Short Signature (GeMSS)* is a signing scheme that follows the hash-and-sign paradigm with the application of Feistel-Patarin iterations. *GeMSS* suffered a catastrophic key recovery attack and NIST decided to discard it [Tao et al., 2021].
- *Supersingular Isogeny Key Encapsulation (SIKE)* is a specific implementation of the *Supersingular Isogeny Diffie-Hellman (SIDH)* protocol. *SIKE* is based on the difficulty of finding isogenies between supersingular elliptic curves. It was an unusual candidate, as it is based on a different problem than all other post-quantum schemes. But an efficient key recovery attack in about an hour on a single classic core against the *SIDH* protocol was published [Castryck and Decru, 2023]. This fact excluded this scheme and reduced confidence in isogeny-based schemes.

These assumptions open the possibility of discovering a solution that allows breaking the security of these algorithms. However, these premises are the same ones that have always been taken into consideration with pre-quantum cryptographic solutions, so it is not something intrinsic to PQC.

Recently, a series of articles have been published about possible attacks on LWE algorithms and their structured variants (RLWE, PLWE) which are the mathematical basis of the main PQC solutions standardized by NIST both for CRYSTALS-Kyber KEM and CRYSTALS-Dilithium DSA. Due to the great capacity of this mathematical family to generate schemes that are both efficient and lightweight (at the key size level), a great focus has been placed on trying to derive attacks against this type of mathematical structures [Z. Zhao and Ding, 2022]. If these attacks are proven true, the cryptographic solutions being used to carry out the migration of the systems would be invalidated.

In view of this, it is advisable to analyze and investigate alternative cryptographic methods based on physical never explored until now for security purposes. This is the case of quantum cryptography, which is the focus of this thesis.

2.3.2 Quantum Cryptography

The quantum properties of physical systems have been known for just over a century. However, its control and manipulation for the development of technological applications is more recent and its full potential has not yet been discovered. In the last two decades, the use of these quantum mechanical systems has been proposed and promoted for computing applications, as we have just seen in the section 2.2, but also in the development of new sensors, communications and cryptographic applications.

We are going to briefly describe the main physical phenomena that make these new technologies represent a paradigm shift in practically all aspects and how these fundamental properties are applied to quantum cryptography.

Laws of physics in the macroscopic world determine the position of objects, measure properties such as their speed, acceleration, etc. However, when physicists of the late 19th and early 20th centuries delved into the world of the subatomic applying the same rules, they discovered that the laws of classic physics were not fulfilled. Does that mean that classic physics has errors or is poorly formulated? The answer is no. With the advancement of the years and a better understanding of the subatomic world, new mathematical models capable of describing this type of systems were developed and it was demonstrated that the properties of the classic physics, as we know them, can be derived from the laws of quantum physics.

The main events that helped shape what we know today as quantum mechanics had their origin, on the one hand, in the study of electromagnetic radiation and, on the other hand, in the development of models to describe the atomic behavior. Firstly, Max Planck's proposal in 1900 to quantize energy to develop the theory of black body radiation. In 1905, this idea of quantization of energy was taken up by Albert Einstein in order to explain the photoelectric effect, discovered by Heinrich Hertz at the end of the 19th century. Einstein earned the Nobel Prize in 1921 for this study.

Regarding the description of atoms, in 1913, Niels Bohr proposed what is now known as the Bohr atomic model, again taking up Planck's idea of quantization. Until years later, in 1924, Louis de Broglie proposed the famous hypothesis of wave-particle duality.

At that time, there was already enough knowledge so that Werner Heisenberg, Max Born, and Pascual Jordan could formulate for the first time the principles of quantum mechanics, as a mathematical framework to describe the behavior of subatomic particles, based on all the experimental evidences collected to date. This framework, together with the formulation of Schrödinger's wave equation in 1926, provided the foundations for the new field of quantum physics. The four postulates of quantum mechanics describe: 1) an isolated quantum system as a space of states, 2) its temporal evolution following the Schrödinger equation, 3) the concept of measurement in this type of systems, together with the probability of obtaining a result starting from an initial state, and 4) how two or more quantum systems are combined to give rise to a composite system.

How are all these concepts and properties transferred to the field of cryptography and communications? As we already know, quantum cryptography was born from the need to design new cryptographic paradigms that are resistant to CRQC. Quantum cryptographic protocols base their security on several of the basic principles of quantum mechanics and not on the strength of a mathematical problem or on assumptions about the computational capacity of an adversary. This opens a completely new field in cryptography in terms of the development of security proofs and the implications that the transition from theory to practice has when these systems are implemented. These challenges are addressed in more detail in chapter 5, where the technological and political panoramas are analyzed.

Quantum cryptographic protocols are based on the sending and receiving of quantum states, so quantum effects are measurable. The underlying physical system is photons. The information is encoded in different ways, such as polarization, phases or time. We describe the coding based on polarization on an illustrative example. We suppose a source of depolarized light, that is, light that has components in all directions, as illustrated in Figure 2.5. If this depolarized

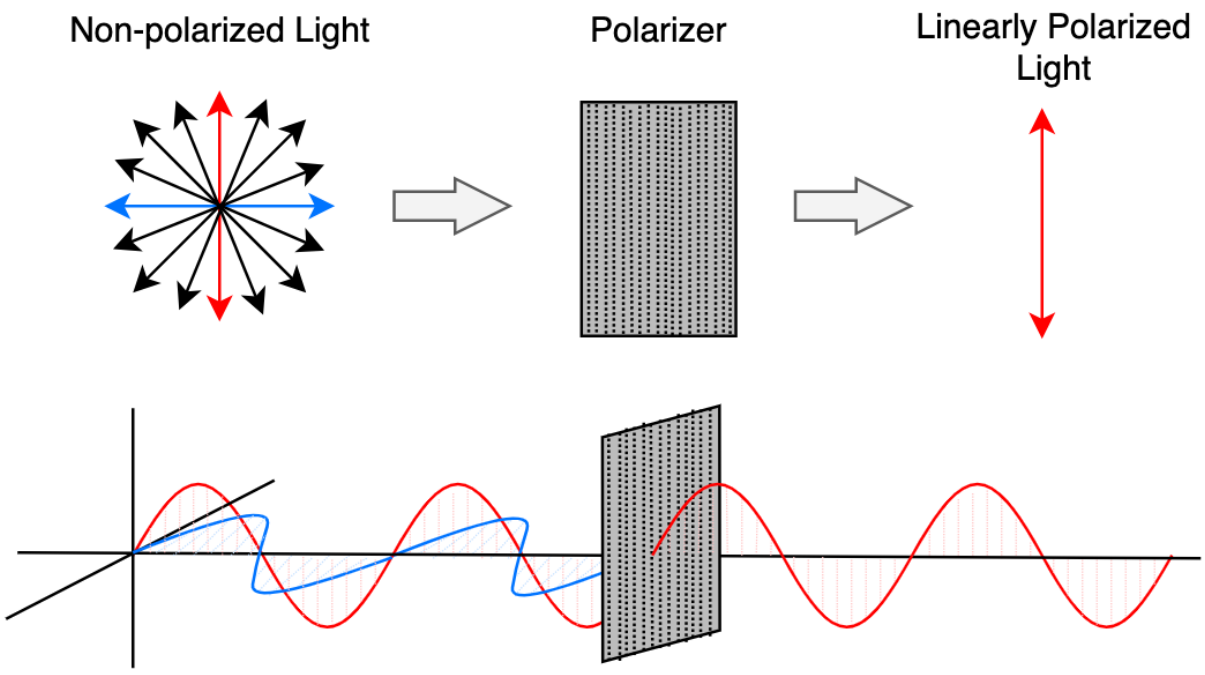


Figure 2.5: Polarization of light from a depolarized source.

light goes through a polarizer that filters all its components except the vertical one, we obtain linearly polarized light. The polarizer acts as a slit that only allows to go through the light in a specific direction, as shown in the example diagram in Figure 2.5. Once we have polarized light in the direction set by the polarizer, if it is put through the polarizer again, depending on its orientation, we will observe the situations shown in Figure 2.6. In the first case, with vertically polarized photons and the polarizer in a vertical position, the result is that all the photons pass through. If, on the other hand, the polarizer is in a horizontal position, the result is that no photon passes through. In the third case, the photons are vertically polarized and the polarizer is diagonally oriented. In this case, it would be expected that no photon would be able to cross the polarizer following classic intuition and based on the results from the two previous cases. However, what it is observed is that a certain percentage of photons go through and adopt the orientation of the polarizer. This phenomenon is a consequence of what is known as **superposition principle**.

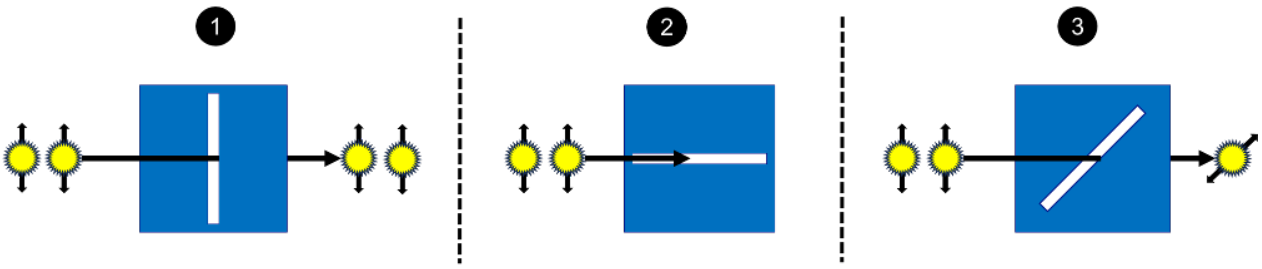


Figure 2.6: Behavior of photons when measured, represented by slits with different orientations.

Taking these behaviors into account, it is possible to encode information based on the

polarization of photons and define cryptographic protocols whose security is based on the indeterminacy of quantum states, when we measure two non-orthogonal states due to the superposition principle. To do this, Dirac notation is used, which allows us to describe pure quantum states in the computational basis $\{|0\rangle, |1\rangle\}$ (vertical and horizontal polarization, respectively) and in the diagonal basis $\{|+\rangle, |-\rangle\}$ (diagonal polarizations at 45^o and -45^o, respectively). States in the diagonal basis are a linear combination of the pure states, i.e. superposition of pure states. In matrix representation they are described as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}; |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{2.2}$$

At this point we have four polarization *states* that can be encoded in the bit values 0 or 1, as indicated in the Figure 2.7. Thus, a bit with value 0 will correspond to the measurement of a photon with vertical or diagonal polarization at 45^o. While a bit with value 1 will correspond to the measurement of a photon with horizontal or diagonal polarization at -45^o.

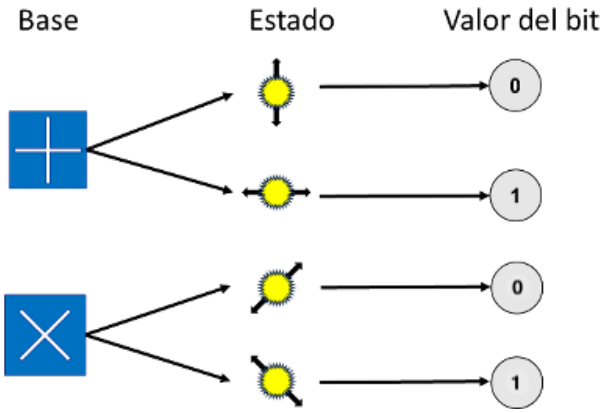


Figure 2.7: Information encoding with photonic quantum states in BB84 protocol.

In order to determine the *state* of the photons that the emitter has sent to a receiver (which are unknown by him), the receiver has to *measure* those photons. Coming back to the example of the polarizer again, but this time it will allow two orthogonal polarizations to go through. That is, the polarizer will allow polarized photons in computational basis to go through, as illustrated in Figure 2.7. If the incident photons are in state $|0\rangle$ or $|1\rangle$, all of them will be detected and properly measured. If, on the other hand, they are in the $|+\rangle$ or $|-\rangle$ state, a detection will be obtained 50% of the times. Let's look at this phenomenon mathematically. According to the third postulate of quantum mechanics, quantum measurements are described as a collection of measurement operators $M_w = |w\rangle\langle w|$. Given a system that is in the state $|\psi\rangle$ immediately before the measurement, the probability of obtaining w as a result is:

$$p(w) = \langle\psi|M_w^+ M_w|\psi\rangle \tag{2.3}$$

And the state of the system after the measurement is defined as:

$$\frac{M_w|\psi\rangle}{\sqrt{\langle\psi|M_w^+ M_w|\psi\rangle}} \tag{2.4}$$

Based on this, if the state of the qubit before the measurement is $|\psi\rangle = |0\rangle$, and we are going to measure it using the computational basis (i.e. the polarizer that allows the vertical and horizontal states to go through), we obtain that the probability of obtaining $w = 0$ is:

$$p(0) = \langle 0|M_0^+ M_0|0\rangle = \langle 0|M_0|0\rangle = 1 \tag{2.5}$$

And the state after the measurement is:

$$\frac{M_0|0\rangle}{\sqrt{\langle 0|M_0^+ M_0|0\rangle}} = M_0|0\rangle = |0\rangle \tag{2.6}$$

That is, with a probability of 100% the state after passing through the polarizer will be $|0\rangle$. If now the state of the qubit before the measurement is $|\psi\rangle = |+\rangle$, and it is measured using the computational basis again, we obtain that the probability that in this case the result is $w = 0$ is:

$$p(0) = \langle +|M_0^+ M_0|+\rangle = \langle +|M_0|+\rangle = \frac{1}{2} \tag{2.7}$$

And the status after the measure is:

$$\frac{M_0|+\rangle}{\sqrt{\langle +|M_0^+ M_0|+\rangle}} = \frac{1}{\sqrt{2}} M_0|+\rangle = |0\rangle \tag{2.8}$$

That is, with a probability of 50%, the state of the qubit after going through the polarizer will be $|0\rangle$.

The same applies to the case of a polarizer that allows $|+\rangle$ and $|-\rangle$ to go through but, in that case the base is called the Hadamard base [Nielsen and Chuang, 2010].

The polarizers described are defining two possible *bases* (computational and Hadamard) in which to measure quantum states and constitute the foundations of one of the best-known quantum key distribution protocols, the Bennett and Brassard protocol (BB84) [Cryptography, 1984].

The optical elements that are used to carry out these processes are explained in the experimental systems described in chapters 3 and 4, where we highlight the two experimental setups used through this thesis to implement the novel protocols proposed.

In addition to the superposition of states, there are other physical properties of quantum systems that have no equivalent in the macroscopic world. For example, the entanglement

property which consists of two qubits being correlated in such a way that, even though they are separated by a large distance, when an operation is performed on one qubit of the entangled pair, the result is transferred to the other. One of the operations that can be carried out on the entangled pair is what is known as entanglement swapping. In this case, a third qubit is taken and a series of operations between it and one of the entangled qubits are performed. By doing this, the information encoded in the single qubit can be transferred to the location of the second entangled qubit of the pair. This is the basis of the design of quantum repeaters.

Finally, the non-cloning property prevents a particle in the quantum regime from being measured, copied or replicated without disturbing its quantum state. This has the consequence that a qubit in an unknown state cannot be faithfully amplified, preventing the use of classic repeaters. However, this property brings the advantage that if there is an attacker intercepting the qubits while they are transmitted, they will be altered and this alteration will be detected by the sender and receiver of the communications.

Quantum Cryptographic Primitives

Based on the physical properties described above, a series of cryptographic primitives have been proposed over the years. Today, the Quantum Key Distribution (QKD) is the most analyzed, developed and implemented cryptographic primitive. But primitives that go beyond key distribution have also been proposed, such as quantum digital signatures [Wallden et al., 2015], quantum oblivious transfer [Bennett et al., 1991], quantum secret sharing protocols [Tittel et al., 2001] and, as part of the fundamental results of this thesis, a new quantum zero-knowledge protocol for user authentication, described in chapter 4.

The QKD primitive allows the distribution of completely random secret symmetric keys between two nodes in a network. These keys can be latter used, for example, to encrypt information using a symmetric encryption mechanism such as AES. The process by which these keys are established does not depend on any algorithm or mathematical assumption, and the distributed keys have been demonstrated to be information-theoretically secure keys (ITS), as defended by theorists in the field [Lo and Chau, 1999; Renner et al., 2005; Shor and Preskill, 2000]. Among the multiple cryptographic primitives used today to guarantee the confidentiality, integrity and authenticity of communications, having secure secret keys shared between users is critical. As we mentioned, the establishment of keys is currently done through pre-quantum asymmetric mechanisms vulnerable to Shor's algorithm implemented in a CRQC. Hence the great relevance of QKD is prominent.

Let's see an overview of the most relevant QKD protocols within the quantum cryptographic landscape. Over the years, several QKD protocols have been proposed. The difference between them lies in the way the information is encoded and the key generation and distillation processes. The main protocols are:

- Prepare and measure protocols using discrete variable (P&M-DV). These protocols are based on the preparation of individual qubits (in this case single photons) by the sender, sending them through a quantum channel and measuring them on the receiving side. These types of protocols were the first to be designed and implemented. The most

prominent protocols in this category are *BB84* [Cryptography, 1984], *B92* [Bennett, 1992] and *SARG04* [Acin et al., 2004].

- Prepare and measure protocols using continuous variable (P&M-CV). These types of protocols are gaining great relevance in the quantum cryptographic landscape since they can be implemented using standard communications hardware. In this type of protocols, light carries information continuously (and not discretely as in the previous case) and on the receiver side the value of the quadrature of a coherent state is analyzed. An example of CV protocol is *GG02* [Grosshans and Grangier, 2002].
- Entanglement-based protocols. This type of protocol is similar to those of P&M with the big difference that in this case individual qubits are not used, but rather pairs of entangled qubits. Of this type we highlight *E91* [Ekert, 1991] and *BBM92* [Bennett et al., 1992].
- Measure-Device-Independent QKD (MDI QKD). It is a protocol in which, instead of extracting the symmetric key from the preparation on the sender (Alice) side and measurement of the quantum states on the receiver (Bob) side, the key is extracted from the correlations between the signals sent by both Alice and Bob to an intermediate point. Thus, if the signals are equivalent they write down that value and if they are not, they discard it. An example of this type is the Twin field MDI [H.-L. Yin and Fu, 2019].

We are going to describe in detail the steps of the QKD *BB84* protocol commented before, since it has been used as the basis for the design of the cryptographic protocols resulting from this thesis.

The BB84 protocol encodes the information as indicated in figure 2.7. The broad description of the steps that BB84 follows are represented in Figure 2.8 and are the followings:

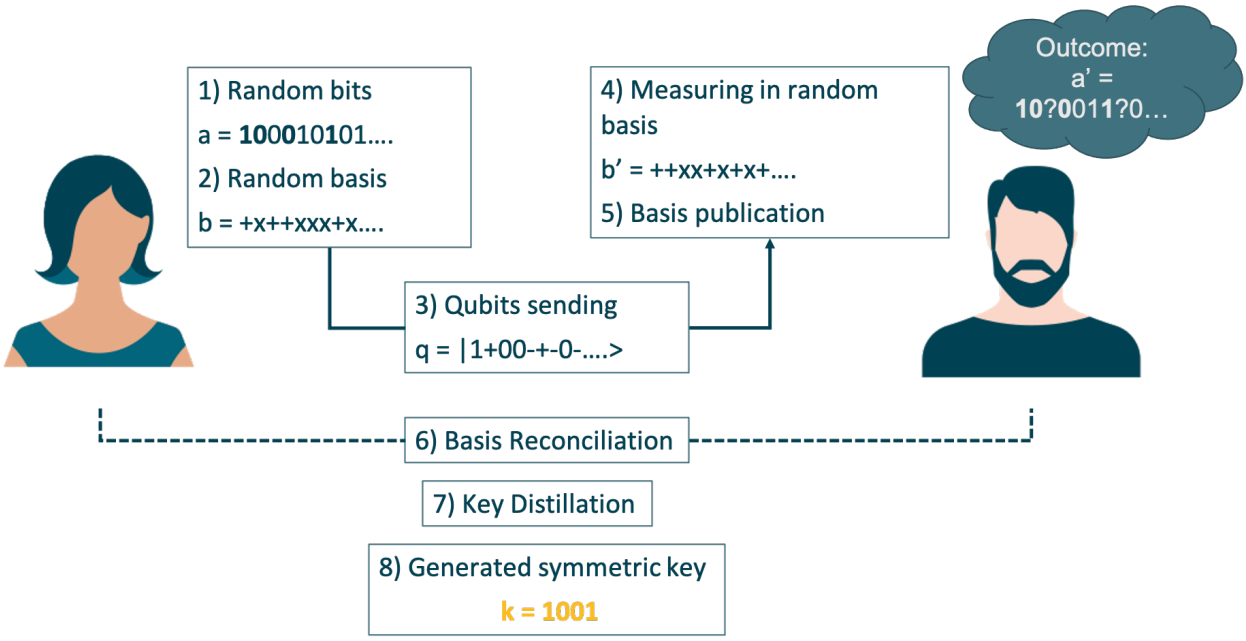


Figure 2.8: QKD BB84 protocol steps.

1. Alice generates a random sequence of bits using a quantum random number generator (QRNG). QRNG are capable of generating fully unpredictable random numbers, instead of pseudo-random numbers as it is the case with classical RNG, thanks to the use of quantum systems [Aldama, 2022].

2. For each bit of the sequence, Alice randomly chooses between the computational basis and the Hadamard basis, for the encoding of the information as shown in the figure 2.7 and as described below:

   - In case the randomly chosen basis is computational and the randomly generated bit is 0, the state of the resulting qubit is $|0\rangle$;
   - If the basis is computational and the bit is 1, the resulting qubit state is $|1\rangle$;
   - In case the randomly chosen base is Hadamard and the randomly generated bit is 0, the state of the resulting qubit is $|+\rangle$;
   - If the basis is Hadamard and the bit is 1, the state of the resulting qubit is $|-\rangle$.

3. Alice sends to Bob the qubits, through a quantum channel like the ones described in moree detail in section 2.4.

4. When Bob receives each qubit he carries out the measurements by randomly choosing the computational or Hadamard basis, also supported by a QRNG.

5. With a certain probability Bob will choose for the measurement the same basis that Alice has used to prepare the qubit.

6. Once the measurement process is finished, Alice and Bob have a so-called raw key that slightly differs from each other. This is due to the randomness in the preparation and measurement of the qubits and the losses that occur during transmission due to channel noise. Therefore, they proceed to distillation of the key, carrying out a series of steps that do not involve quantum processes anymore. First, they perform a bases reconciliation, where Bob makes public the bases in which he has measured, always keeping secret the value of the bit obtained after the measurements. Alice, for her part, tells him the positions in which she has used the same basis. In this way, they can locate and eliminate the bits where the measurements do not match. After reconciliation, they get the so-called sifted key.

7. They then carry out an error correction process to identify those bits that may be erroneous, despite having measured on the right basis, and correct them. These errors are a consequence of the physical transmission process. To carry out error correction different approaches are used such as Low-Density Parity Check (LDPC) [Gallager, 1962] or CASCADE [Toyran et al., 2013]. Once this step is completed, the key they share is identical. This process also provides the Quantum Bit Error Rate (QBER) result obtained from the execution of the QKD protocol. This parameter allows us to quantify the amount of noise that has been generated in the execution of the BB84 protocol and, therefore, to determine if there is an eavesdropper intercepting the communications. If the QBER is above a certain threshold, as we will see in the next section when we describe the security of QKD, the protocol would be aborted. If the QBER is below the

allowed noise threshold Alice and Bob would continue with the next step.

8. Although the key shared at this point is identical, an additional step called privacy amplification is carried out, so that, in case any bit of information has been leaked, the security of the key can be increased. To do this, a hash function is applied to the key and the resulting digest is the final secret symmetric key [Yan et al., 2022].

In the case of a QKD protocol based on entanglement, such as E91, the steps are very similar to BB84. The main difference is that at the beginning of the protocol, pairs of entangled photons are generated. They can be generated by Alice or by a third party who then sends one qubit of the pair to Alice and another to Bob. In this case, both Alice and Bob measure the qubits that they receive in the computational or Hadamard basis randomly. As in the case of BB84, after the measurements they carry out the processes of basis reconciliation, error correction and privacy amplification, obtaining the final secret symmetric key.

As we mentioned at the beginning of the section, there are other primitives within the field of quantum cryptography in addition to the QKD protocols that allow establishing pairs of symmetric keys between users, which can then be used to encrypt the information and guarantee confidentiality of communications. These primitives address other security needs, such as the integrity and authenticity of information, or the authentication of a user.

We are going to introduce two cryptographic primitives that have been the subject of study in this thesis. Specifically, Quantum Digital Signatures (QDS) and Quantum Zero-Knowledge Proofs (QZKP). QDS allows to guarantee that the information received by the receiver has been generated and signed by the sender of the message, without its identity being impersonated, and without the original message having changed during transmission. This type of mechanism also guarantees the non-repudiation of the message, that is, in the message delivery chain, the original sender cannot deny the authorship of its digital signature. The quantum-assisted digital signature proposed in this thesis guarantees all this requirements. The results obtained from the research carried out on this primitive are detailed in chapter 3. For its part, a QZKP allows a user, named the prover, to demonstrate to another user, named the verifier, that he or she knows certain information without revealing it. One of the applications of zero-knowledge proofs is as an authentication mechanism. A quantum version of ZKP has been proposed in this thesis for the very first time. All the research on this cryptographic primitive and the results obtained are detailed in chapter 4.

Security of Quantum Cryptography

As we have commented on several occasions, quantum cryptography bases its security on the foundations of quantum mechanics. Therefore, the security proofs that have been published over the years have a different approach than the security proofs of pre-quantum and post-quantum algorithms. Most of the security proofs found in the literature are focused on QKD, since it is the most analyzed primitive within the field of quantum cryptography. Thus, we highlight the most relevant security analysis:

- Ref. [Cryptography, 1984]. In the article in which Bennett and Brassard published their famous quantum key distribution protocol in 1984, which would later be known by the community as BB84, they included a security analysis. In this analysis they

considered different cheating strategies coming from a malicious emitter or receiver, such as photon-number splitting (PNS) attack. And, the authors demonstrated the robustness of the protocol against these specific attacks at that time. However, over the years new forms of attack were discovered that had not been taken into account back in 1984. From that moment on, different evolution of the security proof began to be published, most of them of great complexity [Biham et al., 2000; Mayers, 2001].

- Ref. [Lo and Chau, 1999]. This security proof, unlike the previous ones, takes into account imperfect sources, devices and noisy quantum channels, which more faithfully represent a real system. This security proof does not correspond to the BB84 protocol but to a variant that considers the distribution of Einstein–Podolsky–Rosen (EPR) entangled pairs between Alice and Bob who, in addition, must have a quantum computer to execute the protocol.
- Ref. [Shor and Preskill, 2000]. In 2000, Peter Shor, author of the cryptographic algorithm capable of breaking pre-quantum asymmetric cryptography, together with John Preskill, analyzed the QKD BB84 protocol, demonstrating its security under a simpler approach. The analysis is based on the results of H.K. Lo et al. [Lo and Chau, 1999] described above, considering as a starting system a pairs of entangled qubits in which entanglement purification operations are carried out with error correction codes (CSS). Once the security of these systems has been demonstrated, the implicit security for the BB84 is derived as a result. This security proof is where the maximum Quantum Bit Error Rate threshold is calculated, $QBER = 11\%$, above which a secret key cannot be generated. This limit is taken into account in the analysis of the protocols proposed in this thesis for Q-DS in chapter 3 and QZKP in chapter 4.
- Ref. [Renner et al., 2005]. Finally, we highlight the proof published by R. Renner, N. Gisin and B. Kraus in 2005. The authors establish a general security framework for a family of protocols with similar key post-processing processes and apply it as an example to three QKD protocols: BB84, the six-state, and B92. It should be noted that in this security proof, the classic channel through which key distillation processes are carried out are considered insecure, although authenticated. In this case, they consider the use of perfect emitters and receivers devices.

2.3.3 Hybrid and Composite Systems

Although current cryptographic systems are based on asymmetric systems vulnerable to CRQC, quantum cryptography protocols are not yet technologically prepared to be used in daily operations for the transmission of sensitive information. And, alternative PQC solutions still present implementation problems and the potential discovery of vulnerabilities that could render these systems useless, as we have seen in previous sections. That is why, in this context, the proposal of solutions that combine two or more cryptographic techniques is taken into consideration for the design of systems with different security layers and that require completely different cryptanalytic methods. This introduces an additional degree of complexity that makes attackers' tasks more difficult. These types of solutions are based on the proposal of hybrid and/or composite schemes.

A composite system [A. Vaira, 2024] is made up of two or more cryptographic solutions independent of each other called components. An example of this type of system would be a digital signature that is composed of two independent digital signatures generated through different mechanisms, one with Elliptic Curve Digital Signature Algorithm (ECDSA) and the other with CRYSTALS-Dilithium. In order to verify the composite signature, each of the component signatures must be verified individually. Another example would be to generate a key k_1 through the QKD BB84 protocol and encrypt a message with that key using One-Time Pad (OTP). Now generate a second key k_2 with RSA and encrypt the result of the previous OTP with this key also with an OTP. The result would be a double nested encryption independent of each other. To decrypt the information the order in which the keys are used does not affect.

For its part, we refer to a hybrid system when two or more components are combined in such a way that the final result is a new element [E. Barker and Davis, 2024]. For example, we generate a key k_1 of 256 *bit* via the QKD BB84 protocol and a second key k_2 of 256 *bit* via RSA. Now we use both keys as input in Key Derivation Function (KDF), which are functions that allow secrets to be derived from other inputs, with an operation similar to hash functions. The result that we are going to obtain is a new key k_3 of 256 *bit* resulting from the hybridization of k_1 and k_2.

The use of one approach or another has security implications. In a composite system, if one of the components is attacked and turns out to be vulnerable, this can impact the security of the entire system. However, in the event that one of the elements of the hybrid system is proven vulnerable, this does not have to directly imply that the security of the entire system has been compromised. Although this will depend on the specific definition of each cryptosystem.

Whether hybrid or composite systems are considered, three types of combinations can be explored:

- PQC with pre-quantum cryptography;
- QKD with pre-quantum cryptography;
- QKD with PQC.

For a key negotiation scenario, apart from the previous example using a KDF to obtain a hybrid key, the easiest way to combine two schemes is to generate a shared key for each scheme and then calculate an XOR between the shared keys to obtain a shared hybrid key whose robustness is based on the security of both schemes.

In the case of digital signatures, there are various approaches such as the example we have seen before signing using each of the methods and validating each signature independently. But it is also possible to combine the signature schemes to generate a single combined signature algorithm. There are other proposals under study [Bindel et al., 2017], such as first signing a message using one of the methods, and then signing the message and the signature generated by the first scheme with the second scheme that makes up the hybridization. This proposal seems to provide greater security properties than simply signing the same message using the two schemes to be combined.

2.4 Quantum Communication Infrastructures

Quantum cryptography requires a quantum communications infrastructure (QCI) to distribute the qubits.

Throughout the years, when implementing QCI, different strategies have been used, such as the deployment of ad-hoc dark fiber infrastructures for the exclusive use of quantum communications or the integration of quantum technologies such as QKD devices and fiber optics-based quantum links in current communication networks in production, sharing the infrastructure with the classic links. The first strategy optimizes the quantum channel for a better performance, but it implies higher deployment costs and a lower scalability and flexibility of the network. The second strategy is less expensive, more scalable, flexible and manageable, but it can be affected by the noise of the classic communications. A network design to optimize the coexistence of classic and quantum communications drives to a decrease of the quantum channel performance. However, the later approach shows a more realistic choice when it comes to large network deployments, such as those being considered for future QCI. Regardless of the infrastructure deployment strategy (ad-hoc or shared), a QCI is made up of a series of disruptive elements and technologies that increase the security and functionalities compared to current communication networks. In the same way as the current network components, the types of applicable QCI topologies are also independent of the deployment strategy in the sense that all the topologies discussed later in this section are feasible in both cases.

2.4.1 Components of an ideal quantum network

All network management and control processes, synchronization of quantum devices, key distillation processes, classic network elements such as switches, routers, communication channels, servers, etc. are needed. In addition to the elements of a classic network, in order to have a fully equipped QCI, a series of key features shall be included: quantum channels (QC), quantum repeaters (QR), quantum memories (QM) and quantum nodes (QN). This does not mean that it is strictly necessary to have all of these components in order to have an operative QCI, but rather that having all of them at the same time, it is possible to have all the capabilities and functionalities that are expected (today) from these networks and from the future quantum internet, as we will see in chapter 5.

Quantum nodes (QN). Depending on the context in which the quantum nodes are being discussed, they can be understood from different approaches, as shown in Figure 2.9.

- *Approach 1 – Nodes as devices.* In this approach quantum nodes are each of the qubit emitting/receiving devices. In this case, a pair of QKD devices are described as two quantum nodes connected through a quantum channel.
- *Approach 2 – Nodes as locations.* Nodes will be those physical locations that have the capacity to emit and/or receive qubits. In this approach, a quantum node could have more than one emitter/receiver module that connects it with other.
- *Approach 3 – Nodes as relays.* Networks sometimes have intermediate active and/or passive elements that simply relay the quantum resources, switch the signal path or

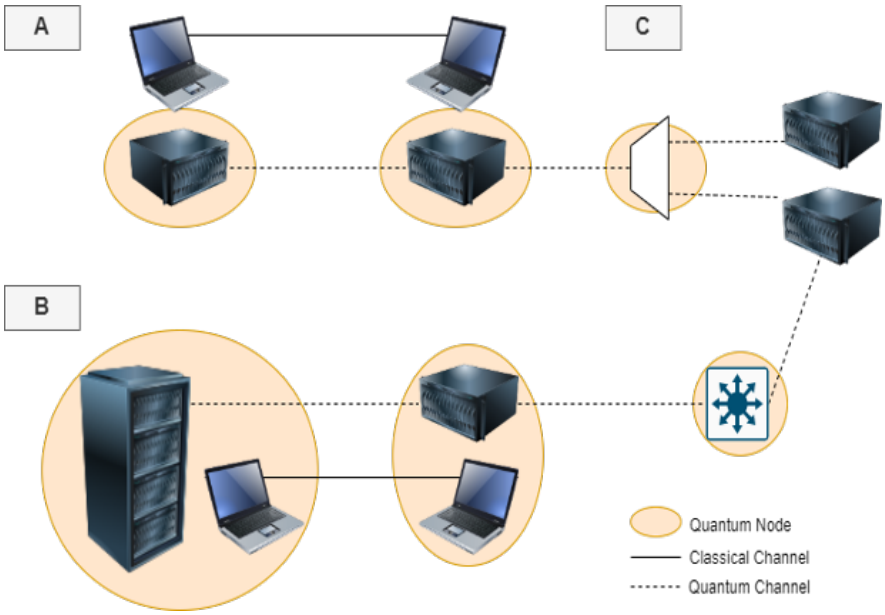


Figure 2.9: Diagram of quantum nodes in the 3 approaches. (A) Approach 1: nodes as devices. (B) Approach 2: nodes as locations. (C) Approach 3 – Nodes as repeaters

(de)multiplex it.

In order to later present the architecture for the integration of different quantum networks, it is also convenient to distinguish a last type of node, which can be included within any of the three previous approaches, called border node or network access [Ciurana, Martínez-Mateo, et al., 2014]. A border node is that node within a network domain that is linked to the border node of a different one, thus enabling the communication between different network domains. From here on we will use approach 2 to refer to the nodes of a quantum network.

Quantum channels (QC). Several transmission media for qubits acting as quantum channels have been explored: optical fibre, open air, space and water. Each of them has its own characteristics. When the transmission of photonic qubits is carried out through optical fiber, the signal loss increases exponentially with distance, but metropolitan distances with losses less than about $30dB$ are within reach using available technology. In this case, quantum channels could - under certain circumstances [A. Aguado et al., 2019] - share infrastructure with classic communications in order to minimize deployment costs and increase the availability of this technology. For its part, free space transmission in metropolitan areas suffers from turbulence and other atmospheric effects [Conrad et al., 2021]. Satellite transmission seems the most optimal option for long-range quantum communications since the qubits would suffer the major disturbance through 10 km of thickness corresponding to the lower atmosphere where the losses are higher, but when entering the space regime, these losses would drop [Y.-A. Chen et al., 2021]. However, this type of channel is not easy to control. Low Earth Orbits (LEO) would have better performance, but the visibility period of the satellite is only a few minutes. Geostationary satellites (GEO) provide 24/7 visibility, but the great distance means more dispersion and requires large telescopes for delivering a better performance. Finally, in recent years feasibility studies have been developed to carry out quantum communications in an

aquatic environment, with the first successful laboratory tests and obtaining promising results [Hufnagel et al., 2019]. Proofs of concept outside the laboratory are currently being planned.

Quantum memories (QM). Normally, in QKD protocols, qubits are received and measured, storing their final classic value (0 or 1). However, in order to store the qubits and ensure that they continue to retain their quantum nature, it is necessary to use so-called quantum memories. This type of memory ingests the photon and assigns it to stationary states of matter, which requires extreme control of the light-matter interaction system. Thus, the way to quantify how good a quantum memory is is in terms of the degree of coupling between light and matter and the degree of coherence of the system [Heshami et al., 2016]. There are different approaches for the development of quantum memories, including solid-state atomic assemblies in rare earth doped crystals, NV centers in diamond, semiconductor quantum dots, trapped individual atoms, cold and room temperature atomic gases, and optical phonons. QM are necessary components to store the entangled qubits in the nodes, preserving their quantum properties to carry out operations (quantum gates) on them in order to transmit the quantum correlations. This is an essential step to support teleportation, a central application for the creation of the non-classic correlation that are the key ingredient to support the new capabilities afforded by a QCI.

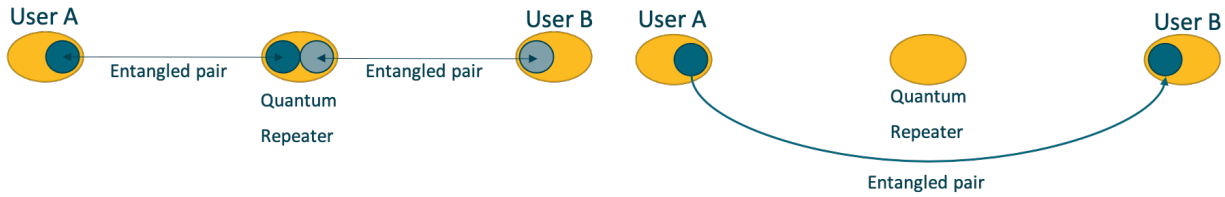


Figure 2.10: Entanglement swapping in a quantum repeater.

Quantum repeaters (QR). The no-cloning theorem implies that qubits cannot be copied, repeated or amplified as classic signals can, and therefore there is a maximum range for direct transmission of qubits. However, this does not rule out the possibility of creating entanglement between two distant locations through intermediate steps, which effectively provides the ability to teleport qubits through entanglement swapping, and thus transmit them, over greater distances. These devices are known as quantum repeaters [Ruihong and Ying, 2019]. Building one is currently a challenge that many research groups are working on since the basic protocol requires the production of entangled pairs in remote locations, their storage in quantum memories to then carry out the correlations. Making a chain of these steps is extremely challenging, especially in the absence of quantum memories with long coherence times and the possibility of performing operations on entangled qubits. Quantum repeaters not only increase distances in quantum communications networks, but by establishing entanglements between two distant nodes, they increase the number of possible new functionalities of a network that do not have a classic equivalent, that is, teleportation. Since today there is no QR fully available, a provisional approach based on trusted nodes has been adopted to reach greater distances in QKD. Trusted nodes are based on the premise that intermediate nodes are trustworthy since the information is decrypted and re-encrypted in those intermediate nodes. In contrast, quantum repeaters do not require the intermediate or repeater nodes to be trusted and, not only they increase the distances in quantum communications, but also, they

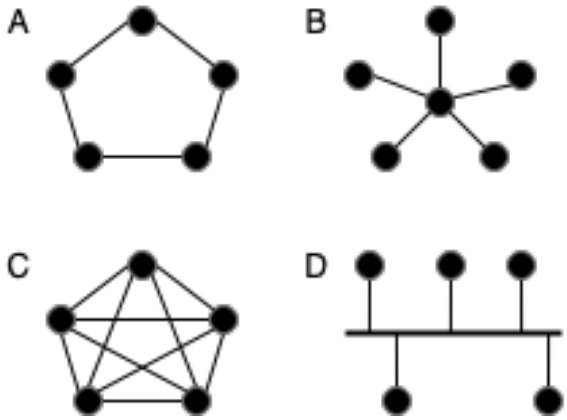


Figure 2.11: Quantum network topologies corresponding to (A) ring, (B) star, (C) mesh and (D) bus.

can establish entanglement between two distant nodes following the entanglement swapping process shown in Figure 2.10.

2.4.2 Network topologies

Although an ideal QCI would be composed of all the elements described in the previous section, the reality is that with the technological maturity level of QR and QM, current networks are related to QKD capabilities deployed and managed in different ways depending on the network architecture, topology chosen and the functionality expected from the network. These components are classic and quantum channels, pairs of QKD modules, optical elements such as switches, Wave-Division Multiplexers (WDM), Time-Division Multiplexers (TDM) or Polarization-Division Multiplexers (PDM) and common passive network components. Quantum networks can be deployed in equivalent topologies to those found in classic networks as shown in Figure 2.11, being each black dot a QN. Thus, to date QCI can be found in ring, star, mesh or bus topology or hybrid configurations of several of these topologies. Being hybrid topologies those made up of a network backbone connecting different subnetworks, each one with its own topology.

As an example, without the need for QR, a quantum network in star topology can be obtained by making use of a passive optical switch as the central element that redirect qubits to any QN applying a one-to-many approach [Woo et al., 2020]. And the absence of QM means that the qubits must be measured upon receiving them, obtaining and storing the classic output.

2.4.3 First deployments and current status of QCI

A review of the most prominent networks deployed worldwide has been carried out, which are summarized in Table 2.1.

Quantum communications have exponentially evolved since the first networks that were deployed. As can be seen in Table 2.1, this evolution has not only been in size but also in key generation rates, detection efficiency, key distillation refinement and performance in

Table 2.1: Historical and current QKD networks and their characteristics. QC: Quantum Channel; D_{Max}: Maximum Distance; KGR: Maximum Key Generation Rate.

Network	QC	Nodes	D_{Max}	KGR_{Max}	Losses
Madrid	Fibre	12	55 km	70 $kbps$	0.2 dB/km
DARPA	Fibre&Air	10	29 km	1 $kbps$	0.2 dB/km
SECOQC	Fibre&Air	6	83 km	11 $kbps$	0.2 dB/km
UQCC	Fibre	6	90 km	304 $kbps$	0.4 dB/km
China	Fibre	32	89 km	250 $kbps$	–
Jinan	Fibre	32	65 km	65 $kbps$	–
Wuhan	Fibre	71	16 km	141 $kbps$	2.2 dB/km
HCW	Fibre	9	85 km	16 $kbps$	0.2 dB/km
Micius (I)	Space	2	1203 km	–	0.16 dB/km
Micius (II)	Fibre&Space	$2 + 107$	4600 km	48 $kbps$	0.08 dB/km

general. The original networks, i.e. DARPA [Elliott, 2018], SECOQC [Peev et al., 2009], UQCC [Sasaki et al., 2011], were ad hoc dark fiber terrestrial deployments that had between 6 and 10 nodes and were capable of generating around 304 $kbps$ over 45 km.

Currently, terrestrial networks have been expanded, mainly in China, deploying between 46 [T.-Y. Chen et al., 2021] and 70 nodes [Y. Zhao, 2019], with similar key rates and maintaining a dark fiber infrastructure model dedicated exclusively to QKD. Due to the proven feasibility of implementing these technologies covering increasingly greater distances, two major challenges have been overcome, opening the doors to real quantum communication network deployments and not just research-oriented networks. The first challenge is the deployment of quantum links using in-production classic communication infrastructures under the Software-Defined Network (SDN) paradigm [A. Aguado et al., 2019], which represents a drastic improvement in terms of implementation costs, increased control over the network and where a greater stabilization of quantum systems was needed, since they have to coexist with classic channels and the unavoidable noise generated without causing the decoherence of the quantum states. The second great challenge has been the launch of Low Earth Orbit (LEO) satellites with a quantum payload allowing two distant ground stations to be connected. This began with feasibility studies and it has already been possible to generate key rates about 48 kbps between two cities located at a distance of 2,600 km, covering a total distance of 4,600 km [Y.-A. Chen et al., 2021]. With this achievement, together with the field tests carried out for transmitting qubits between two distant drones [Conrad et al., 2021], it is possible to begin to consider theoretical architectures and feasibility studies for satellite constellations acting as key relay nodes.

It is clear that the degree of technological maturity has highly increased in terrestrial and spacial quantum communication networks based on fiber optics and LEO satellites, respectively. In addition, the availability of standards from standardization bodies such as ETSI, Institute of Electrical and Electronics Engineers (IEEE) or International Telecommunication Union (ITU), among others, can currently allow the deploy of QKD networks in metropolitan areas to guarantee the security of communications between buildings scattered throughout the city.

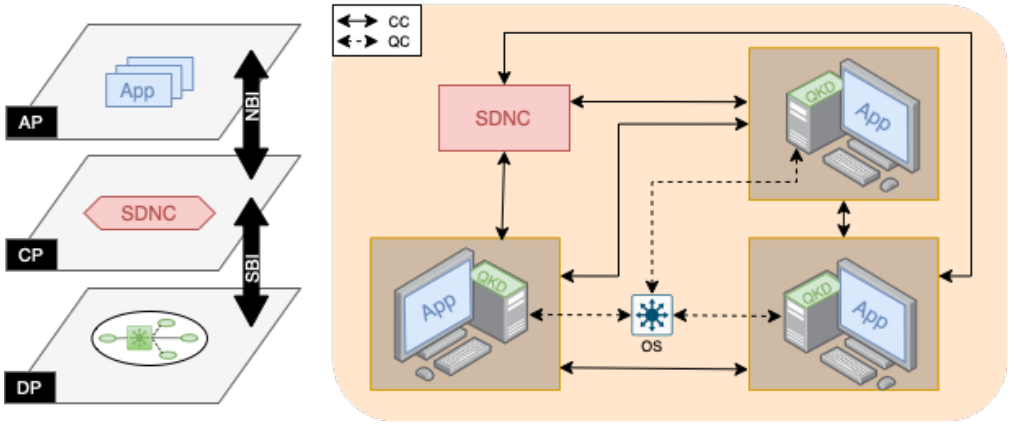


Figure 2.12: SDN quantum network. (Left) Data (DP), control (CP) and application (AP) planes of the SDN model. AP-CP communicate through the North-bound interface (NBI) and CP-DP through the South-bound interface (SBI). (Right) Example of SDN quantum network with three QN in star topology and managed by the Software-defined network controller (SDNC).

QCI based on the Software-Defined Network (SDN) paradigm have been historically implemented and tested in the Spanish network MadQCI [A. Aguado et al., 2019]. In general, SDN facilitates the management of the network, both of the classic and quantum elements, and increases its flexibility and scalability, regardless of the chosen network topology. This approach allows the integration of QKD devices from different providers where, in a trusted node model, each point-to-point link may use a different QKD protocol (BB84, E91, GG02). The components of a quantum network described at the beginning of this section would be located in the lower layer of the model showed in Figure 2.12, together with the classic communication devices such as optical switches (OS) and satellite links to communicate different networks located at long distances. This layer corresponds to the data plane (DP) and it is where all the hardware elements and communication infrastructures are located to carry out the generation of qubits, their detection, processing and storage of the cryptographic keys in the Key Management System (KMS), in addition to classic traffic. It also contains the links between QN through quantum channels (QC), but a classic channel (CC) is also required for synchronization tasks and key distillation processes.

All these elements (classic and quantum) are orchestrated in the upper layer, which is an abstraction layer called the control plane (CP) where the SDN controller (SDNC) acts, in communication with the data plane through the South Bound Interface (SBI). The controller is in charge of collecting service requests from the application plane (management of notifications and requests), collecting the availability status of the intervening elements found in the DP (device and link management), elaborate the entire routing flow to be followed (network topology, routes between applications involved in the connection and security mechanisms) and orchestrate all the processes that have to be carried out to provide the requested service (status management). Although a single controller is capable of managing the entire network, to ensure the network security and resilience it is convenient to have a redundant controller.

Finally, through the North Bound Interface (NBI), the control plane receives the service

requests from the application plane (AP) and provides it with the information necessary to initiate the service between end users. The AP is also provided with cryptographic keys from the KMS whose forwarding module is allocated in the DP to encrypt the communication between end users' applications. This communication is done through the classic channels, whether they are fiber optics or wireless connections. Each quantum node is linked to the SDNC by means of an SDN Agent, which is located between the CP and the AP [ETSI, 2022a]. Since quantum elements are not involved in the AP, the functional and non-functional requirements of this layer as well as the network policies (e.g., access policies) are almost replicable from classic network models, although depending on the QKD key generation rate of the network or its availability in the KMS. In addition to all the applications and services that currently exist in the AP, applications based in QKD-generated keys are added such as Network Function Virtualization (NFV), IPSEC, OPoT, quantum digital signatures (QDS), quantum secret sharing (QSS), quantum teleportation, among others.

The European Telecommunications Standards Institute (ETSI) [ETSI, 2024] has already published a series of standards related to QCI based on SDN, where several specifications and interfaces currently in use are provided. Of particular relevance are the interfaces defined to communicate the key manager with the applications allocated in the AP defined in the ETSI GS QKD 004 [ETSI, 2020] and 014 [ETSI, 2019] standards, the interface between CP and DP defined in the ETSI GS QKD 015 standard [ETSI, 2022a] and the interface between SDNC and a network orchestrator defined in the ETSI GS QKD 018 standard [ETSI, 2022b].

The next steps for the evolution of terrestrial quantum communications networks will be set mainly by the designs that are being carried out under the EuroQCI program [Commission, 2019], which aim to develop a pan-European quantum communication infrastructure, in which they are currently being designed, evolving and deploying national networks in Spain [Spain, 2023], Greece [Greece, 2023], Italy [Italy, 2023], Portugal [Portugal, 2023] among others.

For its part, the European Space Agency (ESA) is also promoting the deployment of satellite links in both LEO and GEO orbits, with projects such as the SAGA (Security And crypto-GrAphic) mission [Agency, 2019] or TeQuantS [Space, 2023] as part of ESA's ARTES 4.0 Core Competitiveness program [Agency, 2024]. Another example is the success of Phase A of definition of the CARAMUEL project in Spain [Agency, 2023] where different technological solutions were analyzed and an architecture was proposed to provide a QKD service between a GEO satellite and a ground station. The investment in these programs and their implications are described in the chapter 5.

2.4.4 Madrid Quantum Communication Infrastructure

The Madrid Quantum Communication Infrastructure was first deployed in 2006 [Lancho et al., 2010] as a point to point network and has been growing and evolving over the years. A network prototype designed to maximize infrastructure sharing in a quantum-only network was built in 2013 [Ciurana, Martínez-Mateo, et al., 2014] at Telefónica's facilities, the Spanish leading telecommunications company. It was subsequently redesigned to show the ability to distribute entangled pairs [Ciurana, Martin, et al., 2014] in 2014. A major step came in 2018 [A. Aguado et al., 2019], when it was installed at Telefónica's production facilities. Today, it

is a metropolitan network based on trusted nodes with 12 nodes distributed among different points of presence located in research centers, companies and universities [e. a. Martin, 2024]. The future evolution of the network is currently under design and development. In the following subsections we will review the highlights of each of the evolution carried out in the MadQCI.

First deployments

The first Spanish quantum communications network, the Madrid quantum network or Madrid Quantum Communication Infrastructure (MadQCI), began in 2006 [Lancho et al., 2010]. The starting point was a network covering a metropolitan area and in which as many quantum channels as possible were integrated into the classic infrastructure. The objective was to analyze the feasibility of establishing a point-to-point connection between two nodes, crossing the entire metropolitan area in a single hop, that is, without the presence of intermediate trusted nodes.

The structure used was the usual one in metropolitan networks (canonical metropolitan optical network), as shown in the diagram in Figure 2.13, and consisted of the following elements:

- A core based on Coarse Wavelength Division Multiplexing (CWDM) for high-speed communications. According to ITU standard [Union, 2003], CWDM is implemented in a spectrum of 18 channels (i.e. 18 different wavelengths) separated by 20 nm and with a central wavelength of 1270 nm.
- Reconfigurable Optical Add-Drop Multiplexer (ROADM) nodes. They are used in networks that employ WDM and are able to aggregate, block, pass or redirect light beams of various wavelengths in a fiber optic network.
- A Gigabit-capable Passive Optical Network (GPON) access network. It is a standard for connecting the Optical Line Termination (OLT) on the core side of the network to the Optical Network Terminal (ONT) on the client side [Union, 2020]. The standard defines a wavelength of 1490 nm for the downstream channel (from OLT to ONT), 1310 nm for the upstream channel (from ONT to OLT), and 1550 nm for analog video transmission. This last channel is the one used as a quantum channel.
- A splitter located between the OLT and the set of ONTs divides the signal between all the ONTs.

Thanks to the fact that this type of network is composed of passive optical elements, the implementation of QKD systems was possible.

Two experiments were carried out in which the complete BB84 protocol was implemented with error correction by LDPC and privacy amplification. Both are indicated in Figure 2.13. The first experiment was crossing nuclei (Experiment 1 in Figure 2.13). For this, two wavelengths were used for the classic signals (1510 and 1470 nm) and a wavelength of 1550 nm for the quantum signal. A key rate of about 500 bps was obtained for a distance of 6 km between the ROADMs. The key rate dropped to 100 bps for a distance of 10 km, which is greater than the distance at which ROADMs are typically placed. The highest value of Quantum Bit Error Rate (QBER) was around 6% and was obtained at 10 km.

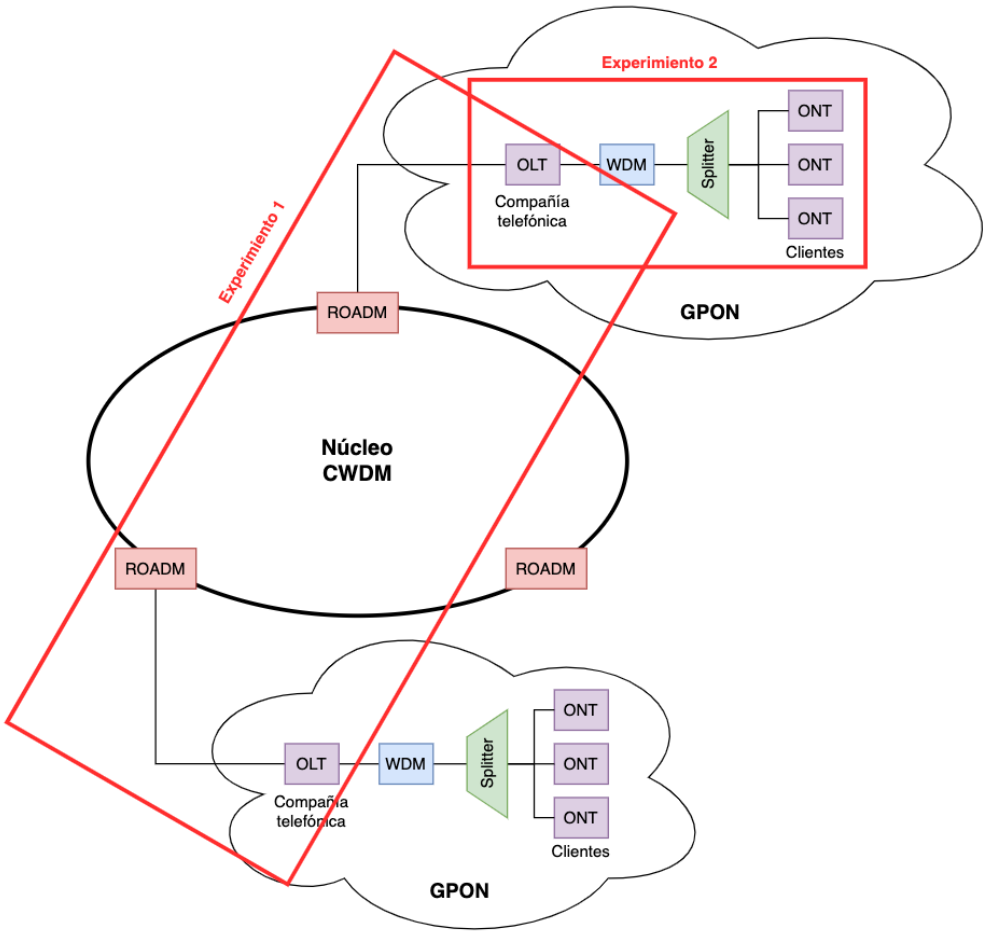


Figure 2.13: Original network topology and first experiments. The first experiment was core crossing (Experiment 1) and the second was Gigabit-capable Passive Optical Network (GPON) crossing (Experiment 2).

The second experiment was GPON crossover (Experiment 2 in Figure 2.13). Again, two wavelengths were used for the classic signals (this time 1490 and 1310 nm) and a wavelength of 1550 nm for the quantum signal. A key rate of about 500 bps was obtained for a back-to-back configuration between the OLT and the splitter. The key rate dropped drastically to 20 bps for a distance of 3.5 km and beyond this distance no secret key could be obtained. Even so, the standard distance at which the OLT and ONT are located is usually 1 or 2 km. It was observed that these results would be easily improved by assigning time slots to the quantum channel through Time Division Multiplexing (TDM) in the GPON.

Even so, the key rates obtained in both scenarios were valid to maintain a more than acceptable AES key renewal rate of 256 $bits$.

These experiments represented a great advance in the field of quantum communications since most of the QKD networks that were being developed (see Table 2.1) at the international level consisted on ad-hoc QKD networks whose implementation required an enormous initial investment. On the contrary, the integration of quantum channels into existing classic

communications infrastructures not only drastically reduced implementation costs, but was also shown to facilitate network scalability, since standard passive optical devices were used for the signal transmission.

In 2008 [Martín, 2021], the research group published an article that describes the security and industrialization requirements that the market demanded for the commercialization of QKD technology.

The Madrid quantum network was rebuilt in 2014 [Ciurana, Martínez-Mateo, et al., 2014] with the main objective of increasing the number of user in the network to be able to execute QKD among them, without focusing as much on the simultaneous emission of classical and quantum signals as occurred in previous experiments. Another objective was to show the ability to distribute entangled pairs [Ciurana, Martin, et al., 2014].

In this case, the typology of the network remained the same as in the previous iteration, that is, a canonical metropolitan optical network architecture composed of a ring-shaped core and a series of accesses. The essential difference is that, in this case, instead of using a GPON approach in accesses with splitters as network components, a WDM-PON approach was chosen, replacing the previous network components by wave division multiplexers (WDM). This modification brought with it great improvements in terms of the losses produced in the network components with the increase in the number of users. That is, for a network with 32 users, the splitter introduced a minimum of 15 dB of losses, while the WDM introduced 3 dB.

Finally, the correct functioning of the network was achieved with 32 users using it simultaneously. Furthermore, these users did not carry out QKD between fixed pairs, but rather were capable of quantum key generation between any two users.

Current State

Since the first proposal of integration of QKD in Software-Defined Networks [e. a. Aguado, 2016], MadQCI was redesign and evolved in 2018 [A. Aguado et al., 2019]. This evolution consists of a hybrid infrastructure where quantum technology and classic communications coexist, and also with QKD devices from different providers integrated into the same network, with some key generation devices based on discrete variables (DV) and others based on continuous variables (CV). It also has switches that can reconfigure the network and can connect, as long as they are compatible, different pairs of emitters / receivers. This integration shows the flexible and scalable nature of the network. The Madrid network consists of 12 nodes, a longest distance between nodes is approximately 55 km. The maximum key rate is 70 $kbps$ and the losses are between 0.2 dB/km and 1.1 dB/km in the worst case (in the center of Madrid, where fiber optics are older and many intermediate points of presence intersect, while still having a continuous quantum channel). This architecture is shown in Figure 2.14. These values are similar to those obtained in other networks (See Table 2.1).

Unlike the other networks, the MadQCI is an Software Defined Network (SDN). The flexibility and programmability of SDN enables the integration of quantum communications into the infrastructure.

This flexibility in MadQCI comes from the implementation of a Quantum Abstraction Interface

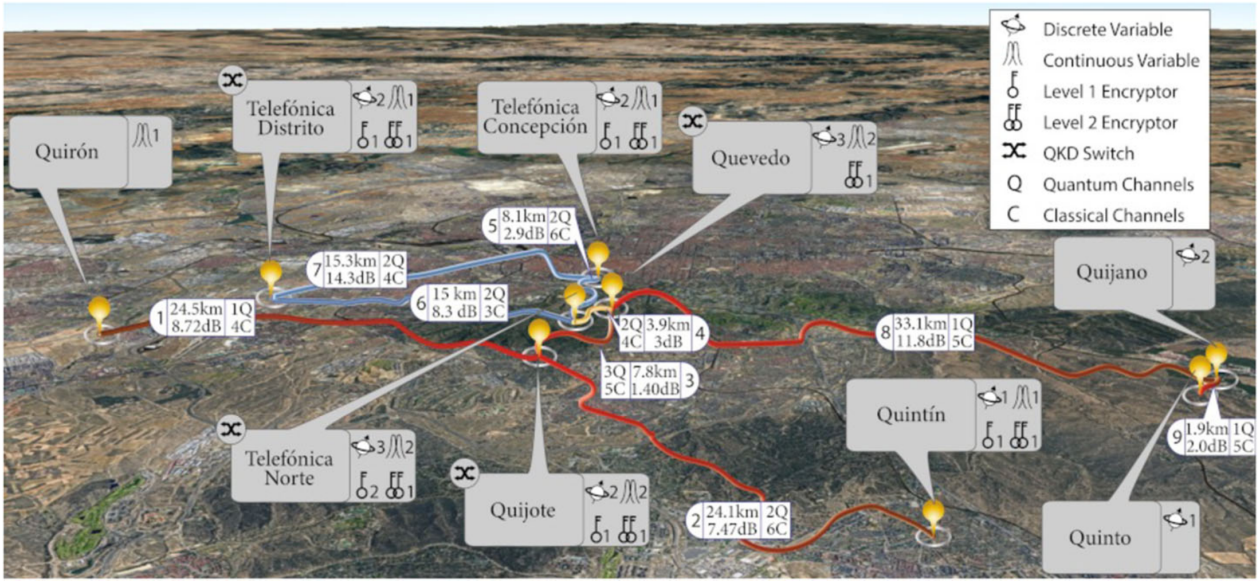


Figure 2.14: Current status of the MadQCI architecture. Source: Nature [e. a. Martin, 2024]

(QuAI) which is a hardware abstraction layer that allows the integration of QKD devices from different vendors on the same network and makes the network vendor agnostic [Mendez et al., 2020]. In addition, an SDN allows to optimize the use of the network and the deployment of services. The level of flexibility and dynamic control over the network provided by the SDN paradigm also facilitates the integration and simultaneous operation of classic and quantum channels. The software stack seamlessly integrates QKD and pre-quantum cryptography into a common infrastructure. All these characteristics make MadQCI a heterogeneous network capable of integrating devices from different commercial brands and suppliers, as well as different quantum and post-quantum cryptographic protocols. Furthermore, the devices currently used in Madrid QCI have different fundamental characteristics at the quantum level, which can provide raw or distilled key to execute QKD and beyond QKD protocols. This versatility increases the functionalities that the network can support. Examples of use cases that have been implemented in the Madrid QCI are Network Functions Virtualization (NFV) based on QKD [A. Aguado, Hugues-Salas, et al., 2017; A. Aguado, Lopez, Martinez-Mateo, et al., 2017], IPSEC [A. Aguado et al., 2018], OPoT [A. Aguado et al., 2020].

To demonstrate a higher level of maturity, MadQCI adheres to existing standards and recommendations [e. a. Martin, 2024]. It already implements approved ones such as ETSI004 [ETSI, 2020], 014 [ETSI, 2019], 015 [ETSI, 2022a] and 018 [ETSI, 2022b], among others. This effort will, in the future, allow communication between the Madrid QCI and other networks either by fiber optics, through the use of trusted nodes or quantum repeaters when available, or via satellite, with the connection of ground stations thousands of kilometers away.

MadQCI is currently in a new redesign and deployment phase as part of the EuroQCI Spain program [Spain, 2023]. The network will be expanded, including new nodes that will connect academic and industrial partners as well as end users. Together with the deployment of a QCI in Barcelona, the Spanish EuroQCI will allow the testing several use cases and new technologies such as free space links or links with entanglement distribution capabilities. In

next phases of the EuroQCI program, the different European cities will be interconnected to create a completely integrated European Quantum Communication Infrastructure. The new network architecture of MadQCI is shown in Figure 2.15 and it is expected to be completed by the second half of 2025.

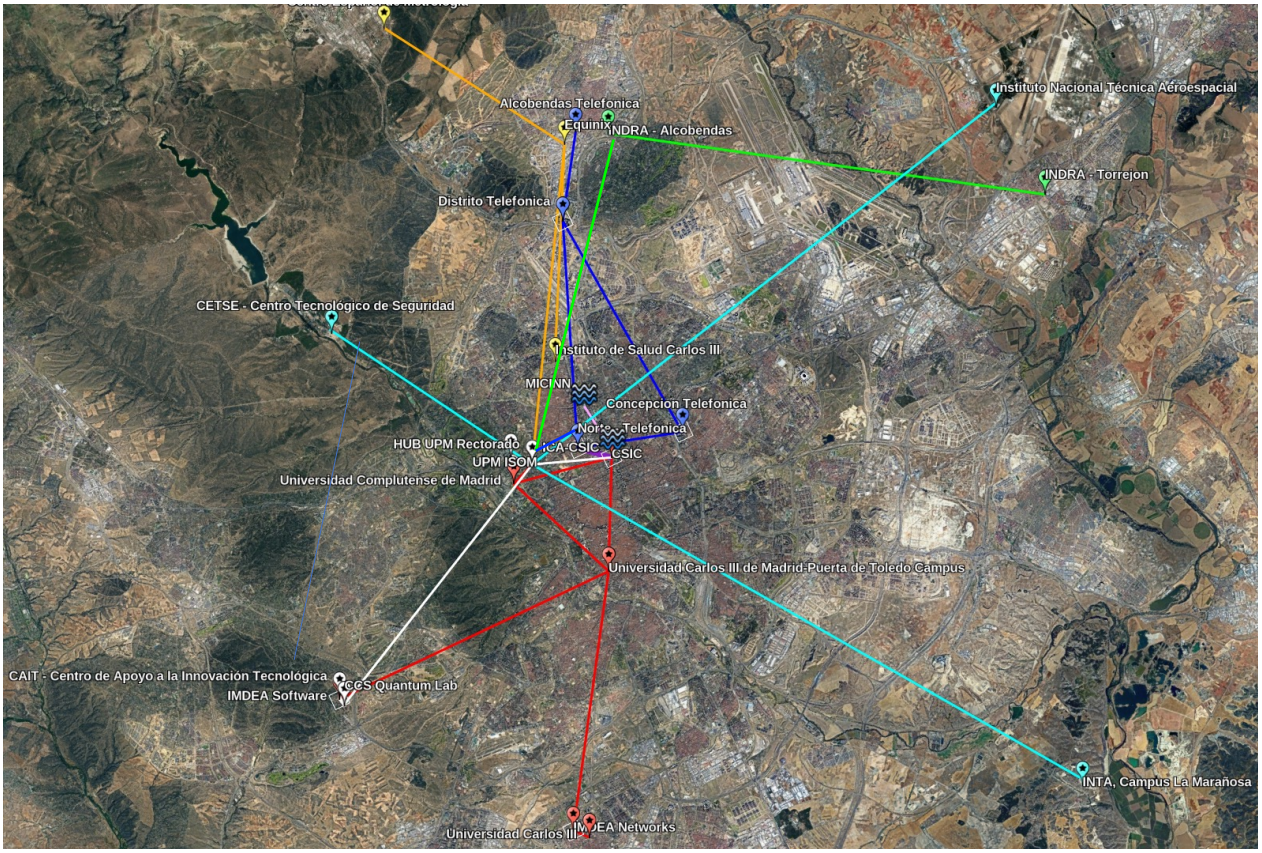


Figure 2.15: MadQCI architecture envisioned for 2025.

Chapter 3

Quantum-assisted Digital Signature Protocol

3.1 Context

Cryptography guarantees the confidentiality, authentication, integrity and non repudiation of transmitted information. There are two major answers within cryptography to ensure these four properties: encryption and digital signature. Encrypting communications ensures the confidentiality of the transmitted information between sender and receiver, that is, that no unauthorized user can extract and understand this information. Meanwhile, digital signature aims to guarantee the identity of the sender of a message, as well as the integrity and non-repudiation of the information sent. The former meaning that the content of the message has not been modified after signing, and the later meaning that the signer can not deny its authorship.

Over the years, a large number of digital signature protocols have been proposed, analyzed and standardized. Examples of digital signature algorithms are Lamport-Diffie's, RSA, El Gamal and signatures based on elliptic curves, among others. Their security is based on one-way functions, i.e. mathematical problems that are easy to calculate in one direction but extremely hard to calculate in the reverse way. A typical example is prime factoring; while is easy to multiply two numbers, it is very difficult to find the prime factors of a large number. These protocols make use of a public-private key system whose security relies in the difficulty of solving such a mathematical problem, i.e. in its computational complexity.

The arrival of the quantum computer, has altered the computational complexity panorama. In particular, the ability to implement Shor's [Shor, 1994] or Grover's [Grover, 1996] algorithms, makes the digital signature algorithms (DSA) vulnerable.

To solve this security challenge, two new cryptographic paradigms have been explored in recent years: quantum cryptography [Cryptography, 1984] and post-quantum cryptography (PQC) [NIST, 2016]. In PQC, cryptographic algorithms based on new mathematical problems are defined, such as lattices, codes, etc. It should be noted that PQC is purely classical, that is, it is not based on any quantum phenomenon, unlike quantum cryptography. PQC schemes

are currently under a standardization process launched by the National Institute of Standards and Technology (NIST) in 2016 [NIST, 2016]. Candidates are selected for both Public-key encryption and Key-encapsulation mechanisms (KEM) and for Digital Signature Algorithms (DSA). At the time of writing this work, NIST has started the standardization of the finalist DSA CRYSTALS-DILITHIUM [NIST, 2024b], FALCON and SPHINCS+ [NIST, 2024c] (the process is expected to be completed in 2024) and, at the same time, a fourth round of the evaluation process has started for the KEM algorithms as well as a Call for Proposals for new DSA. A timeline for the phase-out of the current schemes, based on RSA or ECC was also suggested. However, it is important to note that these new algorithms are demonstrated to be resistant only against a quantum computer running Shor's algorithm, being still unknown what a full-fledged quantum computer might be capable of. It is also important to note that the new algorithms have not been scrutinized so deeply as currently used algorithms, a fact put in sharp evidence during the NIST process, where several algorithms where unexpectedly broken [Beullens, 2022; Castryck and Decru, 2023; Tao et al., 2021].

On the other hand, quantum cryptography uses cryptographic protocols based on quantum mechanical properties. These protocols do not depend on any mathematical problem, but are based on the laws of physics. Consequently, they are resistant to computational attacks and offer a security that does not depend on assumptions on the computational capabilities of the attacker, a fact known as Information Theoretic Security (ITS). The most widely known quantum cryptographic protocols are those used for Quantum Key Distribution (QKD) [Cryptography, 1984], which allow the generation of a random symmetric key between two users by using the quantum properties of photons. Currently, commercial devices are already available to execute QKD protocols, which have been implemented in long-range networks and whose QKD-generated keys have been employed to encrypt transmitted information [e. a. Martin, 2024]. As a drawback, the hardware dedicated to quantum systems requires greater technological maturity to improve their performance and range, several challenges raised related to implementation attacks must be overcome [C. Marquardt, 2023], and the deployments of networks capable of supporting quantum communications require a significant economic investment.

Taking into account the pros and cons of each cryptographic solution, and with the aim of making a transition from classical to quantum-resistant cryptographic systems as easily and smoothly as possible, we focus our research in the development of hybrid cryptographic solutions composing classical functions with quantum protocols that can be implemented with current technology. Specifically, in this chapter we present a quantum-assisted digital signature (Q-DS) based on the composite of symmetric keys generated by QKD with NIST-recommended cryptographic functions, such as SHA2 and SHA3 families.

In the last two decades, several Quantum Digital Signature (QDS) protocols have been proposed. The first QDS was proposed in 2001 [Gottesman and Chuang, 2001] and was based on Lamport's one-way function scheme. This signature scheme has been demonstrated ITS but, despite being a robust QDS, its implementation is currently not possible since it requires the use of long-term quantum memories. In 2014, a QDS scheme was proposed that did not require quantum memories for its implementation since the measurement of quantum states is done upon receiving them [Dunjko et al., 2014]. In this case, the main

disadvantages are the vulnerability to coherent forging attacks. In addition, the presence of spies is not allowed in the analysis which means that the use of secure quantum channels must be guaranteed. Two years later, a new scheme was published whose security no longer depends on the availability of secure quantum channels [Amiri et al., 2016], but on secure classical channels in order to carry out a symmetrization step. In this case, the signer receives and measures the quantum states of the receivers, without carrying out error correction and privacy amplification mechanisms corresponding to the key distillation processes, which are used both for the signature and for the securitization of the classical channels. These types of protocols have certain limitations regarding the maximum length of the message that can be signed, i.e. 1 bit, and the number of participants, which decreases the protocol efficiency as they increase. More recently, in 2021 a scheme was proposed where the symmetrization step [Lu et al., 2021] was removed. With this improvement, the scheme achieves greater execution efficiency, but the limitation regarding the length of the signed message remains the same.

In this chapter, we propose a new quantum-assisted digital signature (Q-DS) protocol implementable with current technology, which simplifies the previous schemes and allows to sign messages with an arbitrary length and for different levels of security. Using symmetric keys generated by QKD as the basis of the scheme, the protocol is built implementing known hash functions and extendable output functions (XOF), with current NIST recommendations, thus providing a highly parametrizable composite system that integrates quantum and classical cryptography. The security of the protocol has been analyzed to demonstrate its robustness against integrity, authenticity and non-repudiation attacks, considering as well the security strength of the classic functions. Then, the Q-DS protocol was implemented and its efficiency analyzed during the key generation, signature generation and signature verification, for several system configurations. In addition, 9 classic DSA and 17 PQC DSA algorithms have also been implemented and a comparative evaluation was carried out taking into consideration all classic, PQC and quantum solutions for different security levels.

3.2 Q-DS Protocol Design

By definition, a digital signature, whether classical or quantum-assisted, must fulfill a series of characteristics:

1. Dependence with the content of the message;
2. Generation using secret information from the sender;
3. Efficiency in the generation and verification processes;
4. Unforgeable and non-repudiable.

These characteristics ensure the properties of authenticity, integrity and non-repudiation that all digital signatures must guarantee. The quantum-assisted digital signature protocol proposed in this work does indeed meet each of these requirements (see Section 3.3).

The general structure of the proposed quantum-assisted digital signature (Q-DS) protocol is divided in two phases. A **distribution phase**, in which Alice establishes secret symmetric keys through quantum key distribution (QKD) processes with all possible receivers. After that,

the receivers exchange between them random elements of those keys. These QKD-generated keys are the foundation of the security in the protocol, since it allows us to remove the asymmetric vulnerable elements of a digital signature and replace them with ITS keys. These keys have the security features provided by QKD systems [Shor and Preskill, 2000]. As already mentioned, it is an ITS key that is not vulnerable to brute force attacks nor does it depend on the solution to a complex mathematical problem, plus no one else knows that key but Bob and Alice, which guarantees its confidentiality, since the knowledge that an eavesdropper can have over the key can be made arbitrarily small. The protocol continues with a **messaging phase** in which Alice generates the digital signature for a given message and sends it to the recipients who verify the validity of both the message and the signature. This second phase involves completely classical procedures and can be carried out some time after the first phase. However, in order to create the digital signature of the message, it is necessary to rely on the secret symmetric keys from the distribution phase, which have been generated by QKD. This is why, although the digital signature production and verification processes are classic, the full protocol is meant to be quantum-assisted. These two phases of the protocol are described in detail in the following subsections, assuming a scenario with three users, one signer (Alice) and two verifiers (Bob and Charlie).

3.2.1 Distribution Phase

The protocol begins with the distribution phase in which Alice and Bob carry out a QKD process, for example the well-known BB84 protocol [Cryptography, 1984]. This protocol is executed and the result is a secret symmetric key k_1 of length l, shared by Alice and Bob.

These same steps are carried out between Alice and Charlie, obtaining at the end of the process a secret symmetric key k_2 of length l.

The keys k_1 and k_2 are divided into n blocks of length $\frac{l}{n}$, as shown in Figure 3.1, and stored. Each block has a fixed labeling $B = \{B1, B2, ..., Bn\}$ which is known by all the users. Once the generation of symmetric keys between pairs is finished, Bob and Charlie carry out a process of exchanging random blocks of key. For that, given S_n as the group of permutations of n elements so that $|S_n| = n!$, we denote the random permutation of n elements $\gamma_j \in S_n$, with $j = \{b, c\}$ as:

$$\gamma_j = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}, \gamma_j(i) = a_i, a_i \in \{1, 2, ..., n\} \tag{3.1}$$

Bob sends to Charlie through a classic authenticated and encrypted channel (for example with other keys generated by QKD) the subset of elements k_1' corresponding to the first $n/2$ indices of B associated to k_1 after applying γ_b. For its part, Charlie sends to Bob the subset of elements k_2' corresponding to the first $n/2$ indices of B associated k_2 after applying γ_c. At no point does Alice know which blocks Bob and Charlie have exchanged. This is a necessary condition so that Alice cannot repudiate the authorship of the message, as we will see later.

The distribution phase does not have to be carried out immediately before the messaging phase, but the users may have generated and stored several keys beforehand to be used later,

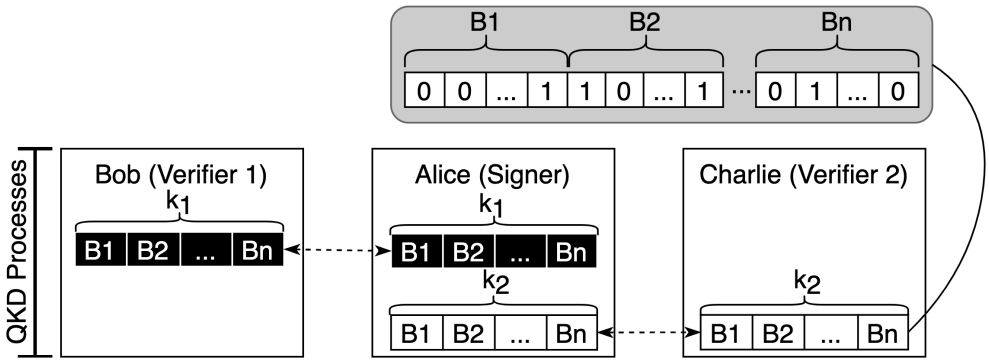


Figure 3.1: Distribution phase of the proposed Quantum-assisted Digital Signature scheme. A Quantum key Distribution protocol is carried out between Alice-Bob and Alice-Charlie to generate symmetric keys k_1 and k_2, respectively. The keys are divided in n blocks for the exchange of random blocks between the verifiers.

as long as the security requirements for the maximum storage time of the keys defined by the users are fulfilled.

3.2.2 Messaging Phase

The messaging phase begins, following the flow shown in Figure 3.2. Alice, the signer, wants to send Bob, the first verifier, a message (m) of any length and its associated signature (S_a). To do so, Alice generates a combined key k_a of length $2l$ by concatenating the secret symmetric key shared with Bob to the secret symmetric key shared with Charlie ($k_a = k_1||k_2$).

The novelty is using a hash function by which takes as input a text of any size (D) and returns a fixed-size digest equal to d. Alice calculates the hash of the message as $h_a = h(m)$. These functions have the property of being one-way functions or preimage resistant since knowing the value of h_a makes it computationally infeasible to extract the value of m, under certain conditions as explained in Section 3.3.

Then, Alice encrypts h_a with the combined secret key k_a using a One-Time Pad (OTP) encryption function, whereby an element-by-element XOR is made between h_a and k_a, obtaining $c_a = ENC_{k_a}(h_a)$. In order to carry out this step h_a and k_a must have the same length, so $2l = d$.

At this point, it is important to remember that k_1 and k_2 were divided into n blocks each (see Figure 3.1), so k_a has $2n$ blocks. And, in turn, c_a will also be made up of $2n$ blocks. As a last step, Alice generates individual hash for each of the blocks of c_a, thus obtaining the signature S_a of length $2l \cdot 2n = 4nl$, associated with her message.

Alice then sends to Bob the (m, S_a) tuple. Once the information is received, Bob starts the signature verification process, which consists in performing the same steps as those performed by Alice for the generation of S_a. Note that in this case, Alice sent the message without encryption, because the objective of this protocol is not confidentiality of the message but authenticity, integrity and non-repudiation. Thus, Bob makes the concatenation of the secret

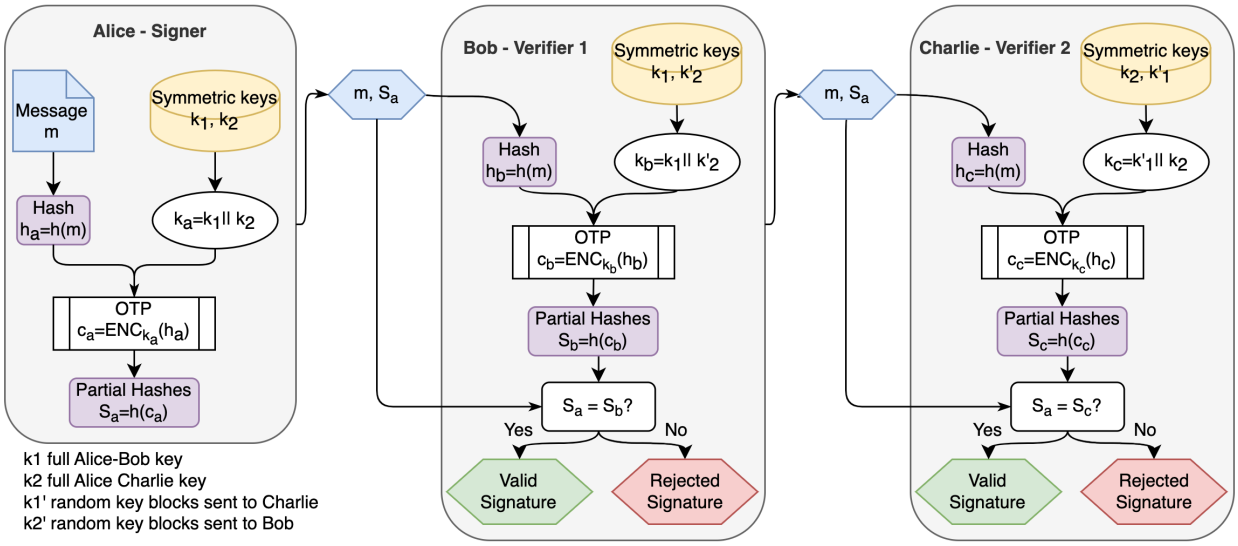


Figure 3.2: Messaging phase of the proposed Quantum-assisted digital signature scheme. Alice generates the signature S_a associated to a message m and sends both to Bob who verifies their validity. Then, the message and the signature is forwarded to Charlie who also verifies them. OTP=One-Time Pad.

symmetric key shared with Alice and the known blocks of Charlie's key ($k_b = k_1||k'_2$). By using the same hash function as Alice, Bob calculates the hash of the message as $h_b = h(m)$ and encrypts h_b with k_b also using an OTP cipher, $c_b = ENC_{k_b}(h_b)$. Finally, Bob generates the hash of each of the blocks of c_b, taking into account that he does not know half of the blocks in c_b that have the same labeling as the unknown blocks in k'_2. Doing this he obtains S_b and compares it with the received S_a in such a way that, if all the known elements match $S_a \approx S_b$, being the number of coincidences above a predefined verification threshold V_B (see Section 3.3.3), Bob accepts the message and the signature as genuine. However, if the number of coincidences is below V_B, $S_a \neq S_b$ and Bob rejects the validity of the message and/or the signature. The signature S_a is approximately equal to S_b but not strictly equal because the information that each of the users has about the keys, $\{k_a, k_b\}$, is different due to the partial exchange of blocks.

For completing the sending chain, Bob forwards the tuple (m, S_a) to Charlie, who performs the same signature verification procedure as Bob:

1. Concatenation of the key shared with Alice and the known blocks of Bob's key ($k_c = k'_1||k_2$);
2. Calculation of the hash of the message as $h_c = h(m)$;
3. OTP Encryption of h_c with k_c getting $c_c = ENC_{k_c}(h_c)$;
4. Generation of the hash of each of the blocks of c_c obtaining S_c;
5. Comparison of S_c with S_a, for a verification threshold V_C:
    - Acceptance of the message and the signature as genuine if $S_a \approx S_c$;

- Rejection of the validity of the message and/or the signature if $S_a \neq S_c$.

3.3 Security Analysis

In this section, the security of the proposed Q-DS protocol is analyzed from different perspectives. For this aim, malicious users will be introduced to verify that the scheme is robust against attacks on message integrity, forgery attempts and message repudiation. The section ends with a study of the security strength of the cryptographic functions that make up the scheme.

3.3.1 Security Against Message Integrity Attack

We are going to validate the robustness of the scheme against the integrity of the message that is sent, that is, if m is modified along the way, this will be detected and the protocol aborted. The entire process is collected in Table 3.1, which sequentially shows the steps followed by each of the users. To do so, we assume the scenario described in Section 3.2 but, in this case, Bob is a malicious player.

It begins with Alice generating the quantum-assisted digital signature with the usual steps indicated in the second column of the table. Bob receives (m, S_a) from Alice and verifies and accepts the received signature as shown in the third column of Table 3.1. After that, he modifies the message $m \to M$, but keeping the signature generated by Alice S_a. Bob sends to Charlie the tuple (M, S_a), with the modified message. Upon receiving it, Charlie performs the verification process as shown in the fourth column of the table and at the end of the process detects that $S_c \neq S_a$, so he rejects the signature and the message.

Table 3.1: Q-DS protocol with a message integrity attack. Alice generates (m, S_a) and Bob verifies and accepts it. Bob sends to Charlie a modified message M along with Alice's original signature. Charlie detects that $S_c \neq S_a$ and rejects the signature and the message.

	Alice	Bob	Charlie	Parameters Comparison
Initial data	m, k_1, k_2	M, k_1, k_2'	k_1', k_2	–
Step 1	$k_a = k_1 \|\| k_2$	$k_b = k_1 \|\| k_2'$	$k_c = k_1' \|\| k_2$	$k_a \approx k_b \approx k_c$
Step 2	$h_a = h(m)$	$h_b = h(m)$	$h_c = h(M)$	$h_a = h_b \neq h_c$
Step 3	$c_a = ENC_{k_a}(h_a)$	$c_b = ENC_{k_b}(h_b)$	$c_c = ENC_{k_c}(h_c)$	$c_a \approx c_b \neq c_c$
Step 4	$S_a = h_p(c_a)$	$S_b = h_p(c_b)$	$S_c = h_p(c_c)$	$S_a \approx S_b \neq S_c$
Verification	–	Accepted	Rejected	–

The fifth column in Table 3.1 compares step by step the parameters generated by each of the users during their turn and indicates the inequalities produced by the malicious Bob that lead to the final rejection of (m, S_a). Note that in this case, Charlie cannot distinguish whether the reason for the negative verification test was an attack on the integrity of the message or a forgery attempt of the signature.

In a scenario in which all users are honest, when doing the parameter comparison all of them would be strictly equal (h_x) or approximately equal (k_x, c_x, S_x), respectively (due to the unknown elements of k_1 and k_2 by Charlie and Bob). But, in this case, modifying the message causes the first alteration in the calculation of the message hash. Since the calculation of S_a and S_c depends on the value of c_a and c_c, respectively, and these depend on the value of h_a and h_c, the alteration produced by the change of message is propagated along the entire chain, triggering an error in Charlie's verification test.

In order to succeed in an attack on the integrity of the message, Bob would have to be able to find a second preimage of the hash value that is, from the given message digest of m, $h(m)$, finding a different input M that provides the same hash value $h(M) = h(m)$. A second preimage attack can also be prevented applying the conditions defined in section 3.3.4.

3.3.2 Security Against Signature Forgery Attack

In this scenario, Bob is once again a malicious player. As in the integrity test, Table 3.2 shows Bob's attempted forgery of Alice's signature. As before, the second column shows the generation of the signature S_a by Alice and the third column indicates the steps taken by Bob for the verification and subsequent acceptance of the message and the signature.

Table 3.2: Q-DS protocol with a message and signature forgery attack. Alice generates (m, S_a) and Bob verifies and accepts it. Bob forges Alice's signature and sends Charlie the modified message M and the forged signature S_f. Charlie detects that $S_c \neq S_f$ and rejects the signature and the message.

	Alice	Bob		Charlie	Param. Comp.
		Verification	Forgery		
Init. data	m, k_1, k_2	M, k_1, k_2', K		k_1', k_2	–
Step 1	$k_a = k_1 \| \| k_2$	$k_b = k_1 \| \| k_2'$	$k_f = k_1 \| \| K$	$k_c = k_1' \| \| k_2$	$k_a \approx k_b \approx k_c \neq k_f$
Step 2	$h_a = h(m)$	$h_b = h(m)$	$h_f = h(M)$	$h_c = h(M)$	$h_a = h_b \neq h_f = h_c$
Step 3	$c_a = ENC_{k_a}(h_a)$	$c_b = ENC_{k_b}(h_b)$	$c_f = ENC_{k_f}(h_f)$	$c_c = ENC_{k_c}(h_c)$	$c_a \approx c_b \neq c_c \neq c_f$
Step 4	$S_a = h_p(c_a)$	$S_b = h_p(c_b)$	$S_f = h_p(c_f)$	$S_c = h_p(c_c)$	$S_a \approx S_b \neq S_c \neq S_f$
Verif.	–	Accepted	–	Rejected	–

In this case, the fourth column shows how Bob generates a fake digital signature S_f, associated to the tampered message M. As it can be seen, the signature generation process is the same as Alice's, except that Bob does not know the 50% of Charlie's key k_2, so the key $K \neq k_2$ used to generate k_f will produce the alteration shown in the comparison of parameters in the sixth column. This alteration will propagate through all the steps of the Charlie verification test and will result in $S_f \neq S_c$, and the message and signature rejected.

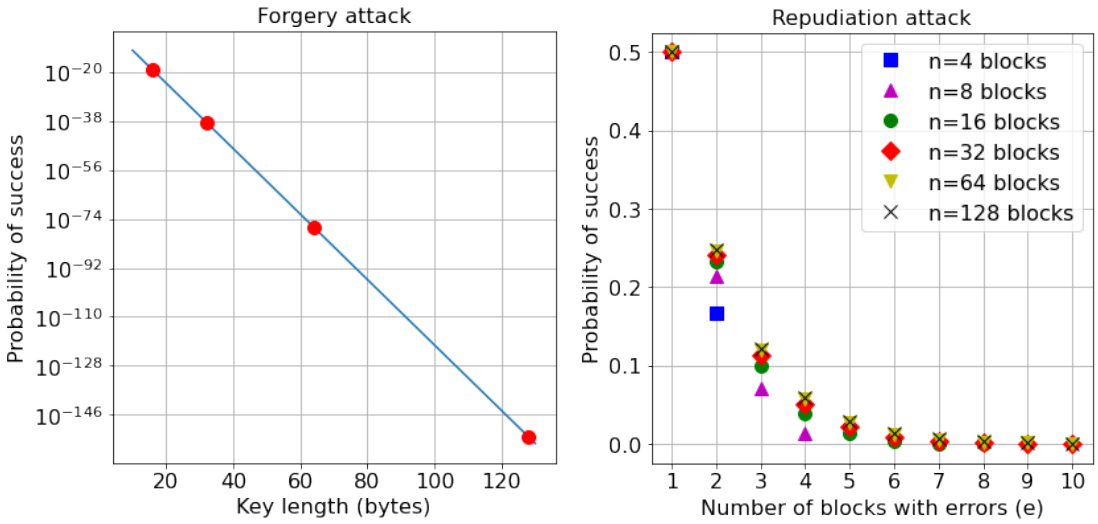


Figure 3.3: (Left) Probability for Bob to succeed in a forgery attack as a function of the number of blocks (n) and their length (L) when a SHAKE-256($m, \delta = 1024$) function is chosen. (Right) Probability for Alice to succeed in a repudiation attack as a function of the number of blocks with errors (e) and the configuration of the number of blocks that is dependent on the choice of the hash function.

In order to successfully forge the signature, Bob would have to be able to guess the unknown elements of k_2. To do this, he could:

1. Guess the unknown bits of k_2. Due to the randomness of the QKD-generated key, he has a 50% chance of matching the value of each bit. If he has to guess $0.5l$ bits, where l is the length of k_2, the probability that all his guesses are correct is $\frac{1}{2^{l/2}}$. Therefore, P_{guess} will be smaller the larger the length of the key and the smaller the number of defined blocks, as plotted in Figure 3.3-left using a SHAKE-256($m, \delta = 1024$) function on k_1 and k_2.

2. Extract the unknown elements of k_2 from the signature S_a. If block hashes were not done in the last step of signature generation, Bob could compare c_c and c_a, and extract the remaining k_2 elements simply by undoing the OTP cipher. But, block hashes of certain size prevent him from accessing the full value of c_a and therefore the keys from being extracted.

3. Find a preimage, that is, given a hash value H, identifying the input message m that provides $h(m) = H$. These kind of attacks are mainly done by brute force but can be prevented by taking into account a series of security parameters and requirements in the choice of hash functions and the input length, as it is explained in section 3.3.4.

3.3.3 Security Against Repudiation Attack

Finally, we assume a scenario where Alice is the malicious player whose goal is to generate a signature that Bob accepts but Charlie rejects, thus denying authorship of her message.

The steps followed by each of the users in this scenario are shown in Table 3.3. Before starting the process, Alice is aware that Bob only knows half of Charlie's key k_2, but she has no clue about which elements Bob knows. For Bob to accept the signature and Charlie to reject it, Alice is going to concatenate Bob's and Charlie's keys as usual, but introducing some errors in random bits of k_2, so that $k_2 \rightarrow K$. For the strategy to be successful, Alice has to ensure that 100% of the errors introduced are in the elements of k_2 that Bob does not know about. Otherwise, Bob detects that $S_a \neq S_b$, as shown in the third column of the table, rejects the validity of the signature and aborts the protocol.

Table 3.3: Q-DS protocol with a repudiation attempt. Alice generates (m, S_a) introducing some errors in k_2 and sends it to Bob. Bob performs the verification test and detects that $S_b \neq S_a$, so he rejects the signature and the message and aborts the protocol.

	Alice	Bob	Charlie	Parameters Comparison
Initial data	m, k_1, k_2, K	k_1, k_2'	k_1', k_2	–
Step 1	$k_a = k_1 \| \| K$	$k_b = k_1 \| \| k_2'$	–	$k_a \neq k_b$
Step 2	$h_a = h(m)$	$h_b = h(m)$	–	$h_a = h_b$
Step 3	$c_a = ENC_{k_a}(h_a)$	$c_b = ENC_{k_b}(h_b)$	–	$c_a \neq c_b$
Step 4	$S_a = h_p(c_a)$	$S_b = h_p(c_b)$	–	$S_a \neq S_b$
Verification	–	Rejected	Aborted	–

The probability for Alice to introduce all the errors in the unknown blocks by Bob depends on the total number of blocks and the number of blocks where introduce errors. If she introduces errors in 1 of the blocks ($e = 1$) the probability of success will be $\frac{n/2}{n} = 0.5$, which is independent of n, the number of blocks. The probability that Alice introduces errors in the blocks unknown to Bob is given by:

$$P_{rep} = \prod_{i=0}^{e-1} \frac{n-2i}{2(n-i)} \tag{3.2}$$

As an example, for $e = 7$, for a scheme of 32 blocks, the probability that Alice will succeed in making a repudiation attack is 0.34%. Then, the more blocks with errors Alice introduces, the lower the probability of success, as plotted in Figure 3.3-right. Based on that, Bob and Charlie can define thresholds of permissible errors or verification thresholds V_B and V_C, above which $S_a \neq S_b, S_c$, forcing Alice to introduce a greater number of error and, thus, decreasing her probability of success.

3.3.4 Security Strength Analysis

So far we have analyzed the security of our proposed quantum-assisted digital signature scheme against attacks on the integrity of the signed message, falsification of the identity of the signer and attempts to repudiate the message by the author. In this final part, we analyze the security strength of the scheme in terms of its cryptographic functions. We ensure that the protocol is as secure as the most vulnerable of its elements: the secret keys, the hash

function used on the message, the OTP encryption and the hash function used on the blocks (partial hashes) - in case it differs from initial hash function.

Both the QKD-generated keys and the OTP encryption are classified, under certain conditions, as Information-Theoretic Secure (ITS) [Shor and Preskill, 2000] and, therefore, conform to perfect secrecy as far as each key is only used once. Therefore, the most vulnerable elements are the hash functions. A priori, the hash functions applied to the message and to the blocks are considered secure as long as one of the approved hash functions defined in the NIST FIPS 180-4 [NIST, 2015a] or NIST FIPS 202 [NIST, 2015b] standards is used (see Table 3.4), with the exception of the SHA-1 function, which is not longer recommended by the NIST.

Table 3.4: Strength of NIST-approved hash functions [NIST, 2015b]. CR=Collision Resistance, PR=Preimage Resistance, 2PR=Second Preimage Resistance.

	CR (bits)	PR (bits)	2PR (bits)
SHA2-224	112	224	201-224
SHA2-256	128	256	201-256
SHA2-384	192	384	384
SHA2-512	256	512	394-512
SHA3-224	112	224	224
SHA3-256	128	256	256
SHA3-384	192	384	384
SHA3-512	256	512	512
SHAKE-128	$min(\delta/2, 128)$	$\geq min(\delta, 128)$	$min(\delta, 128)$
SHAKE-256	$min(\delta/2, 256)$	$\geq min(\delta, 256)$	$min(\delta, 256)$

Table 3.4 lists four of the NIST-approved hash functions from the SHA-2 family and from the SHA-3 family and their strength measured in bits against collisions (CR), preimage (PR), and second preimage (2PR) [NIST, 2015b]. In section 3.3.2, we saw the difference between preimage and second preimage attacks. For its part, a collision attack means finding any two messages m and M, being $M \neq m$, such that $h(M) = h(m)$. The difference between collision and second preimage is that in the later the malicious user can be unaware of the content of m if, for example, if it is encrypted. The security strength of a hash function is determined by the lowest of the CR, PR and 2PR strengths. Our Q-DS protocol needs Collision, Preimage and Second preimage resistance, so the security strength is set by CR for all SHA functions. As it can be seen, the functions with the greatest security strength are SHA-512 and SHA-384.

Collision resistance.

The collision resistance depends directly on the space of possible inputs I which has a size l_i and the space of possible output hash values O of size l_o, and can be calculated as follows [Peyravian et al., 1998]:

$$P_{col} = 1 - exp\left[-\frac{(2^x + 1)^2}{2(2^k + 1 - 2^x)}\right] \tag{3.3}$$

Where x is the length in bits of the input message which defines the size of I as $l_i = 2^x$, k is the length of the message digest and defines the size of O as $l_o = 2^k$. For the SHA2-224 function $k = 224$ bits, for SHA2-256 function $k = 256$ bits, etc. Above the thresholds defined in Table 3.4, the probability that there are any two messages $m \neq M$ that produce a collision is different from zero. As an example, the amount of work needed to find a collision for SHA2-256 is 2^{128}.

Second preimage resistance.

As we have seen above, for Bob to successfully carry out a message integrity attack he has to be able to find another M message such that $h(M) = h(m)$. The calculation of second preimage resistance for SHA2-224, SHA2-256 and SHA2-512 functions, collected in Table 3.4, is given by:

$$2PR = d - log_2 (D/B) \tag{3.4}$$

Where d is the size of the hash output, D is the size of the input message in bits and B is the input block size of the function. In the case of SHA2-384, the security strength does not depend on the size of the input message, so its resistance to second preimage is given by $d = 384$. This value allows us to obtain the amount of work required to find a second preimage, which is 2^{384}.

Preimage resistance.

The most favorable alternative for Bob to forge the signature is to try to find the preimage of each of the unknown key blocks. These types of attacks can be carried out by brute force if the input block size is small enough. As an example, if the block size is 4 bits, it would only take 2^4 tries to find the value of the block. It is also possible to attack using more efficient methods such as rainbow tables.

For this reason, we have to find the optimal balance between having as many blocks as possible to reduce P_{rep}, and having the size of each block large enough to be secure against a dictionary attack. In this sense, the use of an extendable-output function (XOF) SHAKE from the SHA-3 family is proposed (see Table 3.4), prior to the key-blocks exchange between Bob and Charlie during the distribution phase. This type of functions allows, given an input and a variable δ parameter, to securely extend the length of the input up to δ bits [NIST, 2015b]. If Alice, Bob and Charlie carry out this operation in k_1 and k_2, prior to the block division, they can increase $l \rightarrow \delta$. To maintain the requirement that $2l = d$, this operation can be done directly on the message, modifying its size from $D \rightarrow 2\delta$. As a consequence, the security against dictionary attacks is improved and, furthermore, Bob and Charlie do not exchange plane key blocks but the blocks resulting from the XOFs, which increases the privacy of k_1 and k_2.

From this analysis we obtain as an example that, if SHAKE-256$(m, \delta = 2048)$ is implemented to generate the message hash in the Q-DS protocol, it gives $CR = 256$, $PR = 256$ and $2PR = 256$. We suppose that k_1 and k_2 are $l = 256$. A SHAKE-256 is applied to k_1 and k_2, with $\delta = 1024$. For $n = 32$ blocks, the size of each block is 64 bits. Given these values, the amount of work needed to find a preimage is 2^{64}. According to these values, if Bob sets a

verification thresholds of $V_B = 25\%$ (maximum number of blocks known to Bob, $n = 16$, with errors, $e = 4$), then the probability of Alice succeeding in a repudiation attack is $P_{rep} = 0.05$ (see Figure 3.3).

Finally, when choosing a proper hash function for the blocks, it could be interesting to consider the SHA2-256 function due to performance reasons, since it already is a function supported by Intel's native instructions.

We conclude the security analysis of the protocol with a brief mention of Denial of Service (DoS) attacks. Any malicious user could simply send wrong information about their key shared with Alice to the rest of users, causing them to reject the signature. Dealing with this issue involves increasing security thresholds, which leads to increasing some of the probabilities of the security analysis.

3.4 Implementation

In this work, three different types of solutions for DSA have been implemented and analyzed: Classical, Post-quantum and Quantum-assisted digital signatures.

The study has been carried out under the Digest and Sign paradigm, whereby before signing a message it is hashed and the message digest is signed afterwards. This is a standard technique used for singing procedures on most applications. The digital signature algorithms evaluated are those listed in Table 3.5, where it is also indicated to what type of cryptographic solution they belong to, i.e. quantum, classic or post-quantum, and the security level. A more detailed description of the classic algorithms used today and the PQC DSA that are being standardized by NIST are provided in the following subsections.

The classic digital signature algorithms that have been selected are those most widely implemented in current systems, that is, Elliptic Curves (ECDSA and EDDSA) and RSA. RSA cryptosystem is based upon the mathematical problem of factoring integers as product of primes (particularly, RSA uses modules formed by the product of 2 primes). Meanwhile, Elliptic Curve Cryptography is based on another longstanding mathematical problem, the discrete logarithm problem over certain structures, allowing the achievement of the same security levels as RSA cryptosystems with smaller cryptographic sizes and performance constrains. Two ECC paradigms for Digital Signatures are evaluated, ECDSA and EDDSA, differing primarily on the elliptic curve equation considered: ECDSA uses Montgomery form equations, while EDDSA uses Edwards form equations. Also, ECDSA is the elliptic curve variation of the DSA cryptosystem, while EDDSA follows the Schnorr signature paradigm. This provides a great number of security variants between them.

For its part, the PQC digital signature algorithms correspond to those that are being standardized by NIST, which are CRYSTALS-Dilithium under the FIPS 204 standard [NIST, 2024b], SPHINCS+ under the FIPS 205 standard [NIST, 2024c] and FALCON, whose standard will be published in 2024. CRYSTALS-Dilithium, selected as first choice for Post-Quantum DSA, and FALCON, are both lattice-based cryptographic schemes. Specifically, their security is closely tied to presumably hard problems over lattices like the Closest Vector Problem (CVP) or the Shortest Vector Problem (SVP). Their mathematical construction follows in

both cases the 'structured lattices' approach, which means that additional structure is used on the mathematical objects used for the definition of the scheme. While this paradigm allows for smaller key and signature generation, it does provide with an additional source of information that could be potentially turned into practical attacks. Most lattice-based proposals nowadays follow this practice. In turn, SPHINCS+ is based on the symmetric-based post-quantum paradigm, which consists on defining schemes whose security relies on cryptographic symmetric primitives. Specifically, SPHINCS+ is based on a number of symmetric-based constructions, like Few Time Signatures and Merkle trees. Due to its construction, the general scheme can be instantiated with a number of different cryptographic primitives, provided they all provide similar cryptographic requirements. The FIPS 205 draft considers 2 hash-based instances, SHA2 and SHAKE. This scheme can be highly parameterized, having 3 tuples of tuning parameters: the underlying hash function used, the 'robust' vs 'simple' selection (FIPS 205 draft only considers 'simple' variants) and the 'fast' vs 'small' selection, which allows to choose between faster variants or variants which generate smaller signatures.

The Q-DS protocol has been implemented using *C++* language integrating OpenSSL libraries. The system was built and run in an Oracle VM VirtualBox Ubuntu 64 bit with an 11th Gen Intel(R) Core(TM) i7-1185G7 processor. For the key generation, a pair of CLAVIS ID Quantique discrete variable QKD devices has been used in a back-to-back setup, with a security parameter of $\epsilon = 10^{-9}$. The QKD protocol used is a decoy states BB84 composed by one signal, μ_0, and two decoy states, $\{\mu_1, \mu_2\}$, with intensities $\{0.45, 0.225, 0\}$ and probabilities $\{0.2, 0.6, 0.2\}$, respectively. The classic and post-quantum algorithms have been benchmarked using the OpenSSL generic interface, and the Post-Quantum implementation provided by the Open Quantum Safe (OQS) project [Project, 2022].

The Q-DS protocol is divided in three functions, *KeyGen*, *SigGen* and *SigVer*, and is highly parametrizable in terms of message length, hash function to be applied on the message, key length, number of blocks and hash function to be applied on the blocks. Depending on the parameters chosen the system will provide a specific security level and probabilities of a malicious player to succeed in a forgery or repudiation attack, as specified in section 3.3.

These probabilities, as shown in Figure 3.3, can be minimized by increasing the key length l_k, the number blocks n and defining a verification threshold T_v that will force Alice to introduce a greater number of errors, decreasing P_{rep}. Since an increase in the previous parameters will decrease the efficiency of the protocol, the selection of $\{l_k, n, T_v\}$ can also be optimized to guaranty the security of the protocol while maintaining a high performance. In addition, to compare the Q-DS protocol with the classic and PQC solutions from Table 3.5, different combinations of parameters need to be set to achieve comparable security strengths. In general, it is recommended the use of $l_k \geq 256B$, $n \geq 16$ and $T_v \geq 4$.

It should be also noted that, even though this protocol has been analyzed for three users, only the implementation of a signer (Alice) and a verifier (Bob) is required to carry out the analysis of *SigGen* and *SigVer* functions. This is due to two main reasons. The first is that the process for the second verifier is equivalent to that of the first. The second reason is because whenever the messaging phase takes place Bob's verification process is independent from Charlie's.

Table 3.5: Digital Signature Algorithms (DSA) implemented. CC=Classic Cryptography, PQC=Post-Quantum Cryptography, QC=Quantum Cryptography.

	Type	DSA	Security (bit)
CC	ECC	BrainpoolP256r1	128
CC	ECC	BrainpoolP384r1	192
CC	ECC	BrainpoolP512r1	256
CC	ECC	Secp256v1	128
CC	ECC	Secp384r1	192
CC	ECC	Secp521r1	256
CC	ED	ED25519	128
CC	ED	ED448	224
CC	RSA	RSA15360	256
PQC	CRYSTALS-Dilithium	Dilithium2	128
PQC	CRYSTALS-Dilithium	Dilithium3	192
PQC	CRYSTALS-Dilithium	Dilithium5	256
PQC	FALCON	Falcon512	128
PQC	FALCON	Falcon1024	256
PQC	SPHINCS+	sphincssha2128fsimple	128
PQC	SPHINCS+	sphincssha2128ssimple	128
PQC	SPHINCS+	sphincssha2192fsimple	192
PQC	SPHINCS+	sphincssha2192ssimple	192
PQC	SPHINCS+	sphincssha2256fsimple	256
PQC	SPHINCS+	sphincssha2256ssimple	256
PQC	SPHINCS+	sphincsshake128fsimple	128
PQC	SPHINCS+	sphincsshake128ssimple	128
PQC	SPHINCS+	sphincsshake192fsimple	192
PQC	SPHINCS+	sphincsshake192ssimple	192
PQC	SPHINCS+	sphincsshake256fsimple	256
PQC	SPHINCS+	sphincsshake256ssimple	256
QC	Q-DS	QKD+XOF	128
QC	Q-DS	QKD+XOF	256

As a first step, we have analyzed the behaviour of the Q-DS protocol individually. As mentioned earlier, the parameters that can be modified are the message and the key lengths, the number of blocks, the hash applied to the message and to the blocks, since it migth differ, and the security threshold. Different aspects have been explored such as the impact in the key generation, signature generation and signature verification performances with the increase in the message length, the key length and the number of blocks. For this aim, the protocol parameters have been set as shown in Table 3.6. The hash functions applied to the message and the blocks is SHAKE256 in all cases.

Table 3.6: Settings of the Q-DS protocol for the analysis of the key generation, signature generation and signature verification performances when increasing the message length l_m, the key length l_k and the number of blocks n. δ_m and δ_B are the output length of the previous hashes, and L_S is the signature length, and the security strength in bits. The hash functions applied to the message and the blocks is SHAKE256 in all cases.

Iter.	$l_m(B)$	$\delta_m(B)$	$\delta_B(B)$	n	$l_k(B)$	$L_S(B)$	Sec. (bit).
Impact of message size							
100000	1	512	64	16	256	2048	128
100000	10	512	64	16	256	2048	128
100000	10^2	512	64	16	256	2048	128
100000	10^3	512	64	16	256	2048	128
100000	10^4	512	64	16	256	2048	128
100000	10^5	512	64	16	256	2048	128
100000	10^6	512	64	16	256	2048	128
Impact of number of blocks							
100000	10^4	2048	64	16	1024	2048	256
100000	10^4	2048	64	32	1024	4096	256
100000	10^4	2048	64	64	1024	8192	128
Impact of key length							
100000	10^4	512	64	16	256	2048	128
100000	10^4	1024	64	16	512	2048	256
100000	10^4	2048	64	16	1024	2048	256
100000	10^4	4096	64	16	2048	2048	256

In order to carry out a comparison of the different algorithms, common parameters have been set in all of them, as presented in Table 3.7, such as the length of the message, the hash function to calculate the message digest and the output length of the message digest. Also, as shown in Table 3.5, the security level of each algorithm has been taken into account and will allows us to compare related solutions.

Table 3.7: Common parameters for the execution of the algorithms.

Parameters	
Message length	$m = 10\ kB$
Hash Function	$SHAKE256(m, \delta_m)$
Message Digest length	$\delta_m = 512\ B$ (RSA: 256 B)

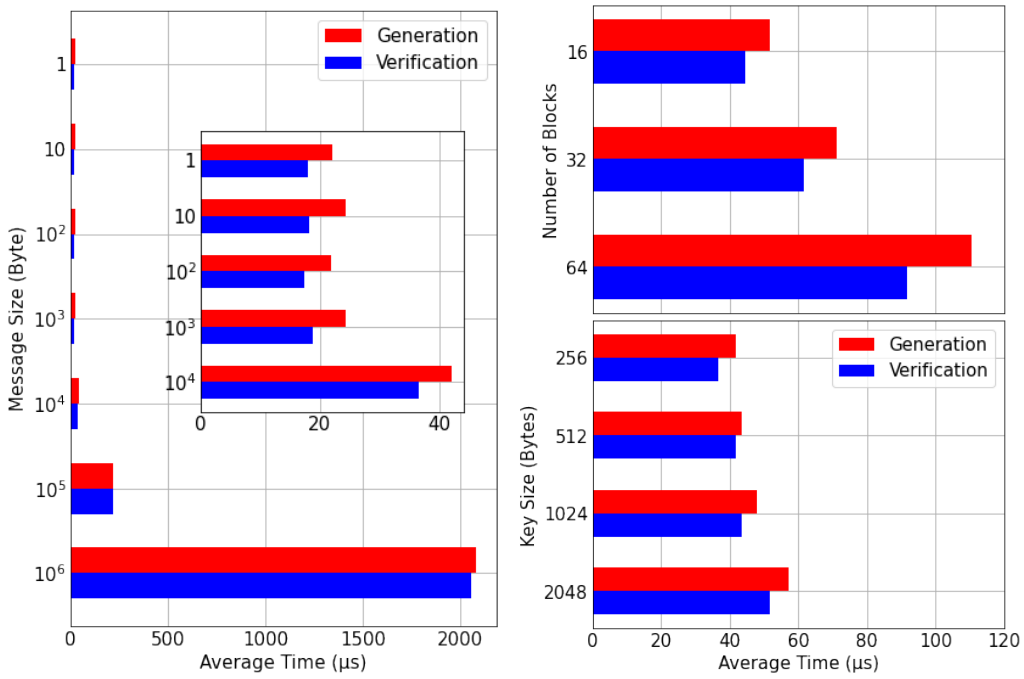
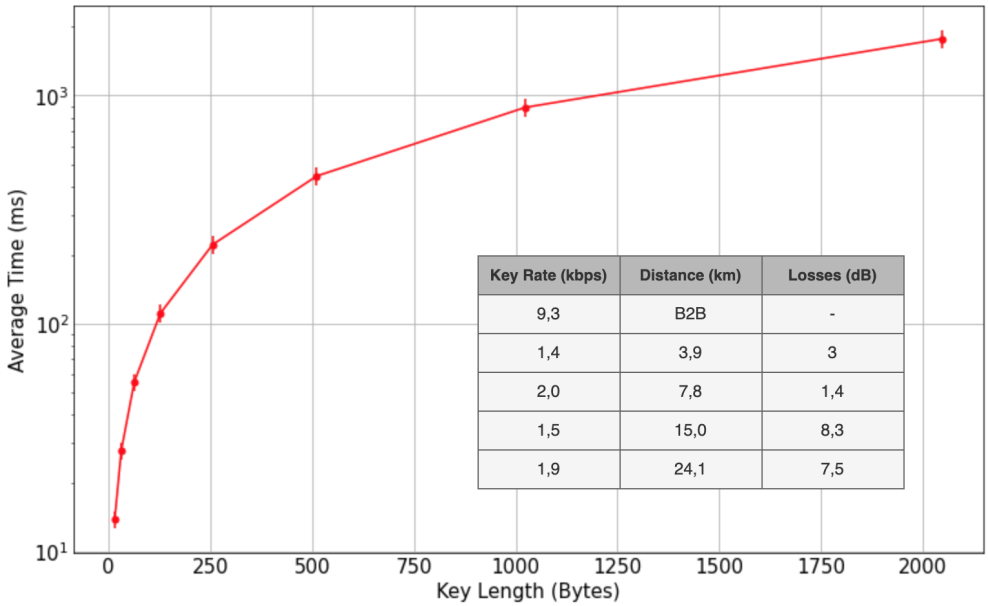


Figure 3.4: Evaluation of the impact in the average generation/verification time when (Left) the message size (left), the number of blocks (top-right) and the key size (bottom-right) are increased.

3.5 Experimental Demonstrations and Results

3.5.1 Q-DS Evaluation

Table 3.6 shows the experiments carried out in the Q-DS, each of then executed 100.000 times. During the execution of the protocol we have evaluated the average time it takes to generate and verify the signature and how it is impacted with the increase in the size of the message. To do this, message sizes from 1 B to 1 MB have been signed. The rest of the parameters are set to reach a security level of 128 bits, that is, an output message and block digest of $\delta_m = 512\ B$ and $\delta_B = 64\ B$, respectively, 16 blocks and a key length of $l_k = 256\ B$. The resulting signature lengths for these setups are always $L_S = 2048\ B$. The results obtained are shown in Figure 3.4-left. The protocol performance remains constant and with an average value of 23 μs up to message sizes of 1 kB. Above this value, the average signature generation and verification times increase exponentially, although the values reached are of the order of 2 ms when $l_m = 1\ MB$.



Key Rate (kbps)	Distance (km)	Losses (dB)
9,3	B2B	-
1,4	3,9	3
2,0	7,8	1,4
1,5	15,0	8,3
1,9	24,1	7,5

Figure 3.5: Average time in ms to generate QKD keys with lengths (Bytes). The data table shows the key generation rate obtained with the QKD devices in a B2B configuration and a comparison with published data of the key rate for different distances (km) and losses (dB) [e. a. Martin, 2024].

A second scenario was analyzed measuring the impact in the process performances when increasing the number of blocks from 16 to 64, for a given message of 10 kB, an output message digest of $\delta_m = 2048$ B, a block digest of $\delta_B = 64$ B and a key length of $l_k = 1024$ B. In this case, these setups provide a security level of 256 bits for $n = \{16, 32\}$, and 128 bits for $n = 64$. As the number of blocks increases, the signature length increases as well. An increase in n implies a greater number of hashes/XOF calculations, giving rise to a linear increase in the execution time, as shown in figure 3.4-right/up. For a division of 16 blocks, the average signature generation (verification) time is 51.7 μs (44.5 μs), while for $n = 64$, the average signature generation (verification) time increases to 110.6 μs (91.6 μs).

Finally, a third scenario was considered where the impact in the performance of the signature generation and verification processes with the increase of the key length and the related length of the message digest was measured. Here, the message was fixed to 10 kB, $n = 16$, and $\delta_B = 64$ B.The key length has been increased from $l_k = 256$ B (security level 128 bits) to 2048 B (security level 256 bits). The resulting signature lengths for these setups were always $L_S = 2048$ B. As it is shown in the figure 3.4-right/bottom, the increase in the size of the keys does not have a significant impact on the signature generation and verification times, being of 41.8 μs when $l_k = 256$ B and 57.3 μs when $l_k = 2048$ B, showing an increase of 15.5 μs. This due to that during the generation and verification of the signature, the key size increase only impacts the OTP calculation, which is a simple, low-consumption operation. However, this increase will have a greater impact on the distribution phase of the protocol, both in the generation of the keys during the QKD protocol and in the distribution of random blocks between Bob and Charlie. Figure 3.5 shows the average time in ms to generate QKD keys

with length from 16 B to 2048 B. The key generation rate obtained with the QKD devices in a B2B configuration is 9.3 $kbps$. This rate will decrease as the distance between the sender and the receiver increases, due to the losses presented in quantum channels. For example, in the case in which the physical medium for the transmission of photons is optical fiber, the behavior of the key generation rate with distance would be impacted with the increase in the distance and in the higher amount of channel losses, as shown in the data table within Figure 3.5, according to published data [e. a. Martin, 2024].

In all the experiments it can be observed that the signature generation process takes on average more time than the verification, despite the symmetry between the steps that constitute both processes. This is an expected result, since during the generation of the signature the digests of all the blocks that will comprise the signature are calculated, while during verification, only the digests of the blocks known to the verifier are calculated. Thus, as the verifier performs fewer operations, the execution time is shorter. However, the difference obtained between average time for the generation and verification of the signature has always been less than 30 μs.

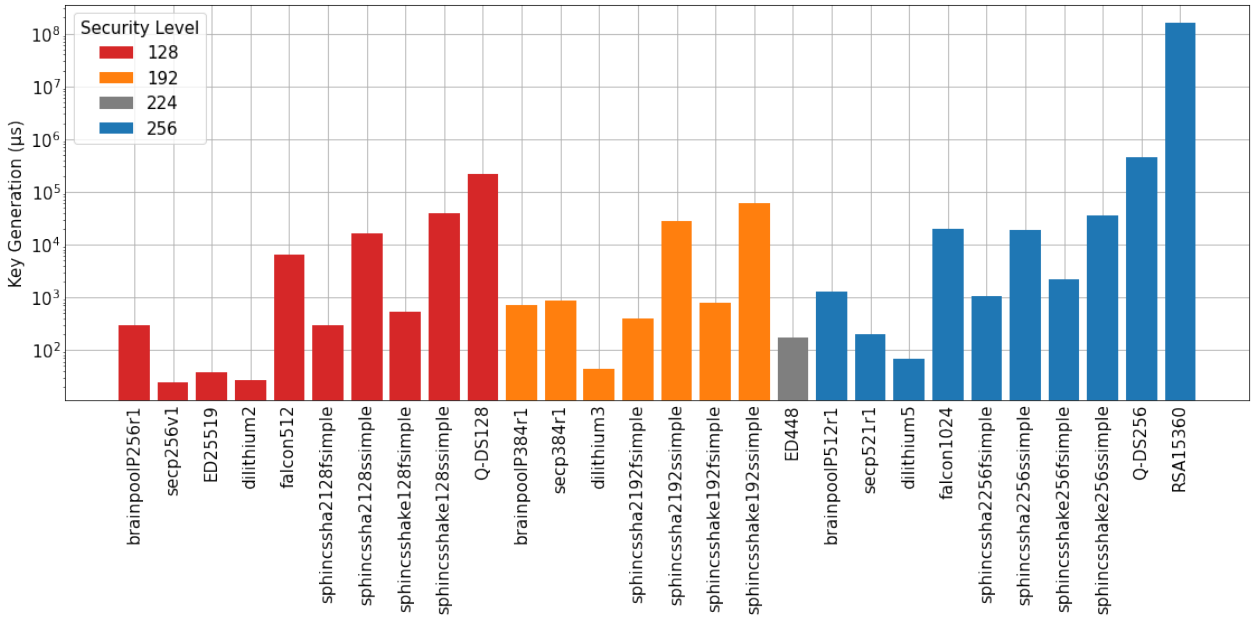


Figure 3.6: Average time for the Key generation per security level for all classical, PQC and Q-DS algorithms gathered in Table 3.5.

3.5.2 Comparative evaluation with classic and PQC DSA

During the execution of each algorithm specified in Table 3.5, the average time taken for the key pair generation, the signature generation and the signature verification for a message digest output length of $\delta_m = 512\ B$ were evaluated. In all cases, the message size was set at 10 kB and hashed using the extendable output function (XOF) *SHAKE256*. Additionally, the Q-DS protocol was set at $\{l_k = 256\ B, n = 16, \delta_B = 64\ B, \delta_m = 512\ B\}$ for a security level of 128 $bits$ and at $\{l_k = 512\ B, n = 16, \delta_B = 64\ B, \delta_m = 1024\ B\}$ for a security level of 256 $bits$. All the results obtained are shown in Figures 3.6, 3.7 and 3.8.

In Figure 3.6 presents the average time in ms that takes the key generation process for each algorithm in logarithmic scale. On the y-axis of the three graphs, the security level of the algorithms is represented (see Table 3.5). As can be seen, RSA is the algorithm that takes the longest to generate the keys, i.e. $1.6 \cdot 10^5$ ms, even in this case where the message digest output length of was set at $\delta_m = 256$ B, instead of 512 B as for the rest of the algorithms, due to the large calculation time. Within the classic algorithms, the most efficient are *prime256v1* and *ED22519* with a key generation average time of 25.1 and 38.0 μs, respectively, for a security level of 128 bits. For a security level of 256 bits, the most efficient classic algorithm is *secp521r1* with an average time of 200.3 μs. Regarding the Q-DS protocol, a 128 and 256 bit security levels setup have been defined to compare this solution with classic and PQC DSA. In this case, as previously explained and shown in Figure 3.5, the key generation through QKD is the most time consuming process impacting the protocol performance. In this case, for a back-to-back setup of QKD devices, the average key generation time for $l_k = 256$ B is 221.8 ms. Finally, regarding PQC, CRYSTALS-Dilithium algorithms are the most efficient ones during the key generation, with average times below 70 μs, for all security levels. The "small" variants of SPHINCS+ algorithms are the less efficient, for all security levels, together with *Falcon1024*, all of them with average times over 16 ms.

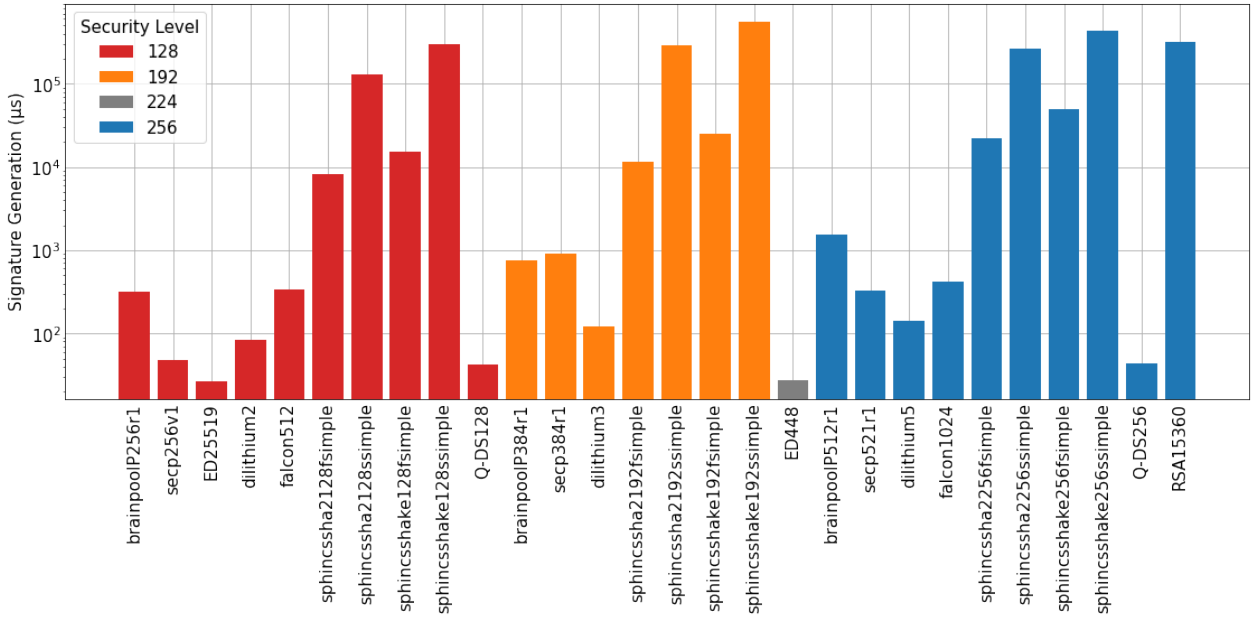


Figure 3.7: Average time for the Signature generation per security level for all classical, PQC and Q-DS algorithms gathered in Table 3.5.

A similar analysis have been carried out for the Signature Generation average times plotted in the graph of Figure 3.7, where the most efficient classic algorithms are the Edwards curve *ED25519* and *prime256v1* for a security level of 128 bits with 27.0 and 48.4 μs. *ED448* for a security level of 224 bits with 27.3 μs. For a security level of 256 bits, the best performer is *secp521r1* with 322.6 μs of average time. These algorithms compete in efficiency with the PQC *Dilithium2* which signature generation average time is 84.3 μs for a security level of 128 bits. *Dilithium3*, *Dilithium5*, *Falcon512* and *Falcon1024* also outperforms, in their respective security levels, over the rest of PQC algorithms providing average times of 122.4, 143.7, 342.7

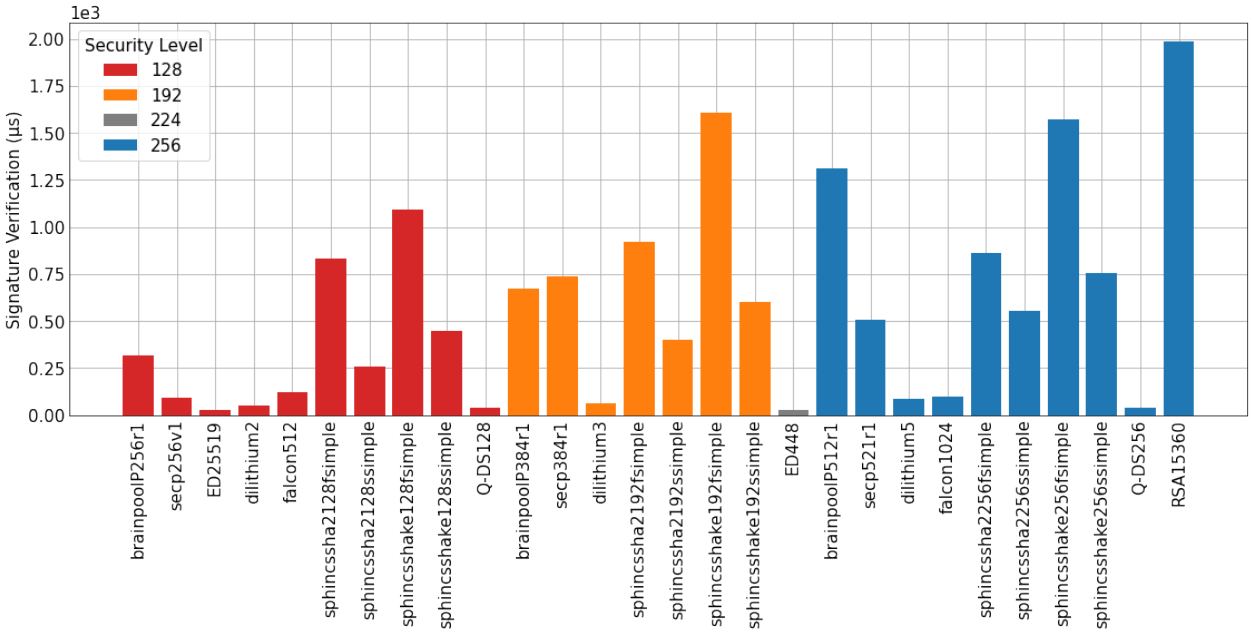


Figure 3.8: Average time for the Signature verification per security level for all classical, PQC and Q-DS algorithms gathered in Table 3.5.

and 416.7μs, respectively. The Q-DS signature generation process is as fast as classic solution being the average time 41.8 μs for 128 bits of security, and 43.6 μs for 256 bits. This is due to the simplicity of the protocol for the signature generation and verification which involves functions such as hash, XOF and OTP which are low-consumption operations. The bottom performers for the signature generation are *RSA* for classic cryptography with 317.6 ms and the "small" variants of SPHINCS+ for PQC with average times over 127 ms.

If we calculate the total generation times, adding the key generation time with the signature generation time, we can compare the overall efficiency of all the DSA solutions. For 128 bits of security, the most efficient quantum-resistant algorithm is *Dilithium2*, with an average execution time of 111.4 μs, giving rise to signatures of length 2420 B, according to the configuration in Table 3.7. For its part, the Q-DS protocol has execution times similar to the "small" variants of the *SPHINCS+* algorithms, i.e. on the order of 10^2 ms. However, QKD key generation time will be reduced as devices improve over time. In fact, in the literature, key generation rates up to 2857 $kbps$ can be found at a distance of 1.9 km [e. a. Martin, 2024]. With this key generation rate, a key of 256 B would be obtained in 0.72 ms, which would give us execution times of the Q-DS protocol of the same order of magnitude as *Dilithium2* and comparable to those of *BrainpoolP256r1*.

Finally, the signature verification process is in general the most efficient process for all algorithms. In the case of the Q-DS protocol, due to the symmetry in the steps that are followed during the signature generation and the signature verification the average time are similar, i.e. 36.6 μs for 128 bit and 41.7 μs for 256 bit. For PQC algorithms, it can be seen in Figure 3.8 that the "fast" variant *sphincsshake256fsimple* and *sphincsshake192fsimple* of *SPHINCS+* present worst performance than the other variants of this family, with average

times of 1571.4 and 1608.3 μs and security level 256 and 192 bits, respectively. The PQC out-performer algorithms are the *Dilithium* algorithms, for all security levels, with average times below 90 μs. Within the classical solutions, for a security level of 128 bits, the most efficient algorithms is *ED25519* with average times of 26.3 μs; *ED448* for a security level of 224 bits with 25.4 μs; and for a security level of 256 bits *secp521r1* stands out with 507.5 μs of average time. While the one with the worst performance is *BrainpoolP512r1* (security level 256 bits) with average time of 1310.0, apart from *RSA*, where the signature verification takes an average time of 2061.0 μs (being $\delta_m = 256\ B$).

3.6 Conclusions

The quantum-assisted digital signature protocol proposed in this article avoids the use of currently employed public-key cryptosystems (RSA, ECDSA, etc.) that are considered vulnerable in a quantum scenario, replacing the key exchange with ITS QKD-generated keys for which commercial devices are available.

Unlike the QDS protocols published to date, the new scheme presented in this thesis provides a hybrid approach that allows to sign messages with an arbitrary length. This is accomplished by taking into account NIST-recommended hash functions and/or XOF from the SHA-2 and SHA-3 families, thus generating a system that composes quantum and classic cryptographic solutions implementable with current technology.

The protocol has been demonstrated secure against attacks on the integrity of the message, forgery of the signature and an attempt of repudiation by the signer. In addition, its high parametrization, in terms of message length, hash function to be applied on the message, key length, number of blocks and hash function to be applied on the blocks, allows us to configure digital signatures with different levels of security and with negligible impact on the efficiency of the signature generation and verification.

The implementation of the proposed Q-DS together with 9 classic DSA and 17 PQC DSA, with different levels of security, has allowed us to make a comparative evaluation in terms of efficiency of the different solutions during the key generation, signature generation and verification. It has been observed that, for the same level of security, the Q-DS protocol is the most efficient solution during the generation and verification of the signature, only surpassed by the classic solution *ED25519*. The greatest impact on the efficiency of the protocol is observed in the generation of QKD keys, which, with the devices used, results in a key generation rate of 10 *kbps* in a B2B configuration. However, with other types of devices and/or manufacturers, key generation times of the order of 0.72 ms can be achieved for key sizes of 256 B. This reduction in the key generation times makes the Q-DS protocol comparable to the most efficient quantum-resistant algorithm *Dilithium2*.

Finally, it should be noted that this type of analysis aims to facilitate the selection of possible candidates during the migration processes from current cryptographic systems to quantum-resistant ones, given the needs of a specific environment.

Chapter 4

Quantum Zero-Knowledge Protocol

4.1 Context

The second cryptographic primitive that this thesis has focused on is the zero-knowledge proof or zero-knowledge protocol (ZKP).

Zero-knowledge proofs (ZKP) are cryptographic mechanisms where a user who is called the prover has to prove that he is aware of a secret to another user, called the verifier, without revealing the secret itself or any information about it. This type of proof can be used for many applications, but in the field of security they are very useful tools to improve privacy.

The origin of ZKP dates back to 1985 when S. Goldwasser, S. Micali and C. Rackoff [S. Goldwasser and Rackoff, 1985] introduced the concept of ZKP for the first time. These authors showed that certain types of problems, such as graph isomorphism, could be proven without revealing any additional information beyond the truth of the statement. Since their conceptual proposal, ZKP have advanced rapidly, with new techniques, protocols and applications being developed and refined, becoming an important tool in cryptography. As the technologies mature, ZKP are expected to play an increasingly important role in improving information privacy and security.

Generally, these proofs consist of the prover having to solve a challenge sent by the verifier, and in order to solve it, he must know a specific secret. To illustrate how a ZKP works, we will use the commonly used example, known as the Alibaba's cave [J. Quisquater, 1990]. We suppose a cave through which two paths can be taken, one to the left (L) and another to the right (R), and that both paths converge again at a point further ahead, tracing a circular path, as shown in Figure 4.1.

At the convergence point of the two paths there is a door that only opens when the magic word is said, this will be the secret that Bob will have to prove to the verifier Alice that he knows, but without revealing it to her. The test begins with Bob entering the cave and randomly choosing one of the paths L or R, without Alice seeing which one he chooses. Then Alice randomly chooses one of the paths as well and shouts to Bob to go out that way. Thus, the following situations can occur, according to Figure 4.1:

- (Situation 1) Bob chooses a path and Alice tells him to go out that same way → Bob will go out the correct way;
- Bob chooses a path and Alice tells him to go out the other way:
  - (Situation 2) Bob will go out the correct way if he knows the secret;
  - (Situation 3) Bob will go out the wrong way if he does not know the secret.

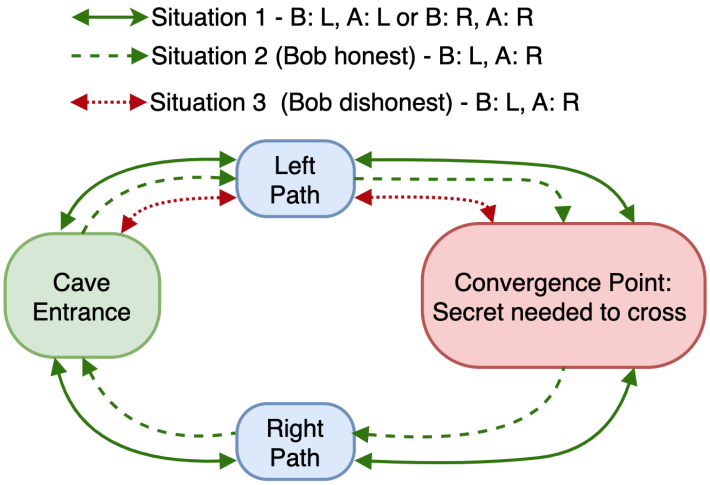


Figure 4.1: Example of the Alibaba's cave. B is the path chosen by Bob (the prover) and A the one chosen by Alice (the verifier). In situation 1 it does not matter if Bob knows the secret to open the door or not. In situations 2 and 3 Bob knows and does not knows the secret, respectively.

If they carry out an isolated proof, Bob has a 50% chance of getting it right, even if he does not know the magic word. However, if they repeat this proof an i number of times, that probability decreases according to: $P = 1/2^i$. For example, if $i = 15$ the probability that Bob gets it right every time without knowing the secret is $P = 3 \cdot 10^{-5}$.

As we mentioned at the beginning of the section, a large number of use cases can be defined in which a ZKP can be implemented and, depending on each use case, an initial configuration will be defined based on the specific needs of the system. These use cases or applications can be:

- Authentication systems to prove the identity of an entity or person [Fiat and Shamir, 1986];
- Payment validation that allows verification that a party has sufficient funds to make the payment, without revealing the actual balance or transaction history [Gabay et al., 2020];
- Access control systems where users can demonstrate that they meet access requirements without revealing any additional information [Backes et al., 2005], among others.

Depending on the scope of the application, it may be the case that both the verifier and the prover know the secret before carrying out the proof or, on the contrary, that only the

prover knows the secret, as in the Alibaba's cave example. In addition to this, zero-knowledge proofs can be divided into two types: interactive [S. Goldwasser and Rackoff, 1985] and non-interactive [Blum et al., 2019]. In the first case, both the prover and the verifier must be present simultaneously during the execution of the proof. An example of an interactive ZKP is the protocol proposed by Fiat-Shamir [Fiat and Shamir, 1986]. This protocol starts from two secret prime numbers p and q, whose product is equal to $n = p \cdot q$. The prover (Bob) knows the secret s and the verifier (Alice) knows a public value $v = s^2 \cdot mod\ n$. The steps of the Fiat-Shamir proof can be summarized as follows:

1. Bob chooses a random number r such that $r \in \mathbb{Z}_n$. He computes $x = r^2 \cdot mod\ n$ and sends the result to Alice;
2. Alice chooses a random bit $b \in \{0, 1\}$ and sends it to Bob;
3. If $b = 0$, Bob replies $y = r$ and Alice checks that $y^2 = x \cdot mod\ n$. This verifies that y was the original r value sent by Bob;
4. If $b = 1$ instead, Bob replies $y = r \cdot s \cdot mod\ n$ and Alice verifies that $y^2 = x \cdot v \cdot mod\ n$. This ensures that y is related to s, the prover's secret;
5. The proof is repeated several times to confirm that Bob really does know s.

In the second type of proofs, non-interactive ZKP, the verifier can launch the proof when the prover is absent, thus solving it later. For example, the Fiat-Shamir protocol described above can be transformed into a non-interactive version, eliminating the need for interaction between the two parties. This is achieved by using cryptographic hash functions, known as the Fiat-Shamir transformation.

To make the protocol non-interactive, the Fiat-Shamir transformation replaces the random bit b with a value derived from a hash function applied to x. This eliminates the need for direct interaction between the prover and the verifier. The steps of the proof can be summarized as follows:

1. Bob chooses a random value r and computes $x = r^2 \cdot mod\ n$;
2. Bob generates the challenge b as $b = hash(x)$;
3. Bob responds according to b as in the interactive protocol;
4. Alice verifies everything without interaction with Bob.

The Fiat-Shamir protocol is a great example of how secure and private mechanisms can be created using cryptography, and is widely applied in various computer security systems such as digital signatures or authentication mechanisms. However, although it is efficient for certain specific problems, such as authentication, it is not scalable or flexible for more complex problems. Therefore, for advanced applications, protocols such as the zero-knowledge succinct non-interactive argument of knowledge (zkSNARK) [Sasson et al., 2014] are used. zkSNARK is a much more advanced solution, which has been designed to be more efficient and applicable to a wider range of problems than the Fiat-Shamir protocol. Like the Fiat-Shamir transformation, zkSNARK is a non-interactive protocol and its proofs are compact and easy to verify, even if the computation to be performed is very complex. This is a great advantage

over other zero-knowledge proof techniques. On the other hand, zkSNARK requires a trusted setup, so that certain public parameters that are necessary for the operation of the system are generated. This step is critical since it requires a reliable and secure generation of these parameters.

The implementation of ZKP protocols in quantum communications is of special interest for use cases such as the authentication of several users with access to the same quantum node within a quantum communication infrastructure (QCI). However, the ZKP we have discussed are based on asymmetric mechanisms similar to RSA (as in the case of Fiat-Shamir) or elliptic curves (in the case of zkSNARK) and are therefore vulnerable to Shor's algorithm. Therefore, solutions capable of offering quantum-resistant ZKP are required, and this is the main objective of this section.

Within the field of quantum cryptography, Quantum Key Distribution (QKD) still presents many challenges to be solved in terms of defining a complete system that guarantees end-to-end security. All these challenges are identified in section 5. One of these challenges is to guarantee the identity of a person accessing a QKD node that is accessed by multiple people or services, which fits perfectly with the capabilities provided by a ZKP. Therefore, as part of the research, it was proposed to adapt the concepts of classical zero-knowledge proofs to the field of quantum cryptography, proposing a new quantum zero-knowledge proof (QZKP).

Regarding previous published works, there are not many studies on QZKP in the literature, however some proposals and approaches, mainly for increasing the efficiency of QKD devices, have turned out to be of great interest for the design of the QZKP. Specifically, in 2005 the floating bases protocol was published [V. Kurochkin and Kurochkin, 2009; Y. Kurochkin, 2005], proposing an increase of the number of possible bases to be used in QKD protocols in order to achieve a more efficient system, simultaneously increasing the threshold of the allowed error rate and reducing the information that can be extracted by Eve. To carry out this scheme, it is required that Bob and Alice have a pre-shared secret key on which the selection of the bases will depend. Another strategy to improve the efficiency of the QKD devices is the one in [Wei et al., 2013], where the authors propose a decoy-state protocol for QKD characterized by a biased bases selection, where signal states are always encoded in basis Z, while decoy signals can be randomly encoded in basis X or Z with a pre-determined probability. More recently, in 2018, modifications of BB84 protocol were proposed through the use of pseudo-random states generated from a pre-shared secret key [Trushechkin et al., 2018], in order to achieve higher key rates. The main drawback of the proposed scheme is the strict requirement of the employment of a perfect single-photon source. The use of pre-shared keys and the pseudorandom selection of the quantum states are the main concepts applied for the design of the proposed QZKP.

In this chapter, we propose and implement a new interactive QZKP where both the prover and the verifier possess a shared secret in advance. It is important not to confuse a user-oriented authentication with the authentication of the classic channel in the QCI. The latter pursues the authentication at a network level, but there is still a need of guaranteeing the identity of the end user who is on the other side of the screen in such a way that his data remains private. In this work, a user-oriented authentication is addressed.

A real use case of a user-oriented authentication could be a situation where the same computer is used by several doctors in a hospital to upload their patient information into the health system. When accessing the health system each of the doctor must be authenticated which could be done with the proposed QZKP. The proof is based on purely quantum mechanisms and has been implemented and experimentally tested on quantum cryptographic devices.

The chapter is organized as follows: firstly, the design of the new QZKP in Section 4.2 is presented; then, the security of the protocol is analyzed in Section 4.3. Finally, the experimental setup and the outcomes are described in Section 4.4.

4.2 QZKP Design

In this chapter, we propose an interactive quantum zero-knowledge proof (QZKP) protocol, where both the verifier (Alice) and the prover (Bob) must pre-share a secret s to successfully validate the proof. Specifically, Bob utilizes the QZKP with Alice to authenticate himself, as shown in Figure 4.2. This process always applies when a quantum key distribution (QKD) channel has already been established. The proof consists of three stages: Pre-processing, Quantum and Verification stages.

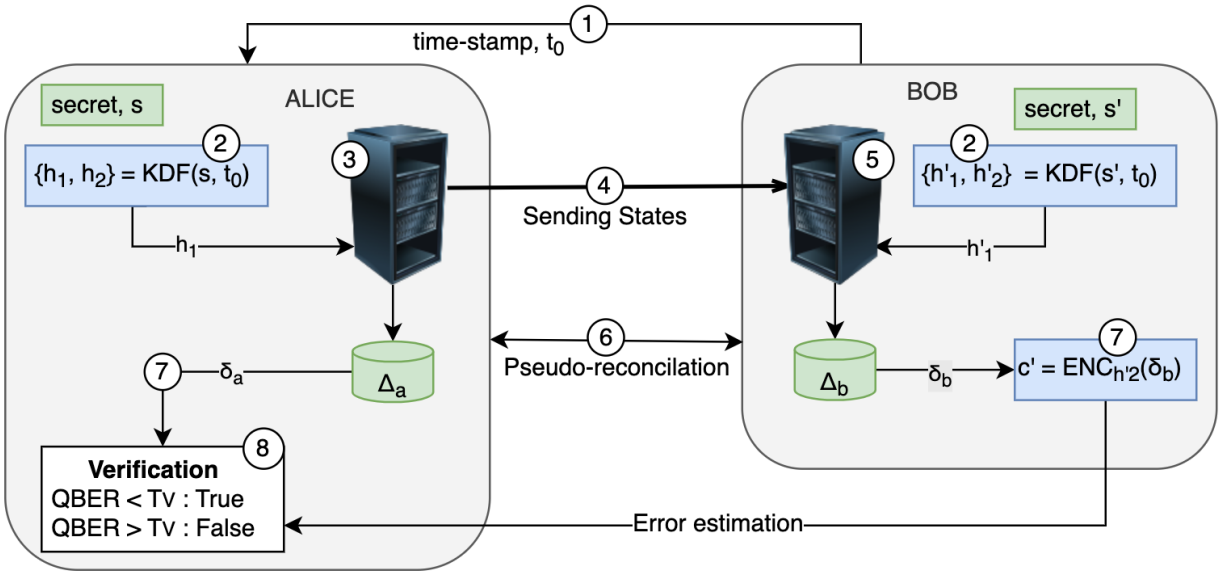


Figure 4.2: Flowchart of the quantum zero-knowledge proof protocol between Alice and Bob. Steps 1 and 2 represent the pre-processing stage, where the necessary information for executing the proof is prepared. Steps 3 through 5 correspond to the quantum stage, during which quantum states are prepared, transmitted, and measured. In Steps 6 to 8, the proof is verified by estimating the quantum bit error rate ($QBER$). If both parties are honest, $s = s'$; otherwise, $s \neq s'$. KDF refers to the Key Derivation Function; $\Delta_{a,b}$ are the raw measurement results; $\delta_{a,b}$ are the post-processed versions of $\Delta_{a,b}$; ENC denotes the encryption of $\delta_{a,b}$ using h'_2; and T_v is the verification threshold.

First, the **pre-processing stage** which involves preparing all the necessary information and setup to carry out the QZKP. The steps carried out here are entirely classical and correspond

to steps 1 and 2 in Figure 4.2. Following the pre-processing, in the **Quantum phase** the quantum states are generated, transmitted, and measured, allowing both the transmitter and receiver to create a raw bit string. Quantum processes are involved in this stage, corresponding to steps 3, 4, and 5 in Figure 4.2. Finally, in the **Verification phase** the validity of the proof is determined by estimating the quantum bit error rate ($QBER$). Classical protocols are used for this evaluation, corresponding to steps 6, 7, and 8 in Figure 4.2.

The pre-processing stage begins with a handshake between Alice and Bob, during which both parties generate an identical timestamp t_0. After that, given a secret s of arbitrary length, Alice and Bob apply a Key Derivation Function (KDF) [Barker et al., 2018] to derive two values, h_1 and h_2, using t_0 and s as inputs. Both Alice and Bob perform this operation simultaneously. On Alice's side, the results are $h_1 \in \{0,1\}^m$ and $h_2 \in \{0,1\}^n$, where the lengths m and n (with $n < m$) are predetermined by the participants before executing the protocol. Bob performs the equivalent process, obtaining $h_1' \in \{0,1\}^m$ and $h_2' \in \{0,1\}^n$. If both Alice and Bob are honest, then $s = s'$; otherwise, $s \neq s'$. Further details about the KDF are provided in Section 4.3.2.

Once $\{h_1, h_2\}$ and $\{h_1', h_2'\}$ have been computed, the protocol advances to the second phase, where the quantum bit string is generated. Unlike conventional QKD protocols, where the bases and states are chosen randomly, Alice's bases are determined by the bit values of h_1, while the states within each basis are selected at random. Alice then transmits the quantum signals to Bob, who measures them using the bases derived from h_1'.

When Bob knows the secret and Alice is an honest verifier, $h_1 = h_1'$. Therefore, during the preparation and measurement of quantum states, both parties will obtain nearly identical bit strings, denoted Δ_a^r on Alice's side and Δ_b^r on Bob's. The superscript r indicates that these are raw strings, with no post-processing applied. The bit strings are almost identical because, despite using the same bases for preparation and measurement, losses occur during transmission, even in the absence of malicious interference. In an ideal scenario, with perfect transmission and no errors or eavesdropping, Bob's detected bit string would match Alice's exactly.

After the quantum transmission and measurement, the protocol proceeds to the verification stage, beginning with a partial sifting process. Unlike in standard BB84 QKD protocol (see Chapter 2), Bob does not reveal the bases he used for measurement, as doing so would expose information about h_1, violating the zero-knowledge requirement. Instead, Bob simply informs Alice of the times when he detected a single photon. Both parties then select the corresponding bits from their bit strings, resulting in the sifted strings Δ_a^s for Alice and Δ_b^s for Bob, without disclosing any additional information. The superscript s indicates these are sifted strings.

Next, an error estimation is conducted between Δ_a^s and Δ_b^s to calculate the quantum bit error rate (QBER). In typical BB84 QKD, this process involves both parties publicly revealing a fragment of their key for comparison, and the resulting error count provides an estimate for the rest of the key. However, in QZKP, publishing even a fragment of Δ_a^s or Δ_b^s would disclose information tied to the pre-shared secret s, violating the zero-knowledge principle. Instead, Bob selects a random fragment δ_b from Δ_b^s, with length n, and encrypts it using a One-Time Pad

(OTP) encryption with h'_2. The encryption, performed by bitwise XORing δ_b with h'_2, results in $c' = ENC_{h'_2}(\delta_b)$. The positions of the bits in δ_b can be randomly selected by Alice using a Quantum Random Number Generator (QRNG) and then communicated to Bob. Bob sends the encrypted fragment c' to Alice, who decrypts it as $ENC_{h_2}(c') = ENC_{h_2}(ENC_{h'_2}(\delta_b)) = \delta_b$, assuming $h_2 = h'_2$. Finally, Alice compares δ_a with δ_b to estimate the QBER. In QZKP, only a rough error estimate is needed, and no error correction or privacy amplification is performed, as the process does not require the generation of a secret symmetric key.

Once the QBER has been estimated, the proof's validity is determined. If the QBER exceeds a predefined verification threshold T_v, the proof is rejected; otherwise, if $QBER < T_v$, the proof is accepted, confirming Bob's identity. To ensure a statistically accurate QBER estimate, the QZKP must be repeated N times.

4.3 Security Analysis

4.3.1 Security assumptions

A set of security assumptions must be considered during the execution of the protocol.

First, the security analysis of the BB84 QKD protocol [Lo and Chau, 1999; Renner et al., 2005; Shor and Preskill, 2000] introduces several assumptions about the adversary, which also apply to the QZKP. Specifically, the following are assumed:

1. Any adversary, whether external or participating, has unlimited computational resources, including access to a quantum computer;
2. The quantum channel is considered untrusted;
3. An external adversary can eavesdrop on the communication over the classical channel, but cannot inject or alter messages, as the channel is assumed to be authenticated.

Additionally, a security perimeter must be maintained around both Alice and Bob's nodes to prevent unauthorized physical access to their hardware. Adequate cybersecurity measures are also required to ensure that side-channel attacks cannot be conducted on either the classical or quantum channels.

4.3.2 Key-Derivation Function details

Key-Derivation Functions (KDFs) are critical components of modern cryptographic systems, designed to take initial keying material and derive one or more cryptographically secure secret keys. According to the NIST SP800-56C (r2) standard [Barker et al., 2018], there are two types of KDFs:

- One-Step Key Derivation: Cryptographic material is derived directly from a set of inputs and a secret.
- Two-Step Key Derivation: Before derivation, the secret undergoes a transformation.

In the proposed QZKP, a Two-Step Key Derivation function using a counter mode is recom-

mended [Krawczyk and Eronen, 2010]. This process is divided into two main phases:

1. Extract phase: The keying material (s) and a salt value (t_0) are used to generate a fixed-length pseudorandom key, K_{IN}.
2. Expand phase: The pseudorandom key K_{IN} is expanded into multiple pseudorandom keys (h_1, h_2).

During the expand phase, additional inputs such as a label, context (which are fixed), and the required output length ($m + n$) are used. It is important to note that while the sources of entropy, h_1 and h_2, are derived from the secret s, the encryption $\delta_a \oplus h_2$ is performed between two independent elements. This is because δ_a, despite being derived from s, is constructed as a random bit string, ensuring independence from h_2.

4.3.3 QZKP security analysis

A ZKP must ensure three main properties: Completeness, Soundness, and Zero-knowledge, all three depicted in Figure 4.3. The security of the proposed QZKP is demonstrated as follows:

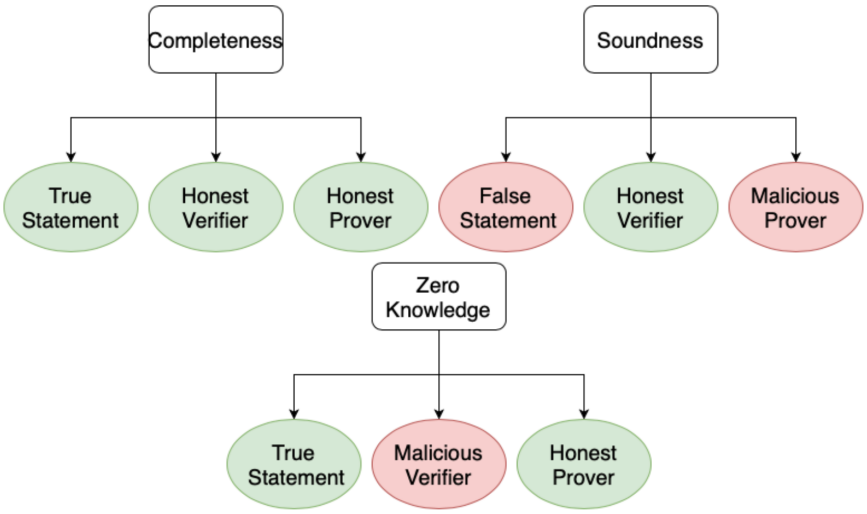


Figure 4.3: Properties of a ZKP and QZKP.

Completeness. When both the verifier and prover are honest and know the secret, the prover can convince the verifier of this knowledge without revealing the secret. In this case, since both parties are aware of the secret, they will use identical bases for state preparation (by Alice) and measurement (by Bob). In an ideal scenario, without photon losses or electronic noise, Δ_a^r and Δ_b^r will match perfectly, resulting in a $QBER = 0$. However, as we will see in Section 4.4, in a real-world scenario, transmission losses and noise may increase the error rate to $QBER \neq 0$.

To demonstrate **Soundness**, we assume that the verifier is honest, but the prover is dishonest and unaware of the secret. It must be ensured that a malicious prover cannot convince the verifier of knowing the secret, except with negligible probability. In this case, the measured

QBER will reflect the attempt to cheat during protocol execution. As described by H.-K. Lo's analysis [Lo et al., 2005], the QBER is:

$$QBER = \frac{p_{A,Z}^2 \cdot e_B^Z + p_{A,X}^2 \cdot e_B^X}{p_{A,Z}^2 + p_{A,X}^2} = \frac{(1-r)^2 p_B^X + r^2 p_B^Z}{2\left[(1-r)^2 + r^2\right]} \tag{4.1}$$

Where, $0 < r \leq 1/2$ is a variable parameter which depends on the value of the bits in h_1; $p_{A,Z} = (1-r)p_\mu$ and $p_{A,X} = rp_\mu$ are Alice's probabilities of preparing the states in each basis; $e_B^Z = p_B^X/2 = (1-p_B^Z)/2$ the error rate for the case when Alice prepares the state on Z basis and Bob measures on X basis; and $e_B^X = p_B^Z/2$ the error rate for the case when Alice prepares the state on X basis and Bob measures on Z basis. To try to cheat on Alice, Bob can carry out the following strategy. Given $p_B^Z = 0.5$ and $r = 1/2$, that is, 50% of the signal states are encoded in the Z basis and 50% in the X basis, since Bob does not know the value of h_1, he will measure the signals randomly. In this way he will guess correctly 50% of the times in the selected basis and of the other 50% he will get an uncorrelated result but he will guess correctly the value of the resulting bit half of the times. In total, he will get 75% of the measurements correct, but without knowing which elements are wrong and which are correct. This strategy raises the QBER to 25% without taking physical errors into account. Therefore, for a $T_v < 25\%$ the proof would give a negative result, proving the soundness of the QZKP. This analysis agrees with what is obtained in Eq. (4.1) by introducing the parameters.

Finally, to ensure **Zero-knowledge**, if the prover is honest and the verifier malicious, the verifier should not learn anything from the proof. Similar to the previous scenario, Alice could randomly prepare quantum states without knowing s. During error estimation, she cannot extract any useful information from δ_b because she lacks h_2' to decrypt the OTP. The probability of guessing all elements of c' correctly is $P_{guess} = 1/2^n$. Thus, the QBER will behave similarly, ensuring zero-knowledge.

More complex attacks, such as collective attacks could be considered that can be performed in the classical part of the protocol and in the transmission of the quantum states. To the best of our knowledge, collective and coherent attacks on the quantum states differs from the ones analyzed for BB84 protocol, since in the QZKP case no information about the basis is published for distillation purposes. Thus, in the case of an eavesdropper with the capability of storing quantum states, he would not be able to extract information about the secret.

4.4 Experimental Setup

4.4.1 Experimental system

The protocol outlined in Section 4.2 has been experimentally implemented using a pair of discrete-variable (DV) quantum cryptographic devices, previously tested for standard QKD transmission, including deployment in a network alongside classical channels [Gatto, Brunero, et al., 2021]. A diagram of the transmitter and receiver setup is provided in Figure 4.4.

The DV-QKD prototypes are based on the BB84 protocol with polarization encoding and the decoy-state method [Ma et al., 2005]. Alice and Bob use a fully-automated synchronized

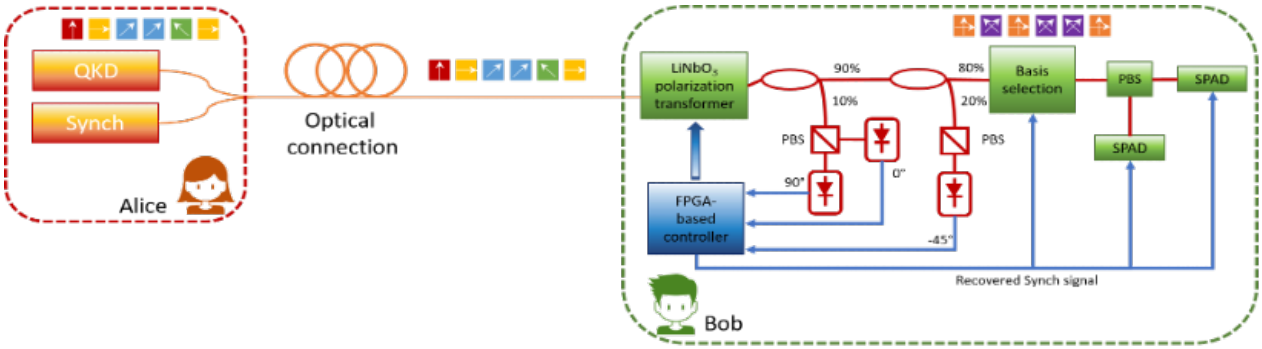


Figure 4.4: Schematics of the pair of discrete-variable quantum cryptographic devices.

architecture, utilizing two distributed-feedback (DFB) lasers with the same nominal wavelength as sources for both the quantum and auxiliary channels [Gatto, Brito, et al., 2021]. The quantum signal consists of weak optical pulses, each with a duration of 20 ns and a repetition rate of 1 kHz. The chosen wavelength of 1310 nm helps avoid Spontaneous Raman scattering caused by co-propagating classical sources in the C-band. The decoy-state method involves signal (μ), weak decoy-state (ν), and vacuum state (0), each occurring with a predetermined probability: p_μ, p_ν, and p_0, respectively. The measured losses in the receiver module were approximately 5 dB.

The scheme was first tested in a back-to-back (B2B) setup under two cases: 1) all participants are honest, and 2) the prover is a malicious user who does not know the secret and randomly measures the quantum states sent by the verifier.

After successfully validating the QZKP in these initial short-distance experiments, the distance between Alice and Bob was increased to assess the impact on the $QBER$ under honest conditions, ensuring a minimal occurrence of false positives or negatives. To this end, the QZKP was evaluated over a point-to-point standard single-mode fiber (SSMF) link, with performance measured to estimate the effect of signal loss on the protocol.

Different distances were emulated by introducing controlled optical attenuation in two ways. First, by implementing a manual attenuator between the devices and gradually increasing the dBs in a controlled manner. The second approach was the one shown in Figure 4.5, where a variable optical attenuator (VOA) was introduced followed by a $1X2/90:10$ coupler.

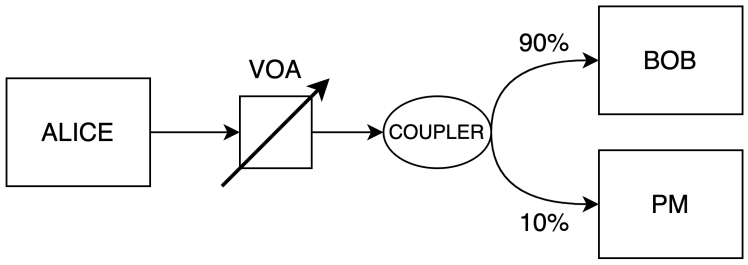


Figure 4.5: Schematics of the system for distance emulation introducing a variable optical attenuator (VOA), a 1X2/90:10 coupler and a power meter (PM) between the quantum cryptographic devices.

In both approaches, all the intermediate elements were previously characterized to determine the initial losses, so that the manual attenuator introduces 4.11 dB and the second setup introduces a total of 2.5 dB. Taking into account that the losses in a standard optical fiber are 0.21dB/km, the presence of the manual attenuator or the second setup establishes an emulated initial distance between the devices of 19.6 km and 11.9 km, respectively. Thus, the evaluated propagation distances ranges from 11.9 km to 60.6 km, covering a link attenuation from 2.5 dB to 13 dB, approximately.

4.4.2 Parameter settings

In all the experiments conducted for the honest scenario, the protocol parameters were kept constant except for the length of the sifted string $\Delta^s_{a,b}$, denoted as L_Δ, which was varied to include string lengths between 256 $bits$ and 2048$bits$. For the length n of $\delta_{a,b}$, 15% of the total $\Delta^s_{a,b}$ was used for $QBER$ estimation. The parameter settings are summarized in Table 4.1. A similar approach was followed for the dishonest case, but in this instance, Bob's protocol was adjusted to perform random measurements, assuming he is unaware of the secret, as detailed in Section 4.3.

For each experiment, Table 4.1 provides the emulated distance in kilometers, with B2B referring to the back-to-back configuration, setup 1 to the VOA-Coupler-PM configuration and setup 2 to the manual attenuator, the losses in dB, the length L_Δ of $\Delta^s_{a,b}$, the number of iterations of the QZKP, the average time required to generate 1 bit, the average $QBER$ estimate, and the $QBER$ standard deviation. As shown in Figure 4.6, the time required to generate 1 bit exhibits a logarithmic trend as losses increase in the honest case, for both setups.

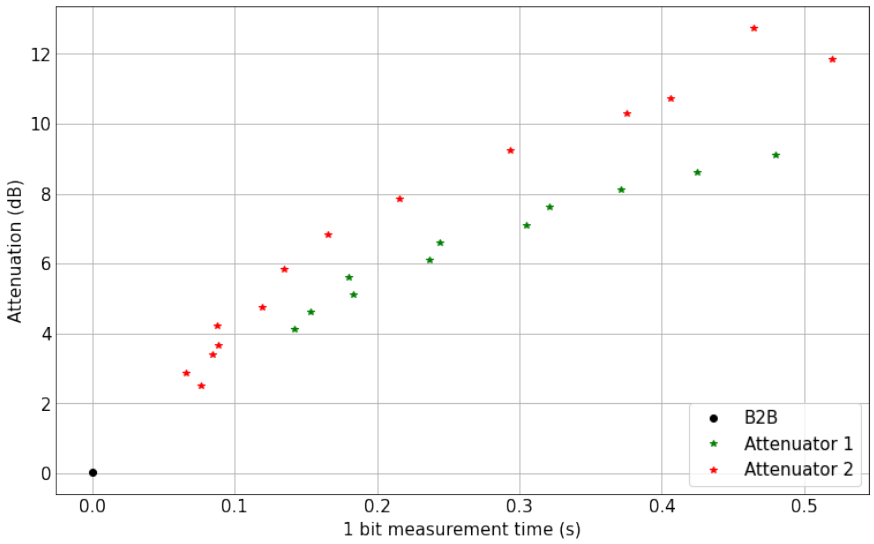


Figure 4.6: Amount of time needed for the generation of 1 bit in the honest case. The time needed shows a logarithmic behaviour when increasing the losses. The black dot corresponds to the back-to-back (B2B) configuration, green stars to setup (Attenuator) 1 VOA-Coupler-PM and red stars to setup 2 with the manual attenuator.

Table 4.1: Parameter settings used in back-to-back setup (B2B), setup 1 (VOA-Coupler-PM) and setup 2 (manual attenuator) during the QZKP executions for both the honest and dishonest cases, along with the results for the emulated distances (in km, with B2B indicating back-to-back configuration), the corresponding losses (in dB), the length L_Δ of $\Delta^s_{a,b}$, the number of QZKP iterations, the average time taken by the system to generate 1 *bit*, the average $QBER$ estimation, and the standard deviation of the $QBER$.

Setup	Losses (dB)	Distance (km)	L_Δ (bits)	Iterations	Time (s)	QBER	σ_{QBER}
Honest Case							
B2B	0	–	2048	173	0.033	0.029	0.007
2	4.11	19.57	2048	190	0.140	0.029	0.007
2	4.61	21.95	1024	105	0.153	0.023	0.008
2	5.11	24.33	1024	1232	0.183	0.036	0.011
2	5.61	26.71	1024	170	0.180	0.028	0.008
2	6.11	29.10	1024	215	0.237	0.036	0.010
2	6.61	31.48	1024	141	0.244	0.028	0.008
2	7.11	33.86	1024	162	0.305	0.037	0.010
2	7.61	36.24	512	175	0.321	0.026	0.013
2	8.11	38.62	512	301	0.372	0.037	0.013
2	8.61	41.00	512	137	0.425	0.029	0.012
2	9.11	43.38	512	225	0.480	0.040	0.015
1	2.50	11.90	1024	189	0.077	0.028	0.008
1	2.86	13.62	1024	858	0.065	0.033	0.009
1	3.39	16.14	1024	165	0.084	0.024	0.009
1	3.67	17.48	1024	171	0.089	0.029	0.009
1	4.24	20.19	1024	612	0.088	0.033	0.010
1	4.75	22.62	512	229	0.119	0.023	0.011
1	5.84	27.81	512	10	0.135	0.033	0.014
1	6.82	32.48	512	10	0.166	0.027	0.009
1	7.85	37.38	512	10	0.216	0.028	0.011
1	9.24	44.00	512	11	0.294	0.021	0.010
1	10.29	49.00	256	11	0.376	0.040	0.022
1	10.74	51.14	256	11	0.406	0.028	0.016
1	11.83	56.33	256	10	0.520	0.037	0.013
1	12.73	60.62	256	26	0.465	0.033	0.018
Dishonest Case							
B2B	0	–	2048	190	0.030	0.266	0.015

4.5 Results

4.5.1 Comparison between honest and dishonest cases in B2B

For each scenario, the QZKP protocol was executed for over 170 iterations, as detailed in Table 4.1. The results for the average estimated $QBER$ and its standard deviation are provided in both Table 4.1 and Figure 4.7.

When both the verifier and prover are honest (indicated by blue stars), the $QBER$ remains well below the standard security threshold of 11% [Shor and Preskill, 2000]. Specifically, the measured average $QBER$ shows a floor of 2.9%, due to system imperfections such as the finite extinction ratio (ER) of the polarization beam splitter (PBS), limited to 20 dB, and the presence of dark counts in the two single-photon avalanche detectors (SPADs). Conversely, when the prover is dishonest (red stars), the $QBER$ rises to 26.6%, exceeding the 11% security limit defined by the BB84 protocol.

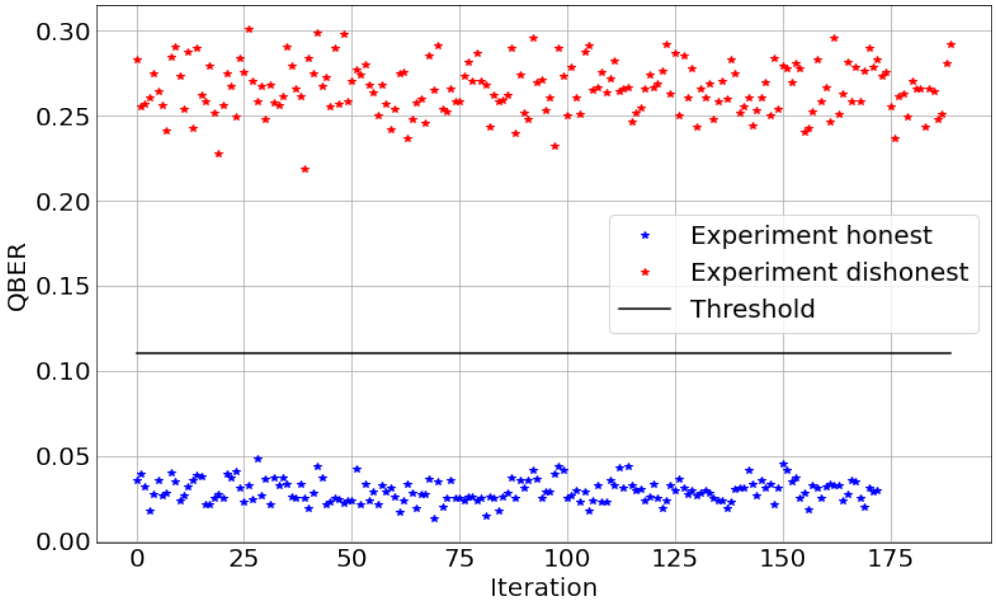


Figure 4.7: Experimental results of the QBER in a back-to-back setup. Blue stars: all players are honest, Red stars: dishonest prover. The black line refers to the standard security threshold value of 11% for the BB84 protocol [Shor and Preskill, 2000].

The $QBER$ remains stable throughout the 170 iterations, though some fluctuations are visible in both the honest and dishonest cases, due to the limited bit count used for the QBER estimation (15% of m). For example, with a raw key length of $m = 2048$ $bits$, the estimation is based on $n = 307$ $bits$. The standard deviations for the honest and dishonest configurations are 0.7% and 1.5%, respectively. The greater fluctuation in the dishonest case stems from the prover's random measurement strategy, with equal probability for each basis, while Alice sends $N_\mu^Z = p_\mu \cdot m \cdot (1 - r)$ in the Z basis and $N_\mu^X = p_\mu \cdot m \cdot r$ in the X basis, where p_μ is the signal probability, and m is the length of h_1. Despite these fluctuations, no false positives or false negatives were introduced, ensuring successful user authentication in all iterations.

4.5.2 Results over the distance

The impact of inserting additional losses in setups 1 and 2 is illustrated in Figure 4.8 and detailed in Table 4.1.

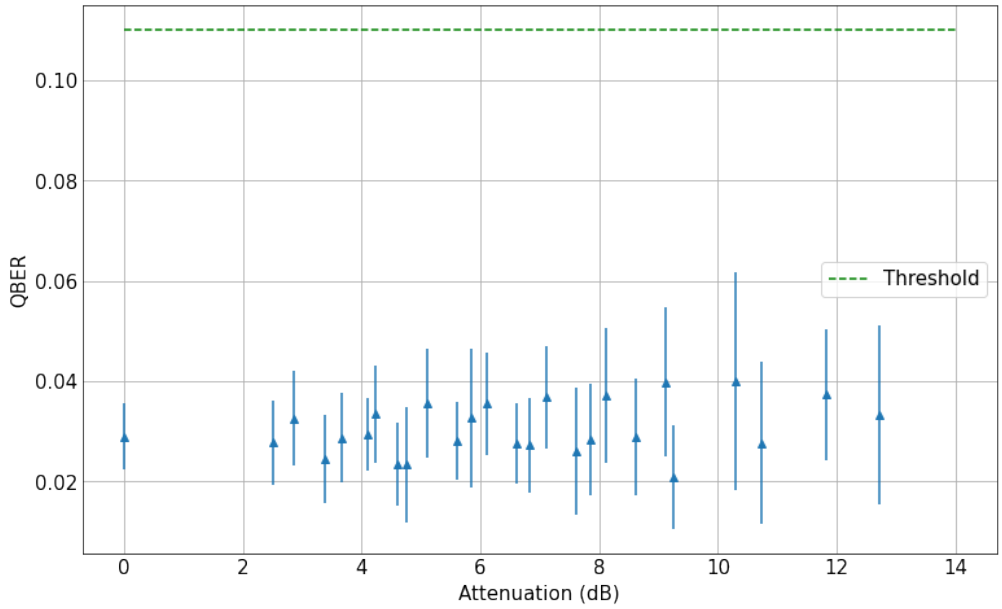


Figure 4.8: Measured QBER performance in setups 1 and 2 together with the associated standard deviations versus additional link losses in case of honest parties. The green dashed line refers to the standard security threshold value of 11% for the BB84 protocol [Shor and Preskill, 2000].

As in previous tests, multiple acquisitions were performed for each propagation length, corresponding to several runs of the QZKP. Figure 4.8 presents the average $QBER$ values along with their standard deviations. The minimum attenuation at 0 dB corresponds to the back-to-back (B2B) scenario described earlier. As the link losses increase, the $QBER$ also increases slightly, although it remains below the 11% security threshold. A minimum error rate of around 3% is observed, due to the limited extinction ratio (ER) of the polarization caused by the intrinsic properties of the optical devices and unavoidable misalignments before the PBS. Improvements in optical components and polarization alignment could reduce the $QBER$ to values below 1% in the B2B scenario, allowing for a more detailed observation of the gradual increase in $QBER$ as attenuation rises.

Furthermore, it is noted that higher losses lead to greater dispersion in the measured $QBER$. This is expected because fewer bits are used for $QBER$ estimation as the length of Δ_a decreases with increased system attenuation, resulting in longer measurement times to acquire the required Δ_a. In the B2B scenario, generating 1 *bit* takes an average of 0.033 seconds, with a $QBER$ deviation of 0.7% for the full protocol execution. At 12.7 dB, generating 1 *bit* takes an average of 0.465 seconds, with a standard deviation of 1.8%.

It is important to note that the dishonest case was only tested in the B2B setup to demonstrate the $QBER$ impact when a malicious prover, who does not know the secret, is involved in the

execution of the QZKP. This setup represents the best-case scenario for the attacker, as there are no additional transmission losses due to the distance.

4.5.3 Comparison between real and estimated QBER

Finally, since the $QBER$ used to authenticate a user is based on an estimate derived from a fragment of length n from Δ_a and Δ_b, the variation between this estimate and the actual $QBER$ has been analyzed for the back-to-back (B2B) setup and for raw string outputs over the longest distances, ranging from 22.6 km to 60.6 km. As mentioned earlier, the fragment used for the $QBER$ estimation comprises 15% of the total segment. To determine the actual $QBER$, each element of Δ_a and Δ_b was compared bit by bit, with the results shown in Figure 4.9 (blue downward triangles).

The $QBER$ estimation was calculated based on the L_Δ values provided in Table 4.1, with the corresponding results displayed in Figure 4.9 (red upward triangles).

As illustrated, the difference between the estimated and actual $QBER$ is less than 1% in the best case at 4.75 dB and shows an underestimation of up to 25% in the worst case at 9.24 dB. Despite this, there was no negative impact on the authentication process, and this behavior remains consistent across all tested lengths of Δ_a and Δ_b.

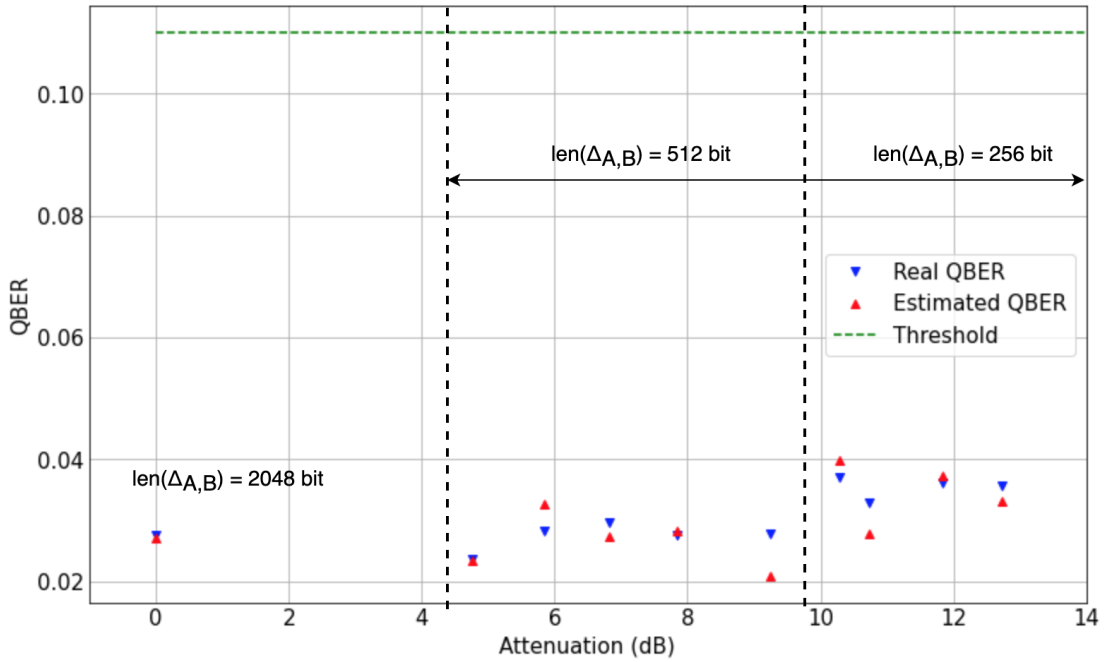


Figure 4.9: Comparison of the real QBER of (Δ_a, Δ_b), blue down triangles, versus the estimated QBER obtained from the fragments (δ_a, δ_b), red up triangles, for different string lengths.

4.6 Conclusions

To fully leverage the benefits of QKD, it is essential to design an end-to-end secure cryptographic system, where verifying the identity of the two communicating users plays a crucial role. The novel QZKP protocol proposed offers a method for user authentication in networks that already employ quantum communication infrastructure, without revealing any personal information or the user's secret. By relying on purely quantum processes, this protocol delivers a quantum-safe authentication mechanism that not only enhances the security of the entire system but is also straightforward to implement with existing QKD technology. Moreover, it is more efficient as it avoids the need for full error correction steps compare to the BB84 protocol. The QZKP was implemented in experimental devices designed to perform QKD, but where the degree of freedom to modify all parameters needed allowed us to execute de QZKP.

In terms of security, both theoretical analysis and back-to-back experimental results have demonstrated a 25% increase in $QBER$ when comparing the honest case, where $QBER = (2.9 \pm 0.7)\%$, to an attack by a malicious prover attempting to guess the bases linked to the secret-derived h_1 function, resulting in $QBER = (26.6 \pm 1.5)\%$. Additionally, the protocol holds up over long distances, with tests conducted over metropolitan-scale distances (up to 60 km), where an increase in $QBER$ and greater data dispersion were observed. Importantly, the QZKP did not produce any false positives or false negatives, demonstrating the robustness of the protocol. The QZKP has been thoroughly tested, guaranteeing completeness, soundness, and zero-knowledge, even against various malicious strategies. Finally, for bit lengths of 2048, 512, and 256, error estimation using 15% of Δ_a and Δ_b has provided reliable $QBER$ values for validating or rejecting the QZKP execution.

It is worth nothing that the protocol has a part of theoretical research but also a very strong experimental research part. Both were done as part of the development of this thesis thanks to the collaboration with Politecnico di Milano (Italy) during the international PhD stay.

Chapter 5

Geostrategic, Political and Technological Panorama

In this chapter we are going to analyze the impact that the emergence of quantum communication technologies has had in recent years in the communications and cryptography fields from different points of view. On the one hand, the impact from a technological point of view, with all the challenges and opportunities that arise and the ambition to develop the so-called quantum internet in the future. Another aspect in which quantum cryptography has had great impact has been in the political and strategic areas, leading several national security agencies to make public their position regarding the new cryptographic paradigms. Finally, the economic sphere, where a generalized increase in investment in R&D is observed, as well as in specific sectors such as defence, in which quantum technologies can lead to the development of new key military capabilities. This opens up a whole range of investment opportunities that can help continue research in the field and, as an ultimate goal, achieve the ambitious quantum internet.

This section is the result of the industrial nature of the thesis, in which, in addition to the scientific research of chapters 3 and 4, more business oriented and strategic aspects have been covered.

5.1 Technological sphere

We have already covered the impact that quantum computers will have from different aspects in chapter 2. Regarding, quantum communications and cryptography, in view of the investments and advances in these areas and their potential, the quantum internet concept arose as a natural extension of the internet. This term began to be used in the late 1990s [Weiss, 1999] and has regained interest in the second decade of the 21st century.

Although elements that will build the future quantum internet and the possible functionalities that it can provide have been proposed and defined [Kimble, 2008; Wehner et al., 2018], there are still gaps when referring to the definition of a common architecture for the integration of current quantum communication infrastructures that are being handled as part of the

EuroQCI activities. These definitions will support the future quantum internet.

For that, in this section, we define and compare two architectural model for the integration of quantum communication networks: one hierarchical and one distributed, and an analysis of today's technological and security challenges that still exist and that must be solved. This analysis takes as input the review carried out in chapter 2 about the historical and current quantum communication deployments.

5.1.1 Context

Although QCI are currently being deployed in isolation in different countries as part of the EuroQCI program, as we will see later in this chapter, there are already parallel projects, such as PETRUS [PETRUS, 2023] or the recently published Connecting Europe Facility (CEF) call to start connections between Member States. PETRUS is a Coordination and Support Action (CSA) set up by the European Commission, which aims to coordinate the QCI definitions and deployments. This type of programs promoting large quantum communication deployments will allow the future quantum internet (QI) to become a reality. This is why it is of great importance to analyse the current QCI and to propose a series of architectures that facilitate the network integration and evolution but, at the same time, allow the management of increasingly complex and large networks.

In this section, we will briefly review what QI is and what is expected from it in order to extract the main requirements needed to define the integration models of isolated quantum networks presented in Section 5.1.2.

The understanding of the Internet at the classical level can be formulated in two ways [Kurose and Ross, n.d.]:

- **Statement 1**: Set of necessary hardware and software components that compose it.
- **Statement 2**: Services of distributed applications that it provides.

Both approaches can be transferred when defining the QI. Thus, QI is considered as a set of devices with specific functionalities, which provides a series of services. After the commercialization of QKD devices, some definitions of QI have been given [Kimble, 2008; Wehner et al., 2018]. Apart from the definitions, some basic properties that the QI has to fulfill can be summarized as follows:

- Capability to communicate quantum information between network nodes.
- Cover long distances using quantum repeaters, satellites, etc.
- Be able to generate and distribute entangled pairs between network nodes.
- The infrastructure must host classical communications as well.

The property of entanglement plays a central role since it will allow the generation of non-classical correlations between users, which is a functionality that has no classical equivalent. To date it has been achieved the transmission through satellite links of distance between $1600 - 2400\ km$ [Y.-A. Chen et al., 2021; J. Yin et al., 2017]. However, the creation of entangled pairs at a reasonable generation rate is still a complex task, which means that it is

a technology that is still in an early research phase.

In chapter 2, we specified the basic elements that build a QCI that can be used as a base for a full quantum internet, following Statement 1. Following the approach from Statement 2, four stages that make up the development of the QI can be sketched modifying the approach presented in [Wehner et al., 2018]. Each of these phases adds a new functionality while increasing the difficulty of the developments. As a summary, Stage 1 are networks based on trusted nodes in which a prepare and measure QKD protocol is established between trusted contiguous nodes in order to share a symmetric key between two final end nodes. This is the state of current QCI. Stage 2 where quantum entanglement is established between nodes and qubits can be transmitted without the need of intermediate trusted nodes. This stage must also introduce Quantum Memories to build networks in which nodes have the ability to store a qubit in a location for certain time. In Stage 3 networks have a larger temporary storage capacity that favour functionalities such as distributed computing. And, finally, in Stage 4 networks will be integrated with quantum computers.

5.1.2 Integration models of isolated quantum networks

Based on the network components, topologies and SDN paradigm reviewed in chapter 2, we are going to define now two possible integration models - Hierarchical and Distributed - for isolated QCI. In both approaches, we will be referring to different domains, understanding a domain as a collection of quantum nodes that are controlled by a SDNC. In this case, a domain could be equivalent to a local quantum network.

Hierarchical model

When different network domains with their own controller are integrated into a larger network, a hierarchy of controllers similar to the hierarchy of ISPs (Internet System Providers) of the current internet is established. Within the context of a country, the Level 1 (L1) local controller knows the status of a specific network domain and is coordinated by a higher-level regional controller (L2) which knows the status of several L1 domains. Then, the regional controllers are coordinated by a national controller (L3) which has the global network state, as showed in Figure 5.1-left. More than 3 level can be set in a hierarchical model.

Establishing a hierarchy makes it possible to reduce the complexity of the operations, increase the overall network control and avoids having a single point of failure that disables the entire network by replicating the higher levels SDNC [Ali and Roh, 2020]. On the other hand, it presents less flexibility in terms of asset reorganization. In the diagram showed in Figure 5.1-left, four isolated QCN are integrated in a hybrid topology composed of a backbone that implements a bus topology including two satellite nodes. Each subnetwork domain connected to the backbone has a different topology, specifically, two rings, a simple point-to-point link and a star topology. Each of these subnetworks has its own L1 SDNC, which are connected to their associated L2 SDNC and these to the general L3 SDNC. In this scenario, L1 SDNC do not have direct communication links between them but an interface for communicating with upper level controllers, e.g. L1 SDNC with L2 SDNC.

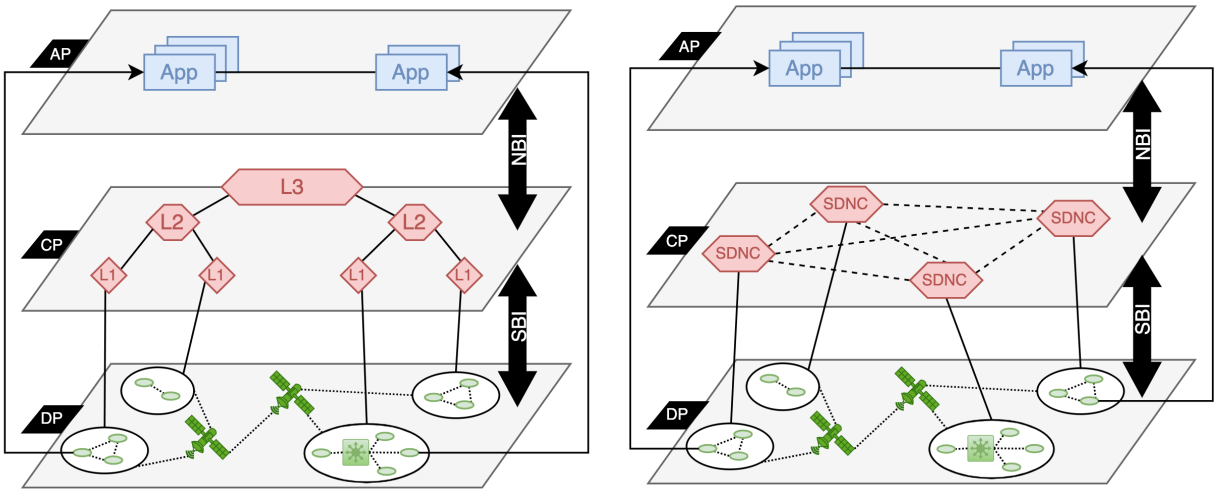


Figure 5.1: (Left) Hierarchical and (Right) distributed models of SDN-based networks integration. AP: Application Plane, App: Application, CP: Control Plane, LX: Level X, NBI: North-Bound Interface, SDNC: Software-Defined Network Controller, DP: Data Plane, SBI: South-Bound Interface.

Distributed model

The second SDN-based quantum communications network integration model is the distributed controller model. In this case, the management and control of the entire network is decentralized, in such a way that each domain has its own SDNC in charge of the intradomain services but at the same time each controller knows the whole network state. The different controllers communicate with each other, through an East-West Bound Interface (EWBI), to exchange network information in order to establish a path for quantum communications between two network end users belonging to different domains. In this way, each domain can act as an isolated network or as one more segment of a large QCN. This type of configuration favors the scalability of the network, since new domains can become part of it, as well as the robustness of the network, since it prevents single point of failures [Oktian et al., 2017]. If a network domain suffers a failure, the whole network is capable of reorganizing the routes to avoid the damaged segment. However, by not having a central controller, the amount of information that each controller has to handle increases, thus increasing the complexity of the operations. In addition, robust synchronization and prioritization mechanisms are required to avoid simultaneity in key requests that could lead to a wrong key distribution.

As in the previous model, four isolated QCN are integrated in the same hybrid topology composed of a backbone bus topology, as showed in Figure 5.1-right. Each of these subnetworks has its own SDNC, which are connected through the EWBI to SDNC from other domains.

5.1.3 Simulations and Results

Once both network integration models have been defined, a series of simulations were carried out to study the impact that each of the models has when the size of the networks in term of number of domains is increased for a specific use case. The use case consists of two users,

Table 5.1: Parameters of the simulations of the hierarchical and distributed integration models.

	Local	**Regional**	**National**
Entities in hierarchical	*L1-SDNC*, $QN_{1,2}$	*L2-SDNC* $L1\text{-}SDNC_{1,2}$ $QN_{1,2}$	*L3-SDNC* $L2\text{-}SDNC_{1,2}$ $L1\text{-}SDNC_{1,2,3}$ $QN_{1,2,3}$
Entities in distributed	*L1-SDNC*, $QN_{1,2}$	$L1\text{-}SDNC_{1,2}$ $QN_{1,2}$	$L1\text{-}SDNC_{1,2,3}$ $QN_{1,2,3}$
# Domains	1	2	3
# QN intra.	2	1	1
# Relays inter.	0	0	1

located in different quantum nodes (within the same network domain or not) and separated by a great distance, that want to start a videoconference application encrypted with keys generated by QKD.

To carry out these simulations, the Pragmadev Studio SDL tool has been used, where the videoconferencing use case has been defined and the number of steps that the system has to execute in each scenario has been measured, according to the parameterization described in Table 5.1. The table contains information such as the entities participating in each model, the number of domains involved, the number of quantum nodes (QN) within each domain, and the number of key relays between domains. As for the entities participating in each simulation based on the chosen model, the application running on each end node (App_1 and App_2) must also be taken into account, which in this case is a videoconference application.

First, we consider the scenario gathered in the second column of Table 5.1, which is composed of a single domain that involves a L1 SDNC, where the number of quantum nodes it manages can be increased, $QN_i, i = \{2, ..., n\}$. In this case, the complexity lies in the type of network topology within this domain. That is, if for example the network within this domain has a mesh topology, all nodes have visibility with all and, therefore, the establishment of a QKD key for the application is direct. But if the network has a ring topology, in order to establish a QKD key between non-adjacent nodes, a series of key relays will have to be carried out, as many as there are intermediate nodes. This not only has implications in the number of steps that must be completed to be able to execute the application but also has security implications, since it must be guaranteed that these intermediate nodes are trusted. However, this case is independent of the integration model with other domains, since all the QN are managed by their *SDNC*. Thus, only two QNs with direct connection have been taken into account, as shown in Figure 5.2, where the App on location 1 (App_1) makes a request for cryptographic material to its quantum node (QN_1), which has no key stored, so it is necessary to start a QKD protocol for key provision. Thus, the QN_1 ask for availability to L1 SDNC ($L1 - SDNC$) to execute a QKD with QN_2. The SDNC checks the availability of QN_2, establishes the route between both nodes, and opens the communication channels. Once the channels are opened, QN_1 and QN_2 execute a QKD protocol and when finished the connection is closed. Keys are provided to App_1 and App_2, and the encrypted videoconference begins.

Secondly, we simulate the scenarios listed in the third column of Table 5.1, with the regional

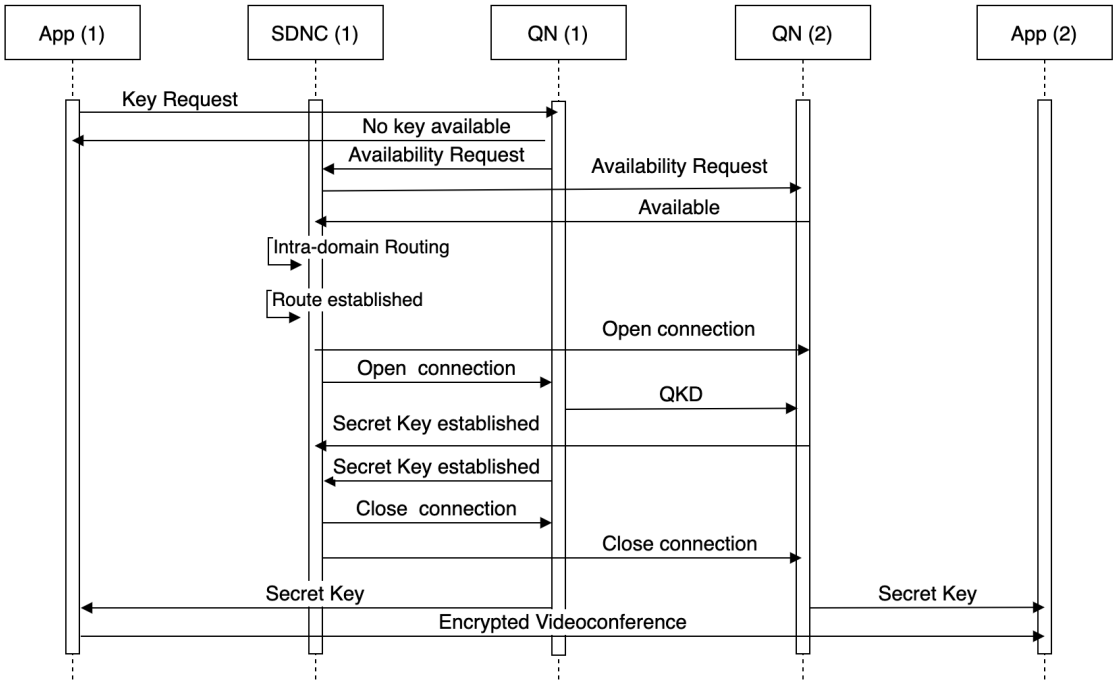


Figure 5.2: Sequence diagram of an encrypted videoconference established between two quantum nodes within a network domain.

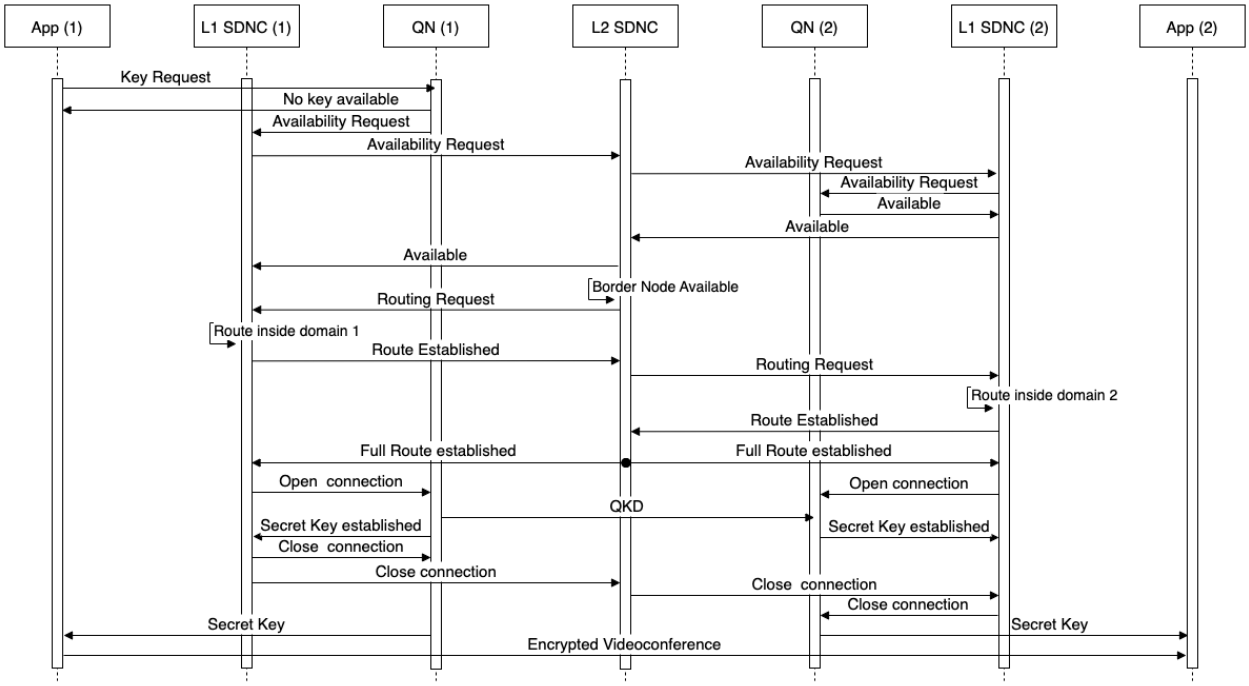


Figure 5.3: Sequence diagram of an encrypted videoconference established between two network domains integrated in a hierarchical model.

case. Figure 5.3 shows the sequence diagram for the use case in the context of the described hierarchical model, where the two users are located in different network domains. The scenario involves the application (App), controller and QKD device within a quantum network on the origin (domain 1) and destination (domain 2) and a L2 SDNC. We also consider that the two network domains are are adjacent domains with a border node. The App on domain 1 (App_1) makes a request for cryptographic material to its quantum node (QN_1), which has no key stored. Thus, the QN_1 ask to for availability to L1 SDNC of domain 1 ($L1-SDNC_1$) to execute a QKD with QN_2. $L1-SDNC_1$ detects that the destination QN is out of its domain so that it communicates to L2 SDNC. L2 SDNC analyses the status of both subnetworks and communicates with L1 SDNC of domain 2 ($L1-SDNC_2$). Once the availability of all the intervening elements in DP has been confirmed and the two local SDNC have been coordinated, L2 SDNC establishes the interdomain communication route between domain 1 and 2 through the border node and each L1 SDNC establishes the intradomain route inside their own domains. The connection between QN_1 and QN_2 is established and the QKD protocol is performed establishing a final secret symmetric key between both QN. The symmetric key is provided to the App at each location and, once the process is finished, $L1-SDNC_1$ communicates to the L2 SDNC the end of the connection and L2 SDNC to $L1-SDNC_2$. Finally, the end users are able to establish an encrypted videoconference.

The same use case is depicted in Figure 5.4, but in the context of the described distributed architecture. The scenario involves the application, controller and QKD device within a quantum network on the origin (domain 1) and destination (domain 2). The App on domain 1 (App_1) makes a request for cryptographic material to its associated QN, which ask $L1-SDNC_1$ for availability to execute a QKD protocol with QN_2. After confirmation, SDNC from domain 1 ($L1-SDNC_1$) communicates to SDNC from domain 2 ($L1-SDNC_2$), which in turns performs its own availability requests with its QN. Once the availability of all the intervening elements has been confirmed, the two local SDNC coordinate and agree the border node between the interdomain segments and each SDNC establishes the intradomain route. The connection between QN_1 and QN_2 is established and a QKD protocol is performed between adjacent nodes. Once the process is finished, the end of the connection is agreed between both SDNC. Finally, the key is provided to the App and the end users establish an encrypted videoconference.

Finally, at the national level we assume a scenario with three domains and, therefore, three L1 SDNCs. In the hierarchical model, local $L1-SDNC_1$ and $L1-SDNC_2$ are managed by regional $L2-SDNC_1$, while $L1-SDNC_3$ is managed by $L2-SDNC_2$. In turn, $L2-SDNC_1$ and $L2-SDNC_2$ are managed by a higher national level $L3-SDNC$. Again, at the local level we consider a single QN per domain, which are also adjacent. In this case, the videoconference is established between the Apps of domains 1 and 3, so we define have a key relay in the QN of domain 2 in between.

All the results obtained about the number of steps required in each scenario to complete the use case and for both integration models are collected in Figure 5.5. As can be seen, in the local case the number of steps is the same for both models to execute the application since the entire process takes place within a single domain and, therefore, management does not depend on external entities. However, as we add domains to the network, the number of steps

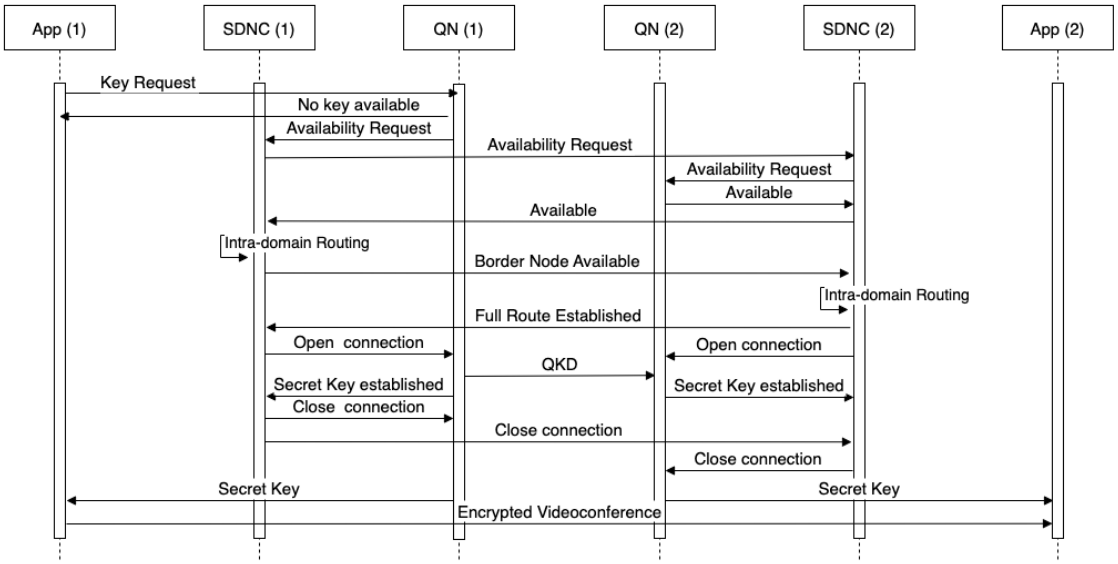


Figure 5.4: Sequence diagram of an encrypted videoconference established between two network domains integrated in a distributed model.

increases, this increase being more evident in the hierarchical case due to the greater number of interactions between the different SDNC levels. Despite presenting a greater number of steps in the hierarchical case than in the distributed case, as the number of domains increases, coordination between *SDNC-L1s* in the distributed model becomes more complex. This is due to that the availability of a path that allows the execution of the complete chain of QKD protocols must be guaranteed and since there is no upper-level management entity, the different *SDNC-L1s* have to exchange much more information to be able to coordinate properly and with an optimal route path.

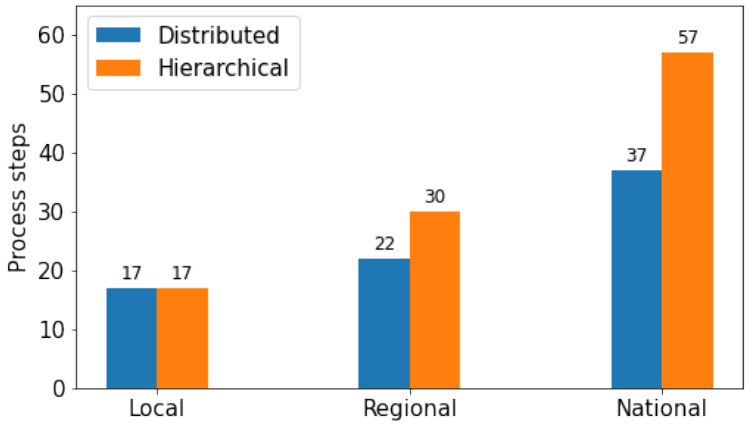


Figure 5.5: Results of the number of steps obtained for the different scenarios applying the distributed and hierarchical models.

In addition to the two integration models presented, it is also possible to define a third hybrid model, which assumes a distributed SDNC system in which, during the execution of a process between several domains, an *SDNC-L1* takes on the role of a master SDNC, centralizing the

information, for that specific process. This would avoid having a single, fixed *SDNC-L2*, thus giving greater flexibility to the network.

5.1.4 Challenges of quantum cryptography

The security risk once quantum computers reach the capabilities necessary to break pre-quantum public key cryptosystems such as RSA or Elliptic-curves families, could be avoided by merging classic internet infrastructures with QCI with new quantum cryptographic algorithms. This integration will also bring new functionalities that could not be achieved with classical internet in isolation. The new functionalities (those that are currently known, since others might be discovered in the future) and the advantages that the complete QI will bring over the classical internet can be summarized as follows:

- High, long-term, security without computational assumptions, i.e. Information Theoretic Security (ITS). Quantum Key Distribution (QKD) makes possible the creation of shared random symmetric keys with unconditional security.
- Increase in security levels by applying widely studied quantum cryptographic protocols and/or quantum assisted protocol such as the quantum-assisted digital signature or quantum zero-knowledge protocols proposed in this thesis, as well as hybrid approaches where pre-quantum, post-quantum and quantum cryptographic tools are integrated. This added to the ability to have systems with cryptoagility, that is, to quickly change from one cryptographic algorithm to another in case the first one is compromised.
- Increase in the efficiency of quantum cryptographic protocols compared to their classic counterparts, under the same operating conditions, as demonstrated in chapter 3.
- Assisted information transmission through quantum entanglement driving to new capabilities such as distributed quantum computing.

These opportunities, except for entanglement distribution capabilities, are already feasible and directly transferable into today's QCI covering metropolitan areas and into space to ground segments.

However, there are a number of elements or conditions that still require development to increase the TRL of certain technology, improve the Size, Weight, Power and Cost (SWaP-C), or to be able to certify quantum cryptographic devices. Throughout chapter 2 we commented on some of the elements that still have a low technological maturity such as QR and QM, but there is also a need of implementing quantum cryptographic solution assuring the end-to-end security of the entire system. For that, the following needs to be guaranteed:

- the implementation of quantum channels with measures against physical attacks or side channel attacks;
- the implementation of quantum cryptographic devices with measures against physical attacks such as the ones identified in [C. Marquardt, 2023];
- the capability to authenticate new cryptographic modules on the network for the very first time;

- the capability to guarantee the identity of a user who access a service to which several users have access, which can be overcome with the execution of the QZKP proposed in chapter 4.;
- the design of key management systems capable of storing, managing, hybridizing and composing pre-quantum, post-quantum and quantum keys;
- the standardization and certification of quantum cryptographic modules;
- the standardization of hybrid cryptosystems combining pre-quantum, quantum and post-quantum cryptographic mechanisms;
- the design of QCI removing the need of intermediate trusted nodes.

In addition, although standards related to different SDN interfaces on quantum networks have already been published by ETSI, there is still a need of standards for a clear interface definition between controllers and between AP-CP (i.e. EWBI and NBI, respectively) in both hierarchical and distributed models but also interfaces between KMS to leverage the integration of quantum communication subnetworks to rise a full QI. All these challenges, point out the need of international programs such as EuroQCI.

5.2 Political sphere

The different national security agencies (NSA) and organizations as relevant as NATO have been following the progress of the quantum communications projects. In addition, they have helped identify the challenges that quantum cryptographic systems present and that need to be addressed by the scientific and industrial community. They have also been following the succession of rounds of the NIST post-quantum algorithm standardization process, reviewed in chapter 2. Given the current status of NIST's activities, and with the availability of the first PQC standards for KEM (FIPS 203) and DSA (FIPS 204 & 205), these organizations have made public, partially or totally, their vision and positioning regarding solutions based on quantum cryptography and post-quantum. Some examples are discussed below:

- **NIST SPECIAL PUBLICATION 1800-38C - Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards** [N. NIST, 2023b]. This document is one of the results of the project executed by the NIST National Center of Cybersecurity Excellence (NCCoE), whose objective is to accelerate the migration of current cryptography vulnerable to quantum computer attacks [N. NIST, 2023a]. During the development of the project, several protocols and modules (SSH, TLS, QUIC, X.509, HSM) have been evaluated and tested to integrate PQC algorithms. In this process, the Transport Layer Security (TLS) protocol has been identified as critical to be protected with PQC solutions, since it is the most used Internet protocol for security worldwide. Other protocols, such as QUIC, have strong dependencies on TLS for key establishment, and the NCCoE has identified protecting SSH and QUIC authentication as "*less urgent as attacks require an active quantum computer during key establishment." the session*". Finally, X.509 certificates and Hardware Security Modules (HSM) have also been tested with PQC algorithms. In the first case, different types of certificates

have been identified in terms of their level of hybridization with classic certificates. For their part, HSMs are critical devices that must migrate pre-quantum asymmetric cryptography to the recommended PQC algorithms.

- **Summary of NATO's Quantum Technologies Strategy** [NATO, 2024]. A brief summary of the main conclusions drawn from NATO's analysis is provided, although the full document remains confidential. However, a clear statement is made about the need for "*coherence in investment, cooperation among allies on technological development opportunities, development and protection of a qualified workforce and greater situational awareness, as well as exchange of information*". Furthermore, NATO considers PQC as a cryptographic solution to be deployed against the threat of the quantum computer, but also contemplates future integration with QKD services.
- **El Centro Criptológico Nacional (CCN) - Recomendaciones para una transición post-cuántica segura** [Nacional, 2022]. This public document provides a clear view of the state of current cryptographic systems, the threat of quantum computers and what is the migration plan recommended by the CCN for this decade. As a differential point, CCN considers the PQC *FrodoKEM* algorithm as an accepted KEM solution, in addition to *CRYSTALS-Kyber*. It is worth noting that, in the short term, the CCN strongly recommends the design of a hybrid solution that combines pre-quantum cryptographic mechanisms with PQC and, in addition, to provide cryptoagility in scenarios where new vulnerabilities are found in the implemented solutions.
- **Position paper on QKD** published by Bundesamt für Sicherheit in der Informationstechnik (BSI-Germany), Agence nationale de la sécurité des systèmes d'information (ANSSI-France), Netherlands National Communications Security Agency (NLNCSA) and Swedish National Communications Security Authority, Swedish Armed Forces [French Cybersecurity Agency (ANSSI) and Swedish National Communications Security Authority, 2024]. This paper presents the official position on QKD solutions and their role in the transition to quantum-resistant cryptography. The overall message is to focus the current migration effort towards PQC and a hybrid solution due to its criticality, but to provide greater support for the study of QKD.
- **"Quantum-Readiness: Migration to Post-Quantum Cryptography" factsheet** [Cybersecurity et al., 2023] created in collaboration between U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA), and NIST. Provides more details on the steps to follow in terms of preparing a cryptographic inventory, preparing the technological roadmap with suppliers, identifying the supply chain, among others, for a rapid migration to quantum-resistant systems.
- **Quantum security technologies** [NCSC, 2020], white paper published by the National Cyber Security Center (NCSC) about their position on QKD and Quantum Random Number Generation (QRNG). They conclude that the use of QKD is not endorsed for any government or military applications and classical RNG still meets their needs. However, the continuation of research activities in QRNG is encouraged.

The conclusion is that in general the implementation of solutions based on post-quantum

cryptography is recommended to face the threat of the quantum computer and the hybridization of PQC with pre-quantum algorithms. However, the continuation of research activities related to quantum technologies is proposed, for a possible use of these technologies in the long term if the technological challenges covered in the previous section are solved to increase their level of maturity and improvement in the SWaP-C, as well as security challenges against implementation attacks and certification of the devices.

5.2.1 Migration plans

As we have just seen, security authorities recommend migrating to quantum-resistant systems as soon as possible. Some of them provided specific calendars, such as the Spanish CCN [Nacional, 2022], where 4 phases of migration have been identified with time frames, as shown in Figure 5.6. Based on the steps identified in the CISA, NSA and NIST's factsheet [Cybersecurity et al., 2023], a prior phase 0 is defined, in order to carry out these steps that are essential before starting a process of these characteristics. Each phase is explained in more detail below.

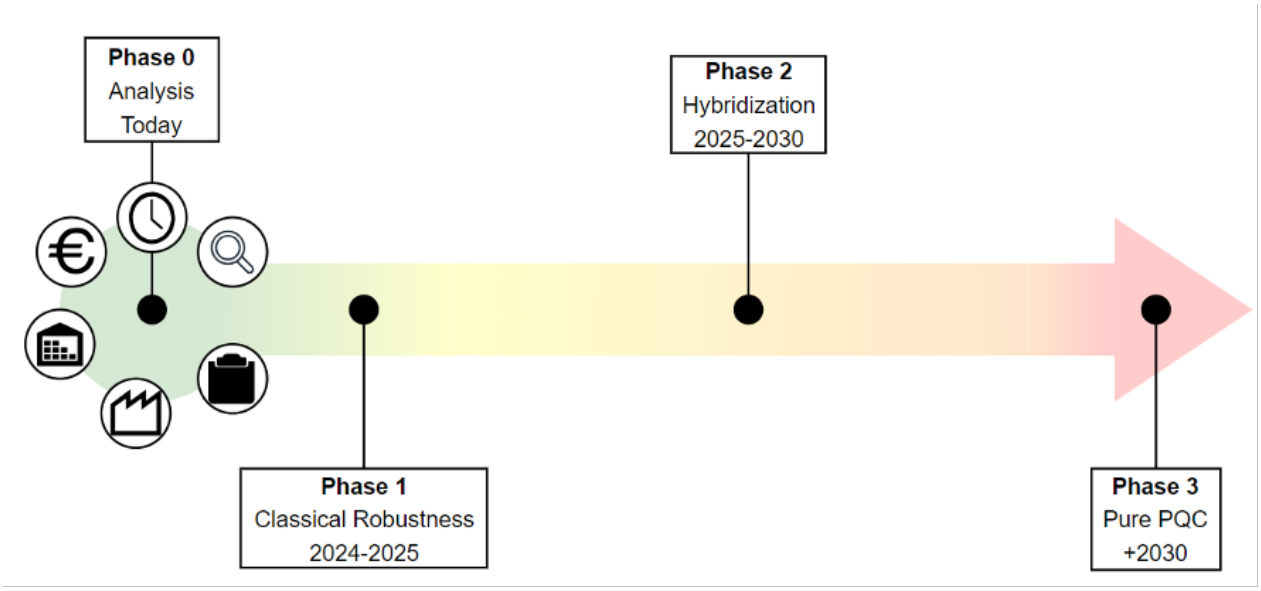


Figure 5.6: Timeline and phases for the migration of systems to quantum-resistant solutions.

Phase 0

Based on the strategies and recommendations published by relevant standardization bodies and national security agencies, a list of steps is presented that must be executed as part of phase 0 represented in Figure 5.6.

- **Step 1** – General evaluation (technical, temporal and financial) of the current state of cryptographic systems. In this step, the entire system must be analyzed, identifying what information should be protected and for how long. Applying Mosca's theorem [Mosca, 2015] to estimate how much time does an organization have available for their specific case. A first estimate of the financing needed for the migration could also be prepared, although this calculation can be made more precisely at the end of step 5.

- **Step 2** – Creation of an inventory of cryptographic products (hardware and software). Create or update a complete inventory of products currently used to protect information systems and assets.
- **Step 3** - Identify which products have been updated by vendors to support CRQC-resistant cryptographic solutions.
- **Step 4** - Determine the supply chain to acquire quantum-resistant products. With the previous inventory and supplier information a decision can be made (from a technical point of view) about what new products are needed, how long it can take the supplier to deliver them, and how long it will take to implement the new products or an update of the inherited in the system.
- **Step 5** – Define a migration plan to hybrid solutions based on priorities. Two main groups of priorities have been identified. The first priority is all systems susceptible to the "store now, decrypt later" attack [Cho, 2019]. The second priority is all systems that require the availability of a CRQC to be compromised. From all the previous information collected, a personalized technical, temporal and financial migration plan can be designed, taking into account the specific recommendations provided by national security agencies.

Phase 1
In this phase the main objective is to increase the security of those pre-quantum cryptographic mechanisms, when possible, that do not need new deployments or features. As an example:

- Maintain symmetric algorithms that make use of keys of at least 256 *bits*.
- The use of *AES* is recommended.
- Hash functions must provide a digest of at least 256 *bits*.
- It is recommended to use SHA2 and SHA3 families that meet the previous condition, that is, SHA2-256, 384, 512 and SHA3-256, 384, 512.

Phase 2
The main objectives of this phase are the migration of pre-quantum public-key cryptography applications (such as secure communications protocols, digital signature protocols, Public Key Infrastructures (PKI), authentication protocols, identity and access management, KMS, etc.) and the implementation of hybrid systems based on standard classical primitives and new PQC solutions. The design of this type of system must consider more than one cryptographic mechanism, avoiding hardcoded implementations. This approach will allow the system to switch from one cryptographic mechanism to another easily and quickly, providing cryptoagility in a scenario where a new vulnerabilities could be found in an algorithm in use. This point becomes especially relevant due to the novelty of the PQC algorithms, which will require more time to continue with their cryptanalysis, as could be seen in chapter 2. The following recommendations for this phase are provided as examples:

- Implement NIST-approved PQC KEM algorithms, such as *CRYSTALS-Kyber* (FIPS 203) [NIST, 2024a], to obtain hybrid or composite keys with pre-quantum KEM solutions.

- Implement NIST-approved PQC DSA algorithms such as *CRYSTALS-Dilithium* (FIPS 204) [NIST, 2024b], *SPHINCS+* (FIPS 205) [NIST, 2024c], or *Falcon* (FIPS under construction).
- Implement approved symmetric algorithms with a key length of at least 256 *bits*.
- Evolve Internet security protocols such as TLS or IKEv2.
- Develop hybrid KMS to manage keys generated through quantum-resistant mechanisms.
- Evolve public key infrastructures (PKI).

A high-level layout on how to implementing crypto-agility capabilities can be approached from different ways. As a first step, the Crypto-Agility Maturity Model (CAMM) proposed by J. S. Hohm et al. [Hohm et al., 2022] might be used to evaluate the system's ability to implement crypto-agility requirements. The CAMM consist of 5 levels, from the lowest maturity level (Initial / Not Possible) to the higher maturity level (Sophisticated), passing through the intermediate levels: Possible, Prepared and Practiced. Each level has several requirements (except for the lowest level) that must be fulfilled to go to the next level. The first levels of the CAMM could be addressed during the development of Phases 0 and 1 of the migration plan. Additional published studies that have been analysed, include the review performed by A. Wiesmaier et al. [Wiesmaier et al., 2021] or the review performed by the Computing Community Consortium (CCC) [Ott, Peikert, et al., 2019]. Below, the list of requirements under the CAMM approach for a successful crypto-agility implementation is provided. These requirements have been divided in general requirements applicable to a previous preparation phase (*Req-G-XX*) and specific and functional requirements of the system (*Req-S-XX*).

- **Req-G-01**. Effectively evaluating crypto-agility requirements necessitates a thorough understanding of the system and its environment.
- **Req-G-02**. System maintainers must have the ability to modify the system and deliver updates to newer software versions.
- **Req-G-03**. The cryptographic functions used are well-documented, and their current security levels are understood.
- **Req-G-04**. All algorithms used are uniquely identifiable.
- **Req-G-05**. The additional effort and impact of ensuring crypto-agility are recognized and accepted.
- **Req-G-06**. A strategy is in place to ensure the overall system remains functional during the transition phase of updates.
- **Req-S-01**. The system is extendable with new cryptographic algorithms and configurable parameters.
- **Req-S-02**. It is possible to roll back the system to a previous state if needed.
- **Req-S-03**. The system's modular design ensures that changes to cryptographic components do not affect the functionality of other interconnected components.

- **Req-S-04**. A common set of cryptographic algorithms is shared across all subsystems.
- **Req-S-05**. The system allows the disabling of unsupported algorithms when required.
- **Req-S-06**. The system consistently employs the strongest available algorithm.
- **Req-S-07**. Policies govern the permissible algorithms and their parameters.
- **Req-S-08**. Hardware and software improvements or replacements are possible independently, with compatibility maintained.
- **Req-S-09**. The system undergoes regular testing to ensure compliance with crypto-agility requirements.
- **Req-S-10**. The crypto-agility mechanism is resistant to attacks.
- **Req-S-11**. New system versions maintain compatibility with older versions.
- **Req-S-12**. Migrating between cryptographic algorithms is achievable within a reasonable timeframe.
- **Req-S-13**. Modifications to crypto-agile modules do not require manual intervention.
- **Req-S-14**. The requirements and techniques used for crypto-agility can be applied to other scenarios.
- **Req-S-15**. The crypto-agility implementation is deployable across additional systems.
- **Req-S-16**. Changes to cryptographic functions take effect in the production system as quickly as possible.
- **Req-S-17**. Cryptographically agile systems are interoperable with one another.

It should be taken into account that hybrid systems are not recommended as a final solution, but rather as an intermediate step to secure systems in the medium term [Nacional, 2022].

During Phase 2, development of a feasibility analysis for the implementation of quantum cryptography capabilities (e.g., QKD-oriented infrastructure) may also be considered. Phase 2 should be completed by 2030, as recommended by national security agencies.

Phase 3
Quantum-resistant cryptographic solutions will eventually become fully established and reliable solutions. Due to this, the objective of phase 3 is to gradually eliminate the use of hybrid solutions, to finally achieve a system based on pure PQC algorithms and, if possible by then, quantum cryptography mechanisms.

5.3 Economical sphere

Since quantum cryptography provides high security mechanisms, this type of technology can greatly benefit sectors such as defence, where classified information is handled. Therefore, this section reviews expenditures and investments in defence and R&D at a global, European and national level in recent decades, which provides an idea of the available business figures

and trends. In addition, an overview is provided of the different European funding programs available for R&D that are serving as economic mechanisms to promote quantum cryptography and quantum communications.

5.3.1 Defence expenditures and business figures

We begin by reviewing the defence expenditures by continent reported by SIPRI [Nan Tian, 2023], between 1988 and 2022. The American continent is the one that has historically invested the most in defence, followed by Europe. There is also a clear growing trend in defence investment in Asia and Oceania as a whole, which in the last two decades has even exceeded European investment. In total, $2,240,000M\$$ was reached in 2022. In Europe there has been an increase in defence expenditures of 13% in 2022, reaching $480,000M\$$. The largest expenditure is concentrated in central and western Europe, with a total of $345,000M\$$. Within the previous metrics, Spain is in position 16 in terms of defence expenditures within the world ranking, with a total of $20.3billion\$$ in 2022. As relevant actors within Europe, with figures above the Spanish we find Germany ($55.8B\$$), France ($53.6B\$$) and Italy ($33.5B\$$).

Moving from the general economic context to a business context, the global market volume in Defence was valued at $1,937,590M\$$ in 2022, and is projected to reach $2,839,520M\$$ in 2031 with a compound annual growth rate (CAGR) around 4.5% [Analytics, 2024].

In terms of turnovers, the Spanish defence industry invoiced a total of 12,130 million euros in 2023 [(Expansion), 2023]. Segmenting the market based on the domains of defence plus security operation, we find that the distribution by segments is as follows (2021 data [(Flynews), 2023]): Space: 2%, Land: 12%, Naval: 20%, Air: 64%, Security: 2%.

It must be taken into account that this segmentation has not considered the fifth domain of cyberspace, which is increasingly taking a more relevant role in the defence sector, especially in the field of communications and cryptography.

5.3.2 R&D expenditures and business figures

Investments in R&D present great differences depending on the continents, always led by North America and Asia, as reported by Eurostat [Eurostat, 2024]. World powers such as Japan and the United States show values around 3.2% and 3% on average, respectively, of Gross Domestic Expenditure on R&D (GERD) relative to Gross Domestic Product (GDP) between 2012 and 2022. For their part, Europe and China have remained on similar values in the last decade with average GERD around 2.1%. However, a growing trend of China, as with investment in Defence, has surpassed Europe. In 2022, the GERD in Europe amounted to 354 billion euros [Eurostat, 2024].

Regarding the breakdown of the GERD relative to Europe's GDP according to the following sectors between 2012 and 2022:

- Business sector. Throughout this period, most of the R&D expenditure was made in the business sector with an average value of around 1.4%, one point above the rest of the sectors considered;

- Higher education sector, with an average value around 0.5%;
- Government sector, with an average value below 0.3%;
- Private non-profit sector. It is the sector with the lowest expenditure on R&D, always below 0.04%.

At the national level, in Spain, there has been a slight increase in gross domestic expenditure on R&D between 2012 and 2022, but always with values below 1.5%. These GERD values broken down by sectors show that, as in the rest of the countries, in Spain the business sector is the one that carried out most of the expenditure in R&D, followed by higher education and government sectors, with similar expenditures.

In the specific case of the quantum communications and quantum cryptography markets, these are jointly valued around USD 0.5 billion in 2023 [Research, 2024a, 2024b]. In the coming years, a growing at a CAGR of 38% is expected. Therefore, by the beginning of the next decade, the quantum communications and cryptography market is estimated to reach a value of around USD 6.8 billion.

This represents an excellent opportunity to continue research in these areas and achieve the necessary technological maturity, promote national industry supporting SMEs and develop military capabilities, thereby boosting European sovereignty in quantum technologies.

5.3.3 European funding mechanisms

The European Union recurrently launches R&D funding and co-funding programs, as part of the European budget and the NextGenerationEU [Commission, 2024b] funds. In 2020, a series of funding opportunities (Multiannual Financial Framework and NextGenerationEU) were launched for the period 2021-2027, divided into 6 large blocks, which are shown in Figure 5.7.

Within each of these blocks we find different sub-blocks that contain one or more financing programs. Some of these programs have already included calls related to the deployment of quantum communications infrastructures, execution of use cases or to increase the level of technological maturity of some components. Specifically, we highlight the following programs within Heading 1: Single Market, Innovation and Digital:

- In the Research&Innovation section with the Horizon Europe (HE) program. Horizon Europe finances R&D projects in a multitude of different topics. It has a total budget of $95,500M€$ between 2021 and 2027 [Commission, 2024e]. The predecessor of this program was Horizon 2020 (H2020), which began in 2014 until 2020 and had a total investment of approximately 80 billion euros.
- In the section European Strategic Investments with Digital Europe Program (DEP). DEP seeks to promote digital transformation in Europe. It has a total budget of $7,590M€$ between 2021 and 2027 [Commission, 2024a].
- In the Space section with the European Space Program (ESP). ESP finances R&D projects in space and satellite technologies. It has a total budget of $14,880M€$ between

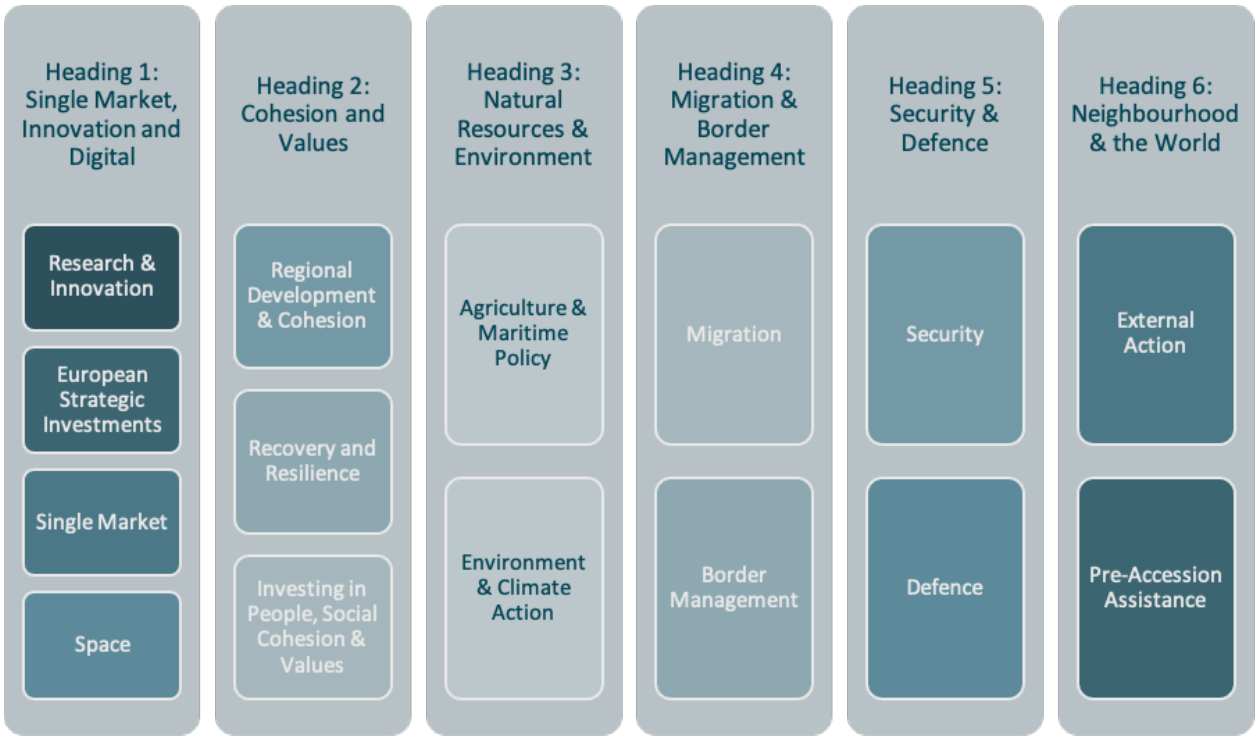


Figure 5.7: European Programs and funds financed by the European budget and NextGenerationEU.

2021 and 2027 [Commission, 2024d].

Under these programs, especially HE and DEP, the Quantum Flagship [QT, 2024] was launched in 2018, an initiative to finance projects related to quantum technologies. Quantum Flagship has a duration of 10 years and a total investment by the European Commission of 1*b*€. Within quantum communications, the OpenQKD project [OPENQKD, 2024] also stood out, covered first under the H2020 program and later by HE. OpenQKD began in 2019 and aimed to mature QKD technologies and implement them in communications infrastructures for the execution of a wide variety of use cases. The project ended in 2023. As a continuation, the EuroQCI [Commission, 2019] program was launched in 2021, with funding from the DEP, for the deployment of quantum communication infrastructures in Europe to, in a later phase, establish lines between them and achieve a pan-European network. The first projects started in January 2023. The unified network model that the EuroQCI program aims to achieve will favor interoperability and cooperation between the QCIs of the member countries and will promote European sovereignty in matters of research, innovation, infrastructure and communications security. With the aim of achieving this network integration, work is being done on the definition of standards through organizations such as ETSI, European Committee for Standardization (CEN), Internet Engineering Task Force (IETF), ISO/IEC and ITU-T, which describe and specify the interfaces that can be used for these networks integration, and that are already being implemented by marketed QKD devices, encryptors, etc., compliant with ETSI standards. Regarding the QKD devices marketed and implemented in quantum communications networks until now, they are, for the most part, original from countries

outside the European Union and non-members of NATO, such as Switzerland, China, Japan. However, thanks to the encouragement of the European Commission, the number of European startups with capabilities in quantum technologies is increasing year after year, allowing greater industrial positioning in this field. Currently, there are more than 5 EU companies able to supply QKD systems.

In addition, the terrestrial QCIs will be linked to the space segments as part of $IRIS^2$ [Commission, 2024f], which aims to create a constellation of satellites capable of providing quantum-resistant secure communications services. These deployments are carried out jointly with the European Space Agency (ESA).

Finally, in Heading 5: Security & defence, the European Defence Fund (EDF) stands out within the Defence section. These types of funds seek to support research and the development of defence capabilities. The EDF has a total budget of $7,950M€$ between 2021 and 2027 [Commission, 2024c]. Initially, they have focused more on the development of quantum sensing capabilities, although in previous programs such as the European defence Industrial Development Program (EDIDP) the DISCRETION [DISCRETION, 2024] project the use of quantum cryptography in the deployment of SDN networks is being defined. Furthermore, in the 2024 call the topic has been extended to also cover quantum communications and quantum-resistant cryptography (both quantum and PQC).

The conclusion is that there are currently large investments in the field of Defence and R&D aimed at the development of quantum technologies. This was to be expected given the criticality of finding alternative secure cryptographic mechanisms to face the threat of a CRQC. As we have seen in section 5.2, this agrees with the public positioning made by several national and international security authorities regarding the new cryptographic paradigms.

5.4 Conclusions

As we have seen throughout the chapter, investments in R&D have increased globally in the last decade and in sectors as specific as defence where technologies related to security are considered critical elements for military operations. In addition to the recent programs launched by the European Commission, there are many funding opportunities for the development of the challenges identified in the 5.1.4 section. The solution to these challenges is of special relevance since they directly impact the concerns raised by the different national security agencies and defence organizations. Managing to address each of these challenges will not only lead to the certification of quantum cryptography devices (e.g. NOSTRADAMUS project with the aim of building a certification infrastructure), but will also allow us to take another step towards the future quantum internet, which is one of the ultimate goals of quantum communication infrastructures.

As describe in chapter 2, terrestrial quantum communications networks have evolved enormously since their initial approaches. However, two strategies continue to prevail for the deployment of this type of networks: infrastructures based on dark fiber dedicated exclusively to quantum communications and infrastructures with the coexistence of classical and quantum communications. Regardless of the chosen strategy, networks of different types have been

deployed and are capable of implementing new functionalities compared to classical networks.

The vision of a quantum internet based on the integration of a set of isolated communication networks leveraged by the EuroQCI program can be facilitated with an SDN perspective, thanks to the reduction in complexity in the data plane, virtualizing management and control functions of the physical elements in the CP. Based on the architecture of each network, they can be integrated through a hierarchical model of controllers that manage subnetworks at different levels or a distributed model where each controller is the owner of a specific domain and is capable of coordinating with neighboring domains SDNC. Each of these models has pros and cons. The hierarchical model is able to reduce the complexity of the operations and provide full network control, however, greater network control means a loss in flexibility for asset reorganization. In addition, to avoid having single points of failure, it requires SDNC redundancy at all levels. The distributed model facilitates the scalability of the network as well as its robustness, since it prevents single point of failures, but it presents a major complexity in operations, demanding robust synchronization mechanisms and prioritization policies.

In addition to the previous challenges, many technological and scientific advances are still required in terms of the development of elements such as quantum repeaters or quantum memories, to finally deploy a functional and economically viable quantum internet.

Chapter 6

Conclusion

In this chapter, the main academic and industrial contributions of this thesis are summarized. In addition, the compliance with the thesis objectives defined in chapter 1 is evaluated. Finally, a series of new objectives are proposed to continue the research, as well as new research lines of interest for the field of quantum-resistant cryptography.

6.1 Main Contributions

In this section we will summarize the academic contributions first, which include scientific publications, conference proceedings and posters. Secondly, industrialization activities are presented, such as participation in industrial working groups, in R&D projects focused on specific applications and activities aimed at business development.

6.1.1 Academic Results

The contributions are divided into articles published or sent to be published in journals, conferences in which the advances and results of the research have been presented, the associated conference proceedings if any, and participation in scientific dissemination events.

Journals

- *Marta I. García-Cid et al. "Experimental implementation of a quantum zero-knowledge proof for user authentication", Opt. Express 32, 15955-15966, 2024. [M. I. García-Cid et al., 2024]* This work, exposed in chapter 4, covers all the research carried out about the QZKP proposed, from the design and security analysis to the experimental results.
- *Marta I. García-Cid et al. "A Feasible Hybrid Quantum-Assisted Digital Signature for Arbitrary Message Length", Submitted to: J. Opt. Commun. Netw.* This work, exposed in chapter 3, covers all the research carried out about the Q-DS proposed, from the design and security analysis to the experimental results, including the comparative evaluation with pre-quantum and post-quantum DSA.

Conferences

- *Marta I. García-Cid et al. "Madrid quantum network: A first step to quantum internet". In Proceedings of the 16th International Conference on Availability, Reliability and Security, ACM DL, pp. 1-7, 2021. [M. I. García-Cid et al., 2021]*
- *Marta I. García-Cid et al. "Disruptive Quantum Safe Technologies". In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, ACM DL, pp. 1-8, 2022. [M. I. García-Cid et al., 2022]*
- *Marta I. García-Cid et al. "Simulated Multiparty Quantum Digital Signature in Cyberspace Operations". In Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Skopje, North Macedonia, IEEE Xplore, pp. 1-9, 2023. [M. I. García-Cid, Aguado, et al., 2023]*
- *Daniel Gómez et al. "Simulated environment for multiparty quantum digital signature across the network". In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, ACM DL, pp. 1-10, 2023. [Gómez Aguado et al., 2023]*
- *Vicente Martín et al. "The Madrid Testbed: QKD SDN Control and Key Management in a Production Network". Proceedings of the 23rd International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, IEEE Xplore, pp. 1-4, 2023. [V. Martin et al., 2023]*
- *Marta I. García-Cid et al. "Quantum Zero-Knowledge Protocol for Identity Authentication". In Proceedings of the Quantum Engineering and Technology Conference (QET), London, UK, IEEE Xplore, pp. 15-18, 2023. [M. I. García-Cid, Bodanapu, et al., 2023]*
- *Marta I. García-Cid et al. "Firma digital híbrida asistida por distribución cuántica de claves". In Proceedings of the X Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d), Cartagena, Spain, 2023. [e. a. García-Cid, 2023a]*
- *Marta I. García-Cid and Rodrigo Sánchez. "A Feasible Hybrid Protocol for Quantum-Assisted Digital Signature". XVII Jornadas STIC CCN-CERT & V Jornadas de Ciberdefensa ESPDEF-CERT, Madrid, España, 2023. [M. I. García-Cid and Martin, 2023]*
- *Marta I. García-Cid. "Research lines on Quantum Cryptography applied to the Defence sector". European Conference Quantum Technologies and Defence Applications, Warsaw, Poland, 2024. [M. I. García-Cid, 2024b]*
- *Marta I. García-Cid et al. "Experimental Realization of a Quantum Zero-Knowledge Proof". QUANTUMatter Conference, San Sebastian, Spain, 2024. [e. a. García-Cid, 2024b]*
- *Marta I. García-Cid. "Cryptographic Primitives Beyond QKD: Applicability in LEO Satellites". 7th Annual ScyLight Conference & 2nd Quantum Workshop, Eindhoven, The Netherlands, 2024. [M. I. García-Cid, 2024a]*
- *Marta I. García-Cid et al. "Comparative Evaluation of Quantum-Resistant Digital Signatures". International Conference on Quantum Communications, Networking, and*

Computing (QCNC 2024), Kanazawa, Japan, 2024. [e. a. García-Cid, 2024a]

- *Marta I. García-Cid et al. "PQ-REACT: Post Quantum Cryptography Framework for Energy Aware Contexts". The 19th International Conference on Availability, Reliability and Security, Vienna, Austria, 2024. [e. a. García-Cid, 2024d]*
- *Marta I. García-Cid et al. "Panorama Geoestratégico y Tecnológico de la Criptografía Cuántica y Post-Cuántica". In Proceedings of the XI Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d), Jaén, Spain, 2024. [e. a. García-Cid, 2024c]*
- *Marta I. García-Cid et al. "Strategies for the Integration of quantum networks for a future quantum internet", Under preparation to be submitted to: International Conference on Military Communication and Information Systems (ICMCIS25).* This work, exposed in chapter 5, covers all the analysis carried out concerning current deployments of QCI and the requirements to achieve the ambitious quantum internet, proposing for this aim two models for networks integration and testing them through simulations.

Posters

- *Marta I. García-Cid et al. "Quantum-Assisted Digital Signature for user authentication in military operations". NATO Quantum technology for defence and security Research symposium, Amsterdam, The Netherlands, 2023. [e. a. García-Cid, 2023b]* See Figure 6.1

Dissemination Events

This section lists the dissemination activities carried out throughout the period included in the thesis. In this case, the information transmitted to listeners is purely informative and aimed at an audience (technical or not) without in-depth expertise about the subject, unlike previous publications and conferences, where the presentations have higher technical and scientific nature. The dissemination activities carried out have been:

- Marta I. García-Cid and Domingo Castro. "La comunicación cuántica: de dónde venimos y hacia dónde vamos". Podcast Indra Engineering the future talks, 2022. Available in Apple Podcasts, YouTube, iVoox, Spotify, Google Podcast and Podimo. [M. I. García-Cid and Castro, 2023]
- Luz Gil (Indra), Ana Ruiz (Indra), Marta Irene García-Cid (Indra) and Benjamín Villalonga (Google). "Tecnologías Cuánticas: desafiando los límites de la tecnología". Meetup LinkedIn Engineering+Technology Campus, 2023. Available in LinkedIn. [e. a. García-Cid, 2023c]
- Grupo de investigación en Información y Computación Cuántica (GIICC). Semana de la Ciencia, UPM, 2023 & 2024. [GIICC, 2024]

6.1.2 Industrialization Activities

Below, the activities carried out within the industrial field are described, which are divided into three groups. In the first group, the participation in industrial working groups for the

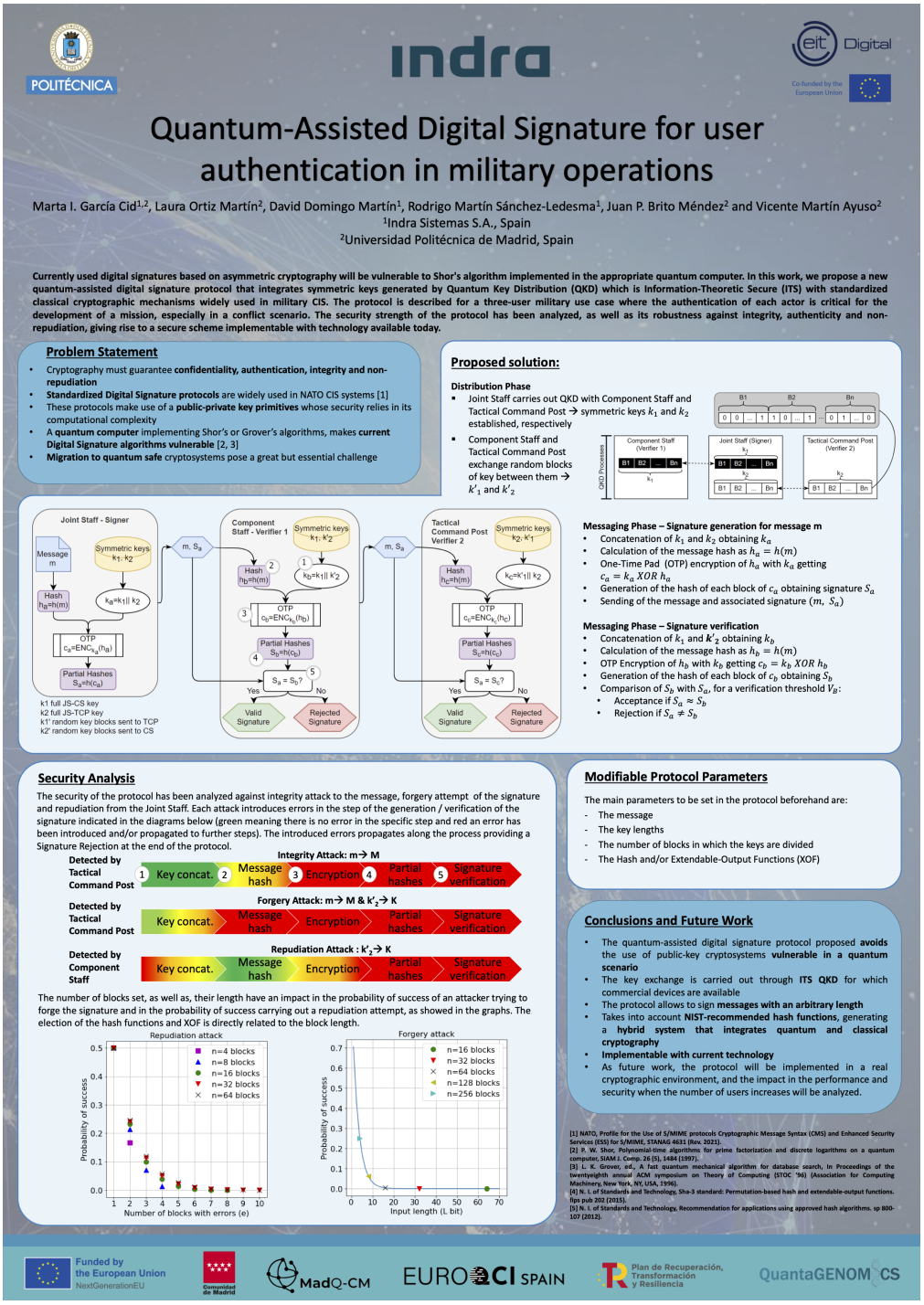


Figure 6.1: Poster presented during the NATO Quantum technology for defence and security Research symposium, in Amsterdam, The Netherlands, in 2023.

generation of knowledge and roadmaps is covered. The objective of this type of activities is to inform and raise awareness of the technology, to possible end users and corporations capable of industrializing them. The second group includes the activities carried out as part of the R&D projects where specific applications of quantum cryptography aimed at end users have been identified and defined, mainly in the defense sector. Finally, the third group are all those activities aimed at business development, such as the development of a product strategy and business plan.

Industrial Working Groups

There are several industrial working groups focused on different quantum technologies. The objective of these groups is to promote these technologies in industrial activities, make small and medium-sized enterprises (SME) visible, cooperate with other institutions, analyze the technological landscape and define industrial strategies and roadmaps. Meetings are usually held where the most relevant advances in each field are presented, presentations of new start-ups, main industrial players, etc, in order to establish relationships between the different actors for further collaborations. Below are the main associations and working groups in which I have participated:

- European Innovation Council (EIC) NEXT-GEN COMPUTING.
  https://eicscalingclub.eu/club
- European Quantum Industry Consortium (QuIC).
  https://www.euroquic.org/
- NATO working group (NATO IST SET).
  https://www.nato.int/cps/en/natohq/topics_88745.htm
- Quantum Security and Defense Working Group.
  https://www.linkedin.com/showcase/quantumdefenseeu/

R&D Projects

Thanks to the different funding mechanisms specified in chapter 5, or other mechanisms such as national funds (i.e. complementary plans, COINCIDENTE, etc.), it has been possible to increase the TRL of technologies, but also the identification of specific use cases with the involvement of interested end users.

Specifically, I have carried out activities in this context and being part of several projects related to quantum communications and quantum-resistant cryptography, such as:

- CARAMUEL [Agency, 2023] to on board a quantum payload in a satellite to achieve geostationary QKD. The output was the delivery of a feasibility study and the design of the system architecture.
- PQREACT [PQREACT, 2023] to design and develop a framework to facilitate the transition from classical to quantum-resistant cryptosystems, including quantum and post-quantum solutions. The, this framework will be implemented in several use cases.
- EuroQCI Spain [Spain, 2023] to enhance the Spanish quantum communication infras-

tructure in Madrid and Barcelona and implement different use cases together with strategic end users.

Business Development

As part of the European Institute of Technology (EIT) Digital grant for the support of this thesis, it was required the development of a Business Development Experience (BDExp) within a company, that is, Indra. The main objective of the BDExp was to develop a product-oriented business plan making use of the knowledge acquired during the EIT Digital seminars and the guidance received during the 6 months of BDExp at Indra. In this case, a business opportunity was detected giving rise to the definition of a specific product.

During the BDExp, I have been in charge of developing a series of activities to accomplish the previous objective. For these activities, several results were expected. The activities and associated results are gathered in Table 6.1. Part of the results of these activities have been covered in chapter 5.

Table 6.1: Business development activities and outcomes

Activity	**Expected Outcome(s)**
Identification of a business opportunity	Business opportunity and Schematic of the points to be covered in the product strategy and business plan
Development of a product definition	Report with description of the product, basic functionalities, products in the markets and users
Market Analysis	Report on Defence and R&D expenditures and investments, and European funding mechanisms
Analysis of potential customers	Customer Persona Definition Customer Journey Description
Analysis of competitors	Competitors comparative table Competitors positioning map
Development of product strategy proposal	Report on product strategy
Development of a related business plan	Data sheet with investment and revenue calculations Final report of the business plan

These results shall define a baseline for progressively integrate the quantum security paradigm to this portfolio while increasingly enhance its maturity level and integrating customer service requirements. It is worth to highlight that most of the mid-term and long-term capacitation roadmaps in which the company participates assume the applicability of related quantum-resistant solutions. These results aim to respond to this roadmap in the medium-long term and to provide a business plan with a clear objective of positioning in the market.

6.2 Assessment of Objectives

In this section we evaluate the fulfillment of the objectives of the thesis, described in chapter 1. To do this, a summary is provided about how each of these objectives have been addressed and what the main results are.

O1. *Study of the state of the art of quantum communications networks and the cryptographic landscape, identifying a series of challenges and opportunities.* This objective is addressed in chapter 2 in terms of the analysis of the types of networks deployed and their main characteristics, but also in chapter 5, covering the analysis from an economic and political point of view, with the purpose of defining the future of the quantum communications. Among the communications infrastructures deployed so far, three different approaches stood out depending on whether the network had been deployed for quantum communications experimentation, if infrastructures shared with classical communications were being used, and if network management was using the SDN paradigm. This distinction provides a lot of information about the possible services that a certain QCI can offer and its technical and economic scalability. In the specific case of networks with shared infrastructure, deployment costs are drastically reduced. Furthermore, the use of the SDN paradigm allows functions that are usually performed at the hardware level to be abstracted and virtualized to be carried out at the software level. This has allowed networks like MadQCI to achieve great heterogeneity in terms of implemented cryptographic devices and, therefore, services that can be offered and designed. This has paved the way to address objectives O2 and O3, since the design of cryptographic protocols must be implementable in this type of QCI and without the need for an exclusive hardware unit for the execution of each primitive. Thus, both the Q-DS and QZKP protocols use QKD devices for their execution. For QZKP it is necessary to slightly modify its configuration but not the internal optical components. Both protocols are implementable in current QCI. Furthermore, the study of quantum communications networks described in chapter 2, together with the monitoring of the international cryptographic panorama addressed in chapter 5, have allowed the identification of a series of technological and security challenges that have to be addressed in order to achieve the goal of the EuroQCI program of having a pan-European quantum communications infrastructure, as well as the European funding mechanisms under which specific problems can be further investigated. Among the challenges at the infrastructure level, the definition of a joint strategy for the integration of the different national QCIs stands out. Concerning the challenges about security, they could be grouped into three large groups: 1) solutions to implementation and physical attacks, 2) authentication mechanisms, 3) hybrid key management capabilities. Solving these challenges would make possible the certification of these devices, which is the necessary step for the total acceptance by the NSA of quantum cryptography as a mature solution to be used in daily operations.

O2 *Design, analyze and implement a new quantum digital signature protocol.* Digital signatures are critical and essential elements in current communications, so it is necessary to investigate alternative solutions to vulnerable pre-quantum asymmetric algorithms. Beyond the signature algorithms that have being standardized by NIST, i.e. CRYSTALS-Dilithium (FIPS 204) and SPHINCS+ (FIPS 205), and FALCON (still under standardization), in this thesis a digital signature protocol, which is quantum-assisted, has been proposed. This protocol releases most

of the limits of previous QDS protocols in the literature. It composes keys generated by QKD with pre-quantum symmetric mechanisms. As stated in chapter 3, the protocol has been analyzed for message integrity attacks, signature forgery attempts and repudiation attempts by the author of the message and the signature, proving to be secure. In addition, the Q-DS protocol allows a large number of configurations depending on the level of security needed. As we have seen in the previous objective, the protocol is implementable in current QCI and it does not present additional infrastructure requirements or changes at the hardware or configuration level of the QKD device. By comparing its performance against several pre-quantum signature algorithms and the standardized PQC ones, we have been able to demonstrate that Q-DS outperforms in the signature generation and verification processes, with the least efficient process being key generation through QKD. However, as the technology improves, it is expected to achieve a key generation rate comparable to pre-quantum ones and even higher. Finally, the Q-DS protocol has been presented in several scientific and industrial forums since the design stage, which has allowed obtaining early feedback from different points of view. With all these results, it is considered that the O2 objective has been met and it is expected that this work will serve as a step forward in the research of new quantum-assisted digital signature protocols.

O3 *Design, analyze and implement a new quantum zero-knowledge protocol.* One of the challenges identified as part of O1, and which is included in chapter 5, is "*the capability to guarantee the identity of a user who access a service to which several users have access*". To address this challenge, a zero-knowledge proof was designed, transferring this classic concept to a system based on the generation and measurement of quantum states, giving rise to the QZKP that is explained in chapter 4. This QZKP was designed in such a way that the three basic properties of a ZKP were met, that is, completeness, soundness and zero-knowledge. At the end of the research, thanks to the availability of the devices developed by the Politecnico di Milano, the implementation and evaluation of the QZKP were possible. As we have commented before, the hardware requirements for the proposed QZKP are the same as for a conventional QKD device, the only change is in the configuration when preparing and measuring the qubits, where the choice of bases is dependent on a foreknown secret. In the experimental phase, the QZKP was executed with both the prover and the verifier being honest users, and the case in which the prover tries to make a fraudulent authentication. In both scenarios, we were able to validate the proof without any false positive or false negative in the hundreds of iterations. A differential point with respect to Q-DS is that no work or proposal for quantum ZKP has been found in the literature at the moment of the research, which is why the novelty of the work carried out stands out. Finally, the QZKP has also been presented at several conferences and the work is published in open access format [M. I. García-Cid et al., 2024], so we conclude that the O3 objective has been met.

We can also conclude that the starting requirements identified in O1 for the fulfillment of the general objective of the thesis, that is, *investigating solutions based on quantum cryptography that go beyond the quantum distribution of keys*, have been met both in the case of the Q-DS as in that of the QZKP. As a reminder these requirements were:

- the proposal of cryptographic mechanisms resistant to a relevant quantum computer as an alternative to the pre-quantum mechanisms considered vulnerable (covered by Q-DS

and QZKP);

- the new cryptographic protocols are, at least, comparable with the pre-quantum and post-quantum protocols in efficiency (covered by Q-DS);
- the protocols are implementable in current quantum communications infrastructures to amortize the investment made in current deployments (covered by Q-DS and QZKP).

In summary, we conclude that this thesis has provided a step forward to new quantum cryptographic primitives.

6.3 Future Work

As we have commented previously, given the position of the different national security agencies regarding quantum cryptography, future work will focus on solving the challenges identified in chapter 5 with the ultimate goal of promoting the certification of these cryptographic devices. These challenges that will allow us to achieve the final objective of certification are grouped into three categories, the first covering everything related to implementation and physical attacks, both of quantum channels and cryptography devices. The second group about authentication mechanisms, this is authentication of new devices on the network for the very first time, classic channel authentication and user authentication. And, finally, the third group for the development of hybrid key management capabilities, which includes everything from the design of key management systems capable of storing and managing pre-quantum, post-quantum and quantum keys to the standardization of hybrid and composite cryptosystems combining pre-quantum, quantum and post-quantum cryptographic mechanisms.

This is the general orientation of future research but, as specific next steps regarding the protocols addressed in this thesis, we identify the following. The Q-DS protocol has been designed and its security analyzed in a three-user scenario, so it is still necessary to extend the analysis to environments with more than two possible verifiers and under collective attacks. Once this analysis is done, the implementation and execution of the protocol in a QCI, generating and verifying signatures between several users will allow us to validate the solution in a relevant environment outside the laboratory. The same goes for the QZKP, which has so far been tested in a laboratory environment.

Furthermore, when transferring these protocols to network environments, it would be advisable to analyze in detail the current ETSI 014 and ETSI 004 standards, which define the key provisioning interface to applications, to determine if evolutions are required to support services beyond the provision of distilled QKD keys for the encryption of communications. Therefore, further steps will focus on deploying the proposed primitives to test them in the already deployed QCI.

References

A. Vaira, e. a. (2024). Post-quantum cryptography migration use cases [https://www.ietf.org/archive/id/draft-vaira-pquip-pqc-use-cases-01.html#name-composite-signatures [Accessed: 28th May 2024]].

Acin, A., Gisin, N., & Scarani, V. (2004). Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Physical Review A*, *69*(1), 012309.

Agency, E. S. (2019). Saga for quantum key distribution [https://www.esa.int/ESA_Multimedia/Images/2019/04/SAGA_for_quantum_key_distribution [Accessed: 28th May 2024]].

Agency, E. S. (2023). Caramuel (geo qkd hosted payload) phase a [https://connectivity.esa.int/projects/caramuel [Accessed: 28th May 2024]].

Agency, E. S. (2024). Esa's artes core competitiveness programme helps european and canadian industry to develop innovative satcom products, services, systems and partnerships [https://connectivity.esa.int/core-competitiveness [Accessed: 28th May 2024]].

Aguado, A., Hugues-Salas, E., Haigh, P. A., Marhuenda, J., Price, A. B., Sibson, P., Kennard, J. E., Erven, C., Rarity, J. G., Thompson, M. G., et al. (2017). Secure nfv orchestration over an sdn-controlled optical network with time-shared quantum key distribution resources. *Journal of Lightwave Technology*, *35*(8), 1357–1362.

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., Folgueira, J., & Martin, V. (2019). The engineering of software-defined quantum key distribution networks. *IEEE Communications Magazine*, *57*(7), 20–26.

Aguado, A., Lopez, V., Martinez-Mateo, J., Peev, M., Lopez, D., & Martin, V. (2018). Virtual network function deployment and service automation to provide end-to-end quantum encryption. *Journal of Optical Communications and Networking*, *10*(4), 421–430.

Aguado, A., Lopez, V., Martinez-Mateo, J., Szyrkowiec, T., Autenrieth, A., Peev, M., Lopez, D., & Martin, V. (2017). Hybrid conventional and quantum security for software defined and virtualized networks. *Journal of Optical Communications and Networking*, *9*(10), 819–825.

Aguado, A., López, D. R., Pastor, A., López, V., Brito, J. P., Peev, M., Poppe, A., & Martín, V. (2020). Quantum cryptography networks in support of path verification in service function chains. *Journal of Optical Communications and Networking*, *12*(4), B9–B19.

Aguado, e. a., A. (2016). Quantum-aware software defined networks. *In 6th International Conference on Quantum Cryptography (QCRYPT 2016): Washington, DC, September 12-16, 2016 Article 188 QCrypt.*

Alabaichi, A., Ahmad, F., & Mahmod, R. (2013). Security analysis of blowfish algorithm. *2013 Second International Conference on Informatics & Applications (ICIA)*, 12–18.

Albash, T., & Lidar, D. A. (2018). Adiabatic quantum computation. *Reviews of Modern Physics*, *90*(1), 015002.

Aldama, e. a., J. (2022). Integrated qkd and qrng photonic technologies. *Journal of Lightwave Technology*, *40*(23), 7498–7517.

Ali, J., & Roh, B.-H. (2020). An effective hierarchical control plane for software-defined networks leveraging topsis for end-to-end qos class-mapping. *Ieee Access*, *8*, 88990–89006.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851–1877.

Amiri, R., Wallden, P., Kent, A., & Andersson, E. (2016). Secure quantum signatures using insecure quantum channels. *Physical Review A*, *93*(3), 032325.

Analytics, I. A. (2024). World defense budget analysis market size, share & trends analysis report [https://www.insightaceanalytic.com/report/world-defense-budget-analysis-market/2171 [Accessed: 28th May 2024]].

Ang, e. a., J. (2014). Arquin: Architectures for multinode superconducting quantum computers. *Transactions on Quantum Computing*, *5*(3), 1–59.

Backes, M., Camenisch, J., & Sommer, D. (2005). Anonymous yet accountable access control. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 40–46.

Barker, E., Chen, L., Davis, R., et al. (2018). Recommendation for key-derivation methods in key-establishment schemes. *NIST Special Publication*, *800*, 56C.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical review letters*, *68*(21), 3121.

Bennett, C. H., Brassard, G., Crépeau, C., & Skubiszewska, M.-H. (1991). Practical quantum oblivious transfer. *Annual international cryptology conference*, 351–366.

Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without bell's theorem. *Physical review letters*, *68*(5), 557.

Beullens, W. (2022). Breaking rainbow takes a weekend on a laptop. *Annual International Cryptology Conference*, 464–479.

Biham, E., Boyer, M., Boykin, P. O., Mor, T., & Roychowdhury, V. (2000). A proof of the security of quantum key distribution. *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, 715–724.

Bindel, N., Herath, U., McKague, M., & Stebila, D. (2017). Transitioning to a quantum-resistant public key infrastructure. *Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8*, 384–405.

Bishop, e. a., L. S. (2017). Quantum volume. *Storage Consortium: Technical Report*.

Blum, M., Feldman, P., & Micali, S. (2019). Non-interactive zero-knowledge and its applications. In *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali* (pp. 329–349).

C. Marquardt, e. a. (2023). A study on implementation attacks against qkd systems [https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html [Accessed: 28th May 2024]].

Castryck, W., & Decru, T. (2023). An efficient key recovery attack on sidh. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 423–447.

Chen, T.-Y., Jiang, X., Tang, S.-B., Zhou, L., Yuan, X., Zhou, H., Wang, J., Liu, Y., Chen, L.-K., Liu, W.-Y., et al. (2021). Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information*, *7*(1), 134.

Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, *589*(7841), 214–219.

Cho, J. Y. (2019). Securing optical networks by modern cryptographic techniques. *Secure IT Systems: 24th Nordic Conference, NordSec 2019, Aalborg, Denmark, November 18–20, 2019, Proceedings 24*, 120–133.

Ciurana, A., Martin, V., Martinez-Mateo, J., Schrenk, B., Peev, M., & Poppe, A. (2014). Entanglement distribution in optical networks. *IEEE Journal of Selected Topics in Quantum Electronics*, *21*(3), 37–48.

Ciurana, A., Martínez-Mateo, J., Peev, M., Poppe, A., Walenta, N., Zbinden, H., & Martín, V. (2014). Quantum metropolitan optical network based on wavelength division multiplexing. *Optics express*, *22*(2), 1576–1593.

Commission, E. (2019). The european quantum communication infrastructure (euroqci) initiative [https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci [Accessed: 27th May 2024]].

Commission, E. (2024a). Digital europe programme [https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en [Accessed: 28th May 2024]].

Commission, E. (2024b). Eu funding programmes [https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes_en [Accessed: 28th May 2024]].

Commission, E. (2024c). European defence fund [https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/european-defence-fund_en [Accessed: 28th May 2024]].

Commission, E. (2024d). European space programme [https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/european-space-programme_en [Accessed: 28th May 2024]].

Commission, E. (2024e). Horizon europe [https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/horizon-europe_en [Accessed: 28th May 2024]].

Commission, E. (2024f). Infrastructure for resilience, interconnectivity and security by satellite [https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en [Accessed: 28th May 2024]].

Conrad, A., Isaac, S., Cochran, R., Sanchez-Rosales, D., Wilens, B., Gutha, A., Rezaei, T., Gauthier, D. J., & Kwiat, P. (2021). Drone-based quantum key distribution (qkd). *Free-space laser communications XXXIII*, *11678*, 177–184.

Courtland, R. (2017). Google aims for quantum computing supremacy [news]. *IEEE Spectrum*, *54*(6), 9–10.

Cryptography, Q. (1984). Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India*, 175–179.

Cybersecurity & (CISA), I. S. A. (2024). Widespread it outage due to crowdstrike update [https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update [Accessed: 17th Nov 2024]].

Cybersecurity, Infrastructure Security Agency (CISA), t. N. S. A. (, the National Institute of Standards, & (NIST), T. (2023). Quantum-readiness: Migration to post-quantum cryptography.

Deutsch, D. (1985). Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, *400*(1818), 97–117.

DISCRETION. (2024). Disruptive sdn secure communications for european defence [https://discretion-eu.com [Accessed: 28th May 2024]].

Dunjko, V., Wallden, P., & Andersson, E. (2014). Quantum digital signatures without quantum memory. *Physical review letters*, *112*(4), 040502.

E. Barker, L. C., & Davis, R. (2024). Sp 800-56cr2: Recommendation for key-derivation methods in key-establishment schemes [https://doi.org/10.6028/NIST.SP.800-56Cr2 [Accessed: 28th May 2024]].

Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Physical review letters*, *67*(6), 661.

Elliott, C. (2018). The darpa quantum network. In *Quantum communications and cryptography* (pp. 91–110). CRC Press.

ETSI. (2006). Etsi tr 102 512: Terrestrial trunked radio (tetra); security requirements analysis for modulation enhancements to tetra [https://www.etsi.org/deliver/etsi_tr/102500_102599/102512/01.01.01_60/tr_102512v010101p.pdf [Accessed: 28th May 2024]].

ETSI. (2016). Etsi eg 203 310: Cyber; post quantum computing impact on ict systems; recommendations on business continuity and algorithm selection [https://www.etsi.org/deliver/etsi_eg/203300_203399/203310/01.01.01_60/eg_203310v010101p.pdf [Accessed: 28th May 2024]].

ETSI. (2017). Etsi gr qsc 006: Quantum-safe cryptography (qsc); limits to quantum computing applied to symmetric key sizes [https://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf [Accessed: 28th May 2024]].

ETSI. (2019). Etsi 014: Quantum key distribution (qkd); protocol and data format of rest-based key delivery api [https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf [Accessed: 28th May 2024]].

ETSI. (2020). Etsi 004: Quantum key distribution (qkd); application interface [https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf [Accessed: 28th May 2024]].

ETSI. (2022a). Etsi 015: Quantum key distribution (qkd); control interface for software defined networks [https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf [Accessed: 28th May 2024]].

ETSI. (2022b). Etsi 018: Quantum key distribution (qkd); orchestration interface for software defined networks [https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018v010101p.pdf [Accessed: 28th May 2024]].

ETSI. (2024). European telecommunications standards institute [https://www.etsi.org [Accessed: 27th May 2024]].

Eurostat. (2024). R&d expenditure [https://ec.europa.eu/eurostat/statistics-explained [Accessed: 28th May 2024]].

(Expansion), C. D. (2023). La industria de defensa atisba cifras pre-covid tras facturar 12.130 millones [https://www.expansion.com/empresas/industria/2023/11/22/655d10cce5fdea37028b45b1.html [Accessed: 28th May 2024]].

Feynman, R. (1985). Quantum mechanical computers. *Optics news*, *11*(2), 11–20.

Fiat, A., & Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. *Conference on the theory and application of cryptographic techniques*, 186–194.

(Flynews), E. A. (2023). Cifras clave de la industria de defensa en españa [https://flynews.es/feindef-2023/cifras-clave-de-la-industria-de-defensa-en-espana/ [Accessed: 28th May 2024]].

Forouzan, B. A. (2007). *Cryptography & network security*. McGraw-Hill, Inc.

French Cybersecurity Agency (ANSSI), N. N. C. S. A. (, Federal Office for Information Security (BSI), & Swedish National Communications Security Authority, S. A. F. (2024). Position paper on quantum key distribution [https://www.bsi.bund.de [Accessed: 27th May 2024]].

Gabay, D., Akkaya, K., & Cebe, M. (2020). Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Transactions on Vehicular Technology*, *69*(6), 5760–5772.

Gaitan, F. (2008). *Quantum error correction and fault tolerant quantum computing*. CRC Press.

Gallager, R. (1962). Low-density parity-check codes. *IRE Transactions on information theory*, *8*(1), 21–28.

Gambetta, J. (2023). The hardware and software for the era of quantum utility is here [https://www.ibm.com/quantum/blog/quantum-roadmap-2033 [Accessed: 17th Nov 2024]].

García-Cid, e. a., Marta I. (2023a). Firma digital híbrida asistida por distribución cuántica de claves [https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/deseid_2023/Paginas/Defensa.aspx [Accessed: 17th Nov 2024]]. *X Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d)*, 1–4.

García-Cid, e. a., Marta I. (2023b). Quantum-assisted digital signature for user authentication in military operations [https://events.sto.nato.int/index.php/upcoming-events/download.file/2870 [Accessed: 17th Nov 2024]].

García-Cid, e. a., Marta I. (2023c). Tecnologias cuanticas: Desafiando los limites de la tecnologia [https://www.linkedin.com/events/tecnolog-ascu-nticas-desafiando7119595192701087744/theater/ [Accessed: 28th May 2024]].

García-Cid, e. a., Marta I. (2024a). Comparative evaluation of quantum-resistant digital signatures. *International Conference on Quantum Communications, Networking, and Computing (QCNC)*, 226–230.

García-Cid, e. a., Marta I. (2024b). Experimental realization of a quantum zero- knowledge proof [https://phantomsfoundation.com/QUANTUM/2024/Abstracts/2024_Garcia_Cid_Marta_Irene_319.pdf [Accessed: 2nd June 2024]].

García-Cid, e. a., Marta I. (2024c). Panorama geoestratégico y tecnológico de la criptografía cuántica y post-cuántica [https://www.tecnologiaeinnovacion.defensa.gob.es/es-

es/Presentacion/deseid_2024/Paginas/Defensa.aspx [Accessed: 17th Nov 2024]]. *XI Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d)*, 1–7.

García-Cid, e. a., Marta I. (2024d). Pq-react: Post quantum cryptography framework for energy aware contexts. *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–7.

García-Cid, M. I. (2024a). 7th annual scylight conference and 2nd quantum workshop [https://atpi.eventsair.com/scylightconference2024/ [Accessed: 17th Nov 2024]].

García-Cid, M. I. (2024b). European conference quantum technologies for defence current and future capabilities [https://defence-industry-space.ec.europa.eu/european-conference-quantum-technologies-defence-current-and-future-capabilities-2024-02-13_en [Accessed: 17th Nov 2024]].

García-Cid, M. I., Aguado, D. G., Martín, L. O., & Ayuso, V. M. (2023). Simulated multiparty quantum digital signature in cyberspace operations. *2023 International Conference on Military Communications and Information Systems (ICMCIS)*, 1–9.

García-Cid, M. I., Álvaro González, J., Ortíz Martín, L., & Del Río Gómez, D. (2022). Disruptive quantum safe technologies. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–8.

García-Cid, M. I., Bodanapu, D., Martín, R., Ortiz, L., Martín, V., Brunero, M., Gatto, A., & Martelli, P. (2023). Quantum zero-knowledge protocol for identity authentication. *Quantum Engineering and Technology Conference (QET 2023)*, *2023*, 15–18.

García-Cid, M. I., Bodanapu, D., Gatto, A., Martelli, P., Martín, V., & Ortiz, L. (2024). Experimental implementation of a quantum zero-knowledge proof for user authentication. *Opt. Express*, *32*(9), 15955–15966. https://doi.org/10.1364/OE.517754

García-Cid, M. I., & Castro, D. (2023). La comunicación cuántica: De dónde venimos y hacia dónde vamos [https://podcasts.apple.com/es/podcast/la-comunicaci%C3%B3n-cu%C3%A1ntica-de-d%C3%B3nde-venimos-y-hacia/id1621047580?i=1000560494321&l=ca [Accessed: 28th May 2024]].

García-Cid, M. I., & Martin, R. (2023). A feasible hybrid protocol for quantum-assisted digital signature [https://youtu.be/ejZmjcAvu7o?feature=shared [Accessed: 28th May 2024]].

García-Cid, M. I., Ortiz, L., & Martín, V. (2021). Madrid quantum network: A first step to quantum internet. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–7.

Gatto, A., Brito, J. P., Brunero, M., Bodanapu, D., Mendez, R. B., Vicente, R. J., Comi, P., Martin, V., & Martelli, P. (2021). Quantum technologies for future quantum optical networks. *2021 International Conference on Optical Network Design and Modeling (ONDM)*, 1–5.

Gatto, A., Brunero, M., Ferrari, M., Tarable, A., Bodanapu, D., Brito, J. P., Mendez, R. B., Vicente, R. J., Bianchi, F., Frittelli, M., et al. (2021). A bb84 qkd field-trial in the turin metropolitan area. *Photonics in Switching and Computing*, Tu1A–2.

GIICC. (2024). Tecnologias cuanticas: Desafiando los limites de la tecnologia [https://blogs.upm.es/semanadelaciencia/actividad/comunicaciones-cuanticas-en-madrid-en-linea-con-europa/ [Accessed: 17th Nov 2024]].

Gómez Aguado, D., García-Cid, M. I., Ortiz Martín, L., & Martín Ayuso, V. (2023). Simulated environment for multiparty quantum digital signature across the network. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1–10.

Gottesman, D., & Chuang, I. (2001). Quantum digital signatures. *arXiv preprint quant-ph/0105032*.

Greece, E. (2023). Hellasqci - quantum communications infrastructure for greece [https://hellasqci.eu [Accessed: 28th May 2024]].

Grosshans, F., & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical review letters*, *88*(5), 057902.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 212–219.

Guardian, T. (2021). 'cyber-attack' hits iran's transport ministry and railways [https://www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways [Accessed: 27th May 2024]].

Heshami, K., England, D. G., Humphreys, P. C., Bustard, P. J., Acosta, V. M., Nunn, J., & Sussman, B. J. (2016). Quantum memories: Emerging applications and recent advances. *Journal of modern optics*, *63*(20), 2005–2028.

Ho, K. O., Wong, K. C., Leung, M. Y., Pang, Y. Y., Leung, W. K., Yip, K. Y., Zhang, W., Xie, J., Goh, S. K., & Yang, S. (2021). Recent developments of quantum sensing under pressurized environment using the nitrogen vacancy (nv) center in diamond. *Journal of Applied Physics*, *129*(24).

Hofheinz, D., Hövelmanns, K., & Kiltz, E. (2017). A modular analysis of the fujisaki-okamoto transformation. *Theory of Cryptography Conference*, 341–371.

Hohm, J., Heinemann, A., & Wiesmaier, A. (2022). Towards a maturity model for crypto-agility assessment. *International Symposium on Foundations and Practice of Security*, 104–119.

HTCoeurGrandEst. (2022). Le ght coeur grand est victime d'une cyberattaque [https://ght-coeurgrandest.fr/wp-content/uploads/2022/04/CP_Cyberattaque_GHT_Coeur_Grand_Est_21042022.pdf [Accessed: 27th May 2024]].

Hufnagel, F., Sit, A., Grenapin, F., Bouchard, F., Heshami, K., England, D., Zhang, Y., Sussman, B. J., Boyd, R. W., Leuchs, G., et al. (2019). Characterization of an underwater channel for quantum communications in the ottawa river. *Optics express*, *27*(19), 26346–26354.

ISO. (2024). International organization for standardization [https://www.iso.org [Accessed: 27th May 2024]].

Italy, E. (2023). Quid - quantum italy deployment [https://quid-euroqci-italy.eu [Accessed: 28th May 2024]].

J. Quisquater, T. A. B., L. C. Guillou. (1990). How to explain zero-knowledge protocols to your children. *Advances in Cryptology - CRYPTO '89*, 628–631.

Kielpinski, D., Monroe, C., & Wineland, D. J. (2002). Architecture for a large-scale ion-trap quantum computer. *Nature*, *417*(6890), 709–711.

Kimble, H. J. (2008). The quantum internet. *Nature*, *453*(7198), 1023–1030.

Krawczyk, H., & Eronen, P. (2010). *Hmac-based extract-and-expand key derivation function (hkdf)* (tech. rep.).

Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology*, *8*(1), 24.

Kurochkin, V., & Kurochkin, Y. (2009). Principles of the new quantum cryptography protocols building. *Physics of Particles and Nuclei Letters*, *6*, 605–607.

Kurochkin, Y. (2005). Quantum cryptography with floating basis protocol. *Quantum Informatics 2004*, *5833*, 213–221.

Kurose, J. F., & Ross, K. W. (n.d.). Computer networking.

Lancho, D., Martinez, J., Elkouss, D., Soto, M., & Martín, V. (2010). Qkd in standard optical telecommunications networks. *Quantum Communication and Quantum Networking: First International Conference, QuantumComm 2009, Naples, Italy, October 26-30, 2009, Revised Selected Papers 1*, 142–149.

Lo, H.-K., & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *science*, *283*(5410), 2050–2056.

Lo, H.-K., Chau, H. F., & Ardehali, M. (2005). Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, *18*, 133–165.

Lu, Y.-S., Cao, X.-Y., Weng, C.-X., Gu, J., Xie, Y.-M., Zhou, M.-G., Yin, H.-L., & Chen, Z.-B. (2021). Efficient quantum digital signatures without symmetrization step. *Optics Express*, *29*(7), 10162–10171.

Ma, X., Qi, B., Zhao, Y., & Lo, H.-K. (2005). Practical decoy state for quantum key distribution. *Physical Review A*, *72*(1), 012326.

Martin, e. a., V. (2024). Madqci: A heterogeneous and scalablesdn-qkd network deployed in production facilities. *npj quantum information*, *10*(80).

Martin, V., Brito, J., Ortíz, L., Brito-Méndez, R., Vicente, R., Saez-Buruaga, J., Sebastian, A., Aguado, D., García-Cid, M., Setien, J., et al. (2023). The madrid testbed: Qkd sdn control and key management in a production network. *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, 1–4.

Martín, e. a., Vicente. (2021). Quantum technologies in the telecommunications industry. *EPJ Quantum Technology*, *8*(19).

Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, *48*(3), 351–406.

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., et al. (2020). Quantum key distribution: A networking perspective. *ACM Computing Surveys (CSUR)*, *53*(5), 1–41.

Mendez, R. B., Brito, J. P., Vicente, R. J., Aguado, A., Pastor, A., Lopez, D., Martín, V., & Lopez, V. (2020). Quantum abstraction interface: Facilitating integration of qkd devices in sdn networks. *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, 1–4.

Michielsen, K., Nocon, M., Willsch, D., Jin, F., Lippert, T., & De Raedt, H. (2017). Benchmarking gate-based quantum computers. *Computer Physics Communications*, *220*, 44–55.

Mosca, M. (2015). Cybersecurity in a quantum world: Will we be ready. *Workshop on Cybersecurity in a Post-Quantum World, Invited Presentation*.

Nacional, C. C. (2022). Ccn-tec 009: Recommendations for a secure post-quantum transition [https://www.ccn.cni.es/index.php/en/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file [Accessed: 17th Nov. 2024]].

Nan Tian, e. a. (2023). Trends in world military expediture [https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf [Accessed: 28th May 2024]].

NATO. (2024). Summary of nato's quantum technologies strategy [https://www.nato.int/cps/en/natohq/official_texts_221777.htm [Accessed: 28th May 2024]].

NCSC. (2020). Quantum security technologies [https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies [Accessed: 28th May 2024]].

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

NIST. (2001). Fips 197: Advanced encryption standard (aes) [https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf [Accessed: 27th May 2024]].

NIST. (2015a). Fips 180-4: Secure hash standard (shs) [https://doi.org/10.6028/NIST.FIPS.180-4 [Accessed: 28th May 2024]].

NIST. (2015b). Fips 202: Sha-3 standard - permutation-based hash and extendable-output functions [https://doi.org/10.6028/NIST.FIPS.202 [Accessed: 28th May 2024]].

NIST. (2016). Post-quantum cryptography [https://csrc.nist.gov/projects/post-quantum-cryptography [Accessed: 6 May 2024]].

NIST. (2023a). Fips 186-5: Digital signature standard (dss) [https://doi.org/10.6028/NIST.FIPS.186-5 [Accessed: 27th May 2024]].

NIST. (2023b). Sp 800-56r3: Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography [https://csrc.nist.gov/pubs/sp/800/56/a/r3/final [Accessed: 27th May 2024]].

NIST. (2024a). Fips 203: Module-lattice-based key-encapsulation mechanism standard [https://csrc.nist.gov/pubs/fips/203/final [Accessed: 17th Nov 2024]].

NIST. (2024b). Fips 204: Module-lattice-based digital signature standard [https://csrc.nist.gov/pubs/fips/204/final [Accessed: 17th Nov 2024]].

NIST. (2024c). Fips 205: Statelesshhash-based digital signature standardd [https://csrc.nist.gov/pubs/fips/205/final [Accessed: 17th Nov 2024]].

NIST. (2024d). National institute of standards and technology [https://www.nist.gov [Accessed: 27th May 2024]].

NIST, N. (2023a). Migration to post-quantum cryptography [https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms [Accessed: 28th May 2024]].

NIST, N. (2023b). Sp 1800-38c: Migration to post-quantum cryptography quantum readiness [https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf [Accessed: 28th May 2024]].

Oktian, Y. E., Lee, S., Lee, H., & Lam, J. (2017). Distributed sdn controller system: A survey on design choice. *computer networks*, *121*, 100–111.

OPENQKD. (2024). Openqkd [https://openqkd.eu [Accessed: 28th May 2024]].

Ott, D., Peikert, C., et al. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility. *arXiv preprint arXiv:1909.07353*.

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., et al. (2009). The secoqc quantum key distribution network in vienna. *New Journal of Physics*, *11*(7), 075001.

PETRUS. (2023). Petrus euroqci [https://petrus-euroqci.eu [Accessed: 28th May 2024]].

Peyravian, M., Roginsky, A., & Kshemkalyani, A. (1998). On probabilities of hash value matches. *Computers & Security*, *17*(2), 171–176.

Portugal, E. (2023). Ptqci - portuguese quantum communication infrastructure [https://ptqci.pt [Accessed: 28th May 2024]].

PQREACT. (2023). Post quantum cryptography framework for energy aware contexts [https://pqreact.eu/ [Accessed: 28th May 2024]].

Project, T. O. Q. S. (2022). Liboqs - an open source c library for quantum-safe cryptographic algorithms [https://openquantumsafe.org/liboqs/ [Accessed: 28th May 2024]].

QT. (2024). Quantum flagship [https://qt.eu [Accessed: 28th May 2024]].

Renner, R., Gisin, N., & Kraus, B. (2005). Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, *72*(1), 012332.

Research, V. M. (2024a). Global quantum cryptography market size and forecast [https://www.verifiedmarketresearch.com/product/global-quantum-cryptography-market-size-and-forecast/ [Accessed: 28th May 2024]].

Research, V. M. (2024b). Quantum communication market [https://www.verifiedmarketresearch.com/product/quantum-communication-market/ [Accessed: 28th May 2024]].

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Rosales-Pelaez, P., Garcia-Cid, M. I., Valeriani, C., Vega, C., & Sanz, E. (2019). Seeding approach to bubble nucleation in superheated lennard-jones fluids. *Physical Review E*, *100*(5), 052609.

Ruihong, Q., & Ying, M. (2019). Research progress of quantum repeaters. *Journal of Physics: Conference Series*, *1237*(5), 052032.

S. Goldwasser, S. M., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *17th Annual ACM Symposium on the Theory of Computing*, 291–304.

Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., et al. (2011). Field test of quantum key distribution in the tokyo qkd network. *Optics express*, *19*(11), 10387–10409.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *2014 IEEE symposium on security and privacy*, 459–474.

Schaller, R. R. (1997). Moore's law: Past, present and future. *IEEE spectrum*, *34*(6), 52–59.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th annual symposium on foundations of computer science*, 124–134.

Shor, P. W., & Preskill, J. (2000). Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, *85*(2), 441.

Space, T. A. (2023). Thales alenia space and partners sign contract with european space agency for tequants quantum satellite communications project [https://www.thalesaleniaspace.com/en/press-releases/thales-alenia-space-and-partners-sign-contract-european-space-agency-tequants [Accessed: 28th May 2024]].

Spain, E. (2023). Developing and deploying the quantum communications infrastructure [https://euroqci-spain.eu [Accessed: 28th May 2024]].

Takeda, S., & Furusawa, A. (2019). Toward large-scale fault-tolerant universal photonic quantum computing. *APL Photonics*, *4*(6).

Tao, C., Petzoldt, A., & Ding, J. (2021). Efficient key recovery for all hfe signature variants. *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Con-*

ference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41, 70–93.

Tittel, W., Zbinden, H., & Gisin, N. (2001). Experimental demonstration of quantum secret sharing. *Physical Review A*, *63*(4), 042301.

Toyran, M., Pedersen, T. B., Hasekioğlu, A. A., Can, M. A., & Berber, S. (2013). A study on cascade error correction protocol. *2013 21st Signal Processing and Communications Applications Conference (SIU)*, 1–4.

Trushechkin, A., Tregubov, P., Kiktenko, E. O., Kurochkin, Y. V., & Fedorov, A. K. (2018). Quantum-key-distribution protocol with pseudorandom bases. *Physical Review A*, *97*(1), 012311.

Union, I. T. (2003). G.694.2 : Planes espectrales para las aplicaciones de multiplexación por división de longitud de onda [https://www.itu.int/rec/T-REC-G.694.2-200312-I/es [Accessed: 28th May 2024]].

Union, I. T. (2020). G.984.1 : Gigabit-capable passive optical networks (gpon) [https://www.itu.int/rec/T-REC-G.984.1 [Accessed: 28th May 2024]].

Wallden, P., Dunjko, V., Kent, A., & Andersson, E. (2015). Quantum digital signatures with quantum-key-distribution components. *Physical Review A*, *91*(4), 042304.

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*(6412), eaam9288.

Wei, Z., Wang, W., Zhang, Z., Gao, M., Ma, Z., & Ma, X. (2013). Decoy-state quantum key distribution with biased basis choice. *Scientific reports*, *3*(1), 2453.

Weimer, H., Yao, N. Y., Laumann, C. R., & Lukin, M. D. (2012). Long-range quantum gates using dipolar crystals. *Physical Review Letters*, *108*(10), 100501.

Weiss, P. (1999). Quantum internet: The quirks of quantum mechanics may lead to better computer networks. *Science News*, *155*(14), 220–221.

Wiesmaier, A., Alnahawi, N., Grasmeyer, T., Geißler, J., Zeier, A., Bauspieß, P., & Heinemann, A. (2021). On pqc migration and crypto-agility. *arXiv preprint arXiv:2106.09599*.

Woo, M. K., Park, B. K., Kim, Y.-S., Cho, Y.-W., Jung, H., Lim, H.-T., Kim, S., Moon, S., & Han, S.-W. (2020). One to many qkd network system using polarization-wavelength division multiplexing. *IEEE Access*, *8*, 194007–194014.

Yan, B., Li, Q., Mao, H., & Chen, N. (2022). An efficient hybrid hash based privacy amplification algorithm for quantum key distribution. *Quantum Information Processing*, *21*(4), 130.

Yin, H.-L., & Fu, Y. (2019). Measurement-device-independent twin-field quantum key distribution. *Scientific reports*, *9*(1), 3045.

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, *356*(6343), 1140–1144.

Zhao, Y. (2019). The integration of qkd and security services. *ITU QIT4N Workshop, Shanghai, China*, 5–7.

Zhao, Z., & Ding, J. (2022). Several improvements on bkz algorithm. *Cryptology ePrint Archive*.

"Nada te turbe, nada te espante todo se pasa,
Dios no se muda, la paciencia todo lo alcanza,
quien a Dios tiene nada le falta, sólo Dios basta."

Santa Teresa de Ávila