MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Puesta en marcha y operación de una red conmutada de comunicaciones cuánticas para investigación y desarrollo

Autor: Pablo Ruiz-Tagle Valcarce

Director: Alberto Juan Sebastián Lombraña

Co-Director: Mario Castro Ponce

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título Puesta en marcha y operación de una red conmutada de comunicaciones cuánticas para investigación y desarrollo en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el curso académico 2024/25 es de mi autoría, original e inédito y no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada de otros documentos está debidamente referenciada.

Fdo.: Pablo Ruiz-Tagle Valcarce Fecha: 26/ 06/ 2025

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Alberto Juan Sebastián Lombraña.
Firmado digitalmente el día
07/07/2025 (AC FNMT Usuarios)

Fdo.: Alberto Juan Sebastián Lombraña Fecha: ……/ ……/ ……

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. PABLO RUIZ-TAGLE VALCARCE

DECLARA ser el titular de los derechos de propiedad intelectual de la obra: PUESTA EN MARCHA Y OPERACIÓN DE UNA RED CONMUTADA DE COMUNICACIONES CUANTICAS PARA INVESTIGACIÓN Y DESARROLLO, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.

d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 26 de …JUNIO... de 2025.

ACEPTA

Fdo PABLO RUIZ-TAGLE VALCARCE

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Puesta en marcha y operación de una red conmutada de comunicaciones cuánticas para investigación y desarrollo

Autor: Pablo Ruiz-Tagle Valcarce

Director: Alberto Juan Sebastián Lombraña

Co-Director: Mario Castro Ponce

Madrid

Agradecimientos

Muchas gracias a mi tutor, Alberto, por ayudarme a empezar mi camino en la óptica cuántica. A Laura y a Vicente, por la oportunidad que me han brindado, y a mi cotutor Mario Castro, por ponerme en contacto con este grupo de investigación.

PUESTA EN MARCHA Y OPERACIÓN DE UNA RED CONMUTADA DE COMUNICACIONES CUÁNTICAS PARA INVESTIGACIÓN Y DESARROLLO

Autor: Ruiz-Tagle Valcarce, Pablo.
Director: Sebastián Lombraña, Alberto.
Entidad Colaboradora: Universidad Politécnica de Madrid – Grupo de Investigación en Información y Computación Cuántica

RESUMEN DEL PROYECTO

El presente Trabajo de Fin de Máster se centra en el diseño, implementación y validación de una red de comunicaciones por fibra óptica orientada a la experimentación en tecnologías cuánticas, con especial énfasis en la planificación de caminos de conmutación óptica. Esta infraestructura permitirá la prueba y evaluación de distintas tecnologías emergentes de distribución cuántica de claves (QKD), sentando las bases para futuras aplicaciones comerciales y certificaciones.

Palabras clave: QKD, comunicaciones cuánticas, conmutación, óptica

1. Introducción

Los sistemas de comunicación a distancia han sido factores determinantes en la percepción del mundo durante los últimos dos siglos, moldeando la visión contemporánea de una humanidad conectada. En el marco de las telecomunicaciones, surge la tecnología de comunicaciones cuánticas, desarrollada para hacer frente a las amenazas que plantea la computación cuántica sobre los sistemas criptográficos clásicos.

Basándose en principios fundamentales de la mecánica cuántica, como la superposición, el entrelazamiento y el principio de no clonación, estas tecnologías permiten el establecimiento de canales de comunicación seguros, invulnerables a la interceptación y capaces de detectar intentos de espionaje. Entre estas tecnologías, destaca la distribución cuántica de claves (*quantum key distribution*, QKD)**,** que se

perfila como una solución revolucionaria para la protección de la información en escenarios sensibles.

Uno de los riesgos más críticos en el contexto actual es el denominado ataque «s*tore now, decrypt later*» (SNDL)**,** en el que un atacante intercepta comunicaciones cifradas hoy, protegidas con criptografía clásica, para almacenarlas y descifrarlas en el futuro con ayuda de ordenadores cuánticos. Este tipo de amenazas introduce una urgencia tecnológica, ya que incluso los datos confidenciales actuales podrían quedar comprometidos si no se protege su transmisión desde ahora.

Ante esta situación, gobiernos, instituciones científicas y empresas tecnológicas están apostando por el desarrollo de redes cuánticas seguras y escalables. Proyectos como la Infraestructura de Comunicación Cuántica Europea (EuroQCI) o redes nacionales como MadQCI en España están sentando las bases de una nueva generación de telecomunicaciones. Sin embargo, su implementación aún plantea múltiples desafíos: desde la ampliación de distancias útiles hasta la compatibilidad con infraestructuras ópticas tradicionales.

2. Definición del proyecto

La aplicación de principios de la física cuántica al campo de las telecomunicaciones ya sea mediante QKD o mediante la transmisión de pares de fotones entrelazados, representa un avance disruptivo en materia de seguridad de la información. Aunque existen sistemas funcionales que aplican esta tecnología, los actuales esfuerzos se centran en mejorar su eficiencia, alcance e integración con las redes ópticas clásicas.

No obstante, debido a la novedad de estas tecnologías, aún no se dispone de infraestructuras, normativas, bancos de pruebas ni sistemas de certificación que generen confianza para su adopción por parte de entidades públicas o privadas. Para abordar este vacío surge el proyecto europeo NOSTRADAMUS, una iniciativa enfocada en el desarrollo de estándares de prueba y validación para las tecnologías cuánticas en el marco de EuroQCI.

Este Trabajo de Fin de Máster se centra en el desarrollo y expansión de la red MadQCI en Madrid. El proyecto tiene por objetivo analizar, diseñar e implementar mejoras

sobre la infraestructura ya existente, optimizando su rendimiento, extendiendo su cobertura y validando su integración con infraestructuras ópticas clásicas.

Para ello, se estudiarán los protocolos de distribución cuántica de claves, la viabilidad de enlaces ópticos de largo alcance y la interoperabilidad entre distintos nodos de la red cuántica nacional y europea. El objetivo final es contribuir al establecimiento de una infraestructura robusta y escalable que posicione a Madrid como un nodo esencial dentro del ecosistema europeo de comunicaciones cuánticas.

3. Descripción del sistema

La expansión de la red cuántica madrileña en la que se enfoca el proyecto se realizará en las instalaciones de la Universidad Politécnica de Madrid situadas en el campus de Montegancedo.

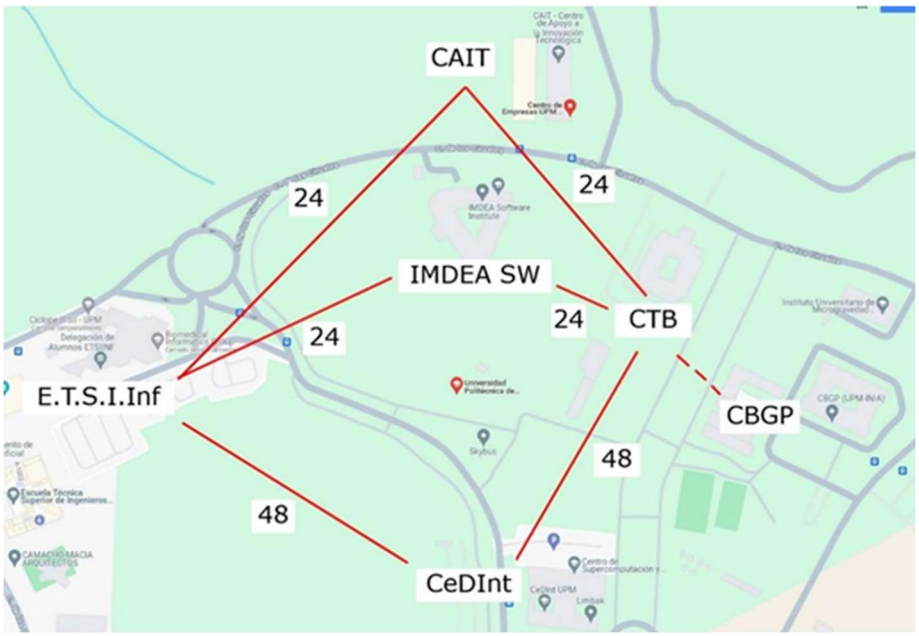

Ilustración 1. interconexión en el campus de Montegancedo

En esta nueva iteración de la red, la mayoría de los nodos estarán bajo control de la UPM y se utilizarán como plataformas de investigación, desarrollo y pruebas, facilitando el despliegue de sistemas de QKD con potencial comercial. Estos entornos permitirán realizar mediciones reales sobre fibra óptica física, evitando simulaciones que no contemplan las pérdidas, interferencias y variaciones reales de canal.

La interconexión de los cinco nodos del campus se realizará a través de fibra oscura (*dark fiber*) dedicada. Esta fibra no compartida garantiza el aislamiento del canal y la eliminación de factores externos que podrían distorsionar las mediciones o poner en riesgo la fiabilidad de los dispositivos.

Dentro del marco de pruebas definido por el proyecto NOSTRADAMUS, se identificó la necesidad de experimentar con métodos de conmutación de caminos cuánticos. Para ello, se han diseñado escenarios de conmutación inspirados en tecnologías de redes ópticas clásicas como DWDM (*dense wavelength division multiplexing*), y modelos FOADM y ROADM (conmutación basada en óptica fija o reconfigurable respectivamente; el nombre proviene de generalizar el uso de los componentes llamados *optical add-drop multiplexing*).

4. Resultados

Para certificar que los sistemas puedan conmutar correctamente y en un tiempo razonable, se ha diseñado dos escenarios de ROADM y FOADM:

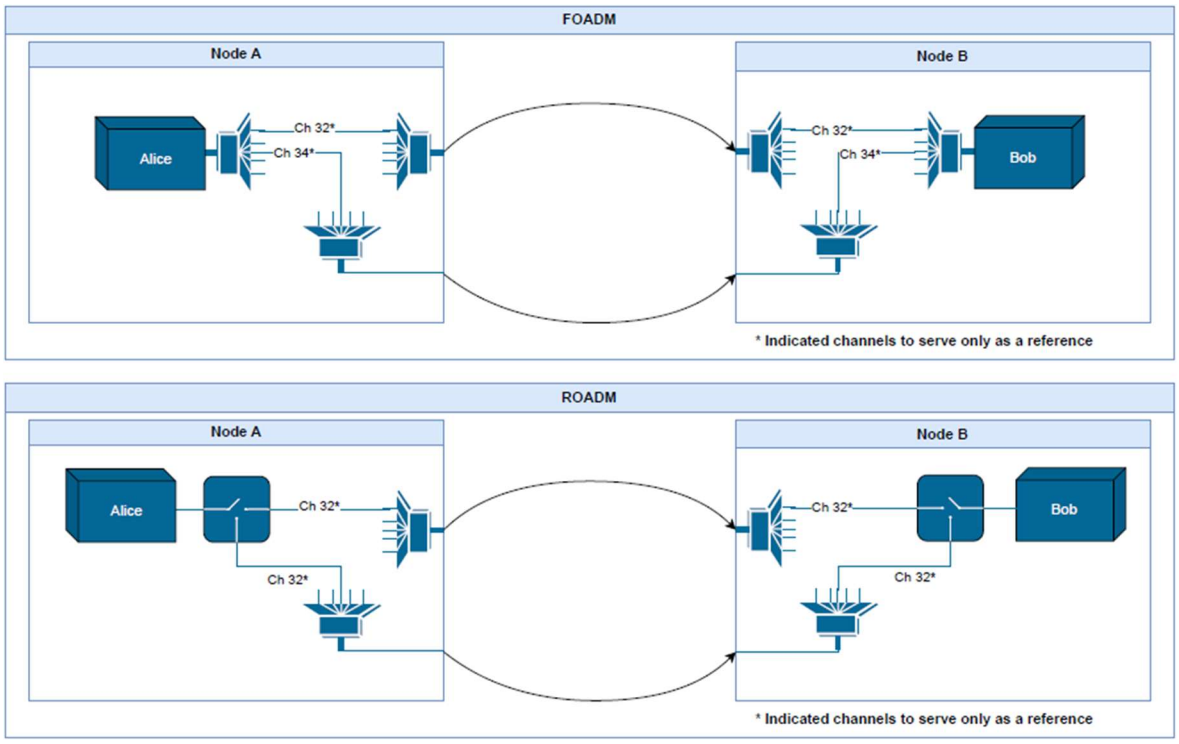

Ilustración 2. Escenarios test FOADM y ROADM

- En el caso **FOADM**, la señal cuántica (QKD) es redirigida a través de un canal distinto al cambiar su longitud de onda, sin modificar la configuración física de la red.

- En el caso **ROADM**, se realiza un cambio dinámico de ruta mediante un conmutador óptico, manteniendo la misma longitud de onda, pero modificando la topología de paso.

En ambos casos, se ha observado que los sistemas QKD requieren un tiempo de sincronización y reajuste tras la conmutación. Este tiempo es crítico para garantizar la seguridad del canal y el éxito en la regeneración de claves.

5. Conclusiones

El control preciso de los tiempos de reconfiguración y sincronización es fundamental, ya que durante estos intervalos la red cuántica puede quedar expuesta a vulnerabilidades o interrupciones del servicio. Un sistema diseñado para entornos críticos, como el ámbito gubernamental, financiero o de defensa, debe garantizar conmutaciones rápidas, estables y seguras.

Además, la capacidad de conmutar dinámicamente en caso de fallo de un canal, ataque o congestión en la red añade una capa adicional de resiliencia y permite que las redes cuánticas evolucionen hacia arquitecturas más escalables y tolerantes a fallos.

Este trabajo constituye una aportación práctica al desarrollo de estas redes, proporcionando tanto una plataforma experimental de validación como una base conceptual para futuras extensiones en campo abierto.

DEPLOYMENT AND OPERATION OF A SWITCHED QUANTUM COMMUNICATION NETWORK FOR RESEARCH AND DEVELOPMENT

Author: Ruiz-Tagle Valcarce, Pablo
Supervisor: Sebastián Lombraña, Alberto.
Collaborating Entity: Universidad Politécnica de Madrid – Quantum Information and Computing Research Group

ABSTRACT

This project focuses on the design and implementation of an optical fiber communication network oriented towards experimentation in quantum communications. It includes the planning of switching paths to test the effectiveness of various emerging QKD (Quantum Key Distribution) technologies.

Keywords: QKD, quantum communications, switching, optics**.**

1. Introduction

Long-distance communication systems have been key factors in shaping the modern view of a connected humanity. Within the field of telecommunications, quantum communication technologies have emerged to confront the threats posed by quantum computing to classical cryptographic systems.

Based on fundamental principles of quantum mechanics, such as superposition, entanglement, and the no-cloning theorem, these technologies enable the establishment of secure communication channels that are invulnerable to interception and capable of detecting eavesdropping attempts. Among them, quantum key distribution (QKD) stands out as a revolutionary solution for information security in critical contexts.

One of the most pressing risks today is the so-called store now, decrypt later (SNDL) attack, in which adversaries capture encrypted communications today, protected by classical cryptography, to decrypt them in the future using quantum computers. This threat introduces an urgent need for action, as sensitive information transmitted today could be compromised retroactively in a post-quantum era.

In response to this challenge, governments, research institutions, and technology companies are investing in secure and scalable quantum networks. Projects such as the European Quantum Communication Infrastructure (EuroQCI) and national deployments

like MadQCI in Spain are laying the foundations for a new era of secure communications. However, their implementation still faces major challenges, including increasing transmission distances and ensuring compatibility with existing optical infrastructure.

2. Project definition

The application of quantum mechanics to telecommunications, either via QKD or entangled photon pairs, represents a disruptive advance in information security. While operational systems already exist, current efforts are focused on improving their efficiency, reach, and integration with conventional optical networks.

Nevertheless, as a novel technology, there are still no established infrastructures, standards, testbeds, or certification systems that can provide the trust needed for widespread adoption. To address this gap, the European project NOSTRADAMUS aims to develop testing and validation standards for quantum technologies as part of EuroQCI.

This Master's Thesis focuses on the development and expansion of the MadQCI network in Madrid. The objective is to analyze, design, and implement improvements to the existing infrastructure, optimizing its performance, extending its reach, and validating its integration with classical optical networks.

To this end, the project explores QKD protocols, the feasibility of long-distance quantum fiber links, and interoperability with other nodes in the national and European quantum communication ecosystem. The ultimate goal is to contribute to a robust and scalable infrastructure that positions Madrid as a key node within the EuroQCI framework.

3. System description

The expansion of the Madrid quantum network will be carried out at the Universidad Politécnica de Madrid, specifically at the Montegancedo campus.

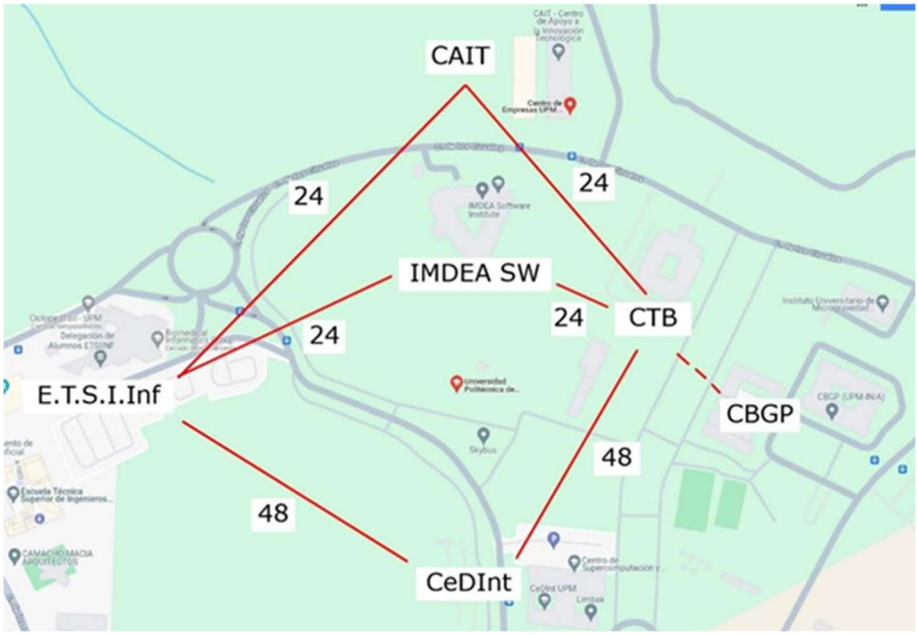

Figure 1: Interconnection within the Montegancedo campus

In this iteration, most of the nodes will be controlled by UPM and dedicated to research, development, and testing. These environments will support the deployment of potentially commercial QKD systems in real conditions, enabling direct measurements over physical fiber as opposed to simulated environments, which often overlook real-world imperfections.

The five nodes will be interconnected using dedicated dark fiber, ensuring isolation from external disturbances that could affect device performance or data integrity.

As part of the NOSTRADAMUS test plan, it is necessary to implement and evaluate quantum path switching mechanisms. For this purpose, the project includes experimental scenarios inspired by conventional optical technologies such as Dense Wavelength Division Multiplexing (DWDM), as well as FOADM and ROADM (Fixed and Reconfigurable Optical Add-Drop Multiplexing).

4. Results

Two basic experimental setups were implemented to test FOADM and ROADM architectures in the lab:

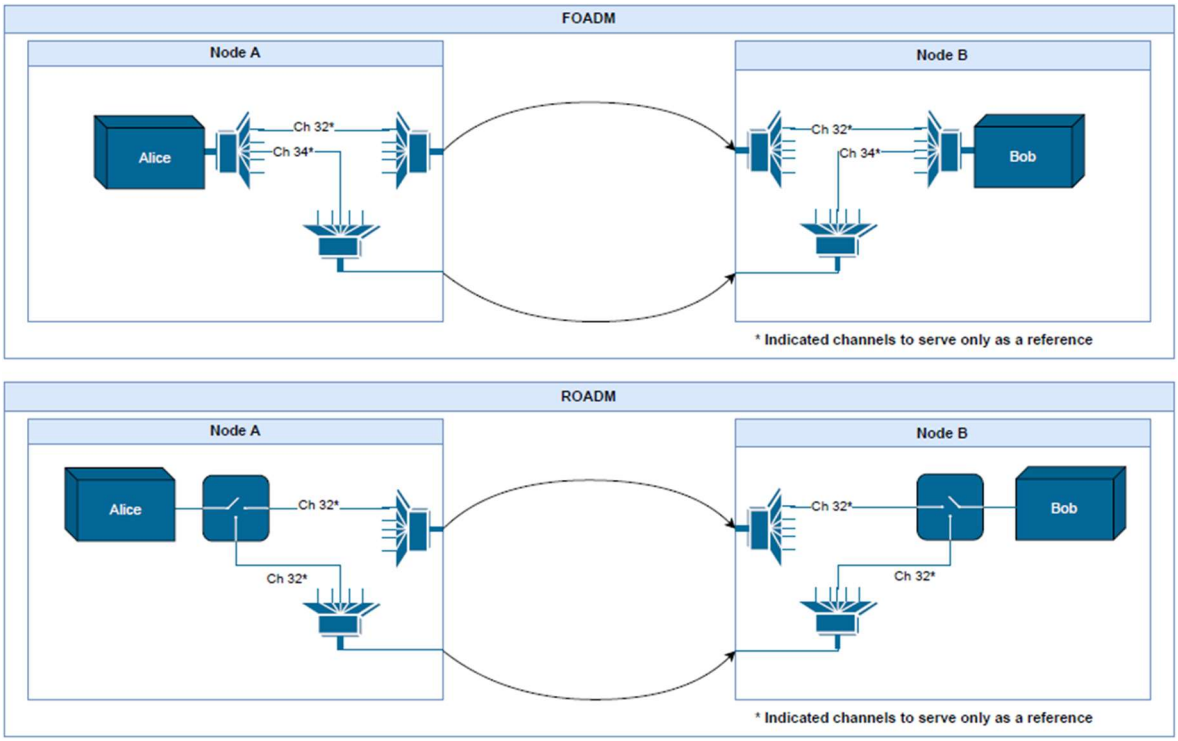

Figure 2: Test scenarios for FOADM and ROADM

- In the **FOADM** scenario, the QKD signal is routed through a different channel by changing its wavelength, with the physical network configuration remaining static.
- In the **ROADM** scenario, a dynamic switch modifies the signal's path while keeping the wavelength constant.

In both cases, the QKD system has been observed to require a certain amount of time for recalibration and synchronization after switching. These parameters are critical to ensure security and proper key generation.

5. Conclusions

Accurately controlling reconfiguration and synchronization times is essential, as the network may be vulnerable during this interval. In systems designed for critical applications, such as defense, finance, or government, the ability to perform fast and secure switching is non-negotiable.

Moreover, dynamic switching capabilities allow the network to adapt to link failures or attacks, increasing its resilience and enabling scalable topologies suitable for real-world deployment.

This thesis contributes a practical platform for testing and evaluation of quantum switching in real optical environments, laying the groundwork for future, more complex implementations of quantum-secure communication infrastructure.

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

La seguridad de las comunicaciones se enfrenta a una amenaza sin precedentes: la llegada de la computación cuántica. La criptografía actual, fundamento de la seguridad digital contemporánea, podrían volverse vulnerable en cuestión de años, poniendo en riesgo todo tipo de comunicaciones desde transacciones bancarias hasta la protección de datos gubernamentales de carácter sensible. Ante este escenario, las comunicaciones cuánticas han surgido como una solución innovadora y adaptable a las prácticas de hoy en día, aportando garantías sobre la inviolabilidad de la información mediante principios físicos fundamentales de la mecánica cuántica.

En estos últimos años, naciones y empresas han dirigido sus esfuerzos e inversiones impulsando iniciativas para la creación y desarrollo de infraestructura de comunicaciones cuánticas seguras y escalables orientadas a la investigación de estas tecnologías. Europa con la iniciativa *EuroQCI* (*European Quantum Communication Infrastructure*, por sus siglas en inglés) con el objetivo de establecer una red de comunicaciones cuánticas que interconecte toda Europa. Otros países como Estados Unidos o China, que ha sido pionera con su red cuántica interurbana y el satélite Micius, también han hecho grandes avances en este campo, estableciendo sus propias redes experimentales de distribución de clave cuántica (*quantum key distribution*, QKD) a gran escala. Sin embargo, esta tecnología aún está en una etapa lejana a su maduración, por lo que problemas de alcance, integración con redes ópticas clásicas y fiabilidad operativa siguen siendo desafíos importantes a los que enfrentarse.

En este contexto, España y diversos actores en la Comunidad de Madrid han desarrollado la red MadQCI (Madrid Quantum Communication Infrastructure) como parte de su estrategia nacional para la implementación de tecnologías cuánticas en las telecomunicaciones. Este trabajo de fin de máster se centra en la expansión de la red MadQCI con un nuevo escenario de red, analizando su viabilidad técnica y proponiendo mejoras para su integración en redes ópticas existentes. Una de las líneas principales de investigación abordadas en este trabajo es la prueba de conmutación de QKD en un escenario basado en multiplexación óptica

ROADM y FOADM, lo que permitiría mejorar la flexibilidad y escalabilidad de la red cuántica. Este tipo de arquitectura facilitaría la integración de QKD en redes ópticas de alta capacidad, optimizando el uso de los recursos de fibra y reduciendo los costos de implementación.

Además de analizar la expansión de la infraestructura cuántica en Madrid, este trabajo también busca ofrecer una visión divulgativa de las comunicaciones cuánticas. Para ello, se incluyen secciones explicativas que contextualizan la importancia de estas tecnologías dentro del marco de la óptica y la mecánica cuántica. Se presentará un resumen de la óptica clásica, abordando conceptos clave como la propagación de la luz en fibra óptica y los principios de la multiplexación, fundamentales para entender la implementación de redes cuánticas. Posteriormente, se introducirá una síntesis de la mecánica cuántica, explicando los fenómenos físicos que hacen posibles las comunicaciones cuánticas, como el entrelazamiento y la superposición cuántica.

Finalmente, este trabajo también explora las perspectivas futuras de las comunicaciones cuánticas, analizando proyectos emergentes que están dando forma a la próxima generación de redes cuánticas. En particular, se discutirá el proyecto Nostradamus, una iniciativa innovadora que busca ampliar la infraestructura cuántica europea y desarrollar nuevas aplicaciones de estas tecnologías en escenarios de comunicación segura.

Para estructurar este análisis, el documento se organiza de la siguiente manera:

En primer lugar, se establece un contexto teórico fundamental mediante el cual se podrá establecer las bases para comprender la tecnología desarrollada y utilizada, introduciendo los principios de la óptica clásica y la mecánica cuántica.

En segundo lugar, se presenta una descripción del estado tecnológico actual sobre el que se basa este trabajo. Con ello se abarca desde las tecnologías actuales de redes cuánticas, incluyendo su desarrollo actual e innovaciones importantes en *hardware*. Asimismo, se adentra en los protocolos desarrollados para QKD y otras tecnologías emergentes, haciendo inflexión en su implementación en infraestructuras ópticas.

Se prosigue con un análisis detallado del proyecto EuroQCI, centrándonos en la red MadQCI, su expansión y desarrollo, y la expansión en UPM-Montegancedo junto con las pruebas de conmutación ROADM y FOADM que se realizarán en ese campus.

Finalmente se abordan los desarrollos futuros en este campo, con especial atención al proyecto Nostradamus y otras iniciativas relevantes. Y junto con posibles líneas de investigación relevantes se recogen conclusiones al proyecto.

Con este enfoque, este trabajo no solo busca analizar la evolución y los retos de las comunicaciones cuánticas, sino también ofrecer una visión accesible para aquellos que deseen comprender cómo estas tecnologías están revolucionando el mundo de las telecomunicaciones.

Capítulo 2. CONTEXTO TEÓRICO

Antes de adentrarse en las interacciones ópticas de los sistemas cuánticos sobre los que se desarrolla el proyecto, resultaría apropiado dedicar un momento para repasar brevemente tanto la descripción clásica de la luz como los principios de mecánica cuántica que gobiernan la óptica cuántica.

2.1 ÓPTICA CLÁSICA

La óptica clásica se fundamenta en la teoría electromagnética de Maxwell y describe la propagación de la luz en términos de ondas electromagnéticas. Estos principios son esenciales para comprender las tecnologías de comunicación cuántica, que a su vez se construyen sobre el marco de la mecánica cuántica.

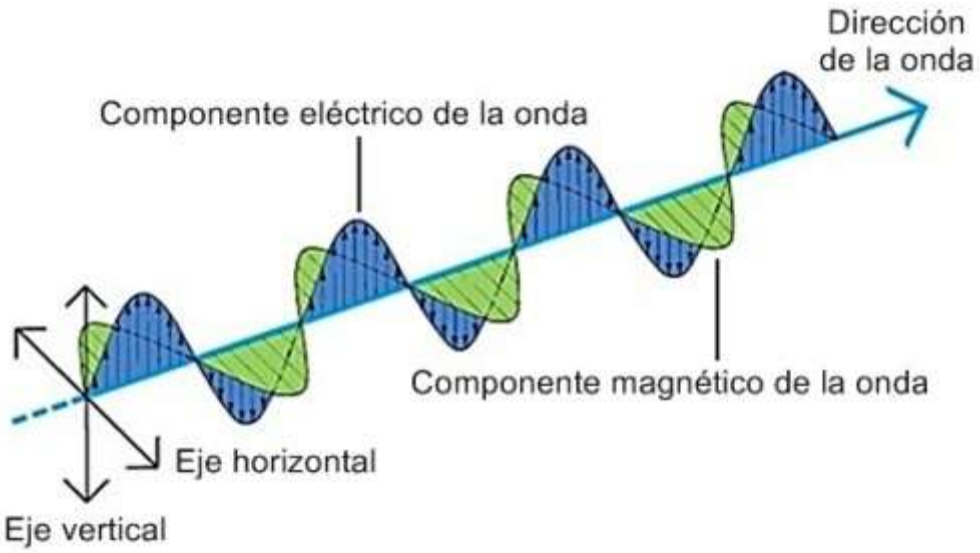

Ilustración 3: Naturaleza ondulatoria de la luz

Naturaleza Ondulatoria de la Luz

La luz descrita por las ecuaciones de Maxwell es una onda electromagnética transversal. Su propagación en el espacio libre o en medios materiales está gobernada por la ecuación de onda:

$$\nabla^2 E = \frac{1}{v^2}\frac{\partial^2 E}{\partial t^2}$$

donde E es el campo eléctrico y v es la velocidad de propagación de la onda (c o la velocidad de la luz si dicha onda se propaga en el vacío).
Esta descripción es válida para explicar la gran mayoría de fenómenos ópticos, con variedad de evidencias que lo respaldan. Es por ello que, normalmente, al hablar de óptica es común referirse a ella en términos de rayos y ondas, omitiendo menciones a la mecánica cuántica.
Esta ecuación describe la propagación de la luz y permite analizar fenómenos como la interferencia, la propagación, la polarización y la difracción.

Polarización

La polarización se refiere a la orientación del campo eléctrico de una onda electromagnética. Existen diferentes tipos de polarización posibles:

- Lineal: El vector campo eléctrico apunta en una dirección determinada de manera constante.

- Circular: El vector campo eléctrico rota según se propaga la onda. Completando una rotación completa por cada longitud de onda. Luz con esta polarización puede ser descompuesta en dos rayos de luz de polarizaciones lineales y ortogonales entre sí, con un desfase de 90º entre ellas.

- Elíptica: Similar a la circular salvo que o las amplitudes de los rayos ortogonales que la componen son diferentes o que la fase entre ellos no es ni 90º ni 0º, haciendo que el campo eléctrico dibuje una elipse al propagarse.

- Apolar: La luz tiene polarización arbitraria.

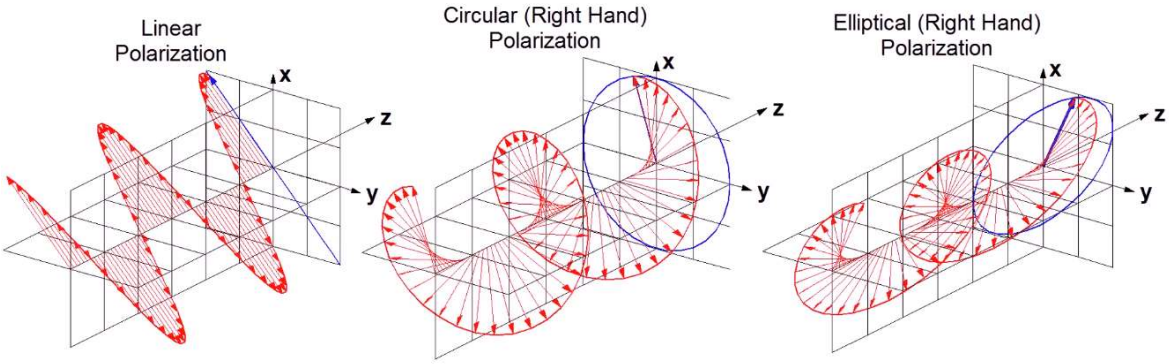

Ilustración 4: Polarización de la luz

Se describe a través del vector de Stokes y la matriz de Mueller, herramientas clave en la descripción de la manipulación de estados de luz polarizados. En las comunicaciones cuánticas, los estados de polarización se usan para la codificación de información en protocolos QKD como BB84 y E91.

En el vacío, la polarización de una onda es constante según se propaga. Sin embargo, al propagarse en ciertos materiales esta polarización puede ir cambiando. Un fenómeno a tener en cuenta, utilizado en los divisores de rayo polarizantes (*polarizing beam splitter*, o PBS por sus siglas en ingles), es la birrefringencia, o doble refracción. Los materiales birrefringentes son capaces de separar rayos de luz incidentes en dos rayos de polarización ortogonales entre sí. Estos rayos se denominan el rayo ordinario y el extraordinario, que se separan después de experimentar dos índices de refracción distintos.

Interferencia y Difracción

La interferencia y la difracción son los fenómenos que más claramente demuestran la naturaleza ondulatoria de la luz. La interferencia en particular toma un papel importante en el funcionamiento de algunos tipos de QKD.

La interferencia es el resultado de la combinación coherente de ondas electromagnéticas de fase diferente, ejemplificada típicamente en el experimento del interferómetro de Michelson.

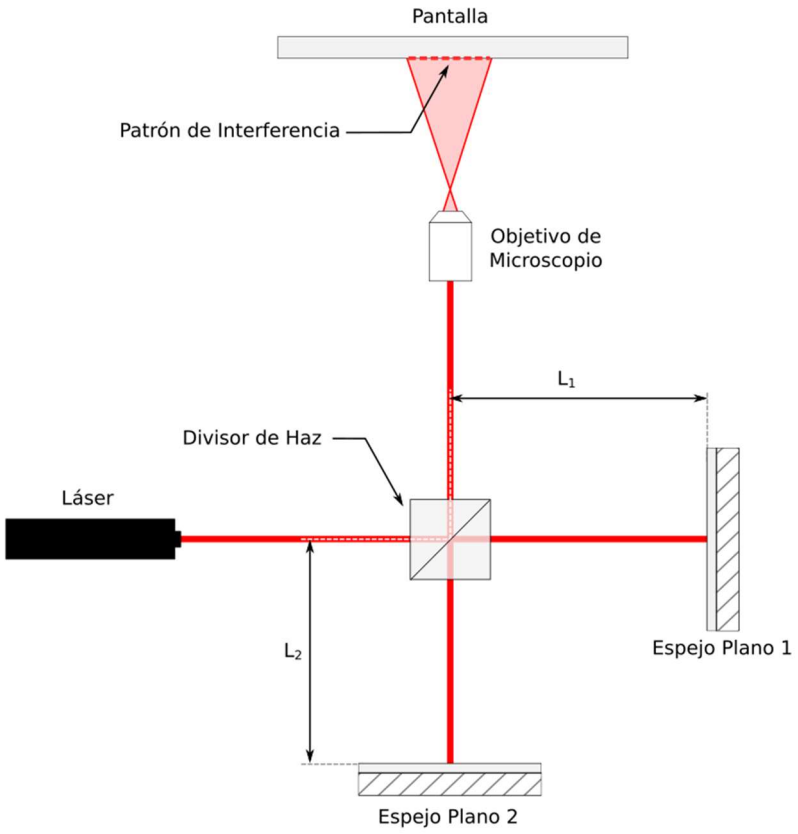

Ilustración 5: Interferómetro de Michelson

. En función de las distancias L_1 y L_2, se observará una cantidad de luz distinta en la pantalla superior que, además, podrá mostrar los típicos patrones de interferencia.

Se describe matemáticamente mediante la adición de campos eléctricos de las ondas individuales, lo que puede dar lugar a interferencia constructiva o destructiva según la diferencia de fase entre ellas.
La difracción, por otro lado, explica la propagación de la luz alrededor de objetos y a través de aberturas. Se puede distinguir dos regímenes principales llamados la difracción Fresnel y la difracción Fraunhofer, según la distancia entre el hueco y la pantalla sobre la que se proyecta la luz.

Propagación en Medios Ópticos

La propagación de la luz en fibras ópticas está gobernada por la ecuación de Helmholtz y la ecuación de onda guiada. En un medio dieléctrico, la relación de dispersión se expresa como:

$$K^2 = \frac{\omega^2}{c^2} n^2$$

Donde K es el vector de onda, ω la frecuencia angular y n el índice de refracción del medio. La transmisión eficiente de fotones individuales en sistemas QKD está limitada por la atenuación y la dispersión modal y cromática en las fibras ópticas.

Estos conceptos, si bien son conocidos en la ingeniería de telecomunicaciones más tradicional, son el fundamento de muchas de los protocolos de criptografía cuántica actuales, por lo que tienen una vigencia mayúscula.

2.2 MECÁNICA CUÁNTICA

Esta sección se fundamenta en la obra *Quantum Optics: An Introduction* de M Fox; su lectura y análisis en profundidad ha facilitado en gran medida el aprendizaje en tecnologías de red cuántica y criptografía cuántica.

La mecánica cuántica describe la naturaleza discreta de la energía y el comportamiento probabilístico de las partículas, representa la fusión entre comportamiento como onda o partícula. Ayuda a explicar el comportamiento como partículas de lo que se considera una onda (p. ej., la luz) y el comportamiento como ondas de lo que se considera una partícula (electrones).
Su formulación se basa en la ecuación de Schrödinger:

$$i\hbar \frac{\partial}{\partial t}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle$$

Donde $|\psi(t)\rangle$ representa el estado cuántico del sistema y $\hat{H}$ es el operador Hamiltoniano.

Principio de Incertidumbre

El conmutador de dos operadores $\hat{A}$ y $\hat{B}$ en la mecánica cuántica se define mediante:

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$$

Dichos operadores conmutan si $[\hat{A}, \hat{B}] = 0$. Si se da esto, las medidas de estas propiedades no interfieren entre sí, por lo que estas variables no están conjugadas y se pueden tomar medidas precisas simultáneamente. En cambio, si estas variables no conmutan, resultará imposible tomar medidas reales precisas simultáneamente. La medición de una de las variables cambia el resultado de la medición de la otra.

El principio de incertidumbre de Heisenberg establece que la medición simultánea de ciertas variables conjugadas, como la posición y el momento, está sujeta a la relación:

$$\sigma_x \sigma_p \geq \frac{\hbar}{2}$$

Esto implica que la medición de un estado cuántico perturba inevitablemente el sistema, una propiedad clave en la seguridad de la criptografía cuántica. Los protocolos de criptografía cuántica descritos más adelante se fundamentan parcialmente en este fenómeno, dado que un posible espía alterará la información transportada y los comunicantes experimentarán un ruido que le delatará.

Cuantización del Campo Electromagnético

Esta sección aborda la cuantización del campo electromagnético, fundamental para que se manifiesten sus propiedades cuánticas.

En lugar de tratar la luz como una onda clásica, se modela como un conjunto de osciladores cuánticos asociados a cada modo del campo electromagnético. La energía de cada modo está cuantizada en múltiplos de $\hbar\omega$, lo que da lugar a los estados de Fock $|n\rangle$, con fotones. El hamiltoniano del campo es:

$$\hat{H} = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2}\right)$$

Donde $\hat{a}^\dagger$ y $\hat{a}$ son los operadores de creación y aniquilación.

Coherencia Cuántica y Estados de Luz

En óptica cuántica, los estados coherentes y los estados cuasi-coherentes (como los generados por láseres atenuados) son fundamentales para aplicaciones como QKD. Los estados coherentes $|\alpha\rangle$ tienen propiedades similares a los campos clásicos y son descritos por distribuciones de Poisson en el número de fotones.

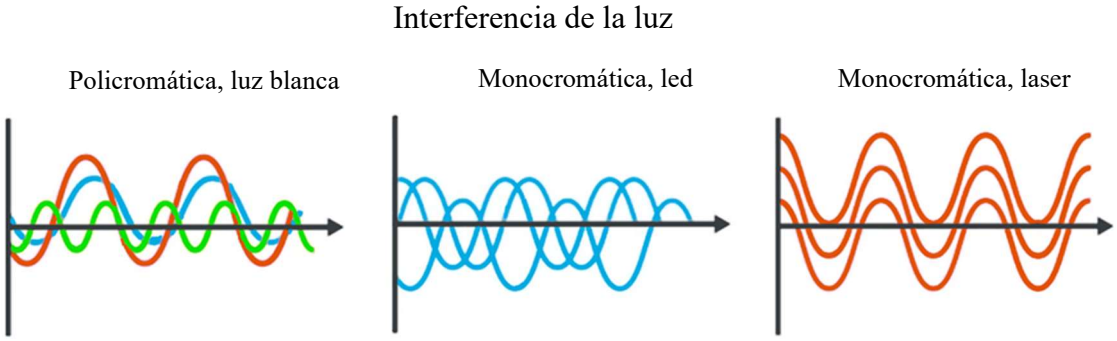

Ilustración 6: Estados de luz

Polarización Cuántica y Bases de Medición

Los fotones tienen un grado de libertad asociado a su polarización. Los estados $|H\rangle$, $|V\rangle$, $|+\rangle$, $|-\rangle$ representan estados ortogonales en distintas bases, y en parejas son ambiguos entre sí. Es decir, en función de la pareja de vectores elegidos para implementar la medida del fotón, se puede hacer una media inequívoca o ambigua. Si el fotón se generó con una pareja de vectores como base, y se mide con esa misma base, la medida será inequívoca. Sin embargo, habrá ambigüedad si no es así.

El uso de estas bases ambiguas es el fundamento del protocolo BB84. La no conmutatividad de los operadores de polarización asegura que la medición en una base incorrecta perturba el estado del fotón. Por ello, se consigue el efecto descrito encima. Así,

las partes comunicantes podrán estar seguras de que el estado medido ha sido el generado si están seguras de haber generado y medido el fotón en la misma base. De no ser así, pueden descartar la comunicación. Este juego permite componer protocolos como el BB84, explicado más adelante.

Detección de Fotones y Estadísticas

Los detectores de fotones, como los diodos de efecto avalancha y los detectores superconductores, se describen por operadores de número $\hat{n} = \hat{a}^{\dagger}\hat{a}$. La probabilidad de detección sigue distribuciones estadísticas (como la de Poisson), y las imperfecciones como la eficiencia cuántica y los conteos oscuros afectan la fidelidad de la detección.

La evolución tecnológica de estos dispositivos en las últimas dos décadas, especialmente para operar en bandas ópticas de teleco, ha sido fundamental para habilitar la criptografía cuántica.

Interferencia Cuántica y Beam Splitters

Los divisores de haz y los interferómetros producen interferencia entre estados cuánticos. Cuando dos fotones indistinguibles llegan a un *beam splitter*, se puede observar la interferencia de Hong-Ou-Mandel, un fenómeno puramente cuántico que evidencia la naturaleza de indistinguibilidad y la simetría bosónica de los fotones.

Este fenómeno es fundamental para las pruebas de seguridad de los protocolos de criptografía cuántica, que son unos modelos matemáticos y físicos de gran complejidad y mayor discusión hoy en día.

Principio de No Clonación y Medición Cuántica

Un postulado clave de la mecánica cuántica es que no es posible clonar la información que porta un estado cuántico arbitrario a otro estado; sí que es posible copiarlo, en el sentido de trasladar su información al segundo eliminándola del primero. Este principio es crucial para la seguridad de QKD, puesto que un posible espía no puede hacer una infinitud de pruebas sobre un estado cuántico desconocido como el que porta un fotón que intercepte.

Además, el formalismo de mediciones proyectivas sobre estados no ortogonales implica que cualquier intento de medición por parte de un atacante deja huella detectable.
Esta estructura conceptual es esencial para comprender cómo se utilizan los fenómenos cuánticos para asegurar la comunicación mediante protocolos como BB84, y proporciona las herramientas teóricas para analizar la evolución, detección e interferencia de estados cuánticos de luz.

La criptografía cuántica hace uso de todos estos postulados para implementar formas de comunicación únicas que, por sí solas, son inmunes a cualquier ataque, ya sea de la informática clásica o de la cuántica.

Además, la criptografía cuántica es la primera gran aplicación de las telecomunicaciones cuánticas, pero no la única, por lo que estos fenómenos y otros análogos tendrán un papel fundamental en el estado de la cuestión presente y futura.

Capítulo 3. ESTADO DE LA CUESTIÓN

La mecánica cuántica ha abierto el camino a nuevas tecnologías de la información que redefinen la seguridad, la conectividad y la informática. Las comunicaciones cuánticas emergen como una de las aplicaciones más prometedoras, fundamentadas en propiedades como el entrelazamiento, la superposición y la no clonación de estados cuánticos.

El panorama actual de las tecnologías cuánticas se puede clasificar en varios ámbitos de investigación y desarrollo:

3.1 INTERNET CUÁNTICO

El internet cuántico aspira a interconectar nodos cuánticos, como ordenadores cuánticos, a través de canales de comunicación seguros basados en entrelazamiento. Este tipo de red permitiría realizar tareas imposibles en redes clásicas, como la sincronización cuántica, la distribución segura de estados cuánticos y el teletransporte cuántico.

Aunque aún en fase de investigación, se han logrado hitos importantes, como la distribución de entrelazamiento a cientos de kilómetros mediante satélites (por ejemplo, el experimento chino con el satélite Micius). Sin embargo, esta forma de comunicación no será posible hasta que existan los «amplificadores cuánticos», un sistema que teleportará pares entrelazados salto a salto por una red para lograr pares entrelazados de distancia arbitraria. A su vez, para implementarlos, es necesario que existan las memorias cuánticas, es decir, el almacenamiento de información cuántica más o menos persistente.

Ilustración 7: Comunicación cuántica por satélite

Si bien esta comunicación estaba dedicada a un ejercicio de QKD punto a punto, se usó el entrelazamiento cuántico, fundamental para el futuro internet cuántico.

Por todo ello, el internet cuántico se postula como la forma dominante de comunicación cuántica en el futuro, aunque hoy no haya podido salir de los laboratorios.

3.2 CRIPTOGRAFÍA CUÁNTICA. DISTRIBUCIÓN CUÁNTICA DE CLAVES (QKD)

La criptografía cuántica es la forma de comunicación cuántica más madura y posee un grado casi comercial, con una docena de empresas que venden equipos afines en Europa. Además, ha tenido un impulso singular en el marco de los proyectos europeos de I+D y la iniciativa EuroQCI.

La QKD es la técnica de criptografía cuántica más madura. Permite a dos partes generar una clave secreta simétrica compartida cuya seguridad está garantizada por las leyes de la mecánica cuántica. Sustituiría, por ello, a primitivas como el intercambio de clave RSA o Diffie-Hellman, cuya seguridad está cuestionada en la actualidad por la vigencia de la informática cuántica.

La distribución cuántica de claves puede clasificarse en dos grandes familias tecnológicas, según el tipo de codificación cuántica que se utiliza para transmitir la información: variable discreta (DV) y variable continua (CV). Ambas parten de principios fundamentales de la mecánica cuántica, pero difieren profundamente en la forma en que los estados cuánticos son preparados, transmitidos y medidos.

A continuación se describen ambas aproximaciones, sus ventajas e inconvenientes, y los principales protocolos.

3.2.1 QKD DE VARIABLE DISCRETA (DV-QKD)

Los protocolos DV-QKD codifican la información en variables cuánticas discretas, como la polarización, la fase o el número de fotones. y la detección se realiza mediante detectores de fotón único, capaces de anunciar la presencia o la ausencia de fotones tras hacerlos pasar por los componentes que implementen las bases de medida. Es la tecnología históricamente más desarrollada y utilizada en los primeros experimentos de QKD.

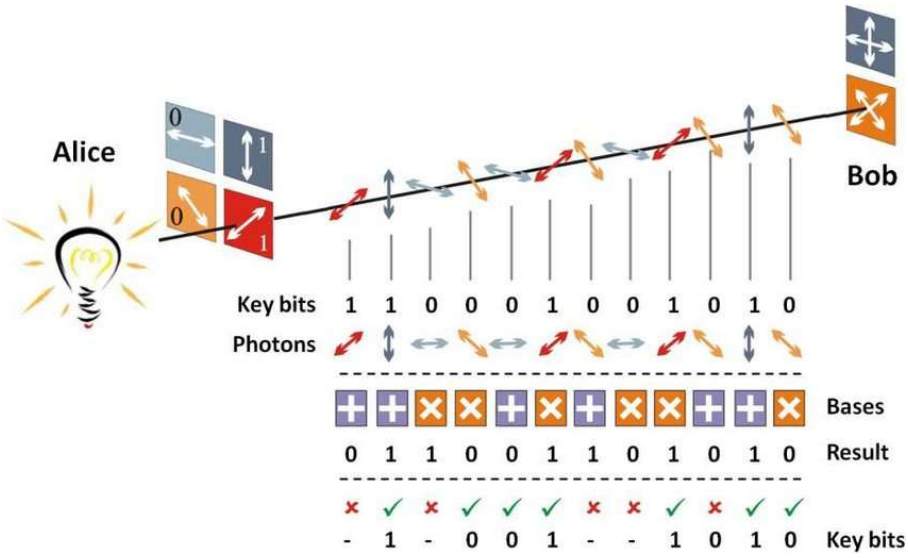

Ilustración 8: BB84.

Este protocolo es el decano de los de la criptografía cuántica y está vigente más de 40 años después de su ideación en muchos sistemas cuánticos comerciales.

Protocolo BB84 – Paso a paso

Desarrollado por Bennett y Brassard en 1984, es el primer protocolo de QKD y el más influyente. Se fundamenta en los siguientes pasos:

1. **Generación aleatoria**: Alice genera una cadena de bits aleatorios y elige aleatoriamente una de dos bases de codificación para cada bit: rectilínea (|H⟩/|V⟩) o diagonal (|+⟩/|−⟩).

2. **Emisión**: Alice envía un fotón polarizado de acuerdo con el bit y la base seleccionada.

3. **Medición**: Bob mide cada fotón recibido en una base aleatoria (rectilínea o diagonal).

4. **Comparación de bases**: Alice y Bob comunican públicamente qué base usaron para cada fotón.

5. **Filtrado**: Conservan solo los bits correspondientes a las mediciones con bases coincidentes.

6. **Estimación de errores**: Comparan públicamente una fracción de bits para estimar la tasa de error.

7. **Reconciliación y privacidad**: Se corrigen errores y se aplican técnicas de amplificación de privacidad para obtener una clave segura.

Nótese que este protocolo se fundamenta en lo descrito sobre los fenómenos de la mecánica cuántica. En efecto, se hace uso de dos bases de generación y medida, pero ortogonales entre sí. Alice y Bob las usan de forma aleatoria y, tras ello, anuncian sus bases en la reconciliación. Por las peculiaridades de la medida descritas, sólo se quedan con aquellas transmisiones con la misma base de generación y medida. El uso de dos bases ambiguas garantiza que un espía no medir y regenerar la transmisión, dado que desconoce las bases usadas y sólo logra generar ruido. El teorema de no clonación garantiza que no copie el estado en múltiples fotones para hacer un mejor análisis que minimice el ruido por debajo del umbral de seguridad.

Ventajas

- Alta seguridad probada teóricamente.
- Existen implementaciones comerciales.
- Compatible con distancias medianas.

Inconvenientes

- Requiere detectores de fotón único, costosos y complejos.
- Sensible a pérdidas y a ataques como *photon number splitting* (PNS).
- Limitada velocidad de clave comparada con CV-QKD.

3.2.2 QKD DE VARIABLE CONTINUA (CV-QKD)

Los protocolos CV-QKD codifican la información en las cuadraturas electromagnéticas (amplitud y fase) de pulsos de luz coherente, los cuales se modulan con distribuciones continuas, usualmente gaussianas. La detección se realiza mediante técnicas de detección homodina o heterodina, sin necesidad de detectores de fotón único.

Protocolo GMCS (Gaussian Modulated Coherent States) – Paso a paso

1. **Modulación gaussiana**: Alice genera números aleatorios xxx y ppp según una distribución gaussiana, y los usa para modular la amplitud y fase de un estado coherente |α⟩|\alpha⟩|α⟩.
2. **Emisión**: El estado coherente es enviado a través de un canal óptico (típicamente una fibra).
3. **Medición**: Bob mide la cuadratura XXX, PPP o ambas usando detección homodina (1 cuadratura) o heterodina (ambas).
4. **Sifting**: Alice y Bob comparten públicamente las bases medidas (si aplica) y filtran los datos correspondientes.
5. **Estimación de canal**: Se analizan estadísticas de las muestras para estimar la pérdida, ruido y tasa de error.

6. **Reconciliación**: Se aplica un protocolo de corrección de errores (*reverse reconciliation*, a menudo).

7. **Amplificación de privacidad**: Se obtiene la clave final secreta a través de reducción de información disponible al posible atacante.

Ventajas

- Compatible con componentes ópticos estándar (láseres y fotodiodos).
- Tasa de clave potencialmente más alta que DV-QKD.
- Mejor integración con redes ópticas metropolitanas (DWDM, amplificadores, etc.).

Inconvenientes

- Menor alcance debido a sensibilidad al ruido y a la atenuación.
- Requiere detección precisa y baja variación térmica.
- Seguridad más compleja de analizar (aunque bien fundamentada).

Consideraciones prácticas

- **DV-QKD** se adapta mejor a implementaciones de largo alcance y redes punto a punto donde el rendimiento prima sobre el coste. La implementan los fabricantes HEQA, ID Quantique, QTI, ThinkQuantum o Toshiba.
- **CV-QKD** resulta ideal para redes metropolitanas, multiplexadas y entornos con limitaciones presupuestarias, dada su compatibilidad con componentes ópticos estándar. La implementan los fabricantes KEEQuant y Luxquanta.

3.2.3 QKD INDEPENDIENTE DEL DISPOSITIVO DE MEDICIÓN (MDI-QKD)

Una de las mayores vulnerabilidades prácticas en la implementación de QKD radica en los dispositivos de detección. Aunque los protocolos cuánticos son teóricamente seguros, los ataques de canal lateral, como los ataques de «*detector blinding*» o «*time-shift*», pueden comprometer la seguridad explotando imperfecciones físicas en los detectores.

MDI-QKD (Measurement Device Independent QKD), propuesto en 2012 por Lo, Curty y Qi, elimina esta vulnerabilidad trasladando la detección a un tercer nodo intermedio no confiable. La seguridad del protocolo se basa en la interferencia cuántica entre los pulsos enviados por Alice y Bob, y no en la fidelidad de los detectores.

Ventajas

- Inmune a ataques sobre detectores, que son los elementos más vulnerables en implementaciones prácticas.
- Permite crear arquitecturas en estrella con nodos intermedios no confiables.
- Puede combinarse con DV-QKD o incluso con fuentes cuánticas compartidas.

Inconvenientes

- Requiere interferencia cuántica indistinguible entre dos fuentes independientes, lo cual es técnicamente exigente.
- Necesita sincronización precisa, control de fase y compensación de fluctuaciones del canal.
- La tasa de generación de clave es menor que en BB84 o CV-QKD para distancias comparables.
- Sólo existe un único fabricante, Q*Bird.

En el contexto de despliegues cuánticos nacionales y europeos, como MadQCI y EuroQCI, el uso combinado de estas tecnologías es clave. **DV-QKD** proporciona robustez y experiencia operativa; **CV-QKD** permite integración con infraestructuras ópticas existentes a bajo coste; y **MDI-QKD** ofrece una ruta clara hacia arquitecturas seguras con nodos intermedios no confiables, ideales para redes escalables y abiertas.

Existen dos métodos principales para la implementación de QKD:

- **Distribución a través de fibra óptica**: Limitada por la atenuación, actualmente se alcanzan distancias de hasta 500 km con enlaces punto a punto.
- **Distribución vía satélite**: Ofrece una solución para superar los límites de distancia en la Tierra, siendo útil para redes globales.

Estas tecnologías se integran cada vez más con infraestructuras ópticas clásicas, aprovechando dispositivos como ROADM y FOADM para conmutar rutas cuánticas dinámicamente. El presente trabajo se inscribe en este contexto, explorando la expansión de la red cuántica madrileña (MadQCI) y su uso para realizar pruebas de conmutación de QKD en escenarios conmutados ópticamente.

Capítulo 4. DEFINICIÓN DEL TRABAJO

4.1 JUSTIFICACIÓN

La computación cuántica representa una de las revoluciones tecnológicas más profundas de las próximas décadas. Esta técnica tiene el potencial de resolver problemas hoy inabordables para la informática clásica, lo que impulsará sectores como la simulación de materiales, la inteligencia artificial y la optimización logística. Pero junto a estas oportunidades, llega una amenaza crítica: la posibilidad real de romper los sistemas criptográficos que actualmente protegen nuestra sociedad digital**.**

El cifrado que se usa hoy en día en aplicaciones cotidianas —como el acceso a cuentas bancarias, correos electrónicos, videoconferencias, infraestructuras críticas o datos gubernamentales— se basa en algoritmos que suponen la imposibilidad práctica de resolver ciertos problemas matemáticos. Esta suposición dejará de ser válida cuando los ordenadores cuánticos alcancen un umbral mínimo de capacidad. De hecho, según múltiples estimaciones científicas y gubernamentales, este momento podría llegar en las próximas dos décadas, y algunos expertos alertan de que podría ser antes.

Aquí entra en juego un factor clave: la seguridad retrospectiva. Muchas comunicaciones actuales deben permanecer confidenciales durante años o décadas (por ejemplo, historiales médicos, contratos comerciales, secretos de Estado). Si hoy se interceptan comunicaciones cifradas y se almacenan, podrían ser desencriptadas en el futuro cuando existan ordenadores cuánticos lo suficientemente potentes, aunque hoy parezcan seguras. Este tipo de ataque es conocido como «*store now, decrypt later*» (almacena ahora, descifra después), y ya está ocurriendo según agencias de inteligencia y expertos en ciberseguridad.

Por eso, el momento para actuar es ahora.

4.1.1 DOS CAMINOS COMPLEMENTARIOS: PQC Y QKD

Frente a esta amenaza, el desarrollo de soluciones cuántico-resistentes no es opcional, sino imperativo. Las dos principales líneas tecnológicas son:

1. **Criptografía Post-Cuántica (PQC)**: Son algoritmos diseñados para ejecutarse en ordenadores clásicos, pero estructurados de manera que se cree que son seguros incluso frente a un ordenador cuántico. Están siendo estandarizados por el NIST (National Institute of Standards and Technology), y tienen la ventaja de poder ser implementados rápidamente sobre infraestructuras existentes.
2. **Distribución Cuántica de Claves (QKD)**: A diferencia de PQC, QKD no depende de supuestos matemáticos, sino de las leyes de la física cuántica. Utiliza fotones individuales y el principio de no clonación para distribuir claves secretas entre dos usuarios. Cualquier intento de interceptación altera el sistema y queda al descubierto. Esto proporciona seguridad física incondicional, algo que ningún algoritmo clásico puede ofrecer.

Ambas tecnologías no se excluyen, sino que se complementan: mientras PQC puede ofrecer escalabilidad rápida, QKD proporciona seguridad a prueba de futuro y protege frente a amenazas incluso desconocidas.

4.1.2 IMPORTANCIA DEL DESARROLLO EXPERIMENTAL Y DE INFRAESTRUCTURA

La investigación no puede quedarse en el nivel teórico. Implementar estas tecnologías en redes reales, estudiar su rendimiento, adaptarlas a las condiciones del mundo físico y preparar las infraestructuras actuales para soportarlas es un paso esencial.

En este sentido, el presente Trabajo de Fin de Máster contribuye a esa transición tecnológica en dos dimensiones clave:

- Por un lado, proponiendo una expansión técnica y estratégica de la red MadQCI (Madrid Quantum Communication Infrastructure)**,** una red piloto para la transmisión segura de información mediante QKD.
- Por otro, experimentando con la integración de sistemas QKD en arquitecturas ópticas dinámicas, concretamente mediante conmutación en redes ROADM y FOADM. Esto sienta las bases para un modelo de red cuántica flexible, escalable y adaptable a las necesidades reales de comunicación.

Además, al incluir un enfoque divulgativo y formativo, el proyecto también ayuda a preparar al capital humano necesario para sostener estas tecnologías en el futuro.

4.1.3 ESPAÑA Y EUROPA: SEGURIDAD Y SOBERANÍA DIGITAL

Europa ha reconocido el carácter estratégico de esta transición y ha puesto en marcha EuroQCI (European Quantum Communication Infrastructure)**,** con el objetivo de desplegar una red cuántica paneuropea que proteja infraestructuras críticas, servicios públicos y gobiernos.

España participa activamente a través de diversos nodos y proyectos regionales, entre ellos MadQCI, impulsado por el Instituto IMDEA Networks, que busca crear un entorno experimental para integrar tecnologías QKD en redes metropolitanas.

Estos esfuerzos no solo posicionan a España dentro del liderazgo europeo en seguridad cuántica, sino que garantizan soberanía tecnológica, reduciendo la dependencia de proveedores extranjeros en un área tan sensible como las telecomunicaciones seguras.

4.1.4 EL COSTE DE NO ACTUAR A TIEMPO

No anticiparse a la llegada de la computación cuántica no es una opción sin consecuencias. Los datos críticos que hoy consideramos seguros podrían quedar expuestos en el futuro. Las infraestructuras estratégicas que no se adapten a tiempo podrían quedar vulnerables. Los países y regiones que no inviertan hoy en el desarrollo y despliegue de estas tecnologías podrían quedarse rezagados frente a aquellos que ya están construyendo su infraestructura cuántica.

Por eso, desarrollar, probar y ampliar redes cuánticas como MadQCI es mucho más que un experimento académico. Es una acción estratégica para proteger nuestro futuro digital**.**

4.1.5 EL RIESGO SILENCIOSO: ATAQUES "STORE NOW, DECRYPT LATER"

Una de las amenazas más serias —y a menudo menos comprendidas por el público general— relacionadas con la computación cuántica es el **SNDL**, *almacena ahora, descifra después*. Este ataque no requiere un ordenador cuántico funcional en el presente; solo exige la posibilidad de que exista en el futuro.

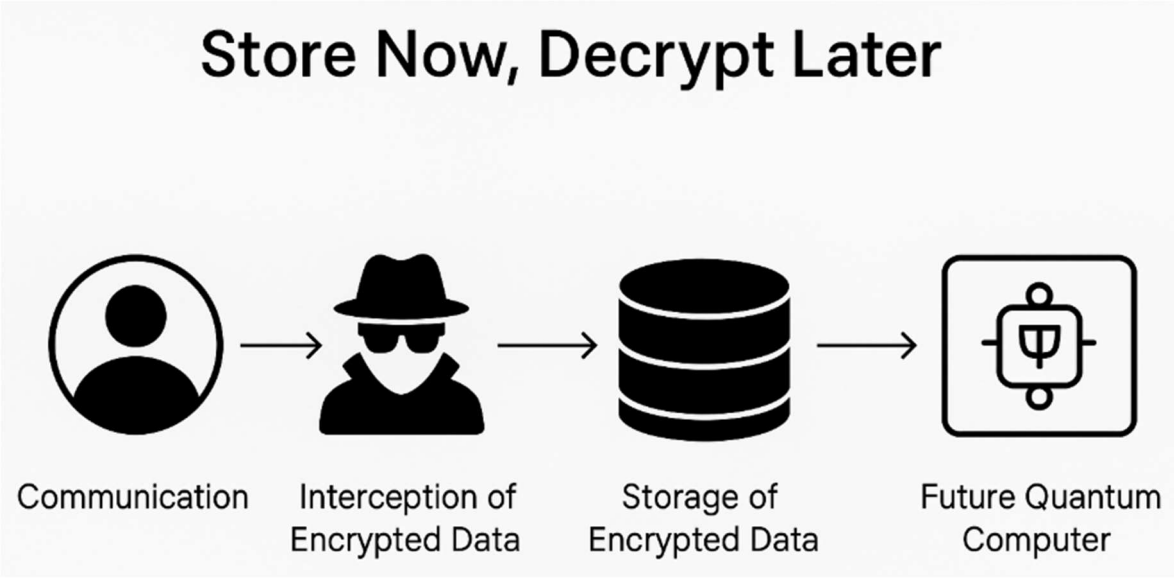

Ilustración 9: Store Now Decrypt Later

El principio es sencillo, pero devastador: un atacante intercepta hoy una comunicación cifrada, la almacena en su totalidad (incluyendo los mensajes y las claves cifradas), y espera pacientemente hasta que disponga de capacidad cuántica suficiente para descifrarla. En ese momento, toda la información que en el pasado se consideró privada puede ser revelada.

- **¿Por qué es tan crítico este riesgo?**

Porque muchas comunicaciones actuales tienen valor a largo plazo:

- **Datos médicos** deben mantenerse privados durante toda la vida de una persona.
- **Contratos empresariales y patentes** implican secretos industriales que pueden ser estratégicos durante décadas.
- **Correspondencia diplomática o militar** podría desestabilizar gobiernos si se revela más adelante.
- **Identidades digitales y credenciales** utilizadas para acceso a sistemas críticos podrían explotarse años después de su creación.

El riesgo es, por tanto, acumulativo y permanente. A medida que los años pasan, más datos han sido interceptados y almacenados por actores con capacidad técnica (gubernamental o criminal), y más cerca estamos del momento en que podrán ser descifrados si no se ha hecho una transición previa a tecnologías resistentes al cómputo cuántico.

- **Evidencia actual y alerta institucional**

Este tipo de ataque ya no es una hipótesis teórica. Organismos como el National Security Agency (NSA), el Centro Criptológico Nacional (CCN) en España y la European Union Agency for Cybersecurity (ENISA) han emitido advertencias claras sobre este riesgo.

Por ejemplo:

- El **CCN-CERT** advierte en sus guías de protección criptográfica que "la llegada de computadores cuánticos de propósito general supone una amenaza directa para la confidencialidad de las comunicaciones actuales y futuras".

- Según un informe de **ENISA (2022)**, *"existen motivos fundados para creer que actores estatales están recopilando grandes volúmenes de tráfico cifrado con fines de descifrado futuro, especialmente en redes de infraestructura crítica"*.

- En 2021, la **NSA** publicó la guía *Commercial National Security Algorithm Suite 2.0*, recomendando explícitamente que todos los sistemas clasificados y gubernamentales comiencen la migración hacia criptografía post-cuántica antes de 2030.

- En España, el **CCN-CERT** ha incluido la amenaza cuántica en su *Guía CCN-STIC 140*, donde recomienda implementar estrategias de "criptografía cuántica o post-cuántica" para garantizar la confidencialidad de largo plazo de información crítica.

- En la conferencia **Black Hat USA 2021**, expertos de empresas de ciberseguridad como **Cryptosense** y **PQShield** expusieron evidencia técnica de que ciertos servicios de mensajería y plataformas empresariales utilizan cifrados potencialmente vulnerables al almacenamiento y descifrado cuántico futuro. Se mostró cómo, con el tráfico TLS recogido hoy y herramientas de análisis en evolución, es posible capturar conversaciones cifradas que serían vulnerables en un horizonte temporal cercano.

- En **RSA Conference 2022**, el panel *"Quantum Readiness: Are We Storing Our Future Risk?"* presentó datos de sondeos donde más del 60 % de los responsables de seguridad corporativa admitieron no haber migrado aún a soluciones cuántico-resistentes, a pesar de tener comunicaciones que deberían seguir protegidas más allá de 2035.

- En **DEF CON 30 (2022)**, investigadores del ámbito académico y privado presentaron simulaciones de ataques SNDL realizados contra infraestructuras de prueba, demostrando la factibilidad técnica de interceptar y almacenar grandes volúmenes de datos cifrados sobre redes públicas.

Estas evidencias demuestran que el ataque *store now, decrypt later* no es una amenaza teórica o futura, sino una realidad presente. Su mayor peligro es que sus consecuencias se materializan tarde, cuando la información ya ha sido expuesta de forma irreversible.

Esto implica que, incluso si la amenaza cuántica no es inminente, su impacto podría ser retroactivo, afectando incluso a aquellos sistemas que ya se han cerrado o mensajes que ya se han enviado.

4.2 OBJETIVOS

Este Trabajo de Fin de Máster se centra en el desarrollo de infraestructuras de comunicaciones cuánticas a escala europea, nacional y regional, constituyendo así a el desarrollo del programa EuroQCI (European Quantum Communication Infrastructure), más específicamente de su implementación en Madrid, España mediante el proyecto MadQCI (Madrid Quantum Communication Infrastructure).

Dicha iniciativa busca sentar las bases para una red cuántica segura, interoperable y escalable, que pueda servirse de las actuales redes ópticas desplegadas en todo el mundo para así poder integrarse sin requerir inversión desmedida en infraestructura o despliegue de nuevas redes.

En este marco, el trabajo se centra en el diseño, planificación y análisis de una expansión de la red MadQCI con un nuevo escenario único, situado en el nodo del campus de Montegancedo (UPM) y fundamentado en técnicas de conmutación óptica. Asimismo, se aborda la evaluación experimental de esquemas de conmutación para sistemas de distribución cuántica de claves (QKD) sobre infraestructuras ópticas avanzadas.

Todo esto se desarrolla con el objetivo de avanzar hacia redes híbridas, combinando componentes cuánticos y clásicos que trabajan simultáneamente y en coordinación, que sean

adaptables, eficientes y seguras frente a amenazas futuras, incluyendo aquellas derivadas de la computación cuántica.

4.2.1 OBJETIVO GENERAL

Contribuir al desarrollo de una red cuántica metropolitana avanzada y funcional en la Comunidad de Madrid, mediante la expansión de la infraestructura MadQCI e integración de tecnologías ópticas reconfigurables (ROADM/FOADM) para pruebas de conmutación cuántica, alineada con las metas estratégicas del programa EuroQCI.

4.2.2 OBJETIVOS ESPECÍFICOS

1. **Análisis del marco estratégico europeo: EuroQCI**

   - Estudiar los fundamentos técnicos, institucionales y geoestratégicos del programa EuroQCI, su cronograma, actores implicados y sus implicaciones a largo plazo para la seguridad digital en Europa.
   - Analizar la estructura de despliegue propuesta por la Comisión Europea: redes de fibra seguras, nodos nacionales de confianza, enlaces satelitales cuánticos y sistemas de gestión y control.
   - Evaluar cómo los nodos experimentales como MadQCI pueden evolucionar hacia una infraestructura operativa interoperable con el resto de nodos europeos.

2. **Estudio detallado del estado actual de MadQCI**

   - Documentar los elementos actuales de la red MadQCI, incluyendo:
     - Topología física y lógica.
     - Tipología de enlaces (monomodo, dúplex, multiplexados).

- Sistemas QKD instalados o proyectados (BB84, CV-QKD, etc.).
- Infraestructura de soporte (amplificadores, filtros, láseres, switches ópticos).

- Evaluar los retos tecnológicos y operativos actuales de la red: limitaciones de distancia, sensibilidad a la pérdida, compatibilidad con redes clásicas, mantenimiento, etc.
- Estudiar el papel de MadQCI como banco de pruebas de soluciones que luego puedan escalarse a nivel nacional.

3. Diseño y planificación de la expansión hacia UPM-Montegancedo

- Realizar una propuesta técnica detallada para extender la red MadQCI hasta el campus UPM-Montegancedo, sede de centros como CeSViMa, el Centro de Domótica Integral, el Instituto IMDEA Software o la Faculta de Informáticos de la UPM.
- Justificar el interés estratégico y experimental de incluir este nodo:
  - Alta capacidad de cómputo y análisis.
  - Posibilidad de despliegue físico de equipos de red y fibra oscura.
  - Participación en proyectos de I+D europeos y nacionales relacionados con seguridad, redes y computación cuántica.
- Diseñar la arquitectura física y lógica de la expansión:
  - Trazado de fibra.
  - Elementos ópticos activos y pasivos.
  - Criterios de redundancia y seguridad física.

4. Desarrollo y validación de pruebas de conmutación QKD en entornos ROADM y FOADM

- Estudiar el funcionamiento de los sistemas ROADM (de *reconfigurable optical add-drop multiplexer*) y FOADM (de *fixed optical add-drop multiplexer*) desde el punto de vista de compatibilidad con enlaces cuánticos:
    - Estabilidad de fase y polarización.
    - Inserción de pérdidas.
    - Crosstalk entre canales cuánticos y clásicos.
- Diseñar pruebas de conmutación QKD simuladas o experimentales dentro del campus UPM, empleando tecnologías comerciales o prototipos de ROADM y FOADM.
- Evaluar el impacto de la conmutación dinámica en la fidelidad de las claves distribuidas:
    - Medición de QBER (Quantum Bit Error Rate).
    - Tasa de claves secretas netas.
    - Tiempo de conmutación y retardo.
- Proponer soluciones de control y gestión del tráfico cuántico que permitan optimizar el uso de recursos ópticos sin comprometer la seguridad física de las claves.

5. Contribución al desarrollo de redes híbridas cuántico-clásicas

- Explorar arquitecturas de red que integren canales cuánticos y clásicos mediante técnicas como multiplexación por longitud de onda (DWDM) y segmentación espectral.

- Analizar la posibilidad de orquestar redes cuánticas mediante tecnologías SDN (*software defined networking*), estableciendo políticas de encaminamiento seguras y dinámicas.

- Establecer criterios para una futura implementación escalable de una red cuántica regional basada en nodos interconectados y conmutación automática.

6. Divulgación técnica y contribución académica

- Elaborar material explicativo y divulgativo sobre el funcionamiento de redes cuánticas, QKD, y tecnologías ópticas avanzadas, dirigido a estudiantes, investigadores y profesionales del sector TIC.

- Sistematizar los resultados obtenidos como parte del ecosistema nacional de innovación en tecnologías cuánticas, facilitando la replicabilidad en otros entornos universitarios o industriales.

4.3 METODOLOGÍA

La metodología adoptada para este Trabajo de Fin de Máster combina análisis documental, diseño técnico, simulación y exploración experimental. El enfoque parte de un estudio del marco estratégico europeo y nacional, seguido por una evaluación de la red cuántica MadQCI, el diseño de su expansión hacia el campus UPM-Montegancedo, y el desarrollo de pruebas sobre la integración de QKD en arquitecturas ópticas avanzadas como ROADM y FOADM. Esta metodología se estructura en cuatro fases principales:

Fase 1. Estudio del estado del arte y del contexto estratégico

Esta primera fase tiene como objetivo sentar una base teórica y contextual sólida para el desarrollo del proyecto. Se realiza un análisis exhaustivo del estado del arte en

tecnologías de comunicación cuántica, con especial énfasis en QKD, sus protocolos (BB84, E91, CV-QKD, MDI-QKD) y su integración en redes ópticas. Paralelamente, se examina el marco institucional y geoestratégico de iniciativas como EuroQCI, así como el papel de España y de la red MadQCI en ese ecosistema.

Actividades:

- Estudio de la evolución y principios fundamentales de las tecnologías de QKD.
- Análisis de protocolos relevantes (BB84, E91, CV-QKD, MDI-QKD, etc.).
- Revisión de las especificaciones del programa EuroQCI.
- Documentación de la arquitectura y objetivos del proyecto MadQCI.
- Identificación de casos de uso y requisitos de seguridad en sectores clave.
- Revisión bibliográfica de publicaciones académicas y técnicas sobre QKD y redes cuánticas.
- Análisis de documentación oficial de la Comisión Europea, el CCN-CERT y el NIST.
- Estudio de casos de uso reales y potenciales para redes cuánticas.

Resultados esperados:

- Fundamento conceptual sólido sobre el que estructurar las siguientes fases.
- Marco estratégico definido y actualizado.

Fase 2. Análisis técnico de la red MadQCI y diseño de su expansión

En esta fase se estudia en detalle la infraestructura actual de la red MadQCI, con el fin de identificar oportunidades de expansión y evaluar su capacidad de integración con

nuevas tecnologías ópticas. El foco se centra en el campus UPM-Montegancedo, evaluando su viabilidad técnica como nodo adicional dentro de la red cuántica metropolitana madrileña.

Actividades:

- Evaluación de la topología actual de MadQCI.
- Análisis de conectividad, disponibilidad de fibra, equipamiento óptico y condiciones de seguridad física.

Resultados esperados:

- Propuesta técnica de expansión documentada.
- Esquemas preliminares de red e identificación de requisitos tecnológicos.

Fase 3. Diseño y simulación de pruebas de conmutación QKD en ROADM y FOADM

Esta fase explora la viabilidad técnica de implementar enlaces de QKD sobre arquitecturas ópticas reconfigurables, utilizando conmutadores ROADM (dinámicos) y FOADM (estáticos). El objetivo es comprender cómo estas tecnologías afectan a la transmisión cuántica y a la fidelidad de la clave compartida. Se diseñan y simulan distintos escenarios de conmutación cuántica en condiciones realistas.

Actividades:

- Modelado del comportamiento de señales cuánticas en sistemas ROADM y FOADM.
- Simulación de trayectorias ópticas, atenuación, dispersión, y errores de polarización.

- Evaluación de métricas como el QBER (*quantum bit error rate*), tasa de claves secretas y estabilidad del canal.

Resultados esperados:

- Comparación entre topologías de red conmutadas y fijas.
- Recomendaciones sobre configuraciones ópticas óptimas para QKD.

- **Fase 4. Sistematización de resultados y elaboración de conclusiones**

  La fase final consiste en la integración de los conocimientos y resultados obtenidos, orientados tanto a la documentación técnica como a la comunicación académica y divulgativa. Se recopilan conclusiones técnicas sobre la expansión y las pruebas realizadas, y se genera contenido visual y explicativo para facilitar la comprensión del proyecto.

Actividades:

- Redacción del documento final del TFM.
- Elaboración de esquemas, figuras y diagramas explicativos.
- Reflexión sobre posibles líneas de desarrollo futuro y aportaciones del trabajo al ecosistema nacional de redes cuánticas.

Resultados esperados:

- Entregables finales del proyecto: memoria técnica, gráficos, propuestas de continuidad.
- Contribución al conocimiento académico y aplicado en el ámbito de las comunicaciones cuánticas.

4.4 PLANIFICACIÓN

El desarrollo de este Trabajo de Fin de Máster se ha estructurado en seis fases encadenadas y parcialmente solapadas, con el fin de optimizar la ejecución progresiva del análisis, diseño, simulación y redacción del proyecto. La planificación comienza el 2 de diciembre de 2024 y concluye en julio de 2025, contemplando un calendario realista que permite la maduración técnica de cada bloque de trabajo y la validación cruzada entre etapas.

La primera fase, **Exploración Fundamental**, está dedicada a la adquisición de conocimientos teóricos y tecnológicos básicos en óptica cuántica, criptografía cuántica, computación cuántica y redes ópticas. Esta fase establece las bases conceptuales para abordar las fases siguientes con el rigor y profundidad adecuados.

Durante la segunda fase, **Marco y Diagnóstico**, se realiza una revisión detallada del estado del arte en tecnologías QKD, sus protocolos y aplicaciones, además de un estudio del marco institucional y estratégico europeo, nacional y regional en el que se inserta el proyecto, incluyendo EuroQCI y MadQCI.

La tercera fase, **Anatomía de MadQCI**, se centra en el análisis técnico de la red cuántica madrileña, su infraestructura actual, su topología y los requisitos necesarios para su expansión hacia nuevas localizaciones como el campus UPM-Montegancedo.

La cuarta fase, **Diseño Experimental Cuántico**, se enfoca en el desarrollo de simulaciones y diseño de pruebas de conmutación QKD mediante tecnologías ópticas ROADM y FOADM, evaluando su viabilidad en un entorno metropolitano dinámico.

La quinta fase, **Síntesis y Transferencia**, está orientada a la recopilación de resultados, formulación de conclusiones técnicas y elaboración de material divulgativo. Aquí se articula el documento final del TFM, incluyendo figuras, anexos y propuestas de continuidad.

Por último, en la sexta fase, **Revisión y Defensa**, se contempla la revisión por parte de los tutores, la incorporación de ajustes finales y la preparación de la defensa pública ante el tribunal académico.

Fase	Nombre	Fechas estimadas	Descripción resumida
F0	Exploración Fundamental	02/12/2024 – 12/01/2025	Estudio teórico de mecánica cuántica, QKD y contexto tecnológico del proyecto.
F1	Marco y Diagnóstico	13/01/2025 – 07/02/2025	Revisión del estado del arte y análisis del marco estratégico e institucional.
F2	Anatomía de MadQCI	10/02/2025 – 21/03/2025	Análisis técnico de la red MadQCI y diseño preliminar de su expansión.
F3	Diseño Experimental Cuántico	24/03/2025 – 16/05/2025	Diseño y simulación de pruebas de conmutación QKD sobre redes ópticas avanzadas.
F4	Síntesis y Transferencia	19/05/2025 – 27/06/2025	Integración de resultados, redacción final del TFM y elaboración de material divulgativo.
F5	Revisión y Defensa	30/06/2025 – 08/07/2025	Revisión final con tutores, preparación y defensa del trabajo.

Tabla 1: Cronología TFM

4.5 ESTIMACIÓN ECONÓMICA

Clasificación de nodos comerciales MadQCI por coste:

Tipo de nodo	**Rango de precios aproximado (EUR)**	**Observaciones**
Tipo 1	80.000 € – 170.000 €	Equipamiento completo y avanzado
Tipo 2	55.000 € – 80.000 €	Configuración reducida
Tipo 2 (*outlier*)	130.000 €	Nodo de IMDEA Networks; coste atípico

Tabla 2: Coste de nodos por tipo

Coste medio estimado por nodo experimental de laboratorio: ~15.000 €

Esto es una aproximación redondeada basada en componentes discretos y controladores de bajo coste.

Los nodos comerciales desplegados en el marco de MadQCI muestran una diferencia de coste significativa respecto a los entornos de laboratorio, justificada por la necesidad de confiabilidad, interoperabilidad, soporte remoto, capacidad DWDM, y redundancia. El nodo de IMDEA Networks aparece como un caso atípico, reflejando probablemente costes asociados a su integración específica o equipamiento adicional.

Capítulo 5. LA INICIATIVA EUROQCI

En un contexto global de creciente digitalización y amenazas emergentes a la seguridad de la información, la Unión Europea ha lanzado una de las iniciativas más ambiciosas en ciberseguridad cuántica a nivel internacional: la European Quantum Communication Infrastructure (EuroQCI). Esta iniciativa forma parte de la estrategia digital europea y pretende dotar al continente de una infraestructura robusta, escalable y soberana para el intercambio seguro de información basado en tecnologías cuánticas.

EuroQCI está impulsada conjuntamente por la Comisión Europea, la Agencia Espacial Europea (ESA) y los 27 Estados miembros, así como Noruega y otros países asociados. El objetivo es desplegar una infraestructura cuántica paneuropea que integre enlaces de fibra óptica y satelitales para permitir la distribución de claves cuánticas (QKD) entre gobiernos, infraestructuras críticas, centros de defensa y sistemas digitales estratégicos.

5.1 ÁREAS DE ACTUACIÓN

La infraestructura EuroQCI se articula en torno a dos segmentos principales:

- **Red terrena (*fiber-based* QKD):**
  Enlace de nodos nacionales mediante fibra óptica, conectando centros de datos, instalaciones gubernamentales, hospitales, infraestructuras de defensa y servicios públicos. Las redes nacionales se integrarán progresivamente en una macro infraestructura europea, interoperable y supervisada.

- **Red espacial (*satellite-based* QKD):**
  Desarrollo de enlaces ópticos a través de satélites de baja órbita, permitiendo cubrir zonas remotas, conexiones intercontinentales y redundancia estratégica. Esta parte

está coordinada en estrecha colaboración con la ESA y se alinea con el sistema de comunicaciones seguras por satélite europeo IRIS².

5.2 OBJETIVOS ESTRATÉGICOS

Los objetivos fundamentales de EuroQCI pueden resumirse en cinco grandes líneas:

1. **Garantizar la soberanía digital europea** frente a amenazas futuras como la computación cuántica.
2. **Proteger datos sensibles e infraestructuras críticas**, especialmente en sectores como la defensa, la salud, las telecomunicaciones y la energía.
3. **Establecer una red europea certificada y estandarizada** que sirva de modelo para aplicaciones civiles y militares.
4. **Impulsar el liderazgo industrial y tecnológico europeo** en el campo de la criptografía cuántica y los componentes optoelectrónicos.
5. **Consolidar la posición europea en el ecosistema global cuántico**, fomentando la colaboración entre Estados miembros y actores estratégicos.

5.3 INVERSIÓN Y FINANCIACIÓN

EuroQCI se financia principalmente a través de los programas **Digital Europe Programme (DEP)**, que financia el proyecto EuroQCI-Spain, y **Connecting Europe Facility – Digital (CEF-Digital)**. Asimismo, en función del estado miembro, se han articulado otras financiaciones. Por ejemplo, en Madrid, el proyecto MADQuantum-CM, que es una acción complementaria entre PRTR y Comunidad de Madrid, ha financiado

gran parte de la red en esta región. Todos estos fondos se destinan tanto a proyectos nacionales como a enlaces transfronterizos, investigación, estandarización y certificación.

A continuación, se presenta una tabla resumen con las principales cifras de inversión identificadas:

Categoría de inversión	**Importe estimado (€)**	**Fuente de financiación**
Infraestructura nacional terrestre por Estado miembro	3–5 millones por fase	CEF-Digital (cofinanciación 50–70 %)
Proyectos piloto multinacionales	hasta 10 millones	CEF-Digital
Segmento espacial (misión Eagle-1, fase inicial)	40 millones (estimación ESA)	ESA + fondos nacionales
Fase de investigación (proyectos H2020, Horizon Europe)	> 100 millones (desde 2020)	H2020, Horizon Europe
Proyecto NOSTRADAMUS (evaluación QKD y certificación)	~20 millones (2024–2028)	Digital Europe Programme
Total inversión pública acumulada estimada (2020–2025)	> 300 millones	Diversas fuentes europeas y nacionales

Tabla 3: Inversiones EuroQCI

Estas cifras además serían complementadas con financiación extra por cada respectivo país donde se desarrolla el proyecto.

5.4 GEOGRAFÍA DEL DESPLIEGUE

El despliegue de EuroQCI se estructura por países, cada uno desarrollando su segmento nacional (National QCI Segment). Todos los segmentos deben cumplir requisitos de interoperabilidad, criptoseguridad y certificación establecidos por la Comisión Europea.

Hasta la fecha, han iniciado fases activas de despliegue países como:

- **Francia**: con el nodo nacional desarrollado por Thales, Orange y CNRS.
- **Alemania**: liderado por Deutsche Telekom, Fraunhofer y Siemens.
- **Italia**: con proyectos coordinados por INRiM y Leonardo.
- **España**: a través del proyecto MADQuantum-CM y colaboraciones con RedIRIS, Telefónica e IMDEA Software, entre otros.

A medio plazo, se prevé el despliegue de estaciones ópticas terrestres conectadas a satélites QKD en puntos estratégicos como:

- Oberpfaffenhofen (Alemania),
- Toulouse (Francia),
- Ispra (Italia),
- Canarias (España),
- Kourou (Guayana Francesa).

Ubicación	Tipología de despliegue	Conectividad y nodos	Tecnología clave
Madrid	Red urbana operativa	29 nodos en 700 km de enlaces	QKD + SDN + switches + multiplexación
Malta	Red piloto nacional	Múltiples nodos interconectados	Fibra + satélite
Luxemburgo	Nodo nacional integrado	Enlaces terrestres y satelitales	SES Eagle-1 + estaciones ópticas
Italia	Backbone nacional QKD	Conexiones entre ciudades	Trusted nodes + DWDM
Suecia	Red de demostración QKD	Instalación temporal en evento nacional	Sistemas QKD comerciales + control central

Tabla 4: Comparativa de despliegue

5.5 PROYECTO NOSTRADAMUS

Uno de los pilares del EuroQCI es garantizar que las tecnologías desplegadas cumplan con estándares europeos de seguridad cuántica**.** Para ello, se ha lanzado el proyecto NOSTRADAMUS, financiado por el programa Digital Europe con más de 20 millones de euros hasta 2028. Este proyecto establecerá una infraestructura de testing, validación y certificación de tecnologías y servicios de QKD en colaboración con el Joint Research Centre (JRC).

NOSTRADAMUS permitirá evaluar desde componentes ópticos hasta protocolos completos, y será clave para facilitar la adopción regulada de tecnologías QKD en el entorno europeo.

5.6 PERSPECTIVA A FUTURO

A lo largo de 2025 y 2026, EuroQCI evolucionará hacia su integración con otras redes de comunicaciones seguras, especialmente el sistema IRIS², que actuará como una constelación europea de satélites de defensa y seguridad.

Además, se espera que los desarrollos realizados en EuroQCI impulsen:

- La adopción temprana de criptografía post-cuántica (PQC),
- La creación de estándares europeos de interoperabilidad QKD,
- La consolidación de redes cuánticas metropolitanas como nodos funcionales del futuro internet cuántico europeo.

Capítulo 6. MADQCI

La red MadQCI (Madrid Quantum Communication Infrastructure) constituye uno de los despliegues más avanzados y funcionales de infraestructura de comunicaciones cuánticas en Europa. Inserta en la estrategia nacional para el desarrollo de tecnologías cuánticas seguras, MadQCI nace como respuesta al impulso europeo representado por EuroQCI y a la necesidad de crear entornos reales para la evaluación y validación de tecnologías QKD y futuras soluciones híbridas con criptografía post-cuántica.

Esta red no es una red de laboratorio ni un simple demostrador: es una infraestructura realista, operativa y de propósito general, integrada en el tejido urbano de Madrid, con el potencial de ofrecer servicios de comunicaciones seguras para entornos gubernamentales, institucionales, industriales y académicos.

6.1 INICIOS Y EVOLUCIÓN DEL PROYECTO

MadQCI se construye a partir de la experiencia previa del nodo de Madrid en los proyectos europeos OpenQKD (H2020) y CiViC, donde ya se exploraron las primeras pruebas de coexistencia de canales cuánticos y clásicos sobre fibra óptica urbana. A partir de esa experiencia, y con el impulso institucional de la Comunidad de Madrid y fondos europeos (NextGenerationEU y PRTR), nace el consorcio MADQuantum-CM, coordinado por la Universidad Politécnica de Madrid (UPM) e integrado por actores clave como CEM, UCM, UAM, INTA, IMDEA Software (REDIMadrid), Telefónica o IMDEA Networks y su laboratorio 5TONIC, así como diversos fabricantes tecnológicos.

A lo largo de los años 2021 a 2024, MadQCI ha superado múltiples etapas críticas: desde la integración de múltiples dispositivos QKD de distintos fabricantes, hasta la [illegible]n de un modelo de red SDN (*software-defined networking*) para la gestión dinámica de flujos cuánticos. En la actualidad, se encuentra en expansión, incorporando nuevos nodos, casos

de uso y capacidades de reconfiguración óptica que incluyen pruebas con sistemas ROADM y FOADM.

6.2 ACTORES CLAVE Y COLABORACIÓN INSTITUCIONAL

MadQCI se caracteriza por una fuerte colaboración interinstitucional y por su enfoque transversal, que combina investigación académica, despliegue técnico y transferencia tecnológica:

- **UPM**: lidera el diseño y evaluación de arquitecturas de red, modelado del sistema y pruebas funcionales, así como el análisis de escalabilidad.
- **IMDEA Networks**: desarrolla tecnologías de integración, simulación de tráfico, análisis de seguridad, digital twins y pruebas de interoperabilidad.
- **Telefónica y RedIMadrid**: proporcionan la infraestructura de fibra óptica en la que se apoya la red, permitiendo el uso real de enlaces compartidos con tráfico clásico.
- **5TONIC y UC3M**: funcionan como bancos de pruebas para tecnologías híbridas QKD + PQC y como entorno de validación para sistemas de red autónomos.
- **Fabricantes y proveedores tecnológicos**: se integran soluciones de **ID Quantique**, **Toshiba**, **ADVA**, **Rohde & Schwarz**, **AIT**, entre otros, permitiendo una interoperabilidad sin precedentes en redes cuánticas europeas.

6.3 CARACTERÍSTICAS TÉCNICAS DE MADQCI

La red MadQCI está concebida como una infraestructura experimental y operativa de referencia, diseñada para permitir el despliegue, testeo e integración de tecnologías cuánticas de comunicación sobre redes ópticas existentes. En este sentido, representa una arquitectura metropolitana avanzada con múltiples capas de innovación técnica. Sus principales características son las siguientes:

6.3.1 ARQUITECTURA DE RED URBANA HETEROGÉNEA

MadQCI está compuesta por múltiples nodos interconectados distribuidos por toda la ciudad de Madrid y su entorno metropolitano. Estos nodos están conectados por una infraestructura de fibra óptica compartida, gestionada por los operadores Telefónica y REDIMadrid, así como por la propia UPM, con enlaces que abarcan unos 700 km de huella de fibra dedicada.

La red combina:

- Enlaces troncales urbanos de fibra óptica monomodo, ya desplegados y en operación.
- Segmentos ópticos dedicados a tráfico cuántico (QKD), aislados mediante multiplexores WDM y filtros ópticos específicos.
- Infraestructura mixta: algunos enlaces son compartidos entre tráfico cuántico y tráfico IP convencional, validando escenarios de coexistencia realista.
- Más de 700 km de fibra óptica en producción, incluyendo redes académicas y de investigación, así como enlaces empresariales y gubernamentales.

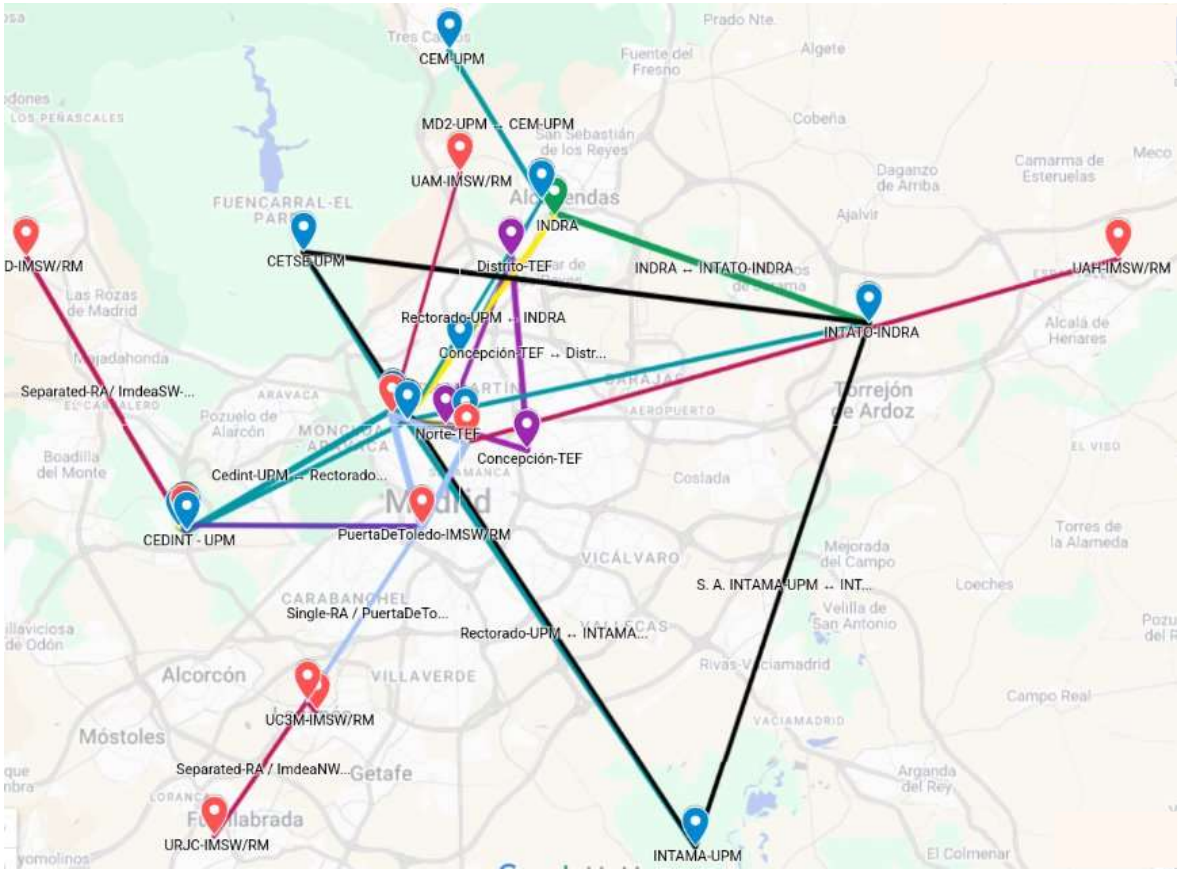

Ilustración 10: Red MadQCI tal y como está planificada y desplegándose en 2025.

Cada color representa un escenario de aplicación distinto; este trabajo expande la red con uno nuevo basado en la conmutación.

6.3.2 DISPOSITIVOS QKD Y PROTOCOLOS

La red MadQCI integra un conjunto multifabricante y multiprotocolo de sistemas QKD, lo cual representa un hito técnico a nivel europeo. Entre los fabricantes que han participado en las distintas fases del proyecto se encuentran: HEQA, ID Quantique, KEEquant, Luxquanta, QTI y Toshiba, entre otros.

HEQA (Israel)

Dispositivo: *HEQA QKD Sceptre*

HEQA ofrece sistemas DV-QKD diseñados para entornos de infraestructura crítica. Utilizan codificación de fase y cuentan con funcionalidades de autenticación física de dispositivos y control de canal cuántico. Su arquitectura es robusta y está pensada para condiciones de operación exigentes. Capaz de integrarse con sistemas de cifrado tradicionales.

ID Quantique (Suiza)

Dispositivos: *Cerberis XGR*.

Sistema comercial preparado para la investigación, totalmente automatizado con integración en redes ópticas metropolitanas, soporte para autenticación y cifrado IPsec, y operaciones 24/7. Alcanza distancias de hasta 100 km y genera claves a velocidades del orden de decenas de kbps en fibra estándar.

KEEQuant (Alemania)

Dispositivo: *KEEQuant Anadriel Testbed Series*

Un sistema DV-QKD compacto orientado a despliegues comerciales. Emplea codificación de fase con *decoy states*, e incorpora medidas para autocalibración y mantenimiento remoto. Su diseño facilita integración en redes DWDM y aplicaciones dentro del marco EuroQCI. Aún en fase de piloto avanzado.

LuxQuanta (España)

Dispositivo: *Nova-LQ*

Es un sistema de QKD por variable continua basado en modulación gaussiana. Ofrece una tasa de generación de clave elevada (del orden de Mbps brutos en distancias cortas) y se integra fácilmente en infraestructuras ópticas DWDM. Opera en el C-band estándar, con

compatibilidad con amplificadores ópticos y ROADMs. Destaca por su bajo coste operativo y su diseño *plug-and-play*.

QTI (Italia)

Dispositivo: *Quell-X*.

Sistema DV-QKD operativo en redes ópticas urbanas. Compatible con protocolos BB84 y variantes. Incorpora canal clásico cifrado, autenticación fuerte y capacidad de gestión remota. Está preparado para entornos de demostración y pilotos precomerciales. Se ofrece con herramientas de monitorización y soporte para entornos SDN.

Toshiba Europe (Reino Unido/Japón)

Dispositivo: *QKD4.3-MU / QKD4.3-LD*

Sistema DV-QKD de grado comercial con soporte para codificación de fase, *decoy states* y variantes de MDI-QKD. Puede operar con enlaces de hasta 120 km y tasas de clave superiores a 100 kbps en condiciones óptimas. Totalmente automatizado, con gestión centralizada, cifrado IPsec y sincronización de canal integrada. Toshiba también desarrolla prototipos funcionales de MDI-QKD de campo.

Rohde & Schwarz Cybersecurity (Alemania) – cifradores integrados.

En total, la red dispone de:

- **23 sistemas QKD activos**, con posibilidad de conmutación.
- Soporte para múltiples **versiones del protocolo BB84**, así como variantes como ***decoy states***, protocolos coherentes (CV-QKD) y *key distillation* automatizada, y un sistema MDI-QKD desplegado en el escenario de alta seguridad.

- Integración con protocolos ETSI GS QKD para control, gestión y reenvío de clave.

6.3.3 GESTIÓN SDN Y CONTROL DE RED

Uno de los principales avances de MadQCI es su control de red definido por *software* (SDN), que permite la gestión centralizada e inteligente del sistema. Esta capa de control está diseñada con los siguientes objetivos:

- Reconfiguración automática de rutas cuánticas en función del estado de la red.
- Adaptación a fallos o eventos de seguridad mediante agentes de red locales.
- Distribución optimizada de claves cuánticas para distintos servicios y usuarios.
- Gestión simultánea de múltiples tecnologías QKD bajo una única arquitectura.

El controlador SDN se comunica con cada uno de los nodos de red y módulos QKD a través de API estándar (RESTful, ETSI QKD 015), permitiendo:

- Redirección de claves en tiempo real.
- Coordinación entre conmutadores ópticos (*switches*) y dispositivos QKD.
- Balanceo de carga entre enlaces redundantes.
- Supervisión y diagnóstico de parámetros físicos: tasa de error, intensidad de señal, estabilidad de fase/polarización.

Este enfoque permite que MadQCI actúe como una red de servicios de claves, más allá de una simple conexión punto a punto.

6.3.4 COEXISTENCIA CUÁNTICO-CLÁSICA

MadQCI ha sido diseñada desde el inicio para validar escenarios de coexistencia real entre tráfico clásico y cuántico sobre la misma infraestructura física. Para ello, se emplean diversas técnicas:

- **Multiplexación densa por longitud de onda (DWDM)**: permite separar el tráfico cuántico (generalmente en la banda C) del tráfico IP convencional.
- **Filtrado óptico pasivo** (AWG, FBG, etc.): utilizado para eliminar interferencias de Raman u otras fuentes de ruido que puedan afectar al canal cuántico.
- **Control activo de potencia óptica**: garantiza que el tráfico clásico no sature los receptores de los sistemas QKD.
- **Aislamiento temporal y espacial** entre señales cuando se emplean fibras compartidas.

6.3.5 ELEMENTOS ÓPTICOS AVANZADOS: ROADM Y FOADM

En el marco de su expansión hacia el campus UPM-Montegancedo, MadQCI está incorporando elementos de conmutación óptica dinámica, en concreto:

FOADM: es un enfoque más simple y económico, útil para escenarios estáticos o de coste reducido, especialmente en nodos periféricos.

En FOADM se usan dispositivos pasivos que permiten insertar (*add*) o extraer (*drop*) ciertas longitudes de onda predeterminadas en una red óptica. Su funcionamiento se basa en la configuración física de filtros ópticos y no requiere control electrónico o *software* para operar. Son los sistemas que transmiten la señal óptica los que seleccionan uno u otro camino al usar uno u otros canal DWDM.

Ventajas:

- Baja complejidad y coste.
- Ausencia de consumo energético.
- Ideal para enlaces estables o topologías fijas.

Limitaciones:

- No se puede modificar la configuración sin intervención manual.
- Escasa flexibilidad para redes dinámicas.
- Su reconfiguración implica interrupción del servicio.

ROADM: este modelo permite redirigir dinámicamente canales cuánticos a través de la red, facilitando la creación de rutas alternativas y la tolerancia a fallos.

El enfoque ROADM usa dispositivos reconfigurables capaces de seleccionar y redirigir longitudes de onda específicas entre distintos puertos mediante control remoto (por *software*, pudiendo ser SDN). Esto permite construir redes que se reconfiguran dinámicamente según la demanda o en respuesta a eventos de fallo.

Ventajas:

- Alta flexibilidad para redes dinámicas.
- Permite reconfiguración sin intervención física.
- Facilita la creación de topologías resilientes.

Limitaciones:

- Coste elevado en comparación con FOADM.
- Mayor complejidad de operación e integración.
- Introduce mayores pérdidas ópticas que los FOADM pasivos.

Estas técnicas permiten a MadQCI experimentar con topologías dinámicas, con reconfiguración automatizada de nodos cuánticos, lo que es esencial para el futuro despliegue de redes cuánticas resilientes.

6.3.6 INTEGRACIÓN CON CIFRADO CLÁSICO Y APLICACIONES REALES

Además de distribuir claves cuánticas, MadQCI permite su uso directo en:

- Sistemas de cifrado simétrico AES-256 mediante integración con dispositivos de red.
- Transmisión segura de datos científicos y administrativos en entornos reales.
- Soporte para servicios distribuidos en 5G y redes de edge computing.
- Aplicaciones e-health, banca, ciberseguridad y defensa, en colaboración con partners institucionales.

Los servicios de clave cuántica se integran con protocolos convencionales de red (IPSec, TLS) gracias a la estandarización de interfaces de software (ETSI QKD 004, 005, 014).

Capítulo 7. MADQCI MONTEGANCEDO

El campus de Montegancedo de la Universidad Politécnica de Madrid (UPM) representa uno de los componentes más estratégicos del ecosistema MadQCI. A diferencia del resto de la red urbana, orientada a pruebas de interoperabilidad, tráfico en producción con múltiples aplicaciones y coexistencia con redes IP, los nodos de Montegancedo están concebidos como entorno controlado de experimentación, con capacidades avanzadas de conmutación óptica y reconfiguración dinámica.

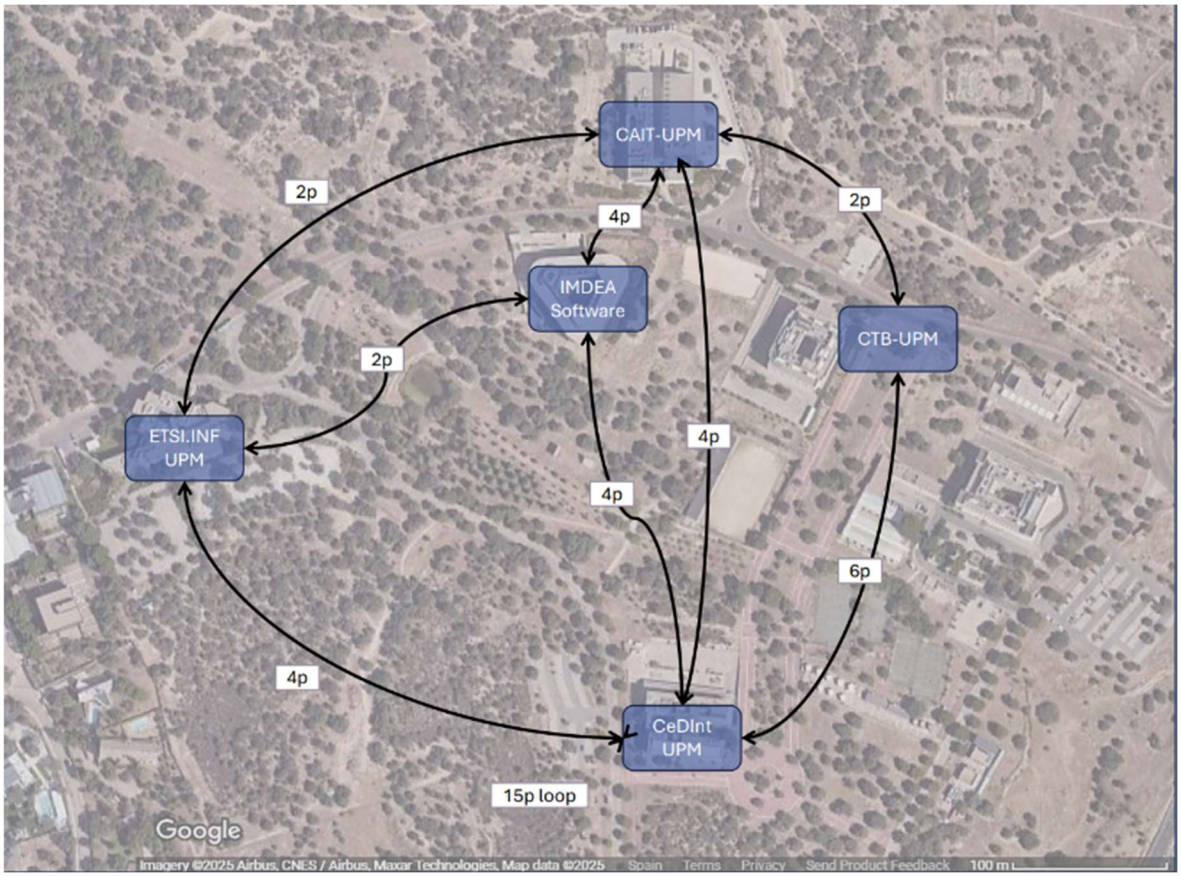

Ilustración 11: Campus de Montegancedo

Montegancedo no es solo un punto de distribución de claves cuánticas, sino un verdadero laboratorio de integración para tecnologías de *switching* fotónico, interoperabilidad QKD, y validación de arquitectura escalable para redes cuánticas. Además, está destinado a

funcionar como banco de pruebas de EuroQCI en escenarios de red resiliente, dinámica y modulable.

7.1 ROL DENTRO DEL PROYECTO

La creación de un nodo especializado en Montegancedo responde a varios objetivos estratégicos:

- Proporcionar un entorno aislado y controlado para pruebas sin impacto sobre nodos de producción.
- Validar tecnologías avanzadas como ROADM y FOADM, fundamentales para el futuro de las redes cuánticas troncales.
- Servir como punto de anclaje académico donde integrar nuevos módulos QKD, controladores SDN y *software* de gestión.
- Desarrollar prototipos funcionales de red cuántica adaptativa y resiliente, simulando fallos, reconfiguraciones y crecimiento progresivo.

Al estar ubicado dentro de un campus universitario multidisciplinar, el nodo también cumple una función formativa, apoyando trabajos de investigación, formación doctoral y colaboración con empresas.

7.2 INFRAESTRUCTURA TÉCNICA

El nodo de Montegancedo se está desplegando con una arquitectura modular, que permite una evolución progresiva desde una configuración de laboratorio a un nodo plenamente funcional. A continuación, se describen sus elementos principales:

7.2.1 SUBSISTEMA ÓPTICO

- **Enlaces internos de fibra monomodo**: conectan diversos *racks* con módulos QKD y dispositivos de red.
- **Enlaces externos**: conexión con el *backbone* de REDIMadrid y el de CeDInt-UPM, permitiendo el acceso a enlaces urbanos reales.
- **Sistema de multiplexación WDM**: separación de tráfico cuántico y clásico, así como canalización paralela de múltiples usuarios.

7.2.2 CONMUTACIÓN ÓPTICA RECONFIGURABLE

El escenario dispondrá de dos tipos de *switching* óptico:

- **FOADM**: unidades pasivas utilizadas para simular nodos de bajo coste, ideales para probar rutas estáticas y evaluar pérdidas de inserción y compatibilidad espectral.

- **ROADM**: dispositivos activos, configurables por software, que permiten reconfigurar dinámicamente qué canales ópticos se enrutan por cada puerto. Esto permite simular:
    - Cambios topológicos instantáneos.
    - Rutas alternativas ante fallos.
    - Balanceo de carga entre rutas.
    - Segmentación lógica de red para múltiples experimentos simultáneos.

Los dispositivos que implementen el enfoque ROADM estarán gestionados mediante controladores SDN que también supervisan la red cuántica.

7.2.3 MÓDULOS QKD

El nodo Montegancedo integrará al menos dos pares de sistemas QKD de fabricantes distintos, siguiendo el enfoque multi-vendor del resto de MadQCI. Las configuraciones previstas incluyen:

- Un sistema BB84 basado en polarización.
- Un sistema coherente de codificación por fase.
- Posibilidad de integrar dispositivos basados en CV-QKD para análisis de compatibilidad espectral con WDM.

Se evaluará su interoperabilidad, estabilidad temporal, sensibilidad al ruido inducido por el switching óptico y su respuesta ante reconexiones dinámicas.

7.2.4 SISTEMA DE CONTROL Y ORQUESTACIÓN

Montegancedo contará con su propio controlador SDN local, capaz de:

- Gestionar la red óptica reconfigurable.
- Supervisar el estado de los enlaces y dispositivos QKD.
- Simular escenarios de fallo y recuperación.
- Orquestar la asignación de claves cuánticas según demanda.

Este sistema estará sincronizado con el controlador central de MadQCI, permitiendo una federación entre el entorno experimental y la red urbana.

7.3 CASOS DE USO Y VALIDACIONES PREVISTAS

El nodo permitirá llevar a cabo pruebas de casos de uso avanzados:

1. **Escenarios de fallo y recuperación automática**
    - Simulación de desconexión de enlaces ópticos y reconexión mediante ROADM.
    - Validación de recuperación de sesiones QKD sin reinicialización.
2. **Distribución multicamino de claves**
    - Reparto de clave cuántica en paralelo por distintas rutas ópticas.
    - Evaluación de consistencia y sincronización.
3. **Comparación entre FOADM y ROADM**
    - En términos de flexibilidad, pérdidas, fidelidad y coste.
    - Determinación del rol ideal de cada tipo de nodo en EuroQCI.
4. **Conmutación dinámica controlada**
    - Mediante *software* externo (orquestador), para integración con redes inteligentes.
    - Aplicación a servicios *cloud* y *edge computing* con QKD.
5. **Entrenamiento y formación**
    - Pruebas para personal técnico y estudiantes, integrando herramientas de visualización y simulación.

7.4 VENTAJAS DEL ENTORNO MONTEGANCEDO

- **Bajo coste operativo** al estar integrado en un campus académico.
- **Flexibilidad máxima** en la configuración, sin impacto sobre nodos en producción.
- **Accesibilidad remota** mediante entornos de simulación (*digital twins*).
- **Sinergia con actividades de investigación** y transferencia tecnológica.

- **Capacidad de prueba de tecnologías emergentes** sin restricciones regulatorias ni comerciales.

7.5 PERSPECTIVAS DE INTEGRACIÓN CON EUROQCI

El escenario desplegado en el campus de Montegancedo está concebido como un laboratorio de referencia para la fase de despliegue de EuroQCI, con potencial para:

- Simular nodos de borde o intermedios en una red nacional.
- Validar arquitecturas resilientes con *switching* óptico.
- Generar conocimiento transferible a despliegues productivos en otras regiones.
- Actuar como punto de referencia para estándares ETSI e ITU.

A medio plazo, se proyecta su integración en una topología regional que conecte Montegancedo con nuevos nodos en otras universidades, organismos públicos o centros hospitalarios, como parte de la expansión planificada en MADQuantum-CM.

Capítulo 8. CONMUTACIÓN ÓPTICA EN REDES QKD

En el marco de la contribución de la Universidad Politécnica de Madrid (UPM) al proyecto NOSTRADAMUS, se ha formulado una propuesta experimental orientada a desarrollar y validar un procedimiento de testeo para medir los tiempos de recalibración de dispositivos QKD en situaciones de operación dinámica y disrupción del canal cuántico. Esta propuesta, registrada como FUN G2, responde a una necesidad clave en el avance de las redes cuánticas seguras: la transición desde arquitecturas estáticas hacia redes conmutadas dinámicamente, capaces de adaptarse en tiempo real a los cambios de topología o de carga.

8.1.1 CONTEXTO

El avance de las tecnologías ópticas y de control en redes QKD está impulsando la implementación progresiva de elementos de *switching* como los usados en ROADM y FOADM. Este cambio de paradigma no solo mejora el rendimiento general de la red, permitiendo el uso eficiente de recursos y la escalabilidad, sino que también incrementa la seguridad al reducir el número de nodos de confianza necesarios (*trusted nodes*).

Sin embargo, este nuevo modelo introduce una necesidad crítica: la recalibración adecuada de los parámetros del enlace cuántico tras cada evento de conmutación. El éxito de dicha recalibración no solo afecta a la continuidad del servicio, sino que es fundamental para mantener la seguridad del sistema, ya que una mala configuración de los parámetros cuánticos puede abrir la puerta a vulnerabilidades explotables por un atacante.

8.1.2 DESCRIPCIÓN TÉCNICA DEL TEST PROPUESTO

La propuesta de la UPM consiste en la implementación de pruebas de *switching* sobre dispositivos CV-QKD, una vez estos se encuentren disponibles en el laboratorio (previsto para marzo de 2025). Las pruebas se realizarán mediante técnicas de *wavelength routing*, en un entorno tipo FOADM, donde el camino óptico está definido por la longitud de onda de entrada.

El esquema general del experimento incluye:

- **Conmutación pasiva** basada en la selección de longitud de onda: al cambiar la frecuencia de emisión del dispositivo CV-QKD, el canal se enruta pasivamente hacia un receptor distinto.
- **Sin necesidad de intervención sobre el plano físico de la red** (no hay reconfiguración activa del ROADM), lo que permite testear únicamente el impacto de la recalibración sobre los sistemas cuánticos.

Se evaluarán parámetros clave:

Parámetro	**Descripción**	**Unidad / Método de Medida**
Tiempo de sincronización	Tiempo que tarda el sistema en reestablecer la sincronización tras el cambio de canal.	ms / registros de sincronización QKD
Tiempo de establecimiento de enlace	Tiempo desde el inicio del *switching* hasta que se establece el canal cuántico.	ms / logs de enlace QKD

Tiempo hasta generación de clave válida	Tiempo necesario para que el sistema genere clave tras la conmutación.	ms / tiempo hasta 'final key material'
QBER (Quantum Bit Error Rate)	Tasa de error de bits cuánticos durante la transmisión tras el cambio.	% / monitorización QKD
Pérdida óptica total (dB)	Pérdida total introducida por la red y el *switching* óptico.	dB / medidor óptico
Estabilidad de la señal (*drift*)	Variación temporal de la señal recibida (*drift* en la alineación).	Unidades arbitrarias / oscilación en el tiempo
Entropía de la clave	Medida de la calidad del secreto de la clave generada.	bits / test de entropía mínima
Resultado del test de aleatoriedad	Evaluación estadística de la aleatoriedad de la clave generada.	NIST STS / Diehard tests
Repetibilidad del experimento	Capacidad del sistema para producir resultados consistentes entre ejecuciones.	Criterio cualitativo / desviación estándar
Impacto del VOA (atenuación variable)	Relación entre atenuación impuesta por VOA y rendimiento de la clave generada.	dB / ajuste del VOA en laboratorio

Tabla 5: Parámetros del experimento de conmutación QKD

8.1.3 JUSTIFICACIÓN DE LA ELECCIÓN TECNOLÓGICA: CV-QKD

Se opta por dispositivos CV-QKD frente a DV-QKD por su mayor flexibilidad inherente en frecuencia y su compatibilidad natural con técnicas de multiplexación temporal y por longitud de onda. Como se ha demostrado en la literatura [1], CV-QKD permite la integración con tecnologías ópticas convencionales, facilitando experimentos FOADM sin necesidad de *switching* activo.

La prueba se desarrollará inicialmente en un entorno de laboratorio controlado, con vistas a su posterior replicación en escenarios reales, como los previstos en el escenario de conmutación de Montegancedo.

8.1.4 IMPORTANCIA Y PROYECCIÓN

Este experimento permitirá:

- Obtener métricas críticas para el diseño de redes QKD reconfigurables.
- Evaluar la robustez de los sistemas CV-QKD ante cambios de canal sin intervención manual.
- Validar condiciones de seguridad ante el riesgo de canales mal calibrados.
- Proporcionar datos para alimentar sistemas de control de red SDN, que dependen del conocimiento preciso de los tiempos de respuesta del sistema cuántico.

La integración de estos resultados en una red cuántica metropolitana con elementos FOADM/ROADM, como la que se está desplegando en Montegancedo, es un paso esencial hacia la automatización segura de redes QKD escalables y distribuidas, alineadas con los objetivos técnicos de EuroQCI.

8.2 MODELOS BÁSICOS DE CONMUTACIÓN FOADM Y ROADM

En el contexto de redes cuánticas metropolitanas, la necesidad de establecer enlaces dinámicos y escalables entre emisores y receptores ha impulsado el estudio de tecnologías de conmutación óptica.

Dos de los modelos más empleados en redes ópticas clásicas y actualmente evaluados para su integración en redes QKD son los previamente explicados FOADM y ROADM**.**

8.2.1 PROCESO DE DESARROLLO DE LOS MODELOS DE PRUEBA

Para evaluar el uso de estos dispositivos en redes QKD, se han desarrollado modelos básicos de conmutación que reproducen el comportamiento funcional de FOADM y ROADM, pero adaptados al entorno de laboratorio y a las limitaciones de los sistemas cuánticos.

El proceso ha consistido en:

- **Definir topologías mínimas viables** para cada modelo, integradas en un banco de pruebas de red óptica controlado.
- **Medir parámetros críticos** como pérdidas de inserción, estabilidad térmica, compatibilidad con señales de baja potencia y sensibilidad a polarización.
- **Emular funciones básicas** de los aparatos ROADM y FOADM comerciales mediante componentes ópticos elementales.
- **Simular eventos de *switching*** tanto manual (FOADM) como programado (ROADM) para analizar su impacto sobre la fidelidad cuántica (QBER) y la capacidad de recuperación del enlace.

8.3 ASUNCIONES Y REQUISITOS DE DISEÑO

En el diseño de los modelos experimentales se han considerado las siguientes asunciones técnicas:

- La sensibilidad a pérdidas es crítica, por lo que las inserciones deben mantenerse < 3 dB por salto.
- Las sesiones QKD se reinicializan tras cada evento de conmutación.
- El *switching* no debe degradar la aleatoriedad de las claves generadas (FUN G4).
- Se usarán enlaces de hasta 30 km simulados con fibra enrollada.

Los **requisitos principales** definidos para ambos modelos incluyen:

Requisito	**FOADM**	**ROADM**
Inserción de pérdida máxima	< 1.5 dB	< 3 dB
Tiempo de conmutación	No aplicable	< 1 segundo
Integración con sistema QKD	Pasiva (transparente)	Activa (control SDN)
Reconfiguración dinámica	No	Sí
Dependencia de polarización	Alta	Media
Coste estimado por unidad	Bajo (~100 €)	Alto (>1000 €)

Tabla 6: Requisitos FOADM y ROADM

Los dispositivos empleados en el laboratorio, tanto FOADM como ROADM, son versiones adaptadas a bajo coste para pruebas de investigación. A nivel comercial, los ROADM empleados en redes de operadores como Telefónica, Orange o Deutsche Telekom presentan características muy superiores en cuanto a gestión de canal, amplificación integrada y supervisión óptica.

En redes ópticas comerciales, los dispositivos ROADM incorporan una amplia variedad de funciones integradas, como amplificación óptica (EDFA), multiplexación y demultiplexación DWDM, y matrices de conmutación reconfigurables, todo ello gestionado mediante interfaces de control remoto estandarizadas (ej. NETCONF/YANG sobre SDN). Estas características, aunque potentes, presentan una barrera de entrada económica y de complejidad para entornos de investigación académica o laboratorios de pruebas con recursos limitados.

Por ello, en este proyecto se ha optado por emular las funciones esenciales de FOADM y ROADM utilizando únicamente componentes discretos y fácilmente integrables, como:

- **Filtros DWDM** para seleccionar longitudes de onda específicas.
- **Acopladores ópticos** para combinar o dividir señales.
- Switches **ópticos 4x4** gobernados mediante interfaces simples para simular reconfiguración.

La siguiente figura muestra una comparación entre un ROADM comercial típico y el modelo experimental implementado para este proyecto:

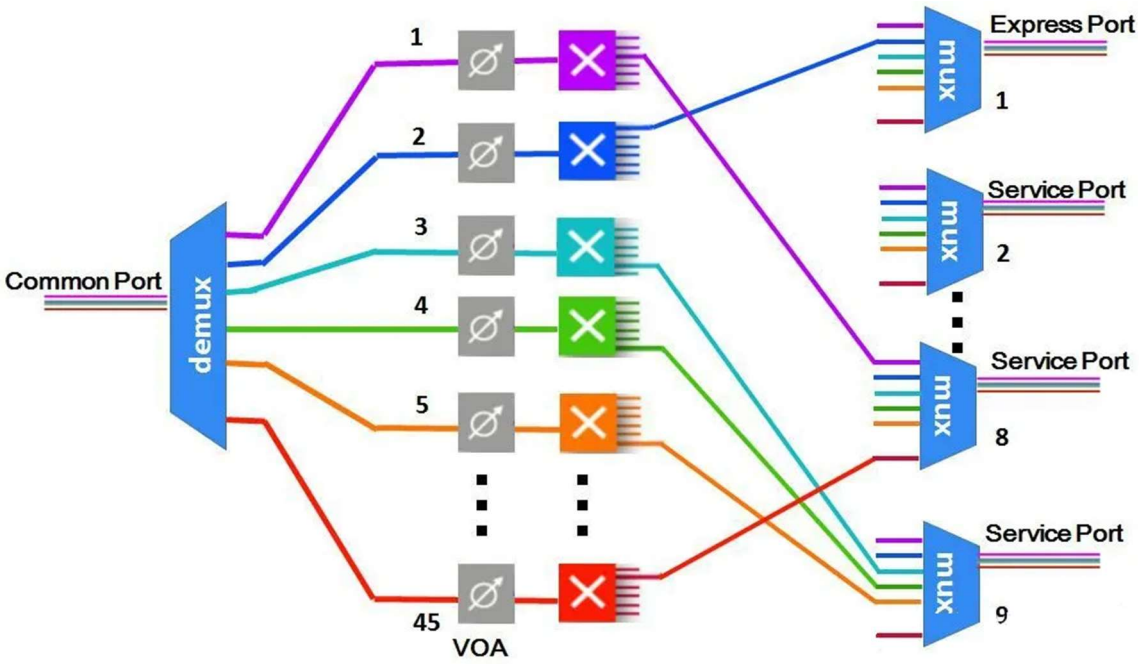

Ilustración 12: Estructura interna de un WSS

Un WSS (*wavelength selective switch*) es un elemento esencial en las redes ROADM. Esta tecnología ha ido evolucionando hasta hoy en día, que esta en plena transición a su cuarta generación con la introducción de CDC-ROADM: incoloro, no direccional e incontenido (*colourless, directionless, contention-less*) que permite conectar cualquier frecuencia a cualquier puerto, atajando así el problema de utilizar la misma banda de frecuencia en el mismo nodo. Estas innovaciones facilitan la recuperación ante fallos.

Como podemos observar en el diagrama estructural, después del multiplexor de entrada, los canales pasan por una matriz de atenuadores ópticos variables (*variable optical atenuator*), un dispositivo utilizado en la gran mayoría de dispositivos ópticos comerciales para ajustar manual o electrónicamente la potencia de una señal, equilibrar pérdidas o proteger receptores sensibles.

Sin embargo, su uso en el contexto de comunicaciones cuánticas, especialmente QKD, presenta serias limitaciones, tanto físicas como de seguridad, que justifican su exclusión en configuraciones reales de canal cuántico.

A continuación, se detallan los principales motivos:

- **Introducción de pérdidas no controladas ni estables**

  Las señales cuánticas, especialmente en protocolos como BB84 o CV-QKD, operan en regímenes de potencia extremadamente bajos, a nivel de unos pocos fotones por pulso. Los VOA introducen pérdidas que, aunque ajustables, pueden fluctuar térmica o mecánicamente, afectando la estabilidad del canal cuántico y dificultando la calibración precisa de los sistemas.

- **Degradación de la tasa de generación de clave**

  Cualquier pérdida adicional en el canal se traduce directamente en una reducción de la tasa de detección de fotones, lo que disminuye la tasa de generación de clave y puede llevar a que la sesión QKD no se establezca si se supera el umbral de tolerancia al ruido (QBER máximo permitido).

- **Aumento del QBER y del riesgo de ataque**

  En presencia de pérdidas artificiales (como las introducidas por un VOA), el sistema receptor debe compensar mediante ajustes internos de ganancia o calibración, lo que puede hacer el sistema más vulnerable a ataques de interceptación, como el ataque de separación de canal (*channel-splitting attack*) o el ataque de inyección por canal de control.

- **Ausencia de control de polarización**

  Los VOA estándar no garantizan preservación del estado de polarización, lo que es crítico en protocolos como BB84, donde la codificación de la información se realiza

sobre este grado de libertad. Cualquier fluctuación introducida puede provocar errores en la decodificación y aumento del QBER.

- **Incompatibilidad con la seguridad post-cuántica**

  En un entorno orientado a seguridad post-cuántica, se debe asegurar que todo el canal es físicamente seguro y ópticamente transparente. La presencia de componentes activos o semiactivos, como algunos modelos de VOA electrónicos, puede suponer vectores de ataque laterales, especialmente si son accesibles por red.

8.4 DISEÑOS BÁSICOS FOADM Y ROADM

Para no tener que lidiar con estas limitaciones, en el laboratorio se trabaja con sistemas compuestos de los componentes individuales de FOADM y ROADM:

8.4.1 DISEÑO FOADM

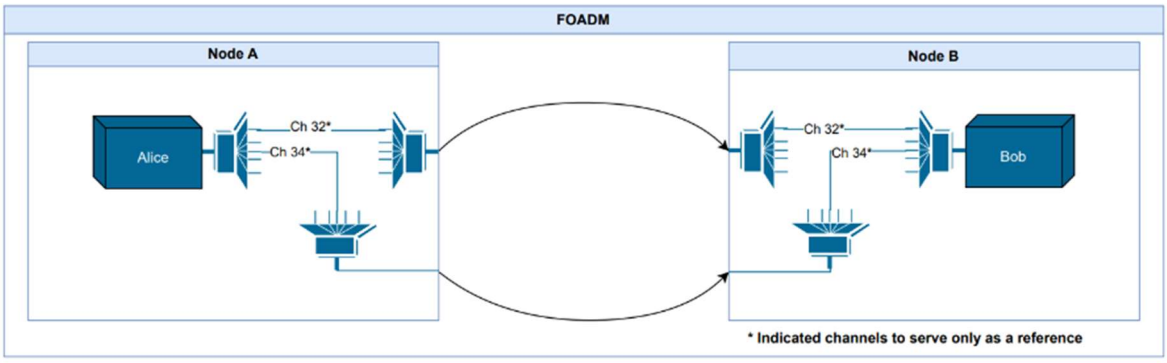

Ilustración 13: Diseño FOADM Simplificado

El sistema de FOADM se sirve de la capacidad del emisor de variar la longitud de onda en emisión según el canal que quiera utilizar. Esta variación de canal sirve para, mediante un demultiplexor, enviar la señal por fibras distintas que mandan la señal a otros multiplexores que, a su vez, acoplan la señal a fibra que puede llevar señal de otras longitudes de onda, permitiendo así integrar la señal cuántica en circuitos de señal clásicos.

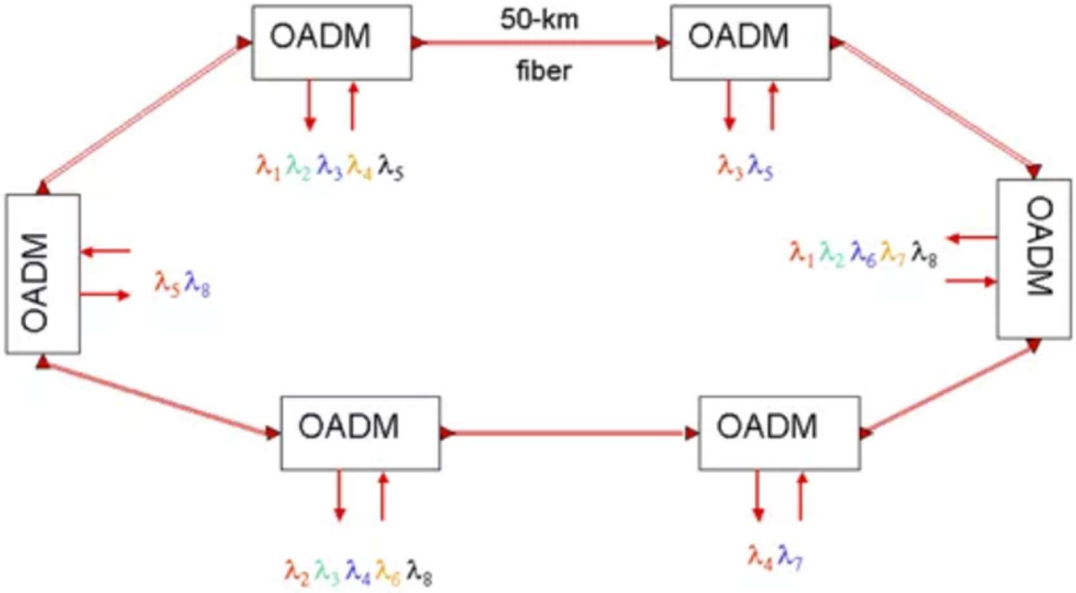

Ilustración 14: FOADM en anillo.

Con una hipotética configuración como la que vemos en la imagen, podemos hacer el despliegue de fibra mucho más eficiente, ya que cada nodo puede controlar que frecuencias absorbe (*drop*), y que frecuencias inserta (*add*).

El emisor puede seleccionar una u otra longitud de onda para conmutar el camino óptico y llegar a uno u otro nodo.

8.4.2 DISEÑO ROADM

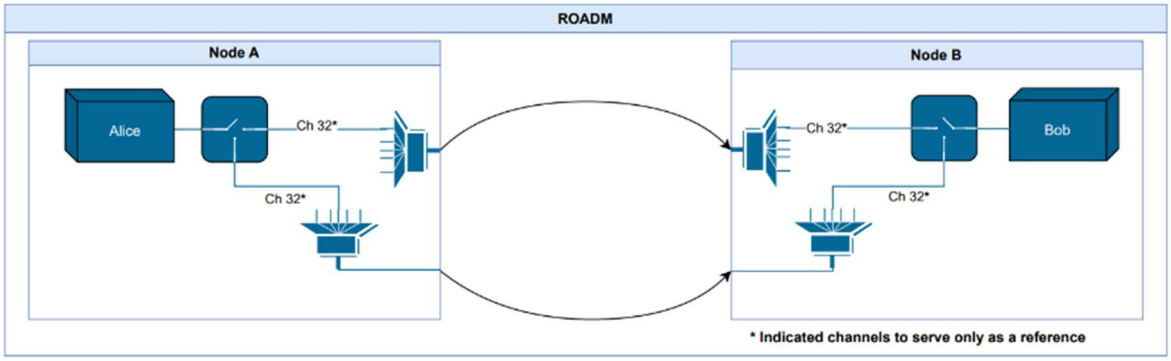

Ilustración 15: Diseño ROADM simplificado

En comparación en un sistema ROADM el destino de la señal se define mediante *switches* ópticos reconfigurables. Este sistema es más complejo, a la vez que más flexible y eficiente, ya que la longitud de onda de la señal es independiente del nodo destino, lo que permite adaptarlo a las capacidades del enlace y de la red.

Así se consigue una red reconfigurable que se puede adaptar en tiempo real a cambios, como pueden ser accidentes con los cables de fibra, ataques a nodos, extensiones de la red y demás.

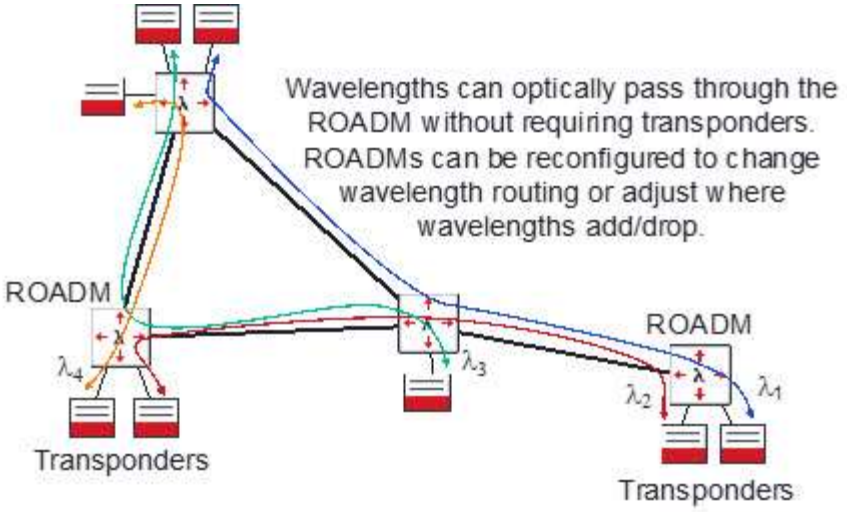

Ilustración 16: Funcionamiento red ROADM

8.5 CONECTIVIDAD ROADM MONTEGANCEDO

La red experimental implementada en el campus de Montegancedo está concebida como un banco de pruebas escalable para el estudio de tecnologías cuánticas de comunicación en entornos dinámicos. Si bien los modelos básicos de conmutación ROADM y FOADM permiten validar el comportamiento individual de los enlaces QKD con *switching* óptico, la siguiente etapa lógica consiste en escalar esta arquitectura para interconectar múltiples nodos dentro del entorno de la UPM.

El esquema de conexiones y fusiones de Montegancedo consiste en 5 nodos interconectados:

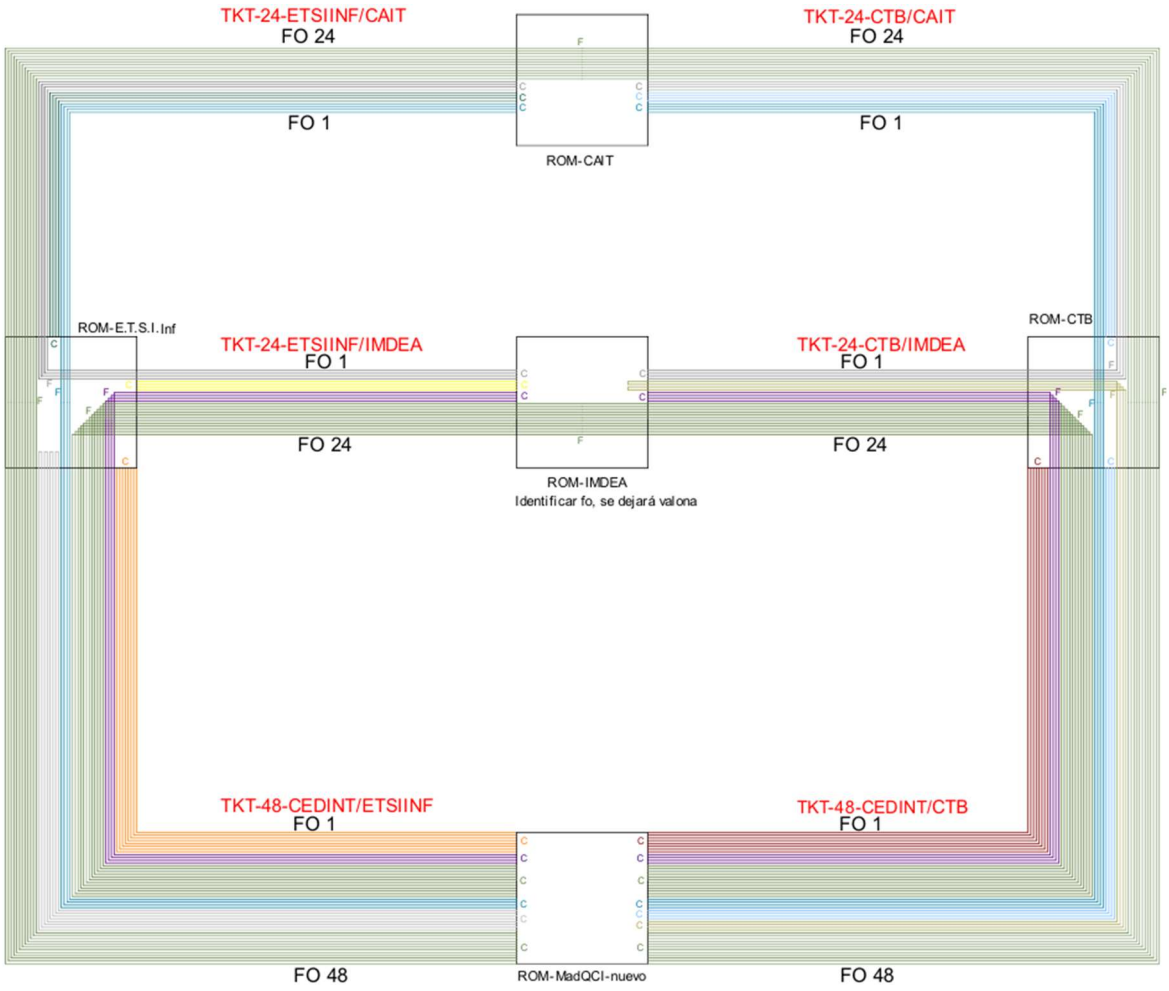

Ilustración 17: Esquema de interconexión desplegado por Elecnor en Montegancedo, expediente de contratación OB 01/24 OTT de la UPM.

Los pares de fibra están dispuestos según estas tablas:

CeDInt [East]				E.T.S.I.Inf				IMDEA SW				CTB				CeDInt [West]	
Id	East		West	Id	East		West	Id	East			West	Id	East		West	Id
1	C	1.1	C	1	F	1.1	I	1	I	3.1		F	1	C	1.1	C	1
2	C	1.2	C	2	F	1.2	I	2	I	3.2		F	2	C	1.2	C	2
3	C	2.1	C	3	F	2.1	I	3	I	4.1		F	3	C	2.1	C	3
4	C	2.2	C	4	F	2.2	I	4	I	4.2		F	4	C	2.2	C	4
5	C	3.1	C	5	C	1.1	I	5	I	1.1-out		F	5	C	3.1	C	5
6	C	3.2	C	6	C	1.2	I	6	I	1.1-in		F	6	C	3.1	C	6
7	C	4.1	C	7	C	2.1	I	7	I	1.2-in		F	7	C	4.1	C	7
8	C	4.2	C	8	C	2.2	I	8	I	1.2-out		F	8	C	4.2	C	8
9	C	1.1	F	9	F	1.1	I	9	I	3.1		F	9	F	3.1	C	9
10	C	1.2	F	10	F	1.2	I	10	I	3.1		F	10	F	3.1	C	10
11	C	2.1	F	11	F	2.1	I	11	I	4.1		F	11	F	4.1	C	11
12	C	2.2	F	12	F	2.2	I	12	I	4.2		F	12	F	4.2	C	12
13	C	1.1	F	13	F	1.1	F	13	F	1.1		F	13	F	1.1	C	13
14	C	1.2	F	14	F	1.2	F	14	F	1.2		F	14	F	1.2	C	14
15	C	2.1	F	15	F	2.1	F	15	F	2.1		F	15	F	2.1	C	15
16	C	2.2	F	16	F	2.2	F	16	F	2.2		F	16	F	2.2	C	16
17	C	3.1	F	17	F	3.1	F	17	F	3.1		F	17	F	3.1	C	17
18	C	3.2	F	18	F	3.2	F	18	F	3.2		F	18	F	3.2	C	18
19	C	4.1	F	19	F	4.1	F	19	F	4.1		F	19	F	4.1	C	19
20	C	4.2	F	20	F	4.2	F	20	F	4.2		F	20	F	4.2	C	20
21	C	5.1	F	21	F	5.1	F	21	F	5.1		F	21	F	5.1	C	21
22	C	5.2	F	22	F	5.2	F	22	F	5.2		F	22	F	5.2	C	22
23	C	6.1	F	23	F	6.1	F	23	F	6.1		F	23	F	6.1	C	23
24	C	6.2	F	24	F	6.2	F	24	F	6.2		F	24	F	6.2	C	24

Tabla 7: Interconexión I

CeDInt [East]				E.T.S.I.Inf				CAIT				CTB				CeDInt [West]	
Id	East		West	Id	East		West	Id	East			West	Id	East		West	Id
25	C	1.1	F	25	F	1.1	C	1	C	3.1	F	25	F	3.1	C	25	
26	C	1.2	F	26	F	1.2	C	2	C	3.1	F	26	F	3.1	C	26	
27	C	2.1	F	27	F	2.1	C	3	C	4.1	F	27	F	4.1	C	27	
28	C	2.2	F	28	F	2.2	C	4	C	4.2	F	28	F	4.2	C	28	
29	C	1.1-out		29	C	1.1	C	5	C	1.1	C	29	C	1.1	C	29	
30	C	1.1-in		30	C	1.2	C	6	C	1.2	C	30	C	1.2	C	30	
31	C	1.2-out		31	C	2.1	C	7	C	2.1	C	31	C	2.1	C	31	
32	C	1.2-in		32	C	2.2	C	8	C	2.2	C	32	C	2.2	C	32	
33	C	2.1-out		33	F	1.1	C	9	C	3.1	F	33	F	1.1-out	C	33	
34	C	2.1-in		34	F	1.2	C	10	C	3.2	F	34	F	1.1-in	C	34	
35	C	2.2-out		35	F	2.1	C	11	C	4.1	F	35	F	1.2-out	C	35	
36	C	2.2-in		36	F	2.2	C	12	C	4.2	F	36	F	1.2-in	C	36	
37	C	7.1	F	37	F	7.1	F	13	F	7.1	F	37	F	7.1	C	37	
38	C	7.2	F	38	F	7.2	F	14	F	7.2	F	38	F	7.2	C	38	
39	C	8.1	F	39	F	8.1	F	15	F	8.1	F	39	F	8.1	C	39	
40	C	8.2	F	40	F	8.2	F	16	F	8.2	F	40	F	8.2	C	40	
41	C	9.1	F	41	F	9.1	F	17	F	9.1	F	41	F	9.1	C	41	
42	C	9.2	F	42	F	9.2	F	18	F	9.2	F	42	F	9.2	C	42	
43	C	10.1	F	43	F	10.1	F	19	F	10.1	F	43	F	10.1	C	43	
44	C	10.2	F	44	F	10.2	F	20	F	10.2	F	44	F	10.2	C	44	
45	C	11.1	F	45	F	11.1	F	21	F	11.1	F	45	F	11.1	C	45	
46	C	11.2	F	46	F	11.2	F	22	F	11.2	F	46	F	11.2	C	46	
47	C	12.1	F	47	F	12.1	F	23	F	12.1	F	47	F	12.1	C	47	
48	C	12.2	F	48	F	12.2	F	24	F	12.2	F	48	F	12.2	C	48	

Tabla 8: Interconexión II

En base a estas esquemáticas, se diseña un diagrama simplificado para poder visualizar las conexiones con más claridad:

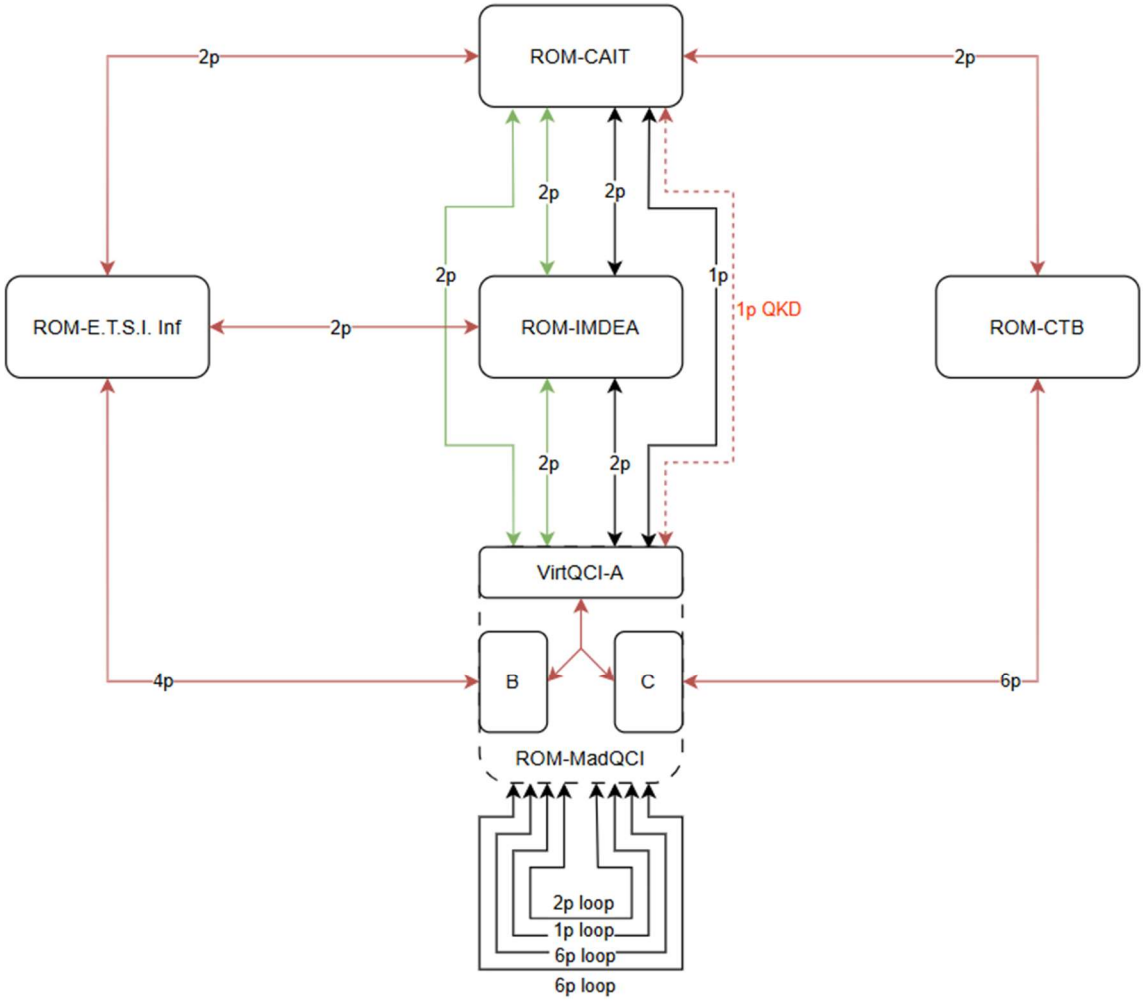

Ilustración 18: Diagrama simplificado Montegancedo de elaboración propia, fundamentado en la documentación del expediente de contratación OB 01/24 OTT de la UPM

Como se muestra en el diagrama, el nodo ROM_MadQCI o CEDINT se puede dividir en tres nodos diferentes "virtuales" para más variedad en la conmutación, creando así los nodos

VirtQCI-A, VirtQCI-B y VirtQCI-C para las direcciones Norte, Oeste y Este, respectivamente.

En este caso, se quiere poder interconectar mediante ROADM los cinco nodos de Montegancedo, diseñando cada nodo según la estructura mostrada en la imagen de diseño ROADM simplificado.

Se busca desarrollar un modelo funcional y operativo en el que diversos laboratorios y equipos de investigación del campus puedan establecer enlaces cuánticos entre sí, de forma flexible y reconfigurable, utilizando exclusivamente *switching* óptico sin intervención manual.

Esta interconexión multi-nodo permitirá:

- Validar la interoperabilidad entre distintos sistemas QKD dentro de una red.
- Estudiar cómo afecta la conmutación a la fidelidad cuántica en topologías complejas.
- Desarrollar políticas de encaminamiento cuántico dinámico mediante control SDN.
- Integrar nodos con diferentes tecnologías (DV-QKD, CV-QKD, multiplexados) en una única infraestructura.

8.5.1 DISEÑO DE LA RED MULTI-NODO

La red se concibe como una malla parcialmente conectada, donde cada nodo representa un laboratorio o *rack* cuántico dotado de un sistema emisor y receptor QKD. Estos nodos estarán conectados a un plano común de conmutación óptica que utilizará elementos ROADM experimentales desarrollados con componentes discretos, como se explicó anteriormente.

Cada nodo contará con:

- **Un puerto de entrada DWDM**, asociado a su longitud de onda específica.
- **Una interfaz de control local** basada en *software* SDN para activar o desactivar rutas.
- **Un *switch* óptico programable**, controlado por la interfaz de control para dirigir el flujo de información
- **Una conexión física a la red de fibra campus**, con distancias típicas inferiores a 2 km.

La selección de destino se hará con la intervención de la interfaz de control, mediante la cual controlamos los *switches* ópticos de la red para establecer los caminos ópticos necesarios:

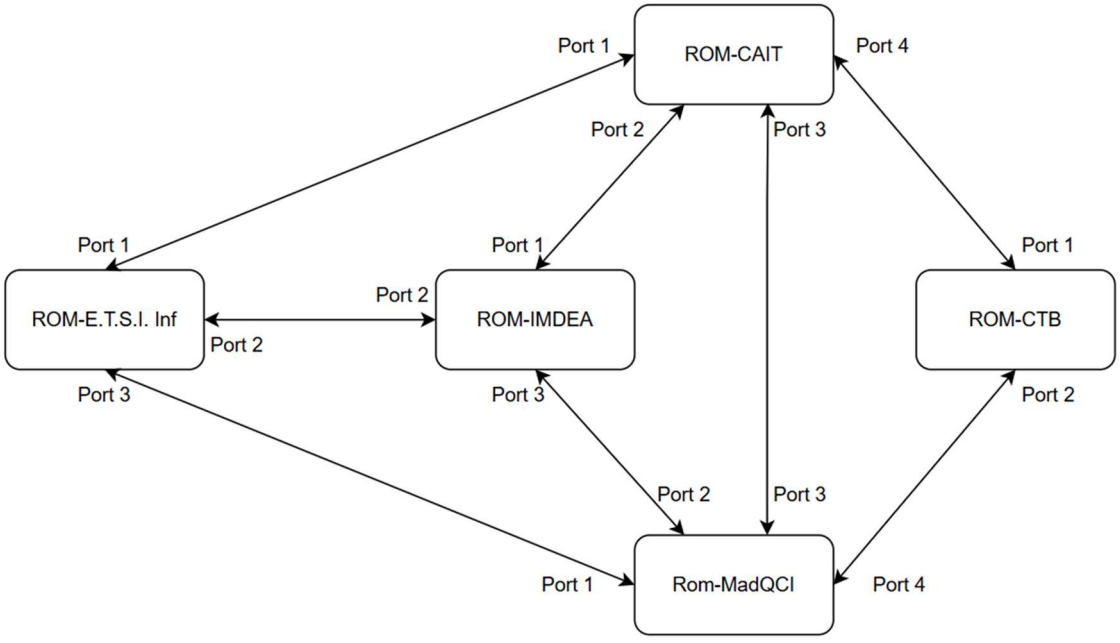

Ilustración 19: Puertos de switch de cada nodo

Los puertos del *switch* óptico de cada nodo salen indicados en la imagen, pero se ven más claramente en la siguiente tabla:

Nº Puerto	CAIT	IMDEA	ETSI	CTB	MadQ-CEDINT
1	ETSI	CAIT	CAIT	CAIT	ETSI
2	IMDEA	ETSI	IMDEA	MadQ-CED	IMDEA
3	MadQ-CED	MadQ-CED	MadQ-CED		CAIT
4	CTB				CTB

Tabla 9: Asignación de puertos de cada nodo

Una de las principales limitaciones a la hora de idear las conexiones son los *switches* ópticos utilizados.

Dado que el laboratorio es un entorno de pruebas, y que necesitábamos un dispositivo de bajo nivel, simple y sin ningún tipo de amplificación o atenuación, los dispositivos de *switching* óptico disponibles no son muchos.

Después de un proceso de selección exhaustivo seleccionamos los *switches* ópticos 4x4 de Gezhi photonics:

Ilustración 20: Switch óptico Gezhi Photonics. Los usados en el laboratorio tenían menos entradas y salidas.

Parameter	Unit	2x4	2x8	2x12	2x16	2x24	2x32	2x64	4x4	8x8	16x16
Wavelength Range	nm	1260~1650									
Testing Wavelength	nm	1310/1550									
Insertion Loss	dB	≤1.5	≤1.5	≤1.5	≤1.5	≤1.8	≤1.8	≤2.0	≤2.0	≤2.0	≤2.5
Return Loss	dB	SM ≥ 50									
Crosstalk	dB	≤-55									
PDL	dB	≤0.05									
WDL	dB	≤0.25									
TDL	dB	≤0.25									
Repeatability	dB	≤0.02									
Lifetime	times	>107									
Switching Time	ms	≤8 (Adjacent Channel)									
Optical Power	mW	≤500									
Connector	/	FC, SC, LC, ST, SMA or customized									
Monitor Port	/	RJ45 , RS232									
Working Power Supply (Plug Tyep)	V	AC: 220V (50/60Hz) or DC: 36V~72V									
Operating Temperature	℃	-10~+60									
Storage Temperature	℃	-40~+85									
Rackmount	mm	19" Rack mount 1U , 2U, 3U or 4U									

Tabla 10: Información técnica del conmutador.

Estos switches son dispositivos muy simples:

Ilustración 21: Panel frontal

Y esa simplicidad nos lleva a un problema, alguno de estos nodos tiene 4 grados de libertad, por lo que todos los puertos de salida estarían ocupados, y en el caso de querer usar un nodo de puente para llegar a otro necesitaremos improvisar.

Con estas restricciones llegamos a una solución, comenzamos mirando el mapa de conectividad interna:

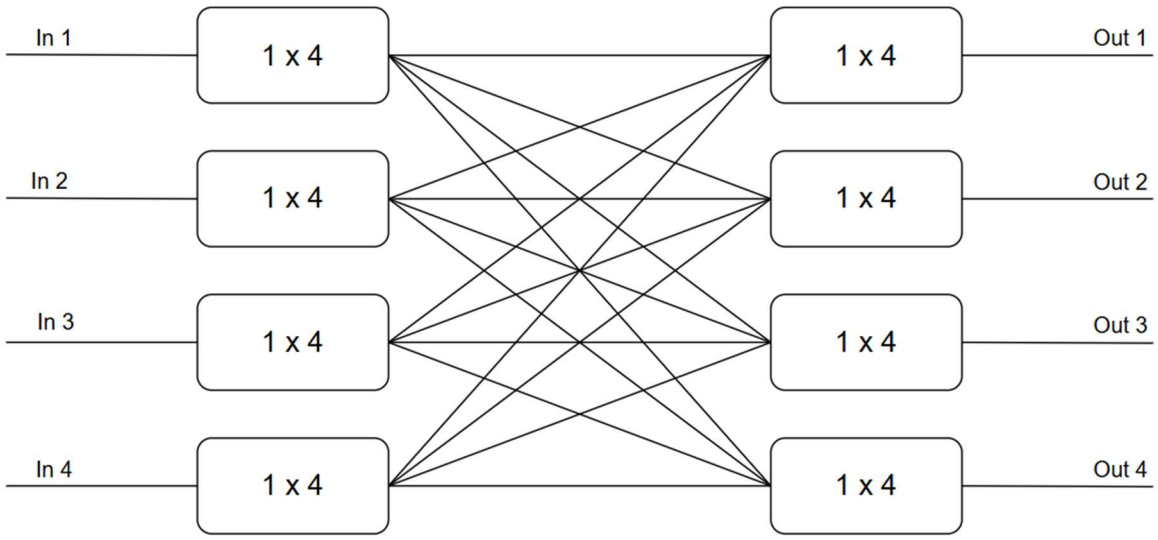

Ilustración 22: Mapa conexión OSW

Durante la planificación hemos asignado los puertos de salida de cada nodo y, para estandarizar, vamos a asignar también los puertos "In" de cada nodo.

Como ya hemos comentado, entre los requisitos esta que cada nodo tiene un dispositivo QKD emisor "Alice" y un dispositivo QKD receptor "Bob". A estos dispositivos les vamos a dedicar respectivamente los puertos In 1 para la emisión y el puerto In 2 para la recepción.

Importante mencionar que, debido a la ausencia de elementos internos cuya función vaya más allá de la redirección de la señal de luz, la función del *switch* es totalmente bidireccional y la nomenclatura "In" u "Out" es una mala elección de diseño por parte del fabricante.

Para mejor comprensión podríamos entenderlos como "In" refiriéndose a los puertos en la "User Network Interface" y "Out" refiriéndose a los puertos en la "Network Node Interface".

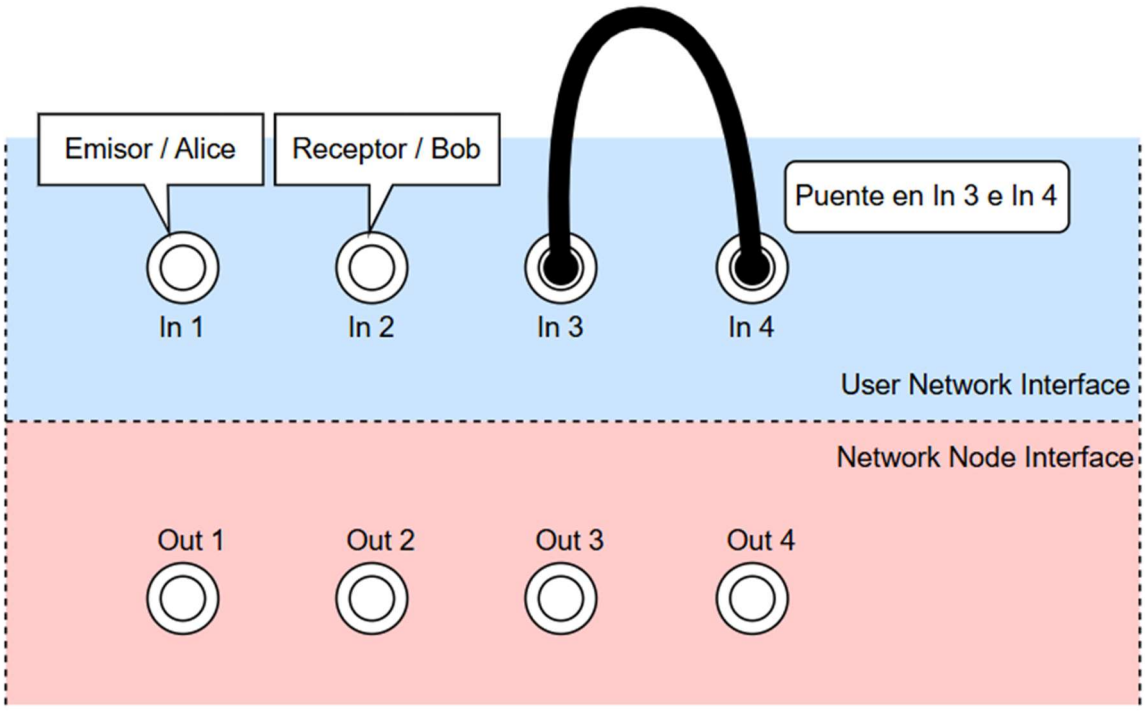

Ilustración 23: Disposición puertos del SWO

Esta disposición es necesaria para conectar nodos que no tengan conexión directa, ya que la funcionalidad básica de este *switch* solo permite conectar puertos de in a out e viceversa.

La propagación seria de esta manera:

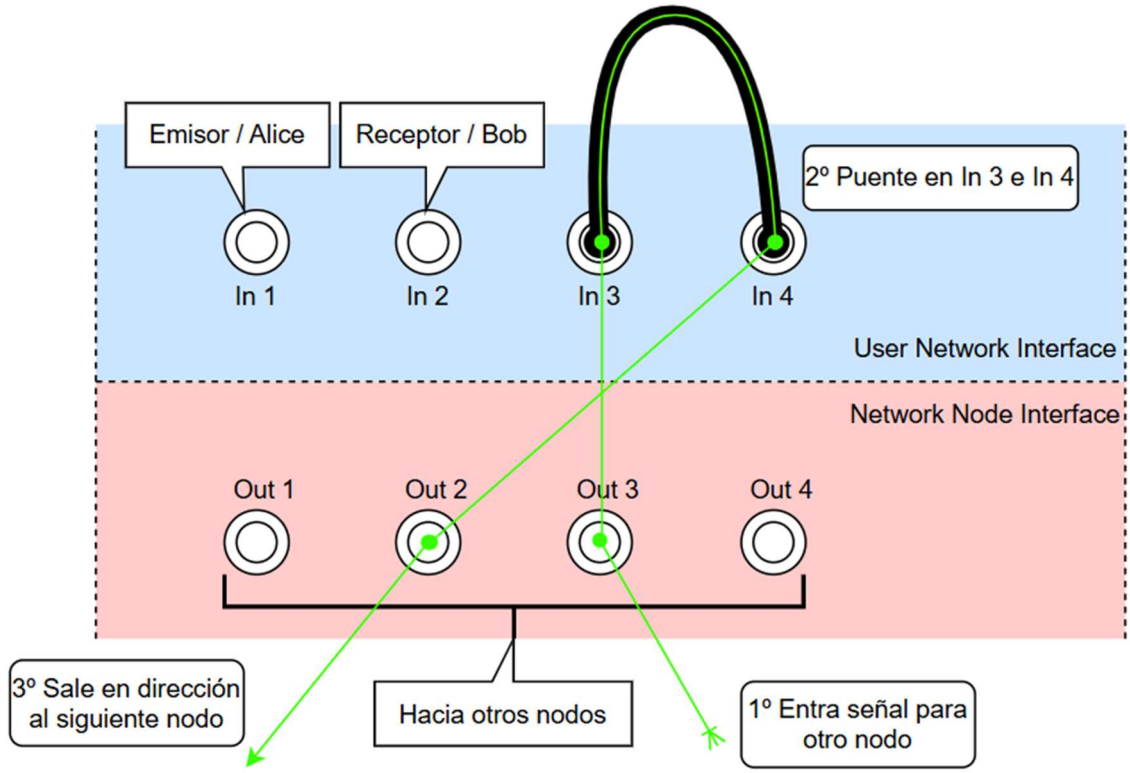

Ilustración 24: Propagación en el switch

Estos *switches* se pueden controlar por la propia pantalla y botones físicos del dispositivo, pero también tienen expuesto un bus serial y un enchufe RJ45 para acceder remotamente y controlarlo mediante esta :

Name	Instructions	Describe
Set Optical Switch Channel	Send:<OSW01_OUT_01_02_03_N>	Setup the optical switch channel to IN1-OUT1,IN2-OUT2,...IN6-OUT6 ,returned successfully;
	Return1:<OSW01_OUT_OK>or Return2:<OSW01_OUT_E1> (go beyond)or Return3:<OSW01_OUT_E2>(fault)	
Query Optical Switch Channel	Send:<OSW01_OUT_?>	Query the optical switch channel,returned successfully; 01: optical switch channel to IN1-OUT1 02: optical switch channel to IN2-OUT2 ------ N: optical switch channel to INM-OUTN
	Return:<OSW01_OUT_01_02_03_N>	
Sets Device Address	Send:<OSW01_ADD_02>	Setup the device address 01 to 02,returned successfully
	Return:<OSW02_ADD_OK>	
Query Device Address	Send:<OSW_ADD_?>	Query the device address, returned successfully 01:device address to 01
	Return:<OSW01_OK>	
Set the IP Address	Send:<OSW01_IP_192.168.1.100>	Setup the IP addresse to 192.168.1.100,returned successfully
	Return:<OSW01_IP_OK>	
Query IP Address	Send:<OSW01_IP_?>	Query the IP address, returned successfully 192.168.1.100:IP address to 192.168.1.100
	Return:<OSW01_IP_192.168.1.100>	
Set the Port Number	Send:<OSW01_PORT_5000>	Setup the port number to 5000,returned successfully
	Return:<OSW01_PORT_OK>	
Query Port Number	Send:<OSW01_PORT_?>	Query the port number ,returned successfully 5000:port number to 5000
	Return:<OSW01_PORT_5000>	
Set the Subnet Mask	Send:<OSW01_SM_255.255.255.0>	Setup the subnet mask to 255.255.255.0, returned successfully
	Return:<OSW01_SM_OK>	
Query Subnet Mask	Send:<OSW01_SM_?>	Query the subnet mask ,returned successfully 255.255.255.0:subnet mask to 255.255.255.0
	Return:<OSW01_SM_255.255.255.0>	
Set the Default Gateway	Send:<OSW01_GW_192.168.1.1>	Setup the default gateway to 192.168.1.1,returned successfully
	Return:<OSW01_GW_OK>	

Tabla 11: API Tabla I

Query Default Gateway	Send:<OSW01_GW_?>	Query the default gateway, returned successfully
	Return:<OSW01_GW_192.168.1.1>	192.168.1.1:default gateway to 192.168.1.1
Set the Baud Rate	Send:<OSW01_BAUD_9600>	Set the baud rate to 9600,returned successfully
	Return:<OSW01_BAUD_OK>	
Query Baud Rate	Send:<OSW01_BAUD_?>	Query the baud rate ,returned successfully
	Return:<OSW01_BAUD_9600>	9600:baud rate to 9600
Lock Keys	Send:<OSW01_KEY_OFF>	Setup the Lock keys to Lock(OFF), returned successfully
	Return:<OSW01_KEY_OK>	
Unlocking Keys	Send:<OSW01_KEY_ON>	Setup the Unlocking keys to Unlocking(ON) , returned successfully
	Return:<OSW01_KEY_OK>	
Query Keys State	Send:<OSW01_KEY_?>	Query the keys state , returned successfully
	Return:<OSW01_KEY_ON>Or Return:<OSW01_KEY_OFF>	ON:Unlocking OFF:Lock
Device Restarts	Send:<OSW01_RESET>	Setup the device restarts , returned successfully
	Return:<OSW01_RESET_OK>	
Query Device Information	Send:<OSW01_TYPE_?>	Query the device information ,returned successfully; Model: FSW-XXXX Wavelength Range: 1260~1650nm Fiber Type: SM(9/125um) Working Power Supply: AC:100~240V
	Return:<OSW01_TYPE_FSW-6X6_1260~1650NM_SM9/125um_FP_	
Query Version	Send:<OSW01_VERSION_?>	Query the version, returned successfully Hardware version: V1.0.1 SOFTWARE: V1.0.1
	Return:<OSW01_VERSION_HARDWARE:V1.0.1SOFTWARE:V1.0.1>	

Tabla 12: API Tabla II

Con esta API, una vez que ya hemos establecido la IP, *gateway* y puerto de cada *switch*, la gran mayoría de operaciones que haremos será de alterar los canales del *switch* óptico con el primer comando de la API.

8.6 SISTEMA DE CONTROL DE SWITCHES ÓPTICOS

Uno de los elementos clave en la implementación de una red cuántica conmutada es la automatización del plano de control, que permite gestionar de forma dinámica las rutas ópticas entre emisores y receptores QKD.

En este proyecto, se ha desarrollado un sistema de asignación de caminos adaptado a una red física experimental basada en *switches* ópticos discretos.

8.6.1 DISEÑO GENERAL DEL SISTEMA DE CONTROL

El sistema de control actúa sobre un conjunto de *switches* ópticos 4x4, que permiten seleccionar rutas entre nodos QKD sin intervención manual. Cada *switch* se controla mediante comandos de red que activan combinaciones específicas de puertos, en función del nodo origen, destino y del rol que desempeña cada uno (origen, intermedio, destino).

Este diseño asume una topología de red definida y conocida, con *switches* que operan de forma determinista según reglas predefinidas. El sistema no depende de descubrimiento de rutas dinámico, lo cual simplifica su implementación, pero mantiene suficiente flexibilidad para representar múltiples configuraciones de red.

El sistema desarrollado consiste de una abstracción de funcionalidades tal que con la red de nodos tenemos un programa que puede actualizar dicha red, y que sirve para calcular caminos óptimos de conexión y traducir estos caminos a los comandos para los switches involucrados.

Estos comandos los envía después de calcularlos, para así establecer la conexión.

Procedemos a comentar las partes más importantes del código:

La primera parte del programa es la carga de los nodos de la red.

Está hecho para que cargue los nodos de la red Montegancedo por defecto, pero se le puede indicar un archivo JSON con la misma estructura para que los cargue desde ahí:

```
def load_nodes(file):
    if file:
        nodes = [
        {'nombre': 'CAIT', 'ID': '01', 'IP':'192.168.220.101', 'port': '5000',
'vecinos': [{'nodo': 'ETSI', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'MADQ', 'peso': 1},{'nodo': 'CTB', 'peso': 1}]},
        {'nombre': 'IMDEA', 'ID': '02', 'IP':'192.168.220.102', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1}, {'nodo': 'ETSI', 'peso': 1}, {'nodo':
'MADQ', 'peso': 1}]},
        {'nombre': 'ETSI', 'ID': '03', 'IP':'192.168.220.103', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'MADQ', 'peso': 1}]},
        {'nombre': 'CTB', 'ID': '04', 'IP':'192.168.220.104', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1},{'nodo': 'MADQ', 'peso': 1}]},
        {'nombre': 'MADQ', 'ID': '05', 'IP':'192.168.220.105', 'port': '5000',
'vecinos': [{'nodo': 'ETSI', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'CAIT', 'peso': 1},{'nodo': 'CTB', 'peso': 1}]},
        ]
    else:
        with open("nodos.json", "r") as f:
            nodes = json.load(f)
    return nodes
```

Después de cargar los nodos, comienza la interacción con el usuario. Se le pregunta por la integridad de la red, donde puede reportar enlaces como rotos o inoperables:

```
print("Are there any compromised connections? (Y/N)")
        ans = input(">>").strip()
        if ans == "Y":
            print("Input node1 name")
            node1 = input(">>").strip()
            print("Input node2 name")
            node2 = input(">>").strip()
            nodes = nm.cambiar_peso_conexion(nodes, node1, node2, 999)
            n_nodos = []
```

Todo este programa opera sobre un grafo que, para hallar la conexión óptima, se analiza con el algoritmo de Djikstra, que funciona para redes pequeñas, pero para redes más amplias se debería cambiar a A*, que utiliza métodos heurísticos para hallar el camino óptimo.

```
def dijkstra(grafo, inicio, destino):
    cola = [(0, [inicio])]
    visitados = set()

    while cola:
        coste, camino = heapq.heappop(cola)
        actual = camino[-1]

        if actual == destino:
            return camino, coste

        if actual in visitados:
            continue
        visitados.add(actual)

        for vecino in grafo.get(actual, [])['vecinos']:
            if vecino['nodo'] not in camino:
                heapq.heappush(cola, (
                    coste + vecino['peso'],
                    camino + [vecino['nodo']]
                ))

    return None, float('inf')
```

Una vez se tiene el camino más corto entre dos nodos formamos los comandos a enviar a cada OSW.

Para generar esos comandos hay que tener en cuenta la configuración del cableado del switch. Separando los nodos según si son emisor, receptor o un nodo intermedio.

Tras generar los comandos se levantan los sockets necesarios para, mediante switches clásicos, comunicarse con los dispositivos ópticos.

Estos comandos siguen el formato OSW01_OUT_XX_XX_XX_XX, donde cada par XX significa el puerto Out por el que va la salida del orden en el que están.

```
def conmutacion_simplex(nodos, nodo1, nodo2):
    camino, coste = os.obtener_camino_mas_corto(nodos, nodo1, nodo2)
    comandos = {}
    for i in range(0,len(camino)):
        prev = camino[i-1] if i > 0 else None
        sig = camino [i+1] if i < (len(camino)-1) else None

        asignacion = os.puertos_comando(nodos, camino[i],prev,sig)
        comm = "<OSW" + asignacion[0] + "_OUT_" + "_".join(asignacion[3]) + ">"
        print(comm)
        ret = dr.sendfunc( asignacion[1], asignacion[2], comm, False)
        if not ret:
            raise RuntimeError(f"Fallo en el envío del comando a {camino[i]}")
        comandos[camino[i]] = asignacion
    return camino, coste, comandos
```

Pudimos probar el programa antes de instalar los componentes en sus nodos:

Ilustración 25: Prueba programa.

En la derecha, el ordenador y la capa de red Ethernet de gestión. En el centro, los conmutadores ópticos, siendo reconfigurados desde la primera. Por último, a la izquierda, dos dispositivos de QKD de HEQA.

Capítulo 9. ANÁLISIS DE RESULTADOS

Este capítulo presenta y analiza los resultados obtenidos durante el proceso de validación experimental del sistema de conmutación óptica cuántica, con especial énfasis en el comportamiento de los parámetros críticos tras los eventos de *switching* y en las implicaciones prácticas de la arquitectura desarrollada. Las pruebas se han realizado en un entorno de laboratorio controlado, simulando diferentes escenarios de operación y disrupción.

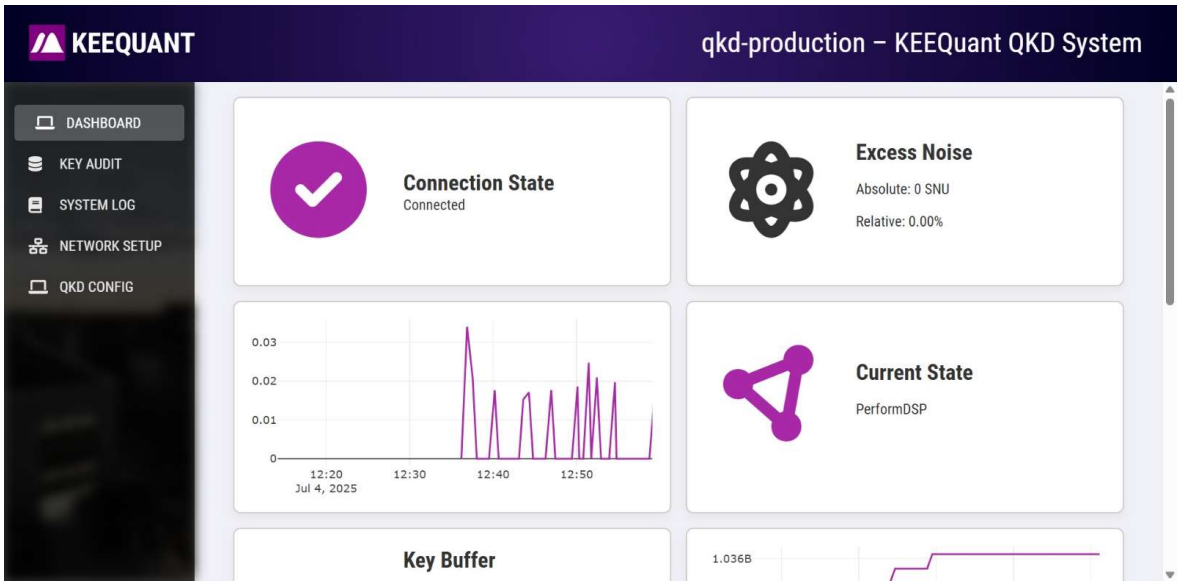

Ilustración 26: Panel de administración KEEQuant.

Las pruebas de conmutación del proyecto Nostradamus se habían comprometido con un sistema CV-QKD, por lo que se seleccionó este sistema.

9.1 METODOLOGÍA DE EVALUACIÓN

Para cada configuración experimental —correspondiente a una ruta entre nodos configurada mediante el sistema FOADM o ROADM emulado— se deben monitorizar los siguientes indicadores clave:

- Tiempo de sincronización y recuperación del enlace cuántico.
- Tasa de generación de clave válida (kbps).
- QBER antes y después del evento de conmutación.
- Entropía de la clave generada.
- Resultados de tests de aleatoriedad (NIST STS).

9.2 RESULTADOS CUANTITATIVOS

Debido al funcionamiento de los dispositivos QKD utilizados, no se han podido tomar medidas de tiempo, ya que contaban con un *buffer* de claves generadas y durante la conmutación no se interrumpía la entrega de clave.

Si se puede apreciar un pico en el QBER, pero se recupera rápidamente.

El análisis muestra que la conmutación, cuando está bien calibrada, no compromete la seguridad ni la funcionalidad del canal cuántico, siempre que los parámetros se reajusten tras cada evento. La degradación momentánea en QBER y sincronización es tolerable y se recupera en menos de 1 segundo en ambos casos.

En particular, se ha observado que:

- Los tiempos de recuperación son lo suficientemente cortos como para permitir *switching* en redes dinámicas.
- La aleatoriedad de las claves generadas no se ve comprometida, incluso tras eventos de *switching*.

Los resultados respaldan la viabilidad del modelo propuesto de conmutación óptica para redes cuánticas experimentales, confirmando que:

- Se pueden realizar pruebas funcionales de *switching* cuántico con equipamiento de bajo coste.
- La arquitectura es extensible a redes más complejas, como la prevista para UPM Montegancedo.
- La integración de *switching* y QKD es técnica y conceptualmente sólida, siempre que se monitoricen y reajusten los parámetros críticos tras cada evento.

Con este trabajo, se asientan las bases para avanzar hacia escenarios más complejos y realistas.

Capítulo 10. CONCLUSIÓN Y TRABAJO FUTURO

Este trabajo ha abordado el diseño, implementación y validación experimental de un sistema de conmutación óptica orientado a redes de distribución cuántica de claves (QKD), con aplicación directa en el contexto de la red MadQCI y su expansión dentro del campus de la Universidad Politécnica de Madrid, Montegancedo. A través de una arquitectura basada en modelos de conmutación ROADM y FOADM, se ha demostrado que es posible crear un entorno de pruebas funcional, flexible y económicamente viable para experimentar con *switching* óptico en redes cuánticas metropolitanas.

Entre los principales logros destacan:

- La implementación de un sistema de control automatizado de switches ópticos, basado en lógica determinista y extensible a plataformas SDN.
- La validación experimental del impacto del *switching* en parámetros críticos de una sesión QKD.
- La conceptualización de una red campus escalable, con *switching* óptico interno, como modelo funcional para redes cuánticas de futuro.

Este trabajo aporta una prueba de concepto completa que contribuye a preparar el terreno para despliegues cuánticos dinámicos más complejos, y al mismo tiempo proporciona una plataforma educativa útil para el desarrollo de talento en el área de las tecnologías cuánticas.

10.1 IMPORTANCIA DEL DESARROLLO FRENTE A AMENAZAS FUTURAS

Uno de los principales motores para el desarrollo de tecnologías como QKD es la amenaza emergente que representa la computación cuántica para los sistemas de cifrado clásicos. Algoritmos como Shor pueden, en teoría, romper sistemas de clave pública ampliamente

utilizados (RSA, ECC) en tiempos reducidos cuando se disponga de ordenadores cuánticos suficientemente potentes.

En este contexto, el desarrollo de tecnologías como QKD no es solo una innovación técnica, sino una necesidad estratégica. Uno de los escenarios más preocupantes es el del ciberataque conocido como *Store Now, Decrypt Later* (SNDL), en el que actores maliciosos interceptan y almacenan comunicaciones cifradas hoy, con la intención de descifrarlas en el futuro cuando los medios cuánticos lo permitan.

Las infraestructuras críticas, la diplomacia, la defensa o el sector financiero son particularmente vulnerables a esta amenaza, y requieren desde hoy soluciones cuánticamente seguras que protejan la confidencialidad a largo plazo. En este sentido, el presente trabajo, aunque centrado en el plano experimental y local, se inscribe en una línea de desarrollo que responde a esta necesidad.

10.2 DESARROLLO FUTURO

Este trabajo se proyecta hacia el futuro en varias direcciones, muchas de ellas alineadas con las estrategias europeas para la soberanía digital y cuántica. Entre los principales desarrollos contemplados se incluyen:

10.2.1 CONTRIBUCIÓN AL PROYECTO NOSTRADAMUS

El sistema desarrollado en este TFM servirá de base para la ejecución de uno de los tests definidos en el marco del proyecto europeo NOSTRADAMUS, liderado por ETSI, cuyo objetivo es explorar tecnologías cuánticas seguras y robustas para entornos dinámicos. Concretamente, se aplicará en el test FUN G2, centrado en la medición de tiempos de recalibración de dispositivos QKD tras disrupciones o cambios de canal. Gracias a su arquitectura modular y a su compatibilidad con CV-QKD, el sistema podrá ser utilizado para evaluar comportamientos críticos en *switching* basado en multiplexación en longitud de onda.

10.2.2 HACIA REDES QKD SATELITALES

Uno de los desarrollos más prometedores en el campo de las comunicaciones cuánticas es la expansión hacia QKD por satélite. Esta tecnología permite superar las limitaciones geográficas y de atenuación de las fibras ópticas mediante enlaces espacio-tierra.
El sistema de conmutación diseñado en este trabajo puede adaptarse a este tipo de redes como parte del plano terrestre de recepción, en el que múltiples estaciones ópticas deben conectarse dinámicamente a nodos de procesamiento cuántico.
Futuros desarrollos podrían incluir:

- Integración con estaciones ópticas móviles para seguimiento de enlaces satelitales.
- Adaptación del sistema a condiciones de atmósfera variable y baja señal.
- Compatibilidad con protocolos híbridos de comunicación (clásica + cuántica).
- Gestión de *switching* multi-usuario para uso compartido de satélites QKD.

10.3 CONSIDERACIONES FINALES

El presente trabajo demuestra que es posible reproducir y evaluar funcionalmente tecnologías de conmutación cuántica avanzadas en entornos controlados y de bajo coste, contribuyendo así a la preparación técnica y académica para los retos que plantea el despliegue de redes cuánticas europeas.

Desde su aplicación en contextos de ciberseguridad estratégica hasta su integración en misiones espaciales, la conmutación óptica cuántica representa un eje transversal de innovación, donde convergen la física, la ingeniería, la informática y la política tecnológica. Preparar hoy estas herramientas es, sin duda, una inversión para el mañana.

Capítulo 11. BIBLIOGRAFÍA

[1] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145.

[2] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012-1236.

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

[4] Mark Fox. (2006). Quantum Optics: An Introduction. Oxford Master Series in Physics. Oxford University Press.

[5] European Commission. (2021). The European Quantum Communication Infrastructure (EuroQCI). https://digital-strategy.ec.europa.eu/en/policies/euroqci

[6] ETSI Industry Specification Group QKD. (2024). Test plan for quantum key distribution networks. Draft version.

[7] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., & Zeilinger, A. (2000). A fast and compact quantum random number generator. Review of Scientific Instruments, 71(4), 1675-1680.

[8] Wang, S., Chen, W., Yin, Z. Q., He, D.-Y., Ye, P., Wang, Y., ... & Pan, J.-W. (2017). Practical gigahertz quantum key distribution robust against channel disturbance. Optics Letters, 42(4), 379-382.

[9] NIST. (2010). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 Revision 1a.

[10] Quantum Flagship. (2024). European Quantum Communication Infrastructure (EuroQCI). https://qt.eu/about-quantum-flagship/euroqci/

[11] Ministerio para la Transformación Digital y de la Función Pública. (2024). Plan Nacional de Tecnologías Cuánticas. https://transformaciondigital.gob.es/planes/plan-nacional-tecnologias-cuanticas

[12] Digital Strategy of the European Commission. (2023). Europe's Digital Decade and EuroQCI. https://digital-strategy.ec.europa.eu/en/policies/euroqci

[13] European Space Agency – ScyLight programme. https://www.esa.int/Applications/Telecommunications_Integrated_Applications/ScyLight

[14] NOSTRADAMUS – ETSI Quantum-Safe Cryptography Project. https://www.etsi.org/technologies/quantum-safe-cryptography

ANEXO I: ALINEACIÓN DEL PROYECTO CON LOS OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS)

El presente Trabajo de Fin de Máster, centrado en el desarrollo de tecnologías para redes de comunicaciones cuánticas seguras y eficientes, se enmarca dentro de una tendencia global orientada a promover la sostenibilidad digital, la resiliencia tecnológica y la protección de la información crítica. En este sentido, el proyecto mantiene una alineación directa con varios de los Objetivos de Desarrollo Sostenible (ODS) definidos por las Naciones Unidas en la Agenda 2030.

A continuación, se detallan los ODS más relevantes en los que este trabajo tiene un impacto directo o indirecto:

ODS 9 – Industria, Innovación e Infraestructura

Meta 9.5: Mejorar la investigación científica y la capacidad tecnológica de los sectores industriales en todos los países.

El desarrollo de redes cuánticas, así como los sistemas de conmutación óptica de nueva generación, forma parte de la infraestructura crítica del futuro. Este proyecto contribuye a la investigación aplicada en tecnologías emergentes y fortalece las capacidades de innovación del ecosistema académico-tecnológico europeo, a través de una red universitaria de pruebas y desarrollo (MadQCI) alineada con las estrategias del proyecto EuroQCI.

ODS 4 – Educación de calidad

Meta 4.4: Aumentar el número de jóvenes y adultos con habilidades técnicas y profesionales relevantes.

Este trabajo no solo se inscribe en un entorno formativo avanzado, sino que también desarrolla herramientas prácticas que pueden ser utilizadas en la enseñanza y divulgación de tecnologías cuánticas. Al diseñar un sistema modular y reproducible, se favorece la formación de talento especializado en una de las áreas más estratégicas del conocimiento tecnológico actual.

ODS 16 – Paz, justicia e instituciones sólidas

Meta 16.10: Garantizar el acceso público a la información y proteger las libertades fundamentales.

Las tecnologías de distribución cuántica de claves (QKD) permiten asegurar la confidencialidad de las comunicaciones en sectores como la diplomacia, la defensa, la salud o la economía. Este trabajo se alinea con la promoción de infraestructuras de comunicación seguras, robustas frente a amenazas futuras como la computación cuántica, contribuyendo así a la resiliencia institucional y la soberanía digital.

ODS 13 – Acción por el clima *(conexión indirecta)*

El desarrollo de infraestructuras digitales seguras y eficientes como alternativa a soluciones energéticamente costosas y centralizadas contribuye, de forma indirecta, a la reducción del consumo energético en la seguridad informática, evitando sobredependencia de sistemas de cifrado de alto coste computacional. Además, el uso de redes ópticas pasivas en el diseño experimental favorece la eficiencia energética en el transporte de datos.

ANEXO II: PROGRAMAS DESARROLLADOS

SERIAL DRIVER DE SWITCH ÓPTICO

```
"""
Autoría y Licencia

Este software ha sido desarrollado por Pablo Ruiz-Tagle en el marco del proyecto
europeo NOSTRADAMUS, dedicado a la investigación en tecnologías de redes
cuánticas.

Queda expresamente prohibido el uso de este código con fines comerciales. Se
autoriza su uso, modificación y distribución exclusivamente para fines
académicos, de investigación y desarrollo no comercial, siempre que se mantenga
esta nota de autoría.

© Pablo Ruiz-Tagle, 2025. Todos los derechos reservados.
"""

import serial
import time

SERIAL_PORT = 'COM3'  # Replace with your actual port
BAUD_RATE = 9600  # 9600 by default, can be changed to 115200
TIMEOUT = 1  # seconds

COMMAND1 = '<OSW01_OUT_01_02_03_04>'
COMMAND2 = '<OSW01_OUT_02_01_03_04>'

try:
    # Open the serial connection
    with serial.Serial(SERIAL_PORT, BAUD_RATE, timeout=TIMEOUT,
                       bytesize=serial.EIGHTBITS,
                       parity=serial.PARITY_NONE,
                       stopbits=serial.STOPBITS_ONE) as ser:
        print("Select Optic path 1 or 2")
        path = input()
        if (path == '1'):
            print(f"Sending command: {COMMAND1.strip()}")
            ser.write(COMMAND1.encode('utf-8'))  # Send

            time.sleep(0.2)  # Wait for response

            response = ser.read(100)  # Read up to 100 bytes
            print(f"Response: {response.decode(errors='replace').strip()}")
        elif (path == '2'):
            print(f"Sending command: {COMMAND2.strip()}")
            ser.write(COMMAND2.encode('utf-8'))  # Send
```

```
            time.sleep(0.2)  # Wait for response

            response = ser.read(100)  # Read up to 100 bytes
            print(f"Response: {response.decode(errors='replace').strip()}")
        else:
            print("Sel. currently disabled")

except serial.SerialException as e:
    print(f"Serial error: {e}")
except Exception as e:
    print(f"Unexpected error: {e}")
```

RJ45 DRIVER DE SWITCH ÓPTICO

```
"""
Autoría y Licencia

Este software ha sido desarrollado por Pablo Ruiz-Tagle en el marco del proyecto
europeo NOSTRADAMUS, dedicado a la investigación en tecnologías de redes
cuánticas.

Queda expresamente prohibido el uso de este código con fines comerciales. Se
autoriza su uso, modificación y distribución exclusivamente para fines
académicos, de investigación y desarrollo no comercial, siempre que se mantenga
esta nota de autoría.

© Pablo Ruiz-Tagle, 2025. Todos los derechos reservados.
"""

import socket
import sys

# Code to establish an IP connection and send commands to a gezhi photonics
Optical switch, either via program arguments or console input
# Proper Use:
#
# Usage via program arguments: python gezhiRJ45.py <IP> <Port> <"Command">
# Example: python gezhiRJ45.py 192.168.220.100 5000 "<OSW01_OUT_02_01_03_04>"
# When executed, Optical Switch 01 with said ip address and port will set its
channels to: IN1-OUT1 IN2-OUT2 IN3-OUT3 IN4-OUT4
#
# Usage via console imput: python gezhiRJ45.py <IP> <Port>
# Example: python gezhiRJ45.py 192.168.220.100 5000
# When executed, a prompt will ask you for the comands you want to send to said
ip address and port.
```

```
def sendfunc( ip, puerto, comando, console):
    try:
        with socket.create_connection((ip, puerto), timeout=10) as sock: # Socket
creation
            if console:    # console is a boolean variable that establishes
operation via program arguments or console input
                print(f"Conected to {ip}:{puerto}. input commands or type exit to
end the program")

            while True:
                if console:     # Enter loop asking for console imput only if
command isn´t set as argument
                    comando = input(">> ").strip()
                    if comando.lower() in ('exit'):     # When sending commands
via console, exit breaks loop
                        print("Connection closing...")
                        break

                sock.sendall(comando.encode('utf-8'))
                respuesta = sock.recv(1024)
                print(f"Rx: {respuesta.decode(errors='replace').strip()}")
                if not console :     # Break loop if command is stated as an
argument
                    break
            return True
    except socket.timeout:
        print("Timeout: no response.")
        return False
    except socket.error as e:
        print(f"Socket error: {e}")
        return False
    except KeyboardInterrupt:
        print("\nSession ended by User")
        return False

if __name__ == "__main__":
    if len(sys.argv) == 3:
        ret = sendfunc(sys.argv[1], int(sys.argv[2]), 0, True)
    elif len(sys.argv) == 4:
        ret = sendfunc(sys.argv[1], int(sys.argv[2]), sys.argv[3].strip(), False)
    else :
        print("Uso: python gezhiRJ45.py <IP> <Port> or python genzhiRJ45.py <IP>
<Port> <\"Command\">")
        sys.exit(1)
```

NODE MANAGER

```
"""
Autoría y Licencia

Este software ha sido desarrollado por Pablo Ruiz-Tagle en el marco del proyecto
europeo NOSTRADAMUS, dedicado a la investigación en tecnologías de redes
cuánticas.

Queda expresamente prohibido el uso de este código con fines comerciales. Se
autoriza su uso, modificación y distribución exclusivamente para fines
académicos, de investigación y desarrollo no comercial, siempre que se mantenga
esta nota de autoría.

© Pablo Ruiz-Tagle, 2025. Todos los derechos reservados.
"""

import json

def load_nodes(file):
    if file:
        nodes = [
        {'nombre': 'CAIT', 'ID': '01', 'IP':'192.168.220.101', 'port': '5000',
'vecinos': [{'nodo': 'ETSI', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'MADQ', 'peso': 1},{'nodo': 'CTB', 'peso': 1}]},
        {'nombre': 'IMDEA', 'ID': '02', 'IP':'192.168.220.102', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1}, {'nodo': 'ETSI', 'peso': 1}, {'nodo':
'MADQ', 'peso': 1}]},
        {'nombre': 'ETSI', 'ID': '03', 'IP':'192.168.220.103', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'MADQ', 'peso': 1}]},
        {'nombre': 'CTB', 'ID': '04', 'IP':'192.168.220.104', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1},{'nodo': 'MADQ', 'peso': 1}]},
        {'nombre': 'MADQ', 'ID': '05', 'IP':'192.168.220.105', 'port': '5000',
'vecinos': [{'nodo': 'ETSI', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'CAIT', 'peso': 1},{'nodo': 'CTB', 'peso': 1}]},
        ]
    else:
        with open("nodos.json", "r") as f:
            nodes = json.load(f)
    return nodes

def cambiar_peso_conexion(nodos, nodo_origen, nodo_destino, nuevo_peso):
    for nodo in nodos:
        if nodo['nombre'] == nodo_origen:
            for vecino in nodo['vecinos']:
                if vecino['nodo'] == nodo_destino:
                    vecino['peso'] = nuevo_peso
        elif nodo['nombre'] == nodo_destino:
            for vecino in nodo['vecinos']:
                if vecino['nodo'] == nodo_origen:
                    vecino['peso'] = nuevo_peso
```

```
    return nodos
```

GRAPH MANAGER

```
"""
Autoría y Licencia

Este software ha sido desarrollado por Pablo Ruiz-Tagle en el marco del proyecto
europeo NOSTRADAMUS, dedicado a la investigación en tecnologías de redes
cuánticas.

Queda expresamente prohibido el uso de este código con fines comerciales. Se
autoriza su uso, modificación y distribución exclusivamente para fines
académicos, de investigación y desarrollo no comercial, siempre que se mantenga
esta nota de autoría.

© Pablo Ruiz-Tagle, 2025. Todos los derechos reservados.
"""

import heapq

def construir_grafo(nodos):
    grafo = {}
    for nodo in nodos:
        nombre = nodo['nombre']
        id = nodo['ID']
        ip = nodo['IP']
        port = nodo['port']
        vecinos = nodo['vecinos']
        grafo[nombre] = {
            'id': id,
            'ip': ip,
            'port': port,
            'vecinos': vecinos
        }
    return grafo

def dijkstra(grafo, inicio, destino):
    cola = [(0, [inicio])]
    visitados = set()

    while cola:
        coste, camino = heapq.heappop(cola)
        actual = camino[-1]

        if actual == destino:
            return camino, coste
```

```
        if actual in visitados:
            continue
        visitados.add(actual)

        for vecino in grafo.get(actual, [])['vecinos']:
            if vecino['nodo'] not in camino:
                heapq.heappush(cola, (
                    coste + vecino['peso'],
                    camino + [vecino['nodo']]
                ))

    return None, float('inf')

def obtener_camino_mas_corto(nodos, origen, destino):
    grafo = construir_grafo(nodos)
    camino, coste = dijkstra(grafo, origen, destino)
    return camino, coste

def indice_vecino(grafo, nodo_origen, nodo_destino):
    for i, vecino in enumerate(grafo[nodo_origen]['vecinos']):
        if vecino['nodo'] == nodo_destino:
            return i
    return -1  # No encontrado

def puertos_comando(nodos, nodo, prev, sig):
    grafo = construir_grafo(nodos)
    if not prev:    # Nodo Origen
        puerto = indice_vecino(grafo,nodo,sig)+1
        comando = []
        comando.append(f"{puerto:02d}")
        for i in range(1,5):
            if i != puerto:
                comando.append(f"{i:02d}")
    elif not sig:     # Nodo Destino
        puerto = indice_vecino(grafo, nodo, prev)+1
        comando = []
        for i in range(1,5):
            if i != puerto:
                comando.append(f"{i:02d}")
        comando.insert(1,f"{puerto:02d}")
    else:           # Nodo Intermedio
        puerto_in = indice_vecino(grafo,nodo,prev)+1
        puerto_out = indice_vecino(grafo,nodo,sig)+1
        comando = []
        for i in range(1,5):
            if (i != puerto_in) and (i != puerto_out):
                comando.append(f"{i:02d}")
        comando.append(f"{puerto_in:02d}")
        comando.append(f"{puerto_out:02d}")
    id = grafo[nodo]["id"]
    ip = grafo[nodo]["ip"]
    port = grafo[nodo]["port"]
    return id, ip, port, comando
```

```
if __name__ == "__main__":
    nodos = [
        {'nombre': 'CAIT', 'ID': '01', 'IP':'192.168.220.101', 'port': '5000',
'vecinos': [{'nodo': 'ETSI', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'MADQ', 'peso': 1},{'nodo': 'CTB', 'peso': 1}]},
        {'nombre': 'IMDEA', 'ID': '02', 'IP':'192.168.220.102', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1}, {'nodo': 'ETSI', 'peso': 1}, {'nodo':
'MADQ', 'peso': 1}]},
        {'nombre': 'ETSI', 'ID': '03', 'IP':'192.168.220.103', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'MADQ', 'peso': 1}]},
        {'nombre': 'CTB', 'ID': '04', 'IP':'192.168.220.104', 'port': '5000',
'vecinos': [{'nodo': 'CAIT', 'peso': 1},{'nodo': 'MADQ', 'peso': 1}]},
        {'nombre': 'MADQ', 'ID': '05', 'IP':'192.168.220.105', 'port': '5000',
'vecinos': [{'nodo': 'ETSI', 'peso': 1}, {'nodo': 'IMDEA', 'peso': 1},{'nodo':
'CAIT', 'peso': 1},{'nodo': 'CTB', 'peso': 1}]},
        ]

    camino, coste = obtener_camino_mas_corto(nodos, 'ETSI', 'CTB')
    comandos = {}
    for i in range(0,len(camino)):
        prev = camino[i-1] if i > 0 else None
        sig = camino [i+1] if i < (len(camino)-1) else None

        comandos[camino[i]] = puertos_comando(nodos, camino[i],prev,sig)
    print("Camino:", camino)
    print("Coste:", coste)
    print("comandos:", comandos)
```

CONMUTATION MAIN

```
"""
Autoría y Licencia

Este software ha sido desarrollado por Pablo Ruiz-Tagle en el marco del proyecto
europeo NOSTRADAMUS, dedicado a la investigación en tecnologías de redes
cuánticas.

Queda expresamente prohibido el uso de este código con fines comerciales. Se
autoriza su uso, modificación y distribución exclusivamente para fines
académicos, de investigación y desarrollo no comercial, siempre que se mantenga
esta nota de autoría.

© Pablo Ruiz-Tagle, 2025. Todos los derechos reservados.
"""
```

```
import gezhiRJ45 as dr
import OSW_commands as os
import node_manager as nm

def conmutacion_simplex(nodos, nodo1, nodo2):
    camino, coste = os.obtener_camino_mas_corto(nodos, nodo1, nodo2)
    comandos = {}
    for i in range(0,len(camino)):
        prev = camino[i-1] if i > 0 else None
        sig = camino [i+1] if i < (len(camino)-1) else None

        asignacion = os.puertos_comando(nodos, camino[i],prev,sig)
        comm = "<OSW" + asignacion[0] + "_OUT_" + "_".join(asignacion[3]) + ">"
        print(comm)
        ret = dr.sendfunc( asignacion[1], asignacion[2], comm, False)
        if not ret:
            raise RuntimeError(f"Fallo en el envío del comando a {camino[i]}")
        comandos[camino[i]] = asignacion
    return camino, coste, comandos


nodes = nm.load_nodes(True)
n_nodos = []
for nodo in nodes:
    n_nodos.append(nodo['nombre'])
print("Nodos disponibles en la red:")
print(n_nodos)
while True:
    print('Input TX node name, "nodelist", "network" or "exit" to end program')
    tx = input(">>").strip()
    if tx == ("exit"):
        break
    elif tx == ("nodelist"):
        print("Nodos disponibles en la red:")
        print(n_nodos)
    elif tx == ("network"):
        print("Change connection status")
        print("Input node1 name")
        node1 = input(">>").strip()
        print("Input node2 name")
        node2 = input(">>").strip()
        print("Connection is up?(Y/n)")
        ans = input(">>")
        if ans == "Y":
            weigh = 1
        else:
            weigh = 999
        nodes = nm.cambiar_peso_conexion(nodes, node1, node2, weigh)

    elif tx not in n_nodos:
        print("No existe ese Nodo")
```

```
    else:
        print('Input RX node')
        rx = input(">>").strip()
        if tx not in n_nodos:
            print("No existe ese nodo")
        else:
            camino, coste, comandos = conmutacion_simplex(nodes, tx, rx)
            print("Camino:", camino)
            print("Coste:", coste)
            print("comandos:", comandos)
print("OSW closing tasks")
```