GRADIANT, Fundación Centro Tecnolóxico de Telecomunicacións de Galicia

Investigación de la aplicabilidad de las tecnologías cuánticas a las telecomunicaciones

Isabel Burdon Hita
Óscar Iglesias González
Javier Abia Álvarez
Luis Pérez Roca
Gabriel María Carral López
Miguel Ferreira Cao

[21/09/2023]

Unha maneira de facer Europa.

Despregamento dunha infraestructura baseada en tecnoloxías cuánticas da información que permita impulsar a I+D+i en Galicia.

Apoiar a transición cara a una economía dixital.

Operación financiada pola Unión Europea, a través do FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL (FEDER) como parte da resposta da Unión á pandemia da COVID-19

Tabla de contenidos

Lista de figuras

Lista de tablas

Lista de acrónimos

AES	*Advanced Encryption Standard (estándar de encriptación avanzado)*
AI	*Artificial Intelligence (inteligencia artificial)*
APD	*Avalanche Photodiode (fotodiodo de avalancha)*
BQC	*Blind Quantum Computing (computación cuántica a ciegas)*
CA	*Certification Authority (autoridad de certificación)*
CMOS	*Complementary Metal-Oxide-Semiconductor (semiconductor complementario de óxido metálico)*
CSRNG	*Cryptographically Secure Random Number Generator (generador de números aleatorios criptográficamente seguro)*
DSA	*Digital Signature Algorithm (algoritmo de firma digital)*
EIT	*Electromagnetic-Induced Transparency (transparencia inducida electromagnéticamente)*
EuroQCI	*European Quantum Communication Initiative (iniciativa europea para la comunicación cuántica)*
GAN	*Generative Adversarial Network (red generativa adversarial)*
IoT	*Internet-of-Things (Internet de las cosas)*
ITS	*Information-Theoretic Secure (segura según teoría de la información)*
IRS	*Intelligent Reflecting Surfaces (superficies reflectantes inteligentes)*
KPI	*Key Performance Indicator (indicador clave de rendimiento)*
MIMO	*Multiple-Input Multiple-Output (entradas múltiples con salidas múltiples)*
ML	*Machine Learning (aprendizaje automático)*
MUBs	*Mutually Unbiased Bases (bases mutuamente imparciales)*
NISQ	*Noisy Intermediate-Scale Quantum (régimen cuántico de escala*

	intermedia ruidosa)
NIST	*National Institute of Standars of Technology (instituto de estándares de la tecnología de EEUU)*
NN	*Neural Network (red neuronal)*
NOMA	*Non-Orthogonal Multiple Access (acceso múltiple no ortogonal)*
NP	*Non-deterministic Polynomial (polinomial no-determinístico)*
NV center	*Nitrogen-Vacancy Center (centro de vacante de nitrógeno)*
ODMR	*Optically Detected Magnetic Resonance (resonancia magnética detectada ópticamente)*
OTP	*One-Time Pad (libreta de un solo uso)*
PKI	*Public-Key Infrastructure (infraestructura de clave pública)*
PNS	*Photon-Number Splitting*
PQC	*Post-Quantum Cryptography (criptografía post-cuántica)*
PRNG	*Pseudorandom Number Generator (generador de números pseudoaleatorios)*
QAI	*Quantum Internet Alliance (alianza por el internet cuántico)*
QAOA	*Quantum Approximate Optimization Algorithm (algoritmo de optimización aproximada cuántica)*
QBER	*Quantum Bit Error Rate (tasa de error binaria cuántica)*
QC	*Quantum Computing (computación cuántica)*
QCH	*Quantum Communications Hub (centro de comunicaciones cuánticas)*
QEC	*Quantum Error Correction (corrección cuántica de errores)*
QFT	*Quantum Fourier Transform (transformada cuántica de Fourier)*
QI	*Quantum Internet (internet cuántico)*
QKD	*Quantum Key Distribution (distribución cuántica de claves)*
CV-QKD	*Continuous-Variable QKD (QKD de variable continua)*
DV-QKD	*Discrete-Variable QKD (QKD de variable discreta)*
DI-QKD	*Device-Independent QKD (QKD independiente de dispositivo)*
MDI-QKD	*Measurement Device-Independent QKD (QKD independiente de dispositivo de medida)*
TF-QKD	*Twin Field QKD (QKD de campos gemelos)*
QM	*Quantum Mechanics (mecánica cuántica)*
QML	*Quantum Machine Learning (aprendizaje automático cuántico)*
QNN	*Quantum Neural Network (red neuronal cuántica)*

QPE	*Quantum Phase Estimation (estimación cuántica de fase)*
QPU	*Quantum Processing Unit (unidad de procesamiento cuántico)*
QRNG	*Quantum Random Number Generator (generador cuántico de números aleatorios)*
QSDC	*Quantum Secure Direct Communication (comunicación cuántica directa segura)*
QSVM	*Quantum Support Vector Machine (máquina de soporte de vectores cuántica)*
QUBO	*Quadratic Unconstrained Binary Optimization (optimizaciones binarias cuadráticas sin restricciones)*
RAN	*Radio Access Network (red de acceso de radio)*
C-RAN	*Centralized RAN (RAN centralizada)*
RL	*Reinforcement Learning (aprendizaje por refuerzo)*
SDN	*Software Defined Networks (redes definidas por software)*
SNS	*Sending-Not-Sending*
SNSPD	*Superconducting Nanowire Single-Photon Detector (detectores de fotón único basados en nanocables superconductores)*
SQL	*Standard Quantum Limit (límite cuántico estándar)*
SVD	*Singular Value Decomposition (descomposición en valores singulares)*
SVM	*Support Vector Machine (máquina de soporte de vectores)*
SVP	*Shortest-Vector Problem (problema del vector más corto)*
TIC	*Tecnologías de la Información Cuántica*
TLS	*Transport-Layer Security (seguridad de la capa de transporte)*
TRL	*Technological Readiness Level (nivel de madurez tecnológica)*
TRNG	*True Random Number Generator (generador de números aleatorios verdaderos)*
UE	*User Equipment (equipo de usuario)*
ULL	*Ultra-Low Loss (pérdida ultra-baja)*
VLC	*Visible Light Communication (comunicación de luz visible)*
VPP	*Vector Perturbation Precoding (precodificación de perturbación vectorial)*
VQA	*Variational Quantum Algorithm (algoritmo cuántico variacional)*
WCP	*Weak-Coherent-Pulse (pulso débil coherente)*
WDM	*Wavelength Division Multiplexing (multiplexado por división de longitud de onda)*

1. Introducción

La industria de las telecomunicaciones desempeña un papel fundamental en la sociedad actual [1]. El teletrabajo, la banca en línea, los pagos electrónicos, las redes móviles, los servicios de streaming, de correo electrónico, los videojuegos, las redes sociales... Son sólo algunos ejemplos de las omnipresentes aplicaciones de uso intensivo de la información en nuestro mundo hiperconectado. Por todo ello, la llamada Era de la Información exige redes de alta velocidad y baja latencia, que abarquen miles de kilómetros.

Hasta ahora, esta tarea se ha abordado admirablemente con tecnologías procedentes tanto del mundo clásico como del cuántico, pero en este último caso desde un punto de vista macroscópico. Aún no se han explotado plenamente las capacidades de los fenómenos cuánticos. Con la llegada de la Segunda Revolución Cuántica [2] esta situación experimentará un cambio fundamental. Por un lado, las soluciones actuales están mostrando síntomas de fatiga [3], dada la creciente necesidad de conexiones mejores y más rápidas con anchos de banda mayores, que impliquen a muchos más dispositivos -no solo ordenadores- como en el futuro Internet de las Cosas (IoT). Por otro lado, los avances de la mecánica cuántica (QM) han demostrado que la manipulación, generación y detección controladas de sistemas cuánticos pueden mejorar la tecnología actual proporcionando más potencia de cálculo, más seguridad y mediciones más precisas [4].

La explotación de la QM hacia la computación cuántica (QC) permite una computación más rápida, proporcionando notables aumentos de velocidad en muchos problemas complejos. Estas mejoras computacionales con ventajas cuánticas, clásicamente inaccesibles, también conocidas como supremacía cuántica, ofrecen buenas expectativas en el contexto de las telecomunicaciones, especialmente en relación con tecnologías como el estándar 5G y su evolución hacia las comunicaciones 6G. Las redes móviles 5G iniciaron la transición hacia ecosistemas inteligentes, interconectados y basados en datos en todos los sectores, aumentando el tráfico de datos móviles al permitir una comunicación y un intercambio de datos más rápidos y eficientes. Sin embargo, conseguir una red totalmente inteligente, que ofrezca todo como un servicio y proporcione a los usuarios una experiencia totalmente inmersiva con el desarrollo de la realidad aumentada y virtual, sigue siendo un objetivo exigente e inalcanzado. Con la

esperanza de superar estos retos, los investigadores ya han empezado a explorar las necesidades y posibilidades de una red 6G [5], [6], [3], [7], cuya llegada está prevista en torno a 2030. La gestión óptima de los recursos en sistemas interconectados tan complejos es un tema de creciente interés. Problemas como la descodificación en redes RAN, la fragmentación de redes, la asignación y programación de recursos de red y la mejora de los sistemas MIMO pueden abordarse con QC.

Sin embargo, el hardware de la computación cuántica aún está madurando y presenta muchas limitaciones. Algunos de los retos más destacados son reducir la decoherencia y el *dephasing* de los sistemas físicos, lograr un control óptimo de las interacciones y el entrelazamiento, así como aumentar la precisión al manipular qubits mediante secuencias de control cuántico diseñadas para implementar operaciones de puerta. Por lo tanto, las unidades de procesamiento cuántico actuales (QPU) operan en el denominado régimen cuántico de escala intermedia ruidosa (NISQ, cuyas siglas provienen de la expresión *Noisy Intermediate-Scale Quantum*). Actualmente estamos limitados por los errores en las operaciones cuánticas. Se espera que esto mejore con el creciente nivel de control para refinar la fidelidad de las puertas de las plataformas cuánticas existentes y nuevas. Una vez que las tasas de error de las puertas bajen de cierto umbral, combinadas con métodos de Corrección Cuántica de Errores (QEC), se conseguirá la tolerancia a errores [8]. Hasta la fecha, las plataformas de computación cuántica siguen en desarrollo, basadas en diferentes materializaciones físicas de los qubits (superconductores, átomos neutros de Rydberg, iones fríos, espines de semiconductores, defectos cuánticos en cristales, qubits topológicos y otros), con muchos grupos de investigación y desarrollo, corporaciones tecnológicas implicadas en todo el mundo.

Una vez que los ordenadores cuánticos tolerantes a fallos sean una realidad, la solución a problemas criptográficamente difíciles, a través de algoritmos y problemas complejos de procesamiento de señales que dependen de la Transformada Cuántica de Fourier (QFT), será posible en un tiempo computacional razonable, poniendo en peligro la seguridad de las telecomunicaciones. Ante este evento, que podría estar al alcance en décadas, es necesario realizar esfuerzos hacia una comunicación cuántica segura. Se están desarrollando nuevos criptosistemas basados en problemas matemáticos que además de no poder resolver un ordenador clásico, tampoco lo pueden hacer un ordenador cuántico; es lo que se conoce como

Criptografía Post-Cuántica (PQC). Por otro lado, la Mecánica Cuántica en sí misma puede utilizarse para proporcionar sistemas de información teóricamente segura (ITS), mediante la confianza en principios físicos bien probados y establecidos [9], en combinación con sistemas de cifrado infalibles como la "libreta de un solo uso" (OTP) u otros criptosistemas de clave simétrica, resistiendo así los ataques de los ordenadores cuánticos. En concreto, la Mecánica Cuántica permite la Distribución Cuántica de Claves (QKD), que es una tecnología madura con un considerable Nivel de Madurez Tecnológica (TRL) (Purohit, Krelina). Este es un cambio fundamental de paradigma con respecto a la criptografía clásica, donde la seguridad se induce mediante problemas matemáticamente difíciles (si nadie puede resolverlos, un adversario seguramente no podrá hacerlo).

Las nuevas soluciones criptográficas tienen que afrontar varios retos, principalmente relacionados con problemas de implementación. Aunque son tecnologías fundamentalmente diferentes, PQC y QKD están limitadas por un equilibrio entre seguridad y recursos. Aplicar PQC en el IoT no es una tarea trivial, ya que muchos de los dispositivos no tienen suficiente potencia de cálculo para soportar PQC y ser funcionales. En QKD, donde se requiere una capa física adicional con propiedades ajenas a los sistemas de comunicación clásicos, las dificultades son más rigurosas. Las señales cuánticas sufren pérdidas, pero no pueden ser amplificadas ya que la información cuántica no puede ser copiada, por lo que QKD está limitada en distancia. Desde esta perspectiva, se puede trabajar con distancias más pequeñas, como las redes metropolitanas [10], [11]. En ese caso, la aplicación de QKD para asegurar la información en la infraestructura actual es un área de investigación activa. La extensión a distancias mayores implica el uso de líneas de fibra óptica dedicadas o de comunicación Tierra-satélite, o de nuevas tecnologías que lo posibiliten, como los repetidores cuánticos. Esto posibilitará crear redes cuánticas completas que permitirían el desarrollo de un Internet Cuántico (QI), que incluiría redes aseguradas por QKD (posiblemente integrando protocolos de PQC) y ordenadores cuánticos interconectados.

Desde un punto de vista fundamental, los problemas asociados a las tecnologías cuánticas se derivan esencialmente del hecho de que los sistemas cuánticos son ultrasensibles a las perturbaciones externas. Sin embargo, la explotación de esa delicadeza de forma controlada, de modo que el sistema permanezca robusto salvo ante una perturbación deseada y cuantificable, abre enormes posibilidades en los campos del sensado y la metrología. Estas tecnologías tienen el potencial de

superar las capacidades de detección de los sensores clásicos sin la necesidad obligatoria de un nivel extremo de control de los qubits individuales, a menudo aprovechando el uso de grandes conjuntos y sistemas entrelazados para mejorar la sensibilidad incluso más allá del Límite Cuántico Estándar (SQL) para detectar pequeños efectos. En la actualidad, las tecnologías de detección y metrología cuánticas están alcanzando un TRL considerable y presentan múltiples aplicaciones en la industria de las telecomunicaciones: desde relojes atómicos y ópticos de alta precisión que permiten la sincronización de redes de alta velocidad hasta sensores cuánticos inerciales capaces de mejorar los sistemas de navegación, sensores cuánticos de RF compactos con gran rango dinámico y ancho de banda o transductores de longitud de onda que convierten una frecuencia de entrada en otra de salida de interés en las telecomunicaciones ópticas.

A continuación, llevaremos a cabo una revisión de las aplicaciones de las Tecnologías de la Información Cuántica (QIT) en el sector de las telecomunicaciones, donde los enfoques cuánticos pueden desempeñar un papel decisivo en la mejora de las soluciones tecnológicas de telecomunicaciones en un futuro cercano, complementando las soluciones clásicas existentes. Nuestro objetivo es proporcionar una visión integral del impacto de la computación cuántica, las comunicaciones cuánticas y el sensado cuántico en diversas aplicaciones de telecomunicaciones. En primer lugar, se presenta una descripción general de los algoritmos cuánticos actuales y sus implementaciones, así como posibles casos de uso en telecomunicaciones. En segundo lugar, abordamos la cuestión de la seguridad de las comunicaciones, informando sobre los fundamentos de los criptosistemas de clave pública actuales y diferentes enfoques para la criptografía post cuántica y la distribución cuántica de claves. Aquí también se presenta el posible desarrollo del internet cuántico, resaltando la necesidad de varias componentes habilitadoras y resumiendo sus principales aplicaciones. Finalmente, exponemos diferentes tecnologías de sensado y metrología cuántica que tienen un gran potencial para su integración en sistemas de telecomunicaciones de uso cotidiano.

2. Computación cuántica en el sector de telecomunicaciones

2.1 Introducción a la computación cuántica

La computación cuántica es un novedoso paradigma informático en el que se explotan las propiedades de los sistemas cuánticos, como la superposición y el entrelazamiento, para resolver problemas de clásicamente difíciles. Esta idea fue propuesta por primera vez por Benioff [12], Manin y Feynman [13] a principios de los años ochenta, y posteriormente ampliada por David Deutsch en su trabajo a mediados de los ochenta [14]. Uno de los conceptos clave que hacen posible la computación cuántica es el paralelismo que se puede obtener en estos sistemas, permitiendo a los ordenadores cuánticos realizar determinados cálculos sobre múltiples posibilidades al mismo tiempo, lo que aumenta significativamente su capacidad de procesamiento.

Los ordenadores cuánticos se encuentran actualmente en una fase denominada era NISQ [15]. Esta fase se define por una cantidad moderada de qubits, lo cual es suficiente para demostrar la supremacía cuántica sobre los ordenadores clásicos sólo en tareas específicas. La supremacía cuántica es un punto crítico que se alcanza cuando los ordenadores cuánticos pueden resolver un problema más rápido de lo que es factible para cualquier ordenador clásico. Es importante destacar que la supremacía cuántica es especialmente significativa en relación con los problemas NP [16], ya que estos problemas exhiben un aumento exponencial en su complejidad conforme aumenta el tamaño de la entrada al problema, lo cual los convierte en problemas extremadamente difíciles de resolver eficientemente en ordenadores clásicos (véase la Figura 1).

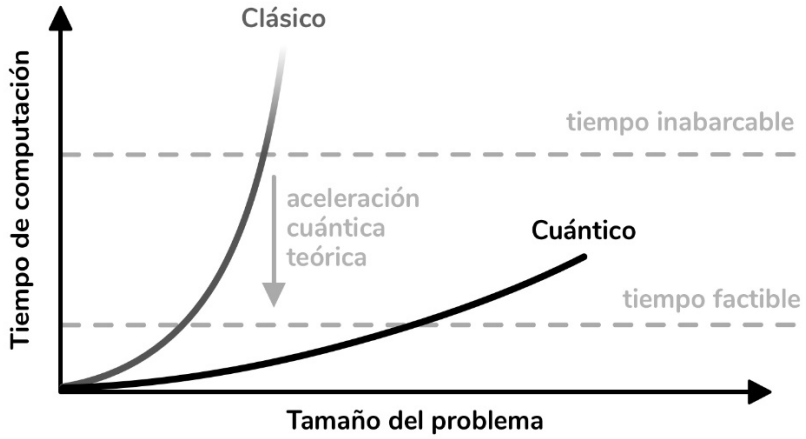


Figura 1: Se muestra el escalado temporal de problemas clásicamente difíciles. Su resolución podría volverse factible gracias a las aceleraciones exponenciales proporcionadas por la computación cuántica.

En la era NISQ, el número de operaciones que se pueden ejecutar de manera secuencial está limitado por la acumulación de errores. Además, el número de qubits de los ordenadores cuánticos actuales es insuficiente para llevar a cabo cálculos tolerantes a fallos, es decir, operaciones que implican corregir errores más rápido de lo que se crean. Con el fin de establecer sistemas tolerantes a fallos de este tipo, se debe desarrollar e implementar un conjunto de técnicas conocidas colectivamente como la corrección de errores cuánticos (QEC), que dependen de grandes cantidades de qubits interconectados para llevar a cabo operaciones de manera conjunta. Consecuentemente, lograr QEC en sistemas escalables establece un claro umbral para la computación cuántica.

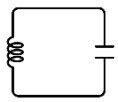
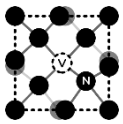
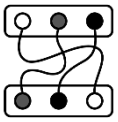
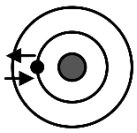
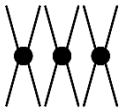
Otro obstáculo importante en la búsqueda de la supremacía cuántica es la decoherencia, un fenómeno derivado de la interacción entre los sistemas cuánticos y su entorno. Este fenómeno hace que los sistemas cuánticos pierdan sus propiedades cuánticas inherentes, lo que desestabiliza los qubits y limita la escalabilidad de los algoritmos. El tiempo necesario para ejecutar un algoritmo desempeña un papel fundamental: cuanto mayor sea el tiempo de ejecución, mayor será la probabilidad de que los qubits pierdan coherencia durante el proceso.

Si se pueden superar las limitaciones de la decoherencia y de la era NISQ, la computación cuántica puede ofrecer aceleraciones exponenciales en varios problemas NP con aplicaciones significativas, como la factorización de números con muchos dígitos (algoritmo de Shor [17]) y la búsqueda en bases de datos sin ordenar (algoritmo de Grover [18]). Además, existen métodos alternativos de resolución de

problemas más adecuados para la era NISQ, como los algoritmos cuánticos variacionales (VQA) [19] o el método de "*quantum annealing*". Estos algoritmos son aplicables a determinados problemas de optimización, siendo soluciones prometedoras para ciertos problemas como el plegamiento de proteínas y la optimización de rutas.

2.2 Hardware cuántico

El campo de la computación cuántica está avanzando constantemente y no existe una arquitectura ni un lenguaje de programación estandarizados. Entre las opciones de hardware, existen diversas propuestas, desde qubits superconductores a sistemas atómicos y de espín, chips fotónicos integrados o incluso plataformas topológicas (véase la Tabla 1). Más allá de los sistemas basados en puertas, también existen paradigmas alternativos, como la computación en estado de clúster y la computación adiabática.

Sistemas de hardware para la computación cuántica					
					
Superconductor	**Espín**	**Topológico**	**Iones atrapados**	**Átomos neutros**	**Fotónica**
Corrientes oscilantes en circuitos superconductores, con excitaciones por microondas	Qubits codificados en espín (vacantes de diamante, puntos cuánticos semiconductores, resonancia magnética nuclear...)	Cuasipartículas topológicas	Iones atrapados en campos electromagnéticos	Átomos manipulados por campos electromagnéticos (átomos de Rydberg, retículos ópticos)	Plataforma óptica que usa fotones para codificar qubits (por ejemplo, en placas de Si)
Puertas lógicas con alta velocidad y fidelidad Requiere criogenia, coherencia corta	Buena fidelidad y velocidad. Puede operar a temperatura ambiente Conseguir estados entrelazados	Tolerancia a fallos, resistencia inherente a la decoherencia Investigación en fase inicial, técnicamente	Alta fidelidad en puertas lógicas y larga coherencia Operaciones lentas y baja conectividad. El escalado es	Coherencia larga. Las operaciones de puertas lógicas son rápidas Inicialización lenta.	Velocidades de puerta muy rápidas. No requiere criogenia ni condiciones de vacío Baja fidelidad.

	supone un reto	difícil de implementar	difícil. Requiere criogenia por láser en vacío	Requiere criogenia por láser en vacío	Las puertas de dos qubits son difíciles de implementar
OQC, Google, IBM, Rigetti, Raytheon, D-WAVE, Intel, Alibaba, QuTech, IQM, Origin Quantum	Quantum Brilliance, NVision, SpinQ, Intel, Silicon Quantum Computing, Diraq, Quantum Motion,	Microsoft, Bell Labs	AQT, IonQ, Honeywell, Oxford Ionics, Quantinuum, Universal Quantum	PASQAL, ColdQuanta, QuEra, Atom Computing, Planqc	PsiQuantum, Xanadu, ORCA, Quandela QuiX

Tabla 1. Comparación de plataformas de hardware para la computación cuántica [20]–[22].

Cada plataforma de hardware ofrece algunas ventajas y desventajas. Por ejemplo, los qubits superconductores requieren temperaturas extremadamente bajas para funcionar, del orden de decenas de milikelvins, al tiempo que necesita electrónica costosa. A pesar de esto, la plataforma superconductora ha sido escalada con éxito a cientos de qubits y continúa avanzando rápidamente.

La computación cuántica basada en iones atrapados es otro enfoque notable, donde iones individuales y sus niveles energéticos son manipulados mediante campos electromagnéticos e interacciones de Coulomb. La plataforma de iones atrapados ha demostrado una coherencia excepcional de qubits y tasas de error bajas, pero su escalabilidad es actualmente limitada.

Otros enfoques incluyen la computación cuántica basada en fotónica y sistemas basados en el espín de semiconductores, que pueden funcionar a temperatura ambiente y ser implementados en chips de silicio. Sin embargo, actualmente existen dificultades para lograr un entrelazamiento robusto de los qubits. Las plataformas cuánticas basadas en redes ópticas de átomos neutros (Rydberg) también ofrecen un control preciso de los átomos individuales, aunque en estos sistemas es necesario aplicar el enfriamiento láser para minimizar eficazmente desfases no deseado causados por efectos térmicos.

Por último, los qubits topológicos son un competidor emergente que muestra un gran potencial para la creación de ordenadores cuánticos robustos y tolerantes a fallos, ya que son inherentemente resistentes a la decoherencia y a los errores. Sin embargo, el desarrollo de los qubits topológicos todavía se encuentra en sus primeras etapas de investigación, quedando múltiples obstáculos por resolver.

En resumen, el ámbito del hardware para la computación cuántica está evolucionando rápidamente, con una diversa serie de tecnologías que compiten por alcanzar la supremacía cuántica.

2.3 Descripción general de algoritmos cuánticos

Los algoritmos cuánticos son procedimientos secuenciales que controlan y manipulan el hardware cuántico para resolver problemas y realizar cálculos. Se basan en las propiedades específicas de los sistemas cuánticos para los que están diseñados, y son capaces de explotarlas de formas que les otorgan importantes aumentos de velocidad con respecto a sus homólogos clásicos.

El objetivo de esta sección es ofrecer una visión técnica general de diversos algoritmos cuánticos de potencial relevancia en el campo de las telecomunicaciones.

2.3.1 Transformada de Fourier cuántica

La transformada de Fourier cuántica (QFT) [23] es un algoritmo que revela patrones periódicos o fases ocultas en un estado de superposición cuántica. Este concepto es análogo al de la Transformada de Fourier clásica (FT), que expresa una señal o función como una combinación de varias ondas sinusoidales con diferentes frecuencias y amplitudes. Aunque son similares, la transformada de Fourier basada en la física cuántica, actúa sobre un registro cuántico (vector de estado cuántico), aprovechando las ventajas de la superposición y haciendo que el algoritmo sea más eficiente, ya que requiere menos operaciones y recursos para llevarse a cabo.

En términos prácticos, la TFC se implementa como un circuito cuántico que comprende $O(n^2)$ puertas, formado por puertas Hadamard y de cambio de fase controlado, donde "n" representa el número de qubits. Esto es exponencialmente más eficiente que la TF clásica, que requiere $O(n2^n)$ bits para realizar la misma tarea. La TFC puede implementarse en los dispositivos actuales para tamaños de entrada pequeños; sin embargo, para aplicaciones prácticas, se necesitan ordenadores cuánticos más grandes con corrección de errores.

La capacidad de discernir y cuantificar los componentes de frecuencia dentro de una superposición cuántica es la clave para la utilidad de la TFC, ya que permite a los ordenadores cuánticos desvelar patrones ocultos y fases codificadas en dichas

superposiciones, información que de otro modo permanecería oculta dentro de estos complejos estados cuánticos. Hoy en día, la QFT constituye la base de muchos algoritmos cuánticos importantes que presentan grandes aumentos de velocidad respecto a las alternativas clásicas, como el algoritmo de Shor y la Estimación Cuántica de Fase (QPE) [24].

2.3.2 Factorización de Shor

El algoritmo de Shor para la factorización de números primos de enteros grandes [17] es un algoritmo cuántico que ofrece una mejora exponencial en la velocidad de ejecución de esta tarea en comparación con los algoritmos clásicos. Aunque al hablar del "algoritmo de Shor" se entiende normalmente aquel que resuelve la factorización, cabe mencionar que es sólo una parte de tres algoritmos similares del problema del subgrupo oculto, que resuelven el problema de encontrar el periodo, el problema de la factorización y el problema del logaritmo discreto.

El algoritmo de factorización funciona creando primero un registro cuántico de qubits, cada uno de los cuales representa un bit del número entero que hay que factorizar. El registro se inicializa con una superposición de todos los estados posibles del número entero. A continuación, se utiliza un oráculo cuántico para marcar el estado correspondiente a los factores del número entero. El oráculo funciona invirtiendo la fase del estado cuántico correspondiente a los factores, mientras que las fases de los demás estados permanecen inalteradas. Después de utilizar el oráculo, se aplica una transformada de Fourier cuántica al registro. Esta operación transforma la superposición de estados en una superposición de los valores propios del entero, que son sus factores primos. Por último, se mide el estado cuántico, con cierta probabilidad de medir un estado correspondiente a un factor del número entero (esta probabilidad puede encontrarse en [17] Para un número entero de n bits, el algoritmo requiere asintóticamente $O\big((\log n)^2(\log\log n)(\log\log\log n)\big)$ pasos en un ordenador cuántico y un postprocesamiento polinómico en $\log n$ en un ordenador clásico. Esto supone un aumento significativo de la velocidad con respecto a los algoritmos clásicos más rápidos, que requieren un tiempo de $O\left(e^{1.9(\log n)^{1/3}(\log\log n)^{2/3}}\right)$ para factorizar un número entero con n bits [25].

Entre las posibles futuras aplicaciones del algoritmo de Shor, destaca la ruptura del cifrado RSA [26]. Sin embargo, sigue siendo un algoritmo teórico y aún no se ha implementado en un ordenador cuántico real, debido a los problemas físicos que

implica, como superar la decoherencia en un ordenador cuántico con un gran número de qubits, necesarios para la implementación de un algoritmo de Shor práctico. Por lo tanto, su realización será posible con la aparición de QC tolerante a fallos.

2.3.3 Algoritmo de búsqueda de Grover

El algoritmo de Grover [18] es un algoritmo cuántico diseñado para la búsqueda no estructurada de una base de datos no ordenada. Ofrece una velocidad cuadrática en comparación con métodos clásicos de búsqueda por fuerza bruta. El algoritmo consiste en crear una superposición de todos los estados posibles, los cuales representan los elementos de la base de datos.

A continuación, se utiliza un oráculo cuántico, al igual que en el algoritmo de Shor. Tras utilizar el oráculo, se aplica un operador de difusión de Grover, que aumenta la amplitud del elemento marcado y reduce las amplitudes de los demás elementos. Este operador involucra un proceso que invierte el signo de las amplitudes de todos los estados que están por debajo de la amplitud media, y deja inalteradas las amplitudes de todos los estados que están por encima de la amplitud media.

A continuación, el algoritmo repite los pasos que involucran al oráculo y al operador de difusión de Grover durante un número determinado de iteraciones (bastan unas $O(\sqrt{n})$ veces para resolver el problema, siendo n el número de elementos de la base de datos). Esta repetición aumenta la probabilidad de medir el estado cuántico de forma que se corresponda con el elemento objetivo.

Por último, se mide el estado cuántico, teniendo una alta probabilidad de encontrar el elemento buscado; lo que resulta en un enfoque más rápido en comparación con un algoritmo clásico de fuerza bruta, que tarda aproximadamente $O(n)$ evaluaciones de la función para encontrar el elemento buscado. Aunque el algoritmo de Grover no proporciona una mejora exponencial como otros algoritmos cuánticos, puede acelerar algunos problemas como el problema de colisión [27] o el problema de satisfacción de restricciones [28]. Sin embargo, aunque pueda acelerar algunos procesos, existen otras áreas como en la criptografía, el algoritmo de Grover tiene un impacto moderado en la criptografía simétrica, aunque no es el algoritmo más eficiente para esta tarea [29].

Sin embargo, para aprovechar el aumento cuadrático de velocidad que proporciona el algoritmo de Grover, es necesario utilizarlo en un gran conjunto de datos, lo que

requiere un gran número de qubits. Esta es una tarea que los futuros ordenadores cuánticos con tolerancia a errores podrían ser capaces de ejecutar, utilizando el algoritmo de búsqueda de Grover para conjuntos de datos de uso práctico [30].

2.3.4 Algoritmos variacionales

Hay una rama concreta de los algoritmos cuánticos que se adapta especialmente bien al hardware disponible en la actualidad: los circuitos cuánticos variacionales.

Estos circuitos se basan en un conjunto diferenciado de puertas lógicas cuánticas conocidas como puertas ajustables o parametrizadas -principalmente rotaciones de qubits y cambios de fase- que dependen de parámetros ajustables. Esta configurabilidad es una característica clave que distingue a los circuitos cuánticos variacionales de otros algoritmos cuánticos, ya que permite crear circuitos que pueden adaptarse a distintos problemas sin necesidad de cambiar la estructura fundamental de las puertas. Además, como los parámetros pueden ajustarse y actualizarse de forma iterativa, los propios circuitos no necesitan ser profundos o amplios para garantizar buenos resultados en comparación con otros algoritmos.

Los circuitos cuánticos variacionales, con su adaptabilidad y capacidad para trabajar eficazmente con sistemas cuánticos relativamente pequeños, son especialmente prometedores para los dispositivos NISQ a corto plazo. No exigen grandes recursos de qubits ni secuencias de operaciones complejas, lo que los hace idóneos para tareas basadas en datos, como la codificación clásica de datos y el aprendizaje automático (ML) [31].

Mapas de características

Los mapas cuánticos de características, también conocidos como *embeddings* cuánticos, son circuitos capaces de codificar datos clásicos dentro de estados cuánticos. Esto permite que los datos clásicos se conviertan en la entrada de un circuito cuántico y sean procesados por algoritmos cuánticos. Además, esto podría resultar útil para tareas de aprendizaje posteriores, traduciendo los datos a un espacio de Hilbert conveniente y facilitando el trabajo de un posible modelo de forma similar a los embeddings clásicos [32].

Algunas de estas estrategias de embedding cuántico implican circuitos cuánticos cuya composición depende directamente de los datos de entrada, como el embedding de bases (donde los datos clásicos se representan como cadenas de N bits que se asignan directamente a los estados base de un sistema cuántico de n

qubits), o el embedding de amplitud (donde 2^n puntos de datos se codifican en las amplitudes de un estado de n qubits) [33].

Mientras tanto, también existen circuitos de embedding cuántico variacional, en los que los datos se introducen en el circuito directamente a través de sus parámetros configurables. Ejemplos prácticos de este tipo de circuitos son los mapas de características Pauli, Z y ZZ de Qiskit [34]. Estos se basan en rotaciones de qubits y operaciones de entrelazamiento para alcanzar un espacio de Hilbert rico y de gran dimensión, y además ser difíciles de simular clásicamente (lo cual es un objetivo importante cuando se intenta demostrar la ventaja cuántica) [35].

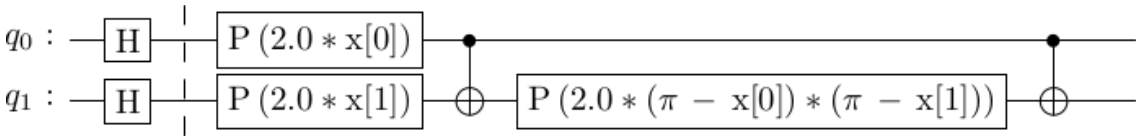


Figura 2: Ejemplo de un mapa de características variacional de 2 qubits, codificando dos valores clásicos x[0] y x[1].

Métodos de kernel

Emergiendo naturalmente del concepto de mapas de características, las funciones de kernel cuántico son capaces de calcular eficientemente la similitud entre puntos de datos en los mencionados espacios de Hilbert de alta dimensionalidad sin tener que calcular los propios -potencialmente caros - embeddings.

Al igual que los kernels clásicos de alta dimensionalidad, los kernels cuánticos operan en espacios de características en los que los conjuntos de datos con un comportamiento no lineal y difíciles de separar pueden llegar a ser linealmente separables mediante hiperplanos.

En la práctica, toman la forma de un circuito cuántico parametrizado (un mapa de características) seguido de su adjunto [32], computando a efectos prácticos los productos escalares entre los vectores de entrada. Al trabajar con datos finitos, se pueden usar para precomputar matrices de kernel completas (i.e. las similitudes entre todos los puntos del conjunto de datos), que entonces pueden ser utilizadas directamente por métodos de machine learning clásicos basados en kernels, incluyendo a las populares máquinas de soporte de vectores (SVMs) [36], regresión kernel ridge, o análisis de componentes principales con kernel.

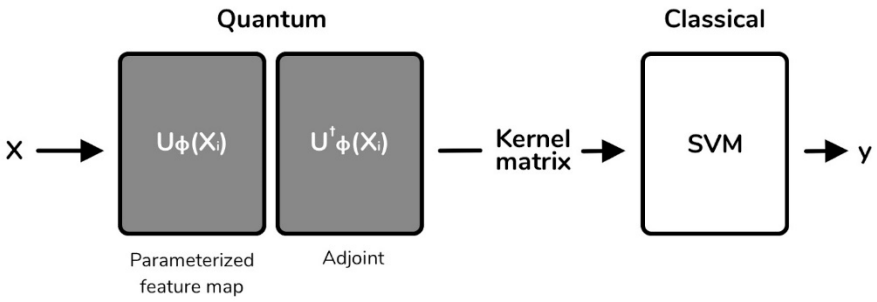


Figura 3: Arquitectura básica de kernel cuántico, donde un kernel cuántico computa una matriz de kernel para un conjunto de datos X, y un método clásico basado en kernel la usa para realizar una tarea de machine learning.

La ventaja cuántica podría alcanzarse usando kernels que explotasen espacios de Hilbert ricos y difíciles de simular, y en la aceleración del cálculo de productos escalares [32], [35].

Redes neuronales cuánticas

Aunque todavía no existe una definición estándar, una forma habitual de aplicar el concepto de redes neuronales cuánticas (QNNs) consiste en combinar un mapa cuántico de características para codificar los puntos de datos de entrada con una serie de unidades variacionales (también conocidas como ansatze) cuyos parámetros son entrenables y actúan como las capas de una red neuronal típica. Para entrenar un circuito de este tipo, se define una función de pérdida (normalmente, el valor esperado del circuito) y, a continuación, se minimiza con respecto a esos parámetros mediante procedimientos clásicos de optimización iterativa [37].

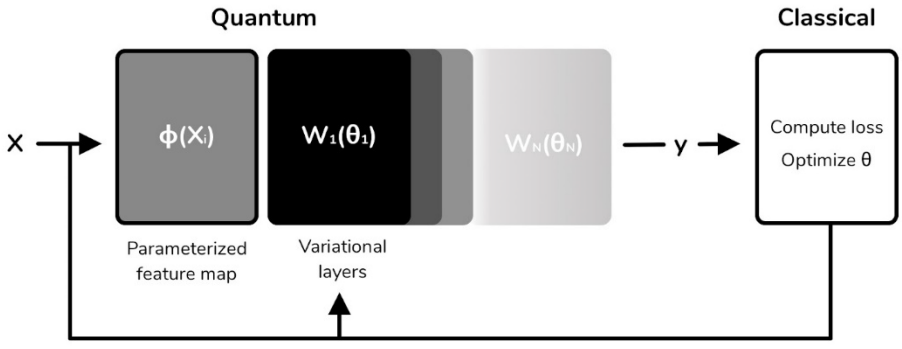


Figura 4: Arquitectura de una QNN, donde un ordenador cuántico estima las etiquetas "y" a partir de la entrada "X", y un ordenador clásico calcula la función de pérdida y ajusta los valores de θ iterativamente hasta la convergencia.

El diseño de estos circuitos es bastante flexible, y puede acomodar diferentes mapas de características y capas variacionales de diversos tipos, cantidades y tamaños.

Re-uploading de datos

Una variante eficaz es un enfoque conocido como *re-uploading* de datos, en el que las capas de entrada de datos (mapas de características) se intercalan con capas variacionales entrenables. En la práctica, esto evita el teorema de no clonación e imita la capacidad de las redes neuronales clásicas de "ver" los mismos puntos de datos más de una sola vez. Esto mejora su rendimiento y permite estrategias flexibles de entrada de datos y aprendizaje (hasta el punto de que un clasificador universal podría implementarse en un circuito cuántico de un solo qubit, a costa de la profundidad del circuito [38]).

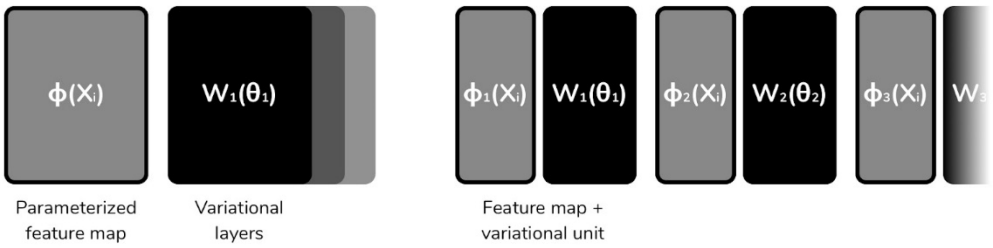


Figura 5: Comparación entre una QNN estándar (izquierda) y una que implementa re-uploading de datos.

Redes neuronales cuánticas híbridas

Es posible integrar una red neuronal cuántica entera dentro de una red neuronal clásica más grande, considerarla como una capa más, y entrenarla de la misma forma que las demás. Estas arquitecturas, conocidas como QNNs híbridas, pueden ser una forma directa de aprovechar la potencia del ML cuántico sin alejarse demasiado de las estrategias confiables del ML clásico [39].

Autoencoder cuántico

Un *autoencoder* es un tipo particular de red neuronal con forma de reloj de arena. Su primera mitad se entrena para que transforme sus entradas a un espacio latente de baja dimensionalidad, y su segunda mitad para decodificarlas y llevarlas de vuelta a su forma original con el menor error de reconstrucción posible.

Los autoencoders cuánticos siguen el mismo principio, expresando estados de N qubits usando un número de qubits menor, y reconstruyéndolos después; donde el

error de reconstrucción es una medida de la fidelidad entre los estados de entrada y salida [40].

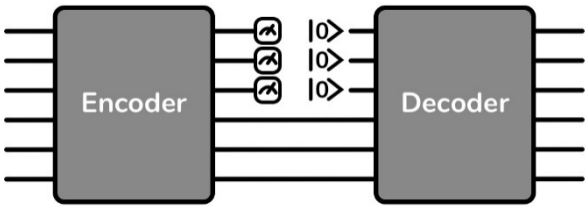


Figura 6: Forma general de un autoencoder cuántico con una dimensión de entrada de 6 qubits, y un espacio latente de 3 qubits. El codificador y el decodificador son circuitos variacionales entrenables.

Redes generativas adversariales cuánticas

Otra arquitectura deep learning popular es la red generativa adversarial (GAN). En una arquitectura GAN, un generador produce nuevas muestras de datos plausibles, y un discriminador intenta distinguirlas de muestras reales provenientes de un conjunto de datos de referencia. Ambos modelos se entrenan a la vez de forma competitiva, y el proceso suele terminar cuando el generador consigue engañar al discriminador un 50% de las veces [41]. El generador entrenado resultante es capaz de fabricar nuevas observaciones nunca antes vistas que son difíciles de distinguir de las originales.

Se han propuesto GANs cuánticas basadas en circuitos variacionales, en las que las imágenes a ser generadas/discriminadas se dividen en secciones para poder ser procesadas en hardware con un bajo número de qubits [42].

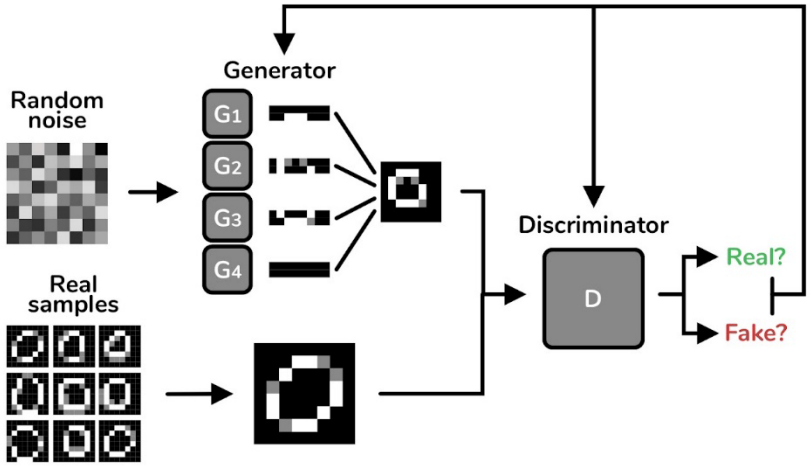


Figura 7: Arquitectura de una GAN cuántica que implementa el truco de las secciones, en la que G y D son modelos entrenables variacionales.

Una variante conocida como GAN condicional, en la que se pasa cierta información sobre el dominio a los modelos para orientar y facilitar su entrenamiento, también se ha modelado como un circuito cuántico híbrido en el trabajo de Liu et al. [43], donde el generador es cuántico y el discriminador clásico.

Aprendizaje por refuerzo cuántico

El aprendizaje por refuerzo (RL) es una rama del ML en la que se entrena a agentes que son conscientes de su entorno para que realicen tareas a base de recompensar o castigar sus comportamientos.

Algunos algoritmos RL clásicos tienen componentes que se pueden reemplazar por modelos cuánticos variacionales, como los basados en política-gradiente [44]; o los basados en aproximar una función Q [45]. Estos enfoques han demostrado su éxito en entornos de referencia sencillos [46].

QAOA

El algoritmo de optimización aproximada cuántica (QAOA) es un algoritmo variacional usado para resolver problemas de optimización combinatoria. Está basado en los principios de la evolución temporal, en la que la solución a un problema se codifica como el estado fundamental de un Hamiltoniano dependiente del tiempo y se hace evolucionar el sistema hasta que alcanza una aproximación a dicho estado fundamental. En este caso, los parámetros variacionales son los pasos temporales de la expansión del Hamiltoniano [47].

2.3.5 Algoritmos basados en annealing cuántico

El annealing cuántico es un proceso de optimización en el que un conjunto de soluciones candidatas se modelan como una superposición de estados en un sistema cuántico. El sistema, con un Hamiltoniano inicial conocido, se hace evolucionar físicamente a través de fluctuaciones cuánticas hasta que alcanza el estado fundamental, cuyo Hamiltoniano codifica la solución final al problema (de hecho, el algoritmo QAOA se puede considerar como una aproximación de este proceso usando puertas lógicas).

Aunque el principio de *annealing* se puede aplicar a cualquier tipo de Hamiltoniano, normalmente se estudia dentro de un tipo particular de sistema llamado modelo de *Ising*: una retícula periódica de espines que pueden estar en los estados +1 o -1, e interactuar favorable o desfavorablemente con sus espines vecinos.

QUBO

Las optimizaciones binarias cuadráticas sin restricciones (QUBOs) se resuelven encontrando la combinación de variables binarias (i.e. con solo dos valores posibles) que minimizan una función que codifica el problema de interés. Los problemas QUBO tienen complejidad NP clásicamente, pero como están íntimamente relacionados con el modelo de Ising (en el que los spins toman valores binarios), pueden ser resueltos de forma eficiente con annealing cuántico.

El enfoque QUBO puede aplicarse directamente a problemas combinatorios clásicos como el Vendedor Ambulante o el Corte Máximo, pero gracias a su formulación flexible puede acomodar una amplia variedad de casos de uso de diferentes campos [48].

Por ejemplo, ciertos algoritmos de machine learning como regresión lineal, máquinas de soporte de vectores y clustering k-means han sido expresados como QUBOs, permitiendo su entrenamiento en hardware de annealing cuántico [49], [50]. Otras formulaciones QUBO creativas y útiles incluyen el ensemble learning [51], selección de características [52], y redes neuronales completamente cuánticas [53].

2.4 Aplicaciones de la computación cuántica al sector de telecomunicaciones

Como se ha mencionado previamente en la introducción, la transición hacia las redes 6G exige el desarrollo de nuevas tecnologías capaces de superar las limitaciones de los sistemas de telecomunicaciones actuales.

De manera más concreta, la red 6G tiene como objetivo proporcionar una cobertura global, manejar tasas de datos más altas y aumentar la capacidad de transmisión ampliando el uso del espectro a las frecuencias de onda milimétricas (mmWave) y sub-THz. En paralelo, es necesario establecer estándares globales como los del 3GPP, de forma que se garantice la interoperabilidad y la coherencia en el despliegue de las redes 6G en todo el mundo.

Además de estos objetivos, la sostenibilidad será una cuestión clave en las redes del futuro, un aspecto que se analiza en profundidad en [54]. A medida que evolucionen las redes 6G, será crucial minimizar su impacto ambiental mediante el

desarrollo de tecnologías energéticamente eficientes y mediante el diseño de redes con menores huellas de carbono.

Para ilustrar mejor estos objetivos, Hexa-X ha identificado seis retos académicos principales como componentes integrales de su visión. Hexa-X es una iniciativa colaborativa, formada con el propósito de sentar las bases para las inversiones europeas en redes inalámbricas y definir las prioridades de investigación en 6G. Los retos clave identificados por Hexa-X para 6G abarcan los siguientes ámbitos: conectar la inteligencia, red de redes, sostenibilidad, cobertura global de servicios, experiencia extrema y mayor fiabilidad.

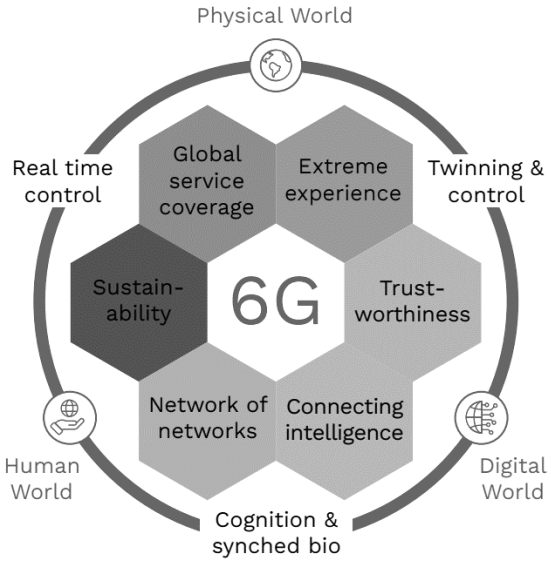


Figura 8: Retos principales identificados por Hexa-X en su visión para la red 6G [55].

Además de la integración del aprendizaje automático (ML) en las redes 6G ([56], [57]) en el segundo entregable del Paquete de Trabajo 1 (WP1) del proyecto Hexa-X, los investigadores resaltan la importancia que tienen las tecnologías cuánticas en el desarrollo de comunicaciones seguras. Sin embargo, el uso de la mecánica cuántica para el futuro 6G no se limita únicamente a las comunicaciones cuánticas. Adicionalmente, se está explorando la aplicabilidad de la computación cuántica para reducir la latencia y gestionar una asignación óptima de recursos más allá de los límites clásicos, como se menciona en [58]. Esto se ha añadido como una visión clave para el desarrollo de 6G, recogido en la documentación técnica de 5G PPP del 7 de junio de 2021 [59].

Se resumen los conceptos clave de telecomunicaciones que son relevantes para esta memoria y, a continuación, se presentan algunas aplicaciones específicas de la computación cuántica en este sector. Estas aplicaciones específicas se han

seleccionado debido a su relevancia en el marco tecnológico actual. No obstante, es innegable que a medida que las tecnologías cuánticas maduren, emergerán nuevas aplicaciones en este campo.

2.4.1 Resumen de conceptos clave en el sector de telecomunicaciones

MIMO

En los sistemas inalámbricos tradicionales, se utiliza una sola antena para la transmisión y recepción de señales. Sin embargo, los sistemas de entradas múltiples con salidas múltiples (MIMO) aprovechan las dimensiones espaciales del canal de comunicación para lograr tasas de datos más altas, mayor fiabilidad y un rendimiento general mejorado mediante el uso de un conjunto de antenas. Entre las posibles técnicas disponibles para optimizar la transmisión de datos en estos sistemas, la precodificación y decodificación se destacan como métodos ampliamente investigados. La importancia de la precodificación radica en su papel fundamental en la mejora de las transmisiones MIMO al modificar las señales antes de que viajen a través del canal de comunicación. La decodificación desempeña un papel igualmente crucial, ya que permite una recuperación precisa de la información transmitida, asegurando así una comunicación eficiente y confiable en sistemas de transmisión de datos.

Redes de Acceso de Radio

En el contexto de las redes de comunicación móvil, las Redes de Acceso de Radio (RAN) desempeñan un papel importante como la interfaz entre los dispositivos móviles y la infraestructura general de la red. Esto las convierte en un punto focal para los avances en la próxima era de la tecnología 6G [60], ya que, al ser la interfaz más cercana a los usuarios finales, las RAN influyen de manera significativa en el rendimiento y la capacidad de la red.

Una RAN consta de varias componentes esenciales de infraestructura y de funciones de red, abarcando el hardware, protocolos y los mecanismos que facilitan la comunicación inalámbrica entre dispositivos móviles. Por ejemplo, las unidades de procesamiento desempeñan un papel vital en los RAN al gestionar tareas como la modulación y demodulación de señales, corrección de errores, asignación de recursos y gestión de varios protocolos de red. A medida que las redes inalámbricas continúan evolucionando, mejorar los componentes de las RAN se vuelve cada vez

más necesario para alcanzar tasas de datos más altas, menor latencia y servicios más avanzados. Por lo tanto, la optimización y el fortalecimiento de las capacidades de las RAN representan un área clave para futuras mejoras en sistemas de comunicación inalámbrica.

Con este fin, se están proponiendo diversas estrategias para futuras redes masivas de acceso de radio, tales como el *beamforming*, superficies reflectantes inteligentes, técnicas de aprendizaje automático y estrategias para manejar señales multiplexadas [61]. Los ordenadores cuánticos también son un enfoque atractivo para mejorar los RAN, ya que proporcionan algoritmos que no escalan exponencialmente en complejidad y, por lo tanto, pueden habilitar tecnologías que dependen de la resolución de problemas de optimización computacionalmente intensivos.

Asignación de Recursos

Los recursos de la capa física de una RAN (como los intervalos de tiempo de transmisión o los canales espaciales) deben asignarse de manera rápida y equitativa a los dispositivos que los utilizan; una tarea que generalmente es realizada por un algoritmo de *scheduling* que opera en la capa MAC del modelo OSI.

Los conjuntos de reglas predefinidas que favorecen una u otra métrica pueden funcionar como algoritmos de programación válidos, como los basados en el orden de llegada "*First-Come First-Served*" y el "*Round Robin*" [62]. No obstante, la creciente demanda de latencias cada vez más bajas y la necesidad de brindar soporte a dispositivos heterogéneos resaltan la potencial utilidad de algoritmos más sofisticados y dinámicos.

NOMA: Acceso Múltiple No Ortogonal

Técnica que permite proporcionar el servicio simultáneo a múltiples usuarios mediante el uso compartido de recursos. Este concepto facilita un aumento en la capacidad normalizada del sistema, al asignar dinámicamente niveles de potencia y modulación a usuarios dentro del mismo ancho de banda de frecuencia.

2.4.2 Decodificación en redes RAN

En las RAN convencionales, los algoritmos de procesamiento lineal actuales funcionan bien para la precodificación y decodificación si hay pocos usuarios por antena, pero presentan limitaciones cuando cada antena se utiliza para emitir a un gran número de usuarios. Al emplear un método de procesamiento alternativo

basado en la máxima verosimilitud, es posible lograr mejoras significativas en el rendimiento de las antenas, especialmente en sistemas MIMO de gran envergadura. Sin embargo, este método resulta computacionalmente prohibitivo al ser ejecutado en ordenadores clásicos. Aquí la computación cuántica puede desempeñar un papel crucial, al habilitar el uso de la máxima verosimilitud mediante la aplicación de técnicas como el *quantum annealing* o el algoritmo QAOA a este problema.

En el caso del *quantum annealing*, algunos diseños ya se han implementado como pruebas de concepto en el *annealer* cuántico de D-Wave [63], [64], [65]. Estos diseños están destinados a las redes de acceso de radio centralizadas (C-RAN), donde la computación cuántica puede llevarse a cabo desde una estación central conectada a múltiples estaciones base. Los principales pasos en este proceso consisten en codificar el problema de máxima verosimilitud en una formulación QUBO y, a continuación, configurar los qubits físicos del *annealer* cuántico con las variables de la formulación cuadrática.

La codificación puede mejorarse mediante la utilización de la paralelización de subproblemas, como se muestra en [64], y la incorporación en la red de qubits es específica a la arquitectura de los *annealers* cuánticos, donde se están produciendo mejoras constantes tanto en tamaño como en conectividad. Los procesadores cuánticos actuales ya pueden competir con los métodos clásicos y, con las futuras generaciones de procesadores cuánticos, se podrán lograr mejoras sustanciales.

2.4.3 Beamforming

El *beamforming* es una técnica utilizada para enfocar y dirigir señales en haces más estrechos mediante el uso de múltiples antenas (véase figura 9). Al enfocar la señal en una dirección específica, el *beamforming* minimiza la interferencia con otras señales y aumenta el alcance efectivo de las antenas, al tiempo que mejora la eficiencia energética. La transición hacia sistemas MIMO en las redes actuales y futuras es un factor clave para la implementación del *beamforming*, ya que aumentar el número de elementos radiantes permite crear haces más enfocados, precisos y potentes. Además, la tecnología 5G se está expandiendo hacia el espectro de ondas milimétricas (*mmWave*) para aumentar la capacidad, pero las ondas milimétricas presentan algunos desafíos, como una mayor pérdida de propagación y una mayor susceptibilidad al bloqueo de señal. Debido a estos desafíos, el beamforming también es altamente relevante en este contexto,

permitiendo la implementación de la tecnología *mmWave* y aumentando la eficiencia espectral.

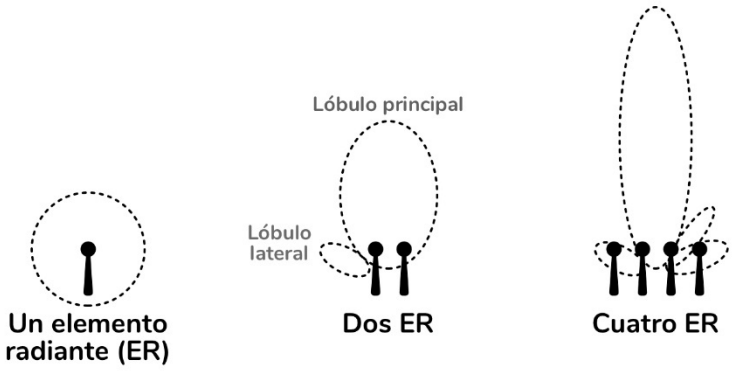


Figura 9: Ilustración de los principios de funcionamiento del beamforming. Mediante el uso de múltiples antenas, las ondas radiadas pueden enfocarse en una dirección específica. Los lóbulos laterales son patrones de radiación secundarios no deseados que se generan junto con el haz principal en el proceso de beamforming.

El *beamforming* ya se está implementando en las redes inalámbricas 5G. También será una componente clave en las futuras redes 6G, que incorporarán un control direccional adaptativo de las señales junto con el acceso a conjuntos de antenas más grandes.

El *beamforming* opera resolviendo un problema de optimización para minimizar la dispersión de la onda transmitida, controlando cada antena en la red de antenas para enfocar el haz en la dirección deseada. La complejidad del problema de optimización aumenta al considerar restricciones sobre las antenas o al tener que gestionar un mayor número de antenas, lo que rápidamente se vuelve intratable para los ordenadores clásicos. Afortunadamente, la computación cuántica es aplicable a este problema. Se han probado soluciones híbridas basadas en el *annealing* cuántico [66], donde se aplica un método de bisección para convertir el problema original de optimización en un grupo de subproblemas en formulación QUBO. Estos subproblemas deben incorporarse de manera iterativa en los qubits físicos de un annealer cuántico. El paso de incorporación actualmente representa un cuello de botella para los *annealers* cuánticos, ya que es computacionalmente costoso y se ejecuta en computadoras clásicas en la era NISQ. Debido a esto, obtener soluciones con *annealers* cuánticos es comparable en términos de tiempo al uso de algoritmos clásicos, aunque cada paso de *annealing* se resuelve más rápido de lo que sería posible de manera clásica. Por lo tanto, los avances en la resolución del problema de incorporación son un paso crucial para alcanzar una ventaja

cuántica, que a su vez proporcionará los medios para lograr importantes ahorros de tiempo y energía.

2.4.4 Superficies reflectantes inteligentes

La eficiencia energética es un factor crítico tanto en los sistemas de comunicación inalámbrica actuales como para futuros sistemas de comunicación. Reducir el consumo de energía no solo impacta directamente en los costes, sino que también es necesario para alcanzar objetivos de sostenibilidad y para mejorar el rendimiento y durabilidad de los dispositivos móviles. Se han desarrollado diversas soluciones innovadoras para abordar este problema. Una de estas propuestas es el uso de superficies reflectantes inteligentes (IRS) para controlar de manera dinámica la propagación de las señales desde el transmisor hasta el receptor, manipulando la fase y la amplitud de las señales reflejadas. De esta manera, las IRS pueden mitigar la interferencia de señales y mejorar la intensidad de las mismas, extendiendo efectivamente la cobertura de las estaciones base y reduciendo bloqueos de señal en entornos urbanos. Esto no solo optimiza el ancho de banda de frecuencia, sino que también disminuye la necesidad de infraestructura adicional, reduciendo en última instancia los costes operativos. Además, las IRS permiten dirigir las señales de manera precisa hacia los destinatarios deseados, lo que resulta en un menor consumo de energía.

La funcionalidad de una IRS depende de su capacidad para gestionar y aplicar cambios de fase para manipular las señales reflejadas. Un diseño posible para gestionar los cambios de fase es utilizar un horario o programación, que se comparte con el sistema para que los recursos de radio se asignen de manera óptima según este horario. La asignación de recursos es donde reside la complejidad computacional en este enfoque, ya que se trata de un problema de optimización combinatorio. La computación cuántica ofrece una solución para resolver este tipo de problemas mediante el uso de QAOA o la formulación QUBO, como se detalla en [67]. Además, la computación cuántica también se puede utilizar para optimizar dinámicamente el coeficiente de reflexión de una IRS [68].

De forma general, los esquemas para gestionar sistemas de IRS que son computacionalmente intensivos pueden beneficiarse de la computación cuántica para mejorar la eficiencia energética.

2.4.5 Optimización de precodificación

La Precodificación de Perturbación Vectorial (VPP) es una técnica que se utiliza para reducir la interferencia entre señales y mejorar la calidad de la transmisión, pero encontrar la matriz de precodificación óptima en VPP es computacionalmente costoso.

Existen algunas propuestas con relación al VPP [69], [70]. Sin embargo, destaca una propuesta prometedora que hace uso del *annealing* cuántico basado en Perturbación Vectorial (QAVP) [71]. Al convertir el problema del VPP en un problema QUBO y aprovechar las capacidades de las máquinas de QA, el diseño de QAVP puede encontrar eficientemente la perturbación óptima. Este enfoque permite lograr una comunicación de baja latencia y realizar ajustes finos para mitigar el ruido del hardware, lo que conduce a soluciones aún más precisas.

Investigadores han concebido escenarios en los cuales las máquinas de *annealing* cuántico (QA) se integran con centros de datos centralizados en la arquitectura de Red de Acceso Centralizado de Radio (C-RAN) [71]. Tras simular los problemas en el D-Wave 2000Q, los resultados indican que QAVP puede superar a las técnicas del estado del arte, como los algoritmos FSE y ZF para la VPP, especialmente en el enlace descendente (la ruta de transmisión desde una estación base hasta los móviles).

Además de la VPP, existen otras técnicas de precodificación que pueden mejorar los sistemas MIMO aprovechando las ventajas de la computación cuántica. En este contexto, investigadores en [72] han propuesto VQ-SVD, un enfoque innovador que combina el poder de los algoritmos variacionales cuánticos y la descomposición en valores singulares (SVD) para la precodificación en sistemas MIMO-NOMA, aprovechando el hecho de que VQA genera variables que modifican el código de precodificación. En este estudio, se utiliza IBM Qiskit como plataforma de computación cuántica para realizar la simulación. Desafortunadamente, los resultados no pueden competir con técnicas actuales de optimización para realizar la precodificación. Por tanto, aunque parece prometedor, VQ-SVD todavía se encuentra en fase de investigación.

2.4.6 Asignación óptima de recursos en sistemas MIMO sin células

Los sistemas MIMO convencionales suelen enfrentarse a dificultades para tratar con problemas de interferencia y capacidad. Estos problemas se acentúan en áreas

densamente pobladas, ya que los sistemas MIMO están restringidos a mejorar la calidad de la comunicación en enlaces o celdas específicas. Los sistemas MIMO sin celdas (Cell-Free) se consideran una solución prometedora para abordar las limitaciones de la comunicación inalámbrica en áreas densamente pobladas, ya que permiten aprovechar numerosas antenas distribuidas en un área más grande para crear una red coordinada frente a la interferencia. En otras palabras, un teléfono móvil puede ser atendido por múltiples antenas coordinadas.

Uno de los principales problemas de estos sistemas es la asignación eficiente de recursos, para lo cual los autores en [73] sugieren una solución orientada a la computación cuántica. En este estudio, los investigadores exploran las potenciales ventajas de emplear redes neuronales cuánticas (QNN) dentro del contexto de MIMO sin celdas. En particular, se utiliza un planteamiento basado en QNN para optimizar la asignación entre elementos de transmisión y usuarios en el sistema MIMO sin celdas. A pesar de que los QNN han recibido una creciente atención académica debido a las potenciales ventajas de la computación cuántica, su uso en escenarios con múltiples transmisores aún es limitada. Los autores respaldan la eficacia del algoritmo propuesto (basado en QNN) con resultados numéricos, incluyendo los recursos necesarios para su viabilidad en términos del número de qubits.

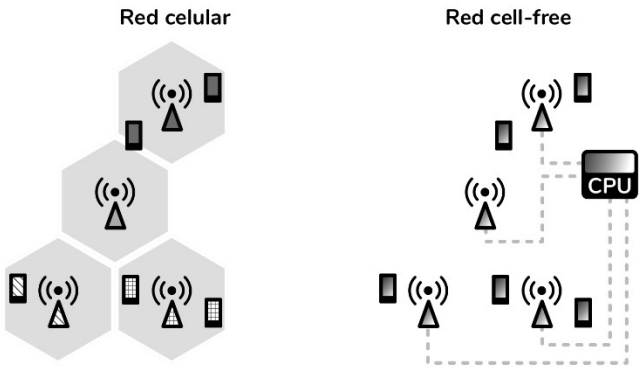


Figura 10: En una red sin celdas, los puntos de acceso están distribuidos en toda la zona y conectados a una unidad central de procesamiento. Cada equipo de usuario (UE) puede estar conectado a múltiples estaciones base.

Un estudio relacionado realizado por el mismo autor principal propone la utilización de una QNN inspirada en el Aprendizaje por Refuerzo (RL) para emparejar usuarios en un sistema NOMA. En esta red inspirada en RL, los qubits desempeñan el papel de entorno y agente, según se introduce en el trabajo de Cárdenas-López et al. [74].

Se concluye en el estudio que las QNN logran un rendimiento comparable a la de una red neuronal clásica equivalente, con una complejidad temporal inferior.

En el ámbito del RL clásico, un estudio realizado por Paz et al. [75] propone el uso de un algoritmo de política-gradiente que se basa en redes neuronales profundas para aproximar tanto la política como la recompensa acumulativa esperada [76]. En este enfoque, el agente tiene conocimiento de las características específicas de cada dispositivo de usuario y, en consecuencia, puede ajustar sus recursos. Basándose en esta estrategia, se puede implementar una versión cuántica del algoritmo sustituyendo las redes neuronales clásicas por redes neuronales cuánticas variacionales.

2.4.7 Sistemas de comunicaciones end-to-end entrenados

La capa física de un sistema de comunicaciones tiene tres componentes importantes: un transmisor que codifica y modula mensajes digitales, un canal físico ruidoso a través del cual son enviados, y un receptor que eventualmente los demodula y decodifica. El diseño de estos componentes puede hacerse por separado, y a menudo depende de modelos analíticos o del conocimiento de expertos.

Los autoencoders, un tipo específico de arquitectura de red neuronal, proveen un marco para generar estrategias de codificación y decodificación simultáneamente, aprendiendo de datos en lugar de depender de reglas fijas [77]. Este enfoque, demostradamente efectivo en su implementación clásica, puede ser llevado al dominio de las redes neuronales cuánticas [40], [78].

Las implementaciones de este enfoque podrían adoptar la forma de arquitecturas totalmente cuánticas, en las que todo el procesamiento lo realizara un circuito cuántico; o de autoencoders híbridos, en los que o bien la codificación o bien la decodificación fuera realizada por un algoritmo cuántico (realizándose la otra de forma clásica).

Una limitación a corto plazo de este enfoque sería la falta de ordenadores cuánticos portátiles, lo que en el contexto de las comunicaciones móviles implicaría que sólo la parte clásica del procedimiento de codificación/decodificación podría realizarse en dispositivos personales.

Un ejemplo notable de utilización de autoencoders cuánticos en el diseño de sistemas de radiocomunicación end-to-end es un enfoque híbrido presentado por Tabi et al., en el que se combina un codificador clásico con un decodificador cuántico para transmitir 16 símbolos diferentes en forma de señal bidimensional. Como parte de esta prueba de concepto, la señal se transmite a través de un canal de ruido gaussiano blanco aditivo con una relación señal-ruido de 15 dB [79]. Aprovechando una estrategia de doble re-uploading de datos y al menos 16 capas variacionales, la QNN utilizada como decodificador es capaz de alcanzar tasas de error comparables a los de la línea base clásica. Cuando se ejecuta en hardware cuántico real utilizando las 1000 repeticiones estándar, sus tiempos de inferencia (del orden de 100 ms) no son capaces de cumplir los estándares de los sistemas de radio en tiempo real. Sin embargo, si el autoencoder está bien entrenado y presenta una distribución de probabilidad con un pico pronunciado, el tiempo de inferencia podría reducirse enormemente computando muchas menos repeticiones.

Un trabajo relacionado por Ye et al. [80] va incluso más allá, proponiendo el uso de una GAN condicional para modelar los efectos del canal físico, convirtiendo el sistema entero en data-driven y haciendo que sea agnóstico del canal. Aunque en este trabajo sólo se discuten modelos ML clásicos, algunos de ellos podrían ser reemplazados por sus contrapartes cuánticas para beneficiarse de las posibles mejoras de rendimiento.

2.4.8 Detección de ciberataques en redes

A medida que las tecnologías e infraestructuras de comunicación evolucionan, surgen vulnerabilidades imprevistas y se desarrollan nuevas estrategias de ataques a la red. Es importante mantenerse al día e investigar técnicas de caracterización y detección de ciberataques.

Los diferentes niveles de una red de comunicación tienen sus propios tipos de amenazas y preocupaciones en materia de ciberseguridad.

En el nivel físico, donde las propiedades de las ondas desempeñan un papel primario, identificar rápidamente los esquemas de modulación puede ayudar a detectar dispositivos no autorizados, puntos de acceso fraudulentos, o intentos de escucha e interferencia [81].

Esta tarea, realizada originalmente mediante la extracción cuidadosa de características y la selección manual de límites de decisión, se ha resuelto

exitosamente utilizando técnicas de deep learning en las que una gran red convolucional es capaz de distinguir entre 24 esquemas de modulación [82]. Aunque esta arquitectura específica depende de un gran número de parámetros entrenables y el hardware NISQ es limitado en ese sentido, podría evaluarse una versión cuántica más pequeña de esta estrategia basada en las propuestas actuales de redes neuronales convolucionales cuánticas [83].

En protocolos de nivel superior, los flujos de paquetes de tráfico de red son el principal objeto de interés.

Existen dos enfoques principales para la detección de las amenazas del tráfico de red: la clasificación (en la que los modelos aprenden los patrones que caracterizan a cada tipo de ataque) y la detección de anomalías (en la que lo que se aprende es el comportamiento normal de la red, y cualquier cosa que se salga de su distribución se señala como una amenaza potencial).

En el primer caso, se han hecho múltiples propuestas que aprovechan una variedad de clasificadores cuánticos. Un trabajo de Payares et al. aplica SVMs cuánticas, NN híbridas cuántico-clásicas y un conjunto de dos clasificadores cuánticos para clasificar paquetes de red como benignos o como parte de un ataque distribuido de denegación de servicio (DDoS) [84]. Un estudio relacionado realizado por Kalinin et al. aborda la clasificación de 6 tipos diferentes de ataques utilizando tanto una SVM cuántica como una red neuronal convolucional cuántica [85].

La segunda técnica, la detección de anomalías, también se ha explorado desde el ámbito del ML cuántico. Stein et al. investigan el uso de máquinas cuánticas de Boltzmann (entrenadas mediante annealing cuántico) para modelar la distribución normal de un conjunto de datos de juguete en el contexto de la detección de fraudes. Otros enfoques incluyen el quantum variational rewinding, útil para series temporales [86], y la estimación cuántica de la densidad de amplitud [87].

2.5 Roadmap a largo plazo

Mientras que es posible simular sistemas cuánticos pequeños en ordenadores clásicos, es una tarea que se vuelve exponencialmente cara a medida que aumenta el número de qubits. Por ejemplo, para representar en una memoria clásica el estado de un sistema de n qubits, podría hacer falta guardar hasta 2n amplitudes,

que al ser números complejos con un cierto grado de precisión flotante podrían ocupar decenas de bytes cada una. Aunque este consumo depende de las características del circuito cuántico a simular (el grado de entrelazamiento, sus posibles particiones...) y existen aproximaciones para reducirlo, es fácil ver cómo a partir de cierto tamaño la simulación se vuelve inviable y emerge la ventaja de los dispositivos realmente cuánticos.

Como ya se ha mencionado, los ordenadores cuánticos actuales (dispositivos NISQ) se enfrentan a importantes retos prácticos, como tiempos de decoherencia cortos, errores en puertas y mediciones, y un número restringido de qubits. Como resultado, los practicantes cuánticos se ven constreñidos a la hora de implementar algoritmos, teniendo que limitar tanto su profundidad (el número de puertas) como su anchura (el número de qubits) [88].

Para exprimir todo el potencial que pueden ofrecer los ordenadores cuánticos, hay que encontrar la manera de escalar el número de qubits sin perder coherencia, y en este punto la corrección de errores cuánticos y la tolerancia a fallos se convierten en factores significativos. QEC es un conjunto de técnicas usadas para asegurar la tolerancia a fallos de los qubits a nivel algorítmico (aunque hay algunas propuestas que se enfrentan a la tolerancia a fallos a nivel de arquitectura [89]). QEC protege la información lógica a base de medir información síndrome sobre los errores cíclicamente, permitiendo que los ordenadores cuánticos sigan operando de forma fiable y precisa incluso en presencia de errores y ruido. Un problema es que la corrección de errores requiere qubits auxiliares, por lo que la anchura de los circuitos aumenta, lo que hace que esta técnica no sea apropiada para dispositivos NISQ [89]. Además, el teorema de no clonación de la física cuántica impide la creación de un duplicado separado e idéntico de cualquier estado cuántico arbitrario y desconocido [90]. La idea de QEC es utilizar múltiples qubits físicos imperfectos para representar un único qubit lógico perfecto y realizar mediciones para la detección de errores. Sin embargo, estas mediciones deben diseñarse cuidadosamente de forma que no revelen ninguna información sobre los valores de los qubits, siendo su único propósito indicar si se ha producido un error y en qué posición se ha producido.

En la era NISQ basada en puertas lógicas, en la que el objetivo es optimizar el número de qubits en uso, obtener resultados prácticos y evitar errores, el concepto de algoritmos cuánticos variacionales es, quizás, el desarrollo más influyente. Su

corta profundidad y bucle de optimización híbrido los hace particularmente adecuados para el hardware NISQ.

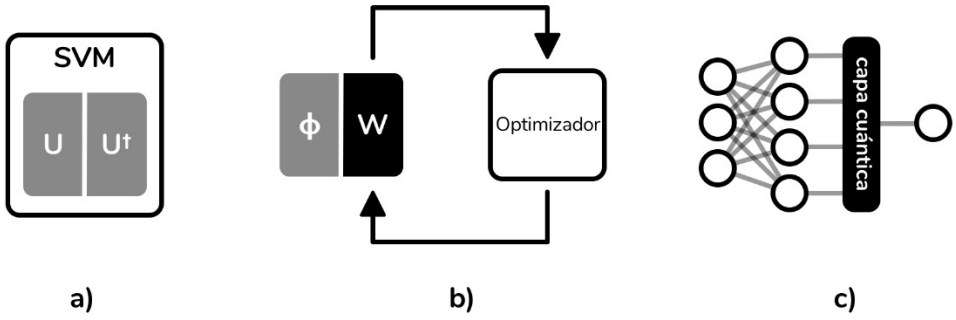


Figura 11: Enfoques híbridos a la computación cuántica. a) Un método clásico basado en kernel utilizando un kernel cuántico internamente, b) El bucle de entrenamiento típico de una QNN, incluyendo un circuito cuántico variacional y un optimizador clásico, c) Una capa cuántica integrada en una arquitectura de red neuronal clásica.

Estos enfoques híbridos son excelentes para resolver problemas sin necesidad de usar circuitos cuánticos de gran anchura. Son la base del machine learning cuántico, y se están aplicando a otros casos específicos como la adaptación de algoritmo cuánticos "caros" al hardware limitado actual.

Otras técnicas consideradas como híbridas utilizan computación clásica para post-procesar o combinar las salidas de circuitos cuánticos. Un caso particular es la reciente propuesta de una versión distribuida del algoritmo de Shor [91], que es uno de los más relevantes gracias a su capacidad para factorizar números grandes exponencialmente más rápido que los algoritmos clásicos (lo cual supone una amenaza para algunos métodos de encriptación clásicos). El inconveniente principal de este algoritmo es el gran número de qubits que requiere su implementación; sin embargo, en esta versión distribuida se consigue factorizar un entero de n bits reduciendo la anchura de los circuitos en $^{n}/_{2}$ qubits (comparado con la implementación original).

Concluyendo, el desarrollo de algoritmos cuánticos basados en puertas presenta dos vertientes principales. Por un lado, la explotación de algoritmos puramente cuánticos potentes requiere el desarrollo de ordenadores con corrección de errores y tolerancia a fallos, una tarea compleja que requiere superar limitaciones relacionadas con la propia naturaleza cuántica del hardware. Por otro lado, el camino práctico hacia la supremacía cuántica dentro de las limitaciones actuales ha favorecido la aparición de prometedores enfoques híbridos. Como se menciona en [92], mientras que existen algoritmos difíciles de catalogar como híbridos o no-

híbridos, existe una tendencia que se puede observar en algoritmos como el de Grover o en la Estimación de Amplitudes Cuántica (QAE): los algoritmos no-híbridos a menudo evolucionan y dan lugar a variantes híbridas más ricas y potentes.

3. Comunicaciones cuánticas

3.1 Introducción

Las Comunicaciones cuánticas consisten en comunicarse a través de un canal cuántico, en oposición a un canal clásico. Por canal cuántico entendemos el proceso de codificar y enviar información mediante sistemas cuánticos. La aplicación más consolidada, aparte de resultados sorprendentes como la teleportación cuántica y la codificación superdensa, es la seguridad [93]. En concreto, la Distribución de Clave Cuántica o QKD. QKD es capaz de, a través de un canal cuántico, proporcionar clave entre dos usuarios de forma totalmente segura desde el punto de vista de la Teoría de la Información (*information-theoretic secure*, o ITS). La necesidad de esta clase de técnicas estriba en que, como hemos visto, los ordenadores cuánticos son capaces de romper de forma eficiente los sistemas actuales de clave pública. La criptografía clásica convencional proporciona una solución alternativa a la QKD, la cual, por su potencial (relativamente) fácil integración en la infraestructura de comunicaciones actual es merecedora de atención. En concreto, esta solución se conoce como Criptografía Post-Cuántica (PQC). Se trata de una forma de criptografía clásica que es sin embargo segura tanto ante ataques de ordenadores clásicos como ante ataques de ordenadores cuánticos *(quantum-safe*), en oposición a la QKD, que podría considerarse una forma de criptografía potenciada por la física cuántica. Antes de proceder, revisaremos primero conceptos básicos de criptografía de clave pública, para determinar en términos más concretos la problemática asociada a la computación cuántica y dotarnos de una base y lenguaje comunes para criptografía.

3.1.1 Criptografía de clave pública

La criptografía es una técnica matemática mediante la cual esconder la información de un mensaje, llamado texto plano (o *plaintext*). Esto se realiza de forma algorítmica, mezclando el texto plano con una secuencia llamada clave, en un proceso denominado encriptación. Como resultado, se obtiene un texto cifrado que es sólo legible para el destinatario legítimo, el cuál está en posesión de una clave para descifrarlo.

En criptografía simétrica, la clave de cifrado es la misma que se usa para descifrar. Eso significa que cualquiera que tenga acceso a la clave puede descifrar mensajes.

Es por tanto crucial mantener la clave en secreto, permaneciendo esta sólo disponible para los usuarios legítimos (generalmente llamados Alice y Bob). El proceso de hacer que la clave pueda ser compartida entre dichos usuarios y así puedan comunicarse con seguridad se conoce como distribución de clave. Como ejemplo importante, a la par que simple, de criptografía simétrica, y que se asocia comúnmente con QKD [94] es el cifrado Vernam, al que también se le puede denominar *one-time-pad* (OTP) o libreta de un solo uso. Este sistema consiste en expresar el texto plano en forma de una secuencia de unos y ceros y mezclarla, mediante la operación XOR, con una secuencia aleatoria de la misma longitud, la clave. El resultado es otra secuencia también aleatoria, de la que un adversario podría deducir cualquier mensaje imaginable con idéntica probabilidad. Con lo cual, sin la clave, el contenido del mensaje no puede obtenerse. El sistema OTP es totalmente seguro (ITS) [95]–[97]. Como desventaja, se requiere que la clave sea de la misma longitud del mensaje. Asimismo, la clave solo puede usarse una vez por mensaje ("un solo uso"), por lo cual debe ser continuamente refrescada. Si la misma clave se usase para cifrar dos mensajes distintos, un espía podría obtener información sobre los mensajes intercambiados simplemente aplicando la operación XOR sobre ambos textos cifrados.

En criptografía asimétrica, por el contrario, la clave usada para cifrar es distinta a la usada para descifrar [98]. Los sistemas de cifrado asimétricos hacen uso de dos claves: una clave pública, que se puede enviar a través de un canal inseguro (es decir, cualquiera puede tener acceso a él); y una clave privada, que debe mantenerse en el más estricto secreto. El sistema, en términos simples, funciona de la siguiente manera: supongamos que Alice y a Bob quieren intercambiar mensajes secretos. Para conseguirlo Alice calcula una clave pública a partir de su clave privada y se la manda a Bob. Éste usa dicha clave pública para cifrar su mensaje y mandárselo a Alice, quien lo descifra con su clave privada. Es crucial pues que la clave privada se mantenga como tal. Una tercera persona con acceso a ella podría interceptar el mensaje y descifrarlo sin que Alice y Bob se diesen cuenta. Si bien originalmente la criptografía de clave pública buscaba evitar el problema de la distribución de clave [99] no siempre la criptografía asimétrica compite con la simétrica. De hecho, ciertos sistemas simétricos son más rápidos (y por lo tanto, más prácticos) que los sistemas asimétricos. Por lo tanto, los asimétricos se usan para dotar de clave a dichos sistemas, como ocurre en el protocolo TLS (*Transport Layer-Security*) [100].

La criptografía asimétrica también provee de medios para autentificar, como es el caso de las firmas digitales. En un sistema de firma digital [101], [102] la clave privada se usa para firmar y la clave pública para verificar la firma. Podría verse como la forma opuesta del encriptado asimétrico que hemos comentado. De hecho, la clave privada encripta y la pública desencripta. Concretamente, Alice usa su clave privada para operar en un mensaje dado, generando una firma. Esa firma está unida al mensaje y es introducida por Bob en un algoritmo de verificación, juntamente con la clave pública de Alice. El algoritmo devuelve o bien una respuesta positiva o negativa, dependiendo de si la clave pública concuerda con la firma o no. La clave pública descifra lo que la privada cifró. Si Bob no es capaz de hacerlo, esto significa dos cosas: o bien alguien manipuló la firma o bien el mensaje fue firmado por alguien que no es Alice pero quiere hacerse pasar por Alice. En cualquier caso, la firma se rechazaría al no poder verificarse con certeza la identidad del firmante.

Tanto para cifrar mensajes como para firmas digitales, la identidad de Alice (o Bob) debe estar debidamente asociada a su clave pública [99]. Esto se realiza mediante una entidad de certificación de confianza (CA), como puede ser por ejemplo una institución gubernamental, que autentifica a los usuarios (la primera vez, sino no sería práctico) mediante métodos más tradicionales (en persona y mediante DNI, por ejemplo), y proveyendo a la comunidad con la seguridad de que cierta clave pública pertenece a una persona y solo una (en este caso, Alice). Cuando hay muchos usuarios, esto no es sencillo. Además, existen varias CAs. El esfuerzo coordinado en esta materia se denomina infraestructura de clave pública (PKI) [103].

Existe una relación entre las claves pública y privada. Obtener la clave privada a partir de la pública, no obstante, se conjetura como imposible para cualquier ordenador clásico concebible. La intratabilidad de ciertos problemas, como son la factorización de números primos grandes y el problema del logaritmo discreto (y en particular, el problema del logaritmo discreto sobre curvas elípticas), es la base de la seguridad de la criptografía de clave pública actual. De acuerdo con esto, podemos limitarnos al importante sistema RSA [104], [98], basado en el primero de estos problemas, y el sistema DSA (*digital signature algorithm*) [101], basado en el segundo de ellos (variante de *ElGamal*, relacionado con el esquema Diffie-Hellman).

3.1.2 Necesidad de las comunicaciones cuánticas

La existencia de computadores cuánticos que puedan implementar el agoritmo de Shor pone en entredicho la dificultad de los problemas matemáticos mencionados

arriba. Mientras que la criptografía asimétrica se volvería vulnerable, la simétrica, que se vería afectada por el algoritmo de Grover aún podría ser capaz de resistir, siempre y cuando se incremente el tamaño de las claves empleadas [105]. Es más, las claves usadas por sistemas como AES (advanced encryption standard) podrían ser generadas mediante QKD [106]. Es pues imperativo, no sólo para la seguridad de las futuras comunicaciones en un mundo de computadores cuánticos funcionales, sino también para proteger la información (tal como secretos de estado) que está hoy en día cifrada con métodos vulnerables. Se necesita pues de soluciones *quantum-resistant* para una seguridad apropiada. Dos alternativas, PQC y QKD, existen para contrarrestar la llamada "amenaza cuántica". PQC es una aproximación más tradicional a dicha amenaza, y no involucra comunicaciones cuánticas per se. En cualquier caso, se admite la existencia de ordenadores cuánticos como hipótesis de trabajo. La otra alternativa, QKD, es un ejemplo concreto de comunicaciones cuánticas: los *qubits*, codificando información digital (en bits), se envían a través de una conexión cuántica y se recuperan al final de forma que Alice y Bob compartan una clave.

3.2 Criptografía Post-Cuántica

En esencia, la tarea de la PQC consiste en desarrollar nuevos estándares criptográficos que un ordenador cuántico no pueda romper con eficiencia. En términos más específicos, el concepto de nivel de seguridad captura (parcialmente) esta noción de dificultad. Un nivel de seguridad de n bits implica que un atacante precisa de 2^n operaciones para romperlo. Mientras que los sistemas actuales de criptografía de clave pública pueden romperse totalmente mediante ordenadores cuánticos con tolerancia a errores, algunos sistemas simétricos solo ven su nivel de seguridad reducido, esto es, para romperlos, menos operaciones son necesarias, y por eso los tamaños de clave han de incrementarse [100].

La metodología para el diseño e implementación de algoritmos PQC requiere del cumplimiento de dos condiciones simultáneas: la primera, que los algoritmos sean seguros, en el sentido de que deben, una y otra vez, resistir los ataques que se lancen contra ellos (estudio exhaustivo); y la segunda, que sean eficientes. Por tanto, el desarrollo de algoritmos PQC es la búsqueda de los sistemas irrompibles por ordenadores cuánticos y clásicos que sean a su vez más rápidos [105].

Existen varias propuestas para candidatos de algoritmos PQC. En concreto, aquí nos centraremos en aquellos que hayan sido seleccionados por el National Institute of Standards of Technology (NIST) para ser estandarizados próximamente (no analizaremos aquellos que hayan pasado a la cuarta ronda de análisis). El NIST, el cual es bien conocido en este ámbito, ha estado detrás de la estandarización de algoritmos de uso muy extendido como son AES y SHA-3 (*secure hash algorithm*). El NIST trabaja de forma muy cercana con empresas del sector tecnológico, esperándose un mercado para la PQC que crezca significativamente a corto-medio plazo [107].

3.4.1 Aproximaciones a PQC

Entre los problemas que se conjetura que ni un computador clásico ni uno cuántico son capaces de resolver encontramos:

1. **Problemas basados en retículos** (*lattices*). Simplificando, un retículo es como un espacio vectorial en el que los coeficientes de las combinaciones lineales son números enteros [99]. Un ejemplo muy conocido de un problema difícil en retículos es el problema del vector más corto (SVP, shortest-vector problem) [108]. La criptografía basada en retículos es muy segura y versátil, si bien requiere de más volumen de análisis y testeo [109].

2. **Problemas basados en funciones *hash*.** Una función *hash* (o función resumen) es una función *one-way* que transforma un input muy largo en uno muy corto, de forma que es muy complicado obtener el input (la preimagen) a partir del output, o encontrar otro input tal que de como resultado el mismo output (colisión) [99]. Como ventaja, los sistemas *hash* son muy rápidos, pero sólo son útiles para construir firmas digitales, a la par que requieren claves notablemente grandes que deben ser transmitidas con el mensaje [109].

3. **Problemas basados en polinomios de múltiples variables**. Las claves son pequeñas, lo cual es positivo, y los esquemas basados en ellos son rápidos. No obstante, carecen de la suficiente seguridad [109].

4. **Problemas basados en *isogenias***, asociados con la dificultad de encontrar *isogenias*, esto es, aplicaciones entre curvas elípticas que

satisfagan una serie de condiciones [110].. Como desventaja, no pueden ser usados para desarrollar firmas digitales.

5. **Problemas basados en códigos**, relacionados con la dificultad de ciertos problemas en teoría de corrección de errores. Aunque están bien estudiados y son seguros, requieren de un uso notable de memoria [109].

3.4.2 Algoritmos PQC candidatos a ser estandarizados por el NIST

En julio de 2022, el NIST anuncio cuatro candidatos para ser estandarizados, y que se recogen en la tabla de abajo, mientras otros avanzaron a la cuarta ronda de estudio [111]. De las aproximaciones mencionadas arriba, tres de los candidatos están basados en retículos, mientras que el cuarto está basado en hash. Uno de ellos es un algoritmo de clave pública y establecimiento de clave, mientras que los otros tres son sistemas de firma digital. Los borradores de los estándares de los algoritmos CRYSTALS-KYBER, CRYSTALS-Dilithium y SPHINCS+ se anunciaron en agosto de 2023, mientras que el borrador del estándar para FALCON se espera que sea anunciado próximamente [112].

Algoritmos PQC sujetos a estandarización por el NIST		
ALGORITMO	TIPO	BASADO EN
CRYSTALS-KYBER	Encriptación de clave pública y establecimiento de clave	Retículo
CRYSTALS-DILITHIUM	Firma digital	Retículo
SPHINCS+	Firma digital	Retículo
FALCON	Firma digital	Hash

Tabla 2. Resumen de los algoritmos PQC candidatos a ser estandarizados por el NIST.

Además de esto, la IRTF (Internet Research Task Force, parte de la Internet Engineering Task Force), está desarrollando estándares basados en hash para firmas digitales [113]. Asimismo, dentro del proyecto Open Quantum Safe, se está investigando en la materia [114], entre otras iniciativas. Por otro lado, compañías bien conocidas como Cloudflare, Cisco o Samsung están contribuyendo a migrar a sistemas PQC [115].

3.4.3 Ventajas y desventajas generales de la PQC

En general, la PQC hace uso de la infraestructura ya disponible [116]. Por tanto, no requiere de hardware altamente especializado, al contrario que QKD. Por tanto, su mayor ventaja es su comparativamente reducido coste de implementación. Microsoft y Amazon ya están desplegando versiones post-cuánticas del protocolo TLS [117], [118]. Por otro lado, los algoritmos de PQC deben ser lo suficientemente prácticos, como ya adelantamos. Esto es especialmente crítico teniendo en cuenta el surgimiento IoT, dado su uso en hardware embebido [109]. La velocidad es un problema [100]: ha de hacerse un compromiso entre seguridad y la tasa de transmisión de datos. En general, existe una tensión entre seguridad y recursos [119].

Dicho esto, la PQC sufre del mismo problema que la criptografía de clave pública actual, en el sentido de que no existe garantía de que los problemas que hoy consideramos como computacionalmente difíciles lo sigan siendo [120], de la misma manera que nadie pensaba, cuando RSA fue inventado, en la existencia de computadores cuánticos capaces de romperlo.

3.3 Distribución de Clave Cuántica

La distribución de clave cuántica o QKD basa su seguridad en las leyes de la mecánica cuántica, la cual es una teoría física bien establecida [9]. En particular, hace uso de propiedades como la imposibilidad de clonar estados cuánticos arbitrarios o el entrelazamiento cuántico. Como tal, la QKD puede ser considerada como una primitiva criptográfica basada en la mecánica cuántica [121]. Por otro lado, hemos visto que sistemas como OTP son seguros en sentido ITS. La pregunta que la QKD resuelve es pues como proporcionar clave para su uso en OTP de forma que podamos asegurar que nadie, excepto Alice y Bob, tiene acceso a dicha clave, sin tener que usar, por ejemplo, mensajeros en los que se deba confiar, no solo por practicidad, sino en un sentido más absoluto de seguridad.

La solución es, en esencia, el uso de mensajeros cuánticos. En particular, dadas las propiedades de estos mensajeros, cualquier intento de espiar puede ser detectado, y después reducido, lo que contrasta con los métodos clásicos, en los que un adversario puede obtener información confidencial sin ser detectado. Dicho esto, la QKD necesita de algún método clásico de autentificación, para asegurar que efectivamente Alice es Alice y Bob es Bob, y evitar así ataques del tipo *man-in-the-*

middle. Para autentificar la conexión, Alice y Bob deben tener acceso a una clave previa, si bien está puede ser muy pequeña y eficientemente distribuida de forma clásica. Lo que la QKD haría sería hacer crecer esa clave para cifrar comunicaciones de forma continua e indefinida [122].

La QKD es una de las tecnologías de comunicaciones cuánticas más desarrolladas. En lo que sigue, haremos mención de experimentos y ensayos de campo, incluso sobre redes de fibras ya desplegadas y en uso. Por el momento, como casos de uso populares (y hasta pioneros), puede tenerse en cuenta el uso de QKD en las elecciones suizas en 2007 [123] o durante el mundial de fútbol de 2010 en Sudáfrica [124].

3.3.1 Aspectos básicos de QKD

En un escenario típico de QKD, Alice y Bob tienen acceso simultáneo a dos canales fundamentalmente distintos. En primer lugar, un canal cuántico, a través del cual se envían y detectan pulsos fotónicos. Un canal cuántico puede ser un cable de fibra óptica, o una conexión entre un satélite y una base terrestre. En segundo lugar, un canal clásico, satisfaciendo dos propiedades: que ha de estar autentificado y que no puede ser interferido [125]. La primera propiedad ya la hemos visto: significa que Alice sabe con certeza que nadie se está haciendo pasar por Bob y viceversa. La segunda propiedad garantiza la integridad de los mensajes clásicos. Ambos canales son públicos, es decir, cualquiera puede monitorizarlos. Si alguien (un adversario comúnmente llamado Eve) pretendiese monitorizar el canal cuántico, sería detectado con una cierta probabilidad. Esta es la característica principal de la QKD.

En cuanto a los detalles de este canal, la información se codifica en estados cuánticos. La información clásica en términos de bits se traslada a bits cuánticos, o qubits. Los detalles sobre que grado de libertad del fotón usar, como la luz se propaga por el canal y que transformaciones se le aplican, o cuál es el esquema de detección y análisis, definen un protocolo QKD y su implementación. Esto es, en general, en que forma particular se intercambian las señales clásicas y que post-procesado clásico se aplica a continuación.

El protocolo QKD más conocido (y pionero) es el protocolo BB84 [126]. Consiste en que Alice prepara un cierto estado, codificado en una señal a nivel de un solo fotón, y luego lo envía a Bob, quien lo mide. El protocolo se dice entonces que es de tipo preparar y medir (*prepare & measure*). La comunicación se realiza de punto a punto,

ya que los dos usuarios se comunican directamente, sin ningún tipo de nodo intermedio.

En BB84, Alice prepara un qubit en una de las dos siguientes bases mutuamente no-sesgadas: la base Z o rectilínea o la base X o diagonal. Esto quiere decir que los estados de cada una son no-ortogonales con respecto a los de la otra y el resultado (probabilidad) de medir en una base cuando los estados se preparan en la otra es el mismo cualquiera que sea el estado.

Base Z: $|0\rangle$, $|1\rangle$,
Base X: $|+\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$, $|-\rangle = 2^{-1/2}(|0\rangle - |1\rangle)$.

Alice escoge su base de forma aleatoria, mediante un generador cuántico de números aleatorios (QRNG). El estado se manda a Bob a través del canal cuántico. Bob selecciona su base de medida también aleatoriamente, usando su propio QRNG. Aquellas veces en las que la base resulte ser la misma (50%), Bob obtendrá el mismo bit que Alice codificó, y compartirán pues un bit de clave idéntico. Para determinar esto, Alice y Bob se comunican mediante el canal clásico. Los eventos para los cuales la base seleccionada fue distinta se descartan. Este proceso de post-procesado básico de la clave en crudo se denomina *sifting*. El proceso de QKD actúa como un cifrado de flujo [99], mediante el cual la clave se genera a medida que los pulsos son medidos y procesados. La clave se genera a una cierta tasa, llamada tasa de clave.

Consideremos ahora como Eve altera este proceso. Eve no sabe en que base emite Alice. No puede copiar estados a la perfección, y tampoco puede dividir la señal como se haría de forma clásica. Por tanto, debe intentar adivinar que estados envía Alice. Como posible estrategia (ataque de tipo *intercept-resend*) Eve puede medir el estado, obtener cierta medida, y mandar a Bob un estado de acuerdo con dicha medida (el estado al que colapse). Sin embargo, los estados de las diferentes bases son no-ortogonales, con lo cual Eve no puede estar segura. Alice puede enviar $2^{-1/2}(|0\rangle + |1\rangle)$ y Eve medir $|1\rangle$, con lo que preparará y mandará a Bob justamente $|1\rangle$. Ahora, si Bob mide en la base X, dado que $|1\rangle$ puede escribirse como $|+\rangle - |-\rangle$ (excepto normalización), Bob puede obtener $|-\rangle$ en su medida, lo que sería imposible si nadie hubiese modificado el estado enviado por Alice. Si ambos comparan ciertos eventos, descubrirán esta clase de incompatibilidades. Estos errores ocurrirán con una cierta tasa (QBER, *quantum bit error rate*). Si esta tasa se encuentra por encima de un cierto valor, Eve podrá ser descubierta.

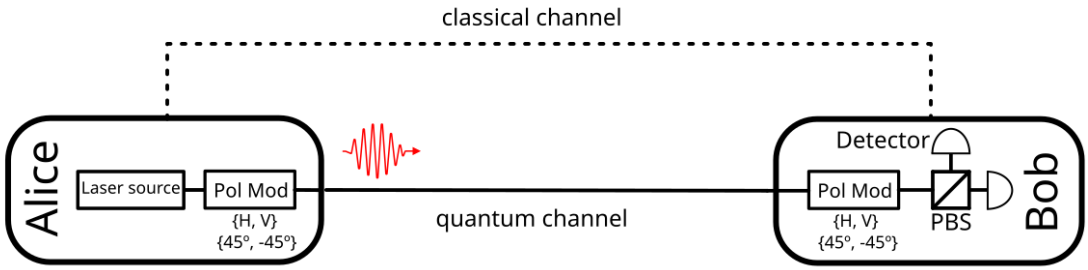


Figura 12: Descripción esquemática del protocolo BB84 en polarización. Alice prepara un estado en alguna de las bases Z y X y se lo envía a Bob, quien escoge aleatoriamente en que base medir (en este caso, de forma activa), y envía el resultado a un PBS con detectores en ambos outputs. Un canal clásico permite a Alice y Bob reconciliar las bases de medida, chequear posibles errores etc. y seleccionar así los bits válidos que formarán la clave final.

3.3.2 Codificaciones

Al describir el protocolo BB84, hemos permanecido generales y usado la notación computacional. En una implementación real, uno debe codificar la información en un grado de libertad concreto del fotón. Quizás el más popular sea la polarización. En ese caso, dado un eje de referencia, los estados de la base Z van a representar polarización vertical y horizontal, respectivamente, y los estados de la base X van a representar polarización a 45 y -45 grados, respectivamente. Consecuentemente, componentes ópticos como láminas de onda y divisores de haz por polarización serán necesarios.

La codificación en polarización es sólo un ejemplo. Se refiere a un grado de libertad específico y que además es discreto. Tendríamos así protocolos QKD basados en variable discreta (DV-QKD). Las dimensiones no están limitadas a dos; estados de dimensión $d<2$ arbitraria (llamados *qudits*) pueden ser empleados, con ciertos beneficios asociados, como una mayor cantidad de información enviada por fotón y una mayor protección ante la influencia de Eve [127]. Estas codificaciones de alta dimensión se adaptan particularmente bien cuando se hace uso de fibras *multicore* o *few-mode* para transmitir la señal cuántica [128], [129].

Otra posibilidad atractiva es usar estados en espacios de Hilbert de dimensión infinita, lo cual correspondería a grados de libertad continuos, o variable continua (CV-QKD, por tanto). En este caso, la información no viaja codificada a nivel de un solo fotón, sino que lo hace en las cuadraturas del campo eléctrico cuantizado [130]. Hardware por lo pronto poco eficiente como detectores a nivel monofotón estándar no supondría un problema usando variable continua [131]. Por otro lado, el proceso de comunicación sería más parecido a su contrapartida clásica, y contaminación por

coexistencia con señales clásicas supondría un problema menos grave. A pesar de este potencial (de hecho idealmente los protocolos CV-QKD podrían superar a los DV-QKD [132]), las implementaciones prácticas tienen varias dificultades asociadas. Por ejemplo, la atenuación se vuelve más crítica y el post-procesado es significativamente más complejo [93].

La decisión de que codificación escoger debe atender a las necesidades experimentales. Si se usa la polarización del fotón y se transmiten estos a través de fibra, uno puede encontrarse con fluctuaciones en la polarización que introduzcan ruido en la comunicación. Esto es así ya que la mayoría de las fibras reales presentan cierta birrefringencia no deseada y que es suficiente como para producir acoplamiento entre los modos de polarización. Esta variará de forma aleatoria. Como consecuencia, un estado que originalmente esté polarizado horizontalmente puede adquirir una componente verticalmente polarizada, dando lugar a errores en la clave final.

Una forma de atajar este problema podría ser usar una fibra especial, del tipo *polarization-mantaining*, bien monitorizar de forma activa las fluctuaciones en polarización y corregirlas [133], [134], o bien restaurar el estado original mediante técnicas pasivas de autocompensación [135], útiles incluso en codificaciones de fase relativa [136], done las señales monofotón interfieren al final de la línea. Otra opción podría ser emplear otra codificación, como la codificación por tiempo de llegada del fotón *(time-bin)*. En particular, este sistema es robusto ante variaciones de polarización, y, si bien está limitado por el *dead-time* de los detectores, sigue siendo una de las elecciones habituales para QKD basada en fibra. La polarización, sin embargo, se conserva razonablemente bien si los fotonces se propagan por espacio libre, con lo cual esta codifciación es popular en links QKD base terrestre-satélite. Por otro lado, estos canales introducen otros desafíos relacionados con la propagación de pulsos de luz a través de la atmósfera [137]–[140].

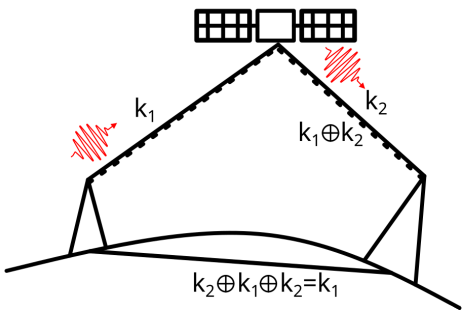


Figura 13: Principio de QKD Tierra-satélite con un nodo confiable (el satélite). Entre la base de la izquierda y el satélite se establece una clave privada k_1 mediante QKD. Entre la base de la derecha y el satélite se establece una clave k_2 mediante QKD. Después, el satélite envía a esta la clave k_1, cifrada mediante la clave k_2. Posteriormente, dicha base realiza la operación XOR entre dicho texto cifrado y la clave k_2, obteniendo la clave k_1. El resultado es que ambas bases terrestres comparten ahora la clave k_1.

3.3.3 Corrección de errores y amplificación de privacidad

Las fluctuaciones no deseadas en la polarización son un ejemplo de ruido en el canal cuántico. Ese ruido reduce la tasa de clave, ya que parte de los bits intercambiados han de sacrificarse para corregir errores. Dos clases de errores afectan al canal cuántico: los provenientes del propio hardware, y los que genera Eve. Desde un punto de vista criptográfico estricto, en el que se asume que Eve posee recursos ilimitados, todos los errores se entienden como causados por Eve [141]. Por encima de un cierto umbral de error, el protocolo QKD debe abortarse. Por debajo de dicho limite, una cierta tasa de clave secreta puede ser extraída (*distilled*).

Para conseguir esto, la información que Eve posee debe limitarse. En general, la tasa de clave secreta será igual a la información compartida entre Alice y Bob menos la información entre Eve y Alice (reconciliación directa) o Eve y Bob (reconciliación inversa). Si es Bob el que deduce el bit de Alice, necesitando que Alice le ayude mediante envío de información por el canal clásico, entonces estamos ante un escenario de reconciliación directa. Si ocurre lo opuesto, estaríamos ante el caso de reconciliación inversa. El aspecto principal aquí es que Eve se beneficia de la comunicación clásica entre Alice y Bob. Debe notarse que esta noción de reconciliación directa o inversa es de fundamental importancia en CV-QKD [132].

Los análisis rigurosos de seguridad en QKD [142]–[144] tienen por objetivo calcular de forma precisa un límite inferior de la tasa de clave secreta que puede extraerse a partir de la clave después del *sifting*. Esto requiere sacrificar bits en dos procedimientos separados: la corrección de errores y amplificación de privacidad. El primer paso implica minimizar errores en la clave, de modo que Alice y Bob compartan los mismos valores binarios. El segundo paso reduce a una cantidad despreciable la información que Eve pudiera tener sobre la clave privada. En un escenario en el que se intercambiasen infinitas señales a nivel de un solo fotón (*asymptotic scenario, single-photon limit*), y la corrección de errores se aplicase con una eficiencia f (se han de sacrificar más bits que en el caso ideal para corregir errores), la tasa de clave estará dada por (límite inferior)

$$R \geq 1 - H(e_b) - H(e_p),$$

Donde e_b es la tasa de errores en términos de bits y e_p es la tasa de errores de fase. $H(x)$, por su parte, es la función de entropía binaria de Shannon, definida como $H(x) = -x\,log_2\,x - (1-x)\,log_2(1-x)$.

En general, la tasa de clave tendrá expresiones más complicadas, involucrando parámetros que pueden medirse directamente en un experimento QKD y otros que deben ser estimados a partir de los datos experimentales. Por otro lado, si el número de señales intercambiadas es finito, como sucede en la realidad, efectos de clave finita (*finite key size effects*) deben de ser tenidos en cuenta [132].

3.3.4 Problemas de implementación

Los análisis de seguridad más estrictos no limitan de alguna manera el tipo de ataque que Eve pudiera lanzar. El más general de ellos se conoce como ataque coherente [132], y asume que Eve puede hacer interaccionar qubits auxiliares (*ancillas*) a los qubits de Alice y Bob para después realizar una medida conjunta del sistema, incluso después de que Alice y Bob se hayan comunicado a través del canal clásico, guardando mientras tanto los estados en una memoria cuántica. Ataques menos potentes son el ataque colectivo, en el que Eve mide los estados auxiliares, pero no los estados señal y el ataque individual, en el que Eve monitoriza las señales cuánticas una a una.

Los ataques prácticos, que se benefician de las imperfecciones del hardware (*side channel attacks*) escapan a esta clasificación teórica, abriendo la puerta al hackeo de sistemas QKD [145]. Es de crucial importancia modelizar adecuadamente los sistemas físicos que implementan las distintas tareas de QKD, para así poder evitar dichas vulnerabilidades [146]. Como alternativa, pueden construirse protocolos QKD que, por diseño, sean seguros ante imperfecciones en los componentes. Por ejemplo, los protocolos de tipo MDI-QKD [147] (*measurement-device independent*), esto es, protocolos independientes del sistema de medida, son inmunes por definición contra cualquier intento de hackear los sistemas de detección. De hecho, esto último se deja en manos de un nodo no confiable e intermedio entre Alice y Bob (normalmente llamado Charlie). Como desventaja, la tasa de clave es baja, ya que se requiere de una medida de estados de Bell (que Charlie realiza) y, por tanto, de coincidencias de dos fotones. Por su parte, los protocolos independientes de los dispositivos (DI-QKD, *device-independent*) van un paso más allá [148]. En DI-QKD no sólo los detectores pueden tratarse como una caja negra, sin necesidad de confiar en lo que pasa dentro, a parte del funcionamiento en si en relación con el protocolo,

sino que todos los componentes pueden tratarse de la misma manera, analizando exclusivamente si su estadística input-ouput viola una desigualdad de Bell. A pesar de esfuerzos recientes [149], DI-QKD sigue siendo muy difícil de realizar a nivel práctico, ya que requiere que se viole, por un amplio margen, una desigualdad de Bell -sin cabos sueltos (*loophole free Bell test*), y al mismo tiempo generar una QBER lo suficientemente baja para QKD.

Un ejemplo particular que explota imperfecciones en el hardware es el llamado ataque *Photon-Number Spliting* (PNS) [150]. Las fuentes láser reales que se usan en protocolos QKD emiten pulsos que, si bien se atenúan casi hasta nivel de un solo fotón (*weak coherent pulses*, WCP), contienen de hecho, y con una cierta probabilidad (de acuerdo con la distribución de Poisson), más de un fotón. Esto implica que, por cada pulso, existen varias copias del mismo estado cuántico, codificando varias veces el mismo bit. Dada esta circunstancia, considerando por ejemplo BB84, Eve podría dividir esta señal multi-fotónica y reenviar un fotón solo a Bob, mientras ella se queda con el resto, resultando indetectable. Si guarda ese estado en una memoria cuántica, puede esperar a que Alice y Bob se comuniquen para realizar su medida y obtener información total sobre la clave. Por tanto, Alice y Bob se ven forzados a considerar solo las señales monofotón como seguras, lo cual reduce extensiblemente la tasa de clave. Existe, no obstante, una solución, consistente en emitir estados señuelo (*decoy states*) [151] -otra posibilidad es el uso del protocolo SARG04 [152], que puede considerarse esencialmente como una variante de BB84 en la parte de post-procesado clásico, y que implementa hardware comercial de IDQuantique.

Ya que el ataque PNS es común a muchos protocolos, normalmente todas las implementaciones experimentales usan estados señuelo, sistemas comerciales de QKD inclusive (Toshiba). El método de estados señuelo consiste en lanzar pulsos con varias intensidades escogidas de forma aleatoria, y por tanto desconocidas para Eve. Esto permite a Alice y a Bob detectar a Eve, mediante la estimación de ciertos parámetros del canal cuántico. Asimismo, la estimación de dichos parámetros (y otros) mejora considerablemente. Como resultado, Alice y Bob pueden usar pulsos débiles sin generar *backdoors* y en términos de clave el comportamiento es casi como si se empleasen fuentes monofotón ideales [153].

3.3.5 Capacidad del canal cuántico

Los protocolos QKD se diseñan para que la tasa de clave sea óptima en presencia de ruido y pérdidas en el canal. Hacer *benchmarking* del rendimiento de los protocolos se vuelve una cuestión básica. Puede establecerse un límite fundamental para la obtención de tasa de clave en el escenario ideal en el que no haya ruido, pero si pérdidas. Para protocolos QKD punto a punto (Alice a Bob, sin nodo intermedio), el límite PLOB [154] establece el escalado de la tasa de clave en relación a las pérdidas, sin ningún tipo de repetidor cuántico. La tasa de clave viene dada por $-\log_2(1-\eta)$, donde η es la transmisividad del canal (atenuación, dependiente de la longitud del canal, y otras pérdidas *fijas* por otros componentes, eficiencia de los detectores <1 etc.). Para valores de $\eta << 1$, la tasa de clave escala linealmente con η.

Twin-Field QKD

La realización práctica de repetidores cuánticos es crucial para extender el alcance en distancia de la QKD. En particular, es también un ingrediente básico para una red cuántica [155]. Por el momento, es una tecnología no lo suficientemente madura. Esto limita las conexiones QKD punto a punto, de acuerdo con el límite PLOB. Sin embargo, existe una manera de solventar esto. Mediante una estructura semejante a MDI, con un nodo intermedio, el protocolo Twin-Field [156] es capaz de sobrepasar el límite PLOB, obteniendo un rendimiento semejante a un link QKD con un repetidor, mediante el uso de interferencia a nivel de un solo fotón entre campos ópticos ("gemelos") emitidos por Alice y Bob, y que se encuentran en dicho nodo intermedio no confiable. En particular, TF-QKD consigue un escalado con la transmisividad igual a $\sqrt{\eta}$ para $\eta << 1$. La versión *sending-not-sending* (SNS) de este protocolo [157] es mucho más robusta ante desalineamientos de fase ente los campos ópticos, llegándose a alcanzar distancias de 1000 km en fibra [158].

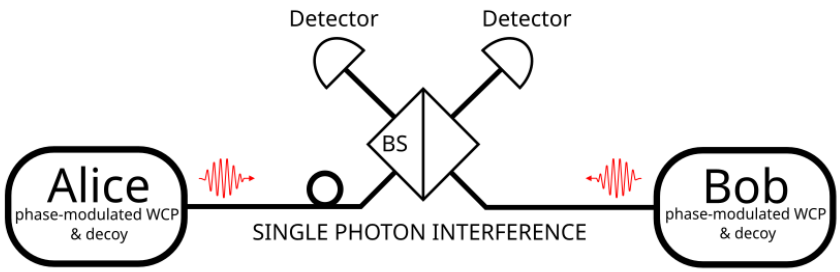


Figura 14: Esquema básico de TF-QKD. Alice y Bob envían campos ópticos débiles y decoy states a un nodo central que los combina realizando interferencia de un solo fotón.

3.3.6 Hardware para QKD y comparación entre protocolos

Hay muchas maneras de implementar un protocolo QKD. Existe una diversidad, beneficiosa (=versatilidad) de realizaciones o protocolos. Éstos pueden ser clasificados en categorías amplias, dependiendo si son del tipo punto a punto, como BB84, o si necesitan nodos intermedios, como MDI y Twin Field. Pueden estar basados en variable continua o discreta. Pueden implementarse en fibra o espacio libre... A la hora de considerar implementaciones prácticas, ya sea en un entorno controlado, como un laboratorio o un ensayo de campo, se hacen necesarias adaptaciones ad-hoc no consideradas a nivel teórico que a veces convierten dichas implementaciones en protocolos que podrían considerarse hasta nuevos.

Existen muchos elementos en común: en particular, la necesidad de mejores fuentes de un solo fotón y detectores de un solo fotón. Los estados *decoy* resuelven razonablemente bien el primer aspecto, con lo cual se usan pulsos tenues de forma corriente. Para el caso de los detectores, APDs estándar pueden reemplazarse por SNSPDs (*superconducting nanowire single-photon detectors)* en aplicaciones a nivel estado-del-arte, dada su mejorada eficiencia y baja tasa de *dark count* ("cuentas oscuras") [158]–[160]. Para el caso de las fibras, dependiendo de la implementación, se emplean mejores o peores fibras. En ensayos de campo las fibras suelen ser peores: más pérdidas y más ruido [161], [162]. En laboratorios, se suelen emplear fibras enrolladas de más calidad, y que presentan pérdidas bajísimas (*ULL, ultra-low loss*) [158], [163]. Debe tenerse en cuenta el requisito de operar a la longitud de onda adecuada. En fibra, la banda convencional de telecomunicaciones (C-band, alrededor de 1550 nm) es la longitud de onda a escoger. El hardware que acompañe a la fibra debe ser consecuente con esto: por ejemplo, la eficiencia de los APDs de un tipo u otro depende de la longitud de onda [141].

Se muestra a continuación una tabla con varios protocolos relevantes, algunos de ellos ya mencionados en el cuerpo principal del texto, acompañados de una descripción resumida y una exposición breve de ventajas y desventajas. La lista no es exhaustiva, dada la diversidad de protocolos. Revisiones especializadas en la materia tal como [145] dan cuenta del desarrollo de la QKD. El objetivo general de cualquier protocolo es, en general, alcanzar mayores distancias con tasas de clave más grandes (lo cual depende también de la tasa de repetición de la fuente) sin comprometer su seguridad.

Comparativa entre protocolos QKD

Protocolo	Descripción breve	Ventajas	Desventajas
BB84 [126]	Alice prepara un estado en la base Z o en la base X. Lo envía a Bob, que mide y obtiene el bit de Alice. Transmisión punto a punto del tipo preparar y medir.	Muy estudiado (pionero), tanto a nivel teórico (demostración formal de su seguridad) como experimentalmente.	Vulnerable a ataques prácticos -*side channel attacks*.
MDI [147]	Alice y Bob envían qubits a un nodo intermedio no confiable que realiza una medición de estados de Bell.	Inmune a cualquier ataque en la detección.	Baja tasa de clave, ya que requiere coincidencia bifotón.
TWIN-FIELD [156]	Alice y Bob envían pulsos ópticos que interfieren en un nodo intermedio no confiable. Se trata de una interferencia monofotónica, no de una medición por coincidencia, como en MDI, lo que mejora el rendimiento.	Supera el límite PLOB, como si hubiese un repetidor presente.	Sensible a desalineamientos de fase, que tiene que ser muy estable. Esto se mitiga en la versión SNS.
SARG04 [164], [10]	Similar a BB84 pero con un post-procesado mejorado.	Más robusto ante ataques PNS sin necesidad de estados señuelo. Presente en hardware comercial de QKD – IDQuantique Cerberis.	No mejora a BB84 en tasa de clave.
GG02 [165]	Quadraturas p y q, distribuidas aleatoriamente de forma gaussiana. Alice envia estados coherentes con $\alpha = q + ip$ y Bob mide	Ventajas asociadas a variable continua	Desventajas asociadas a variable continua
COW [10], [166], [167]	Codificación en función del tiempo de llegada de pares de pulsos, uno vacío y otro no vacío, según las secuencias: *no vacío y vacío: bit 0*; *vacío y no vacío: bit 1*.	Implementación simple; poco ruido por diseño. Se usa en algunos componentes comerciales.	No es apropiado para QKD de larga distancia (*long-haul*)
DPS [168], [169]	Información codificada como fase diferencial entre pulsos; descodificación por interferencia (normalmente interferometría Mach-Zehnder).	La versión *round-robin* (RRDPS) es robusta ante QBER gigantes (50%) y efectos de clave finita	Requiere estabilidad de fase.
B92 [132]	Comparte parecido con BB84, pero solo emplea dos estados ortogonales y no cuatro.	Simplicidad de implementación.	Peor rendimiento que BB84
E91 [170]	Basada en entrelazamiento cuántico. Una estación central emite estados entrelazados que Alice y Bob comparten. Éstos comprueban si Eve está interfiriendo realizando un test de Bell. La idea es que Eve no	Seguridad garantizada por un test de Bell. La fuente es robusta al estar entrelazada (monogamia del entrelazamiento).	Dificultad asociada con realizar un test de Bell sin cabos sueltos. Requiere una fuente de estados entrelazados.

	puede imitar las correlaciones contenidas en el estado entrelazado (en forma de violación de desigualdad de Bell) y al mismo tiempo obtener información sobre él.		
BBM92 [171]	Basado en entrelazamiento. Similar a E91 pero sin test de Bell. Un nodo intermedio entre Alice y Bob emite estados de Bell que luego son medidos por Alice y Bob en sus respectivos laboratorios, con las bases habituales de BB84.	Seguridad gracias a la monogamia del entrelazamiento.	Requiere una fuente de estados entrelazados.
DI [172], [149]	Inspirado por E91. La legitimidad de los dispositivos se garantiza a través de tests de Bell.	Independencia de los dispositivos físicos.	Muy difícil de realizar a nivel práctico. Requiere un test de Bell sin cabos sueltos.

Tabla 3. Principales protocolos QKD, junto con su principio básico de funcionamiento, ventajas y desventajas.

Recopilación de esfuerzos experimentales y prácticos en QKD						
PROTO -COLO	**MAX DISTANC E (km)**	**CODIFICA -CIÓN**	**FUENTE**	**CANAL**	**DETECCIÓN**	**LAB O CAMPO, AÑO**
BB84 [173]	275	*Time-bin* (eficiente con tres estados)	WCP (un *decoy*)	Fibra ULL	SNSPD	Lab, 2023
BB84 [160]	96	*Time-bin* (eficiente con tres estados)	WCP (un *decoy*)	Fibra submarina, atenuación sobre 0.2 dB/km	InGaAs/InP SPAD *(single-photon avalanche diode)* a medida (estado-del-arte)	Campo, 2023
BB84 [174]	421	*Time-bin* (eficiente con tres estados)	WCP (un *decoy*)	Monomodo ULL 0.17 dB/km de Corning	SNSPD 40-60% pol. dependiente manufacturado a tal efecto	Lab, 2018
BB84 [175]	Estudio práctico de un canal turbulento (teoría y simulación).	Polarización	WCP (dos *decoy*)	Canal atmosférico turbulento simulado	SPAD	Simulación incluyendo condiciones atmosféricas complicadas (aerosoles, residuos volcánicos), 2021

BB84 [176]	1200	Polarización	WCP (un *decoy*)	22 dB pérdidas; espacio libre Tierra-satélite (Micius)	SPD	Campo, 2017
BB84 [177]	7600 (nodos confiables)	Polarización	WCP	Tierra-satélite	-	Campo, 2018
BB84 [178]	144	Polarización	WCP (un *decoy*)	35 dB espacio libre entre La Palma y Tenerife	APD	Lab, 2007
MDI [179]	404	*Time-bin* fase	WCP (cuatro *decoys*)	ULL 0.16 dB/km & fibra estándar 0.19 dB/km	SNSPD	Lab, 2020
MDI [180]	200	*Time-bin* fase	WCP (dos *decoys*)	Aprox. 0.2 dB/km en fibra	SNSPD	Lab, 2014
MDI [181]	19.2	Polarización (probablemente)	WCP (tres *decoys*)	Canal atmosférico urbano	SNSPD	Lab, 2020
TF [158]	1000 (aprox.)	SNS	WCP (dos *decoys*)	ULL 0.157 dB/km	SNSPD	Lab, 2023
TF [163]	658	SNS	WCP (tres *decoys*)	ULL 0.16 dB/km	SNSPD	Lab, 2021
TF [159]	511 (431 larga dist. + 81 enrollada)	SNS	WCP	0.17 dB/km	SNSPD	Campo (red metropolitana), 2021
TF [161]	428	SNS	WCP (dos *decoys*)	0.185 dB/km fibra enterrada	SNSPD	Campo, 2021
GG02 [162]	30-50	Gaussiana	WCP	Fibra comercial 0.416 dB/km (30.02 km) y 0.233 dB/km (49.85 km)	Homodina con fotodetectores	Campo, 2019
COW [182]	307	Codificación COW	WCP	ULL 0.17 dB/km	InGaAs	Lab, 2014
DPS [183]	336	Fase diferencial	WCP	Alrededor de 0.2 dB/km	SNSPD	Lab, 2014

DPS [184]	200	Fase diferencial	WCP	Alrededor de 0.2 dB/km	SNSPD	Lab, 2007
RRDPS [185]	50 (a 28% QBER)	Fase diferencial	WCP	Fibra	Detector monofotón basado en silicio	Lab, 2015

Tabla 4. Recopilación de resultados experimentales y realizaciones prácticas de protocolos QKD.

Atención especial merecen implementación QKD orientadas a redes cuánticas. Daremos cuenta de ellas en la sección dedicada al Internet Cuántico. En esos casos, el énfasis no es tanto en el alcance (distancia), como en la interoperabilidad con redes ya desplegadas, por ejemplo, a nivel metropolitano.

QKD comercial

Varias empresas han empezado ya a abrir mercado para soluciones QKD. Podemos destacar por lo menos tres: Toshiba, ID Quantique y MagiQ. En el caso de Toshiba, por un lado, cabe señalar las contribuciones fundamentales a QKD desde un punto de vista teórico, a través del Toshiba Cambridge Research Laboratory (TF-QKD se desenvolvió allí). Por otro lado, la empresa comercializa hardware para QKD. En particular, módulos QKD capaces de alcanzar distancias de 70 – 120 km con tasas de clave de 40 – 300 kb/s con pérdidas de 10 dB, implementando BB84 con codificación de fase y estados *decoy* [186]. Por su parte, IDQuantique, quien se relaciona de forma cercana con la empresa coreana SK Telecom, surgió de la experiencia del grupo de QKD de la Universidad de Ginebra. Comercializa una serie de productos QKD, además de QRNGs y sensores cuánticos. Su producto Cerberis XG [187] implementa el protocolo COW y, de acuerdo con las especificaciones, puede alcanzar 60 km a 0.2 dB/km de atenuación en fibra. Finalmente, MagiQ es otra empresa relevante en el panorama, comercializando productos como MagiQ QPN [188]. Es importante señalar que se han lanzado con éxito ataques de hacking cuántico (en el ámbito académico) contra algunos productos fabricados por IDQuantique (Clavis2) y MagiQ (QPN 5505) [189].

3. 4 Internet Cuántico

Todos los esfuerzos realizados en el ámbito de las comunicaciones cuánticas deberían converger en una red (de redes) completa que podría denominarse Internet Cuántico (QI, *quantum internet*) [190]. El objetivo del QI será explotar

recursos y funcionalidades cuánticos que no pueden lograrse con el Internet clásico [191]. Se espera que dicha red interconecte varios nodos con enlaces protegidos por QKD. Hay que tener en cuenta que la QKD, la *distribución de entrelazamiento* y la *teleportación cuántica* (y por tanto, los repetidores) necesitan de comunicación clásica entre nodos para funcionar. Es de esperar, pues, que el QI se complemente con su homólogo clásico, el Internet actual.

No sólo entrará en juego la QKD, sino también otros protocolos de comunicación cuántica. En particular, la teleportación cuántica [192] es un elemento básico para las futuras redes cuánticas [193]. Detrás de ella, es esencial que los nodos compartan pares entrelazados (pares EPR) de alta fidelidad (por lo que QEC es imprescindible, también aquí) o *ebits* [155]. Esto se denomina distribución de entrelazamiento y es un requisito básico para el QI. De hecho, el entrelazamiento puede (y ha de) considerarse como un recurso.

Construir un QI va a ser una tarea compleja, con muchos pasos (previos) necesarios para la plena funcionalidad de las futuras aplicaciones. Se necesita un salto tecnológico en muchos aspectos, precisándose de tecnologías clave denominadas tecnologías facilitadora o habilitantes.

3.4.1 Tecnologías facilitadoras

Repetidores cuánticos

Debido a la fragilidad de los estados cuánticos (decoherencia) y a la imposibilidad de copiarlos, la señal no puede amplificarse como se hace habitualmente de forma clásica. Hemos visto límites fundamentales en la capacidad del canal cuántico en el contexto de la QKD; éstos afectan también a la distribución del entrelazamiento. Para una red cuántica de larga distancia, con canales cuánticos de gran alcance, los repetidores cuánticos constituyen una tecnología facilitadora.

Uno de los protocolos para repetir una señal cuántica más conocidos, basado en la distribución de entrelazamiento, es el protocolo DCLZ [194]. Éste utiliza sistemas atómicos para almacenar información cuántica, es decir, memorias cuánticas. El intercambio de entrelazamiento consiste en dividir el canal cuántico de longitud d en un número n de pequeños segmentos elementales de longitud $\frac{d}{2^n}$ entre los que se distribuye un par entrelazado [195]. Mediante técnicas de teleportación cuántica, el entrelazamiento se transfiere y $\frac{d}{2^{n-1}}$ nodos quedan así dotados de pares EPR. Repitiendo el proceso n-1 veces se consigue el entrelazamiento a lo largo de una

distancia d, sin que los nodos finales hayan estado nunca en contacto. El entrelazamiento no se distribuye instantáneamente. En su lugar, un par de nodos puede tener que esperar a otro hasta que complete su entrelazamiento, lo que hace necesaria la existencia de memorias cuánticas [196].

La técnica de repetición del protocolo DCLZ es característica de los repetidores cuánticos de primera generación (1G) [155]. Actualmente, existen tres generaciones de repetidores cuánticos [155], [197]. Difieren en las tecnologías internas que requieren y la forma en la que operan. Dos clases de errores influyen en los repetidores cuánticos: errores debidos a la pérdida de un fotón (errores de pérdida) y errores que tienen lugar cuando se manipulan los estados cuánticos (errores operativos). Cada generación de repetidores corrige estos errores de forma distinta. 1G aplica corrección de errores probabilística tanto para los errores de pérdida como operativos *(heralded entanglement generation & heralded entanglement purification)*. 2G emplea corrección de errores probabilística para errores de pérdida, pero determinista para errores operativos (QEC). Finalmente, los repetidores 3G hacen uso de QEC para ambos tipos de errores. Cada generación mejora a la anterior, pero a expensas de implementaciones más complejas [107], en una forma semejante a los ordenadores cuánticos.

Memorias cuánticas

Las memorias cuánticas realizan las tareas de almacenamiento (y recuperación) de estados cuánticos. En el contexto de las comunicaciones cuánticas, hacen la función de interfaz entre fotones y qubits de materia [198], [199]. Las memorias cuánticas almacenan estados mediante la conversión de *flying qubits* (qubits voladores) en qubits estáticos (sexto criterio de DiVincenzo [200]). Fuentes de un solo fotón deterministas, así como sensores cuánticos, son aplicaciones que se benefician de las memorias cuánticas [201], de la misma manera que lo hacen los repetidores cuánticos. De hecho, tanto los repetidores 1G como 2G necesitan memorias cuánticas [155]. Dicho esto, en el caso de la tercera generación, aquellos basados en computación cuántica de tipo *one-way* no necesitan de memorias cuánticas [196].

Existen distintos protocolos de operación y distintas plataformas materiales en las cuales implementar memorias cuánticas, como son vapores atómicos, tierras raras de estado sólido, centros NV (*nitrogen vacancy*), sólidos cristalinos o moléculas [198], [202]. En el caso de protocolos, existen dos mecanismos básicos para construir una memoria cuántica (pueden también combinarse de forma híbrida).

Existen memorias ópticamente controladas, como aquellas basadas en el fenómeno de transparencia inducida de forma electromagnética (EIT) [203], y que se manipulan con pulsos ópticos; y memorias basadas en *photon-echoes* [204], a partir del aprovechamiento del ensanchamiento homogéneo de las líneas de absorción en ciertos materiales. Las memorias de tipo EIT encuentran su implementación predilecta en plataformas atómicas [203], mientras que las memorias de tipo *photon-echo* lo hacen en tierras raras dopadas de estado sólido [204].

Las memorias cuánticas deben satisfacer una serie de requisitos. Cuatro importantes figuras de mérito han de maximizarse: eficiencia, tiempo de almacenamiento, fidelidad y ancho de banda [205], [206]. La eficiencia es esencialmente el cociente entre las intensidades input y ouput de la señal fotónica. El segundo parámetro se refiere a cuánto tiempo puede el estado cuántico permanecer en la memoria. La fidelidad mide cuan parecido es el estado que se lee de la memoria respecto al estado que originalmente se guardó en ella. Finalmente, el ancho de banda está relacionado con la velocidad a la que la información se lee de la memoria.

Las diferentes plataformas para las memorias cuánticas "puntuán" distinto respecto a estos parámetros fundamentales. Aquellas basadas en tierras raras dopadas de estado sólido son por el momento las mejores, consiguiendo alta fidelidad [198], [205],, eficiencias medianas (50%) [207], anchos de banda en el rango de MHz [198], [205] y tiempos de almacenamiento de hasta una hora [198], [205]. En segundo lugar, tenemos a los vapores atómicos calientes, con altas eficiencias (80%) [198], [205], buenas fidelidades, anchos de banda de GHz [205] y tiempos de almacenamiento de segundos [208]. Por su parte, con átomos enfriados por láser se consiguen altas eficiencias [209] y tiempos de almacenamientos de minutos [210]. Sin embargo, los requerimientos experimentales son más exigentes. Entre otras plataformas relevantes tenemos a los centros NV [211], que están aún menos desarrollados en comparación [198], [205]. A modo de ejemplo, tiempos de almacenamiento de un minuto han sido logrados en diamante [212].

Nodos finales e infraestructura adicional

Se espera que el QI conecte varios procesadores cuánticos, desde dispositivos simples de un qubit a computadores cuánticos como tal [190], requiriendose de las memorias cuánticas para almacenar información cuántica en dichos components (algo que un computador cuántico ya necesita [213]).

Dichos dispositivos estarán situados en los nodos finales o de usuario de la red cuántica, que estará mediada por repetidores cuánticos (nodos intermedios, si bien los nodos finales pueden a su vez actuar de repetidores). Infraestructura adicional, como repetidores cuánticos capaces de enrutar información [214] o conmutadores [215] serán componentes necesarios para el funcionamiento pleno de las redes cuánticas.

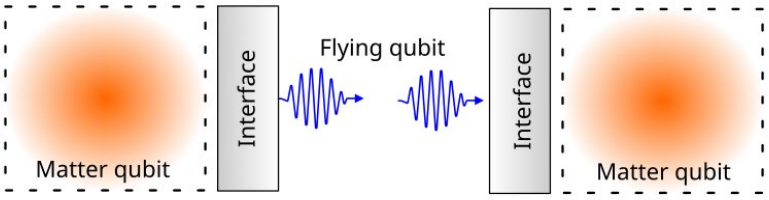


Figura 15: Transducción entre qubits de materia y fotones (flying qubits), a través de una interfaz cuántica, que emite y recibe señales y las traslada a las plataformas de materia, que implementan qubits estáticos.

3.4.2 Aplicaciones

Computación cuántica distribuida

Los nodos finales o nodos de usuario [216] basados en componentes sencillos pueden realizar tareas como el procesamiento óptico lineal que requiere QKD, mientras que otros más evolucionados acabarán proporcionando capacidades de computación cuántica distribuida [193]. La computación cuántica distribuida se presenta como una aplicación crucial del QI futuro, al permitir que una serie de procesadores cuánticos limitados por el número de qubits trabajen de forma combinada [217]. Las unidades de procesamiento cuántico (QPU) interconectadas pueden proporcionar un aumento exponencial de velocidad con un incremento lineal de dispositivos, algo que contrasta con el aumento lineal en el análogo clásico [191], [217].

Computación cuántica a ciegas

La computación cuántica a ciegas (BQC) combina capacidades de computación cuántica y de seguridad cuántica. Permite a un cliente/usuario ejecutar a distancia un trabajo en un ordenador cuántico sin que el contenido del cálculo sea conocido por dicho servidor remoto. El cálculo permanece privado para el usuario, no sólo en la transmisión, como podría lograrse con el cifrado de la comunicación cliente-servidor, sino que además el ordenador cuántico desconoce la estructura (detalles de ejecución y resultado) del cálculo [218]. La BQC puede utilizarse, por ejemplo,

para realizar pagos electrónicos seguros [219]. Se han llevado a cabo demostraciones experimentales de BQC [220]. En dichos trabajos, un servidor basado en trampas de iones se vinculó con un cliente consistente en un dispositivo de detección fotónica, demostrando que el BQC puede lograrse conectando dispositivos más sencillos a nivel de usuario, con ordenadores cuánticos más grandes y remotos [190]. Cabe señalar que los protocolos BQC requieren memorias cuánticas.

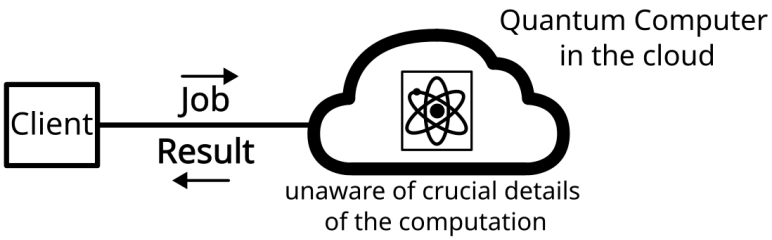


Figura 16: Esquema básico de la computación cuántica a ciegas. Un cliente manda un trabajo ("job") a un computador cuántico en la nube. Éste realiza cálculos sin conocer la estructura real del problema, y devuelve el resultado al cliente, que puede confiar en que el trabajo que delegó sigue permaneciendo confidencial.

Acuerdo bizantino rápido

Como aplicación dentro de la computación cuántica distribuida, en la versión cuántica del acuerdo bizantino (*byzantine agreement*), el cual es un proceso para alcanzar un consenso con la condición de que no se puede confiar en algunos de los sujetos (por ejemplo ordenadores que son defectuosos), el número de rondas de comunicación requeridas escala O(1) con el número de sujetos [221], mientras que clásicamente lo hace de forma polinómica [191].

Elección de líderes

Otro de los problemas que una red cuántica podría atacar es el problema de la elección del líder. En este problema, equivalente al lanzamiento de una moneda en su caso más simple, los usuarios remotos, que no confían los unos en los otros, tienen que hacer una elección basada en el resultado de un proceso aleatorio (como lanzar una moneda). Los usuarios tienen preferencias e intentarán que la balanza se equilibre a su favor [222]. A diferencia del caso clásico, en el que ningún algoritmo puede resolver el problema de la elección de forma exacta, el uso de ordenadores cuánticos distribuidos puede ayudar a superar tales dificultades [190], [222].

3.5 Visión general a futuro. Redes de QKD y desarrollo del Internet cuántico

Nos encontramos aún en una fase muy embrionaria del Internet Cuántico. La IETF está actualmente diseñando las bases [216], [223]. Como ya se dijo en la introducción, el despliegue exitoso del QI depende de desarrollos cruciales en hardware cuántico. Elementos básicos como memorias, repetidores y computadores cuánticos deben mejorar con los años.

Ya que dentro del QI se esperan nodos protegidos mediante QKD, la estandarización y certificación de la QKD es algo básico, con el fin de asegurar interoperabilidad entre redes. El ETSI (European Telecommunications Standards Institute) está trabajando en esa dirección [224]. La empresa coreana SK Telecom envió recientemente dos propuestas de estandarización al ETSI [225]. Diversos proyectos bajo el paraguas de la European Quantum Flagship como OpenQKD [226] reúnen a multitud de agentes (universidades, institutos, empresas) para desarrollar infraestructura de QKD, incluyendo las tareas mencionadas arriba. Con similares objectivos, el proyecto CiviQ [227] trabaja en el contexto de la QKD con variable continua.

Otro proyecto dentro del Quantum Flagship europeo, la Quantum Internet Alliance (QIA) [228] apuesta por el despliegue de un Internet Cuántico en Europa, combinando instituciones académicas, institutos de investigación y socios industriales en diferentes grupos de trabajo dedicados a los diferentes desafíos. Iniciativas similares, como el Quantum Communications Hub (QCH) británico [229] busca compatibilizar QKD dentro de una red de comunicaciones clásicas. Esta integración es un problema complejo, tanto a nivel más lógico, es decir, de gestión de red, como en la propia capa física (coexistencia de señales cuánticas y clásicas). En este contexto, las redes definidas mediante software (SDN, *software defined networks*) se posicionan como una solución viable dentro de este nivel abstracto layer [93], [230]. Dentro de QCH, se han llevado a cabo implementaciones de QKD en variable discreta dentro de la red de pruebas 5GUK, integrando la clave generada mediante QKD en el sistema de cifrado AES [231]. De la misma manera, una prueba de concepto de estas ideas, en este caso con QKD en variable continua, fue realizada en una red real a través de la colaboración de la Universidad Politécnica de Madrid, Telefónica y Huawei en 2018 [232]. A un nivel más físico, se emplea comúnmente el multiplexado por división de la longitud de onda (WDM, *wave*

división multiplexing). Debe atenderse con especial cuidado a las distorsiones que la señal clásica pueda causar en la cuántica, evitando polución fotónica, como es el caso de la dispersión Raman [233], [234].

La European Quantum Communication Initiative (EuroQCI) [235] pretende establecer una red cuántica segura conectando a los países de la Unión Europea, combinando tanto conexiones de fibra como satelitales, contando con la colaboración de la Agencia Espacial Europea (ESA). Como primera piedra, coincidiendo con la reunión del G20 en Trieste en 2022, se desplegó una red QKD viable entre ciudades en Italia, Eslovenia y Croacia, que fue usada para encriptar video-llamadas de dicha conferencia [236].

El protagonismo de China en las comunicaciones cuánticas ha quedado patente a lo largo de este texto, con resultados punteros en QKD tanto en fibras ópticas como conexiones Tierra-satélite. China ha invertido fuertemente en tecnologías cuánticas desde ya hace varios lustros [237]. El 14avo plan quinquenal chino, que acaba en 2025, incluye un enfoque muy serio en comunicaciones cuánticas [238], [239].

En el caso de Japón, por su parte, cabe destacar los experimentos realizados en redes de fibra metropolitanas reales, como es la red de Tokio. En este caso, el esfuerzo combinado de varios agentes, incluyendo instituciones de investigación y grandes empresas como NEC o Mitsubishi, en cooperación con IDQuantique, se estudió el uso de QKD en conexiones de entre 10 y 100 km, combinando múltiples protocolos [240].

Al mismo tiempo, aparte de los esfuerzos del NIST por llevar a cabo una estandarización de PQC, la cual probablemente se combine con QKD en las futuras redes a prueba de ataques cuánticos [120], el proyecto QNEXT [241] estadounidense, liderado por el Argonne National Laboratory, tiene metas similares, como son la investigación y la formación de personal especializado en tecnologías cuánticas, estableciendo nexos de unión entre centros de investigación y empresas. El CQN [242] (Center for Quantum Networks) trabaja en cuatro direcciones: 1) arquitectura de redes cuánticas; 2) subsistemas basados en tecnologías cuánticas; 3) materiales cuánticos y 4) impacto social del Internet Cuántico. Finalmente, el HQAN [243] se centra en computación cuántica distribuída.

3.6 Otros protocolos notables

Realizamos aquí una recopilación breve de otros protocolos en comunicaciones cuánticas que son relevantes, si bien están mucho menos avanzados que la QKD.

1. *Firma digital cuántica* [10]. Análogo cuántico de la firma digital. Relacionado con: función *one-way* cuántica
2. *Comunicación Cuántica Directa Segura* (QSDC) [244]. Intercambio de mensajes seguros, sin necesidad de clave anterior como en QKD.
3. *Quantum Oblivious Transfer*. Objetivo: primitiva para computación cuántica distribuida segura [245], [246]. Relacionado con: *quantum bit commitment*

3.7 Generadores cuánticos de números aleatorios para la protección de las comunicaciones

Una de las características principales de la mecánica cuántica es su aleatoriedad intrínseca. En el mundo clásico, el resultado de lanzar una moneda puede ser cara o cruz, con el 50% de probabilidad. No puede predecirse cual será el resultado, ya que es tremendamente complicado modelizar adecuadamente el vuelo y aterrizaje de la moneda, y tener en cuenta todas las variables en juego. Ya que no podemos ser deterministas, tenemos que "conformarnos" con modelos probabilísticos. En la mecánica cuántica, no obstante, la aleatoriedad es un aspecto fundamental [9]. Dado un qubit en superposición entre dos estados, con idénticas amplitudes de probabilidad, es intrínsecamente imposible predecir cual será el resultado de la medida. Este hecho puede explotarse para obtener generadores de números aleatorios verdaderos (TRNG, true random number generators), superando pues a cualquier generador de números pseudoaleatórios (PRNG, pseudorandom number generator) [132]. Estos dispositivos se conocen como generadores cuánticos de números aleatorios (QRNG) y son una de las tecnologías cuánticas más viables [247]. Dicho esto, debe notarse que los QRNGs, por su propia naturaleza, no gozan del mismo nivel de reproducibilidad que los PRNGs, ya que en estos una misma *semilla* da lugar a la misma secuencia de números aleatorios.

La aleatoriedad, o entropía, que los QNRGs proporcionan se usa de forma continua en los protocolos QKD (excepto aquellos que se implementan de forma pasiva [248], y que contienen sus propios generadores ya embebidos en el propio protocolo), ya que muchos elementos han de ser escogidos de forma aleatoria: bases, intensidades de los *decoy* states, fases globales para aleatorizar los estados

coherentes débiles... Debe notarse que la QKD requiere QRNGs de muy alta calidad [249]. La criptografía clásica necesita también de números genuinamente aleatorios. Los sistemas criptográficos estándar, como los que ya mencionamos, necesitan inputs aleatorios [98]. Incluso si RSA dejase de usarse, los algoritmos PQC pueden acabar necesitando de ellos [250]. En general, existe la demanda de generadores de números aleatorios criptográficamente seguros (CSPRNG, *cryptographicaly secure random number generators*) para tareas criptográficas diversas [247]. Con la llegada del IoT, se vuelve crítico que aquellos pequeños o limitados dispositivos que no puedan integrar QRNGs en si mismos, tengan acceso a buenas fuentes de entropía en la nube [251].

4. Sensores Cuánticos

El hecho de que los sistemas cuánticos sean delicados los hace muy apropiados para realizar tareas de sensado [252]. El campo del sensado cuántico se está convirtiendo, de hecho, en una tecnología cuántica con un nivel cada vez más alto de madurez tecnológica [4], [253], con un mercado diverso [254] el cual se espera que crezca ya en el corto-medio plazo [255]. Con respecto a las telecomunicaciones y el uso ubicuo del campo electromagnético (EM), la idea esencial aquí es que muchos sensores cuánticos constituyen opciones muy buenas para el sensado de campos EM. Pueden emplearse plataformas diversas, dotando de versatilidad a las implementaciones. En esta sección, nos centraremos en aquellas que tengan propiedades adecuadas o deseables para casos de uso en telecomunicaciones. En particular, se tratará el sensado con átomos de Rydberg y centros NV, además de la metrología cuántica variacional, que conecta el sensado cuántico con la computación cuántica.

Otros sensores, que podrían estar también relacionados con las telecomunicaciones, ya que mejoran algunos sistemas necesarios para tareas relacionadas, pueden ser los sensores inerciales, cuyo objetivo es medir efectos rotacionales, gravitacionales e inerciales a través de interferometría con ondas de materia [256]. Por otro lado, las características transversales de las tecnologías fotónicas también son de señalar. En general, la fotónica es capaz de fornecer a aplicaciones diversas con soluciones robustas, estables y compactas de setups ópticos complejos. Experimentos ópticos de laboratorio pueden integrarse en chips, incluyendo fuentes de luz y detectores. Los sensores cuánticos no son una excepción. La integración CMOS de los centros NV [257] y la espectroscopía atómica *on-chip* [258] son dos ejemplos importantes.

Aquellos candidatos a sensores cuánticos no deben solo ser sensibles a pequeños cambios en los parámetros de interés, dado un agente externo que los modifique (un campo eléctrico, por ejemplo) pero deben también ser controlables. Específicamente, un sensor cuántico ha de reunir los siguientes cuatro ingredientes [252]: a) tener una serie de niveles de energía discretos y resolubles; b) posibilitar una inicialización y lectura de estados factible y práctica; c) ser susceptible de ser manipulado de forma coherente; y d) que la interacción con el agente externo sea en forma de un acoplamiento, que va a ser proporcional a un cierto parámetro de

transducción y a los cambios del agente externo, modificándose los niveles energéticos del sistema. Esta última condición otorga de universalidad al sensor, ya que la respuesta de éste se basa pues en cantidades fundamentales como frecuencias de transición.

La figura de mérito definitoria de un sensor cuántico es su **sensibilidad**. Esta se define de una forma un tanto contraintuitiva: la sensibilidad es la señal mínima detectable por unidad de tiempo [252]. Por lo tanto, ha de hacerse muy pequeña (pero el sensor, en efecto, será mucho más sensible). Para que esto ocurra dos factores han de hacerse muy grandes: el parámetro de transducción y el **tiempo de decoherencia**. Considerando sensores operando con estados producto, la sensibilidad está limitada por el llamado límite **SQL** (SQL, *standard quantum limit)* [259]. No obstante, siendo los sensores cuánticos, podemos tener acceso a estados no clásicos, como estados *squeezed* o entrelazados con el fin de superar este límite [260] (ventaja metrológica), estando entonces la sensibilidad acotada, ya a nivel fundamental, por el **límite de Heisenberg** [261]. En particular, una mejora decisiva a la capacidad de sensado la proporciona el uso de una red interconectada de sensores cuánticos [262]. En este caso, un cierto sistema susceptible de ser interrogado se analiza con un estado entrelazado entre n sensores. La sensibilidad que se obtiene escala como $1/n$, mientras que si no existiese entrelazamiento lo haría como $1/\sqrt{n}$ (escalado SQL), estando esto sujeto a restricciones en el los recursos de sensado [262]. En el contexto del IoT y las próximas redes 6G, el sensado distribuido se incorporará, probablemente, como una nueva funcionalidad [263], y se espera que los sensores cuánticos jueguen un papel importante en ese aspecto.

4.1 Sensores RF con plataformas atómicas

Las comunicaciones inalámbricas, especialmente en el contexto 5G, 6G (e IoT), precisan de receptores de radiofrecuencia (RF) de alta ganancia, gran rango dinámico y capacidad de sintonización. Esto no es exclusivo de aplicaciones civiles, sino que, en el ámbito militar, y especialmente en el contexto de la guerra electrónica, se necesitan sensores RF mejorados tanto para detectar anomalías en el espectro de radiofrecuencia como para proporcionar una mayor robustez ante ataques de este tipo. Los sensores cuánticos basados en átomos podrían cumplir con todas estas características, siendo ya explotados en el proyectos como QuASar

de DARPA [264], y a nivel comercial por empresas como Rydberg Technologies [265] o BT [266], quien ha aplicado ya sensores RF cuánticos en escenarios 5G.

Los vapores atómicos a temperatura ambiente en estados de Rydberg son generalmente la mejor opción (los centros NV son la alternativa, pero son menos sensibles y sintonizables [267]). Los electrones excitados en estados de Ryberg tienen un número cuántico principal n muy grande, y se encuentran muy lejos del núcleo, exhibiendo una polarizabilidad gigante. Los electrones externos poseen momentos dipolares tremendamente grandes, siendo la interacción del átomo de Rydberg con el campo eléctrico muy notable. Es decir, incluso campos muy pequeños provocan efectos medibles. En concreto, estos efectos son detectables a través de los cambios en el espectro EIT provocados por un campo RF externo. Los niveles energéticos de Rydberg se vuelven cada vez más cercanos a medida que n crece, permitiendo multitud de transiciones que pueden interaccionar con un rango muy amplio de campos RF, otorgando así a los sensores Rydberg una gran capacidad para sintonizarse a múltiples canales de telecomunicaciones.

Los sensores RF de Rydberg son también muy compactos (en términos de SWaP, es decir, tamaño, peso y potencia), dándoles una ventaja clara sobre homólogos clásicos que necesitan de complejos sistemas de antenas. Un solo dispositivo puede usarse para detectar radiofrecuencias entre DC y THz. La cuarta condición para un sensor (universalidad) mencionada antes también se satisface: la calibración es absoluta, dependiendo únicamente de constantes físicas universales (esto también se conoce como auto-calibración). En conclusión, los sensores RF de Rydberg mejoran a sus alternativas clásicas, permitiendo la medida también de fases mediante técnicas heterodinas o superheterodinas [268]. Si se construye un clúster de varios sensores, probablemente también sería posible realizar medidas de direccionalidad del campo.

4.2 Sensores basados en espín

Existen varias plataformas basadas en espín para la metrología cuántica. Espines nucleares en conjuntos de átomos, puntos cuánticos (*quantum dots*) en semiconductores... son algunos ejemplos. De entre distintos candidatos, aquel que ha recibido más atención, dadas sus notables propiedades, ha sido el centro NV [252].

El centro NV en diamante es un sistema de estado sólido que se comporta como un átomo, y que posee propiedades de espín susceptibles de interacción óptica. Puede también ser utilizado a temperatura ambiente. El centro NV para sensado cuántico ofrece la posibilidad de captar señales diminutas en ambientes con un alto nivel de ruido, con aplicación en varios ámbitos más allá del campo telecom. El espín del estado cuántico del centro NV puede inicializarse de forma óptica, y la evolución de este puede detectarse también de forma óptica.

La técnica de ODMR (optically detected magnetic resonance) permite modular la intensidad de fluorescencia que depende del espín electrónico en el centro NV, permitiendo así el acceso a la medida de campos magnéticos y eléctricos. El campo magnético aplicado se determina a través de la detección de los corrimientos Zeeman de los subniveles de espín en el estado triplete fundamental. Cuando la frecuencia de microondas está en resonancia entre el estado $m_s = 1$ y uno de los estados $m_s = \pm 1$, la rotación de espín se obtiene a partir de la bajada en la fotoluminiscencia de la señal. El uso del espectro de dicha señal permite realizar espectroscopia de las energías de espín, lo cual es sensible a cambios en el campo magnético externo, así como temperatura y tensión.

El rápido desarrollo de tecnologías de RF precisa de herramientas que puedan monitorizar eficientemente el espectro electromagnético. En relación a esto, como fruto de una reciente colaboración entre el Thales Research Group y la Universidad de Paris-Saclay, se ha propuesto un analizador de señales de microondas explotando precisamente las propiedades de espín del centro NV, cuya frecuencia de resonancia se codifica de forma espacial a través del gradiente de campo magnético externo [267].

4.3 Relojes atómicos y ópticos

La necesidad de una referencia temporal ultra-precisa es proporciona una mejor coordinación y sincronización de redes de comunicación [233]. Las frecuencias de transición atómicas pueden emplearse a tal efecto, si los átomos se controlan apropiadamente (incluso mediante enfriamiento laser), reduciendo el ensanchamiento por efecto Doppler, colisiones etc. De hecho, los estándares actuales se basan en relojes atómicos en elementos alcalinos. En concreto, el estándar de cesio (Cs) usa una transición en el rango de los GHz (9.192 631 770 GHz).

Si nos movemos hacia frecuencias más grandes (ya en el rango de las frecuencias ópticas), podremos realizar ajustes más finos. Los relojes que usan esas transiciones, típicamente a partir de elementos alcalino-térreos, se denominan **relojes ópticos**. Se basan en láseres estabilizados en frecuencia, peines ópticos y enfriamiento laser mediante retículos ópticos o iones atrapados [233], [269] . La mejora en los relojes ópticos es continua, mejorando la precisión del estándar de Cs, al que probablemente remplacen en la próxima década [270].

Por otro lado, si esto se combina con entrelazamiento cuántico, en un contexto de QI, tendríamos capacidades mejoradas de sincronización de relojes [271]. Si se interconectan una serie de relojes distantes, de forma que compartan un estado entrelazado, podría tenerse una referencia temporal que fuese a la vez super-estable, precisa y actualizada en tiempo real [272].

4.4 Metrología Cuántica Variacional

Hemos visto que existe un límite fundamental a la sensibilidad de un sensor cuántico, condicionada por el principio de incertidumbre de Heisenberg. No obstante, acercarse a dicho límite (incluso a SQL) sigue siendo un gran desafío.

La **metrología cuántica variacional** se basa en el método variacional (sección 2.3.4) para mejorar esta sensibilidad. De acuerdo con esta aproximación, ciertos pasos del procedimiento de sensado pueden realizarse mediante circuitos cuánticos parametrizados, los que, al contrario que los circuitos fijos, pueden ser optimizados de forma iterativa mejorando así el rendimiento y adaptándose a escenarios de sensado concretos.

Un posible paso a optimizar es la generación del estado sonda [273], i.e el estado entrelazado que interaccionará con el sistema de interés. En este caso, la preparación del estado se lleva a cabo mediante un circuito variacional cuyos parámetros se van ajustando hasta que se minimiza una función de coste dependiente de la sensibilidad del sistema. Como resultado se obtiene un estado sonda optimizado para la tarea metrológica específica.

Otro posible paso a mejorar es la medida [274]. En este caso, un circuito parametrizado aproxima la medida (o decodificacón) en si misma. De la misma

manera, sus parámetros se ajustan hasta que se alcance la sensibilidad óptima dado un cierto modelo de ruido.

Los sistemas que emplean esta clase de mejoras se pueden denominar "sensores cuánticos programables". En este sentido, la metrología cuántica variacional convierte a dispositivos NISQ y simuladores cuánticos programables en sensores. Asimismo, aunque estos circuitos tienden a mejorar a medida que se incluyen más y más capas variacionales, el rendimiento obtenido incluso con circuitos de poca profundidad es notable, haciéndolos muy compatibles con el hardware de tipo NISQ.

Bibliografía

[1] «Strategic Research and Innovation Agenda 2022», *NetworldEurope ETP*, 19 de diciembre de 2022. https://www.networldeurope.eu/sria-2022-announcement/ (accedido 18 de septiembre de 2023).

[2] A. G. J. MacFarlane, J. P. Dowling, y G. J. Milburn, «Quantum technology: the second quantum revolution», *Philos. Trans. R. Soc. Lond. Ser. Math. Phys. Eng. Sci.*, vol. 361, n.º 1809, pp. 1655-1674, jun. 2003, doi: 10.1098/rsta.2003.1227.

[3] A. Salameh y M. Tarhuni, «From 5G to 6G—Challenges, Technologies, and Applications», *Future Internet*, vol. 14, p. 117, abr. 2022, doi: 10.3390/fi14040117.

[4] A. Purohit, M. Kaur, Z. C. Seskir, M. T. Posner, y A. Venegas-Gomez, «Building a Quantum-ready Ecosystem». arXiv, 8 de septiembre de 2023. Accedido: 11 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2304.06843

[5] K. David y H. Berndt, «6G Vision and Requirements: Is There Any Need for Beyond 5G?», *IEEE Veh. Technol. Mag.*, vol. 13, n.º 3, pp. 72-80, sep. 2018, doi: 10.1109/MVT.2018.2848498.

[6] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Kténas, N. Cassiau, y C. Dehos, «6G: The Next Frontier». arXiv, 16 de mayo de 2019. Accedido: 12 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/1901.03239

[7] «White Paper 5G Evolution and 6G».

[8] E. Knill, R. Laflamme, y W. H. Zurek, «Resilient Quantum Computation», *Science*, vol. 279, n.º 5349, pp. 342-345, ene. 1998, doi: 10.1126/science.279.5349.342.

[9] A. Aspect, «Closing the Door on Einstein and Bohr's Quantum Debate», *Physics*, vol. 8, p. 123, dic. 2015, doi: 10.1103/PhysRevLett.115.250401.

[10] S. Pirandola *et al.*, «Advances in Quantum Cryptography», *Adv. Opt. Photonics*, vol. 12, n.º 4, p. 1012, dic. 2020, doi: 10.1364/AOP.361502.

[11] S. Pirandola, «End-to-end capacities of a quantum communication network», *Commun. Phys.*, vol. 2, n.º 1, p. 51, may 2019, doi: 10.1038/s42005-019-0147-3.

[12] P. Benioff, «The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines», *J. Stat. Phys.*, vol. 22, n.º 5, pp. 563-591, may 1980, doi: 10.1007/BF01011339.

[13] R. P. Feynman, «Simulating physics with computers», *Int. J. Theor. Phys.*, vol. 21, n.º 6, pp. 467-488, jun. 1982, doi: 10.1007/BF02650179.

[14] D. Deutsch, «Quantum theory, the Church–Turing principle and the universal quantum computer», *Proc. R. Soc. Lond. Math. Phys. Sci.*, vol. 400, n.º 1818, pp. 97-117, 1985, doi: 10.1098/rspa.1985.0070.

[15] J. Preskill, «Quantum Computing in the NISQ era and beyond», *Quantum*, vol. 2, p. 79, ago. 2018, doi: 10.22331/q-2018-08-06-79.

[16] M. R. Garey y D. S. Johnson, *Computers and intractability: a guide to the theory of NP-completeness*, 27. print. en A series of books in the mathematical sciences. New York [u.a]: Freeman, 1979.

[17] P. Shor, «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer».

[18] L. K. Grover, «A fast quantum mechanical algorithm for database search». arXiv, 19 de noviembre de 1996. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/quant-ph/9605043

[19] M. Cerezo *et al.*, «Variational quantum algorithms», *Nat. Rev. Phys.*, vol. 3, n.º 9, Art. n.º 9, sep. 2021, doi: 10.1038/s42254-021-00348-9.

[20] «Quantum Computing Modalities – A Qubit Primer Revisited», *The Quantum Leap*, 20 de octubre de 2022. https://quantumtech.blog/2022/10/20/quantum-computing-modalities-a-qubit-primer-revisited/ (accedido 5 de septiembre de 2023).

[21] J. Dargan, «81 Quantum Computing Companies: An Ultimate 2023 List», *The Quantum Insider*, 5 de septiembre de 2022. https://thequantuminsider.com/2022/09/05/quantum-computing-companies-ultimate-list-for-2022/ (accedido 5 de septiembre de 2023).

[22] «A Brief Introduction to Quantum Computing | HackerNoon». https://hackernoon.com/a-brief-introduction-to-quantum-computing-d21e578cb7ed (accedido 5 de septiembre de 2023).

[23] D. Coppersmith, «An approximate Fourier transform useful in quantum factoring». arXiv, 16 de enero de 2002. Accedido: 7 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/quant-ph/0201067

[24] A. Y. Kitaev, «Quantum measurements and the Abelian Stabilizer Problem». arXiv, 20 de noviembre de 1995. Accedido: 8 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/quant-ph/9511026

[25] E. W. Weisstein, «Number Field Sieve». https://mathworld.wolfram.com/ (accedido 19 de septiembre de 2023).

[26] C. Gidney y M. Ekerå, «How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits», *Quantum*, vol. 5, p. 433, abr. 2021, doi: 10.22331/q-2021-04-15-433.

[27] G. Brassard, P. Hoyer, y A. Tapp, «Quantum Algorithm for the Collision Problem», 1998, pp. 163-169. doi: 10.1007/BFb0054319.

[28] E. Campbell, A. Khurana, y A. Montanaro, «Applying quantum algorithms to constraint satisfaction problems», *Quantum*, vol. 3, p. 167, jul. 2019, doi: 10.22331/q-2019-07-18-167.

[29] Daniel J. Bernstein, University of Illinois at Chicago, USA *et al.*, «Special-purpose Hardware for Attacking Cryptographic Systems», sep. 2009.

[30] R. Babbush, J. McClean, M. Newman, C. Gidney, S. Boixo, y H. Neven, «Focus beyond quadratic speedups for error-corrected quantum advantage», *PRX Quantum*, vol. 2, n.º 1, p. 010103, mar. 2021, doi: 10.1103/PRXQuantum.2.010103.

[31] M. Brooks, «Beyond quantum supremacy: the hunt for useful quantum computers», *Nature*, vol. 574, n.º 7776, pp. 19-21, oct. 2019, doi: 10.1038/d41586-019-02936-3.

[32] M. Schuld y N. Killoran, «Quantum machine learning in feature Hilbert spaces», *Phys. Rev. Lett.*, vol. 122, n.º 4, p. 040504, feb. 2019, doi: 10.1103/PhysRevLett.122.040504.

[33] «Data encoding». https://learn.qiskit.org/course/machine-learning/data-encoding (accedido 5 de septiembre de 2023).

[34] «PauliFeatureMap - Qiskit 0.44.1 documentation». https://qiskit.org/documentation/stubs/qiskit.circuit.library.PauliFeatureMap.html (accedido 5 de septiembre de 2023).

[35] V. Havlicek *et al.*, «Supervised learning with quantum enhanced feature spaces», *Nature*, vol. 567, n.º 7747, pp. 209-212, mar. 2019, doi: 10.1038/s41586-019-0980-2.

[36] C. Cortes y V. Vapnik, «Support-vector networks», *Mach. Learn.*, vol. 20, n.º 3, pp. 273-297, sep. 1995, doi: 10.1007/BF00994018.

[37] «Training parameterized quantum circuits». https://learn.qiskit.org/course/machine-learning/training-quantum-circuits (accedido 18 de septiembre de 2023).

[38] A. Pérez-Salinas, A. Cervera-Lierta, E. Gil-Fuster, y J. I. Latorre, «Data re-uploading for a universal quantum classifier», *Quantum*, vol. 4, p. 226, feb. 2020, doi: 10.22331/q-2020-02-06-226.

[39] E. F.-C. Alvarez y S. G. Castillo, *PRACTICAL GUIDE TO QUANTUM MACHINE LEARNING AND QUANTUM OPTIMISATION hands-on approach to modern quantum algorithms*, First edition. S.l.: PACKT PUBLISHING LIMITED, 2023.

[40] J. Romero, J. P. Olson, y A. Aspuru-Guzik, «Quantum autoencoders for efficient compression of quantum data», *Quantum Sci. Technol.*, vol. 2, n.º 4, p. 045001, dic. 2017, doi: 10.1088/2058-9565/aa8072.

[41] I. J. Goodfellow *et al.*, «Generative Adversarial Networks». arXiv, 10 de junio de 2014. Accedido: 5 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/1406.2661

[42] H.-L. Huang *et al.*, «Experimental Quantum Generative Adversarial Networks for Image Generation», *Phys. Rev. Appl.*, vol. 16, n.º 2, p. 024051, ago. 2021, doi: 10.1103/PhysRevApplied.16.024051.

[43] W. Liu, Y. Zhang, Z. Deng, J. Zhao, y L. Tong, «A hybrid quantum-classical conditional generative adversarial network algorithm for human-centered paradigm in cloud», *EURASIP J. Wirel. Commun. Netw.*, vol. 2021, n.º 1, p. 37, feb. 2021, doi: 10.1186/s13638-021-01898-3.

[44] S. Jerbi, C. Gyurik, S. C. Marshall, H. J. Briegel, y V. Dunjko, «Parametrized quantum policies for reinforcement learning». arXiv, 9 de diciembre de 2021. Accedido: 5 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2103.05577

[45] A. Skolik, S. Jerbi, y V. Dunjko, «Quantum agents in the Gym: a variational quantum algorithm for deep Q-learning», *Quantum*, vol. 6, p. 720, may 2022, doi: 10.22331/q-2022-05-24-720.

[46] «Parametrized Quantum Circuits for Reinforcement Learning | TensorFlow Quantum», *TensorFlow*. https://www.tensorflow.org/quantum/tutorials/quantum_reinforcement_learning (accedido 5 de septiembre de 2023).

[47] E. Farhi, J. Goldstone, y S. Gutmann, «A Quantum Approximate Optimization Algorithm». arXiv, 14 de noviembre de 2014. doi: 10.48550/arXiv.1411.4028.

[48] «List of QUBO formulations», *QUBO formulations*. https://blog.xa0.de/post/List-of-QUBO-formulations/

[49] P. Date, D. Arthur, y L. Pusey-Nazzaro, «QUBO formulations for training machine learning models», *Sci. Rep.*, vol. 11, n.º 1, Art. n.º 1, may 2021, doi: 10.1038/s41598-021-89461-4.

[50] D. Willsch, M. Willsch, H. De Raedt, y K. Michielsen, «Support vector machines on the D-Wave quantum annealer», *Comput. Phys. Commun.*, vol. 248, p. 107006, mar. 2020, doi: 10.1016/j.cpc.2019.107006.

[51] K. L. Pudenz y D. A. Lidar, «Quantum adiabatic machine learning», *Quantum Inf. Process.*, vol. 12, n.º 5, pp. 2027-2070, may 2013, doi: 10.1007/s11128-012-0506-4.

[52] S. Mücke, R. Heese, S. Müller, M. Wolter, y N. Piatkowski, «Feature Selection on Quantum Computers», *Quantum Mach. Intell.*, vol. 5, n.º 1, p. 11, jun. 2023, doi: 10.1007/s42484-023-00099-z.

[53] S. Abel, J. C. Criado, y M. Spannowsky, «Completely Quantum Neural Networks», *Phys. Rev. A*, vol. 106, n.º 2, p. 022601, ago. 2022, doi: 10.1103/PhysRevA.106.022601.

[54] Hexa-X, «D1.3 - Targets and requirements for 6G - initial E2E architecture», feb. 2022, [En línea]. Disponible en: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf

[55] «Vision - Hexa-X», 11 de octubre de 2021. https://hexa-x.eu/vision/ (accedido 21 de septiembre de 2023).

[56] A. Zappone, M. Di Renzo, y M. Debbah, «Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?» arXiv, 13 de junio de 2019. Accedido: 17 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/1902.02647

[57] A. Patil, S. Iyer, y R. J. Pandya, «A Survey of Machine Learning Algorithms for 6G Wireless Networks». arXiv, 16 de marzo de 2022. Accedido: 17 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2203.08429

[58] R. Ferrara, R. Bassoli, C. Deppe, F. H. P. Fitzek, y H. Boche, «The Computational and Latency Advantage of Quantum Communication Networks», *IEEE Commun. Mag.*, vol. 59, n.º 6, pp. 132-137, jun. 2021, doi: 10.1109/MCOM.011.2000863.

[59] C. J. Bernardos y M. A. Uusitalo, «European Vision for the 6G Network Ecosystem», Zenodo, jun. 2021. doi: 10.5281/ZENODO.5007671.

[60] Y. L. Lee, D. Qin, L.-C. Wang, y G. H. Sim, «6G Massive Radio Access Networks: Key Applications, Requirements and Challenges», *IEEE Open J. Veh. Technol.*, vol. 2, pp. 54-66, 2021, doi: 10.1109/OJVT.2020.3044569.

[61] Md. Shahjalal *et al.*, «Enabling technologies for AI empowered 6G massive radio access networks», *ICT Express*, vol. 9, n.º 3, pp. 341-355, jun. 2023, doi: 10.1016/j.icte.2022.07.002.

[62] S. Seemakuthi, V. A. Siriki, y D. E. L. Lydia, «A Review on Various Scheduling Algorithms», vol. 6, n.º 12, 2015.

[63] M. Kim, D. Venturelli, y K. Jamieson, «Leveraging quantum annealing for large MIMO processing in centralized radio access networks», en *Proceedings of the ACM Special Interest Group on Data Communication*, en SIGCOMM '19. New York, NY, USA: Association for Computing Machinery, ago. 2019, pp. 241-255. doi: 10.1145/3341302.3342072.

[64] M. Kim y K. Jamieson, «Finer-Grained Decomposition for Parallel Quantum Mimo Processing», en *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, jun. 2023, pp. 1-5. doi: 10.1109/ICASSP49357.2023.10096503.

[65] Z. I. Tabi, Á. Marosits, Z. Kallus, P. Vaderna, I. Gódor, y Z. Zimborás, «Evaluation of Quantum Annealer Performance via the Massive MIMO Problem», *IEEE Access*, vol. 9, pp. 131658-131671, 2021, doi: 10.1109/ACCESS.2021.3114543.

[66] A. Stockley y K. Briggs, «Optimizing antenna beamforming with quantum computing», en *2023 17th European Conference on Antennas and Propagation (EuCAP)*, mar. 2023, pp. 1-5. doi: 10.23919/EuCAP57121.2023.10133700.

[67] T. Ohyama, Y. Kawamoto, y N. Kato, «Resource Allocation Optimization by Quantum Computing for Shared Use of Standalone IRS», *IEEE Trans. Emerg. Top. Comput.*, pp. 1-13, 2023, doi: 10.1109/TETC.2023.3292355.

[68] T. Ohyama, Y. Kawamoto, y N. Kato, «Quantum Computing Based Optimization for Intelligent Reflecting Surface (IRS)-Aided Cell-Free Network», *IEEE Trans. Emerg. Top. Comput.*, vol. 11, n.º 1, pp. 18-29, ene. 2023, doi: 10.1109/TETC.2022.3161542.

[69] «Vector Perturbation Precoding Under Imperfect CSI and Inaccurate Power Scaling Factors | IEEE Journals & Magazine | IEEE Xplore». https://ieeexplore.ieee.org/document/8753485 (accedido 7 de septiembre de 2023).

[70] J. Wang, Y. Ma, N. Yi, R. Tafazolli, y F. Tong, «Constellation-Oriented Perturbation for Scalable-Complexity MIMO Nonlinear Precoding», en *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, dic. 2022, pp. 2413-2418. doi: 10.1109/GLOBECOM48099.2022.10001237.

[71] S. Kasi, A. K. Singh, D. Venturelli, y K. Jamieson, «Quantum Annealing for Large MIMO Downlink Vector Perturbation Precoding», en *ICC 2021 - IEEE International Conference on Communications*, jun. 2021, pp. 1-6. doi: 10.1109/ICC42927.2021.9500557.

[72] B. Narottama, T. Jamaluddin, y S. Y. Shin, «Integration of Quantum Variational Circuit and SVD for Precoding Optimization».

[73] B. Narottama y T. Q. Duong, «Quantum neural networks for optimal resource allocation in cell-free MIMO systems: IEEE Global Communications Conference 2022», *Proc. IEEE Glob. Commun. Conf. GLOBECOM 2022*, pp. 2444-2449, ene. 2023, doi: 10.1109/GLOBECOM48099.2022.10001726.

[74] F. A. Cárdenas-López, L. Lamata, J. C. Retamal, y E. Solano, «Multiqubit and multilevel quantum reinforcement learning with quantum technologies», *PLOS ONE*, vol. 13, n.º 7, p. e0200455, jul. 2018, doi: 10.1371/journal.pone.0200455.

[75] A. Paz-Pérez, «Design and Implementation of Reinforcement Learning Scheduling Algorithms for 5G networks for the ns-3 Simulator», TFM, University of Vigo, 2023. [En línea]. Disponible en:

https://secretaria.uvigo.gal/uvigo.sv/index.php?modulo=tfe&accion=visualizaTfe&id=29814

[76] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, y O. Klimov, «Proximal Policy Optimization Algorithms». arXiv, 28 de agosto de 2017. doi: 10.48550/arXiv.1707.06347.

[77] K. Davaslioglu, T. Erpek, y Y. E. Sagduyu, «End-to-End Autoencoder Communications with Optimized Interference Suppression». arXiv, 29 de diciembre de 2021. doi: 10.48550/arXiv.2201.01388.

[78] «The Quantum Autoencoder — Qiskit Machine Learning 0.6.1 documentation». https://qiskit.org/ecosystem/machine-learning/tutorials/12_quantum_autoencoder.html (accedido 6 de septiembre de 2023).

[79] Z. Tabi *et al.*, «Hybrid Quantum-Classical Autoencoders for End-to-End Radio Communication», en *2022 IEEE/ACM 7th Symposium on Edge Computing (SEC)*, dic. 2022, pp. 468-473. doi: 10.1109/SEC54971.2022.00071.

[80] H. Ye, L. Liang, G. Y. Li, y B.-H. F. Juang, «Deep Learning based End-to-End Wireless Communication Systems with Conditional GAN as Unknown Channel». arXiv, 6 de marzo de 2019. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/1903.02551

[81] S. Huang, C. Lin, K. Zhou, Y. Yao, H. Lu, y F. Zhu, «Identifying physical-layer attacks for IoT security: An automatic modulation classification approach using multi-module fusion neural network», *Phys. Commun.*, vol. 43, p. 101180, dic. 2020, doi: 10.1016/j.phycom.2020.101180.

[82] T. J. O'Shea, T. Roy, y T. C. Clancy, «Over the Air Deep Learning Based Radio Signal Classification», *IEEE J. Sel. Top. Signal Process.*, vol. 12, n.º 1, pp. 168-179, feb. 2018, doi: 10.1109/JSTSP.2018.2797022.

[83] I. Cong, S. Choi, y M. D. Lukin, «Quantum Convolutional Neural Networks», *Nat. Phys.*, vol. 15, n.º 12, pp. 1273-1278, dic. 2019, doi: 10.1038/s41567-019-0648-8.

[84] E. Payares y J. C. Martinez Santos, «Quantum machine learning for intrusion detection of distributed denial of service attacks: A comparative overview», mar. 2021, p. 47. doi: 10.1117/12.2593297.

[85] M. Kalinin y V. Krundyshev, «Security intrusion detection using quantum machine learning techniques», *J. Comput. Virol. Hacking Tech.*, vol. 19, n.º 1, pp. 125-136, mar. 2023, doi: 10.1007/s11416-022-00435-0.

[86] J. S. Baker *et al.*, «Quantum Variational Rewinding for Time Series Anomaly Detection». arXiv, 2 de noviembre de 2022. Accedido: 24 de julio de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2210.16438

[87] M. Guo *et al.*, «Quantum algorithms for anomaly detection using amplitude estimation», *Phys. Stat. Mech. Its Appl.*, vol. 604, p. 127936, oct. 2022, doi: 10.1016/j.physa.2022.127936.

[88] F. Leymann y J. Barzen, «The bitter truth about gate-based quantum algorithms in the NISQ era», *Quantum Sci. Technol.*, vol. 5, n.º 4, p. 044007, sep. 2020, doi: 10.1088/2058-9565/abae7d.

[89] M. Scheerer, J. Klamroth, y O. Denninger, «Fault-tolerant Hybrid Quantum Software Systems», en *2022 IEEE International Conference on Quantum Software (QSW)*, jul. 2022, pp. 52-57. doi: 10.1109/QSW55613.2022.00023.

[90] W. K. Wootters y W. H. Zurek, «A single quantum cannot be cloned», *Nature*, vol. 299, pp. 802-803, oct. 1982, doi: 10.1038/299802a0.

[91] L. Xiao, D. Qiu, L. Luo, y P. Mateus, «Distributed Shor's algorithm». arXiv, 13 de julio de 2022. Accedido: 18 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2207.05976

[92] A. Callison y N. Chancellor, «Hybrid quantum-classical algorithms in the noisy intermediate-scale quantum era and beyond», *Phys. Rev. A*, vol. 106, n.º 1, p. 010101, jul. 2022, doi: 10.1103/PhysRevA.106.010101.

[93] V. Martin *et al.*, «Quantum technologies in the telecommunications industry», *EPJ Quantum Technol.*, vol. 8, n.º 1, p. 19, dic. 2021, doi: 10.1140/epjqt/s40507-021-00108-9.

[94] J. D. Morris, M. R. Grimaila, D. J. Douglas D. Hodson, y G. Baumgartner, «Chapter 9. A Survey of Quantum Key Distribution», en *Emerging Trends in ICT security*, Morgan Kaufmann, 2014, pp. 141-152.

[95] C. E. Shannon, «Communication Theory of Secrecy Systems*», *Bell Syst. Tech. J.*, vol. 28, n.º 4, pp. 656-715, oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[96] T. J. Shimeall y J. M. Spring, *Introduction to Information Security. A Strategic-Based Approach*. Elsevier, 2014.

[97] A. Vega, P. Bose, y A. Buyuktosunoglu, *Rugged Embedded Systems. Computing in Harsh Environments*. Elsevier, 2017.

[98] A. Menezes, P. V. Oorschot, y S. Vanstone, «Chapter 8. Public-Key Encryption», en *Handbook of applied cryptography*, CRC Press, 1996, pp. 283-319.

[99] M. I. González Vasco y Á. L. Pérez del Pozo, *Criptografía esencial: Principios básicos para el diseño de esquemas y protocolos seguros*. Madrid: RA-MA Editorial, 2021.

[100] D. J. Bernstein y T. Lange, «Post-quantum cryptography – dealing with the fallout of physics success».

[101] A. Menezes, P. V. Oorschot, y S. Vanstone, «Chapter 11. Digital Signatures», en *Handbook of applied cryptography*, CRC Press, 1996, pp. 425-488.

[102] Alex.Arnaut, «How Digital Signatures Work», *DocuSign*, 3 de noviembre de 2015. https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq (accedido 5 de septiembre de 2023).

[103] «What is PKI?» ttps://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki (accedido 5 de septiembre de 2023).

[104] R. L. Rivest, A. Shamir, y L. Adleman, «A method for obtaining digital signatures and public-key cryptosystems», *Commun. ACM*, vol. 21, n.º 2, pp. 120-126, feb. 1978, doi: 10.1145/359340.359342.

[105] D. J. Bernstein, «Introduction to post-quantum cryptography», en *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, y E. Dahmen, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 1-14. doi: 10.1007/978-3-540-88702-7_1.

[106] E. Diamanti, H.-K. Lo, B. Qi, y Z. Yuan, «Practical challenges in quantum key distribution», *Npj Quantum Inf.*, vol. 2, n.º 1, p. 16025, nov. 2016, doi: 10.1038/npjqi.2016.25.

[107] «Post-Quantum Cryptography Global Revenues to Grow 12% From 2022 to 2023 and 20% Between 2026-2027». https://www.abiresearch.com/press/post-quantum-cryptography-global-revenues-to-grow-12-from-2022-to-2023-and-20-between-2026-2027/ (accedido 6 de septiembre de 2023).

[108] X. Lu y J. Zhang, «Lattice-based PKEs/KEMs», *Natl. Sci. Rev.*, vol. 8, n.º 9, p. nwab090, sep. 2021, doi: 10.1093/nsr/nwab090.

[109] R. Asif, «Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms», *IoT*, vol. 2, n.º 1, pp. 71-91, feb. 2021, doi: 10.3390/iot2010005.

[110] G. Yalamuri, P. Honnavalli, y S. Eswaran, «A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats», *Procedia Comput. Sci.*, vol. 215, pp. 834-845, 2022, doi: 10.1016/j.procs.2022.12.086.

[111] G. Alagic *et al.*, «Status report on the third round of the NIST Post-Quantum Cryptography Standardization process», National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST IR 8413-upd1, sep. 2022. doi: 10.6028/NIST.IR.8413-upd1.

[112] I. T. L. Computer Security Division, «Post-Quantum Cryptography | CSRC | CSRC - August 24 Draft Standards», *CSRC | NIST*, 2023. https://csrc.nist.gov/projects/post-quantum-cryptography (accedido 5 de septiembre de 2023).

[113] I. T. L. Computer Security Division, «Stateful Hash-Based Signatures | CSRC | CSRC», *CSRC | NIST*, 20 de diciembre de 2018. https://csrc.nist.gov/projects/stateful-hash-based-signatures (accedido 5 de septiembre de 2023).

[114] *Open Quantum Safe*. https://openquantumsafe.org/ (accedido 5 de septiembre de 2023).

[115] «Migration to Post-Quantum Cryptography | NCCoE». https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms (accedido 6 de septiembre de 2023).

[116] V. Lovic, «Quantum Key Distribution: Advantages, Challenges and Policy», vol. 1, n.º 2, 2020.

[117] «Post-Quantum TLS - Microsoft Research». https://www.microsoft.com/en-us/research/project/post-quantum-tls/ (accedido 5 de septiembre de 2023).

[118] «Post-quantum TLS now supported in AWS KMS | AWS Security Blog», 4 de noviembre de 2019. https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/ (accedido 5 de septiembre de 2023).

[119] H. Nejatollahi, N. Dutt, y R. Cammarota, «Trends, challenges and needs for lattice-based cryptography implementations: special session», en *Proceedings of the Twelfth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis Companion*, Seoul Republic of Korea: ACM, oct. 2017, pp. 1-3. doi: 10.1145/3125502.3125559.

[120] R. Renner y R. Wolf, «The debate over QKD: A rebuttal to the NSA's objections». arXiv, 27 de julio de 2023. Accedido: 18 de agosto de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2307.15116

[121] V. Martin, J. Martinez-Mateo, y M. Peev, «Introduction to Quantum Key Distribution», en *Wiley Encyclopedia of Electrical and Electronics Engineering*, J. G. Webster, Ed., 1.ª ed.Wiley, 2017, pp. 1-17. doi: 10.1002/047134608X.W8354.

[122] H.-K. Lo y N. Lütkenhaus, «Quantum Cryptography: from Theory to Practice». arXiv, 13 de marzo de 2007. Accedido: 30 de agosto de 2023. [En línea]. Disponible en: http://arxiv.org/abs/quant-ph/0702202

[123] «Cryptography secures Swiss elections». https://optics.org/article/31646 (accedido 11 de septiembre de 2023).

[124] «Encryption kicks off in the quantumStadium», *Physics World*, 27 de mayo de 2010. https://physicsworld.com/a/playing-in-the-quantumstadium/ (accedido 11 de septiembre de 2023).

[125] H.-K. Lo, H. F. Chau, y M. Ardehali, «Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security», *J. Cryptol.*, vol. 18, n.º 2, pp. 133-165, abr. 2005, doi: 10.1007/s00145-004-0142-y.

[126]C. H. Bennett y G. Brassard, «Quantum cryptography: Public key distribution and coin tossing», *Theor. Comput. Sci.*, vol. 560, pp. 7-11, dic. 2014, doi: 10.1016/j.tcs.2014.05.025.

[127]H. Bechmann-Pasquinucci y W. Tittel, «Quantum Cryptography using larger alphabets», *Phys. Rev. A*, vol. 61, n.º 6, p. 062308, may 2000, doi: 10.1103/PhysRevA.61.062308.

[128] G. Cañas *et al.*, «High-dimensional decoy-state quantum key distribution over 0.3 km of multicore telecommunication optical fibers», *Phys. Rev. A*, vol. 96, n.º 2, p. 022317, ago. 2017, doi: 10.1103/PhysRevA.96.022317.

[129]H. Cao *et al.*, «Distribution of high-dimensional orbital angular momentum entanglement over a 1 km few-mode fiber», *Optica*, vol. 7, n.º 3, p. 232, mar. 2020, doi: 10.1364/OPTICA.381403.

[130] S. L. Braunstein y P. van Loock, «Quantum information with continuous variables», *Rev. Mod. Phys.*, vol. 77, n.º 2, pp. 513-577, jun. 2005, doi: 10.1103/RevModPhys.77.513.

[131] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, y M. Peev, «The Security of Practical Quantum Key Distribution», *Rev. Mod. Phys.*, vol. 81, n.º 3, pp. 1301-1350, sep. 2009, doi: 10.1103/RevModPhys.81.1301.

[132]S. Pirandola *et al.*, «Advances in Quantum Cryptography», *Adv. Opt. Photonics*, vol. 12, n.º 4, p. 1012, dic. 2020, doi: 10.1364/AOP.361502.

[133]A. J. Almeida, N. J. Muga, N. A. Silva, J. M. Prata, P. S. De Brito Andre, y A. N. Pinto, «Continuous Control of Random Polarization Rotations for Quantum Communications», *J. Light. Technol.*, pp. 1-1, 2016, doi: 10.1109/JLT.2016.2587818.

[134] Y.-Y. Ding *et al.*, «Polarization basis tracking scheme for quantum key distribution with revealed sifted key bits», *Opt. Lett.*, vol. 42, n.º 6, p. 1023, mar. 2017, doi: 10.1364/OL.42.001023.

[135]D. S. Bethune y W. P. Risk, «Autocompensating quantum cryptography», *New J. Phys.*, vol. 4, pp. 42-42, jul. 2002, doi: 10.1088/1367-2630/4/1/342.

[136]A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, y N. Gisin, «``Plug and play'' systems for quantum cryptography», *Appl. Phys. Lett.*, vol. 70, n.º 7, pp. 793-795, feb. 1997, doi: 10.1063/1.118224.

[137]R. Bedington, J. M. Arrazola, y A. Ling, «Progress in satellite quantum key distribution», *Npj Quantum Inf.*, vol. 3, n.º 1, p. 30, ago. 2017, doi: 10.1038/s41534-017-0031-5.

[138] G. Vallone *et al.*, «Experimental Satellite Quantum Communications», *Phys. Rev. Lett.*, vol. 115, n.º 4, p. 040502, jul. 2015, doi: 10.1103/PhysRevLett.115.040502.

[139]S. Pirandola, «Limits and Security of Free-Space Quantum Communications», *Phys. Rev. Res.*, vol. 3, n.º 1, p. 013279, mar. 2021, doi: 10.1103/PhysRevResearch.3.013279.

[140] H. Chou *et al.*, «Satellite-based Quantum Key Distribution over Atmospheric Channels: Reviews and Research Challenges». arXiv, 29 de julio de 2023. Accedido: 22 de agosto de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2308.00011

[141]N. Gisin, G. Ribordy, W. Tittel, y H. Zbinden, «Quantum Cryptography», *Rev. Mod. Phys.*, vol. 74, n.º 1, pp. 145-195, mar. 2002, doi: 10.1103/RevModPhys.74.145.

[142] P. W. Shor y J. Preskill, «Simple Proof of Security of the BB84 Quantum Key Distribution Protocol», *Phys. Rev. Lett.*, vol. 85, n.º 2, pp. 441-444, jul. 2000, doi: 10.1103/PhysRevLett.85.441.

[143] M. Koashi y J. Preskill, «Secure quantum key distribution with an uncharacterized source», *Phys. Rev. Lett.*, vol. 90, n.º 5, p. 057902, feb. 2003, doi: 10.1103/PhysRevLett.90.057902.

[144] D. Gottesman, H.-K. Lo, N. Lütkenhaus, y J. Preskill, «Security of quantum key distribution with imperfect devices». arXiv, 3 de septiembre de 2004. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/quant-ph/0212066

[145] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, y J.-W. Pan, «Secure quantum key distribution with realistic devices», *Rev. Mod. Phys.*, vol. 92, n.º 2, p. 025002, may 2020, doi: 10.1103/RevModPhys.92.025002.

[146] V. Scarani y C. Kurtsiefer, «The black paper of quantum cryptography: Real implementation problems», *Theor. Comput. Sci.*, vol. 560, pp. 27-32, dic. 2014, doi: 10.1016/j.tcs.2014.09.015.

[147] H.-K. Lo, M. Curty, y B. Qi, «Measurement-device-independent quantum key distribution», *Phys. Rev. Lett.*, vol. 108, n.º 13, p. 130503, mar. 2012, doi: 10.1103/PhysRevLett.108.130503.

[148] V. Zapatero *et al.*, «Advances in device-independent quantum key distribution», *Npj Quantum Inf.*, vol. 9, n.º 1, p. 10, feb. 2023, doi: 10.1038/s41534-023-00684-x.

[149] D. P. Nadlinger *et al.*, «Experimental quantum key distribution certified by Bell's theorem», *Nature*, vol. 607, n.º 7920, pp. 682-686, jul. 2022, doi: 10.1038/s41586-022-04941-5.

[150] B. Huttner, N. Imoto, N. Gisin, y T. Mor, «Quantum Cryptography with Coherent States», *Phys. Rev. A*, vol. 51, n.º 3, pp. 1863-1869, mar. 1995, doi: 10.1103/PhysRevA.51.1863.

[151] H.-K. Lo, X. Ma, y K. Chen, «Decoy State Quantum Key Distribution», *Phys. Rev. Lett.*, vol. 94, n.º 23, p. 230504, jun. 2005, doi: 10.1103/PhysRevLett.94.230504.

[152] V. Scarani, A. Acin, G. Ribordy, y N. Gisin, «Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations», *Phys. Rev. Lett.*, vol. 92, n.º 5, p. 057901, feb. 2004, doi: 10.1103/PhysRevLett.92.057901.

[153] H.-K. Lo, M. Curty, y K. Tamaki, «Secure Quantum Key Distribution», *Nat. Photonics*, vol. 8, n.º 8, pp. 595-604, ago. 2014, doi: 10.1038/nphoton.2014.149.

[154] S. Pirandola, «Capacities of repeater-assisted quantum communications». arXiv, 15 de agosto de 2017. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/1601.00966

[155] K. Azuma *et al.*, «Quantum repeaters: From quantum networks to the quantum internet». arXiv, 18 de julio de 2023. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2212.10820

[156] M. Lucamarini, Z. Yuan, J. F. Dynes, y A. J. Shields, «Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters», *Nature*, vol. 557, n.º 7705, pp. 400-403, may 2018, doi: 10.1038/s41586-018-0066-6.

[157] X.-B. Wang, Z.-W. Yu, y X.-L. Hu, «Sending or not sending: twin-field quantum key distribution with large misalignment error», *Phys. Rev. A*, vol. 98, n.º 6, p. 062323, dic. 2018, doi: 10.1103/PhysRevA.98.062323.

[158] Y. Liu *et al.*, «Experimental Twin-Field Quantum Key Distribution Over 1000 km Fiber Distance», *Phys. Rev. Lett.*, vol. 130, n.º 21, p. 210801, may 2023, doi: 10.1103/PhysRevLett.130.210801.

[159] J.-P. Chen *et al.*, «Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans», *Nat. Photonics*, vol. 15, n.º 8, pp. 570-575, ago. 2021, doi: 10.1038/s41566-021-00828-5.

[160] D. Ribezzo *et al.*, «Quantum Key Distribution over 100 km underwater optical fiber assisted by a Fast-Gated Single-Photon Detector». arXiv, 2 de marzo de 2023. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2303.01449

[161] H. Liu *et al.*, «Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km», *Phys. Rev. Lett.*, vol. 126, n.º 25, p. 250502, jun. 2021, doi: 10.1103/PhysRevLett.126.250502.

[162] Y.-C. Zhang *et al.*, «Continuous-variable QKD over 50km commercial fiber», *Quantum Sci. Technol.*, vol. 4, n.º 3, p. 035006, may 2019, doi: 10.1088/2058-9565/ab19d1.

[163]J.-P. Chen *et al.*, «Quantum key distribution over 658 km fiber with distributed vibration sensing», *Phys. Rev. Lett.*, vol. 128, n.º 18, p. 180502, may 2022, doi: 10.1103/PhysRevLett.128.180502.

[164] C.-H. F. Fung, K. Tamaki, y H.-K. Lo, «On the performance of two protocols: SARG04 and BB84», *Phys. Rev. A*, vol. 73, n.º 1, p. 012337, ene. 2006, doi: 10.1103/PhysRevA.73.012337.

[165] F. Grosshans y P. Grangier, «Continuous variable quantum cryptography using coherent states», *Phys. Rev. Lett.*, vol. 88, n.º 5, p. 057902, ene. 2002, doi: 10.1103/PhysRevLett.88.057902.

[166] D. Stucki *et al.*, «Continuous high speed coherent one-way quantum key distribution», *Opt. Express*, vol. 17, n.º 16, p. 13326, ago. 2009, doi: 10.1364/OE.17.013326.

[167] R. Trényi y M. Curty, «Zero-error attack against coherent-one-way quantum key distribution», *New J. Phys.*, vol. 23, n.º 9, p. 093005, sep. 2021, doi: 10.1088/1367-2630/ac1e41.

[168] Z. Zhang, X. Yuan, Z. Cao, y X. Ma, «Practical round-robin differential-phase-shift quantum key distribution», *New J. Phys.*, vol. 19, n.º 3, p. 033013, mar. 2017, doi: 10.1088/1367-2630/aa6274.

[169] A. Mizutani y G. Kato, «Security of round-robin differential-phase-shift quantum key distribution protocol with correlated light sources», *Phys. Rev. A*, vol. 104, n.º 6, p. 062611, dic. 2021, doi: 10.1103/PhysRevA.104.062611.

[170] A. K. Ekert, «Quantum cryptography based on Bell's theorem», *Phys. Rev. Lett.*, vol. 67, n.º 6, pp. 661-663, ago. 1991, doi: 10.1103/PhysRevLett.67.661.

[171] C. H. Bennett, G. Brassard, y N. D. Mermin, «Quantum cryptography without Bell's theorem», *Phys. Rev. Lett.*, vol. 68, n.º 5, pp. 557-559, feb. 1992, doi: 10.1103/PhysRevLett.68.557.

[172]D. Mayers y A. Yao, «Self testing quantum apparatus». arXiv, 13 de septiembre de 2004. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/quant-ph/0307205

[173]G. Guarda *et al.*, «BB84 decoy-state QKD protocol over long-distance optical fiber», en *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, Bucharest, Romania: IEEE, jul. 2023, pp. 1-4. doi: 10.1109/ICTON59386.2023.10207397.

[174] A. Boaron *et al.*, «Secure quantum key distribution over 421 km of optical fiber», *Phys. Rev. Lett.*, vol. 121, n.º 19, p. 190502, nov. 2018, doi: 10.1103/PhysRevLett.121.190502.

[175]E. Moschandreou, B. J. Rollick, B. Qi, y G. Siopsis, «Experimental decoy state BB84 quantum key distribution through a turbulent channel», *Phys. Rev. A*, vol. 103, n.º 3, p. 032614, mar. 2021, doi: 10.1103/PhysRevA.103.032614.

[176] S.-K. Liao *et al.*, «Satellite-to-ground quantum key distribution», *Nature*, vol. 549, n.º 7670, pp. 43-47, sep. 2017, doi: 10.1038/nature23655.

[177]S.-K. Liao *et al.*, «Satellite-Relayed Intercontinental Quantum Network», *Phys. Rev. Lett.*, vol. 120, n.º 3, p. 030501, ene. 2018, doi: 10.1103/PhysRevLett.120.030501.

[178] T. Schmitt-Manderbach *et al.*, «Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km», en *2007 European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*, Munich, Germany: IEEE, jun. 2007, pp. 1-1. doi: 10.1109/CLEOE-IQEC.2007.4386755.

[179]H.-L. Yin *et al.*, «Measurement device independent quantum key distribution over 404 km optical fibre», *Phys. Rev. Lett.*, vol. 117, n.º 19, p. 190501, nov. 2016, doi: 10.1103/PhysRevLett.117.190501.

[180] Y.-L. Tang *et al.*, «Measurement-Device-Independent Quantum Key Distribution over 200 km», *Phys. Rev. Lett.*, vol. 113, n.º 19, p. 190501, nov. 2014, doi: 10.1103/PhysRevLett.113.190501.

[181]Y. Cao *et al.*, «Long-distance free-space measurement-device-independent quantum key distribution», *Phys. Rev. Lett.*, vol. 125, n.º 26, p. 260503, dic. 2020, doi: 10.1103/PhysRevLett.125.260503.

[182] B. Korzh *et al.*, «Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre», *Nat. Photonics*, vol. 9, n.º 3, pp. 163-168, mar. 2015, doi: 10.1038/nphoton.2014.327.

[183] H. Shibata, T. Honjo, y K. Shimizu, «Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors», *Opt. Lett.*, vol. 39, n.º 17, p. 5078, sep. 2014, doi: 10.1364/OL.39.005078.

[184] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, K. Tamaki, y Y. Yamamoto, «Quantum key distribution over 40 dB channel loss using superconducting single photon detectors».

[185] J.-Y. Guan *et al.*, «Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution», *Phys. Rev. Lett.*, vol. 114, n.º 18, p. 180502, may 2015, doi: 10.1103/PhysRevLett.114.180502.

[186] «Products | Quantum Key Distribution | TOSHIBA DIGITAL SOLUTIONS CORPORATION». https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html (accedido 5 de septiembre de 2023).

[187] «Cerberis XG QKD System», *ID Quantique*. https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/ (accedido 6 de septiembre de 2023).

[188] «MagiQ QPN™| Network Security | Somerville, MA», *MagiQ Technologies*. https://www.magiqtech.com/solutions/network-security/ (accedido 6 de septiembre de 2023).

[189] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, y V. Makarov, «Hacking commercial quantum cryptography systems by tailored bright illumination», *Nat. Photonics*, vol. 4, n.º 10, pp. 686-689, oct. 2010, doi: 10.1038/nphoton.2010.214.

[190] S. Wehner, D. Elkouss, y R. Hanson, «Quantum internet: A vision for the road ahead», *Science*, vol. 362, n.º 6412, p. eaam9288, oct. 2018, doi: 10.1126/science.aam9288.

[191] D. Cuomo, M. Caleffi, y A. S. Cacciapuoti, «Towards a Distributed Quantum Computing Ecosystem», *IET Quantum Commun.*, vol. 1, n.º 1, pp. 3-8, jul. 2020, doi: 10.1049/iet-qtc.2020.0002.

[192] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, y W. K. Wootters, «Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels», *Phys. Rev. Lett.*, vol. 70, n.º 13, pp. 1895-1899, mar. 1993, doi: 10.1103/PhysRevLett.70.1895.

[193] A. Singh, K. Dev, H. Siljak, H. D. Joshi, y M. Magarini, «Quantum Internet—Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions», *IEEE Commun. Surv. Tutor.*, vol. 23, n.º 4, pp. 2218-2247, 2021, doi: 10.1109/COMST.2021.3109944.

[194] L.-M. Duan, M. D. Lukin, J. I. Cirac, y P. Zoller, «Long-distance quantum communication with atomic ensembles and linear optics», *Nature*, vol. 414, n.º 6862, pp. 413-418, nov. 2001, doi: 10.1038/35106500.

[195] N. Sangouard, C. Simon, H. de Riedmatten, y N. Gisin, «Quantum repeaters based on atomic ensembles and linear optics». arXiv, 23 de junio de 2009. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/0906.2699

[196] K. Azuma, K. Tamaki, y H.-K. Lo, «All-photonic quantum repeaters», *Nat. Commun.*, vol. 6, n.º 1, p. 6787, abr. 2015, doi: 10.1038/ncomms7787.

[197] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, y L. Jiang, «Optimal architectures for long distance quantum communication», *Sci. Rep.*, vol. 6, n.º 1, p. 20463, feb. 2016, doi: 10.1038/srep20463.

[198] K. Heshami *et al.*, «Quantum memories: emerging applications and recent advances», *J. Mod. Opt.*, vol. 63, n.º 20, pp. 2005-2028, nov. 2016, doi: 10.1080/09500340.2016.1148212.

[199] M. Ruf, N. H. Wan, H. Choi, D. Englund, y R. Hanson, «Quantum networks based on color centers in diamond», *J. Appl. Phys.*, vol. 130, n.º 7, p. 070901, ago. 2021, doi: 10.1063/5.0056534.

[200] D. P. DiVincenzo y IBM, «The Physical Implementation of Quantum Computation», *Fortschritte Phys.*, vol. 48, n.º 9-11, pp. 771-783, sep. 2000, doi: 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.

[201] C. Simon *et al.*, «Quantum Memories. A Review based on the European Integrated Project "Qubit Applications (QAP)"», *Eur. Phys. J. D*, vol. 58, n.º 1, pp. 1-22, may 2010, doi: 10.1140/epjd/e2010-00103-y.

[202] F. Rozpędek *et al.*, «Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission», *Phys. Rev. A*, vol. 99, n.º 5, p. 052330, may 2019, doi: 10.1103/PhysRevA.99.052330.

[203] L. Ma, O. Slattery, y X. Tang, «Optical quantum memory based on electromagnetically induced transparency», *J. Opt. 2010*, vol. 19, n.º 4, p. 043001, abr. 2017, doi: 10.1088/2040-8986/19/4/043001.

[204] W. Tittel *et al.*, «Photon-Echo Quantum Memory». arXiv, 1 de octubre de 2008. doi: 10.48550/arXiv.0810.0172.

[205] M. Gündoğan *et al.*, «Topical White Paper: A Case for Quantum Memories in Space». arXiv, 19 de noviembre de 2021. Accedido: 7 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2111.09595

[206] A. I. Lvovsky, B. C. Sanders, y W. Tittel, «Optical quantum memory». arXiv, 16 de abril de 2010. Accedido: 8 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/1002.4659

[207] M. Guo, S. Liu, W. Sun, M. Ren, F. Wang, y M. Zhong, «Rare-earth quantum memories: The experimental status quo», *Front. Phys.*, vol. 18, n.º 2, p. 21303, abr. 2023, doi: 10.1007/s11467-022-1240-8.

[208] O. Katz y O. Firstenberg, «Light storage for one second in room-temperature alkali vapor», *Nat. Commun.*, vol. 9, n.º 1, Art. n.º 1, may 2018, doi: 10.1038/s41467-018-04458-4.

[209] Y.-W. Cho *et al.*, «Highly efficient optical quantum memory with long coherence time in cold atoms», *Optica*, vol. 3, n.º 1, pp. 100-107, ene. 2016, doi: 10.1364/OPTICA.3.000100.

[210] Y. O. Dudin, L. Li, y A. Kuzmich, «Light storage on the time scale of a minute», *Phys. Rev. A*, vol. 87, n.º 3, p. 031801, mar. 2013, doi: 10.1103/PhysRevA.87.031801.

[211] E. Bersin, M. Walsh, S. L. Mouradian, M. E. Trusheim, T. Schröder, y D. Englund, «Individual control and readout of qubits in a sub-diffraction volume», *Npj Quantum Inf.*, vol. 5, n.º 1, Art. n.º 1, may 2019, doi: 10.1038/s41534-019-0154-y.

[212] C. E. Bradley *et al.*, «A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute», *Phys. Rev. X*, vol. 9, n.º 3, p. 031045, sep. 2019, doi: 10.1103/PhysRevX.9.031045.

[213] C. A. Perez-Delgado y P. Kok, «What is a quantum computer, and how do we build one?», *Phys. Rev. A*, vol. 83, n.º 1, p. 012303, ene. 2011, doi: 10.1103/PhysRevA.83.012303.

[214] Y. Lee, E. Bersin, A. Dahlberg, S. Wehner, y D. Englund, «A quantum router architecture for high-fidelity entanglement flows in quantum networks», *Npj Quantum Inf.*, vol. 8, n.º 1, p. 75, jun. 2022, doi: 10.1038/s41534-022-00582-8.

[215] M. Caleffi y A. S. Cacciapuoti, «Quantum Switch for the Quantum Internet: Noiseless Communications through Noisy Channels», *IEEE J. Sel. Areas Commun.*, vol. 38, n.º 3, pp. 575-588, mar. 2020, doi: 10.1109/JSAC.2020.2969035.

[216] C. Wang, A. Rahman, R. Li, M. Aelmans, y K. Chakraborty, «Application Scenarios for the Quantum Internet», Internet Engineering Task Force, Internet Draft draft-irtf-qirg-quantum-internet-use-cases-13, jun. 2022. Accedido: 5 de septiembre de 2023. [En línea]. Disponible en: https://datatracker.ietf.org/doc/draft-irtf-qirg-quantum-internet-use-cases-13

[217] M. Caleffi *et al.*, «Distributed Quantum Computing: a Survey». arXiv, 20 de diciembre de 2022. Accedido: 1 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2212.10609

[218] J. F. Fitzsimons, «Private quantum computation: an introduction to blind quantum computing and related protocols», *Npj Quantum Inf.*, vol. 3, n.º 1, Art. n.º 1, jun. 2017, doi: 10.1038/s41534-017-0025-3.

[219] D.-Q. Cai *et al.*, «Implementation of an E-Payment Security Evaluation System Based on Quantum Blind Computing», *Int. J. Theor. Phys.*, vol. 59, n.º 9, pp. 2757-2772, sep. 2020, doi: 10.1007/s10773-020-04536-8.

[220] P. Drmota *et al.*, «Verifiable blind quantum computing with trapped ions and single photons». arXiv, 4 de mayo de 2023. doi: 10.48550/arXiv.2305.02936.

[221] M. Ben-Or y A. Hassidim, «Fast quantum byzantine agreement», en *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, Baltimore MD USA: ACM, may 2005, pp. 481-485. doi: 10.1145/1060590.1060662.

[222] M. Ganz, «Quantum Leader Election». arXiv, 20 de octubre de 2016. Accedido: 4 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/0910.4952

[223] W. Kozlowski *et al.*, «Architectural Principles for a Quantum Internet», Internet Engineering Task Force, Request for Comments RFC 9340, mar. 2023. doi: 10.17487/RFC9340.

[224] «Quantum Key Distribution (QKD)», *ETSI*. https://www.etsi.org/technologies/quantum-key-distribution (accedido 6 de septiembre de 2023).

[225] «Press Release < News < HOME». https://www.sktelecom.com/en/press/press_detail.do?idx=1563 (accedido 15 de septiembre de 2023).

[226] dev, «Home», *OpenQKD*. https://openqkd.eu/ (accedido 6 de septiembre de 2023).

[227] «CIVIQ – CIVIQ». https://civiquantum.eu/ (accedido 8 de septiembre de 2023).

[228] «Quantum Internet Alliance | Building a Global Quantum Internet Made in Europe», *Quantum Internet Alliance*. https://quantuminternetalliance.org/ (accedido 8 de septiembre de 2023).

[229] «Quantum Communications Hub», *Quantum Communications Hub*. https://www.quantumcommshub.net/ (accedido 11 de septiembre de 2023).

[230] R. S. Tessinari, R. I. Woodward, y A. J. Shields, «Software-defined quantum network using a QKD-secured SDN controller and encrypted messages». arXiv, 22 de mayo de 2023. Accedido: 11 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2305.12893

[231]R. S. Tessinari *et al.*, «Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the Bristol City 5GUK test network», en *45th European Conference on Optical Communication (ECOC 2019)*, Dublin, Ireland: Institution of Engineering and Technology, 2019, p. 299 (4 pp.)-299 (4 pp.). doi: 10.1049/cp.2019.1033.

[232] V. Martin *et al.*, «The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure», en *OSA Advanced Photonics Congress (AP) 2019 (IPR, Networks, NOMA, SPPCom, PVLED)*, Burlingame, California: OSA, 2019, p. QtW3E.5. doi: 10.1364/NETWORKS.2019.QtW3E.5.

[233] V. Martin *et al.*, «Quantum technologies in the telecommunications industry», *EPJ Quantum Technol.*, vol. 8, n.º 1, p. 19, dic. 2021, doi: 10.1140/epjqt/s40507-021-00108-9.

[234] T. Ferreira Da Silva, G. B. Xavier, G. P. Temporao, y J. P. Von Der Weid, «Impact of Raman Scattered Noise from Multiple Telecom Channels on Fiber-Optic Quantum Key Distribution Systems», *J. Light. Technol.*, vol. 32, n.º 13, pp. 2332-2339, jul. 2014, doi: 10.1109/JLT.2014.2322108.

[235] «The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future», 5 de julio de 2023. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (accedido 8 de septiembre de 2023).

[236] D. Ribezzo *et al.*, «Deploying an inter-European quantum network», *Adv. Quantum Technol.*, vol. 6, n.º 2, p. 2200061, feb. 2023, doi: 10.1002/qute.202200061.

[237] J. P, «Chinese Quantum Companies and National Strategy 2023», *The Quantum Insider*, 13 de abril de 2023. https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/ (accedido 8 de septiembre de 2023).

[238] «Is China a Leader in Quantum Technologies?», *ChinaPower Project*, 14 de agosto de 2023. https://chinapower.csis.org/china-quantum-technology/ (accedido 8 de septiembre de 2023).

[239] «Translation: 14th Five-Year Plan for National Informatization – Dec. 2021», *DigiChina*. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/ (accedido 8 de septiembre de 2023).

[240] M. Sasaki *et al.*, «Field test of quantum key distribution in the Tokyo QKD Network», *Opt. Express*, vol. 19, n.º 11, p. 10387, may 2011, doi: 10.1364/OE.19.010387.

[241] «Q-NEXT». https://q-next.org/ (accedido 11 de septiembre de 2023).

[242] «Center for Quantum Networks», 9 de junio de 2023. https://cqn-erc.org/ (accedido 11 de septiembre de 2023).

[243] G. E. O. of M. and Communications, «QHAN». https://hqan.illinois.edu (accedido 11 de septiembre de 2023).

[244] C. Wang, «Quantum secure direct communication: Intersection of communication and cryptography», *Fundam. Res.*, vol. 1, n.º 1, pp. 91-92, ene. 2021, doi: 10.1016/j.fmre.2021.01.002.

[245] C. H. Bennett, G. Brassard, C. Crépeau, y M.-H. Skubiszewska, «Practical Quantum Oblivious Transfer», en *Advances in Cryptology — CRYPTO '91*, J. Feigenbaum,

Ed., en Lecture Notes in Computer Science, vol. 576. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 351-366. doi: 10.1007/3-540-46766-1_29.

[246] M. B. Santos, P. Mateus, y A. N. Pinto, «Quantum oblivious transfer: a short review», *Entropy*, vol. 24, n.º 7, p. 945, jul. 2022, doi: 10.3390/e24070945.

[247] M. Herrero-Collantes y J. C. Garcia-Escartin, «Quantum Random Number Generators», *Rev. Mod. Phys.*, vol. 89, n.º 1, p. 015004, feb. 2017, doi: 10.1103/RevModPhys.89.015004.

[248] W. Wang *et al.*, «Fully-Passive Quantum Key Distribution», *Phys. Rev. Lett.*, vol. 130, n.º 22, p. 220801, may 2023, doi: 10.1103/PhysRevLett.130.220801.

[249] J. Bouda, M. Pivoluska, M. Plesch, y C. Wilmott, «Weak randomness seriously limits the security of quantum key distribution», *Phys. Rev. A*, vol. 86, n.º 6, p. 062308, dic. 2012, doi: 10.1103/PhysRevA.86.062308.

[250] A. Sinha, E. R. Henderson, J. M. Henderson, E. C. Larson, y M. A. Thornton, «A programmable true random number generator using commercial quantum computers», en *Quantum Information Science, Sensing, and Computation XV*, M. L. Fanto, M. Hayduk, E. Donkor, y C. M. Torres, Eds., Orlando, United States: SPIE, jun. 2023, p. 7. doi: 10.1117/12.2663497.

[251]I. T. L. Computer Security Division, «Entropy as a Service | CSRC | CSRC», *CSRC | NIST*, 2 de septiembre de 2016. https://csrc.nist.gov/Projects/entropy-as-a-service (accedido 11 de septiembre de 2023).

[252] C. L. Degen, F. Reinhard, y P. Cappellaro, «Quantum sensing», *Rev. Mod. Phys.*, vol. 89, n.º 3, p. 035002, jul. 2017, doi: 10.1103/RevModPhys.89.035002.

[253] M. Krelina, «Quantum technology for military applications», *EPJ Quantum Technol.*, vol. 8, dic. 2021, doi: 10.1140/epjqt/s40507-021-00113-y.

[254] «14 Companies Focused on Quantum Sensing and Manufacturing Superior Instrumentation To Revolutionize The Industry». https://thequantuminsider.com/2021/02/18/14-quantum-sensor-companies-manufacturing-superior-instrumentation-to-revolutionize-the-industry/ (accedido 19 de septiembre de 2023).

[255] «Quantum Sensors Market - Companies, Trends & Share». https://www.mordorintelligence.com/industry-reports/quantum-sensors-market (accedido 19 de septiembre de 2023).

[256] S. Pandey, «Hypersonic Bose–Einstein condensates in accelerator rings».

[257] D. Kim, M. I. Ibrahim, C. Foy, M. E. Trusheim, R. Han, y D. R. Englund, «A CMOS-integrated quantum sensor based on nitrogen–vacancy centres», *Nat. Electron.*, vol. 2, n.º 7, pp. 284-289, jul. 2019, doi: 10.1038/s41928-019-0275-5.

[258] W. Yang, D. B. Conkey, B. Wu, D. Yin, A. R. Hawkins, y H. Schmidt, «Atomic spectroscopy on a chip», *Nat. Photonics*, vol. 1, n.º 6, Art. n.º 6, jun. 2007, doi: 10.1038/nphoton.2007.74.

[259] V. Giovannetti, S. Lloyd, y L. Maccone, «Advances in Quantum Metrology», *Nat. Photonics*, vol. 5, n.º 4, pp. 222-229, abr. 2011, doi: 10.1038/nphoton.2011.35.

[260] F. Wolfgramm, «Atomic quantum metrology with narrowband entangled and squeezed states of light», Ph.D. Thesis, Universitat Politècnica de Catalunya, 2012. Accedido: 19 de septiembre de 2023. [En línea]. Disponible en: https://www.tdx.cat/handle/10803/98460

[261]V. Giovannetti, S. Lloyd, y L. Maccone, «Quantum-Enhanced Measurements: Beating the Standard Quantum Limit», *Science*, vol. 306, n.º 5700, pp. 1330-1336, nov. 2004, doi: 10.1126/science.1104149.

[262] Z. Zhang y Q. Zhuang, «Distributed Quantum Sensing». arXiv, 29 de octubre de 2020. Accedido: 6 de septiembre de 2023. [En línea]. Disponible en: http://arxiv.org/abs/2010.14744

[263] «Our latest research deliverable D1.4 "Hexa-X architecture for B5G/6G networks – final release" has been published - Hexa-X», 8 de agosto de 2023. https://hexa-x.eu/our-latest-research-deliverable-d1-4-hexa-x-architecture-for-b5g-6g-networks-final-release-has-been-published/ (accedido 13 de septiembre de 2023).

[264] «Quantum-Assisted Sensing and Readout». https://www.darpa.mil/program/quantum-assisted-sensing-and-readout (accedido 19 de septiembre de 2023).

[265] «Rydberg Technologies», *Rydberg Technologies*. https://www.rydbergtechnologies.com (accedido 6 de septiembre de 2023).

[266] L. W. Bussey, A. Winterburn, M. Menchetti, F. Burton, y T. Whitley, «Rydberg RF Receiver Operation to Track RF Signal Fading and Frequency Drift», *J. Light. Technol.*, vol. 39, n.º 24, pp. 7813-7820, dic. 2021, doi: 10.1109/JLT.2021.3098348.

[267] S. Magaletti, L. Mayer, J.-F. Roch, y T. Debuisschert, «A quantum radio frequency signal analyzer based on nitrogen vacancy centers in diamond», *Commun. Eng.*, vol. 1, n.º 1, p. 19, jul. 2022, doi: 10.1038/s44172-022-00017-4.

[268] M. Jing *et al.*, «Atomic superheterodyne receiver based on microwave-dressed Rydberg spectroscopy», *Nat. Phys.*, vol. 16, n.º 9, Art. n.º 9, sep. 2020, doi: 10.1038/s41567-020-0918-5.

[269] «Optical atomic clocks», *NPLWebsite*. https://www.npl.co.uk/time-frequency/optical-atomic-clocks (accedido 6 de septiembre de 2023).

[270] «Towards the optical second: verifying optical clocks at the SI limit». https://opg.optica.org/optica/fulltext.cfm?uri=optica-6-4-448&id=408936 (accedido 19 de septiembre de 2023).

[271]J. Shi y S. Shen, «A clock synchronization method based on quantum entanglement», *Sci. Rep.*, vol. 12, n.º 1, p. 10185, jun. 2022, doi: 10.1038/s41598-022-14087-z.

[272] P. Kómár *et al.*, «A quantum network of clocks», *Nat. Phys.*, vol. 10, n.º 8, pp. 582-587, ago. 2014, doi: 10.1038/nphys3000.

[273] B. Koczor, S. Endo, T. Jones, Y. Matsuzaki, y S. C. Benjamin, «Variational-state quantum metrology», *New J. Phys.*, vol. 22, n.º 8, p. 083038, ago. 2020, doi: 10.1088/1367-2630/ab965e.

[274] C. D. Marciniak *et al.*, «Optimal metrology with programmable quantum sensors», *Nature*, vol. 603, n.º 7902, pp. 604-609, mar. 2022, doi: 10.1038/s41586-022-04435-4.