QUIXOTE

WEBINAR · RED CERVERA QUIXOTE

Presentación de la Red de Excelencia Cervera QUIXOTE en Tecnologías Cuánticas

14 de octubre de 2026

ORGANIZA planetic

[FIDESOL] gradiant itecam i2cat LORTEK MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES CDTI INNOVACIÓN

Centro de Excelencia Cervera

Índice

01 Presentación de la Red de Excelencia QUIXOTE

02 Casos de uso

03 Objetivos de i2CAT en QUIXOTE

04 Objetivos de GRADIANT en QUIXOTE

05 Objetivos de LORTEK en QUIXOTE

06 Objetivos de FIDESOL en QUIXOTE

07 Objetivos de ITECAM en QUIXOTE

08 Cierre

Presentación Red Quixote

Red de Excelencia Cervera para la investigación en Tecnologías Quanticas para Infraestructura experimental orientada a la soberanía tecnológica en entornos estratégicos

Convocatoria Cervera CCTT 2025.

Financiado por el CDTI – Ministerio de Ciencia, Innovación y Universidades.

Misión

Consolidar un ecosistema de excelencia científico-tecnológica en el ***ámbito de las tecnologías cuánticas aplicadas a la defensa y la seguridad****, capaz de generar* ***conocimiento avanzado y soluciones innovadoras*** *que fortalezcan la* ***autonomía estratégica nacional, la superioridad en el procesamiento de información y la resiliencia de las capacidades críticas.***

QUIXOTE

Red de Excelencia Cervera QUIXOTE

Objetivos estratégicos

- **Liderazgo tecnológico** Consolidar a QUIXOTE como referente nacional en tecnologías cuánticas aplicadas a la defensa y la seguridad.
- **Conexión y difusión** Comunicar avances a industria, academia, autoridades de defensa y sociedad en general.
- **Talento y cultura cuántica** Atraer, formar y retener talento especializado en el ecosistema cuántico nacional.
- **Proyección global** Posicionar el proyecto en redes internacionales de I+D cuántica: Euro-QuIC, EDF, Horizon Europe, DIANA/OTAN.

Objetivos tecnológicos

- **Redes cuánticas globales** Superación de las limitaciones de alcance de las comunicaciones cuánticas (interoperabilidad y optimización).
- **Tecnología habilitante** Desarrollo de tecnología cuántica habilitante para redes de comunicaciones.
- **Redes quantum-safe** resilientes en entornos de movilidad táctica y estratégica.
- **Plataformas de sensado** para aplicaciones críticas en defensa y seguridad.
- **Ruguerización** de sistemas de sensado cuántico para despliegue en entornos estratégicos reales.

Red de Excelencia Cervera QUIXOTE

Impacto

2023-2025 | **2026-2028**

+30% masa crítica investigadora

+20 empleos netos de alta cualificación

un **aumento** ingresos de I+D cuántica, **x2** si son proyectos internacionales

x2 de oportunidades de colaboración con empresas

x2 publicaciones, + patentes o modelos de utilidad

+1 nueva EBT

Un **efecto tractor sobre empresas** industriales, TIC, de defensa y de seguridad

Transferencia a pymes y grandes empresas mediante casos de uso duales

Mayor competitividad por la optimización de procesos con algoritmos cuánticos

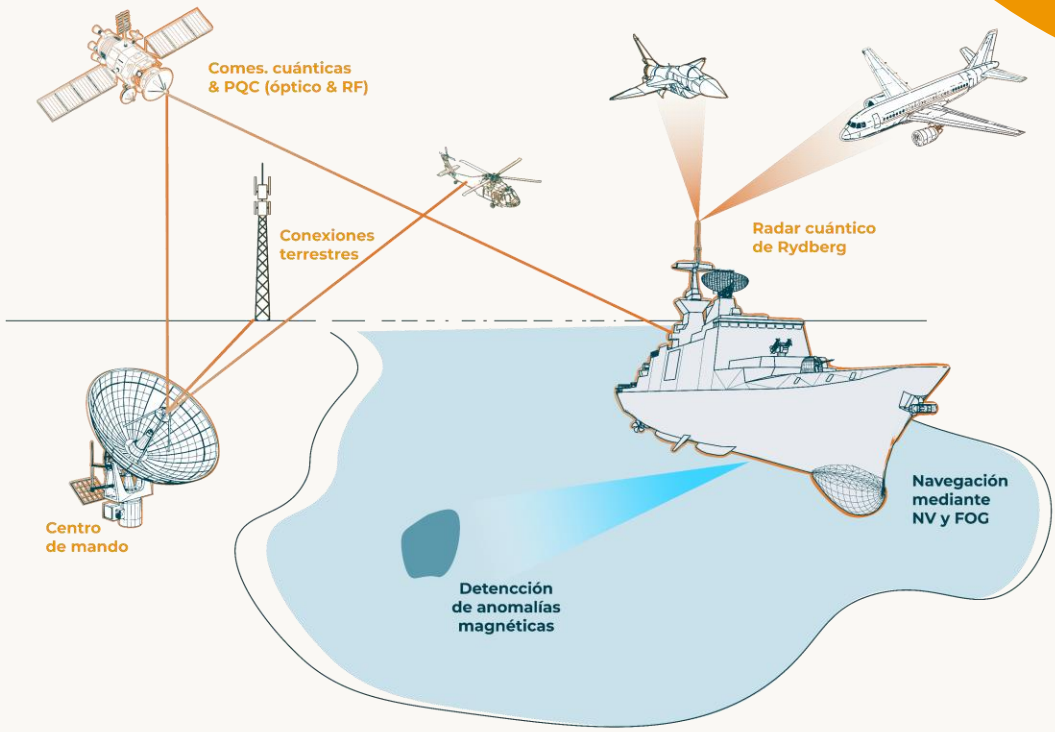
Derivada sobre **impacto medioambiental**

Red de Excelencia Cervera QUIXOTE

Pilares de investigación

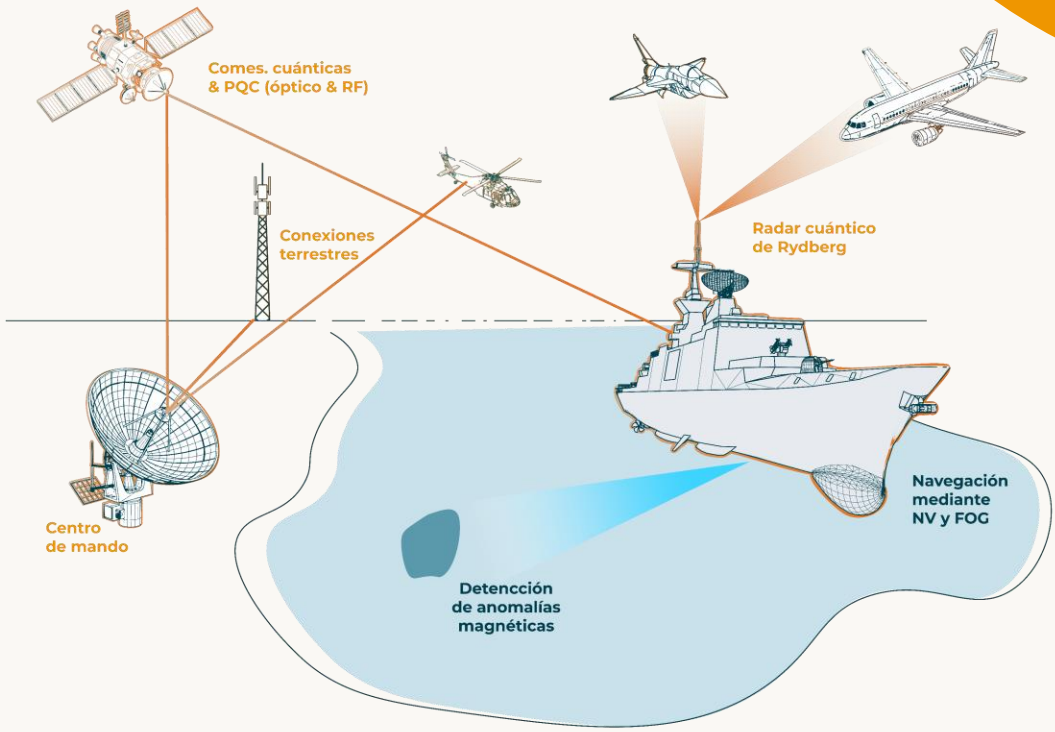
Pilar I — Comunicaciones cuánticamente seguras

Las comunicaciones cuánticas utilizan las leyes de la física para proteger la información de forma inquebrantable: cualquier intento de interceptación deja huella y puede ser detectado. QUIXOTE trabaja en dos tecnologías complementarias: la **distribución cuántica de claves (QKD)**, que asegura los canales de comunicación mediante fotones individuales, y la **criptografía post-cuántica híbrida (PQC)**, que protege las comunicaciones incluso cuando no hay enlace óptico disponible. **El objetivo es blindar las redes de mando y control frente a las amenazas cibernéticas presentes y futuras**.



Pilar II — Sensórica y navegación cuántica

Los sensores cuánticos alcanzan niveles de precisión imposibles con tecnología clásica. En QUIXOTE se investigan tres líneas: **magnetómetros de centros NV** en diamante para navegar por cartografía magnética sin GPS; **sensores de Rydberg** para detección ultrasensible de señales de radiofrecuencia; y **giróscopos de fibra óptica** operados en régimen cuántico para navegación autónoma en plataformas terrestres, navales y aéreas. Todas las tecnologías se desarrollan pensando en su integración y despliegue en entornos estratégicos reales.

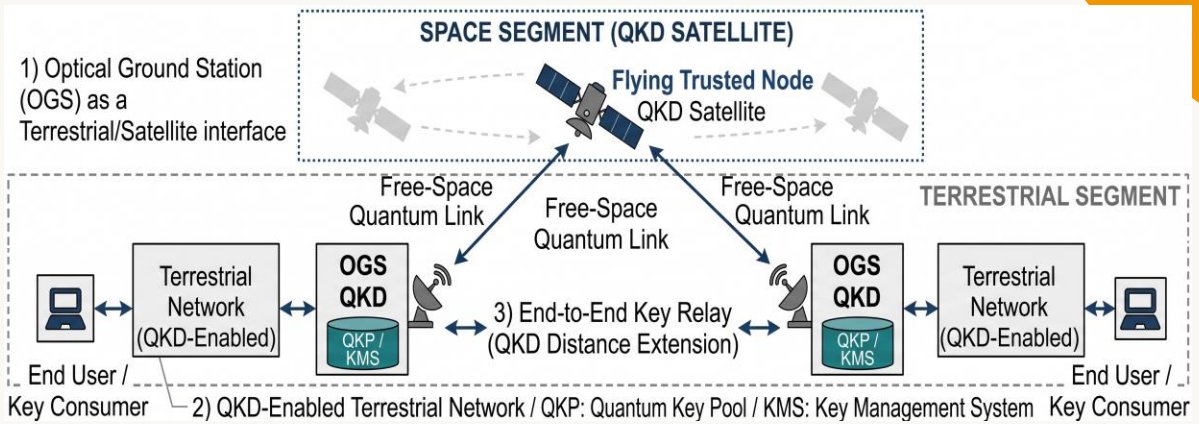


Casos de uso objetivo

Caso 1: Comunicaciones seguras E2E

Comunicaciones cuánticamente seguras entre centros de mando / nodos críticos remotos

- **Conectividad segura extremo a extremo:** conexión de infraestructuras críticas y centros de mando geográficamente separados mediante arquitectura híbrida de distribución cuántica de claves (QKD) y criptografía poscuántica (PQC).
- **Integración satélite-terrestre:** despliegue de comunicaciones QKD a escala global mediante un satélite que actúa como nodo confiable, interoperable e integrable con la red QKD terrestre, extendiendo la infraestructura de comunicaciones seguras de extremo a extremo.

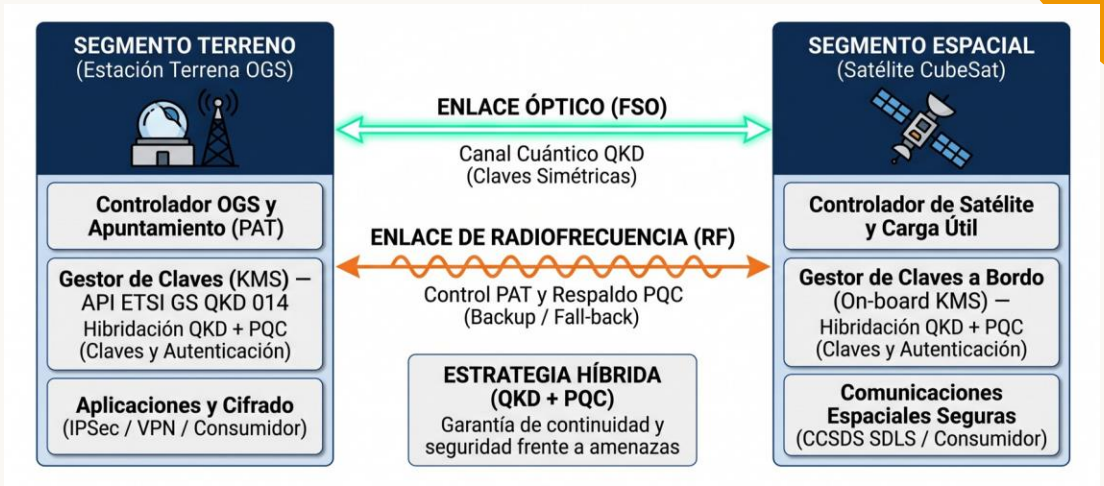


- **Cobertura Global sin Límites de Fibra Óptica:** Uso de satélites LEO como Flying Trusted Nodes (relevo de claves, key-relay) para conectar centros remotos.
- **Seguridad Híbrida Dinámica (QKD + PQC):** QKD aporta el secreto físico; PQC autentica y protege terminales sin enlace óptico directo.
- **Resiliencia Continua (PQC Fall-back):** Conmutación automática a claves PQC puras ante la interrupción del canal cuántico, sin cortes de servicio de suministro de clave segura.
- **Escalabilidad Táctica y Multiusuario:** Túneles VPN híbridos que extienden la protección a unidades móviles y habilitan salas de crisis simultáneas.
- **Integración Directa e Interoperable:** Compatible con infraestructuras estándar (IPsec, ETSI GS QKD 014), evitando disrupciones en redes operativas.

Caso 2: Comunicaciones satelitales seguras

Comunicaciones Satelitales Seguras en Arquitectura satelital Híbrida RF-Óptica

- **Protección de los sistemas satelitales:** securización de las propias comunicaciones satelitales, mediante una arquitectura híbrida QKD+PQC que protege los canales críticos de telemetría, seguimiento y control (TT&C) y de servicio o payload.
- **Extensión a otros escenarios de comunicación:** aplicación de este enfoque de seguridad a enlaces entre terminales móviles terrestres y plataformas aéreas, además de las comunicaciones satelitales.

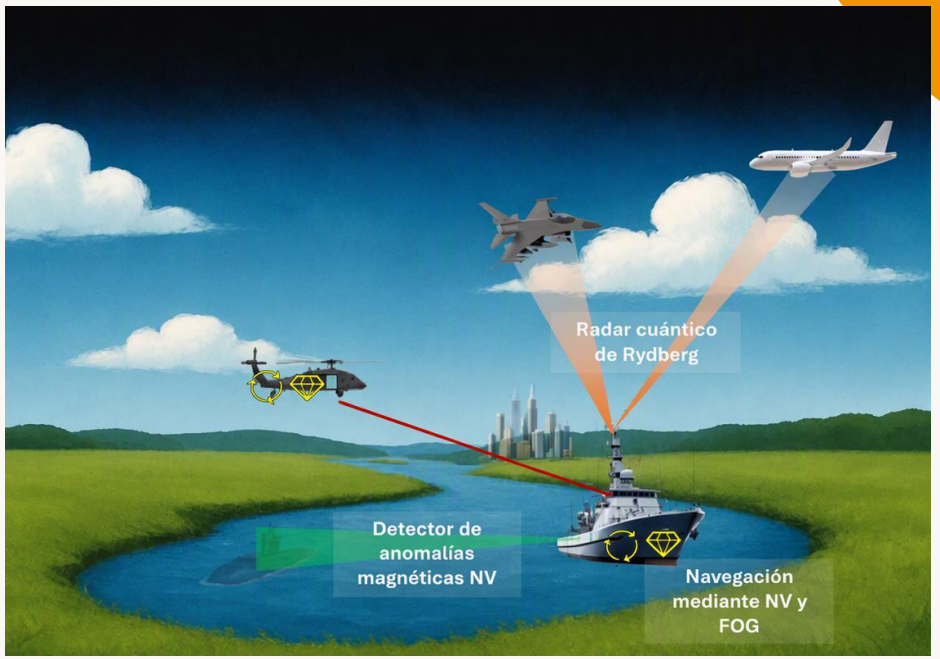


- **El Satélite como Consumidor Activo:** Uso de QKD para el cifrado directo del tráfico de carga útil (servicio, Payload) y de los comandos críticos (TT&C).
- **Apuntamiento Híbrido Asistido (PAT):** Adquisición rápida del haz óptico utilizando el canal RF auxiliar para sincronización y efemérides.
- **Seguridad Híbrida Integral (QKD + PQC):** QKD cifra de forma incondicional; PQC garantiza la autenticación robusta de todos los canales (tanto FSO como RF).
- **Conmutación Inteligente (PQC Fall-back):** Transición automática a protocolos PQC en caso de indisponibilidad de claves QKD, asegurando suficiente seguridad cuántica en todo momento.
- **Operabilidad en Hardware Constreñido (SWaP):** Arquitectura compatible con sistemas estándar (ETSI GS QKD 014 y SDR), viable para plataformas tipo CubeSat o microsatelite.

Caso 3: Redes de sensores cuánticos PNT

Fusión descentralizada de sensores cuánticos en nodos IoT quantum-safe

- **Detección de anomalías espectrales:** detección anticipada de amenazas radioeléctricas o magnéticas, mediante la combinación de receptores de Rydberg y magnetómetros cuánticos de diamante.
- **Localización de señales de radiofrecuencia y magnéticas:** arquitecturas y metodologías de procesado para detección de ángulo de llegada (Angle-of-Arrival, AoA) en radiofrecuencia y descomposición vectorial de campos magnéticos.
- **Navegación asistida por sensores cuánticos:** integración de metodologías de navegación resiliente basadas en giróscopos de fibra óptica (FOG) y cartografía magnética.
- **Acceso *quantum-safe* a la información:** implementación de red de nodos IoT cuánticos con securización PQC.



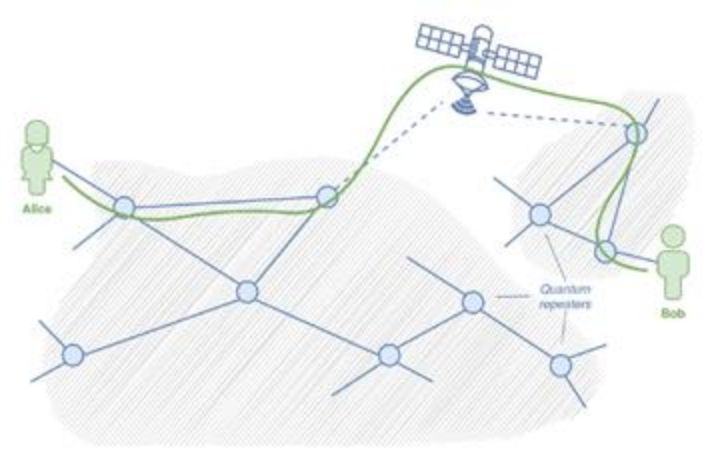
- **Sensores cuánticos de átomos de Rydberg:** Empleo como frontal RF opto-atómico, ampliamente sintonizable en canales de MHz a THz, con capacidad de detección AoA y demodulación RF. Integrable en radares resintonizables.
- **Magnetómetros cuánticos de diamante:** Localización de anomalías magnéticas mediante proyección vectorial de las señales. Estudio de metodologías para navegación, usando los centros nitrógeno-vacancia (NV) como brújula cuántica.
- **Giróscopos de fibra óptica (FOG):** Uso para medición de aceleración, con potencial hibridación con acelerómetros clásicos. Mejora de sensibilidad con estados ópticos cuánticos.

Objetivos de i2CAT

Comunicaciones cuánticamente seguras

Comunicaciones cuánticamente seguras

Redes satelitales cuánticas: construyendo la internet cuántica



Redes cuánticas (quantum networks, QN)

- Computación cuántica distribuida
- Computación segura en la nube (blind computing)
- Sincronización de relojes ópticos
- Sensórica cuántica distribuida y conectada
- Redes basadas en la distribución de **ENTRELAZAMIENTO**

Los satélites permiten superar los límites de distancia de la comunicación cuántica.



<u>Seguridad a prueba de cuántica</u> (**quantum-safe security, QSS)**

- Comunicaciones incondicionalmente seguras a largas distancias
- Combinación de segmento terrestre y espacial
- Comunicaciones cuánticamente seguras (ej: **QKD, QSDC, ...**)

Comunicaciones cuánticamente seguras

Objetivos estratégicos que orientan las contribuciones en QUIXOTE

Objetivo general: Comunicaciones cuánticamente seguras E2E

Desarrollar y evaluar soluciones de comunicaciones cuánticamente seguras de extremo a extremo, integrando redes QKD terrestres y satelitales mediante simulación, emulación y prototipado experimental, incluyendo la protección de las comunicaciones del propio segmento espacial.

Ejes de investigación

1. Seguridad Cuántica: QKD, QSDC, comunicaciones basadas en entrelazamiento, integración QKD-PQC y seguridad cuántica asistida por satélite.

2. Internet Cuántica: Repetidores y memorias cuánticas, distribución de entrelazamiento, teletransporte y nuevas arquitecturas de comunicación que reduzcan la dependencia de nodos confiables.

3. Canales Ópticos Cuánticos (FSO): Enlaces ópticos cuánticos en espacio libre, caracterización atmosférica, apuntado y seguimiento (APT), óptica adaptativa e integración de enlaces RF-ópticos.

4. Simulación y Emulación de Redes Cuánticas: Modelado y evaluación de redes QKD terrestres y satelitales, arquitecturas QKDSat y redes de repetidores, con evaluación del rendimiento E2E y soporte al diseño y validación de prototipos experimentales.



Fundamentos básicos QKD

QKD: Quantum Key Distribution - distribución cuantica de claves simétricas

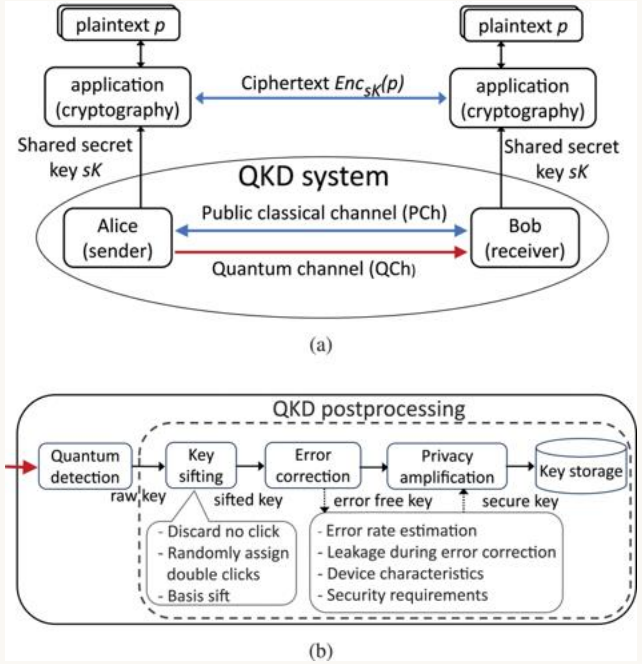
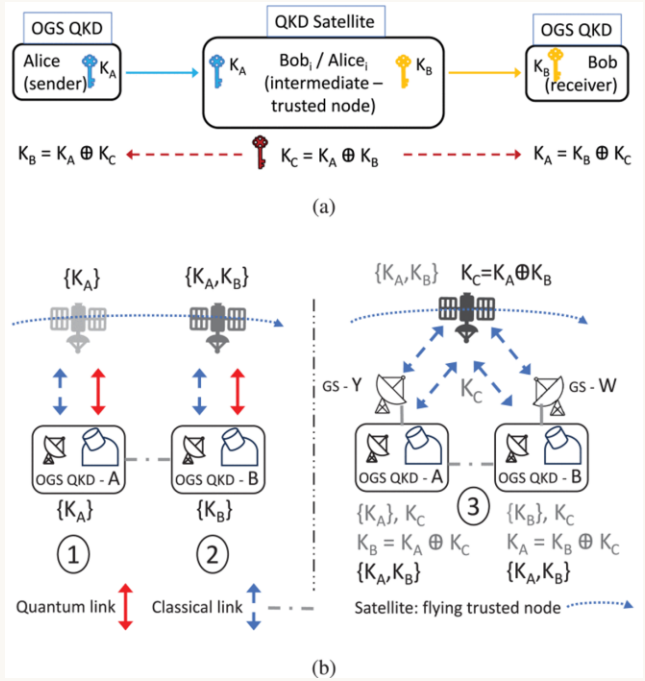


Ilustración de un mecanismo QKD [RJJP]: (a) diagrama esquemático de un sistema QKD, y (b) vista detallada delposprocesamiento de Bob (o Alice) después del intercambio de laseñal cuántica. El posprocesamiento de QKD intercambiainformación entre Alice y Bob a través del canal clásico.

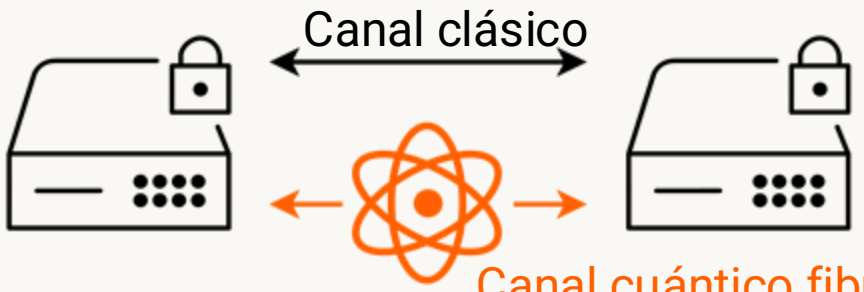


Esquema nodo de confianza – key relay [RJJP] (a): Esquema de un nodo de confianza con mecanismo de retransmisión de claves. En el nodo de confianza, las claves secretas compartidas generadas previamente en cada segmento, K_A y K_B, se combinan digitalmente (mediante operación XOR) para crear K_C, que se envía a través del canal público a ambos extremos correspondientes. (b): esquema de un nodo de confianza QKD por satélite (nodo de confianza "volante").

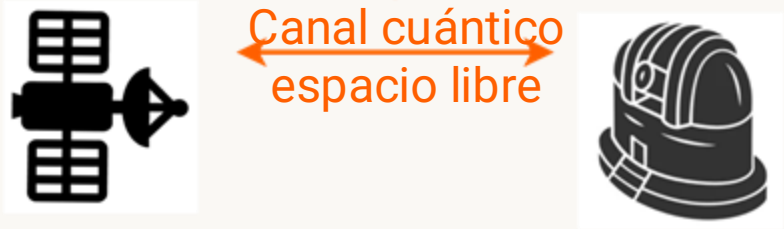
[RJJP]: J. Jordan-Parra, M. Garcia-Romero, J. Gil-Lopez, J. A. Ruiz-De-Azua and J. Paradells, "Satellite Quantum Key Distribution: Analysis, Modeling, Performance Evaluation, and Validation," in IEEE Open Journal of the Communications Society, vol. 6, pp. 8241-8271, 2025, doi: 10.1109/OJCOMS.2025.3614698.

Seguridad cuántica, enlaces fibra y FSO-satelital

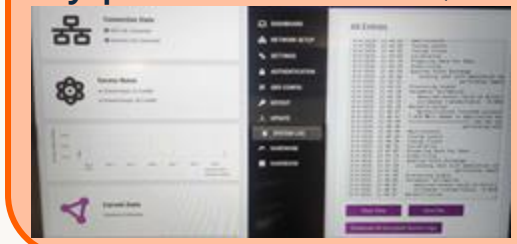
Análisis, simulación y desarrollo experimental – valida y retroalimenta



SKL, QBER, parámetros óptimos, ...
Transmisividad, errores de canal, ruido, ...



Análisis técnico y validación cruzada; equipos y protocolos DV-QKD y CV-QKD:



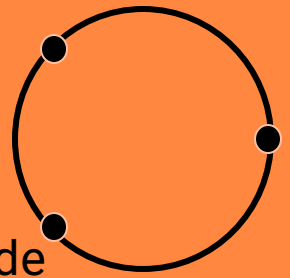
$$SKL_{BB84} = s_{X,0} + (1 - H_b(\phi_X))\, s_{X,1} - \lambda_{EC} - 6\log_2\frac{21}{\varepsilon_s} - \log_2\frac{2}{\varepsilon_c}$$

$$SKL_{BBM92} = \max_{\beta\in(0,\varepsilon_s/4)} \lfloor n_{\text{ext}} + 4\log_2\beta - 2 \rfloor$$

$$SKL_{CV-QKD} = \ldots$$

Integración en simuladores de red y distribución de claves:

Evaluación a nivel de enlace

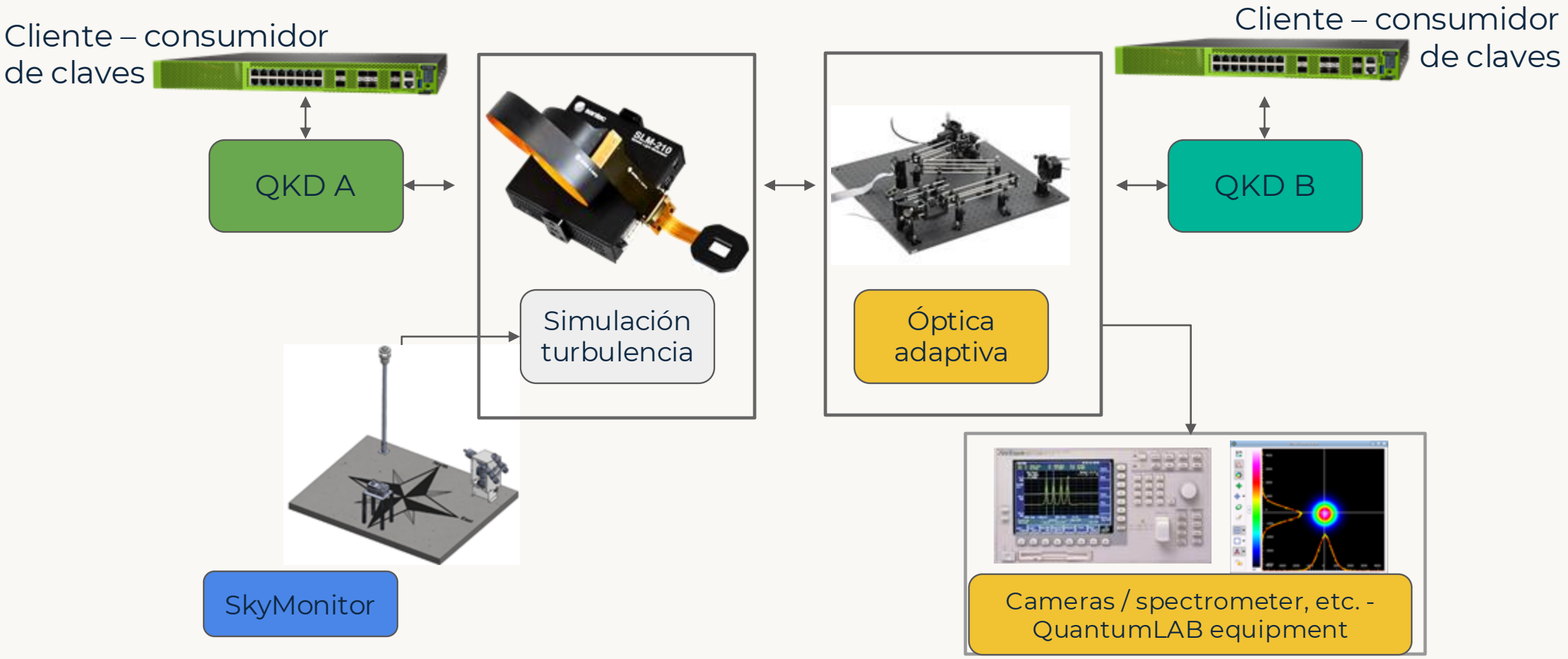


Simulador de red con elementos realistas

Análisis de distribución de claves

Testbed experimental e integración E2E

- Canal cuántico FSO con turbulencia atmosférica
- Emulación OGS-satélite en laboratorio
- Fuentes entrelazadas y protocolos más allá de QKD
- Plataformas QKD (DV y CV-QKD), con KMS y clientes consumidores



Testbed simulación E2E – terrestre y satelital

- Marco unificado para la evaluación de redes QKD
- Integración segmento terrestre y espacial (QKDSat – Flying Trusted Node)

Simulación y Emulación: E2E Testbed – plataforma de pruebas extremo a extremo

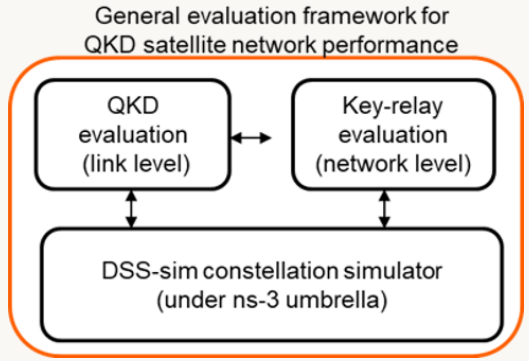
- Desarrollo de un framework basado en NS-3: DSS-SIM y QKDNetSim v2.0 (Open Source) para simulación de escenarios QKD terrestres y no terrestres (satélite en modo “Flying Trusted Node”)
- Modelado de redes QKD terrestres y satelitales bajo condiciones orbitales y operativas realistas
- Protocolos de comunicaciones estándar(ns-3) e Interfaces QKD según ETSI GS QKD (QKDNetSim)

Intención de Hardware-in-the-Loop

- Abordar la integración de equipos físicos reales en el entorno de pruebas E2E.
- Orientado al testeo de protocolos de seguridad extremo a extremo.

Caso de uso asociado:

- Arquitectura híbrida de comunicaciones cuánticamente seguras entre centros de mando remotos.



Distributed Satellite System Simulator (DSS-Sim)

- Orbital mechanics
- Satellite simulation

-Communications protocol integration
-Hardware in the Loop (HIL)

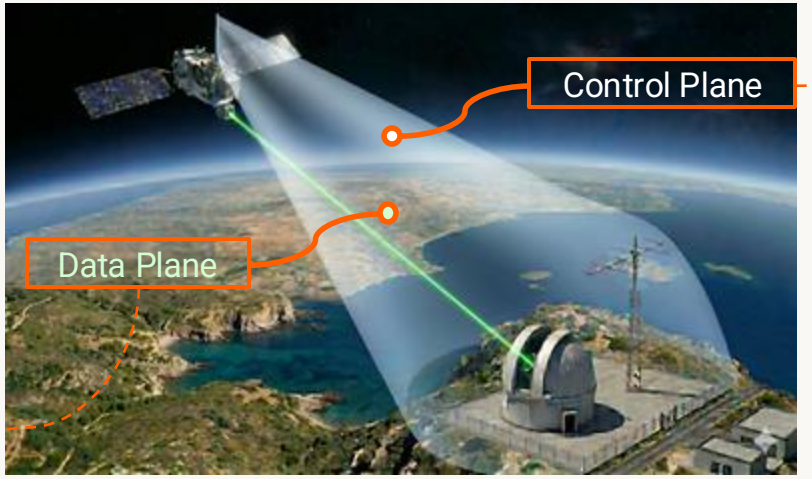
ns-3 NETWORK SIMULATOR

QKDNetSim

- QKD Protocols
- ETSI interfaces
- Native NS-3 module

Comunicaciones satelitales cuánticamente seguras

Seguridad cuántica en arquitectura híbrida RF-óptica y PQC-QKD



RF Communications - Protocol

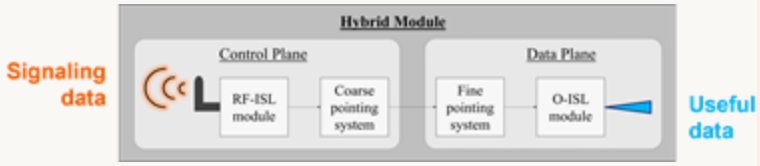
OSI Model-Based [1]

DL — Session management · Interference avoidance

PHY — Long range · Robust against attenuation

Optical System - Pointing and Acquisition Processes

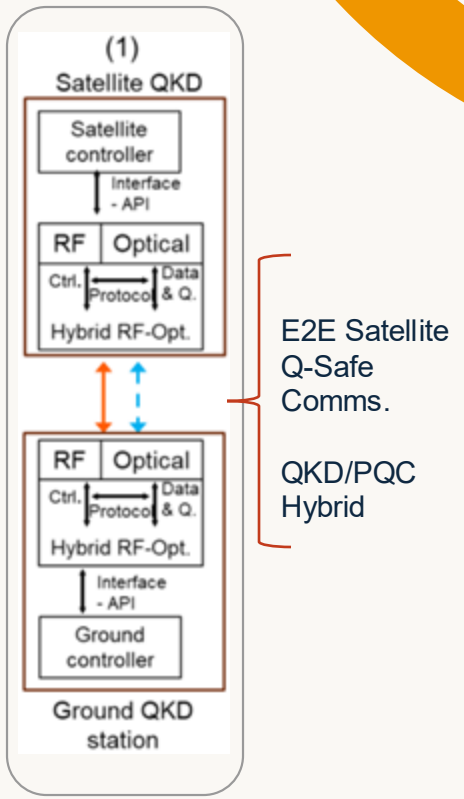
Hybrid Communication System [2]



Objectives: Reduce traditional optical pointing and acquisition times and resilience to disruptions in the free-space optical link with the hybrid communication system.

Comunicaciones satelitales cuánticamente seguras: Combina QKD y PQC, utilizando PQC para la autenticación y QKD (con respaldo o fall-back en PQC) para el cifrado de datos.

- Emplea equipos y desarrollos procedentes de distintos paquetes de trabajo.
- Integra desarrollos de PQC y esquemas híbridos PQC-QKD en un banco de pruebas / prueba de concepto (PoC).
- Incorpora hardware de tipo satelital (satellite-like) para la emulación del enlace estación terrena-satélite (GS-Satélite, HW/SW basados en plataforma MINERVA – 6GStarLab).



Objetivos de GRADIANT

Redes multiusuario de comunicaciones y sensórica distribuida

Redes cuánticas para una mayor resiliencia

Nuevo paradigma para comunicaciones seguras y sensorización

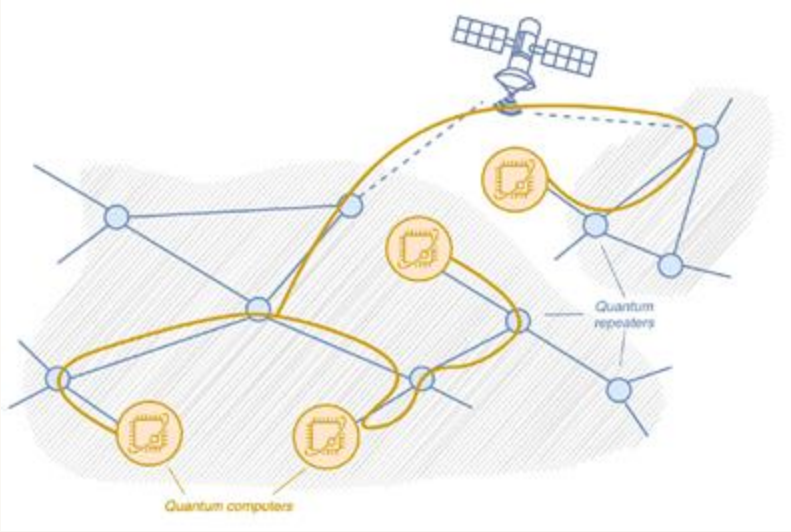
Distribución cuántica de claves (Quantum Key Distribution)

- Seguridad garantizada por los protocolos en capa física, basados en codificación de información en fotones
- Conectividad óptica a largas distancias
- Paradigma end-to-end: gran utilidad en securización con nodos satelitales
- **Vulnerabilidad** ante Denegación de Servicio (DoS): no recomendado por OTAN o MoD europeos para entornos militares ágiles

Redes cuánticas (Quantum Networks)

- Redes basadas en la distribución de **ENTRELAZAMIENTO**
- Ventajas compartidas con QKD
- Paradigma multiusuario: supera limitaciones de aplicabilidad de QKD
- Resiliencia ante Denegación de Servicio (DoS)
- **Prometedor** en escenarios de defensa, redes terrestres y satelitales: encriptación y habilitación de operaciones en centros de mando y control

Las exigencias de los escenarios de Defensa requieren el desarrollo de paradigmas *quantum-safe* versátiles, dinámicos y resilientes a DoS



Redes cuánticas para una mayor resiliencia

Nuevo paradigma para comunicaciones seguras y sensorización

Localización de amenazas

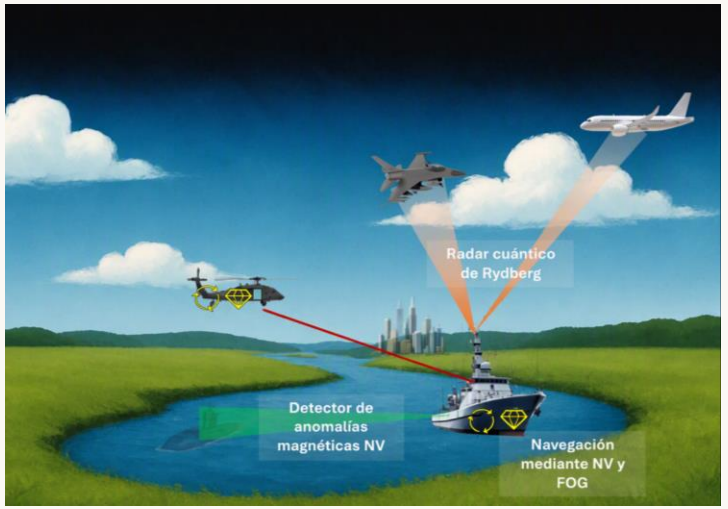
- Receptores de Rydberg RF:
  AoA + demodulación avanzada + sintonización multibanda

- Magnetómetros NV en diamante:
  Posicionamiento vectorial de anomalías magnéticas (Bx, By, Bz)

Navegación resiliente a denegación de GNSS

- Receptores de Rydberg RF:
  Navegación relativa basada en señales de oportunidad

- Magnetómetros NV en diamante:
  Brújula cuántica de precisión para cartografía magnética



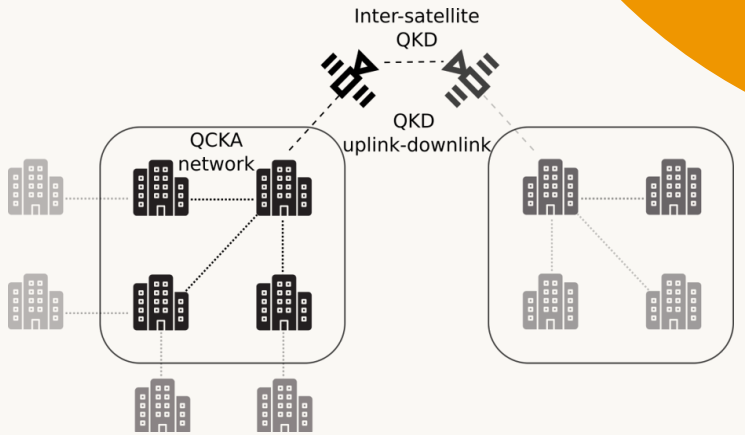
Las redes *quantum-safe* de sensores cuánticos permiten la integración de información precisa sobre amenazas electromagnéticas, localización de precisión y navegación resiliente

Comunicaciones cuánticas: seguridad en red

Objetivos estratégicos y ejes de investigación

Objetivo general: Comunicaciones cuánticamente seguras E2N

Desarrollo de soluciones (fuentes de fotones, sistemas de distribución de clave, memorias cuánticas) para garantizar la seguridad cuántica de las comunicaciones y nuevos paradigmas de redes multiusuario para aumentar la resiliencia y la aplicabilidad de las comunicaciones cuánticas.



Acciones de I+D:

1. Fuentes de entrelazamiento: Desarrollo, validación e integración funcional de fuentes de fotones: láseres, *Spontaneous Parametric Down Conversion* (SPDC).

2. Redes multiusuario (E2N): Arquitecturas experimentales de red de tipo *Quantum Conference Key Agreement* (QCKA) para distribución simultánea de estados entrelazados (GHZ) a N usuarios. Benchmark de simulación de rendimiento.

3. Generación determinista de clave: Validación experimental de memorias cuánticas (atómicas) y prueba de concepto de integración en protocolos QKD como *buffer* determinista.

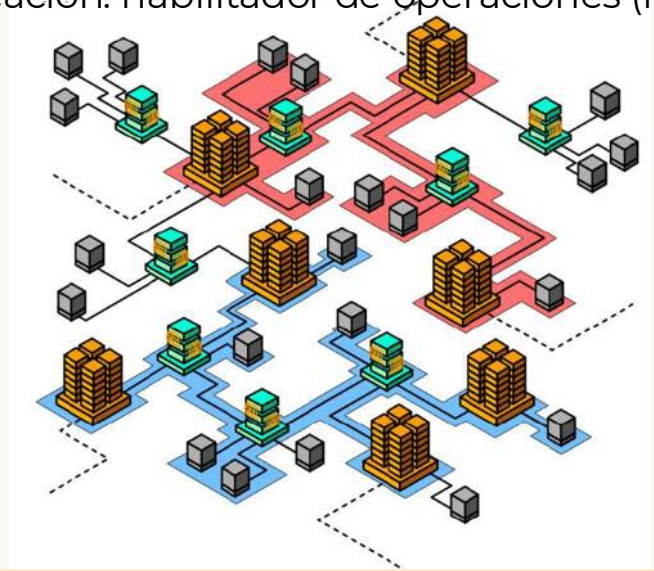
4. Consumo de clave y aplicabilidad: Garantizar la comunicación con seguridad cuántica mediante la transmisión de clave a través de VPN basadas en WireGuard / IPSec, según protocolos ETSI QKD 014 y similares.

Comunicaciones cuánticas: seguridad en red

Desarrollos diferenciales en QUIXOTE

Redes QCKA (de E2E a E2N)

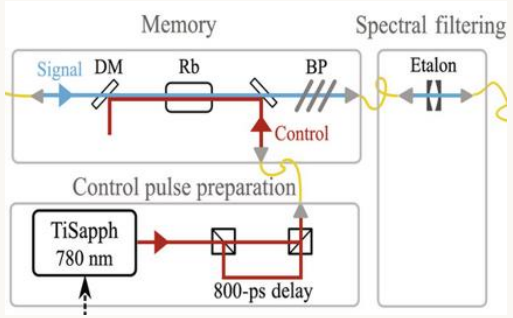
1. Generación de estados entrelazados (SPDC)
2. Generación de estados GHZ (puertas de fusión)
3. Distribución a N usuarios (FSO / fibra óptica)
4. Detección y destilación de clave
5. Aplicación: habilitador de operaciones (redes terrestres)

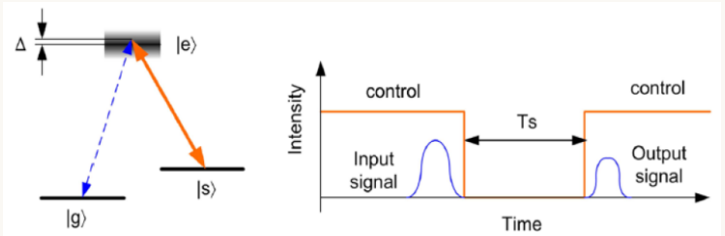


A. Ulibarrena *et al.*, *Guarantees on the structure of experimental quantum networks*. Npj Quantum Inf, vol 10 (2024). doi:10.1038/s41534-024-00911-z

Memorias cuánticas (de la probabilidad al determinismo)

1. Generación de estados cuánticos fotónicos con afinidad espectral
2. Desarrollo de sistema cuántico (atómico) para almacenamiento de fotones
3. Generación de protocolos de almacenamiento y liberación de fotones (clave)
4. Caracterización de memoria cuántica
5. Integración en protocolos QKD deterministas

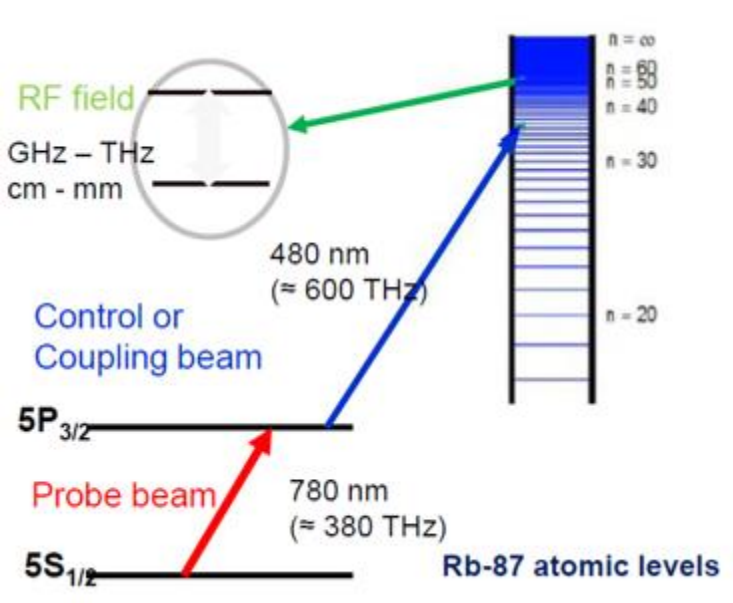




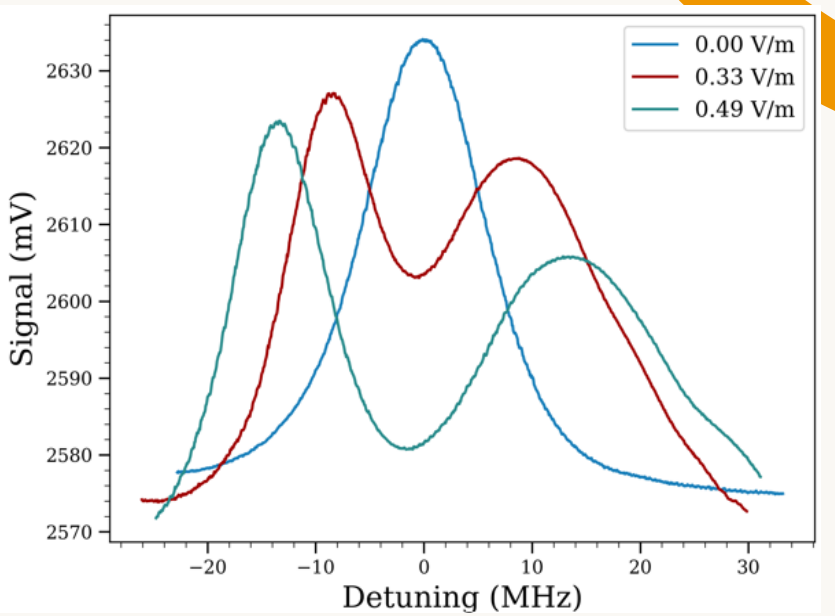
Sarah E. Thomas *et al.*, *Deterministic storage and retrieval of telecom light from a quantum dot single-photon source interfaced with an atomic quantum memory*. Sci. Adv.10, eadi 7346 (2024). DOI:10.1126/sciadv.adi7346

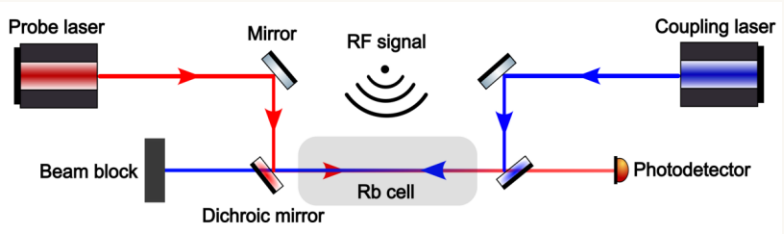
Sensores cuánticos de radiofrecuencia (Rydberg)

Fundamentos generales



Property	Notation	(n^*) scaling
Orbital radius	r	$(n^*)^2$
Electron binding energy	E_n	$(n^*)^{-2}$
Level spacing	$E_{n+1} - E_n$	$(n^*)^{-3}$
Ionization field	$\varepsilon^{(\infty)}$	$(n^*)^{-4}$
Radiative lifetime	τ_0	$(n^*)^3$
Polarizability	α	$(n^*)^7$
Rydberg transition dipole moment	$\langle nl\|er\|n(l+1)\rangle$	$(n^*)^2$
Excitation transition dipole moment	$\langle 5P\|er\|nl\rangle$	$(n^*)^{-3/2}$



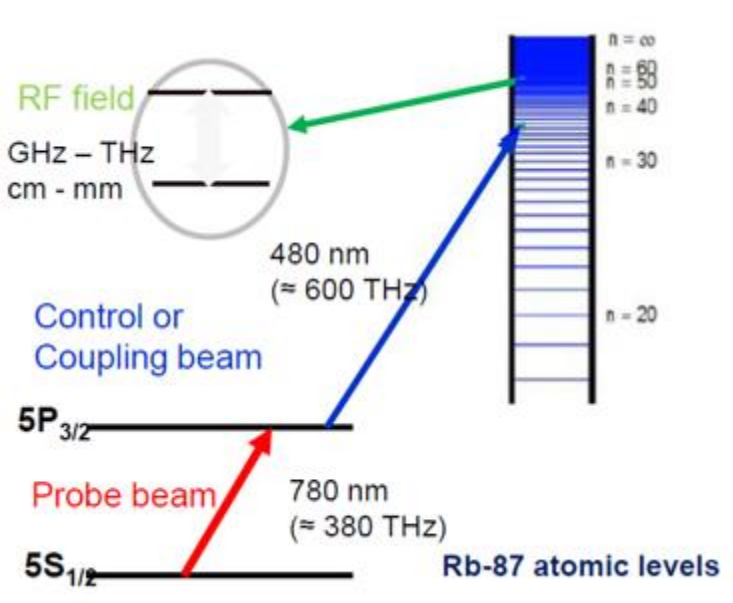


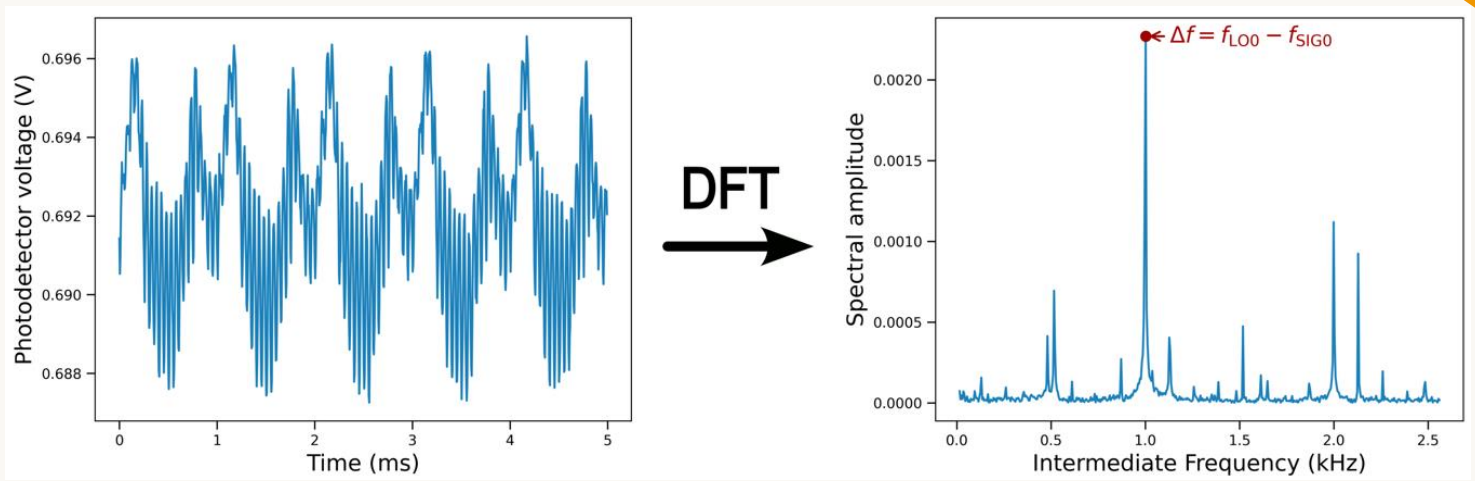
Lectura óptica del acoplamiento de radiofrecuencia externa (antena cuántica sintonizable)

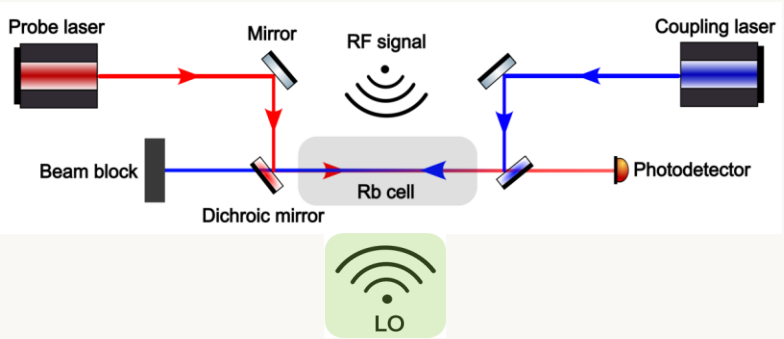
- Sintonización de sub-GHz a THz
- Sensibilidad potencial mejora antena dipolar clásica
- Capacidad de demodulación
- Integrable en aplicaciones de radar y telecomunicaciones
- Múltiples arquitecturas

Sensores cuánticos de radiofrecuencia (Rydberg)

Fundamentos generales







Lectura óptica del acoplamiento de radiofrecuencia externa (antena cuántica sintonizable)

- Sintonización de sub-GHz a THz
- Sensibilidad potencial mejora antena dipolar clásica
- Capacidad de demodulación
- Integrable en aplicaciones de radar y telecomunicaciones
- Múltiples arquitecturas

Sensores cuánticos de radiofrecuencia (Rydberg)

Objetivos estratégicos y ejes de investigación

Objetivos generales: arquitecturas, metodologías y aplicaciones

- Evolución de sistemas cuánticos de detección de radiofrecuencia mediante espectroscopía láser de estados cuánticos de Rydberg, sintonizables a bandas RF entre MHz y THz.
- Desarrollo de arquitecturas para detección de Ángulo de Llegada (AoA), y metodologías avanzadas de procesado de señal y optimización.
- Avance de TRL a entornos relevantes.



Acciones de I+D:

1. Desarrollo de subsistemas *custom* para sensores de Rydberg

Sistemas láser *ad hoc*, electrónica de control y detección, etc.

2. Compactificación de arquitecturas para entorno operativo

De la mesa óptica al sistema operativo.

3. Arquitecturas y metodologías para AoA

Avance en detección AoA más allá del estado del arte.

4. Simulación avanzada y optimización

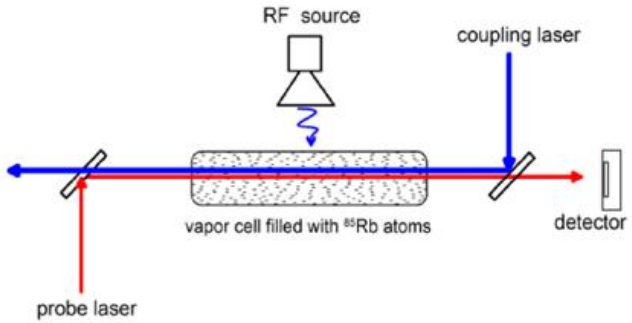
Generación de librerías de benchmark de rendimiento y optimización de *workflow*.

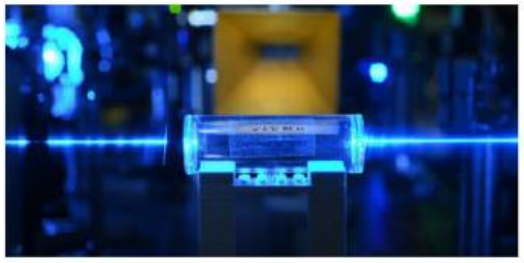
5. Procesado de señal para estrategias de demodulación avanzada

Desarrollo de metodologías novedosas de procesado, monitorización y clasificación.

6. Validación funcional de aplicaciones: detección de amenazas radioeléctricas y localización por AoA

Demostración metodológica experimental de aplicaciones de Defensa.

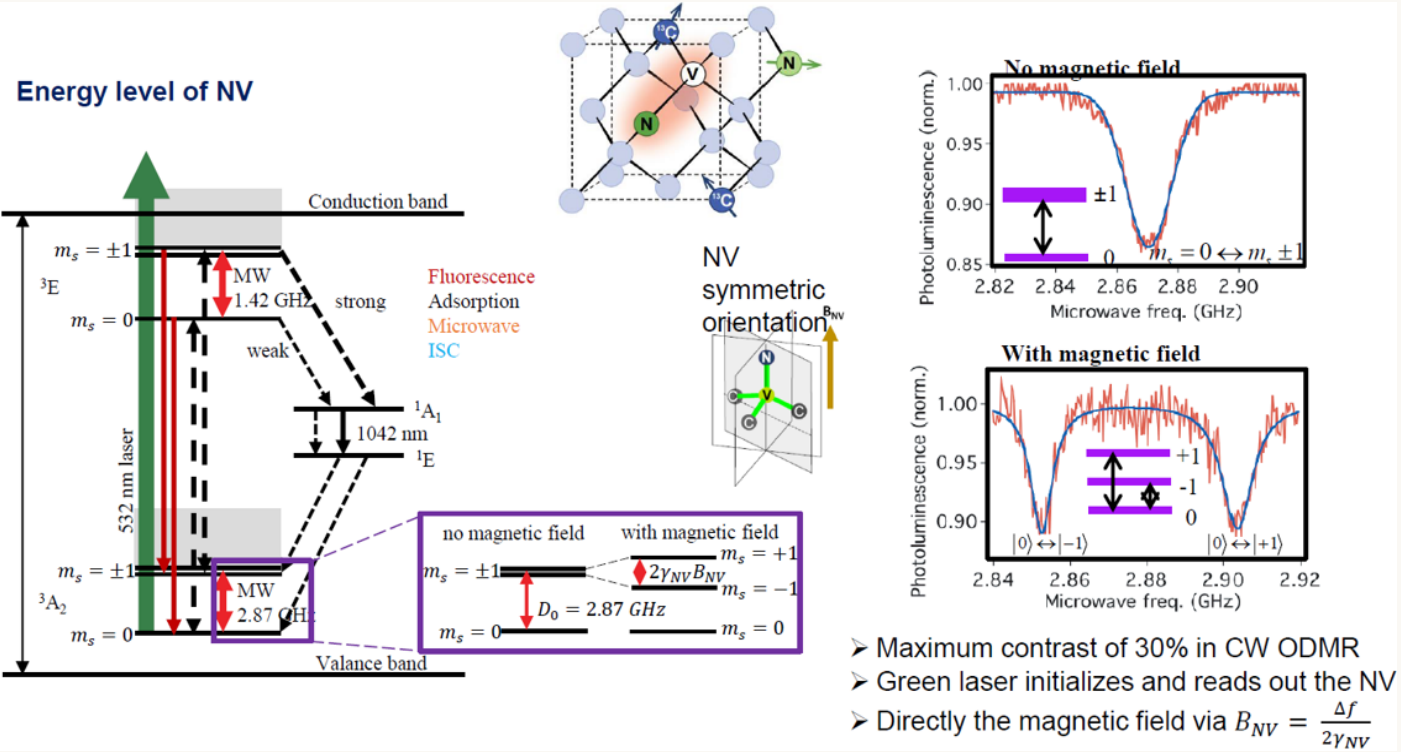




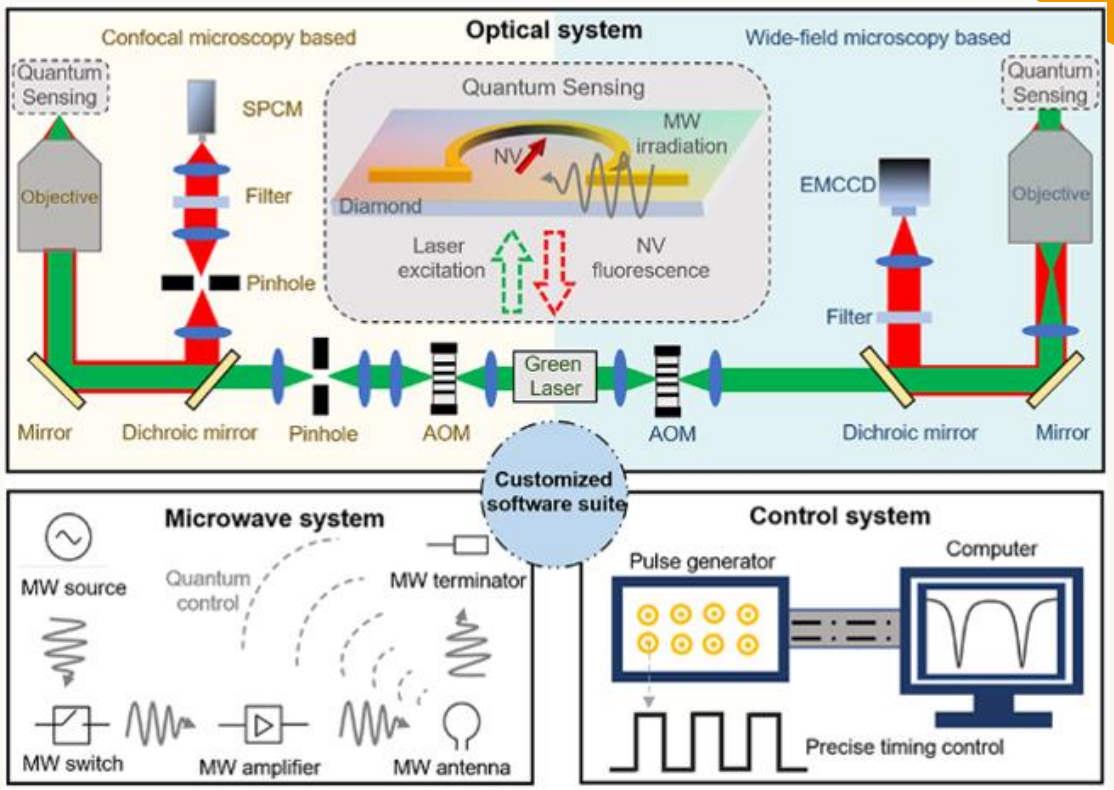
https://phys.org/news/2020-03-scientists-quantum-sensor-entire-radio.html

Magnetómetros cuánticos de diamante (centros NV)

Fundamentos generales



- Maximum contrast of 30% in CW ODMR
- Green laser initializes and reads out the NV
- Directly the magnetic field via $B_{NV} = \frac{\Delta f}{2\gamma_{NV}}$



Lectura óptica de perturbaciones magnéticas, térmicas o electromecánicas que afectan al espectro de fluorescencia en los estados de qudit

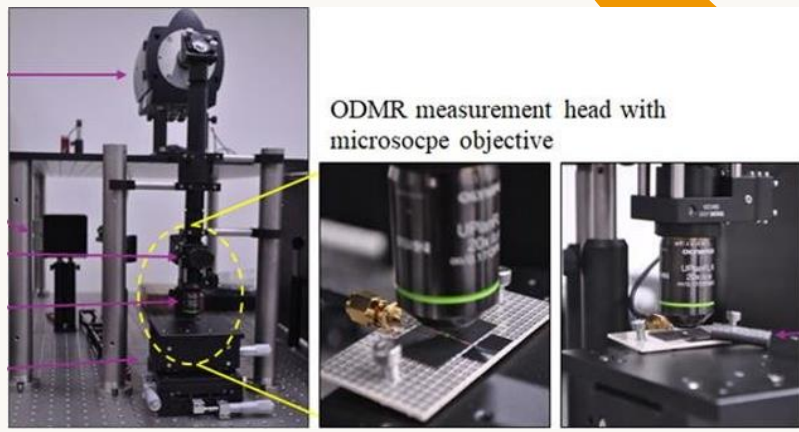
Zhang, T. *et al.*, "Toward Quantitative Bio-sensing with Nitrogen–Vacancy Center in Diamond."
ACS Sensors 2021, 6(6), 2077-2107. DOI: 10.1021/acssensors.1c00415

Magnetómetros cuánticos de diamante (centros NV)

Objetivos estratégicos y ejes de investigación

Objetivos generales: arquitecturas, metodologías y aplicaciones

- Evolución de sistemas cuánticos de detección de campos magnéticos basados en centros nitrógeno-vacancia (NV) en diamante.
- Desarrollo de arquitecturas integradas en chip fotónico para reducción de SWaP
- Desarrollo de metodologías de procesado para localización vectorial y navegación.



Acciones de I+D:

1. Desarrollo de subsistemas *custom* de control de qubits para centros NV

Electrónica de control RF e integración con sincronización avanzada en FPGA.

2. Compactificación de arquitecturas optomecánicas

Sistema óptico integrado en magnetómetro cuántico adaptado a entorno operativo.

3. Diseño de arquitecturas de diamante en chip fotónico

Diseño, simulaciones de rendimiento y validación funcional de arquitecturas en chip.

4. Simulación avanzada y optimización

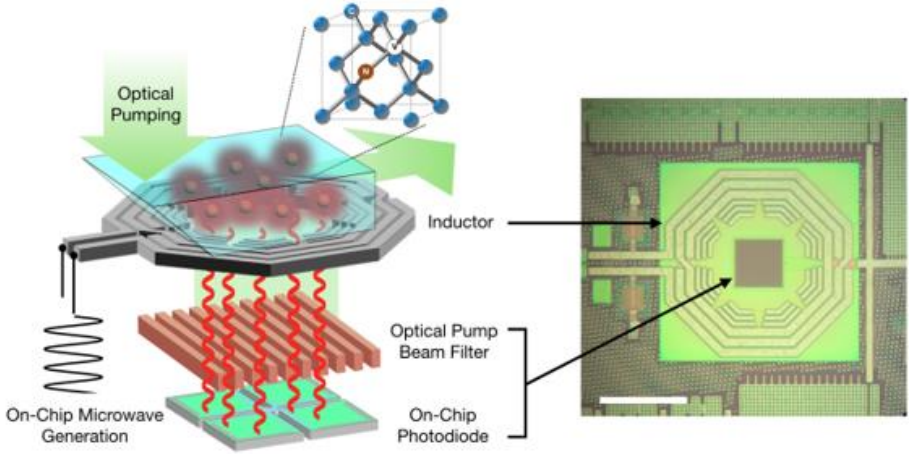
Generación de librerías de benchmark de rendimiento y optimización de *workflow*.

5. Procesado de señal para magnetometría vectorial

Desarrollo de metodologías novedosas de procesado, monitorización y clasificación.

6. Desarrollo de *workflow* funcional para navegación magnética

Implementación de procesos para integración futura en sistemas de navegación.



Kim, D. *et al. A CMOS-integrated quantum sensor based on nitrogen-vacancy centres.* Nature Electronics, 2, 284-289 (2019). DOI: 10.1038/s41928-019-0275-5

Objetivos de LORTEK

Fotónica cuántica para sensores inerciales

Sensores inerciales fotónicos

¿Qué son?

Los sensores inerciales fotónicos utilizan la luz para medir movimiento, aceleración y/o rotación, sustituyendo o complementando tecnologías electromecánicas convencionales.

Ventajas principales

•Alta sensibilidad y estabilidad.
•Inmunidad a interferencias electromagnéticas.
•Ausencia de elementos mecánicos móviles.
•Capacidad de operación en entornos severos.
•Potencial de miniaturización mediante fotónica integrada.

Aplicaciones

✈️ Navegación aeronáutica
🚢 Plataformas navales y submarinas
🛰️ Sistemas espaciales
🤖 Vehículos autónomos (UXV/UAV/UGV)
🏭 Monitorización industrial

Principales tecnologías

Giroscopios fotónicos

Giroscopios interferométricos de fibra (IFOG)

- Basados en el efecto Sagnac.
- La rotación se mide como un desfase entre dos haces que recorren una bobina de fibra en sentidos opuestos.
- Tecnología fotónica de referencia para navegación de alta precisión.

Giroscopios resonantes (RFOG)

- Emplean cavidades ópticas resonantes en lugar de grandes bobinas de fibra.
- La rotación produce una diferencia de frecuencia resonante entre los modos horario y antihorario.
- Permiten reducir tamaño y peso manteniendo altas prestaciones.

Giroscopios fotónicos integrados (PIC Gyros)

- Implementados sobre plataformas de fotónica integrada (SiN, InP, $LiNbO_3$).
- Integran guías de onda, resonadores y detectores en un único chip.
- Orientados a sistemas SWaP-C reducidos para UAV, UXV y aplicaciones espaciales

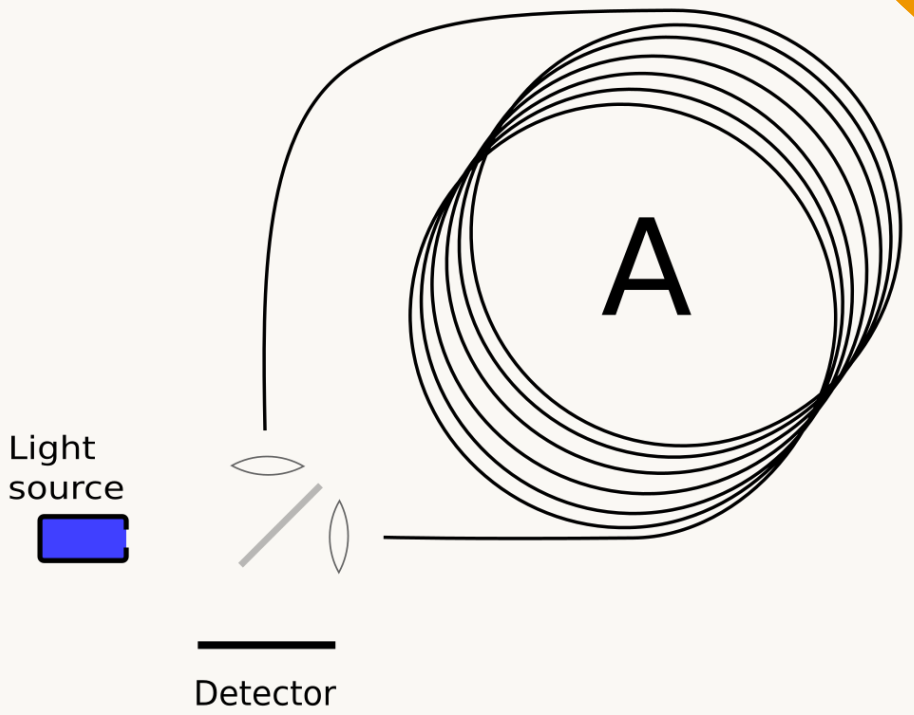
FOG

- **Basado en el efecto Sagnac**: se produce un desfase entre haces de luz que se propagan en sentidos opuestos dentro de un lazo de fibra óptica en rotación.
- La luz procedente de un láser se divide en dos trayectorias al propagarse por una bobina de fibra óptica:
  - **Sentido horario (CW, Clockwise)**
  - **Sentido antihorario (CCW, Counter-Clockwise)**
- La rotación introduce una **diferencia de fase** entre ambos haces:

$$\Delta\phi \propto \Omega \cdot A$$

donde:

- Ω: velocidad angular de rotación.
- A: área encerrada por la trayectoria óptica.
- Los haces se recombinan y generan un patrón de interferencia.
- La **variación de intensidad** de la señal interferométrica codifica la rotación.
- La señal de salida es proporcional a la **velocidad angular**.



D. mcfadden, "Schematic of a fibre-optic-gyroscope based on the sagnac effect," *Wikimedia Commons*, CC BY-SA 3.0

FOG Cuántico: Más allá del límite clásico

Concepto

Los giroscopios cuánticos fotónicos emplean **estados no clásicos de la luz** (squeezed states, estados entrelazados o estados NOON) para mejorar la sensibilidad de un sensor Sagnac convencional. En lugar de aumentar la longitud de fibra o la potencia óptica, la mejora proviene de las propiedades cuánticas de la luz.

Principio de funcionamiento

- Arquitectura similar a un FOG convencional.
- Inyección de estados cuánticos de la luz en el interferómetro.
- Reducción del ruido cuántico (shot noise).
- Mejora de la sensibilidad de medida del desfase Sagnac.

$$\Delta\phi_{\min} \propto \frac{1}{N}$$

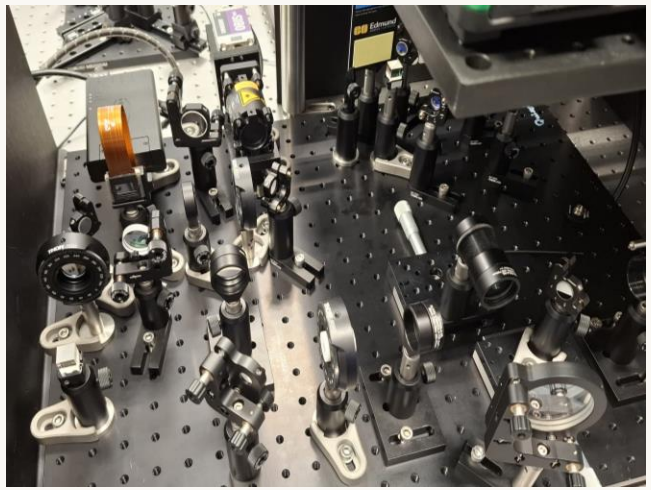
frente al límite clásico

$$\Delta\phi_{\min} \propto \frac{1}{\sqrt{N}}$$

donde N es el número de fotones.

Fuente de fotónes SPDC

Configuración Sagnac



- Componentes principales:
  - Divisor de haz polarizante (PBS)
  - Cristal no lineal (PPKTP)
  - Espejos
  - Láser de bombeo
  - El haz de bombeo se divide en dos trayectorias:
  - Sentido horario (CW, Clockwise)
  - Sentido antihorario (CCW, Counter-Clockwise)
- Ambas trayectorias generan pares de fotones en el mismo cristal mediante SPDC.
- La geometría de camino común (common-path) proporciona una elevada estabilidad pasiva frente a perturbaciones mecánicas y fluctuaciones ambientales

$$|\psi\rangle = |H_s V_i\rangle + e^{i\phi}|V_s H_i\rangle$$

La trayectoria en sentido horario (CW) genera el estado I $H_s V_i\rangle$, mientras que la trayectoria en sentido antihorario (CCW) genera el estado I $V_s H_i\rangle$, dando lugar a entrelazamiento en polarización entre los fotones señal (s) e idler (i).

Herramientas de simulación

QUTIP: Física del problema

QUTIP

- Entorno de dinámica cuántica computacional.
- Modelado teórico y simulación de experimentos.
- Funciones con una sintaxis intuitiva basada en el lenguaje de la física.
- Óptica cuántica de variables continuas (estados de Fock, térmicos, coherentes, solucionadores numéricos, etc.).
- Caracterización de ruido, pérdidas y decoherencia.
- Modelado de óptica no lineal $\chi^{(n)}$.
- Herramientas de visualización: función de Wigner, esfera de Bloch, tomografía cuántica, etc.

Example: Jaynes-Cummings model

Mathematical formulation:

Hamiltonian

$$\hat{H} = \hbar\omega_c \hat{a}^\dagger \hat{a} - \frac{\hbar\omega_q}{2}\hat{\sigma}_z + \frac{\hbar g}{2}\left(\hat{a}\hat{\sigma}_+ + \hat{a}^\dagger\hat{\sigma}_-\right)$$

Initial state

$$|\psi(t=0)\rangle = |1\rangle_c \otimes |0\rangle_q$$

Time evolution

$$\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle$$

Expectation values

$$\langle \hat{a}^\dagger \hat{a}\rangle = \langle\psi(t)|\,\hat{a}^\dagger\hat{a}\,|\psi(t)\rangle$$

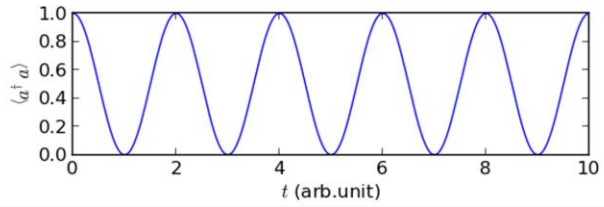
QuTiP code:

```
from qutip import *
N  = 10

a  = tensor(destroy(N),qeye(2))
sz = tensor(qeye(N),sigmaz())
s  = tensor(qeye(N),destroy(2))
wc = wq = 1.0 * 2 * pi
g  = 0.5 * 2 * pi
H  = wc * a.dag() * a - 0.5 * wq * sz + \
     0.5 * g * (a * s.dag() + a.dag() * s)
psi0  = tensor(basis(N,1), basis(2,0))
tlist = linspace(0, 10, 100)
out   = mesolve(H, psi0, tlist, [], [a.dag()*a])

from pylab import *
plot(tlist, out.expect[0])
show()
```

Qobj instances



QuTiP

Herramientas de simulación

QISKIT

- Modelado de circuitos cuánticos y puertas cuánticas (gates).
- Medidas estadísticas y muestreo (sampling) utilizando ordenadores cuánticos reales (IBM).
- Escalabilidad para la simulación de un gran número de fotones, representando la polarización como qubits (y, de forma análoga, otros grados de libertad).
- Estadísticas de medición.
- Comportamiento de la información cuántica.



Objetivos de FIDESOL

qcrypto: simulación y testeo de comunicaciones cuánticas

De los objetivos a la herramienta

Por qué qcrypto en QUIXOTE

Diseñar arquitecturas híbridas QKD-PQC

Necesitamos: Simular enlaces QKD con ruido realista y con un adversario.

Decidir dónde usar QKD y PQC

Necesitamos: Métricas comparables (QBER, tasa de clave, detección de Eve) en distintas condiciones.

Validar antes de desplegar

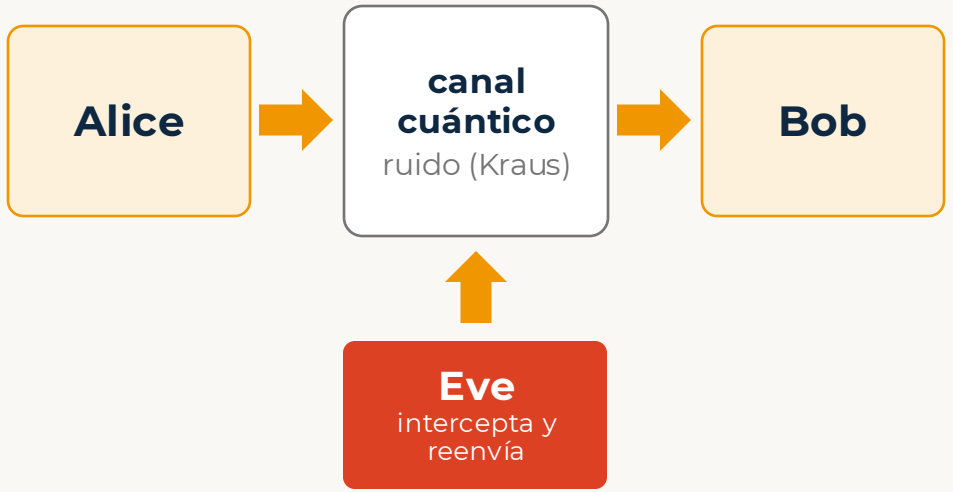
Necesitamos: Pruebas sistemáticas y reproducibles de los protocolos cuánticos.

qcrypto una herramienta de simulación y testeo de protocolos cuánticos que da soporte a estas tareas

La criptografía cuántica ya es software

Motivación

- **La QKD ya está desplegada y en estandarización:** la calidad del software importa hoy.
- **Un protocolo es un programa distribuido** entre varias partes (Alice, Bob… y Eve).
- **El ruido y el adversario forman parte de la especificación**, no son una perturbación.
- **La corrección es estadística:** QBER, valor CHSH o tasa de aceptación sobre miles de rondas.



Salida a validar: clave + QBER / CHSH (estadístico, no un valor fijo)

El hueco en las herramientas actuales

Estado del arte (✓ sí · ~ parcial · ✗ no)

Herramienta	Estados mixtos	POVM	Ruido	Reproducible en paralelo	Protocolos de referencia	Sin runtime C/C++
Qiskit Aer	✓	✗	✓	~	✗	✗
Cirq	✓	✗	✓	~	✗	✗
QuTiP	✓	✓	✓	~	✗	✗
NetSquid	✓	~	✓	~	~	✗
SeQUeNCe	✓	~	✓	~	~	✗
qcrypto	✓	✓	✓	✓	✓	✓

Simuladores generalistas piensan en circuitos unitarios; **los de redes** abstraen el detalle microscópico. Resultado: implementaciones ad hoc, poco reutilizables y difíciles de reproducir.

qcrypto: una biblioteca en Rust

Qué es

Física de sistemas abiertos

Matrices densidad, operadores de Kraus y medidas generalizadas (POVM) como ciudadanos de primera clase.

Correcto por construcción

Puertas no unitarias, canales no CPTP o medidas incompletas se rechazan al crearlas, no en ejecución.

Ruido = inyección de fallos

Canales componibles y parametrizables, más un adversario (Eve) explícito y separado del ruido.

Reproducible bit a bit

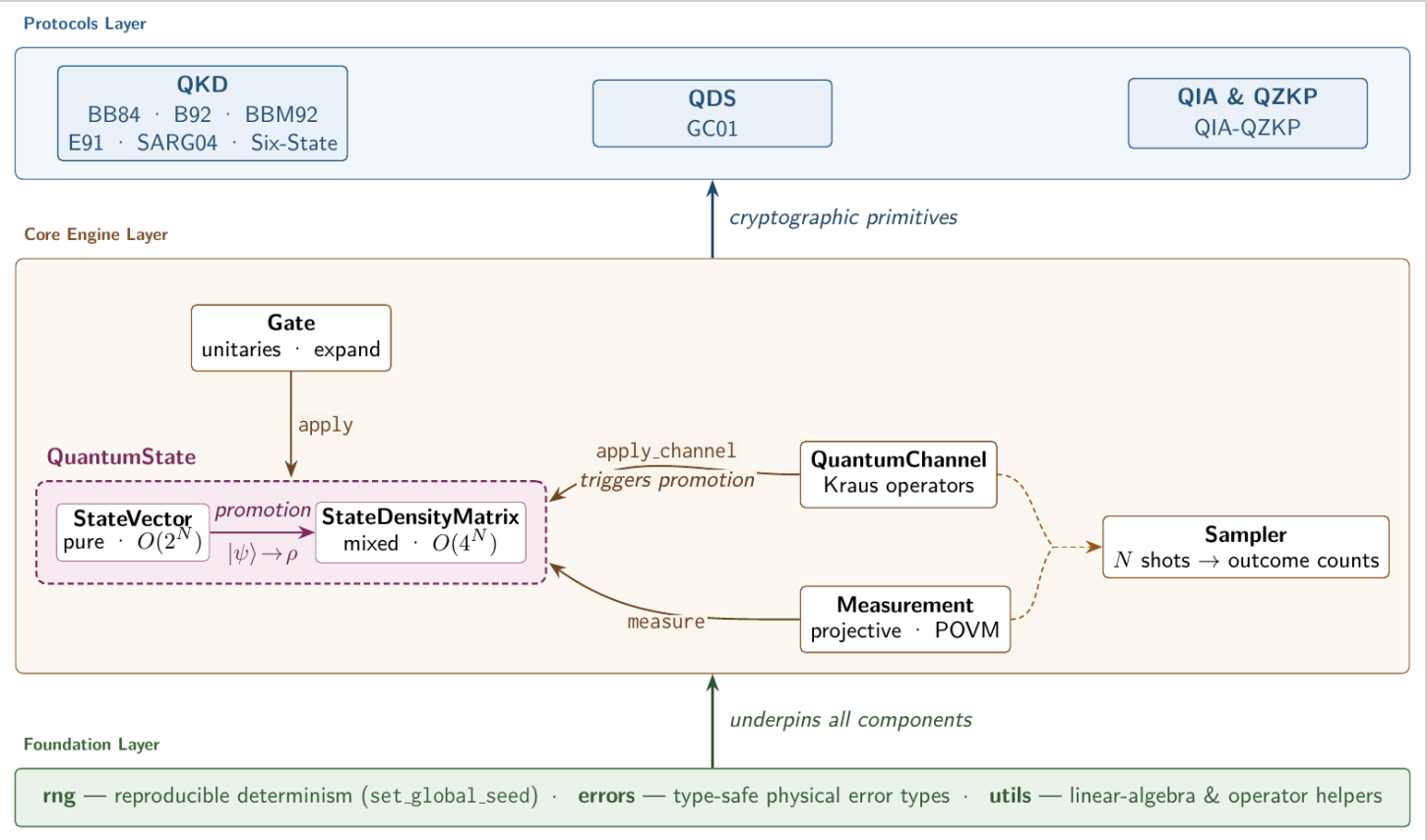
Mismas claves y estadísticas con multihilos gracias a semillas por unidad de trabajo.

Open source · 100 % Safe Rust · publicado en crates.io (v0.3.2) · + qcryptool (CLI)



Arquitectura

Cómo está hecho



Tres capas

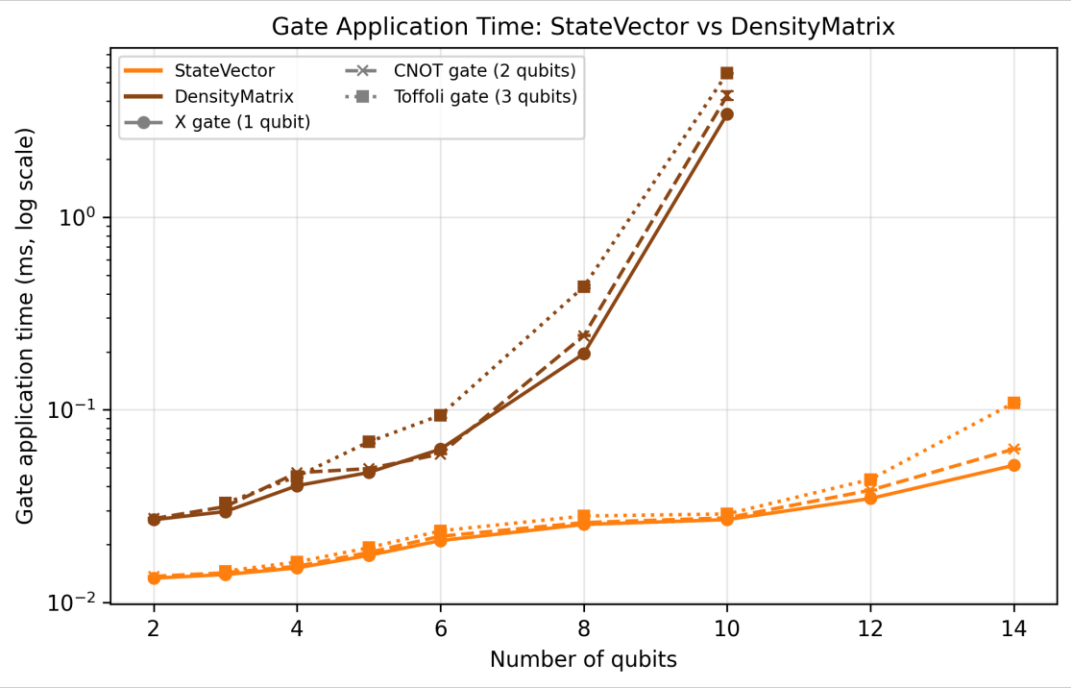
- **Protocolos** (QKD, firma, autenticación)
- **Motor** (estado, puertas, canales, medidas, sampler)
- **Base** (RNG reproducible, errores tipados, álgebra)

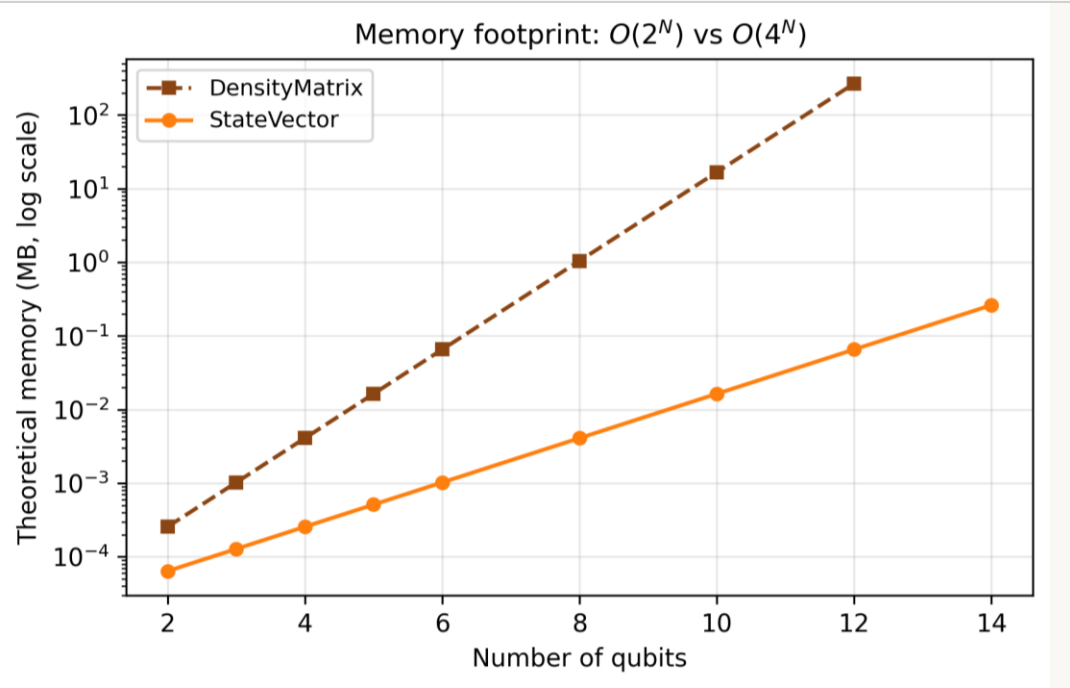
Arquitectura dual

Empieza como vector de estado $O(2^N)$ y solo pasa a matriz densidad $O(4^N)$ cuando aparece ruido.

Por qué una arquitectura dual

Benchmarks internos de qcrypto





Puertas: con matriz densidad el coste se dispara a partir de ~6 qubits; el vector de estado se mantiene casi plano.

Memoria: a 12 qubits, 64 KiB frente a 256 MiB. Por eso solo se promociona a matriz densidad cuando aparece ruido.

Protocolos incluidos y qcryptool

Qué puede hacer hoy

Distribución de claves (QKD)

- BB84, Six-State, SARG04
- B92 con POVM óptima (discriminación inequívoca)
- BBM92 y E91 (entrelazamiento + test CHSH)

Autenticación de identidad

- QIA-QZKP: prueba de conocimiento cero cuántica

Firma digital cuántica

- GC01 (Gottesman–Chuang)



```
# BB84, 100 ejecuciones con ruido despolarizante
$ qcryptool bb84 -n 1024 -s 100 \
    --channel1 depolarizing --p1 0.03 -o results.csv

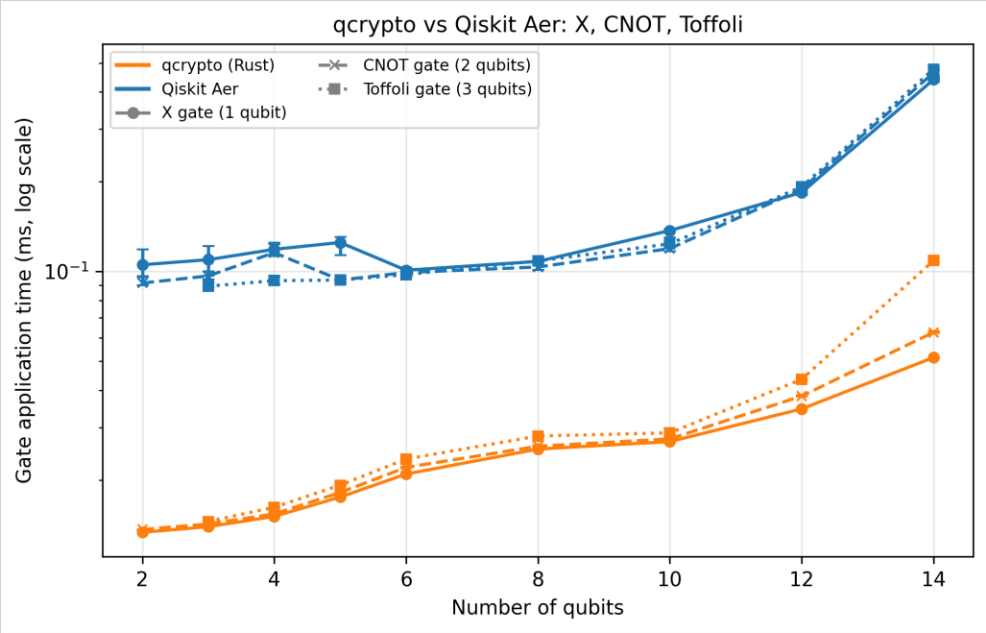
# BBM92 con ruido asimétrico en Alice y Bob
$ qcryptool bbm92 -n 1000 \
    --channel1 depolarizing --p1 0.01 \
    --channel2 depolarizing --p2 0.04

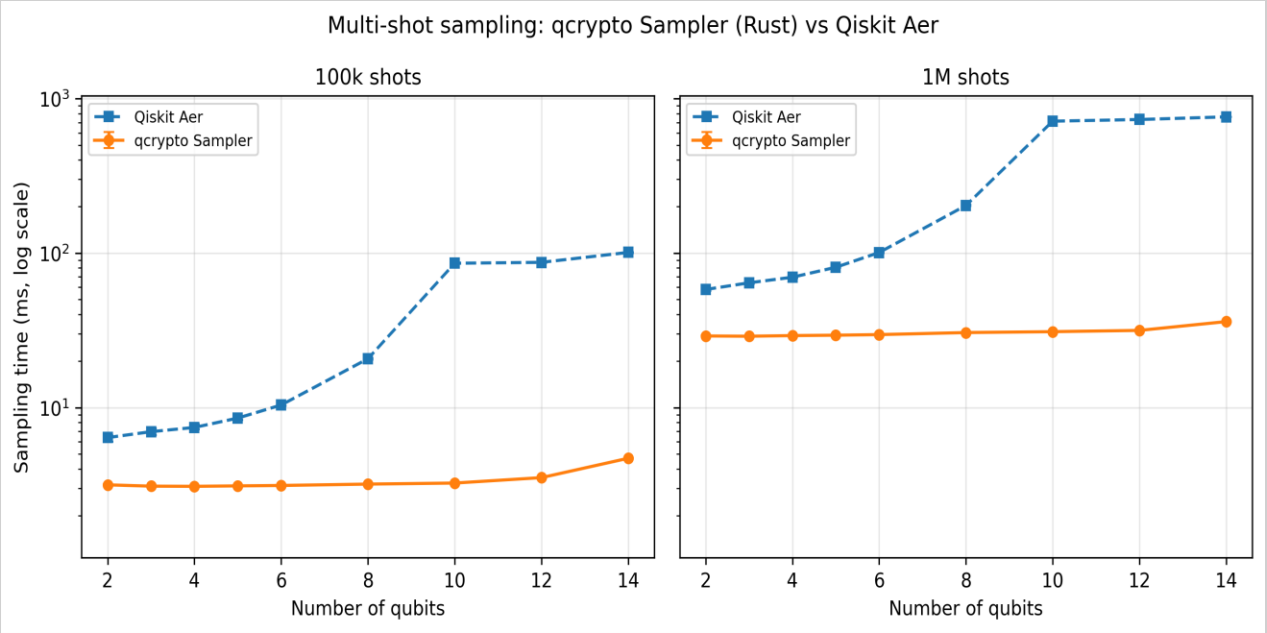
# Experimento completo y versionable
$ qcryptool --experiment-config exp.json
```

qcryptool: experimentos masivos sin escribir una línea de Rust

Resultados: frente a Qiskit Aer

Simulador de vector de estado de referencia



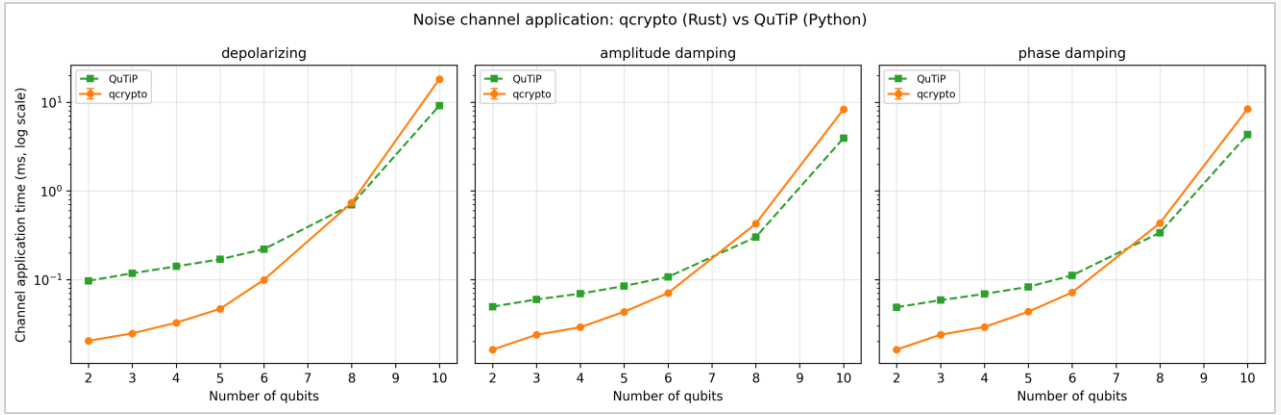


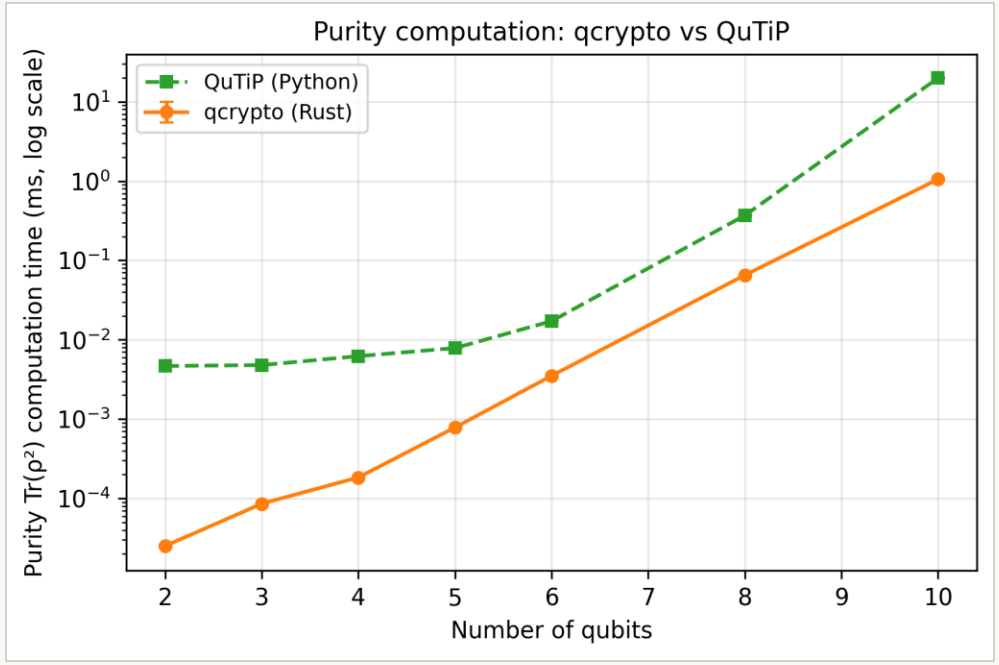
Puertas: qcrypto aplica cada puerta sobre el estado vivo, sin la sobrecarga fija por invocación de Aer.

Muestreo: la distribución se calcula una vez y cada shot es una búsqueda binaria: coste casi plano incluso con 1 M de shots.

Resultados: frente a QuTiP

Referencia para sistemas cuánticos abiertos





Canales de ruido: más rápido hasta ≈ 8 qubits (el régimen de los protocolos); después QuTiP se adelanta ligeramente.

Pureza Tr(ρ^2): entre uno y dos órdenes de magnitud más rápido en todo el rango.

Objetivos de ITECAM

Optimización cuántica para redes cuánticas

EL PUNTO DE PARTIDA

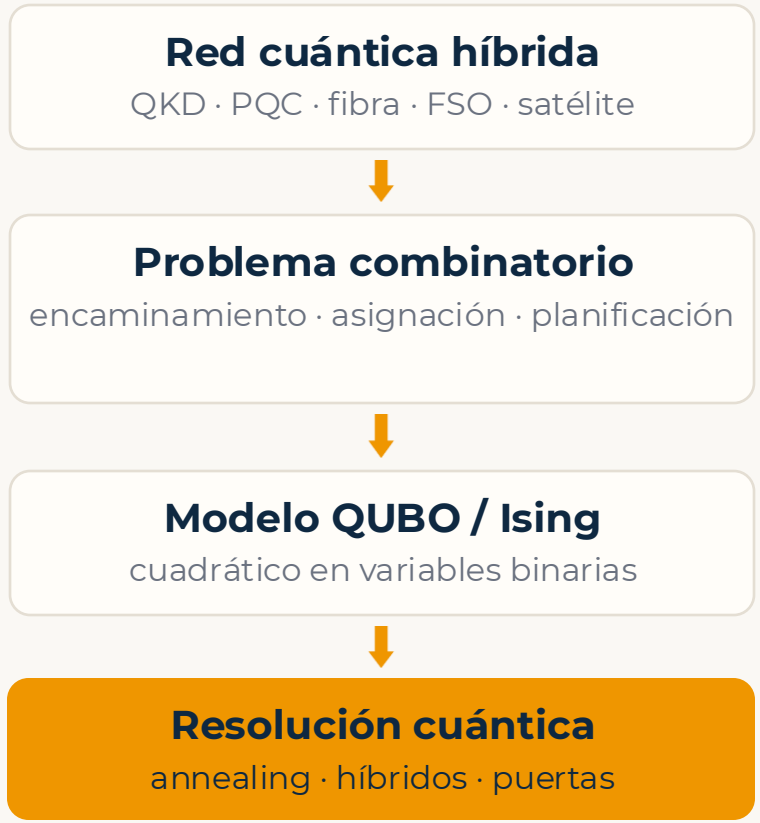
Redes cuánticas: un reto de optimización

1. **Redes híbridas**
   QKD y PQC conviven; enlaces de fibra y de espacio libre; segmento terrestre y satelital.

2. **Decisiones discretas acopladas**
   Rutas de clave, activación de enlaces, reparto de recursos y nodos de confianza.

3. **Explosión combinatoria**
   Con *n* decisiones binarias hay 2^n configuraciones: el espacio crece exponencialmente con la red.

4. **Condiciones cambiantes**
   Pérdidas, QBER y demanda de clave varían: hay que reoptimizar de forma adaptativa.



TRES PARADIGMAS COMPLEMENTARIOS

Líneas de trabajo en computación cuántica



01

Optimización QUBO nativa

Problemas combinatorios modelados como QUBO / Ising, el modelo nativo del annealer.

QUBO · Ising · Annealing



02

Enfoques híbridos

Descomposición del problema: la parte continua al clásico, la binaria cuadrática al cuántico.

Clásico + Cuántico



03

Algoritmia variacional

Circuitos parametrizados en bucle clásico-cuántico, en QPU de puertas y en HPC.

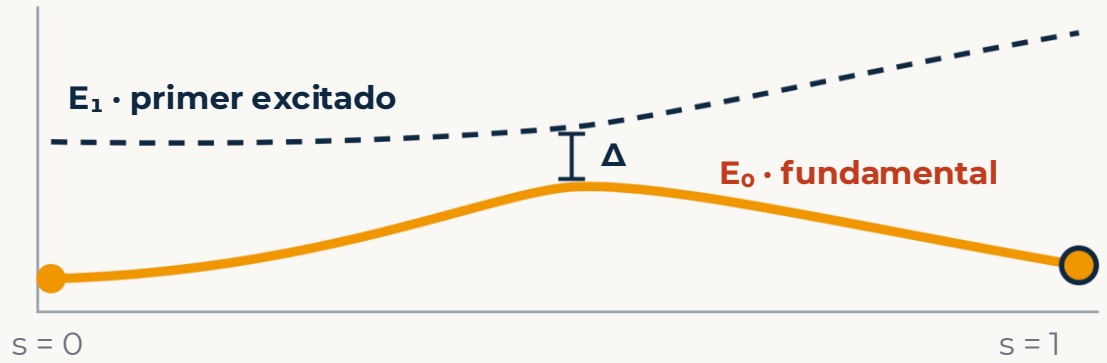
QAOA · VQE

Benchmarking: cada problema se ataca desde los tres paradigmas y se compara con solvers clásicos.

01 · OPTIMIZACIÓN QUBO NATIVA

Quantum annealing

Computación adiabática



$$H(s) = (1 - s)\, H_0 + s\, H_p$$

Se parte del estado fundamental de un hamiltoniano sencillo H_0 y se evoluciona hacia el del problema H_p. Si la evolución es lo bastante lenta frente al gap mínimo Δ, el sistema acaba en el estado de mínima energía: la solución.

Estado tecnológico actual

Conectividad dispersa: cada variable lógica es una cadena de qubits físicos (*minor-embedding*).

Era NISQ: ruido y coherencia limitada; no es computación adiabática pura.

Para qué lo usamos

Modelado QUBO de problemas reales

Set-packing, sequence-pair, TSP, graph coloring…

Annealer como herramienta auxiliar

Subproblemas y acople híbrido en modelado y ejecución.

Enfoques híbridos



MODELADO

Descomposición híbrida

- ADMM híbrido (ADMMOptimizer en Qiskit)
- Benders híbrido cuántico
- Generación de columnas

EJECUCIÓN

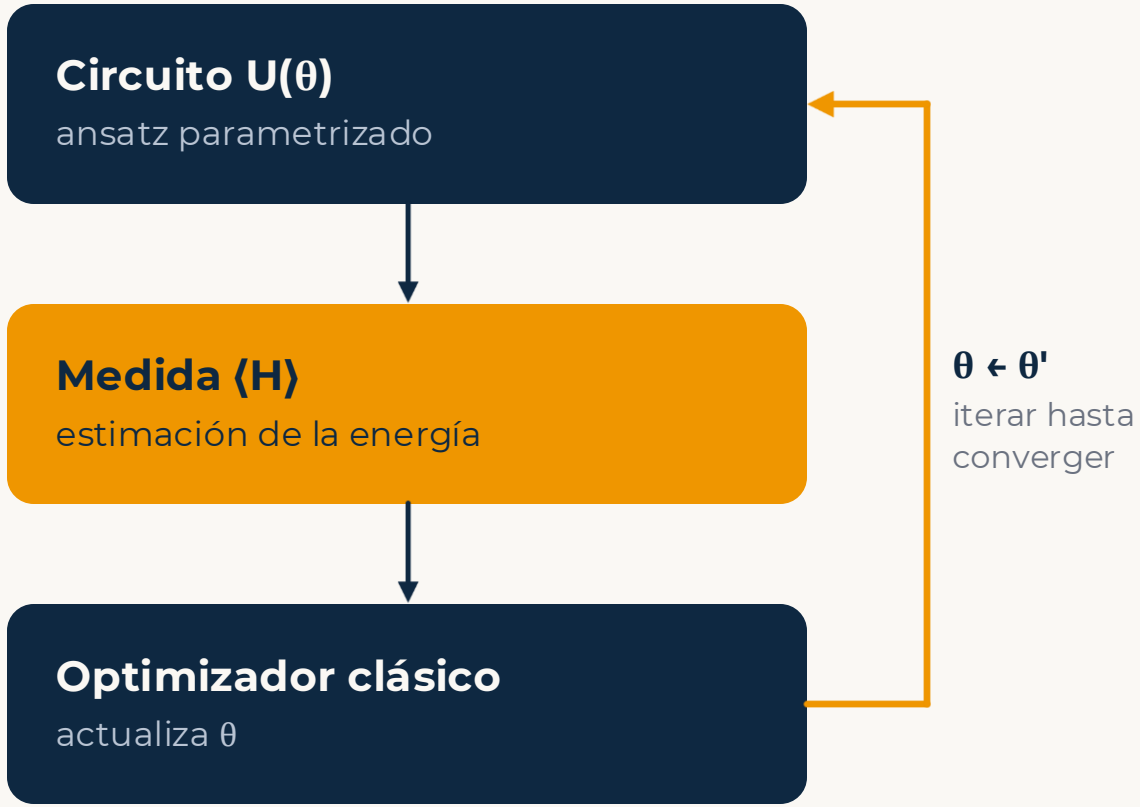
Solvers híbridos cuántico-clásicos

- El clásico descompone y gestiona las restricciones
- El cuántico resuelve los subproblemas más difíciles

Instancias mayores que las que caben en el hardware cuántico actual

03 · PARADIGMA DE PUERTAS (GATE-BASED)

Algoritmia variacional



QAOA Alterna capas de coste y mezclador. Orientado a optimización combinatoria (QUBO).

VQE Minimiza la energía de un hamiltoniano. El coste de medida crece con el número de strings de Pauli.

Lo que hacemos

- VQA para planificación de proyectos multi-habilidad (MS-RCPSP)
- Menos medidas: agrupación de strings de Pauli compatibles
- Emulación con y sin ruido; ejecución en QPU de puertas y simuladores HPC

Objetivos técnicos en QUIXOTE

Redes cuánticas híbridas

Optimización adaptativa

- Formular la gestión de redes QKD + PQC como problemas QUBO / Ising
- Reoptimizar ante cambios del canal y de la demanda de clave
- Comparar annealing, híbridos y puertas frente a solvers clásicos

Redes de sensores cuánticos

Optimización y gestión

- Optimización y gestión de redes de sensores cuánticos
- Analítica de datos segura sobre la información que generan

Ciberseguridad cuántica

PQC y QKD

- Simulación de la capa cuántica de enlaces QKD satelitales
- DLT segura frente a ataques cuánticos
- Necesidades de hibridación QKD-PQC
- Estado actual PQC



preguntas

Contacto

info@redcerveraquixote.es





[FIDESOL]

gradiant

itecam

i2cat

LORTEK
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI INNOVACIÓN

Centro de Excelencia Cervera