gradiant

Aplicación de las tecnologías cuánticas a las telecomunicaciones

Óscar Iglesias González & Gabriel María Carral López

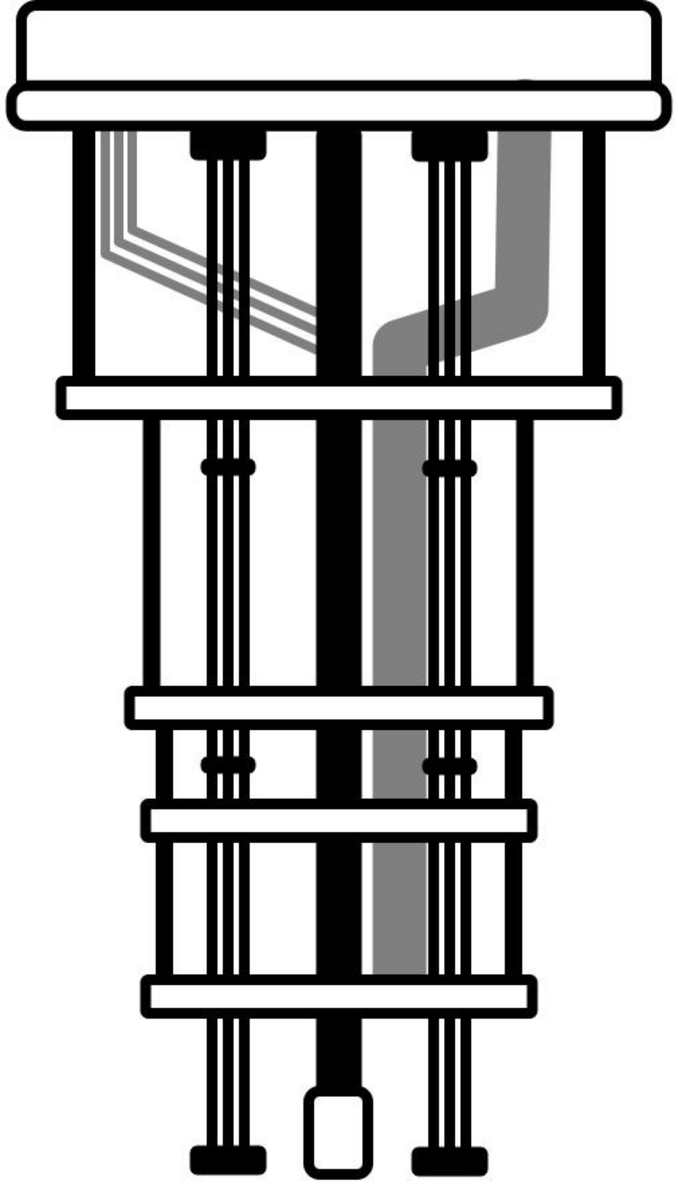
3 ejes de aplicación

- Computación cuántica
- Comunicaciones cuánticas
- Sensórica cuántica

Teleco hoy

Necesidades crecientes de:

- mayor ancho de banda
- menor latencia
- larga distancia
- gestión inteligente
- mayor seguridad
- mejor medida del campo EM y sincronización temporal



Quantum hoy

Era **NISQ**, limitaciones marcadas por:

- bajo número de qubits
- baja profundidad
- errores

Puesta en práctica de la **QKD**:

- Seguridad total, pero infraestructura cara y compleja, con ciertas limitaciones

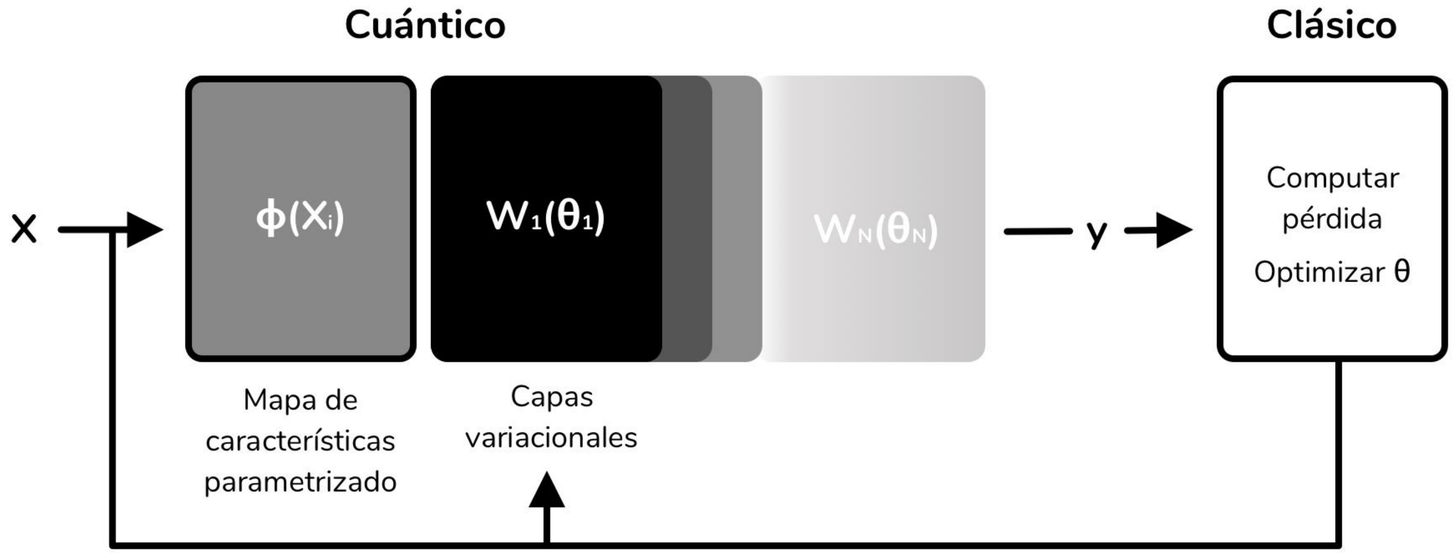
Desarrollo de la **sensórica cuántica**:

- Ventaja cuántica, pero complejidad experimental, quantum bottleneck

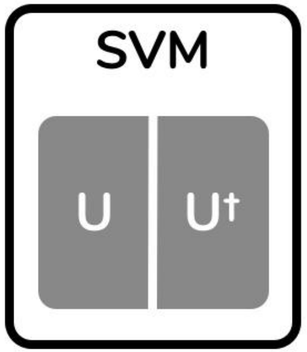
Circuitos variacionales y QML

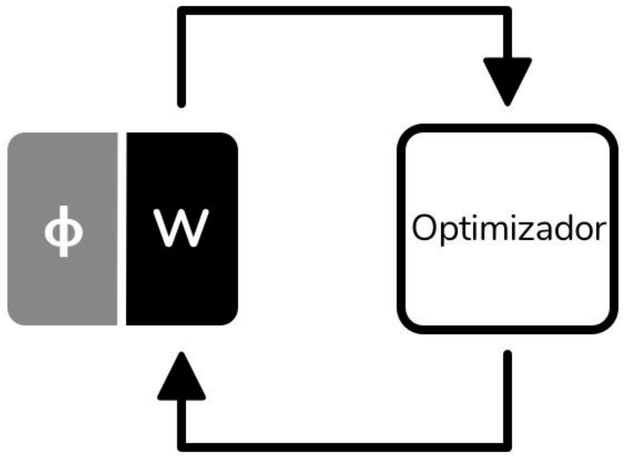
Basados en **puertas lógicas parametrizadas** y bucles de **optimización clásica**.

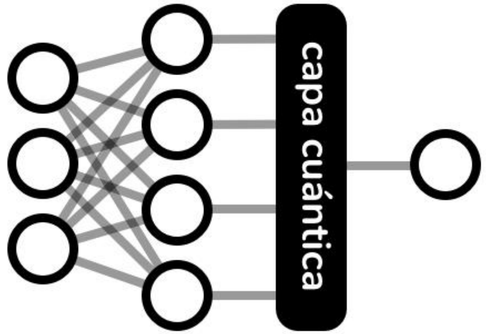
- Baja profundidad
- Circuitos generales de tamaño fijo
- Mitigación de errores implícita
- Conceptos familiares



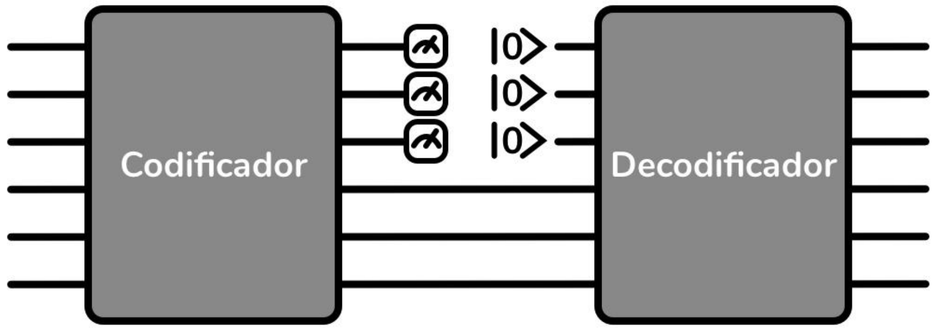
Algunos circuitos QML interesantes

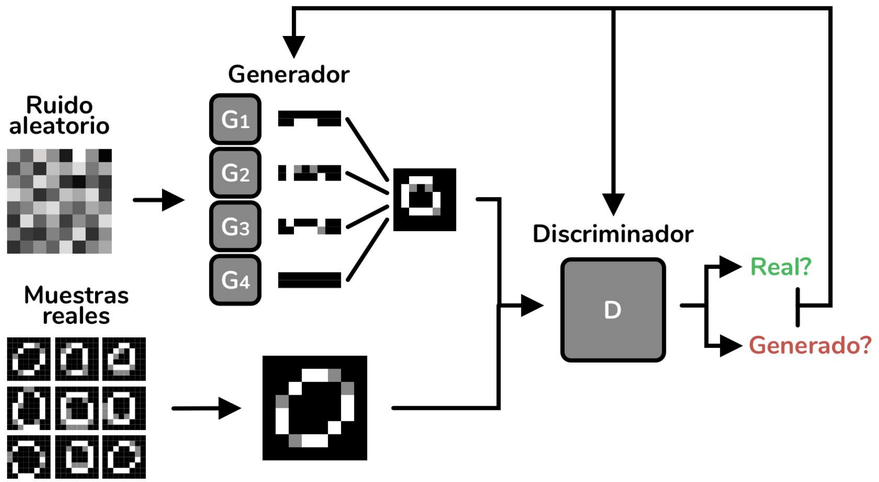




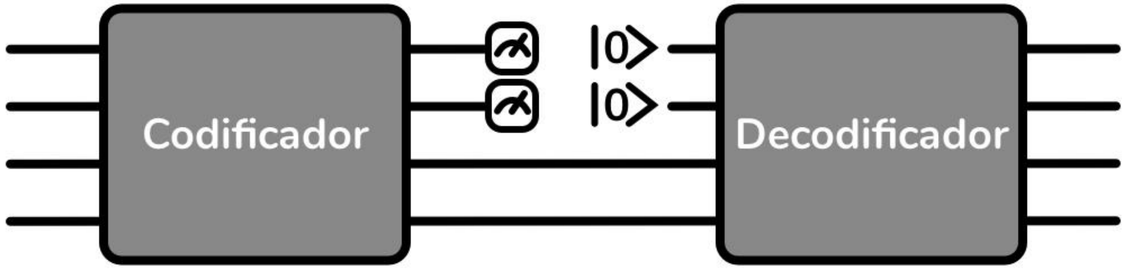


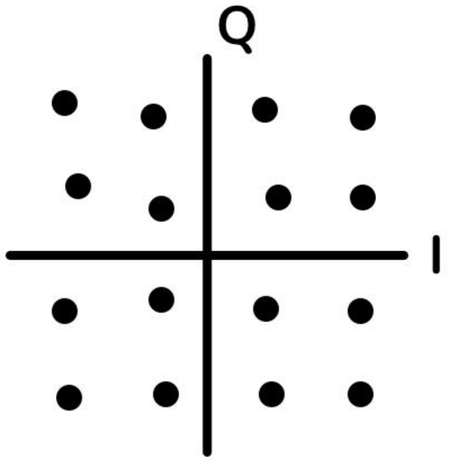
Algunos circuitos QML interesantes



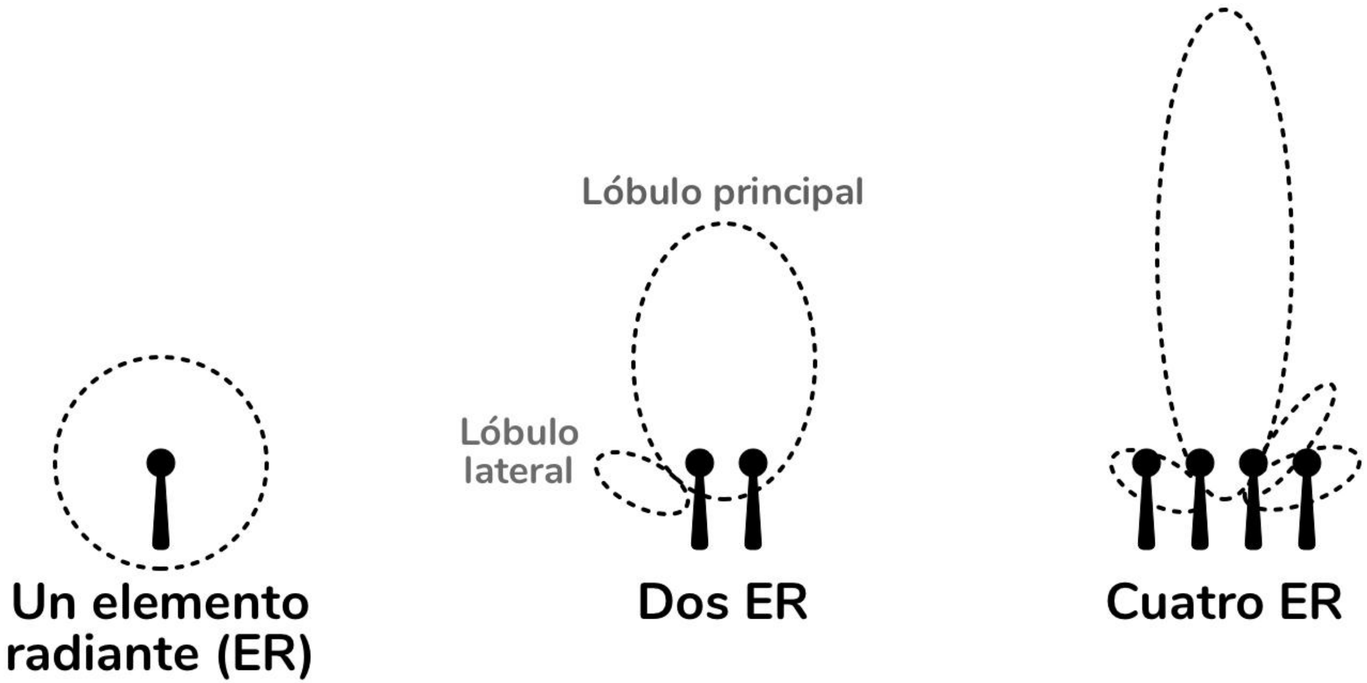


Sistemas de codificación-decodificación entrenables

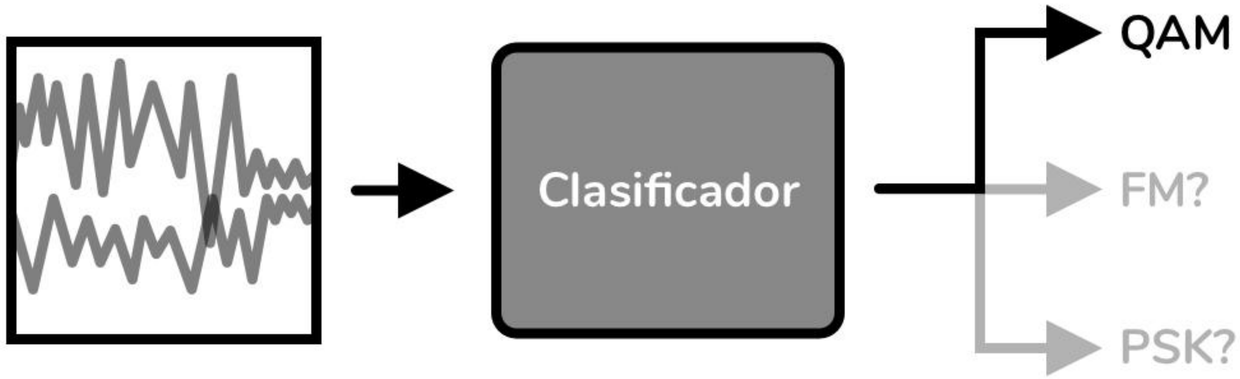




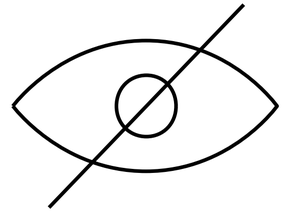
Optimización de conformado de haz



Detección de ciberataques



La criptografía de clave pública está en peligro!



La infraestructura de seguridad actual en las comunicaciones descansa, en gran parte, en sistemas criptográficos de **clave pública** como

- *RSA*
- *Diffie-Hellman*
- …

Se basan en problemas matemáticos que ***se creían*** **irresolubles** pueden atacarse con un ordenador cuántico (algoritmo de Shor):

- *Factorización números primos*
- *Logaritmo discreto*

Se abre una vulnerabilidad crítica: como solucionarla? Algoritmos resistentes a ordenadores cuánticos (**PQC**) y/o cripto simétrica **CON** distribución de clave cuántica (**QKD**)

AGENDA 2030

Criptografía post-cuántica (PQC)

Criptografía matemática: algoritmos que basan su seguridad en problemas muy complicados, como aquellos construidos a partir de:

- **Funciones hash (NIST)**
- **Lattices** (celosías) **(NIST)**
- Teoría de códigos
- Isogenias
- Polinomios de múltiples variables

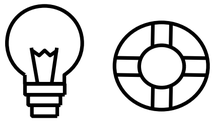
Ventajas:

- No se necesita hardware específico
- Se podría usar la infraestructura ya disponible (“actualización de software”).

Desventajas:

- Coste computacional de estos algoritmos, energía, rapidez (IoT!)
- Seguirán siendo seguros en el futuro?

Distribución de clave cuántica (QKD)



“Peculiaridades” cuánticas que podemos usar a nuestro favor para, entre otras cosas, ***cuantificar si un espía está monitoreando el canal de comunicación!***

- Principio de superposición
- Colapso de la función de onda
- Principio de incertidumbre de Heisenberg
- Aleatoriedad inherente (QRNG)
- Entrelazamiento
- Desigualdades de Bell
- Teorema de No Clonado

Quantum Key Distribution

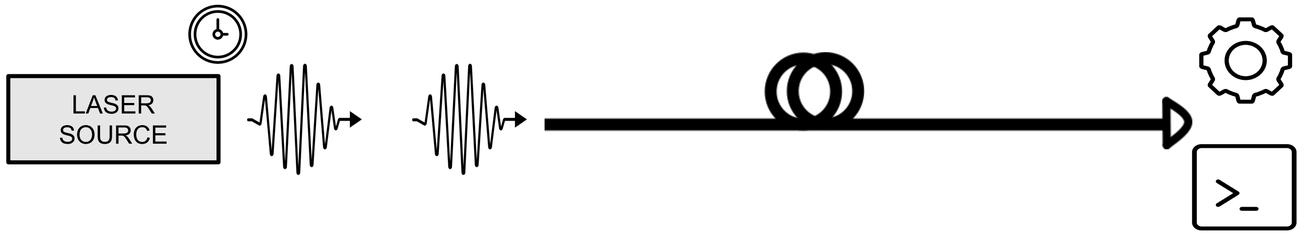
Codificar información en sistemas cuánticos: el mejor flying qubit*, el* ***fotón***

Usar un **grado de libertad del fotón** y codificar información binaria en el:

- Polarización
- Camino
- Tiempo de llegada
- Fase
- …

En términos de **tecnología** necesitamos:

- Fuentes (idealmente *single-photon*)
- Canales de transmisión (fibra, espacio libre)
- Detectores



1010001010110101 (secret key, after EC and PA)

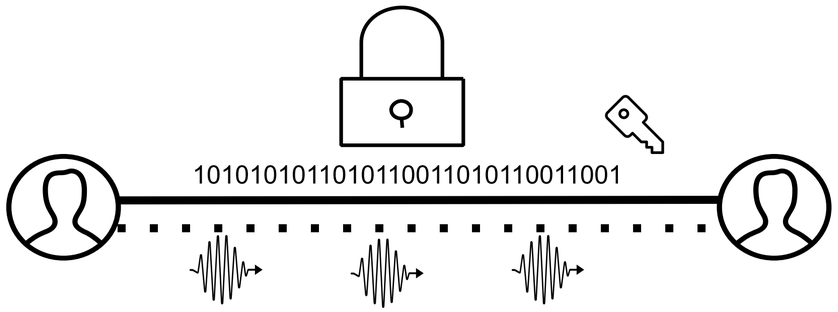
Qué promete la QKD: information-theoretic security

Seguridad incondicional, al **combinar**

- Generación de una clave simétrica totalmente secreta

  &

- Algoritmos seguros de cifrado mediante clave simétrica (OTP, AES)



1010010101 (QKD generated) XOR mensaje = indescifrable

Desventajas:

- Hardware dedicado, gran inversión en infraestructura (*avances: combinar los medios actuales con QKD para minimizar costes, SDN en redes metropolitanas, P&P QKD*)

- Limitaciones de distancia (*avances: TF-QKD*)

- Equipamiento realista (=imperfecto) puede disminuir la seguridad (*avances: MDI-QKD, DI-QKD*)

A futuro: Internet cuántico

Quantum Internet Alliance, EuroQCI…

Landscape

- Convivencia previsible de PQC y QKD
- Nodos asegurados mediante QKD
- **Computación cuántica distribuida** y **a ciegas** (BQC), **acuerdo bizantino**…

Mucho trabajo por hacer:

- **Estandarización** (IETF…)
- Avances en hardware cruciales: repetidores (incluyendo memorias), QPUs, infraestructura QKD

El ordenador cuántico en la nube desconoce los contenidos del job que se le ordena realizar

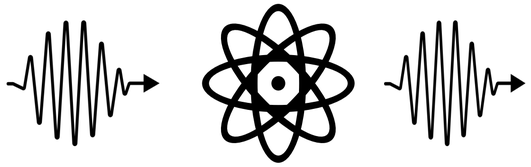
Sensórica cuántica

Medidas más **precisas** y **sensibles**, aprovechando la "delicadez" de los sistemas cuánticos

- Medidas del campo EM
- Relojes ópticos
- Uso de estados **no-clásicos** (squeezed, entrelazados) para superar el Standard Quantum Limit

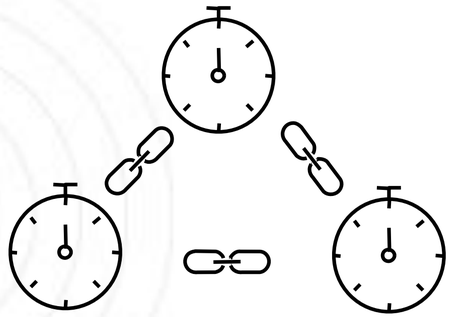
Plataformas (ejemplos):

- **Átomos de Rydberg** para campo E



- **Centros NV** para campo B y E + nodos red cuántica

- **Relojes ópticos que mejoran a los atómicos**: mejor referencia temporal
- Posibilidad de tener **relojes/sensores distribuidos** en un Internet cuántico, con notables mejoras



gradiant

Óscar Iglesias González &
Gabriel María Carral López

oiglesias@gradiant.org

gcarral@gradiant.org

A iniciativa do Polo de Tecnoloxías Cuánticas de Galicia conta con financiamento de:

Fondos REACT EU

AXENCIA GALEGA DE INNOVACIÓN

UNIÓN EUROPEA

Xacobeo 21·22

CESGA
Centro de Supercomputación de Galicia

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

Apoiar a transición cara a unha 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.

PROGRAMA OPERATIVO
FEDER GALICIA
2014-2020

Unha maneira de facer Europa