CESGA
GALICIA SUPERCOMPUTING CENTER

Las tecnologías cuánticas y la Investigación en ciberseguridad

Natalia Costas Lago
Mariamo Mussa Juane | Andrés Gómez
Fundación CESGA

CESGA
GALICIA SUPERCOMPUTING CENTER

¿Qué es el CESGA?

MISIÓN

“Contribuir al avance de la Ciencia y de la Técnica mediante la Investigación y la Aplicación de la Computación y las Comunicaciones de altas prestaciones, […], para beneficio de la Sociedad”

70%

XUNTA DE GALICIA

30%

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

Usuarios CESGA

Universidades

UNIVERSIDADE DA CORUÑA

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Universidade de Vigo

CSIC

MBG MISIÓN BIOLÓGICA DE GALICIA

IIM Instituto de Investigaciones Marinas de Vigo

IIAG

CSIC

Xunta

E.S.O.

Ensinanza Secundaria (*)

Entidades pub.

CEIDA

FEUGA

VIGO
CORUÑA
SANTIAGO

IEO

CENTRO OCEANOGRÁFICO DE CORUÑA

Salud

Complexo Hospitalario Universitario de Santiago de Compostela

RTD Centres

CTC centro tecnolóxico da carne

CIS CENTRO DE INNOVACIÓN E SERVIZOS DE GALICIA

intecmar

ANFACO

cetmar

tecnópole

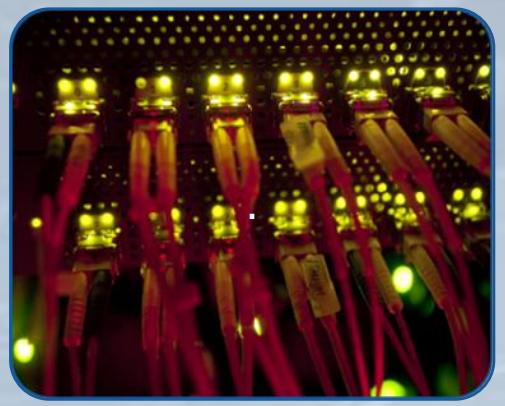
Otros

RES
Proyectos
Convenios

Servicios CESGA

HIGH PERFORMANCE COMPUTING

IA (ML, DL)
BDATA, CLOUD,...



Comunicaciones

Adaptados a la evolución tecnológica y a las necesidades de los investigadores y usuarios de cualquier área de conocimiento o sector productivo.

CESGA
GALICIA SUPERCOMPUTING CENTER

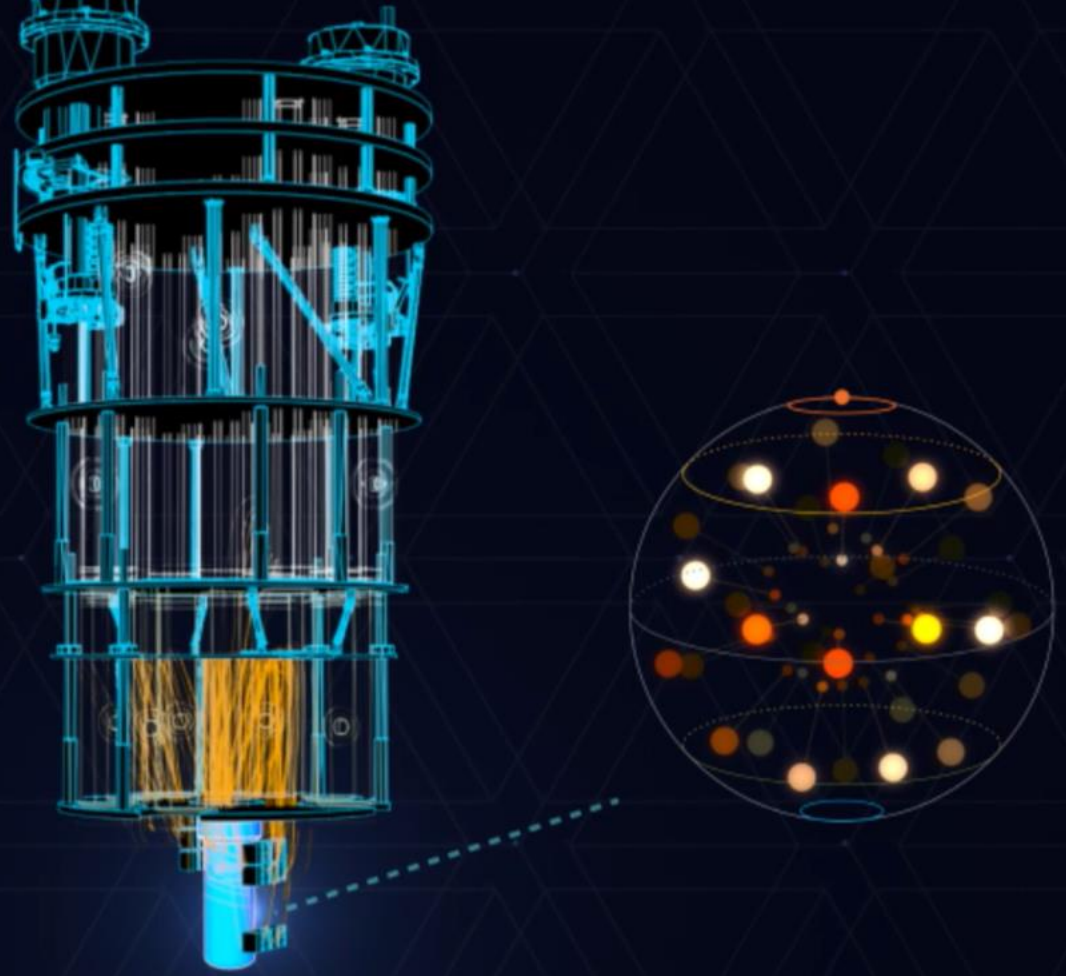
Las tecnologías cuánticas

Tecnologías Cuánticas

- **Nuevos sensores:** uso de física cuántica para mejorar la sensibilidad
  - Nuevos relojes, gravímetros, magnetómetros, radares, etc.
- **Nueva computación**. “Computadoras Cuánticas”. Usa la física cuántica para calcular.
  - **Supercomputación**, criptoanálisis y decodificación o utilizado para vigilancia y detección.
- **Nuevas comunicaciones**:
  - **Quantum Key Distribution (QKD)**. Mejora de los protocolos criptográficos clásicos utilizando canales cuánticos para intercambiar claves.
  - Nueva Internet Cuántica. Permitirá intercambiar información entre dispositivos cuánticos.

CESGA
GALICIA SUPERCOMPUTING CENTER

Computación cuántica

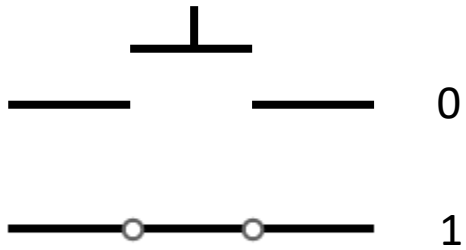


¿Qué es la computación cuántica?

La computación cuántica computa
usando las leyes de la mecánica cuántica

La unidad mínima de información es el qubit

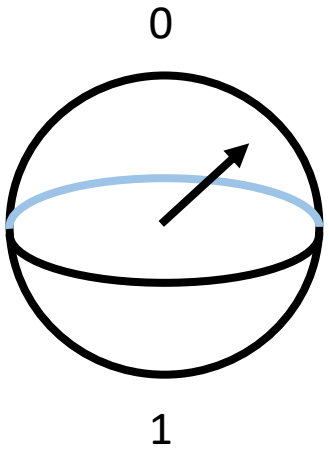
clásica



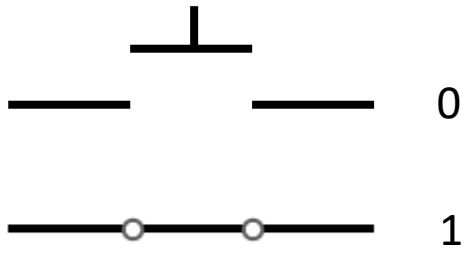
bit

unidad mínima de información

cuántica



clásica

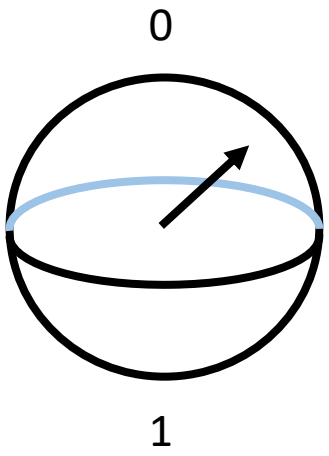


qubit

bit

unidad mínima de información

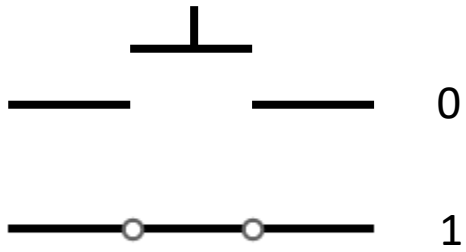
cuántica



medimos

¡colapsa!

clásica



qubit

bit

unidad mínima de información

Benioff (80)

Manin (80)

1^{er} modelo de computación cuántica universal

Simular la naturaleza con sistemas cuánticos

LA NATURALEZA NO ES CLÁSICA, #$%,
PARA SIMULARLA MÁS VALE HACERLO CON
MECÁNICA CUÁNTICA.

fundamentos

Feynman (82)

¿Qué cabe esperar?

(nivel teórico)

Un computador cuántico va a permitir resolver problemas …

… en menos tiempo que un computador clásico

Rapidez cuántica

Un computador cuántico va a permitir resolver problemas …

… en menos tiempo que un computador clásico

Rapidez cuántica

… inabordables para un computador clásico (Shor)

Ventaja cuántica

Un computador cuántico va a permitir resolver problemas …

… en menos tiempo que un computador clásico

Rapidez cuántica

… inabordables para un computador clásico (Shor)

Ventaja cuántica

… de forma más eficiente a nivel implementación

Mejora cuántica

Un computador cuántico va a permitir resolver problemas …

… en menos tiempo que un computador clásico

Rapidez cuántica

… inabordables para un computador clásico (Shor)

Ventaja cuántica

… de forma más eficiente a nivel implementación

Mejora cuántica

… con menor gasto energético

Eficiencia cuántica

rapidez!

Deutsch-Jozsa (92)

1^{er} Algoritmo exponencialmente más rápido que su versión clásica

ventaja!

Shor (94)

Factorización de grandes números

rapidez!

Grover (96)

Algoritmo exponencialmente más rápido que su versión clásica con aplicación:
búsqueda en bases de datos

nivel teórico

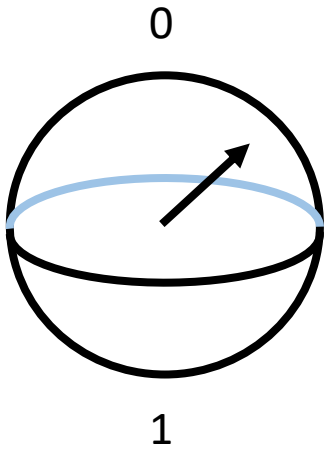
¿Dónde estamos?

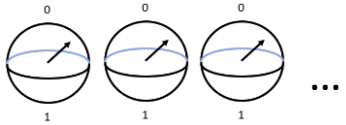
(nivel empírico)

Teórico → Práctico

Requisitos de DiVincenzo

Establecer las bases para la construcción de computadores cuánticos

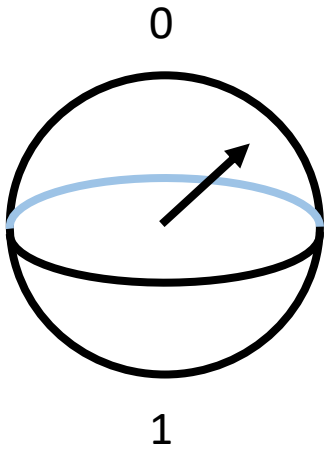




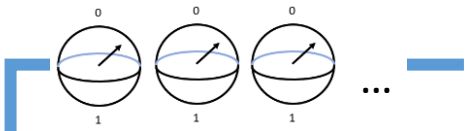
...

Cubit bien caracterizado y escalable

Sistema aislado
indiferente a perturbaciones (ideal)

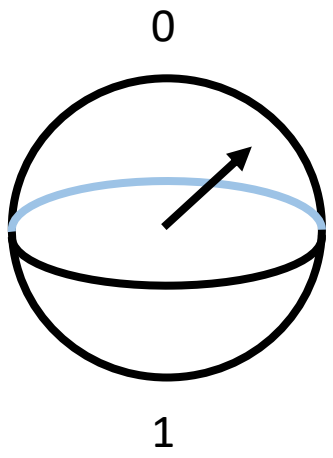


Cubit bien caracterizado y escalable



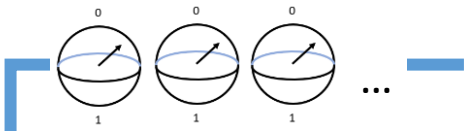
Sistema aislado
indiferente a perturbaciones (ideal)

inicializar → transformar → medir



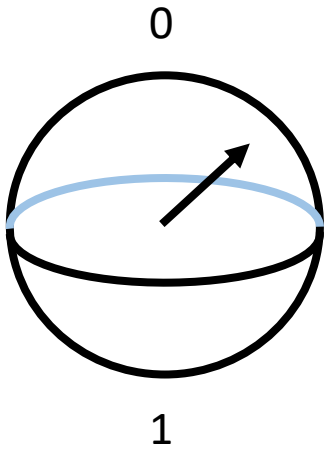
Cubit bien caracterizado y escalable

¡ruido!



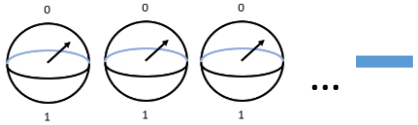
Sistema aislado
indiferente a perturbaciones (ideal)

inicializar → transformar → medir



¡Era **NISQ**!

Cubit bien caracterizado y escalable → **¡ruido!**



Sistema aislado
indiferente a perturbaciones (ideal) →

inicializar → transformar → medir →

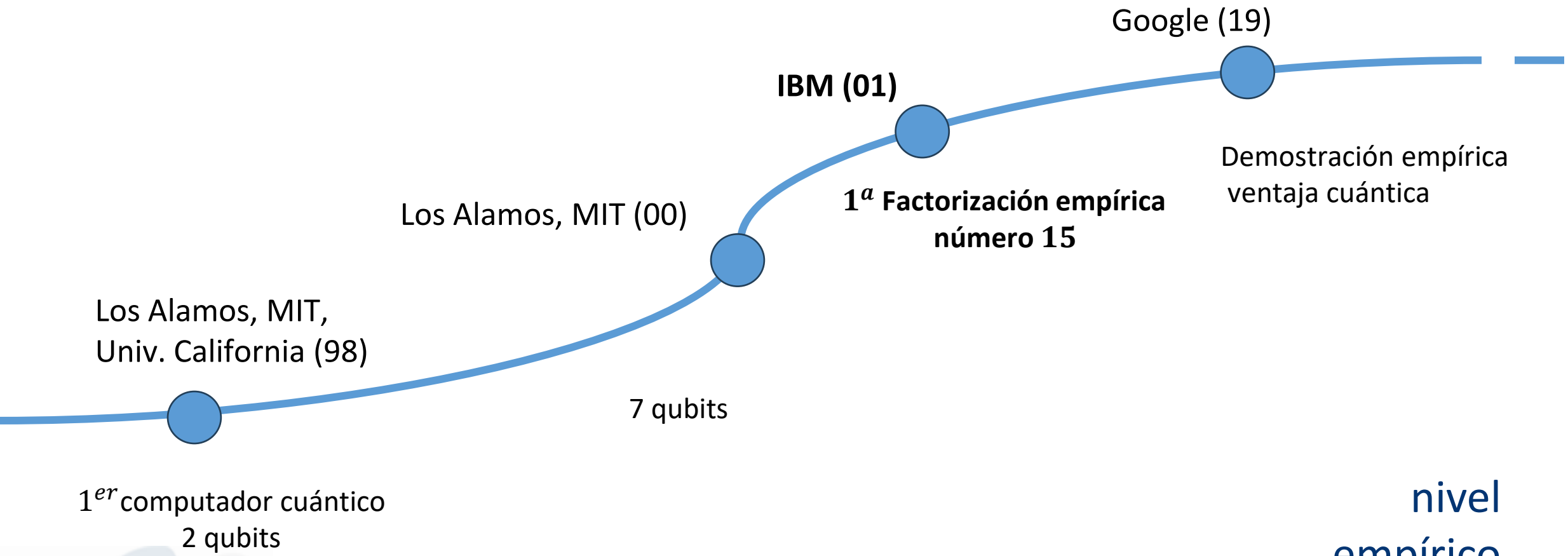
¡Era **NISQ**!

Computadores

N*oisy* **->** ruidosos

I*ntermediate-****S****cale* **->** de escalas intermedias

Q*uantum era*



nivel empírico

El algoritmo de Shor en la era NISQ

¿Cuándo se podrá romper los algoritmos de encriptado?

Algoritmo de Shor necesita:

- **Cubits muy estables** (horas/días/semanas). Ahora estamos del orden de segundos o menos.
- **Una mejor conectividad** entre qubits.
- **Muchos más qubits**. Para claves de 2048 bits, se estima que necesitaremos 20 millones y 8 horas (en el mejor de los casos).
- Doblando anualmente el número de qubits (¿ley de Moore?), **partiendo del valor actual 433**: 2038.

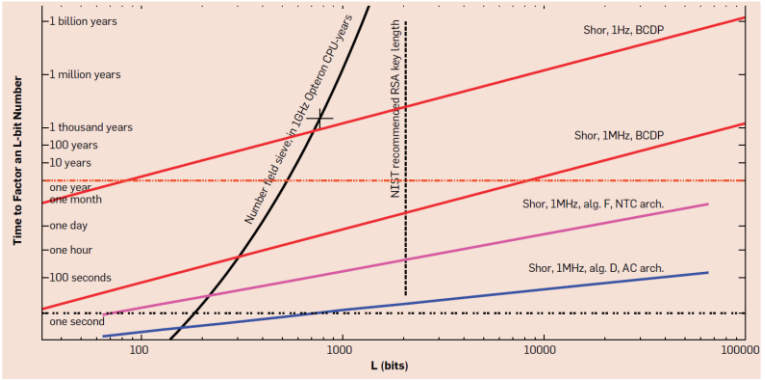
Ir pensando en cambiar el algoritmo de firma y cifrado (**criptografía post-cuántica**)

NIST y Matteo Mariantoni (PQCrypto 2014): primer ordenador cuántico criptográficamente relevante **podría construirse en 2030.**

How a quantum computer could break 2048-bit RSA encryption in 8 hours

MIT Technology Review

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

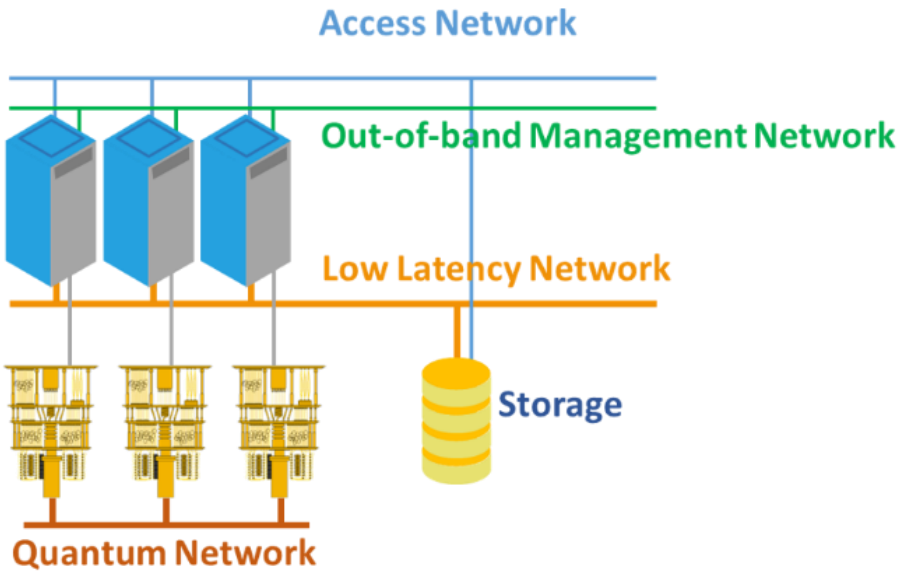


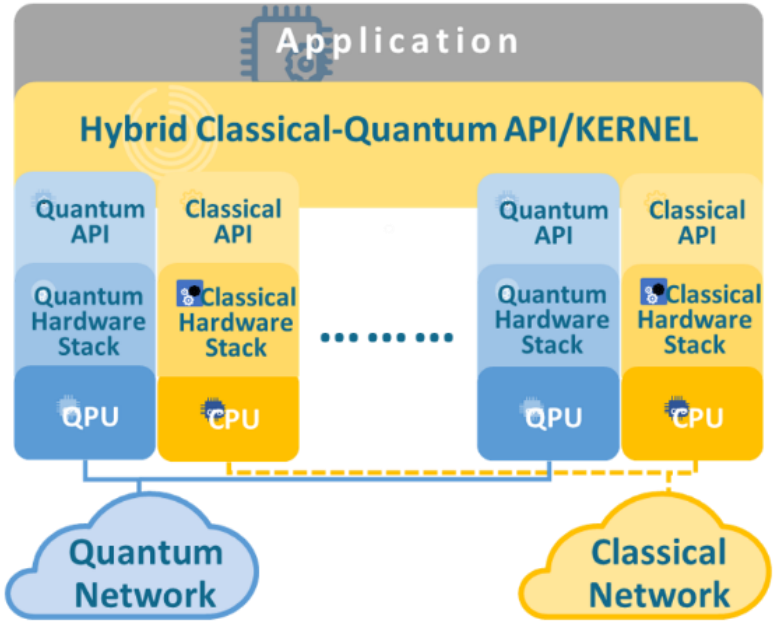
Fuente: Van Meter, R., & Horsman, C. (2013) http://doi.org/10.1145/2494568

¿¡Visión CESGA!?

Un computador cuántico no existe per se

Computación híbrida distribuida





¡El CESGA está instalado el computador de acceso público con mayor nº de cubits (32) de Europa!

Comunicaciones cuánticas

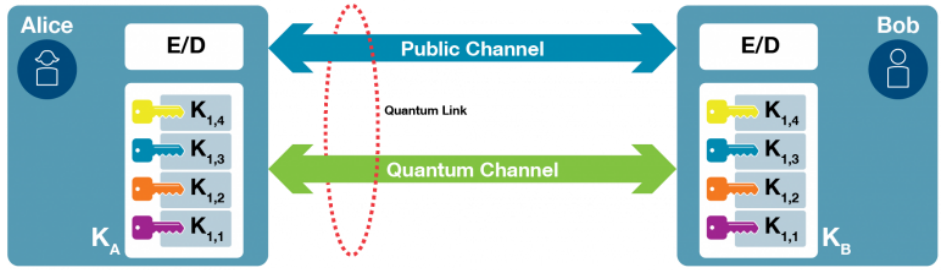
Distribución de clave cuántica (QKD)

Distribución de clave cuántica (QKD)

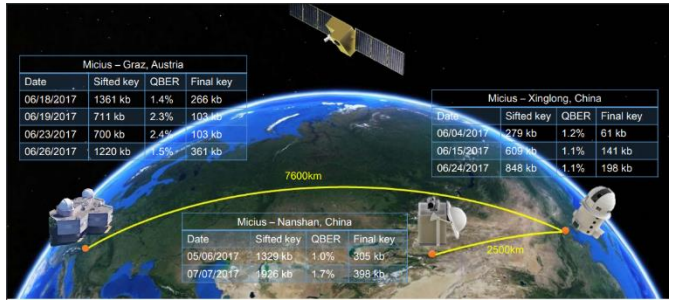
- **Características:**
  - Genera claves simétricas entre puntos distantes aprovechando propiedades de la mecánica cuántica
  - En fibra o espacio libre

- **Limitaciones:**
  - Topologías **limitadas** (punto-punto, estrella).
  - **Distancia limitada** para despliegues en fibra
  - **Coexistencia** de canales clásicos y cuánticos en un mismo medio de transmisión.

- **Seguridad:**
  - Seguridad **teóricamente perfecta** por los propios principios de la física cuántica.
  - La implementación, incluyendo la parte clásica, puede ser insegura (como siempre).



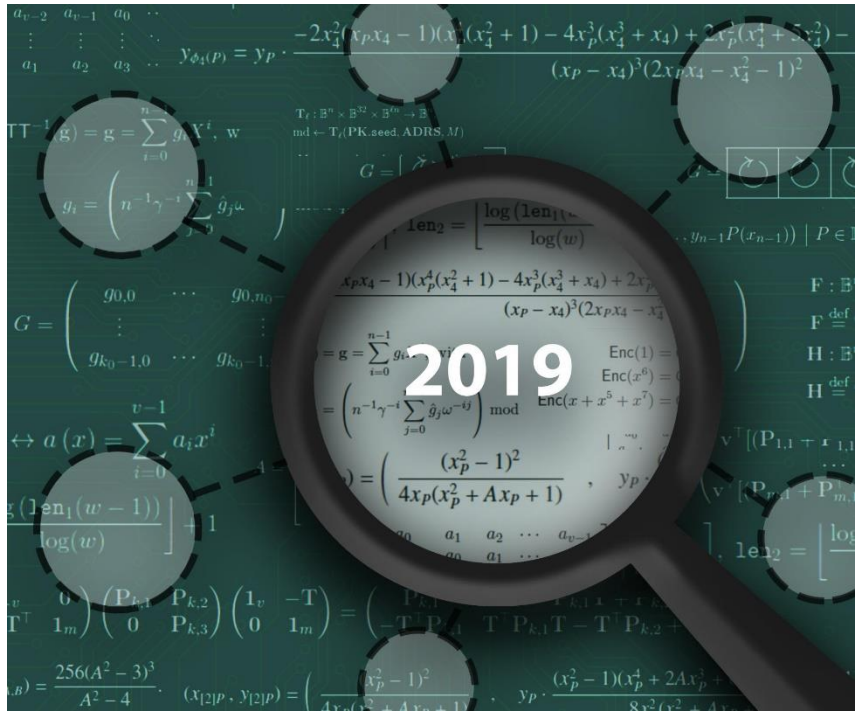
https://securecommunications.airbus.com/en/news/quantum-key-distribution-qkd-networks-key-management



Phys. Rev. Lett. 120, 030501 (2018)

Cifrado poscuántico

- Algoritmos **se consideran seguros ante ataques** mediante medios **cuánticos o clásicos**
- NIST inició proceso de estandarización iniciado en 2016.
  - Algoritmos identificados para estandarización (tras 3ª ronda):
    - Public Key Encryption/KEMs: Crystals-Kyber
    - Digital Signatures: Crystals-Dilithium, Falcon, Sphincs+
  - Una 4ª ronda permitirá incluir nuevos algoritmos para el proceso de estandarización.
- Permitirán interoperar con las redes y protocolos de comunicación existentes y **complementarán a las tecnologías QKD**.



Credit: N. Hanacek/NIST

Comunicaciones cuánticas: Área estratégica

Las comunicaciones cuánticas (CC) se reconocen como un sector especialmente estratégico dentro de las tecnologías cuánticas de segunda generación. Esto se evidencia en los diversos programas de CC en muchos países, desde Estados Unidos hasta China.

- **En Europa dos grandes iniciativas:**
  - Quantum Flagship: Iniciativa de investigación a largo plazo con presupuesto de 1.000 millones con el objetivo de poner a Europa en la vanguardia de la segunda revolución cuántica.
  - EuroQCI: Programa de infraestructura a 10 años con el objetivo de crear una red de comunicaciones cuánticas panaeuropea.
- **En España:**
  - Programa Complementario de Comunicaciones Cuánticas
- **En Galicia:**
  - Polo de Tecnologías Cuánticas

Polo de Tecnologías Cuánticas de Galicia

Polo de tecnologías cuánticas de Galicia

- Misión 2021-2030

> Conseguir un **impulso disruptivo** de las **Tecnologías Cuánticas** en computación e comunicaciones, en **Galicia y España**, para el avance de la Ciencia, de la Tecnología y de la Economía, para el beneficio de la sociedad

- Liderado por el CESGA y el Vigo Quantum Communications Center (VQCC) de la Universidad de Vigo, con la participación de las Universidades de Coruña y Santiago de Compostela.

- Plan de **inversiones en infraestructura**

Infraestructura de computación cuántica

- **Despliegue de infraestructura de <u>computación cuántica</u>:**
  - **1 Computador cuántico de 32 qubits** (sept/2023)
  - 2 Simuladores cuánticos (sept/2023)
  - Infraestructura HPC de soporte (sept/2023)
  - 1 Generador de números aleatorios
    - Orientado a la investigación.
- **Investigación en computación cuántica**

(también financiada vía PCCC)
- Algoritmia | Benchmarking

Actividades financiadas por:

AXENCIA GALEGA DE INNOVACIÓN

UNIÓN EUROPEA

Xacobeo 21·22

Despliegue de una infraestructura basada en tecnologías cuánticas de la información que permita impulsar la I+D+i en Galicia. Operación financiada por la Unión Europea, a través del FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER), como parte de la respuesta de la Unión a la pandemia de la COVID-19.
PROGRAMA OPERATIVO
FEDER 2014-2020
Una manera de hacer Europa

<NE|AS|QC>

Este proyecto recibe financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención n.º 951821.

Quantum SPAIN

España | digital 2026

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

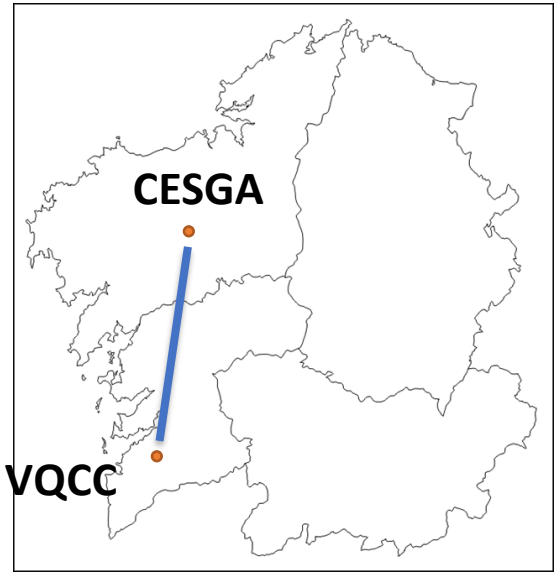
Financiado por la Unión Europea NextGenerationEU

RES RED ESPAÑOLA DE SUPERCOMPUTACIÓN

Apoyado económicamente por el Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España a través de la convocatoria del proyecto QUANTUM ENIA - proyecto Quantum Spain, y por la Unión Europea a través del Plan de Recuperación, Transformación y Resiliencia NextGenerationEU en el marco del Proyecto España Agenda Digital 2025.

Infraestructura de comunicaciones cuánticas

- **CESGA**
  - **Despliegue de un enlace QKD entre Santiago y Vigo**
  - Demostración de casos de uso reales del enlace la QKD.
- **VQCC**
  - **Despliegue de 3 laboratorios de experimentación** en CC en el VQCC, así como potenciación en su línea de investigación teórica en estas líneas



Polo de tecnologías cuánticas de Galicia

Financiación del Plan Complementario de Comunicaciones Cuánticas

- Fondos Next Generation EU (MRR)

This work was supported by MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and with own funding from the Galician Regional Government through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication.

- Fondos propios de la Xunta de Galicia a través de la Axencia Galega de Innovación

Subvencionado por la Axencia Galega de Innovación.

Conclusiones

- Las **tecnologías cuánticas presentan una disrupción** en muchos ámbitos de conocimiento, específicamente en el de ciberseguridad.
- La **Estrategia de Ciberseguridad de la UE destaca la computación cuántica y el cifrado como tecnologías clave** (junto con la IA) para lograr resiliencia, soberanía y liderazgo tecnológico.
- CESGA, bajo los diversos programas de financiación públicos, está en proceso de despliegue de **infraestructuras de computación y comunicaciones** cuánticas de gran relevancia para la comunidad investigadora.

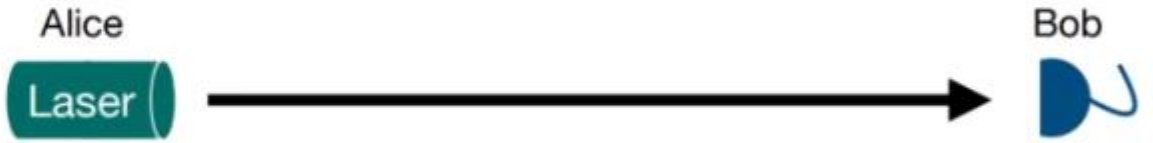
CESGA
GALICIA SUPERCOMPUTING CENTER

¡GRACIAS!

natalia@cesga.es
mmussa@cesga.es

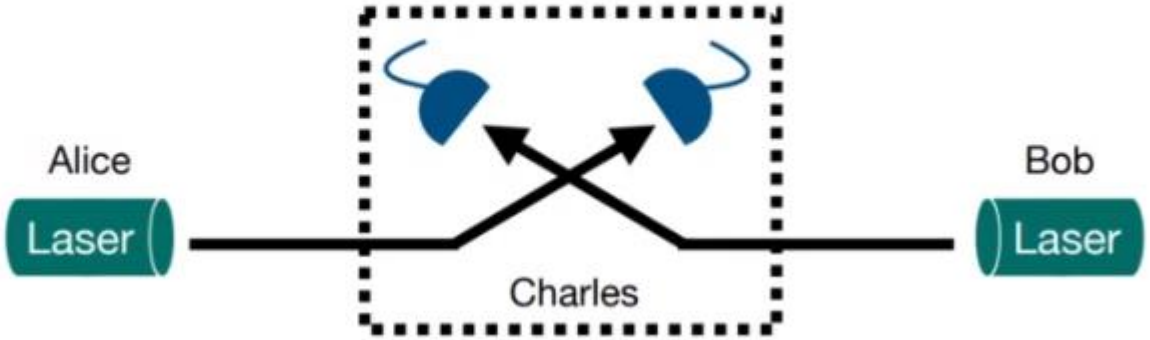
QKD protocols: Types

Prepare & measure



Entanglement based

Interferometric based

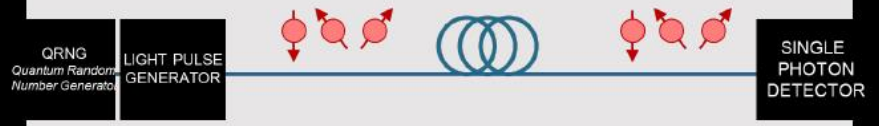


Distribución de clave cuántica (QKD). DV y CV

TWO SOLUTIONS FOR DIFFERENT SCENARIOS

Discrete-Variable QKD

- ~~Commercial systems available~~
- Single photon detection
- Distances up to 120 km
- Limited co-propagation
- High system and implementation cost

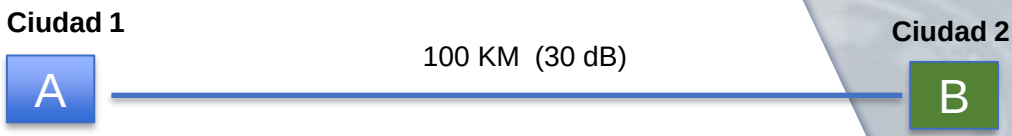


Continuous-Variable QKD

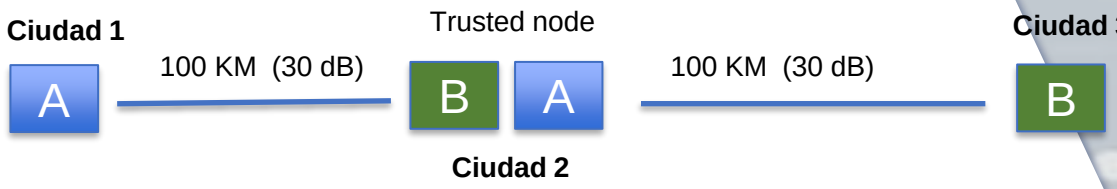
- Coherent detection
- High co-propagation capabilities
- Distances up to 40 km
- Mature telecommunication components
- Reduced system and implementation cost

Distribución de clave cuántica (QKD). Architectures

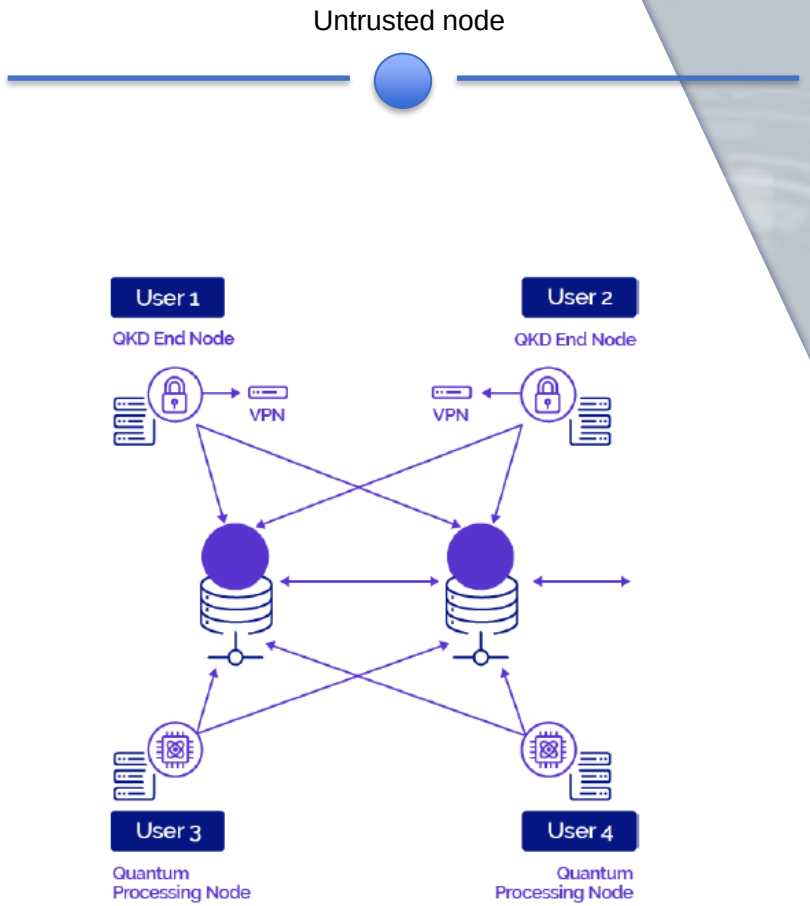
DV QKD (generalmente BB84 con decoy states)



Arquitecturas basadas en nodos confiables



Distribución de clave cuántica (QKD). Architectures



Interference based QKD

MDI QKD ??

Entangled based QKD

Twin-Field QKD??

Distribución de clave cuántica (QKD). Architectures

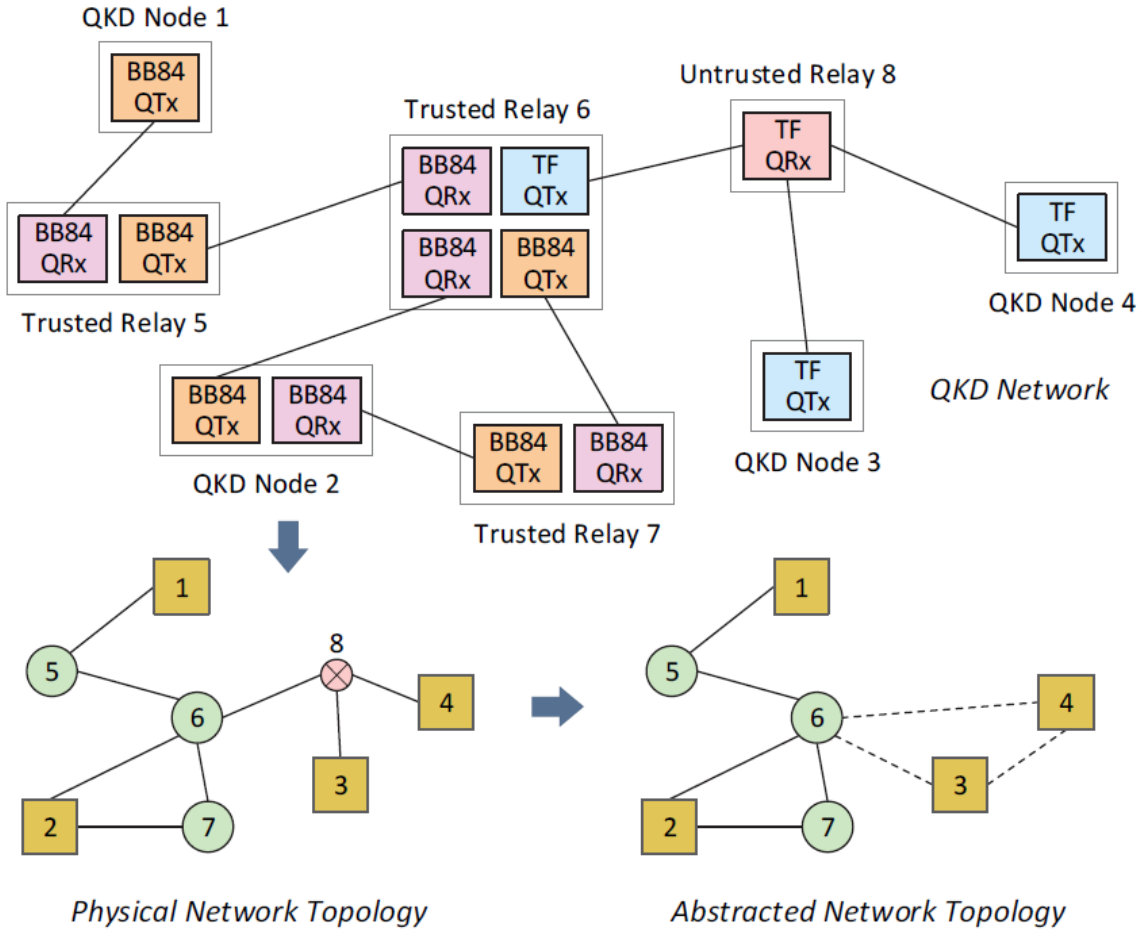


Fig. 4. Physical and abstracted network topologies corresponding to the QKD network emulated in the testbed.

Distribución de clave cuántica (QKD). ARQUITECTURAS COMPLEJAS. SDN o estilo protocolos de routing

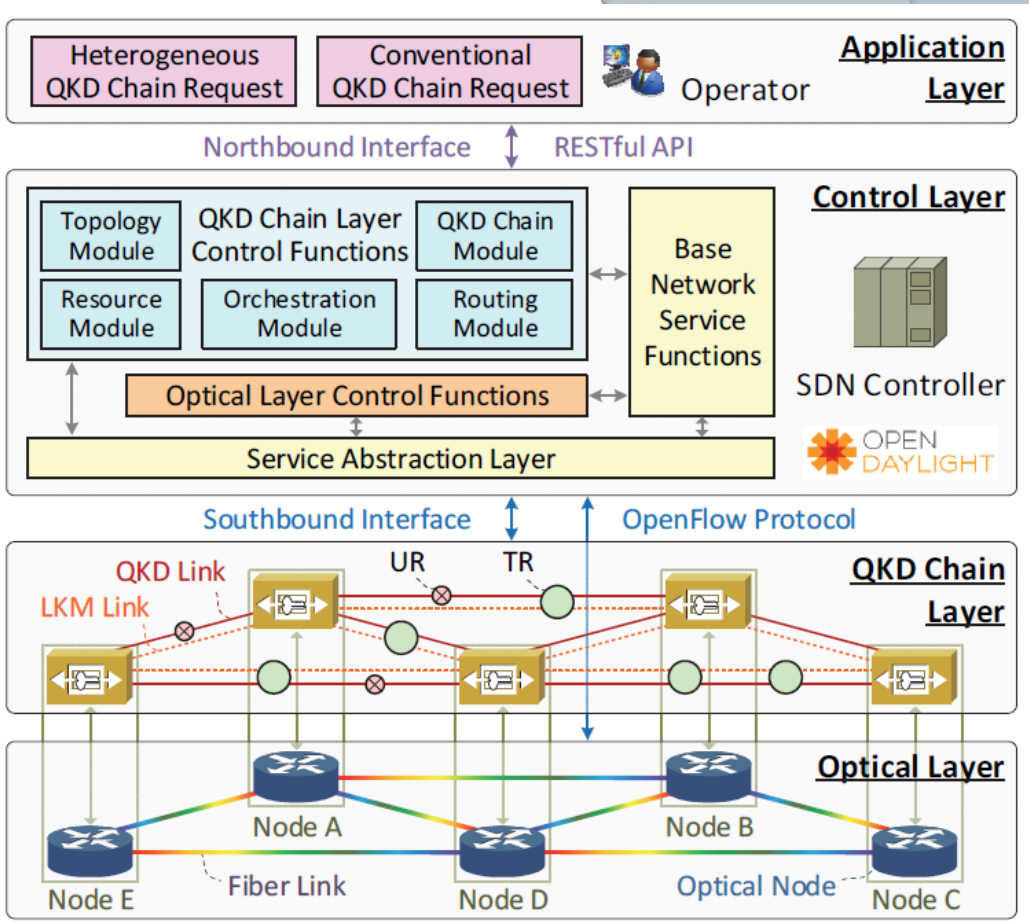
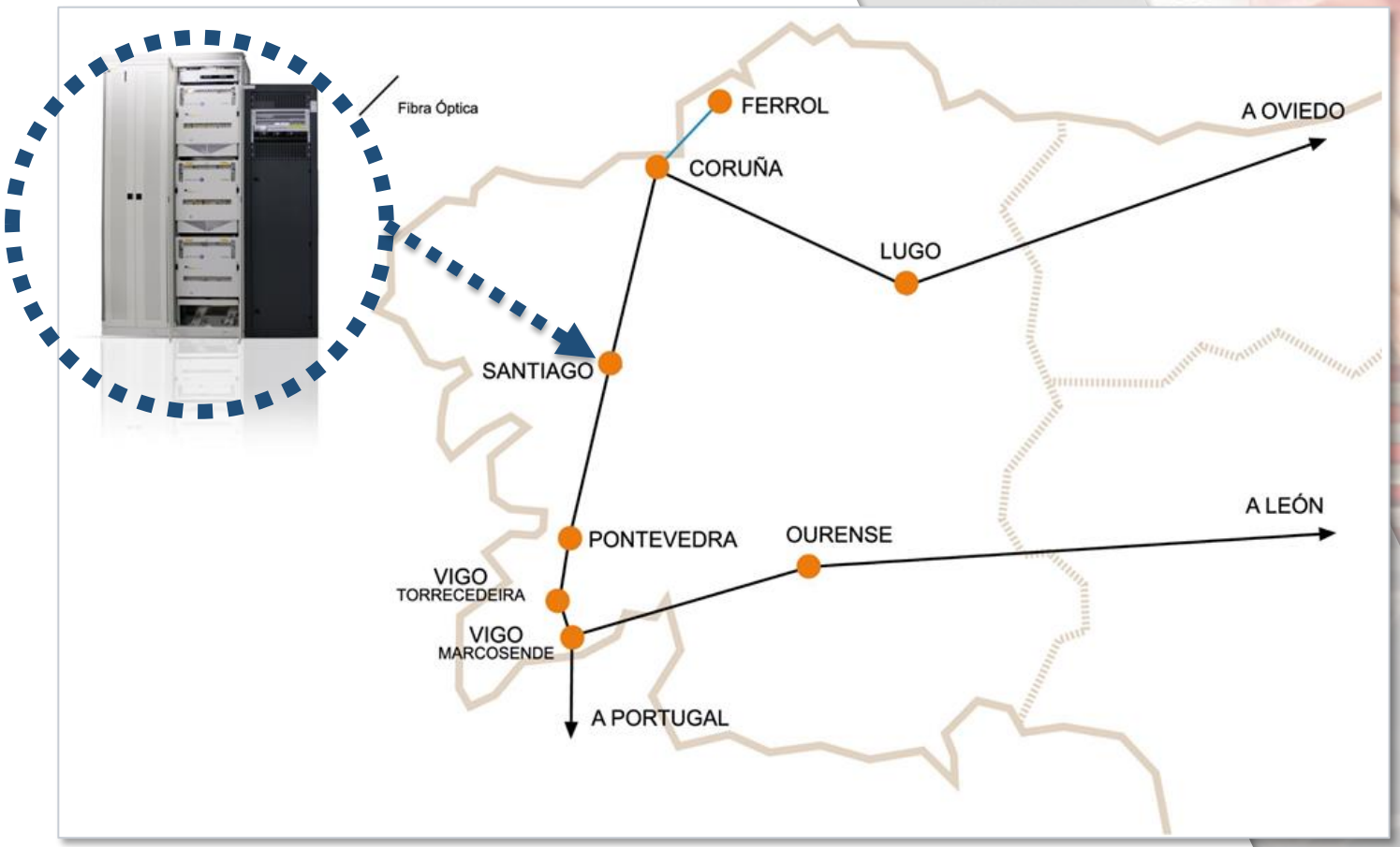
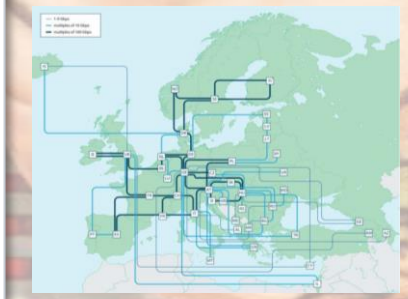


Fig. 1. An architecture of SDN-based QKD chain over optical networks. [LKM: local key manager; UR: untrusted relay; TR: trusted relay]

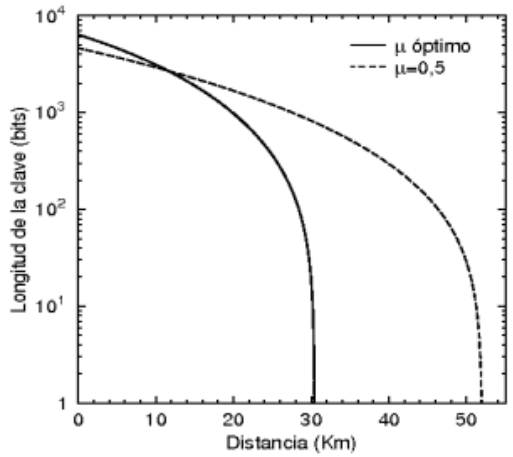
Integración cuántico-clásico



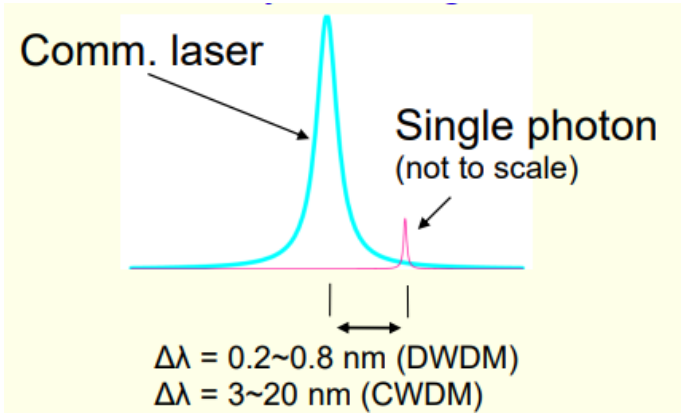


Soluciones y retos:

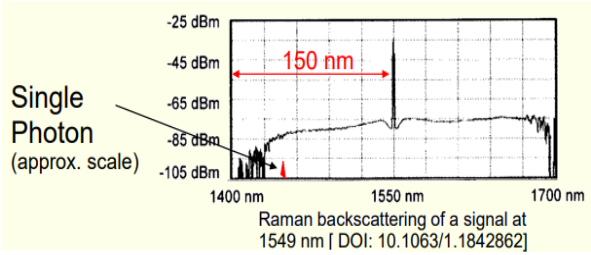
- **Dificultades de la criptografía cuántica(1)**



Alcance limitado
Enlaces P2P



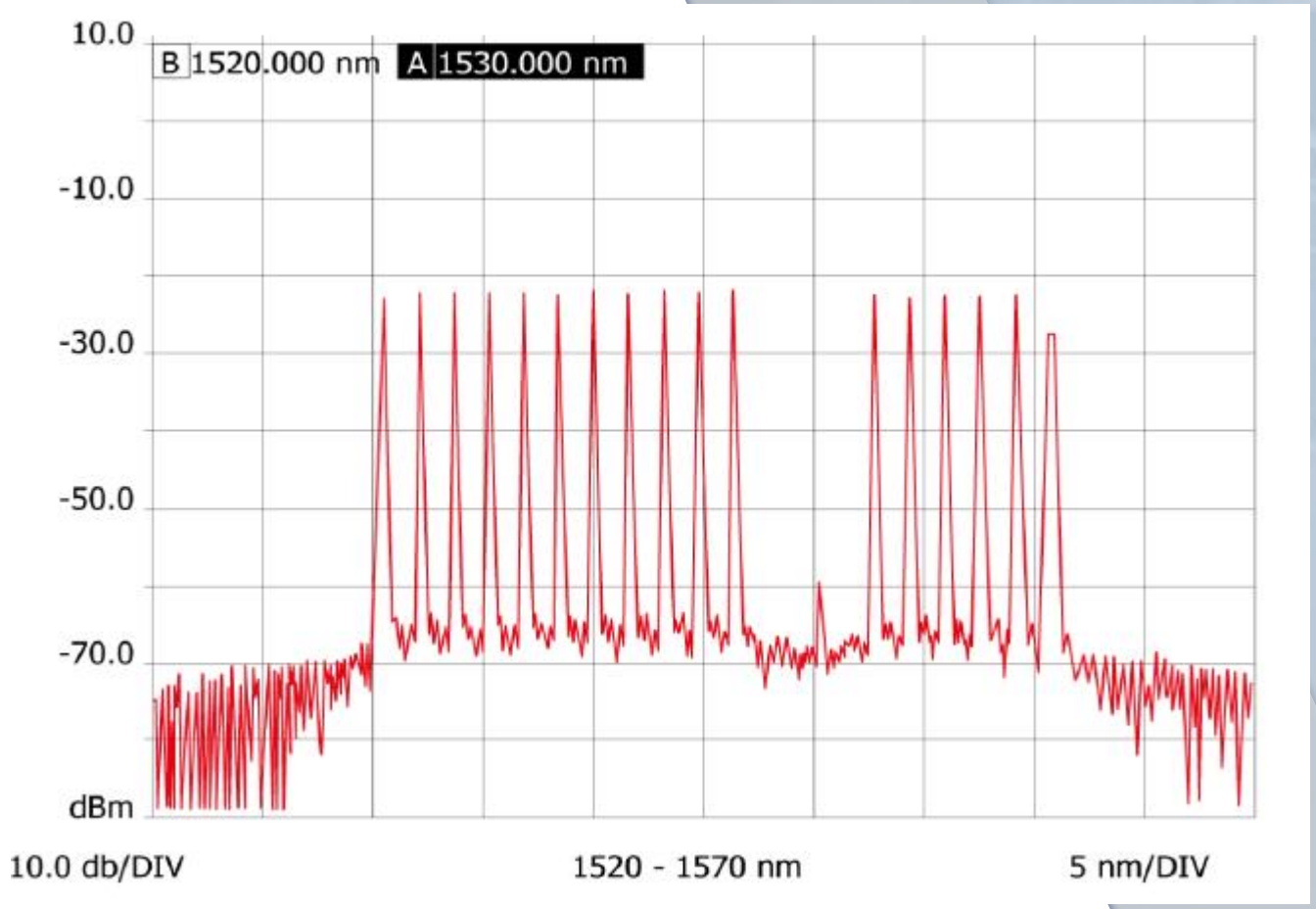
Señales muy débiles



Ruido en la fibra: Raman

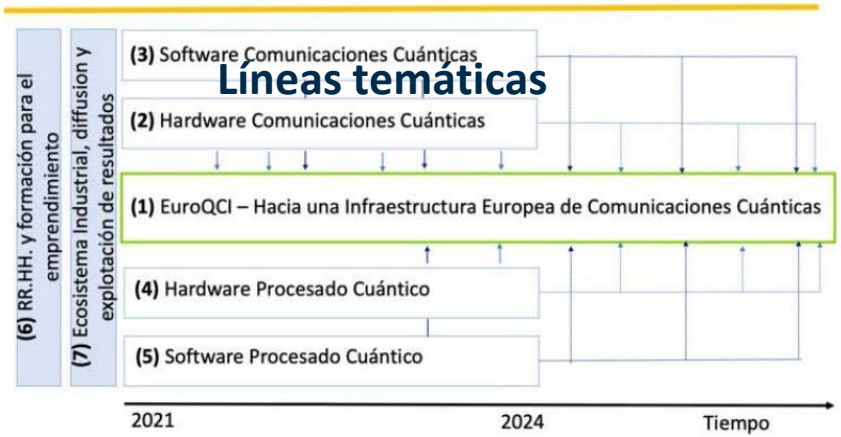
(1) Fuente: Presentación Vicente Martín, Madrid SDN Quantum Network, Madrid 14 mayo 2019

Integración cuántico-clásico



Programa Complementario de Comunicaciones Cuánticas (PCCC)

- **En España:**
  - Comunicaciones cuánticas: 1 de las 8 áreas científico-técnicas priorizadas mediante los **Planes Complementarios con las CCAA** (Plan de Recuperación, Transformación y Resiliencia)
  - Propuesta coordinada entre: **Pais Vasco, Galicia, Cataluña, Madrid, Castilla León y Valencia**.
  - Sigue las líneas maestras del **Quantum Flagship** y **Euro QCI** contribuyendo a sus objetivos tanto científico-tecnológicos como de creación de talento y ecosistema industrial



Distribución de clave cuántica (QKD)

- **Protocolos de variable discreta**
  - Protocolos Prepare and Measure
  - Protocolos basados en entrelazamiento

- **Protocolos de variable continua**
  - Codifican la información en la cuadratura del campo electromagnético de la luz (típicamente)

- **Arquitectura de redes complejas:**
  - Software defined QKD
  - Otros mecanismos de distribución de claves