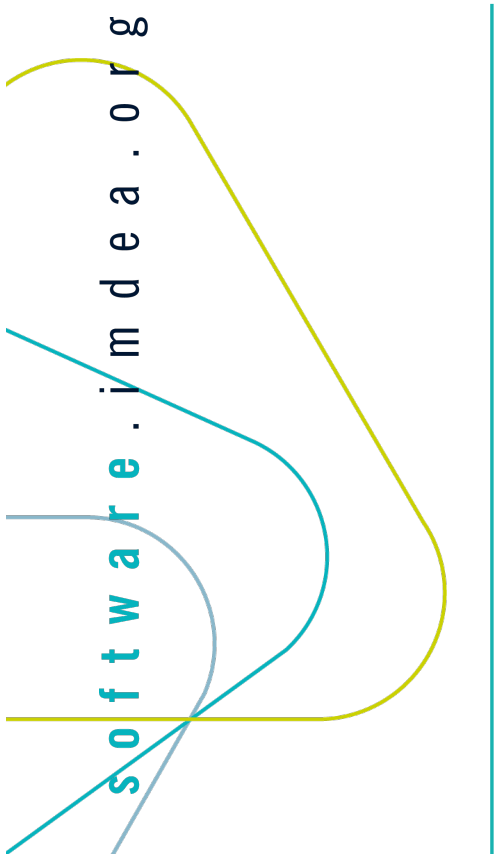
MadQCI, DISEÑO DE LA NUEVA RED DE COMUNICACIONES CUÁNTICAS DE LA COMUNIDAD DE MADRID.

David Rincón

Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea
NextGenerationEU

Jornadas Técnicas de RedIRIS 2024

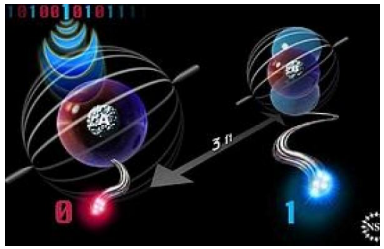
Palma de Mallorca , 29 de mayo, 2024



ÍNDICE

1. REDIMadrid

2. Comunicaciones cuánticas



3. OpenQKD, MadQCI

David Rincón

29 de mayo

** Esta foto de Autor desconocido está bajo licencia CC BY-NC-ND

ÍNDICE

1. REDIMadrid

REDIMadrid (la Red de Madrid)

(Financiada por la Comunidad de Madrid)

32 instituciones afiliadas

REDIMadrid en cifras

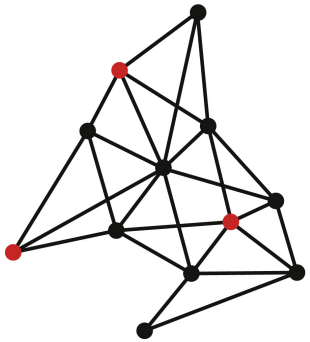
Fibra oscura REDIMadrid:

Total: ≈ 430km:

- 150 un par
- 280 dos pares

Telefónica

Correos Telecom



Trafico cursado en REDIMadrid:

Total: ≈ 100Gb/s

Todas las universidades con posibilidad de conexión a **100G**.

Usuarios de REDIMadrid:

Número total de usuarios: 354.737
Número total de mujeres: 179.149(50.51%)

Equipos de comunicaciones:

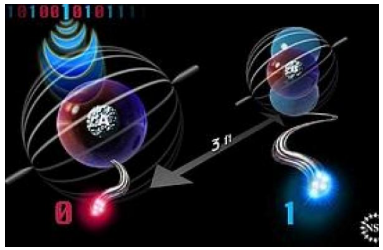
Número total de Router: **17**, de los cuales 2 son P's y 2 son RR.
Número total de equipos ópticos: **9**

JUNIPER NETWORKS

ciena

ÍNDICE

2. Comunicaciones cuánticas

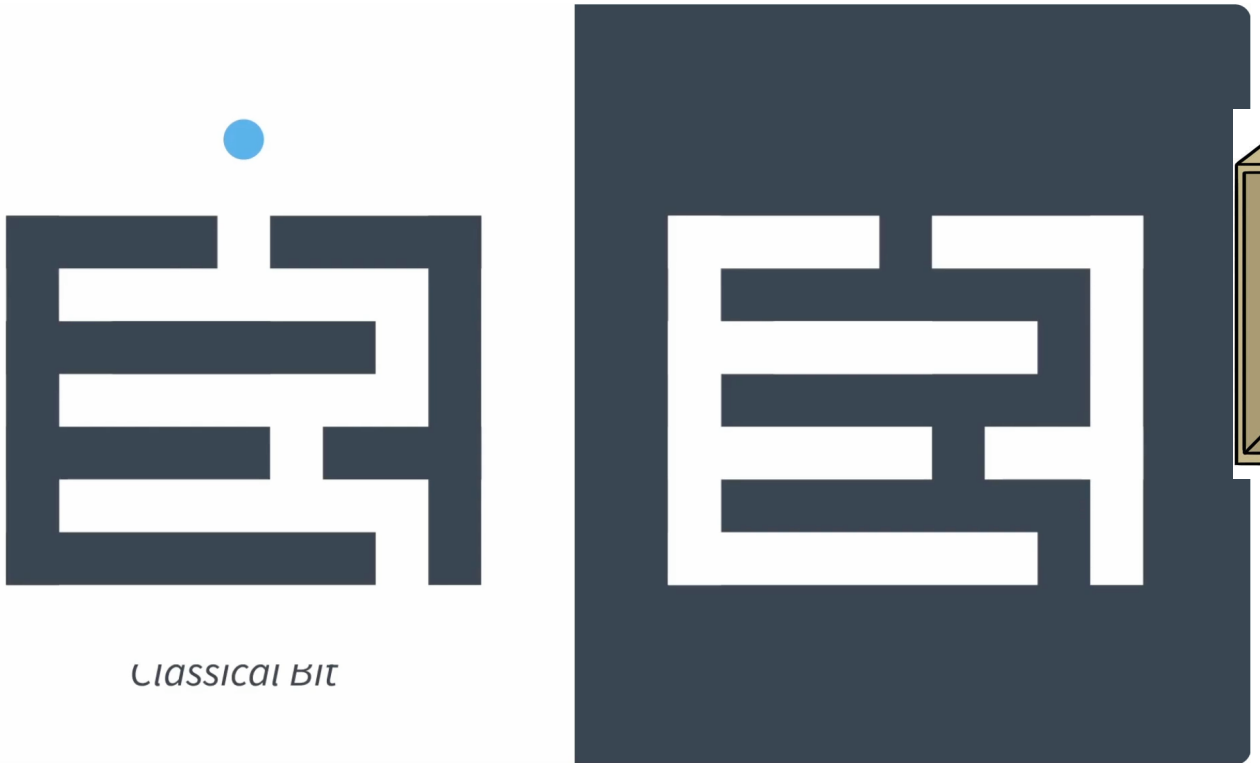


** Esta foto de Autor desconocido está bajo licencia CC BY-NC-ND

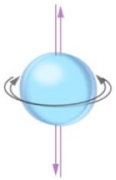
¿Qué son las comunicaciones cuánticas?

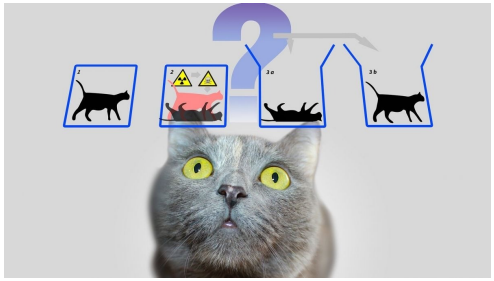
Física Clásica vs Física cuántica

Bits clásico vs Qubits



Superposición cuántica

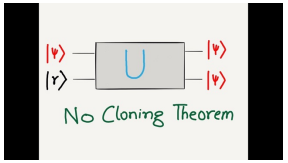




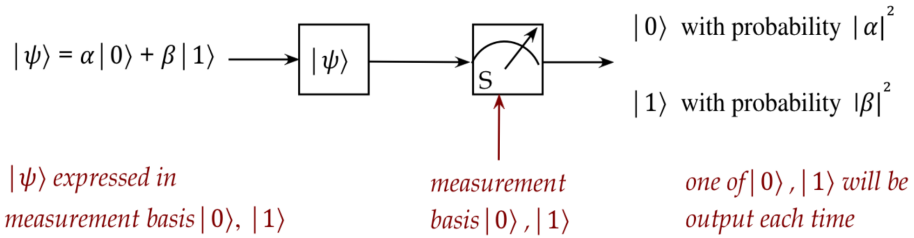
Video de QuTech Academy

¿Qué son las comunicaciones cuánticas?

2. Teorema de la no-clonación



Este teorema fue introducido por Wooters, Zurek y Dieks en 1982 y consiste en que no se pueden realizar copias de un estado desconocido de un sistema

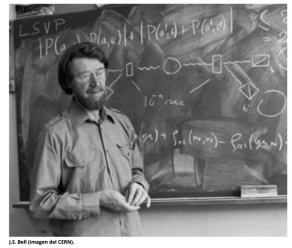


**

Solo con medir el estado del qubit, este se modifica
Problema: No se puede amplificar un fotón cuántico.
Ventaja: No se puede copiar un fotón cuántico.

3. Entrelazamiento cuántico

Permite que dos partículas (fotones) separadas, incluso a kilómetros de distancia, estén conectadas de una forma que la física clásica no puede explicar.



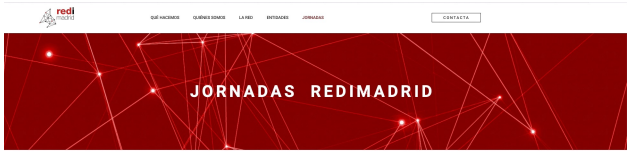
Ventaja: Tenemos la posibilidad de hacer repetidores cuánticos.

**Este diagrama se extrae de la web https://www2.seas.gwu.edu/

¿Qué son las comunicaciones cuánticas?

Referencias para entender las comunicaciones cuánticas:

- En las **Jornadas de REDIMadrid** se ha tratado este tema desde 2017
- Se pueden consultar todas las ponencias en el apartado ”**JORNADAS**” en la página web de REDIMadrid



10:30 - 11:00 **Quantum Key Distribution y Software Defined Networking**

Vicente Martín y Alejandro Aguado Martín

UPM

Descargar presentación ponencia III

OpenQKD y EuroQCI

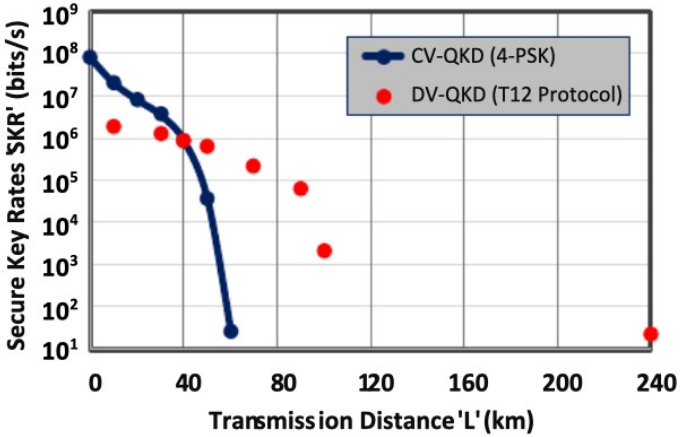
Vicente Martín

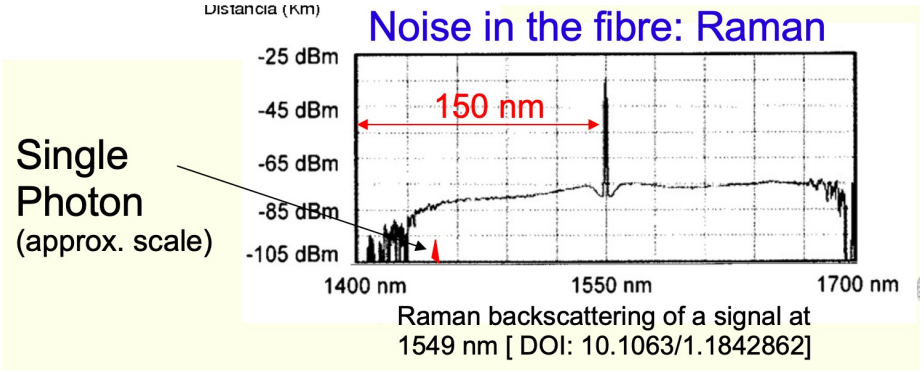
UPM

Descargar presentación

https://www.redimadrid.es/jornadas.html

¿Cómo de fácil es integrar QKD en una red real?





Problema: límite de ~30db, ~150km para transmitir la clave.
Problema: con el aislamiento de los amplificadores entre canales.

Solución: Trusted nodes/ repetidores cuánticos. Satélites para larga distancia.

Co-propagación clave cuántica en una red DWDM → ¿hay solución?

¿Como transmitir QKD en una red real?

a) **¿Tienes fibra oscura libre?**

a) Construcción de una red QKD dedicada.

- Check: arXiv:0804.0122

b) Construir una red QKD dedicada pero que transmita tanto los canales QKD como los canales clásicos asociados (canal de destilado etc..)

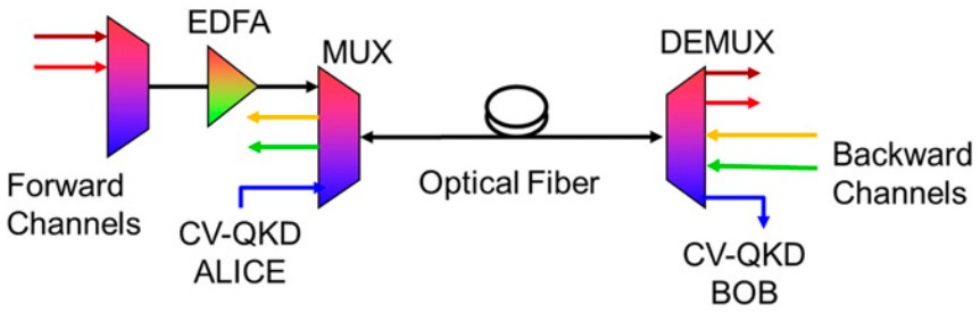
- Check: arXiv:1309.3923

2) **¿No Tienes fibra oscura libre?** → Fully integrated quantum/clasiscal network.

a) *¿Tienes una red DWDM sin amplificación?* → integrar CV-QKD es relativamente sencillo

b) *¿Tienes una red DWDM con amplificación? → Integrar CV-QKD es complicado.*

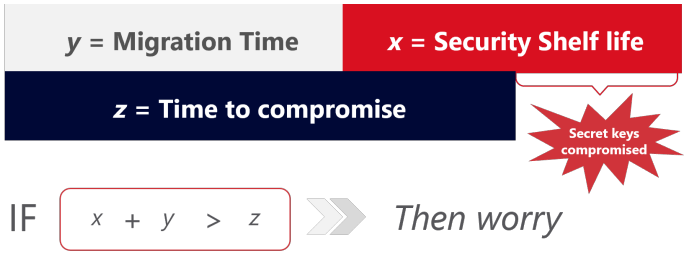
- Check: arXiv:2311.12791



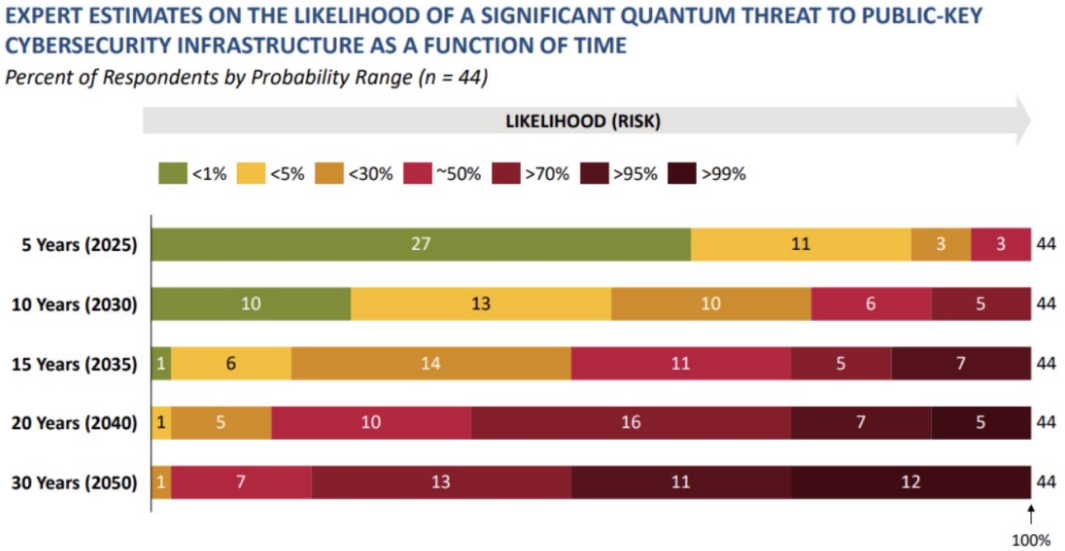
**

Vale, ¿Pero, debo empezar a pensar en hacer una red cuántica?

Teorema Mosca.



¿Cuánto tiempo tienen que estar seguros los datos que estas enviando ahora mismo por la red?



Montar una red cuántica no es inmediato.

Mientras tanto si necesitas seguridad deberías evaluar **PQC (Post-Quantum Crypto)**

Vale, ¿Pero, debo empezar a pensar en hacer una red cuántica?

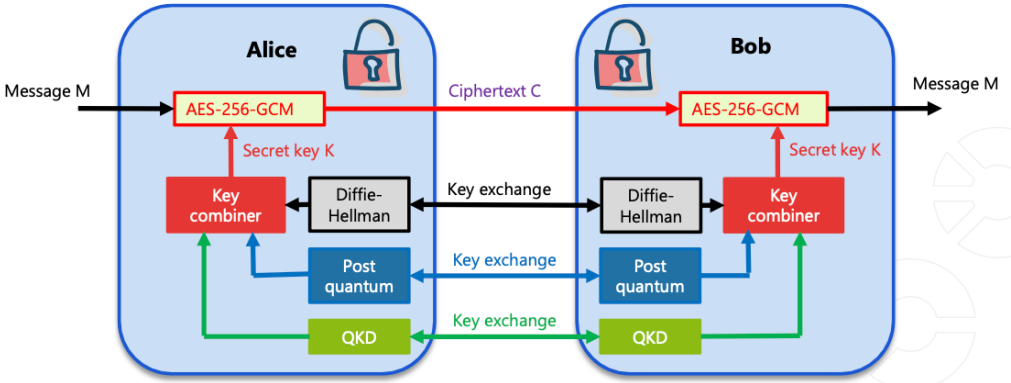
Los ordenadores cuánticos rompen, en tiempo polinómico, los algoritmos más utilizados para la criptografía de clave pública y la distribución de claves.

- RSA
- Elliptic curve cryptography
- Diffie-Hellman (RSA/ECC)

Algoritmo de Shor's

Algoritmo de Gover

La "criptografía post-cuántica" (PQC) o "criptografía resistente a la computación cuántica" (Quantum-Safe Cryptography) engloba aquellos algoritmos criptográficos diseñados para resistir los ataques de los algoritmos de Shor y de Grover.



Source: ADVA

ÍNDICE

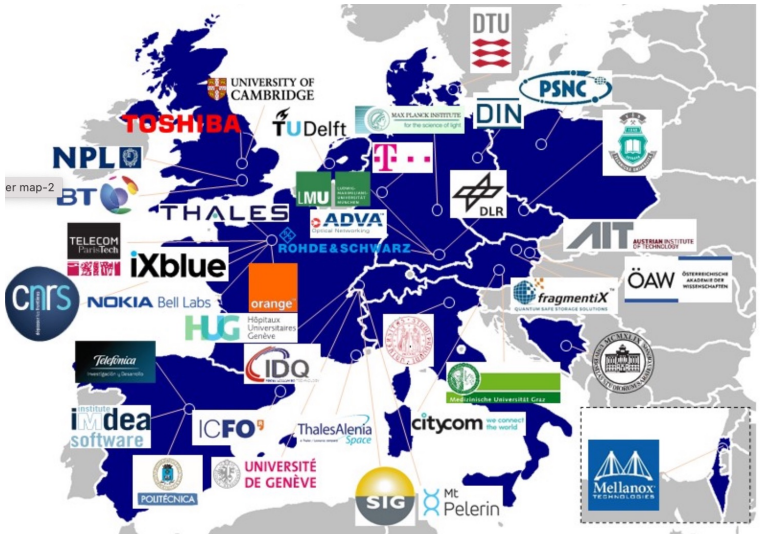
3. OpenQKD

¿De dónde venimos? OpenQKD

- REDIMadrid ha participado como partner en el proyecto OPENQKD que ha sido el proyecto europeo de tecnólogas cuánticas más importante hasta la fecha.

- REDIMadrid: testbed para experimentos QKD sobre fibras ópticas (red con tráfico real + cuántico)

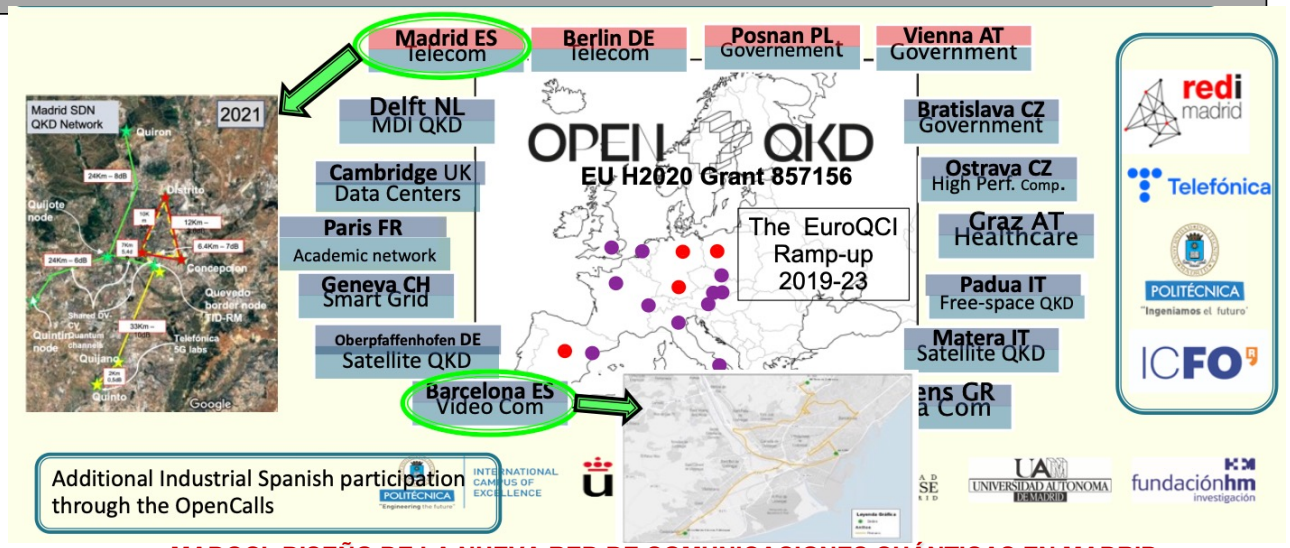
- **Madrid (REDIMadrid):** testbed más grande (germen de red cuántica permanente)



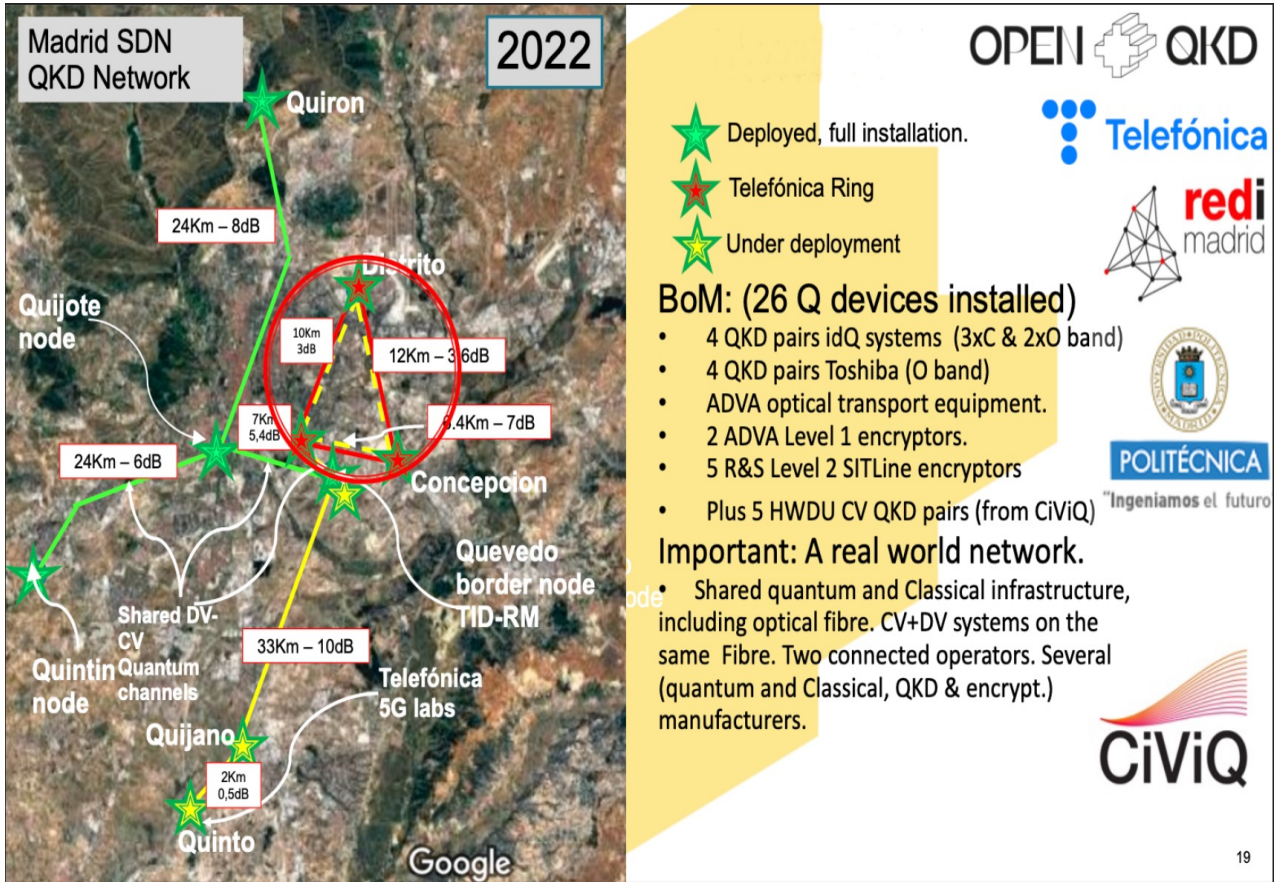
¿De dónde venimos? OpenQKD

- Algunas cifras:
  - Se demuestra los casos de uso en redes reales, no en laboratorios
  - 38 partner y 18 millones de Euros y OpenCalls por valor de 1 millón de Euros.
  - 16 Test en diferentes países y 4 testbed importantes (Madrid, Berlin, Polonia y Viena)

Desplegado en los PdP de REDIMadrid durante más de 3 años con **CERO** incidencias debidas a la infraestructura cuántica.



¿De dónde venimos? OpenQKD

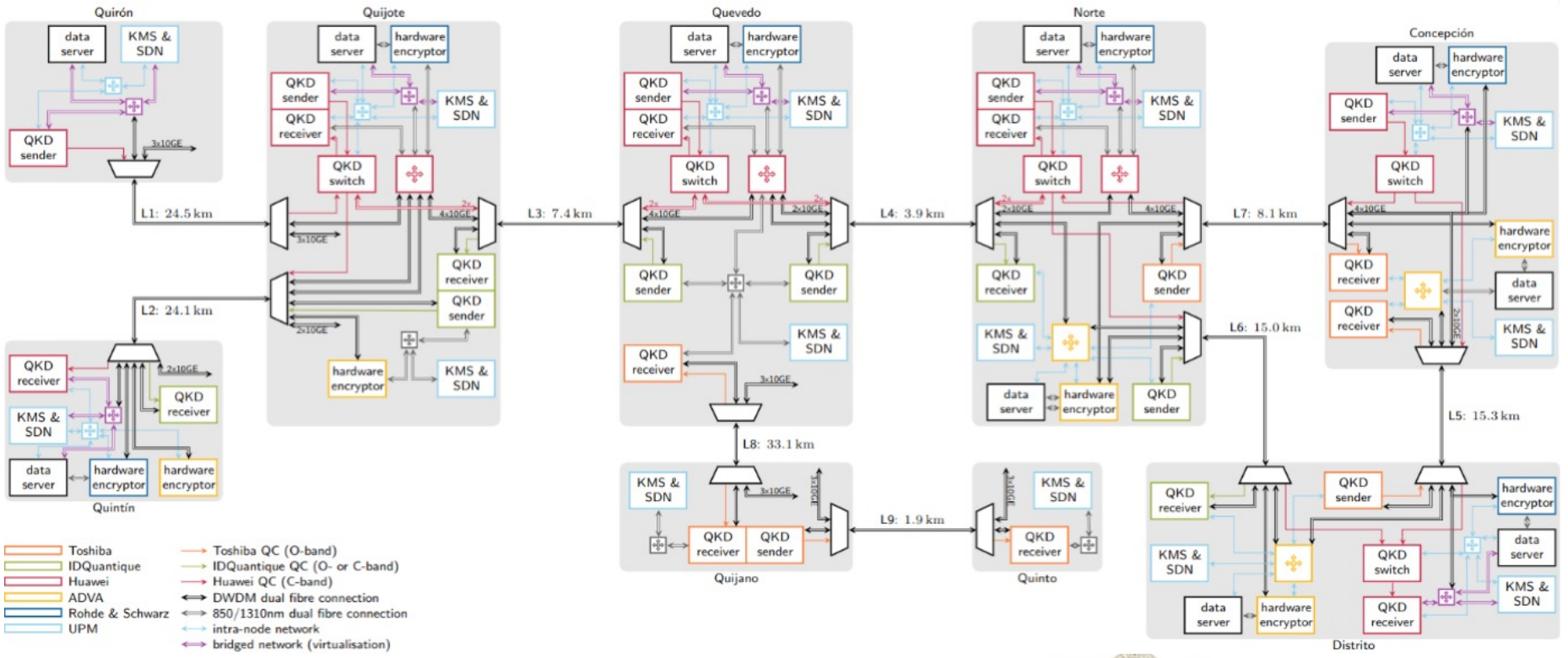


Hitos importantes conseguidos en este proyecto a nivel de RED:

1) Conexión de dos redes, a nivel cuántico, de service provide diferentes (Telefónica y REDIMadrid).
2) Enviar por el mismo par de fibras señal cuántica de diferentes fabricantes (Huawei e IDQ).
3) Hacer **RED Cuántica**, poder transmitir clave cuántica entre un nodo A contra un nodo C pasando por un nodo B. Esto Se hace posible gracias al gestor SDN de la UPM (QoolNet).

QoolNet

¿De dónde venimos? OpenQKD



Source: arXiv:2311.12791

ÍNDICE

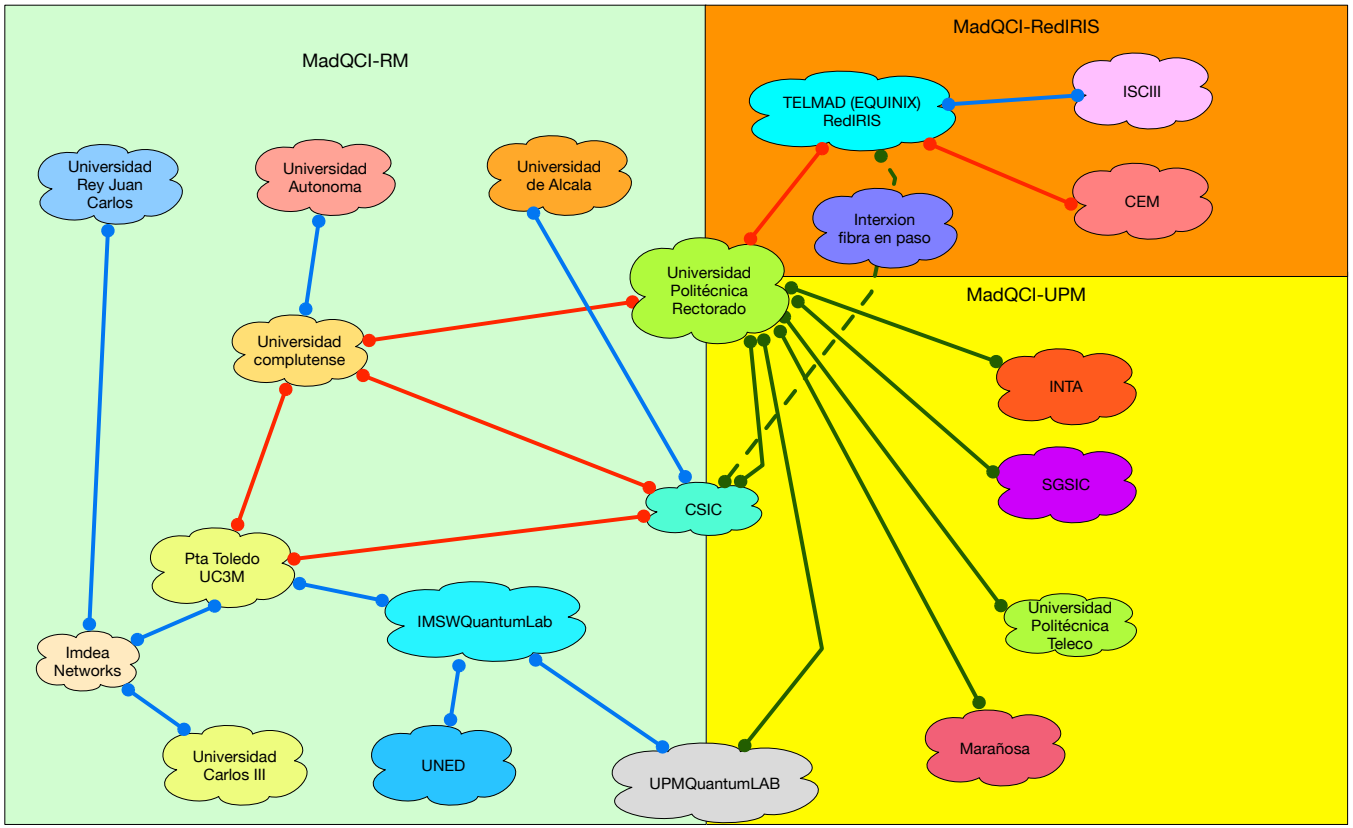
3. MadQCI

El papel de REDIMadrid en MadQCI

- REDIMadrid está diseñando, junto a la UPM, la red cuántica permanente MadQCI, para validar y desplegar la tecnología de comunicaciones cuánticas.
- La red permitirá alojar equipamiento de comunicaciones cuánticas de manera permanente, posibilitando la validación de nuevas tecnologías QKD.
- MadQCI conectará, a través de un despliegue metropolitano de *fibra óptica*, centros de datos de las universidades e instituciones de investigación de la Comunidad de Madrid.
- **HITO:** Fibra del segmento RM adjudicada a Telefónica, todas las universidades públicas están conectadas a la red cuántica de la comunidad de Madrid (MadQCI).

El papel de REDIMadrid en MadQCI

La red de fibra oscura que se está diseñando es la siguiente:



MadQCI en datos:

Km de fibra oscura: ≈ 440km:
* 390 dos pares
* 50 tres pares

Nodos conectados:

≈ 20 instituciones

El papel de REDIMadrid en MadQCI

- Se pretende que se puedan probar todas las tecnologías de comunicaciones cuánticas actuales (variable continua, variable discreta, entrelazamiento, etc…) y ¿todas las tecnologías de comunicaciones cuánticas futuras?.

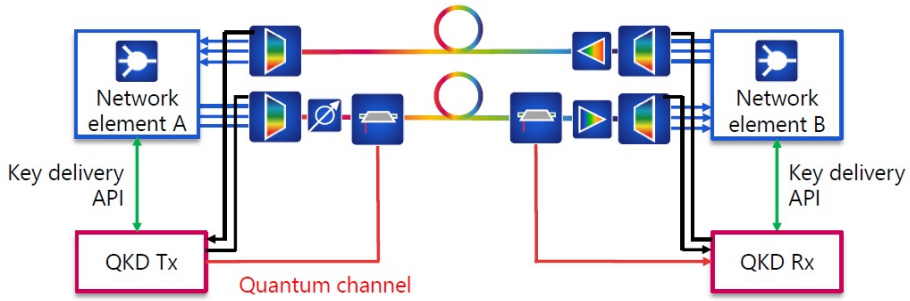
- Para ello la red DWDM tiene que ser lo más abierta posible, por ello **MadQCI** pretende ser una red innovadora y ”open” por las siguientes razones:
  - Equipamiento White boxes para una parte de la red IP.
  - SDN → ¿Hasta dónde podemos llegar para automatizar la red?
  - Red óptica, debe ser una red “industrial” pero que sean fácilmente integrables los equipos QKD, ¿Cómo se puede hacer?

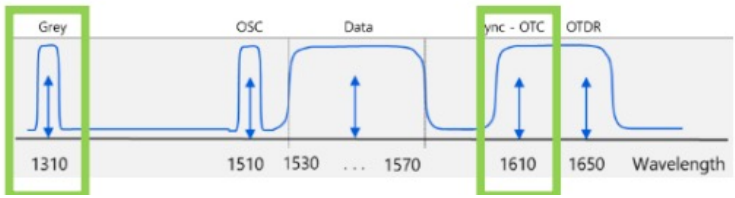
TELECOM INFRA PROJECT

QoolNet

El papel de REDIMadrid en MadQCI

- Para el diseño se ha promovido el concepto “Islas”, para ello en la red se van a crear varias islas:
  - Isla con fibra disponible separa de la red DWDM.
  - Isla FOADM co-propagando la lambda cuántica.
  - Isla RODAM sin booster.
  - Isla RODAM total, isla de operador.
  - Además de banda C, también se podrá poner lambda cuántica co-propagada en banda O y ¿en banda L?

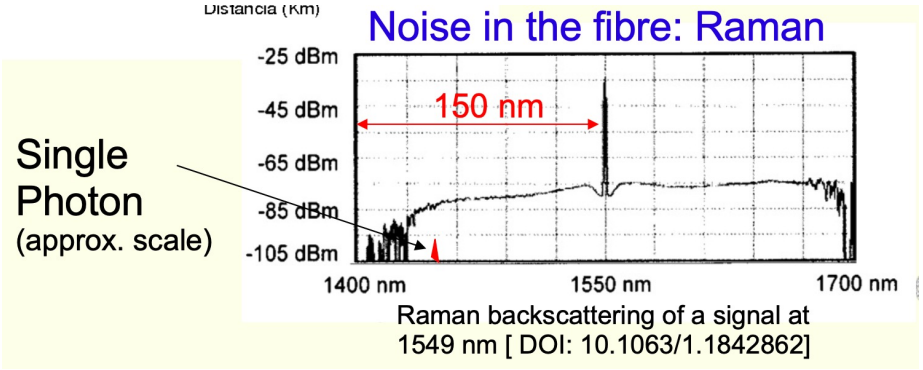


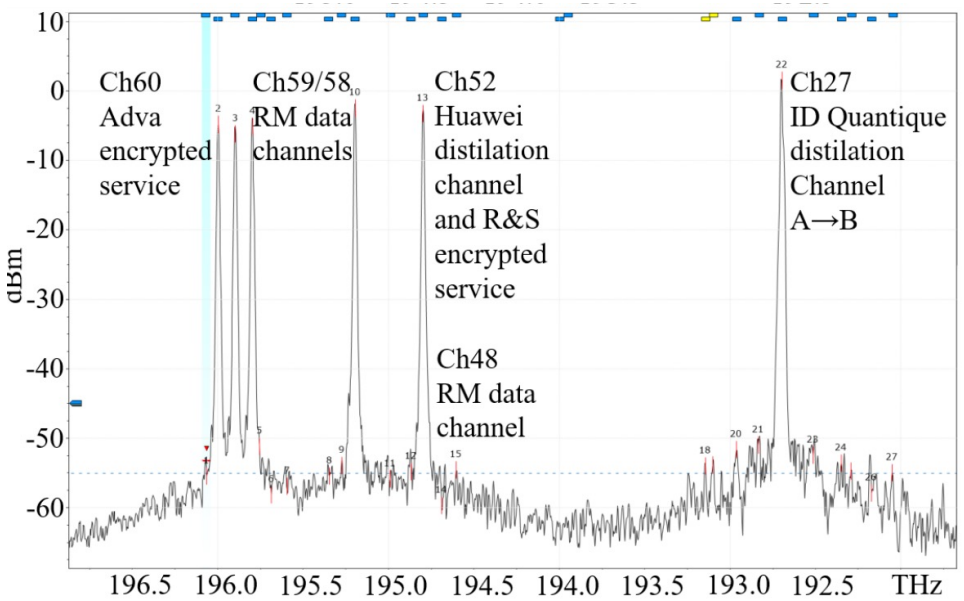


Source: ADVA

El papel de REDIMadrid en MadQCI

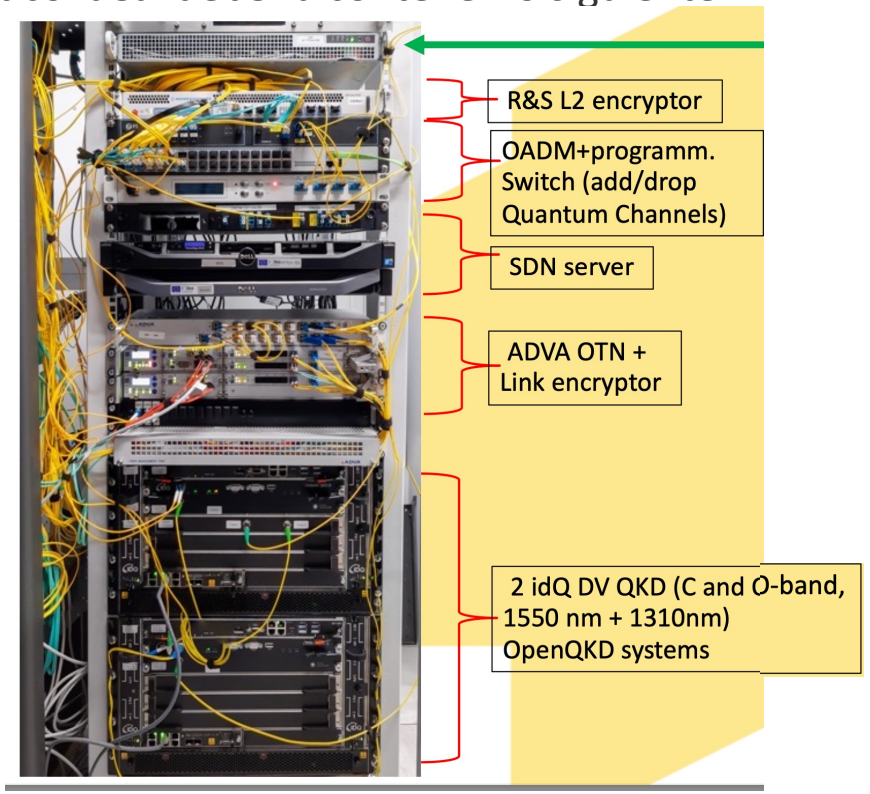
- El mayor problema es el aislamiento entre canales, este es el reto que debemos conseguir, ¿Cuánto podemos aislar entre canales adyacentes?, ¿Cuánto podemos aislar entre canales distantes?





El papel de REDIMadrid en MadQCI

- ¿Qué se entiende por un nodo cuántico? y ¿qué se instalará en los CPDs de las instituciones?:
  - No está definido todavía pero un nodo cuántico ideal debería contener lo siguiente:
    - **Fibra oscura**
    - **Equipamiento IP**
    - **Equipamiento óptico**
    - Equipamiento QKD
    - KMS y cifrador
    - Servidor, gestor SDN



instituto imdea software

C. Sanchez[1], V. Martin[2], J. P. Brito[2], L. Ortíz[2], A. J. Sebastian[2], D. R. Lopez[3], A. Pastor[3], D. Rincón[1]

[1] *IMDEA Software/RedIMadrid, 28660 Madrid. Spain*

[2] *Center for Computational Simulation and ETSI Informáticos, Universidad Politécnica de Madrid 28660 Madrid, Spain*

[3] *Telefónica Investigacion y Desarrollo, Ronda de la Comunicacion s/n 28050 Madrid. Spain*

thank you!

¿PREGUNTAS?

David Rincón

david.rincón@imdea.org

software.imdea.org

software