CCS Center for Computational Simulation

POLITÉCNICA "Ingeniamos el futuro"

OpenQKD & EuroQCI Quantum Networks in Madrid

2022 XVII JORNADAS redi madrid

Madrid, 18 Octubre 2022

Vicente Martin,
Vicente@fi.upm.es

POLITÉCNICA "Engineering the future" | INTERNATIONAL CAMPUS OF EXCELLENCE

Universidad Rey Juan Carlos

UNIVERSIDAD COMPLUTENSE MADRID

UAM UNIVERSIDAD AUTONOMA DE MADRID

fundaciónhm investigación

The Madrid Quantum Network

Index.

- Quantum Communications from a network perspective.
  - Why is it urgent to do Quantum Communications?
  - Why is difficult to do networked quantum comms?
- European and Worldwide Quantum Networks Panorama.
  - Quantum testbeds in Madrid and the OpenQKD project
  - EuroQCI and Madrid Quantum

Quantum Communications

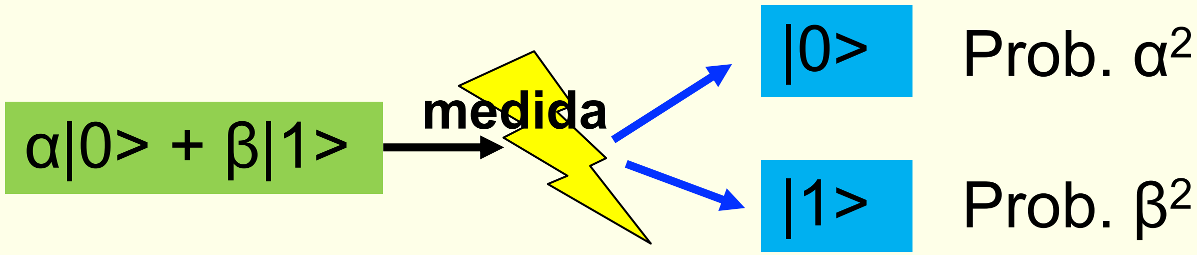
What is Quantum communications?

- Quantum Communications:
  - The ability to **transport information encoded in the states of quantum systems**.
  - E.g. a **qubit** (the analogous of a bit in quantum information) enconded in the polarization states of light (any two-states quantum system could do)
- It allows to do **things that cannot be done using only classical resources:**
  - Quantum Cryptography
  - Quantum state teleportation
  - Quantum Sensing/metrology
  - Communications between quantum computers
  - …

Información Cuántica.

El Qubit.

- Definamos **dos estados cuánticos** como 0 y 1: |0> y |1>
  - **|0>** significa **"el estado cuántico que representa al valor 0 del qubit"**… Sea cual sea su implementación física: la polarización de un fotón, estados de espín…
- Un estado genérico de un **qubit** se escribe: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$
- **Lectura (medida):**



$\alpha|0\rangle + \beta|1\rangle$

medida

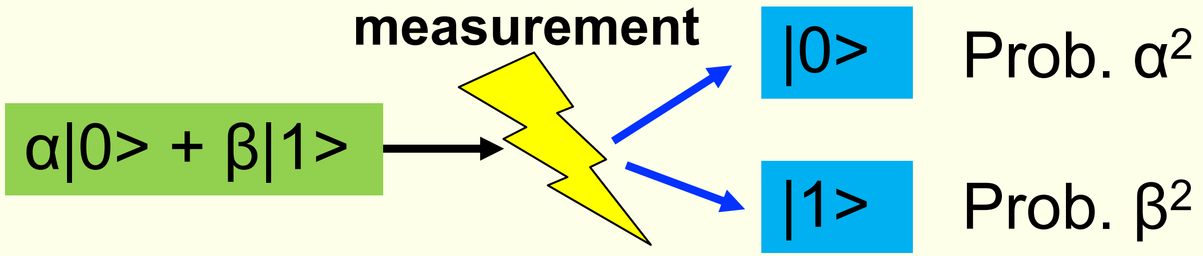
$|0\rangle$ Prob. α^2

$|1\rangle$ Prob. β^2

  - $(\alpha^2+\beta^2 = 1)$
  - Nótese que **la lectura modifica el estado del qubit.**
  - Teorema de la No-clonación: **No se puede copiar un estado cuántico desconocido.**

Resources: The Qubit.

- **Reading** the state of **a qubit** (measurement):



measurement

$\alpha|0\rangle + \beta|1\rangle$

$|0\rangle$ Prob. α^2

$|1\rangle$ Prob. β^2

  - ($\alpha^2+\beta^2 = 1$, measurement done in the $\{|0\rangle,|1\rangle\}$ basis.
  - Note: **measurement modifies the state of the qubit.**
  - We **do not have access to** α or β

It is not like this!!... Cannot store a gazillion bits in α or β !!

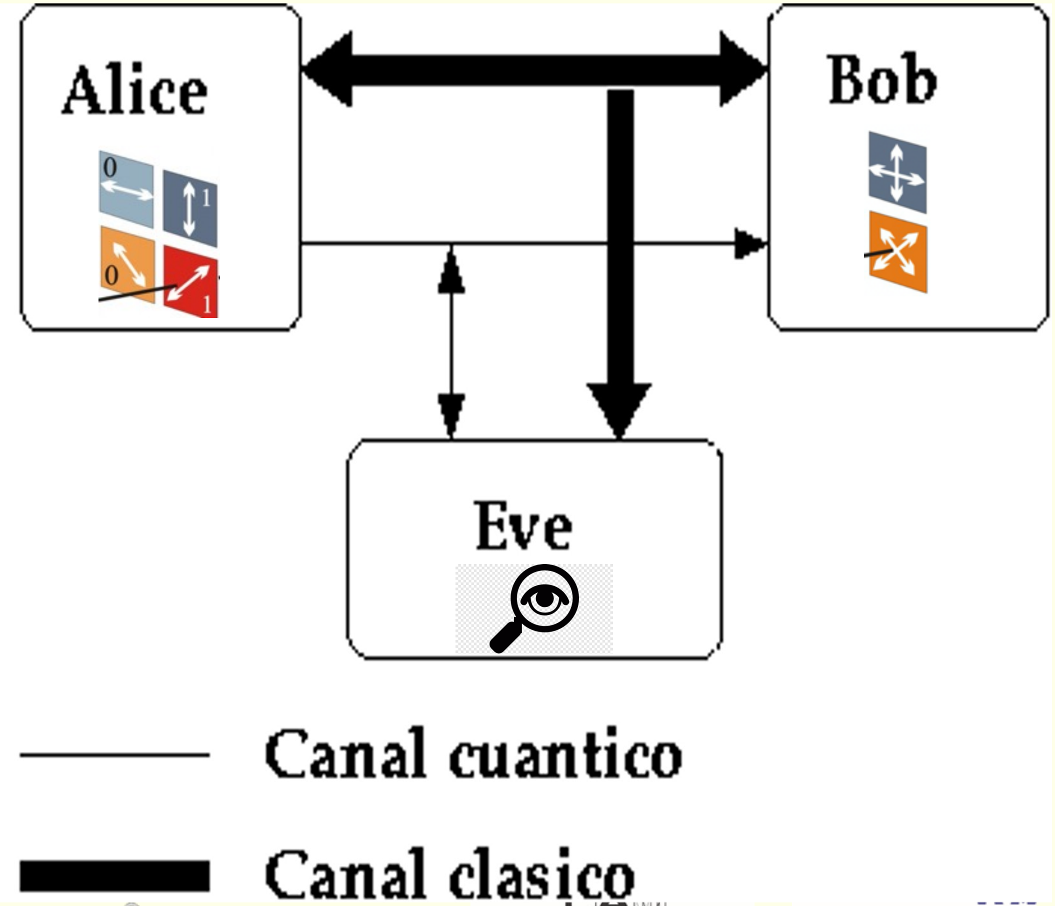
Quantum Cryptography.

"A qubit cannot be cloned* "

* Naive statement with shades of gray…

Ingredients:

- A **qubit emitter** (think photons): Alice.
  - Can prepare qubits in different states and basis.
- A **qubit receiver:** Bob
  - Can measure qubits in different basis
- A **quantum channel** (able to transport the qubits from Alice to Bob)
- A **classical channel** (public but **authentic**)
- … and the spy (Eve)



Quantum communications are not easy

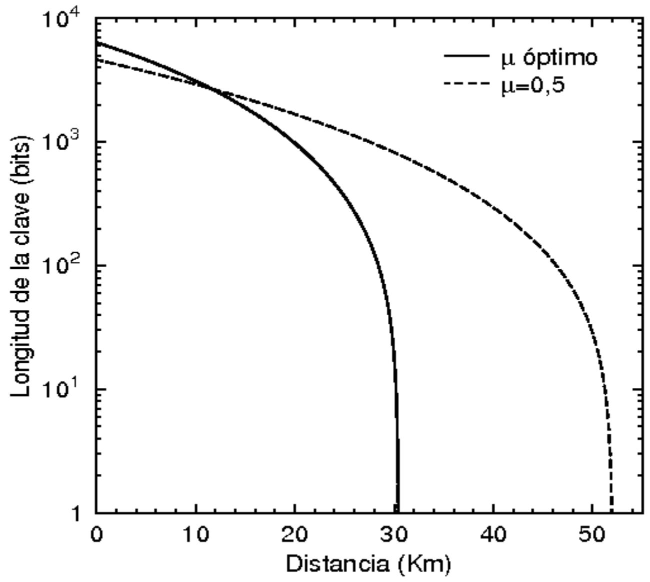
The Quantum channel

Signals are always absorbed.

- Except in perfect vacuum.
  - Exponential decay
- Free space: aperture

Quantum systems interact with the environment

- Decoherence: Loss of information



Quantum cryptography directly sending Quantum systems is fundamentally limited in reach

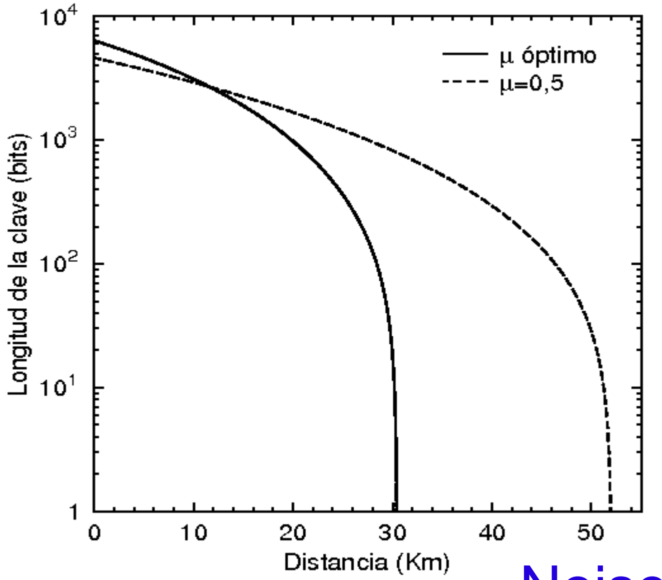
0 km	10^9 photons/sec.
15 km	$5\ 10^8$
150 km	10^6
300 km	1000
600 km	1 p per 20 min.
900 km	1 p per 36 years

Losses in fibre 0.2 dB/km

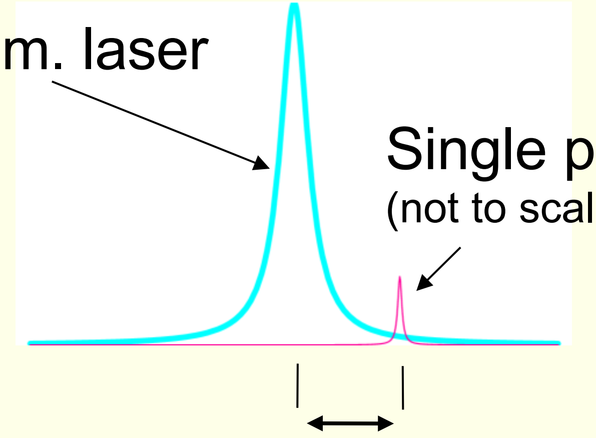
… just a couple of many problems…

… and losses is not the only problem?

Limited reach, point to point.



extremely weak signals.



Comm. laser

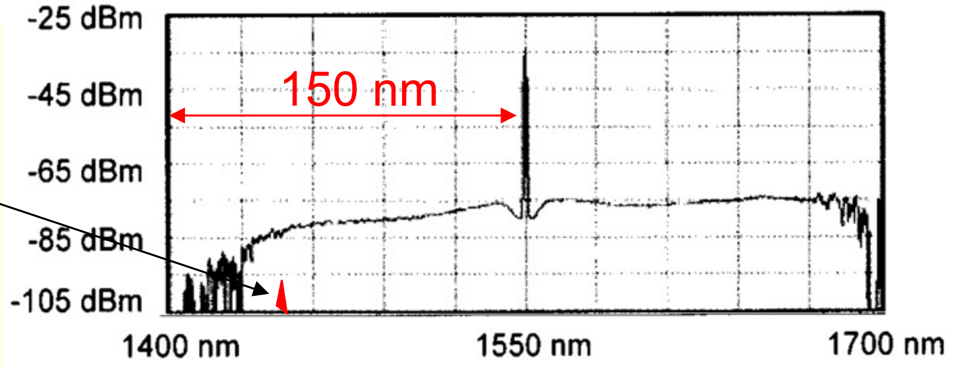
Single photon

(not to scale)

Δλ = 0.2~0.8 nm (DWDM)

Δλ = 3~20 nm (CWDM)

Noise in the fibre: Raman



Single Photon (approx. scale)

Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

- Difficult to detect.
- Absorpions
- Masked by the noise

Center for Computational Simulation

So… ?

We know that quantum information is “more powerful” than classical information.

We know that we can do more things… but dealing with quantum signals is not easy, and in a network is even worse…

- Quantum crypto is the most mature application.
    - Information Theoretic Security : “invulnerable” to computational attacks.

… but, is it worth?

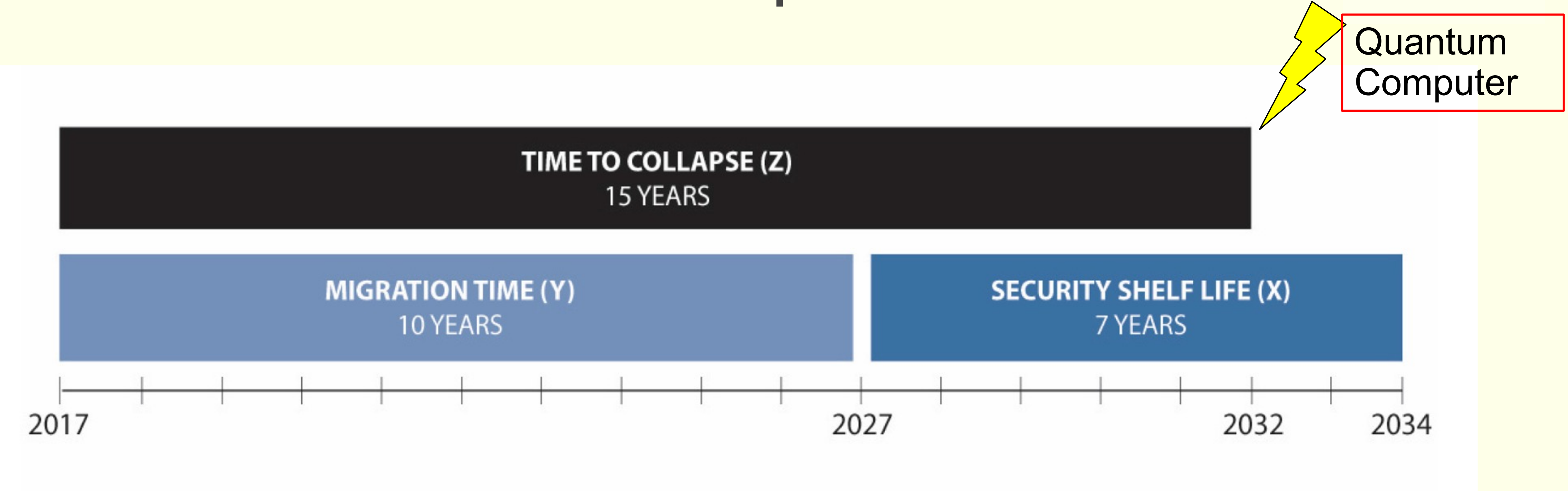
Let’s concentrate just in quantum cryptanalysis.

Quantum Computing and Crypto: Do we have a problem?

- **Quantum computers break**, in polynomial time, the most used **algorithms for public key cryptography and key distribution.**
  - RSA
  - Elliptic curve cryptography
  - Diffie-Hellman (RSA/ECC)
- But, you know, building a quantum computer **will take forever…**
  - Or, at least, so many years that you do not need to worry…

Shor's Algorithm

Quantum Computing and Crypto: Do we have a problem?



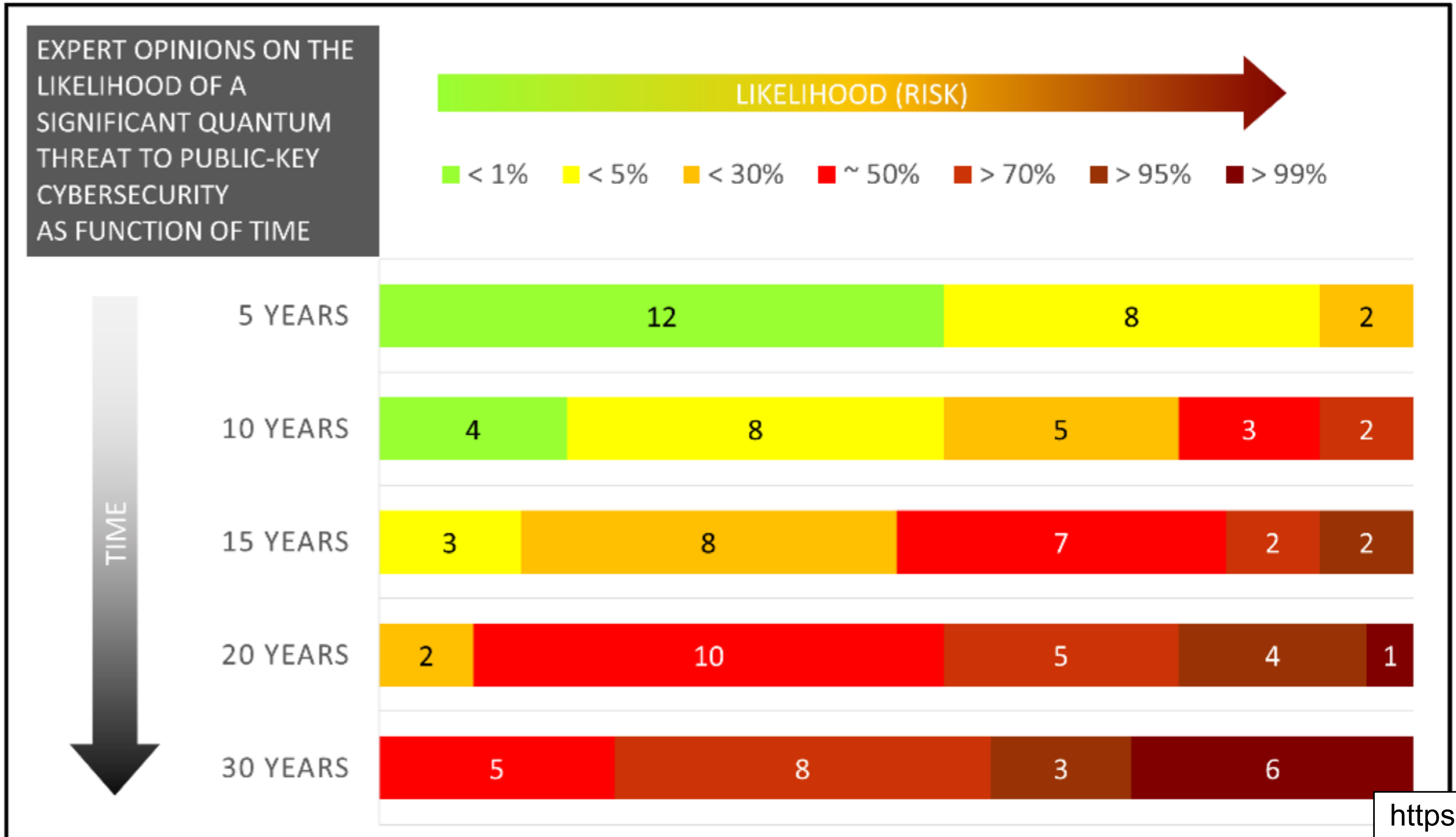
From : Quantum Computing: Progress & Prospects 2018. A Consensus Report. National Academy of Sciences, Engineering and Medicine (adapted from M. Mosca, 2015)

… write your own answer:

- Z: Time to a quantum computer: ?
- Y: Time to fully change the security infrastructure: Estimate (NIST) 20yrs.
- X: Shelf life: 1-50 yrs. (what is your application?)

If X+Y > Z… you have problems.

… people think that in 30 years conventional public crypto as we know it will be killed by Quantum Computing.



Numbers reflect how many experts (out of 22) assigned a certain probability range.

Solution as an experts opinion poll

(Global Risk Institute, 2019)

Please indicate how likely you estimate that a quantum computer, able to factorize a 2048-bit number in less than 24 hours, will be built within the next 5 years, 10 years, 15 years, 20 years, and 30 years,

https://globalriskinstitute.org/download/quantum-threat-timeline-full-report-2/

European Quantum Scenario (and beyond)

QUANTUM
FLAGSHIP

- 10 years Framework.
- First Calls 2018
- 1000 M€
- Alll Quantum Tech.

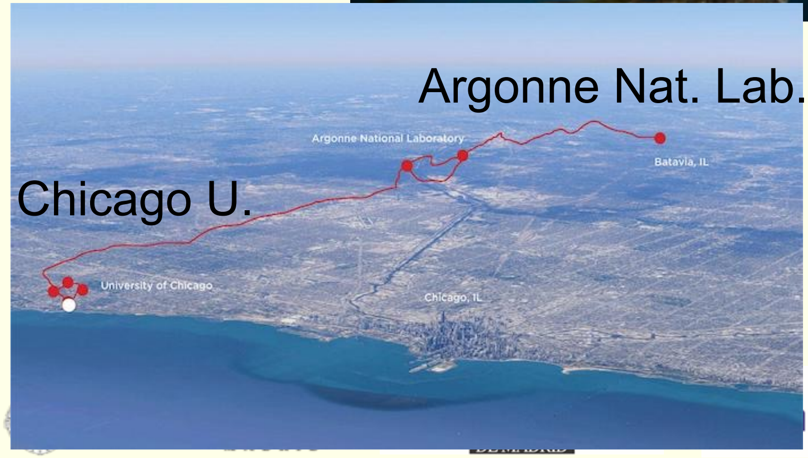
QuantumManifesto
A New Era of Technology
May 2016

Quantum communications Infrastructure

- 10 years Framework
- First Calls 2022. 2000 M€
- Q.Communications only:
- A Pan-European Q. Network

Similar programs in US.

- Last developments on networks: Quantum Cybersecurity Preparedness Act of April 2022. Quantum Chicago Exchange Network, Q-NEXT (DoE Research Centre at Argonne Nat. Lab.)

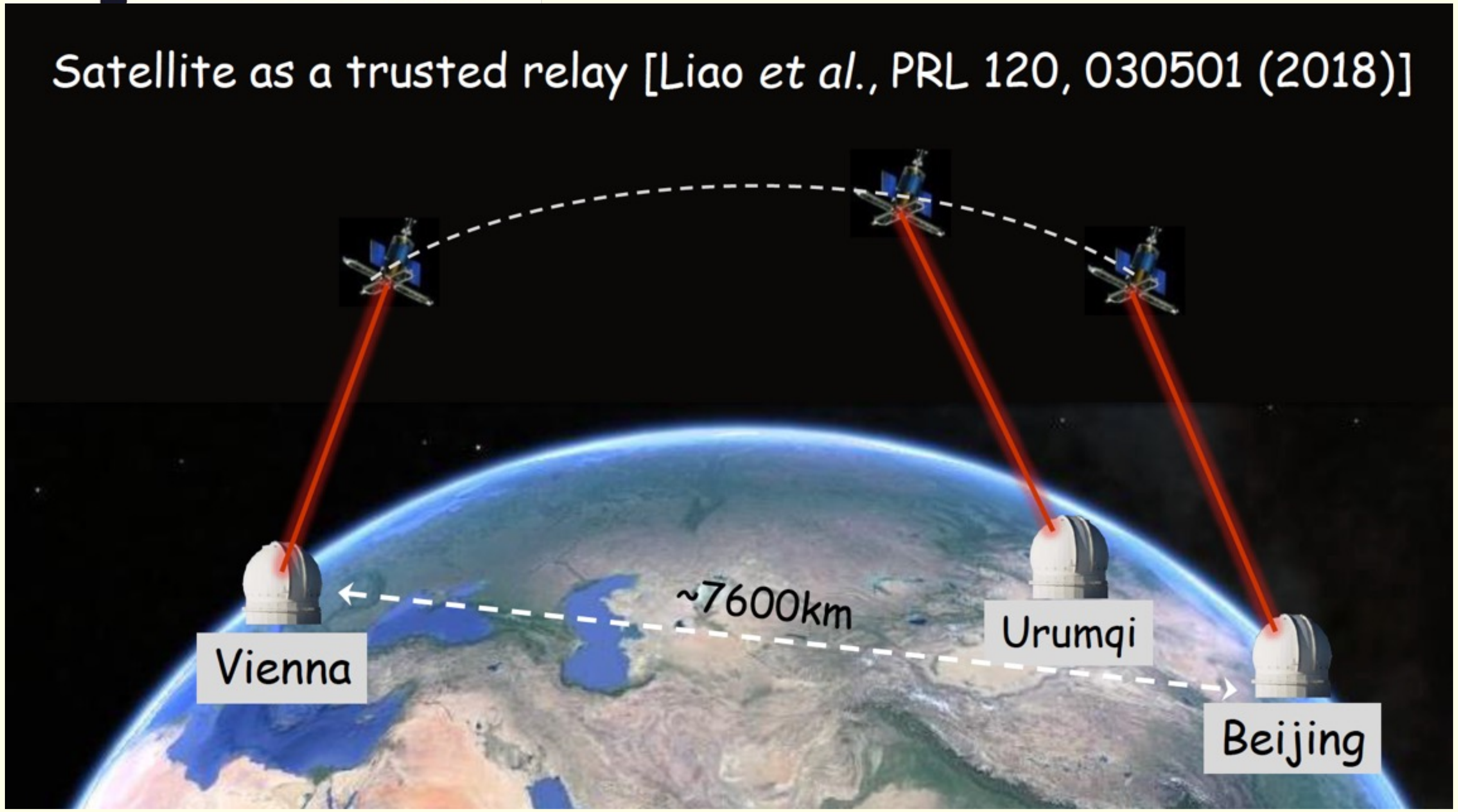


Japan, China, Australia, S. Korea, Russia also have nation-wide quantum programs

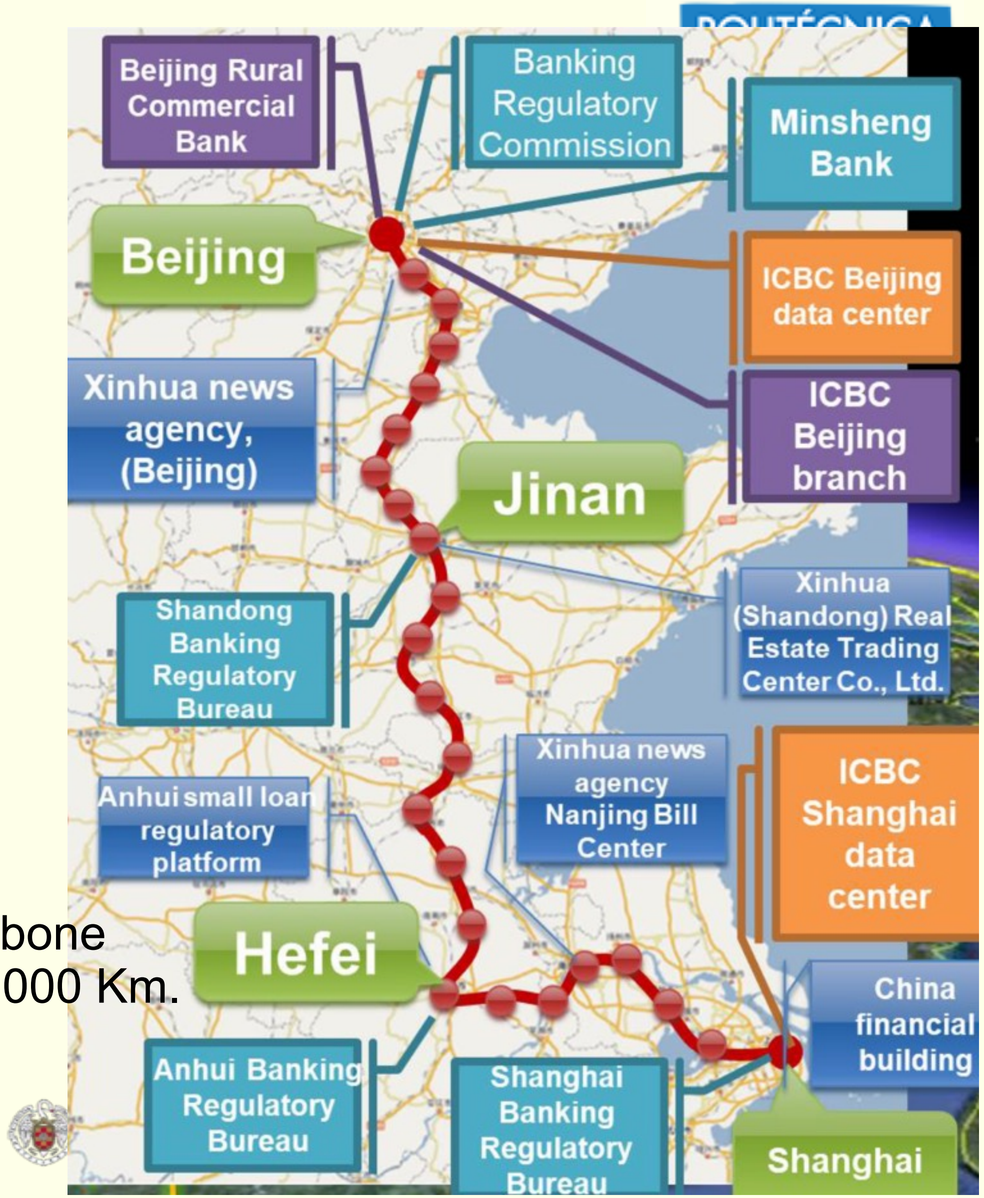
POLITÉCNICA "Engineering the future"
INTERNATIONAL CAMPUS OF EXCELLENCE
Universidad Rey Juan Carlos
ciónhm investigación

China

From J. Pan


Satellite as a trusted relay [Liao et al., PRL 120, 030501 (2018)]
~7600km
Vienna
Urumqi
Beijing

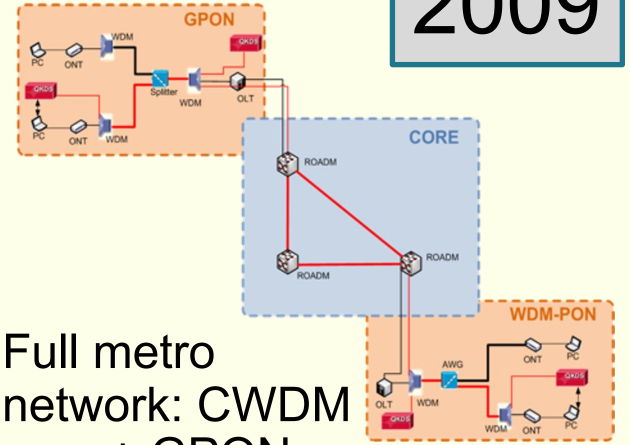
“Micius” satellite. Intercontinental QKD


Beijing Rural Commercial Bank
Banking Regulatory Commission
Minsheng Bank
Beijing
ICBC Beijing data center
Xinhua news agency, (Beijing)
ICBC Beijing branch
Jinan
Xinhua (Shandong) Real Estate Trading Center Co., Ltd.
Shandong Banking Regulatory Bureau
Xinhua news agency Nanjing Bill Center
ICBC Shanghai data center
Anhui small loan regulatory platform
Hefei
China financial building
Anhui Banking Regulatory Bureau
Shanghai Banking Regulatory Bureau
Shanghai

National Quantum Backbone
Beijing-Shangai 2016. 2000 Km.
32 trusted relays

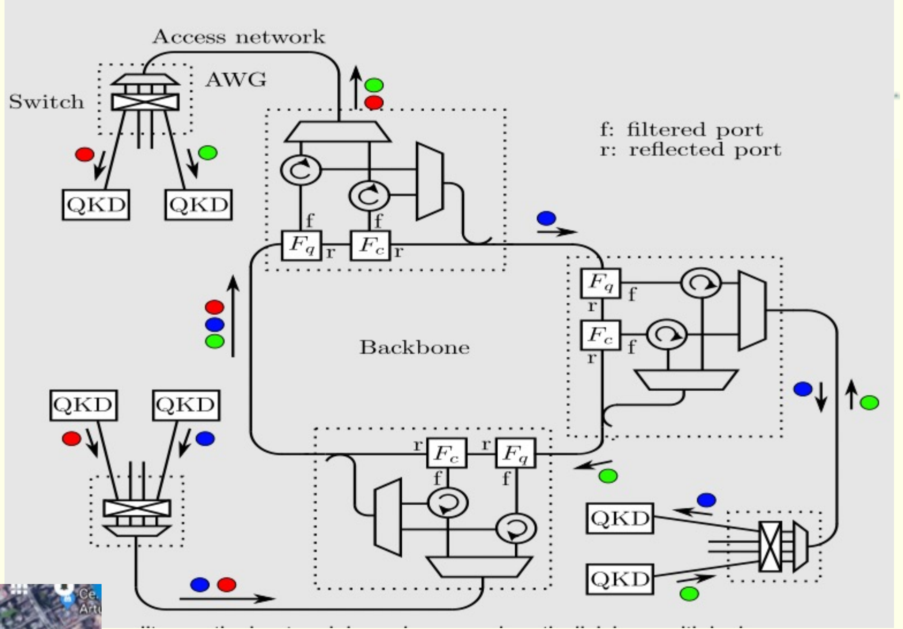
UPM & Quantum Networks

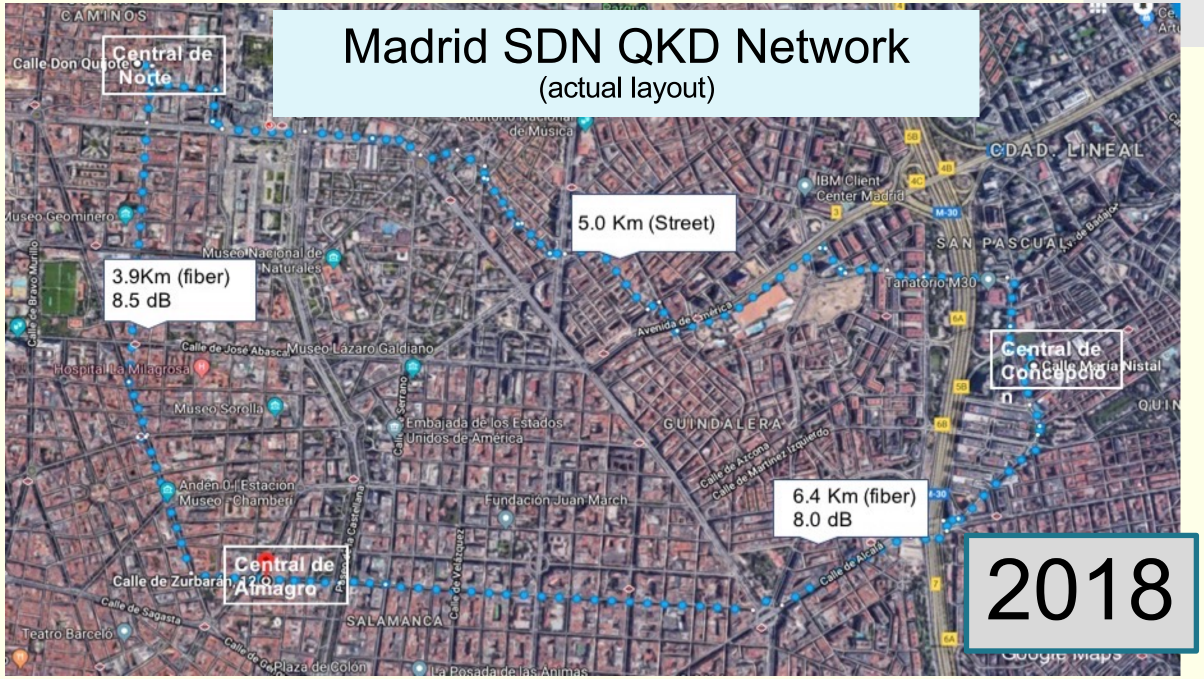
2009



Full metro network: CWDM core + GPON access

2014

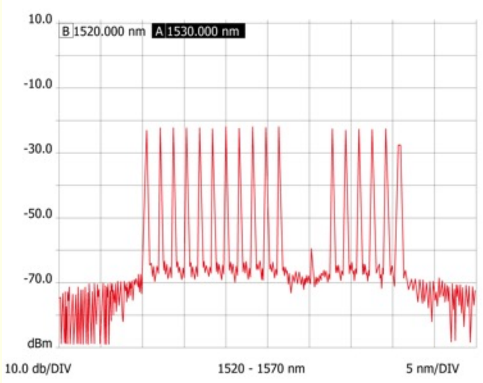




Madrid SDN QKD Network
(actual layout)

2018

- Largest Quantum Network in Europe ever.
- Industrial participation.
- Real world network installed in production facilities.
- Full network stack developed by UPM



1.7Tbps classical / Quantum C-Band copropagation

"The Engineering of a SDN Quantum Key Distribution Network" IEEE Comms. Mag. July 2019, Special number "The Future of Internet" doi: 10.1109/MCOM.2019.1800763 ; http://arxiv.org/abs/1907.00174

CCS Center for Computational Simulation

Madrid Quantum Network. The OpenQKD project

POLITÉCNICA "Ingeniamos el futuro"

- Considered as the "**EuroQCI Ramp up**"
- European Open QKD Network
- Testbeds to **demonstrate** the feasibility and **maturity of Quantum Communications technologies**.
- 33 Use-cases
- OpenCalls to increase the exposure to Quantum Communications of new players.
    - 4 calls runs in the Madrid testbed

OPEN QKD

POLITÉCNICA "Engineering the future" | INTERNATIONAL CAMPUS OF EXCELLENCE

Universidad Rey Juan Carlos

UNIVERSIDAD COMPLUTENSE MADRID

UAM UNIVERSIDAD AUTONOMA DE MADRID

HM fundaciónhm investigación

OPEN QKD : The EuroQCI Ramp-up

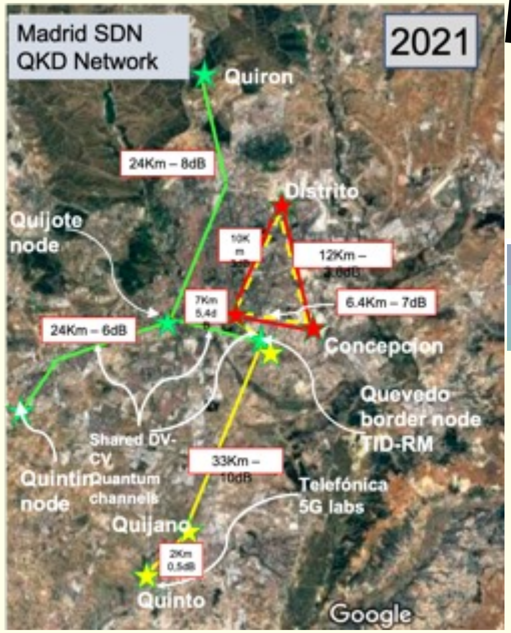
- Demonstrating real world use-cases in real deployments
- 38 partners /18 M€
- 16 Test Sites.
- 4 large Major testbeds
- OpenCalls (1M€)

Madrid ES Telecom

Berlin DE Telecom

Posnan PL Governement

Vienna AT Government



Delft NL MDI QKD

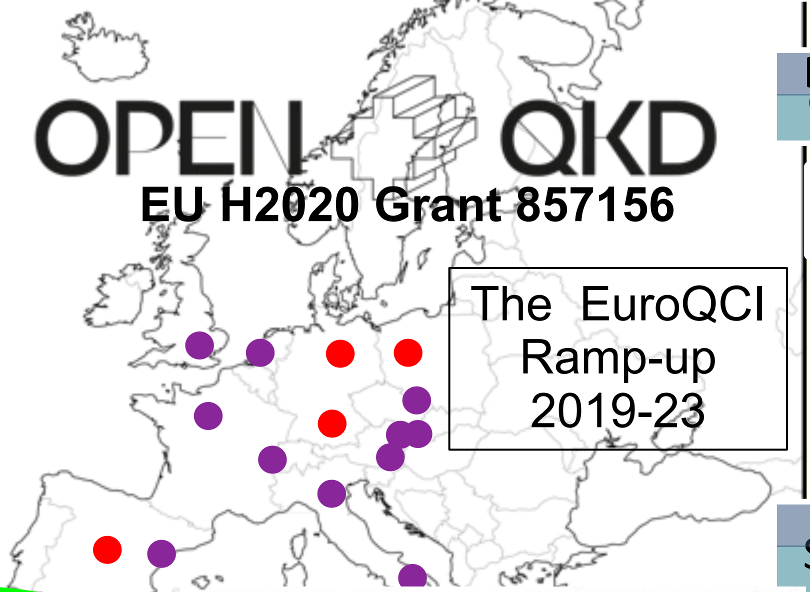
Cambridge UK Data Centers

Paris FR Academic network

Geneva CH Smart Grid

Oberpfaffenhofen DE Satellite QKD

Barcelona ES Video Com



OPEN QKD

EU H2020 Grant 857156

The EuroQCI Ramp-up 2019-23

Bratislava CZ Government

Ostrava CZ High Perf. Comp.

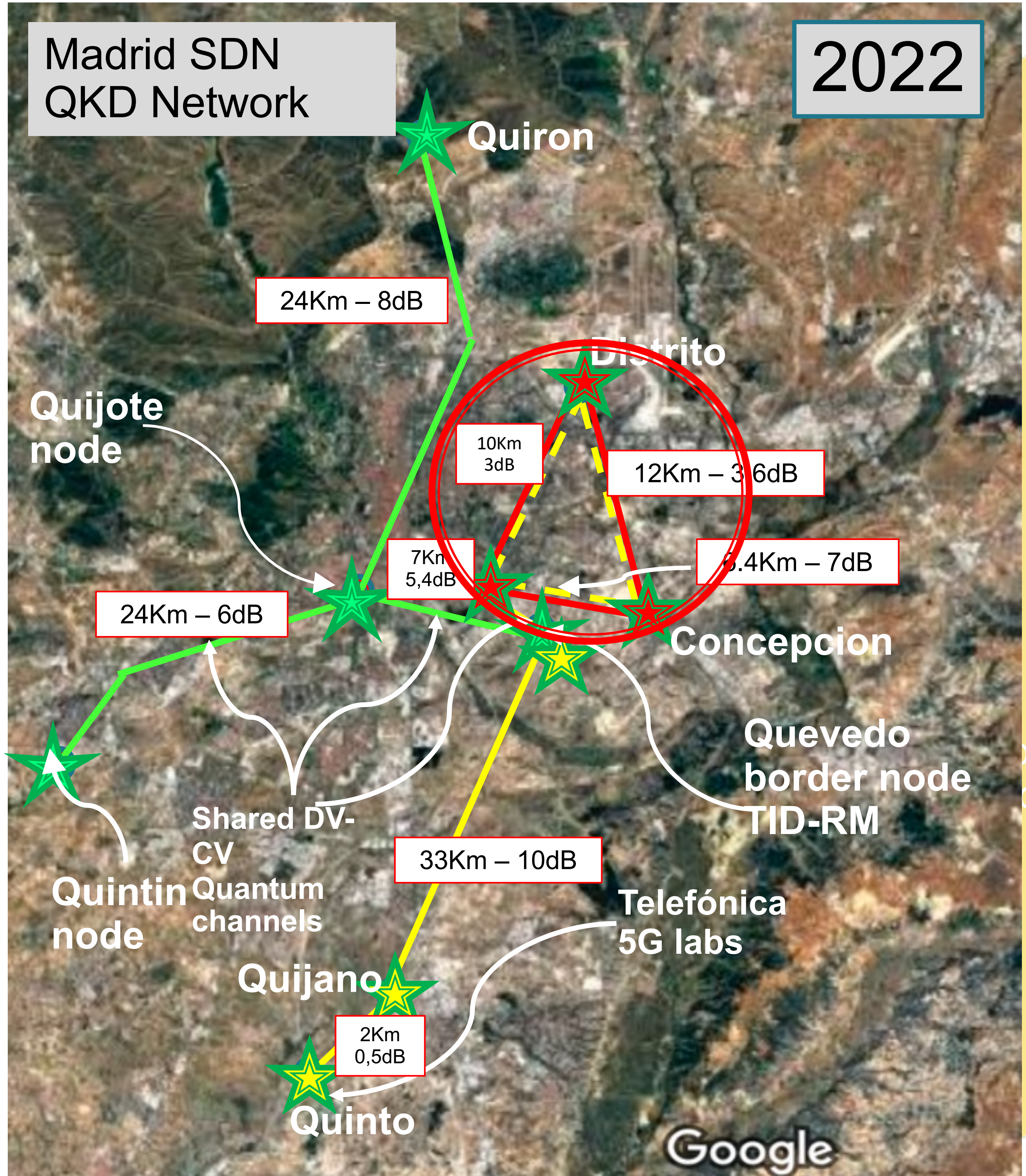
Graz AT Healthcare

Padua IT Free-space QKD

Matera IT Satellite QKD

ens GR a Com

Additional Industrial Spanish participation through the OpenCalls



MadQCI

- ★ Deployed, full installation.
- ★ Telefónica Ring
- ★ Under deployment

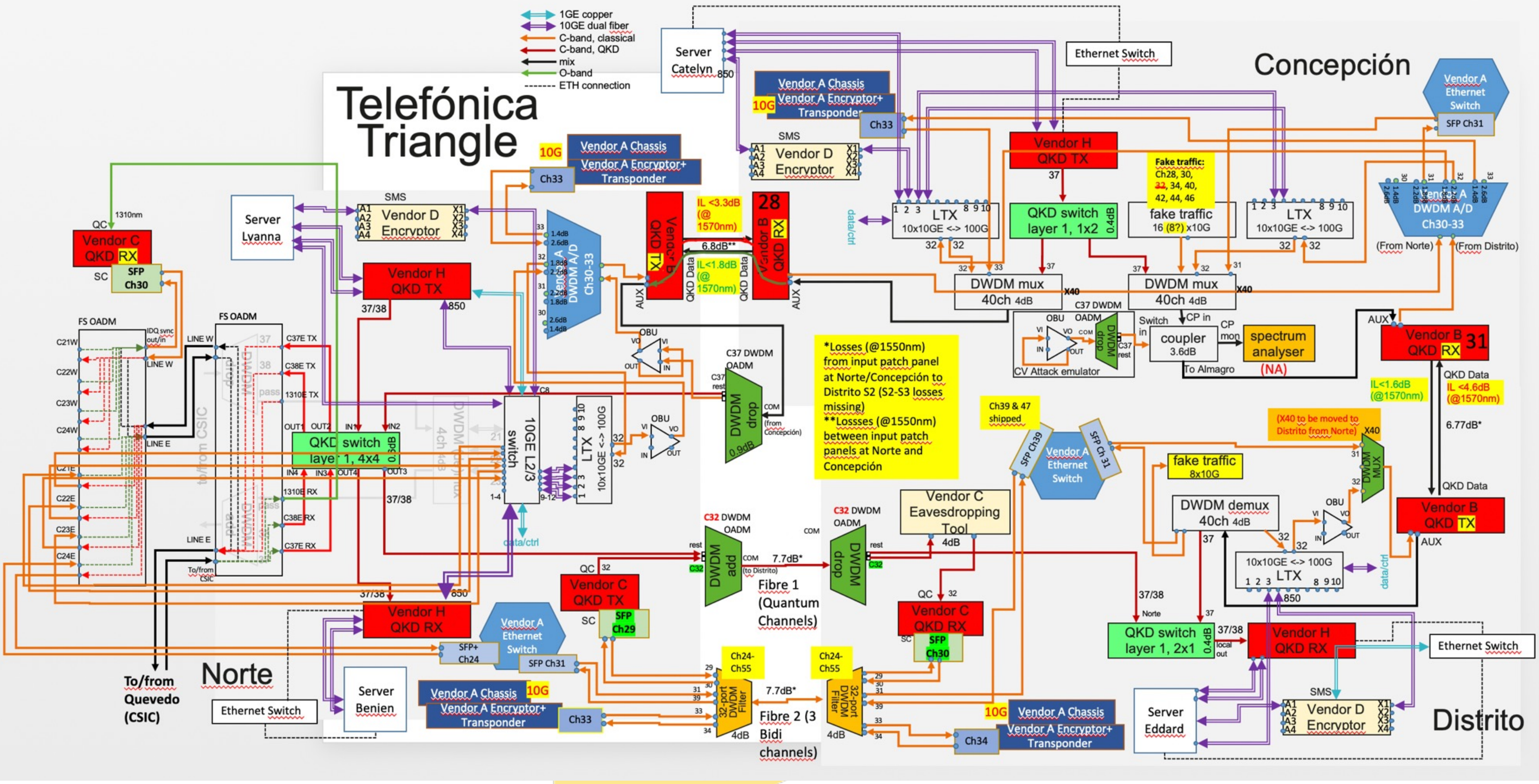
BoM: (26 Q devices installed)

- 4 QKD pairs idQ systems (3xC & 2xO band)
- 4 QKD pairs Toshiba (O band)
- ADVA optical transport equipment.
- 2 ADVA Level 1 encryptors.
- 5 R&S Level 2 SITLine encryptors
- Plus 5 HWDU CV QKD pairs (from CiViQ)

Important: A real world network.

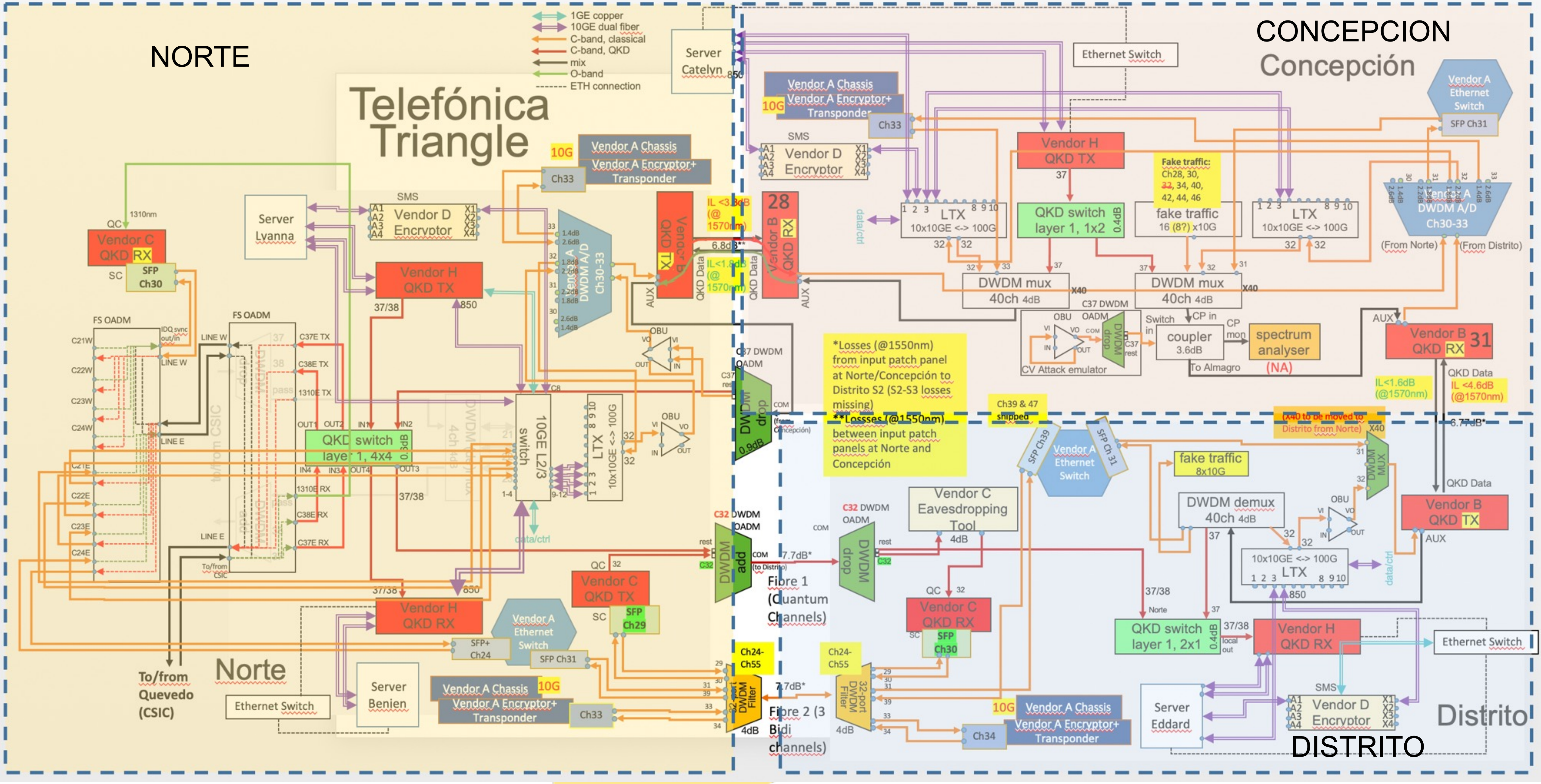
- Shared quantum and Classical infrastructure, including optical fibre. CV+DV systems on the same Fibre. Two connected operators. Several (quantum and Classical, QKD & encrypt.) manufacturers.

Telefónica Triangle



*Losses (@1550nm) from input patch panel at Norte/Concepción to Distrito S2 (S2-S3 losses missing)

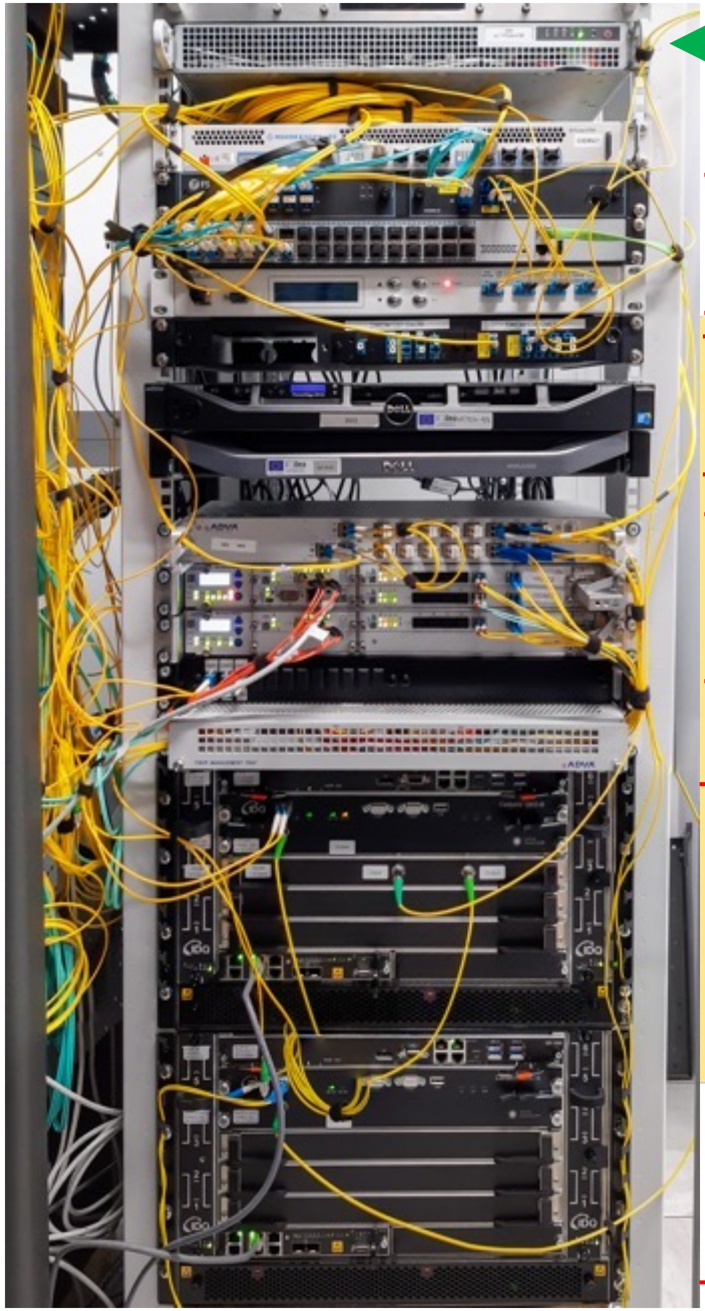
**Lossses (@1550nm) between input patch panels at Norte and Concepción



*Losses (@1550nm) from input patch panel at Norte/Concepción to Distrito S2 (S2-S3 losses missing)

**Lossses (@1550nm) between input patch panels at Norte and Concepción

Quijote
a “central” Node



R&S L2 encryptor

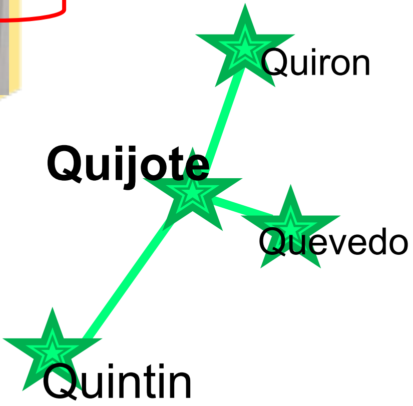
OADM+programm. Switch (add/drop Quantum Channels)

SDN server

ADVA OTN + Link encryptor

2 idQ DV QKD (C and O-band, 1550 nm + 1310nm) OpenQKD systems

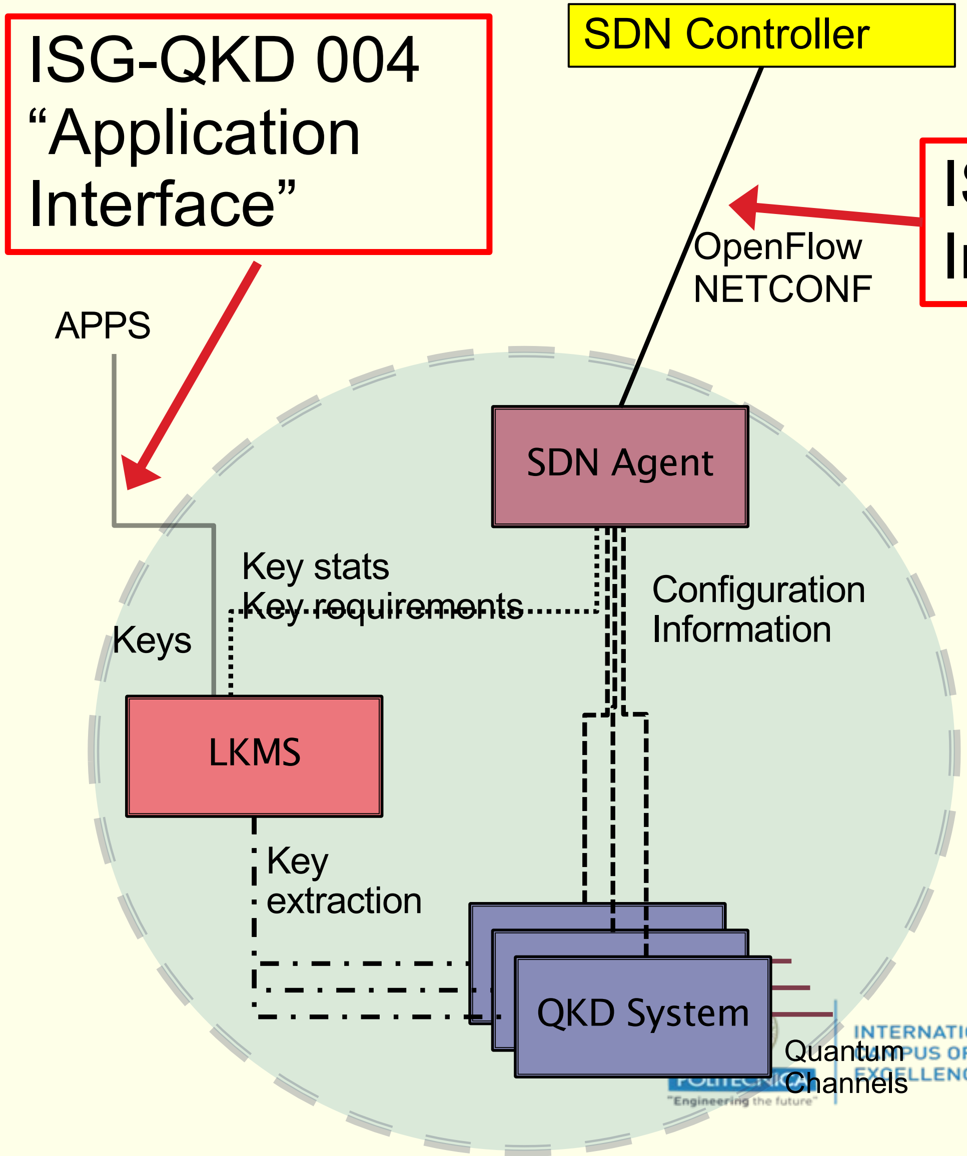
2 HWDU CV QKD + 2 servers From CiViQ



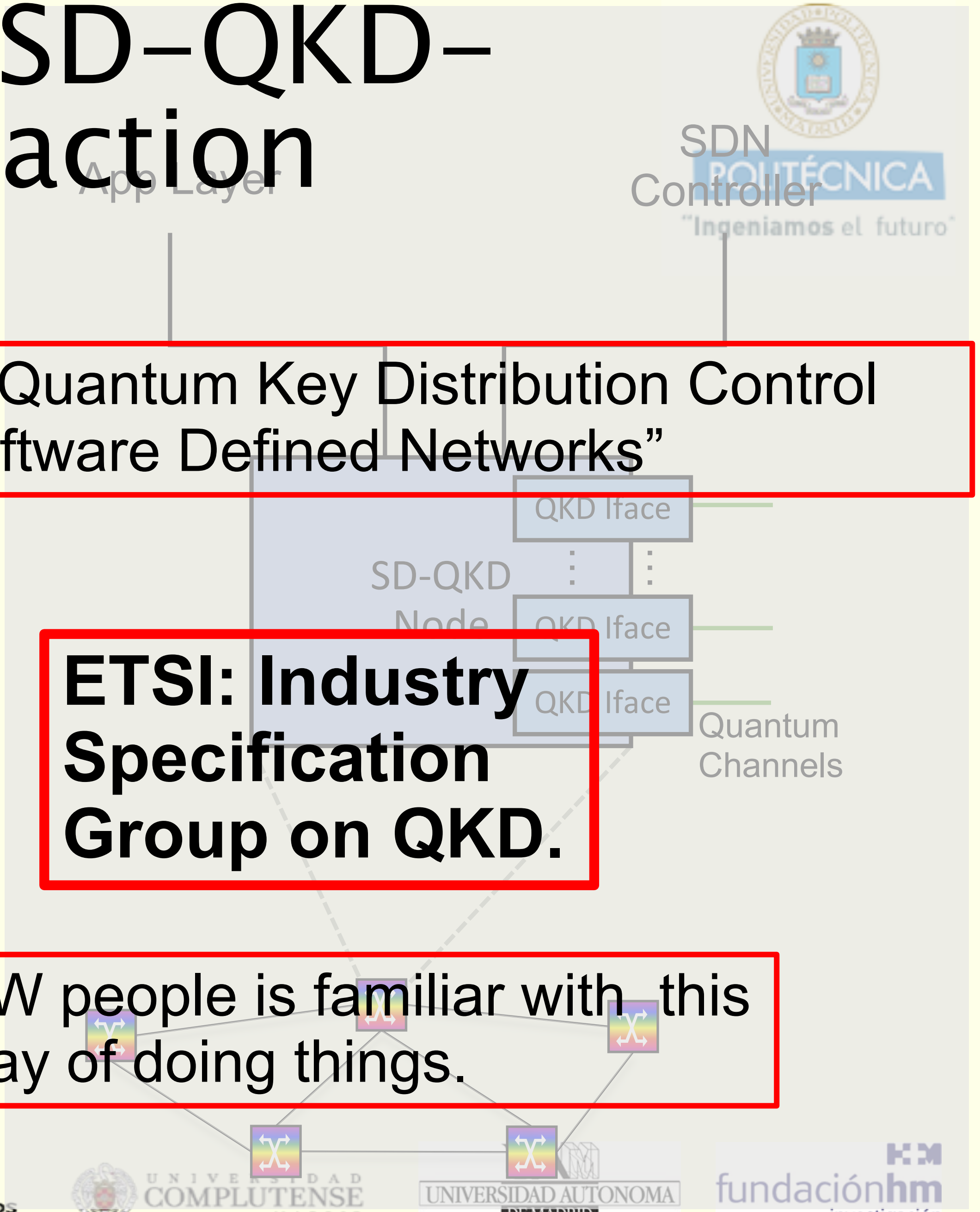
- 2 Quantum & service channels DV and CV from/to previous/next node. Compatibility in C & O bands in same fiber.
- Classical communications in bidi fiber, cyphered L1, L2 & L3 traffic.

Key structure: SD-QKD-Node Abstraction

ISG-QKD 004 “Application Interface”



ISG-QKD 015 “Quantum Key Distribution Control Interface for Software Defined Networks”

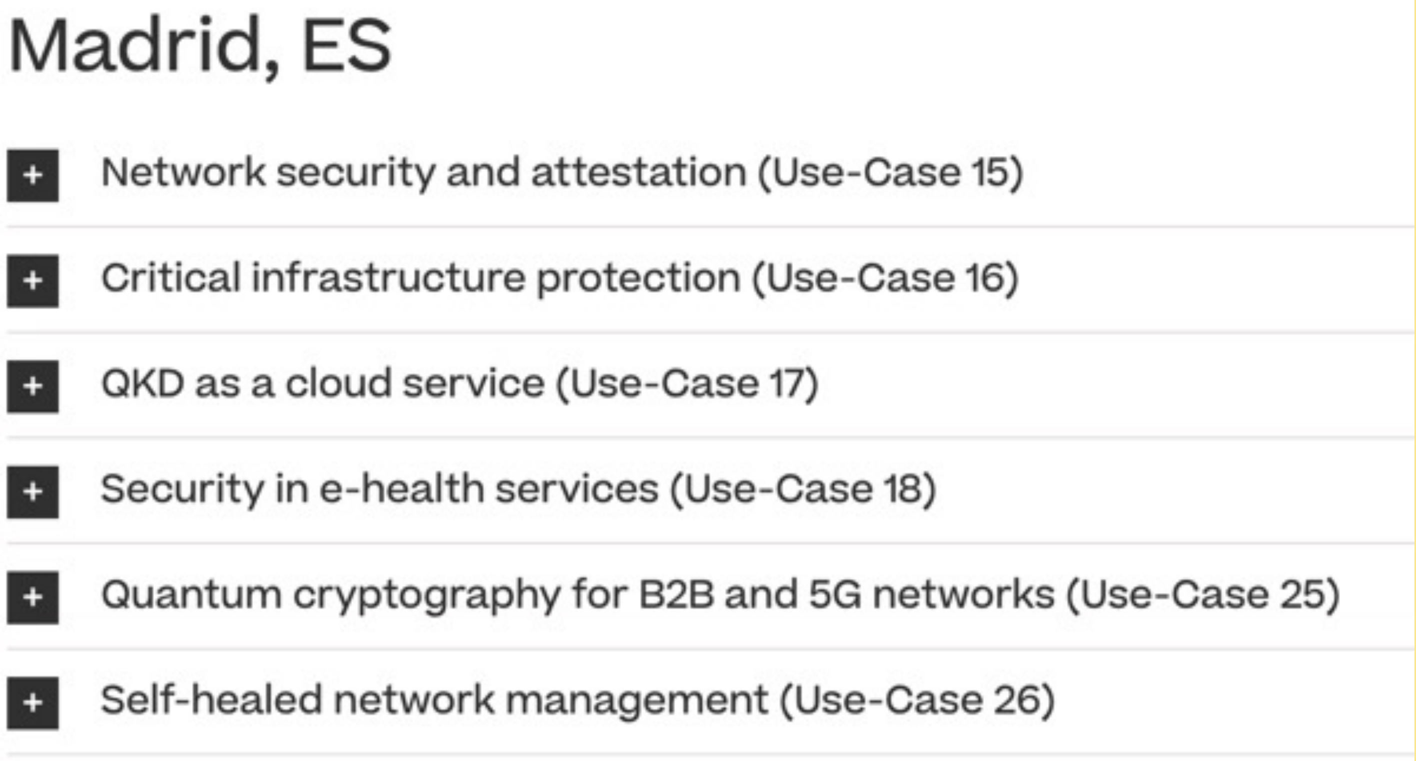


ETSI: Industry Specification Group on QKD.

NW people is familiar with this way of doing things.

Use-cases

OPEN QKD



Madrid, ES

- ＋ Network security and attestation (Use-Case 15)
- ＋ Critical infrastructure protection (Use-Case 16)
- ＋ QKD as a cloud service (Use-Case 17)
- ＋ Security in e-health services (Use-Case 18)
- ＋ Quantum cryptography for B2B and 5G networks (Use-Case 25)
- ＋ Self-healed network management (Use-Case 26)

+ OpenCalls successful submissions:

- **Q-KaaS: QKD Keys as a Service**
  - Up and Running –SME (Spain)
- **Phylogenetic Trees** (Quantum Secure Multiparty)
  - Coimbra Genomics -SME (Portugal)
  - U. Aveiro (Portugal)
  - HWDU Research (Germany, also CiViQ partner)
- **QGeKO** GMV- Access to Galileo Public Regulated Services

+ New approved OpenQKD use case:

- **Private transactions and permissioning in DLT networks**. (UC-35, Telefónica)

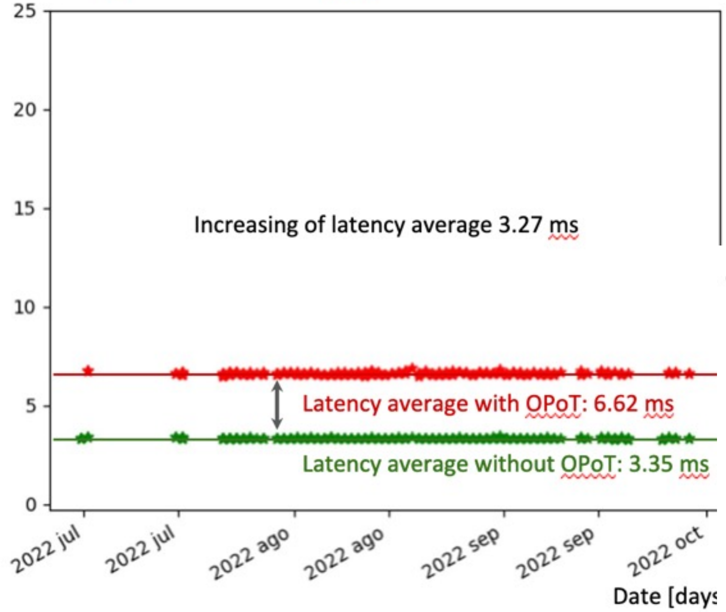
Check www.openqkd.eu for many more use-cases

Ejemplos de Métricas

15. Network security and attestation. KPI 29

Increased latency, in milliseconds

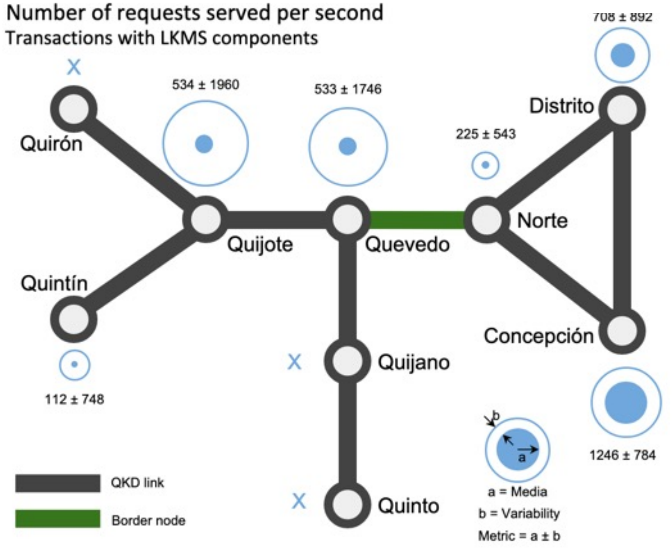
Latency [ms] with and without OPoT. Quintín-Quijote-Quevedo scenario.



17. QKD as a Cloud Service. KPI 17

Number of requests served per second

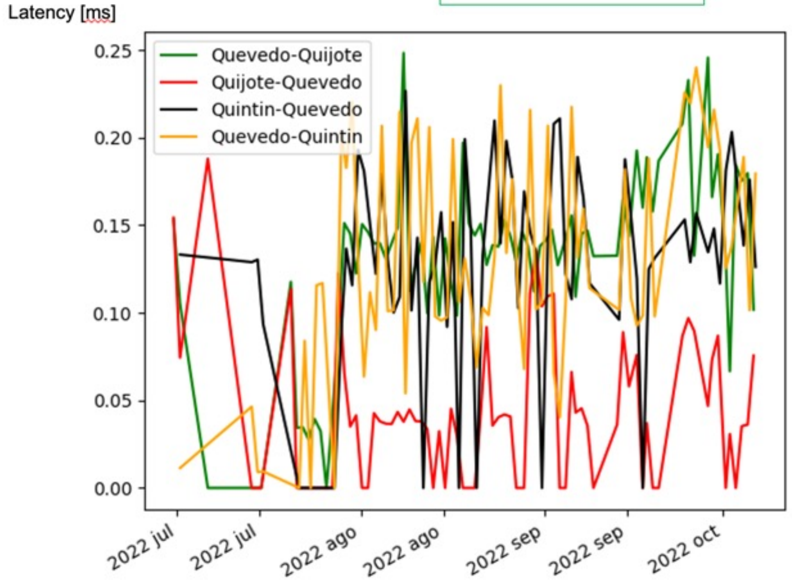
Transactions with LKMS components



18 y 25. e-Health, B2B and 5G services. KPI 30_31

Latency in serving a request, in microseconds

LATENCIA ENTRE MM. VV



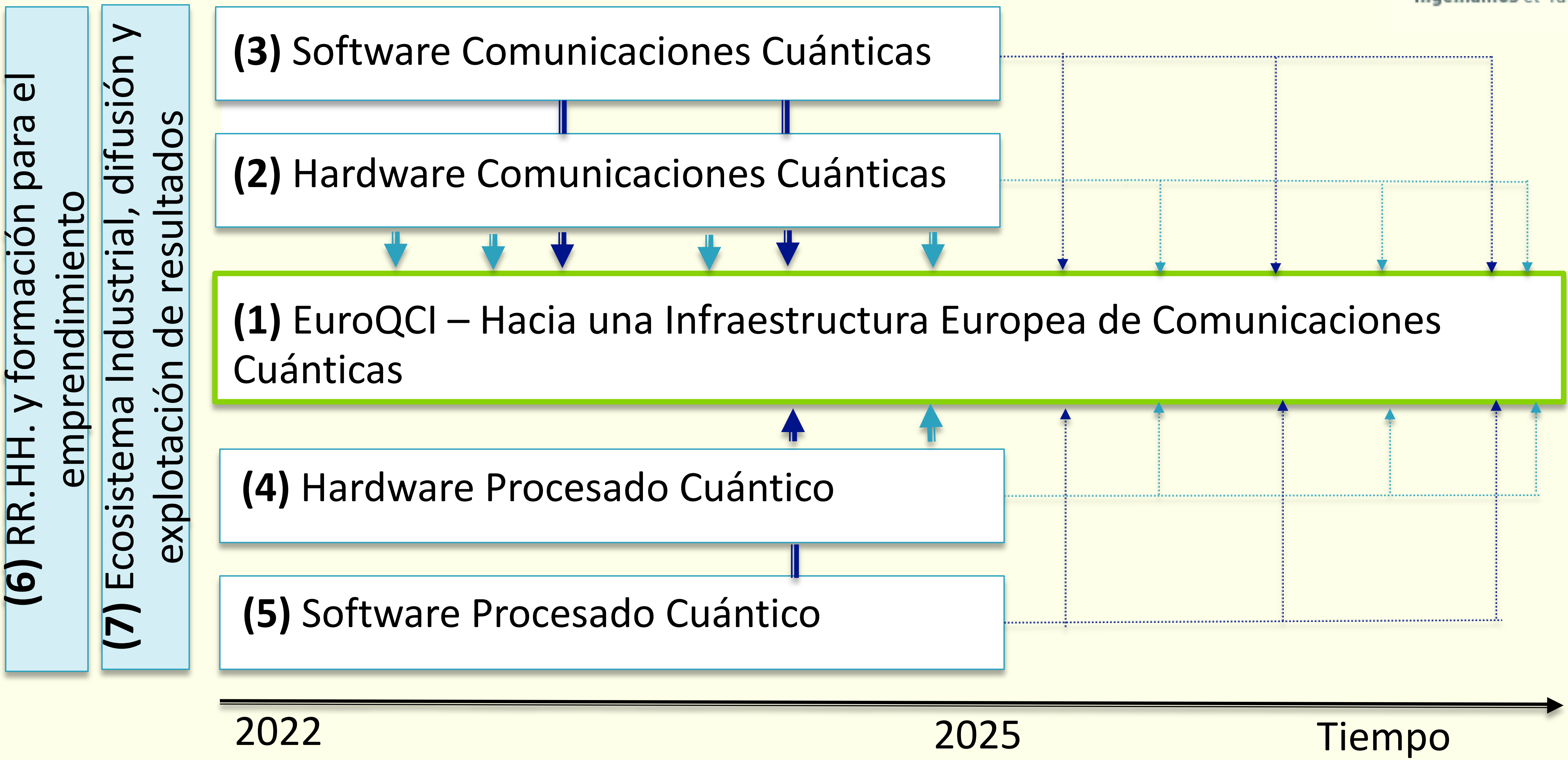
FUTURO: PLAN COMPLEMENTARIO DE I+D+I EN COMUNICACIONES CUÁNTICAS

CONTEXTO:

- **Plan de Recuperación, Transformación y Resiliencia** incluye un paquete de medidas para el fortalecimiento de las capacidades del Sistema Español de Ciencia, Tecnología e Innovación.
- **Planes Complementarios de I+D+I** constituyen una nueva herramienta de **coordinación y co-gobernanza** de la programación de la **Admin. General del Estado** y las **Comunidades Autónomas.**
- Inicialmente priorizadas **8 áreas** (EECTI 21-27). **Comunicaciones Cuánticas** es una.
  - Asignación inicial aproximada para todas las áreas **~ 250M€ + Contribuciones CCAA**
- **Status Comunicaciones Cuánticas**: Últimos pasos: **Pendiente de firma de convenios. 6** CCAA involucradas: Castilla y León, Cataluña, Galicia, Madrid, Pais Vasco + CSIC + Valencia
  - **Estimado total Comunicaciones Cuánticas: +50M€**
  - **Comienzo** esperado**: 2022**
- **Participación Industrial:** Llamadas competitivas

Esquema General:

Coordination with the EC framework



(6) RR.HH. y formación para el emprendimiento

(7) Ecosistema Industrial, difusión y explotación de resultados

(3) Software Comunicaciones Cuánticas

(2) Hardware Comunicaciones Cuánticas

(1) EuroQCI – Hacia una Infraestructura Europea de Comunicaciones Cuánticas

(4) Hardware Procesado Cuántico

(5) Software Procesado Cuántico

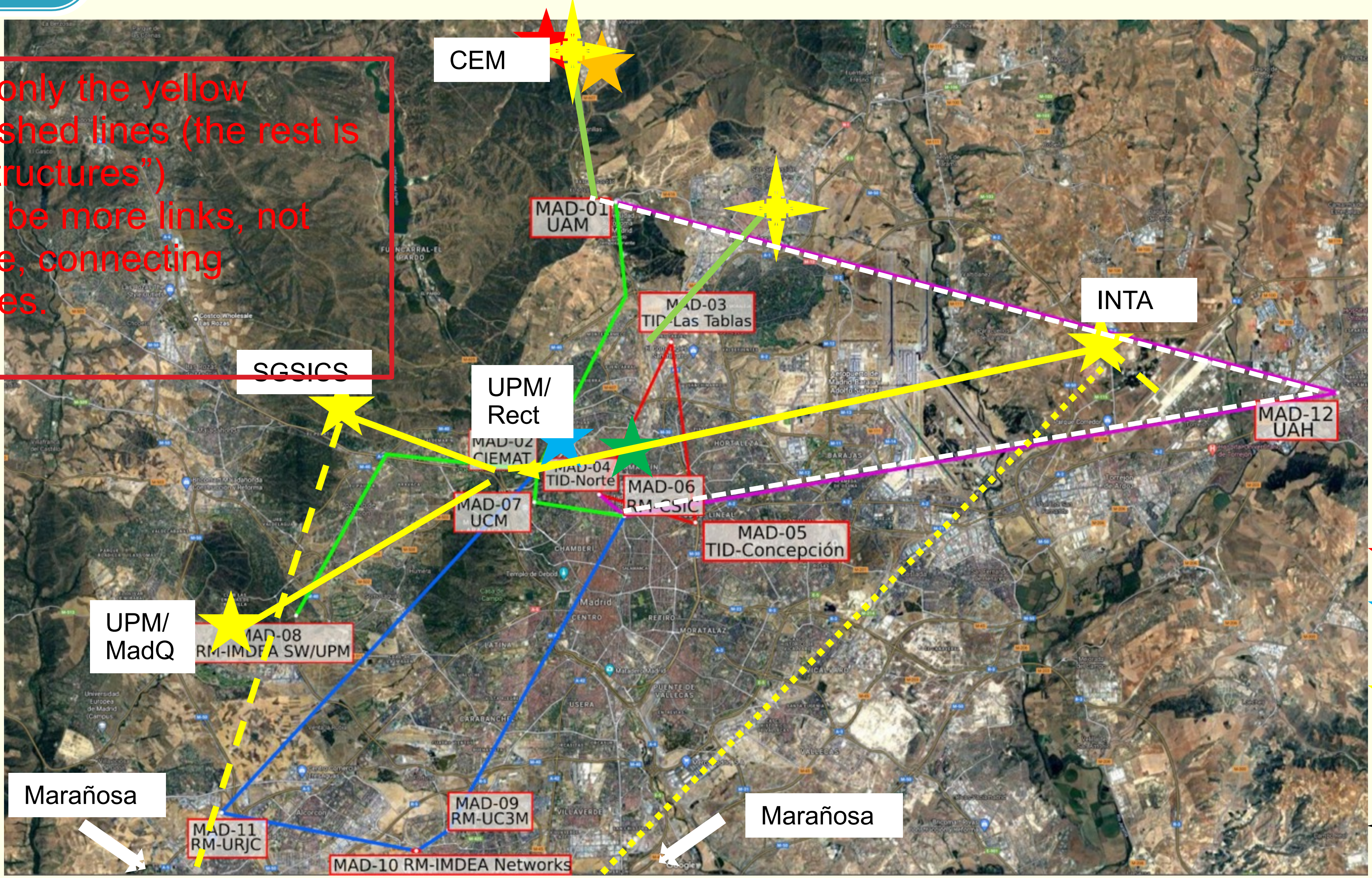
Madrid Quantum Communications Advanced Infrastructure

- Demonstration and capability creation.

1ST phase: 2 years Qualitative growth

POLITÉCNICA

"Ingeniamos el futuro"



- Consider only the yellow Solid and dashed lines (the rest is "other Infrastructures")
- There will be more links, not depicted here, connecting academic sites.

- Connection with EuroQCI Space segment
- Connecting users with Qualitatively different needs
- Evolve the infrastructure from research and demonstration to services

★ Business, banking
★ Health
★ High Security
★ Satellite: Long distan
★ New devs: metrology

✦ Access Network

EU H2020 Grant 820466

EU H2020 Grant 857156

Comunidad de Madrid
S2018/TCS-4342

***J.P. Brito[1], R. Brito[1], R. Vicente[1],
P. Salas[1], L. Ortíz[1], J. Saez[1],
J.L Rosales[1], R. Artiñano[1],
A.J. Sebastian[1], M. García[1],
D. R. Lopez[2], J.M. Rivas[2],
A. Pastor[2], F. Jiménez[2] ,
D. Rincon[3], F. Pérez [3], C. Sanchez[3],
V. Martin[1]***

*[1]Center for Computational Simulation and ETSI Informáticos,
Universidad Politécnica de Madrid 28660 Madrid, Spain
[2]Telefónica Investigacion y Desarrollo, Ronda de la
Comunicacion s/n 28050 Madrid. Spain
[3]IMDEA Software/RedIMadrid, 28660 Madrid. Spain*

Thanks!...
Questions/comments?

Vicente Martin
U. Politécnica de Madrid
Vicente@fi.upm.es
gcc.fi.upm.es