Quantum Cryptography and European Testbeds

XIV jornadas REDIMadrid

Universidad Rey Juan Carlos
Madrid, 22 Octubre 2019

Vicente Martin,
Vicente@fi.upm.es

Quantum Cryptography and New Generation Networks

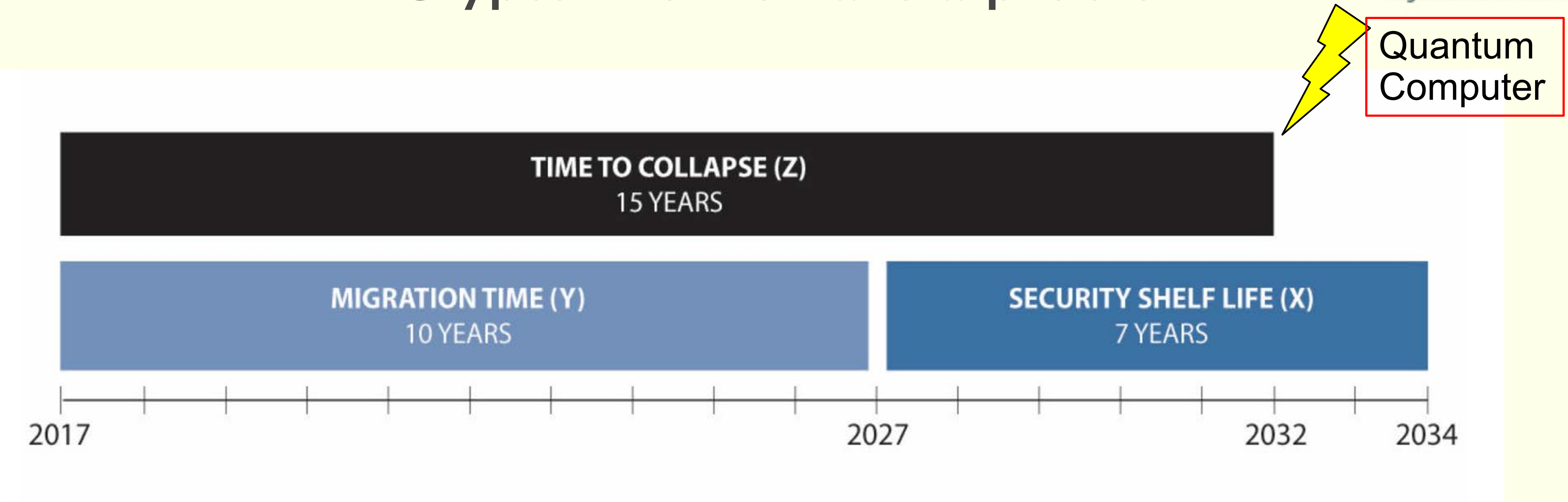
Index.

- Why Quantum Cryptography? Do we have a problem?
- Brief Intro to Quantum Key Distribution
- QKD and networks.
- Software Defined Networking and the Madrid Quantum Network
- OpenQKD: European QKD Testbeds
- Future

Quantum Computing and Quantum 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
- But, you know, building a quantum computer **will take forever…**
  - Or, at least, so many years that you do not need to worry…

Quantum Computing and Quantum 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?)

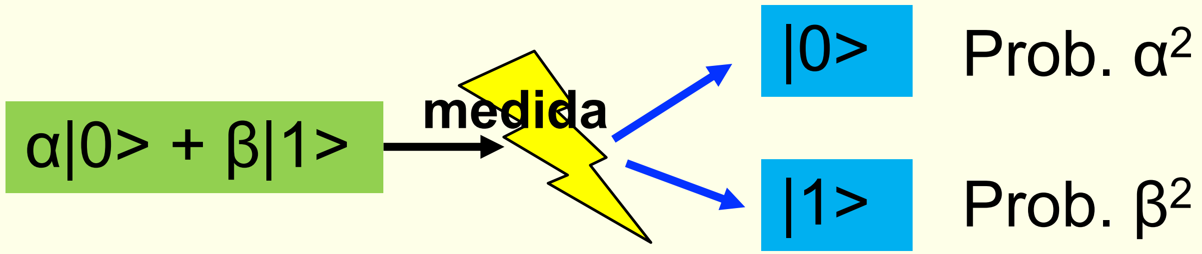
If X+Y > Z… you have problems.

Solutions:

- **Postquantum crypto:** Business as usual.
  - "new" **algorithms** believed to be secure against Quantum Computers.
- **Quantum Cryptography:**
  - **Physical** layer security -> Networks
    - You need hardware
    - … and it is not easy
  - Not a complete substitute! (symmetric crypto)

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):**

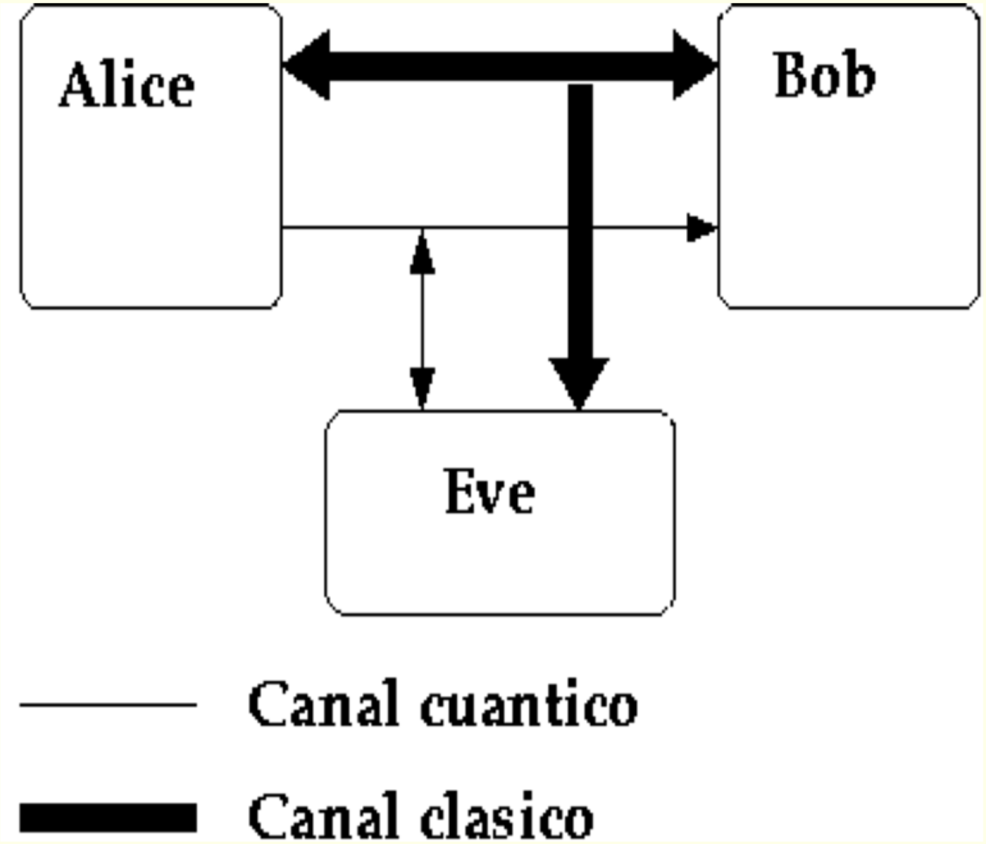


  - $(\alpha^2+\beta^2 = 1)$
  - Nótese que **la lectura modifica el estado del qubit.**
  - Teorema de la No-clonación: **No se puede copiar un estado cuántico desconocido.**

Quantum Criptography

Ingredientes:

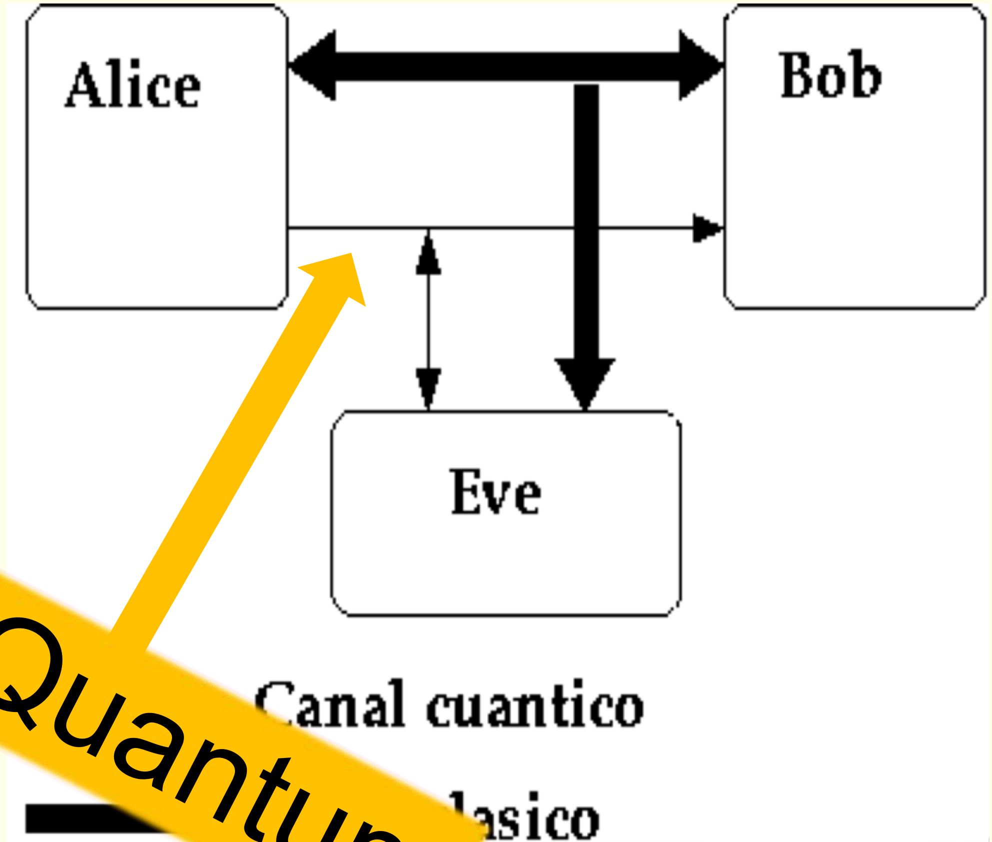
- Un **emisor de qubits** (típicamente fotones) individuales (Alice)
- **Receptores** de qubits individuales (Bob)
- Un **canal cuántico** (capaz de transmitir los qubits de Alice a Bob)
- Un **canal clásico** (público pero **autenticado**)
- … y un espía (Eve)



Quantum Criptography... en redes

Ingredientes:

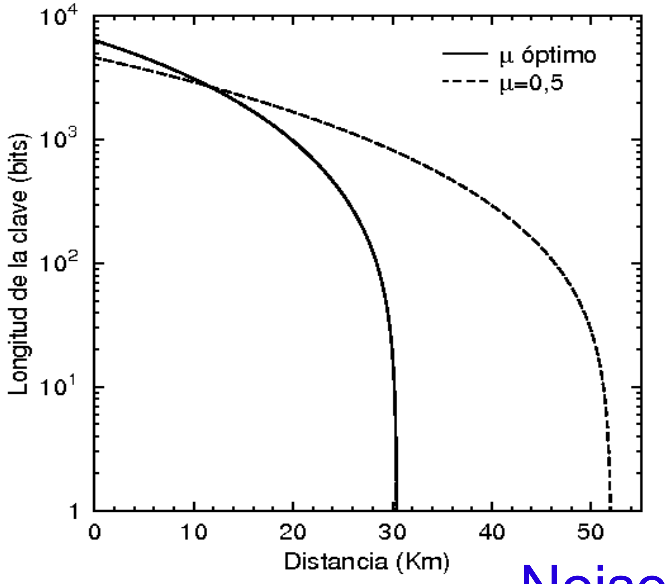
- Un **emisor de qubits** (típicamente fotones) individuales (Alice)
- **Receptores** de qubits individuales (Bob)
- Un **canal cuántico** (capaz de tra... los qubits de Alice a Bob)
- Un **canal clásico** (público pero **autenticad**...
- … y un espía (Eve)



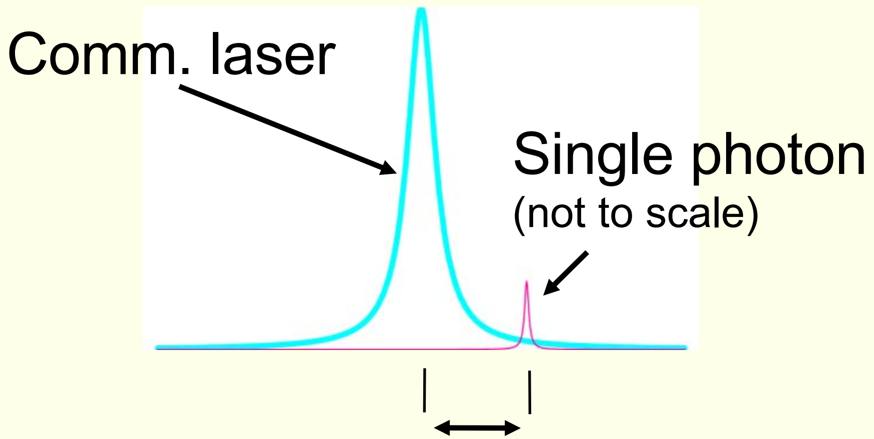
Center for Computational Simulation
POLITÉCNICA "Ingeniamos el futuro"
POLITÉCNICA "Engineering the future" INTERNATIONAL CAMPUS OF EXCELLENCE
Universidad Rey Juan Carlos
UNIVERSIDAD COMPLUTENSE MADRID
UAM UNIVERSIDAD AUTONOMA DE MADRID
fundaciónhm investigación

Quantum communications and networks, why is it difficult?

Limited reach, point to point.



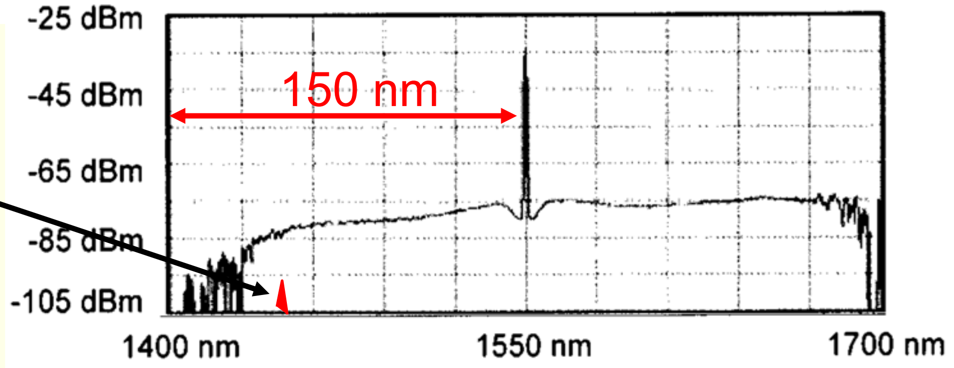
extremely weak signals.



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]

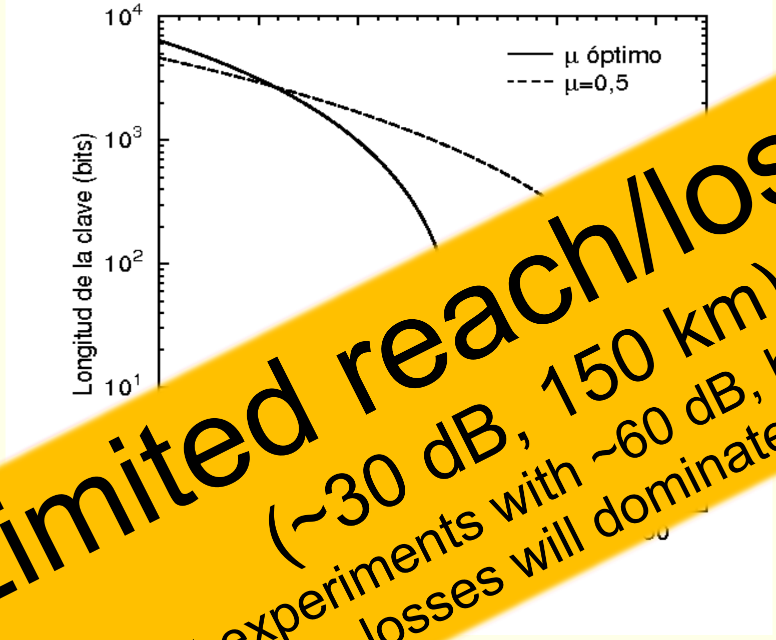
- Difficult to detect.
- Absorpions
- Masked by the noise

Quantum communications and networks, why is it difficult?

Center for Computational Simulation

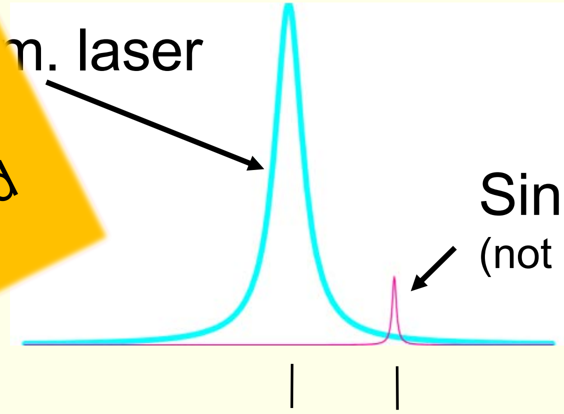
POLITÉCNICA "Ingeniamos el futuro"

Limited reach, point to point.



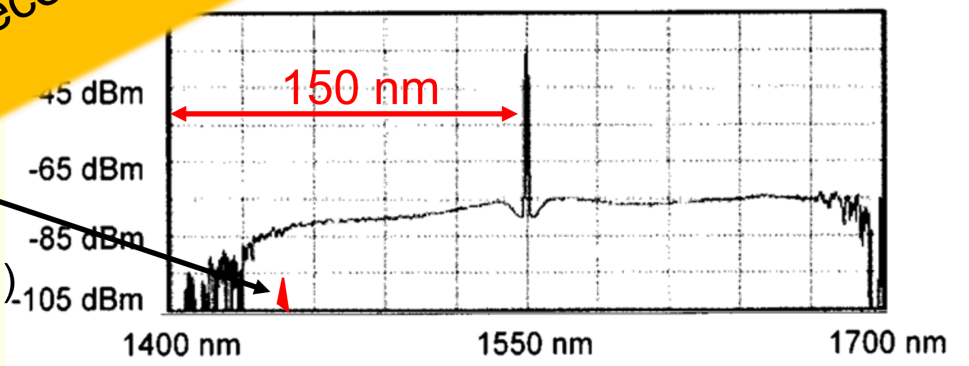
Limited reach/losses
(~30 dB, 150 km)
(recent experiments with ~60 dB, but in the end losses will dominate)

extremely weak signals.



Δλ = 0.2~0.8 nm (DWDM)
Δλ = 3~20 nm (CWDM)

...ise in the fibre: Raman



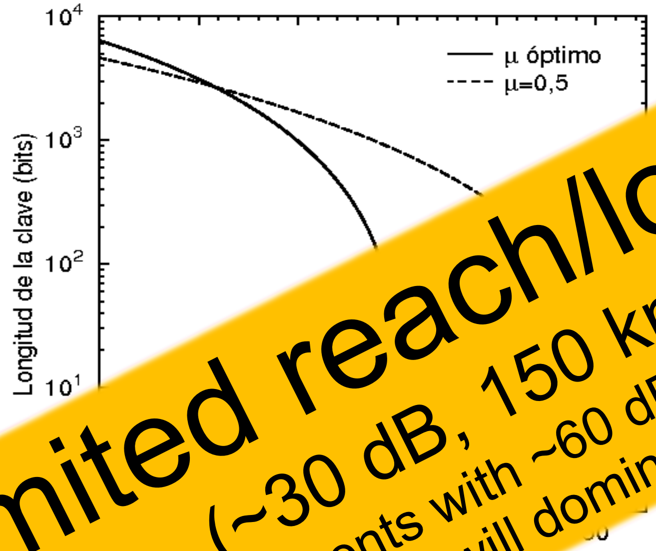
Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

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

Universidad Rey Juan Carlos · UNIVERSIDAD COMPLUTENSE MADRID · UAM UNIVERSIDAD AUTONOMA DE MADRID · fundaciónhm investigación

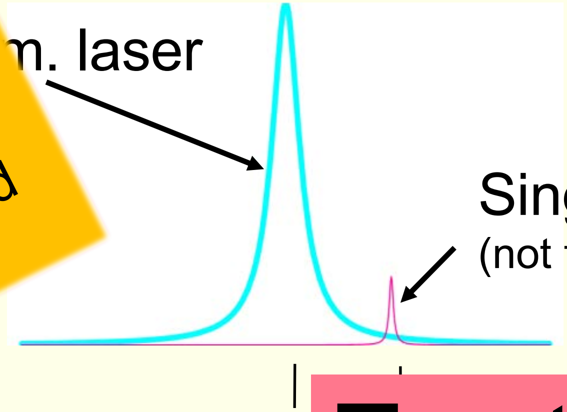
Quantum communications and networks, why is it difficult?

Limited reach, point to point.

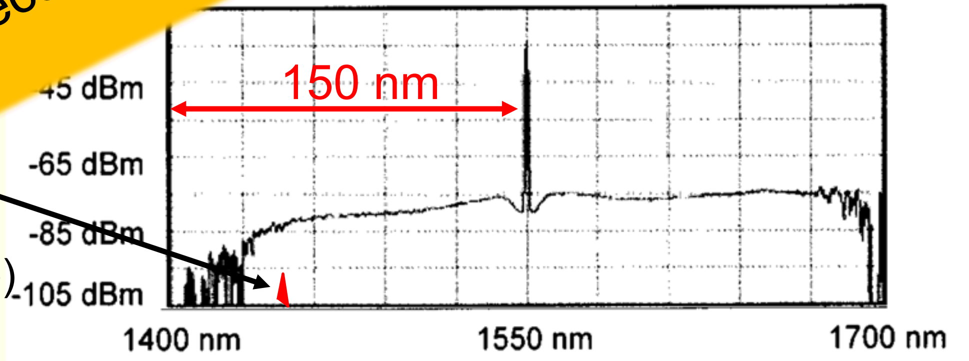


Limited reach/losses
(~30 dB, 150 km)
(recent experiments with ~60 dB, but in the end losses will dominate)

extremely weak signals.



...ise in the fibre: Raman



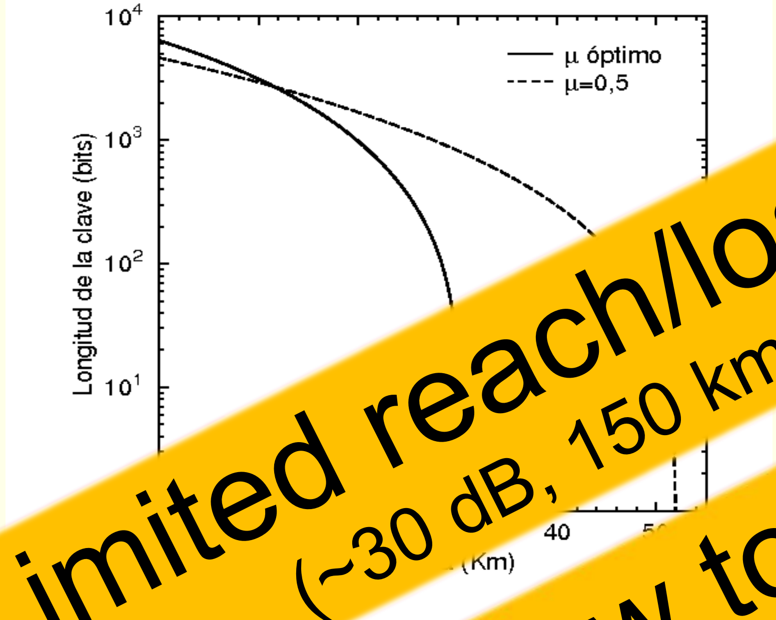
Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

Trusted nodes are required
(security issues)

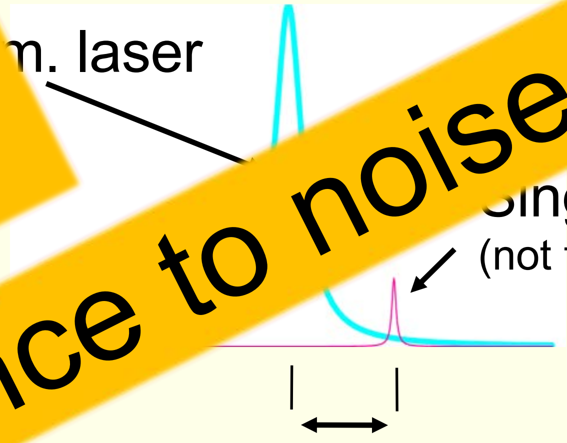
- Absorpions
- Masked by the noise

Quantum communications and networks, why is it difficult?

Limited reach, point to point.



extremely weak signals.

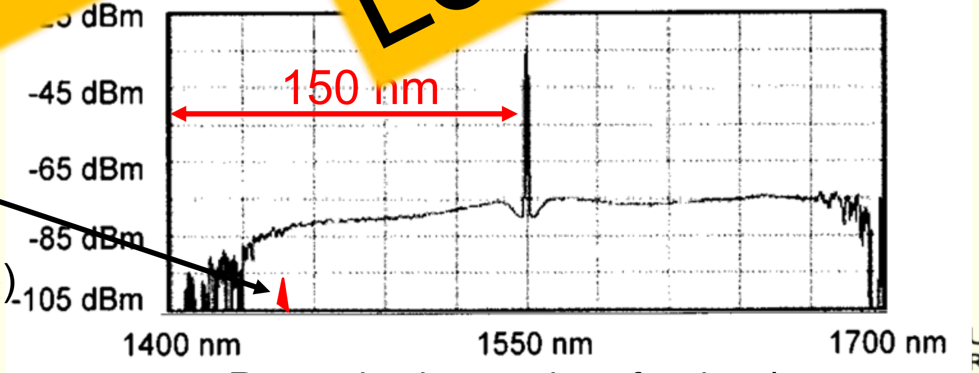


Δλ = 0.2~0.8 nm (DWDM)
Δλ = 3~20 nm (CWDM)

Limited reach/losses
(~30 dB, 150 km)

Low tolerance to noise

Noise source: Raman



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

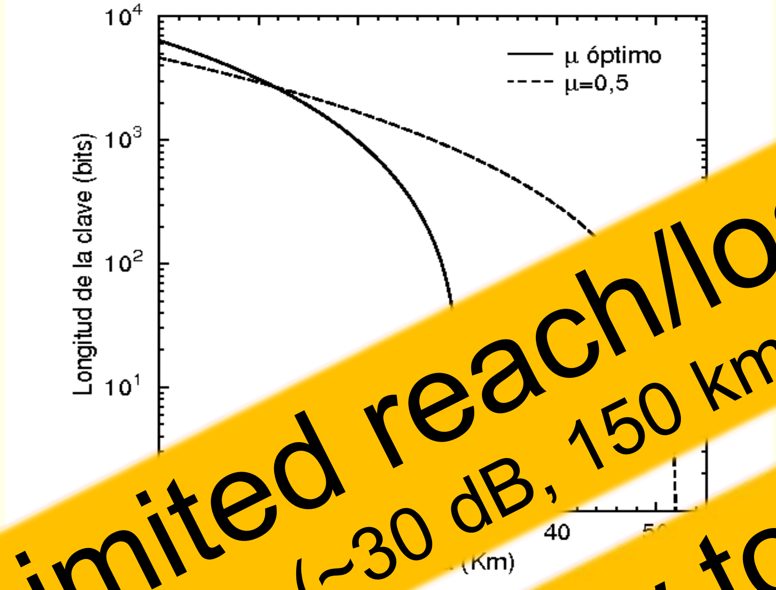
- Difficult to detect.
- Absorptions
- Masked by the noise

Center for Computational Simulation

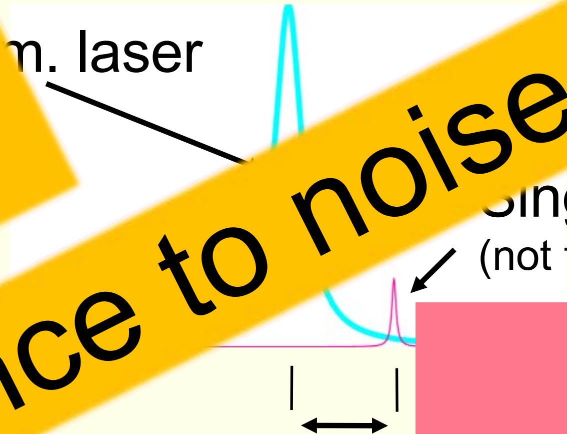
Quantum communications and networks, why is it difficult?

POLITÉCNICA
"Ingeniamos el futuro"

Limited reach, point to point.



extremely weak signals.



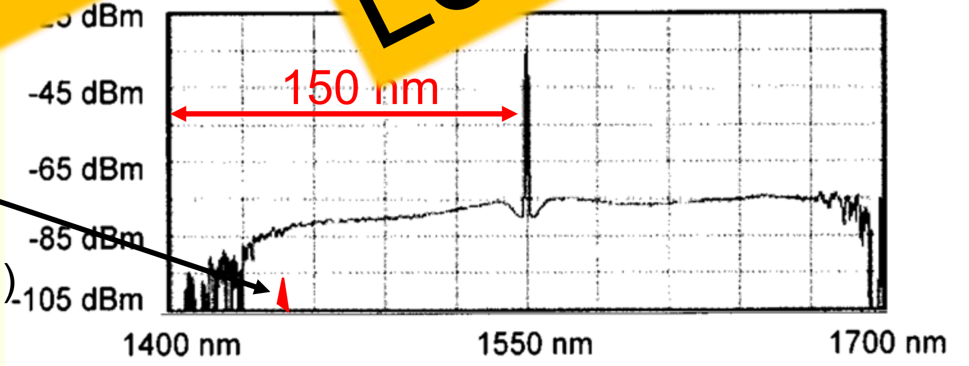
Limited reach/losses
(~30 dB, 150 km)

Low tolerance to noise

Quantum/ classical co-propagation Issues

(not sharing the infrastructure –> Expensive!!)

Noise ... e: Raman



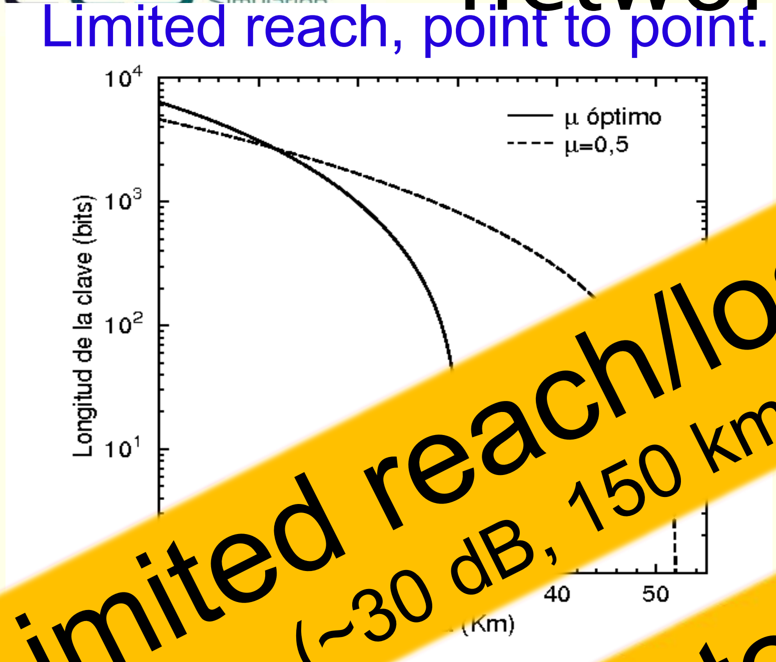
Single Photon (approx. scale)

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

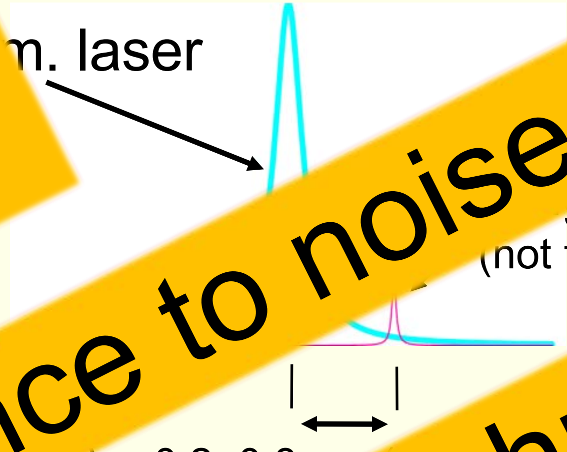
Universidad Rey Juan Carlos
UNIVERSIDAD COMPLUTENSE MADRID
UNIVERSIDAD AUTONOMA DE MADRID
fundaciónhm investigación

Quantum communications and networks, why is it difficult?

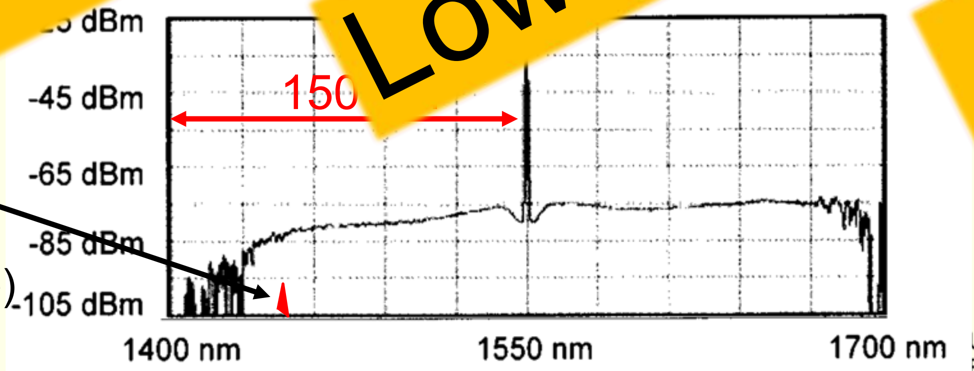
Limited reach, point to point.



extremely weak signals.



Noise i... Raman



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

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

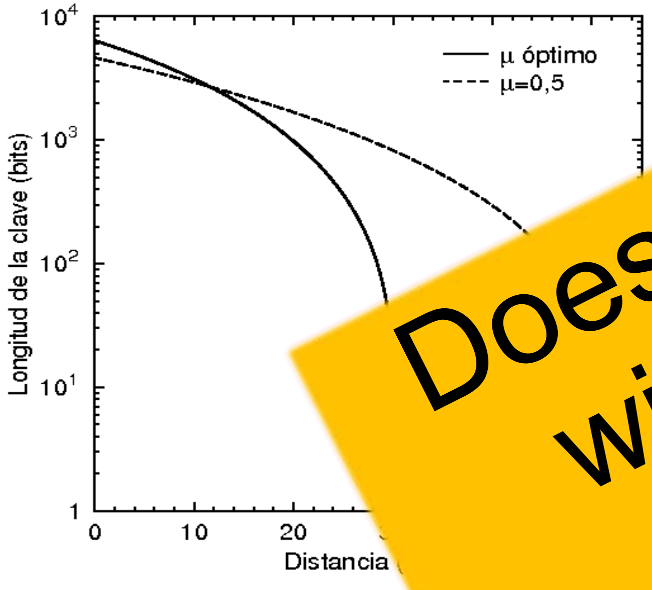
Limited reach/losses
(~30 dB, 150 km)

Low tolerance to noise

Alien technology
(HW &SW)

Quantum communications and networks, why is it difficult?

Limited reach, point to point.



Single
(not to s

Δλ = 0.2~0.8 nm (DWDM)
Δλ = 3~20 nm (CWDM)

Noise in fibre: Raman

Does not play well with (classical) networks.

- Ad-hoc network: Large Up-front costs
- Limited range: Security model requires trusted nodes

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

It is a delicate technology.

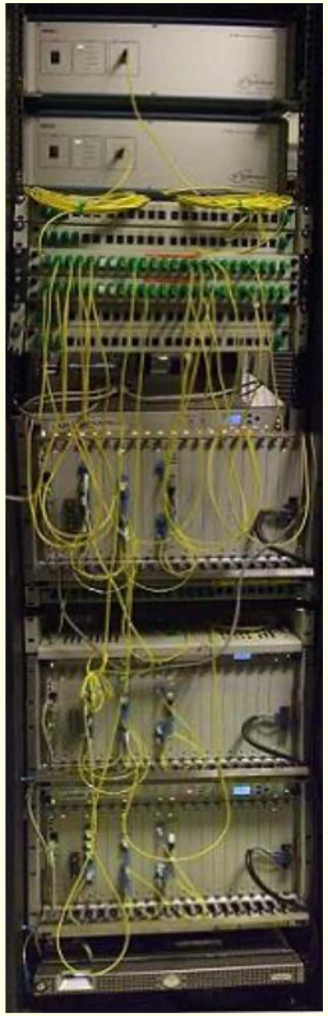
R. Doisneau

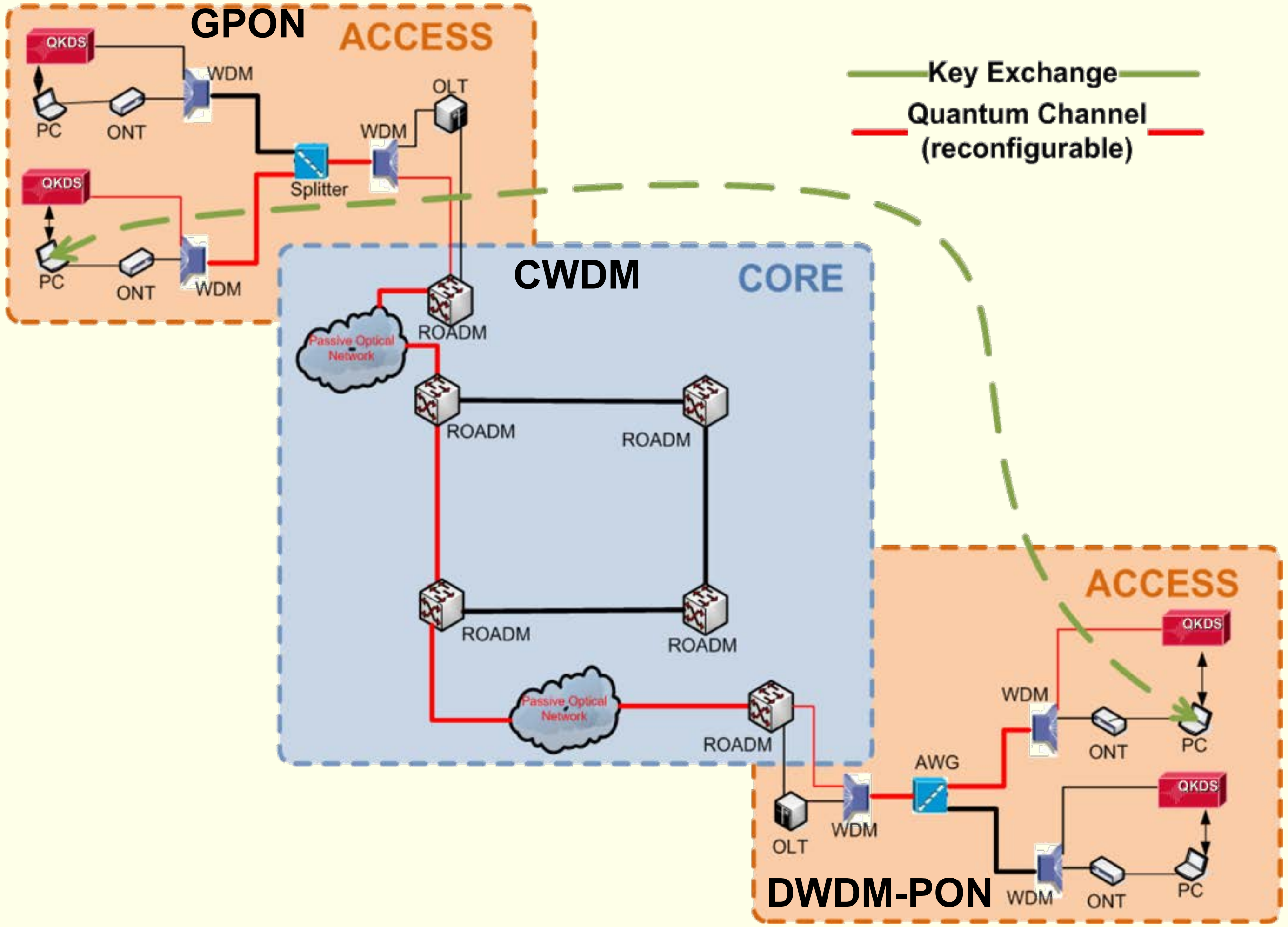
Center for Computational Simulation

POLITÉCNICA "Ingeniamos el futuro"

fundaciónhm investigación

What to do? Madrid UPM-TID QKD Networks: Access + Core metro networks

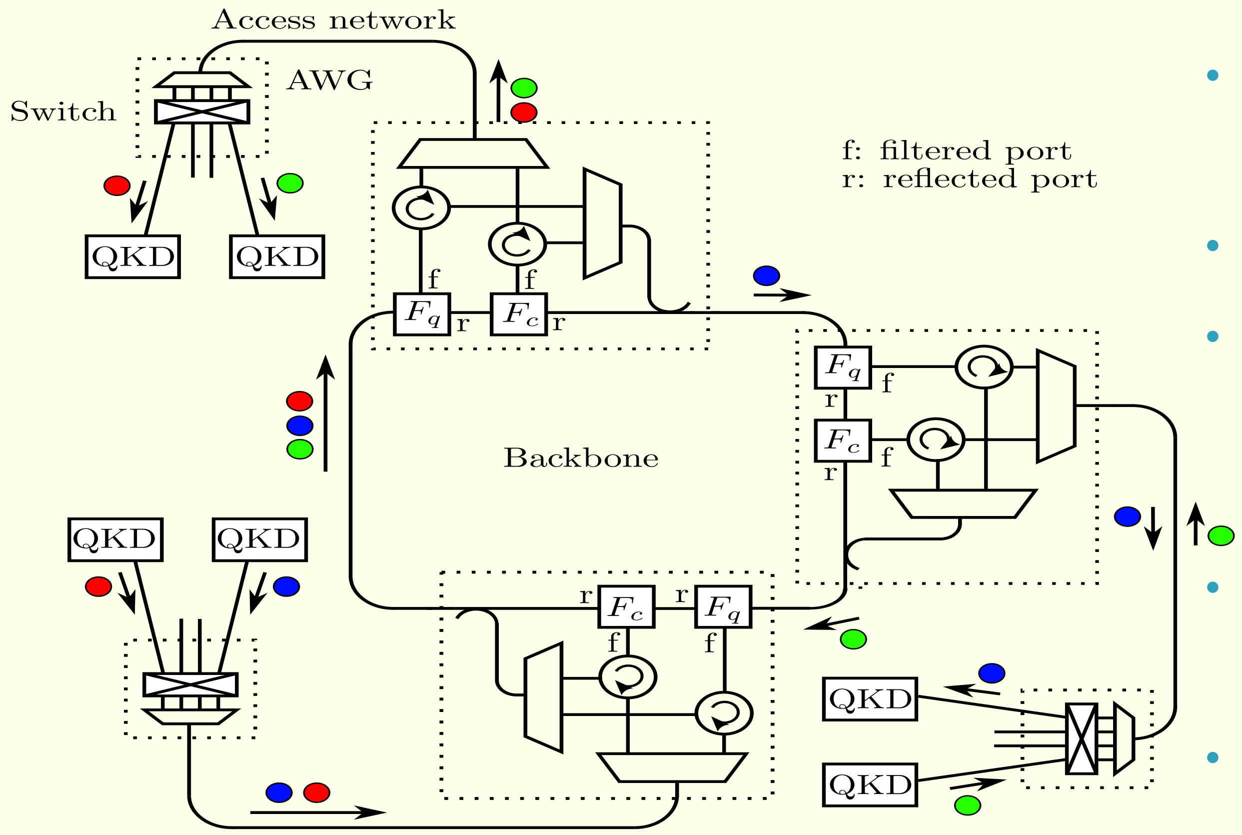




Estudiar la **integración de QKD en redes** de comunicaciones en **coexistencia con señales clásicas** y con **equipos convencionales**

(2009)

What to do? Extreme "ad hoc" network



- **A network just for quantum.**
  - Including "all channels": Quantum, service and distillation.
  - **No trusted nodes** (metro area)
  - **Addressable**: The emitter can decide whom to talk to by chosing the wavelength.
  - As **many users** as possible (dem. 64)
  - Use as much deployed infrastructure and commercial equipment as possible.

- Quantum metropolitan optical network based on wavelength division multiplexing, Optics Express 22, 1576-1593, 2014 (arXiv:1309.3923)
- Entanglement Distribution in Optical Network, IEEE J. S. Topics in Quantum Electronics 21, 37-48, 2015 (arXiv:1409.5965)

What to do? Madrid Quantum Network: First SDN-QKD network in the world

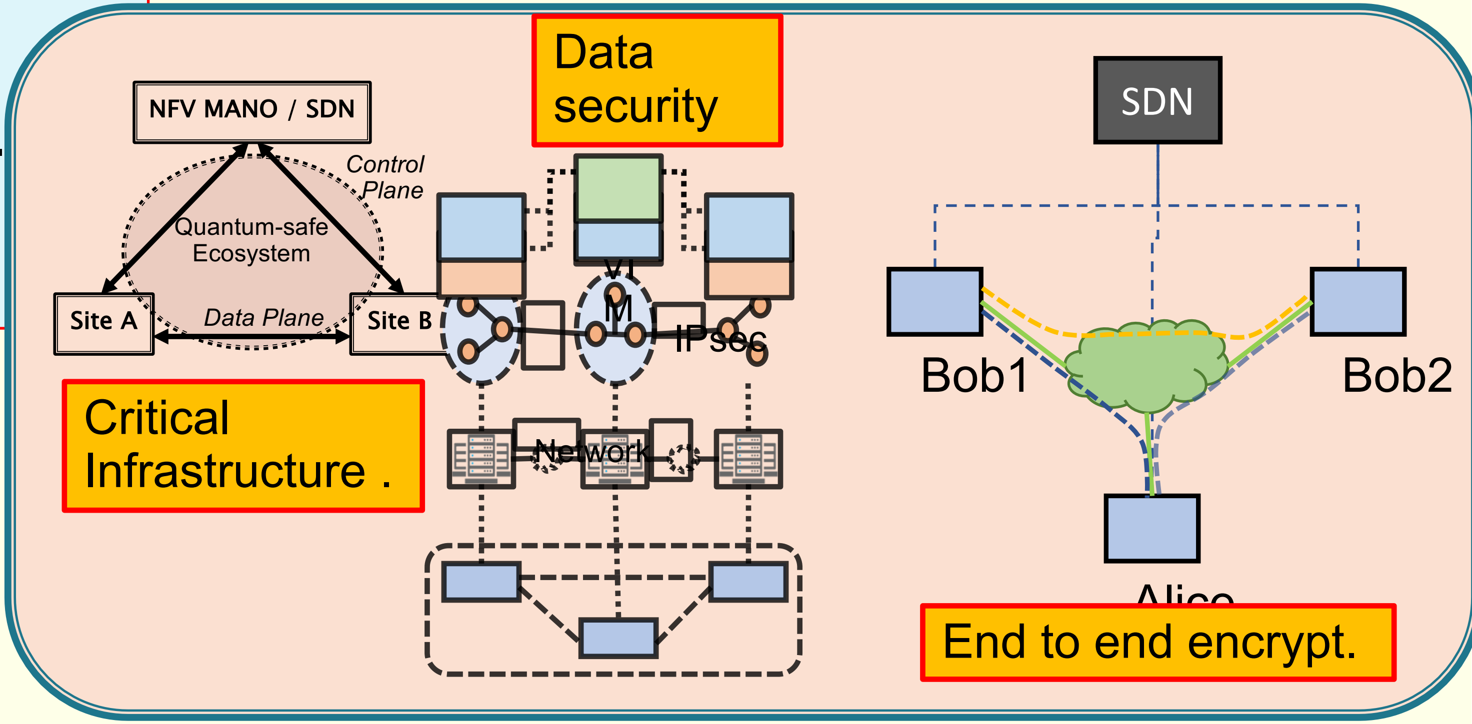
Use the correct technology

- SDN – Software Defined Networking
  - Network Flexibility
- CV-QKD technology:
  - Better tolerance to noise: quantum/classical copropagation.
  - Prospective industrialization path

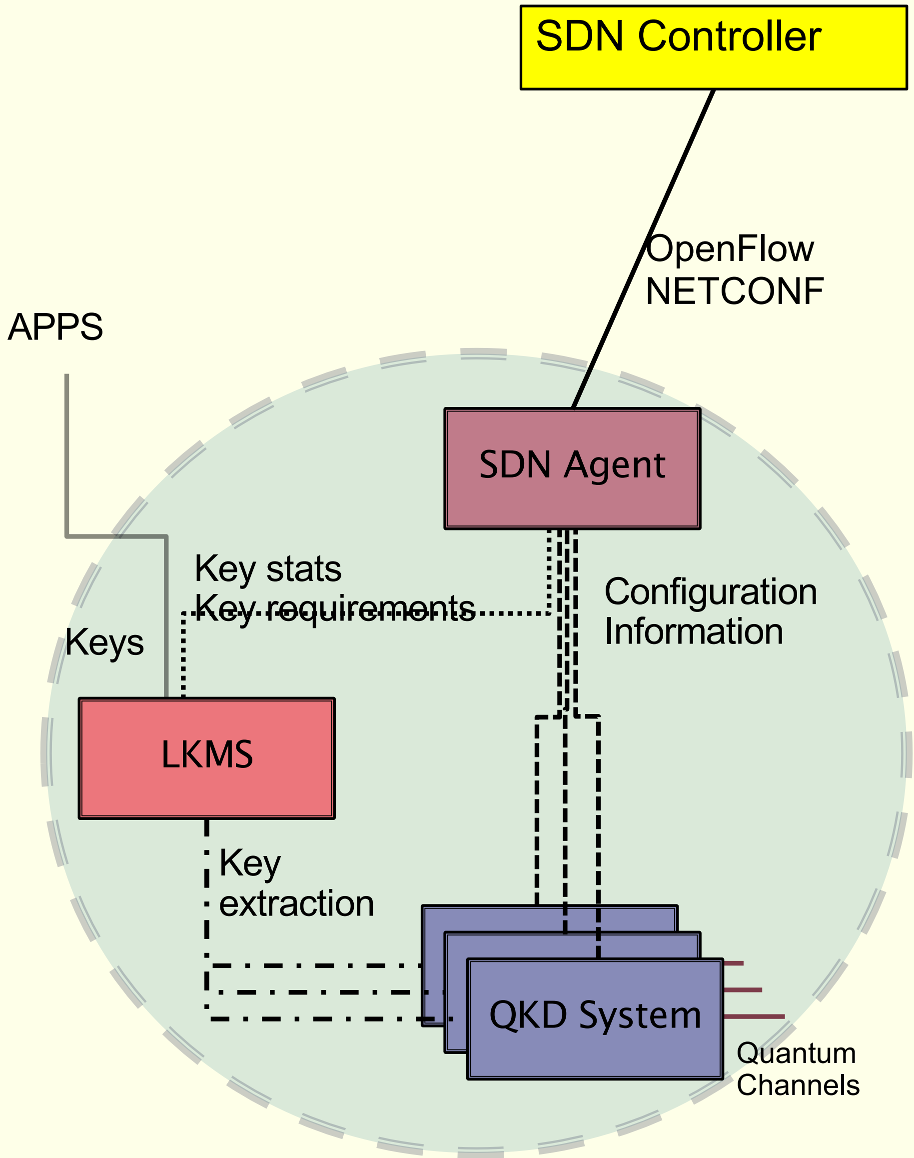
CiViQ

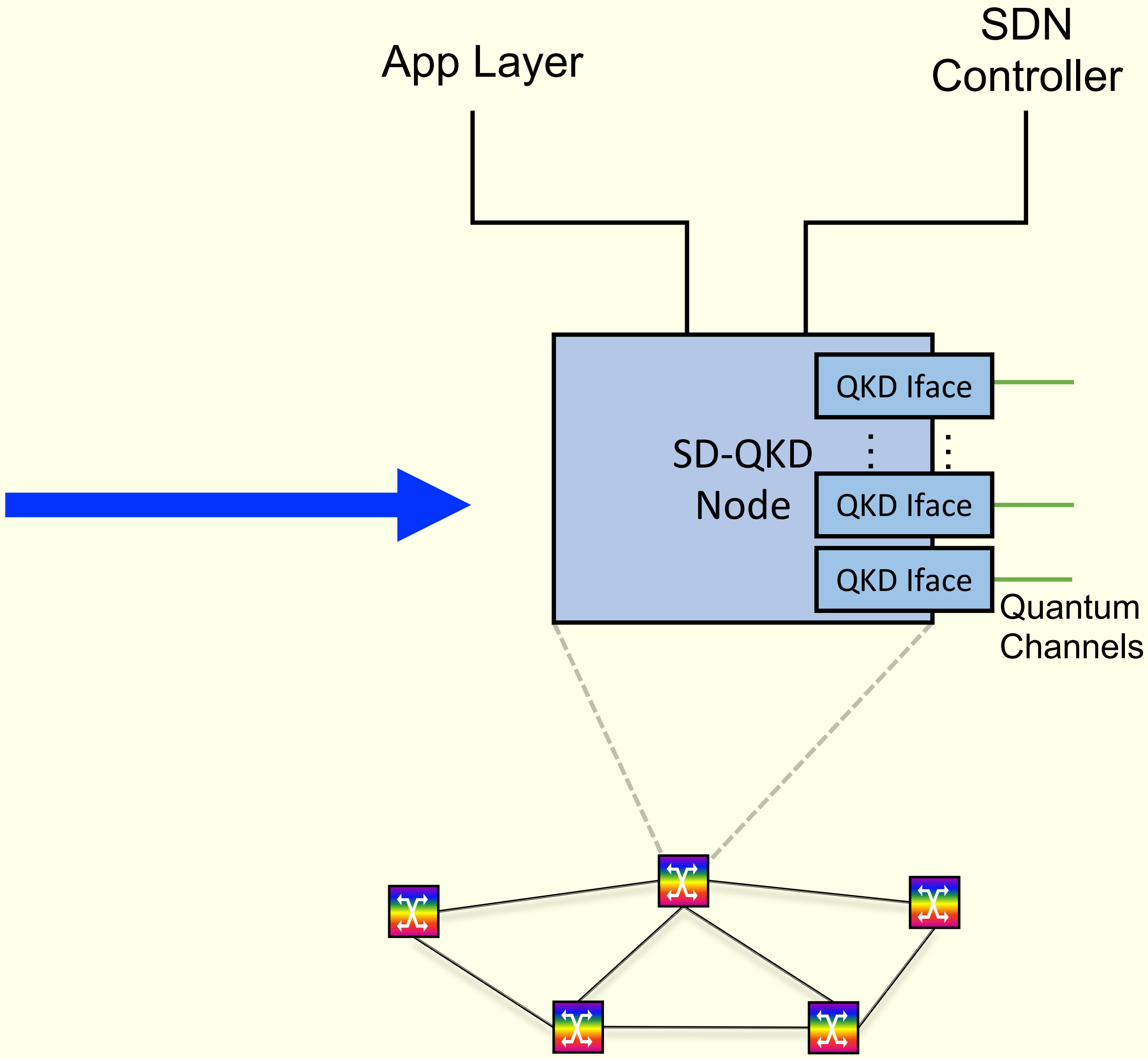
EU H2020
Grant 820466

Real world use cases:

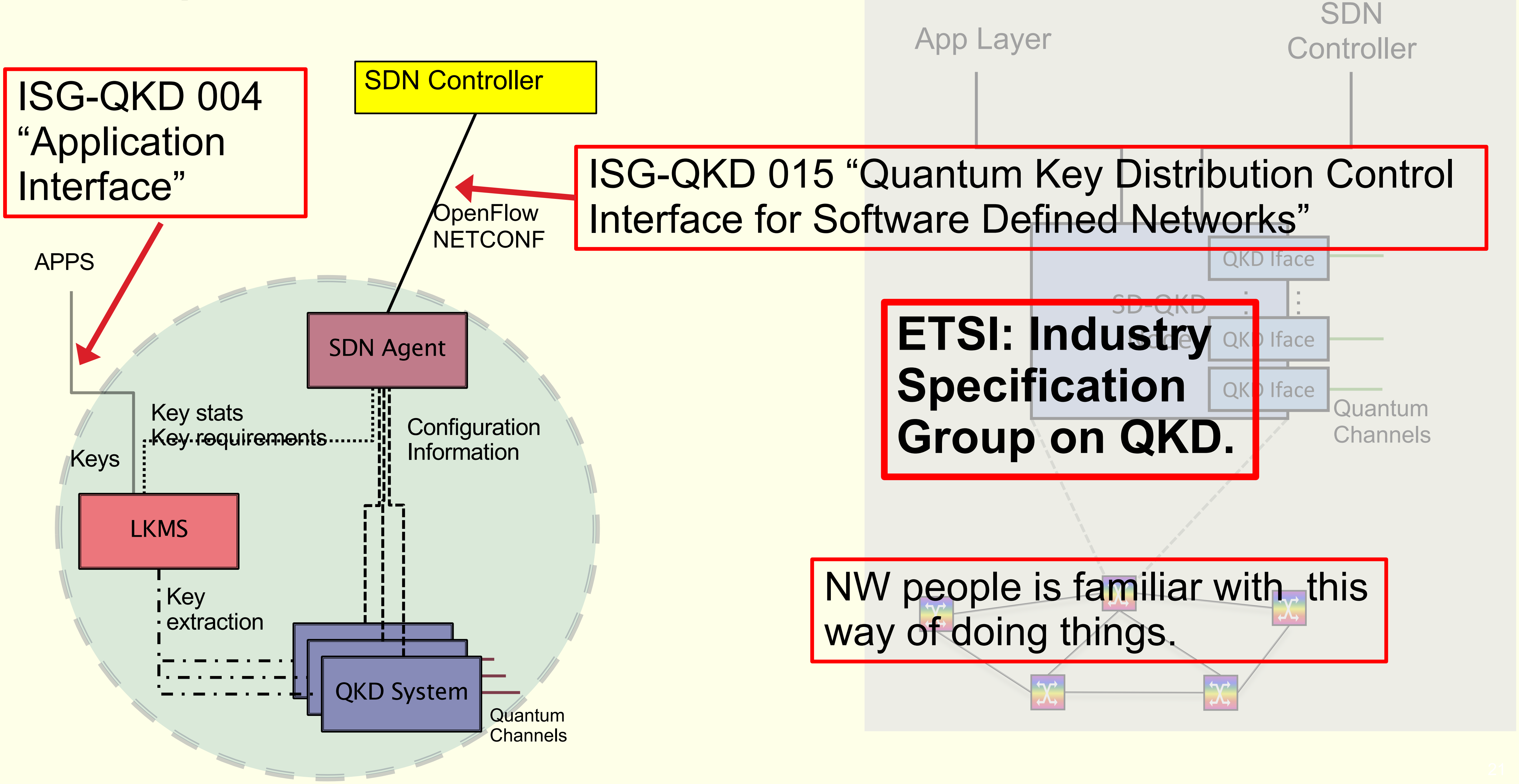


Key structure: SD-QKD-Node Abstraction





Key structure: SD-QKD-Node Abstraction

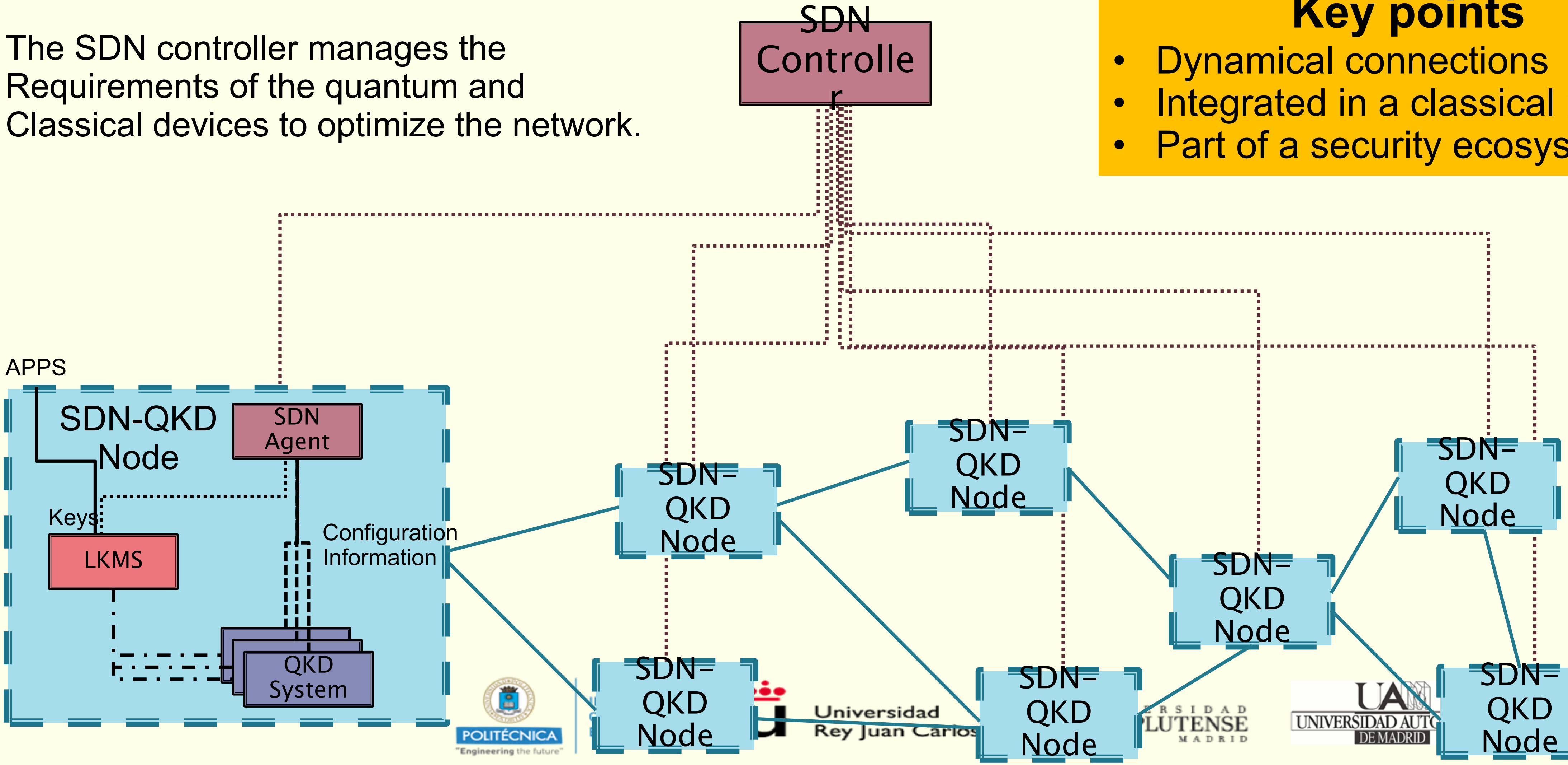


Global view of the SDQKD Network

The SDN controller manages the Requirements of the quantum and Classical devices to optimize the network.

Key points

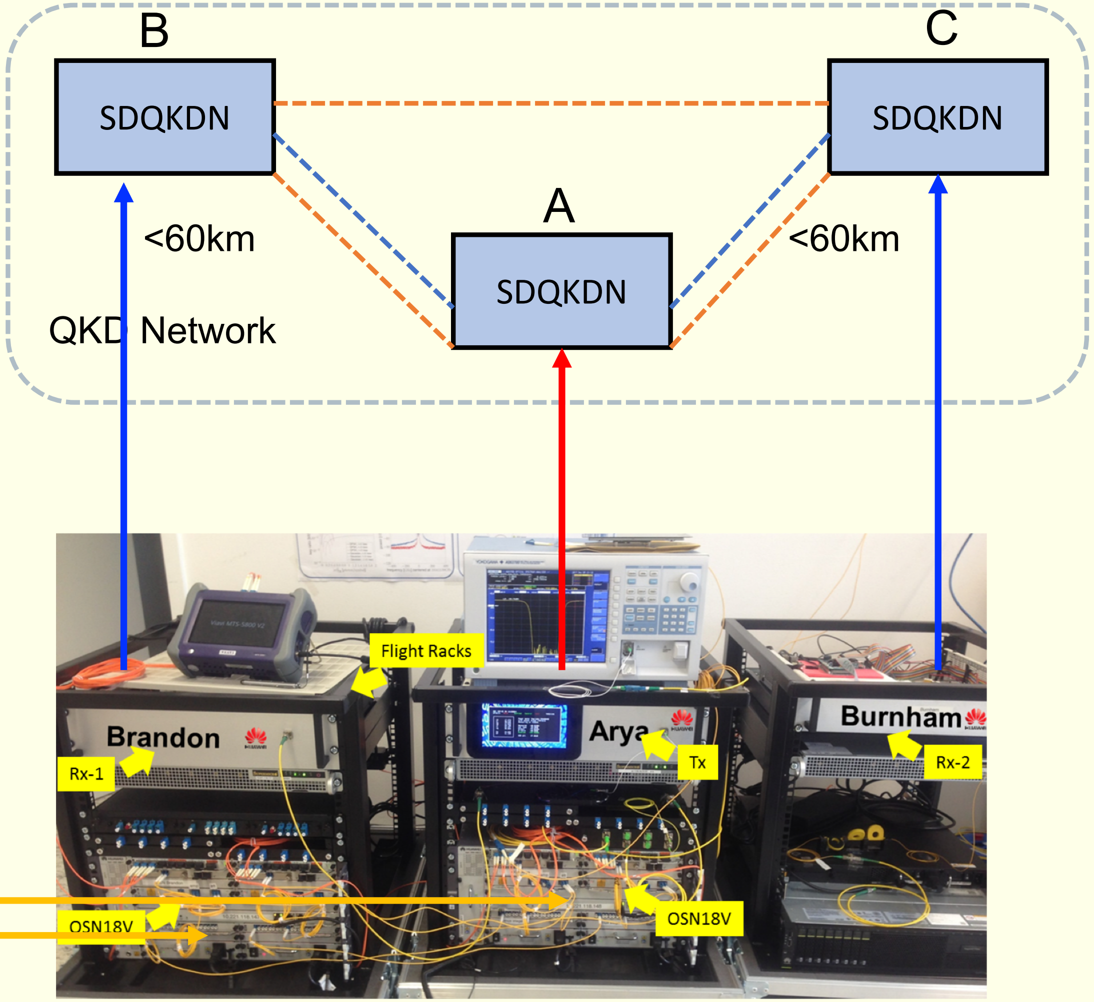
- Dynamical connections
- Integrated in a classical network
- Part of a security ecosystem



Madrid SDN QKD Network

- These **ideas have been implemented** connecting **three production sites** of Telefónica Spain in Downtown Madrid.
- **SDN controller:** Manages the network. Quantum systems in A can be connected with B or C according to the controller's policies.
- **CV systems** (telco-friendly)
- The **connection** with the rest is completely **standard.**

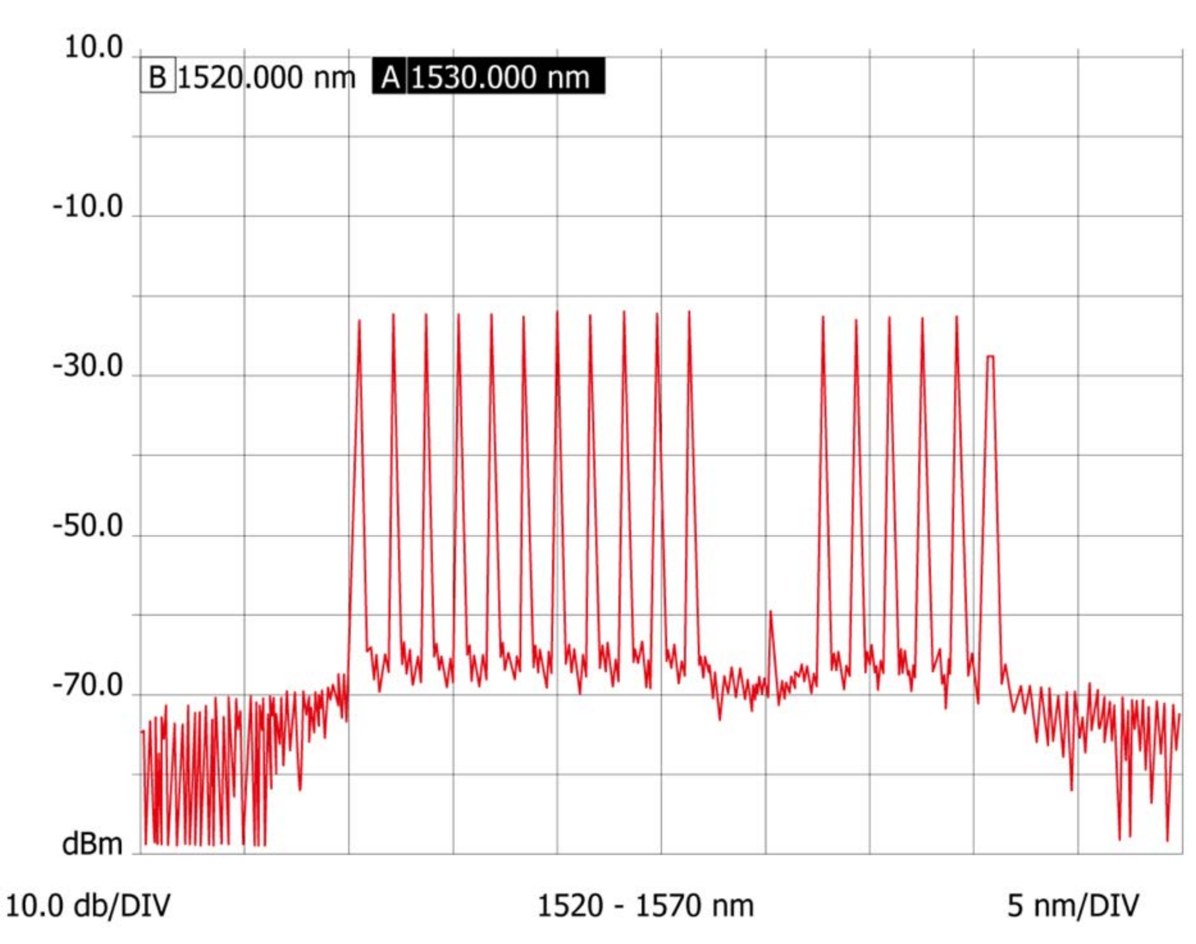
The connection to the network is through standard Communications systems. (Huawei OSN 1800)



CV QKD Systems: Huawei Technologies Dusseldorf

Quantum – Classical coexistence

- Currently up to **17 copropagating classical channels** with the quantum channel.
  - Classical channels in the **same band** (C-band ITU grid)
- Limited only because of the number of free ports in the OSN.
- 100 Gbps x 17 = 1.7 Tbps classical.
- Quantum 20-70 kbps max. (dependent on the link and key distillation)



3. Madrid SDN QKD Network

First Quantum SDN Network in the world.

Installed in Telefónica Spain **production facilities.**

“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

3. Madrid SDN QKD Network

Relevance:

- Integration in real world networks.
  - Logical & physical level.
- Deployment.
- Scalability.
- Relevant industrial cases.

First Quantum ...N Network in the ...d.

...alled in Telefónica ...in **production** ...**ilities**.

“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

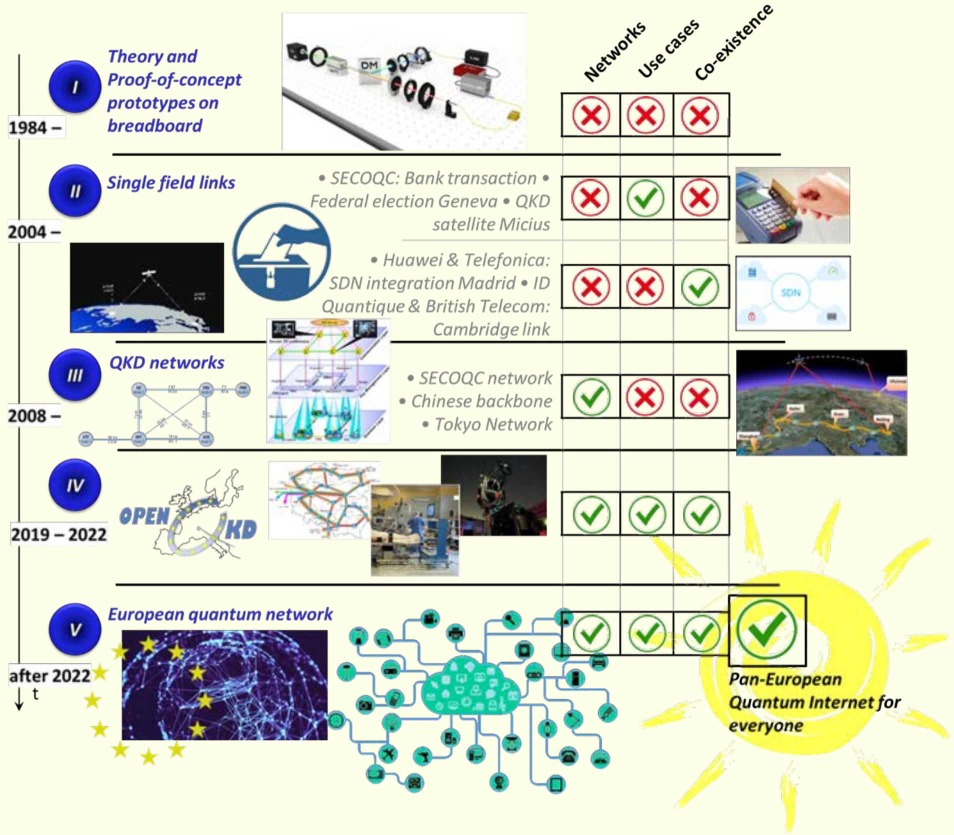
Evolution: European Testbeds. The OpenQKD project

- European Open QKD Network
- Testbeds to **demonstrate** the feasibility and **maturity of Quantum Communications technologies.**

QKD enabled ICT security

Quantum Key Distribution

- a technology offering security in the quantum age
- so far only isolated demos on technological level
- slow take up and low visibility due to lack of understanding and risk-aversion



Need an integrated approach to

- ✓ Raise awareness of QKD in security applications
- ✓ Demonstrate seamless integration into current networks and security architectures
- ✓ Show the benefit of QKD for a wide range of real world use-cases
- ✓ Involve whole supply chain from manufacturers to end-users
- ✓ Set standards for large scale deployment opportunities

Realised in OPENQKD

OPENQKD eco system

38 Partners, 15 M€ (funding)
18 M€ (cost)

- QKD suppliers
- QKD R&D partners
- QKD network developers
- Suppliers of network encryption
- Fiber infrastructure operators
- Telecom operators
- Aerospace and satellite industry
- Standardisation institutes
- Early adopters

Objectives: Use cases

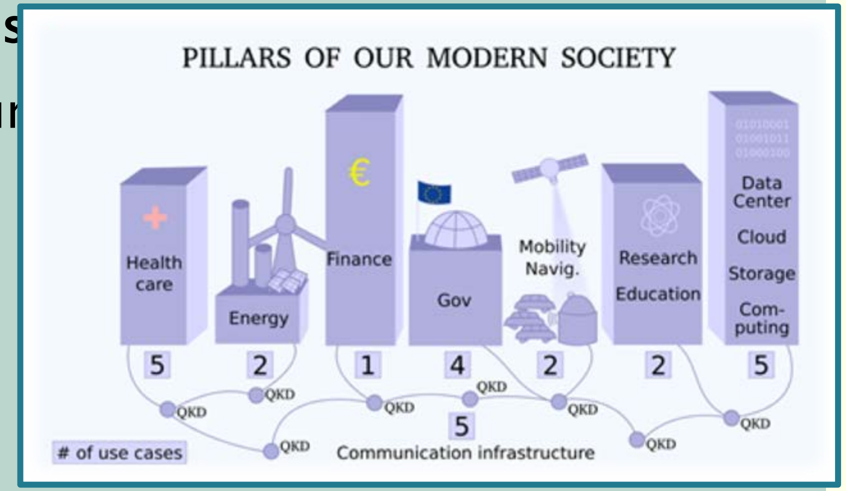
4

Operation of use-cases deriving from Secure Societies needs

- ❑ Demonstration of more than 30 use-cases for QKD featur
  - realistic operating environments
  - end-user applications and support

Range of use-cases:

- ❑ Secure and digital societies
  - Inter/Intra datacenter comm., e-Government, High-Performance computing, financial services, authentication and space applications, integration with post-quantum cryptography
- ❑ Healthcare
  - Secure cloud storage services and securing patient data in transit
- ❑ Critical infrastructure
  - QKD for telecom networks, 5G infrastructure and securing smart grids

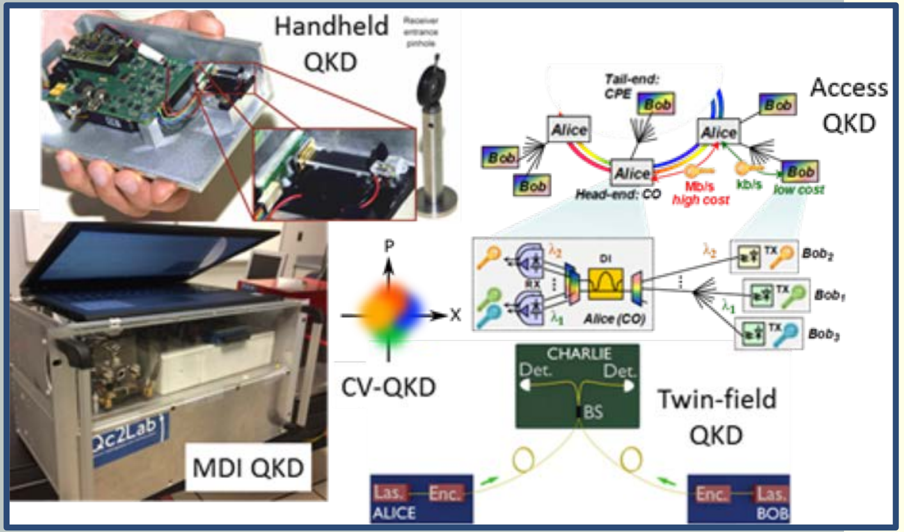


Objectives: Competitive EU industry

7

Kick-start a competitive European QKD industry

- ❑ Industry standard QKD devices (high maturity); 23 devices operational in OPENQKD
- ❑ Next generation QKD systems based on new protocols and novel implementations:
  - Long distance QKD
  - MDI QKD
  - Twin Field QKD
  - Low cost CV-QKD
  - Hand-held QKD
  - Access QKD



- ❑ Adaptation of network encryption devices for QKD operation; 30 encryptors in OPENQKD
- ❑ End-user workshops to raise awareness of security industry
- ❑ Staff training to foster know-how on QKD deployment and operation at test sites

Evolution: European Testbeds. The OpenQKD project

- **Open calls** scheme to bring-in externally defined use cases. (1M€)
  - Continuous call (evaluated 4 times during the lifetime of the Project)

Objectives: Pan-European Quantum Network

6

Lay the foundations for a Pan-European Quantum Network

- 4 large testbed sites and 12 demonstrator sites in 12 European countries
- Long distance cross-border links
- Testbed for free space QKD
- Test GEANT fiber infrastructure for a future large sc quantum communication network
- Study of satellite QKD and development of interfaces to terrestrial QKD networks

16 OPENQKD test sites

Large geographic reach-out

Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

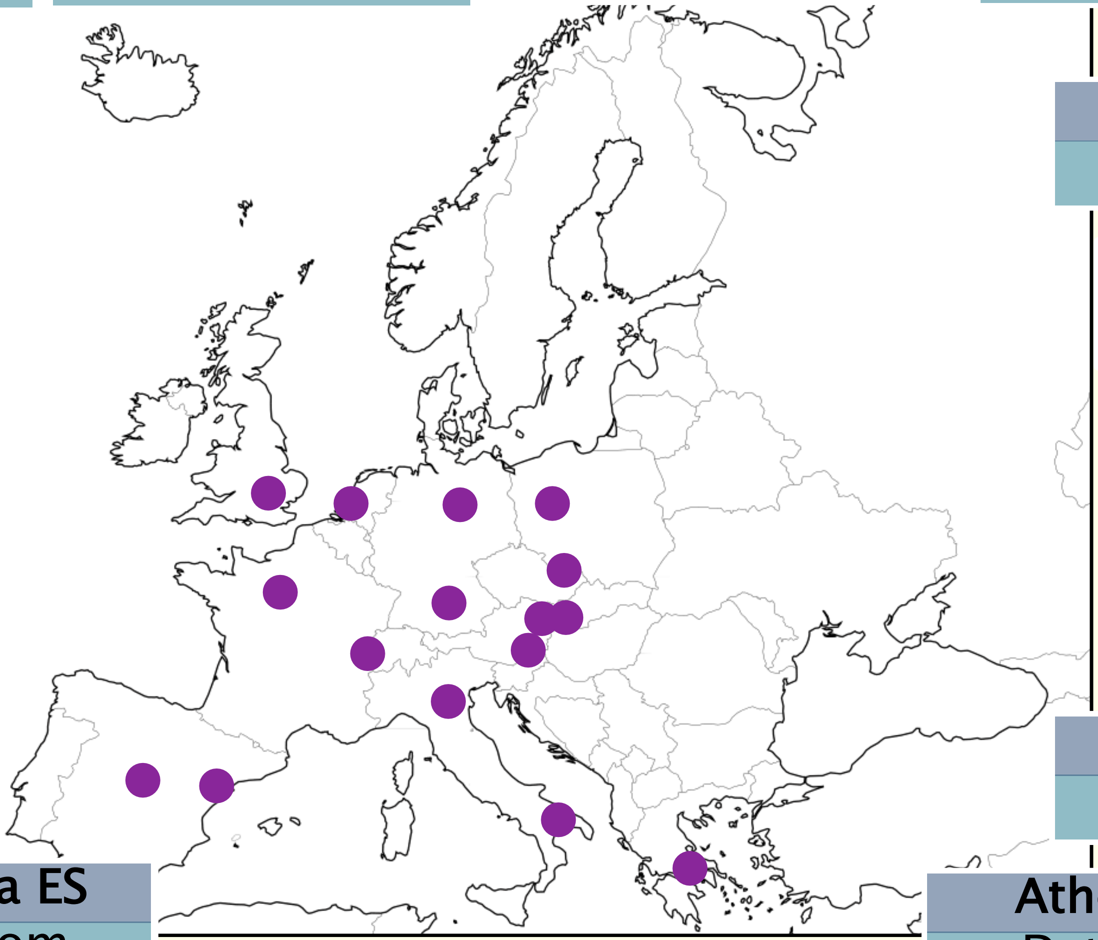
Cambridge UK
Data Centers

Paris FR
Academic network

Geneva CH
Smart Grid

Oberpfaffenhofen DE
Satellite QKD

Barcelona ES
Video Com



Bratislava CZ
Government

Ostrava CZ
High Perf. Comp.

Graz AT
Healthcare

Padua IT
Free-space QKD

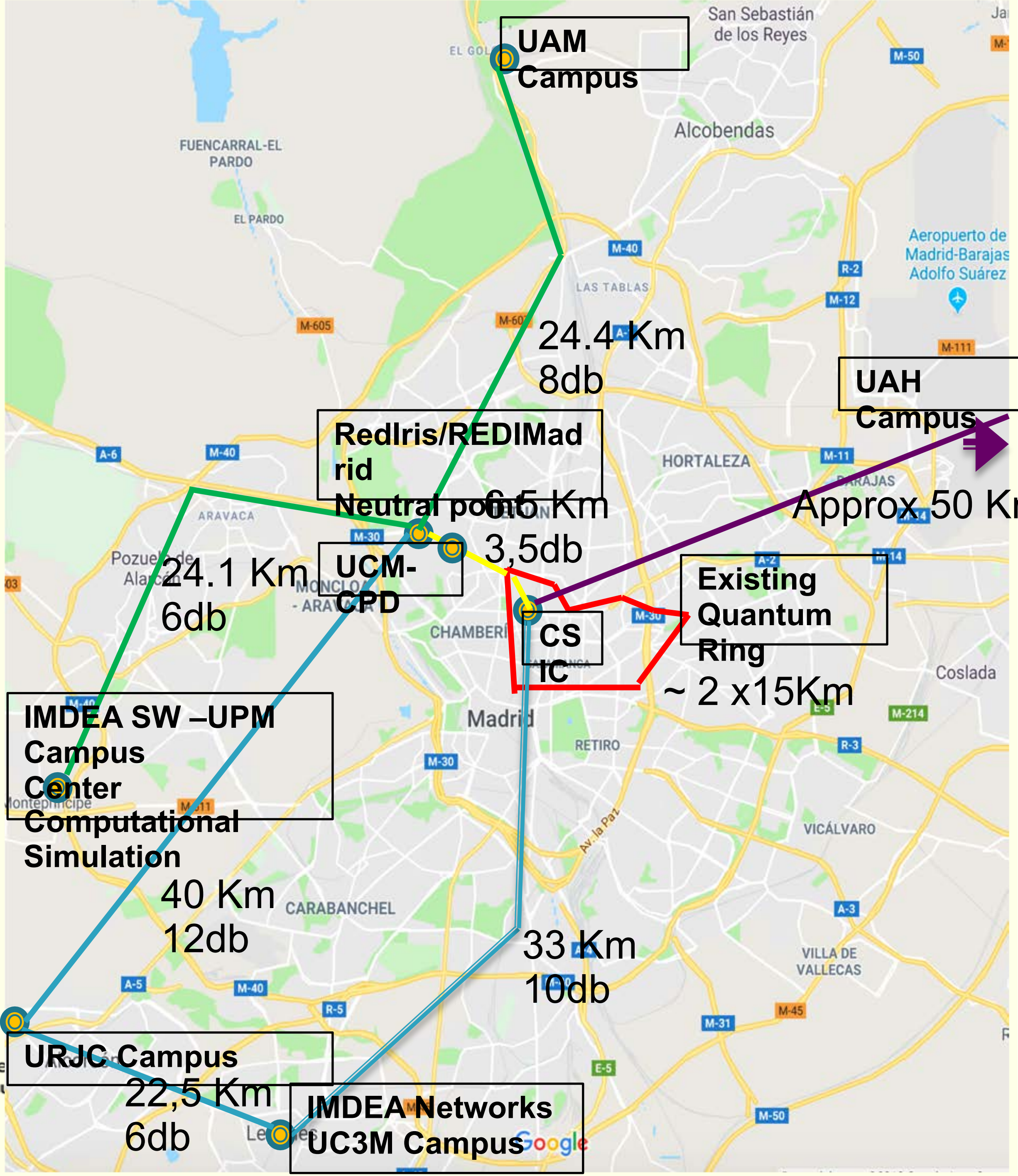
Matera IT
Satellite QKD

Athens GR
Data Com

Center for Computational Simulation

Madrid Testbed

- Evolution of the **Madrid Quantum Network.**
- Partners: RedIMadrid, UPM, Telefónica.
- **8** predefined **use cases.**
- Key use cases: **SDN based** (but also traditional)
- Start: **2-4 links** installed in **November.**
- Up to **9 links for the largest demonstrations.**
- **Distances 3-50 Km**



POLITÉCNICA "Engineering the future"
INTERNATIONAL CAMPUS OF EXCELLENCE
Unive Rey J

Testbed Vienna I

Inner City link

Vienna

Test bed partners: AIT, OEAW, FRX

Node locations: 8 (AIT, 2 IXPs, 5 Federal Ministries)

QKD Links: 7 AIT-IXP2-IXP1, IXP1-end users (star)

Link encryptors: 2 layer-1, 5 layer-2

Distances: 3-10km;

SDQN: optical switching of QKD terminals at IXP1

Coexistence: 2 dark fibers, **5** lit fibers

Use case demos: Secure distribution and cloud storage of government data

Start: Month 12

Duration: 12 months (incl. cross border)

Testbed Vienna II

Cross-Border link

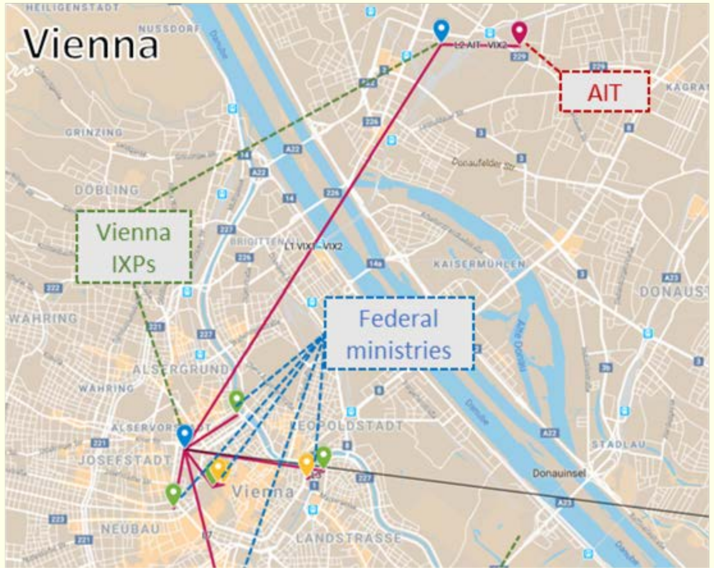
Vienna – Bratislava

Test bed partners: AIT, OEAW

Links: Distance 70 km; 1-2 links (dark fiber) from Vienna (IXP1) to Bratislava, 1 inner city link in Bratislava to Austrian diplomatic mission

Start: Month 18

Duration: 4 months



TRI-STAR link (extension to OPENQKD)

Vienna – Bratislava – Graz

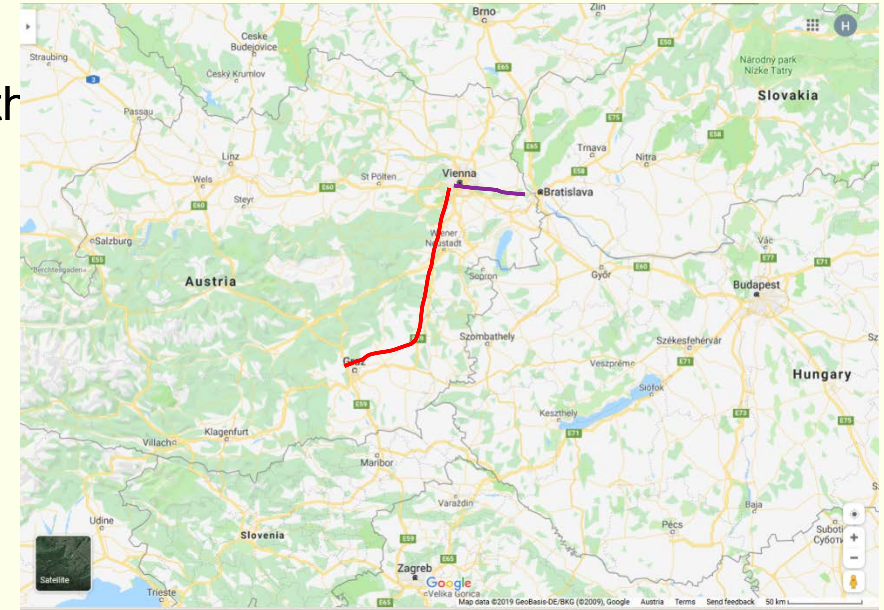
Test bed partners: **AIT, OEAW, CYC,** ASFINAG (ex)

Case study for QCI network structures

Links: 2-3 links for Vienna-Graz, 2 extra links to connect inner city locations to fibers along motorway

Start: Month 24

Duration: 4 month



Future: European Quantum Communication Infrastructure

- **Ten years plan** to "make available a quantum communication infrastructure in Europe, to **boost European capabilities in quantum technologies, cybersecurity and industrial competitiveness.**
- Agreement recently **signed** by 9 member states (Sept. 2019)
- **OpenQKD** Project is considered the **ramp-up phase** of the **QCI**

Source: TU Delft/Scixel

EU H2020 Grant 820466

EU H2020 Grant 857156

Comunidad de Madrid
S2018/TCS-4342

CvQuCo - MINECO/FEDER TEC2015-70406-R

A. Aguado[1], P. Salas[1],
A.L. Sanz[1], J.P. Brito[1],
R. Brito[1], R. Vicente[1],
D. R. Lopez[2], V. Lopez[2],
A. Pastor[2], V. Martin[1]

Thanks!...
Questions/comments?

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

[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*