

Quantum Networks in Practice: The MadQCI Ecosystem

Javier Faba
javier.faba@upm.es

Table of contents

1. QKD in theory
2. QKD in practice
3. Quantum Networks
4. PQC and hybridization
5. Applications: use cases and more
 1. Hybrid IPsec tunnels
 2. Lawful interception
 3. Q-DS
 4. Coherent-One-Way Oblivious Transfer
 5. MadQCI towards Quantum Entanglement Distribution Networks
 6. Future use case for Quantum Entanglement Distribution Networks: RL+ES
 7. Other use cases
6. Acknowledgements



QKD in theory

QKD in theory

Quantum Cryptography.

In principle: **any means to do cryptography based on** the processing and transmission of **quantum signals**.

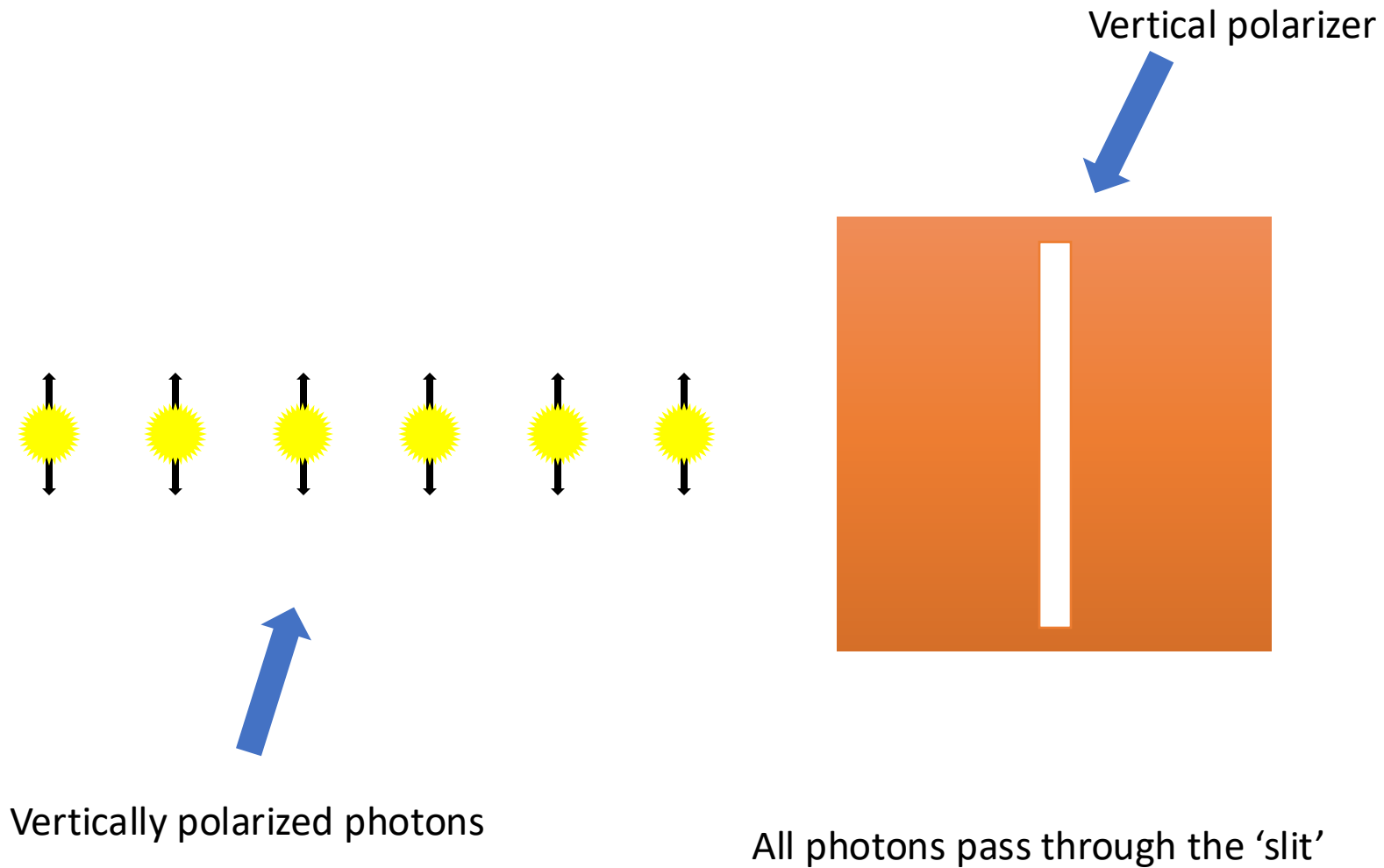
Usually **equated to Quantum Key Distribution (QKD)**.

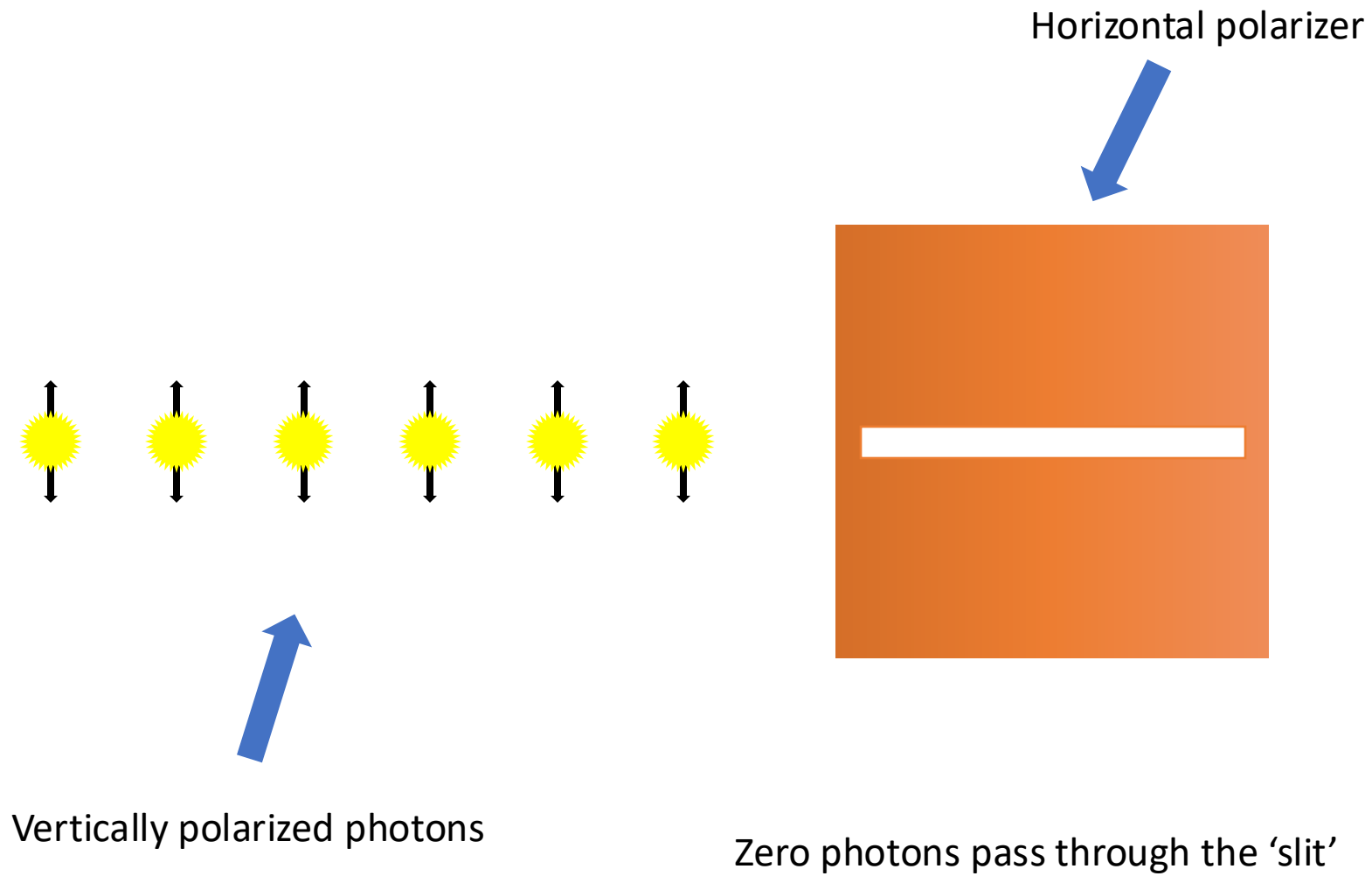
But there are **other algorithms**: oblivious transfer, secret sharing...

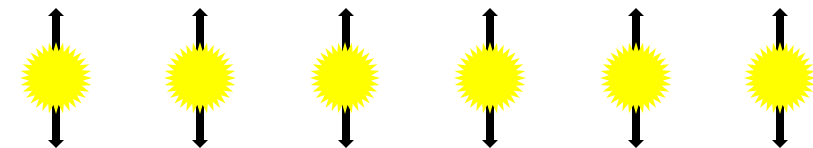
Important: they do not necessarily share the same security properties.

The typical QKD protocol: the BB84.

Actually a QKD protocol does not distribute keys: they are created during the protocol, which needs a first authentication key for the first round: It is **more accurate to think of it as Quantum Key Growing**.







Vertically polarized photons



Diagonal polarizer



Some photons pass through the 'slit'

The resulting photons have the polarization of the polarizer!

More on Measurement

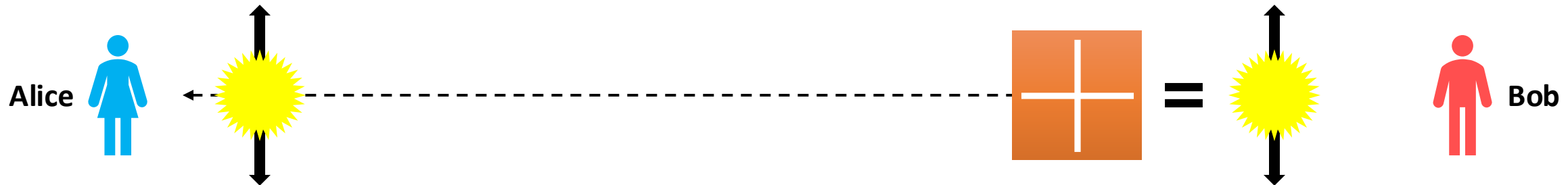
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$$

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

Actually what we are doing is to use two orthogonal basis: If we encode in one and measure in the other, there is a 50% chance of make a mistake



1

Alice chooses one of the four possible photons

2

The photon is sent

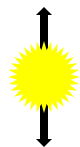
3

Bob measures in a basis

Sent bit

1

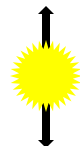
Sent photon



Basis used

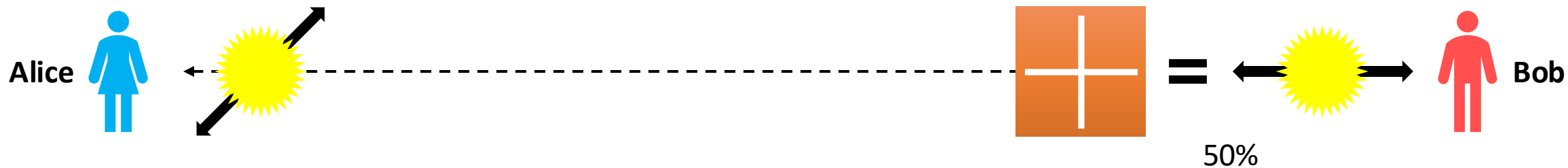


Received photon



Received bit

1



1

Alice chooses one of the four possible photons

2

The photon is sent

3

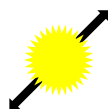
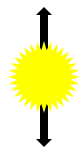
Bob measures in a basis

Sent bit

1

1

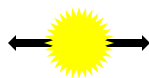
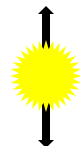
Sent photon



Basis used



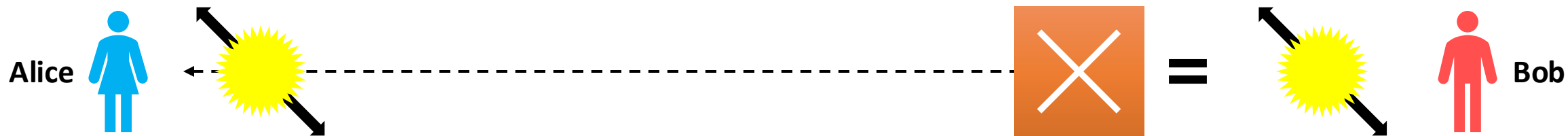
Received photon



Received bit

1

0



1

Alice chooses one of the four possible photons

2

The photon is sent

3

Bob measures in a basis

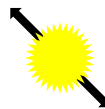
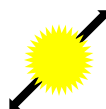
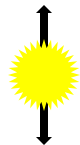
Sent bit

1

1

0

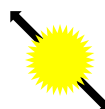
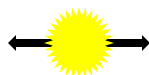
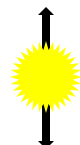
Sent photon



Basis used



Received photon

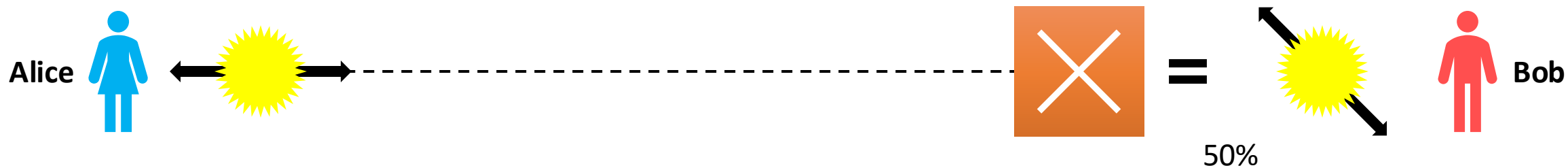


Received bit

1

0

0



1

Alice chooses one of the four possible photons

2

The photon is sent

3

Bob measures in a basis

Sent bit

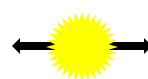
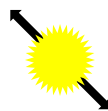
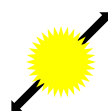
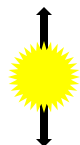
1

1

0

0

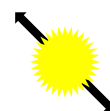
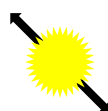
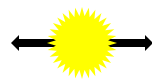
Sent photon



Basis used



Received photon



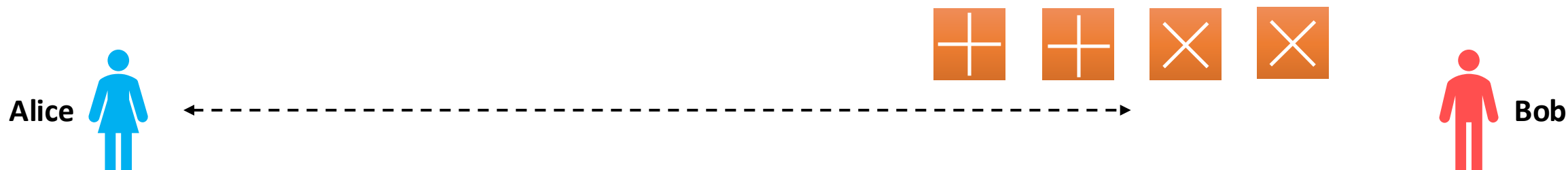
Received bit

1

0

0

0



1

Bob tells Bob which basis he used

Sent bit

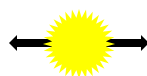
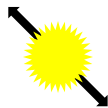
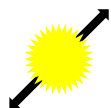
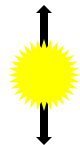
1

1

0

0

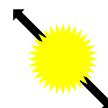
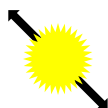
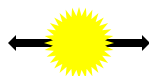
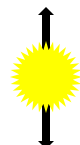
Sent photon



Basis used



Received photon



Received bit

1

0

0

0



1

Bob tells Bob which basis he used

2

Alice checks which ones coincide

Sent bit

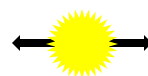
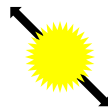
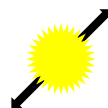
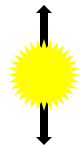
1

1

0

0

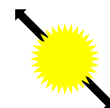
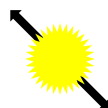
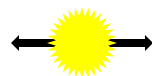
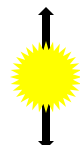
Sent photon



Basis used



Received photon



Received bit

1

0

0

0



1

Bob tells Bob which basis he used

2

Alice checks which ones coincide

3

Both discard the 'bad' photons

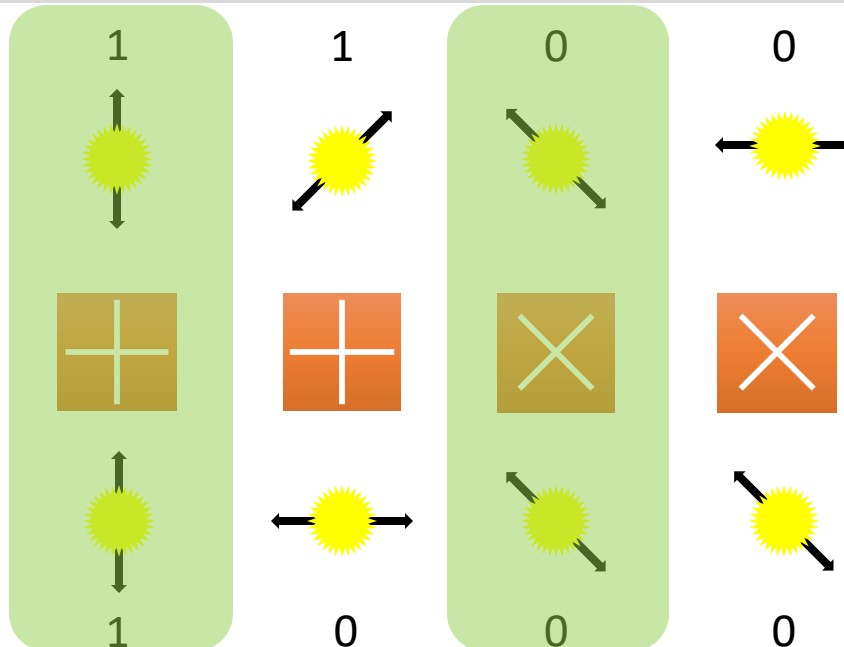
Sent bit

Sent photon

Basis used

Received photon

Received bit





1

Bob tells Bob which basis he used

2

Alice checks which ones coincide

3

Both discard the 'bad' photons

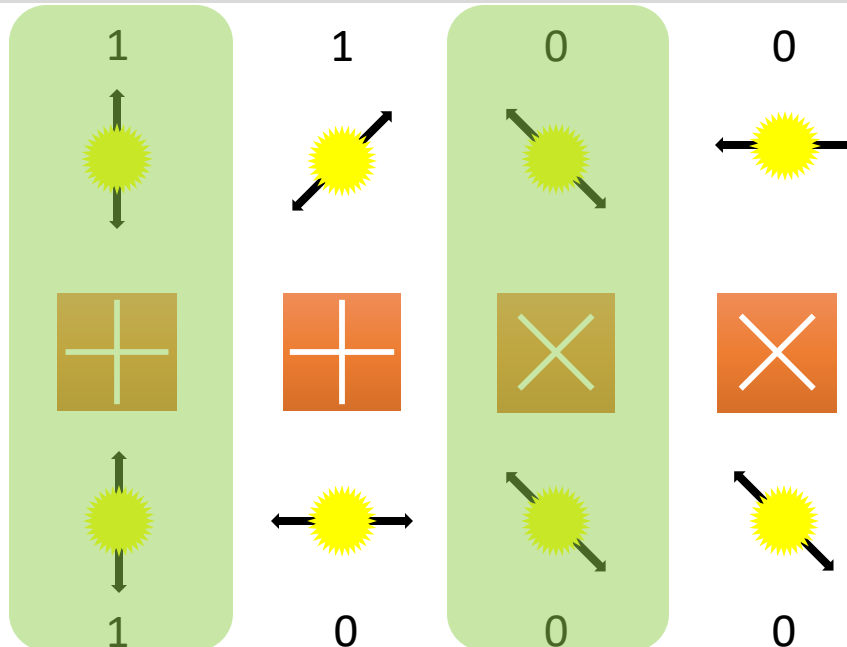
Sent bit

Sent photon

Basis used

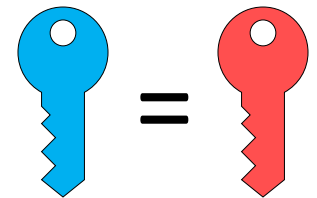
Received photon

Received bit



Alice's
key: 10

Bob's
key: 10

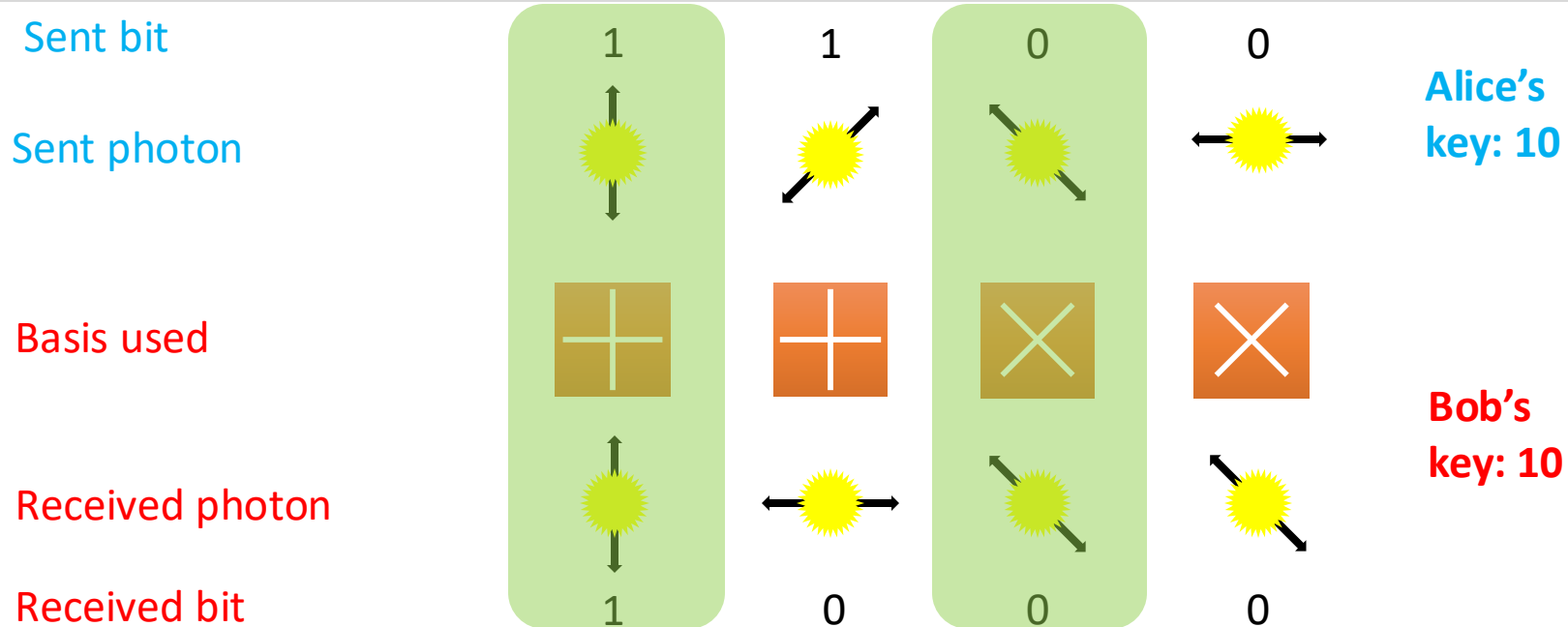




Symmetric key



If there are 'good' photons with different polarization: there is an Eve!

- 1 **Bob** tells Bob which basis he used
- 2 **Alice** checks which ones coincide
- 3 **Both** discard the 'bad' photons



 = 

Symmetric key

QKD in theory

QKD: BB84

QUANTUM TRANSMISSION															
Alice's random bits.....	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases.....	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends.....	↗	↑	↘	↔	↑	↑	↔	↔	↘	↗	↑	↘	↗	↗	↑
Random receiving bases.....	R	D	D	R	R	D	D	R	D	R	D	D	↘	↗	↑
Bits as received by Bob.....	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits.....	R				R	D	D	R		R	D	D		D	R
Alice says which bases were correct.....		D			R	D	D	R		R	D	D		D	R
Presumably shared information (if no eavesdrop)...		OK			OK			OK				OK		OK	OK
Bob reveals some key bits at random.....		1			1			0				1		0	1
Alice confirms them.....					1									0	
OUTCOME															
Remaining shared secret bits.....		1						0				1			1

Bennet, Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing“
International Conference on Computers, Systems and Signal Processing. Bangalore, 1984

QKD in theory

ALICE
Emitter

QUANTUM TRANSMISSION

Alice's random bits.....	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases.....	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends.....	↗	↑	↘	↔	↑	↑	↔	↔	↘	↗	↑	↘	↗	↗	↑
Random receiving bases.....	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob.....	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits.....	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct.....			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)...		1		1			0			1			0		1
Bob reveals some key bits at random.....				1									0		
Alice confirms them.....				OK									OK		
OUTCOME															
Remaining shared secret bits.....		1					0				1				1

QKD in theory

BOB
receiver

QUANTUM TRANSMISSION															
Alice's random bits.....	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases.....	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends.....	↗	↑	↘	↔	↑	↑	↔	↔	↘	↗	↑	↘	↗	↗	↑
Random receiving bases.....	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob.....	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits.....	R				R	D	D	R		R	D	D		D	R
Alice says which bases were correct.....		D				OK						OK			
Presumably shared information (if no eavesdrop)...		1				1		0			1			0	1
Bob reveals some key bits at random.....					1									0	
Alice confirms them.....					OK									OK	
OUTCOME															
Remaining shared secret bits.....		1						0			1				1

QKD in theory

CLASSICAL

QUANTUM TRANSMISSION															
Alice's random bits.....	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases.....	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends.....	↗	↑	↘	↔	↑	↑	↔	↔	↘	↗	↑	↘	↗	↗	↑
Random receiving bases.....	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob.....	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits.....	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct.....			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)...			1		1			0				1		0	1
Bob reveals some key bits at random.....					1									0	
Alice confirms them.....					OK									OK	
OUTCOME															
Remaining shared secret bits.....		1						0			1				1

Error correction

QKD in theory

- **After qubit detection** at Bob, what we have is a **raw key** that needs to be **processed to obtain the final secret key** :
 - Sifting
 - Error correction
 - Privacy amplification
 - Authentication

In the **theoretical world**, it is enough with sifting and error estimation (we don't need to correct errors since one single error is related with the existence of Eve).

However, in the real world, errors come from **Eve AND the environment**... so we have to perform additional postprocessing.

QKD in theory

- **Raw key extraction and sifting:** Using the public channel the emitter publishes the basis in which the qubits were prepared. The receiver acknowledges those in which the measurement was done in the same basis.
- **Raw key will differ between emitter and receiver**, since there will be errors introduced by the spy (and by noise)
- To start the error correction an error estimate is obtained.
- Raw key is also cleaned from artifacts (e.g. double detections...)
- Note the **use of the public channel** (also in the following steps): any revealed information has to be removed from the final key and the communications must be authentic.

QKD in theory

- **Error correction:** The Alice's sifted key will be different from Bob's, either because of noise or a spy.
 - Example: (Cascade) Reveals the parities of blocks of key to recursively locate the errors.
 - **Better codes: LDPC** (Low-density parity-check codes)
 - The number of errors corrected are used to estimate the **Quantum Bit Error Rate**, this is a fundamental quantity guiding the error correcting process and the privacy amplification phase.

$$QBER = \frac{N_{errors}}{N_{errors} + N_{correct}}$$

QKD in theory

The **QBER** also gives the limits when a secret key can be extracted or not.

Typical parameters:

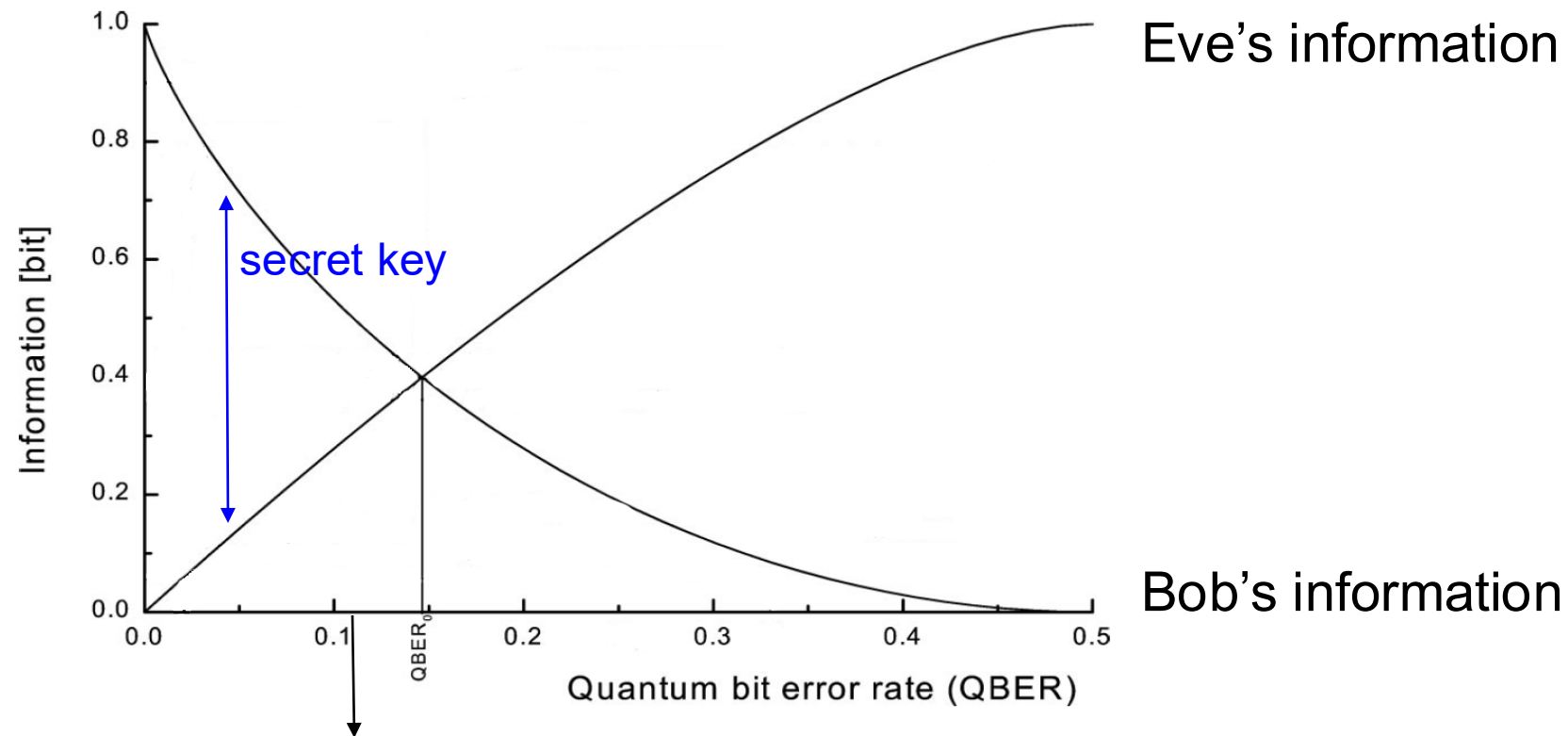
- A very good QBER $\sim 1\%$, with a 3-4% relatively high key rates are possible. Beyond 6-7% the secret key rate is drastically reduced, even although the theoretical limit is 11%
- This limit depends on protocol and assumptions on the spy (e.g. 15% if incoherent attacks)
- A special case is the one for continuous variables, which works with extremely high error rates. Error correction is very demanding in this case.

QKD in theory

- The error corrected key can **still have information known to the spy**. **Privacy amplification** tries to eliminate this mixing bits that are known to the spy (Eve) with others that are unknown. Examples:
 - If a spy knows the value of bit 15 but not the 16, then the spy knows nothing about the value of XOR(15,16)
 - If the spy knows the values of bits 15 and 16 with a 60% of probability , he will know XOR(15,16) with a probability $0.6^2 + 0.4^2 = 0.52$, which is less than the original.
- In practice this can be done using hash functions on blocks of the corrected key, which efficiently mix all the bits.
- Privacy amplification is possible if the mutual information between Alice and Bob is larger than the mutual information between Alice and the spy or Bob and the spy

QKD in theory

Incoherent eavesdropping strategy, BB84



11%, coherent eavesdropping limit

QKD in practice

Ingredients

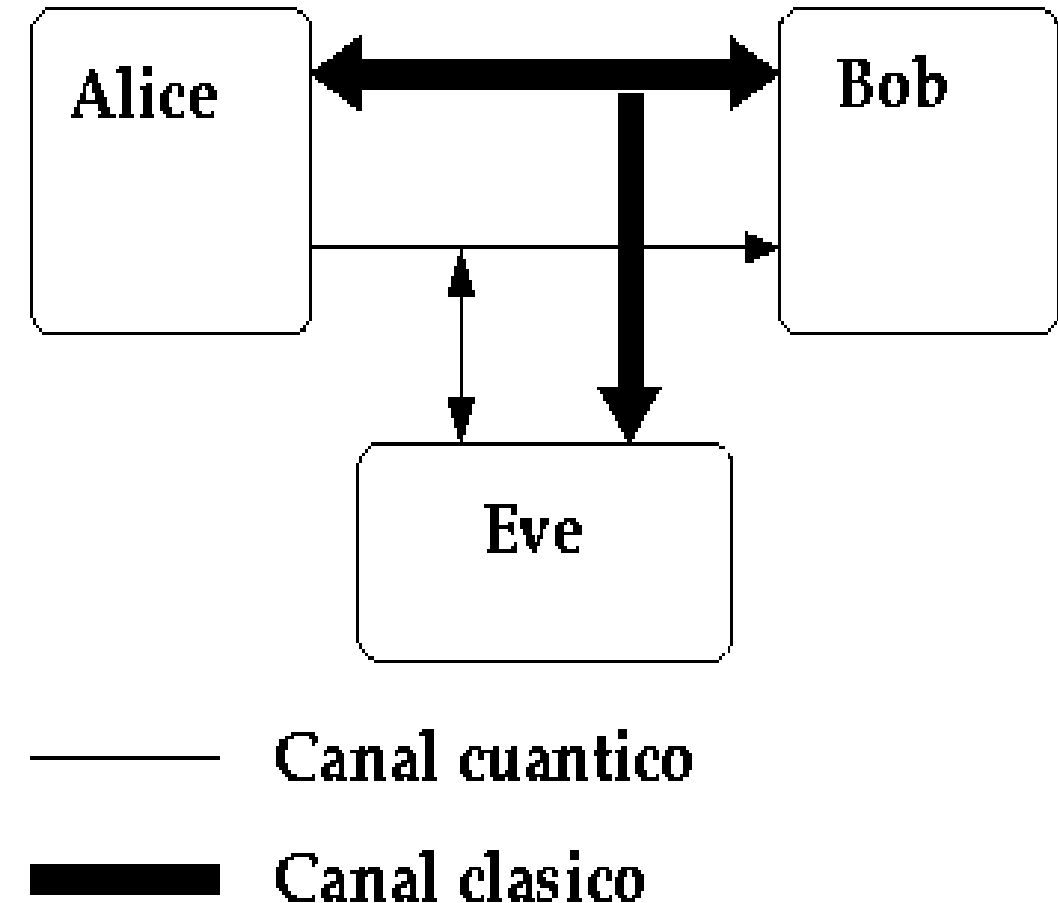
- 1) Quantum channel
- 2) Single quantum detectors
- 3) Single quantum emitters (incl. entangled pairs)
- 4) Quantum state preparation and analysis

QKD in practice

Quantum communications and networks, why is it difficult?

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)

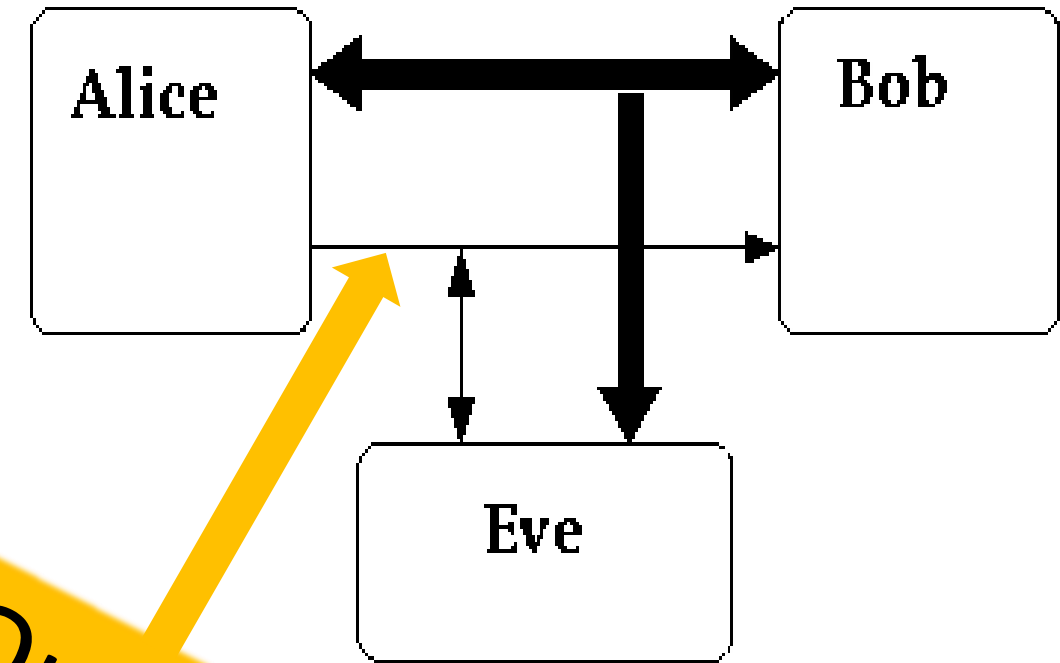


QKD in practice

Quantum communications and networks, why is it difficult?

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 transfer the qubits from Alice to Bob)
- A **classical channel** (public but **authentic**)
- ... and the spy (Eve)

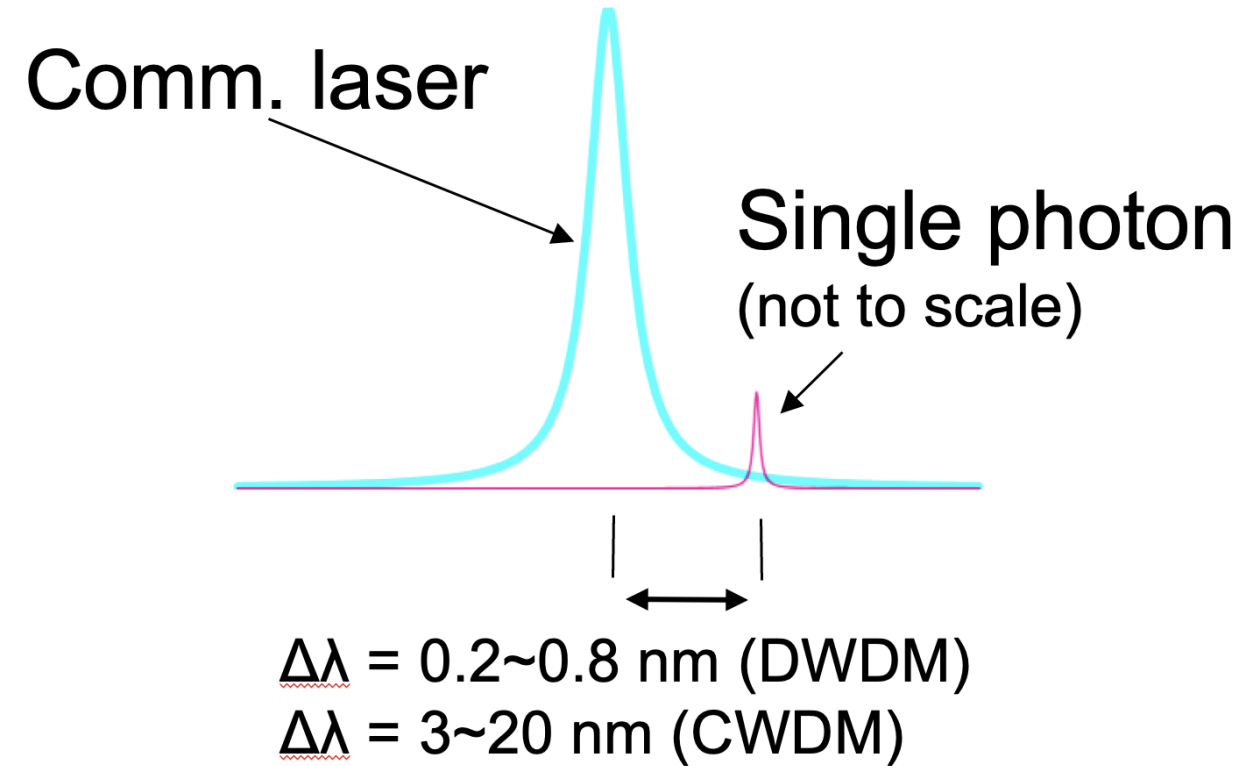


— Canal cuántico
— Canal clásico

The Quantum channel

Extremely weak signals:

- A single pulse in classical communications $\sim 10^8$ photons
- Quantum communications: 1 photon



QKD in practice

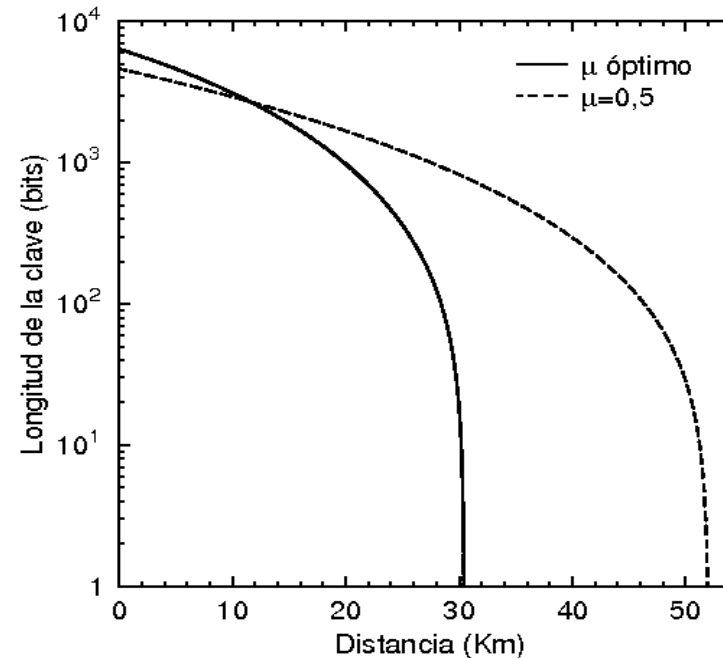
The quantum channel

1- Signals are always absorbed.

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

2- 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	$5 \cdot 10^8$
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

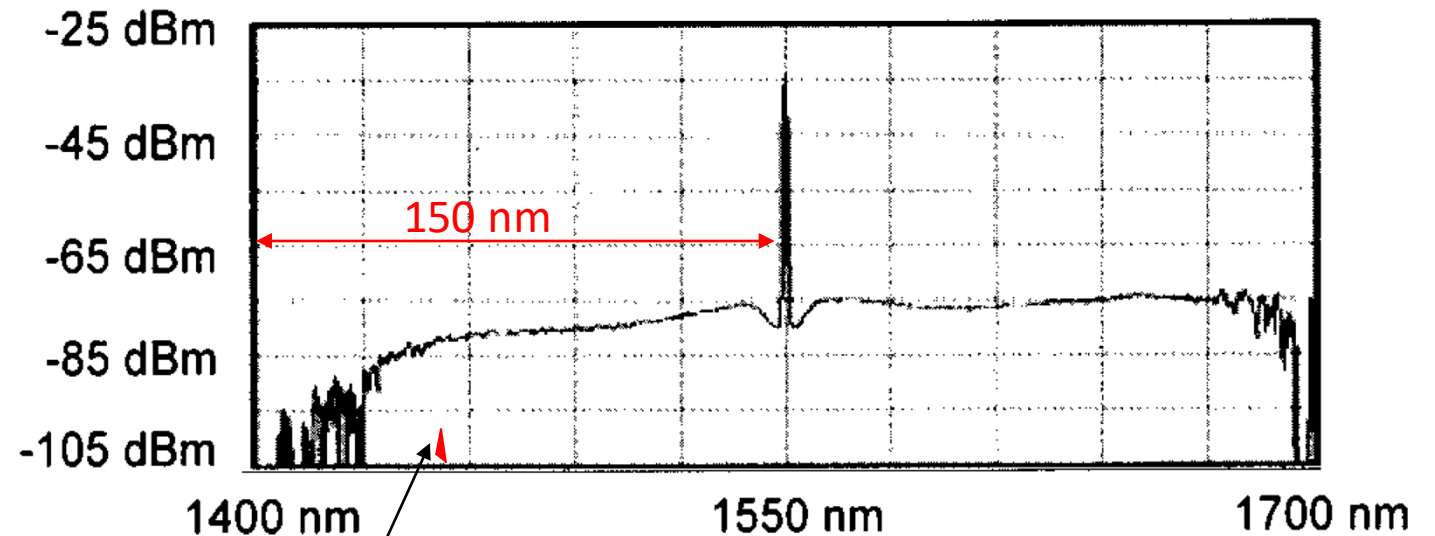
QKD in practice

The quantum channel

Optical infrastructure is expensive: What about sharing?

- Crosstalk is very difficult to avoid when your signal is a single quantum!
- Current trends in classical communications (physical layer): put as many channels as possible in a single fibre.
 - DWDM 25GHz channel spacing: 0.2 nm

Noise in the fibre: Raman



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

Single
Photon
(approx. scale)

QKD in practice

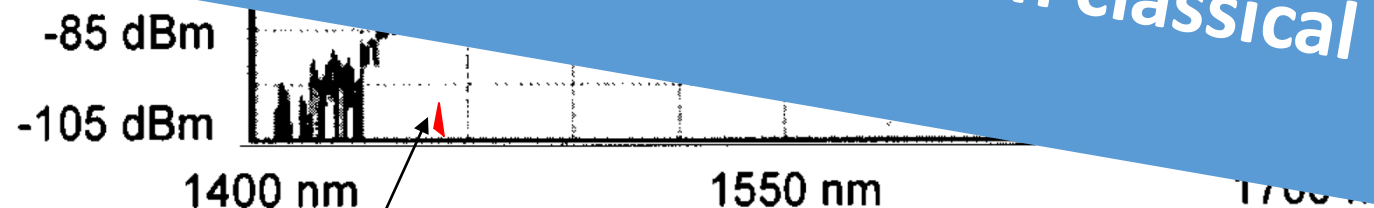
The quantum channel

Optical infrastructure is expensive: What about sharing?

- Crosstalk is very difficult to avoid when your signal is a single quantum!
- Current trends in classical communications (physical layer): put as many channels as possible in a single fibre.
 - DWDM 25GHz channel spacing: 0.2 nm

Noise in the fibre: Raman

Why don't you move to other wavelengths, so you don't have crosstalk with classical signals?



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

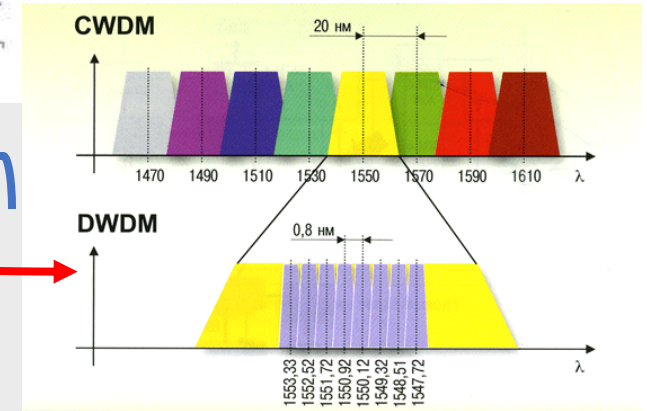
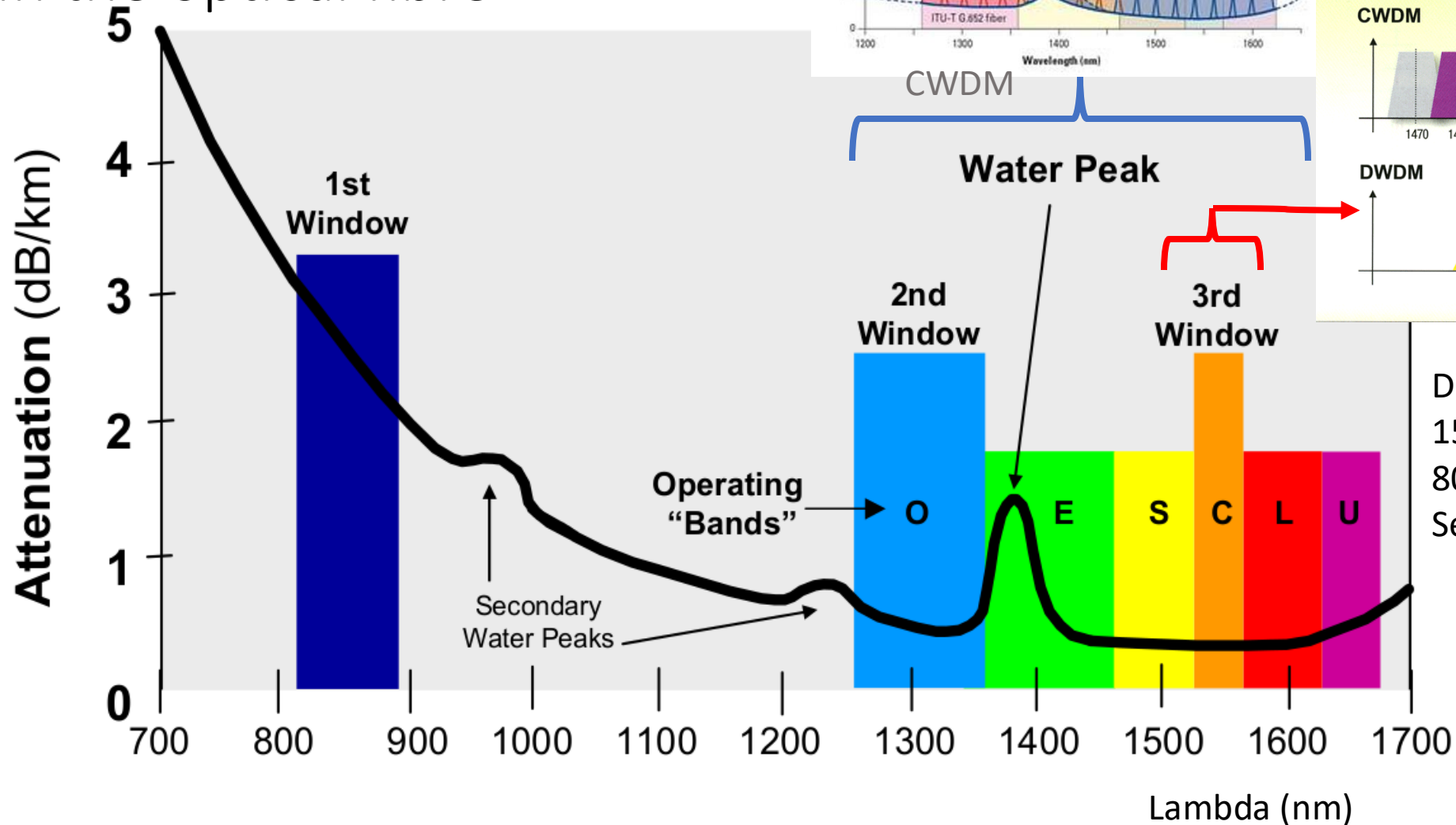
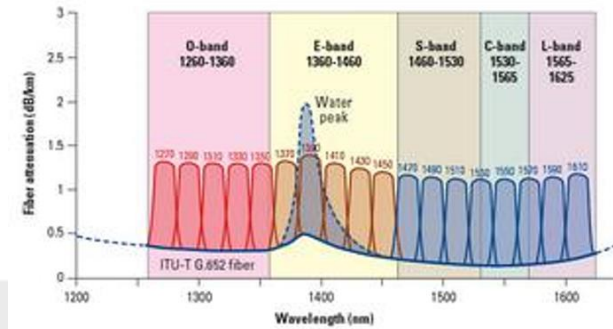
Single
Photon
(approx. scale)

QKD in practice

Life in the optical fibre

CWDM
18 channels
1270-1610 nm
Sep: 20 nm

CWDM wavelength grid as specified by ITU-T G.694.2



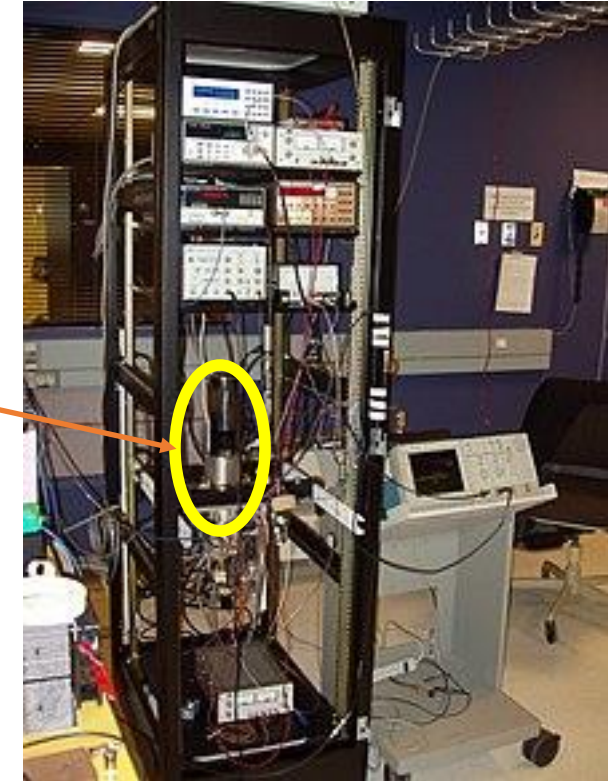
DWDM
1528.77-1536.86 nm
80 channels (50GHz grid.
Sep: 0.4 nm)

QKD in practice

Detectors

Single photons are difficult to detect efficiently (improving!!)

- Superconducting detectors.
 - Low **dark count**, high speed but bulky & low temperature (few K).
- Solid state: not so efficient, **afterpulses**, still bulky and moderate low T (70-200 K) for better performance.
- Homodyne: convenient, compact and telco-friendly. CV only.



Source: Wikipedia

QKD in practice

.Single photons are difficult to produce.

- Only one at a time and on demand!
- Typical: use attenuated laser sources.
 - To produce **single photons on demand** (predictable rate) at the correct wavelength is difficult.
 - Typically: use an attenuated laser.
 - An attenuated laser pulse with an average photon number per pulse of μ , emits according to a Poisson distribution in the number of photons:

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$$

- The probability to emit more than one photon is $\mu/2$. The probability of a vacuum pulse is $1 - \mu$
- A typical value is $\mu = 0.1$

QKD in practice

.Single photons are difficult to produce.

- Only one at a time and on demand!
- Typical: use of laser sources.
 - To produce a single photon (predictable rate) at the correct wavelength.
 - Typically, a laser pulse is attenuated.
 - An attenuated laser pulse emits according to a Poisson distribution.

However, although we have a lot of problems, it is still possible to do QKD in practice...

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$$

- The probability to emit more than one photon is $\mu/2$. The probability of a vacuum pulse is $1 - \mu$
- A typical value is $\mu = 1$

QKD in practice



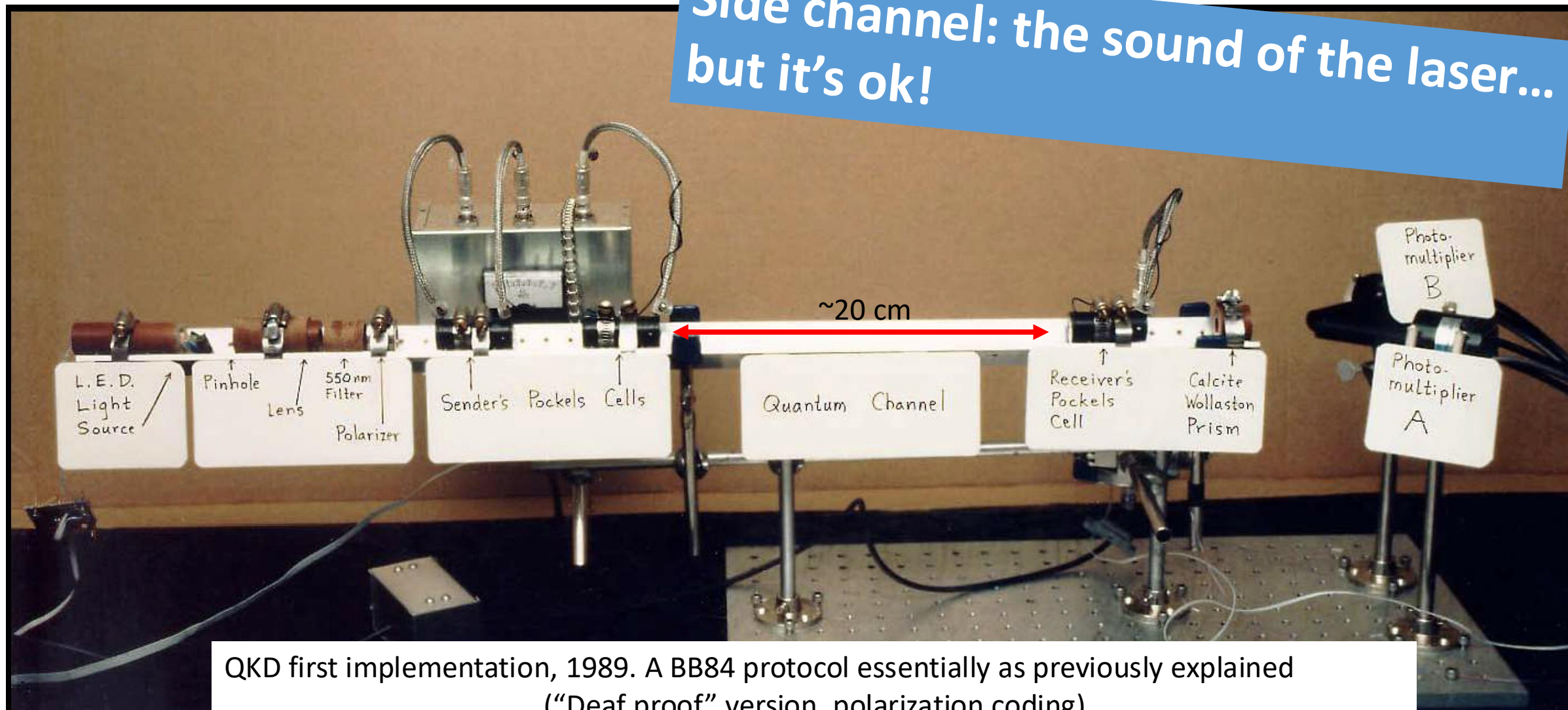
POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID



GCC

Side channel: the sound of the laser...
but it's ok!



QKD first implementation, 1989. A BB84 protocol essentially as previously explained
("Deaf proof" version, polarization coding)

QKD in practice



POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID

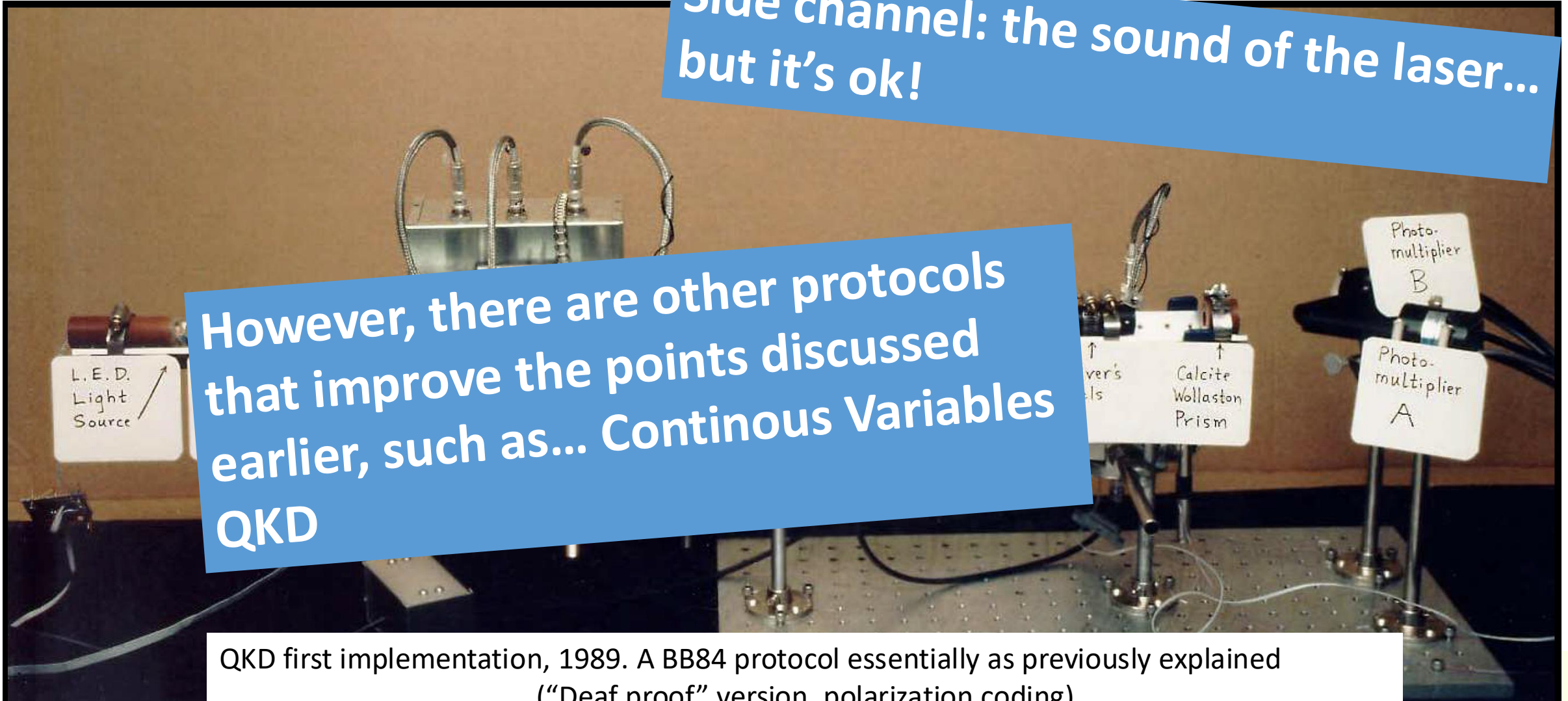


GCC

Side channel: the sound of the laser...
but it's ok!

However, there are other protocols
that improve the points discussed
earlier, such as... Continuous Variables
QKD

QKD first implementation, 1989. A BB84 protocol essentially as previously explained
("Deaf proof" version, polarization coding)



QKD in practice

- Building robust QKD systems is **complex** and require bulky Single Photon Detectors for which a large market does not exist, hence **expensive**. Moreover, the technology is notoriously “**telco unfriendly**” from an integration (e.g. Sharing the physical infrastructure) point of view.

Typical QKD system

- ~150K€
- Difficult to integrate

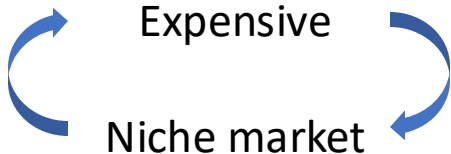


?



SFP module

- Finger sized
- Mass market
- Plug and play
- 50€

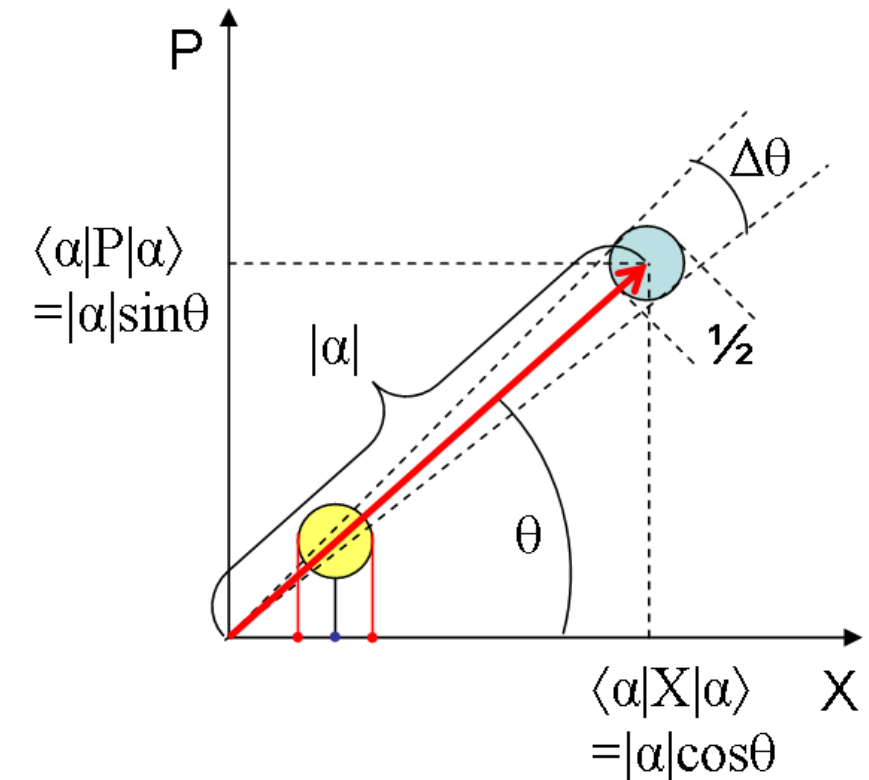


QKD in practice: CV

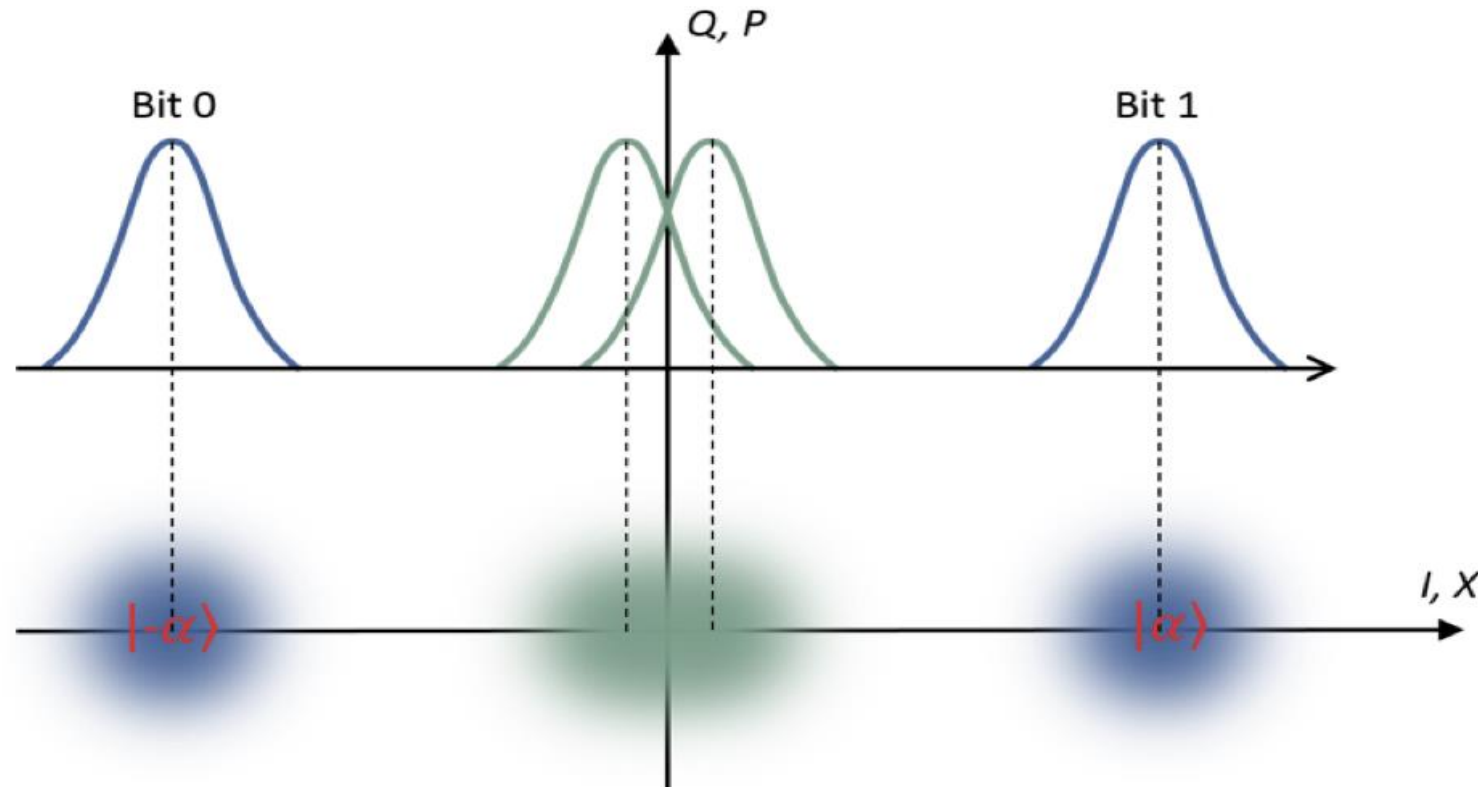
- **Coherent states.**
- The **quadratures of the electric field** of an electromagnetic wave are also subject to the **Heisenberg uncertainty principle**.
 - E.g. the amplitude quadrature (strength of the electric field at phase=0) and the phase quadrature (strength of the electric field at phase=90) are analogous to the position X and momentum P .
 - $\Delta X \Delta P \geq \frac{1}{2}$
 - The quadratures are **Continuous Variables**

In coherent states the uncertainty in X and P are equal (non-squeezed states)

$$X_\theta = X \cos(\theta) + P \sin(\theta)$$



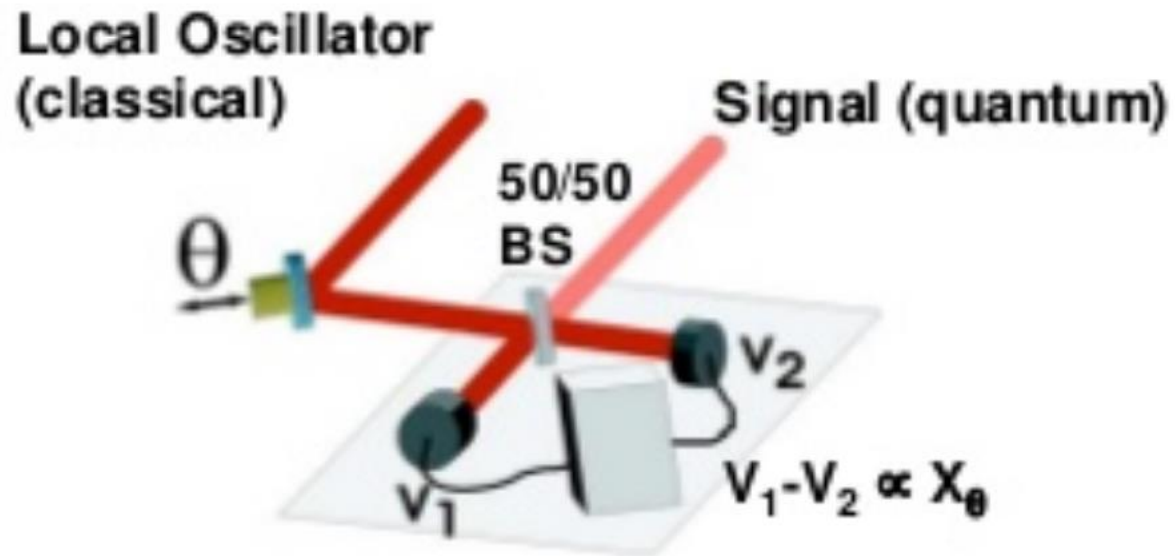
QKD in practice: CV



In classical communications amplitudes are maximized and there is no overlap. In quantum communications, the amplitudes are reduced and the overlap of the uncertainty region allows to do QKD (non-orthogonal bases)

QKD in practice: CV

Homodyne detection



Homodyne detection measures:

$$X_\theta = X \cos(\theta) + P \sin(\theta)$$

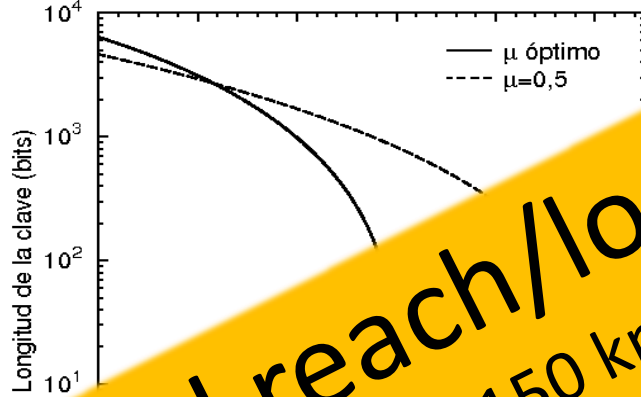
- This detection method is less affected by Raman noise, since you are performing an interference with a classical signal rather than a single photon detection.
- Also, you don't need a single-photon-detector
- Better miniaturization and industrialization possibilities.
- Cheaper
- Heavy post-processing
- In practice, DV reach in general more distance, since it is very affected by losses...

Homodyne detection is very sensitive to the variations of a modulated signal (in phase or frequency) from an oscillating one comparing with it (the local oscillator, that would be identical to the original if it was not carrying any information)

Quantum Networks

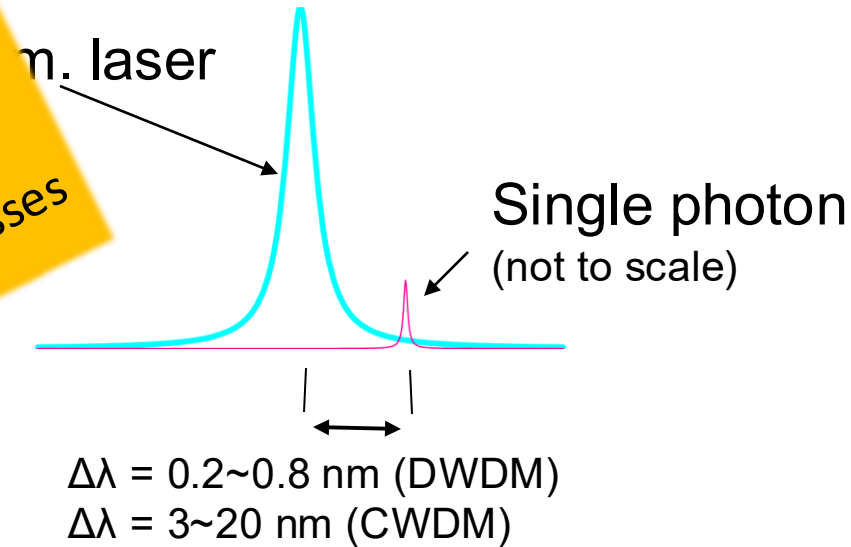
Quantum networks

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.

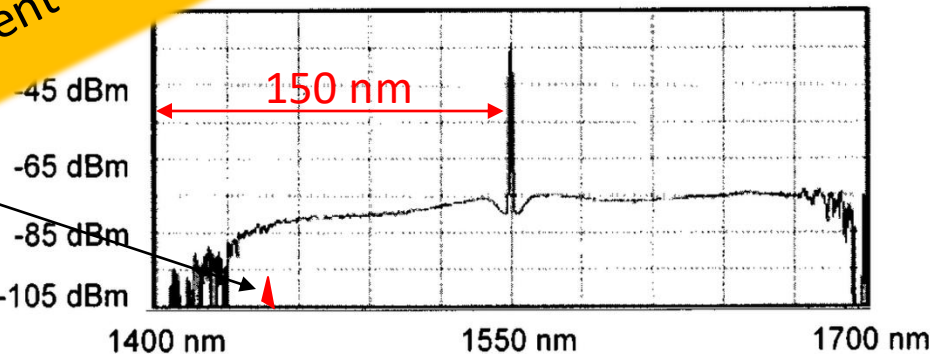


- Difficult to detect.
- Absorptions
- Masked by the noise

Noise in the fibre: Raman

Single Photon

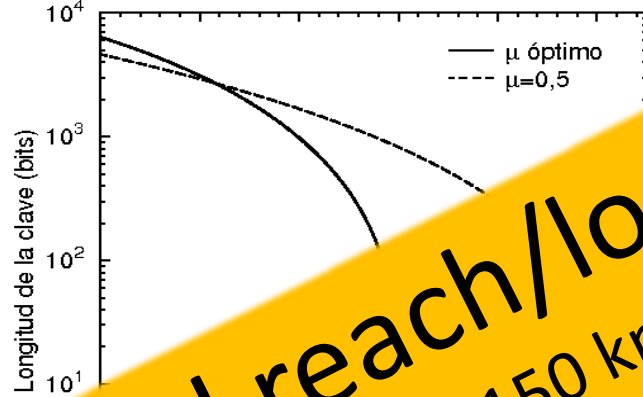
(approx. scale)



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

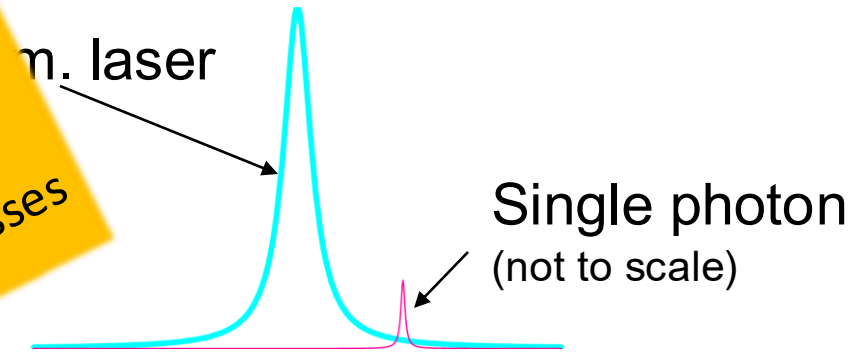
Quantum networks

Limited reach, point to point.



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

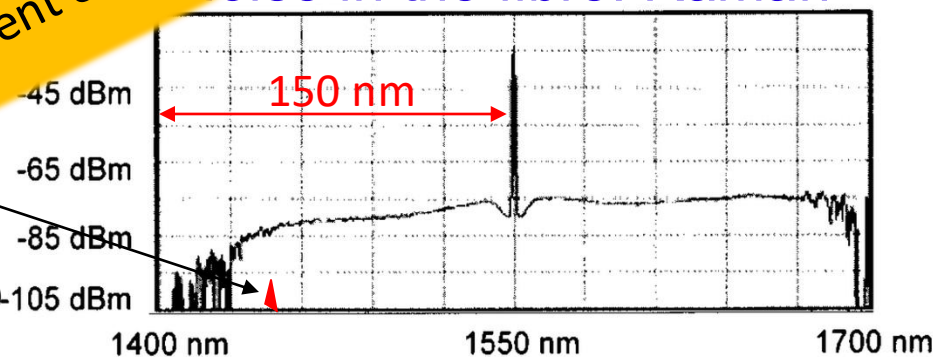
extremely weak signals.



Trusted nodes are required
(security issues)

- Absorptions
- Masked by the noise

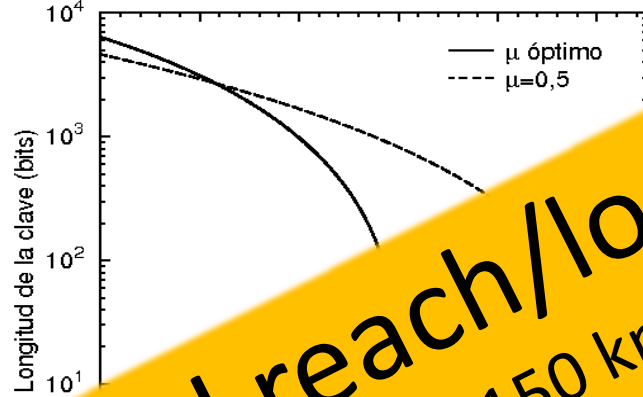
Single Photon
(approx. scale)



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

Quantum networks

Limited reach, point to point.



extremely weak signals.

m. laser

single photon
(not to scale)

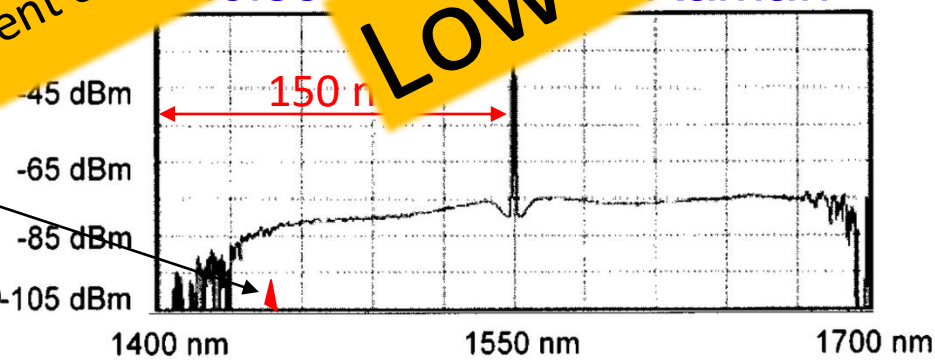
$\Delta\lambda = 0.2\sim 0.8$ nm (DWDM)
 $\Delta\lambda = 3\sim 20$ nm (CWDM)

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

Low tolerance to noise

noise in Raman

Single Photon
(approx. scale)

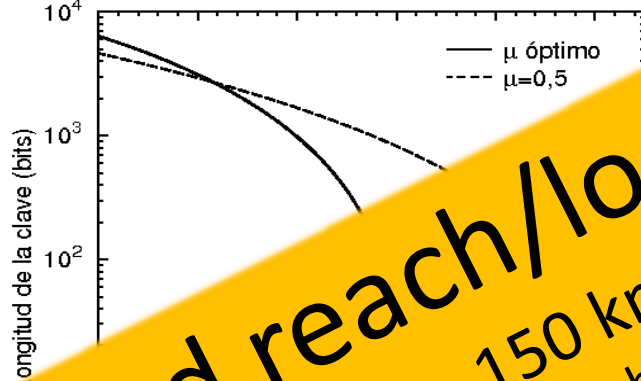


Raman backscattering of a signal at 1549 nm [DOI: 10.1063/1.1842862]

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

Quantum networks

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.

laser

single photon
(not to scale)

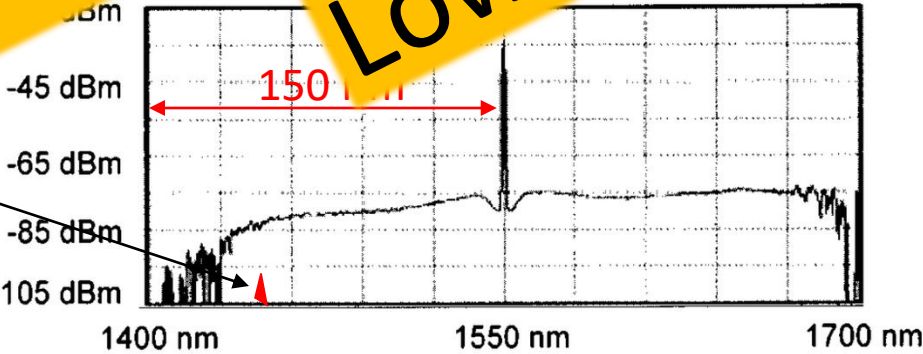
$\Delta\lambda = 0.2 \sim 0.8$ nm (D
SW



Quantum/
classical co-
propagation
Issues

(not sharing the infrastructure
→ Expensive!!)

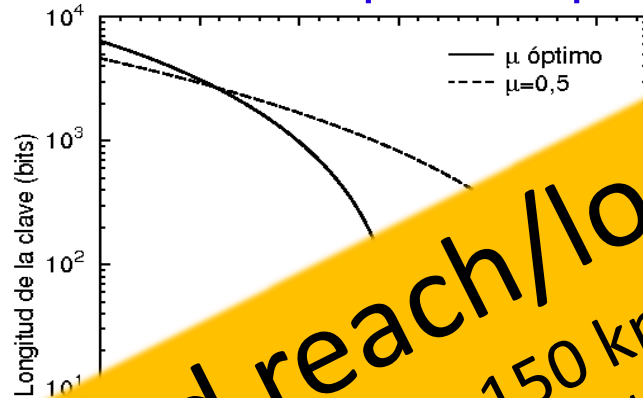
Noise Raman



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

Quantum networks

Limited reach, point to point.



extremely weak signals.

n. laser

photon (not to scale)

$\Delta\lambda = 0.2 \sim 0.8 \text{ nm}$
 $\Delta\lambda = 3 \sim 20$

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

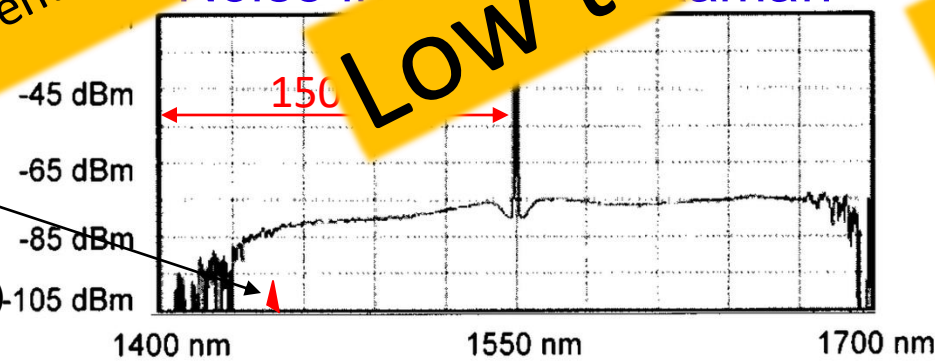
Low tolerance to noise

Alien technology
(HW & SW)

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

Single Photon

(approx. scale)



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

Quantum networks

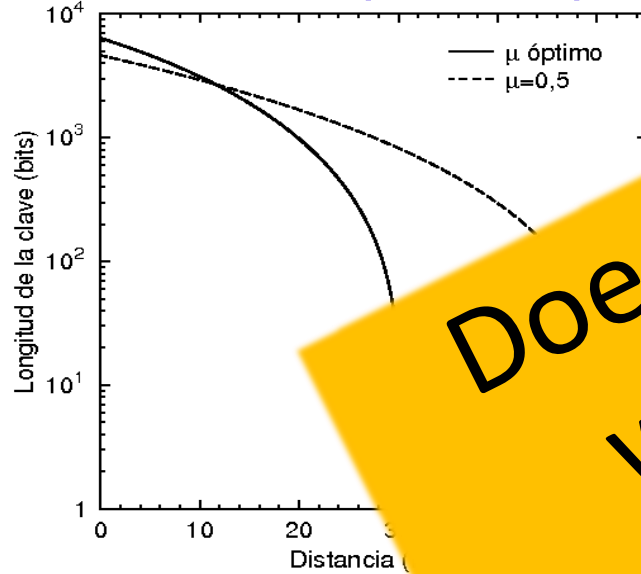


UNIVERSIDAD
TÉCNICA
MADRID



GCC

Limited reach, point to point.



Does not play well
with (classical)
networks.

Single
(not to s

$\Delta\lambda = 0.2\sim 0.8$ nm (DWDM)
 $\Delta\lambda = 3\sim 20$ nm (CWDM)

Noise in Raman

-25 dBm

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



R. Doisneau

What to do? Solutions

- **The traditional view of QKD networks**
 - **Non-Integrative** view: Extreme “ad hoc” **A network just for quantum.**
- **Fully integrated quantum/classical** network: The SDN paradigm.

But first, we are going to take a look to layered networks (classical networks)...

Quantum networks



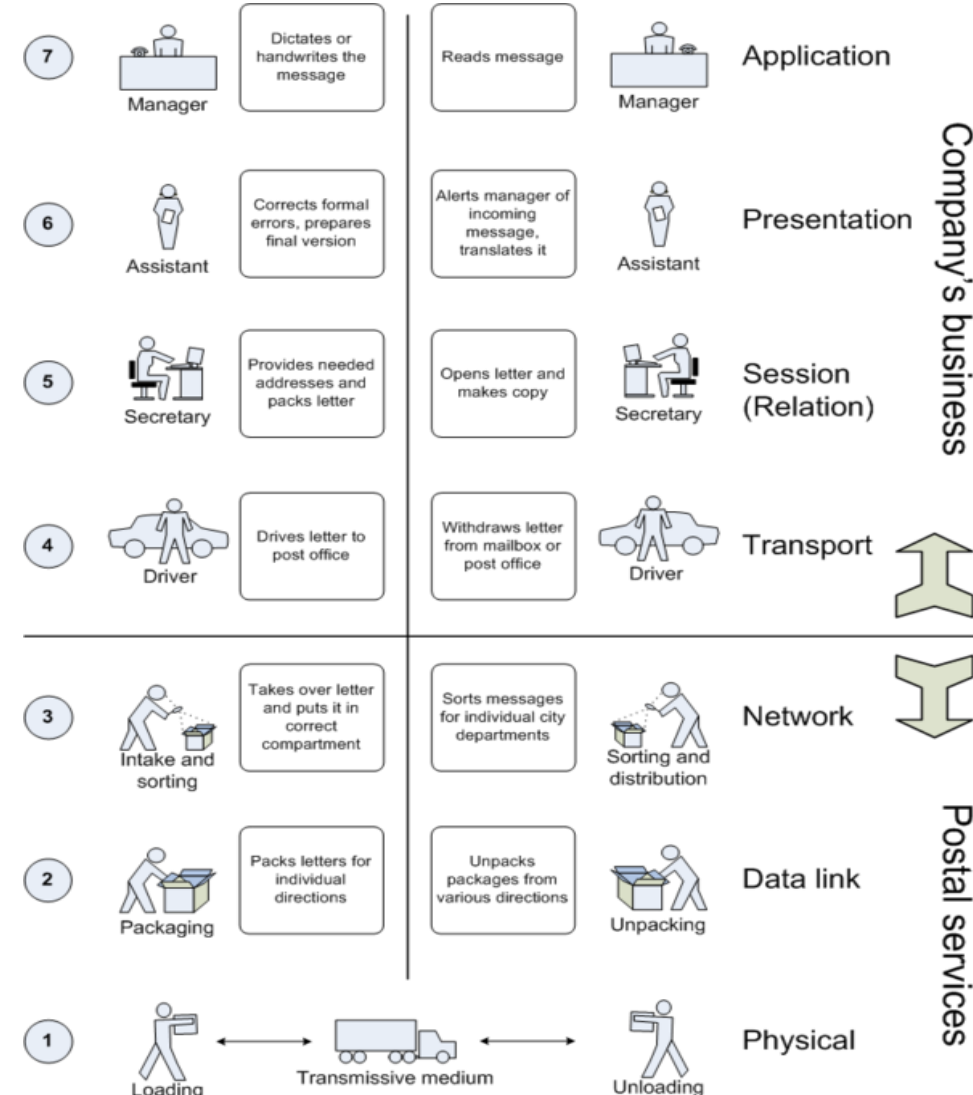
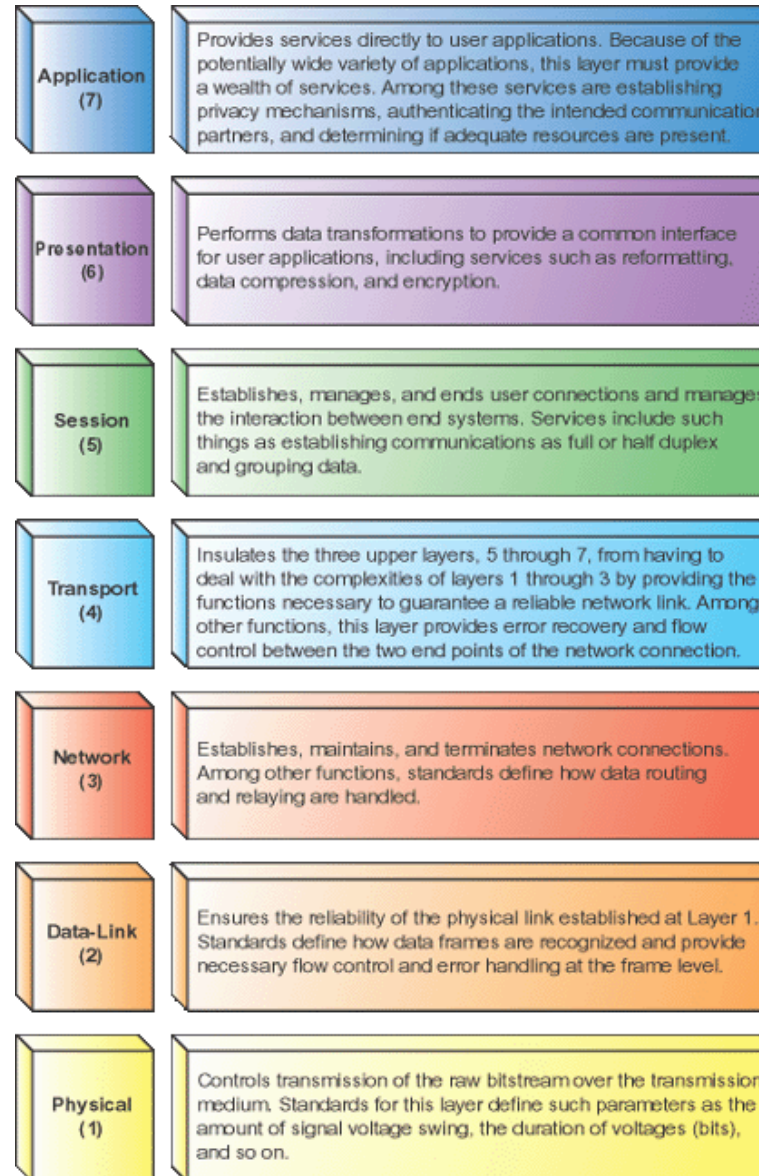
POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID



GCC

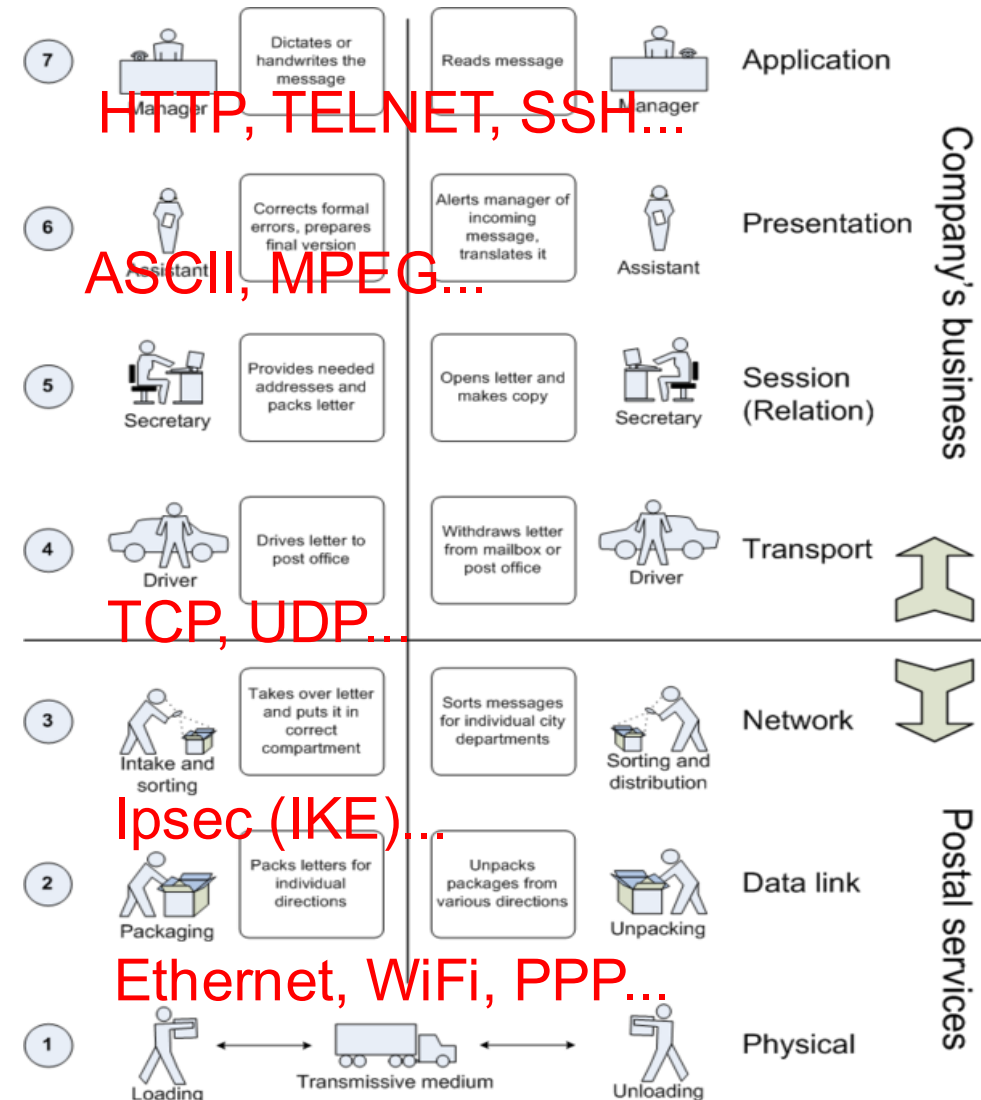
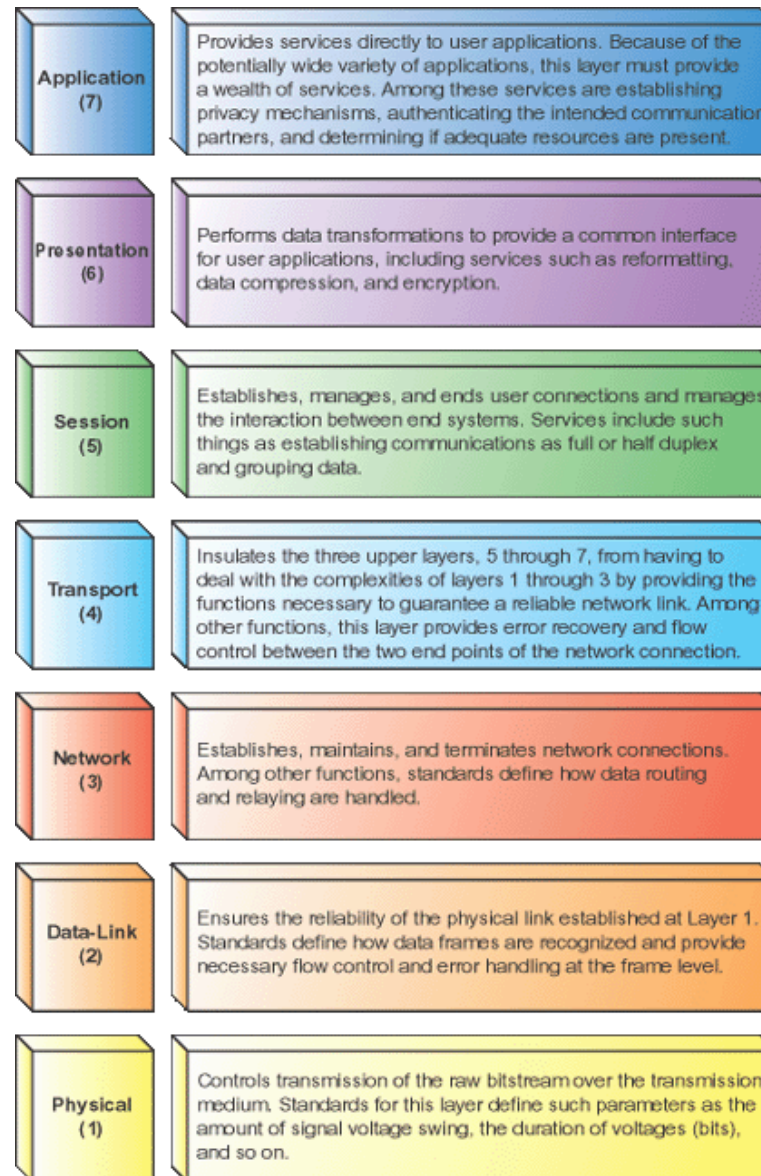
Layered networks: The OSI Model



RM – OSI and letter communication parallel

Quantum networks

Detour:
Layered
networks: The
OSI Model



HTTP, TELNET, SSH...

ASCII, MPEG...

TCP, UDP...

Ipssec (IKE)...

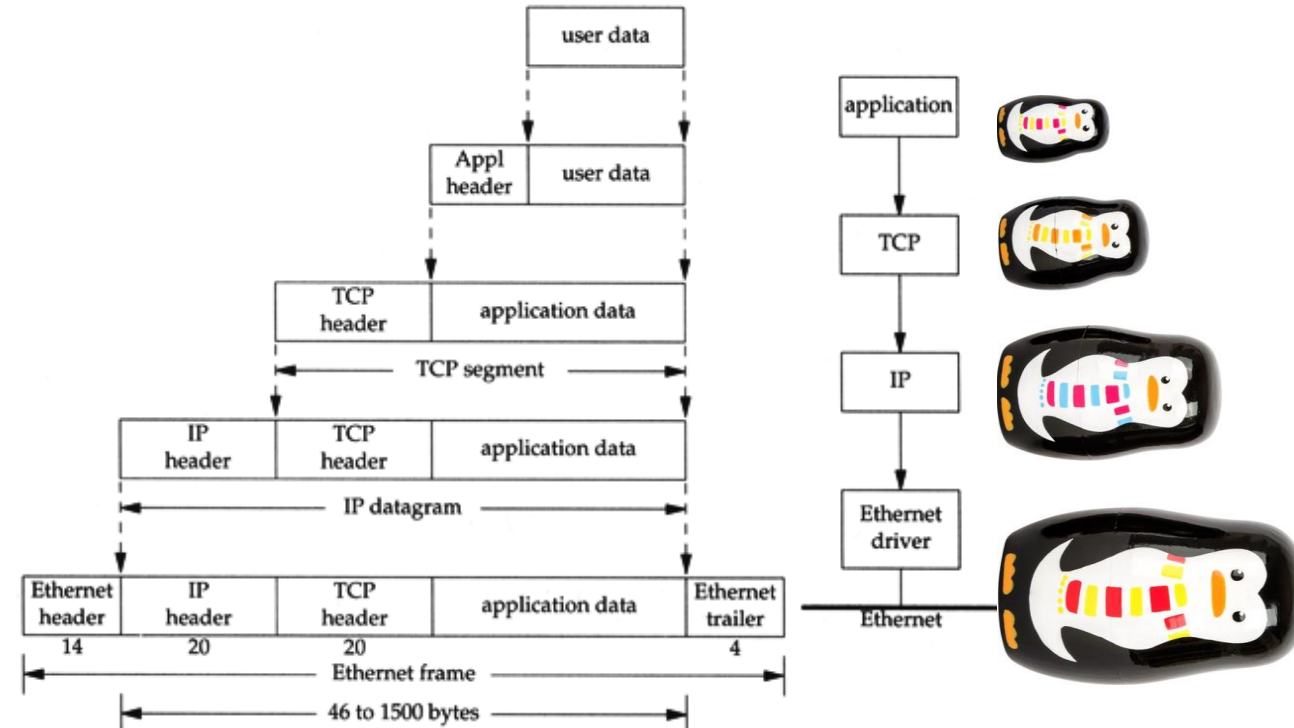
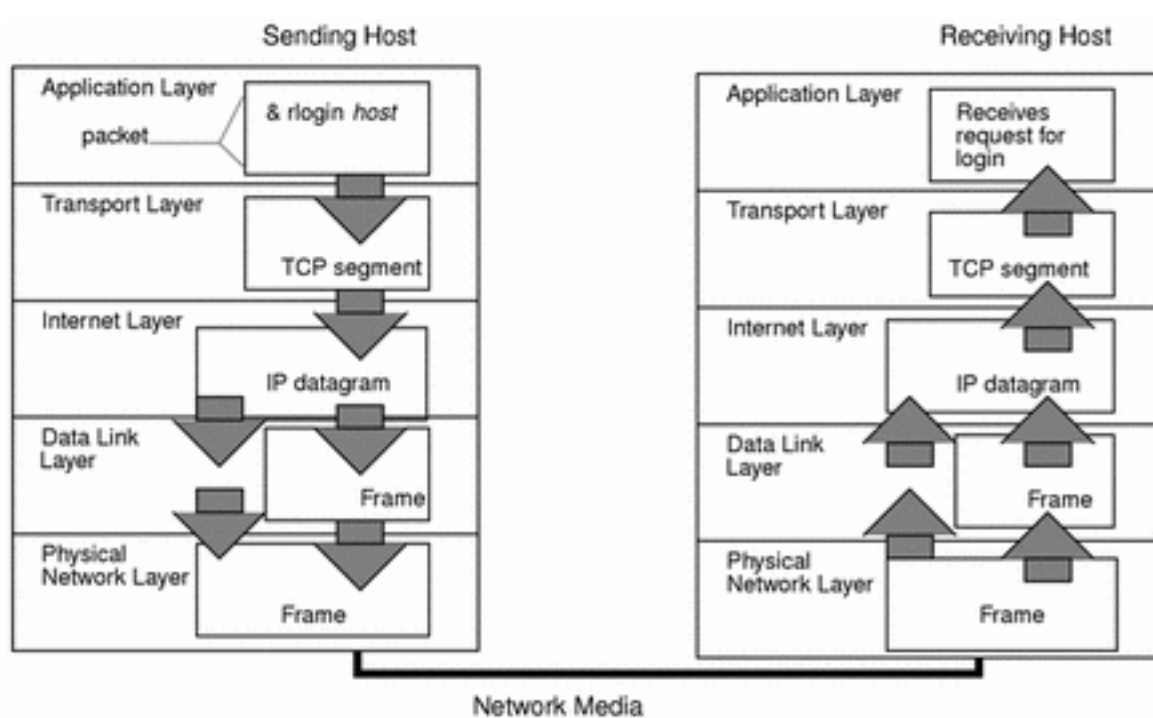
Ethernet, WiFi, PPP...

RS-232, 100BASE-TX, USB, 802.11g...

RM - OSI and letter communication parallel

Quantum networks

Layered networks



This “**matryoshka-like**” behavior “packing-unpacking” does not exist in a QKD network. There is no “packing” of application data into photons — the photons themselves *are* the raw material for generating secret bits. However we can try to adapt this model...

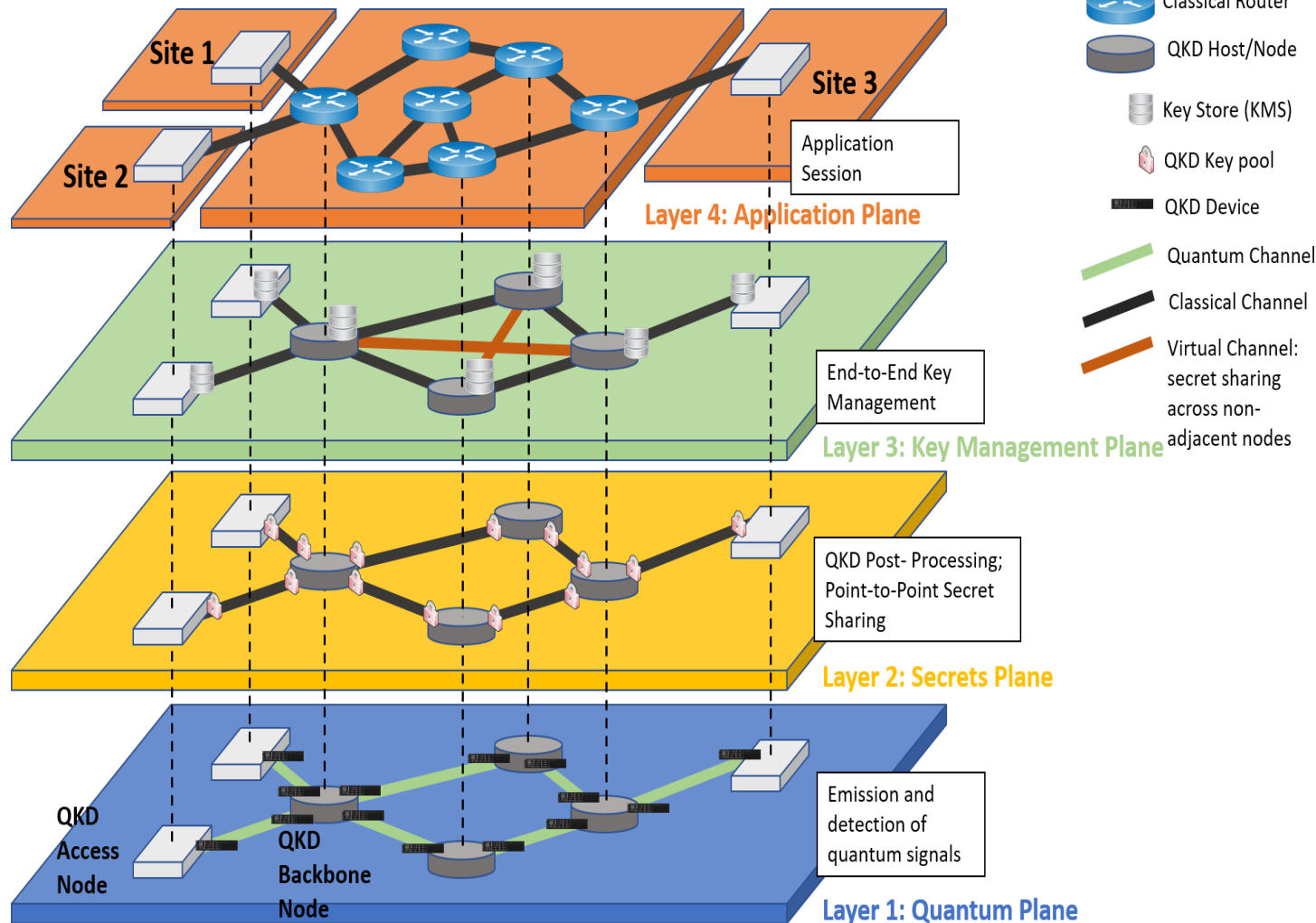
Layered networks



57

Quantum networks

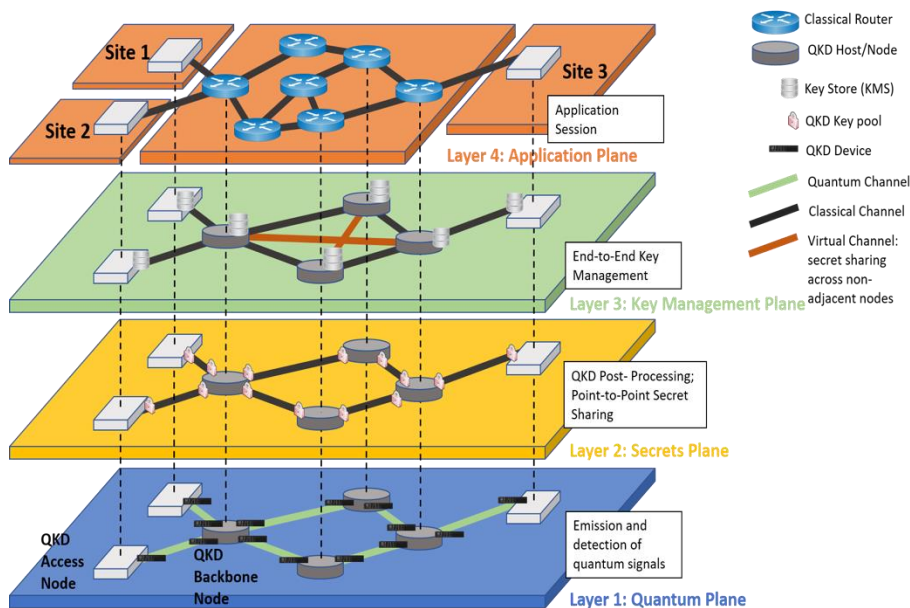
The traditional view of QKD networks



- “Services” feed on the keys from the
- “Key storages” that are filled using the
- “QKD connections” where the quantum links are.

Quantum networks

This is an “ad hoc” parallel network for QKD.



- Dedicated dark fiber or fine-tuned connections.
- It is **not integrated** with existing telco networks.
- **The bad:**
 - **Difficult to deploy and non-incremental.**
 - Static
 - **Very high up-front costs...**
 - ... which means that **either there is a preexisting large market or it cannot create it.**
- **The good:**
 - High performance for QKD

Quantum networks

How to Solve the Integration problem: Software Defined Networking



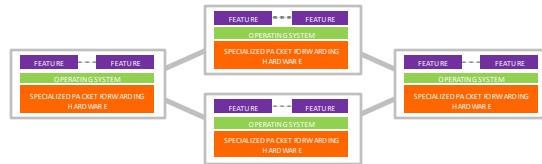
Network equipment as
Black boxes

SDN



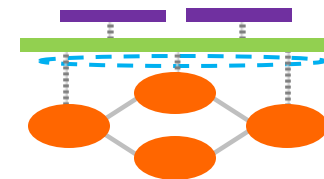
Open interfaces (OpenFlow) for instructing
the boxes what to do

**Programmability is
Key:** A SDN controller
can manage the
Network.



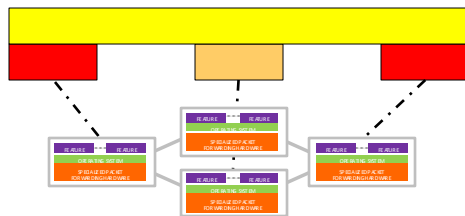
Boxes with autonomous
behaviour

SDN



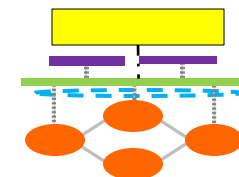
Decisions are taken out of the box

SDN decouples
the data plane
from the control
plane



Adapting OSS to manage black boxes

SDN



Simpler OSS to manage the SDN
controller

SDN can adapt,
allowing for
a fast innovation
Cycle.

Quantum networks

How to Solve the Integration problem: Software Defined Networking



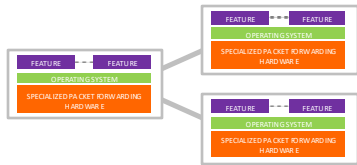
Network equipment as
Black boxes

SDN



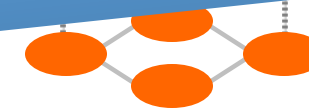
Constructing

Programmability is Key: A SDN controller can manage the Network.



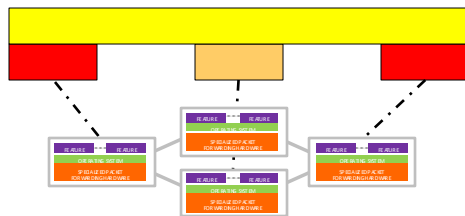
Boxes with autonomous
behaviour

In the 'washing machine example', this is equivalent to be able to 'program the buttons and dials'!



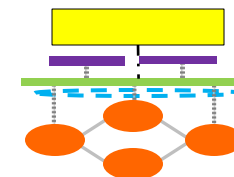
Decisions are taken out of the box

SDN decouples the data plane from the control plane



Adapting OSS to manage black boxes

SDN

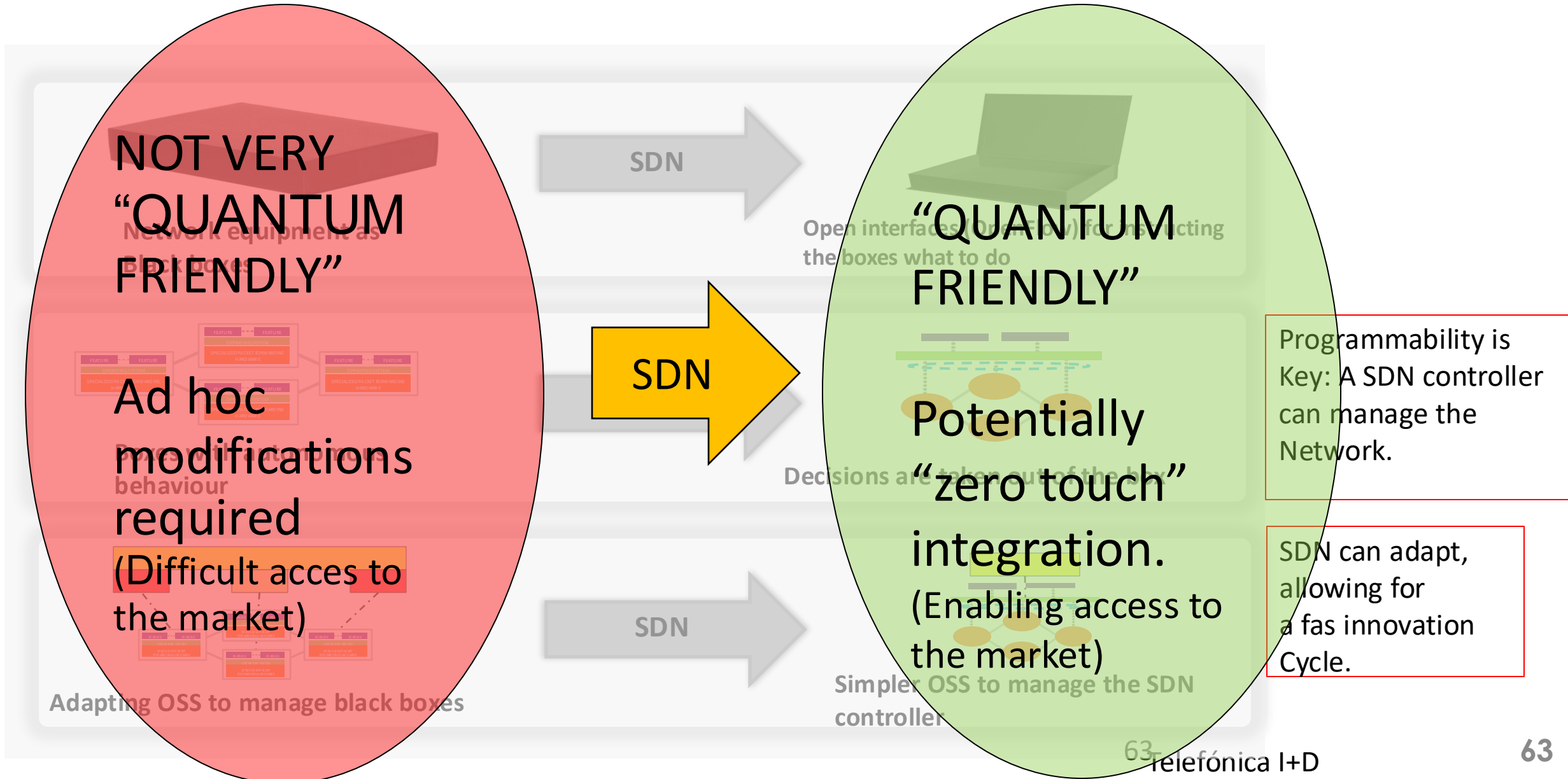


Simpler OSS to manage the SDN controller

SDN can adapt, allowing for a fast innovation Cycle.

How to Solve the Integration problem: Software Defined Networking

- In a QKD network key grows in some pairs of nodes through a physical process (that you cannot control completely), and not by following a 'routing protocol'... If you have hundreds of nodes,
 - how do you route keys across multiple hops?
 - how do you decide which path to use if one link is degraded?
 - how do you allocate key pools to multiple applications?
 - how do you orchestrate different devices from different vendors?
 - how about managing trusted nodes? Those are not necessary in classical networks, in general.
- With SDN...
 - You have a global view of the network
 - You can compute end-to-end paths meeting some requirements.
 - You can dynamically reroute and manage key pools.
 - You can abstract the device heterogeneity.
 - Telcos know SDN (there are protocols, standards...) so QKD can be easily integrated in telecommunications.
- Of course, you need to install more QKD devices 'one by one' if you want to grow your network, but SDN helps to the management of the network once the links have been established.



... but there is more.

- **SDN is an enabler** of QKD in telecommunications networks.
- **SDN is a consumer of QKD:**
 - As a critical infrastructure that “owns” the physical means to do QKD.
 - New security challenges in network “softwarization”
 - Its structure of “secured connected locations”, with typical distances within the QKD range, matches the security model of “connected trusted nodes” in current QKD. **Trusted nodes are already there** (PoPs)

SDN  QKD

... but there is more.

- **SDN is an enabler** of QKD in telecommunications networks.
- **SDN is a consumer of QKD:**

- As a critical infrastructure that “owns” the physical means to do QKD.

SDN is both, an enabler of QKD in communications networks and, at the same time, a very good use case for QKD.

QKD range, matches the security model of “connected trusted nodes” in current QKD. **Trusted nodes are already there (PoPs)**

SDN  **QKD**

... but there is more.

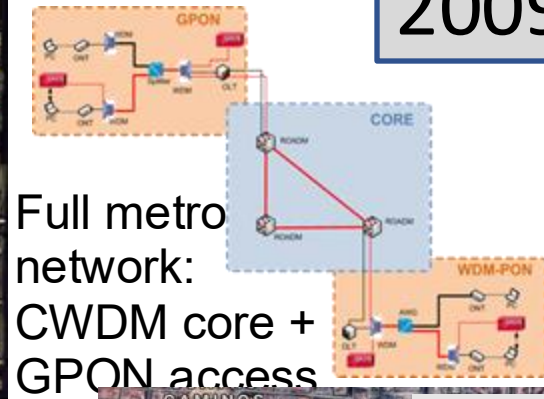
- SDN is **In our case, the first user is the telco.**
- SDN is **(and you can think later about other users)**
 - As a
 - Ne
- Its structure of “secured connected locations”, with typical distances within the QKD range, matches the security model of “connected trusted nodes” in current QKD. **Trusted nodes are already there (PoPs)**

SDN ↔ QKD

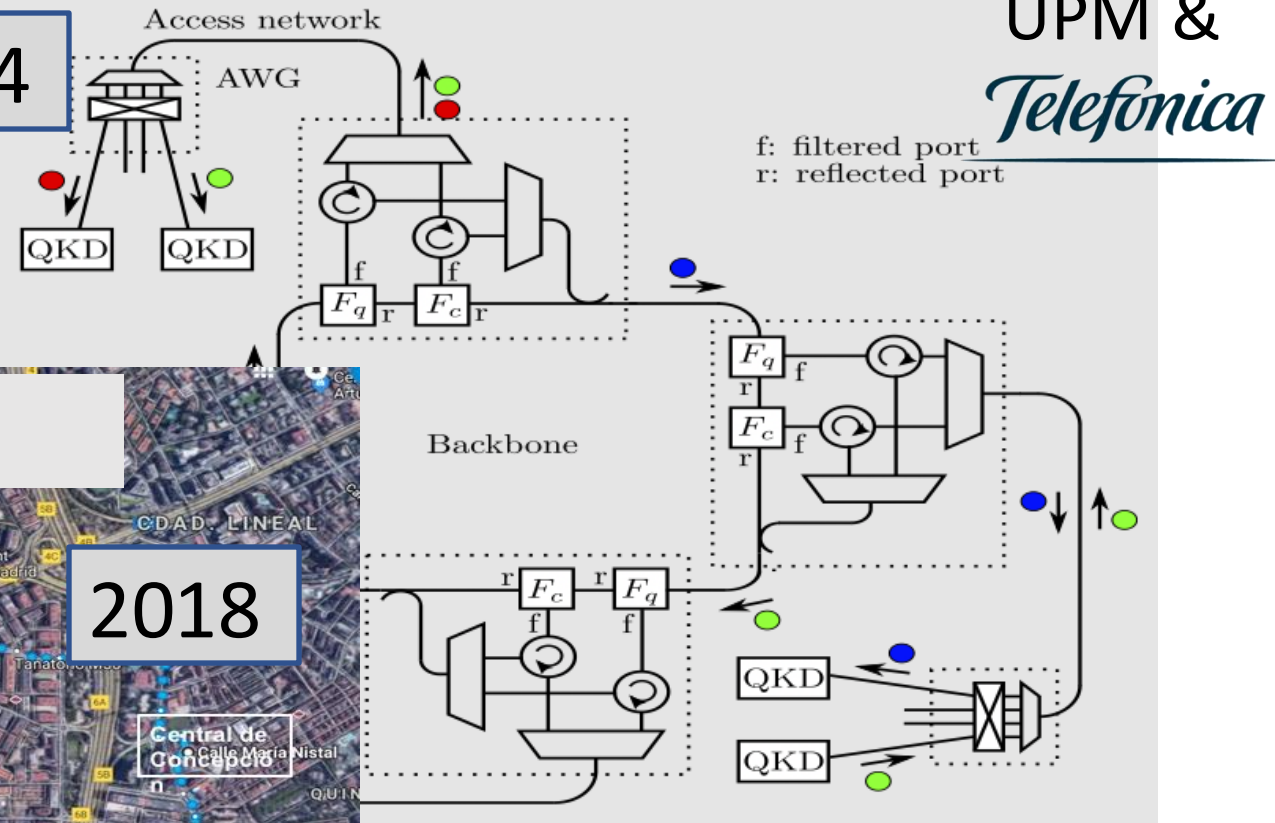
Quantum networks



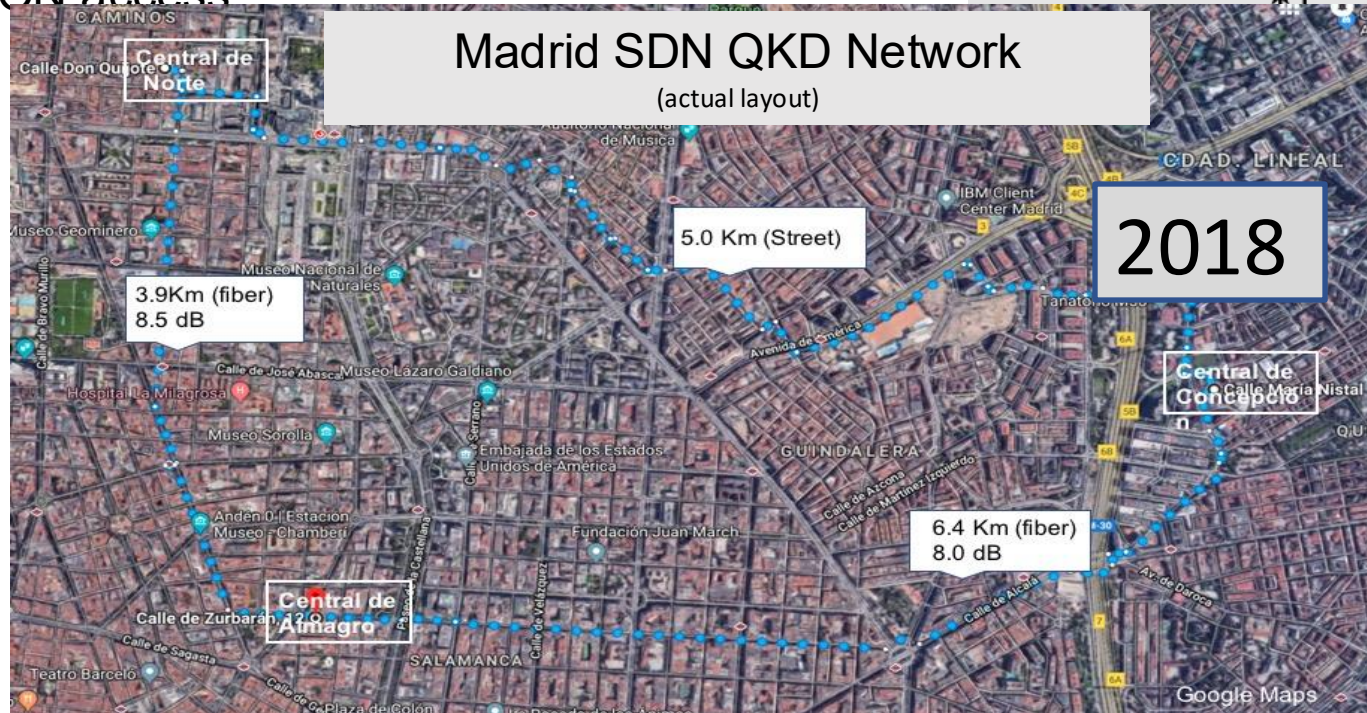
2009



2014



Madrid SDN QKD Network
(actual layout)



Quantum networks



UNIVERSIDAD
POLITÉCNICA
DE MADRID

POLITÉCNICA



GCC



- **First Quantum SDN Network in the world (2018)**
- Installed in **production facilities.**

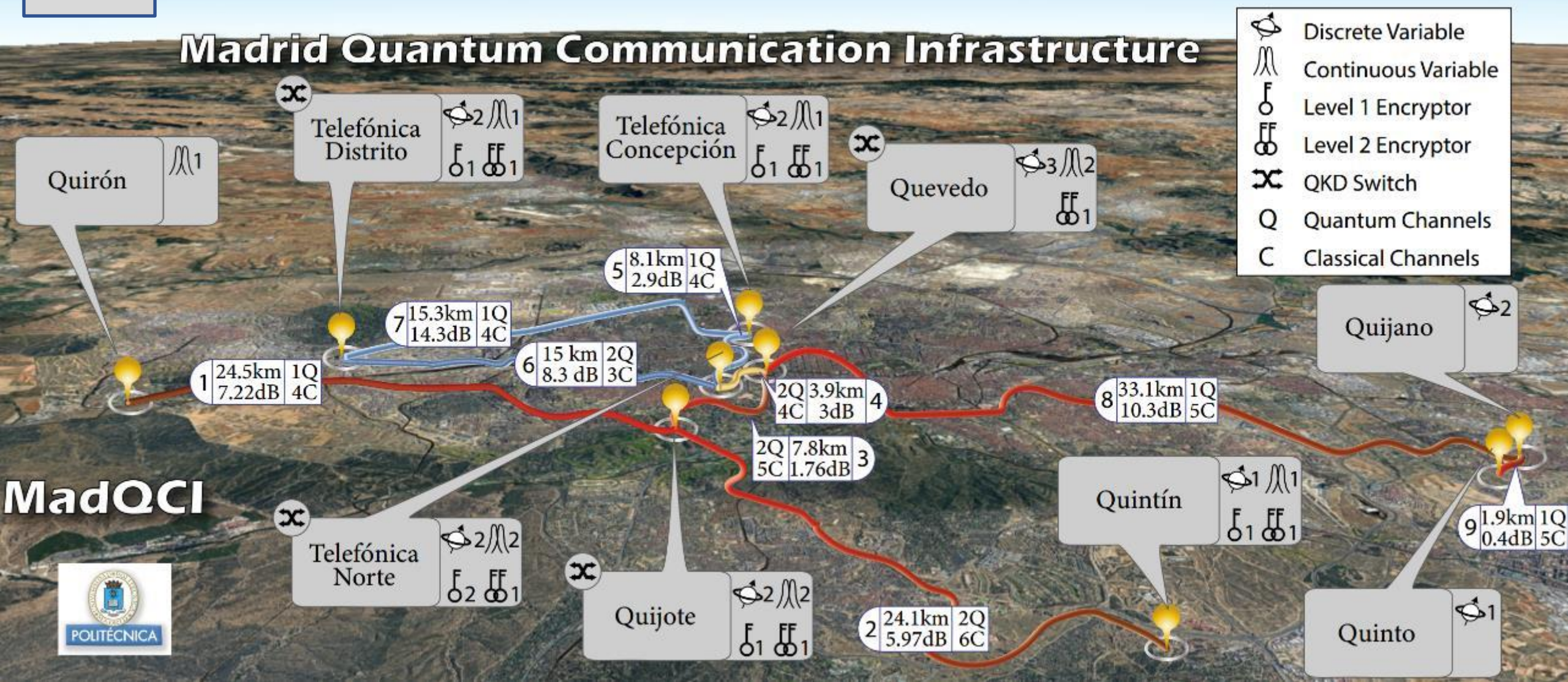
Telefónica

“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>

2023

arXiv:2311.12791v2

Madrid Quantum Communication Infrastructure





R&S L2 encryptor

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

SDN server

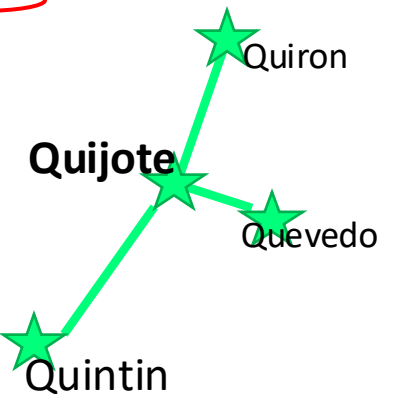
ADVA OTN (optical
transport
management)
+
Link encryptor

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



2 HWDU
CV QKD +
2 servers
From CiViQ

Quijote a “central” Node



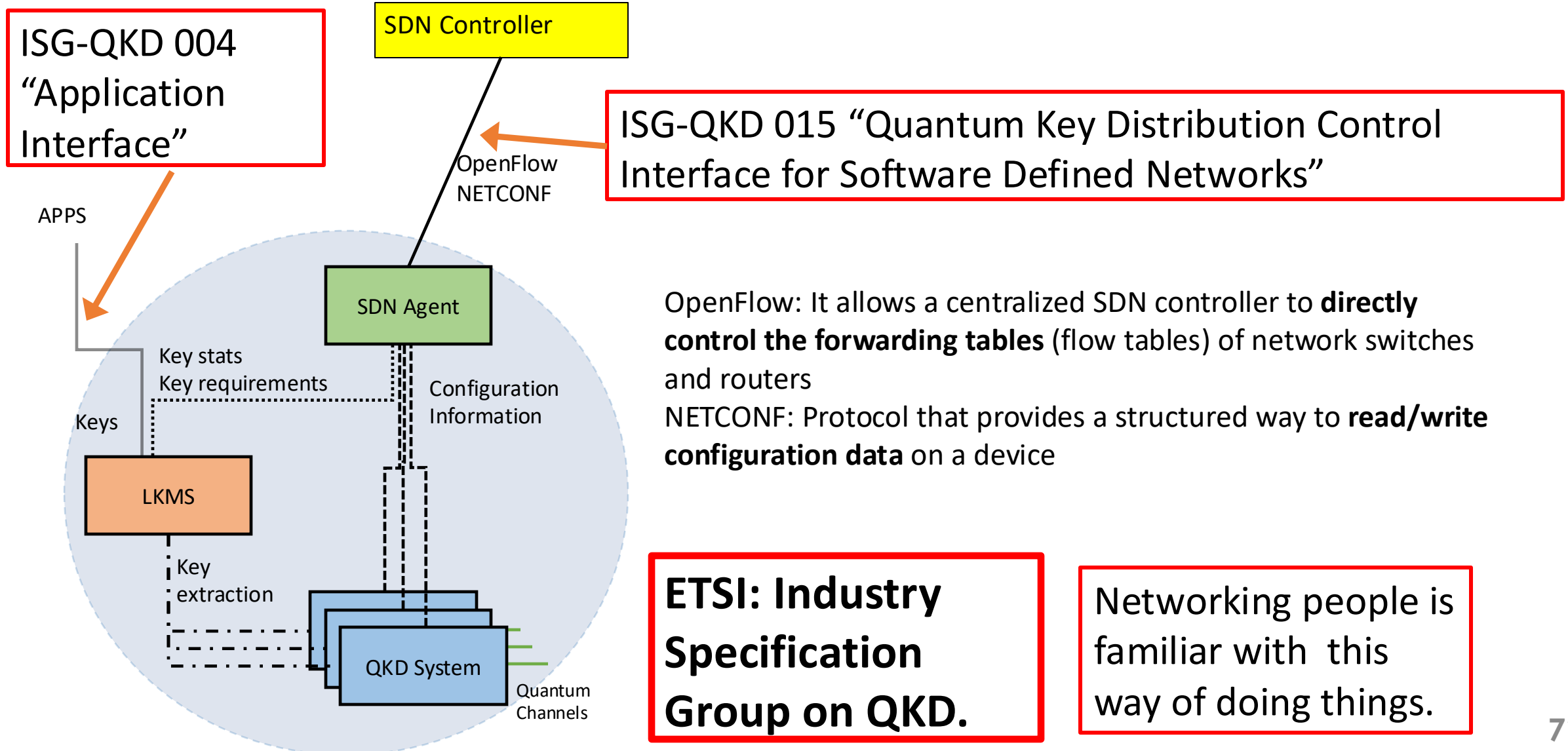
- 2 Quantum & service channels DV and CV from/to previous/next node. Compatibility in C & O bands in same fiber.
- Classical communications in bidi fiber, cyphered L1, L2 & L3 traffic.

Quantum networks

Key structure: SD-
QKD-Node
Abstraction



UNIVERSIDAD
POLITÉCNICA
DE MADRID



Quantum networks

Global view of the SDQKD Network

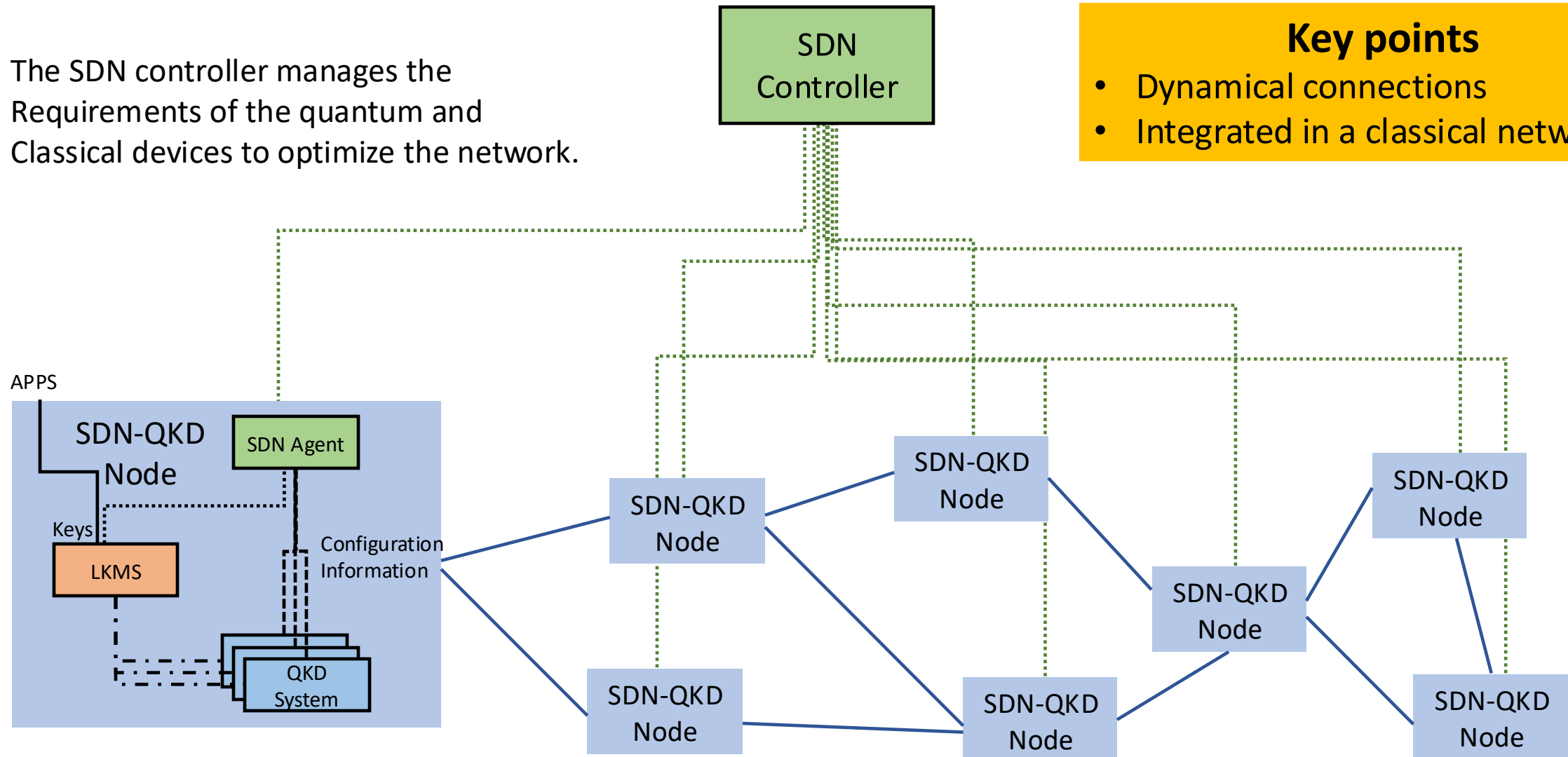
UNIVERSIDAD
POLITÉCNICA
DE MADRID

GCC

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

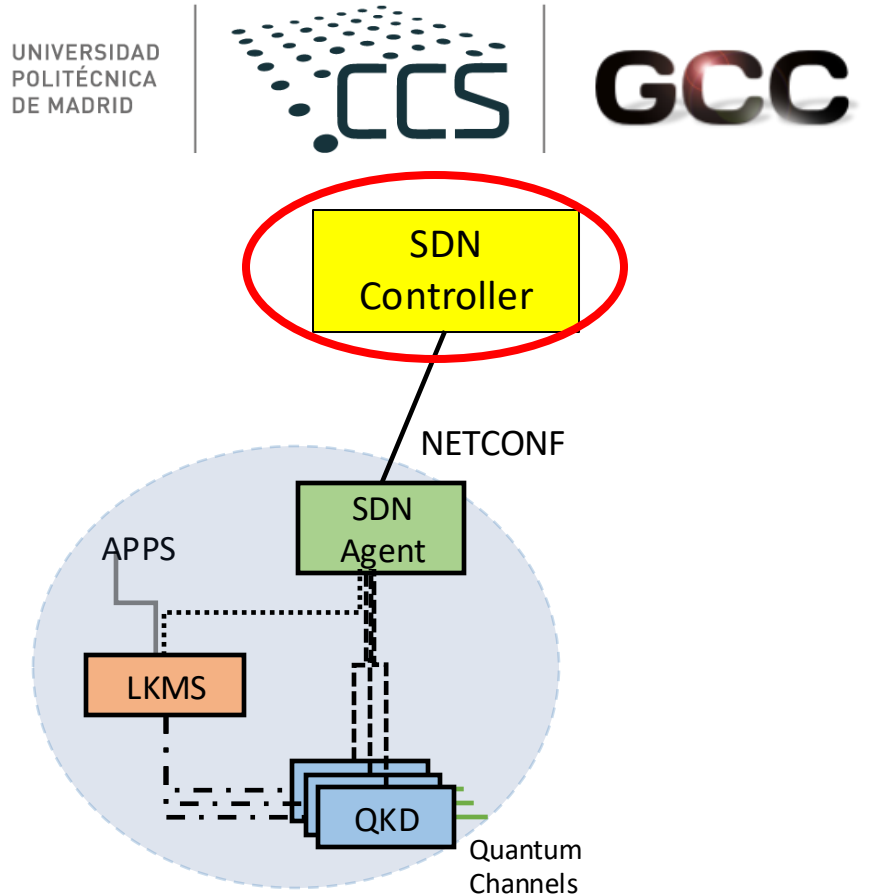
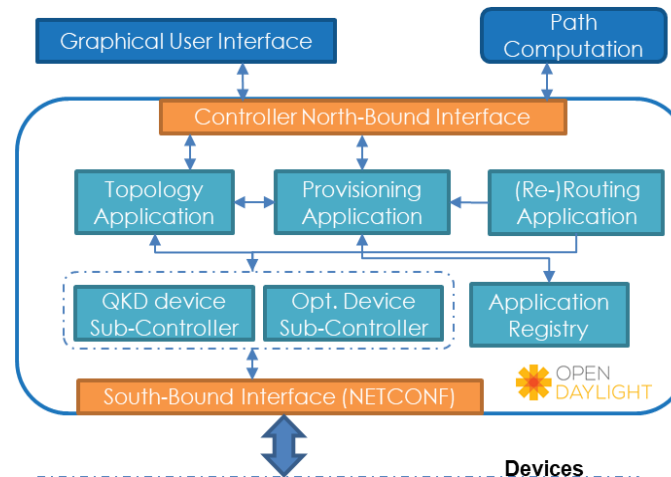


Quantum networks

SDN Controller

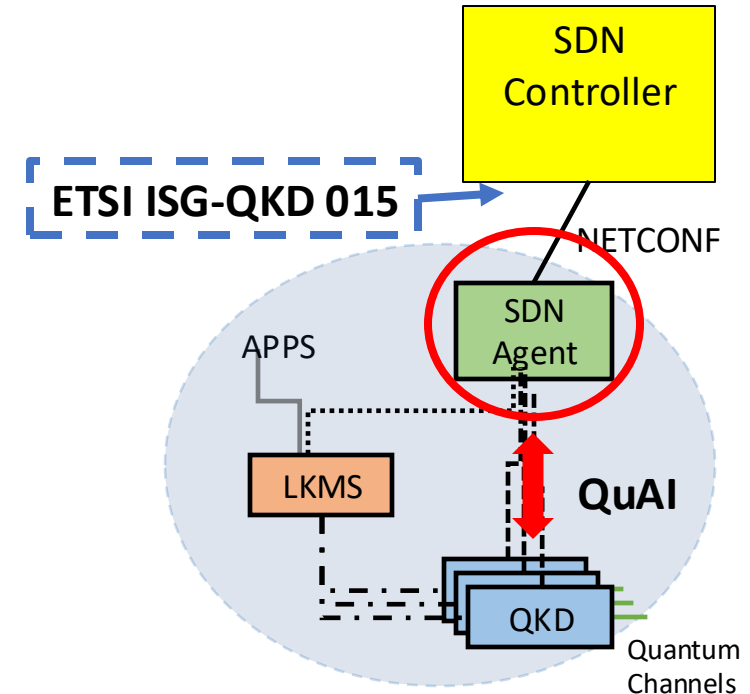
SDN Controller:

- To **control** simultaneously the **quantum and classical resources** in the network.
- Path computation to calculate optical paths for a quantum channel
- Topology application (it collects info about the topology)
- Quantum part designed as a plug-in of existing, commercial grade, controllers (e.g. OpenDaylight)
 - Easier acceptance by telcos.



SDN Agent:

- Manages the **Interactions in the node** with the set of QKD devices installed.
 - Based on:
 - **QuAI** (Quantum Abstraction Interface) minimal set of comms with the QKD system for easy integration.
 - **QuAM** (Quantum Abstraction Module) Translates SDN Control commands into commands that the QKD device can understand via QuAI.
 - Uses ETSI (European Telecommunications Standards Institute) ISG 015 “SDN Control interface” in the northbound interface.

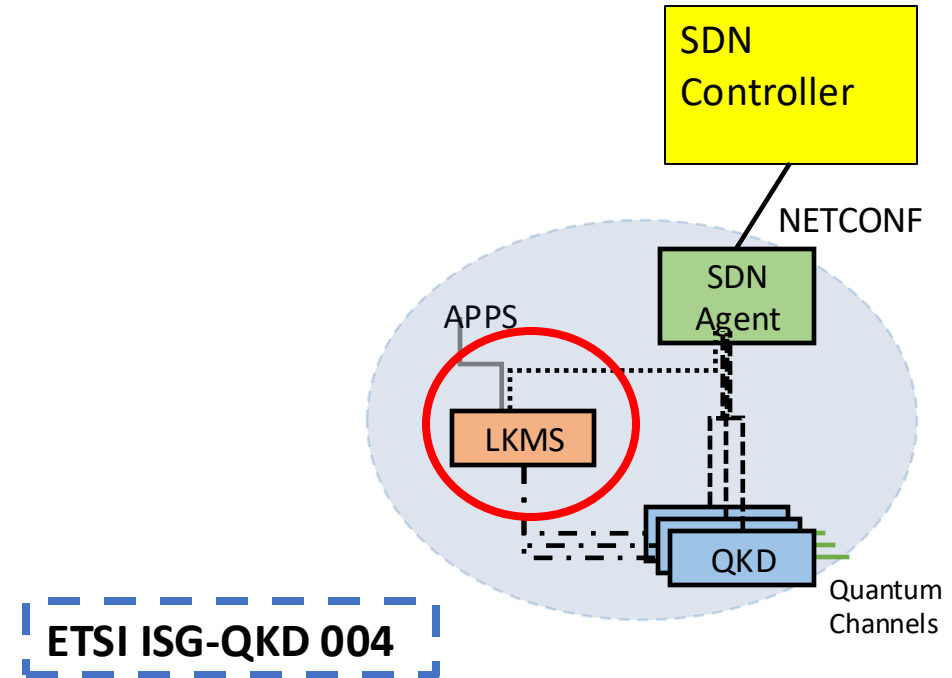


Quantum networks

LKMS

LKMS:

- **Local Key Management System:**
 - Manages the keys extracted from the QKD device and handles it to the Application
 - Keeps statistics and requests services to the SDN Agent (QoS)
 - Uses ETSI ISG 004 “Application Interface”



Noteworthy:

- All components shown are large enough to be **manufactured separately**: Disaggregation.
- Entry point for **new manufacturers**
- Using **trusted technologies** in Telco environments.

Quantum networks: MadQCI



POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID



GCC

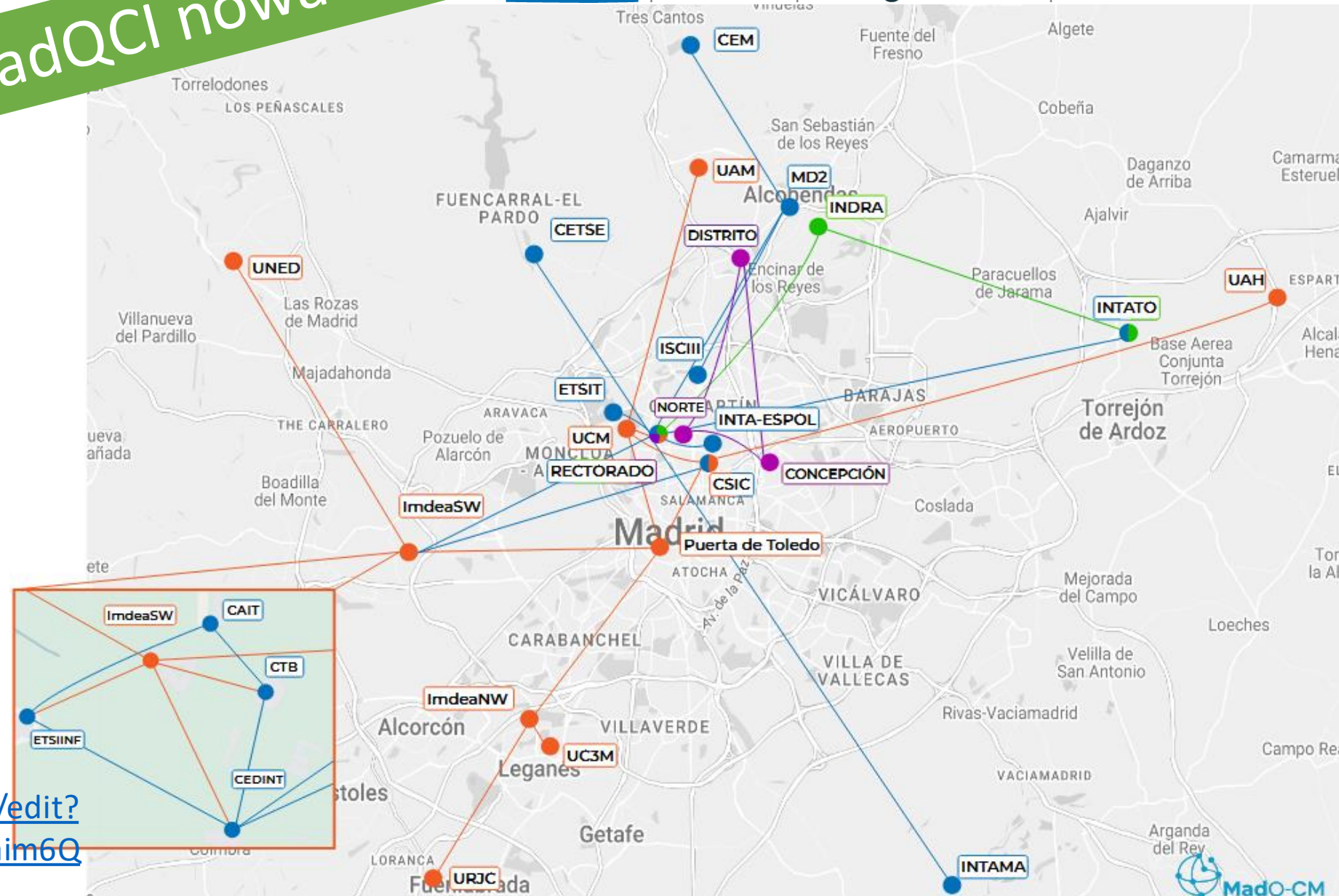
29 locations
19 institutions

700 km of fibre links
(only RM+UPM)

32 quantum systems
23 QKD + 9 QRNG
10 vendors

Heterogeneous
> 10 application
scenarios and
beyond-QKD.

MadQCI nowadays



<https://www.google.com/maps/d/edit?mid=13v1Wy9xpURDulJ6ZkrGqDjaim6QKkvA&usp=sharing>

Quantum networks: MadQCI



UNIVERSIDAD
POLITÉCNICA
DE MADRID



GCC

14 locations

9 institutions

260 km of fibre links

21 QKD + 9 QRNG

10 vendors

Scenarios

Trunk

Demonstration (cloud)

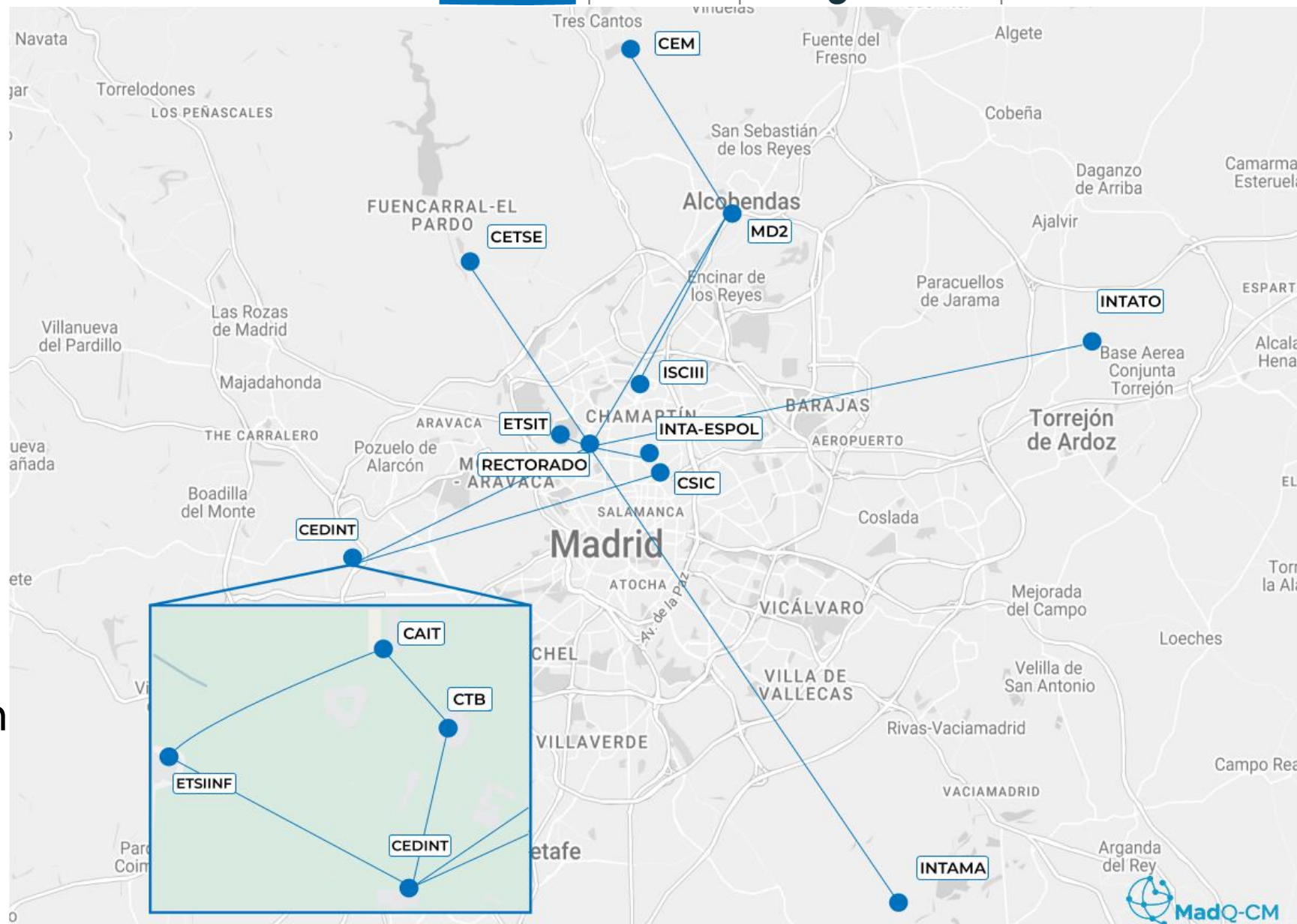
High security

Beyond & hybridisation

Time and synchrony

Switching

Laboratory



Quantum networks: MadQCI UPM in MadQCI



POLITÉCNICA

14 locations

9 institutions

260 km of fibre links

21 QKD + 9 QRNG

10 vendors

Scenarios

Trunk

Demonstration (cloud)

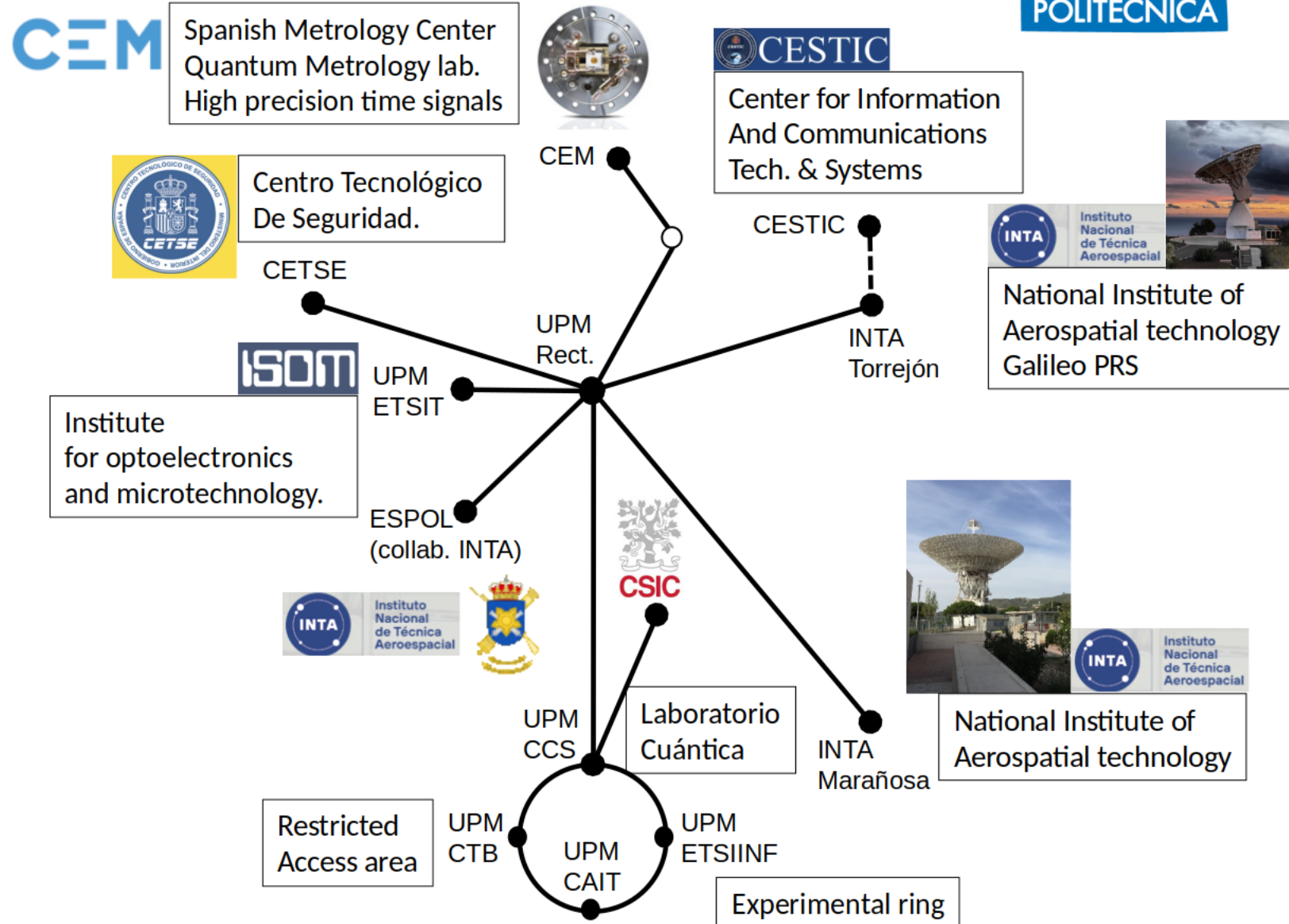
High security

Beyond & hybridisation

Time and synchrony

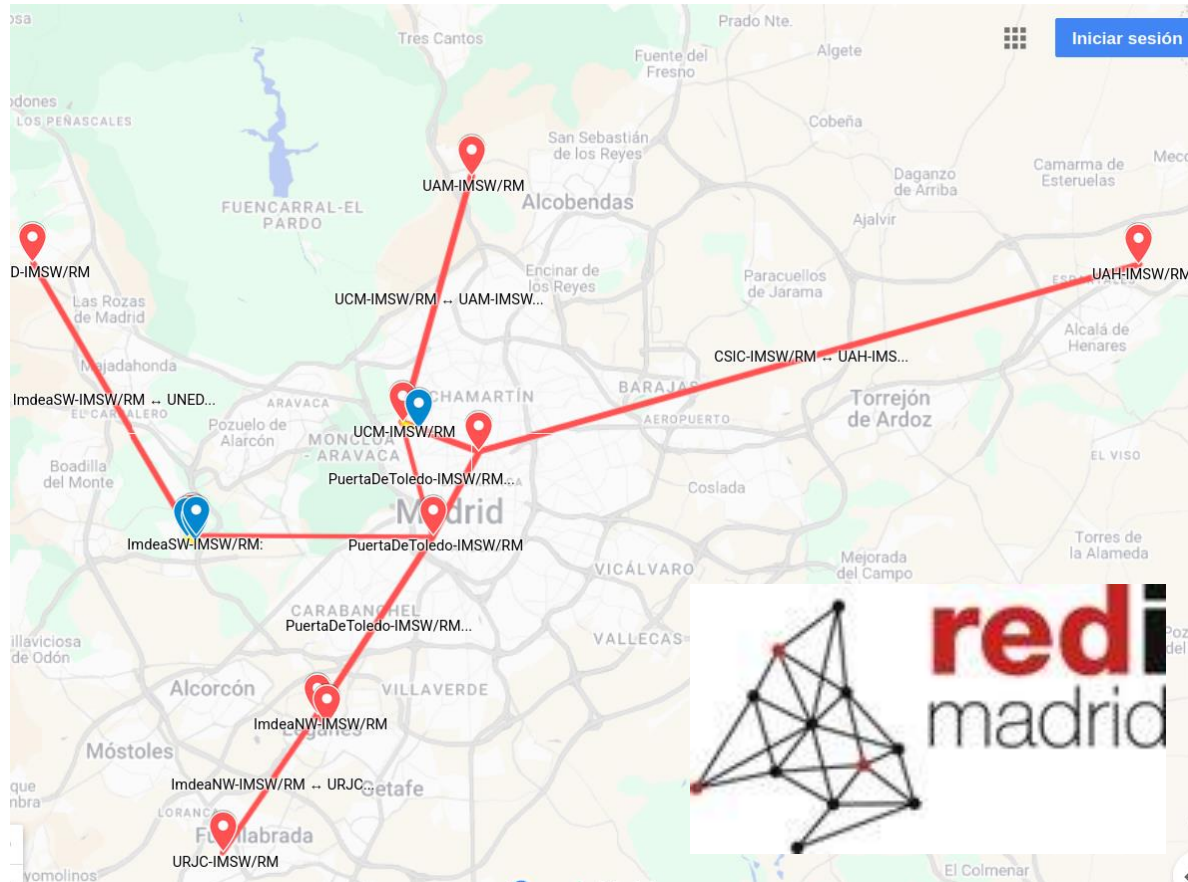
Switching

Laboratory



Quantum networks: MadQCI

An institutional segment



Links all universities in Madrid

An industrial segment



Links Indra and Telefónica

But... quantum networks are QKD networks only?

Remember...

Asymmetric cryptography (RSA, ECC) **relies on one-way functions**, as well as Diffie-Hellman.

The factorization problem.

The discrete logarithm problem.

Without quantum computers, we have **strong evidence** that the one-way functions are one-way functions.

However, because of the Shor's algorithm, we know that **a quantum computer has the power to break those “one-way functions”**.

What is the solution?

- The security relies in **mathematical problems** that are difficult to solve by classical and quantum computers.
- However, **there is no a mathematical demonstration** of the security! (one-way functions).
- As in classical cryptography, **we need confidence** to adopt this technology.
- This confidence is 'boosted' through the **NIST standardization process**.

•Initiative:

The U.S. National Institute of Standards and Technology (NIST) initiated a process in 2016 to standardize post-quantum cryptographic algorithms.

•Process Phases:

- **Round 1 (2017–2019):** Evaluation of 69 proposals.
- **Round 2 (2019–2020):** Narrowing down to 26 candidates.
- **Round 3 (2020–2022):** Selection of finalists and alternate candidates.
- **Round 4 (2022–2024):** Further evaluation of the additional candidates.

•Evaluation Criteria:

Security, efficiency, and feasibility of implementation in various environments.

- **For Encryption and Key Exchange:**

- FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard

- **For Digital Signatures:**

- FIPS 204, Module-Lattice-Based Digital Signature Standard
- FIPS 205, Stateless Hash-Based Digital Signature Standard

These algorithms were selected for their resistance to quantum attacks and strong performance.

Two solutions to the threat of quantum computing...

Quantum Key Distribution (QKD):

- Security is based on the laws of quantum mechanics.
- Therefore, at a theoretical level, it is impossible to break, as it would require violating the laws of physics.
- Depending on the implementation, side-channel attacks may exist.
- Requires very expensive (currently) and specialized devices.

Hybridization of QKD
and PQC provides
two layers of
security!

But we need to
migrate to quantum-
resistant cryptography
fast fast since...

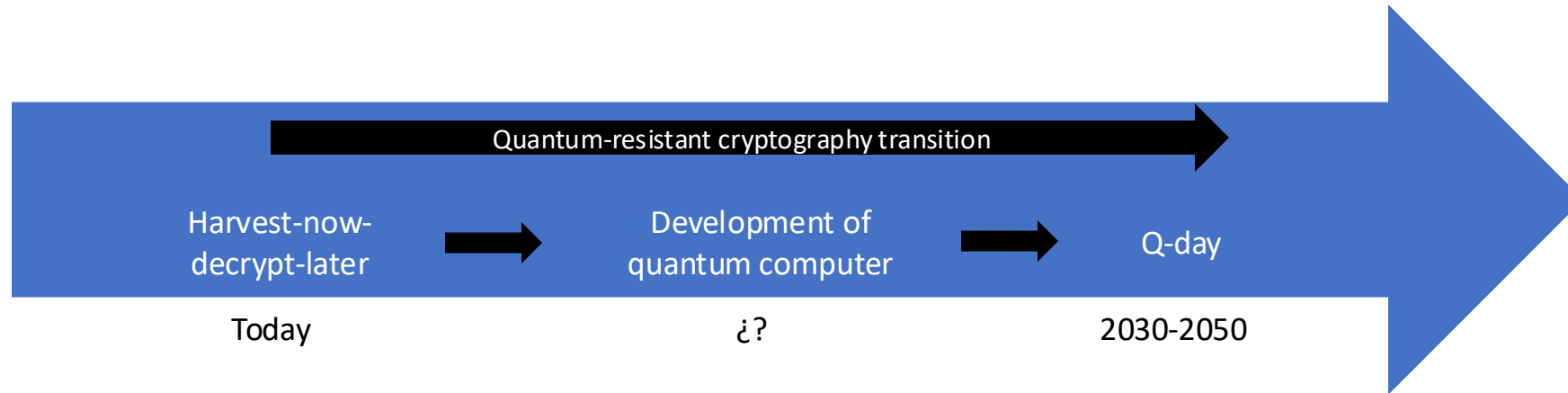
Post-quantum Cryptography (PQC):

- Security is based on mathematical problems that are believed to be difficult to solve for both quantum and classical computers.
- Therefore, at a theoretical level, security is not proven. Like classical cryptography, it relies on experience.
- Depending on the implementation, side-channel attacks may exist, although they are less complex.
- Does not require specialized devices.

Hybridization

Migration to quantum-resistant cryptography

Migration to PQC has to be done now!



Development of quantum computer

vs.

Quantum-resistant cryptography transition

Scenario A: time to quantum computer > cryptographic transition



Scenario B: time to quantum computer < cryptographic transition



- Exclusive-Oring:

$$K = K_1 \oplus \dots \oplus K_n$$

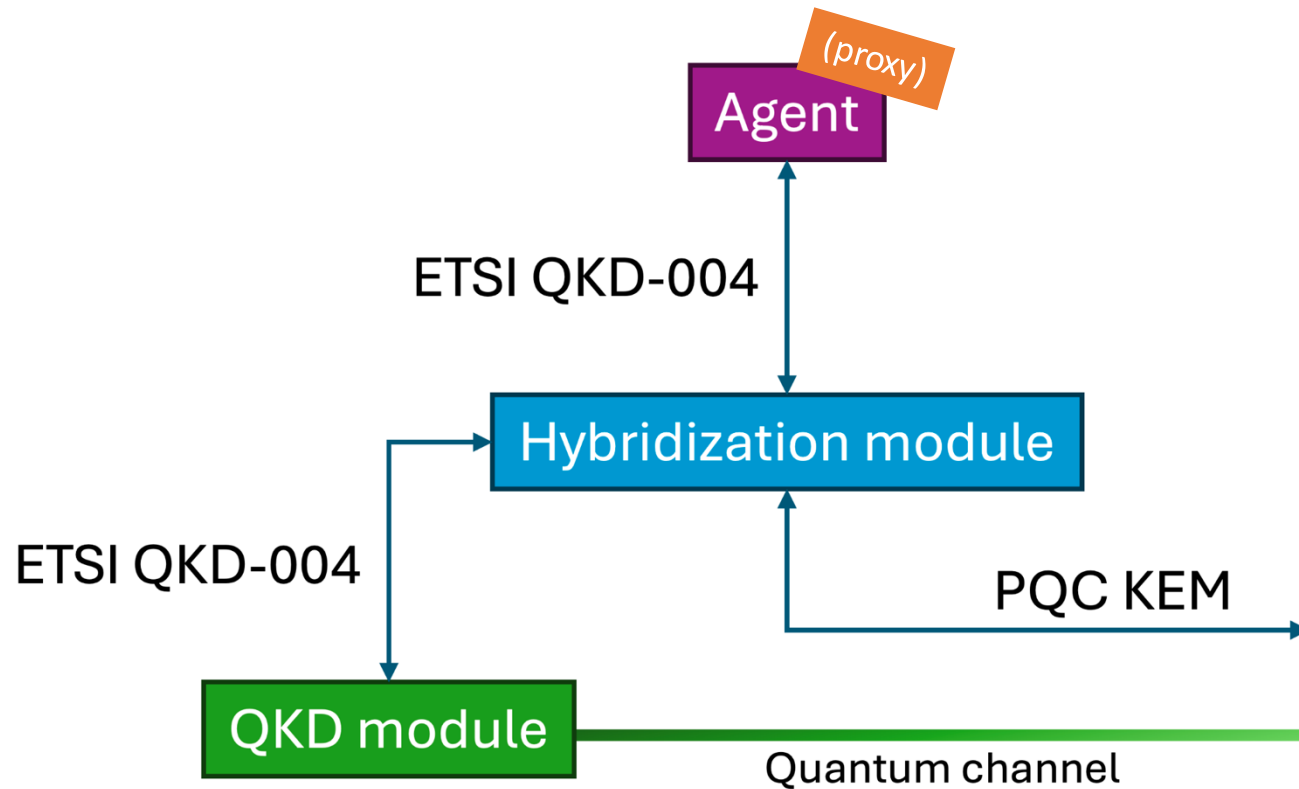
- A key-extraction process:

$$K = T(\text{HMAC-hash}(\text{salt}, \\ K_1 \parallel \dots \parallel K_n \parallel D_1 \parallel \dots \parallel D_m), \text{kLen})$$

- Depending on the method, **different relations among different parameters** such as min-entropy or key length are satisfied for the component and combined keys.
- The combined key **will remain secure as long as at least one of the component keys remains secure**.
- Those methods are **implemented through the hybridization module**.
- Recommended by NIST.

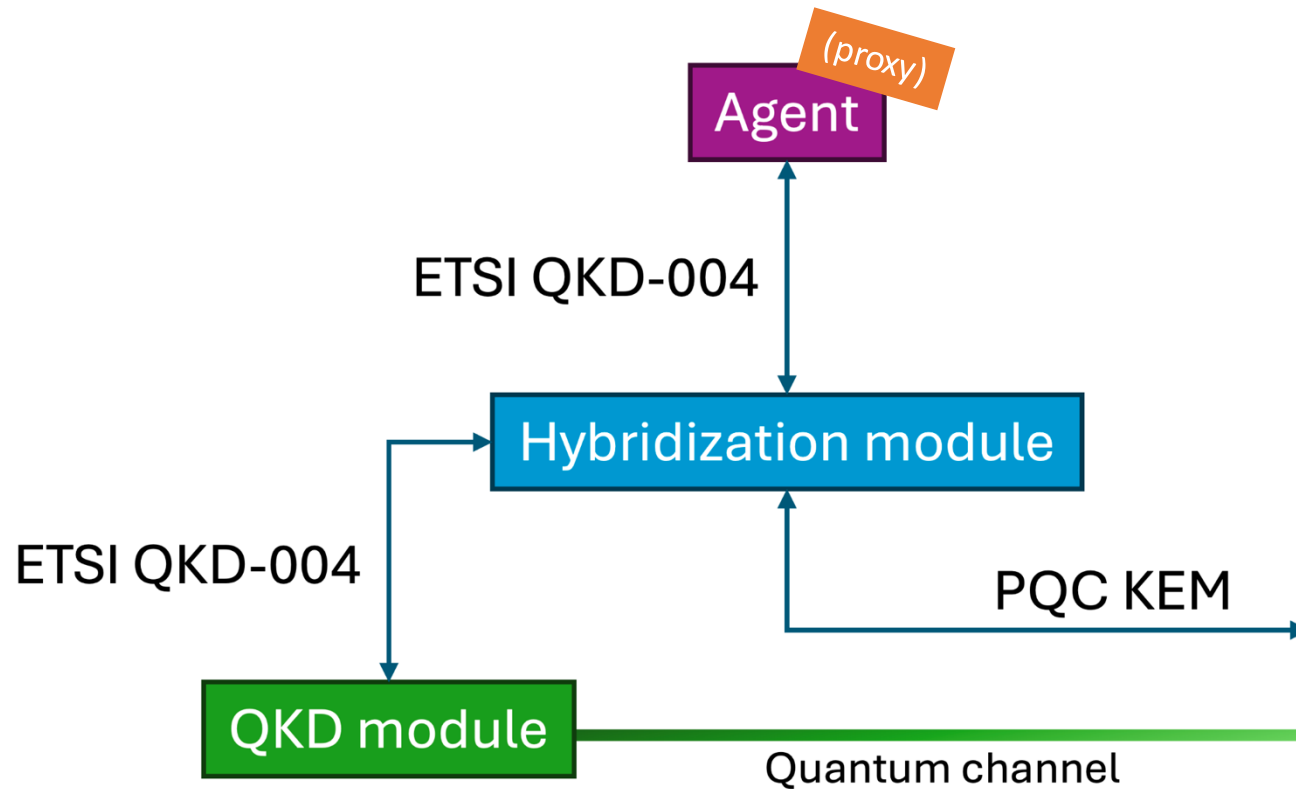
How can we implement this in the SDN model?

Hybridization module



- The module gets key from two sources (PQC and QKD) and **combines** the key to obtain a quantum-resistant hybrid key.
- This is done through a **standardized interfaces** and algorithms (ETSI QKD-004, ML-KEM)
- When the combined key is obtained, **it is sent to the agent** in order to establish the tunnel.
- The hybridization module **manages the key sizes** depending on the hybridization method chosen.
- The module **will deliver key to the agent whenever at least one of the component keys is successfully created.**

Hybridization module

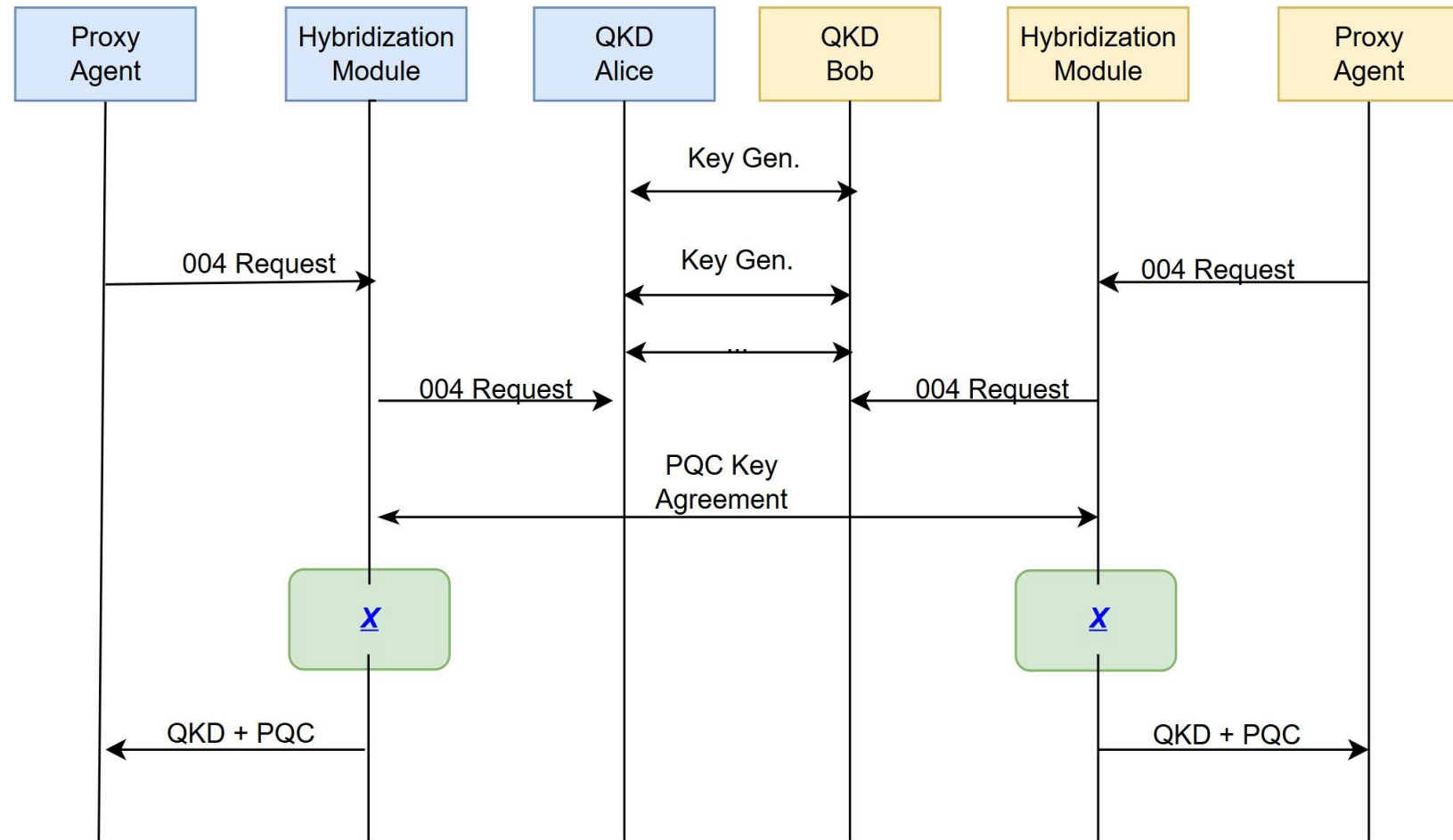


- With this operating mode:
 - The combined key, if generated, will be always at the **maximum level of security**.
 - **Flexibility and continuity of service**. If one of the key sources fails (e.g., eavesdropper on QKD or broken algorithm on PQC), the hybridization module will still be able to create a quantum-resistant hybrid key.
- It is a building block that **enable the implementation of HAKE** algorithms and beyond and **fits perfectly in typical network architectures**.

Hybridization module

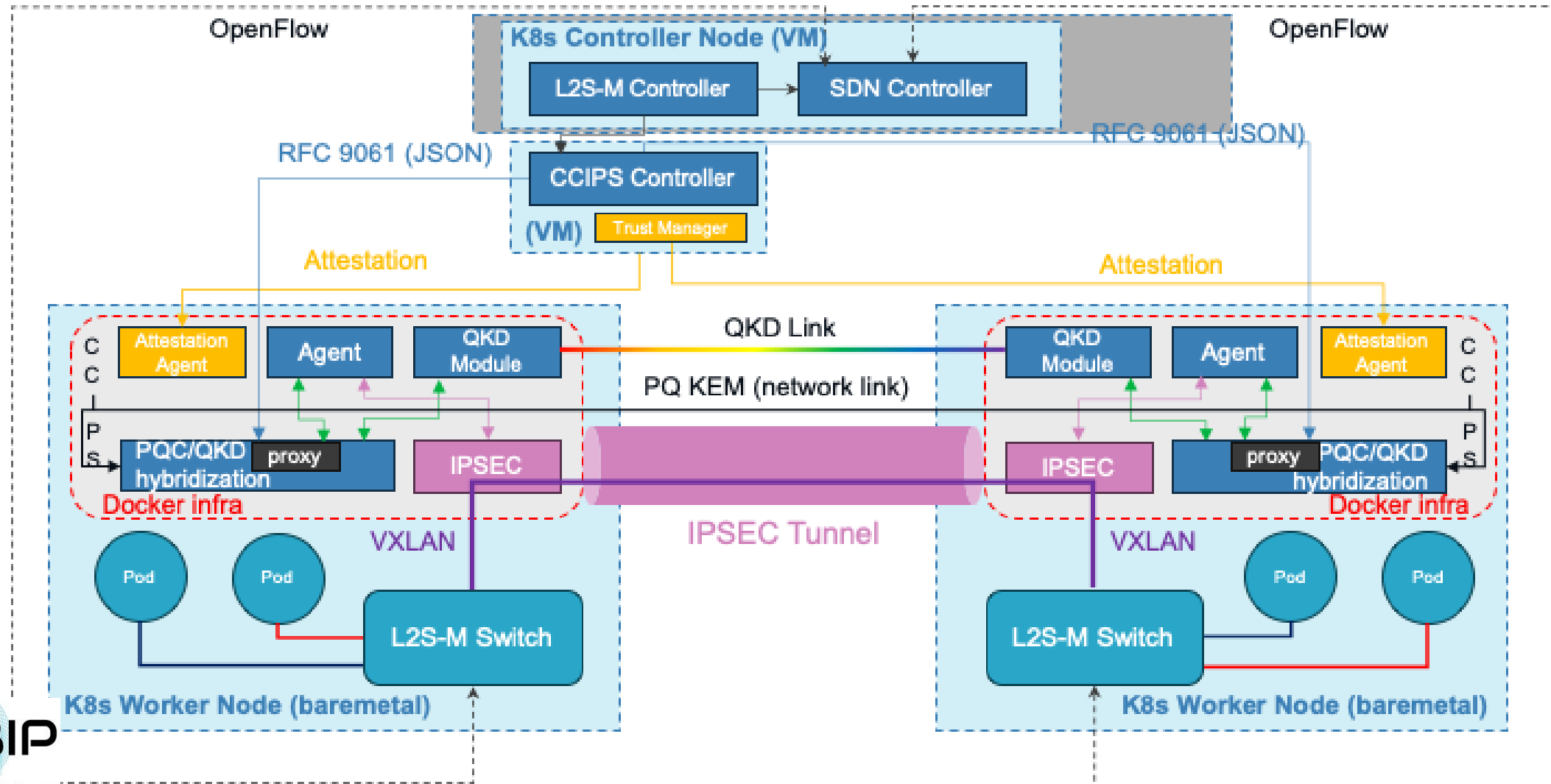
Workflow

The proxy agents request through 004, so the interface is the same as a QKD module. This is good regarding modularity and scalability!



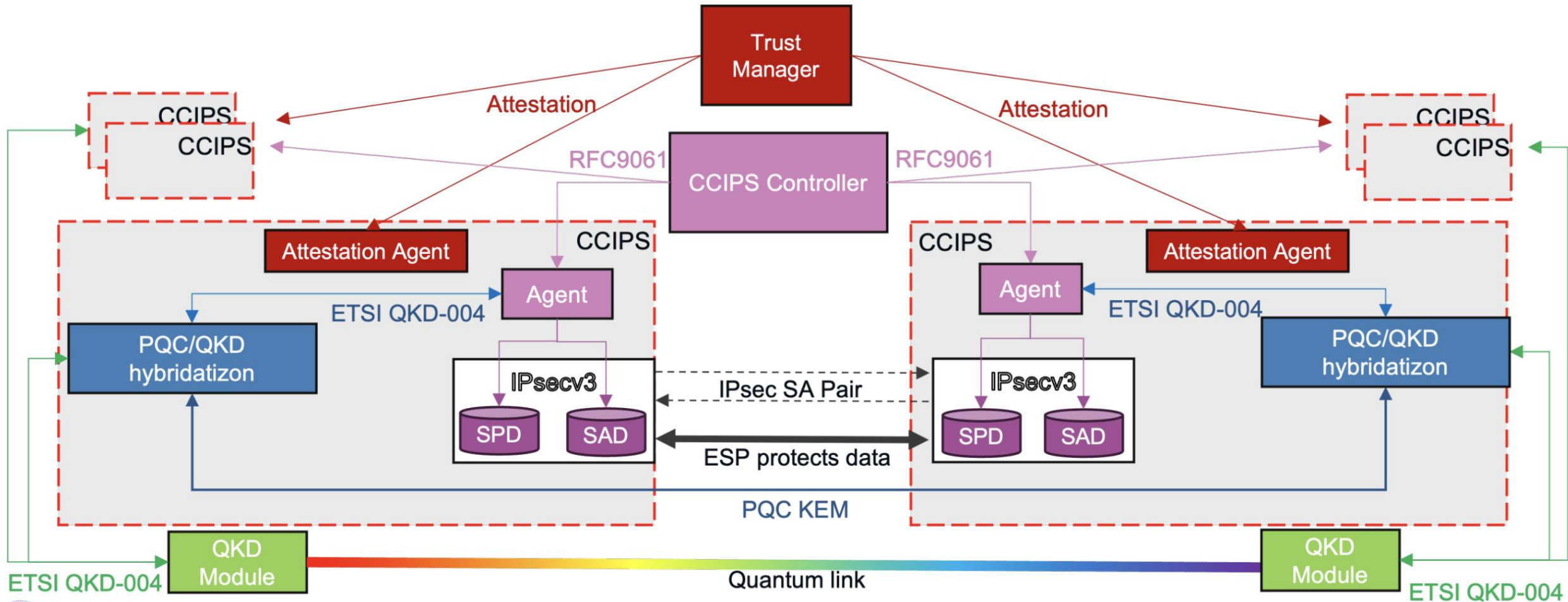
Hybridization module: use case

Single IPsec tunnel establishment



Hybridization module: use case

Whole telco use case



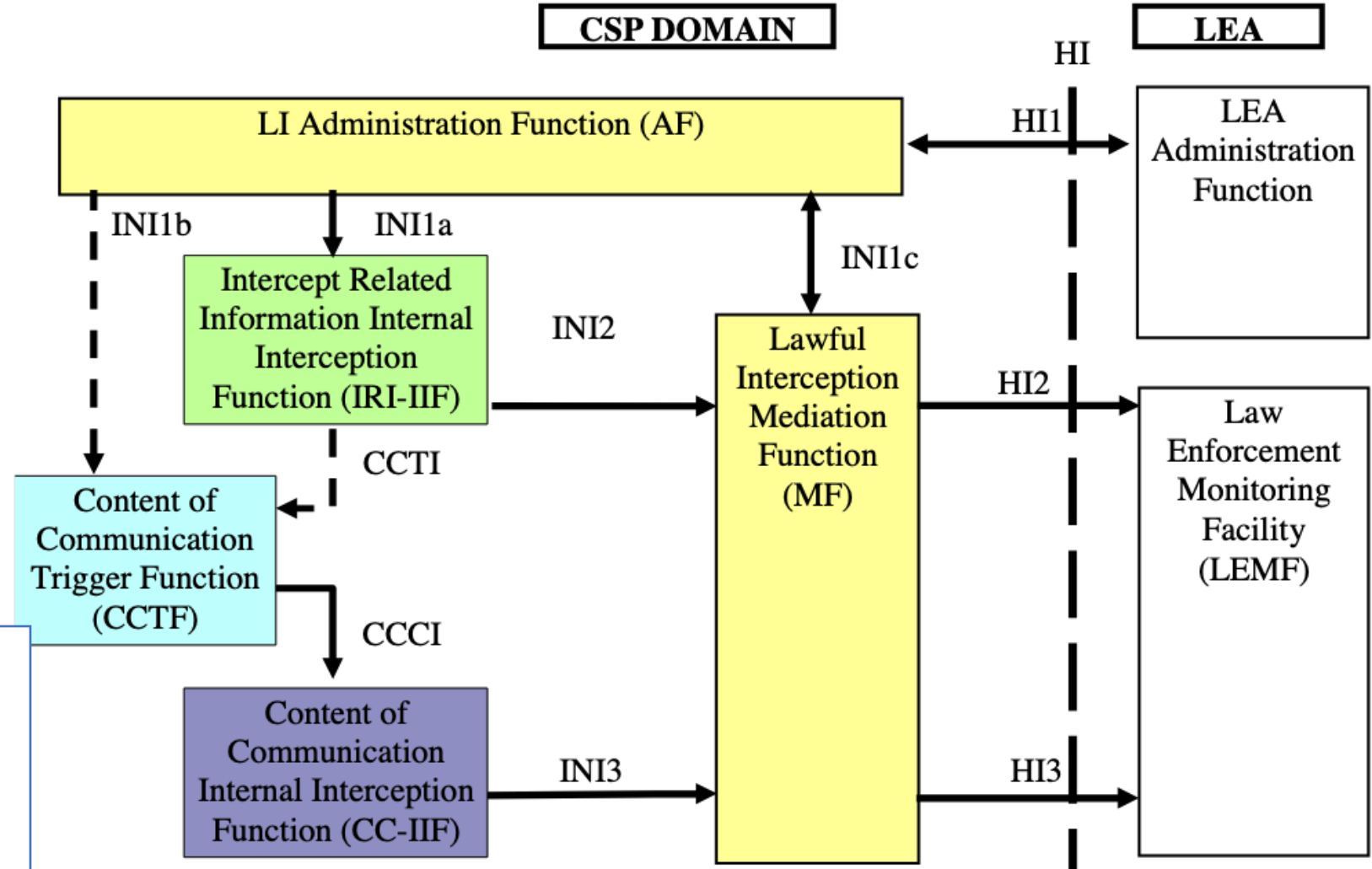
Lawful interception

An example of hybrid (but not hybridized!) quantum network

ETSI TR 102 528 V1.1.1 (2006-10)

Standard LI architecture.

- LEA Administration Function communicates the request through the HI1 interface to the AF.
- AF setup the LI communicating through the INI1 interface to:
 - IRI-IIF, which obtains info about network details.
 - CCTF, which trigger the interception of content.
 - MF, which is the responsible of processing and sending the intercepted info.
- Then, when the target starts a communication:
 - IRI-IIF captures network details and sends them to MF through the INI2 interface.
 - CC-IIF captures the content of the communication and sends it to MF through the INI3 interface.
 - The MF process and sends the network info (HI2) and content (HI3) to the LEMF.



Two different domains, with different securities and policies:

- Communication Service Provider (CSP)
- Law Enforcement Agencies (LEA)

Intercepted data should be protected!

Lawful interception

An example of hybrid (but not hybridized!) quantum network

ETSI TR 102 528 V1.1.1 (2006-10)

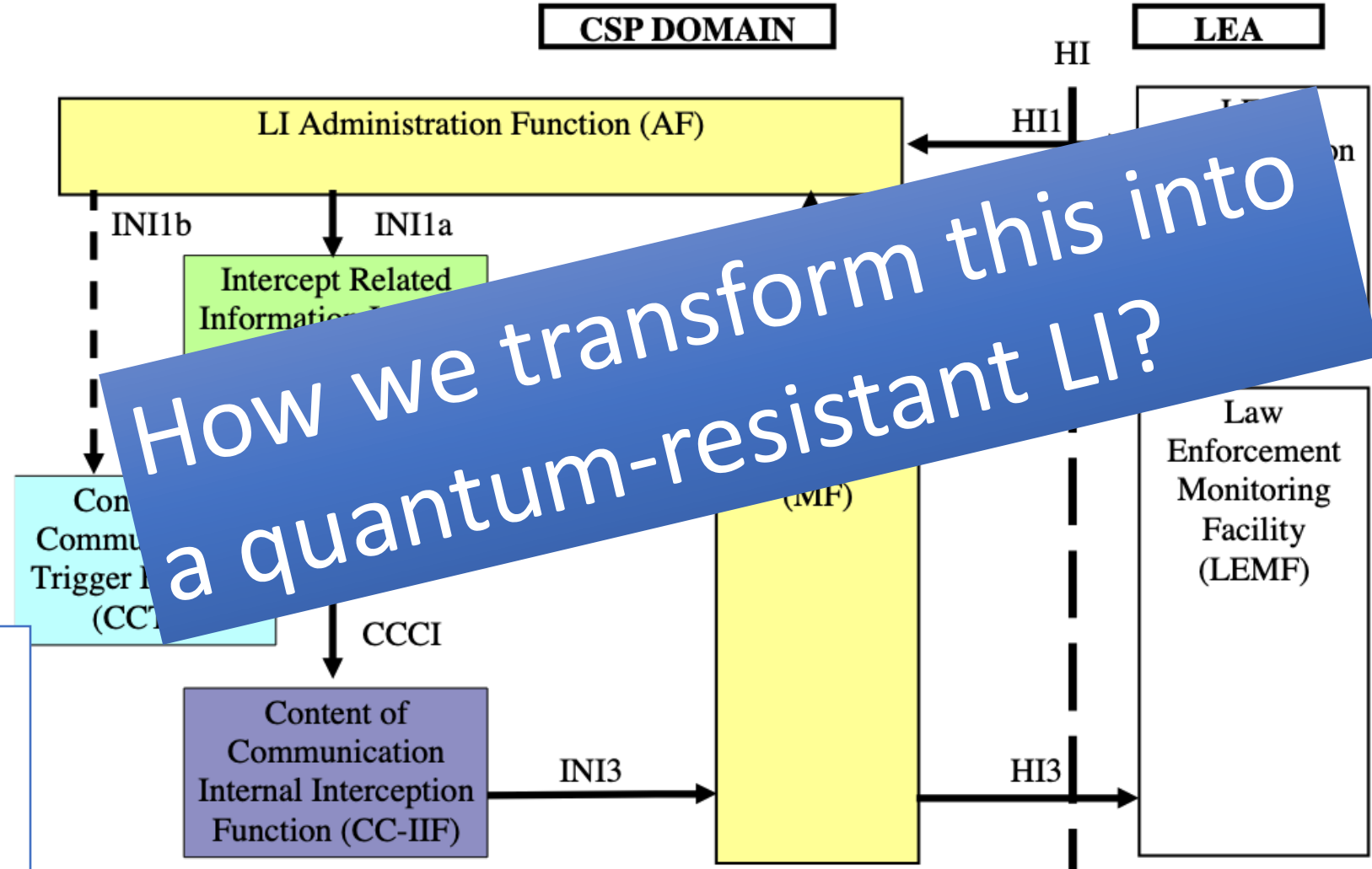
Standard LI architecture.

- LEA Administration Function communicates the request through the HI1 interface to the AF.
- AF setup the LI communicating through the INI1 interface to:
 - IRI-IIF, which obtains info about network details.
 - CCTF, which trigger the interception of content.
 - MF, which is the responsible of processing and sending the intercepted info.
- Then, when the target starts a communication:
 - IRI-IIF captures network details and sends them to MF through the INI2 interface.
 - CC-IIF captures the content of the communication and sends it to MF through the INI3 interface.
 - The MF process and sends the network info (HI2) and content (HI3) to the LEMF.

Two different domains, with different securities and policies:

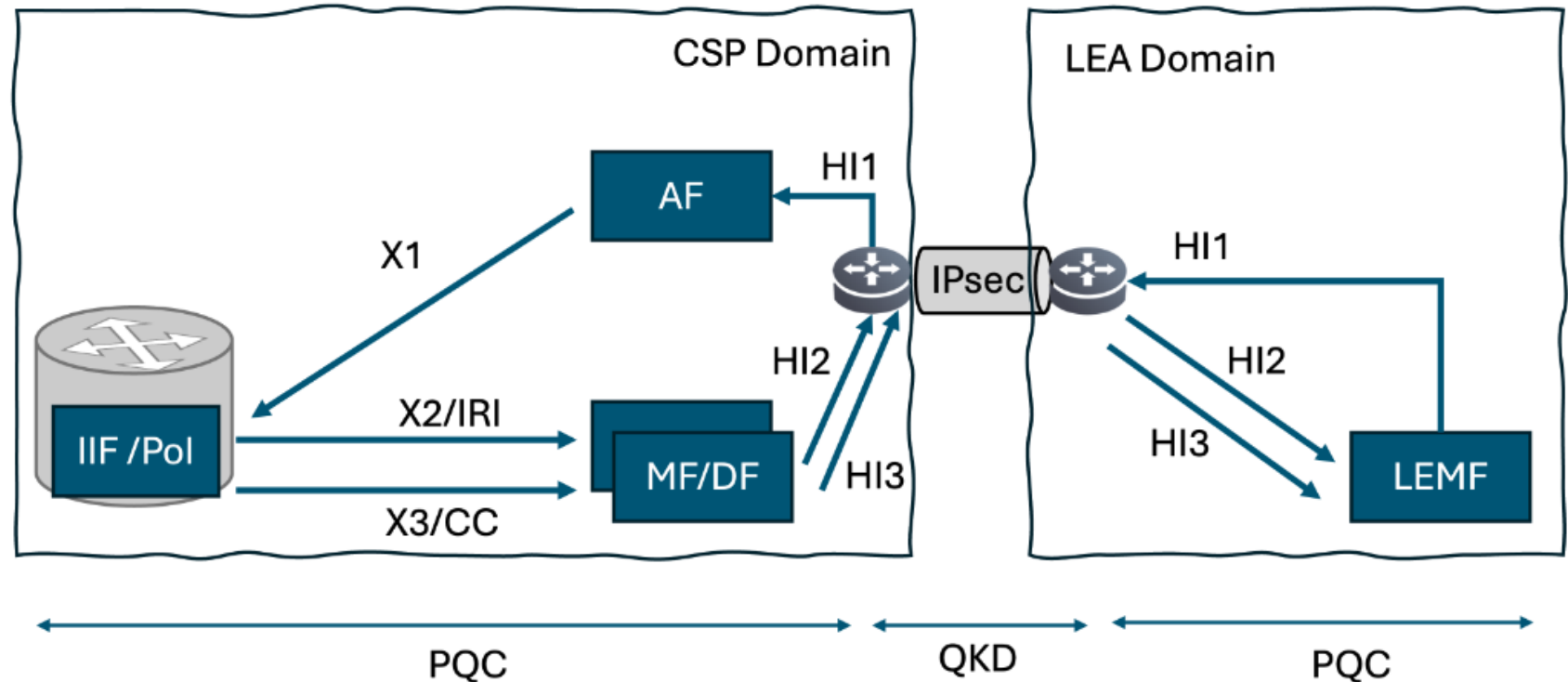
- Communication Service Provider (CSP)
- Law Enforcement Agencies (LEA)

Intercepted data should be protected!



Quantum-resistant scenario:

- The typical approach is to use VPNs and an IPsec tunnel to communicate between the CSP domain and the LEA domain.
- However, the associated IKE protocol is vulnerable to quantum computers!
- The solution is to replace IKE with quantum keys generated through QKD.
- It can be easily integrated to IPsec manufacturers using ETSI 004 or ETSI 014 interfaces for key requests.
- However, this requires dedicated HW and optical links.



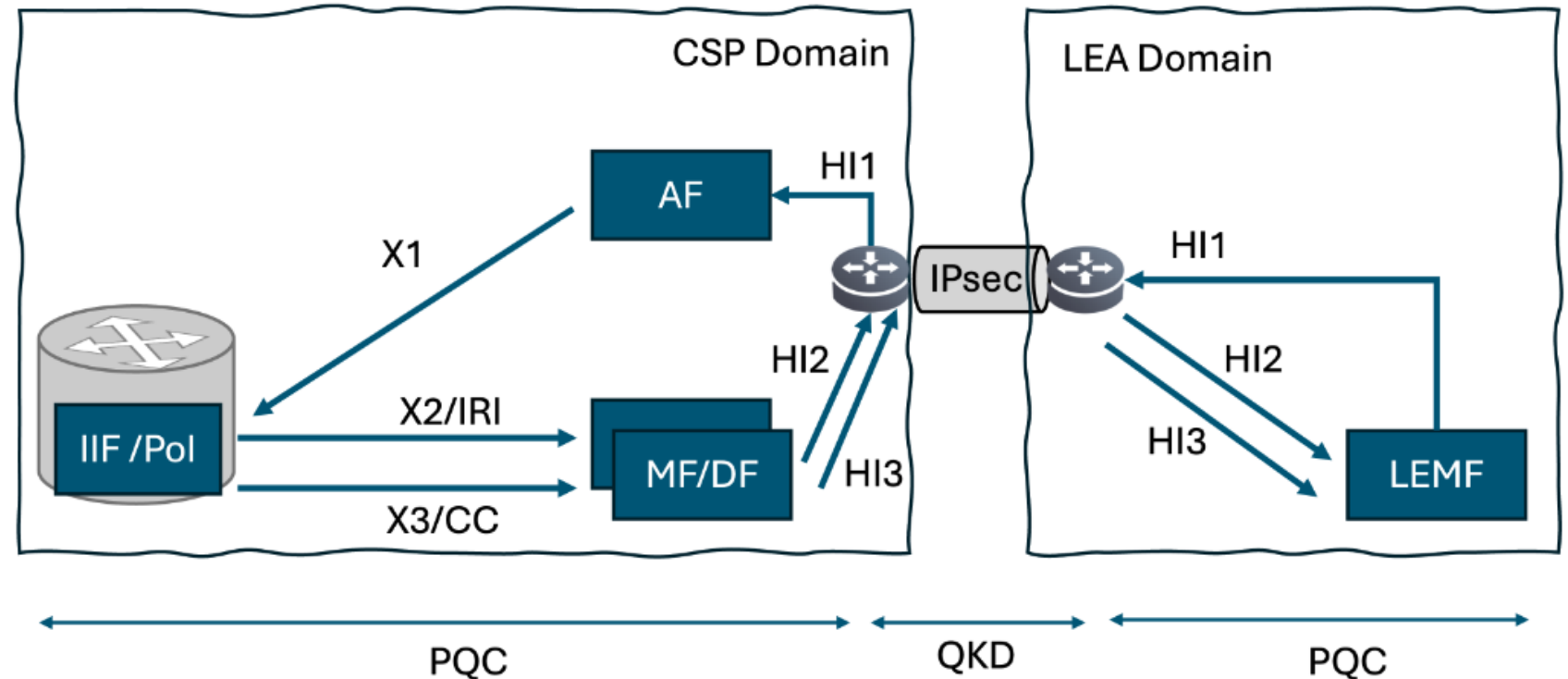
Quantum-Safe Technologies Application to Lawful Interception

Antonio Pastor (Telefonica Innovacion Digital), Laura Dominguez (Telefonica Innovacion Digital), Diego Lopez (Telefonica Innovacion Digital), Juan P. Brito (Universidad Politecnica de Madrid), Javier Faba (Universidad Politecnica de Madrid) and Laura Ortiz (Universidad Politecnica de Madrid)

Quantum-resistant scenario:

Why this use of PQC and QKD?

- In practical scenarios there will be a large number of complex Points of Interception (PoI), and the interfaces X1, X2 and X3 are expanded into multiple sub-interfaces, making the implementation of QKD very costly
- Since the implementation of PQC is simpler than QKD and doesn't require expensive dedicated HW, PQC is preferred.
- Hence, QKD can be used to provide a high quantum-protection between domains.



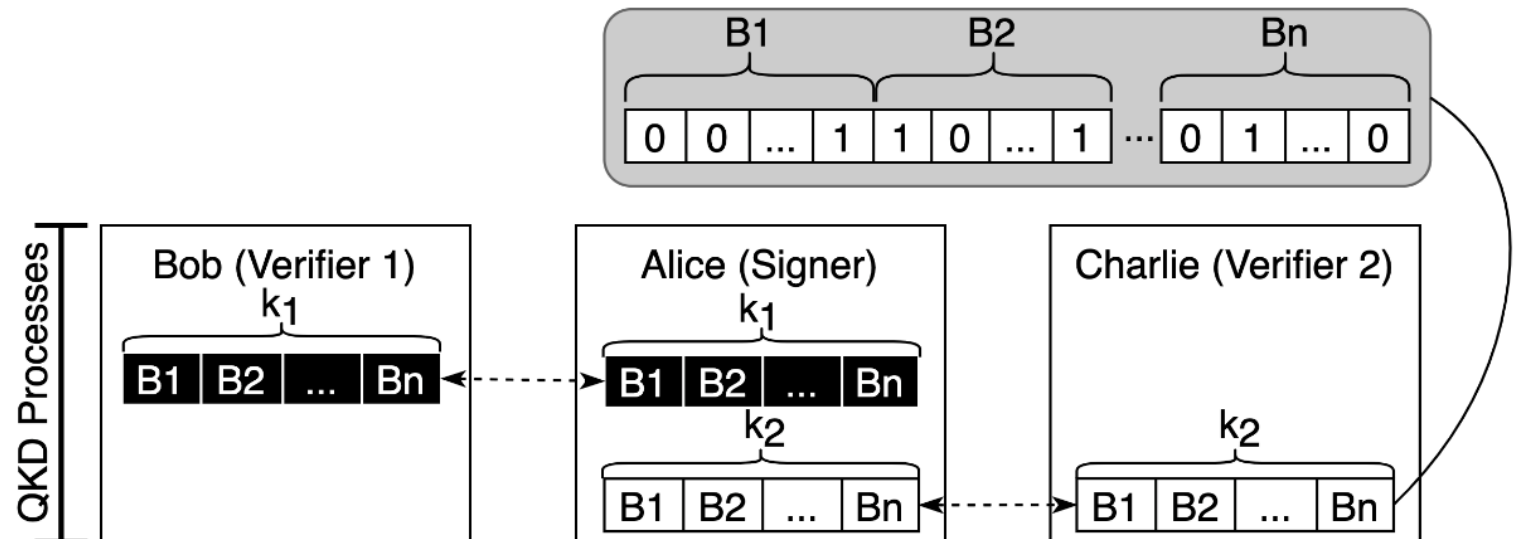
Quantum-Safe Technologies Application to Lawful Interception

Antonio Pastor (Telefonica Innovacion Digital), Laura Dominguez (Telefonica Innovacion Digital), Diego Lopez (Telefonica Innovacion Digital), Juan P. Brito (Universidad Politecnica de Madrid), Javier Faba (Universidad Politecnica de Madrid) and Laura Ortiz (Universidad Politecnica de Madrid)

We can use QKD to more than cyphering: **Quantum Digital Signature (Q-DS)**

Q-DS has two phases: distribution phase and messaging phase

Distribution phase: Alice establishes secret symmetric keys through quantum key distribution (QKD) processes with all possible receivers. After that, the receivers exchange between them random elements of those keys. These QKD-generated keys are the foundation of the security in the protocol, since it allows us to remove the asymmetric vulnerable elements of a digital signature and replace them with ITS keys.

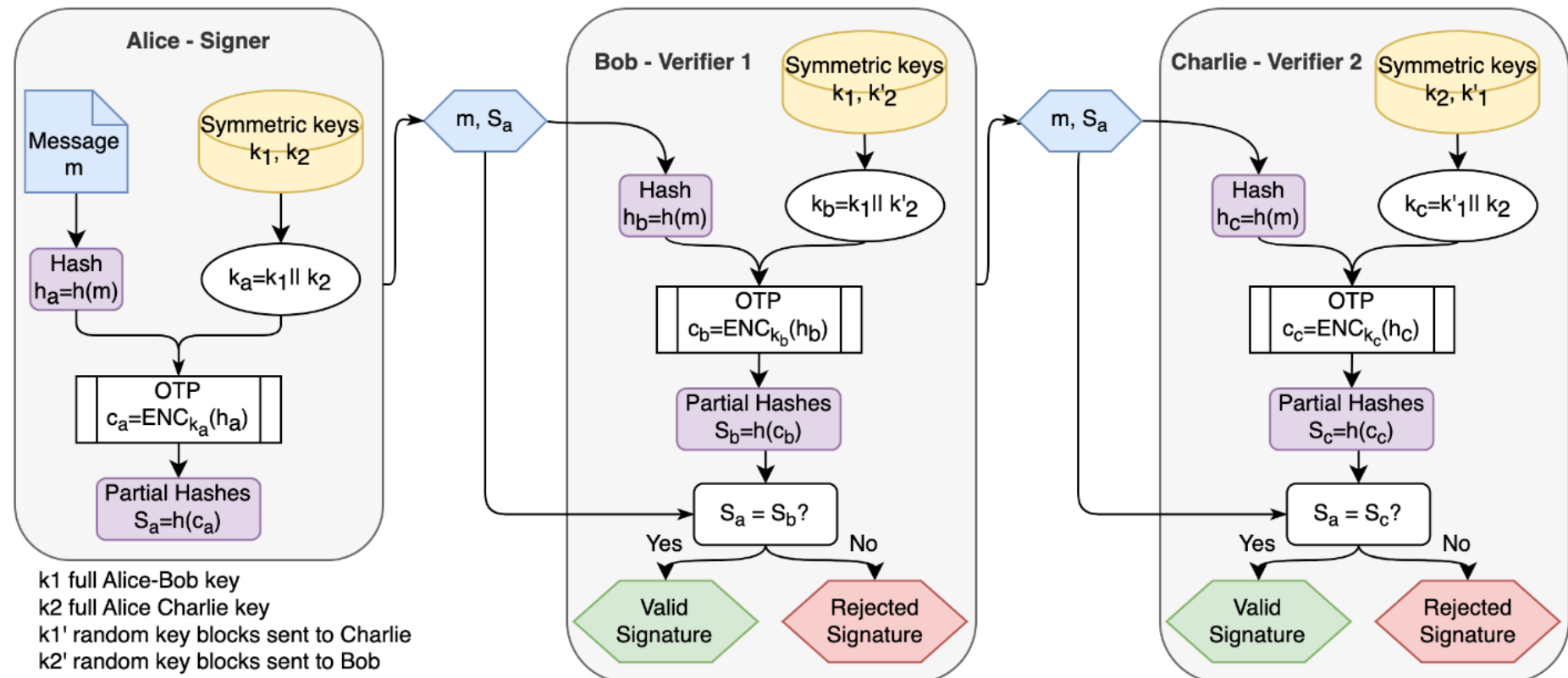


We can use QKD to more than cyphering: **Quantum Digital Signature (Q-DS)**

Q-DS has two phases: distribution phase and messaging phase

Messaging phase:

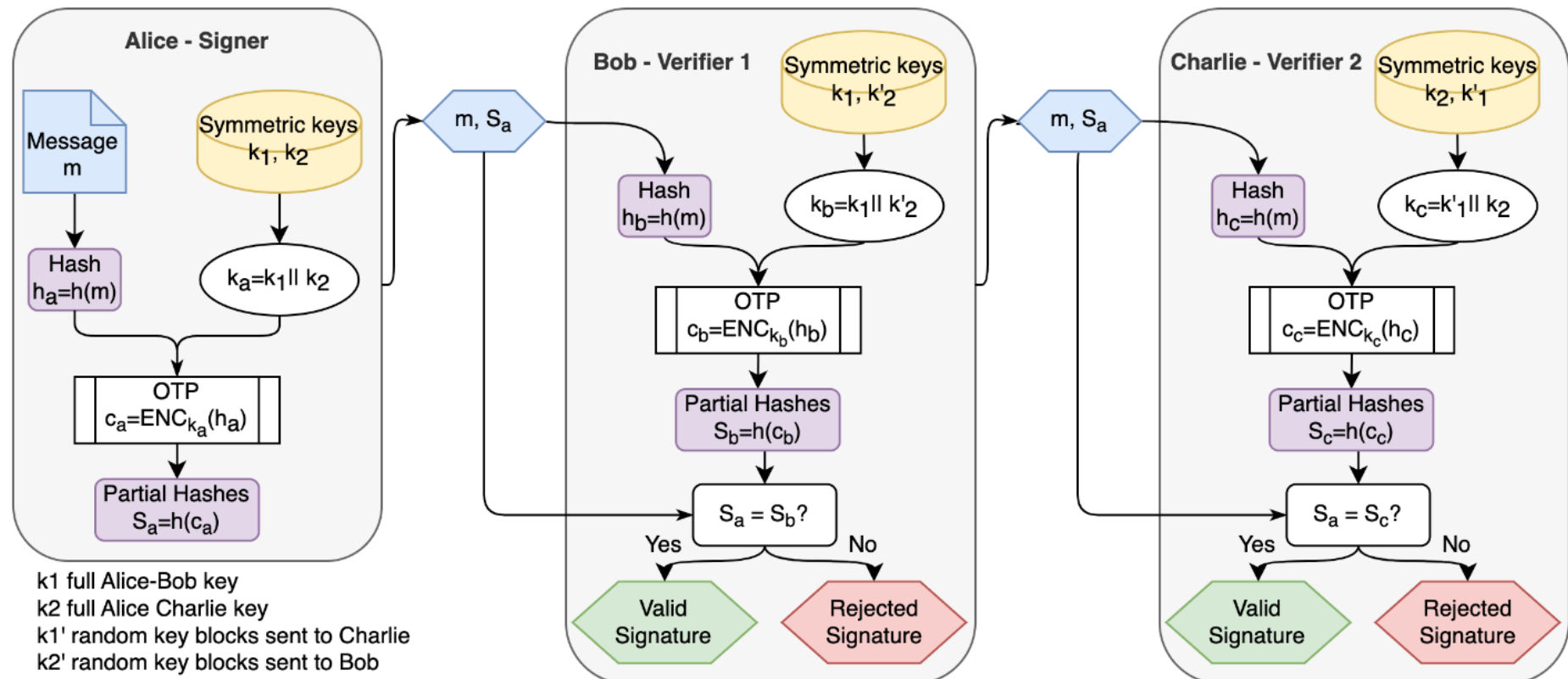
Alice generates the digital signature for a given message and sends it to the recipients who verify the validity of both the message and the signature. This second phase involves completely classical procedures and can be carried out some time after the first phase.



We can use QKD to more than cyphering: **Quantum Digital Signature (Q-DS)**

Q-DS has two phases: distribution phase and messaging phase

- The process ends with Charlie (if Bob accepted the signature). If Charlie rejects, the signature nor the message is not valid.
- Although the cryptographic material is symmetric, we create an asymmetry through the fact that there are two verifiers. Hence, it is possible to use QKD material to DS!
- Of course, this signature has all the desired properties: authenticity, integrity and non-repudiation.
- We can use hybrid key to perform a hybrid DS!



Coherent One-Way (COW) QKD



UNIVERSIDAD
POLITÉCNICA
DE MADRID



We have seen ‘hybridization’ and ‘hybrid’ use cases, and the use of QKD material to perform Q-DS. But...
Is it possible to run beyond-QKD protocols in our QKD network **with commercial QKD devices?**

Coherent One-Way (COW) QKD

Faba, J., Romero, J. J., Ortiz, L., & Ayuso, V. M. (2025). Quantum Oblivious Transfer through Coherent-One-Way Quantum-Key-Distribution. Proceedings of the 2nd Workshop on Quantum Networks and Distributed Quantum Computing, 60–62. <https://doi.org/10.1145/3749096.3750034>

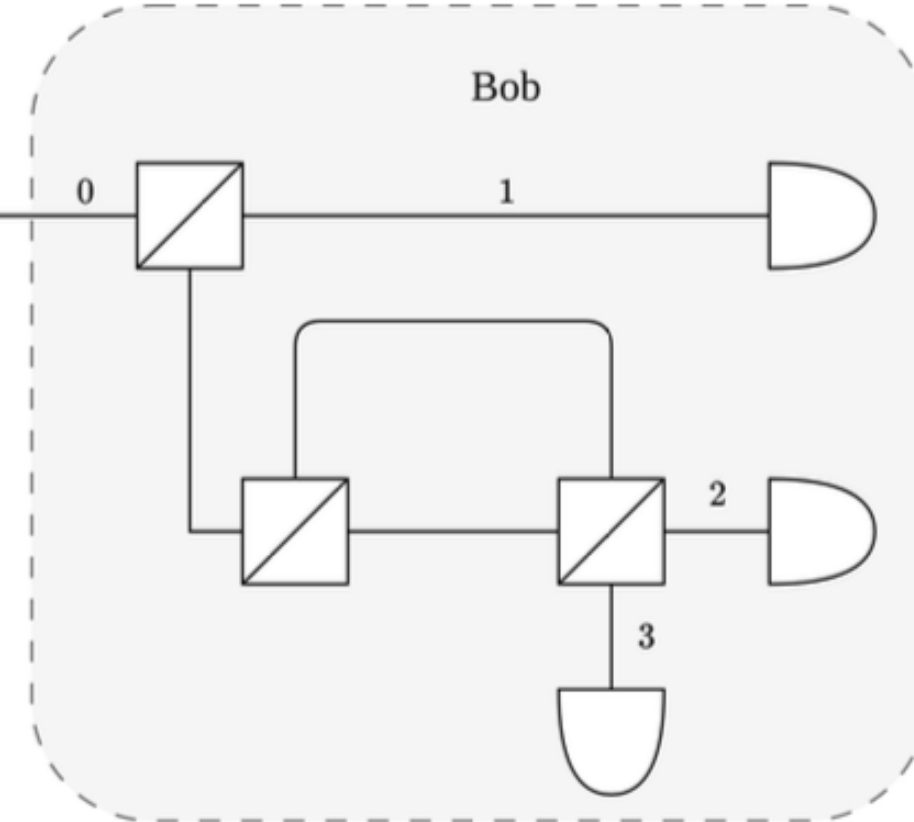
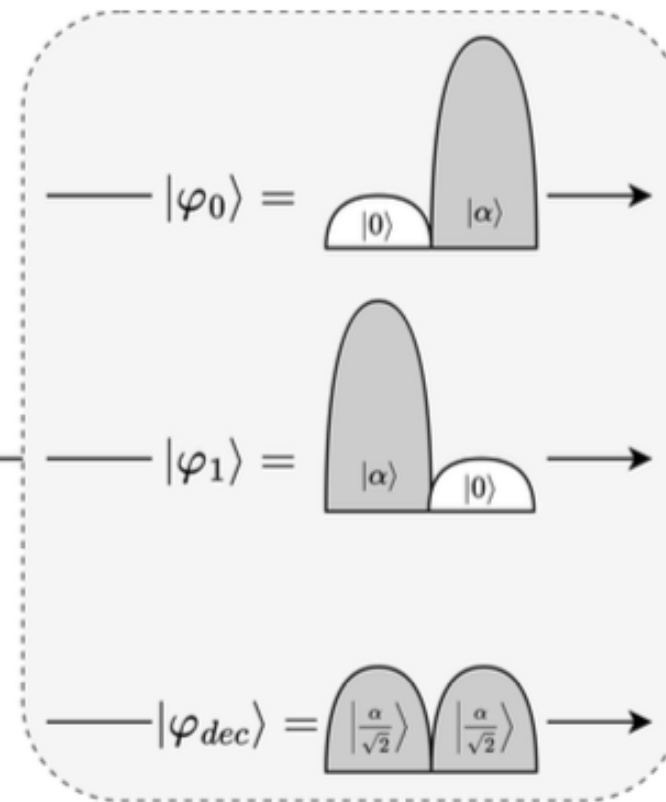
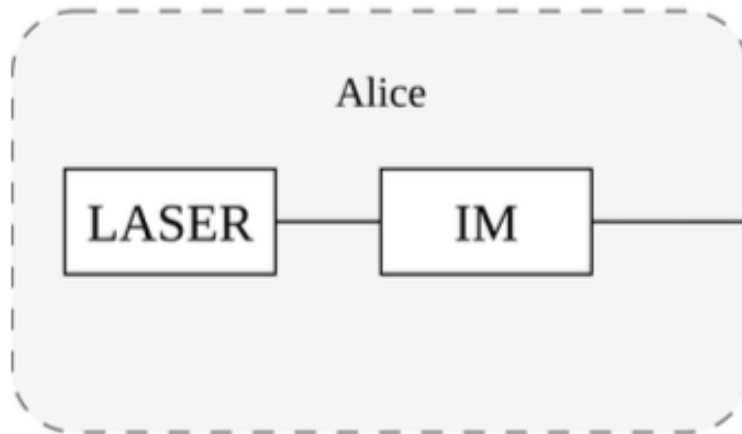


POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID



GCC



- Qubit states: time-bins of **weak** coherent states.
- Only three states:

$$|0\rangle \equiv |\alpha, 0\rangle \quad |1\rangle \equiv |0, \alpha\rangle$$

$$|\text{decoy}\rangle \equiv \left| \frac{\alpha}{\sqrt{2}}, \frac{\alpha}{\sqrt{2}} \right\rangle$$

- The first beam splitter divides the light among the data line, where photons are detected in the early and late states, and the monitoring line, where the detection is done after an unbalanced MZ interferometer.
- The key is derived from data extracted from data line, while data in monitoring line is used to check security.

Oblivious Transfer

Rabin's Oblivious Transfer:

- Alice sends a bit to Bob
- Bob **learns** the message with **probability p**.
- Alice **ignores** if Bob has learnt the message.

Quantum Oblivious Transfer (QOT):

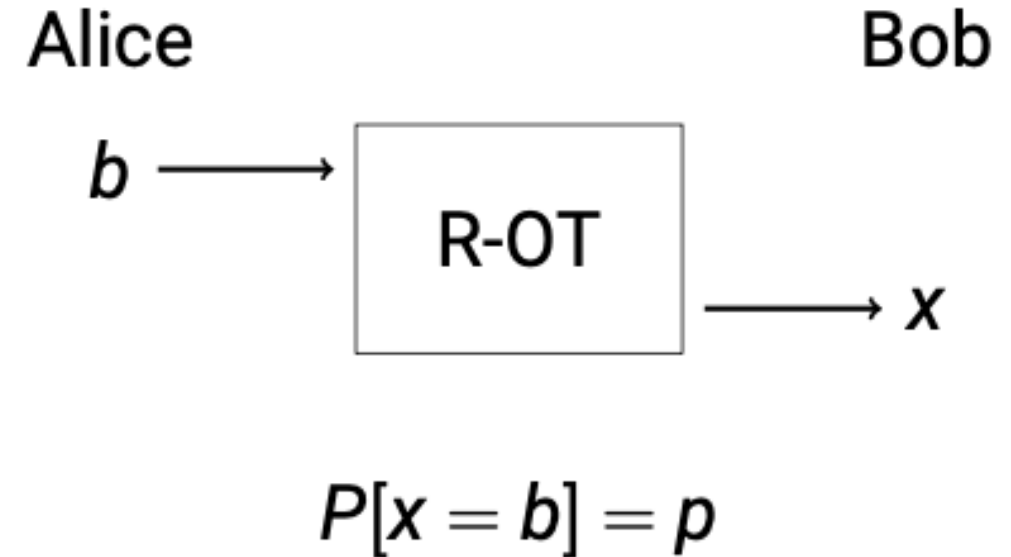
- It is possible due to the existence of **non-orthogonal states**.
- Alice sends one of the two non-orthogonal states to Bob.

$$\langle \psi_0 | \psi_1 \rangle \neq 0$$

- Bob performs unambiguous state discrimination through three-operator POVM.
- Bob will obtain an inconclusive probability (assuming real overlap).

$$p? = \langle \psi_0 | \psi_1 \rangle$$

- Since the requirement for QOT is non-orthogonality, **it seems feasible to use the COW setup to execute QOT**



Using COW experimental setup to perform QOT will allow COW QKD devices to be leveraged for oblivious key generation!

Our proposal (work in progress)

The idea is to use the early and decoy states to encode Alice's message bit:

$$a_0 = \sqrt{T}a_1 - \sqrt{\frac{1-T}{4}}(b_2 + b_3 + a_2 - a_3)$$

$$b_0 = \sqrt{T}b_1 - \sqrt{\frac{1-T}{4}}(c_2 + c_3 + b_2 - b_3)$$

a, b and c stand for early, late or double-late time-bins.

Since the coherent states are **weak**

$$|\text{early}\rangle \approx e^{-\frac{\mu}{2}} (\mathbb{I} + \alpha a_0^\dagger) |0\rangle$$

$$|\text{decoy}\rangle \approx e^{-\frac{\mu}{2}} \left[\mathbb{I} + \frac{\alpha}{\sqrt{2}} (a_0^\dagger + b_0^\dagger) \right] |0\rangle$$

If we combine the equations, we can compute the QOT probabilities:

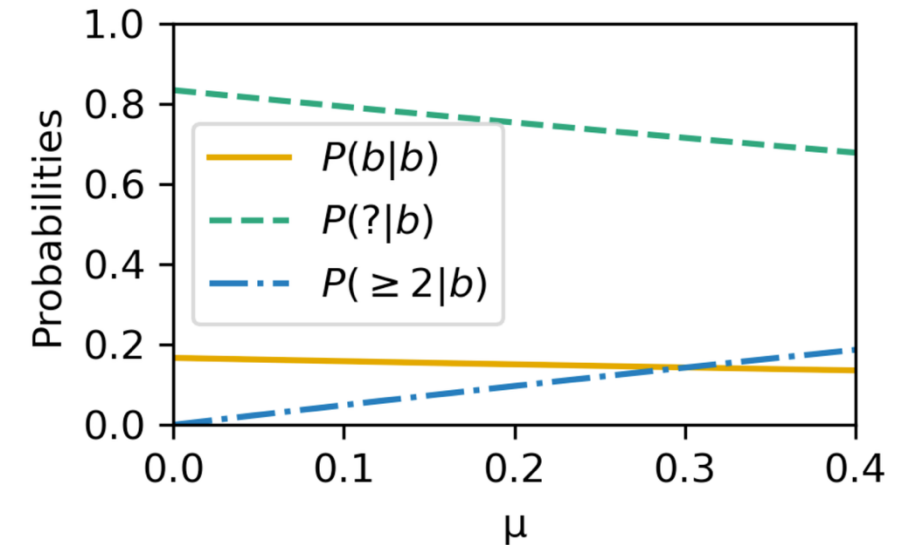
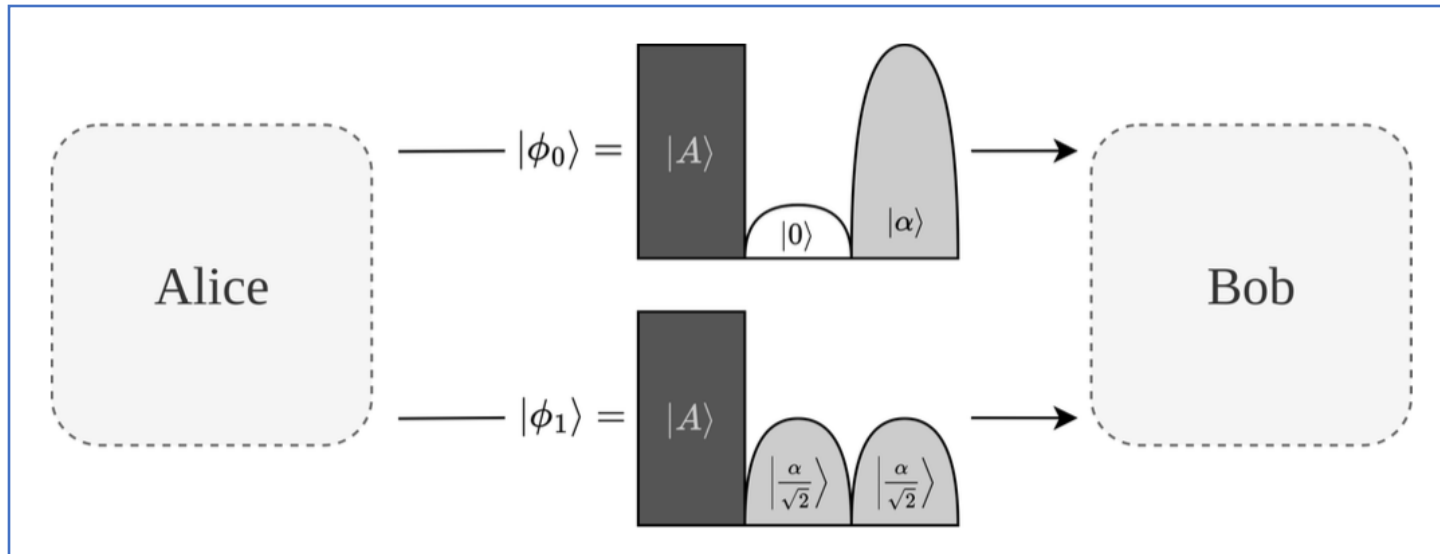
$$P(0|0) = \frac{1-T}{4(1-e^{-\mu})} \mu e^{-\mu} \quad P(1|1) = \frac{T}{2(1-e^{-\mu})} \mu e^{-\mu}$$

$$P(?|0) = \frac{T+3}{4(1-e^{-\mu})} \mu e^{-\mu} \quad P(?|1) = \frac{2-T}{2(1-e^{-\mu})} \mu e^{-\mu}$$

$$P(\geq 2|b) = 1 - \frac{\mu e^{-\mu}}{1-e^{-\mu}}$$

- The vacuum has been discarded from the possible events that Bob can measure. This can be done by simply ignoring the time bins where all single-photon detectors remained without a detection event.
- A bright pulse is needed in the double-late time-bin so Bob cannot obtain information

Our proposal (work in progress)



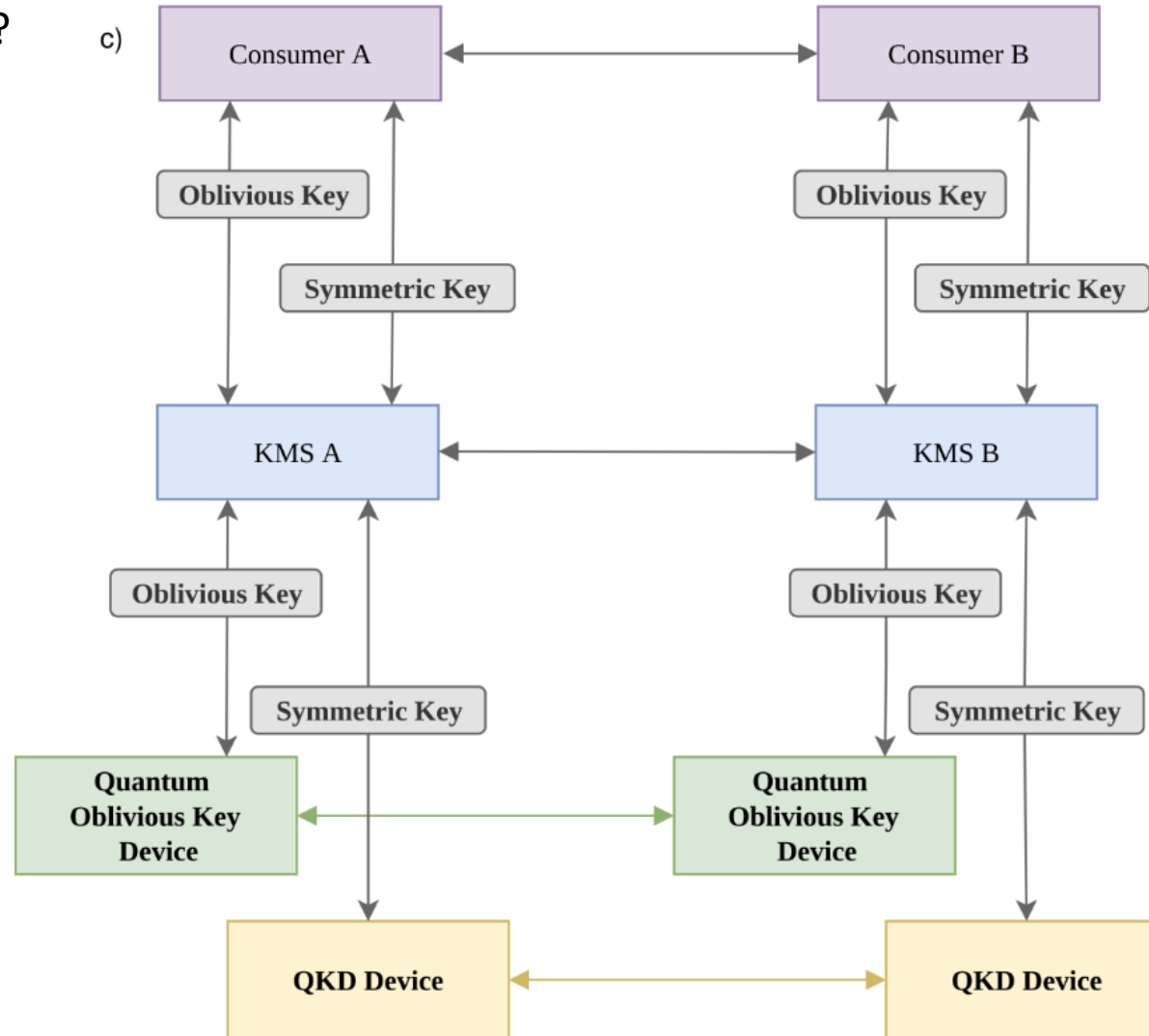
- Alice encodes the message b preparing the corresponding state.
- Clicks on late-time bin allow Bob to decode the message: if line 1 clicks, he decodes a 1 and if line 2 clicks, he decodes a 0.
- The bright pulse is used to prevent Bob from obtaining information in the double-late time-bin.

Next steps:

- Analyse the need for empty pulses between signals
- Analyse the effectiveness of unambiguous state discrimination attacks and possible countermeasures.
- Analyse the need of bit-commitment phase.

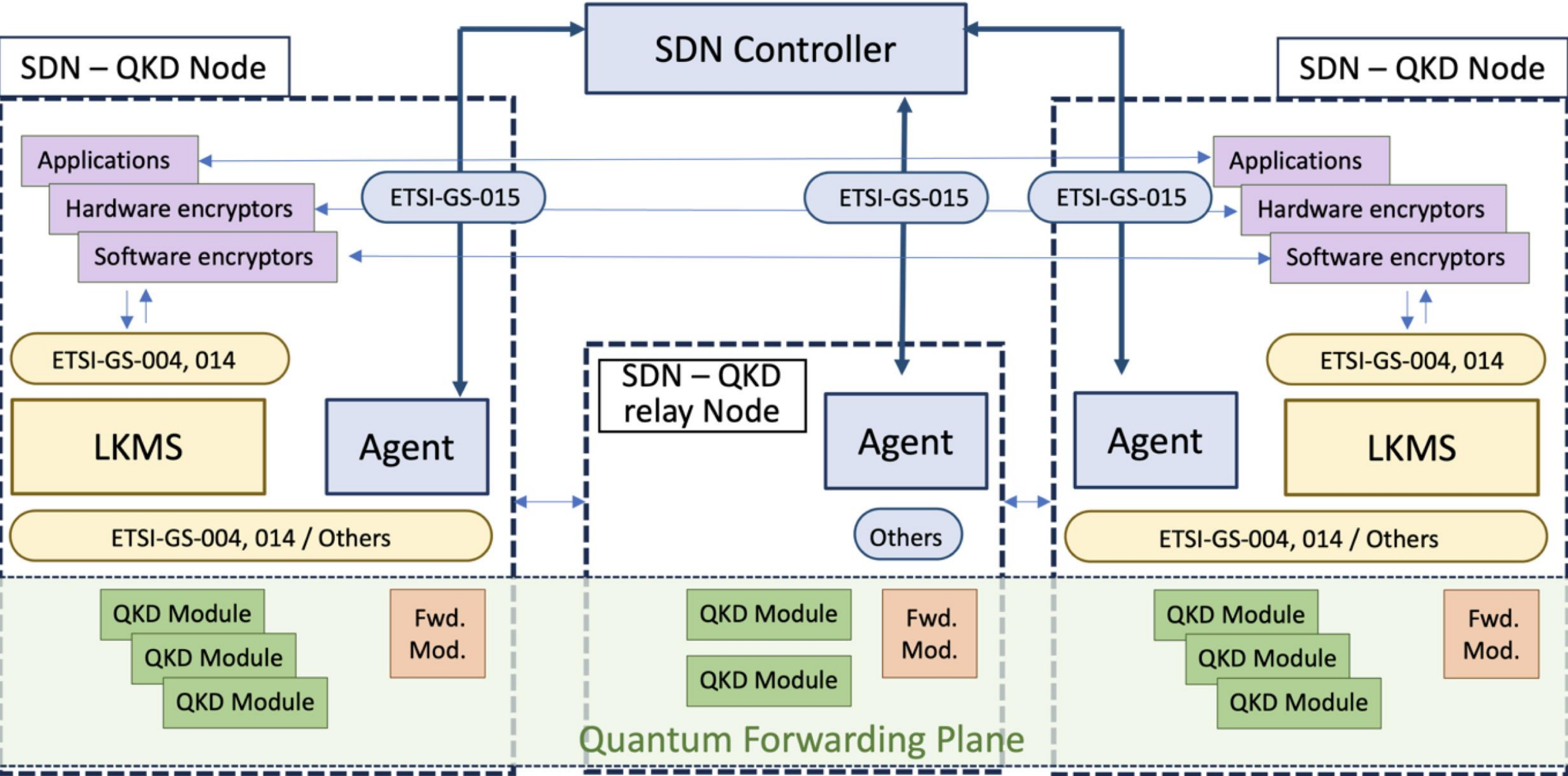
Integrating OT in SDN

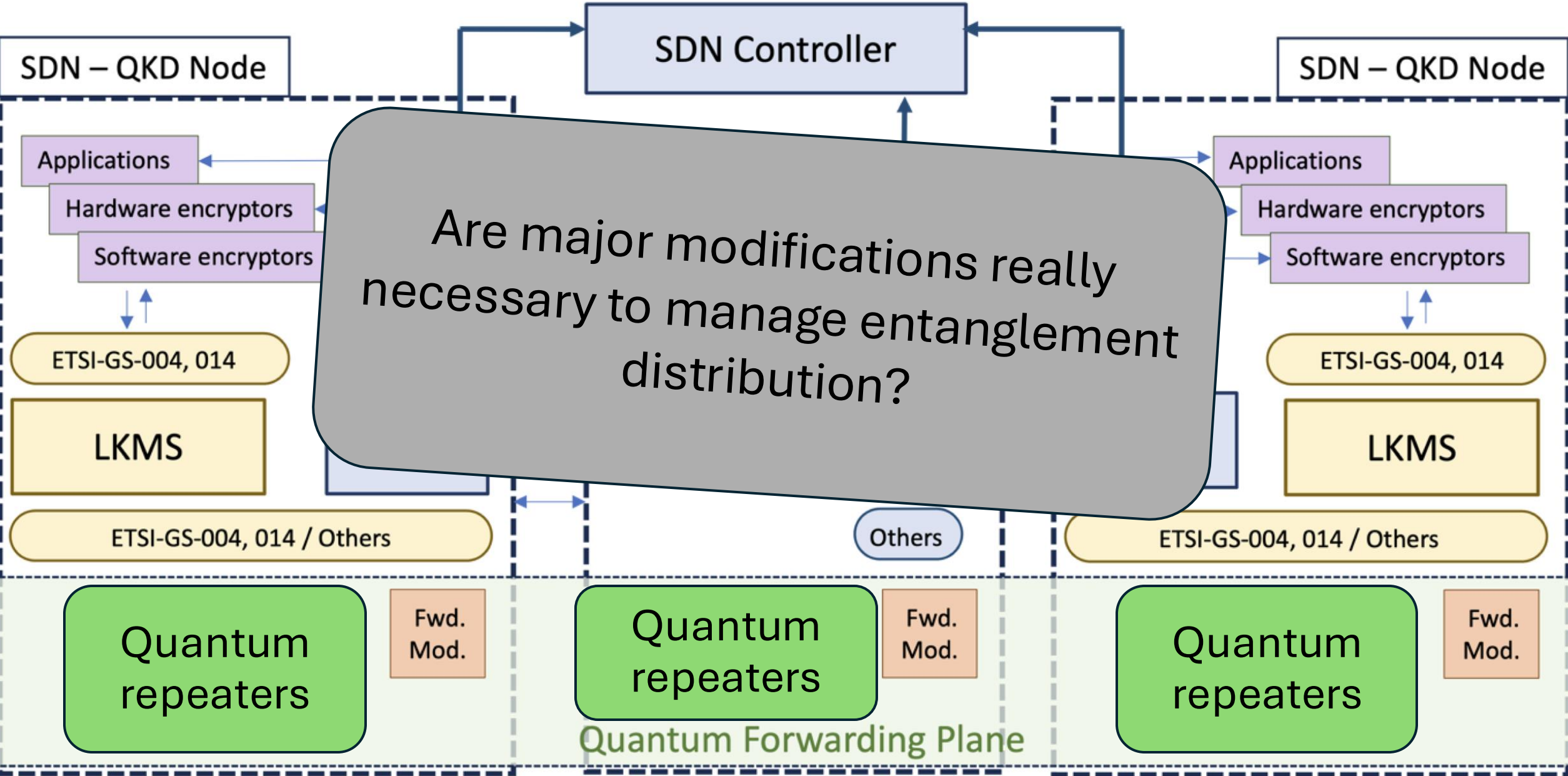
Ok but how oblivious key can be integrated in the architecture?



We have seen ‘hybridization’ and ‘hybrid’ use cases, and the use of QKD material to perform Q-DS. Also, it seems feasible to run beyond-QKD protocols with commercial devices...

Can we integrate entanglement distribution?





- For a quantum internet network, the resource to be distributed across the network is entanglement.
- Due to the non-deterministic and inefficient generation of entanglement, distributing entanglement with quantum repeaters is equivalent to distributing time windows among the network nodes.
- *This is very similar to distribute keys... right?*
We don't know...
- What modifications should be done in the SDN-QKD architecture to accomodate entanglement generation, quantum repeaters, quantum processing units...?

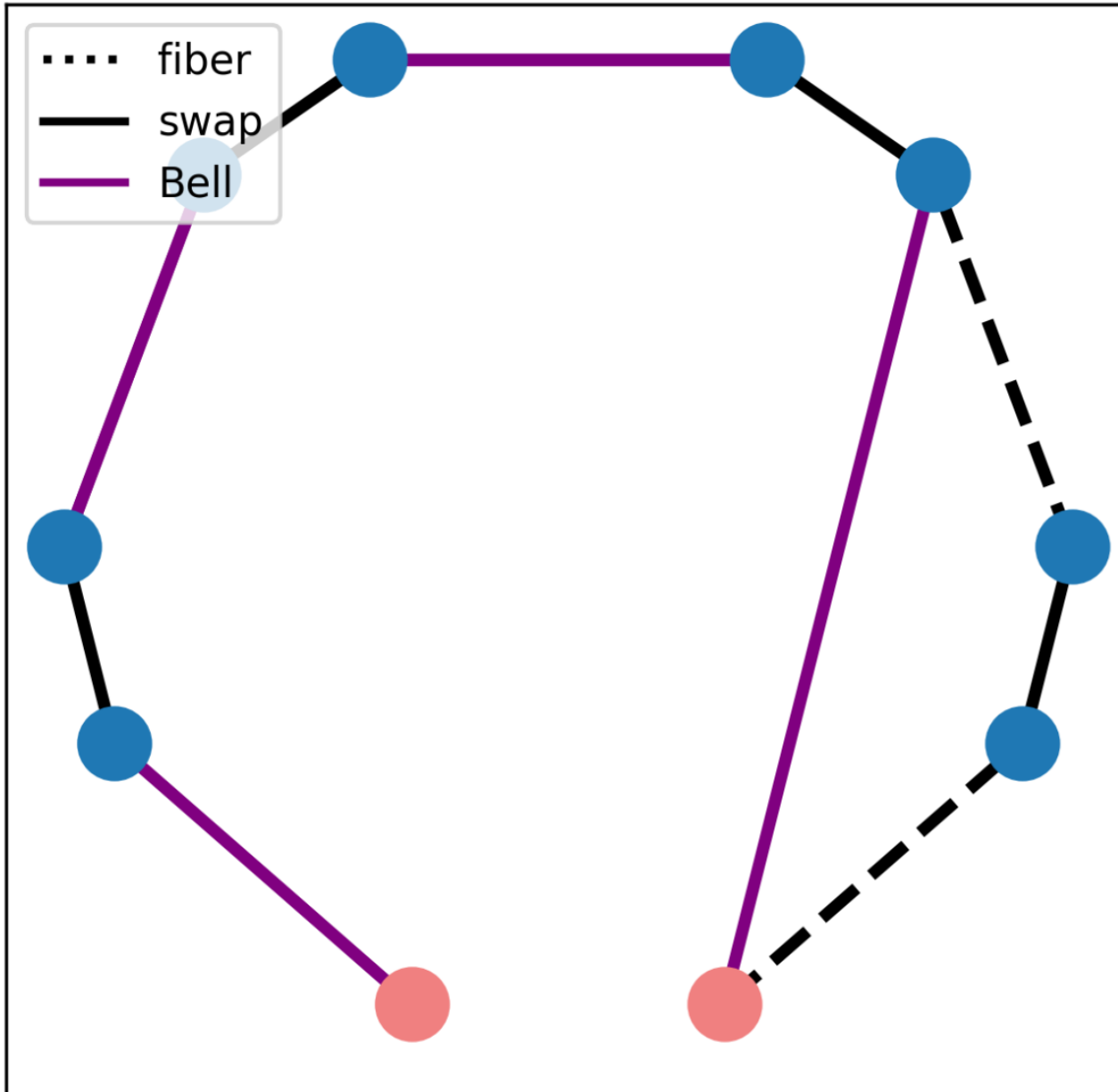
However, from a practical point of view...

- Quantum internet is presented as an improvement over the quantum networks we know so far, but... is that really true?
- Although in theory the quantum internet has the capacity to implement the functionalities of current networks and many more, the reality is very different due to technological limitations.
- The efficiency of these functionalities will likely be much lower compared to the efficiency of current networks... which is why it makes sense for current QKD networks and future quantum internet networks to COEXIST.

- Quantum network
- **QKD network:**
better performance and security
- **Quantum internet:**
better connectivity and new functionalities
- Although the functions are different due to the different resources used, it is very important to work on the development of quantum networks that can coexist with classical networks.
- The efficiency of quantum networks is lower compared to the efficiency of current QKD networks. It makes sense for quantum networks to COEXIST.

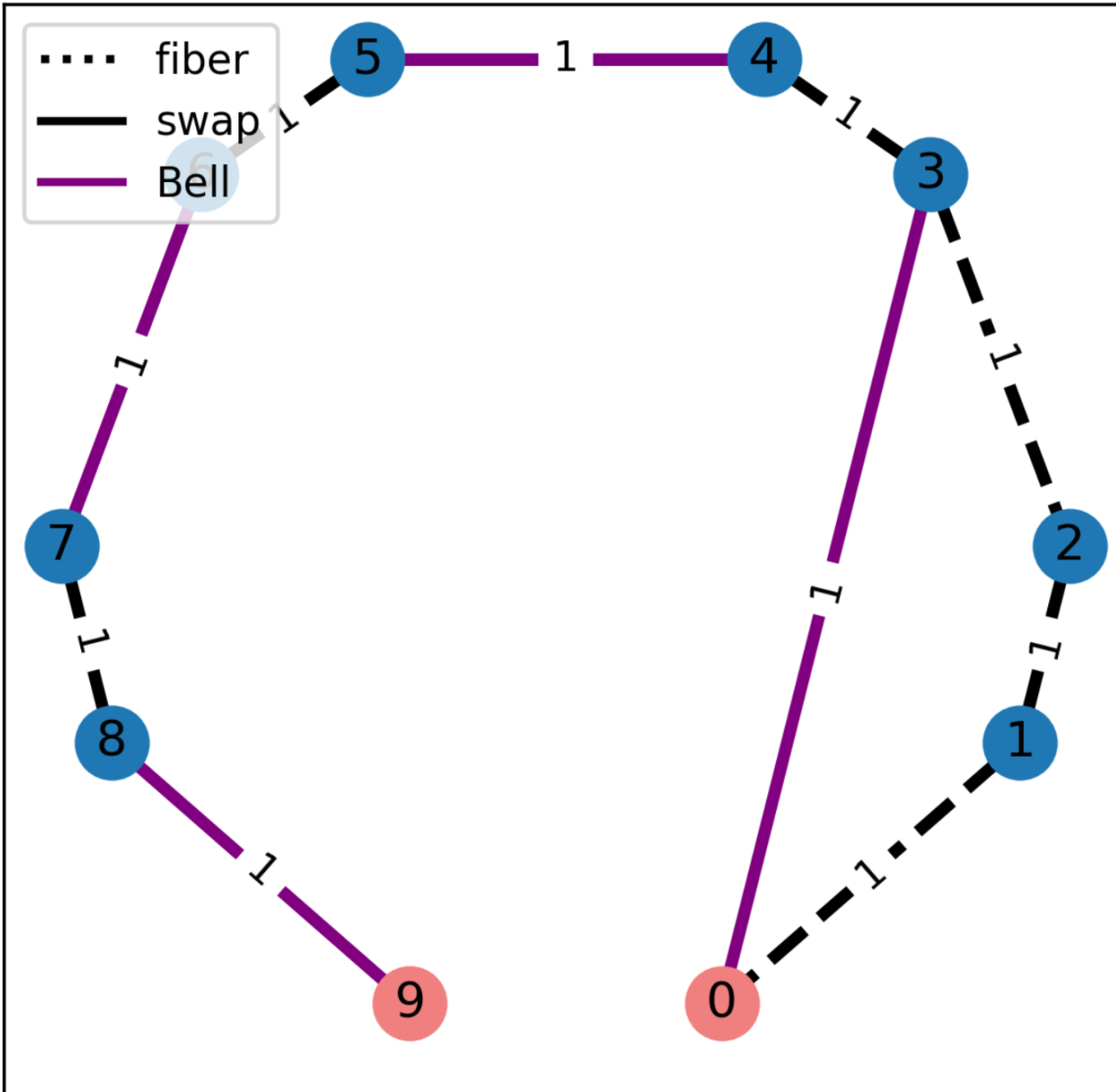
Work in progress: Research and create the necessary resources to enable us to manage **hybrid** networks.

RL for entanglement distribution



- A QRs chain can swap entanglement among very distant nodes.
- We can model QR nodes as follows.
- Does this model captures the physics of the problem when things go wrong?
 - EG may fail
 - ES may fail
 - Quantum memories decohere
- We should add some parameters.

RL for entanglement distribution



- Is long-range entanglement distribution possible in non-ideal scenarios?
- We are looking for a policy that maps these graphs to generation/swapping actions. In the ideal case:
 - If network is empty, use all fiber connections for EG.
 - Then, ES in all stations.
 - This is called greedy.
- However, in non-ideal cases, specially in non-chains, greedy is not optimal.
 - **Reinforcement Learning**
- There are works in this direction
 - G Iñesta et al. [10.1038/s41534-023-00713-9](https://doi.org/10.1038/s41534-023-00713-9)
 - S Haldar et al. [10.1103/PhysRevApplied.21.024041](https://doi.org/10.1103/PhysRevApplied.21.024041)
- We are extending those approaches to
 - Heterogeneous networks
 - Beyond chain
 - Model free

RL for entanglement distribution



UNIVERSIDAD
POLITÉCNICA
DE MADRID



GCC

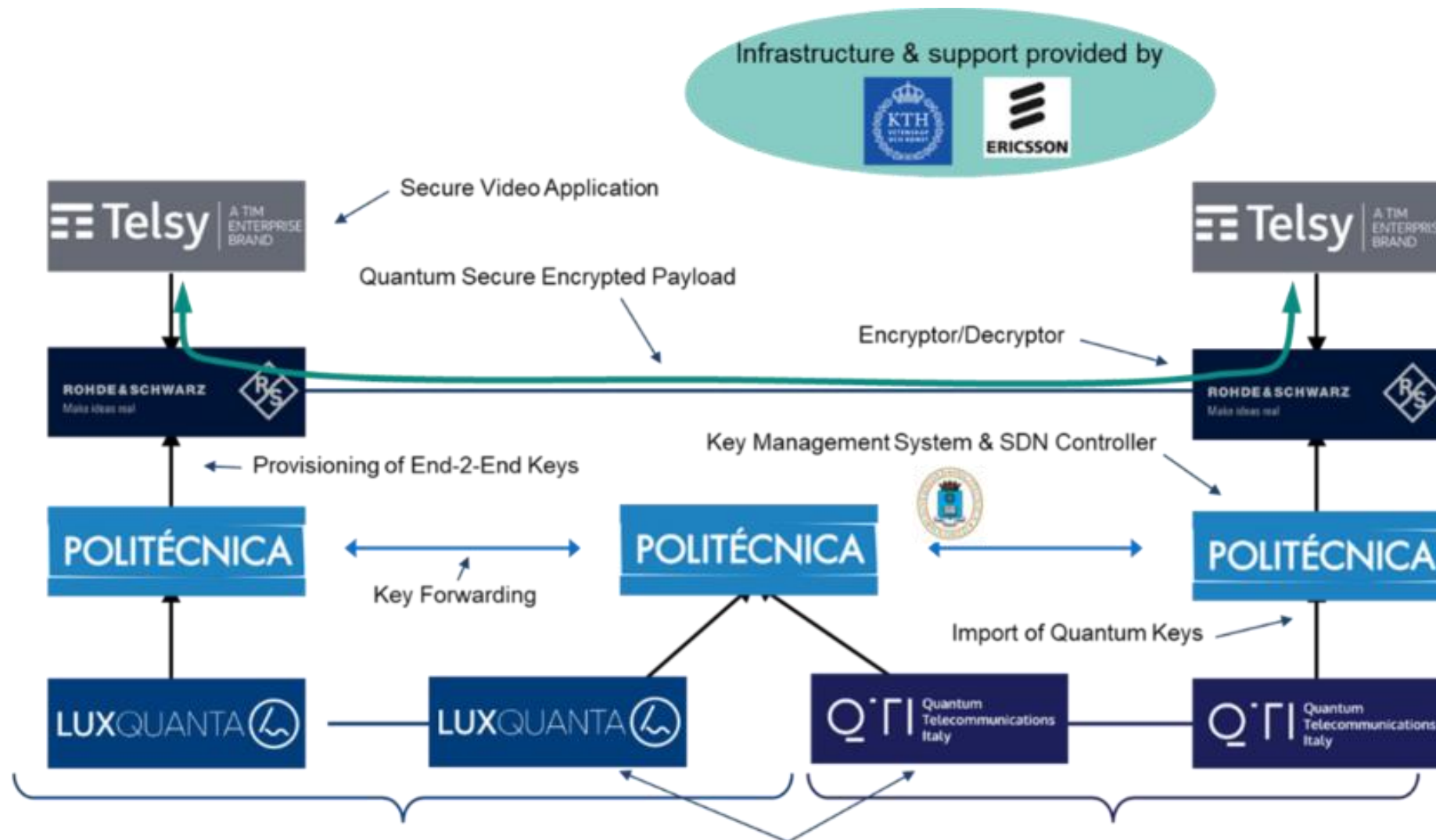
We consider the policy to be a neural network

- It takes as input the Bell graph adjacency matrix
- After some linear algebra and non-linearities...
- ... it outputs a probability distribution of taking actions given the current graph
- We sample an action from it and get a new graph from it
- Repeat until long-range entanglement is obtained or running out of time steps
- Update the weights of the neural network to make successful and quick entanglement distribution likely
- Repeat until convergence or running out of HPC computing time
- These policies can be simulated in MadQCI to computationally study the performance of future entanglement distribution networks in a real network.

We're close to obtain interesting results...

Quantum-resistant video conference

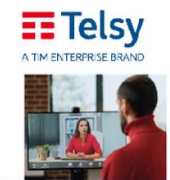
Participating Projects



Multi-domain QKD



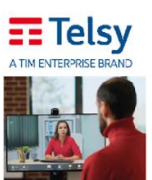
UNIVERSIDAD
POLITÉCNICA
DE MADRID



Videoconference



Quantum Lottery



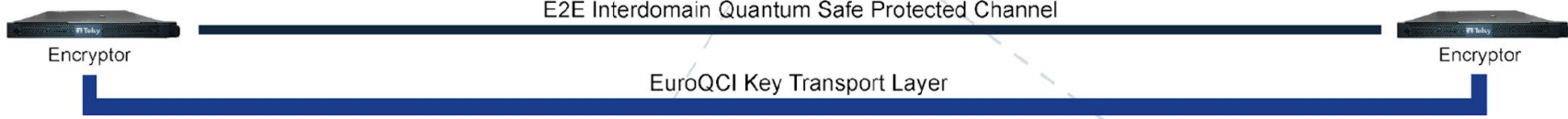
Videoconference



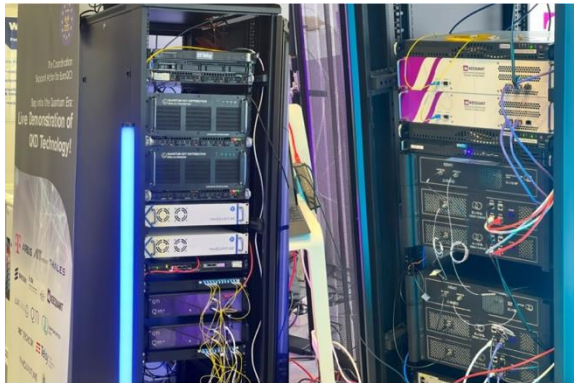
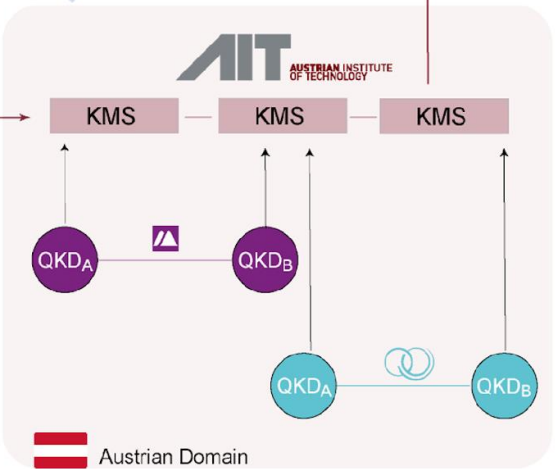
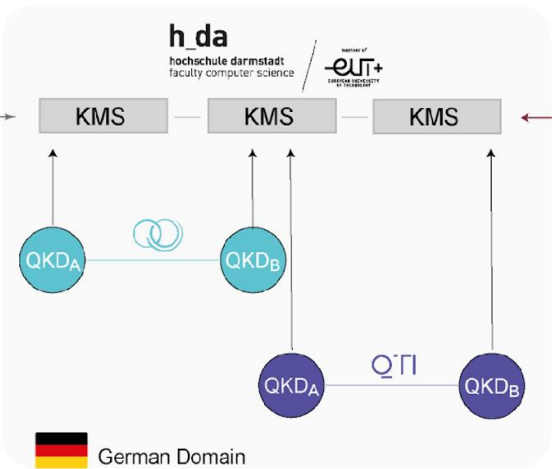
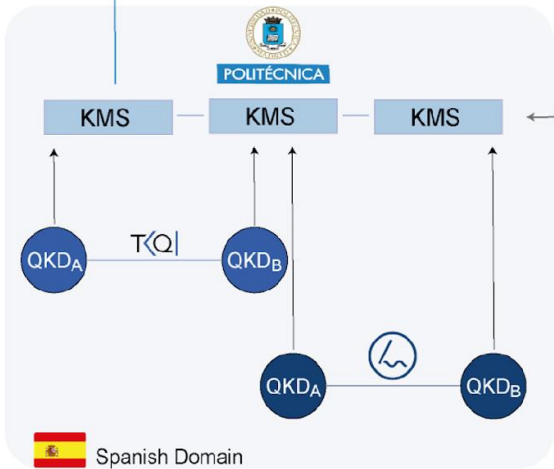
Quantum Lottery



A TIM ENTERPRISE BRAND



A TIM ENTERPRISE BRAND



ThinkQUANTUM

LUXQUANTA

QUANTUM OPTICS
JENA

QTI Quantum
Telecommunications
Italy

KEEQUANT

QUANTUM OPTICS
JENA

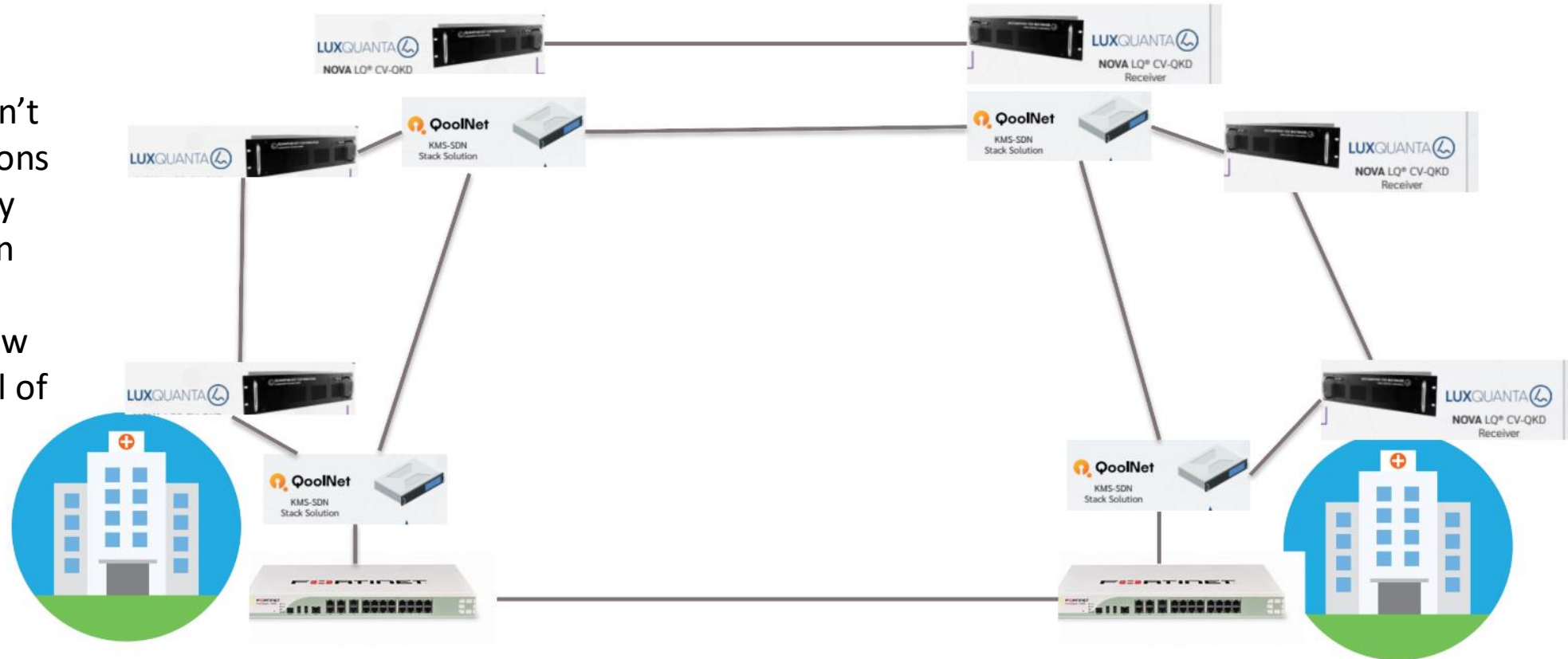
Quantum resistant e-Health

Anexo arquitectura

Central Madrid Concepción

Central Norte

- Sending documents such as reports or imaging results doesn't require strict conditions
- However, to remotely perform an operation requires strict conditions such as low latency or non denial of service



Vithas Arturo Soria

Vithas Milagrosa

Our group: GIICC

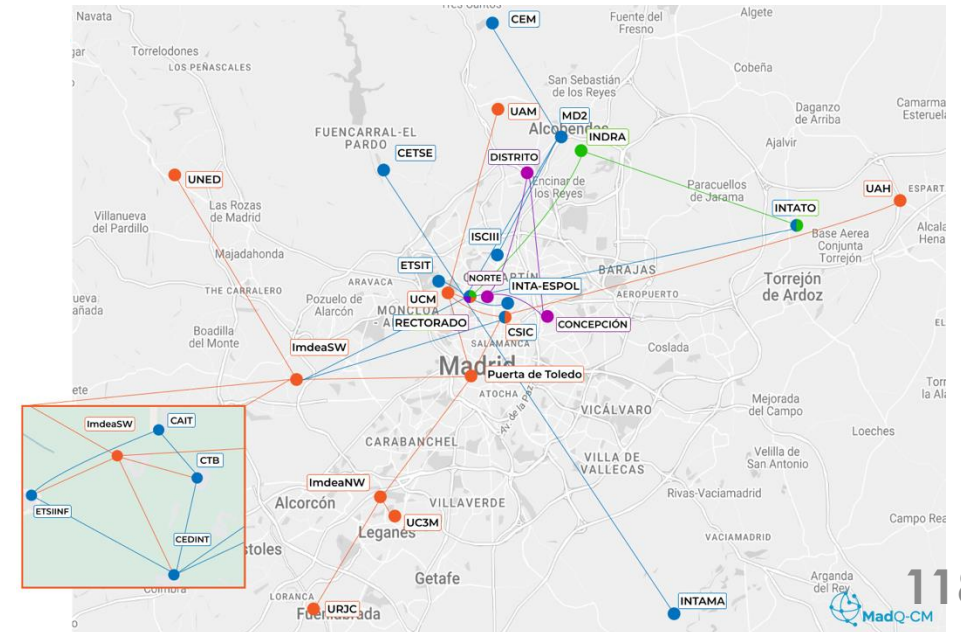
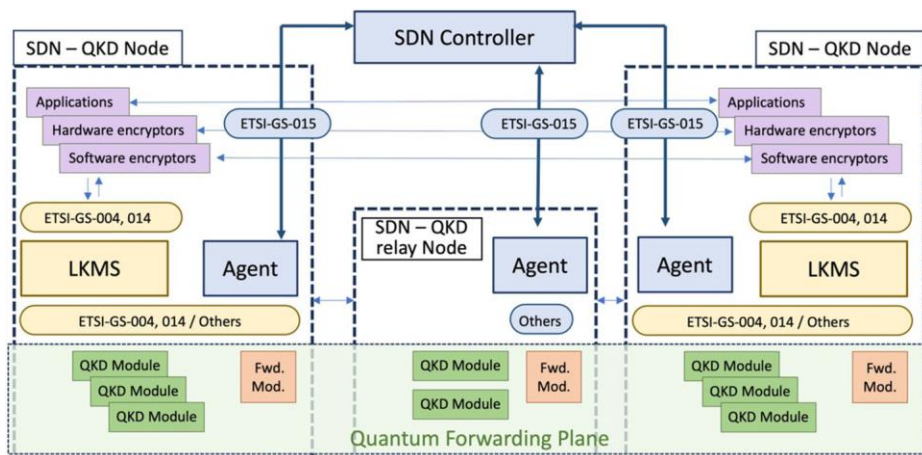


Contact and hiring:

javier.faba@upm.es

gi.icc@upm.es

vicente.martin@upm.es



Acknowledgments



UNIVERSIDAD
POLITÉCNICA
DE MADRID



Cofinanciado por
la Unión Europea

EuroQCI is a European network for quantum communications. This initiative is supported by the European Commission through the Europe Digital program, under the grant number DIGITAL-2021-QCI-01-DEPLOY-NATIONAL



VICEPRESIDENCIA,
CONSEJERÍA DE EDUCACIÓN
Y UNIVERSIDADES



Plan de Recuperación,
Transformación
y Resiliencia



Financiado por
la Unión Europea
NextGenerationEU

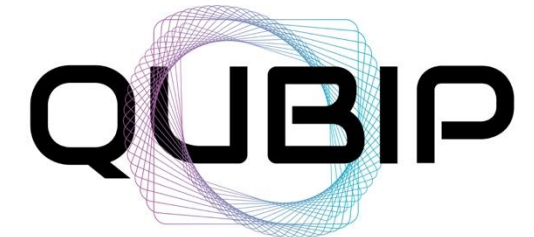
Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación Transformación y Resiliencia, financiado por la Unión Europea – NextGenerationEU



This project has received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).



EU H2020 research and innovation program under Grant 101017733, with funding organizations: Foundation for Science and Technology – FCT, Agence Nationale de la Recherche - ANR, and Spanish Agencia Estatal de Investigación – AEI



Quantum-oriented Update to Browsers
and Infrastructure for the PQ Transition



Thank you!

