Quantum Cryptography and New Generation Networks

XIII jornadas REDIMadrid

Ciudad Universitaria
Madrid, Octubre 2018

Vicente Martin,
Alejandro Aguado
Vicente@fi.upm.es

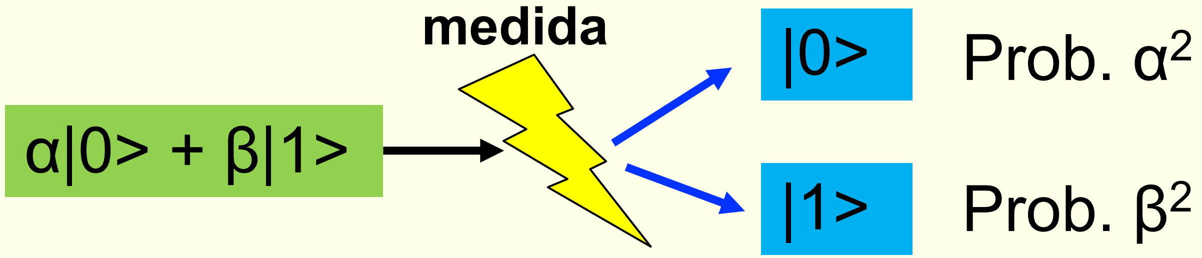
Index.

- Brief Intro to QKD
- QKD and networks.
- Software Defined Networking.
- Why mix QKD and SDN (benefits and beneficial)
- The structure of a SDN QKD Node.
- Madrid Quantum Network and use cases
- Future

Información Cuántica.

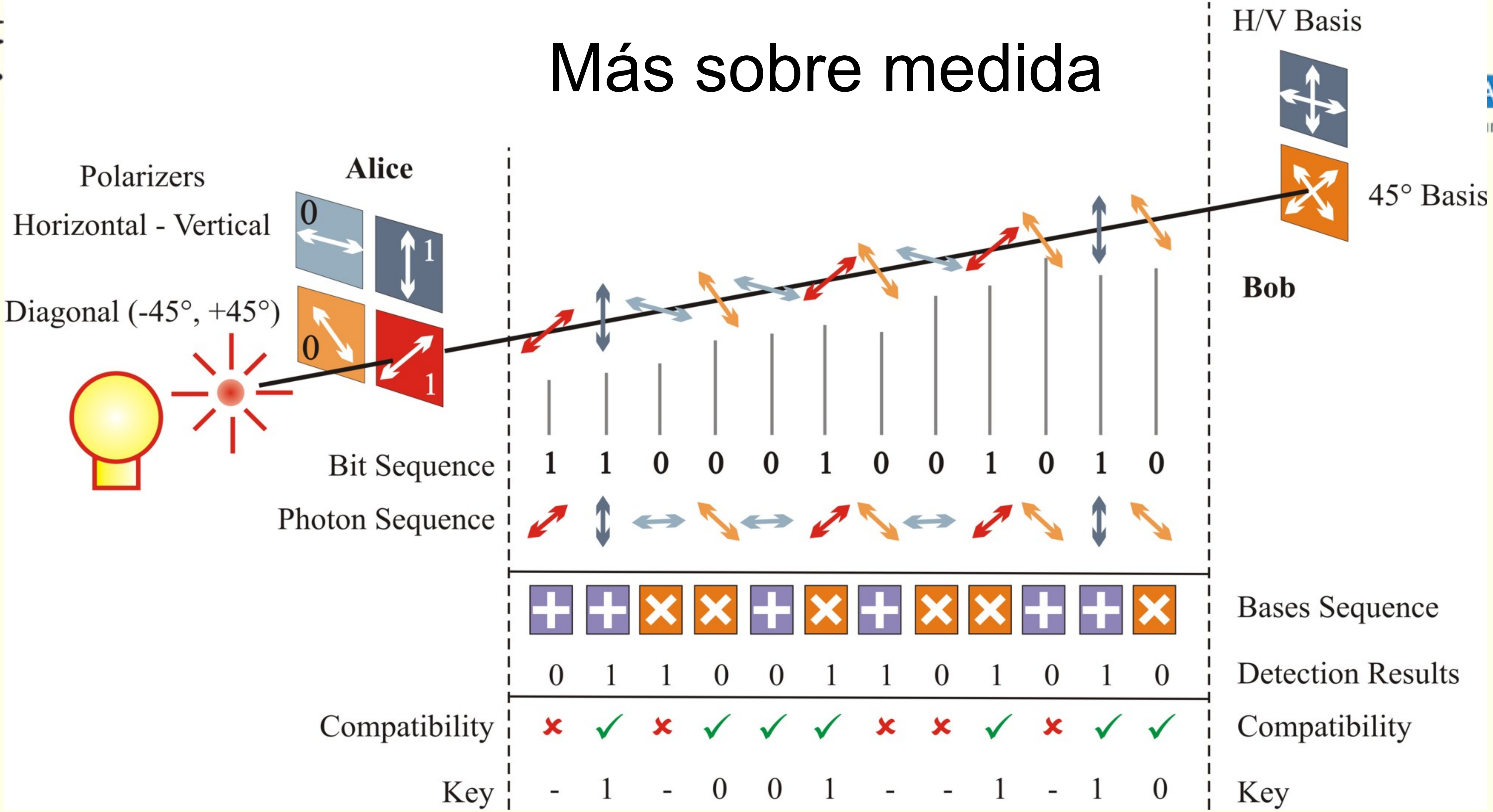
El Qubit.

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

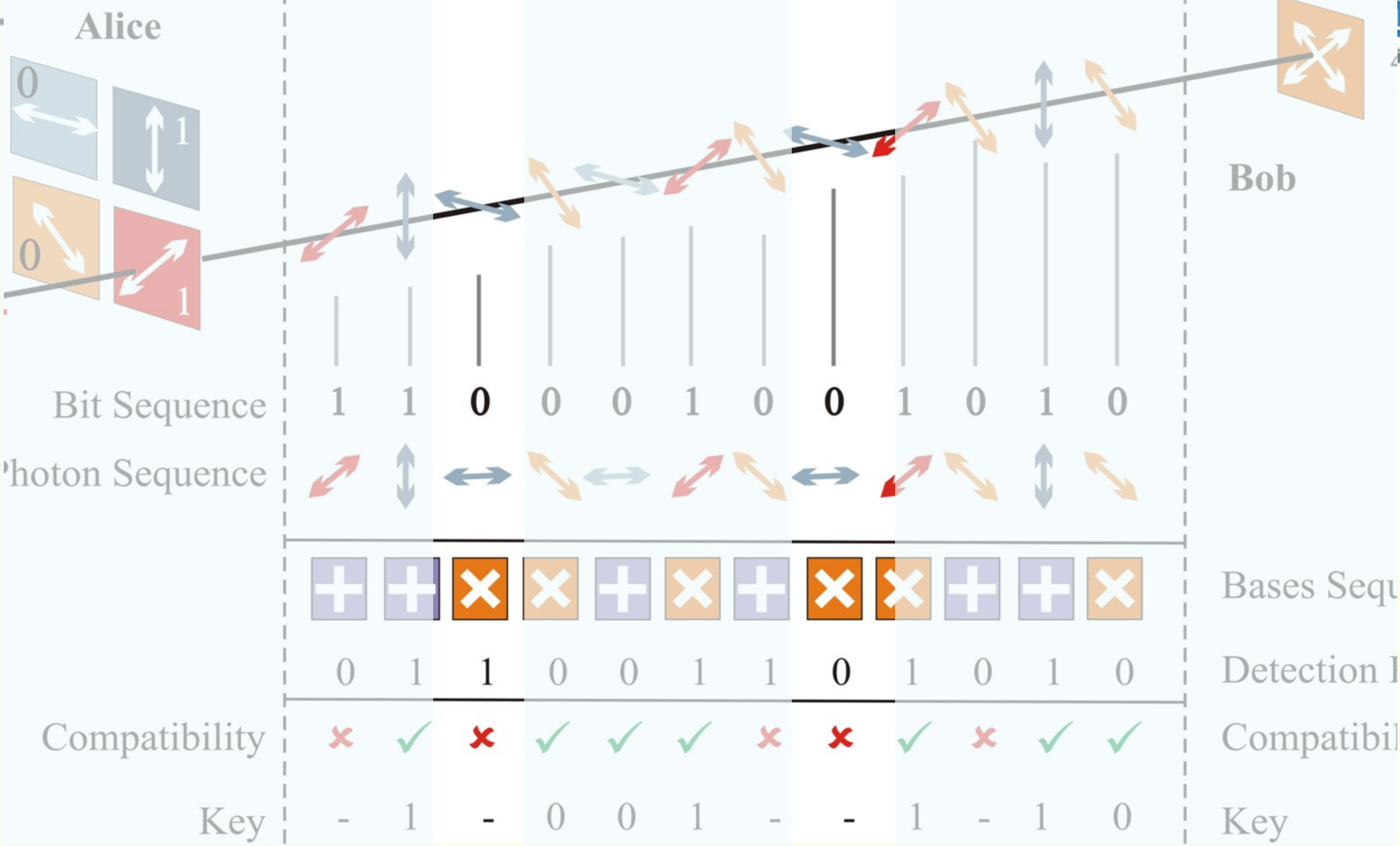


  - $(\alpha^2+\beta^2 = 1)$
  - Nótese que **la lectura modifica el estado del qubit.**
  - Teorema de la No-clonación: **No se puede copiar un estado cuántico desconocido.**

Más sobre medida



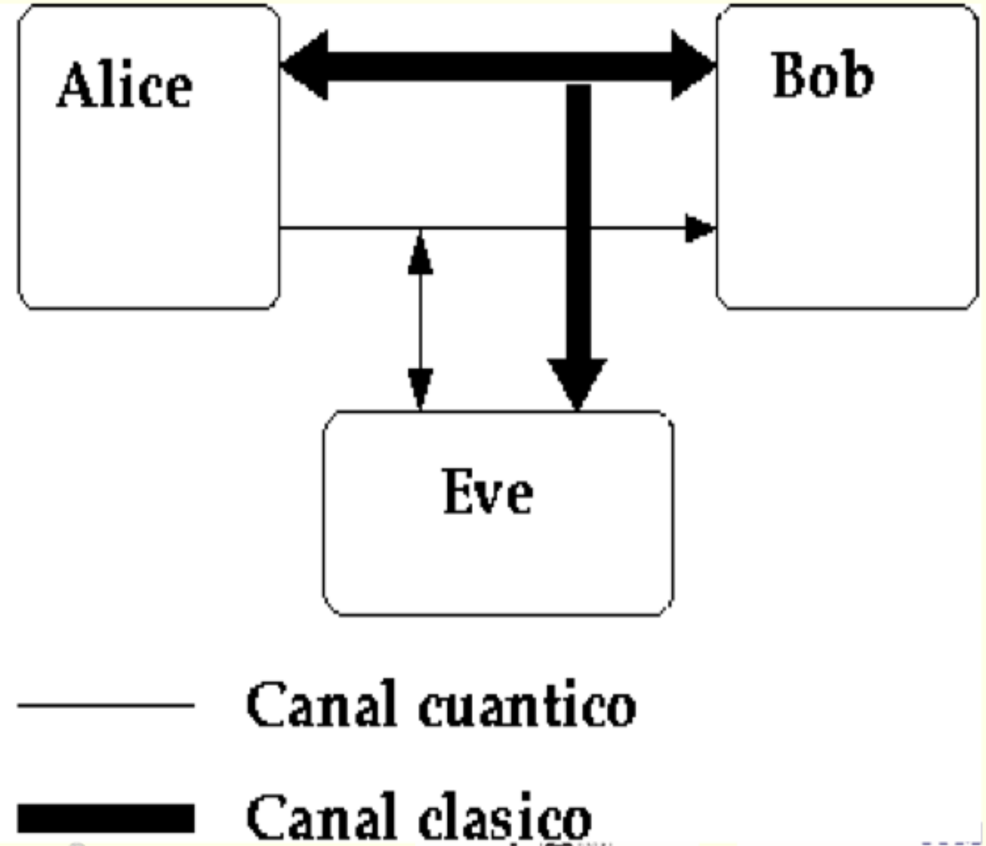
Más sobre medida



Criptografía Cuántica

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)



Criptografía cuántica: BB84 el primer protocolo

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

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

Criptografía cuántica: BB84 el primer protocolo

Center for Computational Simulation

POLITÉCNICA "Ingeniamos el futuro"

ALICE
Emisor

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

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

Criptografía cuántica: BB84 el primer protocolo

BOB receptor

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

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

Criptografía cuántica: BB84 el primer protocolo

Center for Computational Simulation

POLITÉCNICA "Ingeniamos el futuro"

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

(CLÁSICA)

Detección de Intrusos y Corrección de errores (ruido)

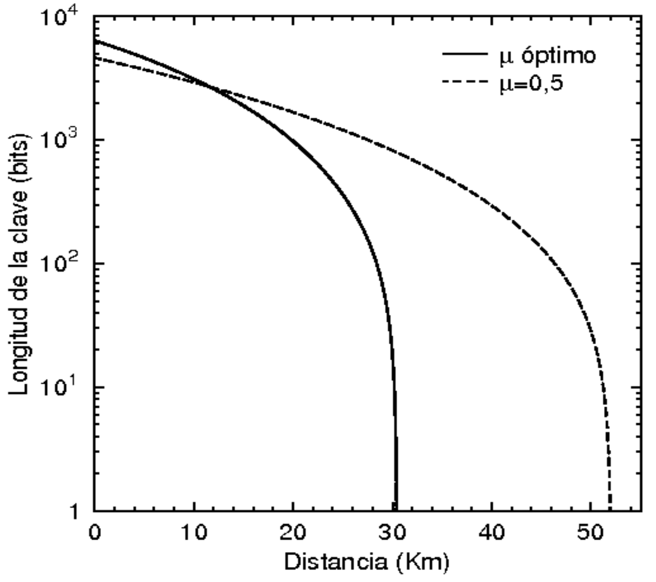
Bennet, Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing"
International Conference on Computers, Systems and Signal Processing. Bangalore, 1984

Criptografía cuántica

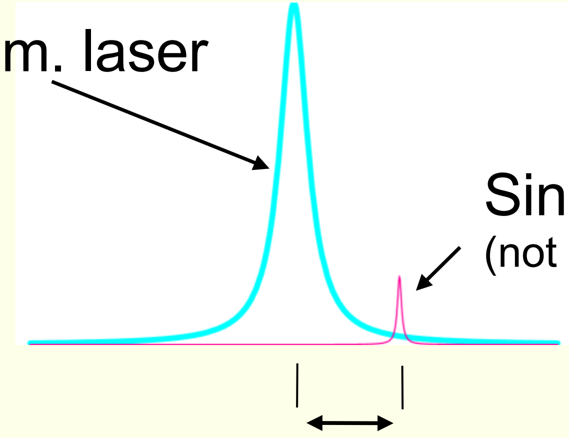
- La **criptografía cuántica** provee un mecanismo para crear una clave idéntica en dos lugares separados. La información perdida (potencialmente en manos de un espía) puede ser acotada tanto como queramos.
  - i.e. **Resolver el problema de la distribución de claves secretas**.
  - Es un mecanismo **absolutamente seguro** desde el punto de vista de teoría de la información (ITS).
  - No depende de suposiciones sobre la complejidad computacional de ciertos problemas.
- Para poder usar esto, tenemos que ser capaces de transmitir qubits.
- Usando fotones como qubits, **podemos usar redes ópticas de comunicaciones.**

Quantum communications and networks, why is it difficult?

Limited reach, point to point.

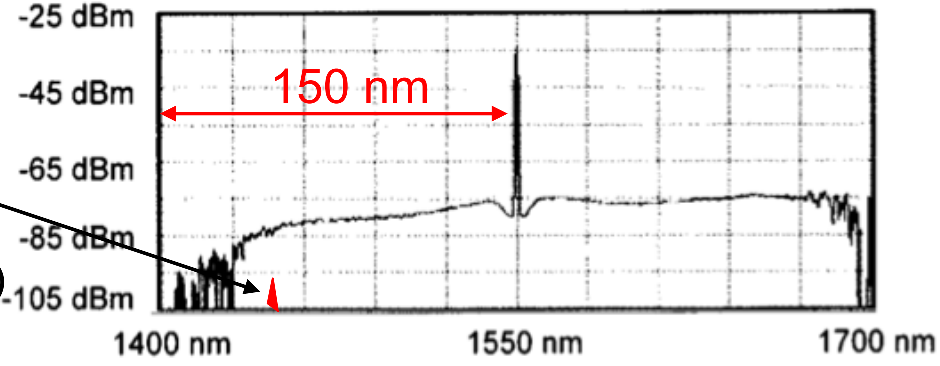


extremely weak signals.



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

Noise in the fibre: Raman



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

It is a delicate technology.

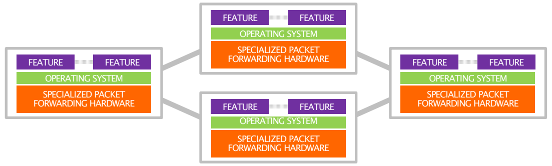
R. Doisneau

SW Defined Networking and the old paradigm

Network equipment as Black boxes

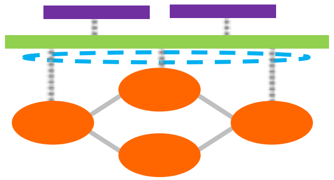
SDN

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



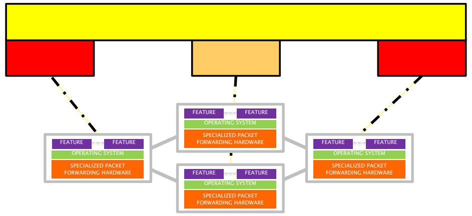
Boxes with autonomous behaviour

SDN



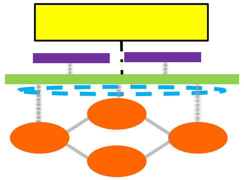
Decisions are taken out of the box

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



Adapting OSS to manage black boxes

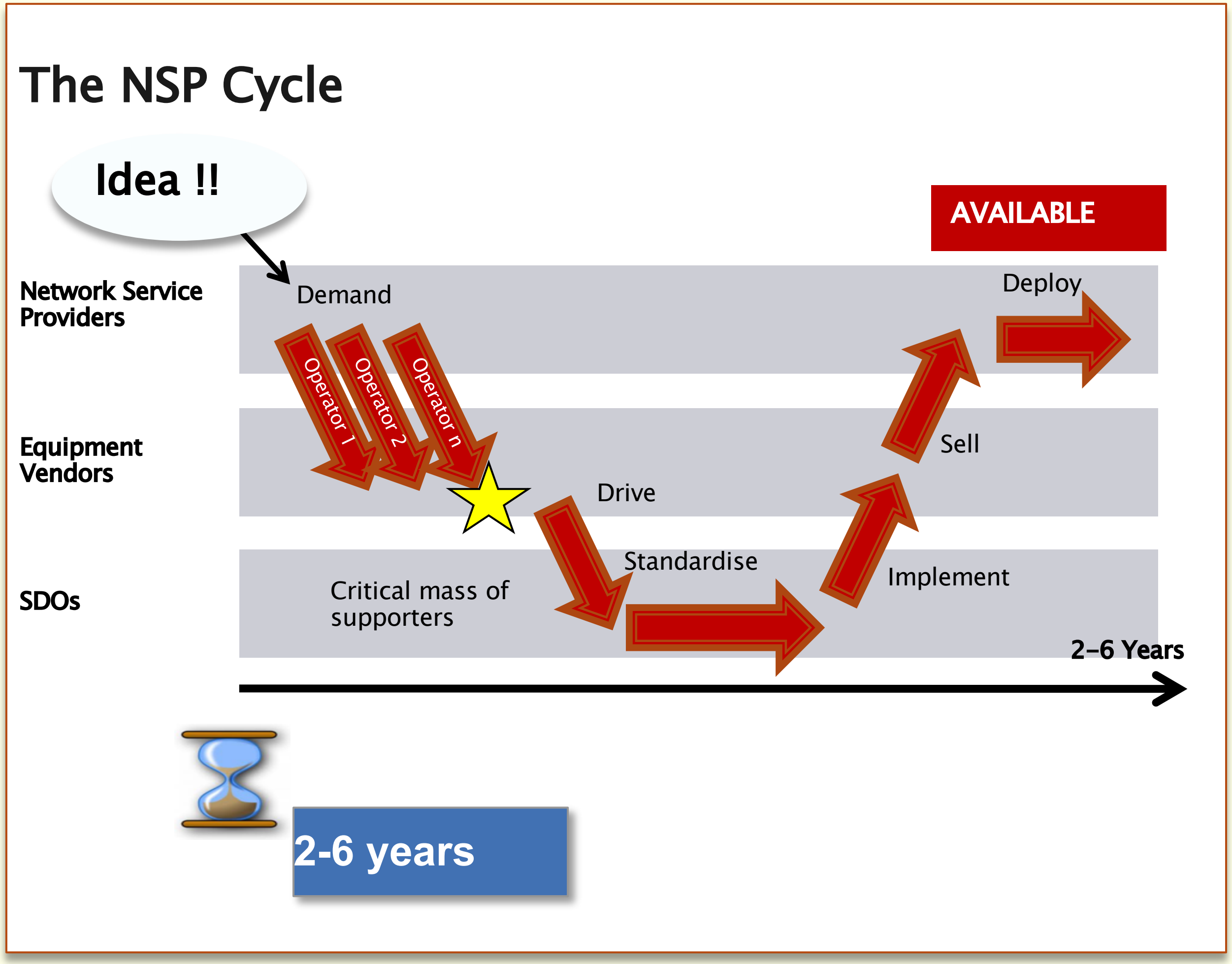
SDN

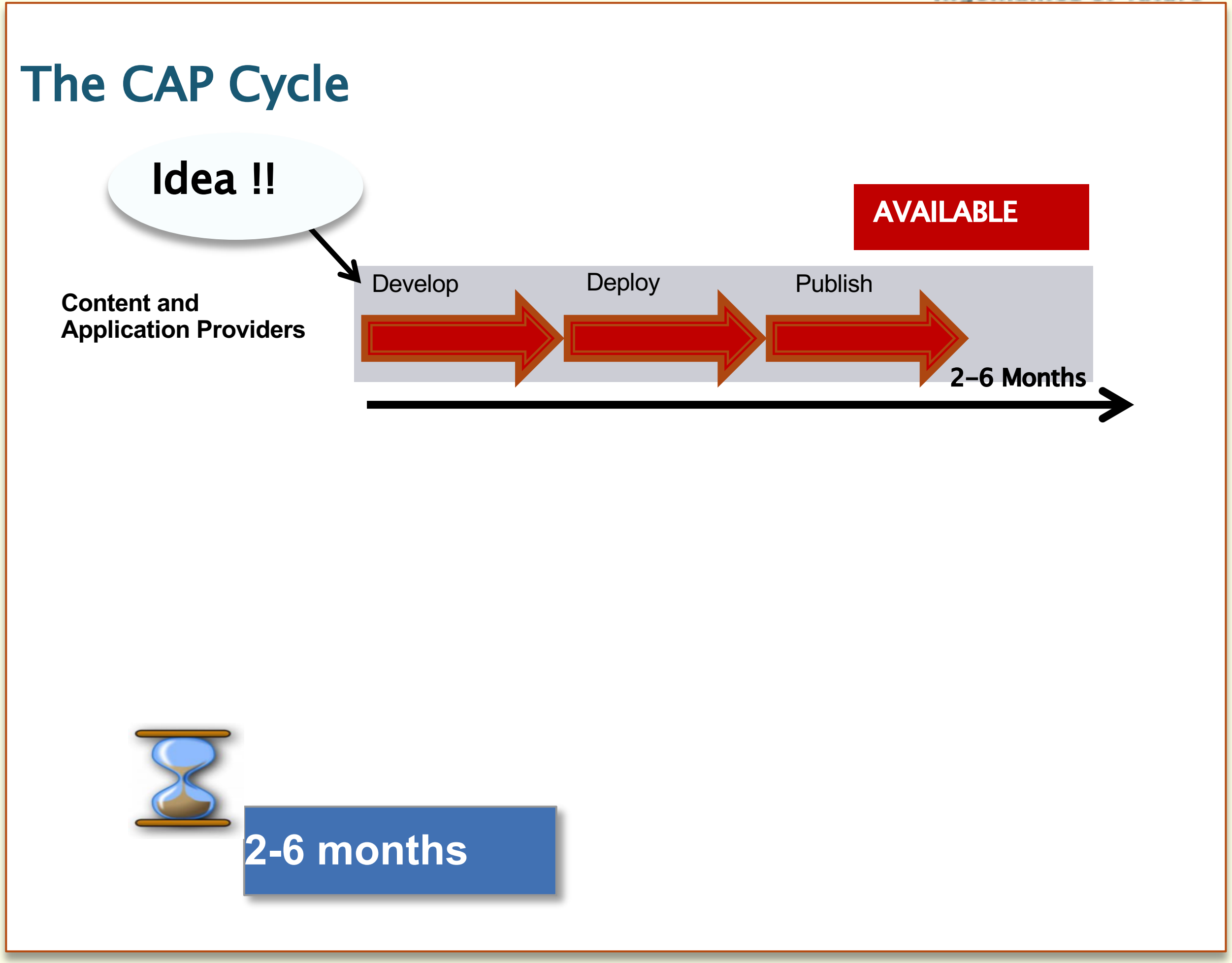


Simpler OSS to manage the SDN controller

SDN can adapt, allowing for a fast innovation Cycle.

Why moving towards these paradigms?





Flexibility, quick adaptation, fast innovation cycle, avoid vendor lock-in…

Diego Lopez,
Telefónica I+D

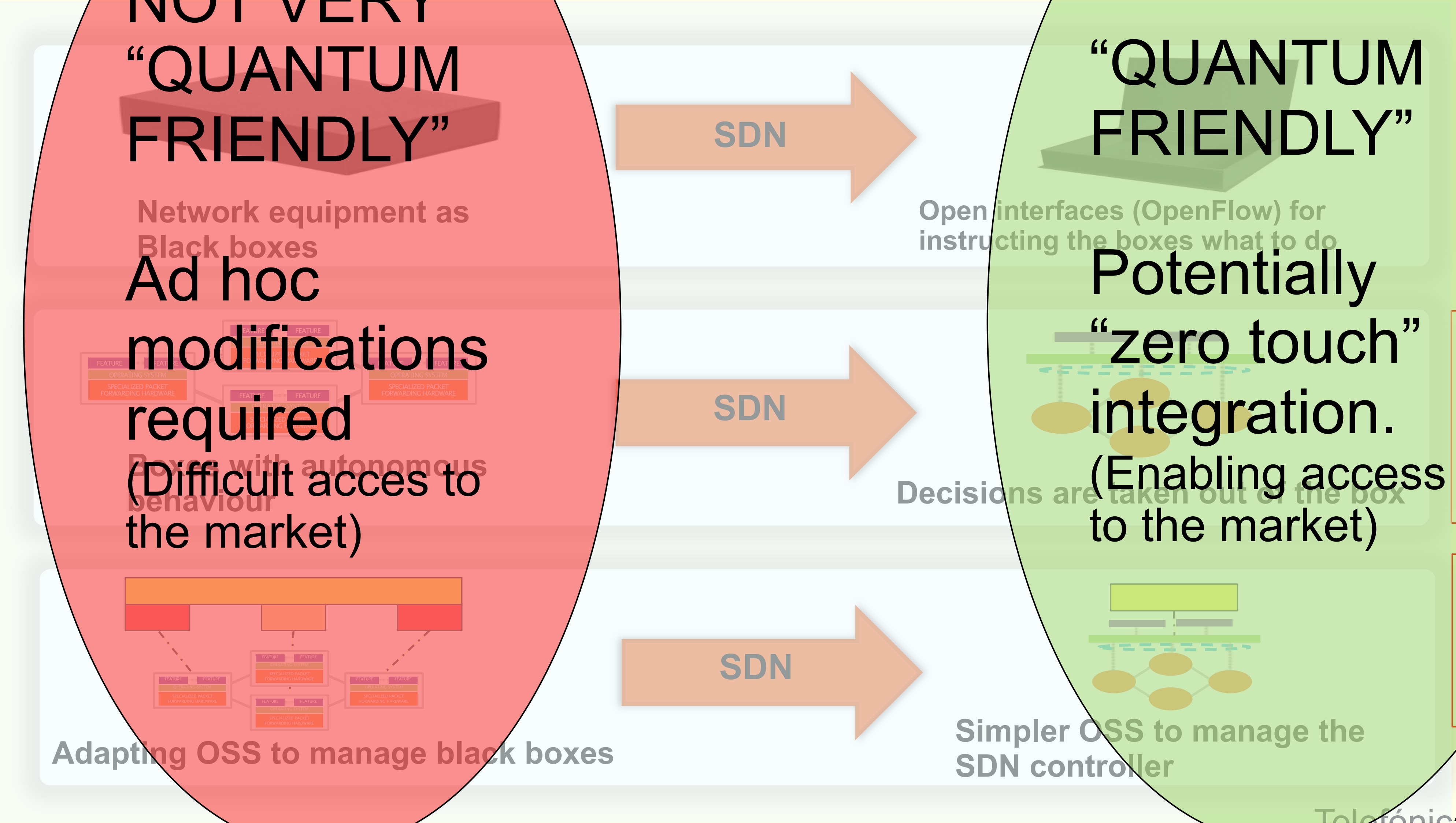
Why SDN for QKD?

NOT VERY “QUANTUM FRIENDLY”

Ad hoc modifications required (Difficult acces to the market)

“QUANTUM FRIENDLY”

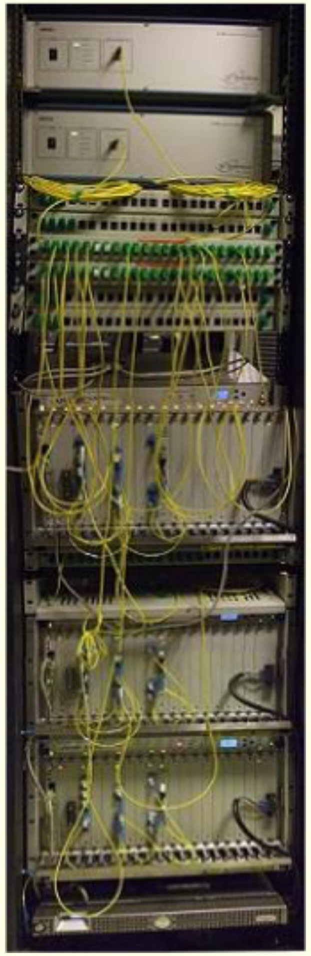
Potentially “zero touch” integration. (Enabling access to the market)



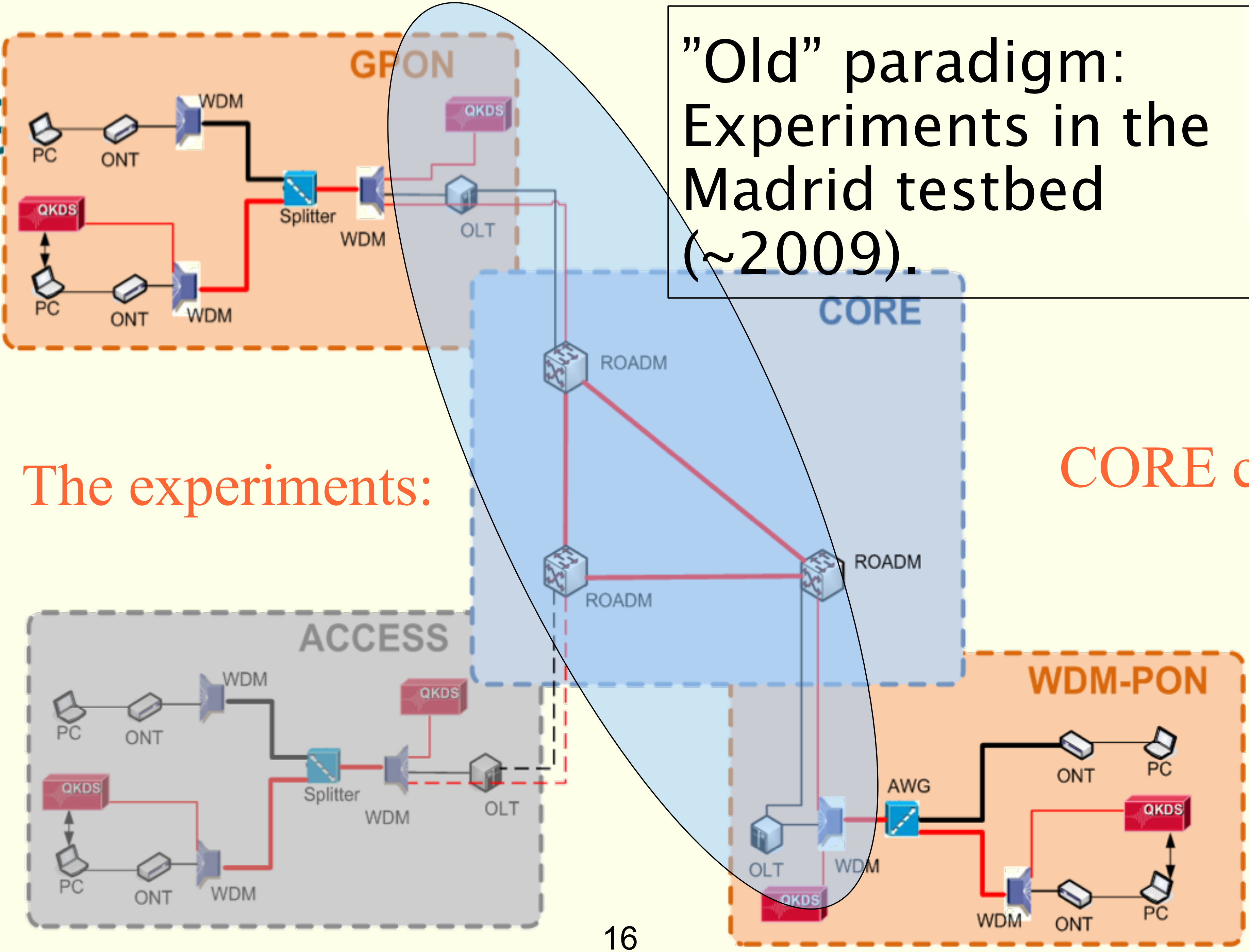
Programmability is Key: A SDN controller can manage the Network.

SDN can adapt, allowing for a fas innovation Cycle.

"Old" paradigm: Experiments in the Madrid testbed (~2009).

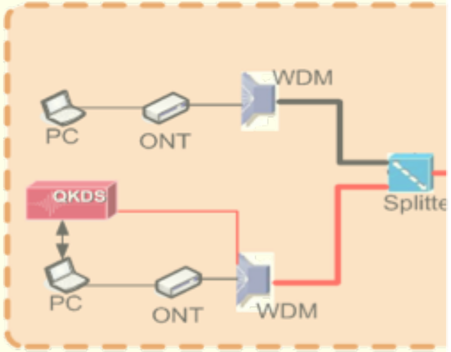


The experiments:

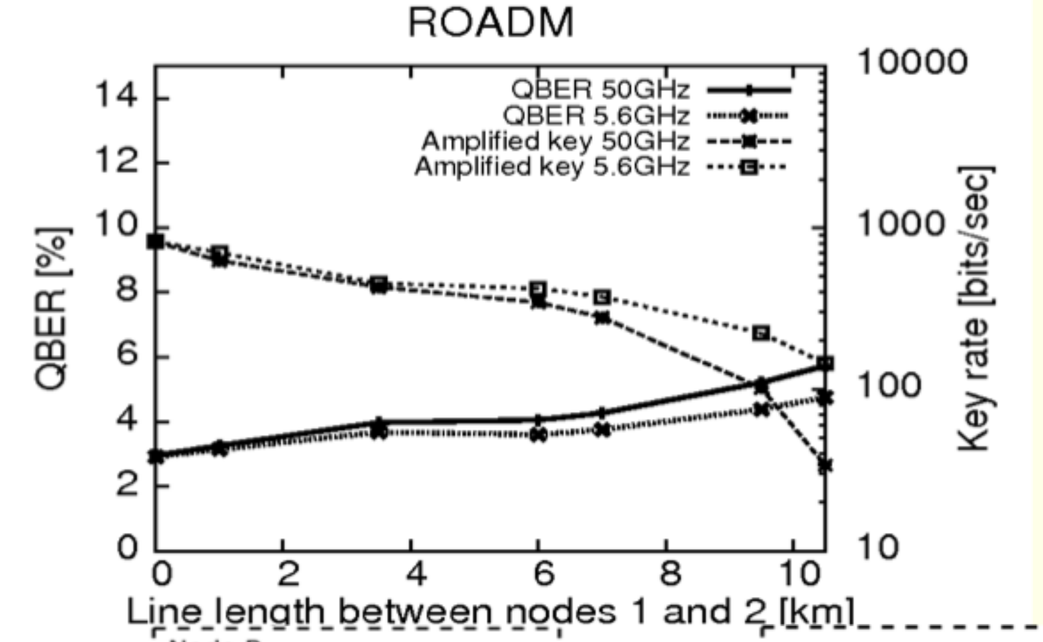


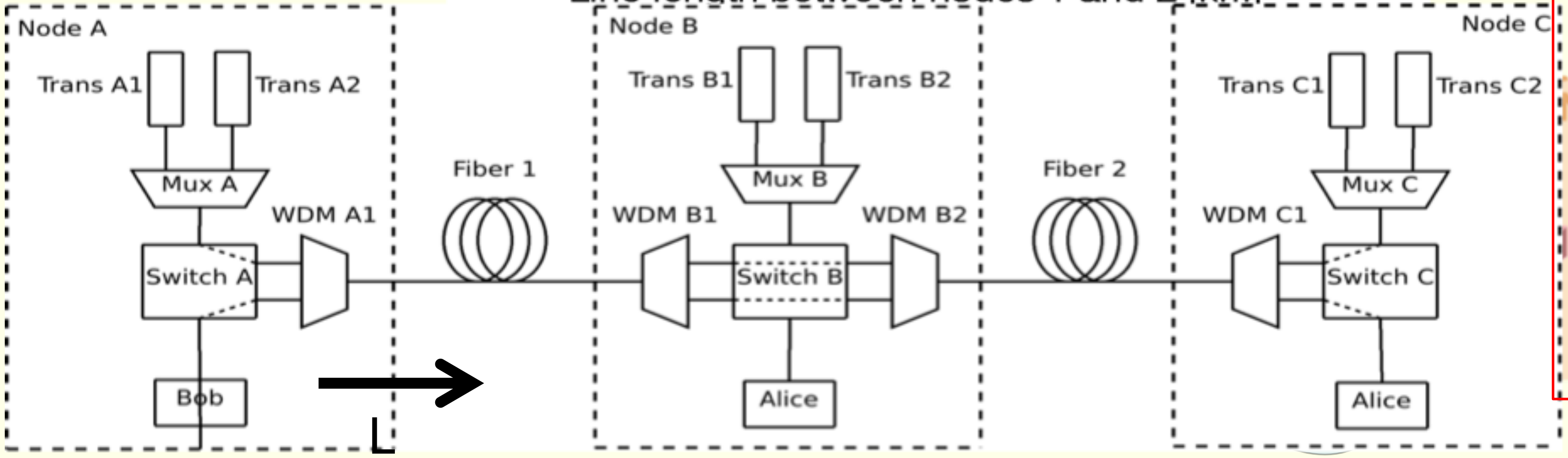
CORE crossing

"Old" paradigm: Experiments in the Madrid testbed (~2009).



The experime
CORE crossi



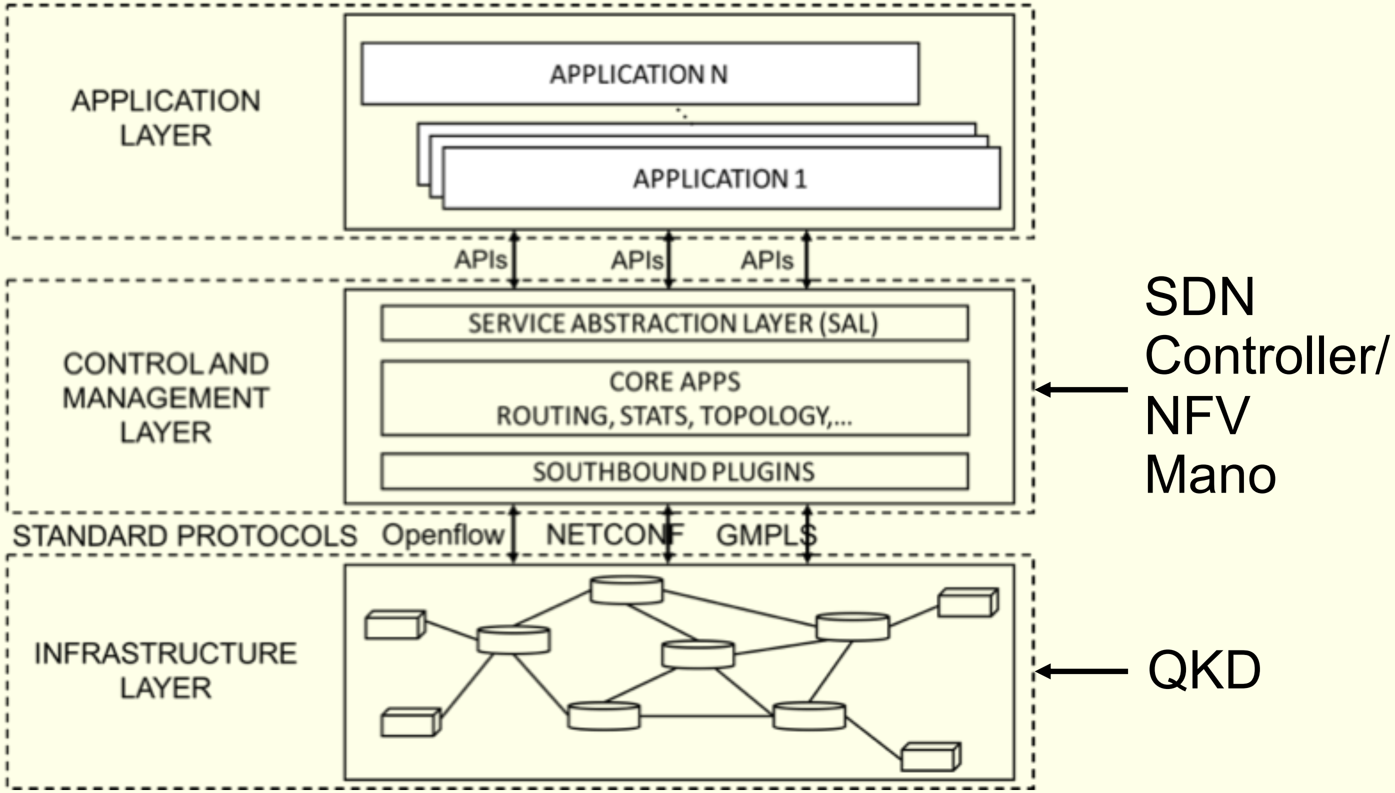


It can work but:
- **Ad hoc modifications** Required.
- **No network optimization** possible.
- **Not flexible**: Has to be readjusted if changed.
- **Hard to deploy**.

Quantum channel at 1550, Classical channels 1470, 1510 nm, 50 Ghz filters (0.4 nm)

The structure of an SDN network.

- The network **connects Points of Presence** (PoPs), where the servers and telco equipment is installed, that are **assumed secure.**
- **Distance limitations are less significant.**
  - Average distance between PoPs in Germany or Spain < 60 Km
- A centralized **(SDN) controller** knows the structure of the network and capabilities of the devices, **managing the requirements to stablish quantum channels and optimize the network.**
- **SDN-Aware devices export capabilities** (can be programmed) so that the controller can manage them, whether they are quantum or not.



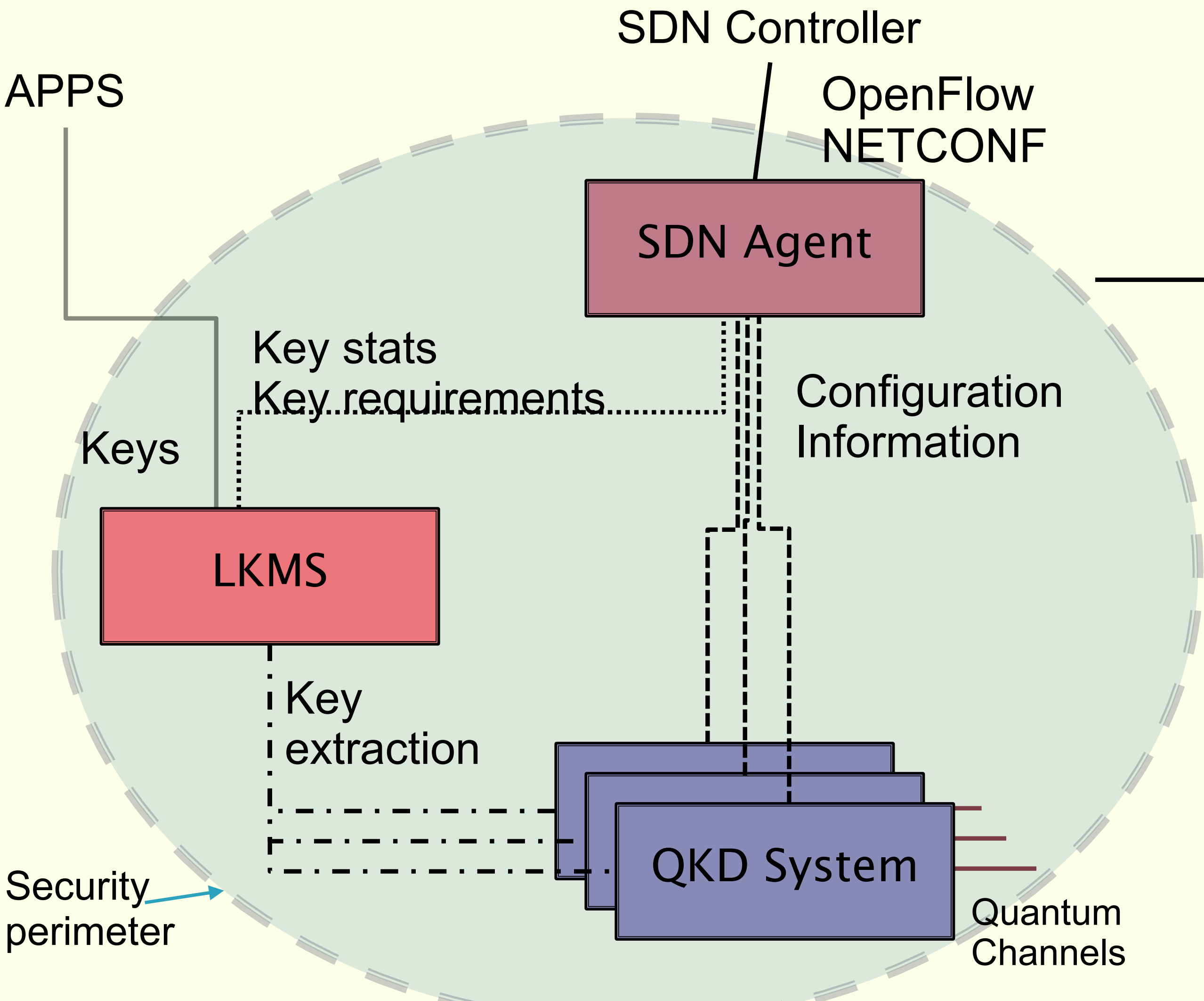
Center for Computational Simulation
POLITÉCNICA "Ingeniamos el futuro"
POLITÉCNICA "Engineering the future" INTERNATIONAL CAMPUS OF EXCELLENCE
Universidad Rey Juan Carlos
UNIVERSIDAD COMPLUTENSE MADRID
UAM UNIVERSIDAD AUTONOMA DE MADRID
fundaciónhm investigación

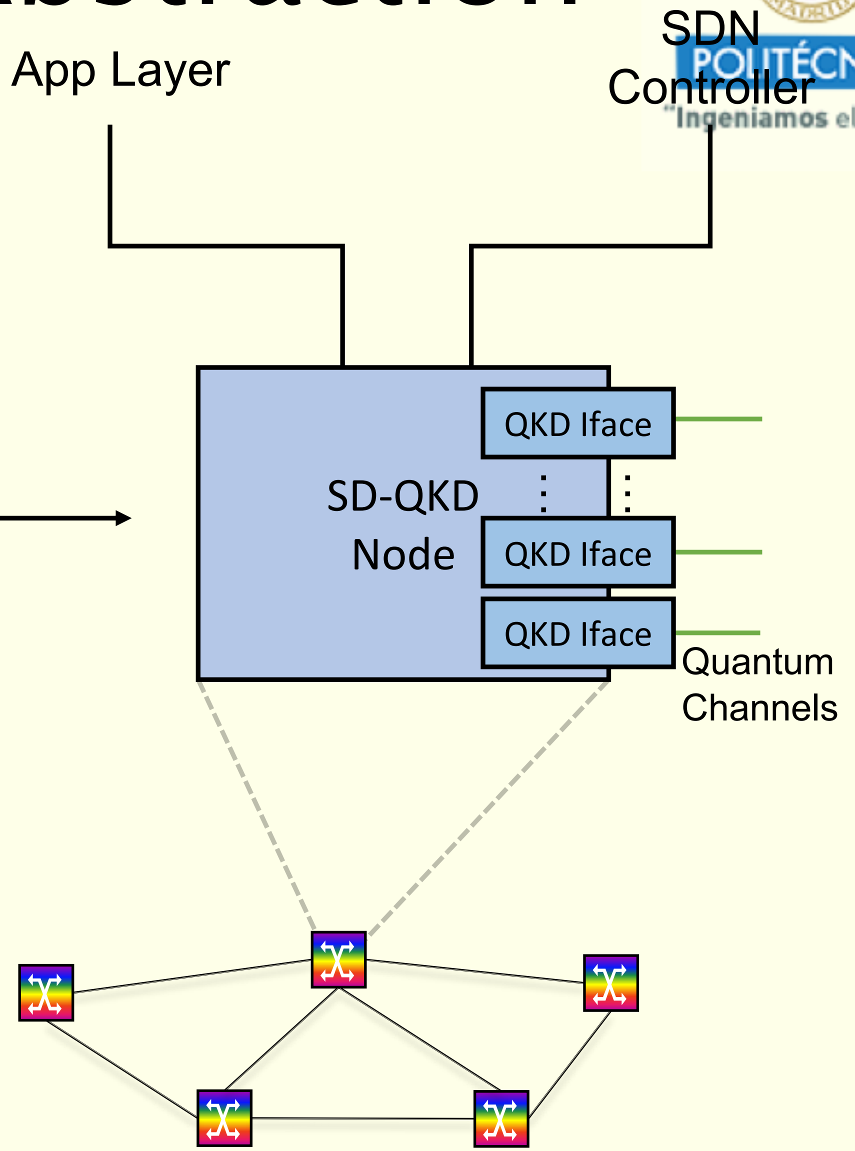
… but there is more.

- **SDN is not only an enabler** of QKD in telecommunications networks.
- SDN is **also a consumer of QKD**:
  - As a critical infrastructure that "owns" the physical means to do QKD.
  - Its structure of "secured connected locations", with typical distances within the QKD range, matches the security model of "connected trusted nodes" in current QKD.

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

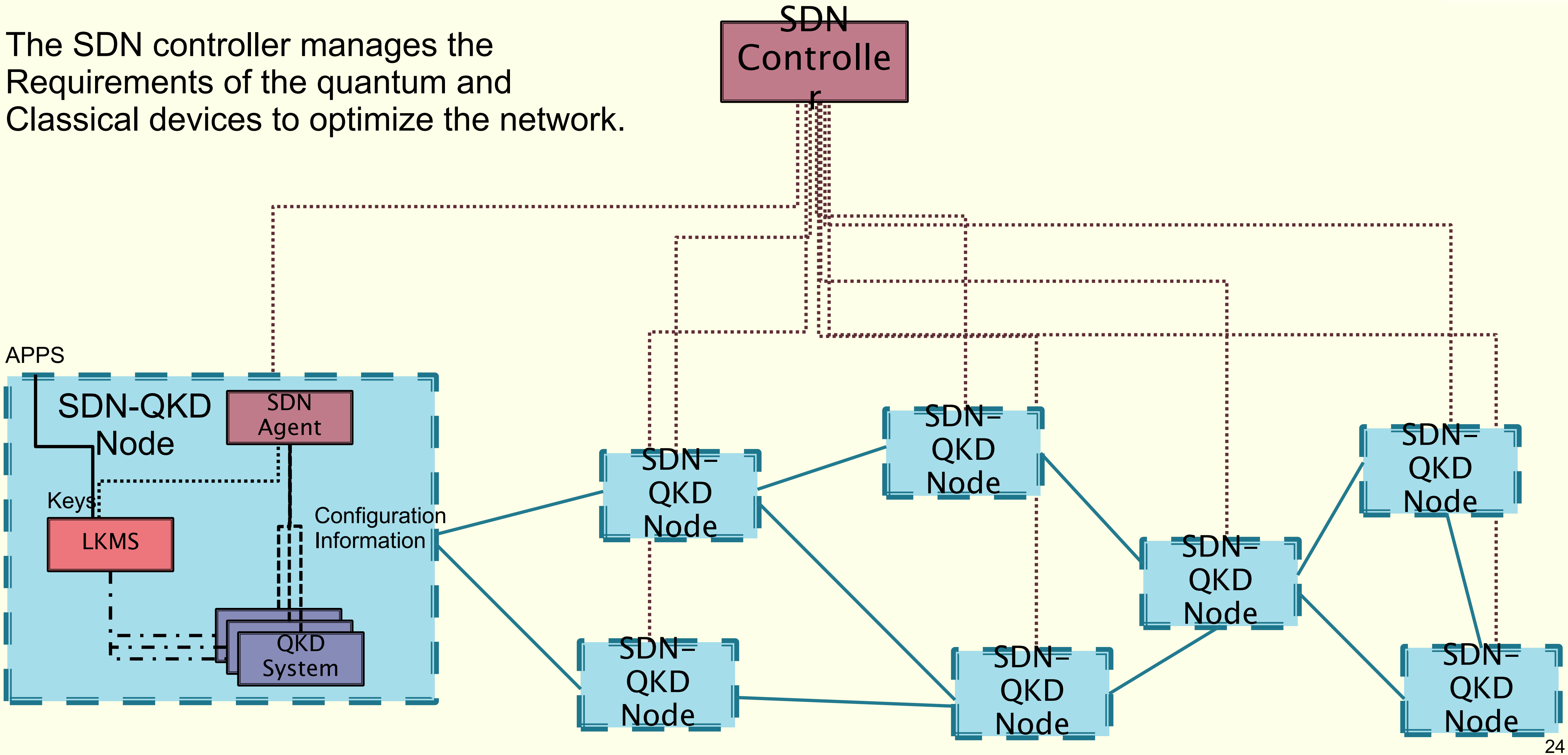
SD-QKD-Node Abstraction





Global view of the SDQKD Network

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



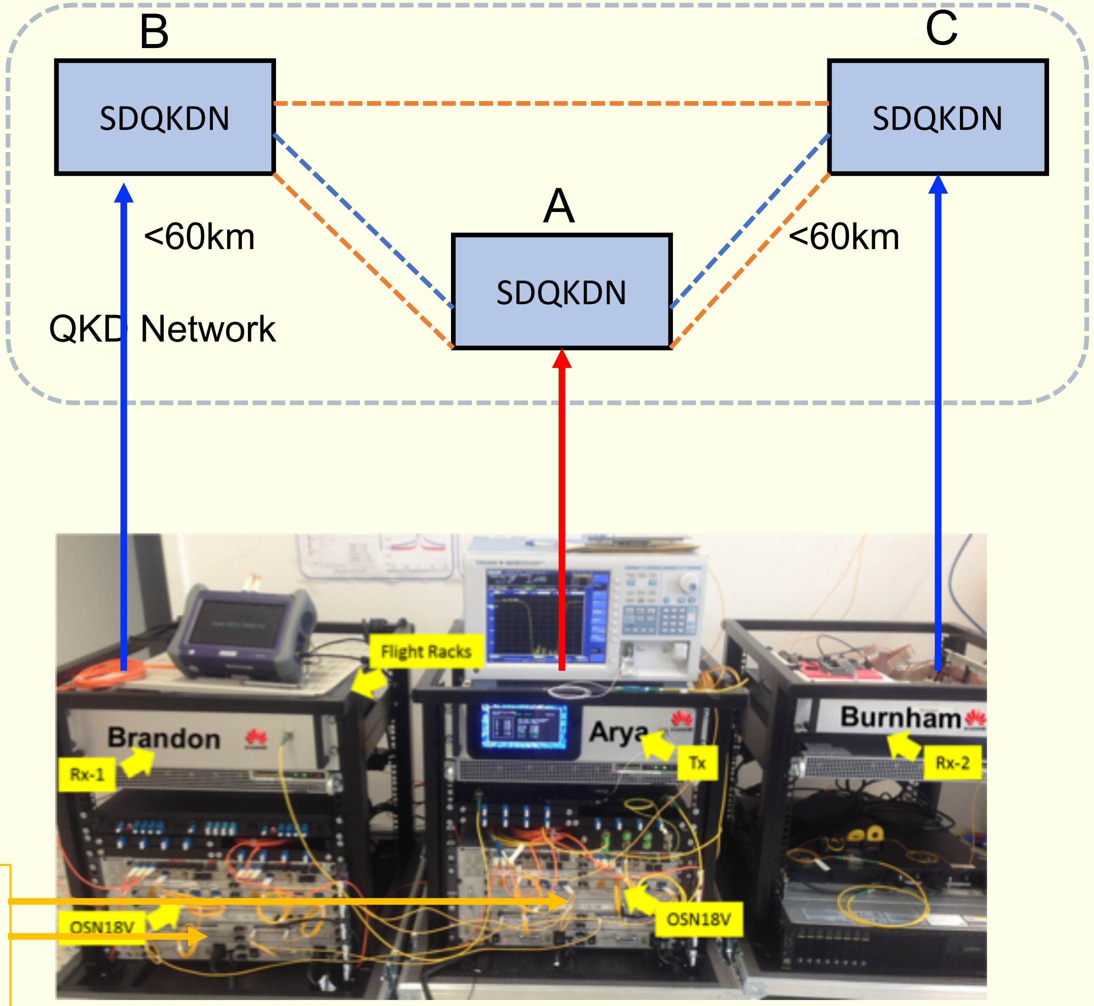
Madrid SDN QKD Network

- These **ideas** have been **implemented** in Madrid.
  - Out of lab **Testbed installed in production sites** of Telefónica of Spain.
  - **Real use cases in real environments**, showing high TRL:
    - Critical infrastructure protection: cyphering the control plane of a SDN+NFV network.
    - End-to-end security using QKD.
    - Data plane security.
- UPM, TID and Huawei Research Dusseldorf
  - And Telefónica of Spain as a provider of the nodes and optical fibre.

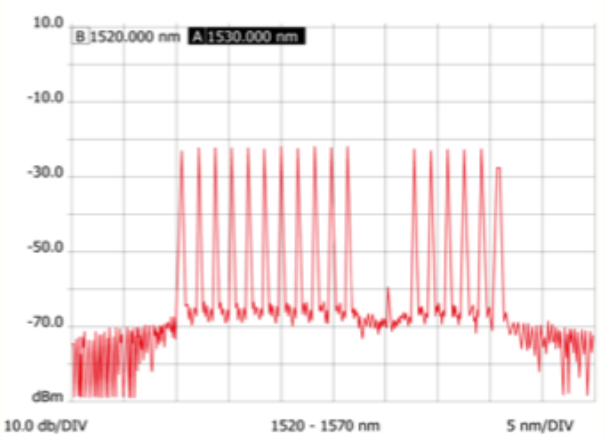
Madrid SDN QKD Network

Madrid SDN QKD Network

- **SDN controller:** Manages the network. Quantum systems in A can be connected with B or C.
- Huawei's systems designed **SDN-aware.**
- New CV-QKD technology:
  - Integration in manufacturing ecosystem.
  - **Quantum-classical coexistence**.
- The **connection** with the rest is completely **standard.**

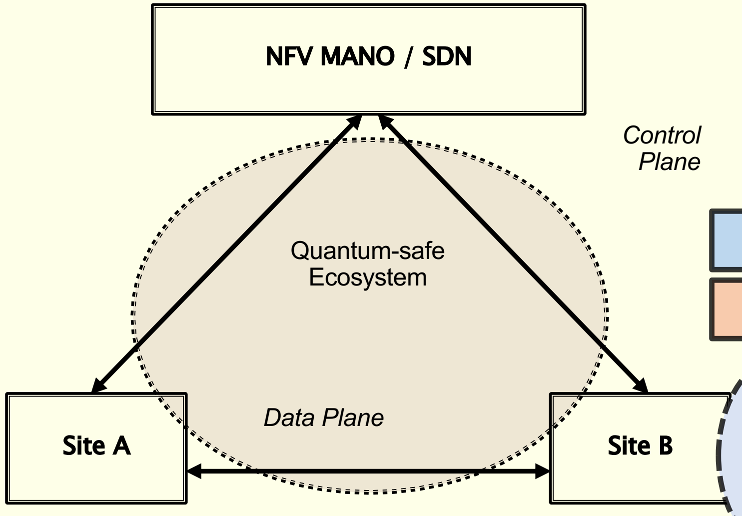


Huawei Research Germany



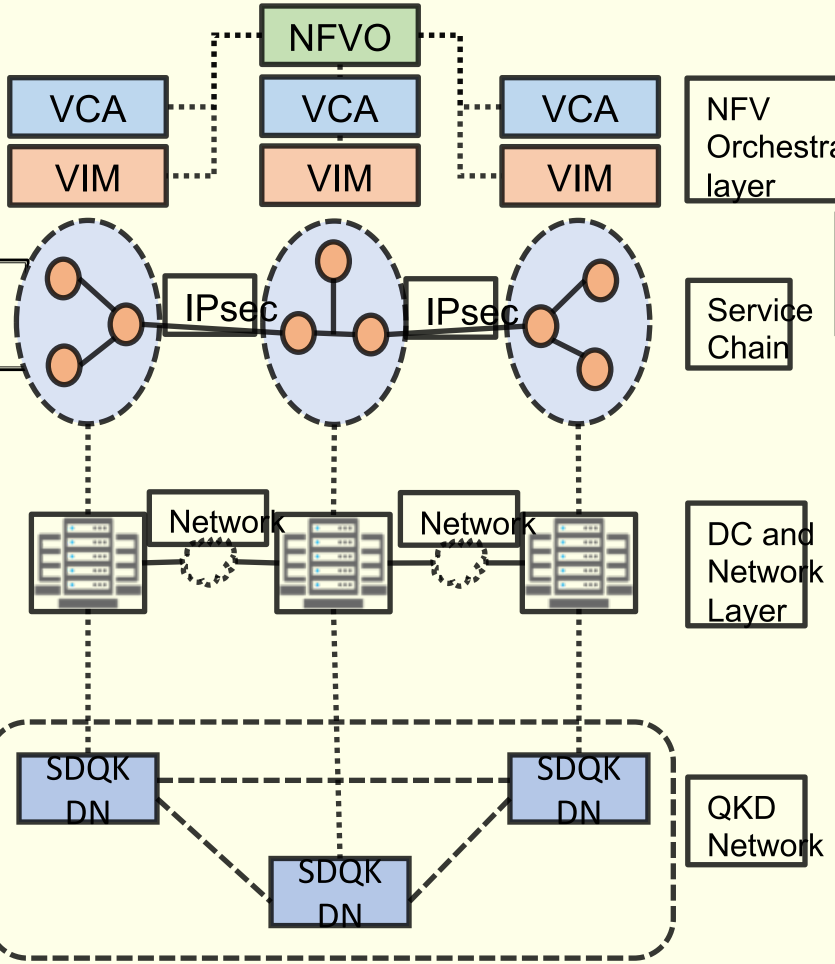
The connection to the network is through standard Communications systems.

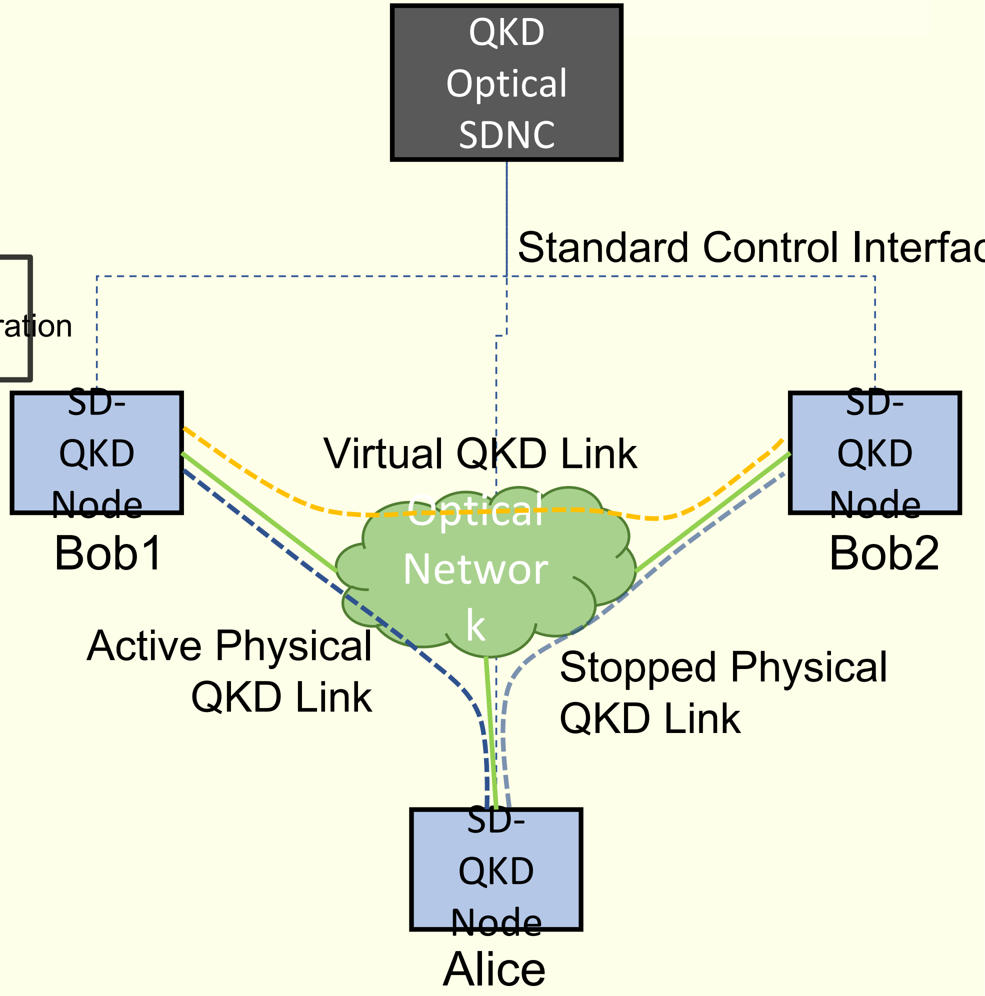
Demonstrated several use cases in a production environment



Critical Infrastructure control plane protection.

Data plane security





End to end quantum encrypted services

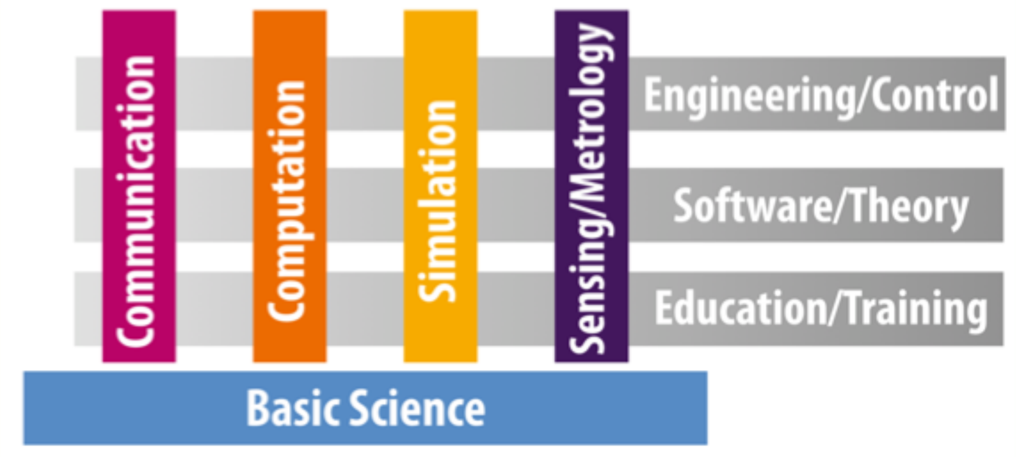
Conclusions

- Implementation of the **SDN concepts in a quantum/classical network.**
- The network is a “real world” network: out of the lab and in a **production environment.**
  - **Classical and quantum** communications **fully sharing the same networ**k, from the infrastructure to the management.
  - **QKD** is seen as an additional capability of the network that can be **exported to the application layer**.
  - Shows **high TRL** for the technology.
- The scheme allows for **incremental and easy deployment of quantum communications.**
  - Avoids large up front costs and ad hoc modifications to the network. Potential “Zero touch” integration.
- **Showcased practical use cases:**
  - Critical infrastructure protection.
  - Data plane security .
  - End to end encryption
  - … Others

SDN as an enabler and consumer of QKD in telco optical networks.

Future.

- H2020 **Quantum Flagship.**



- Extensions of the Madrid Quantum Network testbed.
  - Towards and European QKD network.
- Technological breakthroughs in CV-QKD (continuous variables)
  - CiViQ (Continuous Variables Quantum Communications, H2020 Flagship, Quantum communications pillar)

Future

- Evolution of the Madrid Quantum Network.
  - Technology is starting to be mature enough to be demonstrated in running networks.
  - Obviously: pending on future projects.

Consortium of 21 partners: 4 Research Institutes, 7 Universities, 2 SMEs, and 8 large companies

Call: H2020-FETFLAG-2018-2020

Funding: ~10 M€ over 36M

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 820466

CiViQ

Concept

Enhance the security of telecom network infrastructures using QKD

Requirements

Flexible QKD systems allowing for **seamless network integration** in modern carrier infrastructures

Photonic integration ideal for large-scale production and **cost-effective** QKD systems

Continuous Variable QKD Technology (CV-QKD)

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 820466

Objectives

Make QKD a mainstream technology for network and critical infrastructures security

Requirements and specifications driven by Telecom Industry Partners
(Equipment Manufacturers & Carriers)

Flexible, modular and network-aware QKD systems

- Standardized interface between components **Open Development Platform (ODP)**
- **SDN-interfaced QKD systems and networks**

Develop high performance QKD components and systems

- **GHz key rate** at 30km and **>150km reach**
- Strengthened **WDM Coexistence**
- **Cost-effective** & scalable QKD **system design**
- **Photonic integration** of components

Validation and benchmarking over Datacom and Telecom Infrastructures

- Production network environments
- End-to-end security

Prepare for next-generation Quantum Comm systems and networks

- Add **new CV quantum crypto functionalities**
- **Novel CV-QKD protocols** and **security proofs**
- Interfaces with satellite and quantum repeaters

This project has received

Thank you!

Comments & questions wellcome

Some Bibliography

- Vicente Martin, Jesus Martinez-Mateo, and Momtchil Peev. Introduction to quantum key distribution. In Wiley Encyclopedia of Electrical and Electronics Engineering, pages 1{17. 2017. ISBN 9780471346081. doi:10.1002/047134608X.W8354. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8354.
- D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin. Qkd in standard optical telecommunications networks. In Quantum Communication and Quantum Networking, volume 36, pages 142-149, 2010. doi:10.1007/978-3-642-11731-2 18
- M. Soto, D. Menendez, J. A. Pozas, V. Martin, D. Lancho, and J. Martinez-Mateo. System for integration of channels with quantum information in communications networks, 2011. Patent WO 2011/036322 A2.
- V. Martin, D. Lancho, M. Soto, and J. Martinez-Mateo. Method for a fine optical monitoring in communication lines through qkd systems, 2012. Patent WO 2012/089711 A1.
- A. Ciurana, J. Martinez-Mateo, M. Peev, A. Poppe, H. Walenta, H. Zbiden, and V. Martin. Quantum metropolitan optical network based on wavelength division multiplexing. Opt. Express, 22(2):1576{1593, Jan. 2014. doi:10.1364/OE.22.001576.
- A. Ciurana, V. Martin, J. Martinez-Mateo, B. Schrenk, M. Peev, and A. Poppe. Entanglement distribution in optical networks. IEEE J. Sel. Top. Quantum Electron., 21(3):6400212, May-June 2015. doi:10.1109/JSTQE.2014.2367241.

Some Bibliografía

- A. Ciurana, V. Martin, J. Martinez, and H. Zbinden. Multiplexor óptico pasivo, 2015. Patent P201331312, International extension: PCT/ES2014/070680.
- Alejandro Aguado, Victor Lopez, Jesus Martinez-Mateo, Thomas Szyrkowiec, Achim Autenrieth, Momtchil Peev, Diego Lopez, and Vicente Martin. Hybrid conventional and quantum security for software dened and virtualized networks. J. Opt. Commun. Netw., 9(10):819{825, Oct 2017. doi:10.1364/JOCN.9.000819. URLhttp://jocn.osa.org/abstract.cfm?URI=jocn-9-10-819
- Alejandro Aguado, Victor Lopez, Jesus Martinez-Mateo, Momtchil Peev, Diego Lopez, and Vicente Martin. Virtual network function deployment and service automation to provide end-to-end quantum encryption. J. Opt. Commun. Netw., 10(4):421{430, Apr 2018. doi:10.1364/JOCN.10.000421. URL http://jocn.osa.org/abstract.cfm?URI=jocn-10-4-421.
- Aguado, V. Martin, D. Lopez, and A. Pastor. Method and system for validating ordered proof of transit of traffic packets in a network, 2018. European Patent application EP18382095.