



POLITÉCNICA



Quantum Metropolitan Area Network based on Wavelength Division Multiplexing

V. Martin

U. Politécnica de Madrid

Work by

A. Ciurana, J. Martinez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden and V. Martin

[arXiv:1309.3923](https://arxiv.org/abs/1309.3923) [quant-ph]

1st ETSI Quantum-Safe-Crypto Workshop



26-27 September 2013, Sophia -Antipolis.



POLITÉCNICA

Outline



- Motivation And State of the Art.
- Network Framework.
- Design Principles and Constraints.
- Band Structure and Channel Plan.
- Test Network and Measurements.
- Conclusions



POLITÉCNICA

Motivation & State of the Art



➔ QKD is maturing very rapidly.

• Many **network demonstrators & testbeds** (with different targets):

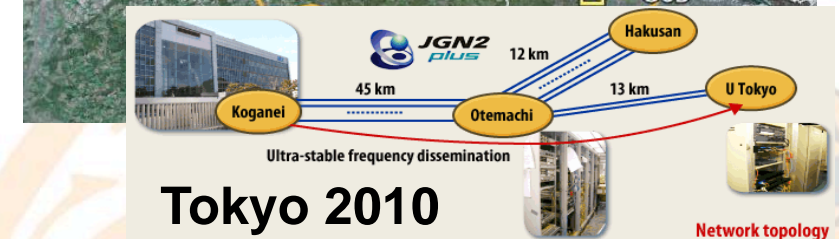
- Different QKD systems.
- Integration (trusted nodes)
- Durability.
- Integration in existing optical networks
- Special cases.
- New planned networks.



Boston 2005



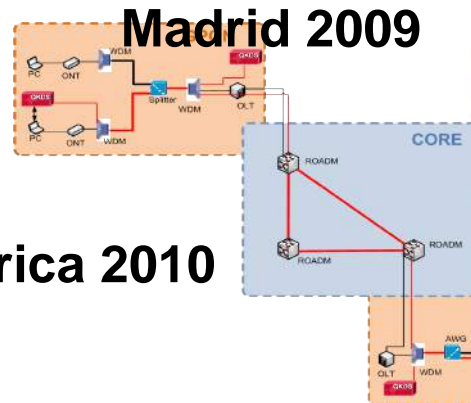
Vienna 2008



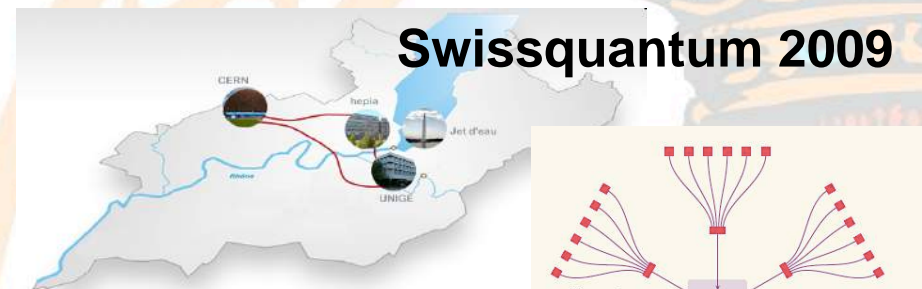
Tokyo 2010



Battelle 2014

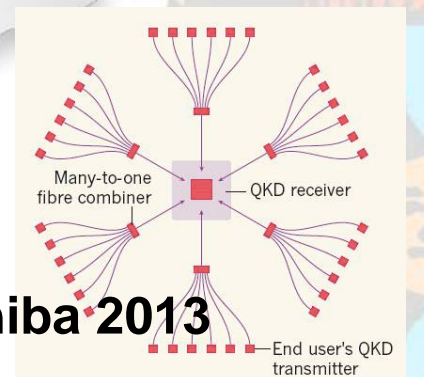


Madrid 2009



Swissquantum 2009

South Africa 2010
China ...



Toshiba 2013



POLITÉCNICA

Motivation & State of the Art



- **Better systems:** Higher rate systems, more tolerance to losses and noise, industrialization, proven technology, attacks, compactness, etc...
- High rate, long-distance... D. Stucki et al. (2008, 42.6 dB losses, COW, SSPD)
 - Coexistence, High-Bit-Rate... K.A. Patel et al. (2012, 18 dB losses, BB84+Decoy, APDs, two 1.25 Gb/s data channels separated 20 and 61 nm from quantum. CWDM)
 - Complete, new high speed systems, NanoTera project N. Walenta et al. (2013) arXiv:1309.2583 [quant-ph]
 - Compact systems with Application to Critical Infrastructure Protection Hughes et al. (2013, network with trusted third party structure...)
 - etc...

→ **Pervasive all optical/passive Networks.**

- Optical fibers everywhere: possibility of establish a quantum channel (metro area).





POLITÉCNICA

Motivation & State of the Art



- However, **despite these advances**, from a **commercial perspective**:
 - **Expensive**: QKD is neither cheap nor easy.
 - **Limited market**: Symmetric key distribution is not a broad market.
 - **Security Level**: “trust what people use”. The claimed level of security has still to be 'proven' in practice by general adoption.
 - **Not flexible**: Limited to ciphering point to point communications: Need to reconfigure connections to serve user's needs.
- **Costs, deployment (and flexibility) penalize** the adoption of **QKD**.
 - **Network infrastructure cost** (deploying, leasing, etc) are much **bigger than the cost of QKD** systems (not cheap, either!).
 - QKD Networks up to date are “exclusive quantum usage”



POLITÉCNICA

Motivation & State of the Art

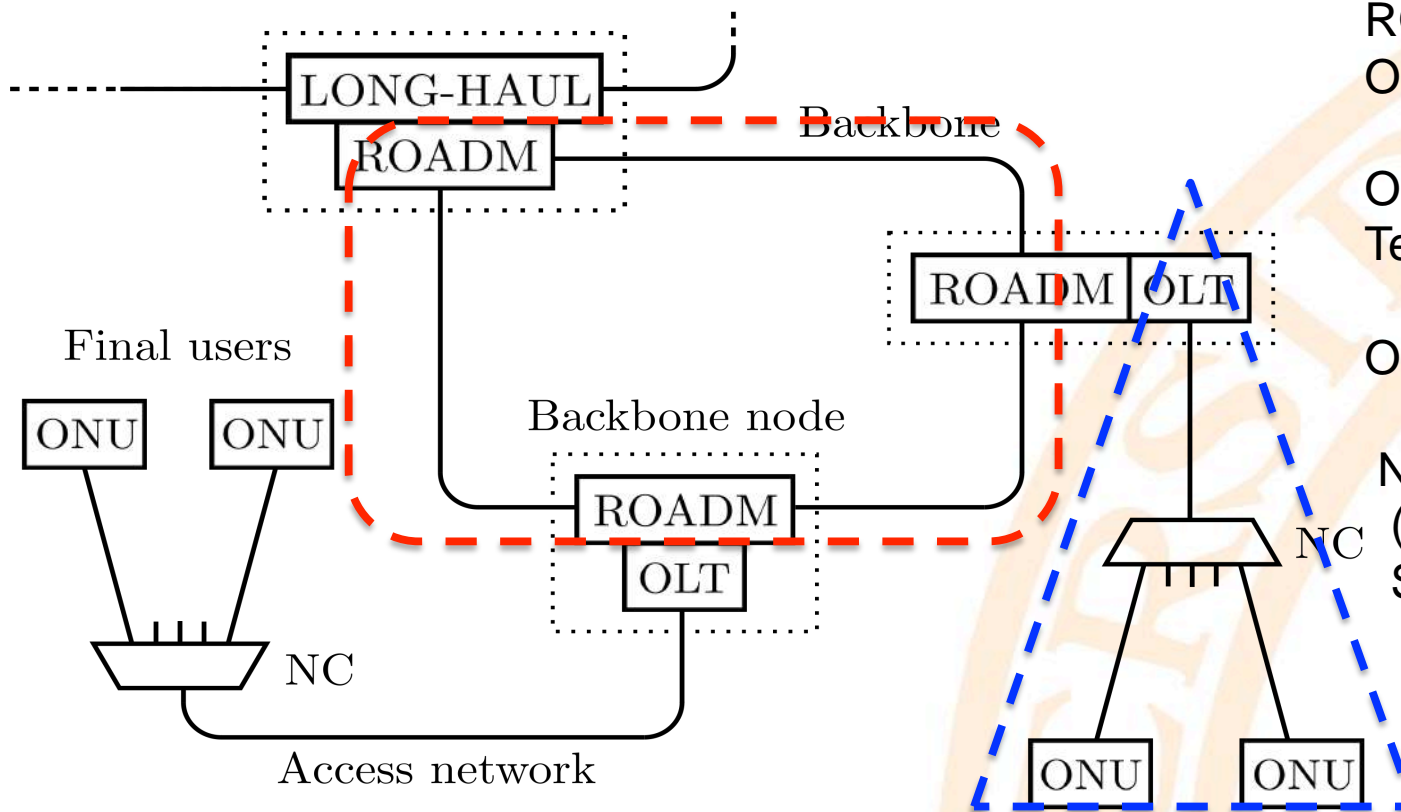


- **OBJECTIVE: Lower the barriers to a wider adoption of QKD by lowering infrastructure costs: A flexible QKD Network easy to deploy**, where the infrastructure **reuses what is installed** and is **shared among as many other systems as possible** in a metro area **without trusted nodes**.
 - Target **32-64 QKD systems** on the same fiber for a **significant cost decrease**.
 - Stay within a maximum **budget loss** (<30 dB, **metro area**)
 - A quantum network transports **not only quantum signals**:
 - It has to support classical signals associated to QKD equipment (service channel). Ideally, include also key distillation.
 - **Possibility of mixing with attenuated classical communications signals**.
 - Very advantageous in certain scenarios.
 - Number of signals is limited.
 - Support for as many different QKD designs as possible: **interoperability**
 - Not targeting alice-bobs of different manufacturers but seamless plugging new QKD devices in existing network. “standard looking” proposal (simple to implement & deploy)



Framework

- We will consider a passive “**canonical metro network**”: A **backbone ring** connecting the **access networks**.



ROADM: Reconfigurable Optical Add/Drop Module

OLT: Optical Line Termination

ONU: Optical Network Unit

NC: Network Component (AWG: WDM-PON, Splitter: GPON)



POLITÉCNICA

Design Principles & Constraints



- Stay well within the loss budget of current QKD systems (<30 dB, Metro area)
- Use existing fiber infrastructure.
- Use existing, industrial grade, network components.
- “standard-like” infrastructure.
- Passive components.
- **Choices** biased towards a maximum coexistence of quantum and classical signals but considering the existing industrial ecosystem.



POLITÉCNICA

Design Idea

[arXiv:1309.3923](https://arxiv.org/abs/1309.3923) [quant-ph]



- Use a **mixture of Coarse/Dense** Wavelength Division Multiplexing.
- **Wavelength Addressing & Standard components:**
 - Use AWGs: **periodicity** and “low” losses.
 - Use the Coarse (20 nm) grid for addressing access networks.
 - Use the Dense (< 0.8 nm) grid for addressing users within an access network.
- **Separated Quantum and Classical bands** (> 150 nm) to avoid noise.
 - **Choice:** 13xx nm for quantum, 15xx for classical.



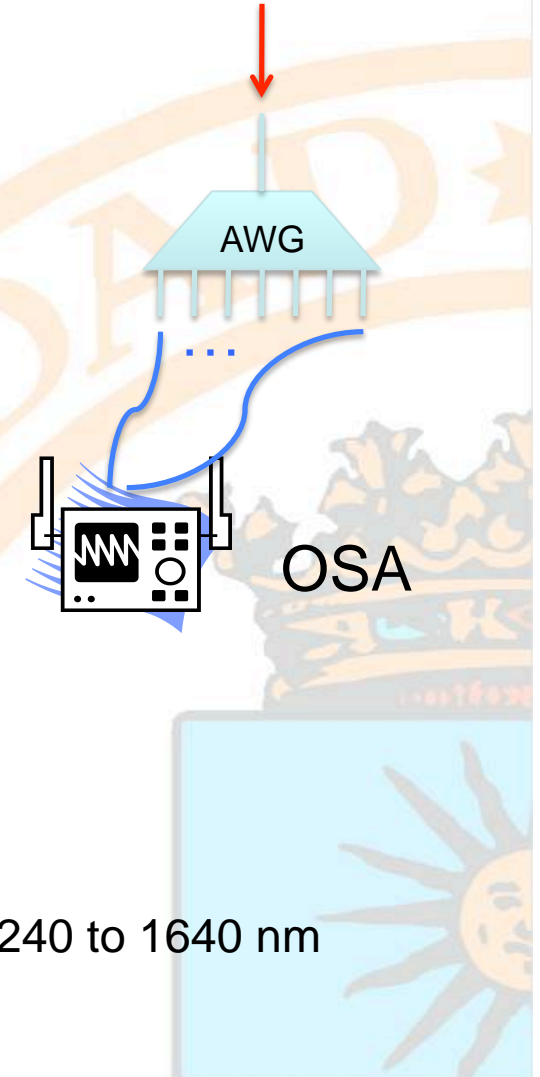
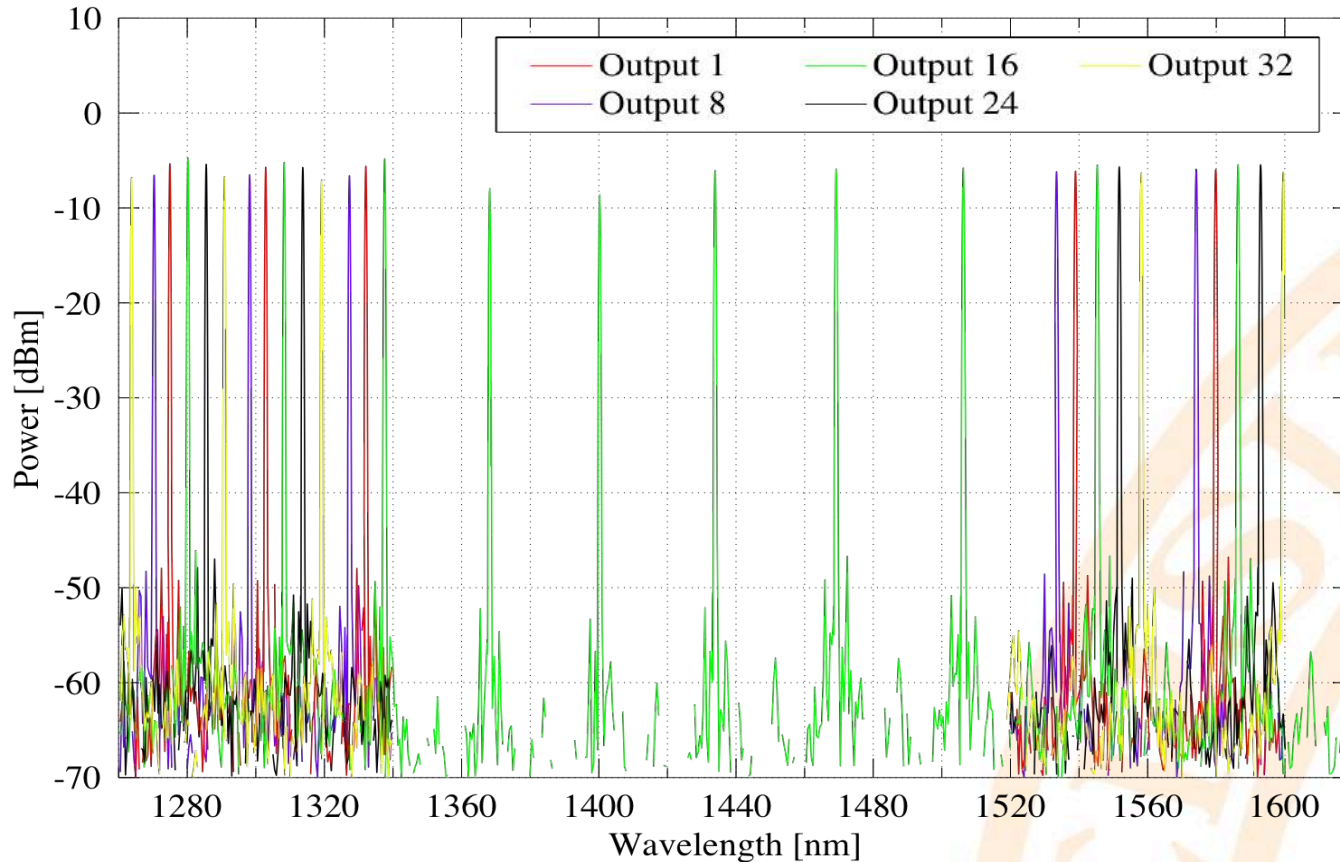
POLITÉCNICA

Design: AWG periodicity



CENTRO DE SUPERCOMPUTACIÓN Y VISUALIZACIÓN DE MADRID

Tunable Laser
1240-1640 nm



Testing the AWG periodicity: An 1:32 AWG is fed with laser light from 1240 to 1640 nm



POLITÉCNICA

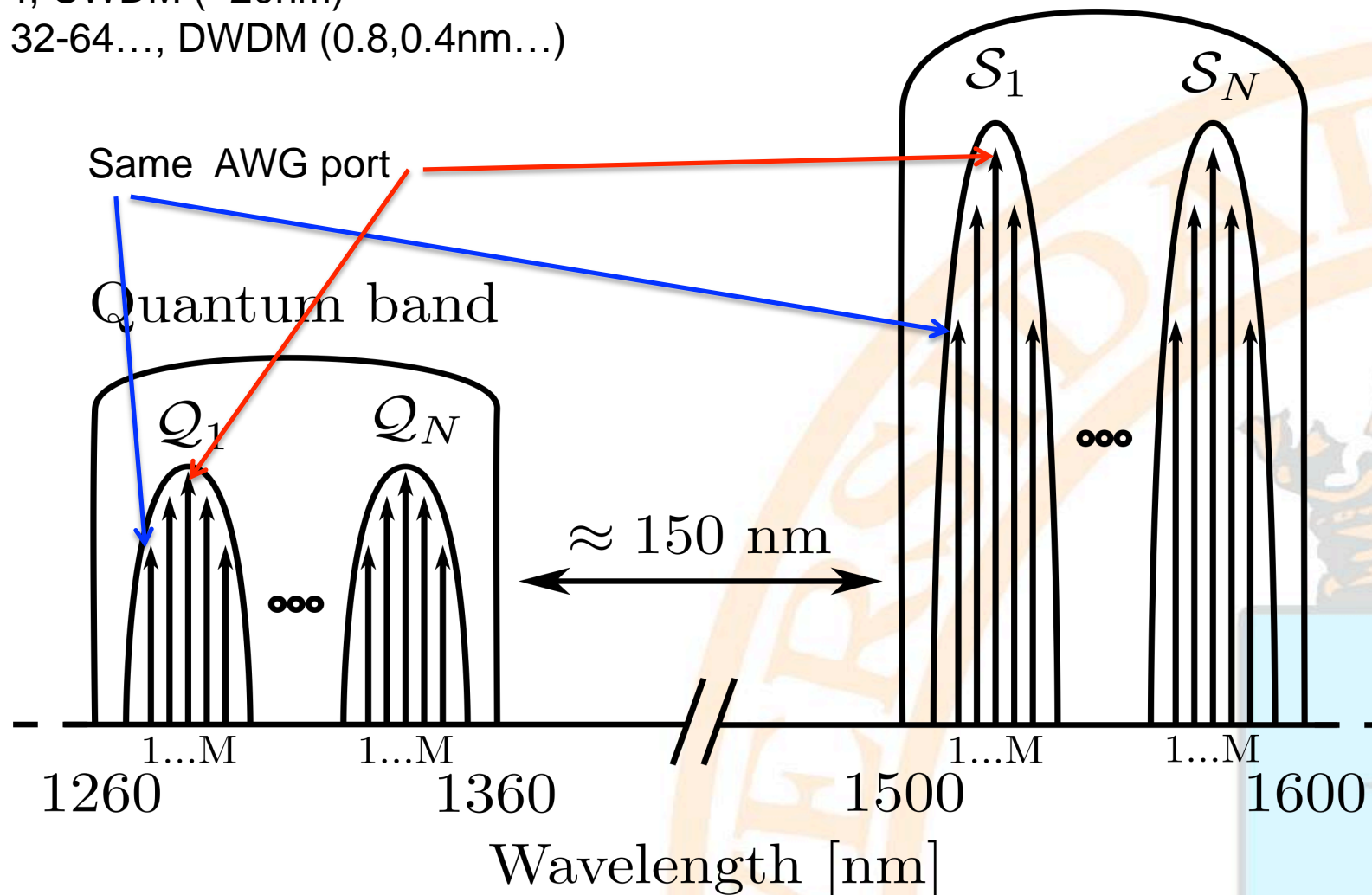
Design: Band Structure and Channel Plan



$N \sim 4$, CWDM ($\sim 20\text{nm}$)

$M \sim 32-64\dots$, DWDM ($0.8, 0.4\text{nm}\dots$)

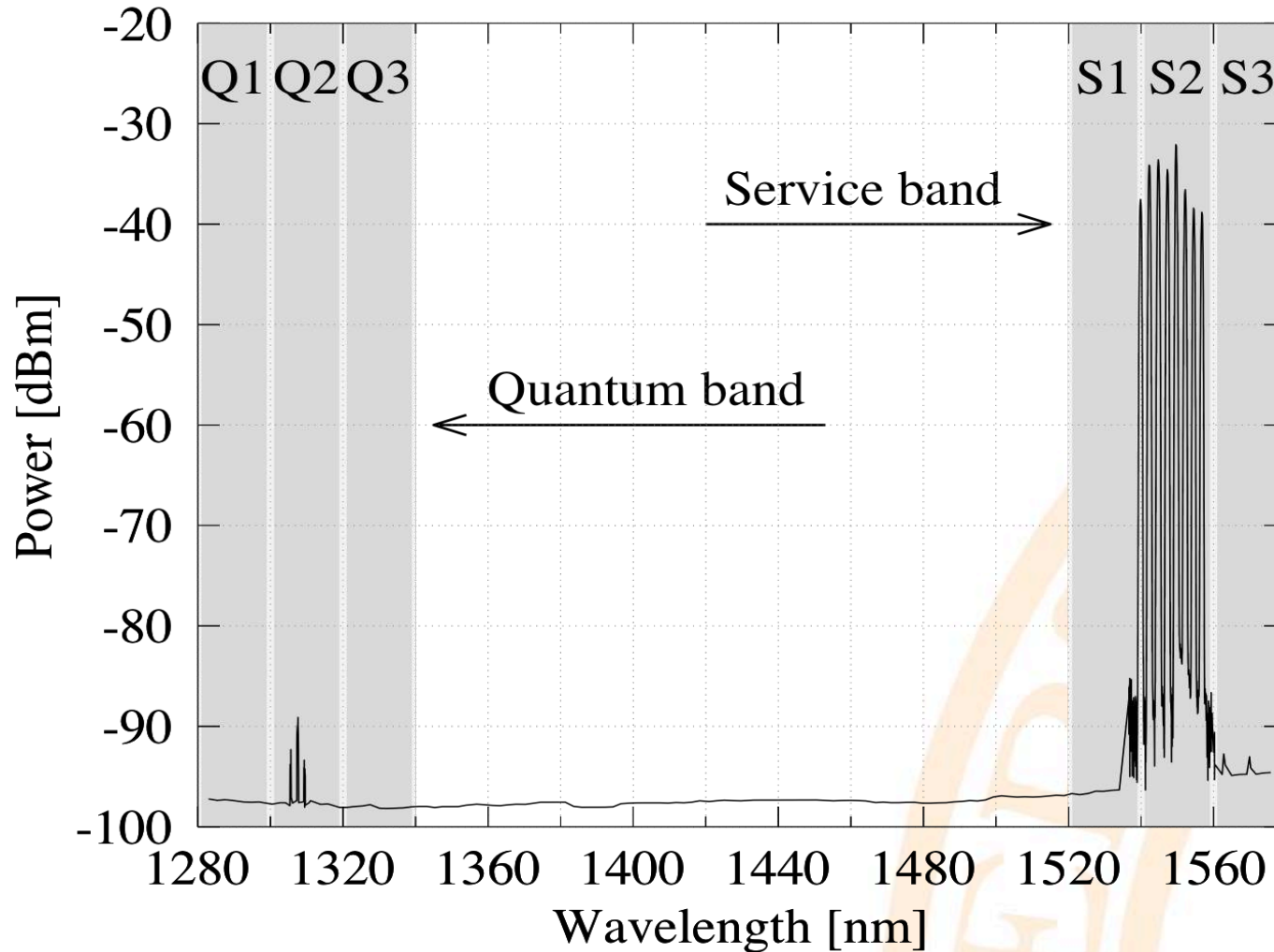
Service band



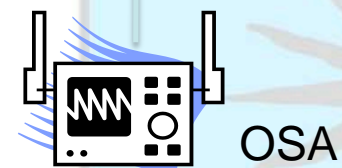


POLITÉCNICA

Design: Band Structure and Channel Plan



The corresponding experimental results: CWDM filters 20nm, 32 channels 100 GHz (0.8nm) DWDM AWG.



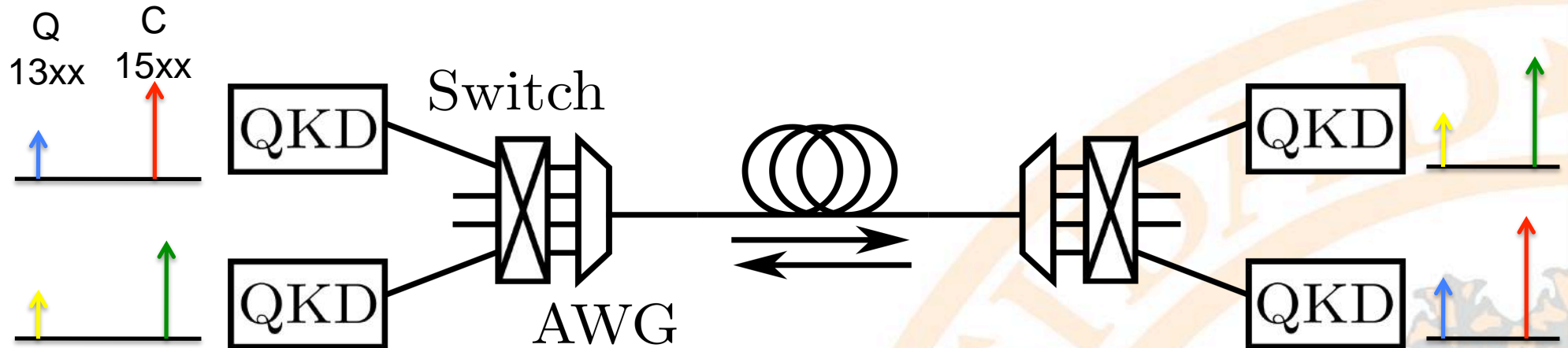


POLITÉCNICA

Use of Periodicity in Practice: A Very Simple Network



Two Access Networks are connected through a backbone that is just a single fiber.



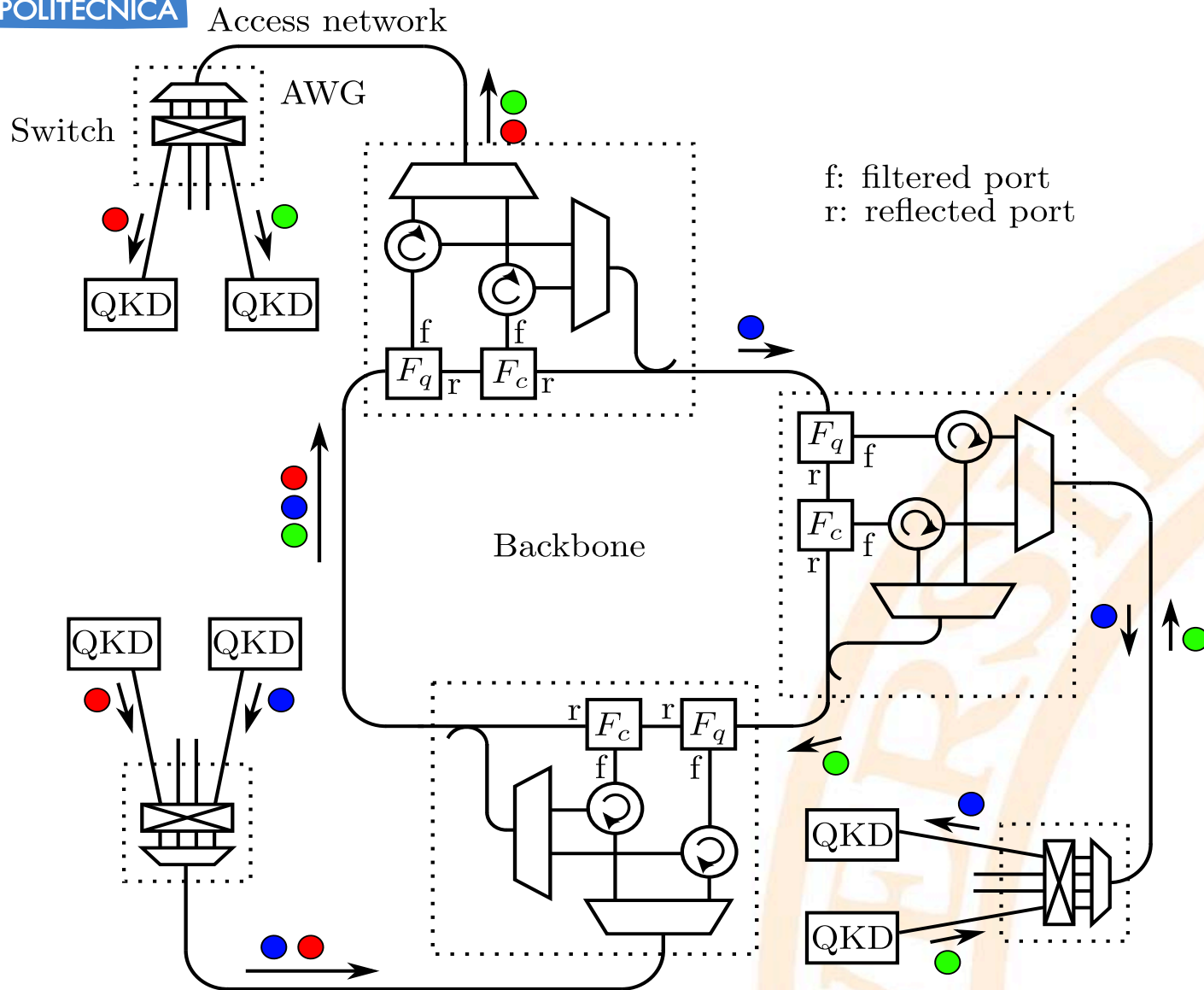
Any Alice system can connect with any Bob system on the other side of the network just by selecting two wavelengths: one for the quantum channel (in 13xx) and other for the service channel (in 15xx, related to the selected quantum 13xx through the AWG periodicity).

- Only one switch is mandatory, but then all Alices must be on one access network and all Bobs on the other. Two are required only Alices and Bobs are to be mixed on the same side.



POLITÉCNICA

Full Test Network



Three Access Networks are connected through a ring backbone. Any QKD Bob device can talk to any QKD Alice device. A colored dot represent a pair of wavelengths on the same AWG-periodical set.



OADM Module

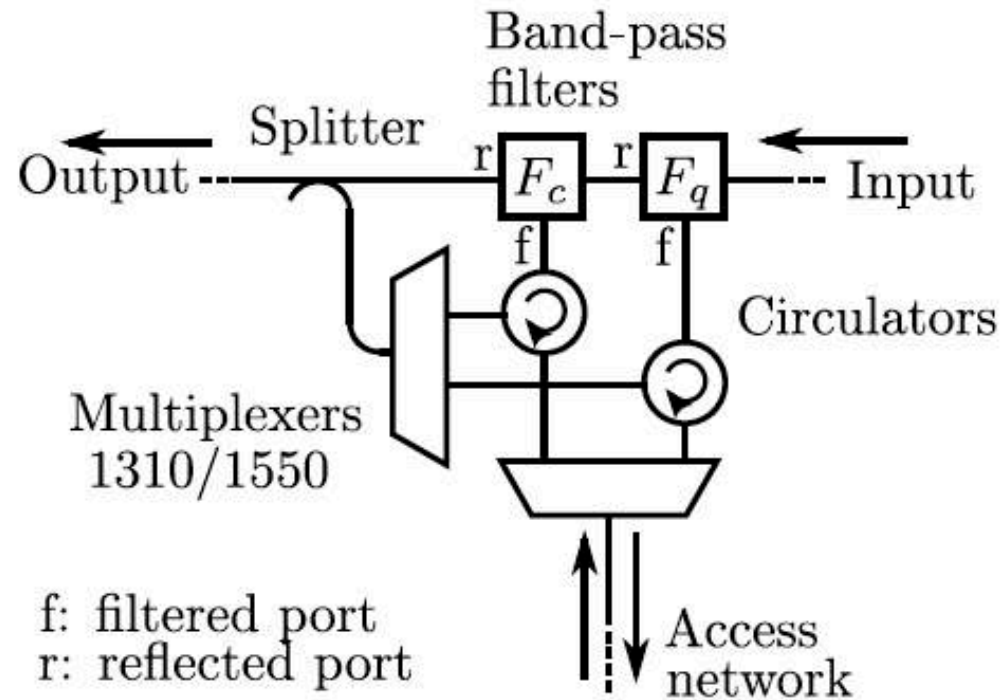
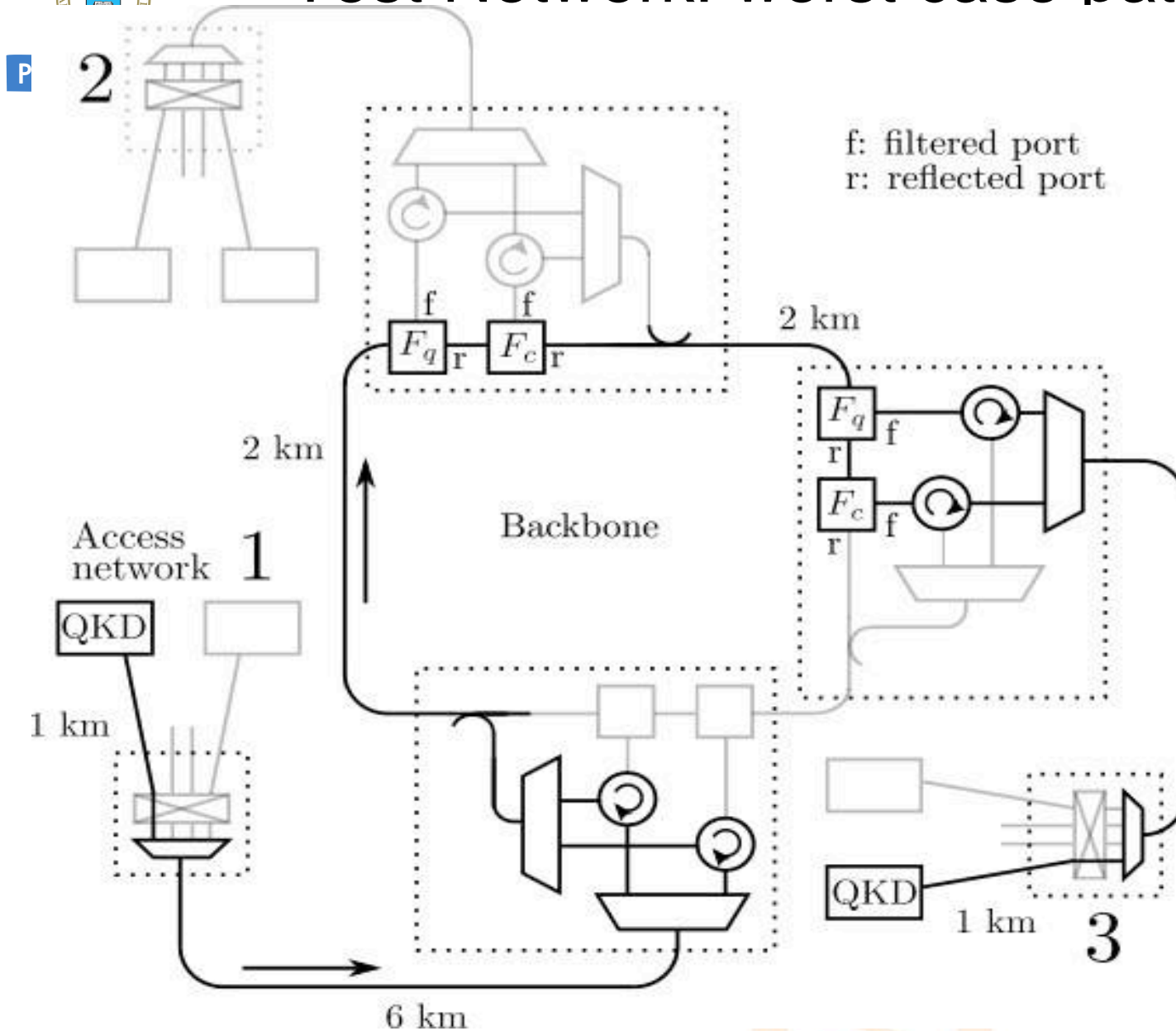


Fig. 5. Backbone node: OADM designed for the QKD-MON. Built out of common network components, it drops the quantum and service subbands from the ring's signal (input) to the access network, and adds any channel coming from the access network, no matter which subband it belongs to, to the ring (output).



Test Network: worst case path



Worst case path (for noise and losses) in the testbed network. The longest fibers are in the entry points, where most Raman is produced.

Worst case Losses:
Quantum = 23.1 dB
Classical = 20.6 dB



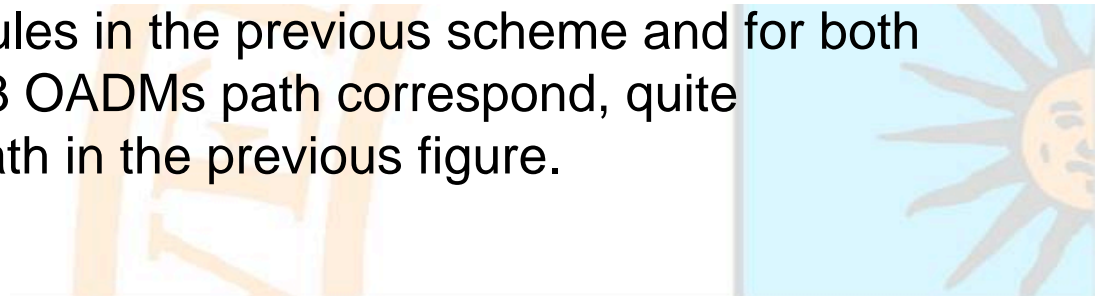
POLITÉCNICA

Test Network: Modules and Total Losses



Network component	Losses (quantum)	Losses (service)
Switched AWG	4 dB	4 dB
OADM (add)	4.8 dB	4.8 dB
OADM (pass)	5.4 dB	5.4 dB
OADM (drop)	1.7 dB	2.3 dB
10-km path (2 OADMs)	18.1 dB	17.5 dB
15-km path (3 OADMs)	24.7 dB	23.2 dB
20-km path (4 OADMs)	31.1 dB	28.9 dB
30-km path (5 OADMs)	39.1 dB	35.5 dB

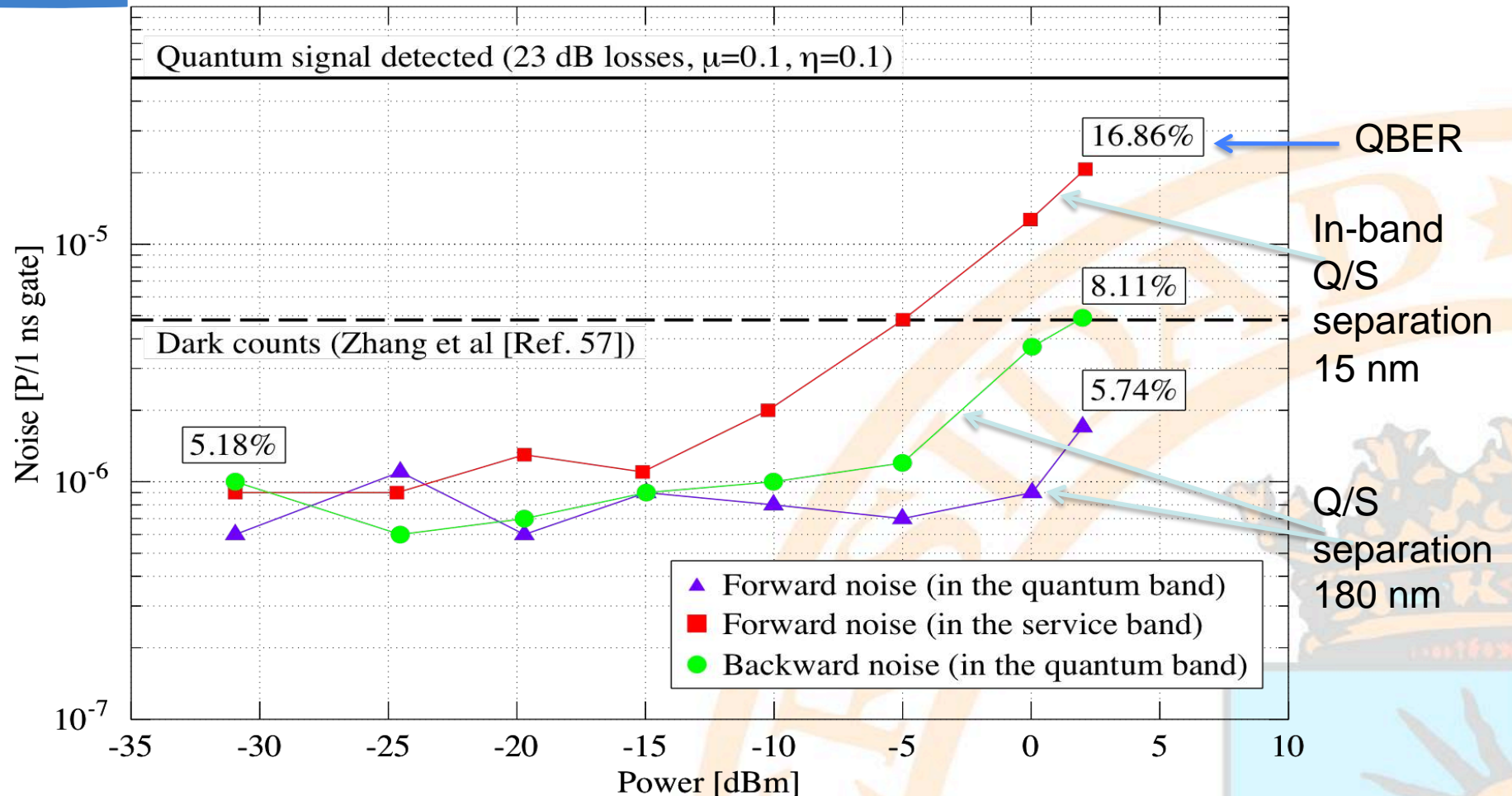
Measured losses for network modules in the previous scheme and for both bands. Losses for the 15 Km and 3 OADMs path correspond, quite approximately to the worst case path in the previous figure.





POLITÉCNICA

Test Network: worst case noise measurements



Total noise measurements in the worst case path. In the forward noise (quantum), all emitters are located on one side and noise is measured on the opposite. Backward noise is measured on the same side. Forward (in service) correspond to an out of specs situation where a quantum channel is located in the service band.



POLITÉCNICA

Conclusions



- The scheme is **easy to integrate** in optical networks, **cheap**, **no trusted nodes**, **compatible** (within limits) with classical signals.
- The scheme can **tolerate, at least, +2 dBm total power in the service** (using 1ns gates) band while keeping the QBER below the threshold.
- This means **32 channels at -13 dBm**.
 - -13 dBm is enough to have a -34 dBm signal in the worst case path of the testbed network.
 - -34 dBm sensitivity SFP detectors exist and the scheme **allows for 32 1.25 Gbps link with less than $10E-9$ error rate**.
 - A 1.25 Gbps link can be used for key distillation or classical communications.



Conclusions

- SPDs with less than 1ns gates are now common. This would increase the number of classical channels allowed and the performance of the network.
- To do key distillation a bidirectional link is needed.
 - The ring is directional.
 - A return path is already located in the network, but the switch must be reconfigured for a different connection.
 - Simultaneous use of the quantum channel and key distillation by the same QKD pair cannot be done.



POLITÉCNICA

Future



- Proposal is designed for One Way Prepare and Measure QKD systems:
 - Extension to Entangled pairs and Continuous Variables Systems.
- Usually a network is considered more resilient to attacks because of the many paths available but, are there network derived attacks and weaknesses from the QKD perspective?
- Characterize network behavior under real loads.



POLITÉCNICA



Thanks for your Attention!!

Questions?

