QKD in Dense WDM Passive Optical Networks

V. Martin
U. Politécnica de Madrid

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

Workshop on Quantum Telecommunications

15-17 May 2013, Lisbon.

Outline

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

Motivation & State of the Art

- QKD is maturing very rapidly:
  - Faster systems reaching further away (more tolerance to losses and noise).
  - More compact and easy to manufacture.
  - Networks (mostly based on trusted repeaters)
  - Standards are starting to be developed.
  - Some maturity due to being “mature”:
    - More proven technology.
    - Type of attacks better known.

- Network technology is mostly becoming all optical/all passive.
  - Optical fibers everywhere.
  - It is possible to create and uninterrupted point to point clear path that can support a quantum channel.
    - At least in a metro area.

Motivation & State of the Art

- High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres.

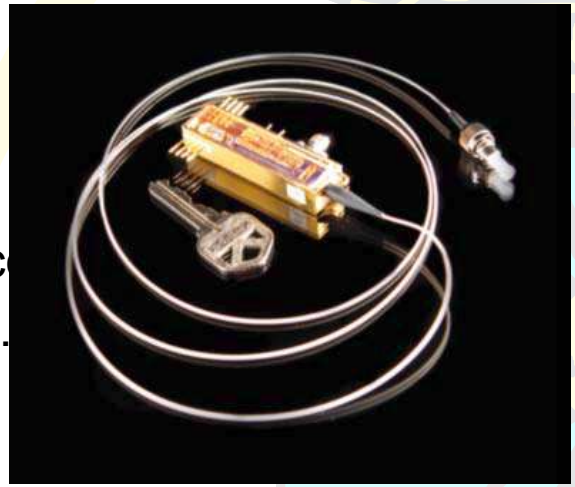
D. Stucki et al. (2008, 42.6 dB losses, COW, SSPD)

- Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber.

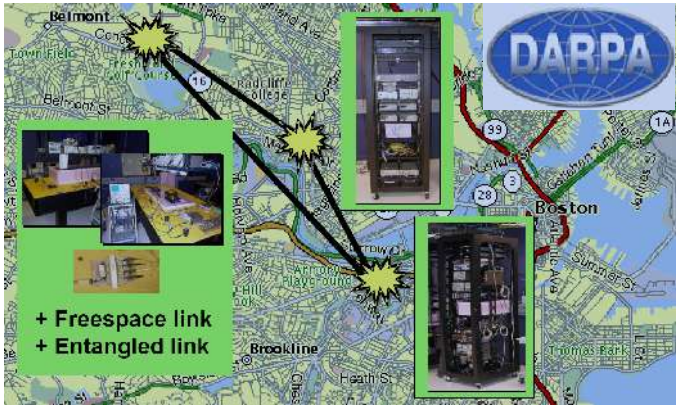
K.A. Patel et al. (2012, 18 dB losses, BB84+Decoy, APDs, two 1.25 Gb/s data channels separated 20 and 61 nm from quantum. CWDM)

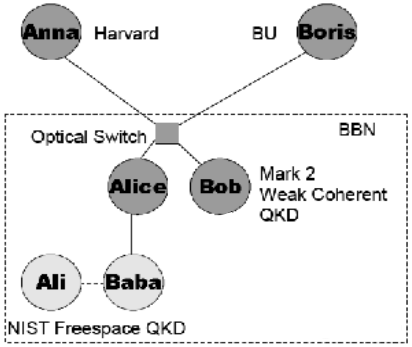
- Network-Centric Quantum Communications with Application to Critical Infrastructure Protection

Richard J. Hughes et al. (2013, network with several protocols. Quantum 15xx + Classical 13xx. BB84+Dec encoding. Compact Bob. Trusted third party structure… Actually a collection of point to point QKDs)

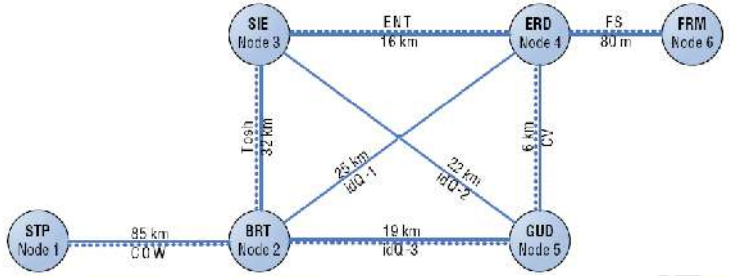


Motivation & State of the Art

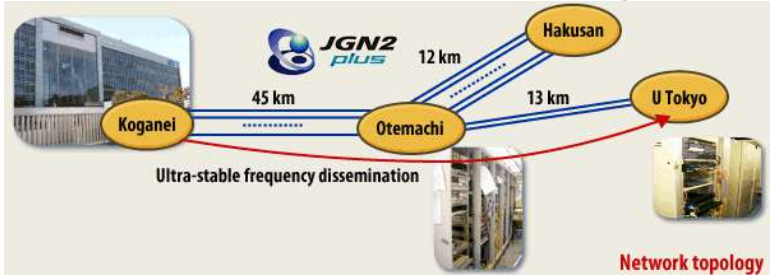




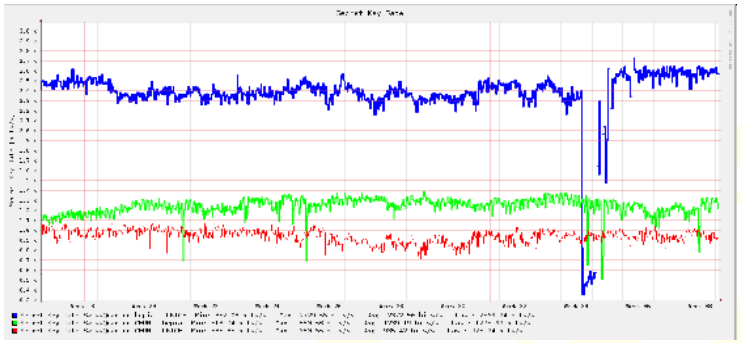
SECOQC **2008**



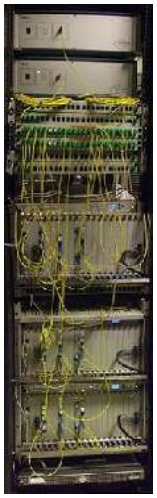
Tokyo QKD Network **2010**

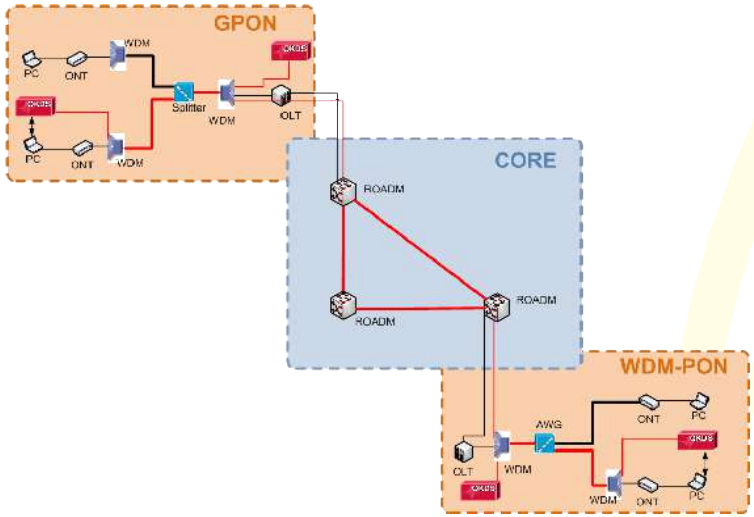


Motivation & State of the Art



SwissQuantum: Stable operation from April 2009 to November 2009





The Madrid QKD Test-Bed: WDM + optical network integration

Motivation & State of the Art

- QKD is maturing very rapidly:
  - Faster systems reaching further away (more tolerance to losses and noise).
  - More compact and easy to manufacture.
  - Networks (mostly based on trusted repeaters)
  - Standards are starting to be developed.
  - Some maturity due to being “mature”:
    - More proven technology.
    - Type of attacks better known.

- Network technology is mostly becoming all optical/all passive.
  - Optical fibers everywhere.
  - It is possible to create and uninterrupted point to point clear path that can support a quantum channel.
    - At least in a metro area.

Motivation & State of the Art

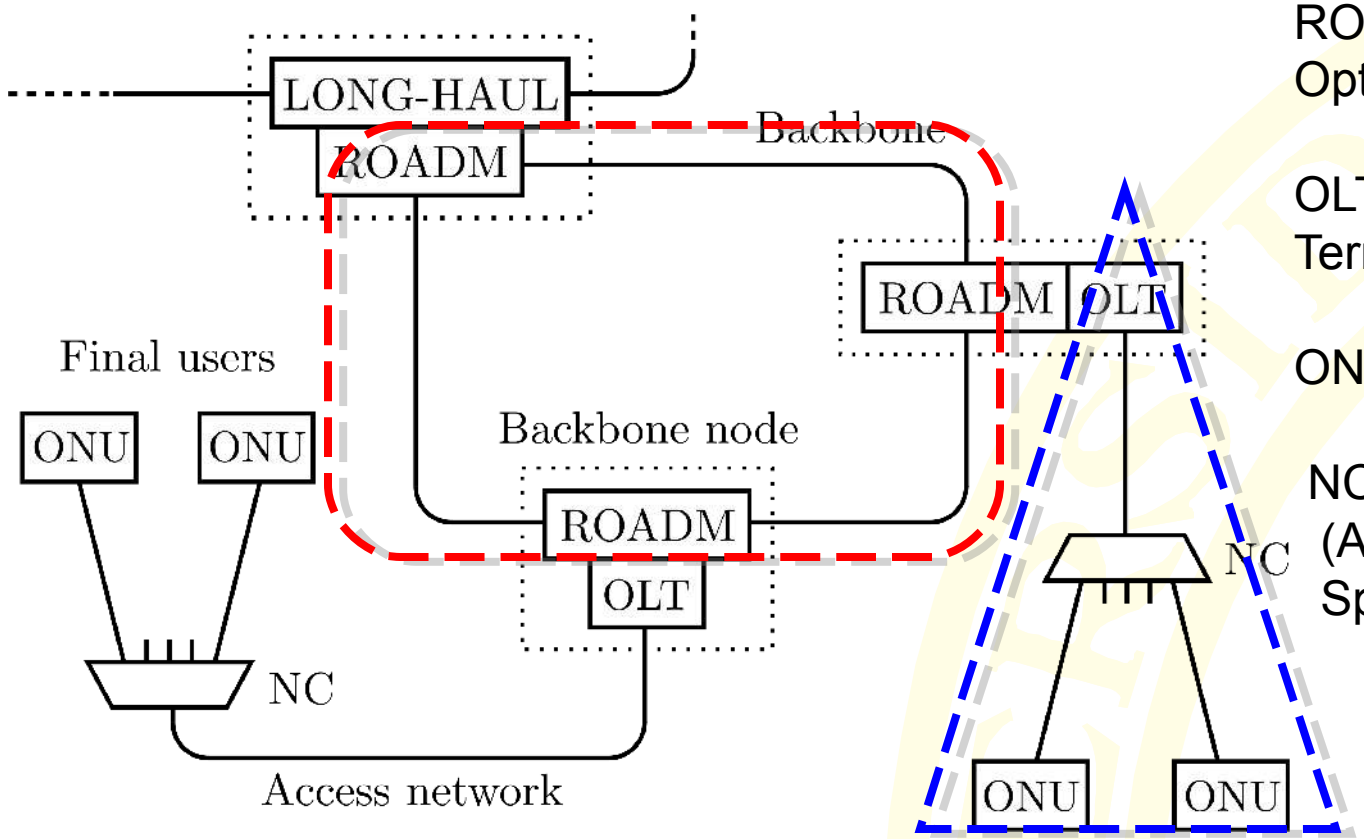
- However, from a commercial perspective:
  - QKD is **neither cheap nor easy.**
  - Symmetric k**ey distribution is not a broad market.**
  - **The claimed level of security has still to be 'proven' in practice by general adoption.**
  - **Limited to ciphering point to point communications: Need to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

Motivation & State of the Art

- **OBJECTIVE: A QKD Network where the infrastructure is shared among as many QKD systems as possible in a metro area.**
- **Possibilities:**
  - **Mix with attenuated classical communications** signals.
    - Very advantageous in certain scenarios.
    - Number of signals is limited.
  - Design **a quantum only network**.
    - Has to support classical signals associated to QKD equipment.
    - Support for as many different QKD designs as possible.
      - Seamless plugging new QKD devices in existing network.
    - Target 32-64 QKD systems on the same fiber for a significant cost decrease.
    - Within a maximum budget loss (<30 dB, metro area)
  - **Both?**

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 Uni

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

Design Principles & Constraints

- First: Quantum Only
  - Must allow the simultaneous use of as many different QKD pairs as possible.
    - Classical signals for the QKD “service” channel must be included.
- Second: Add more classical.
  - Include Key Distillation.
  - Research the limits of including more classical communications

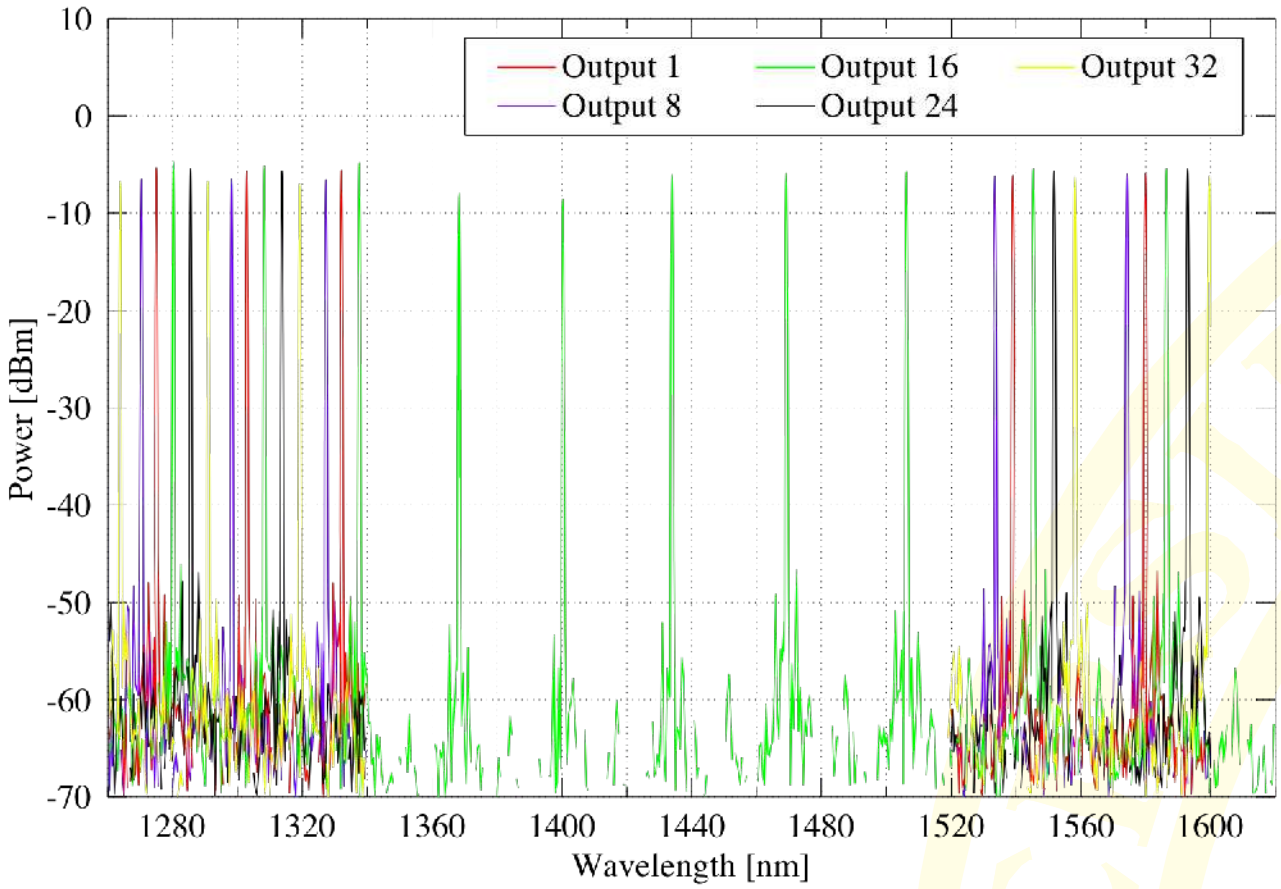
Design Principles & Constraints

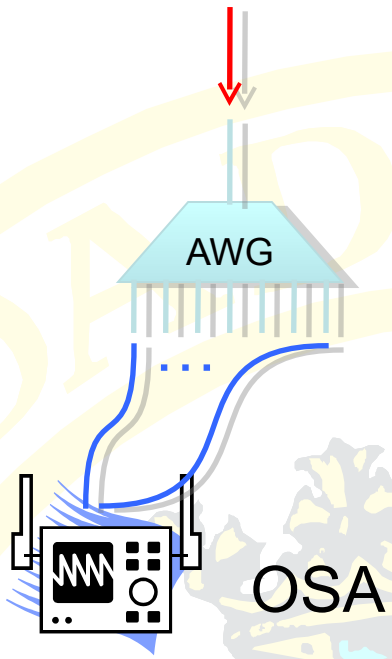
- Stay well within the loss budget of current QKD systems (<30 dB, Metro area)
- Use existing fiber infrastructure.
- Use existing, industrial grade, network components.
- Choices biased towards a maximum coexistence of quantum and classical signals but considering the existing industrial ecosystem.

Design

- Use a mixture of Coarse/Dense Wavelength Division Multiplexing.
- Wavelength Addressing:
  - 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.
- Use a Quantum band and a Classical band separated >150 nm to avoid noise.
  - Choice: 13xx nm for quantum, 15xx for classical.

Design: AWG periodicity

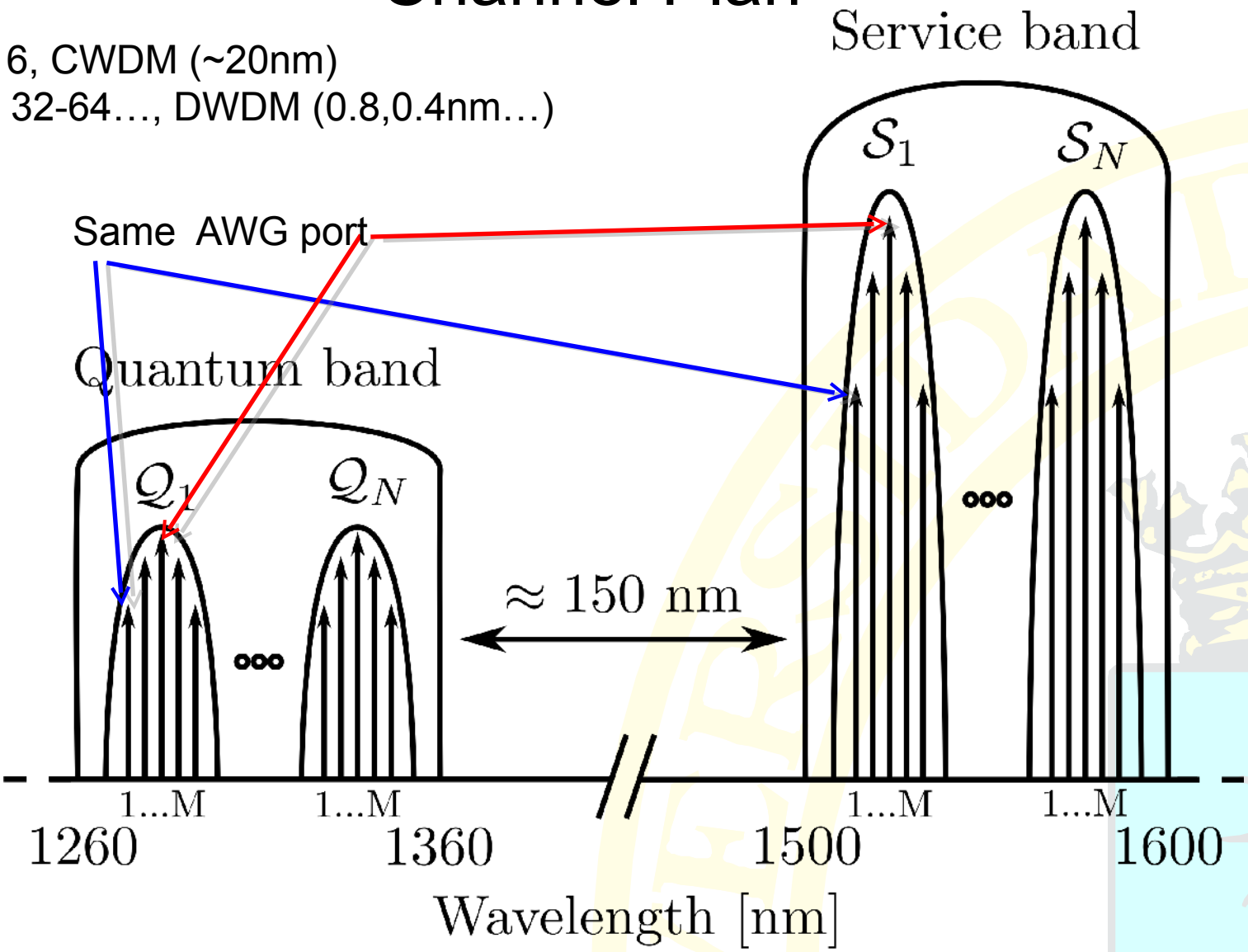




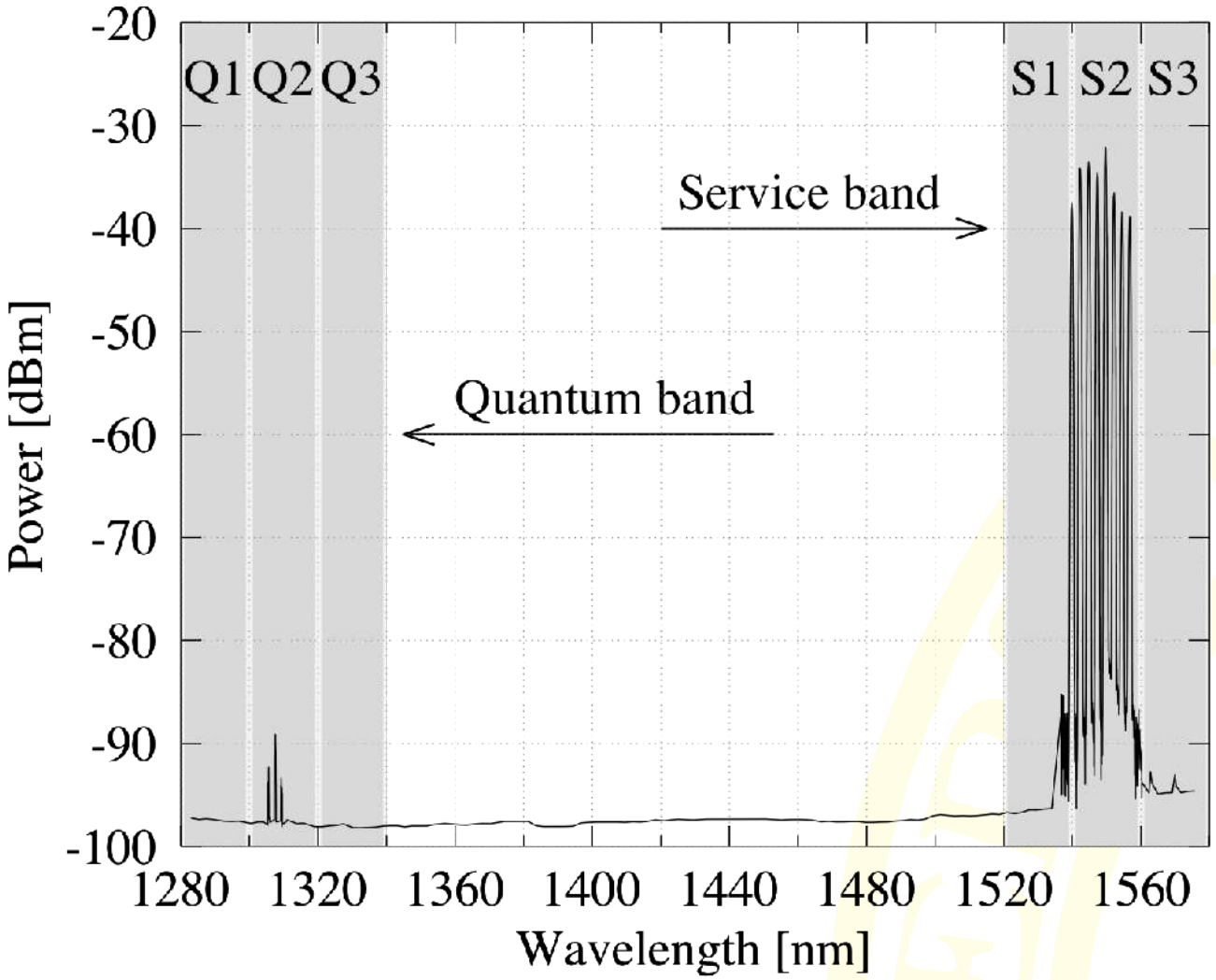
Testing the AWG periodicity: An 1:32 AWG is fed with laser light from 1240 to 1640 nm

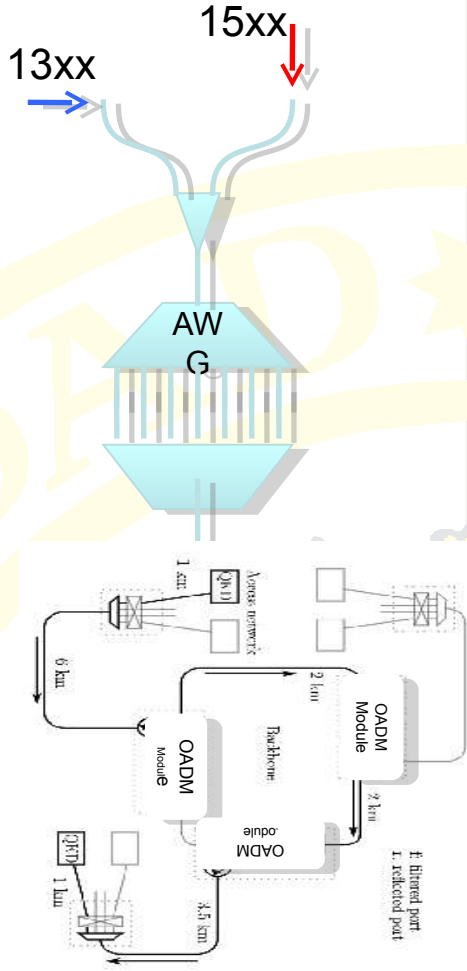
Design: Band Structure and Channel Plan

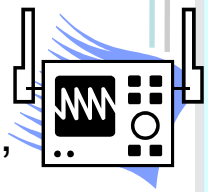
N ~ 6, CWDM (~20nm)
M ~ 32-64…, DWDM (0.8,0.4nm…)



Design: Band Structure and Channel Plan





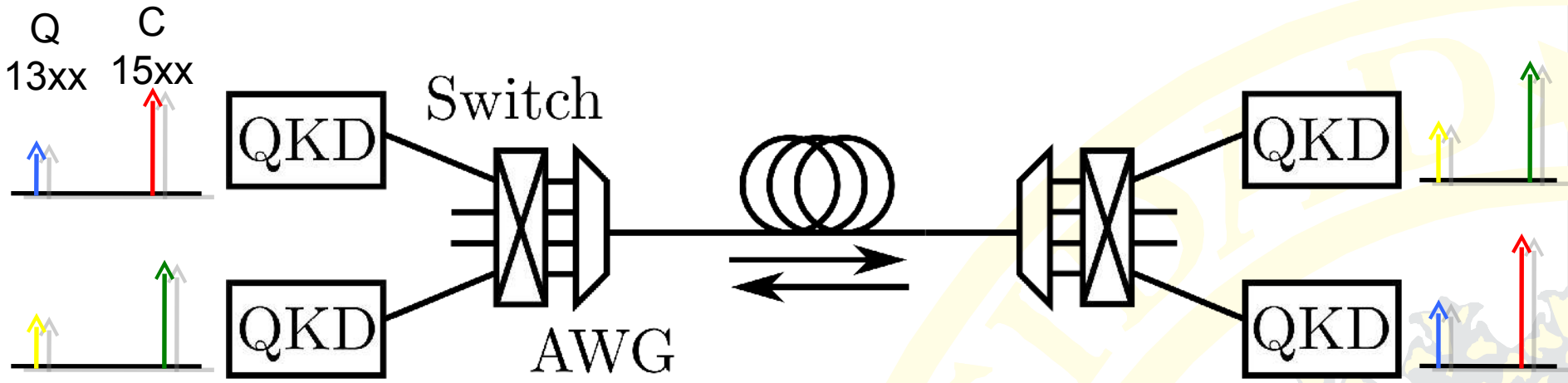


OSA

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

Illustration: A Very Simple Network

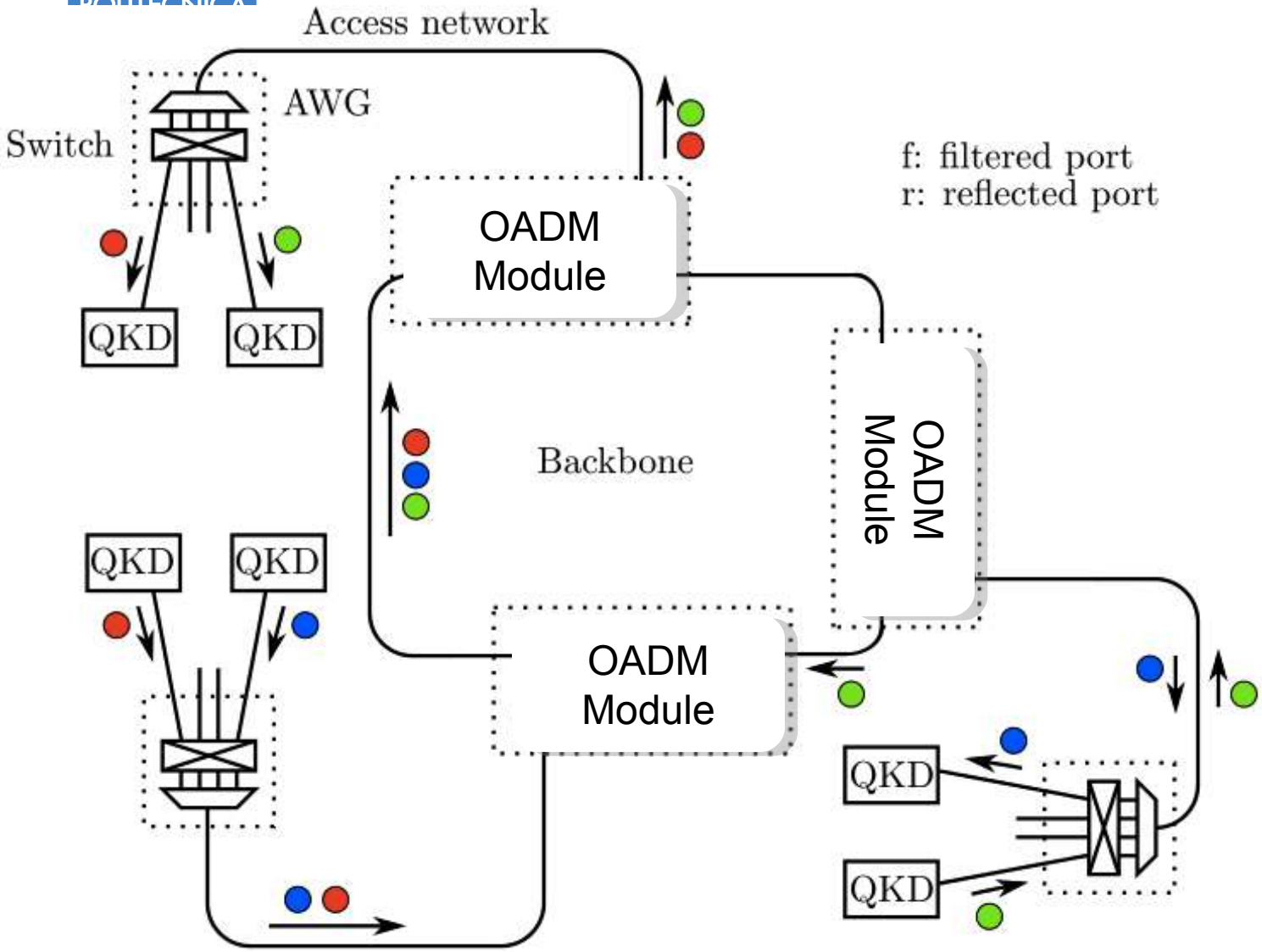
Two Access Networks are connected through a backbone that is just a single fiber.



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.

Test Network



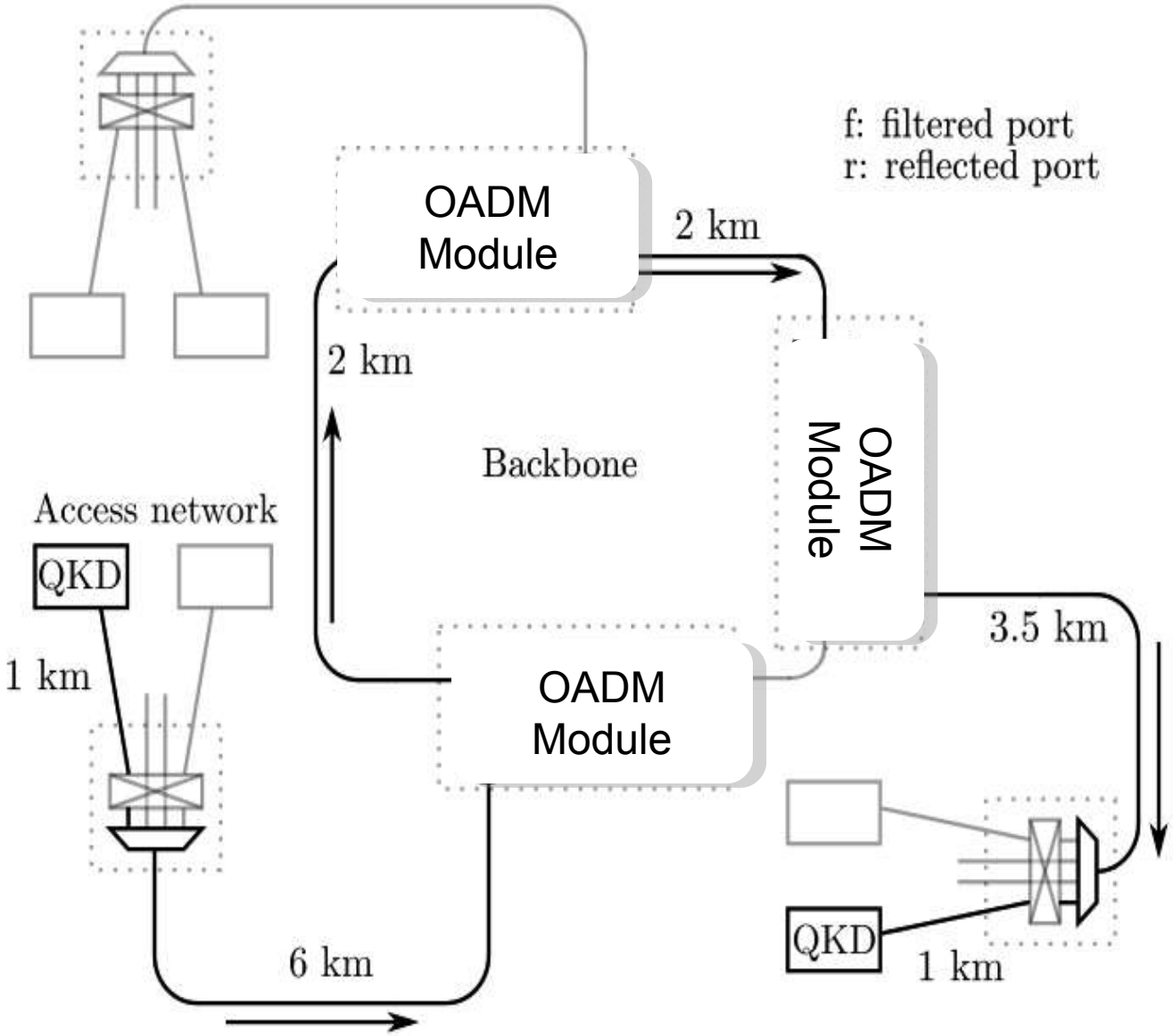
Three Access Networks are connected through a ring backbone. Any QKD Bob device can talk to any QKD Alice device. A colored dot represent a pair of wavelengths on the same AWG-periodical set.

Test Network: Component Losses

Device	Losses
Single-mode fibre (C band)	0.18 dB/km
Single-mode fibre (O band)	0.32 dB/km
Connectors	0.2 dB/pair
1×2 Splitter	3.6 dB
1×32 Splitter	16.5 dB
4×4 to 192×192 Switch	1 dB
Circulator	0.8 dB
CWDM filter	$0.4 - 0.6$ dB
1310/1550 WDM multiplexer	0.5 dB
32-ch AWG DWDM multiplexer	3 dB

Measured losses for network components in the previous scheme. If band is not specified, they are the same for both bands.

Test Network: worst case path measurements



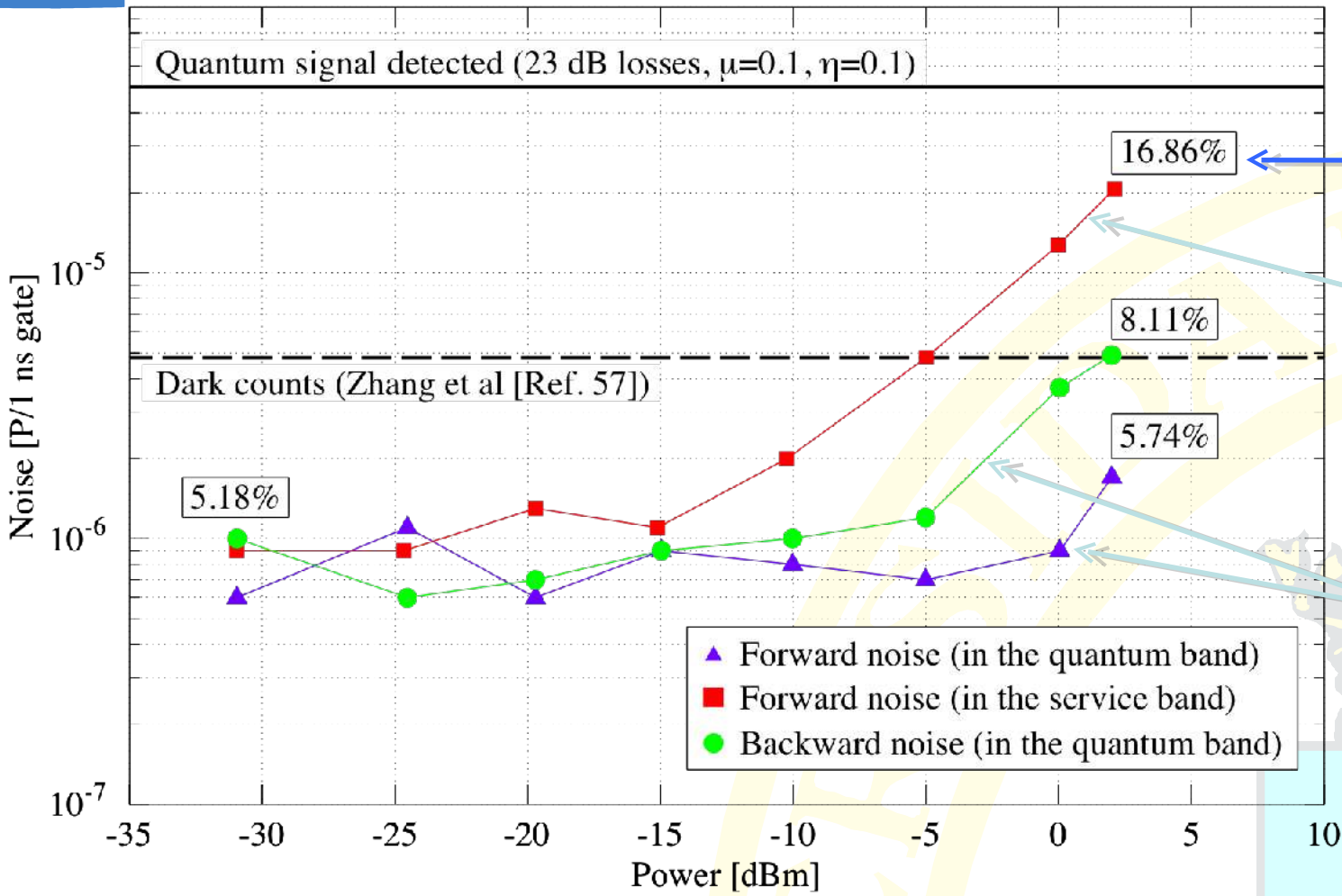
Worst case path (for noise and losses) in the testbed network. The longest fibers are in the entry points, where most Raman is produced.

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.

Test Network: worst case noise measurements



QBER

In-band Q/S separation 15 nm

Q/S separation 180 nm

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.

Conclusions

- The scheme can tolerate, at least, +2 dBm total power in the service 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 allow for a 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.

Future

- Proposal as ETSI ISG as a possible standard.
- 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 behaviour under real loads.

Thanks for your Attention!!

Questions?