Integrating QKD in Telecommunication Networks

Quantum Communication Workshop 2010
UNIK, Norway, Feb 2010

V. Martín, D. Lancho, J. Martínez, D. Elkouss
Quantum Information and Computation Group
Fac. Informática – Univ. Politécnica de Madrid
gcc.ls.fi.upm.es
M. Soto
Security in Networks and Sevices Dept.
Telefónica Investigación y Desarrollo.

vicente@fi.upm.es

Outline

- Frame: Motivation and limits. Why use networks and telco networks?
- Current Metropolitan Optical Networks
- The UPM-TID testbed
- Results
- Conclusions
- What's next?

Motivation, etc.
(1: Mostly market driven)

- We are trying to introduce a technology that:
  - QKD today is **neither a cheap nor easy** technology.
  - From a commercial perspective **key distribution is not a broad market** and the claimed level of security has still to be 'proven' in practice by general adoption.
  - Currently is **limited to ciphering point to point** communications: Need to **reconfigure connections to serve user's needs.**
- In order **for QKD to be widely adopted**, it must **share** the existing **infrastructure to leverage costs** and be **deployed in an scalable way.**
  - It seems unrealistic to think that a new and very expensive infrastructure is going to be created from scratch just for QKD alone.

Motivation, etc.
(2: Mostly technical)

- Limited to **point to point** using a **separate Quantum Channel** and **limited in distance**... or trusted repeaters.
  - **Trusted repeaters** increase the distance and distribution capability... at the cost of **relying in intermediate nodes** under the control of a third party: **Not acceptable for everybody.**
- Other Network Advantages:
  - More **Robustness**: QKD requires to keep the integrity of the protocol (authentication). This is done (nowadays and once initialized) using part of the distributed key. Continuous disruption of the quantum channel could exhaust the key storage. Having **several possible paths improves resiliency** against this.
  - More **Confidentiality:** The pattern of production of keys could reveal future needs of large cyphered transfers. **Monitor a full network** for this is **considerably harder**.

Metro Networks

- The Metro Network **links the long haul** network **to the final user** (and final users within the same area)
  - **Limited span**, tipically on the tens of Km.
  - Composed of **backbone** (core) **and access** segments.
- Real metropolitan networks are actually a mess of old and new technologies but...
  - The **preferred topology for the core is a ring** (Protection protocols: easy redundancy). There might be several.
  - The **access** network is a **one to many network** connected to the core either directly or through secondary 1 or 2 homed rings (segments).

Current Metro Networks

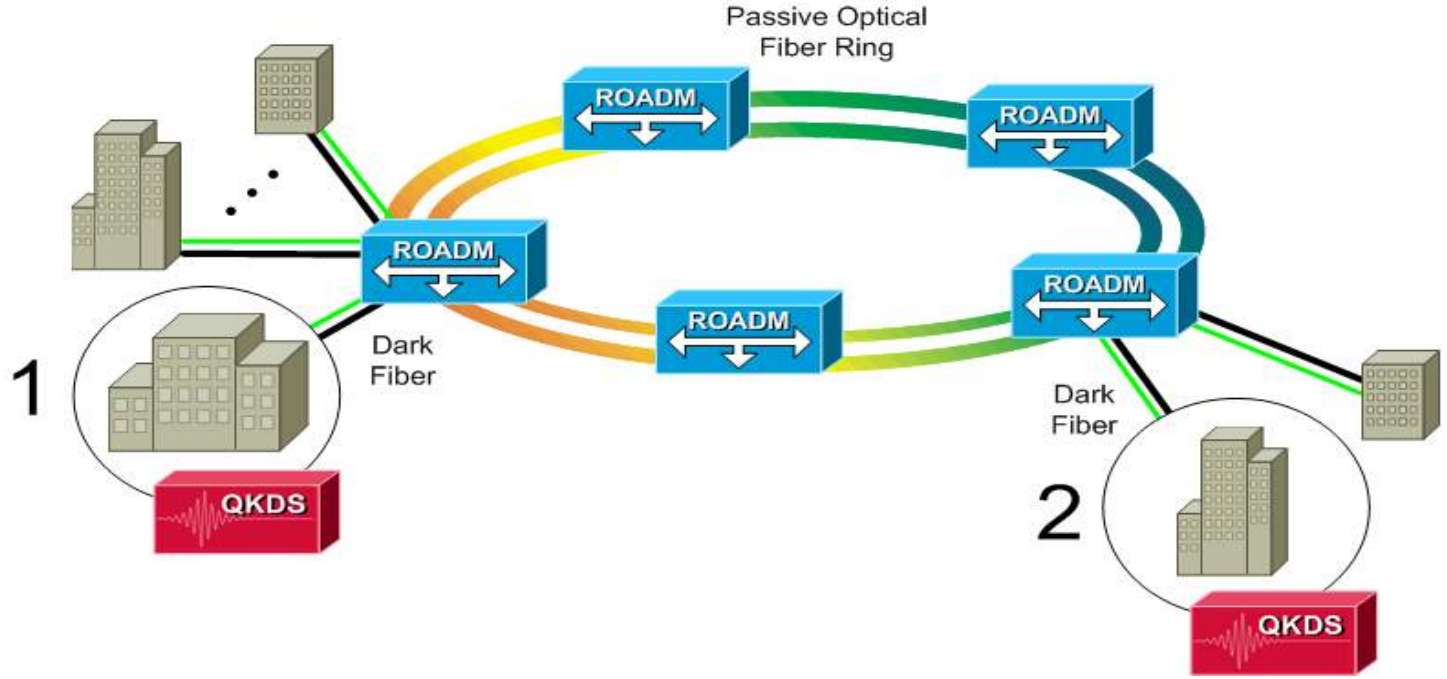
- The general trend is towards **Passive and all Optical Networks** (PONs)
  - A **transparent**, non amplified, **link among any two points** of such a network is possible.
- Current **most used technologies**:
  - Backbone: **CWDM** (Coarse Wavelength Division Multiplexing.)
    - Expect to see increased use of DWDM (Dense WDM)
  - Access: **GPON** (Gigabit PON)
    - Also direct links to the backbone through ”downgraded” variants of core technology.
    - DWDM-PON variant might be widely used.

CWDM

- **Coarse Wavelength Division Multiplexing** is an ITU Standard that defines a band of 20 channels (1270-1610 nm) with an spacing of 20 nm.
- It is a **reasonable technology to use QKD** with:
  - The big channel spacing makes the technology **'amplifier unfriendly'** since no single EDFA amplifier is able to amplify all of the channels at the same time.
  - Big channel spacing means also **easier filtering** (or cheaper and stable... but Raman scattering is quite broad)
  - The **total power** in the line **is manageable** with 'only' 20 channels.
  - There is no Four Wave Mixing problems.

Backbone

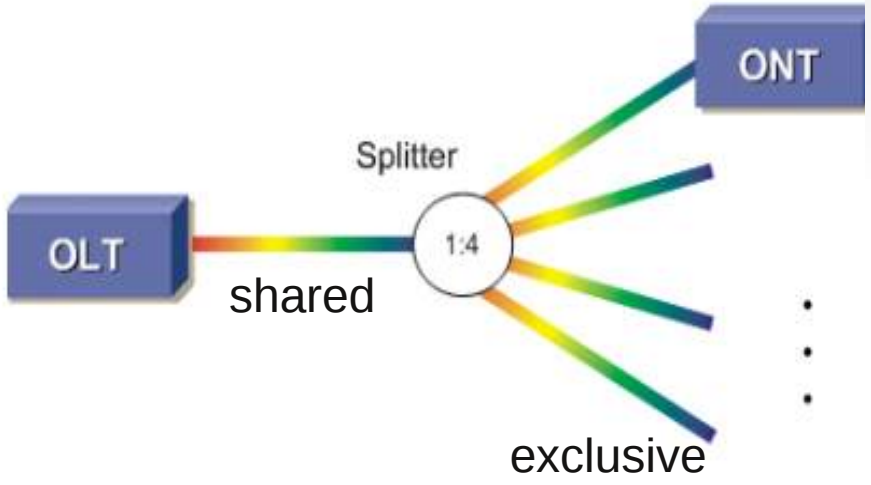
- Typically a **ring made up of 6-8 nodes**.
  - Sometimes **several rings** are **connected** together to cover a big city. **Expect to see rings plus mesh**.
  - Each **node** is a **Reconfigurable Optical Add and Drop Module** (ROADM) where **wavelengths can be dropped or added.**



GPON

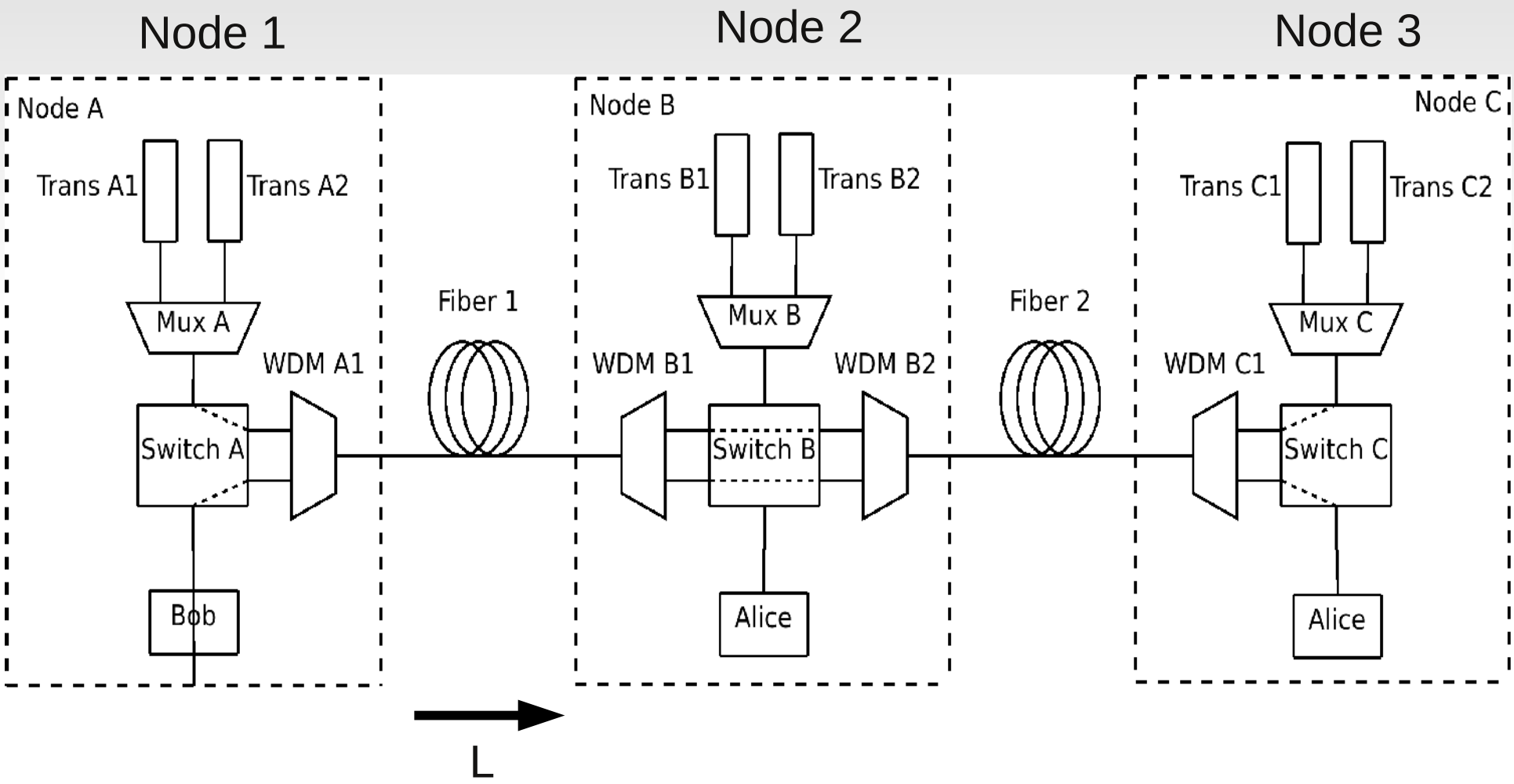
- **Gigabit PON** is an ITU standard that defines a **point to multpoint network** architecture.

Physically consist of an **OLT unit connected to the backbone** that is **connected to several ONTs** (clients) using a shared single fiber from the **OLT to an splitter** located in the neighbourhood of the clients. **From the splitter to the clients the fiber is exclusive** use.



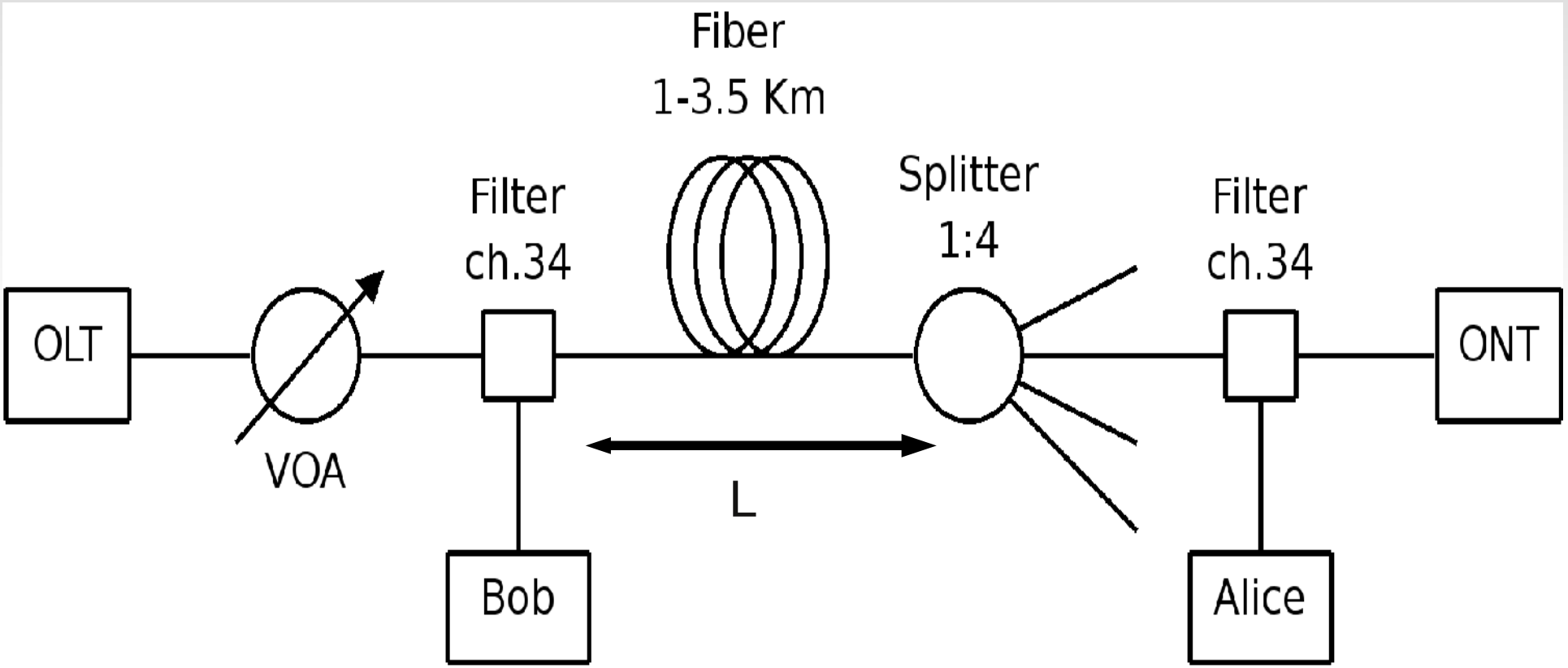
- **Three wavelengths** can travel **at the same time** in the fiber: 1470 nm (downstream), 1310 nm (upstream) and 1550 nm (video broadcast)
- **Time Division Multiplexing**.

ROADM Testbed (CWDM)



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

Access Testbed (GPON)

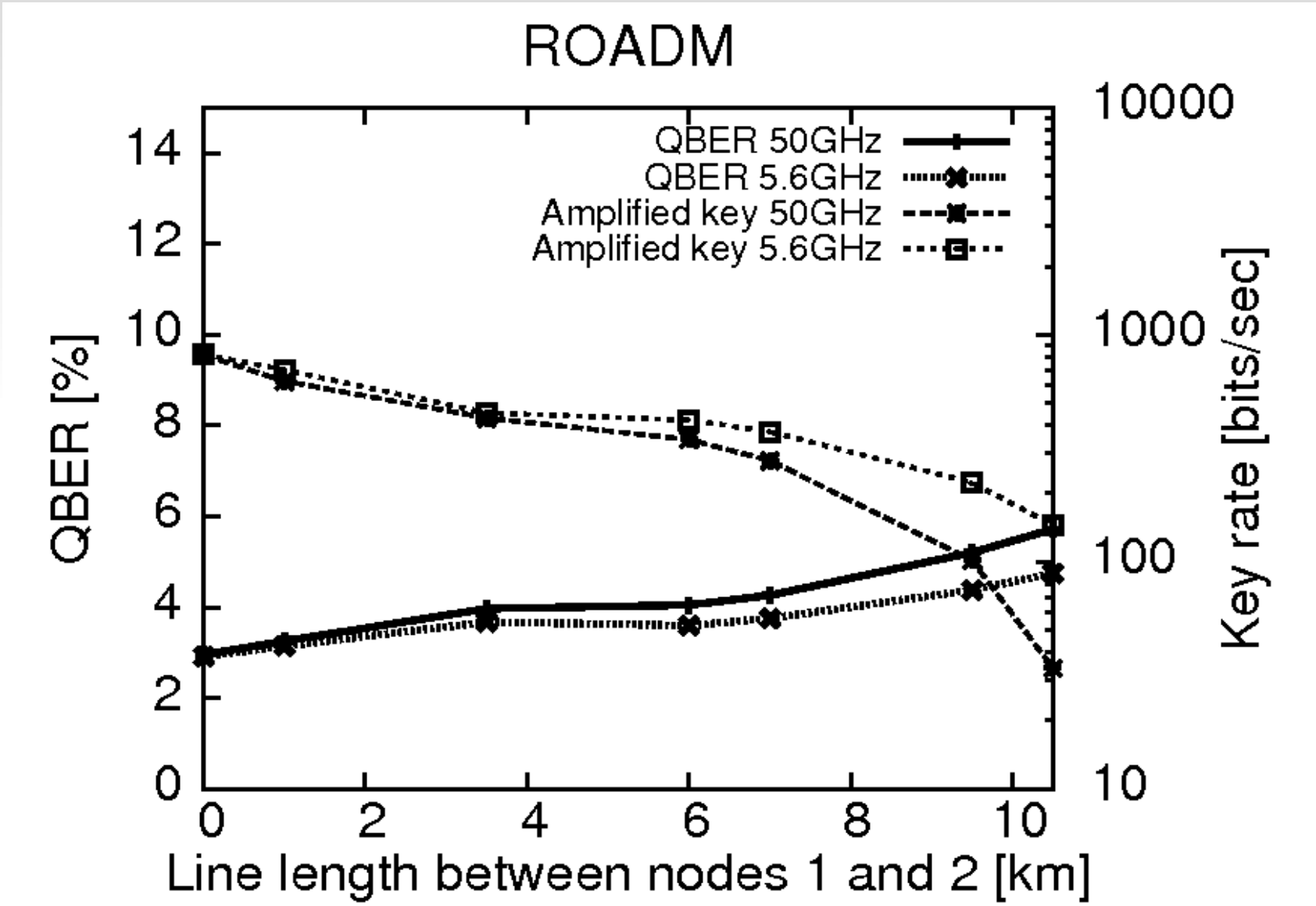


Quantum channel at 1550, Classical channels 1490, 1310 nm, 50 Ghz filters (0.4 nm)

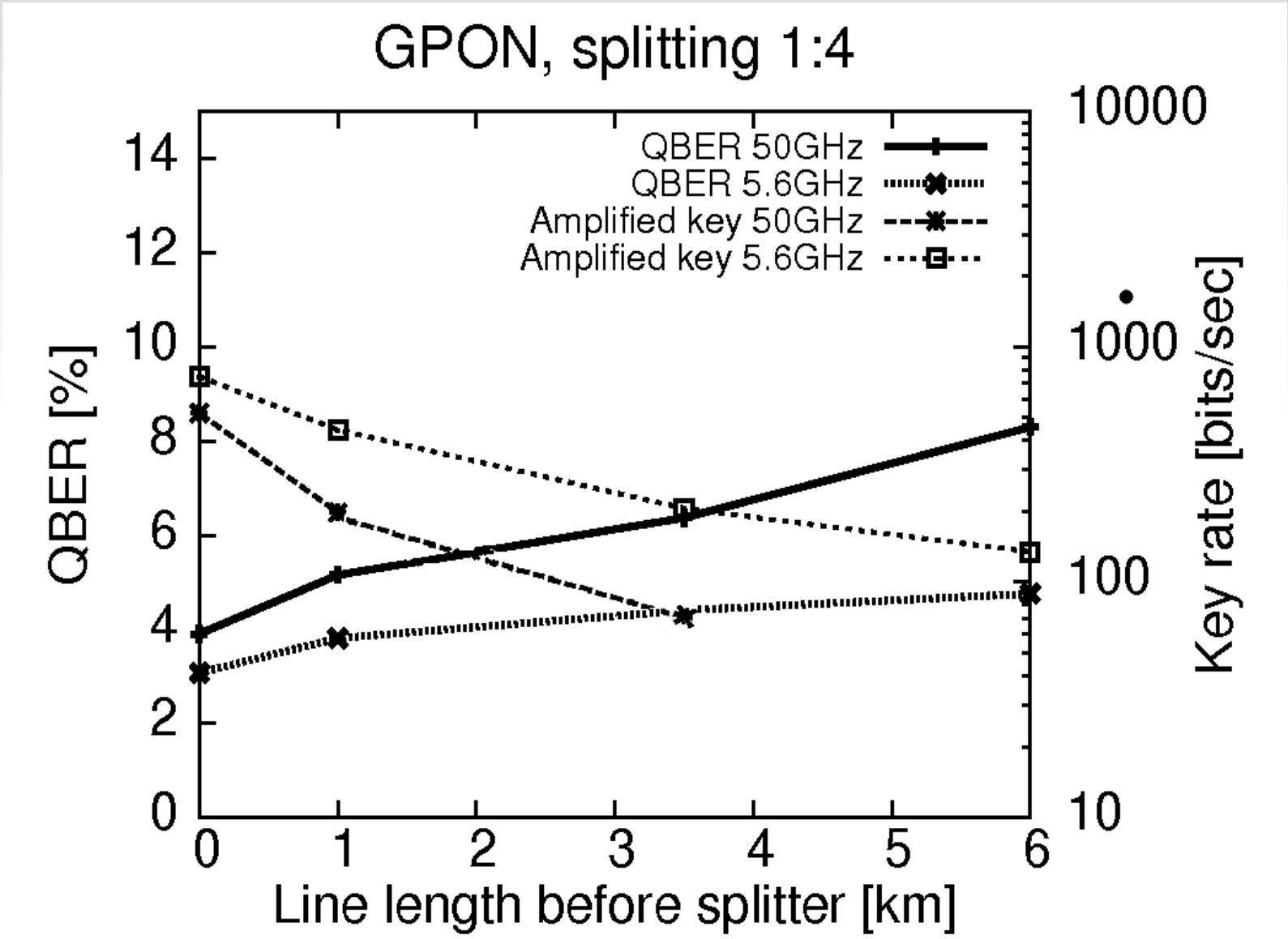
QKD setup

- Id Quantique Clavis model id3000 and id3100.
  - Two way **plug'n'play** systems.
  - Maximum key rate (theoretical, 0% QBER) limited by detector deadtime: 100 Kbit/sec.
    - Real BB84: μ=0.1, a couple of Kbit/sec at 2% QBER
  - Maximum absortion budget ~ 12 dB
- **BB84, Decoy state** (simulation, μ=0.8, 0.12).
- Error correction (using **Low Density Parity Check codes**, 1.07 efficiency) and privacy amplification.

Results (Backbone)



Results (GPON)



Conclusions (I)

- Even in the conditions of real optical networks **it is possible** to make **coexist a quantum channel with classical** signals using **realistic topologies.**
- The **troughput** is, of course, **heavily penalised** by the combination of strong absorption and spureous photons, **but still enough** to be used in a **combined QKD/block cipher** with a **secret key refreshment rate** much **higher** than the usual today.

Conclusions (II)

- **Higher troughput** is possible **not only by improving the QKD** systems, but also **by managing the conventional part.**
  - Using Media Access Protocols to **limit the total power** in the shared lines.
    - Using **better classical detectors** to allow for a **low power working.**
  - Improving the conventional systems to **limit the losses**.
  - Using a full band just for QKD (e.g. In the 1300 window). Or an hybrid Quantum-classical network...
    - There are no conventional PON devices working in this band. → **STANDARDS**

Conclusions (III)

- **QKD devices** able to withstand **~30 dB losses** would allow to **perform a key exchange** among two points **within a metro network**, going up one access network, crossing a backbone ring and down another access network in just one jump, **without the need of trusted repeaters.**
- Current **Infrastructure is rapidly evolving**. The **underlying technologies** are more **quantum friendly** than the old ones, but **this can depend heavily on implementation.**
  - **A clear guide about the needs of QKD** in this new environment **must be produced: More standards.**

But... (remains to be done):

- **Link** transparently **access** network **and backbone**:
  - Use always the same Q-wavelength: quite limited.
  - **Use a set of lambdas exclusively for QKD**: no conventional equipment supports this.
    - But it should not be difficult... once the band and requirements are defined.
- **Future proof** the infrastructure:
  - Optical networks are evolving rapidly:
    - **New access** networks (e.g.: DWDM-PON...)
    - **New backbone** (e.g.: Dynamic Wavelenght Assignment)

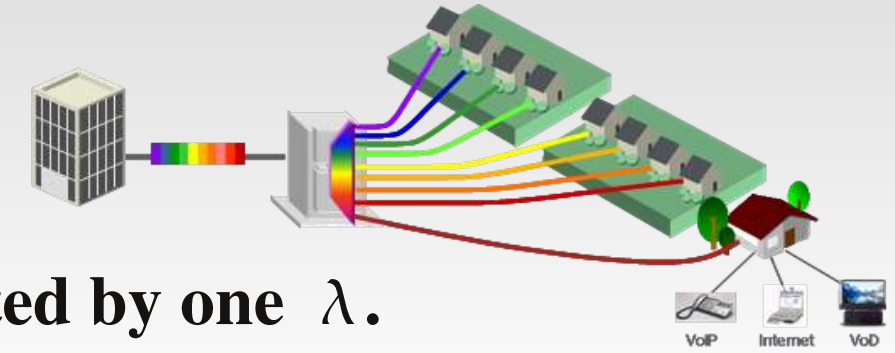
An example: DWDM-PON Access Networks

- Although GPON is the most deployed technology to date, it is expected to evolve rapidly.
  - **Contender : DWDM-PON**

- The **splitter** in GPON is **substituted by an Arrayed Wave Guide.**
  - **This is cheap!!** : No need to substitute optical fibers.
  - But the **OLT and ONT are** completely **different**.
  - **Carriers are exploring** this as a **potential upgrade** to their existing GPON infrastructure. Its being used in several countries already.

DWDM-PON (II)

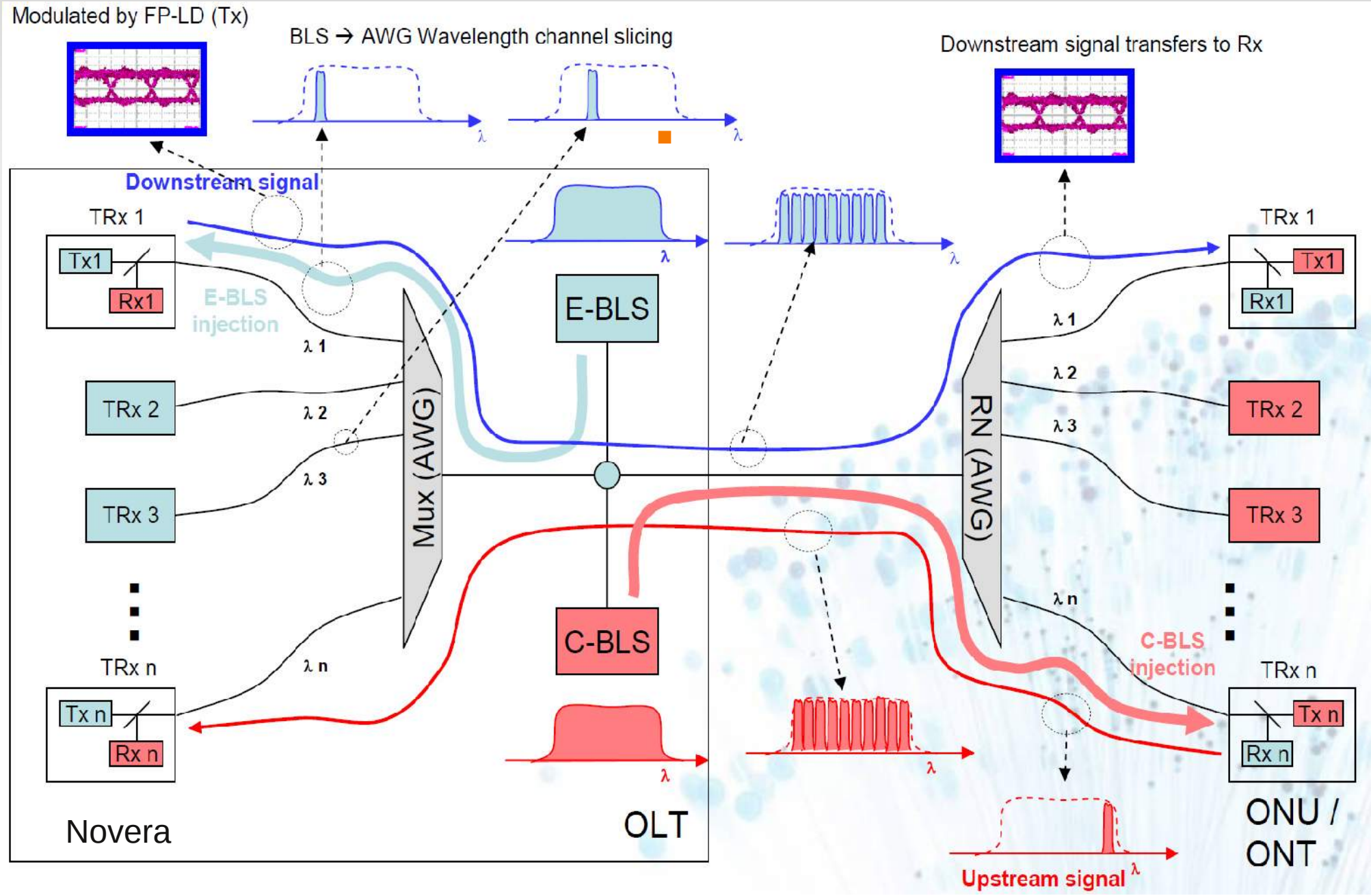
- A full spectrum of λ's are used. **Addressing is done using the λ.**
  - No time division, the **user** has the **full bandwidth transported by one λ.**



- **Ideally**, this could be done using a **tunable laser**. This would be highly convenient for QKD.
  - **A lambda** could be **assigned to every user** for the **quantum channel.**
  - **Power management** to avoid spureous photons would be easier.
  - The **AWG introduces a constant loss of 5 dB, independent of the number of users served.** Compare to the extra 3 dB per double of the number of users in the GPON splitter.

DWDM-PON (III)

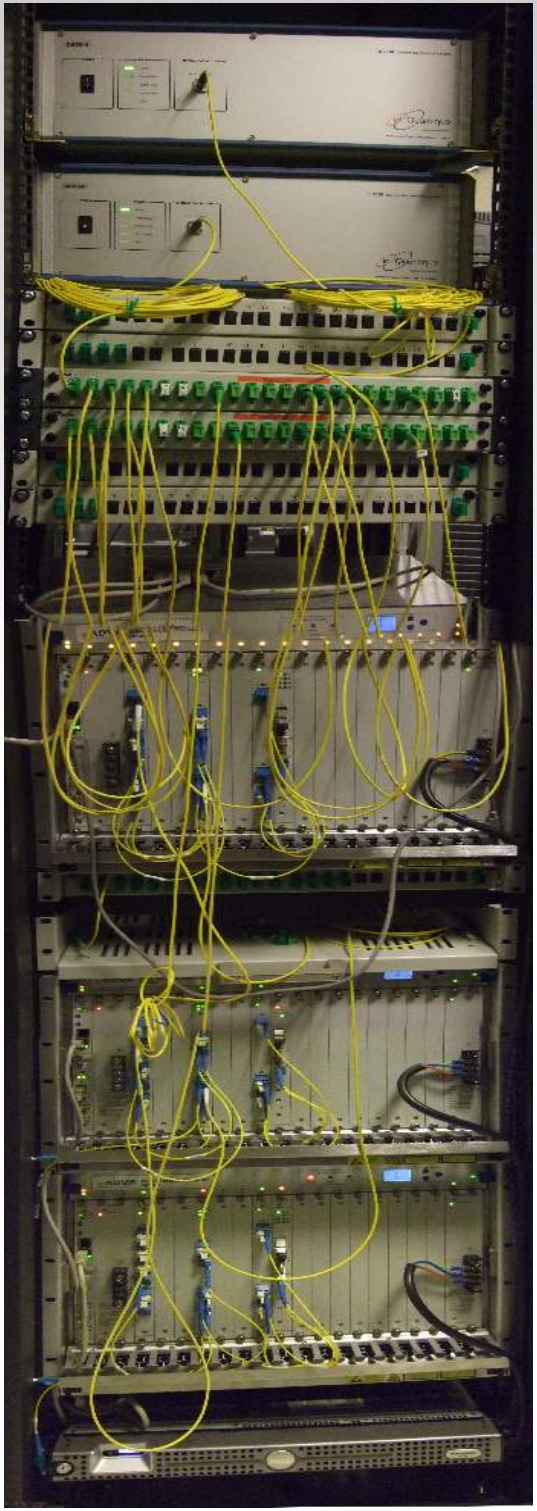
The **existing implementations** avoid the use of a tunable laser by **using a broadband light source** and resonant cavities at the client side (colourless ONT)

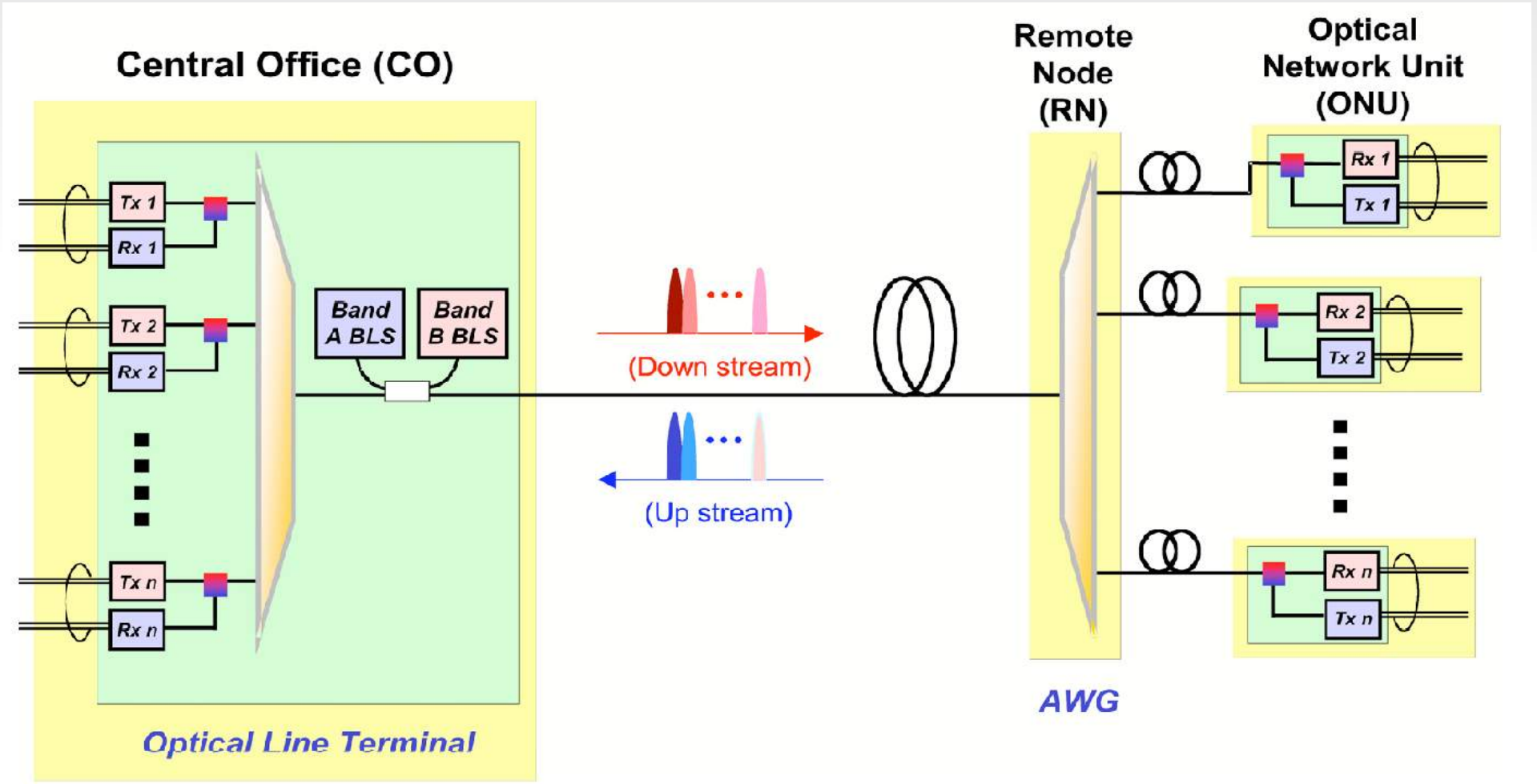


DWDM-PON (IV)

- This implementation has **important advantages for the carrier**:
  - Reduces inventory needs: **all ONT are equal.**
  - Reduces the engineering needs for setup and maintenance.
- But **from the QKD perspective**:
  - **The BLS is very noisy**.
  - Since the BLS power is divided among many ports, **a very high power** must be used for a decent reach, making power management a difficult task.
  - This is **not the ideal for QKD: A tunable laser** implementation **would be more advantageous** ... There is the need to research the limits and **requirements for quantum compatibility.**

Thank you!
Questions?




Central Office (CO)
Tx 1
Rx 1
Tx 2
Rx 2
Tx n
Rx n
Band A BLS
Band B BLS
Optical Line Terminal
(Down stream)
(Up stream)
Remote Node (RN)
AWG
Optical Network Unit (ONU)
Rx 1
Tx 1
Rx 2
Tx 2
Rx n
Tx n