Universidad Politécnica de Madrid
Facultad de Informática

QUANTUM COMMUNICATIONS IN OPTICAL NETWORKS

PhD Dissertation

ALEX CIURANA AGUILAR

Bachelor in Telecommunication Engineering (UPC)
Master in Computational Mathematics (UPM)

2014

Departamento de Lenguajes y Sistemas Informáticos e
Ingeniería de Software
Facultad de Informática

QUANTUM COMMUNICATIONS IN OPTICAL NETWORKS

ALEX CIURANA AGUILAR

Bachelor in Telecommunication Engineering (UPC)
Master in Computational Mathematics (UPM)

Supervisor:

VICENTE MARTÍN AYUSO
Ph.D. in Physics
Associate Professor at UPM

2014

Alex Ciurana Aguilar: *Quantum Communications in Optical Networks,*
PhD Dissertation, © 2014

SUPERVISOR:
Vicente Martín Ayuso

LOCATION:
Madrid

Tribunal nombrado por el Magnífico y Excelentísimo Sr. Rector de la Universidad Politécnica de Madrid,

Presidente: .....

Vocal: .....

Vocal: .....

Vocal: .....

Secretario: .....

Realizado el acto de lectura y defensa de la Tesis Doctoral en Madrid, a ..... de ..... de 20..... .

El tribunal acuerca entregar la calificación de .....

El Presidente Los Vocales

El Secretario

ABSTRACT

The potential use of quantum systems to process and transmit information has impulsed the emergence of quantum information technologies such as quantum key distribution. Despite looking promising, their use out of the laboratory is limited since they are a very delicate technology due to the need of working at the single quantum level. In this work we show how to use them in optical telecommunication networks. Using an existing infrastructure and sharing it with other signals, both quantum and conventional, reduces dramatically the cost and allows to reach a large group of users. In this work, we will first integrate quantum signals in the most common passive optical networks, for their simplicity and reach to final users. Then, we extend this study by proposing a quantum metropolitan optical network based on wavelength-division multiplexing and wavelength-addressing, verifying its operation mode in a testbed. Later, we study the distribution of entangled photon-pairs between the users of the network with the objective of covering as much different technologies as possible. We further explore other network architectures, changing the topology and the technology used at the nodes. The resulting network scales better at the cost of a more complex and expensive infrastructure. Finally, we tackle the distance limitation problem of quantum communications. The solution offered is based on network-coding and allows, using multiple paths and nodes, to modulate the information leaked to each node, and thus, the degree of trust placed in them.

Keywords: quantum communications, quantum key distribution, optical telecommunication networks, wavelength division multiplexing, trusted repeaters, passive optical networks

RESUMEN

La posibilidad de utilizar sistemas cuánticos para procesar y transmitir información ha impulsado la aparición de tecnologías de información cuántica, p. ej., distribución cuántica de claves. Aunque prometedoras, su uso fuera del laboratorio es actualmente demasiado costoso y complicado. En este trabajo mostramos como utilizarlas en redes ópticas de telecomunicaciones. Al utilizar una infraestructura existente y pervasiva, y compartirla con otras señales, tanto clásicas como cuánticas, el coste se reduce drásticamente y llega a un mayor público. Comenzamos integrando señales cuánticas en los tipos más utilizados de redes ópticas pasivas, por su simplicidad y alcance a usuarios finales. Luego ampliamos este estudio, proponiendo un diseño de red óptica metropolitana basado en la división en longitud de onda para multiplexar y direccionar las señales. Verificamos su funcionamiento con un prototipo. Posteriormente, estudiamos la distribución de pares de fotones entrelazados entre los usuarios de dicha red con el objetivo de abarcar más tecnologías. Para ampliar la capacidad de usuarios, rediseñamos la red troncal, cambiando tanto la topología como la tecnología utilizada en los nodos. El resultado es una red metropolitana cuántica que escala a cualquier cantidad de usuarios, a costa de una mayor complejidad y coste. Finalmente, tratamos el problema de la limitación en distancia. La solución propuesta está basada en codificación de red y permite, mediante el uso de varios caminos y nodos, modular la cantidad de información que tiene cada nodo, y así, la confianza depositada en él.

Palabras clave: comunicaciones cuánticas, distribución de claves cuántica, redes ópticas de telecomunicaciones, multiplexación en longitud de onda, repetidores confiables, redes ópticas pasivas

PUBLICATIONS

Some of the ideas described hereafter have been published in the following articles:

JOURNAL PAPERS

1. D. Elkouss, J. Martínez-Mateo, A. Ciurana, and V. Martín, "Secure optical networks based on quantum key distribution and weakly trusted repeaters," *Journal of Optical Communications and Networking*, Vol. 5, No. 4, pp. 316-328, 2013. (JCR 2012, Impact factor 1.433)

2. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, "Quantum metropolitan optical network based on wavelength division multiplexing," *Optics Express*, Vol. 22, No. 2, pp. 1576-1593, 2014. (JCR 2012, Impact factor 3.546)

3. J. Martínez-Mateo, A. Ciurana, and V. Martín, "Quantum key distribution based on selective post-processing in passive optical networks," *IEEE Photonics Technology Letters*, Vol. 26, No. 9, pp. 881-884, 2014. (JCR 2012, Impact factor 2.038)

4. A. Ciurana, A. Poppe, J. Martínez-Mateo, M. Peev, and V. Martín, "Entanglement distribution in optical networks," *in preparation*.

INTELLECTUAL PROPERTY

1. A. Ciurana, J. Martínez-Mateo, V. Martín, and H. Zbinden. Multiplexor óptico pasivo (P201331312) *Patent pending*, Sept. 2013.

PUBLISHED PROCEEDINGS FROM PEER REVIEWED INTERNATIONAL CONFERENCES

1. D. Lancho, J. Martínez-Mateo, D. Elkouss, A. Ciurana, M. Soto, and V. Martín, "Deploying QKD in standard optical networks," *Updating Quantum Cryptography and Communications (UQCC)*, p. 118, Tokio, Japan, Oct. 2010.

2. A. Ciurana, V. Martín, J. Martínez-Mateo, A. Poppe, M. Soto, N. Walenta, and H. Zbinden, "Multiplexing QKD systems in conventional optical networks," *2nd Annual Conference on Quantum Cryptography (QCRYPT)*, Singapore, Singapore, Sept. 2012.

3. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, "QKD in dense WDM passive optical networks," *Workshop on Quantum Telecommunications*, Lisboa, Portugal, May 2013.

4. A. Ciurana, J. Martínez-Mateo, N. Walenta, H. Zbinden, M. Peev, A. Poppe, and V. Martín, "Proposal for a wavelength multiplexed quantum metropolitan area networking," *3rd Annual Conference on Quantum Cryptography (QCRYPT)*, Waterloo, Canada, Aug. 2013.

5. D. Elkouss, J. Martínez-Mateo, A. Ciurana, and V. Martín, "Secure optical networks based on QKD and weakly trusted repeaters," *3rd Annual Conference on Quantum Cryptography (QCRYPT)*, Waterloo, Canada, Aug. 2013.

6. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, "Quantum metropolitan optical network based on wavelength division multiplexing," *ETSI Quantum-Safe-Crypto Workshop*, Sophia Antipolis, France, Sept. 2013.

7. A. Poppe, B. Schrenk, F. Hipp, M. Peev, S. Aleksic, G. Franzl, A. Ciurana, and V. Martín, "Integration of quantum key distribution in metropolitan optical networks," *OSA Research in Optical Sciences Congress*, Berlin, Germany, Mar. 2014.

8. A. Poppe, A. Ciurana, F. Hipp, B. Schrenk, M. Peev, J. Martínez-Mateo, and V. Martín, "Entanglement generation and routing in optical networks," *European Conference on Optical Communication (ECOC)*, Cannes, France, Sept. 2014.

9. A. Ciurana, A. Poppe, J. Martínez-Mateo, M. Peev, and V. Martín, "Entanglement distribution in quantum metropolitan optical networks," *4th Annual Conference on Quantum Cryptography (QCRYPT)*, Paris, France, Sept. 2014, *submitted*.

10. J. Martínez-Mateo, C. Pacher, A. Ciurana, and V. Martín, "Towards an optimal implementation of cascade," *4th Annual Conference on Quantum Cryptography (QCRYPT)*, Paris, France, Sept. 2014, *submitted*.

PUBLISHED PROCEEDINGS FROM NATIONAL CONFERENCES

1. V. Martín, D. Lancho, J. Martínez-Mateo, D. Elkouss, and A. Ciurana, "Integrating QKD in telecommunication networks," *QUITEMAD Workshop 2011*, El Escorial, Spain, Jan. 2011.

2. A. Ciurana, N. Walenta, J. Martínez-Mateo, D. Elkouss, M. Soto, and V. Martín, "Quantum key distribution in WDM-PON access

networks," *XXXIII Reunión Bienal de la Real Sociedad Española de Física*, pp. 191–192, Santander, Spain, Sept. 2011.

3. J. Martínez-Mateo, D. Elkouss, A. Ciurana, D. Espino, and V. Martín, "Minimum Interactive error reconciliation in quantum key distribution," *XXXIII Reunión Bienal de la Real Sociedad Española de Física*, pp. 206–207, Santander, Spain, Sept. 2011.

4. A. Ciurana, J. Martínez-Mateo, V. Martín, and M. Soto, "Quantum optical signals in telecommunication networks," *ICE-o - Workshop Información Cuántica en España*, Madrid, Spain, Sept. 2012.

5. A. Ciurana, J. Martínez-Mateo, and V. Martín, "Quantum key distribution in WDM optical networks," *XIII Seminario de Matemática Discreta*, Valladolid, Spain, June 2013.

ACKNOWLEDGMENTS

I would like to especially thank my advisor, Prof. Vicente Martín, for his help in the preparation of this work. This would not have been possible without his guidance, support and insightful discussions.

I am particularly grateful for the assistance given by my present and former colleagues of the research group on quantum information and computation: Jesús Martínez Mateo, David Elkouss and Daniel Lancho. I appreciate their helpful collaboration, contribution, feedback and advice during my doctoral journey.

I wish to acknowledge the AIT Austrian Institute of Technology, in particular the Optical Quantum Technology unit, for hosting me during my research stay. Especially, I thank Andreas Poppe, Momtchil Peev, Florian Hipp, Bernhard Schrenk and Mike Hentschel for sharing their knowledge and time, and for making my stay enjoyable and memorable.

This work has been funded by project Quantum Information Technologies Madrid (QUITEMAD), P2009/ESP-1594, funded by *Comunidad Autónoma de Madrid*.

I thank Telefónica I+D for the resources, technical expertise and assistance provided during my experiments at their facilities.

CONTENTS

1 INTRODUCTION 1
1.1 Background . . . 2
1.2 Motivation . . . 5
2 PRELIMINARIES 7
2.1 Quantum key distribution . . . 7
2.2 Optical realization of a QKD system . . . 8
2.2.1 Single-photon source . . . 9
2.2.2 Single-photon detector . . . 10
2.2.3 Optical medium . . . 10
2.3 Multiplexing optical signals . . . 14
2.3.1 Raman scattering . . . 16
2.3.2 Four-wave mixing . . . 16
2.3.3 Device's imperfections . . . 18
2.4 Metropolitan optical networks . . . 18
2.4.1 Access network . . . 19
2.4.2 Backbone network . . . 21
2.5 Limitations of quantum optical networks . . . 22
3 QUANTUM COMMUNICATIONS IN A PON 25
3.1 TDM-PON (GPON and EPON) . . . 25
3.1.1 Scattering effects . . . 26
3.1.2 Proposal . . . 28
3.1.3 Simulation . . . 29
3.1.4 Results . . . 30
3.1.5 Next-generation TDM-PONs . . . 30
3.2 WDM-PON . . . 32
3.2.1 Scattering effects . . . 32
3.2.2 Proposal ONU to OLT . . . 33
3.2.3 Proposal ONU to ONU . . . 33
3.3 Conclusions . . . 34
4 QUANTUM METROPOLITAN OPTICAL NETWORK 37
4.1 Channel plan . . . 37
4.2 Network design . . . 39
4.2.1 Simplified network . . . 39
4.2.2 Backbone nodes . . . 39
4.2.3 Full network . . . 41
4.3 Testbed . . . 43
4.4 Integration of QKD systems . . . 47
4.5 Conclusions . . . 48
5 ENTANGLEMENT IN A QUANTUM MON 51
5.1 Broadband source of entangled photon-pairs . . . 51
5.2 Entanglement-only metropolitan optical networks . . . 52
5.2.1 A single access network . . . 52

5.2.2 Two access networks . . . 53
5.2.3 Metropolitan optical network . . . 54
5.3 Channel plan . . . 56
5.4 Upgrading the backbone node . . . 58
5.5 Network design . . . 59
5.5.1 Access network . . . 59
5.5.2 Metropolitan optical network . . . 60
5.6 Conclusions . . . 62
6 ACTIVE QUANTUM MON 63
6.1 Active backbone node . . . 63
6.2 Network design . . . 64
6.3 Effect of switches in QKD networks . . . 68
6.4 Conclusions . . . 70
7 EXTENDING THE REACH OF QUANTUM COMMUNICATIONS 73
7.1 Available solutions . . . 73
7.2 Formalization of Weakly Trusted Repeaters . . . 75
7.2.1 Security . . . 75
7.3 Logical scenarios . . . 76
7.4 Implementation on Metropolitan Optical Networks . . . 78
7.4.1 First prototype . . . 79
7.4.2 Second prototype . . . 80
7.5 Conclusions . . . 82
8 CONCLUSIONS AND FUTURE WORK 85
8.1 Conclusions . . . 85
8.2 Future work . . . 88
Bibliography 88
Acronyms 105

Figure 2.1 Secret-key of a perfect BB84 QKD system with one-way post-processing, no losses and considering coherent attacks. 9
Figure 2.2 Poisson distribution for $\mu = 0.1, 0.5, 1$. 10
Figure 2.3 Attenuation coefficient of an optical fiber for the typical telecommunication spectrum and transmission bands. Major contributors to losses are indicated. it can be seen that the optimal transmission window is around 1550 nm, at the C band. Original figure from Ref. [1]. 12
Figure 2.4 Spectrum of the Rayleigh and Raman backscattering produced by a 0 dBm, 1550 nm pump signal after 20 km of fiber. 14
Figure 2.5 Power of the forward and backward Raman scattering produced by a 0 dBm, 1550 nm pump signal, and measured at 1565 nm. 15
Figure 2.6 First-order FWM products produced by three signals with frequencies w_1, w_2, w_3 equally spaced Δw. 17
Figure 2.7 Scheme of a metropolitan optical network (MON). Users, also called subscribers ($S_{x,y}$ in the figure), are connected to tree-type access networks. Signals from all users are multiplexed using a network component (NC) and sent upstream to the central office (CO). The CO can route them to the backbone or downstream to the same users. Within the ring-shaped backbone, a series of reconfigurable optical add-drop multiplexers (ROADMs) allows to route signals between access networks. They also link to long-haul or other backbone networks. 19
Figure 2.8 Experimental data of the cyclic behavior of a 100 GHz 32-channels AWG in the 1250-1620 nm range. Only outputs 1, 8, 16, 24 and 32 are shown, and, among them, only output 16 is presented over the whole range. Periodic channels have the same color. 22

Figure 3.1 TDM-PON with QKD integration. A fiber Bragg grating (FBG) is used to enable a direct optical path between QKD devices, and an isolator to reduce the backscattering from the upstream signal. Communication frames are depicted as colored rectangles, where the colored squares represent time slots assigned to different ONUs. 26
Figure 3.2 Power of the Rayleigh backscattering produced by a -6.3 dBm pump signal at 1310 nm. We compare the measurement results of the laboratory (points) with the simulated data (solid line). . . 27
Figure 3.3 Upstream frame of a TDM-PON divided into time slots of variable length. Each time slot is assigned to a given ONU, and they are colored depending on whether the emitting ONU is located in the same branch than the QKD systems (gray) or not (white). Two QKD users may exchange key using the time slots marked white, which correspond to low noise periods. 28
Figure 3.4 Effective detection probability p^*_{exp} and QBER of a quantum signal as a function of the non-saturated time per frame (125 μs) in a GPON. Results are compared for two network configurations allowing up to 128 users, a 1:4 (1:8) splitter connected to a 1:32 (1:16) splitter, and two block lengths, $B = 1000$ and 2000. The detection probability assuming TDM synchronization is also shown. 31
Figure 3.5 Spectrum of the upstream signals of a WDM-PON arriving to the OLT (32-ch AWG and 15 km span). Alongside the conventional signals at the C band, a quantum signal is emitted at 1 GHz and at the O band (1310 nm). 33
Figure 3.6 Connection scheme of the AWG of a WDM-PON with QKD integration ONU-to-ONU. A switch is placed before the AWG with enough ports to create return paths for the quantum signals. . . 34

Figure 4.1 Proposed channel plan for the quantum metropolitan optical network. Quantum and conventional signals are separated in two spectrum bands to minimize the crosstalk. Each band is divided into subbands, which are assigned to the access networks. Within the subbands, DWDM channels carry the signals. Subbands are selected such that both quantum and conventional DWDM channels are periodic, and thus, they come out together through the same AWG port. 38
Figure 4.2 Simplified network of two WDM-PON access networks with switches. Using the channel plan described in Sec. 4.1, any pair of users, located in different access networks, can communicate using quantum and conventional signals. 39
Figure 4.3 Design of a passive backbone node for the QKD-MON, built out of common network components. It works as an OADM: (i) drops the quantum and conventional subbands from the input signal to the access network; and (ii) adds any channel coming from the access network to the ring (output signal), no matter which sub-band it belongs to. 40
Figure 4.4 Quantum metropolitan optical network with 3 access networks. The design uses CWDM at the backbone and DWDM at the access networks to arrange both quantum and conventional signals in an any-to-any fashion. A possible communication snapshot is shown using colored circles. Each circle represents a pair of quantum and conventional signal. 41
Figure 4.5 QKD-MON test bed with three OADMs based on the design in Fig. 4.4. The total length of the fiber is approx. 16 km. A longer fiber than usual is used in the access network 1 to generate a higher amount of Raman scattering. Overlaid in black is the worst case path with respect to losses and generated noise. 44

Figure 4.6 Measured noise per 1 ns gate in the testbed depicted in Fig. 4.5. A laser centered at 1520 nm is fed at the access network 1 and three measurements are done: forward node at a quantum channel (1340 nm, triangles), backward noise at a quantum channel (circles), and forward noise at a conventional channel (1530 nm, squares). To facilitate its interpretation, the expected quantum signal detection rate and the dark count rate of an SPD [2] are also presented. Using these data, a rough estimation of the QBER is shown for multiple points. 46
Figure 5.1 Scheme and output of a broadband source of entangled photon-pairs. A laser pumps the ppLN waveguides. Photon pairs are generated over a broad spectrum via SPDC, and divided into DWDM channels using a demultiplexer. Hence, DWDM channels are entangled symmetrically. PBS stands for polarizing beam splitter. 52
Figure 5.2 Broadband entanglement-source directly connected to users. It is equivalent to a WDM-PON access network. The switch is necessary to do all possible user pairings. 53
Figure 5.3 Broadband entanglement-source serving two access networks. The output of the source is demultiplexed in DWDM channels and grouped in CWDM channels 1510 and 1550. Each CWDM channel is dropped in a different access network by an OADM (or just a simple bandpass filter). 53
Figure 5.4 Scheme of a entanglement-only metropolitan optical network with N access networks and ring-shaped passive backbone. Each access networks has assigned a CWDM channel. Sources, added to the backbone traffic, distribute entanglement over all single CWDM channels and possible pairs. 54
Figure 5.5 Possible connection schemes for the entanglement sources in an entanglement-only metropolitan optical network with 2 access networks. In (a), switches are used to decide which source uses each CWDM channel. In (b), switches decide which source uses each DWDM channel; hence, a CWDM channel is used by multiple sources at the same time. In (c), CWDM channels are also shared among all sources but in a fixed way; a source has assigned always the same DWDM channels. 55

Figure 5.6 Channel plan for a quantum metropolitan optical network. Each access network has assigned two CWDM channels, for quantum and conventional signals. They are spectrally separated to avoid any crosstalk. Within the CWDM channel, DWDM channels are used for one-way communications or entanglement distribution. The figure shows how entanglement sources (S_x) are arranged in order to ensure entanglement among any pair of users in the network. 58
Figure 5.7 Possible design of a passive backbone node for a ring-shaped backbone that includes a broadband source of entangled photon-pairs. The design is an upgrade of the previous one (Fig. 4.3) with the addition of the source S and a second splitter. 59
Figure 5.8 Quantum metropolitan optical network based on the design shown in Chap. 4. Besides allowing one-way communications, quantum and conventional, the network is also capable of distributing entangled-photon pairs among any pair of users of the network. 61
Figure 6.1 Design of an active backbone node for a mesh-based backbone that includes a broadband source of entangled photon-pairs. Incoming signals are demultiplexed into quantum and conventional bands using a 1310/1550 WDM mux, and then into CWDM channels. These are routed to their corresponding port via a switch. All signals are multiplexed again before leaving the node. . . . 64
Figure 6.2 Quantum metropolitan optical network with a mesh-type backbone, backbone nodes based on active technology, and 4 access networks (A_x). Reconfiguring the nodes allows to interconnect all users using only 2 CWDM channels for quantum signals, but not at the same time. In the depicted configuration, entanglement is shared between A_1 and A_4, A_2 and A_4, A_2 and A_3, and within A_3. One-way, quantum and conventional, are not configured. 65
Figure 6.3 Possible node configurations of the quantum metropolitan optical network shown in Fig. 6.2. Each backbone node is depicted as an schematic switch-box, and each color represents a CWDM channel for quantum signals. The three configurations cover all communication paths between pairs of access networks. 67

Figure 6.4 Basic network scenario with three users connected using a 1:2 splitter with ratio 50:50 or a 1x2 switch that switches each half a second. . . 68
Figure 6.5 Secret key rate vs path losses of a BB84 QKD system using Eq. 6.1. We compare two scenarios, one with a 1:2 balanced splitter and another one with a 1x2 switch. The switch scenarios takes into consideration 25 ms of switching time. . . . 70
Figure 7.1 Basic scenario of a quantum communication where an emitter e wants to transmit a message m to a receiver r. However, their separation exceeds the reach of e (gray-out area). They need an intermediate node t. 73
Figure 7.2 Logic unicast and multicast scenarios for quantum communications using weakly trusted repeaters. All transmissions are OTP-ciphered using a QKD secret key. (a) In this network, the source s sends a message $m \in \mathcal{M}$, in linear combination with a random message k, to the user u using t_1 and t_2 as intermediate nodes. These can eavesdrop their incoming and outgoing links. If they don't cooperate, they have no information about m. (b) The source s distributes the same secret key to two different users u_1 and u_2. . . 77
Figure 7.3 Logic multi-source scenario for quantum communications using weakly trusted repeaters. Two sources, s_1 and s_2, transmit m_1 and m_2 to the users, u_2 and u_1, respectively. The message is linearly combined with a random message k, and OTP-ciphered with a QKD secret key. No information is leaked to the intermediate nodes or the remaining users. 78
Figure 7.4 Scheme of a QKD-MON with weakly trusted repeaters. Solid lines represent physical links, and dashed lines, logical ones. Intermediate nodes ($\mathcal{T}$) are located at the backbone nodes and the sources ($\mathcal{S}$) and users ($\mathcal{U}$) at the access networks. The resulting scheme is similar to the one in Fig. 7.2a but folded in two by the middle. 79

Figure 7.5 QKD-MON prototype using weakly trusted repeaters. At the backbone, 1550 nm CWDM OADMs are used in parallel with DWDM OADMs (F) that route signals to the corresponding receiver. Finally, a band-pass filter F_a is used to connect the access network with the backbone and route signals into the correct direction within the backbone (bidirectional ring). The figure also shows a WTR communication between Tx_1 and Tx_5 using colored circles. The color indicates the wavelength of the signal. 80

Figure 7.6 Possible types of WTR communications using weakly trusted repeaters in the QKD-MON prototype depicted in Fig. 7.5. Each transmission is labeled with its wavelength (colored circle) and loss budget. 81

Figure 7.7 Second prototype of a QKD-MON with weakly trusted repeaters. Splitters are used instead of CWDM OADMs. These changes permit to use an AWG at the access network, and thus increase the number of users. 82

LIST OF TABLES

Table 2.1 Transmission bands of the optical spectrum . . 11
Table 2.2 Insertion losses of common network components. Values are from commercial models available in the market [3, 4, 5, 6, 7]. 20
Table 4.1 Calculated and measured losses for the main network modules of the QKD-MON (according to Tab. 2.2). 42
Table 4.2 Assignation of CWDM channels to the access networks. 43
Table 5.1 Losses of the passive backbone node with entanglement-capability depicted in Fig. 5.7. 59
Table 5.2 Path losses from an emitter (user or source) in a QKD-MON with a fixed-ring backbone (Fig. 5.8). Values calculated using Tab. 2.2 and Tab. 5.1. . . 61
Table 6.1 Losses of the active backbone node with entanglement-capability depicted in Fig. 6.1. 64
Table 6.2 Path losses from an emitter (user or source) in a QKD-MON with a reconfigurable-mesh backbone (Fig. 6.2). Values calculated using Tab. 2.2 and Tab. 6.1. 66

1 INTRODUCTION

From the rudimentary methods used by ancient civilizations to the computer algorithms used today, there has always been an urgency throughout the history for securing certain communications. For this purpose, the message is ciphered, using a particular key, and deciphered later using another key. The information contained in the message is secret during the communication, and only accessible upon reception by those with the appropriate key. Unlike former schemes, modern cryptography does not hide the algorithm used to cipher and decipher. The security of the procedure relies in the key, the information leakage and the computational hardness of breaking the algorithm. If the procedure does not leak enough information for the eavesdropper to break it, regardless of his computational power, it is called information-theoretically secure [8] (e.g., one-time pad).

Accordingly, the generation and distribution of high-quality keys is at the root of modern cryptography. Besides traditional solutions, like trusted couriers and physical exchanges of key pools, nowadays this is done using asymmetric-key cryptography based on one-way functions (e.g., RSA, Diffie Hellman). However, current asymmetric-key protocols have not been proven secure. They are just too hard—at the moment—to solve in terms of resources. This computational complexity will instantly vanish if an efficient algorithm is discovered or a more powerful computation paradigm is used (e.g., quantum computing). Furthermore, in the meantime, the mere continuous growth in computational power due to technological advances is enough to force a constant revision of the recommended key size. What once was considered secure during the age of the Earth, was actually broken in 17 years [9]. To keep up with security, we have gone from a key length of a few hundred bits to 2048, 3072 or even 15 Kb [10, 11]. However, long-term recommendations are always on the basis that there is no breakthrough in quantum computing [11].

A higher-security alternative emerged with the discovery of quantum mechanics [12]. Physical systems at atomic and sub-atomic scales show properties that are not considered by classical physics. For instance, because of the wave-function collapse after a measurement and the uncertainty principle, the state of a quantum system is somehow volatile and not readily accessible from the exterior. The information that an observer can gain is limited. In particular, these properties are especially attractive for cryptography since they offer the possibility of creating protocols that limit the information leakage based on the fundamental laws of nature. This means cryptography not based on

computational assumptions, but in the laws of nature as we know them. The first quantum cryptography proposal was quantum key distribution (QKD) [13, 14], a protocol that grows a secret key between two parts with informational-theoretical security. In contrast to conventional solutions, the protocol is secure against an attacker with unlimited resources (thus including a quantum computer).

1.1 BACKGROUND

QKD is intrinsically a point-to-point technology that requires the transmission of d-dimensional quantum systems (i.e., *qudits*). Most QKD protocols use quantum systems with $d = 2$, also known as *qubits*, which represent the unit of quantum information [15]. Qubits are typically implemented in quantum communications using single photons and thus propagated through optical fibers or free-space. In a QKD exchange, qubits are prepared by the emitter and transmitted to the receiver, which measures the qubits. Afterwards, a procedure distills a secret key from the extracted information. The length of the secret key will depend on the amount of detections and the quantum bit error rate (QBER). As the QBER increases, the length of the distillable secret key approaches zero. Depending on certain assumptions on the distillation protocol and capabilities of the eavesdropper, a maximum tolerable QBER exists, after which no secret key can be distilled.

Since we always consider the worst-case scenario, any erroneous detection, even if they are caused by imperfections of the QKD devices, should be attributed to an eavesdropper. These imperfections are inherent to any device; consequently, as the signal decreases, the signal-to-noise ratio increases inevitably. Hence, the maximum tolerable QBER can also be seen as a limited loss budget. If the transmission losses are greater than the budget, the signal detected is too weak in comparison with such errors, and thus the QBER surpasses the threshold. The same reasoning applies when we add a source of external noise. This is of special importance because the quantum signal is composed of single-photon pulses, and thus even a small amount of noisy photons can severely harm the transmission. As a result, QKD systems have been traditionally used in dedicated links that isolate the quantum signal from any other source, in particular, from other signals propagating in the same fiber.

From the original proposal of QKD and the first experiment, spanning just a few centimeters and using low rate emitters [16], modern systems have reached hundreds of kilometers [17, 18, 19, 2, 20, 21, 22] and GHz rates [23, 24, 25, 26]. For this, a great mixture of technologies and protocols have been developed: the original BB84 [14], SARG04 [27], differential phase shift (DPS) [28, 29], BB84 with decoy states [30, 31], coherent one-way (COW) [32, 33], using continuous variables (CVQKD) [34, 35], based on entangled photon-pairs

(e.g., E91 [36], BBM92 [37, 38]), device and measure independent QKD [39, 40, 41], high-dimensional QKD ($d > 2$) [42], microwave photonics QKD [43], etc. Moreover, QKD has already demonstrated its practical security [44], long-term stability [45, 46, 47] and commercial maturity [48, 49, 50, 51, 52, 53]. Nevertheless, the fundamental technical drawbacks, which restrain its commercial use, still remain: limited loss budget, point-to-point architecture and dedicated links.

Limited loss budget

The limited loss budget problem is commonly known as the distance limitation since, in a point-to-point link, the transmission medium is the only component. A first approach is to push the limit further away by increasing the rate of the QKD systems—and thus the amount of detections—as well as reducing the intrinsic noise. But, in the end, there is still a limit. A complete solution requires an intermediate device able to regenerate, amplify or repeat the quantum signal. Quantum devices for this purpose are still in an early stage, and a practical version is not expected in the near future [54, 55, 56]. Meanwhile, we are forced to use conventional solutions [57, 58, 59, 60], which will irremediably interrupt the quantum signal and the security of the transmission. The users have to trust the repeater in order to consider it a secure scenario. Although it may seem contradictory, trusted repeaters are the only available solution.

Dedicated links

The second main drawback deals with the use of dedicated links, which dramatically increases the cost of the technology by impeding its use alongside other signals. The operational expenses greatly surpass the capital expenses of a technology that is not cheap. This inefficient operation mode goes against the tendency of conventional communications: share the resources as much as possible. The solution is to multiplex the quantum signal with other quantum or conventional ones. Typically this is done in time (TDM) or wavelength (WDM). Nevertheless, other multiplexing schemes for fiber optics have recently gained the attention of the community, such as subcarrier (SCM) [61] and spatial multiplexing (SDM) [62]. Among all these options, WDM is becoming the popular choice due to its simplicity (no synchronization required) and bandwidth advantages. Since QKD aims to provide secret keys for other communications, most research focuses on multiplexing it with conventional communications. Anyhow, another example of maximizing the fiber usage is wavelength-multiplexing multiple quantum signals that belong to one QKD system, thus increasing the final throughput [63].

Studies can be classified based on whether they use different spectrum bands for quantum and conventional signals [64, 65, 66] or

not [67, 68, 69, 70, 71, 72, 73]. As research advances, the use of better QKD systems and filters has allowed modern schemes to withstand up to 30 simultaneous conventional signals [70]. The limit in the number of conventional signals results directly from the noise produced by them, which increases the QBER of the quantum communication. This noise is produced mainly by three physical phenomena [74, 75, 76, 77]: Raman scattering, Rayleigh scattering, and four-wave mixing (FWM). Besides, we need to take into account the imperfections of WDM devices. Although, no noise is actually generated in this case, part of the signal is leaked to other channels, which results also in a QBER increase. Since, in all of these, the crosstalk increases with the power of the signal, the limit can be seen as a maximum photon flux per second. Hence, lowering the power of each signal allows to withstand more of them.

Point-to-point architecture

The third problem relates to the use of QKD in networks. Using the point-to-point architecture, a network with n users would require $n(n-1)/2$ links in order to directly connect all to all, and thus form a complete graph. As it can be seen, the number of links increases dramatically: 2-4-10-128 users need 1-6-45-8128 links, respectively. Leaving costs aside, it is just unfeasible from a resources standpoint. When dealing with a reasonable amount of users, we need a more advanced approach that includes using other topologies and some sort of networking in order to reduce the number of physical links and the deployment costs.

Among the different topologies (e.g., bus [78]), tree and ring have been the most studied due to its widely use in commercial optical networks [79, 80, 81, 82, 83, 84, 85, 86]. Once all nodes are connected, the signals are routed through them mainly using three types of components: switches [87, 88, 89, 90], trusted repeaters, and passive optical components (e.g., filters, splitters and multiplexers) [91, 92]. More advanced devices are being studied that could add a new degree of flexibility and offer new capabilities, such as quantum wavelength-converters [93, 94], quantum switches [95], or quantum routers [96]. Beyond the physical layer, other work also focuses on further network techniques such as access mechanisms [97], switching time [98] or key storage [98].

As a result of this research, multiple QKD networks have been deployed. Most of them fall into the trusted repeaters networks category with dedicated links [99, 100, 101, 102, 45, 103, 104, 105, 106, 107]. Their purpose has been to show the advantages of QKD, the improvements on distance, key rate and to test its stability in a long-term scenario. Nevertheless, to gain commercial acceptance, the service must be cost competitive. Consistent with this, the integration of QKD in standard telecom networks has gained much attention recently.

The first approach is to move QKD systems to commercial scenarios using deployed, but unused, optical fiber (also known as dark fiber) [108, 109, 110, 111]. Although a remarkable advance, the fiber is still dedicated to only one quantum communication. A more advanced approach is then to share the fiber by transmitting the quantum signals alongside other conventional signals. The goal is to do this into the most used commercial network architectures: TDM-based access networks [112, 113, 114, 115], WDM-based access networks [115, 116, 117, 118, 119], and metropolitan areas [112, 120]. Nevertheless, up to this point, the solutions were limited to connect quantum users in an almost straightforward way, but using a shared deployed infrastructure. They did not aim to create a full-featured quantum network which would include sophisticated routing algorithms, and open the discussion in terms of scalability, flexibility, resiliency... or new weaknesses due to routing (e.g., in trusted repeaters networks).

1.2 MOTIVATION

This thesis focuses on the aforementioned problems of QKD. The final objective is to create a quantum telecom optical network, able to reduce the cost and usability barriers that separate QKD, and future quantum technologies, from its widespread use in society. It is structured as follows.

First, in Chap. 3, we tackle this problem by integrating quantum signals in commercial telecom networks. In particular, we focus on access networks based on passive optical technology. We give various non-intrusive solutions, depending on the specific network technology and the location of the QKD systems.

Later, in Chap. 4, we propose a quantum metropolitan optical network that consists in multiple access networks connected using a backbone ring. The network supports quantum and classical signals between all users and dynamic addressing. For this, we use WDM and wavelength-addressing. In Chap. 5, we extend the previous network design by including the distribution of entangled photon-pairs between all nodes.

We redo the proposed quantum metropolitan optical network using a new architecture in Chap. 6. The new design is based on a backbone mesh and active routing in order to accommodate more users.

Finally, in Chap. 7, we offer a new solution to the loss budget limitation that reduces the degree of trust put on the intermediate nodes called weakly trusted repeaters (WTR).

2 PRELIMINARIES

Here we introduce the basic concepts about quantum key distribution, fiber optics communications and metropolitan optical networks necessary to understand the rest of the thesis.

2.1 QUANTUM KEY DISTRIBUTION

Quantum key distribution (QKD) [1] is a quantum communication technology that allows two parties to grow an initial shared secret key with information-theoretic security, i.e., it is secure versus an eavesdropper with unlimited computational resources (as long as the initial assumptions hold). Simply, the eavesdropper cannot gain enough information to break the cryptosystem[1]. This security [122], based on a set of hypothesis, derives from the laws of quantum mechanics, which govern the quantum information used by QKD to process and transmit the key.

A generic QKD protocol starts with a source of random classical information that the emitter (Alice) codifies into the state of a quantum system selecting a certain preparation basis. Hereafter, we will consider 2-dimensional quantum systems, i.e., qubits. These qubits are then transmitted via a quantum channel to the receiver (Bob), who measures them using one of the possible preparation basis and acquires the information. Alice and Bob share now a correlated string of classical information. From the point of view of an eavesdropper (Eve), Eve could clone the arbitrary qubits and use the clones to obtain the information, but quantum mechanics precludes this option [123]. Furthermore, any attempt by Eve of somehow manipulating the transmitted qubit will modify the state of the qubit, which is later measured by Bob. As a result, the strings of Alice and Bob will differ by containing errors. The amount of errors is measured using the quantum bit error rate (QBER), defined as the number of errors over the total amount of detections. Hence, a posterior calculation of the QBER by both parties allows them to acknowledge the security of the transmission.

Later, Alice and Bob process their strings to distill a secret key using an authenticated classical channel to communicate. The authentication using a secret key is required to avoid man-in-the-middle

1 In information theory [121], the information of a random variable X is measured by its entropy $H(X)$. The entropy can be seen as the uncertainty or expected value of information contained in the variable. Therefore, $H(X) = 0$ means that there is no uncertainty about X; it does not give us any information.

attacks. Therefore, a QKD protocol needs an initial shared secret key between both parties. This procedure consists in: (i) time-tagging to synchronize the strings; (ii) basis reconciliation to discard values where measurement and preparation basis were not the same; (iii) parameter estimation e.g., QBER; (iv) error correction to make both strings identical; and (iv) privacy amplification to reduce the information of an hypothetical Eve.

Despite the variety of protocols, the behavior of a QKD system in terms of distilled secret key is similar. Considering a BB84 with one-way perfect post-processing and coherent attacks, the secret key rate K is a product of the raw key R, which depends on the detection rate and the particular hardware, and the fraction of secret key r. The secret fraction r is bounded by the mutual information between Alice and Bob ($I(A:B)$) and the information shared by Eve and both parties (I_{AE} and I_{BE}) [124]:

$$r = I(A:B) - \min(I_{AE}, I_{BE})$$

In the best case, $I(A:B)$ is the maximum information minus the one wasted during the distillation procedure due to errors ($leak_{EC}$). In case of perfect error correction, $leak_{EC} = H(Q)$, where Q is the QBER; hence: $I(A:B) = 1 - H(Q)$. For the other term, we consider the worst-case scenario where every error gives information to Eve: $I_E = \min(I_{AE}, I_{BE}) = H(Q)$. Therefore, the secret fraction r is bounded by [125, 124]:

$$r = 1 - leak_{EC} - I_E = 1 - 2H(Q)$$

This function is plotted in Fig. 2.1. As expected, the secret fraction r decreases with the QBER, up to a point where it goes down abruptly (in this case, for a QBER of 11%). At this point, the information wasted in error correction and privacy amplification increases dramatically.

2.2 OPTICAL REALIZATION OF A QKD SYSTEM

Typically, QKD uses photons as qubits carriers. The states of the qubit are represented by the photon's properties such as polarization, phase, spin, time-bin, etc. Therefore, the information is codified into the physical state. This implementation decision makes QKD systems an optical communication system, which has three basic components: a single-photon source (transmitter), a single-photon detector (receiver), and an optical medium (channel).

As we will see, all of these components introduce errors and losses, which harm the performance. As a result, all QKD systems have an inherent QBER that increases with the transmission losses between Alice and Bob. Even in an error-free scenario, losses would inevitably reduce the secret key rate to the point of making it unacceptable. Therefore, QKD systems have a limited loss budget that nowadays is

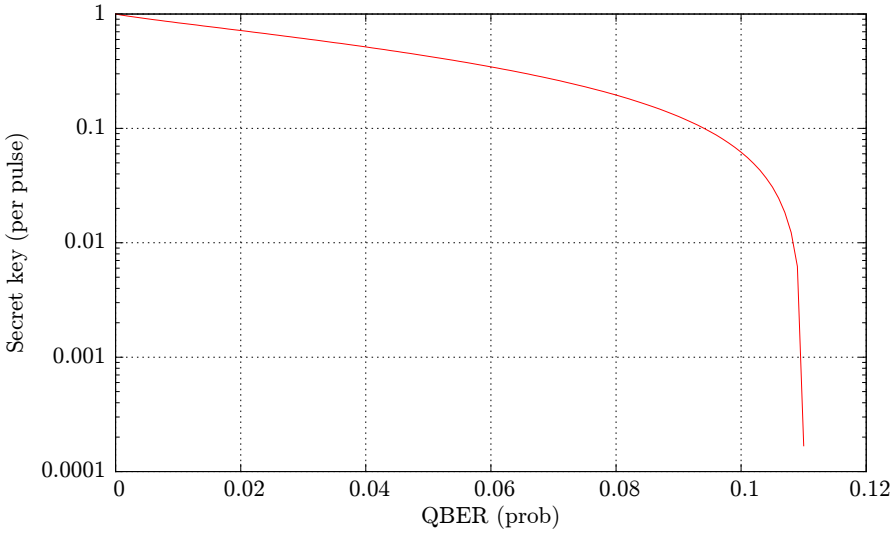


Figure 2.1: Secret-key of a perfect BB84 QKD system with one-way post-processing, no losses and considering coherent attacks.

approx. 20-30 dB [25, 2, 24, 18, 26, 71, 35, 38]. This is 100-150 km in a point-to-point link. Beyond that, QKD systems need to use low-noise detectors based on superconducting technology to achieve a loss budget of 40-50 dB (200-300 km) [20, 32, 21, 22]. However, they are rather unpractical at the moment as they require cryogenic temperatures to work.

2.2.1 *Single-photon source*

A single-photon source should work at high speed and emit photons on demand: only when triggered. However, due to the difficulty and cost of generating such photons, weak coherent pulses emitted by attenuated pulsed lasers are used as a substitute. An attenuated laser is just a laser diode, a common coherent light source, and a variable optical attenuator that allows to reduce the power of the signal to a single-photon level. This is, that the mean photon number per pulse (μ) is approx. 1. The laser diodes utilized for QKD systems are characterized by operating at a single wavelength, a high extinction ratio and, if required, a high coherence time (e.g., COW, DPS).

Given a μ, the probability of emitting a n-photons pulse with a laser follows a Poisson distribution [126]:

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

Therefore, alongside single-photon pulses, the source also emits empty pulses, which reduce the efficiency of the system, and multi-photon pulses, which can be a security hole [127]. For instance, for a typical experimental value of $\mu = 0.1$: 90.5% are empty pulses, 9% are single-photon pulses and the remaining 0.5% are multi-photon pulses. This

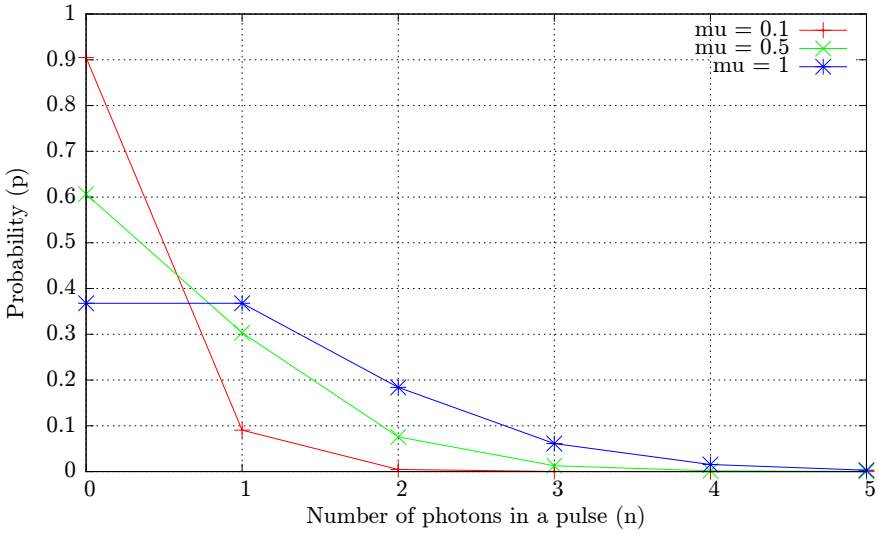


Figure 2.2: Poisson distribution for $\mu = 0.1, 0.5, 1$.

means that a 1 GHz QKD system is effectively working at 100 MHz. Fig. 2.2 shows the probability distribution of having n photons in a pulse for an attenuated laser with different μ configurations.

2.2.2 *Single-photon detector*

Although there are many technologies to detect single photons, most of the single-photon detectors (SPD) [128] are based on avalanche photodiode (APD) technology. The operating mode is simple: photodiodes are biased with a voltage high enough such that, when a photon is absorbed, an avalanche of electrons is generated and the resulting current detected. The probability of generating such an avalanche upon the arrival of a photon is called the quantum efficiency (QE). Similarly, there is also a probability of generating an avalanche even if no photon has been absorbed, known as dark counts. Once a detection has occurred, the SPD is discharged (quenched) and returns to the initial state. During this dead time, no bias is set and no signal can be detected. If the dead time is too short, electrons may remain at the photodiode crystal and generate a spurious avalanche, that will be registered as a detection as soon as the bias current is restored in preparation for another detection. These are the afterpulses. Finally, SPDs can also be gated, i.e., they are only open during short-time windows. In this case, two more parameters are needed: the frequency and the gate width.

2.2.3 *Optical medium*

The preferred optical medium is the optical fiber, typically made of silica, since it offers a closed waveguide that protects the weak single

Table 2.1: Transmission bands of the optical spectrum

Band	Wavelengths
O-band	$1260 - 1360$ nm
E-band	$1360 - 1460$ nm
S-band	$1460 - 1530$ nm
C-band	$1530 - 1565$ nm
L-band	$1565 - 1625$ nm
U-band	$1625 - 1675$ nm

photons and carries them to the detector via total internal reflection. In particular, single-core, single-mode fibers (SMF) are the most used ones. Thus, hereafter we use the term optical fiber to refer to single-core, single-mode fibers (unless noted otherwise).

However, the transmission of photons through an optical fiber reduces the power of the signal. This is known as the attenuation coefficient [129] of the fiber α (wavelength-dependent and expressed in dB/km) and it is calculated with the following expression:

$$\alpha = -\frac{10}{l} \log \frac{P(l)}{P(0)}$$

where l is the distance expressed in km, $P(l)$ is the power at distance l and $P(0)$ is the pumping power ($l = 0$), both in mW. Hence, given α and $P(0)$, we can calculate the power at any l:

$$P(l) = P(0)e^{-\alpha l}$$

Fig. 2.3 shows the attenuation coefficient of a SMF for the typical telecommunication spectrum and the typical spectrum bands for transmitting signals (see Tab. 2.1). As it can be seen, there are mainly two low-attenuation windows [2]: around 1310 nm ($\alpha \approx 0.35$ dB/km) at the O band, and 1550 nm ($\alpha \approx 0.2$ dB/km) at the C band. QKD systems, as modern conventional communications, tend to use the latter. However, to use the rest of the spectrum may be interesting in some scenarios where attenuation losses are not the major concern [64, 130, 65]. Next, we describe three possible origins of attenuation: absorption, bending and scattering.

Absorption

An absorption occurs when a photon interacts with an atom of the fiber and it is absorbed but not re-emitted. Hence, the energy of the photon is directly transferred to the fiber material, thus exciting it to

2 These are historically known as the second and third telecommunication windows, respectively. The first one, between 800 and 900 nm, is only suitable for short-distance transmission due to the high attenuation.

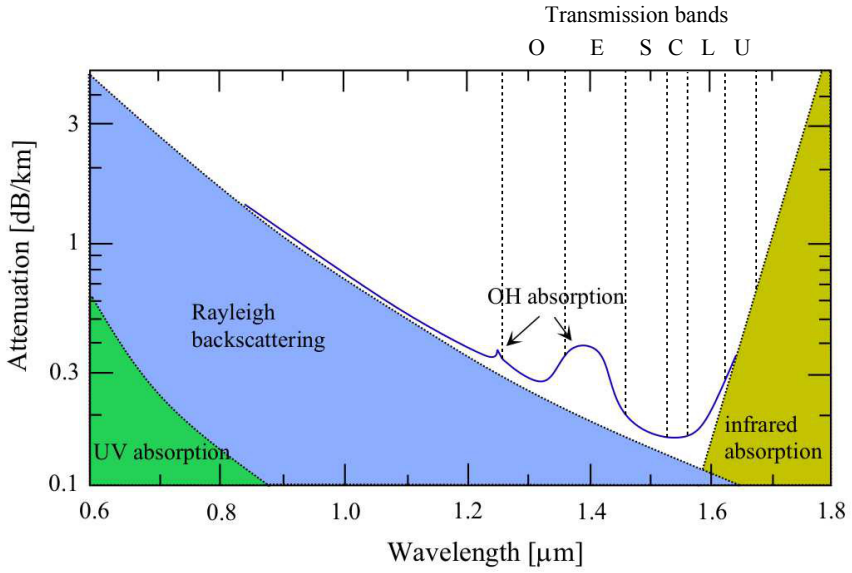


Figure 2.3: Attenuation coefficient of an optical fiber for the typical telecommunication spectrum and transmission bands. Major contributors to losses are indicated. it can be seen that the optimal transmission window is around 1550 nm, at the C band. Original figure from Ref. [1].

a higher state. Absorption is cumulative and uniform, i.e., the same amount of same the material always absorbs the same fraction of light at a certain wavelength. It can be due to three possible factors:

- Imperfections in the fabrication.
- Intrinsic absorption caused by the components that the fiber is made of. In case of silica fibers, there are two main regions: the ultraviolet absorption below 800 nm, and the infrared absorption beyond 1600 nm.
- Extrinsic absorption caused by impurities introduced into the fiber such as metal ions. The most typical ones are the water peaks at 950, 1240 and 1380 nm due to the presence of hydroxyl ions (OH^-).

Note that while imperfections and extrinsic absorption can be minimized by improving the construction of the fiber, intrinsic absorption can only be overcome by changing the own materials of the fibers.

Bending

An improper bending of the fiber (macro and micro) can destroy the total internal reflection phenomenon that guides the light within the fiber and thus lose a portion of the signal that is leaked to the exterior or reflected in the opposite direction.

Scattering

Scattering comprises several physical phenomena where the photon interacts with atoms of the fiber and, as a result, it is altered in terms of direction, phase, polarization or wavelength. Scattering is classified into elastic and inelastic, depending on whether the energy of the incident photon is conserved or not. Note that the energy of a photon E is related to its wavelength λ by:

$$E = \frac{hc}{\lambda}$$

where h is the Planck constant and c the speed of light. Hence, in a non-elastic scattering, where energy is given or taken from the medium, the wavelength of the re-emitted photon changes.

For elastic scattering, the primary source is Rayleigh scattering. Actually, in the telecommunication windows, it is the major contributor to losses (see Fig. 2.3). Rayleigh scattering is caused by the presence of small density fluctuations in comparison with the wavelength of the photon (typically $\lambda/10$) that alter the direction of the photon. The total loss is proportional to λ^{-4}. Hence, as the wavelength increases, the losses caused by Rayleigh scattering decrease. In particular, the power of the Rayleigh backscattering can be estimated as [75]:

$$Ray_{bwd}(z) = \beta(\lambda)P(0)(1 - e^{-2\alpha l})$$

where $\beta(x)$ is the Rayleigh coefficient at $\lambda = x$.

For inelastic scattering, we focus on Raman scattering[3] [131, 132, 129, 133]. Although the amount of signal scattered is much smaller than Rayleigh, it covers a broad spectrum. For instance, with a 1550 nm pump signal, the majority of photons are scattered approximately ± 150 nm around the pump signal. Beyond that, the amount of scattered photons decreases considerably, below the -100 dBm mark [134]. The spectrum is divided into stokes (wavelength higher than pump signal) and anti-stokes (wavelength lower than pump signal). Given a pump signal at λ_p with a certain $P(0)$, we can estimate the power of the Raman scattering, forward and backward, in a given point of the fiber (l) at λ_s as [133]:

$$RS_{fwd}(l) = \frac{G(\Delta\lambda)}{\alpha_s - \alpha_p} P(0)(e^{-\alpha_p l} - e^{-\alpha_s l})$$

$$RS_{bwd}(l) = \frac{G(\Delta\lambda)}{\alpha_s + \alpha_p} P(0)(e^{\alpha_p l} - e^{-\alpha_s l})$$

where α_x is the attenuation coefficient at $\lambda = x$, $\Delta\lambda = \lambda_s - \lambda_p$ and $G(x)$ is the Raman gain coefficient at that wavelength separation.

Fig. 2.4 shows the Rayleigh and Raman backscattering produced by an optical signal with $P(0) = 0$ dBm, $\lambda_p = 1550$ nm and $l = 20$ km.

3 Here we limit ourselves to spontaneous Raman scattering, and not the stimulated phenomena used for example in Raman amplifiers

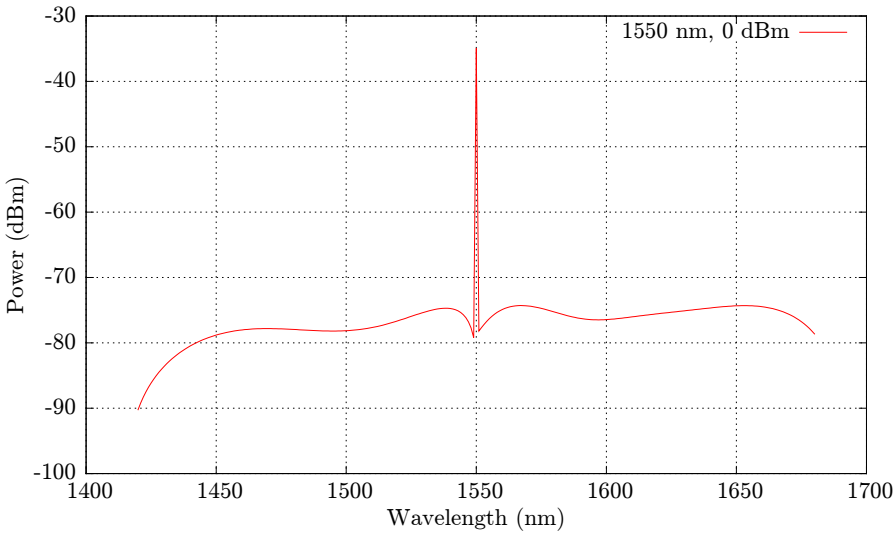


Figure 2.4: Spectrum of the Rayleigh and Raman backscattering produced by a 0 dBm, 1550 nm pump signal after 20 km of fiber.

As pointed out, the power difference between the two phenomena is significant, approx. 45 dB (depending on the particular scenario). As the fiber length, l, increases, the power also increases, until a peak at l_p is reached. Beyond l_p, the amount of previously scattered photons that are absorbed in the transmission surpasses the generation rate of new ones (which depends on the power of the pump signal that in turn decreases with l). Therefore, in the forward case, for $l > l_p$, the total scattering power decreases. However, in the backward case, the power saturates. The reason is that even if no photons are scattered beyond l_p, in the section from $l = 0$ to $l = l_p$ the same number of photons are being scattered than before. Adding more fiber does not change that. This behavior is shown in Fig. 2.5. The figure represents the power of the backward and forward Raman scattering at $\lambda_s = 1565$ nm produced by an optical signal with $P(0) = 0$ dBm, $\lambda_p = 1550$ nm.

2.3 MULTIPLEXING OPTICAL SIGNALS

Sharing the medium—and, in general, the entire communications architecture—, is a common practice in networks in order to reduce the cost per user and take advantage of the existing resources (especially if they are costly to deploy, e.g., optical fiber). This technique is known as multiplexing and consists in combining multiple signals into a unique stream of information that crosses the medium.

Within an optical infrastructure made of fiber, optical signals are multiplexed using a diversity of techniques. In particular, we focus on time division multiplexing (TDM) and wavelength division multiplexing (WDM). The first one divides the time into slots and, during each time slot, only one emitter is on. Hence, the medium is shared but not

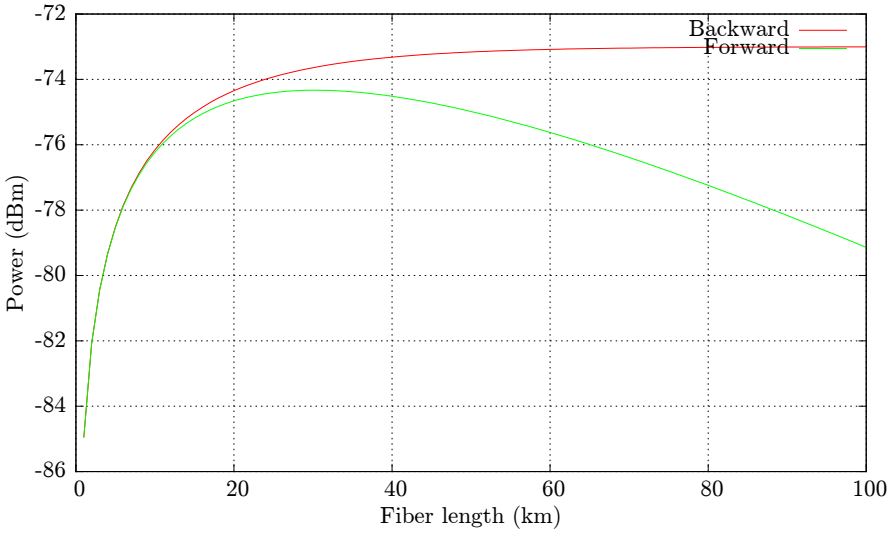


Figure 2.5: Power of the forward and backward Raman scattering produced by a 0 dBm, 1550 nm pump signal, and measured at 1565 nm.

used at the same time. In contrast, WDM allows to simultaneously transmit optical signals using different wavelengths, called channels, thus increasing the bandwidth of the link respect to TDM. Moreover, this configuration does not require synchronization between emitters. Due to these advantages, WDM is becoming widely used [135], even in parallel with TDM. Besides these two, we can found in the literature other multiplexing schemes for quantum signals such as subcarrier (SCM) [61], spatial multiplexing (SDM) [62], etc.

In WDM, each channel is named by its central wavelength, which is standardized by ITU-T. Depending on the spectral distance between adjacent channels, it is called coarse WDM (CWDM) [136] or dense WDM (DWDM) [137, 138]. CWDM is composed of 18 channels from 1270 to 1610 nm, each one spaced 20 nm (O, E, S, C and L bands). DWDM is mainly limited to the 1550 nm region (S, C and L bands) and, depending on the chosen grid, channel separation ranges from 200 GHz down to 12.5 GHz (1.6-0.1 nm) to accommodate from 40 up to hundreds of channels [139].

However, sharing the medium by multiple signals at the same time creates some problems due to the noise generated (or leaked signal) by each one and that affects the rest of the channels (i.e., channel crosstalk). This is especially important if some channels are used by quantum signals. Note that a 1 GHz, 1550 nm quantum signal with $\mu = 0.1$ has a power of -70 dBm, whereas a typical conventional signal has around 0 dBm. That is a 10^7 difference in the flux of photon per second. We focus on three sources of crosstalk: Raman scattering, four-wave mixing and devices' imperfections.

2.3.1 *Raman scattering*

Raman scattering was previously described. Its broad spectrum affects multiple CWDM channels and even entire spectrum bands. Although its power (≈ -70 dBm) is small in comparison with a conventional pump signal (≈ 0 dBm), the Raman scattering from a conventional signal can hinder a quantum signal and impede any quantum communication. There are several solutions: use ultra narrow band pass filters, a higher repetition rate to increase the total power of the quantum signal, put the quantum signal very close to the conventional signal (see Fig. 2.4), or move to an spectrum band where few photons are scattered.

An example of this last solution is allocating the quantum signal at the O band (1310 nm) and leaving the conventional signals at the C band (1550 nm), or vice versa [75, 74].

Another inelastic scattering phenomenon is Brillouin scattering. However, in contrast to Raman scattering, it has a very narrow spectrum bandwidth of approx. 100 MHz [140]. Therefore, in DWDM systems where the channel spacing is typically 200-50 GHz, Brillouin does not suppose a problem in terms of channel crosstalk.

2.3.2 *Four-wave mixing*

Four-wave mixing (FWM) [141] is a nonlinear phenomenon where a signal is created from the interaction of three pumping signals and the third-order susceptibility in silica. Given the following frequencies (w_i, w_j and w_k) for the pumping signals, the frequency of the new signal is defined by the expression:

$$w_{ijk} = w_i + w_j - w_k$$

In the degenerate case of only two pump signals, $i = j$. Given N pumping signals that range from w_{min} to w_{max}, we can calculate the number of first-order[4] mixing products M and the spectrum bandwidth (from w_1 to w_M) [142]:

$$M = \frac{1}{2}(N^3 - N^2)$$

$$w_1 = w_{min} + w_{min} - w_{max}$$

$$w_M = w_{max} + w_{max} - w_{min}$$

4 Higher-order mixing products are generated by mixing products and pumping signals, or other mixing products.

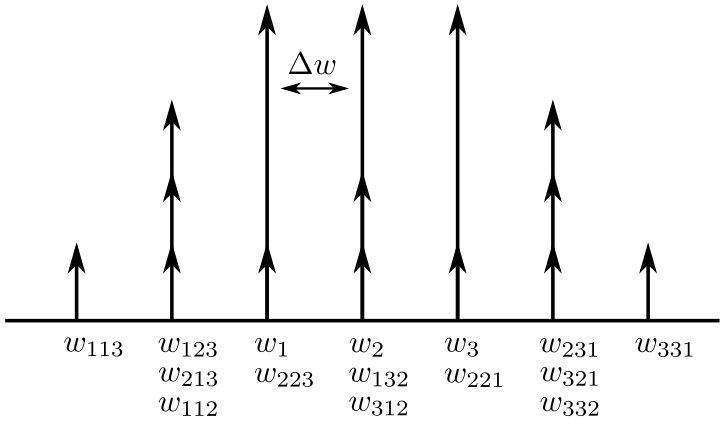


Figure 2.6: First-order FWM products produced by three signals with frequencies w_1, w_2, w_3 equally spaced Δw.

Fig. 2.6 depicts all the first-order mixing products generated by three signals w_1, w_2, w_3 equally spaced Δw. Note that some of them will fall in the same frequencies, e.g.:

$$\begin{aligned} w_{223} &= w_2 + w_2 - w_3 = w_1 \\ w_{132} &= w_1 + w_3 - w_2 = w_2 \\ w_{221} &= w_2 + w_2 - w_1 = w_3 \\ w_{312} &= w_3 + w_1 - w_2 = w_2 \end{aligned}$$

This is critical for WDM systems.

The power of a mixing product can be calculated as [143, 144, 142]:

$$P_{ijk} = \eta \frac{1024\pi^6 D^2 X_{1111}^2}{n^4 \lambda^2 c^2} \frac{L_{eff}^2}{A_{eff}^2} P_i P_j P_k e^{-\alpha L}$$

where η is the FWM efficiency, D is the degeneracy factor (equal to 3 if $i = j$, 6 otherwise), X_{1111} is the third-order nonlinear susceptibility, n is the refractive index of the core, λ is the wavelength of the mixing product, c is the speed of light in free space, L_{eff} is the effective length, A_{eff} is the effective area, P_i, P_j and P_k are the input powers of the pumping signals, α is the fiber attenuation coefficient at λ, and L is the fiber length. L_{eff} is calculated as:

$$L_{eff} = \frac{1 - e^{-\alpha L}}{\alpha}$$

The FWM efficiency η greatly depends on the phase-matching factor, which in turn depends on the channel spacing, the fiber chromatic dispersion (D_c) and the fiber length [143, 144, 142]. Considering a typical value for single-mode fibers of $D_c = 15$ ps/nm.km at the C band, and $L = 10$ km, the efficiency η equals 0 for a common DWDM channel spacing of 100 GHz [143, 144]. In this case, the FWM is negligible. However, in a scenario where η is almost 1 (i.e., zero

dispersion and narrow channel spacing), the power of the mixing product is approx. 20 dB weaker than the pumping signals [142, 140]. Assuming typical input powers for conventional signals of 0 dBm, P_{ijk} would surpass by at least 50 dB the power of a quantum signal (approx. from -70 to -100 dBm).

In order to reduce the FWM contribution, we can: (i) move the center of the channels such that the mixing products do not fall in the exact same wavelength, (ii) move to another band of the spectrum, and (iii) decrease the power of the conventional signals. For instance, given a conventional DWDM system that uses the C band (1530 to 1560 nm), the region affected by the first-order mixing products is delimited from 1501 nm to 1591 nm. Therefore, the solution for inelastic scattering of moving to the O band (1260 to 1360 nm) also works in this case.

2.3.3 *Device's imperfections*

In all network devices (e.g., splitters, filters, multiplexers, circulators), part of the signal is lost, mainly due to absorption or because it is transmitted through another output. There is an internal crosstalk between outputs. The amount of signal that is leaked is measured by the isolation of the device. For instance, given a filter for λ_c with an isolation of 60 dB and an input signal at λ_c of 0 dBm, through the reflected port we will measure a signal at λ_c of -60 dBm.

The isolation is also present in the optical fibers. As we have seen previously, part of a signal that is transmitted through a fiber is leaked to the exterior. Therefore, when multiple optical fibers are packed together in a fiber strand, there is a possibility that such signal enters one of the neighboring fibers [145]. This possibility is increased in multi-core fibers.

Note that in these cases, the signal leaked has the same wavelength than the original and thus it can be filtered.

2.4 METROPOLITAN OPTICAL NETWORKS

Optical fiber is the preferred medium in telecommunication networks. In comparison with the copper, fiber offers a higher bandwidth, longer distance (due to lower losses), and lower latency [140, 146]. All of them are indispensable characteristics for the modern telecom networks which have to withstand an increasing volume of users, traffic and types of services. This has propelled its adoption, starting at the backbone links and reaching now the last-mile [147, 148, 149]. Accordingly, network equipment is also changing to the optical paradigm, thus avoiding unnecessary electro-optical conversions. Through these optical components, signals are routed without modifying its optical nature. As a result, an uninterrupted optical path can be established be-

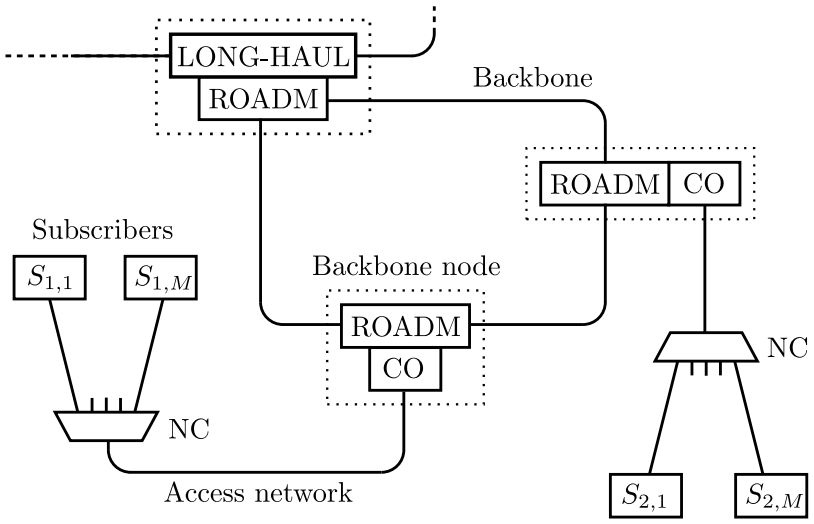


Figure 2.7: Scheme of a metropolitan optical network (MON). Users, also called subscribers ($S_{x,y}$ in the figure), are connected to tree-type access networks. Signals from all users are multiplexed using a network component (NC) and sent upstream to the central office (CO). The CO can route them to the backbone or downstream to the same users. Within the ring-shaped backbone, a series of reconfigurable optical add-drop multiplexers (ROADMs) allows to route signals between access networks. They also link to long-haul or other backbone networks.

tween any pair of network nodes, allowing the creation of a quantum channel.

This enables the possibility of using deployed infrastructure by the QKD systems to exchange keys between any two directly connected users of a telecom network. Moreover, the ability to create direct optical paths that could be used to correctly transport and route a quantum signal, opens the door to the integration or creation of quantum telecommunications networks, instead of just single point-to-point QKD links.

Due to the limited loss budget of QKD systems, among the existing optical networks [140], we restrict ourselves to optical networks up to a metropolitan area [150, 151]. These cover relatively small areas but they serve a huge number of final users, which are the potential market for quantum communications technologies such as QKD.

Fig. 2.7 shows the physical layer of a *canonical* metropolitan optical network (MON). There are two distinct subnetworks: tree-type access networks and a ring-shaped backbone network. The losses introduced by the network components can be found in Tab. 2.2.

2.4.1 *Access network*

The access network follows a point-to-multipoint architecture in order to connect the final users (optical network units, ONU) to a single

Table 2.2: Insertion losses of common network components. Values are from commercial models available in the market [3, 4, 5, 6, 7].

Component	Operating wavelength	Insertion losses
Single-mode fiber	1550 nm	0.20 dB/km
Single-mode fiber	1310 nm	0.32 dB/km
1 : 2 Splitter	1260 – 1610 nm	3.6 dB
1 : 4 Splitter	1260 – 1610 nm	7 dB
1 : 32 Splitter	1260 – 1610 nm	16.5 dB
1-channel CWDM OADM	1270 – 1610 nm	$0.4 - 0.6$ dB
1-channel DWDM OADM	1525 – 1610 nm	$0.4 - 0.6$ dB
4-channels CWDM mux	1270 – 1610 nm	1 dB
1310/1550 WDM mux	1260 – 1360 nm	0.5 dB
	& 1500 – 1600 nm	
Bandpass filter		$0.4 - 0.6$ dB
Fiber Bragg grating		0.1 dB
Circulator		0.8 dB
Connectors		0.2 dB/pair
32-channels AWG (100 GHz)	1533 – 1558 nm	3 dB
4×4 to 192×192 Switch		1 dB

node at the central office of the telecom's provider (optical line terminator, OLT). A first part of the network composed of dedicated fibers goes from the ONUs to a network component (NC) that is in charge of correctly routing all signals. The NC is typically a passive component [152, 153], i.e, it does not require any power. Hence, the access network is commonly called a passive optical network (PON). The second part of the network goes from the NC to the OLT and it only has one fiber, which is shared among all ONUS. No matter the type of access network, in all of them the operating mode is the same: the traffic goes from ONUs to OLT, and vice versa.

In TDM-based access networks, called TDM-PONs, the NC is a 1:N optical splitter that physically divides the signal into N parts, thus reducing the power in half (3 dB) every time that N is doubled. For example, a 1:128 splitter introduces at least 27 dB of losses. Using splitters as NC allows to easily replace a splitter by a series of smaller ones connected in a cascade configuration, thus creating a tree topology with multiple branches, but preserving the overall splitting ratio.

Typically, a TDM-PON uses two signals via WDM: downstream (from OLT to ONU, at 1490 nm) and upstream (from ONU to OLT, at 1310 nm) (a third one is reserved for DTV purposes at 1550 nm). Both signals are shared among users via TDM. The upstream signal, divided into upstream frames, assigns time slots to the ONUs (TDMA)

depending on their activity and type of traffic. On the other hand, the downstream signal is directly broadcasted over all ONUs by the splitter, and ONUs are responsible of using only their data from the downstream frame. TDM-PONs are the core of standards G-PON [154] and E-PON [155], and their next-generation successors XG-PON [156] and 10G-EPON [157], respectively.

In WDM-based access networks, called WDM-PONs, the splitter is replaced by a wavelength multiplexer which has very low losses (3 dB for 32 users), typically based on arrayed waveguide grating technology (AWG). In contrast to the operating mode of TDM-PON, here each ONU has one or more DWDM channels for its own use. Although commercial AWGs have around 32-128 channels, laboratory implementations have reached 512 channels [158]. However, the increased cost per user has prevented momentarily WDM-PON from being a standard. This is expected to change, gradually, in future PONs as the bandwidth requirement keeps increasing. For instance, the second next-generation PON standards, that will replace 10 Gb/s PONs, are based on TWDM-PON technology [159]. The idea is to simply stack several XG-PONs using WDM. By this procedure, the backward compatibility is guaranteed at the same time that new requirements are met.

The ability to use more than one channel per user (port) is due to the cyclic behavior of the AWG. Through each port, not only a channel can be used, but also its periodical ones. For instance, given a grid of 40 channels uniformly arranged from 1520 to 1560 nm, the periodical bands will be 1560-1600, 1480-1520, etc. The common use is to assign to each ONU one channel for downstream and one among the corresponding periodical set for upstream [147]. We have characterized the periodicity of a commercial 100 GHz 32-channels AWG [6] using three tunable lasers to cover the whole 1260-1620 nm range. The lasers were fed to the common port and an optical spectrum analyzer was used to measure the output port. In Fig. 2.8 we present the spectrum obtained summing the outputs 1, 8, 16, 24 and 32. Only output 16 is shown for the full range, including the 1340 to 1520 nm region. As shown in the figure, the AWG successfully works at the O band without introducing extra insertion losses. We can seamlessly implement the mentioned scheme of moving the quantum signals to the O band in any WDM-PON, and thus isolate them from any possible crosstalk.

2.4.2 *Backbone network*

Once all users are grouped in access networks, these have to be connected to create a single metropolitan infrastructure. For this task, OLTs are connected to a series of nodes that are then interconnected

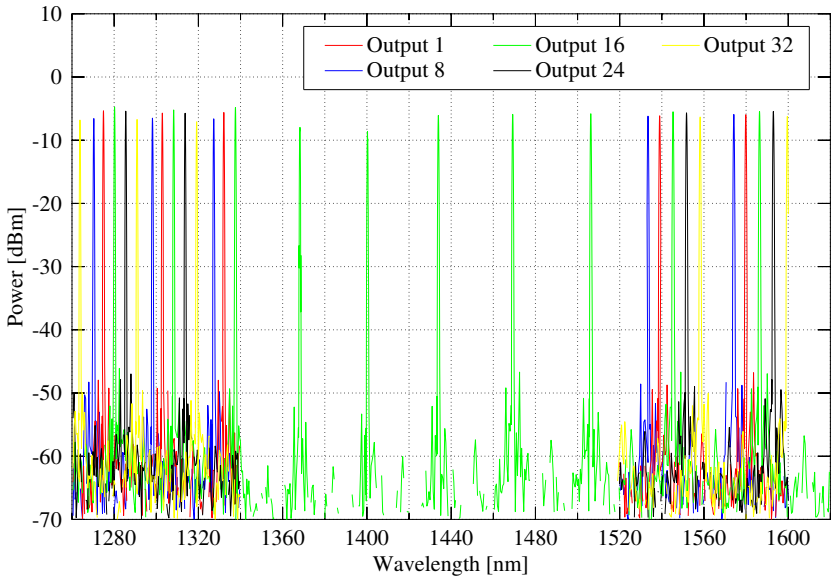


Figure 2.8: Experimental data of the cyclic behavior of a 100 GHz 32-channels AWG in the 1250-1620 nm range. Only outputs 1, 8, 16, 24 and 32 are shown, and, among them, only output 16 is presented over the whole range. Periodic channels have the same color.

following a ring topology with a fixed direction[5]. This second network is known as core or backbone network. Beyond allowing communication between ONUs of different access networks, they can also link to other backbones or long-haul networks.

To support all the traffic, the high capacity links between the backbone nodes use WDM technology. The signals propagating through these channels are added or dropped at the backbone nodes using optical add-drop multiplexers (OADM). OADMs can be based on multiple technologies and architectures [160]. Since their role is to be the core of the network, most of the requirements put on the network finally rely on their flexibility, reliability and resiliency. For this reason, modern OADMs are reconfigurable (ROADMs) and based on wavelength selective switches (WSS) [161] which allows to: dynamically route channels, thus making the ports wavelength-independent; change direction; and to drop a channel through multiple ports. These are known as colorless, directionless and contentionless ROADMs, or simply CDC ROADMs [162].

2.5 LIMITATIONS OF QUANTUM OPTICAL NETWORKS

As we have seen, telecom optical networks offer a unique possibility of integrating quantum signals in a pervasively deployed infrastructure

5 A bidirectional backbone ring is typically constructed by using two different fibers, one in each direction.

that has the potential to reach a huge market share. However, for this task, we have to take into account some fundamental limitations that are imposed by the very own nature of the quantum signals and, in some cases, the imperfections of quantum technologies. Next, we enumerate the most important ones:

- Since the information is carried by qubits that are in turn codified into the physical state of photons, it is mandatory to have a clear direct optical path between Alice and Bob.
- Even at high rates, such as 1 GHz, quantum signals have an extremely low-power in comparison with conventional ones (-70 dBm to 0 dBm). This difference highlights the importance of isolating the quantum signal from the conventional one and its noise. Even the weakest phenomena can mask the quantum signal and increase the QBER dramatically.
- Currently, there are no commercial quantum wavelength-converters [93, 94]. Hence, the quantum signal has to use the same wavelength throughout the whole network.
- Similarly, commercial quantum amplifiers or repeaters are not expected to become mainstream in many years. Therefore, the loss budget of the optical path between the two users has to be inferior to the loss budget of the QKD system. Otherwise, trusted repeaters have to be used.

These limitations create a rigid set of rules in contrast to the flexibility that we found with conventional signals. The result is a quantum telecom network that can be viewed as just one big infrastructure that cannot be modularized in smaller subnetworks due to the absence of quantum intermediate nodes that help to translate between subnetworks, thus, increasing the complexity. For example, if the network is based on WDM, we have to consider the whole network when creating the channel plan. This approach collides with the typical one, where each subnetwork has its own grid and the edge nodes (e.g., ROADMs) operate with the signals.

3

QUANTUM COMMUNICATIONS IN PASSIVE OPTICAL NETWORKS

This first chapter deals with the integration of quantum communications in optical access networks based on passive technology. The objective is to enable the transmission of quantum signals between specific sets of nodes. This basic approach reduces the costs and permits quantum information technologies to slowly become a reality before trying to deploy a complete quantum optical network.

Although access networks are short-span, they seem to be the next logical step after the point-to-point deployments because of their final users, pervasiveness, loss budget, reduced number of signals and routing simplicity. We propose different *ad hoc* solutions for the most common technologies and multiplexing schemes: TDM-PON (in particular, standards GPON and EPON), and WDM-PON.

Before going into details, we have to define the location of the QKD devices: in the ONU and OLT, or only in the ONUs. The former approach is interesting from a telco point of view; it allows them to offer new services based on quantum technologies but retaining the control. Another advantage is that keeps the SPD at the telco facilities. The SPD is the most expensive component, fragile, and likely to be upgraded. Nonetheless, in this scenario the telco would act as a trusted party and the OLT as a trusted repeater: quantum communications are end-to-end, where both ends are final users, not a telco node. The last approach is appealing from a user point of view, which has bought a QKD system and wants to use it in the network. For this, the user will connect the QKD devices to the network nodes that he has access to: the ONUs. In this case, communications preserve the security, and the role of the telco would be just to allow them.

3.1 TDM-PON (GPON AND EPON)

As described in Sec. 2.4.1, TDM-PONs use splitters for routing, typically in a tree topology with multiple branches. This allows us to connect the QKD systems in a branch, as standard ONUs (see Fig. 3.1), and isolate them from ONUs located in the rest of the network [1]. Note that a branch can be always created without hindering the network's performance whenever the maximum loss budget allowed by the standard is not exceeded.

Now, in order to create a direct optical path between the QKD systems, we use a fiber Bragg grating (FBG), after the second splitter,

1 Solutions for the ONU-to-OLT approach already exist [112, 113, 114].

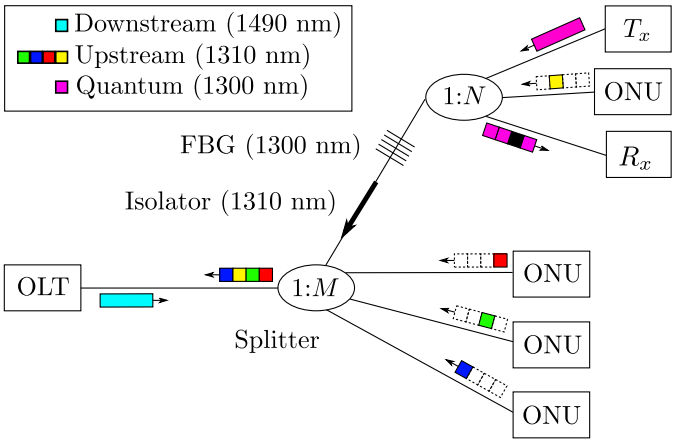


Figure 3.1: TDM-PON with QKD integration. A fiber Bragg grating (FBG) is used to enable a direct optical path between QKD devices, and an isolator to reduce the backscattering from the upstream signal. Communication frames are depicted as colored rectangles, where the colored squares represent time slots assigned to different ONUs.

that reflects back the quantum signal. FBGs are in-fiber filters with low losses (Tab. 2.2) and configurable passband (0.4-70 nm). The passband only affects the quantum signal; the rest of signals remain unaltered. Alongside the FBG, we add a 1310 nm isolator to reduce the backscattering of the upstream signal, especially from ONUs located outside the QKD branch.

3.1.1 *Scattering effects*

Regardless of having a dedicated optical channel, quantum signals still share the fiber with conventional signals (approx. 0 dBm). In order to reduce the noise reaching the SPD, we allocate the quantum channel just beside the upstream, at 1300 nm. The penalty to be paid is an increased absorption of 0.1 dB per km, with respect to the 1550 nm window, a minimal amount considering the expected fiber lengths and the losses of the splitters. Next, we explain the effect of each conventional signal.

From the downstream signal, only the forward Raman scattering can produce crosstalk in the quantum channel. However, the Raman scattering produced by a 0 dBm signal at 1490 nm [66] is negligible at the quantum channel (1300 nm). Furthermore, photons will be scattered mainly between the OLT and the first splitter, and, afterwards, signal and noise are highly attenuated by the splitters. In consequence, we put a band-pass filter before the SPD centered at the upstream signal and wide enough to include the quantum one. The objective of the filter is to remove the downstream signal and its noise (located at other wavelengths). The precise passband will depend in the exact

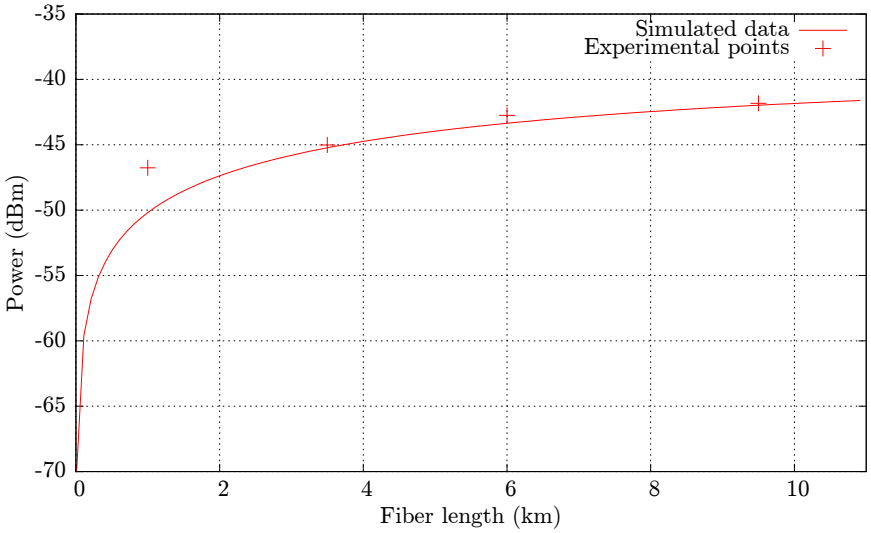


Figure 3.2: Power of the Rayleigh backscattering produced by a −6.3 dBm pump signal at 1310 nm. We compare the measurement results of the laboratory (points) with the simulated data (solid line).

wavelength of the upstream and quantum signal. Note that depending on the spectral and isolation characteristics of the filter, more than one might be necessary.

In the upstream signal, we focused in the two major backscattering phenomena: Raman and Rayleigh. In particular, we measured the backscattering in the laboratory using a SFP transceiver at 1310 nm with a peak power of -6.3 dBm (peak at 1308.35 nm), multiple fiber configurations (1, 3.5, 6 and 9.5 km), a 1310 nm circulator (0.9 dB losses), a power meter and a 5-MHz SPD from the IdQuantique Clavis 3100 QKD System with a dark count probability of $8.8 * 10^{-5}$ per gate. The power measured is shown in Fig. 3.2 over a simulation of the expected Rayleigh backscattering using the formula of Sec. 2.2.3.

After considering the losses of the splitters, isolator and FBG, the measured noise at the QKD branch is: (i) when the ONU is located outside the QKD branch, approx. $8.8 * 10^{-5}$ prob/gate (dark count rate); and (ii) when the ONU is located inside the QKD branch, approx. from $0.09 * 10^{-2}$ to $0.016 * 10^{-2}$ prob/gate (depending on the second splitter ratio). In the last case, the SPD is saturated. This means that a detection occurs with a probability higher than expected (approx. 10^{-4} prob/gate).

For the additional DTV signal, a similar reasoning as in the downstream 1490-nm signal applies. The difference is that the SPD will require a better filtering stage in order to remove both signals and their noise.

Other scattering effects of minor impact were not considered. For instance, due to the channel separation, four-wave mixing (FWM) and Brillouin scattering can be neglected.

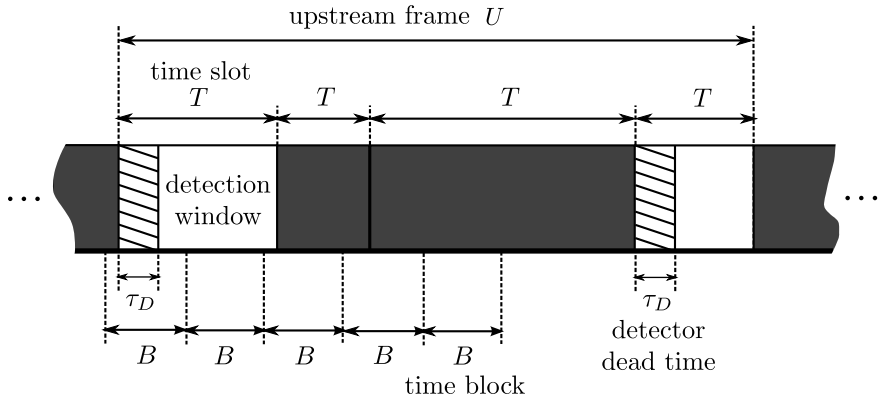


Figure 3.3: Upstream frame of a TDM-PON divided into time slots of variable length. Each time slot is assigned to a given ONU, and they are colored depending on whether the emitting ONU is located in the same branch than the QKD systems (gray) or not (white). Two QKD users may exchange key using the time slots marked white, which correspond to low noise periods.

3.1.2 *Proposal*

Our experiments show that the noise reaching the SPD when the emitting ONU is located outside the branch is nearly zero. Since time slots are dedicated, during an upstream frame (see Fig. 3.3), there will be low-noise periods and saturated periods (depending where the ONU emitting is located). The low-noise periods could be used to transmit quantum signals under the assumption that QKD devices are somehow synchronized with the TDM-PON.

As we will show, this synchronization can be avoided by performing a collision detection during the QKD post-processing. The objective is to distinguish noisy data blocks. Using an estimation of the expected number of detection per block (based on the expected detection probability), most erroneous detections can then be ruled out by simply discarding *blocks* with a number of detections above that threshold. The price to pay is a reduced efficiency when compared to an explicit TDM case.

Note that we are already considering a highly-populated network[2], i.e., one where the usage is close to 100%. Although an apparent contradiction, this is actually a favorable scenario: the number of slots assigned to local ONUs is smaller, which increases the non-saturated time per frame where QKD is possible.

The ability to discard noisy blocks depends on the amount of detections per time slot. The post-processing method can only distinguish a saturated time slot when the number of detections is significantly higher. Therefore, the frequency and dead time of the detector are

2 In a low-usage network, the time slots not assigned to any ONU are also low-noise periods.

crucial parameters to ensure that enough detections are gathered per time slot. For example, in the case of TDM-PONs working at ≈ 1.25 Gbps (e.g., EPON, GPON), we consider ≈ 410 ns to be the shortest time slot, which corresponds to an ethernet frame with the minimum payload (64 bytes).

Up to this point we have only considered the quantum signal. For the distillation procedure, QKD systems can operate as a regular ONU and use their time slots. However, the performance would be reduced since the system could not exchange qubits and distill key at the same time. If this poses a problem, another solution is to use a channel outside the channel plan and well separated from the quantum channel to avoid any crosstalk.

3.1.3 *Simulation*

We have implemented the discussed post-processing method as a proof of concept. For this, we have simulated a 1:128 GPON (loss budget of approx. 28 dB). The total number of ONUs is not needed. The simulation only requires the number of ONUs within the QKD branch and the percentage of the upstream frame that they use. How the rest of the upstream frame is distributed is not a relevant factor. In any case, it is noise-free time for QKD. Accordingly, for the simulation, we generated the traffic produced by only these particular ONUs by:

1. Split the upstream frame (125 μs in the GPON standard) into time slots. Assign a percentage of those to the ONUs in the QKD branch. Time slots have a variable size, with a minimum of approx. 410 ns (ethernet frame without payload).

2. Generate the detection gates and assign a detection probability to each gate depending whether they belong to a saturated time slot (emitting ONU in the QKD branch) or not.

3. Group gates into blocks of length B and count the number of detections. If it surpasses a threshold, discard the block. Note that blocks are not synchronized in any way with time slots (see Fig. 3.3). We discard the neighboring blocks as well, even if they are non-saturated, to ensure that the full time slot is completely removed.

Simulation was computed using typical values for the QKD device: 1 GHz laser and SPD, $\eta = 0.1$, $\mu_{opt} = t_{line} \cdot \eta$, $p_d = 10^{-5}$ ns^{-1}, $\tau_D = 50$ ns, and 100 ps of gate width [24, 114]. The fiber length within the QKD branch is 1 km (i.e. 2 km between a QKD pair) and the whole network ranges from 5 to 15 km. Two network configurations were considered: first splitter with 16 or 32 outputs (M in Fig. 3.1) and a second splitter (QKD branch) with 8 or 4 outputs (N in Fig. 3.1). Ports in the QKD branch not used by the QKD devices are assumed

to be assigned to conventional ONUs, hence there will be two or six conventional ONUs in the QKD branch. Results are compared for different non-saturated time per frame.

3.1.4 *Results*

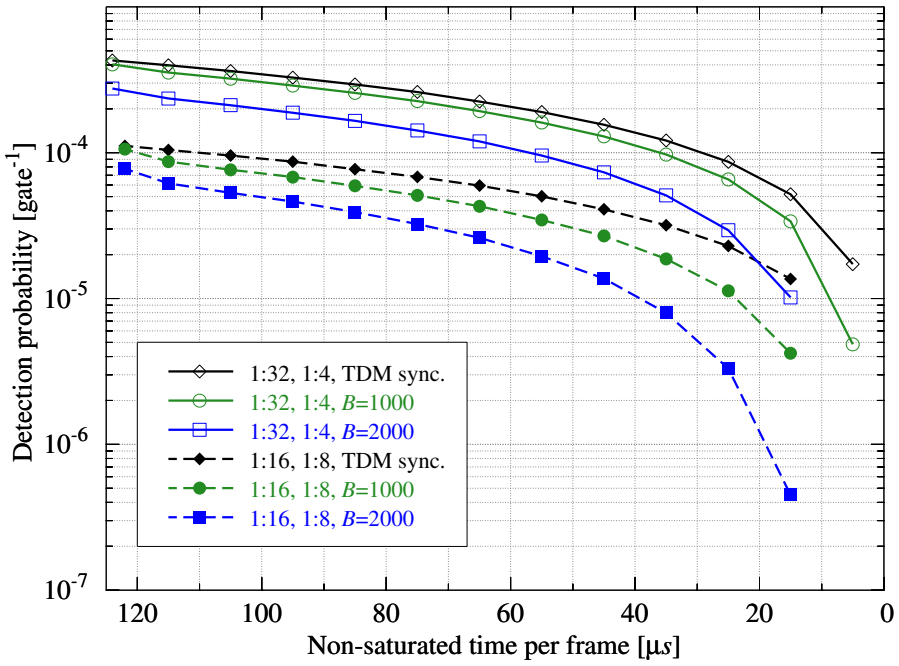
Simulation results are shown in Fig. 3.4. The figure shows the effective detection probability p^*_{exp} and QBER. p^*_{exp} is calculated as the number of detections, after the post-processing, over the total number of opened detection gates. Results are shown for two block lengths B: 1000 and 2000 detection gates. A threshold of 2 detections per block was used in the 1:32 1:4 network, while in the 1:16 1:8 case it was set to 3. The QBER is well below the threshold allowed for secret key distillation under the assumption of BB84 and one-way key distillation (11%). Note that the QBER for low non-saturated times increases because the number of single photon detections decreases, but the dark count probability remains constant. On the other hand, the high QBER for large non-saturated times is due to an increase of the number of small blocks wrongly marked false by the protocol.

In the case of a secondary 1:4 splitter, QBER is below 2% and p^*_{exp} is above 10^{-4} over a wide range of available time. The final secret key rate will depend on the QKD system itself, the security assumptions and the actual load of the network.

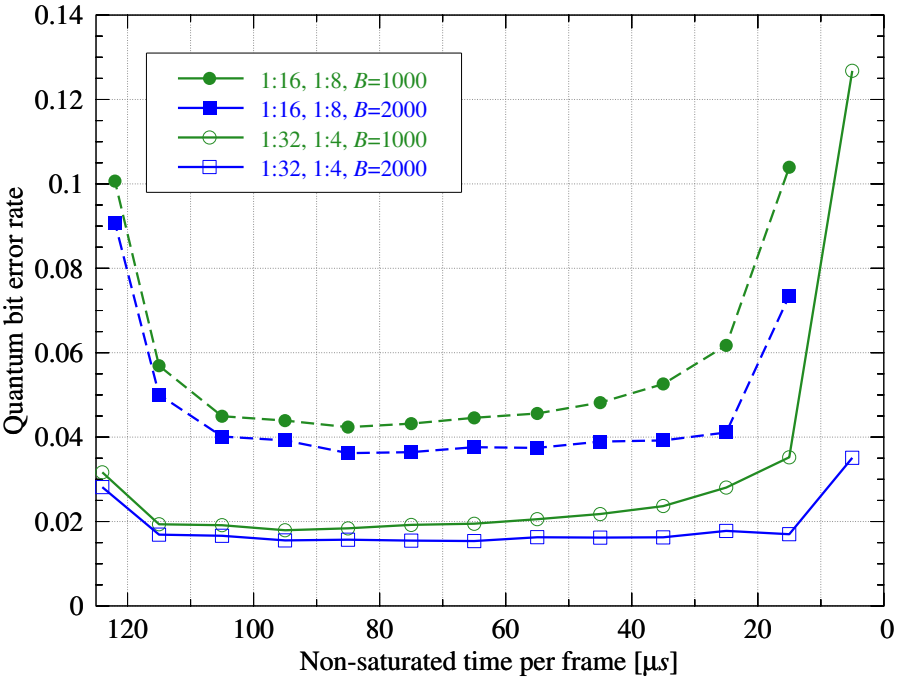
3.1.5 *Next-generation TDM-PONs*

Our solution works for the nowadays mainstream PON standards. Nevertheless, their respective successors, XG-PON and 10G-EPON, have been already standardized and they are expected to replace the old standards in the next years. Fortunately, the new standards are very similar to the old ones. This is of great help for solutions and technologies based on the old standard, like ours, which can adapt to the new one in a relatively easy way.

If we focus on XG-PON, there are two changes that affect our solution: (i) new wavelengths for upstream and downstream, 1290 nm and 1580 nm, respectively; and (ii) a higher upstream line rate (2.48 Gbps). Meanwhile, the physical scheme (topology and network components), loss budget (approx. 29-31 dB), and operation mode (two signals wavelength-multiplexed that are shared among the ONUS via TDM) remains the same. The first change does not suppose a problem. Actually, it benefits our solution since it moves further away the downstream signal from the quantum one. Similarly, the second change does not invalid our solution. A higher speed does not invalidate the fact that the upstream frame is still divided into time slots that are assigned to the ONUs. For that reason, there will be always saturated and non-saturated time slots. But, this puts pressure on the SPD. As



(a)



(b)

Figure 3.4: Effective detection probability p^*_{exp} and QBER of a quantum signal as a function of the non-saturated time per frame (125 µs) in a GPON. Results are compared for two network configurations allowing up to 128 users, a 1:4 (1:8) splitter connected to a 1:32 (1:16) splitter, and two block lengths, B = 1000 and 2000. The detection probability assuming TDM synchronization is also shown.

stated before, the number of detections of the SPD during a time slot of minimum size is a crucial parameter to be able to establish a feasible threshold and thus detect saturated time slots. This is basically set by the relationship between the frequency and dead time of the SPD, and the upstream rate and minimum length of the time slots. If we have the same block length at a higher speed, we will require better SPDs.

Beyond this next-generation, the second next-generation, currently in standardization process, will be based on TWDM-PON. Even though the final version is not available yet, in principle it could work since everything indicates that the channels used will be located at the S, C and L band using a DWDM grid. Despite using more channels, they will be concentrated in a small part of the spectrum. As a result, there will be empty-bands for the quantum channels, e.g., O band. In this case, the post-processing method will be unnecessary. Quantum channels will be used uninterruptedly with a good filtering stage before the SPD.

3.2 WDM-PON

The integration of quantum channels in a WDM-based access network is simpler than in TDM-PON. Like the TWDM-PON case, even though more conventional channels are used (typically, one or two per ONU), they use a DWDM grid and they are located in the C band of the optical spectrum. This arrangement leaves a considerable portion of the spectrum free for using quantum channels at any time without any kind of synchronization or post-processing.

3.2.1 *Scattering effects*

Let us suppose that conventional signals are confined to the C band ($1530 - 1565$ nm) and quantum signals are 200 nm away. Before the SPD, we connect a perfect bandpass filter that removes photons at other wavelengths: we measure our channel and nothing else. Hence, the quantum signal can only be disturbed by phenomena capable of producing crosstalk at the wavelength of the quantum signal. This assumption already discards Rayleigh scattering and crosstalk in the devices. Moreover, the rest of major crosstalk phenomena get minimized (see Fig. 3.5): (i) the Raman scattering is negligible at 1300 nm, and (ii) first-order FWM products fall in between 1495 nm and 1600 nm (See Sec. 2.3).

Surely, the problem lies in the assumption of a perfect filtering stage. Even if no phenomenon produces a considerable amount of crosstalk, the amount of photons that has to be filtered is higher than in the TDM-PON case. While a TDM-PON like GPON/EPON has 2-3 signals, a typical WDM-PON has at least 64 (32 users, 2 signals per user). Filters with a higher isolation are required.

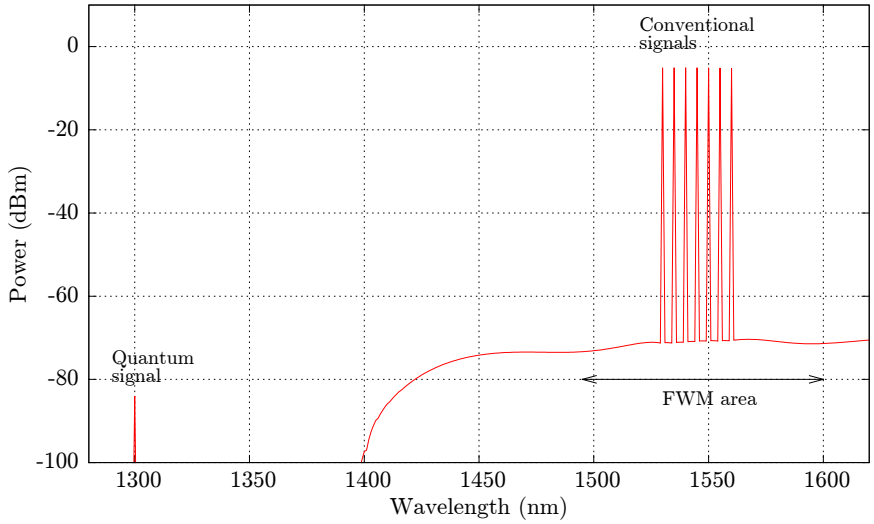


Figure 3.5: Spectrum of the upstream signals of a WDM-PON arriving to the OLT (32-ch AWG and 15 km span). Alongside the conventional signals at the C band, a quantum signal is emitted at 1 GHz and at the O band (1310 nm).

3.2.2 *Proposal ONU to OLT*

With this configuration, the integration consists in looking for a noise-free channel in the spectrum and configuring the QKD system to use it (laser, filters, etc). The channel selected has to belong to the periodic set of the port that the QKD system is connected to. If that is true, the signal will be routed automatically by the AWG thanks to the periodicity (see Sec. 2.4.1) without affecting the operation mode of the rest of ONUs. We suggest to select quantum channels at the O band ($1260 - 1360$ nm) of the spectrum because of the good performance of SPDs at that region [48], the similar network losses (see Tab. 2.2), and the almost 200 nm separation from the C band.

3.2.3 *Proposal ONU to ONU*

For this second approach, we have a fundamental limitation. We need to enter and leave the AWG through different ports, thus using different channels, using only one wavelength. This can only be done using a wavelength converter for quantum signals, but they are commercially unavailable at the moment. The routing has to be done mandatorily before crossing the AWG. For this task, we propose to use an optical switch before the AWG, with a larger number of ports than the AWG. The extra ports are used to create return paths (i.e., two ports connected in loop). This connection scheme is shown in Fig. 3.6. Now, signals can be routed: (i) to the AWG, as before, only

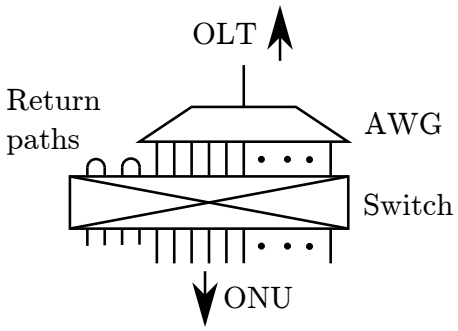


Figure 3.6: Connection scheme of the AWG of a WDM-PON with QKD integration ONU-to-ONU. A switch is placed before the AWG with enough ports to create return paths for the quantum signals.

affected by the losses of the switch (see Tab. 2.2); and (ii) to the return paths, and back to the ONUs.

Note that the switch is an active component and it could require modifications of the network infrastructure (e.g., changing the physical location of the NC). This can be overcome by using a remotely pumped approach based on power-by-light, where the power is supplied from the OLT. Putting aside this possible drawback, this solution brings crucial features: the ports of the switch are wavelength-independent, and the quantum signal is transmitted always over a dedicated fiber without having to coexist with conventional signals. We do not have to worry about noise, selecting wavelengths, building complex filtering stages, and reconfiguring QKD devices. Furthermore, it is compatible with the ONU-to-OLT scheme.

3.3 CONCLUSIONS

Access network based on passive optical components are, in essence, an ideal scenario for the QKD integration whenever we can control the crosstalk from the powerful, conventional signals. Despite their limited reach and number of users, they are the next step for QKD networks after dedicated point-to-point links.

Here we have shown how up-to-date QKD devices can be directly integrated in these networks, in particular in the widely used GPON and EPON standards, based on TDM, and in the promising WDM-PON. Furthermore, proposed solutions are future-proof; the schemes are, in principle, compatible with next-generation and second next-generation PON standards (as long as QKD technology keeps improving).

The main advantage is that the integration is straightforward and transparent to the rest of the network. It does not require any modification, neither of the devices nor of the standards and protocols (e.g., imposing power limitations), or any kind of synchronization. This effort-less and low-cost approach implies an efficiency loss in the worst case, at the benefit of putting all the pressure on the QKD

devices—the part that we control—, instead of demanding work and sacrifice to the conventional part.

The only physical addition is done in the ONU-to-ONU approach, where we need a device capable of routing back the quantum signal to the ONUs. The particular device depends on the type of PON: a bandpass filter in a TDM-PON, and a switch in a WDM-PON. Nevertheless, both devices introduce very few losses and do not affect the rest of signals. The synchronization is substituted by using a channel dedicated to the quantum signal and, in case it is needed, a collision detection mechanism in the QKD post-processing that discards noisy time slots.

4

QUANTUM METROPOLITAN OPTICAL NETWORK

In the last chapter, we discussed solutions to integrate quantum communications in commercial telecom infrastructures. The procedure was to study the commercial network architectures and to find a way to create a quantum channel between a set of nodes of the existing network. These ad-hoc solutions are useful in a first step for quantum communication technologies, but they fall short when we want to, for instance, increase the reach or the number of quantum users. The quantum layer of the network is constrained by the unmodifiable conventional protocols, standards and technologies.

Therefore, the next step is to extend this concept to a full quantum telecom network based on commercial technology that can run in parallel with the conventional one. This offers several benefits: the number of quantum users increases; maximizes the network throughput, resiliency and flexibility; and still uses the deployed commercial infrastructure.

Here we propose a quantum metropolitan optical network that is easy to deploy and maintain. It is based in the canonical metro architecture described in Sec. 2.4 and uses standard commercial optical components to take advantage of all existing resources (telecom facilities, dark fiber, etc), and thus able to pass the quality and availability tests required in a real-world deployment. The network is shared using WDM between many quantum users and it provides each one with a quantum link that is composed of a quantum channel and a conventional channel. The latter carries the conventional signals required by the quantum devices, e.g., the signal used to keep the devices synchronized.

Next, we describe in detail the WDM grid used and the design of the network and its nodes. Finally, we construct a testbed and we characterize it in terms of losses, noise and users.

4.1 CHANNEL PLAN

As state above, the network supports quantum and conventional signals. However, the noise produced by the latter can impede any quantum communication (see Sec. 2.1). In consequence, we separate both type of signals in different bands of the spectrum in order to isolate the quantum signals. This technique has been already used in several publications [81, 130, 74, 65, 66].

We put the quantum signals in the O band (1260-1360 nm), and the conventional ones centered in the C band ($\approx$ 1500-1600 nm). By

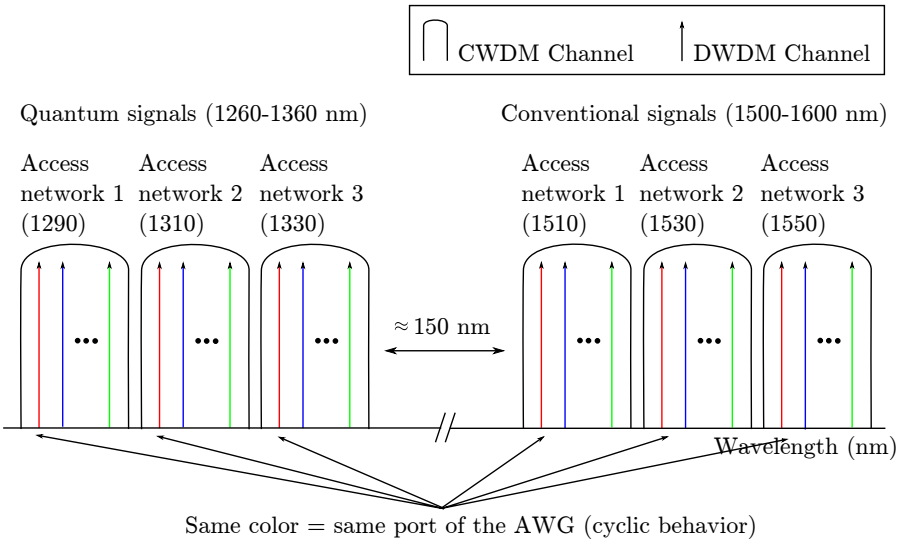


Figure 4.1: Proposed channel plan for the quantum metropolitan optical network. Quantum and conventional signals are separated in two spectrum bands to minimize the crosstalk. Each band is divided into subbands, which are assigned to the access networks. Within the subbands, DWDM channels carry the signals. Subbands are selected such that both quantum and conventional DWDM channels are periodic, and thus, they come out together through the same AWG port.

this, we assure that: (i) first-order FWM products do not reach the quantum signals[1] [68], (ii) Raman scattering has an almost negligible power [75, 74], and (iii) Rayleigh scattering and leaked signals in the WDM devices can be easily filtered. The only drawback is that fiber absorptions are higher in the O band (0.1 dB/km more), but the major contribution to losses in a metropolitan optical network comes from the network components (see Tab. 2.2), and these are similar in both bands. As an advantage, we can use commercial DWDM equipment for the conventional signals, while manufacturing quantum optical equipment at the O band does not create any problem.

Once all signals are allocated, we divide each band in CWDM channels and we assign one of each type to each access network. In the access network, these are demultiplexed into DWDM channels and assigned to the users by the AWG. The number of channels, i.e., users, depends on the grid used (200-12.5 GHz separation). In this way, each user gets a quantum and a conventional channel (by periodicity). Therefore, the selection of a certain pair of wavelengths by an emitter will automatically select a specific access network and, within that network, a specific QKD device. This is known as wavelength-addressing. Fig. 4.1 shows the schematic spectrum resulting from this approach.

1 First-order mixing products from signals within 1500-1600 nm will fall in the 1400-1700 nm range.

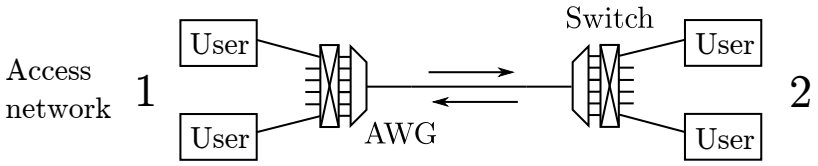


Figure 4.2: Simplified network of two WDM-PON access networks with switches. Using the channel plan described in Sec. 4.1, any pair of users, located in different access networks, can communicate using quantum and conventional signals.

4.2 NETWORK DESIGN

4.2.1 *Simplified network*

Using this WDM grid, we can directly build a metropolitan optical network of two access networks, as depicted in Fig. 4.2 where the backbone is a point-to-point fiber between the access networks. The network follows an any-to-any communication scheme: a QKD emitter can address any QKD receiver located at the other access network just by emitting at the DWDM channels assigned to the receiver (tunable single-photon sources [163]). Note that QKD emitters/receivers can be freely mixed in the access networks. Nevertheless, for this to work, both QKD devices must be connected to the same output port of their respective AWGs since ports are wavelength-selective in both directions. This could be an inconvenience in some scenarios. The solution is to add an optical switch in front of the AWGs, which would make the network dynamically reconfigurable.

4.2.2 *Backbone nodes*

We extend this network using OADMs at the backbone, as in conventional network (Sec. 2.4). This allows to increase the number of access networks. In our case, we need OADMs with a particular design: (i) able to add and drop simultaneously pairs of bands located in different parts of the spectrum, (ii) work for any subband and in the appropriate periodical sets, (iii) introducing the minimal amount of losses as possible, and (iv) without disrupting the quantum channel. Commercial equipment is not designed to do this, hence we devised a dedicated one (see Fig. 4.3).

In our model, all components are passive. Hence, all transmission paths are always available and fixed. The resulting network will be then less flexible and not resilient to link failures. However, passive components are also known to be more robust. The operation mode goes as follows:

- Drop: The signal enters the OADM through the input port and two CWDM filters drop the quantum and conventional CWDM

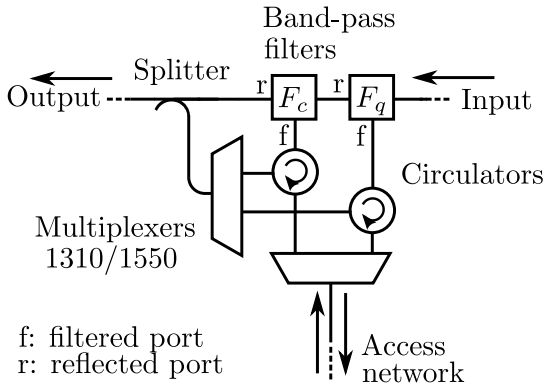


Figure 4.3: Design of a passive backbone node for the QKD-MON, built out of common network components. It works as an OADM: (i) drops the quantum and conventional subbands from the input signal to the access network; and (ii) adds any channel coming from the access network to the ring (output signal), no matter which sub-band it belongs to.

channels assigned to the access network. These channels are routed downstream using circulators and they are coupled using a 1310/1550 WDM multiplexer before they exit the OADM through the Add/Drop port and reach the AWG in the access network.

- Add: The signal enters the OADM through the Add/Drop port. A 1310/1550 WDM mux separates the signal into quantum and conventional band. Both are sent, using the same circulators, to another 1310/1550 WDM mux that joins them. Finally, they are added to the signals reflected by the band-pass filters using a 1×2 splitter and exit the OADM through the Output port.

Note that signals are injected into the ring no matter which CWDM channel they belong to. Otherwise, an access network could only communicate with itself. Equally important is that the scheme is non-blocking. This means that added signals do not block the pass through ones. If that would not be the case, an access network could receive signals from only one, and not all of them. Due to these requirements, the splitter is an essential component, despite its losses. These can be reduced by optimizing the splitting ratio depending on the number of OADMs that have to be crossed in a network design. In this way, we favor the signals traversing the ring, which are the ones with the largest losses, at the expense of increasing the losses in the shorter paths (between neighboring access networks). For instance, for 3-4 backbone nodes, using a splitting ratio of 70:30 reduces the losses about 2 dB in a path crossing the full network.

Now, we can build a backbone ring where multiple access networks are attached to OADMs. Based on the operation mode described, it can be seen that CWDM channels are routed properly to the access

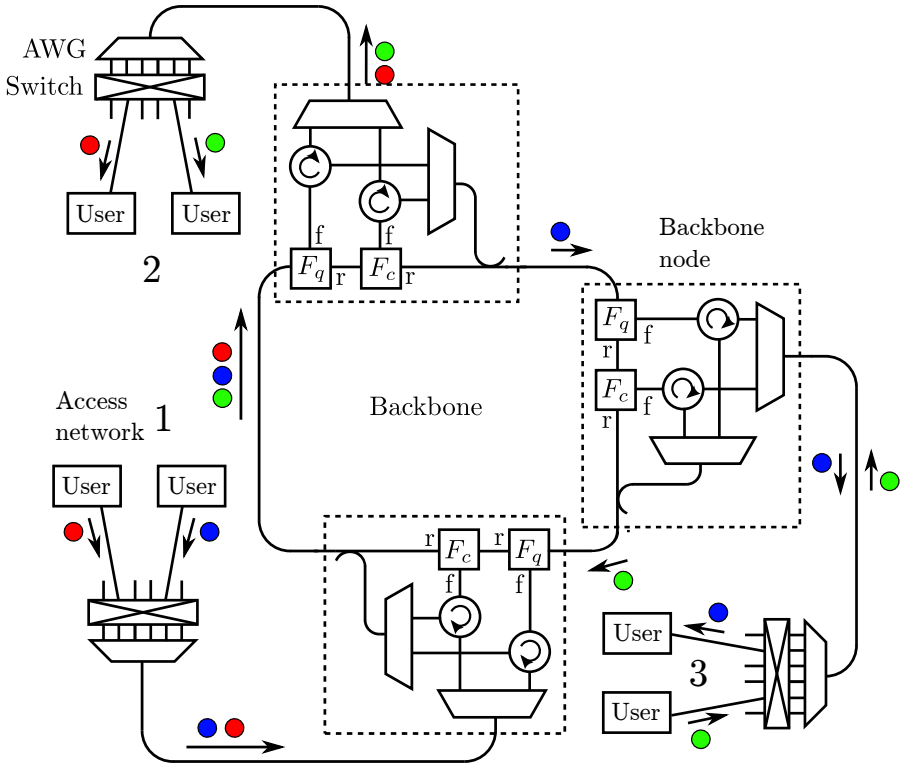


Figure 4.4: Quantum metropolitan optical network with 3 access networks. The design uses CWDM at the backbone and DWDM at the access networks to arrange both quantum and conventional signals in an any-to-any fashion. A possible communication snapshot is shown using colored circles. Each circle represents a pair of quantum and conventional signal.

networks. On the other hand, note that OADMs give directionality to the backbone network. Hence, the backbone must be a closed ring in order to guarantee communications among all access networks.

4.2.3 *Full network*

Fig. 4.4 shows a full quantum metropolitan optical network using the OADMs and the WDM grid. Like in the simplified design, this design is an any-to-any, wavelength-addressed network where QKD devices are freely mixed. Moreover, it can be made dynamically reconfigurable using switches at the AWGs. Colored dots are used to illustrate simultaneous communications between the users. Each dot represents a pair of periodic quantum and conventional DWDM channels.

Note that there is no short path for two QKD systems in the same access network as a result of removing the OLTs in order to simplify the network. All upstream signals go directly to the backbone. There are simple local solutions to this problem, e.g., using a larger switch to create return paths (see Sec. 3.2).

Table 4.1: Calculated and measured losses for the main network modules of the QKD-MON (according to Tab. 2.2).

	Quantum		Conventional	
Network component	Calc. losses	Meas. losses	Calc. losses	Meas. losses
32-ch AWG	3 dB	2.34 dB	3 dB	2.45 dB
Switch	1 dB		1 dB	
OADM (add)	5.4 dB	5.98 dB	5.4 dB	4.91 dB
OADM (pass)	4.8 dB	5.7 dB	4.8 dB	5.8 dB
OADM (drop)	1.7 dB	1.83 dB	2.3 dB	2.24 dB
10-km path and 2 OADMs	18.1 dB		17.5 dB	
15-km path and 3 OADMs	24.7 dB	23.15 dB	23.2 dB	20.64 dB
20-km path and 4 OADMs	31.1 dB		28.9 dB	
30-km path and 5 OADMs	39.1 dB		35.5 dB	

The losses of the network, shown in Tab. 4.1, are calculated using the theoretical values of the components. For mere illustrative purposes, we show examples of full optical paths for scenarios with a different number of OADMs (i.e. access networks) and total fiber length. For instance, a loss budget of approx. 30 dB [25, 2, 24], allows a quantum network with 3-4 OADMs and a span of 15-20 km. Although there are QKD systems with a loss budget over 40 dB [20, 32, 21], at present they are not practical since they are based on superconducting detectors that need cryogenic temperatures to work. Note that the proposed network scheme remains valid even if QKD technology improves: a higher loss budget means more backbone nodes, larger AWGs and a longer reach.

An important characteristic of the proposed metro architecture is its scalability. This is shown, for instance, when an access network, with its corresponding backbone node, is added or deleted. Neither of them imposes a modification of the resulting network (unless the WDM grid is rearranged). For instance, let consider that we connect a fourth access network to the network shown in Fig. 4.4 using remaining some free CWDM channels. Without any additional procedure, the new users can communicate with the old ones by emitting at their channels, and vice versa. The same applies if a user is connected or disconnected from an existing access network. Its channels are considered in the WDM grid, and disconnect them only means that the channels will be unused. The routing is inherent to the network architecture.

Regarding the maximum number of users that the network can serve, it depends on the width of the spectrum bands, the loss budget and the DWDM channel spacing. If CWDM channels are used for the access networks (passband of $\approx$ 13 nm) and the 100 GHz ITU DWDM grid for

Table 4.2: Assignation of CWDM channels to the access networks.

Access network	Quantum CWDM channel	Conventional CWDM channel
1	1290	1570
2	1310	1550
3	1330	1530

the user channels, the network has a theoretical limit of $4 \cdot \lfloor 13/0.8 \rfloor = 64$ users. The first term comes from the maximum number of CWDM channels per band, which is limited by the losses in the O band and by the need of having the quantum and conventional signals well separated. The second term is the passband of the CWDM channel over the DWDM channel spacing in nanometers. Considering that this value increases for shorter wavelengths (due to the relationship frequency-wavelength), we use the C band as reference (0.8 nm). The maximum number of users can be increased by choosing a smaller DWDM grid. But, in practice, the limit is set by the mismatches between network components (e.g. CWDM channels and AWG cycles) and the noise from the conventional signals.

4.3 TESTBED

The QKD-MON depicted in Fig. 4.4 has been implemented using the components detailed in Tab. 2.2. The test bed network is a full-featured quantum metropolitan optical network with a span of 16 km, including three access networks (labeled from 1 to 3), with static paths. The path used for testing is depicted overlaid on the network scheme in Fig. 4.5. It crosses all network components in order to connect access networks 1 and 3. For that reason, it corresponds to the worst case scenario in terms of losses and generated noise.

The bands and subbands are defined primarily by the components used, especially at the OADMs, and their passband. In particular, we use CWDM channels in the backbone for routing subbands (see Tab. 4.2), and 100 GHz DWDM 32-channels in the access network.

The test bed has been firstly characterized by measuring the losses. For this purpose, we use lasers emitting at the access network 1 in order to simulate quantum and service signals communicating with the access network 3. We use then an OSA to measure the peak power of both signals at different points of the network, including the received signals at the end. The results, given in Tab. 4.1, are consistent with the calculated values. This last measurement also proves the operation mode of the network.

Next, we want to find the maximum input power for the conventional channels that does not disrupt the quantum transmissions. The critical power is reached when the noise produced by the conventional

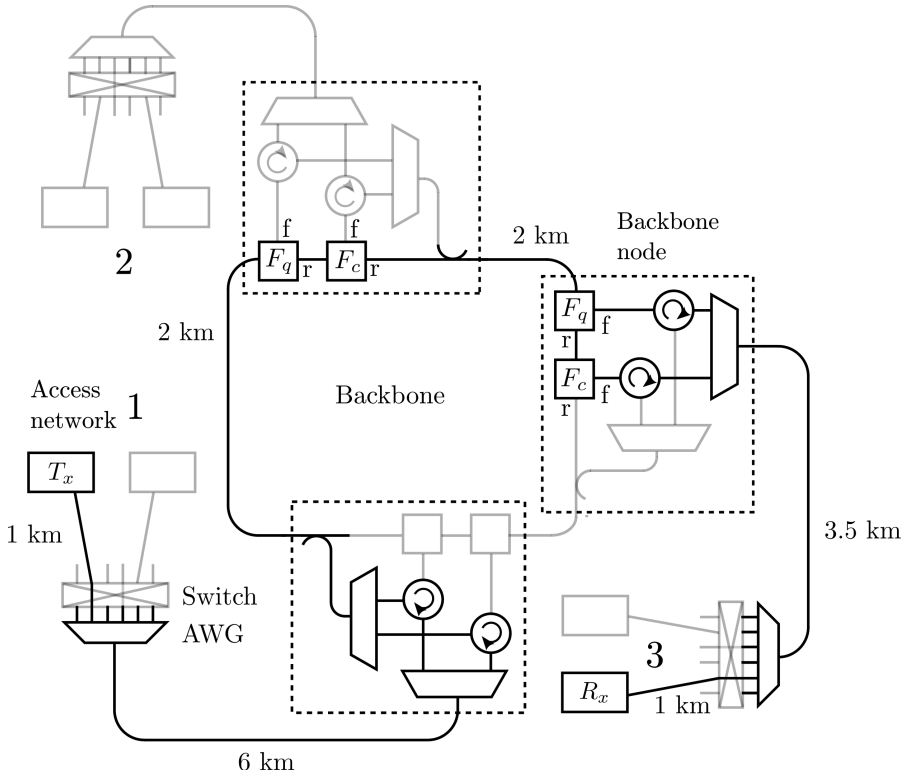


Figure 4.5: QKD-MON test bed with three OADMs based on the design in Fig. 4.4. The total length of the fiber is approx. 16 km. A longer fiber than usual is used in the access network 1 to generate a higher amount of Raman scattering. Overlaid in black is the worst case path with respect to losses and generated noise.

signals in a quantum channel, together with the intrinsic noise of the SPD, yield a QBER above the threshold of the QKD system (11% if we assume a BB84 with one-way communications). Using again the worst-case path, we have performed several measurements of the forward and backward noise.

For the forward noise, measurements are carried out at the smallest wavelength separation between quantum and conventional channels, which is approx. 180 nm (1340 to 1520 nm). This should produce the highest noise possible. As a comparison with the schemes where all signals are placed in the same spectral region, the forward noise at 1530 nm is measured as well. In both setups, the SPD [48] is connected to a WDM multiplexer that is connected at the access network 3. The purpose of the WDM multiplexer is to separate the quantum and conventional bands. At the access network 1, we connect the laser to an erbium doped fiber amplifier in order to try relatively high power configurations (from -30 to $+2$ dBm). Finally, we measure the backward noise by moving the SPD and WDM multiplexer to the access network 1.

The measured noise as a function of the overall power of the conventional channels is presented in Fig. 4.6. In all cases, the result is normalized to 1 ns gates (note that the intrinsic noise of the SPD has been subtracted). The figure also depicts the dark count rate of the SPD [2] and the expected detection rate of the quantum signal. The probability of detecting an emitted single photon is calculated as $1 - e^{-\mu\tau\eta}$, where μ is the mean photon number, τ is the transmittance and η is the quantum efficiency of the SPD. Using these 3 values, we estimate the QBER of several representative points of the experiment as the ratio of erroneous detections over the total number of detections.

As expected, the forward noise in the conventional channel is higher. This is not relevant for our network design, but it highlights the importance of separating quantum and conventional channels in the spectrum. In our testbed, the backward noise is the limiting factor due to the high attenuation suffered by forward-scattered photons, whereas backward-scattered photons reach a saturation peak (see Sec. 2.2.3). In this test bed, it is seen that, even with approx. $+2$ dBm power for all conventional channels, the QBER estimation is below the threshold, consequently a QKD system [2] can exchange key. This overall power would allow for more than 32 simultaneous conventional channels of -13 dBm. For example, in this case, the QBER would increase from 4.37% with no conventional channel to 5.1% with only one and to approx. 5.74% with all 32 channels being used at the same time. Furthermore, with -13 dBm, even in the worst case path, the receiving power would be -34 dBm. This is strong enough to achieve a data modulation rate of 1.25 Gbps with a bit error rate no higher than 10^{-9} [71]. A data rate of 1.25 Gbps is obviously wasted if it is used just for service signals which typically have a small duty cycle. It would

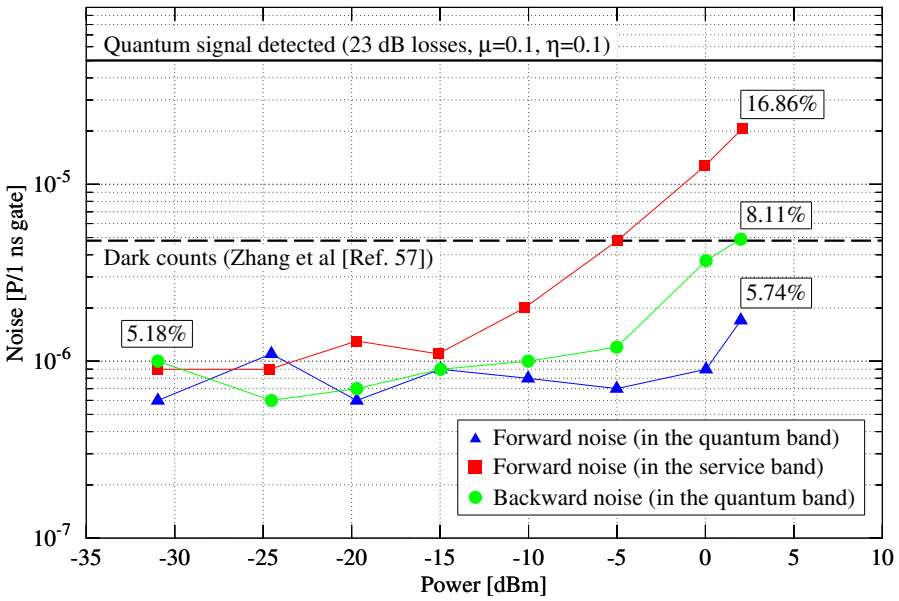


Figure 4.6: Measured noise per 1 ns gate in the testbed depicted in Fig. 4.5. A laser centered at 1520 nm is fed at the access network 1 and three measurements are done: forward node at a quantum channel (1340 nm, triangles), backward noise at a quantum channel (circles), and forward noise at a conventional channel (1530 nm, squares). To facilitate its interpretation, the expected quantum signal detection rate and the dark count rate of an SPD [2] are also presented. Using these data, a rough estimation of the QBER is shown for multiple points.

be highly desirable to go beyond and use the rest of the time for key distillation and/or ciphering.

Modes of network operation

To distill a key, a bidirectional conventional communication is required between receiver and emitter. However, the backbone ring is directional: a signal originated in the receiver cannot propagate back to the emitter using the same channel and path. The receiver has to use the service channel assigned to the emitter. These *return channels* are already considered in the channel plan. By design, every device in the network has a pair of channels assigned. Nevertheless, return channels require a different switch configuration and, thus, they cannot be used simultaneously with the corresponding service channel. This is because, in general, emitter and receiver are connected to different ports of their respective AWGs. Due to the number of signals that need to be generated to produce enough key material to get rid of finite key effects [124], the switching time is not a problem.

In case a simultaneous return channel is necessary, this can be easily taken into account. For instance, in a static version of the network, QKD systems can be arranged in a way that pairs are connected to same port of their AWG. If a dynamic addressable network is needed, then the simplest solution is to use different ports of the AWG for each direction. This means that a QKD device will be connected to the switch using two short fibers. This might not be the most economical use of the fiber, but it is not a technical problem given the short distance between AWG and QKD, and the presence of spare fibers in most installations.

4.4 INTEGRATION OF QKD SYSTEMS

One-way discrete-variable QKD systems, based on weak coherent pulses or entanglement, can be used directly in this network. One example is the coherent-one way (COW) protocol. The most recent implementation of a COW system [33] uses a quantum channel together with two conventional channels (one in each direction) that carry the service signals and the distillation protocol communication via TDM (in Sec. 4.3. This advanced approach to the service channel is discussed in Sec. 4.3. Time multiplexing a wavelength in the presented network does not pose any problem and the scheme works flawlessly without modifications. In addition, the COW system can tolerate delays between quantum and conventional signals, such as those originating from the small differences in path lengths that can occur in our OADM node, or due to chromatic dispersion. The only requirements to adapt a COW system are: (i) move the quantum channel to the O band, this

is feasible by adapting the Faraday mirror and the intensity modulator; and (ii) if addressability is required, use a tunable laser.

Continuous-variable QKD systems are a different topic, though. They are based on coherent detection using a strong signal as a reference, which uses the same wavelength as the quantum signal. If we put it on the quantum band, the reference signal would hinder the neighboring quantum channels. If we put it on the conventional band, the neighboring channels would impair the quantum channel. Between both options, the last is the best one because most noise does not phase-match with the quantum signal. The coherent detection works as a very narrow bandpass filter [72].

Two-way QKD systems cannot be used since they use the same channel in both directions and our network is wavelength-addressed. You cannot address emitter and receiver using the same wavelength. Even if a wavelength converter is used at the receiver, they would need to change the switch configuration (unless the second wavelength belongs to the same periodic set). For this to work, the pool of fiber in the receiver should be long enough to delay the signal and give time to reconfigure the switch.

The case of entanglement-based QKD system with the source located in the middle is discussed in detail in the next chapter (Chap. 5). This topic is radically different since our network design connects final users with final users, in a one-to-one fashion. The actual design does not allow communications following a one-to-many scheme (source-users), or with the emitter located in other place than the access network.

4.5 CONCLUSIONS

We have presented a quantum metropolitan optical network that is designed to share the deployed infrastructure and uses commercial components. This would potentially allow for a cheap, easy and reliable deployment, thus making QKD a more cost-competitive technology.

The scheme is based on WDM and wavelength-addressing. Each user has available a dedicated quantum and conventional channel, and any other user can communicate with him by emitting at those channels. The scheme of communications is thus any-to-any. In addition, it can be made dynamic using switches. The architecture is a conventional one in metropolitan optical networks, comprising backbone and access networks. However, in our case, both subnetworks form a single network to provide direct optical paths between users.

The measurements performed on a testbed demonstrate that quantum signals can be successfully transmitted simultaneously with at least 32 conventional signals, each one supporting a traffic of up to 1.25 Gbps. This traffic could include key distillation communication or even cipher text transmission. This assumes 1 ns detector gates: more

channels would be possible if last generation, sub-ns gated detectors are used (e.g. 100 ps [2]). The scheme is finally limited by the specifications of the network components and the loss budget of actual QKD systems ($\approx$ 20-30 dB). Nevertheless, as discussed above, typical commercial components already allows for a network with a span of 20 km and 64 users distributed among 4 access networks.

Although originally thought for one-way discrete variables systems, we have also discussed the integration of other technologies, e.g. continuous variables, entangled photon-pairs, in an attempt to make the network universal for any type of quantum communication system.

5

DISTRIBUTION OF ENTANGLED PHOTON-PAIRS IN A QUANTUM METROPOLITAN OPTICAL NETWORK

The network presented in Chap. 4 is a solid framework for QKD and further quantum information technologies. In an attempt to cover the distribution of all the basic resources, we will study the distribution of entangled photon-pairs in networks. Entanglement is a fundamental characteristic of quantum mechanics that is used by many quantum information protocols besides quantum key distribution, like superdense coding [164] or quantum teleportation [165].

First, we describe the entangled photon-pairs source considered here. Then, we show how to use a source to distribute entanglement over an entire metropolitan optical network. Later, we will focus on the network design of Chap. 4 and on how the sources can be distributed over the users and integrated in the existing channel plan. Finally, we will modify the network design to include the sources.

5.1 BROADBAND SOURCE OF ENTANGLED PHOTON-PAIRS

Fig. 5.1 shows the scheme and output of a broadband source of entangled photon-pairs based on the spontaneous parametric down-conversion process (SPDC). A continuous wave (CW) laser diode at λ_p pumps the periodically-poled lithium niobate (PPLN) waveguides to obtain a broadband signal with central frequency λ_c. Photons of both halves are entangled with each other symmetrically respect to λ_c. The width of the spectrum depends on the dimensions of the crystal waveguides. Later, a DWDM demultiplexer divides the signal into channels. As a result, DWDM channels are entangled symmetrically: selecting one channel directly fixes the second one that has to be used. Note that we cannot choose which channels have to be produced. We need to use network components at the output (e.g., switch) to control which pairs are distributed.

This broadband behavior makes them especially suitable for their use in DWDM-based networks, such as WDM-PON, since a single source can serve many users.

In particular, we consider a source [119] with the following characteristics: (i) $\lambda_p = 775 \pm 5$ nm, (ii) bandwidth of 70 nm, and (iii) λ_c at the C band (can be slightly tuned by modifying the temperature of the waveguides or λ_p). In terms of output power, the source generates 4.5×10^5 pairs/s/mW/GHz. Note that the generation rate is given by GHz, thus a denser DWDM grid would increase the number of

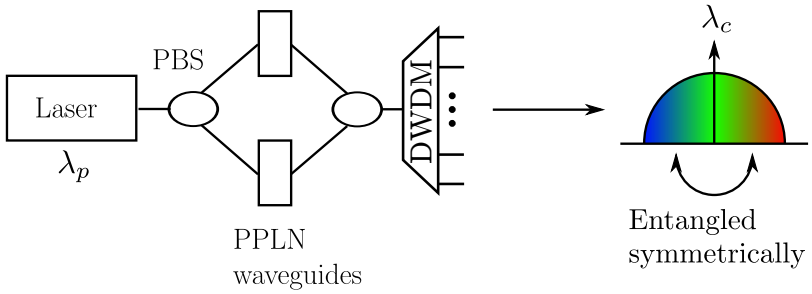


Figure 5.1: Scheme and output of a broadband source of entangled photon-pairs. A laser pumps the ppLN waveguides. Photon pairs are generated over a broad spectrum via SPDC, and divided into DWDM channels using a demultiplexer. Hence, DWDM channels are entangled symmetrically. PBS stands for polarizing beam splitter.

channels at the cost of having a lower count rate at each one. However, we can produce more pairs by increasing the pumping power.

Based on this same scheme, sources using shorter ppLN waveguides (approx. $2-3$ mm) could successfully generate entangled-photon pairs over a bandwidth of 200 nm, enough to cover entire spectrum bands. This can also be done using novel ring structures integrated in silicon-on-insulator (SOI) substrates.

5.2 ENTANGLEMENT-ONLY METROPOLITAN OPTICAL NETWORKS

Before going into detail about the integration of such sources in the network proposed in Chap. 4, we will start proposing designs for entanglement-only metropolitan optical networks: no one-way quantum channels or conventional ones. Despite their simplicity, they are already an advance over the state of the art of entanglement-only networks [117, 166, 118, 119]. Furthermore, they illustrate the operation mode of the sources and their integration in WDM-based networks.

5.2.1 *A single access network*

Using a source as described in the previous section, the first step is to directly connect users at the outputs of a DWDM multiplexer. As Fig 5.2 shows, the result is a point-to-multipoint network that is equivalent to a WDM-PON access network. The switch is required to connect all possible user pairings, and thus build an any-to-any network, i.e., a network in which any user can share entanglement with any other one.

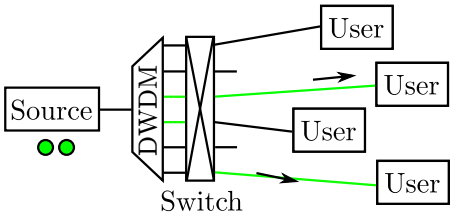


Figure 5.2: Broadband entanglement-source directly connected to users. It is equivalent to a WDM-PON access network. The switch is necessary to do all possible user pairings.

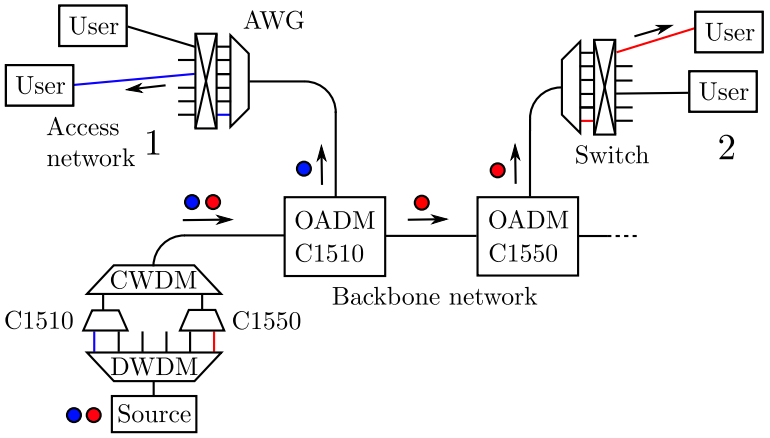


Figure 5.3: Broadband entanglement-source serving two access networks. The output of the source is demultiplexed in DWDM channels and grouped in CWDM channels 1510 and 1550. Each CWDM channel is dropped in a different access network by an OADM (or just a simple bandpass filter).

5.2.2 *Two access networks*

Let us assume now that all DWDM channels from a WDM-PON are contiguous and can be grouped into a single CWDM channel. Therefore, since the spectrum of the source is wider than a CWDM channel, we can distributed entangled photon-pairs among DWDM channels of two different CWDM channels, i.e., between users from two different access networks. For instance, we can add another WDM-PON next to the previous one and connect both using a ring-shaped backbone. Then, we only need a OADM node able to drop each CWDM channel at each access network. The resulting network is shown in Fig. 5.3, where a source distributes entanglement between CWDM channels 1510 and 1550 (blue and red in the figure, respectively). Depending on the particular CWDM channels used, the source configuration will change accordingly by choosing the appropriate multiplexers to group the DWDM channels used.

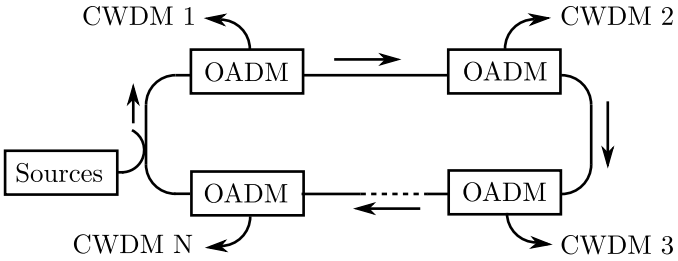


Figure 5.4: Scheme of a entanglement-only metropolitan optical network with N access networks and ring-shaped passive backbone. Each access networks has assigned a CWDM channel. Sources, added to the backbone traffic, distribute entanglement over all single CWDM channels and possible pairs.

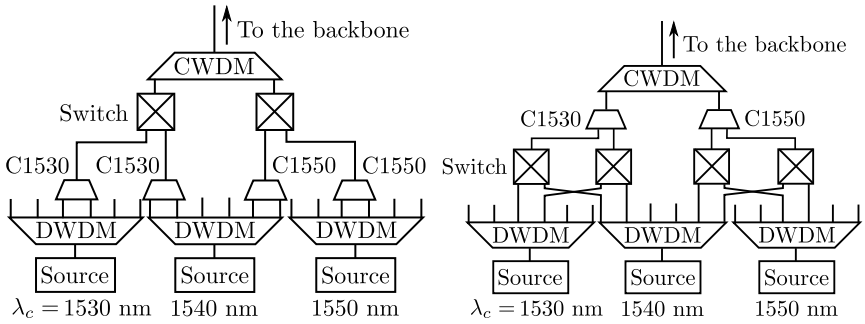
5.2.3 *Metropolitan optical network*

Using these two subnetworks as basic blocks, we can build a entanglement-only metropolitan optical network with N access networks (see Fig. 5.4). For example, given $N = 3$, we need to communicate 3 single access networks as in Fig. 5.2, and $\binom{3}{2} = 3$ pairs of access networks as in Fig. 5.3. Therefore, it requires a maximum of 6 sources: 3 of them to distribute entanglement over each access network, and another 3 to distribute it between the possible 3 pairings of access networks. In this way, any user can share entanglement with any other one. Although the number of sources increases considerably with N, the number of access networks is severely limited by the loss budget and the available spectrum. Moreover, the actual number of sources can be smaller since some of those combinations can be provided by a single source. For instance, a source that distributes entanglement over CWDM channels 1530 and 1570, can distribute it at the same time over the single 1550. Regarding the physical allocation of the sources, all of them are grouped as a single source and connected to the backbone.

Subsequently, a CWDM channel is assigned to each access network and backbone nodes route these channels among different access networks. Finally, once within the access network, the AWG demultiplex the CWDM channel into DWDM channels and a switch route them to the appropriate user. Therefore, a DWDM channel is assigned to each AWG port in the access network thanks to AWG's periodicity[1]. Note that, when emitting using a particular wavelength, the emitter is actually selecting the target/final access network and the AWG port.

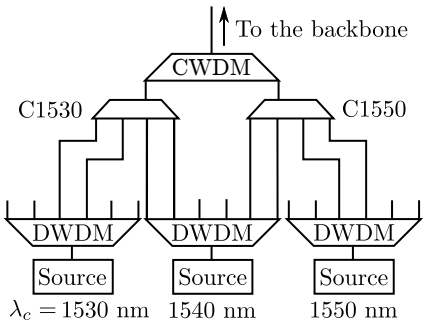
However, in this network, multiple sources would try to reach the same access network and thus to use the same CWDM channel. This is because we want to provide an access network distributing entanglement among its own users and also with the rest of $N - 1$

1 To simplify matters, we assume that a CWDM channel equals an AWG's spectrum band. However, this may not be the case and then some DWDM channels will be unusable.



(a) Connection scheme 1.

(b) Connection scheme 2.



(c) Connection scheme 3.

Figure 5.5: Possible connection schemes for the entanglement sources in an entanglement-only metropolitan optical network with 2 access networks. In (a), switches are used to decide which source uses each CWDM channel. In (b), switches decide which source uses each DWDM channel; hence, a CWDM channel is used by multiple sources at the same time. In (c), CWDM channels are also shared among all sources but in a fixed way; a source has assigned always the same DWDM channels.

access networks. Hence, we need to carefully connect the sources when grouping them. We propose three solutions (see Fig. 5.5). In the first scheme, sources will use the full CWDM channel and a switch will decide which source uses that CWDM channel at each moment. In the second scheme, switches are moved near the source in order to decide which source uses each DWDM channel of each CWDM channel. Therefore, a CWDM channel is used by multiple sources at the same time. However, this flexibility comes at the cost of using a larger number of switches. In the third scheme, we remove all switches. Instead, we simply distribute the available DWDM channels among the sources. Hence, each source always uses the same DWDM channels.

Now, we calculate the maximum number of users that this network can support. We will consider 100 GHz DWDM ITU grid, 32-channels AWG, and the following fiber distances: 1 km between users and the AWG, 3.5 km between the AWG and a backbone node, and 4 km between neighboring backbone nodes. Insertion losses of common

network components are shown in Tab. 2.2. First, the maximum number of access networks N is established by the insertion losses. Note that, when using entangled photon-pairs, the losses are the sum of the two paths. Therefore, the worst path in terms of losses in our network is the sum of the two worst paths: from the source to access network $N-1$, and from the source to N. With a 30 dB loss budget, we calculate $N = 8$: (i) 15.3 dB from the source to a user in the N access network, (ii) 14 dB from the source to a user in the $N-1$ access network, and (iii) $14 + 15.3 = 29.3$ dB. As a result of the fixed mapping of CWDM channels, this is a maximum of 8 CWDM channels. Nevertheless, to reach this upper bound, we need a source able to produce entangled photon-pairs between CWDM 1 and CWDM 8, this is, approx. 160 nm. Hence, depending on the spectrum width of the sources used, the actual number of access networks can be smaller. Finally, we can estimate then the number of users by multiplying N by the number of DWDM channels per CWDM channel (passband of approx. 13 nm), e.g. $8 \cdot \lfloor 13/0.8 \rfloor = 128$ users with a 100 GHz DWDM ITU grid. A higher loss budget would increase the maximum number of users by allowing more backbone nodes and more users per access network (AWGs with denser DWDM grids).

5.3 CHANNEL PLAN

Up to now, the network has been designed to distributes only entangled photon pairs. Now we will discuss how to incorporate direct communications, quantum and conventional, between users. We are going to merge this entanglement-only network with the one described in the previous chapter. Adding other types of quantum signals will allow to use a higher variety of quantum information technologies, whereas conventional signals are essential to perform any conventional communication, either required by the quantum information protocols themselves or by external applications.

For this, let us start by adding the conventional signals to the network. As in Chap. 4, we will use two spectrum bands separated by approximately 150 nm: the O band (1260-1360 nm), and the C band and surroundings (1500-1600 nm). This separation reduces the crosstalk from conventional to quantum signals and thus increases the number of simultaneous signals that can be transmitted in the network. The size of each band is delimited by their separation and the operating wavelength range of the network components (see Tab. 2.2).

Based on the source's characteristics, we assign the O band to the conventional signals and the C band, and surroundings, to the quantum ones. Each band is then divided into CWDM channels and a pair of them, one in the C band and the other in the corresponding AWG period in the O band, is assigned to each access network. The operation mode of the backbone nodes and the AWG at the access network

remains the same. Therefore, now each AWG port has assigned two DWDM channels: one containing single photons that are entangled with other DWDM channel in the C band, and another one, in the O band, containing conventional optical pulses. Note that both should be separated at the receiver using a filter.

For the connection of the sources, we use the scheme depicted in Fig. 5.5c. Since DWDM channels are assigned and fixed to each source, each source is independent of the rest. As long as DWDM channels are distributed over them correctly (e.g., a DWDM channel is not assigned to more than one source), sources can be separated and connected at different points of the backbone network. In addition, by assigning and fixing a dedicated source to a subset of CWDM channels, we avoid wavelength-tuning the source on-the-fly, a complex task that would affect all users receiving from the source.

At this point, CWDM channels are shared among all sources, without leaving place for one-way quantum signals. We could use a third spectrum band for one-way quantum signals. However, we are already occupying both low-attenuation telecommunication windows, and to use a third CWDM channel per access network would also increase the losses at the backbone node (more components would be needed for the OADM). Therefore, we propose to share the quantum band between one-way single photon pulses and entangled pairs. For this, among the DWDM channels assigned to each source, only a set of them will actually be connected to the source. The rest are left free for one-way quantum signals[2]. Furthermore, this set of channels is fixed. Instead of reconfiguring the source, we use the switch at the access network to connect the user to the corresponding AWG port.

The resulting channel plan is shown in Fig. 5.6. The figure shows the arrangement of bands, CWDM and DWDM channels. Colored arrows indicate DWDM channels used by entanglement sources (S_x), where the color points out the CWDM channel. In this case, using 6 sources we can distribute entanglement to any pair of users of the network, within the same access or in separate ones. The rest of DWDM channels (in black) are available for one-way signals. Users can connect to each type configuring the switches at the access networks.

A substantial advantage of our design is its scalability when facing a demand increase of entangled channels. We can gradually provide more channels by just connecting the outputs of the source to the DWDM multiplexer. However, this will decrease the available channels for one-way quantum communications.

2 Vice versa, one-way systems must not emit quantum signals at the DWDM channels dedicated to entanglement distribution.

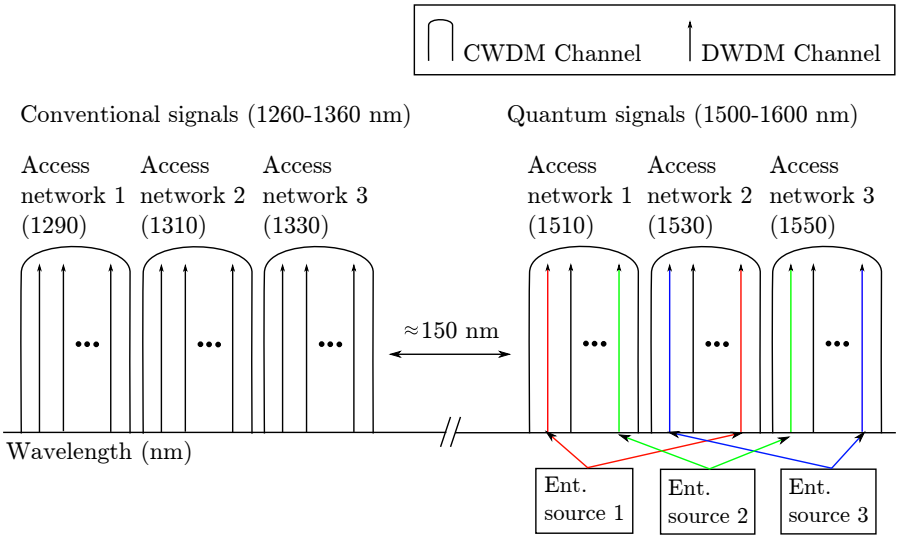


Figure 5.6: Channel plan for a quantum metropolitan optical network. Each access network has assigned two CWDM channels, for quantum and conventional signals. They are spectrally separated to avoid any crosstalk. Within the CWDM channel, DWDM channels are used for one-way communications or entanglement distribution. The figure shows how entanglement sources (S_x) are arranged in order to ensure entanglement among any pair of users in the network.

5.4 UPGRADING THE BACKBONE NODE

For our scheme to work, we need to add the source's signal to the backbone traffic. Backbone nodes are then responsible of routing them. We show a solution in Fig. 5.7. The new backbone node is an upgrade of the old OADM (see Chap. 4) but adding the source (S in the figure) via splitter. This allows for an easy and cheap deployment while maintaining the compatibility with the previous design. Only the *add* operation changes:

- Drop: Not modified.
- Add: The signal enters the OADM through the Add/Drop port and it is separated into quantum and conventional bands by a 1310/1550 WDM mux. Both bands are sent using two circulators to another 1310/1550 WDM mux that joins them. At this point, a splitter combines these signals from the access network with the signal output by the entanglement source. Finally, both are added to the signals reflected by the band-pass filters using a 1×2 splitter and they exit the OADM through the Output port. The signal output by the OADM has now three origins: backbone, access network, entanglement source.
- Pass through: Not modified.

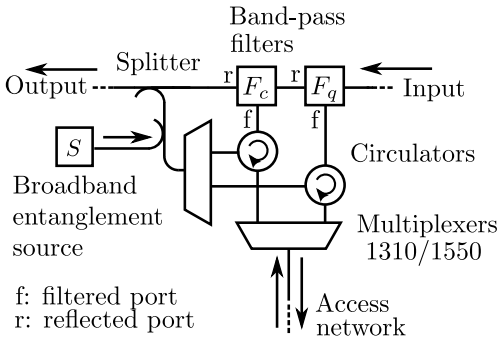


Figure 5.7: Possible design of a passive backbone node for a ring-shaped backbone that includes a broadband source of entangled photon-pairs. The design is an upgrade of the previous one (Fig. 4.3) with the addition of the source S and a second splitter.

Table 5.1: Losses of the passive backbone node with entanglement-capability depicted in Fig. 5.7.

Action	Losses Conv.	Losses Quantum	Losses Ent.
Add	$5.4 + 0.8$ dB	$5.4 + 0.8$ dB	3.6 dB
Pass	4.8 dB	4.8 dB	4.8 dB
Drop	2.3 dB	1.7 dB	1.7 dB

The new component increases the losses of the OADM (see Tab. 5.1). Nevertheless, we put the splitter from the source in the *add path* to minimize its effect: pass trough and drop signals are not affected. In a communication, a signal will only suffer one time these extra losses, no matter how far is the destination. However, this also means that there is no short-path for the immediate access network. Entangled signals always go farther away to other access network. Likewise, we use an unbalanced splitter to not hinder the signals coming from the access network (only +0.8 dB for a 90:10 splitter). Meanwhile, the increment of losses at the source can be counteracted by increasing the pumping power.

5.5 NETWORK DESIGN

5.5.1 *Access network*

The current configuration of the access network routes all upstream signals to the backbone network. If two users from the same access network want to communicate directly, their signals will cross the entire backbone before reaching the receiver. This inefficient operation mode can be solved by creating a shortcut within the access network. We will use the technique already proposed in Sec. 3.2: use a larger switch than needed and use the extra ports to create loops in the

network's side of the switch, i.e., *return paths*. Therefore, two users can connect to the user's side of the switch and use the loop to communicate directly. This is a simple, cost-free and local solution that does not introduce extra losses or modify the channel plan.

5.5.2 *Metropolitan optical network*

We build a quantum metropolitan optical network using the new backbone nodes. The network, depicted in Fig. 5.8, has three access networks (A_x) and a backbone ring. The conventional and quantum CWDM channels assigned to each access networks are: (C1290, C1510) for A_1, (C1310, C1530) for A_2, and (C1330, C1550) for A_3. The entanglement sources (S_x) are configured as in Fig. 5.6:

- S_1 serves A_1 (C1510) and A_2 (C1530) with $\lambda_c = 1520$ nm
- S_2 serves only A_1 (C1510) with $\lambda_c = 1510$ nm
- S_3 serves A_1 (C1510) and A_3 (1550) with $\lambda_c = 1530$ nm
- S_4 serves only A_2 (C1530) with $\lambda_c = 1530$ nm
- S_5 serves only A_3 (C1550) with $\lambda_c = 1550$ nm
- S_6 serves A_2 (C1530) and A_3 (C1550) with $\lambda_c = 1540$ nm.

This arrangement is represented in the figure using colored circles located near each source. They represent the entangled photon-pairs generated by the source. The color indicates the CWDM channel of the photon (i.e., the destination): blue for C1510, green for C1530, and red for C1550. Note that the sources are deployed in a way that they always distribute photon-pairs among the next and second next access networks in order to use the shortest paths.

We calculate the path losses in Table 5.2 using the same considerations as in the entanglement-only network and the values from Table 5.1. We use the notation x-closest to denote proximity: 0-closest would be the same access network, 1-closest the immediate next in the backbone direction, 2-closest the immediate next after the 1-closest, etc. As shown, with a loss budget of 30 dB, our network design allows one-way quantum communications between non-neighboring access networks, e.g., from A_1 to A_3. For entangled communications, the longest path is between a neighboring access network and the next one, e.g., from S_2 to A_1 and A_2. The result is slightly worse in this case because the source always communicates with farther access networks. In the case of one-way, the source is already in one of the ends.

We estimate the maximum number of users[3] following the same procedure as before. The first limitation comes from the losses. With

3 Here we refer to the maximum number of users that could in principle communicate simultaneously. In practice, this is limited by the noise produced by conventional signals.

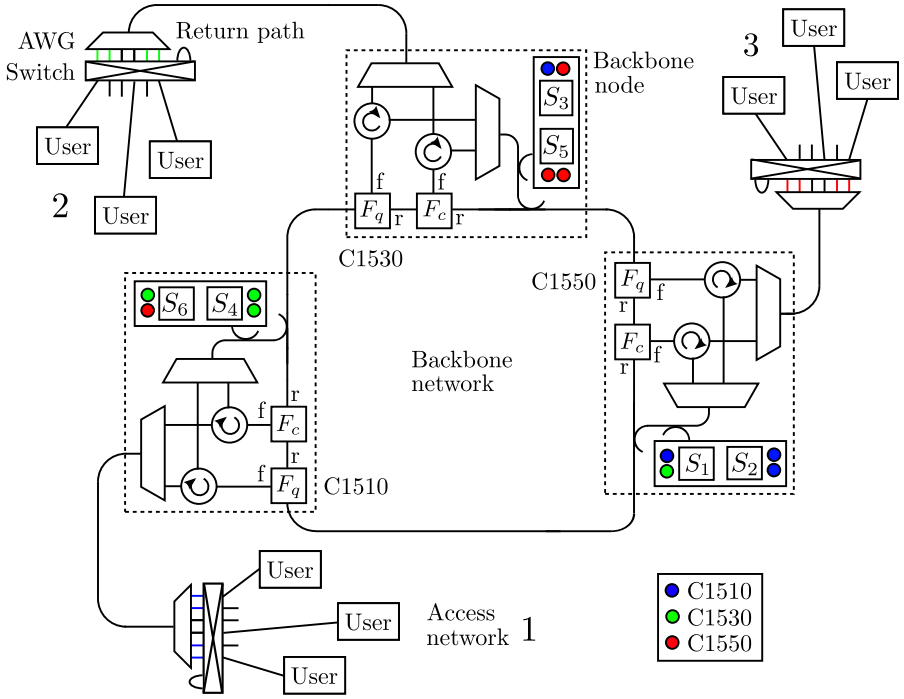


Figure 5.8: Quantum metropolitan optical network based on the design shown in Chap. 4. Besides allowing one-way communications, quantum and conventional, the network is also capable of distributing entangled-photon pairs among any pair of users of the network.

Table 5.2: Path losses from an emitter (user or source) in a QKD-MON with a fixed-ring backbone (Fig. 5.8). Values calculated using Tab. 2.2 and Tab. 5.1.

Path to	Losses Conv.	Losses Quant.	Losses Ent.
1-closest access network	19.1 dB	18.5 dB	11 dB
2-closest access network	24.7 dB	24.1 dB	16.6 dB
3-closest access network	30.3 dB	29.7 dB	22.2 dB

a loss budget of 30 dB, the network design is limited to 3 access networks (approx., 48 users). Adding a fourth access network would inevitably require a source to distribute pairs among non-neighboring access networks (e.g., A_2 and A_4) and to have one-way quantum communications between 3-closest access networks. Beyond the losses, we face again the spectrum width of the source and then the number of CWDM channels available.

5.6 CONCLUSIONS

In this chapter, we have proposed feasible schemes for the distribution of entangled photon pairs in metropolitan optical networks. First, we have shown how to construct entanglement-only metropolitan optical networks. Later, we have integrated the sources in a quantum metropolitan optical network with one-way quantum signals and conventional ones. This is especially helpful if we want to embrace as many as possible quantum information technologies in order to share the costs of the infrastructure.

For this purpose, we have detailed the number of sources needed, how to distribute them over the access networks and their integration within the channel plan. Finally, we have proposed how to include them in the previous network design based on a backbone with ring topology and fixed passive nodes (OADMs). The resulting network provides entangled photon pairs among any pair of access networks. Moreover, the number of pairs per access network can be gradually increased connecting more ports at the source.

The network is limited to a few access networks with current quantum technology due to the fixed mapping of CWDM channels and loss budget. In order to go beyond this network size, we need to explore other communication schemes and network architectures that could potentially allow for a more flexible design.

6

QUANTUM METROPOLITAN OPTICAL NETWORK USING ACTIVE TECHNOLOGY

The network proposed in the previous two chapters fulfills its goals in a cheap and simple way, but falls short when facing a considerable increase in the number of users. The objective here is to devise a larger quantum metropolitan optical network using current quantum technology. For this, we conserve the previous channel plan and access networks, but change the backbone architecture using reconfigurable nodes and a mesh topology. Although, throughout this chapter, we consider both one-way signals and entangled photon-pairs, the scheme works seamlessly with only one of them.

6.1 ACTIVE BACKBONE NODE

The active, reconfigurable version of the backbone node is shown in Fig. 6.1. The design is a transparent optical cross-connect, also called photonic cross-connect (PXC), adapted to our needs. The PXC allows to route any input signal to any output port (even the original one). This opens the door to use a dynamic assignment of CWDM channels for the access networks. The operation mode is simplified to only one function:

- Cross: Signals reach the PXC through a port and they are separated into quantum and conventional bands by a 1310/1550 WDM mux. Both bands are demultiplexed into CWDM channels and sent to the switch. The switch routes each channel to the corresponding CWDM mux. CWDM channels are again multiplexed and combined into one signal that leaves the PXC.

In case entanglement sources are needed, they are directly connected to the switch.

Note that due to the new topology, the backbone node uses the wavelength of the signal to decide through which output port goes the signal. Previously, the wavelength was used to decide whether to drop part of the signal or not. Hence, CWDM channels are now assigned to the communication paths instead of to the receivers.

In comparison with the OADM, the losses of the PXC are slightly lower due to the absence of splitters (see Table 6.1). However, this depends on the number of CWDM channels used per band. In our calculations, we have considered 4, which is almost the worst-case scenario due to the width of the quantum and conventional bands (approx. 100 nm). Although the figure shows a big switch for all signals,

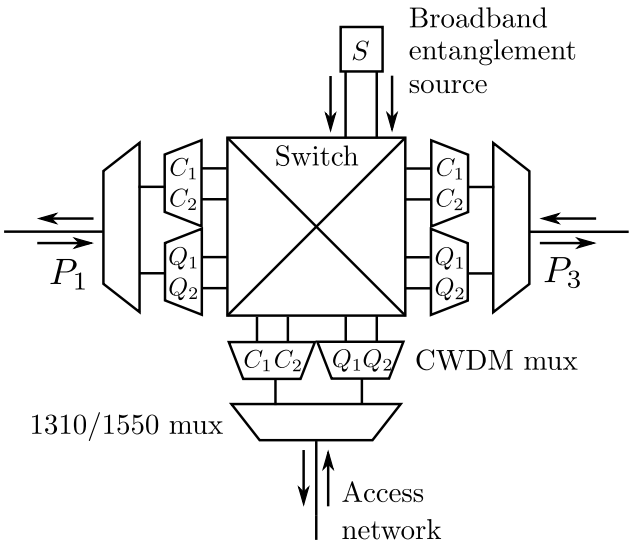


Figure 6.1: Design of an active backbone node for a mesh-based backbone that includes a broadband source of entangled photon-pairs. Incoming signals are demultiplexed into quantum and conventional bands using a 1310/1550 WDM mux, and then into CWDM channels. These are routed to their corresponding port via a switch. All signals are multiplexed again before leaving the node.

Table 6.1: Losses of the active backbone node with entanglement-capability depicted in Fig. 6.1.

Action	Losses Conv.	Losses Quantum	Losses Ent.
Cross	4 dB	4 dB	2.5 dB

we can use separate switches for each of them without increasing the losses.

We highlight the fact that the losses of the node are independent of its degree (number of ports). Signals will still cross the same number of components. This is really helpful when dealing with dense areas like metropolitan ones. For example, we can create redundant paths between nodes for resiliency. Another interesting use case is to connect more than one access network per node. We increase the number of users per area but without adding more backbone nodes.

6.2 NETWORK DESIGN

Fig. 6.2 depicts a quantum metropolitan optical network based on active backbone nodes, a mesh topology, and 4 access networks (A_1, A_2, A_3, A_4). Even though the network has more users and access networks, it only uses 4 sources and 2 CWDM channels per band: C1290 and C1310, and C1530 and C1550, for conventional and quantum signals, respectively. The communication scheme is still any-to-any, but not simultaneously. CWDM channels are not mapped to any access net-

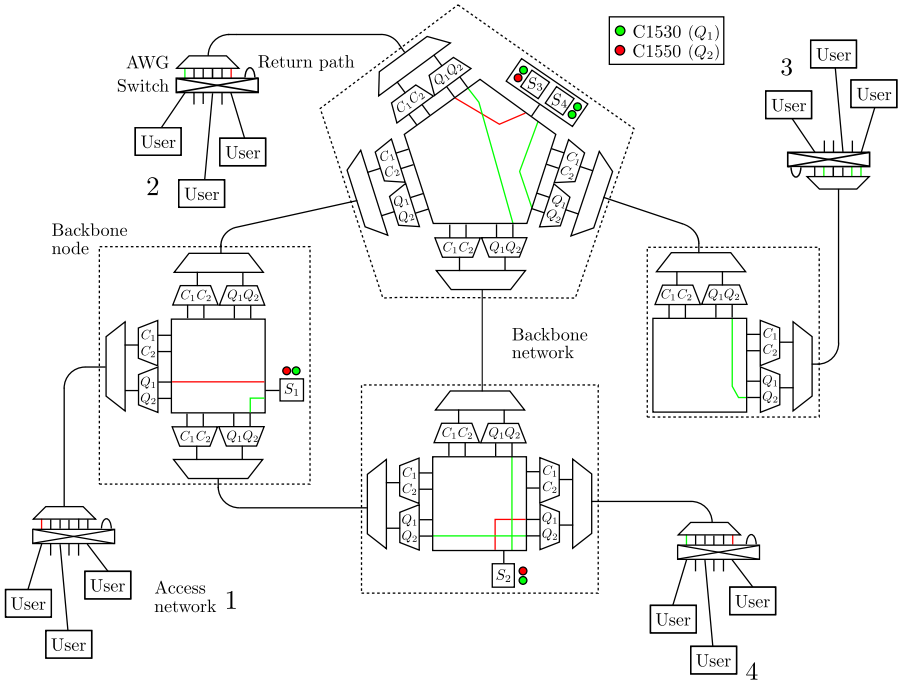


Figure 6.2: Quantum metropolitan optical network with a mesh-type backbone, backbone nodes based on active technology, and 4 access networks (A_x). Reconfiguring the nodes allows to interconnect all users using only 2 CWDM channels for quantum signals, but not at the same time. In the depicted configuration, entanglement is shared between A_1 and A_4, A_2 and A_4, A_2 and A_3, and within A_3. One-way, quantum and conventional, are not configured.

work. Furthermore, using less CWDM channels allows to reduce the number of different sources. Instead of having different sources, we configure the PXCs to route their signal to different access networks.

In contrast to the previous network design, the backbone nodes have to be configured carefully. We have to enable direct optical paths and entanglement-distribution between any pair of users using a fixed number of CWDM channels in the minimum number of steps. For instance, considering the networks in the figure, we need to create the following optical paths a total of 12 pairs:

- Enable direct optical paths between: (A_1, A_2), (A_1, A_3), (A_1, A_4), (A_2, A_3), (A_2, A_4) and (A_3, A_4). These are bidirectional, thus (A_1, A_4) is physically equal to (A_4, A_1). Moreover, we do not need to address direct paths between users from the same access network since that is already solved by the return paths at the switch.

- Distribute entanglement between: (A_1, A_1), (A_1, A_2), (A_1, A_3), (A_1, A_4), (A_2, A_2), (A_2, A_3), (A_2, A_4), (A_3, A_3), (A_3, A_4) and (A_4, A_4). Therefore, covering any pair of users.

Table 6.2: Path losses from an emitter (user or source) in a QKD-MON with a reconfigurable-mesh backbone (Fig. 6.2). Values calculated using Tab. 2.2 and Tab. 6.1.

Path to	Losses Conv.	Losses Quantum	Losses Ent.
0-closest access network	-	-	7.4 dB
1-closest access network	18.6 dB	18.6 dB	12.2 dB
2-closest access network	23.4 dB	23.4 dB	17 dB
3-closest access network	28.2 dB	28.2 dB	21.8 dB

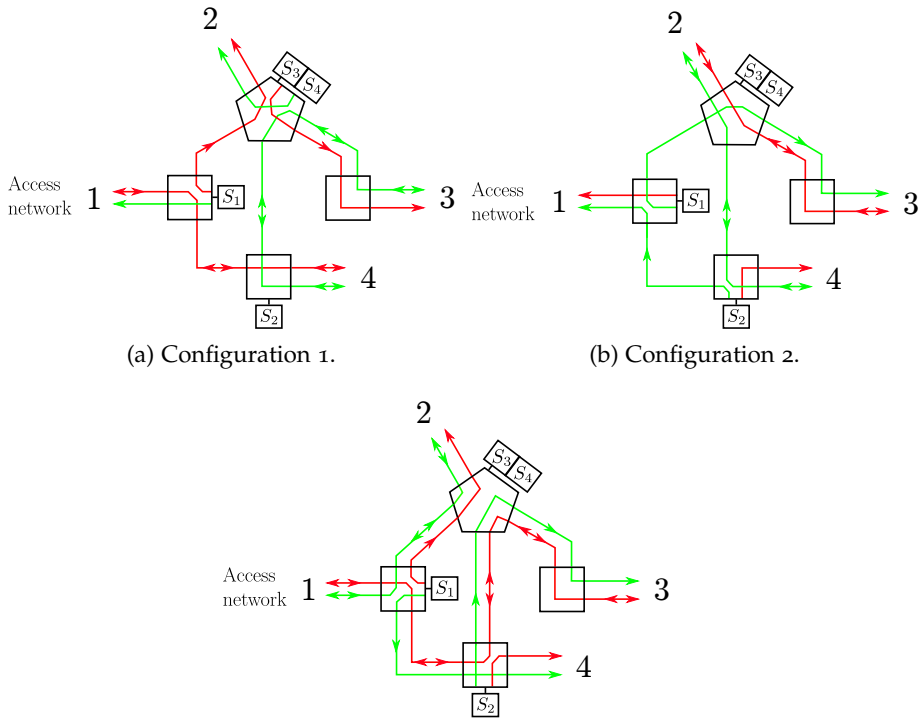
The problem is rather trivial as long as we have enough sources and loss budget. As an example, we show a series of network configurations in Fig. 6.3 for the network depicted in Fig. 6.2. The figure details each configuration over a simplified version of the network. These three steps cover all possible communications between pairs of access networks:

- Configuration 1: entanglement distribution over pairings (A_1, A_2) and (A_2, A_3), and direct optical paths between pairings (A_1, A_4) and (A_3, A_4).
- Configuration 2: entanglement distribution over (A_1, A_3) and (A_1, A_4), and direct optical paths between (A_2, A_4) and (A_2, A_3).
- Configuration 3: entanglement distribution over (A_2, A_4) and (A_3, A_4), and direct optical paths between (A_1, A_2) and (A_1, A_3).

Similarly, the network can be configured also to distribute entanglement over users from the same access network. Then, we can choose to use a fixed set of configurations that cover all possible communication paths and just reuse them over them time, or actively design the configurations depending on the user traffic at the moment.

We recalculate the path losses in Tab. 6.2. As expected, the values are lower because the backbone node introduces fewer losses. Moreover, entanglement sources can now communicate with receivers located at the immediate access network, i.e., the access network that is connected to the same backbone node as the source. Keeping in mind the 30 dB loss budget, the new design is limited to quantum communications between access networks separated by two intermediate backbone nodes: one way, 28.2 dB, and entangled, 29.2 dB ($12.2 + 17$).

Besides allowing farther communications, the number of users is also no longer a problem. In terms of loss budget, the mesh topology allows to add access networks without surpassing the worst-case path (in terms of losses) of the network by adding links that bypass intermediate backbone nodes. On the other hand, using PXCs and a



(a) Configuration 1.

(b) Configuration 2.

(c) Configuration 3.

Figure 6.3: Possible node configurations of the quantum metropolitan optical network shown in Fig. 6.2. Each backbone node is depicted as an schematic switch-box, and each color represents a CWDM channel for quantum signals. The three configurations cover all communication paths between pairs of access networks.

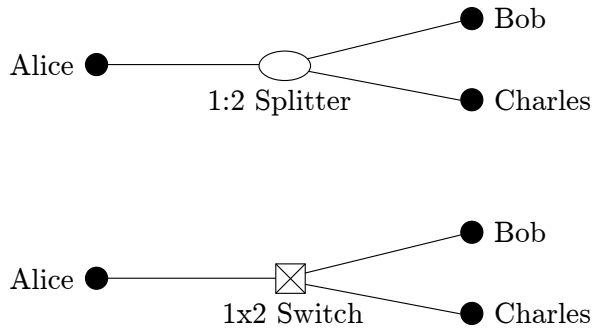


Figure 6.4: Basic network scenario with three users connected using a 1:2 splitter with ratio 50:50 or a 1x2 switch that switches each half a second.

dynamic assignment of CWDM channels allows to rotate the assignation of CWDM channels if we have more access networks than CWDM channels. Hence, the spectrum width of the source is not a limitation anymore. Finally, even if all available CWDM channels are used, the mix of active nodes plus mesh topology allows to reuse them in different parts of the network at the same time (see Fig. 6.3).

In the end, the network can grow and the only effect will be an increase in the number of configurations needed to cover all possible communication paths. It is equivalent to decomposing the reconfigurable network into smaller fixed ones.

6.3 EFFECT OF SWITCHES IN QKD NETWORKS

In this design, we have replaced the splitters by switches in order to decide which communication paths are active at each moment. In contrast, previous designs based on splitters had all paths always available. In terms of QKD, one could wrongly conclude that this always implies now a lower secret key rate per path since qubits are only exchanged during part of the time. However, this may not be always true.

Let us consider the most basic scenario (see Fig. 6.4). The network consists in three users, Alice in one end, and Bob and Charles in the other end. If we connect them using a 1:2 splitter, the communication paths Alice-Bob and Alice-Charles are always available (assuming that Alice's detectors are not a bottleneck). But, if we use a 1x2 switch instead, each communication path will be available only half of the time. Considering the same fiber length l between both ends for each scenario, the path losses using a splitter are then 3.1 dB more (see Tab. 2.2)

For the QKD, we consider a system implementing a standard BB84 with weak coherent pulses and APDs. The fraction of secret key r is thus calculated using the GLLP formula [44, 124, 167], which takes

into consideration imperfect source and detector. We start from the general expression described in Sec. 2.1:

$$r = 1 - leak_{EC} - I_E = (1 - H(Q)) - leak_{EC}$$

Since the source emits multiphoton pulses ($p_{multi}(\mu)$), Eve can gain information from them without being detected by Alice or Bob. She can split the pulses and measure her part. Therefore, we calculate the secret fraction r considering only sinle-photon pulses:

$$r = Y_1(1 - H(Q_1)) - leak_{EC}$$

where Y_1 is the fraction of single-photon pulses detected, and Q_1 is the QBER corresponding to those pulses. Y_1 is calculated as:

$$Y_1 = 1 - \frac{p_{multi}(\mu)}{p_{exp}}$$

where $p_{multi}(\mu)$ is the probability of emitting a multiphoton pulse by an attenuated laser with a mean photon number per pulse of μ, and p_{exp} is the probability of having a detection. Both expressions are calculated as follow:

$$p_{multi}(\mu) = 1 - (1 + \mu)e^{-\mu}$$

$$p_{exp} = p_{signal} + p_{dc} - p_{signal}p_{dc}$$

For p_{exp}, we take into account the probability of detecting a legitimate signal (p_{signal}), and also the probability of having a dark count p_{dc}. We approximate p_{signal} considering: (i) the transmittance of the fiber ($\tau = 10^{-\alpha l/10}$), where α is the attenuation coefficient of the fiber and l is the fiber length; (ii) the mean photon number per pulses ($\mu < 1$); and (iii) the quantum efficiency of the detector (η). Therefore, the final expression is $p_{exp} \approx \mu\tau\eta$. For the QBER, we only considering the dark counts as a noise source, thus:

$$Q = \frac{\frac{1}{2}p_{dc}}{p_{exp}}$$

and the QBER from single-photon pulses is: $Q_1 = Q/Y_1$. Finally, the information leakage of the distillation is lower bounded by $H(Q)$. Hence, any imperfect post-processing will introduce an efficiency factor $f(Q)$. This gives the following formula for the secret fraction r:

$$r = Y_1(1 - H(Q_1)) - H(Q)f(Q)$$

Now, we only have to multiply it by the detection rate R in order to obtain the secret key rate K:

$$K = R[Y_1(1 - H(Q_1)) - H(Q)f(Q)]$$

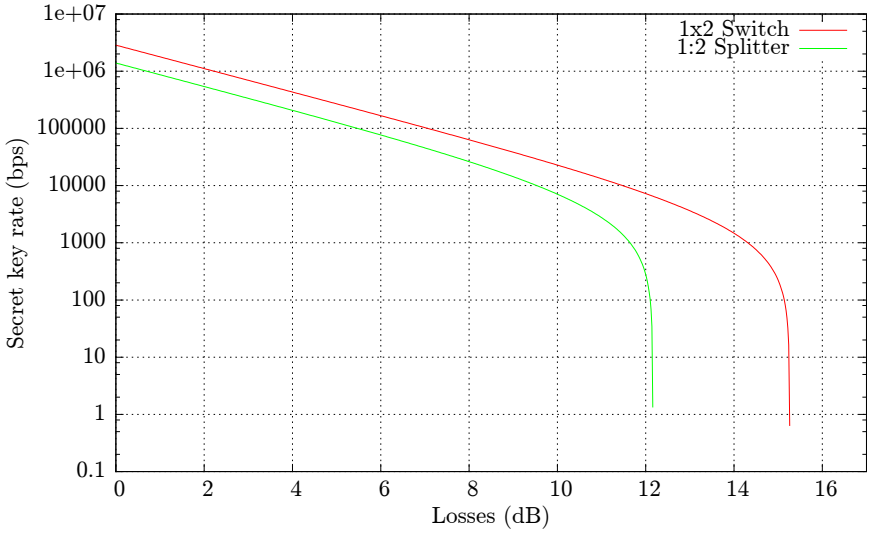


Figure 6.5: Secret key rate vs path losses of a BB84 QKD system using Eq. 6.1. We compare two scenarios, one with a 1:2 balanced splitter and another one with a 1x2 switch. The switch scenarios takes into consideration 25 ms of switching time.

where R is calculated using the frequency of the system f, the protocol efficiency q, and the probability of a detection:

$$K = f \cdot q[-p_{exp} H(Q) f(Q) + Y_1(1 - H(Q_1))] \tag{6.1}$$

Although it may seem contradictory, in this case, the secret key rate when using switches is always greater. This is due to the losses introduced by each component, which translate to a QBER, and how that affects the key distillation. Not only the key rate decreases exponentially with the losses, but as the losses increase, and thus the QBER, the distillation also wastes a bigger part of the key in order to correct the errors and reduce Eve's knowledge. This means that, in our scenario, the secret key rate (K) relationship between both scenarios is:

$$(T - T_s)K_{sw} > K_{spl}$$

where T is the fraction of time that the path is available, and T_s is the switching time, which reduces the available time. We plot both key rates in Fig. 6.5 using $T = 0.5$ (half a second) and $T_s = 25$ ms[5]. For the QKD systems, we have considered the following common parameters: $F = 1$ GHz, $q = \frac{1}{2}$, $\eta = 15\%$, $\mu = \tau\eta$, $p_{dc} = 10^{-6}$, and $f(Q) = 1.2$. As it can be seen, the secret key rate in the switched scenario is always greater, and even withstand more losses.

6.4 CONCLUSIONS

In this chapter we have explored the use of active technology and a more flexible topology in a quantum metropolitan optical network

than the one described in the previous two chapters. The objective is to support more users. In particular, we have changed the backbone network architecture while maintaining the channel plan and access networks. Furthermore, the network also still supports one-way signals along with entangled photon-pairs.

First, we have used active backbone nodes based on PXCs instead of fixed OADMs. We can now configure which CWDM channels are dropped in each access network, and thus intercommunicate more access networks using the same number of CWDM channels. Second, we have also moved from a closed ring to a mesh topology. This has several benefits: (i) add backbone nodes but maintaining the overall network loss budget, (ii) add redundant paths, and (iii) reuse CWDM channels.

The resulting network achieves its main objective of not being limited in terms of users. Moreover, with the same loss budget, it permits farther communications. Despite passive components tend to be more robust and reliable, the flexibility of using at will different paths to reach the same destination also makes the network resilient to attacks and link failures.

Nevertheless, these benefits come at a price. First, both the deployment and operation costs increase considerably. Switches are not, in general, a cheap component (depends on the number of ports) and active nodes require conditioned facilities, a constant consumption of energy, more maintenance and a management protocol. Moreover, the management layer becomes more complex as we add nodes. Similarly, this also affects the scalability. Adding or removing backbone nodes, links and/or access networks requires a complete redo of the configurations.

7

EXTENDING THE REACH OF QUANTUM COMMUNICATIONS

Despite the efforts to provide telecommunication networks with quantum channels—whether it is done via integration or building a parallel network—, we know that quantum communications, as conventional ones, have a limited loss budget. It is mandatory to look for technologies capable of extending their reach. In this chapter, we show the available solutions and propose a new one based on network-coding and current technology. This new solution features modulation of the information gained by the repeater, and thus how much the user is willing to trust the repeater, at the expense of a reduced transmission rate.

7.1 AVAILABLE SOLUTIONS

Fig. 7.1 shows a basic scenario where an emitter e wants to transmit a message m made of qubits to a receiver r, for instance to create a secure key with QKD. However, the losses between both are above the loss budget of their devices (represented as a gray area in the figure). As it can be seen, they are forced to use, at least, one intermediate device or node t that somehow relays m to r. Next, we enumerate the technological solutions for t: quantum amplifier, quantum repeater and trusted repeater.

An optical amplifier increases the power of an input signal by generating photons at the signal's wavelength. However, in a quantum signal the information is carried in the physical state of the photons;

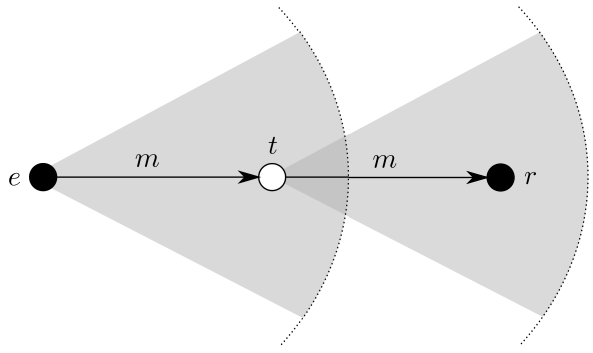


Figure 7.1: Basic scenario of a quantum communication where an emitter e wants to transmit a message m to a receiver r. However, their separation exceeds the reach of e (gray-out area). They need an intermediate node t.

the photons generated would need to be clones of the input ones. As stated in Chap. 2, this is impossible without introducing a degree of fidelity in the process. The clones are not perfect. To overcome this obstacle, a promising solution are the non-deterministic noiseless linear amplification models of heralded photons [56, 168]. Its application to QKD has already been studied [169, 170].

A repeater is a more advanced device that aims to output a signal identical to the one output by the emitter. For conventional communications, this means not only to amplify it but to regenerate it in terms of shape and timing. In case of quantum signals, several schemes have been proposed [54, 171]. Among them, one of the most promising is the BDCZ quantum repeater which has been experimentally demonstrated [172]. The basic idea is to use entanglement swapping to share entanglement between nodes that do not originally share it. The procedure goes as follows: (i) in each link of the scenario (i.e., between e and t, and t and r) a pair of entangled-photons is generated and one photon of the pair is distributed to each end; (ii) t measures his two photons and communicates the result to e or r (teleportation); and (iii) e and r now share a pair of entangled-photons just like if e would have transmitted it to r. Despite the experiment, their requirement of quantum memories hinders their progress towards a practical version (though all-photonics quantum repeaters are being studied [173]). As quantum amplifiers, they are not a commercial solution either.

Beyond quantum technologies, we are forced to use conventional solutions that irremediably intercept and destroy the end-to-end quantum communication. They are basically a trusted man-in-the-middle scheme. Therefore, all solutions imply a degree of trust on t since it will get meaningful information during the process [174]. Formally, these are known as trusted repeaters [57, 58, 59]. The main idea is to create a secret key k in each link using QKD, and then use them to cipher m via a secure symmetric-key algorithm such as one-time pad (OTP)[1]. If t is trusted, this is equivalent to having a secure private channel where a message m is sent from e to r. Since trusted repeaters are the only practical possibility nowadays, most QKD networks deployed up to date use them (e.g. [99, 101, 103, 104, 45, 105, 106, 107]).

In order to alleviate this reliance condition, it is possible to use the trusted repeaters in a secret sharing scheme [60]. In this way, each t only has partial information about m. As long as specified sets of t do not cooperate, m remains secret. Hence, each t can be weakly trusted. Here we formalize this model of *weakly trusted repeaters* (WTR) under the new paradigm of network coding [175], where the intermediate nodes, instead of simply routing the incoming flows through the outgoing paths, distribute a function of the inputs through each outgoing path. It has been shown that linear combinations of the

1 One-time pad (OTP) is an information-theoretically secure cryptosystem with perfect secrecy: no information is leaked to Eve.

inputs suffice to maximize multicast transmissions [175] and allows to improve on several other aspects such as security [174]. The application of network coding in optical networks has been widely studied. For instance, in Ref. [176, 177], the authors improve the performance, robustness and reliability of optical networks, while Ref. [178] focus on PON.

7.2 FORMALIZATION OF WEAKLY TRUSTED REPEATERS

Let us consider a network over a directed acyclic multigraph $\mathcal{G}$ defined by its nodes $\mathcal{N}$ and links $\mathcal{L}$. The links connected to a node are defined by the adjacency of the node $\mathcal{A}(\cdot)$. Therefore, a link $l \in \mathcal{L}$ connects two nodes $v_1, v_2 \in \mathcal{V}$ if $l \in \mathcal{A}(v_1)$ and $l \in \mathcal{A}(v_2)$. All messages traversing l are OTP-ciphered using a key k distributed using QKD between v_1, v_2. Hence, as in trusted repeaters networks, the links are secure. Eavesdropping is reduced to the intermediate nodes. Note that by allowing multiple edges between two nodes we can generalize the model to links with different capacities[2]

Nodes are split in three subsets: sources $\mathcal{S}$, users $\mathcal{U}$ and intermediate nodes $\mathcal{T}$. Every source s generates a source message m_n. We call M the message jointly generated by all source nodes. On the other hand, a user u aims to receive with no error M_u, the messages sent by S_u, a specific subset of $\mathcal{S}$. We will denote by Y_l and Y_u the messages sent through the link l and reaching the user u, respectively. Finally, intermediate nodes t are allowed to output a function of the incoming flows. If we restrict the functions to linear combinations of the inputs, we can easily deduce that they also represent linear combinations of the source messages.

A WTR network is composed of a series of disjoint paths that connect a subset of sources with a subset of intermediate nodes with a subset of users. Each disjoint path is divided into links. We call the n-layer of the WTR network, the set of links that occupies the n-position in each disjoint path, where the position 0 is the one between the source and the first intermediate node. Therefore, the rate of a WTR transmission between s and u is a function of the rate of each layer.

From this generic definition, we can focus in the special case of interest for a quantum communication in which there is one source, one user and the eavesdropper is interested in the whole message m.

7.2.1 *Security*

We define a set of $\mathcal{W}$ independent eavesdroppers where every $w \in \mathcal{W}$ may receive the messages crossing a fixed collection of nodes, or

2 The capacity of a WTR link is bounded by the secret key rate of the QKD system that generates k. Since we use OTP, k has to be as long as the linear combination sent through the link.

eavesdropping pattern B_w, in order to recover a subset of the source message M_w. In consequence an eavesdropper has access to $Y_{B_w} = \{Y_l : l \in \mathcal{A}(v), v \in B_w\}$, the messages traversing B_w. Note that if an intermediate node of a disjoint path is compromised, and then the whole path it is.

Following [174], a network code is admissible over this *eavesdrop network* model if every user node u can recover M_u (decodable condition) and the information that every eavesdropper w holds about M_w does not reduce its entropy[3] (secure condition):

$$H(M_w|Y_u) = 0 \tag{7.1}$$

$$H(M_w|Y_{B_w}) = H(M_w) \tag{7.2}$$

Byzantine adversaries

Until now, the eavesdropper had a passive role. He could gain information only by listening to the intermediate nodes. Adversaries allowed to go beyond this limitation and output any message on their outgoing links are called Byzantine adversaries. Let suppose a WTR network where t intermediate nodes are controlled by a Byzantine adversary. If we want perfect secrecy and perfect resiliency[4], Dolev *et al.* [180] showed that at least $3t + 1$ one-way disjoint paths are required between s and u.

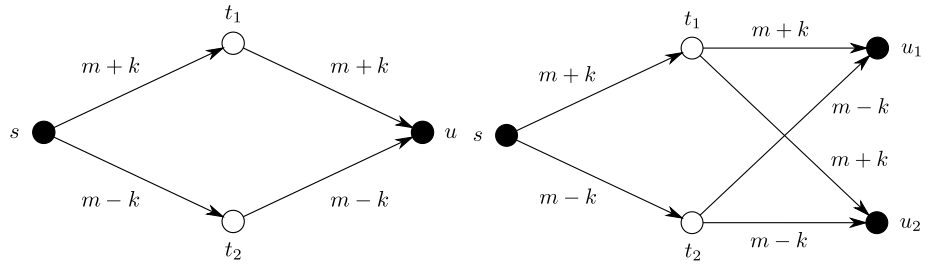
This means that 4 disjoint paths are already required for only 1 byzantine adversary. Considering the early stage of quantum telecom networks in terms of number of nodes and paths between them (e.g., deployed networks typically consist in less than 10 nodes and only 1 path), this condition seems unattainable at the moment. In these cases, a weaker security has to be considered. If we downgrade the perfect resiliency to just message authenticity, Salvail *et al.* show in [58] that only $t + 1$ are required. It only needs one uncorrupted disjoint path between s and u.

7.3 LOGICAL SCENARIOS

A simple scenario of weakly trusted repeaters is shown in Fig. 7.2a. Here, a source s and an user u exchange a secure key relying in two intermediate nodes (t_1 and t_2). The source s generates a message m and a random message r, both taking values over the finite field $GF(3)$, and sends a linear combination of both to t_1 or t_2 using the keys exchanged using QKD in the respective links. The intermediate nodes

3 $H(\cdot|\cdot)$ is Shannon's conditional entropy [179].

4 Perfect resiliency means that the adversaries are unable to stop the sources from reliably transmitting the messages to the users (e.g., a denial of service attack).



(a) Unicast transmission. (b) Multicast transmission.

Figure 7.2: Logic unicast and multicast scenarios for quantum communications using weakly trusted repeaters. All transmissions are OTP-ciphered using a QKD secret key. (a) In this network, the source s sends a message $m \in \mathcal{M}$, in linear combination with a random message k, to the user u using t_1 and t_2 as intermediate nodes. These can eavesdrop their incoming and outgoing links. If they don't cooperate, they have no information about m. (b) The source s distributes the same secret key to two different users u_1 and u_2.

t_1 and t_2 route the messages to u, who is able to recover m using both received messages. It is easy to verify that the information that t_1 or t_2 gets from M (here, $M = m$) is:

$$H(M|Y_{t_1}) = H(M|Y_{t_2}) = 0 \tag{7.3}$$

where Y_{t_1} and Y_{t_2} are the sets of extended messages traversing t_1 and t_2 ($m + r$ and $m - r$, respectively).

The previous scenario can be used to enable multicast distribution, as shown in Fig. 7.2b: the extra links joining t_1 and t_2 with the second user u_2 replicate the links with u_1. Now, m is relayed securely to 2 users. This is of special interest if s is trusted by default, for instance, due to hierarchy. A clear example of this situation can be found in banks. Let suppose that the node s are the headquarters and $\mathcal{U}$ the subset of banks. After an initial m is shared from s to every $u \in \mathcal{U}$, secure communications between the banks are allowed using m as the secret key.

Despite the clear gain shown in the above scenarios, intermediate nodes did not operate with the messages. In order to illustrate the capability of weakly trusted repeaters, consider now the scenario depicted in Fig. 7.3. Here, proposed by Chan *et al.* in [181], four nodes (s_1, s_2, u_1 and u_2) exchange keys pairwise (m_1 between s_1 and u_2, and m_2 between s_2 and u_1) relying in t_1 and t_2. In other words, u_1 and u_2 should be able to recover m_2 and m_1, respectively, but not m_1 and m_2. In effect, the users recover the desired message by adding the incoming flows and

$$H(M_1|Y_{u_1}) = H(M_2|Y_{u_2}) = 0 \tag{7.4}$$

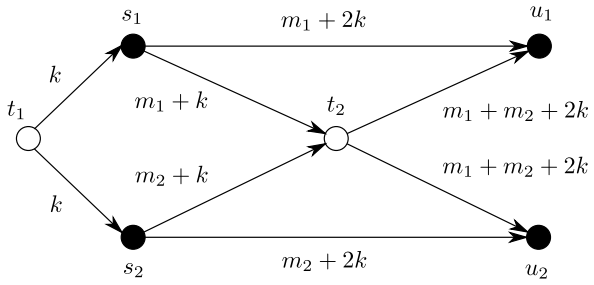


Figure 7.3: Logic multi-source scenario for quantum communications using weakly trusted repeaters. Two sources, s_1 and s_2, transmit m_1 and m_2 to the users, u_2 and u_1, respectively. The message is linearly combined with a random message k, and OTP-ciphered with a QKD secret key. No information is leaked to the intermediate nodes or the remaining users.

It should be noted that $H(M|Y_{t_1}) = 0$, $H(M_1|Y_{t_2}) = H(M_2|Y_{t_2}) = 0$ but $H(M|Y_{t_2}) > 0$. That is, the network code is admissible if t_2 aims to recover either M_1 or M_2 but not both.

Beyond these examples, where network code constructions can be discovered by inspection, explicit code constructions in the general wiretapping model is an open problem [181]. However, in the single source scenario, secure network code constructions are fairly well known [174].

7.4 IMPLEMENTATION ON METROPOLITAN OPTICAL NETWORKS

In this section we implement the unicast and multicast scenarios in quantum metropolitan optical networks (QKD-MON) to show the utility of WTRs. In particular, we focus in the transmission and routing of quantum signals through a typical MON. The network layer where the ciphered messages are transmitted is considered to be available via traditional telecom networks.

Our network model is depicted in Fig. 7.4. The nodes $\mathcal{N}$ are deployed at the backbone nodes and as users of the access networks. The physical links between these two subnetworks are represented by solid lines in the figure. The nodes at the access networks belong to the subset of sources and users, $\mathcal{S}$ and $\mathcal{U}$ respectively, meanwhile the nodes at the backbone are the intermediate nodes, subset $\mathcal{T}$. Using WDM, we enable a logical link (pointed line in the figure) between each source s and user u, and at least two intermediate nodes t: from its own backbone node and a neighboring one. Therefore, each intermediate node t connects at least two access networks.

The type of QKD device selected for each node is not arbitrary. We put the QKD emitters Tx_n at the access network and the QKD receivers Rx_n, more expensive and difficult to maintain due to the SPD, at the backbone nodes, which are located at the telco facilities.

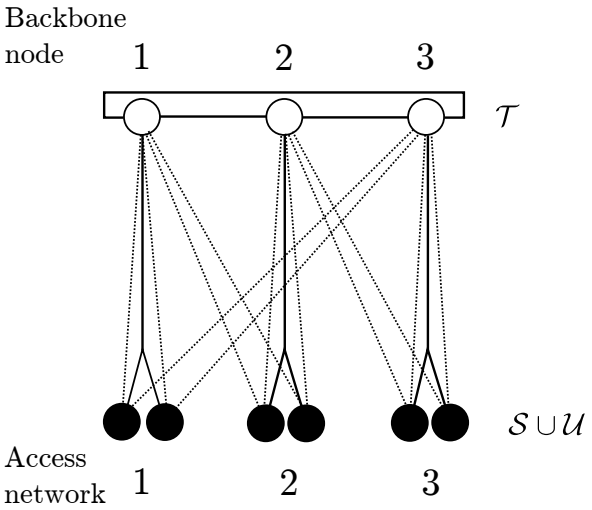


Figure 7.4: Scheme of a QKD-MON with weakly trusted repeaters. Solid lines represent physical links, and dashed lines, logical ones. Intermediate nodes ($\mathcal{T}$) are located at the backbone nodes and the sources ($\mathcal{S}$) and users ($\mathcal{U}$) at the access networks. The resulting scheme is similar to the one in Fig. 7.2a but folded in two by the middle.

Next, we present two network prototypes based on passive optical components and wavelength-addressable: a pair of QKD devices communicate using the wavelength assigned to the receiver. In this way, multiple emitters can communicate simultaneously with different receivers, because each receiver is addressed using a different wavelength.

Note that, QKD systems with a higher loss budget would allow farther away locations, higher secret key rate and increase the number of disjoint paths, thus improving the throughput and security of the protocol.

7.4.1 *First prototype*

A first prototype is depicted in Fig. 7.5. In the backbone nodes, a CWDM OADM is used to route signals to the corresponding access network. Add and drop ports are connected to a DWDM filter F that routes the signals at the corresponding DWDM channel to the receiver. Both filters F are then connected to a band-pass filter, F_a, using the reflected and filtered ports. The common port of F_a connects the backbone with the access network, thus routing signals from the access network in the correct direction of the backbone ring. In consequence, the backbone ring is bidirectional. In the access network several emitters are connected to an splitter, as in GPON.

In particular, each emitter can communicate with the immediate backbone node and both neighboring backbone nodes. For instance, in Fig. 7.5, Tx_5 is able to communicate with Rx_1, Rx_2 and Rx_3. Con-

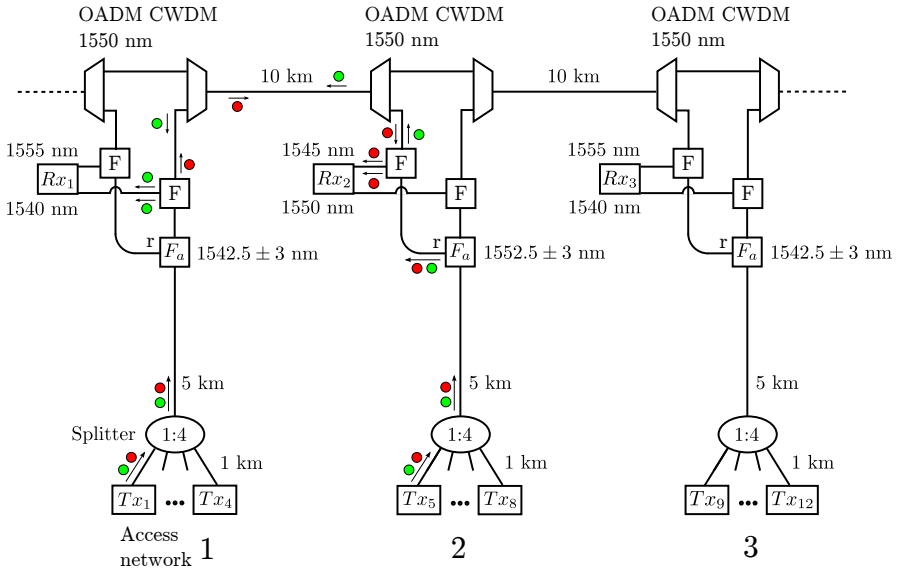


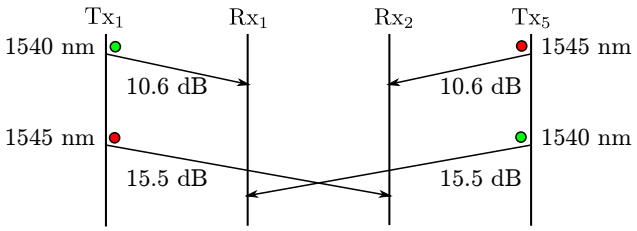
Figure 7.5: QKD-MON prototype using weakly trusted repeaters. At the backbone, 1550 nm CWDM OADMs are used in parallel with DWDM OADMs (F) that route signals to the corresponding receiver. Finally, a band-pass filter F_a is used to connect the access network with the backbone and route signals into the correct direction within the backbone (bidirectional ring). The figure also shows a WTR communication between Tx_1 and Tx_5 using colored circles. The color indicates the wavelength of the signal.

sidering the fiber distances in the figure and the values of Tab. 2.2, the path losses to the quantum receiver at the immediate backbone node is 10.6 dB while the one at the neighboring one is 15.5 dB. Since communications between farther nodes are unfeasible due to losses, wavelengths for the filters can be used repeatedly all over the network. This reduces the number of required wavelengths and simplifies the network construction.

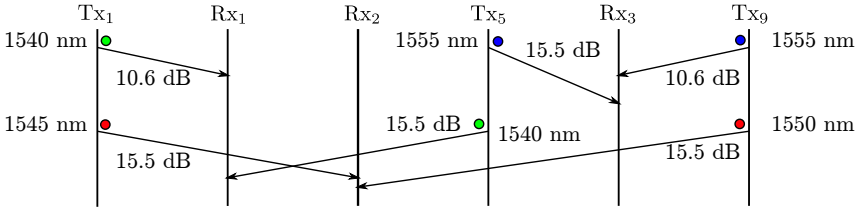
The figure also shows the key exchanges needed for a unicast transmission between Tx_1 (s) and Tx_5 (u) using colored circles. The communication scheme is illustrated in Fig. 7.6a. As it can be seen, Rx_1 and Rx_2 act as intermediate nodes t_1 and t_2. After these key exchanges, Tx_1 and Tx_5 have the required two disjoint paths: $Tx_1 - Rx_1 - Tx_5$ and $Tx_1 - Rx_2 - Tx_5$. This simple case can be extended to exchanges between farther nodes, just repeating the communication pattern (see Fig. 7.6b). Finally, we represent in Fig. 7.6c a multicast scenario where Tx_1 (s) communicates with Tx_5 (u_1) and Tx_8 (u_2). The links between u_1 and the intermediate nodes t_1 and t_2 are replicated to u_2.

7.4.2 *Second prototype*

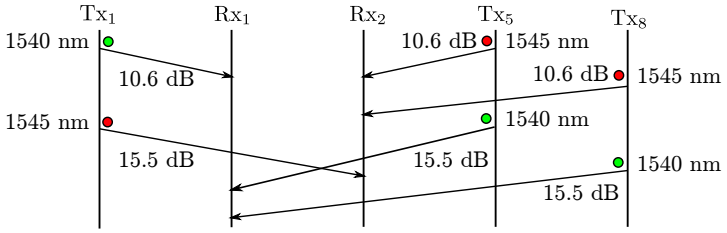
A second network prototype is shown in Fig. 7.7. At the backbone nodes, the CWDM OADM is replaced by a splitter, thus making



(a) Unicast transmission.



(b) Extended unicast transmission.



(c) Multicast transmission.

Figure 7.6: Possible types of WTR communications using weakly trusted repeaters in the QKD-MON prototype depicted in Fig. 7.5. Each transmission is labeled with its wavelength (colored circle) and loss budget.

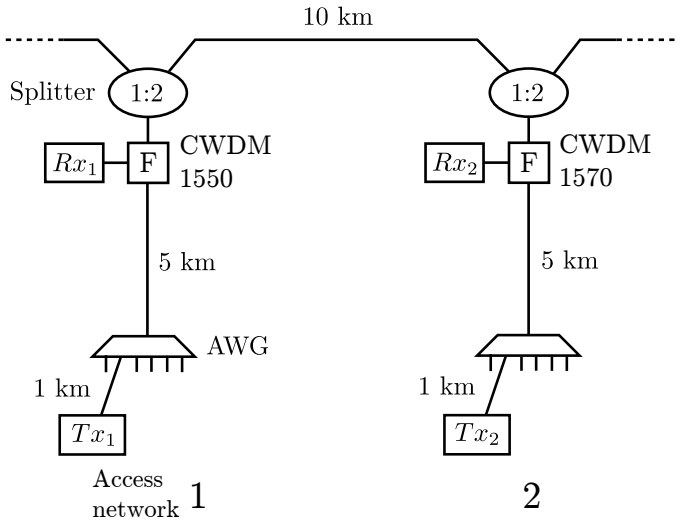


Figure 7.7: Second prototype of a QKD-MON with weakly trusted repeaters. Splitters are used instead of CWDM OADMs. These changes permit to use an AWG at the access network, and thus increase the number of users.

unnecessary F_a since signals are automatically sent in both directions. This also allows to reduce the number of F to one. This modification permits to use an AWG in the access network which increases the number of users up to 32 with less insertion losses (see Tab. 2.2). The operation mode is simple. Let us consider that a band of the AWG is a CWDM channel, then we also use CWDM channels for the filters F (1550 and 1570 in the figure). By periodicity of the AWG, a emitter Tx can, in principle, communicate with any receiver Rx. However, the architecture of the backbone node still limits communications to immediate and neighboring backbone nodes.

As described, this second prototype improves in terms of the number of users and resources, and preserves the communication scheme explained for the first prototype. Moreover, it also reduces the loss budget for all transmissions. Now, a communication with the quantum receiver at the immediate backbone node is 3.6 dB while the one at the neighboring one is 11.2 dB. Note that by reducing the losses we increase the secret-key rate of the QKD system which, in turn, increases the WTR transmission rate.

7.5 CONCLUSIONS

We have introduced weakly trusted repeaters as a solution to the loss budget limitation of QKD communications. WTR are formalized using a network-coding approach and they can be built using current technology. Compared with traditional trusted repeaters, WTR reduces the full trust dependence on the repeaters at the cost of a reduced

efficiency. As long as there is one non-malicious path between Alice and Bob, the communication remains secure.

We have also shown their usefulness via multiple logical schemes, and detailed particular implementations in metropolitan optical networks. These scenarios can be easily extended to a higher number of users and through more intermediate nodes.

WTR can directly founds its niche in private QKD networks where all nodes belong to the same organization, e.g., telecom companies, banks, military institutions or government agencies. In this case, even though there is only one user, nodes are still a potential security threat, suspected of being eavesdropped. They cannot be fully trusted. Nevertheless, communications will remain secure unless all nodes are taken down. Another interesting situation occurs when the user does not own any network, but he can communicate through multiple ones to reach the destination. Although we do not trust any in particular, we are confident that all of them will not cooperate. Hence, we weakly trust them.

8

CONCLUSIONS AND FUTURE WORK

8.1 CONCLUSIONS

Quantum information technologies open up a new range of possibilities in telecommunications, especially in security. For instance, QKD enables two users to grow a secret key between them with information-theoretic security, thus solving the key distribution problem of conventional cryptography. Far from being a futuristic technology, QKD is maturing rapidly and nowadays is ready to use: systems have pushed the records to more than 200 km, 1 GHz repetition rate and 1 Mbps of distilled secret key. Practical QKD systems are being commercialized, and studies have shown its long-term stability.

However, its commercial success has been modest, far from what one could expect for, an a priori, revolutionary technology. The main barriers for its adoption are the cost and usability, including its deployment. Nowadays, QKD systems are used in point-to-point scenarios with a dedicated fiber, which heavily restricts its use beyond some particular use case scenarios with a few nodes. In addition, the dedicated link has to be deployed by the user himself or rented to telecom companies, both options resulting in an unacceptable cost for the user. To have a future, quantum information technologies should aim for its use in networks, in real multiuser scenarios, with shared links. In particular, existing telecom networks based on optical fiber are a perfect environment due to their pervasiveness, reaching almost all potential users. By sharing links, the cost of using QKD would decrease dramatically and the number of possible scenarios would increase. The technology would become cheaper and more useful.

As a first step, in this thesis, we have studied the integration of quantum communications in telecom networks, in the so-called last-mile, which connects to the final users. Our objective was to enable the use of quantum signals in today's most used network standards (GPON, EPON) without modifying the operation mode, affecting the conventional users, or requiring too much effort from the telecom company. Regardless of its feasibility, solutions are limited in terms of reach, number of users and connection scheme. To solve these issues, one has to break free from the restrictions imposed by the conventional users, their signals and protocols, and grow from a simple add-on of an existing network standard to a full-feature quantum telecom network.

Following this idea, we have designed a quantum metropolitan optical network based on wavelength-division multiplexing. The archi-

tecture is a conventional backbone ring connected to multiple access networks, like a conventional metropolitan optical network. Great care was taken in that all network modules could be built using off the shelf commercial components. Therefore, it can benefit from market manufacturing for cheap and easy deployment. Using standard CWDM channels, a 100 GHz DWDM grid and a typical loss budget of 30 dB, the proposed network is able to support up to 64 users, with 32 simultaneous conventional signals. This can be easily improved by using other components, a denser grid, better filtering at the receiver or SPDs with shorter gates. Moreover, users address each other in an any-to-any, dynamic way by emitting at the receiver's assigned channel. Later, we have enhanced the design adding distribution of entangled photon-pairs between all access networks. This extension permits the use of the network by almost all QKD protocols and other quantum information technologies.

With the objective of going beyond those 64 users, we have explored other network architectures. In particular, we have changed the entire backbone. The rest of the network, access networks and channel plan, remains the same. Within the backbone, we have changed the fixed OADMs for reconfigurable PXCs, and the ring topology for a mesh. The result is a network more expensive and complex but without any limit in terms of users and access networks. Moreover, the dynamic routing and availability of multiple paths between nodes allows for a more robust and flexible network.

If we want a larger metropolitan network, connect distant metropolitan networks or even deploy a transnational quantum link, we will need a higher loss budget. Nonetheless, that budget increment is in the end a temporary patch. An increased limit is still a limit. In order to solve the loss budget limitation, we have proposed a classical solution based on the trusted repeaters paradigm but using a network coding approach. This new formalization allows to modulate the degree of trust put in the repeaters by using multiple intermediate nodes and disjoint paths. In the described scenarios, the information is transmitted with information-theoretic security unless all intermediate nodes cooperate to compromise the network.

As it can be seen, the overarching goal of this thesis is to remove the barriers that impede QKD technology to gain a broader market adoption. Nevertheless, this process greatly depends on external factors that are beyond the scope and control of QKD research. For example, it is known that current conventional solutions, based on the problems of the discrete logarithm and integer factorization, are breakable using a quantum computer and the Shor's algorithm; it is a matter of time until they become useless. This has encouraged the research of conventional post-quantum cryptography, protocols that are considered quantum resistant, but that, nowadays, are only Shor's resistant and have not demonstrated security against other

classical or quantum adversaries. Up to now, QKD remains the only one that can be demonstrated secure against any quantum or classical attack. Obviously, security is also a perceived risk, and the closer the realization of a quantum computer is felt, the faster the adoption of QKD will be.

In the meantime, the QKD community is devoted to the study and improvement of the protocols, systems and network solutions in order to make QKD competitive. In particular, the use of QKD in telecom networks is of special importance. Present solutions depend on the current state of conventional telecom networks, which are continuously evolving. Hence, they will become obsolete in a not so distant future unless actions are taken. More importantly, this evolution follows a set of interests that does not necessarily coincide with the ones from the quantum information community. As one could expect, new telecom standards and technologies try to exploit their resources and solve their problems, without taking into account how they can affect quantum signals. Nothing ensures that future networks will be more quantum-friendly, unless we tell them how do it and present compelling reasons.

For example, optical amplifiers are becoming a reality in next-generation optical access networks in order to increase the reach, number of users and loss budget [182]. In addition, the spectrum is being filled up with more signals aiming for a higher bandwidth (e.g., DWDM metro backbone [160, 150], TWDM-PON [159], ultra-dense coherent WDM-PON [183]), which increases the overall photon flux per second in the fiber and typically reduces the available spectrum. Similarly, the backbone topology is starting to deviate from the traditional ring to a more flexible, elastic and dynamic mesh where the nodes are capable of rearranging the routing and logic scheme of the network at any moment depending on the demand, link failures, etc. For that, the backbone nodes use *CDC* ROADMs based on wavelength-selective switches [162, 161].

Despite all these problems, the fundamental characteristic that allows conventional telecom networks to be considered adequate for photonics-based quantum information technologies still remains: the optical medium. Everything indicates that fiber and optical devices will be at the core of the future networks. Moreover, network components based on optical devices are becoming more flexible and the emergence of software-defined optical networks [184], which focus on controlling the components at will, could make a difference for quantum communications and their emergence as feasible commercial technologies.

8.2 FUTURE WORK

Finally, we outline the lines of research that remain open after the results obtained in this thesis:

- Analyze the performance of QKD systems in multiuser networks where simultaneous quantum signals are transmitted between multiple users. Explore the possibility of using a load balancing scheme in reconfigurable networks.
- Characterize the noise produced by conventional signals in a quantum metropolitan optical network with a mesh-shaped backbone and reconfigurable backbone nodes.
- Improve the integration schemes for today's network technologies by reducing the number of requirements and modifications (thus, reducing the cost and effort).
- Study other backbone architectures, based on DWDM technology. This would allow for a more flexible routing, instead of grouping all DWDM channels in CWDM channels and routing them together.
- Investigate the trend of future optical networks, and their standards, and how quantum communications can be used in them.

BIBLIOGRAPHY

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Review of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[2] H. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, "2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution," vol. 7681, pp. 76 810Z–76 810Z–8, 2010.

[3] Corning: SMF-28e+ LL optical fiber, http://www.corning.com/.

[4] Flyin Optronics: splitter, circulators, CWDM filters and 1310/1550 WDM multiplexers, http://www.flyinoptronics.com/.

[5] Polatis: optical switch Series 6000, http://www.polatis.com/products/index.asp.

[6] LG Nortel WPF 1132C (32-channels AWG).

[7] Advanced Optics Solutions (AOS), "Fiber Bragg gratings," http://www.aos-fiber.com/eng/Products.html.

[8] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[9] D. Atkins, M. Graff, A. K. Lenstra, and P. C. Leyland, "The Magic Words are Squeamish Ossifrage," in *Proceedings of the 4th International Conference on the Theory and Applications of Cryptology: Advances in Cryptology*, 1995, pp. 263–277.

[10] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management - Part 1: General (Revision 3)," in *NIST Special Publication 800-57*, 2012.

[11] European Union Agency for Network and Information Security (ENISA), "Algorithms, Key Sizes and Parameters Report," in *Recommendations*, 2013.

[12] R. Shankar, *Principles of Quantum Mechanics*. Springer, 1994.

[13] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[14] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. IEEE Press, 1984, pp. 175–179.

[15] G. Benenti, G. Casati, and G. Strini, *Principles of quantum computation and information: Basic concepts*. World Scientific Publishing Company, Incorporated, 2004.

[16] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[17] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, no. 19, p. 3762, 2004.

[18] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors," *Optics Express*, vol. 14, no. 26, pp. 13 073–13 082, 2006.

[19] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Physical Review Letters*, vol. 98, p. 010504, 2007.

[20] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photonics*, vol. 1, no. 6, pp. 1749–4885, 2007.

[21] S. Wang, W. Chen, J. Guo, Z. Yin, H. Li, Z. Zhou, G. Guo, and Z. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Optics Letters*, vol. 37, no. 6, pp. 1008–1010, 2012.

[22] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," *Optics Express*, vol. 21, no. 20, pp. 23 241–23 249, 2013.

[23] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Passive Optical Network Approach to Gigahertz-Clocked Multiuser Quantum Key Distribution," *Quantum Electronics, IEEE Journal of*, vol. 43, no. 2, pp. 130–138, 2007.

[24] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Optics Express*, vol. 16, no. 23, pp. 18 790–18 979, 2008.

[25] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, no. 7, p. 075003, 2009.

[26] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," *Optics Express*, vol. 19, no. 11, pp. 10 632–10 639, 2011.

[27] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, vol. 92, no. 5, p. 057901, 2004.

[28] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution," *Physical Review Letters*, vol. 89, no. 3, p. 037902, 2002.

[29] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, "Security of Distributed-Phase-Reference Quantum Key Distribution," *Physical Review Letters*, vol. 109, p. 260501, 2012.

[30] X. Ma, H.-K. Lo, Y. Zhao, and B. Qi, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[31] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics Express*, vol. 21, no. 21, pp. 24 550–24 565, 2013.

[32] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," *Optics Express*, vol. 17, no. 16, pp. 13 326–13 334, 2009.

[33] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. LegrÃ©, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New Journal of Physics*, vol. 16, no. 1, p. 013047, 2014.

[34] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Review of Modern Physics*, vol. 84, pp. 621–669, 2012.

[35] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[36] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[37] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[38] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. LorÃ¼nser, E. Querasser, T. Matyus, H. HÃ¼bel, and A. Zeilinger, "A fully automated entanglement-based quantum cryptography system for telecom fiber networks," *New Journal of Physics*, vol. 11, no. 4, p. 045013, 2009.

[39] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature Communications*, vol. 2, p. 238, 2011.

[40] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 108, no. 13, p. 130503, 2012.

[41] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, "Long distance measurement-device-independent quantum key distribution with entangled photon sources," *Applied Physics Letters*, vol. 103, no. 6, 2013.

[42] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, "Quantum key distribution session with 16-dimensional photonic states," *Scientific Reports*, vol. 3, 2013.

[43] A. Ruiz-Alba, J. Mora, W. Amava, A. Martínez, V. García-Muñoz, D. Calvo, and J. Capmany, "Microwave Photonics Parallel Quantum Key Distribution," *IEEE Photonics Journal*, vol. 4, no. 3, pp. 931–942, 2012.

[44] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information & Computation*, vol. 4, no. 5, pp. 325–360, 2004.

[45] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[46] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, "Field test of classical symmetric

encryption with continuous variables quantum key distribution," *Optics Express*, vol. 20, no. 13, pp. 14 030–14 041, 2012.

[47] K.-I. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," *Optics Express*, vol. 21, no. 25, pp. 31 395–31 401, 2013.

[48] ID Quantique SA. [Online]. Available: http://www.idquantique.com

[49] Toshiba Research Europe Ltd. [Online]. Available: http://www.toshiba-europe.com/research/

[50] F. Bovino and M. Giardina, "Practical Quantum Cryptography: The Q-KeyMaker," in *3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies*, nov. 2010, pp. 1 –4.

[51] MagiQ Technologies Inc., http://www.magiqtech.com.

[52] SeQureNet, http://www.sequrenet.com.

[53] AIT, http://www.ait.ac.at/epr.

[54] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication," *Physical Review Letters*, vol. 81, no. 26, pp. 5932–5935, 1998.

[55] R. Van Meter, J. Touch, and C. Horsman, "Recursive quantum repeater networks," *Progress in Informatics*, vol. 8, pp. 65–79, 2011.

[56] C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R. T. Thew, "Heralded photon amplification for quantum communication," *Physical Review A*, vol. 86, no. 2, p. 023815, 2012.

[57] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks," *New Journal of Physics*, vol. 11, no. 7, p. 075002, 2009.

[58] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," *Journal of Computer Security*, vol. 18, no. 1, pp. 61–87, 2010.

[59] S. M. Barnett and S. J. D. Phoenix, "Asynchronous quantum key distribution on a relay network," *Journal of Modern Optics*, vol. 59, no. 15, pp. 1349–1354, 2012.

[60] ——, "Securing a quantum key distribution relay network using secret sharing," in *IEEE GCC Conference and Exhibition*, 2011, pp. 143 –145.

[61] J. Capmany and C. Fernández-Pousa, "Analysis of Passive Optical Networks for Subcarrier Multiplexed Quantum Key Distribution," *IEEE Transactions on Microwave Theory and Techniques*, vol. 58, no. 11, pp. 3220–3228, 2010.

[62] S. Murshid, B. Grossman, and P. Narakorn, "Spatial domain multiplexing: A new dimension in fiber optic multiplexing," *Optics & Laser Technology*, vol. 40, no. 8, pp. 1030 – 1036, 2008.

[63] K.-I. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-speed wavelength-division multiplexing quantum key distribution system," *Optics Letters*, vol. 37, no. 2, pp. 223–225, 2012.

[64] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[65] R. J. Runser, T. E. Chapuran, P. Toliver, M. S. Goodman, J. Jackel, N. Nweke, S. R. McNown, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Demonstration of 1.3 μm Quantum Key Distribution (QKD) Compatibility with 1.5 μm Metropolitan Wavelength Division Multiplexed (WDM) Systems," in *Conference on Optical Fiber Communication (OFC)*. Optical Society of America, 2005, p. 3.

[66] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical networking for quantum key distribution and quantum communications," *New Journal of Physics*, vol. 11, no. 10, p. 105001, 2009.

[67] T. Xia, D. Chen, G. Wellbrock, A. Zavriyev, A. Beal, and K. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels," in *Conference on Optical Fiber Communication (OFC)*, 2006, p. 3.

[68] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New Journal of Physics*, vol. 11, no. 4, p. 045012, 2009.

[69] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[70] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New Journal of Physics*, vol. 12, no. 10, p. 103042, 2010.

[71] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Physical Review X*, vol. 2, no. 4, p. 041010, 2012.

[72] P. Jouguet, S. Kunz-Jacques, R. Kumar, H. Qin, R. Gabet, E. Diamanti, and R. Alleaume, "Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel," in *3rd Annual Conference on Quantum Cryptography (QCRYPT)*, 2013.

[73] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, pp. 051 123–051 123–4, 2014.

[74] P. Toliver, R. Runser, T. Chapuran, S. McNown, M. Goodman, J. Jackel, R. Hughes, C. Peterson, K. McCabe, J. Nordholt, K. Tyagi, P. Hiskett, and N. Dallman, "Impact of spontaneous anti-Stokes Raman scattering on QKD+DWDM networking," in *IEEE Lasers and Electro-Optics Society (LEOS)*, vol. 2, 2004, pp. 491–492.

[75] D. Subacius, A. Zavriyev, and A. Trifonov, "Backscattering limitation for fiber-optic quantum key distribution systems," *Applied Physics Letters*, vol. 86, no. 1, p. 011103, 2005.

[76] N. Nweke, P. Toliver, R. Runser, S. McNown, T. Chapuran, M. Goodman, R. Hughes, C. Peterson, K. McCabe, J. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Experimental characterization of wavelength separation for "QKD+WDM" co-existence," in *Conference on Lasers and Electro-Optics (CLEO)*, vol. 2, 2005, pp. 1503 – 1505.

[77] H. Rohde, S. Smolorz, A. Poppe, and H. Huebel, "Quantum key distribution integrated into commercial WDM systems," in *Conference on Optical Fiber Communication (OFC)*, 2008, pp. 1–3.

[78] P. Kumavor, A. Beal, E. Donkor, and B. Wang, "Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture," *Lightwave Technology, Journal of*, vol. 24, no. 8, pp. 3103 –3106, 2006.

[79] P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, "Design of quantum cryptography systems for passive optical networks," *Electronics Letters*, vol. 30, no. 22, pp. 1875–1877, 1994.

[80] P. D. Townsend, "Secure communications on passive optical networks using quantum cryptography," in *European Conference on Optical Communication (ECOC)*, vol. 3, 1996, pp. 35–38 vol.3.

[81] ——, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, no. 6611, pp. 47–49, 1997.

[82] T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, "'Circular type' quantum key distribution," *IEEE Photonics Technology Letters*, vol. 14, no. 4, pp. 576 –578, 2002.

[83] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, Y. Nambu, and A. Tomita, "Recent Progress in Quantum Key Distribution Network Technologies," in *European Conference on Optical Communication (ECOC)*, 2006, pp. 1 –3.

[84] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, "Field Experiment on a Star Type Metropolitan Quantum Key Distribution Network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575 –577, 2009.

[85] J. Bogdanski, N. Rafiei, and M. Bourennane, "Multiuser quantum key distribution over telecom fiber networks," *Optics Communications*, vol. 282, no. 2, pp. 258 – 262, 2009.

[86] J. Capmany and C. R. Fernandez-Pousa, "Optimum design for BB84 quantum key distribution in tree-type passive optical networks," *Journal of the Optical Society of America B*, vol. 27, no. 6, pp. A146–A151, 2010.

[87] P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, R. J. Hughes, C. G. Peterson, D. Derkacs, J. E. Nordholt, L. Mercer, S. McNown, A. Goldman, and J. Blake, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photonics Technology Letters*, vol. 15, no. 11, pp. 1669–1671, 2003.

[88] T. Honjo, K. Inoue, A. Sahara, E. Yamazaki, and H. Takahashi, "Quantum key distribution experiment through a PLC matrix switch," *Optics Communications*, vol. 263, pp. 120–123, 2006.

[89] L. Ma, A. Mink, H. Xu, O. Slattery, and X. Tang, "Experimental demonstration of an active quantum key distribution network with over gbps clock synchronization," *IEEE Communications Letters*, vol. 11, no. 12, pp. 1019 –1021, 2007.

[90] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, vol. 18, no. 26, pp. 27 217–27 225, 2010.

[91] M. Goodman, P. Toliver, R. Runser, T. Chapuran, J. Jackel, R. Hughes, C. Peterson, K. McCabe, J. Nordholt, K. Tyagi, P. Hiskett, S. McNown, N. Nweke, J. Blake, L. Mercer, and H. Dardy, "Quantum cryptography for optical networks: a systems perspective," in *16th Annual Meeting of the IEEE Lasers and Electro-Optics Society (LEOS)*, vol. 2, 2003, pp. 1040 – 1041.

[92] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Field test of wavelength-saving quantum key distribution network," *Optics Letters*, vol. 35, no. 14, pp. 2454–2456, 2010.

[93] L. Tian and H. Wang, "Optical wavelength conversion of quantum states with optomechanics," *Physical Review A*, vol. 82, no. 5, p. 053806, 2010.

[94] X. Fernandez-Gonzalvo, G. Corrielli, B. Albrecht, M. Grimau, M. Cristiani, and H. de Riedmatten, "Quantum frequency conversion of quantum memory compatible photons to telecommunication wavelengths," *Optics Express*, vol. 21, no. 17, pp. 19 473–19 487, 2013.

[95] J. C. Garcia-Escartin and P. Chamorro-Posada, "Delayed Commutation in Quantum Computer Networks," *Physical Review Letters*, vol. 97, no. 11, p. 110502, 2006.

[96] K. Lemr, K. Bartkiewicz, A. Černoch, and J. Soubusta, "Resource-efficient linear-optical quantum router," *Physical Review A*, vol. 87, no. 6, p. 062333, 2013.

[97] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Transactions on Communications*, vol. 60, no. 10, pp. 3071–3079, 2012.

[98] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for Quantum Key Distribution Networks Integrated With Optical Communication Networks," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 15, no. 6, pp. 1591–1601, 2009.

[99] C. Elliot, "Building the quantum network," *New Journal of Physics*, vol. 4, no. 1, pp. 46.1–46.12, 2002.

[100] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," 2005. [Online]. Available: arXiv:0503058[quant-ph]

[101] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[102] A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," *Journal of the Optical Society of America B*, vol. 27, no. 6, pp. A185–A188, 2010.

[103] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. Dynes, A. Dixon, A. Sharpe, Z. Yuan, A. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[104] K.-I. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in Photonic Networks: Threats and Security Enhancement," *Lightwave Technology, Journal of*, vol. 29, no. 21, pp. 3210–3222, 2011.

[105] A. Morrow, D. Hayford, and M. Legre, "Battelle QKD test bed," in *IEEE Conference on Technologies for Homeland Security (HST)*, 2012, pp. 162–166.

[106] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," 2013. [Online]. Available: arXiv:1305.0305[quant-ph]

[107] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441–442, 2014.

[108] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, "Quantum Cryptography Over Underground Optical Fibers," in *Advances in Cryptology — Proceedings of Crypto '96*. Springer – Verlag, 1996, pp. 329–342.

[109] C. Holloway, E. Meyer-Scott, C. Erven, and T. Jennewein, "Quantum entanglement distribution with 810 nm photons through active telecommunication fibers," *Optics Express*, vol. 19, no. 21, pp. 20 597–20 603, 2011.

[110] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," *Optics Express*, vol. 20, no. 15, pp. 16 339–16 347, 2012.

[111] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of Long-Distance Quantum Key Distribution Over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area," *Lightwave Technology, Journal of*, vol. 32, no. 1, pp. 141–151, 2014.

[112] D. Lancho, J. Martínez, D. Elkouss, M. Soto, and V. Martín, "QKD in Standard Optical Telecommunications Networks," in *1st International Conference on Quantum Communication and Quantum Networking (QuantumCom)*, vol. 36, 2010, pp. 142–149.

[113] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New Journal of Physics*, vol. 13, no. 6, p. 063039, 2011.

[114] B. Frohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, 2013.

[115] S. Aleksic, D. Winkler, A. Poppe, G. Franzl, B. Schrenk, and F. Hipp, "Distribution of Quantum Keys in Optically Transparent Networks: Perspectives, Limitations and Challenges," in *15th International Conference on Transparent Optical Networks (ICTON)*, 2013.

[116] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," *Optics Express*, vol. 18, no. 9, pp. 9600–9612, 2010.

[117] G. Brassard, F. Bussieres, N. Godbout, and S. Lacroix, "Entanglement and Wavelength Division Multiplexing for Quantum

Cryptography Networks," *Aip Conference Proceedings*, vol. 734, no. 1, pp. 323–326, 2004.

[118] J. Ghalbouni, I. Agha, R. Frey, E. Diamanti, and I. Zaquine, "Experimental wavelength-division-multiplexed photon-pair distribution," *Optics Letters*, vol. 38, no. 1, pp. 34–36, 2013.

[119] I. Herbauts, B. Blauensteiner, A. Poppe, T. Jennewein, and H. Hübel, "Demonstration of active routing of entanglement in a multiuser network," *Optics Express*, vol. 21, no. 23, pp. 29 013–29 024, 2013.

[120] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin*, vol. 54, no. 17, pp. 2991–2997, 2009.

[121] C. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[122] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Physical Review Letters*, vol. 106, no. 11, p. 110506, 2011.

[123] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[124] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Review of Modern Physics*, vol. 81, pp. 1301–1350, 2009.

[125] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, pp. 441–444, 2000.

[126] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences, 2004.

[127] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, pp. 1330–1333, 2000.

[128] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photonics*, vol. 3, no. 12, pp. 696–705, 2009.

[129] A. Sarkar, M. Islam, and M. Mostafa, "Performance of an optical wideband WDM system considering stimulated Raman

scattering, fiber attenuation and chromatic dispersion," *Optical and Quantum Electronics*, vol. 39, no. 8, pp. 659–675, 2007.

[130] P. D. Townsend, "Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems," *IEEE Photonics Technology Letters*, vol. 10, no. 7, pp. 1048–1050, jul 1998.

[131] J. AuYeung and A. Yariv, "Spontaneous and stimulated Raman scattering in long low loss fibers," *Quantum Electronics, IEEE Journal of*, vol. 14, no. 5, pp. 347 – 352, 1978.

[132] Q. Lin and G. P. Agrawal, "Raman response function for silica fibers," *Optics Letters*, vol. 31, no. 21, pp. 3086–3088, 2006.

[133] H. Kawahara, A. Medhipour, and K. Inoue, "Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel ," *Optics Communications*, vol. 284, no. 2, pp. 691 – 696, 2011.

[134] S. Aleksic, D. Winkler, F. Hipp, A. Poppe, G. Franzl, and B. Schrenk, "Towards a smooth integration of quantum key distribution in metro networks," in *16th International Conference on Transparent Optical Networks (ICTON)*, 2014.

[135] H. Yoshimura, K.-I. Sato, and N. Takachio, "Future photonic transport networks based on WDM technologies," *Communications Magazine, IEEE*, vol. 37, no. 2, pp. 74 –81, 1999.

[136] Recommendation G.694.2, *Spectral grids for WDM applications: CWDM frequency grid*. ITU-T, 2003.

[137] C. A. Brackett, "Dense wavelength division multiplexing networks: principles and applications," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 6, pp. 948–964, 1990.

[138] Recommendation G.694.1, *Spectral grids for WDM applications: DWDM frequency grid*. ITU-T, 2002.

[139] T. Ohara, H. Takara, T. Yamamoto, H. Masuda, T. Morioka, M. Abe, and H. Takahashi, "Over-1000-channel ultradense WDM transmission with supercontinuum multicarrier source," *Lightwave Technology, Journal of*, vol. 24, no. 6, pp. 2311–2317, 2006.

[140] R. Ramaswami, K. Sivarajan, and G. Sasaki, *Optical Networks: A Practical Perspective*, 3rd ed. Morgan Kaufmann Publishers Inc., 2009.

[141] K. O. Hill, D. C. Johnson, B. S. Kawasaki, and R. I. MacDonald, "CW three-wave mixing in single-mode optical fibers," *Journal of Applied Physics*, vol. 49, pp. 5098–5106, 1978.

[142] R. W. Tkach, A. R. Chraplyvy, F. Forghieri, A. H. Gnauck, and R. M. Derosier, "Four-photon mixing and high-speed WDM systems," *Lightwave Technology, Journal of*, vol. 13, no. 5, pp. 841–849, 1995.

[143] N. Shibata, R. Braun, and R. Waarts, "Phase-mismatch dependence of efficiency of wave generation through four-wave mixing in a single-mode optical fiber," *Quantum Electronics, IEEE Journal of*, vol. 23, no. 7, pp. 1205–1210, 1987.

[144] A. Chraplyvy, "Limitations on lightwave communications imposed by optical-fiber nonlinearities," *Lightwave Technology, Journal of*, vol. 8, no. 10, pp. 1548–1557, 1990.

[145] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, "Photon level crosstalk between parallel fibers installed in urban area," *Optics Express*, vol. 18, no. 21, pp. 22 199–22 207, 2010.

[146] J. Senior, *Optical Fiber Communications: Principles and Practice*, 3rd ed. Prentice Hall, 2008.

[147] S.-J. Park, C.-H. Lee, K.-T. Jeong, H.-J. Park, J.-G. Ahn, and K.-H. Song, "Fiber-to-the-home services based on wavelength-division-multiplexing passive optical network," *Lightwave Technology, Journal of*, vol. 22, no. 11, pp. 2582–2591, 2004.

[148] C.-H. Lee, W. V. Sorin, and B. Y. Kim, "Fiber to the Home Using a PON Infrastructure," *Lightwave Technology, Journal of*, vol. 24, no. 12, pp. 4568–4583, 2006.

[149] K. Twist, "Driving fibre closer to the home," *Nature Photonics*, vol. 1, no. 3, pp. 149–150, 2007.

[150] Y. Chen, M. T. Fatehi, H. J. La Roche, J. Z. Larsen, and B. L. Nelson, "Metro optical networking," *Bell Labs Technical Journal*, vol. 4, no. 1, pp. 163–186, 1999.

[151] IEEE, *IEEE standard for local and metropolitan area networks: overview and architecture*. IEEE, 2002.

[152] M. Maier, "WDM Passive Optical Networks and Beyond: the Road Ahead," *Journal of Optical Communications and Networking*, vol. 1, no. 4, pp. C1–C16, 2009.

[153] A. Dutta, N. Dutta, and M. Fujiwara, *WDM Technologies: Passive Optical Components*, ser. Optics and Photonics Series. Elsevier Science, 2003.

[154] *Gigabit-capable passive optical networks (GPON): General characteristics*, ITU-T Std. G.984.1, 2008.

[155] *Ethernet in the first mile*, IEEE Std. 802.3ah, 2004.

[156] *10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, Abbreviations, and Acronyms*, ITU-T Std. G.987, 2010.

[157] *Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks*, IEEE Std. 802.3av, 2009.

[158] K. Takada, M. Abe, M. Shibata, M. Ishii, and K. Okamoto, "Low-crosstalk 10-GHz-spaced 512-channel arrayed-waveguide grating multi/demultiplexer fabricated on a 4-in wafer," *IEEE Photonics Technology Letters*, vol. 13, no. 11, pp. 1182–1184, 2001.

[159] Y. Luo, X. Zhou, F. Effenberger, X. Yan, G. Peng, Y. Qian, and Y. Ma, "Time-and Wavelength-Division Multiplexed Passive Optical Network (TWDM-PON) for Next-Generation PON Stage 2 (NG-PON2)," *Lightwave Technology, Journal of*, vol. 31, no. 4, pp. 587–593, 2013.

[160] E. Basch, R. Egorov, S. Gringeri, and S. Elby, "Architectural tradeoffs for reconfigurable dense wavelength-division multiplexing systems," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 12, no. 4, pp. 615 –626, 2006.

[161] T. Strasser and J. Wagener, "Wavelength-Selective Switches for ROADM Applications," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 16, no. 5, pp. 1150 –1157, 2010.

[162] Y. Li, L. Gao, G. Shen, and L. Peng, "Impact of ROADM colorless, directionless, and contentionless (CDC) features on optical network performance [Invited]," *Optical Communications and Networking, IEEE/OSA Journal of*, vol. 4, no. 11, pp. B58–B67, 2012.

[163] R.-B. Jin, R. Shimizu, K. Wakui, H. Benichi, and M. Sasaki, "Widely tunable single photon source with high purity at telecom wavelength," *Optics Express*, vol. 21, no. 9, pp. 10 659–10 666, 2013.

[164] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[165] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[166] H. C. Lim, A. Yoshizawa, H. Tsuchida, and K. Kikuchi, "Wavelength-multiplexed entanglement distribution," *Optical Fiber Technology*, vol. 16, no. 4, pp. 225–235, 2010.

[167] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key Reconciliation for High Performance Quantum Key Distribution," *Scientific Reports*, vol. 3, no. 1576, pp. 1–6, 2013.

[168] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, "Heralded noiseless amplification of a photon polarization qubit," *Nature Physics*, vol. 9, no. 1, pp. 23–28, 2013.

[169] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier," *Physical Review Letters*, vol. 105, no. 7, p. 070501, 2010.

[170] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, "Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier," *Physical Review A*, vol. 86, no. 1, p. 012327, 2012.

[171] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413–418, 2001.

[172] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, "Experimental demonstration of a BDCZ quantum repeater node," *Nature*, vol. 454, no. 7208, pp. 1098–1101, 2008.

[173] K. Azuma, K. Tamaki, and H.-K. Lo, "All photonic quantum repeaters," 2013. [Online]. Available: arXiv:1309.7207[quant-ph]

[174] N. Cai and T. Chan, "Theory of Secure Network Coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 421–437, 2011.

[175] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 5, pp. 1204–1216, 2000.

[176] A. E. Kamal, A. Ramamoorthy, L. Long, and L. Shizheng, "Overlay Protection Against Link Failures Using Network Coding," *IEEE/ACM Transactions on Networking*, vol. 19, no. 4, pp. 1071–1084, 2011.

[177] E. D. Manley, J. S. Deogun, L. Xu, and D. R. Alexander, "All-Optical Network Coding," *Journal of Optical Communications and Networking*, vol. 2, no. 4, pp. 175–191, 2010.

[178] K. Fouli, M. Maier, and M. Medard, "Network coding in next-generation passive optical networks," *IEEE Communications Magazine*, vol. 49, no. 9, pp. 38–46, 2011.

[179] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 1991.

[180] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly Secure Message Transmission," *Journal of the ACM*, vol. 40, pp. 17–47, 1993.

[181] T. Chan and A. Grant, "Capacity Bounds for Secure Network Coding," in *Proceedings of Communications Theory Workshop*, 2008, pp. 94–100.

[182] F. Saliou, P. Chanclou, F. Laurent, N. Genay, J. Lazaro, F. Bonada, and J. Prat, "Reach extension strategies for passive optical networks [invited]," *Optical Communications and Networking, IEEE/OSA Journal of*, vol. 1, no. 4, pp. C51–C60, 2009.

[183] D. Lavery, M. Ionescu, S. Makovejs, E. Torrengo, and S. J. Savory, "A long-reach ultra-dense 10 Gbit/s WDM-PON using a digital coherent receiver," *Optics Express*, vol. 18, no. 25, pp. 25 855–25 860, 2010.

[184] B. Collings, "New devices enabling software-defined optical networks," *Communications Magazine, IEEE*, vol. 51, no. 3, pp. 66–71, 2013.

ACRONYMS

AWG Arrayed Waveguide Grating

BB84 Bennett Brassard 1984

BER Bit Error Rate

BES Broadband Entanglement-Source

CDC-ROADM Colorless, Directionless and Contentionless Reconfigurable Optical Add Drop Multiplexer

CH Channel

CO Central Office

COW Coherent One Way

CVQKD Continuous Variables Quantum Key Distribution

CW Continuous Wave

CWDM Coarse Wavelength Division Multiplexing

DPS-QKD Differential Phase Shift Quantum Key Distribution

DTV Digital Television

DWDM Dense Wavelength Division Multiplexing

E91 Ekert 1991

EDFA Erbium Doped Fiber Amplifier

EPON Ethernet-Capable Passive Optical Network

FBG Fiber Bragg Gratings

FWM Four Wave Mixing

GPON Gigabit-Capable Passive Optical Network

MON Metropolitan Optical Network

NC Network Component

OADM Optical Add Drop Multiplexer

OLT Optical Line Terminator

ONT Optical Network Terminator

ONU Optical Network Unit

OSA Optical Spectrum Analyzer

OTP One Time Pad

PON Passive Optical Network

PPLN Periodically Poled Lithium Niobate

PXC Photonic Cross Connect

QBER Quantum Bit Error Rate

QKD Quantum Key Distribution

QKD-MON Quantum Metropolitan Optical Network

ROADM Reconfigurable Optical Add Drop Multiplexer

RSA Rivest, Shamir y Adleman

SFP Small Form-Factor Pluggable Transceiver

SNR Signal to Noise Ratio

SPD Single Photon Detector

TDM Time Division Multiplexing

TDM-PON Time Division Multiplexing Passive Optical Network

WDM Wavelength Division Multiplexing

WDM-PON Wavelength Division Multiplexing Passive Optical Network

WTR Weakly Trusted Repeater

WSS Wavelength Selective Switch