Quantum metropolitan optical network based on wavelength division multiplexing

A. Ciurana,[1] J. Martínez-Mateo,[1] M. Peev,[2] A. Poppe,[2] N. Walenta,[3] H. Zbinden,[3] and V. Martín[1,*]

[1] *Research Group on Quantum Information and Computation, Universidad Politécnica de Madrid, Spain*

[2] *Optical Quantum Technology, Safety & Security Department, AIT Austrian Institute of Technology GmbH, Austria*

[3] *Group of Applied Physics, Université de Genéve, Switzerland*

[*] *vicente@fi.upm.es*

Abstract: Quantum Key Distribution (QKD) is maturing quickly. However, the current approaches to its application in optical networks make it an expensive technology. QKD networks deployed to date are designed as a collection of point-to-point, dedicated QKD links where non-neighboring nodes communicate using the trusted repeater paradigm. We propose a novel optical network model in which QKD systems share the communication infrastructure by wavelength multiplexing their quantum and classical signals. The routing is done using optical components within a metropolitan area which allows for a dynamically any-to-any communication scheme. Moreover, it resembles a commercial telecom network, takes advantage of existing infrastructure and utilizes commercial components, allowing for an easy, cost-effective and reliable deployment.

OCIS codes: (060.5565) Quantum communications; (270.5568) Quantum cryptography; (060.4265) Networks, wavelength routing.

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys **74**, 145–195 (2002).
2. ID Quantique SA, http://www.idquantique.com.
3. Toshiba Research Europe Ltd., http://www.toshiba-europe.com/research/.
4. MagiQ Technologies Inc., http://www.magiqtech.com.
5. SeQureNet, http://www.sequrenet.com.
6. AIT, http://www.ait.ac.at/epr.
7. Swiss Quantum, http://swissquantum.idquantique.com.
8. A. Mirza and P. Petruccione, "Realizing long-term quantum cryptography," J. Opt. Soc. Am. B **27**, A185–A188 (2010).
9. 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," Opt. Express **20**, 14030–14041 (2012).
10. C. Elliot, "Building the quantum network," New J. Phys. **4**, 46 (2002).
11. 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,

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

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 J. Phys. **11**, 075001 (2009).
12. 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 J. Phys. **13**, 123001 (2011).
13. 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. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. 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," Opt. Express **19**, 10387–10409 (2011).
14. K. 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," J. Lightwave Technol. **29**, 3210–3222 (2011).
15. Y. Chen, M. T. Fatehi, H. J. La Roche, J. Z. Larsen, and B. L. Nelson, "Metro optical networking," Bell Labs Tech. J. **4**, 163–186 (1999).
16. C.-H. Lee, W. V. Sorin, and B. Y. Kim, "Fiber to the home using a PON infrastructure," J. Lightwave Technol. **24**, 4568–4583 (2006).
17. P. Townsend, S. Phoenix, K. Blow, and S. Barnett, "Design of quantum cryptography systems for passive optical networks," Electron. Lett. **30**, 1875–1877 (1994).
18. P. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature **385**, 47–49 (1997).
19. P. Townsend, "Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems," IEEE Photonics Technol. Lett. **10**, 1048–1050 (1998).
20. D. Kumavor, C. Beal, S. Yelin, E. Donkor, and C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," J. Lightwave Technol. **23**, 268–276 (2005).
21. 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," IEEE J. Quantum Electron. **43**, 130–138 (2007).
22. W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for quantum key distribution networks integrated with optical communication networks," IEEE J. Sel. Top. Quantum Electron. **15**, 1591–1601 (2009).
23. D. Lancho, J. Martínez, D. Elkouss, M. Soto, and V. Martín, "QKD in standard optical telecommunications networks," in *1st Int. Conf. on Quantum Communication and Quantum Networking* (ICST, 2010), pp. 142–149.
24. I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," Opt. Express **18**, 9600–9612 (2010).
25. J. Capmany and C. Fernández-Pousa, "Analysis of passive optical networks for subcarrier multiplexed quantum key distribution," IEEE Trans. Microwave Theory Tech. **58**, 3220–3228 (2010).
26. I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," New J. Phys. **13**, 063039 (2011).
27. M. Razavi, "Multiple-access quantum key distribution networks," IEEE Trans. Commun. **60**, 3071–3079 (2012).
28. 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," Opt. Express **16**, 18790–18979 (2008).
29. 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," Nat. Photon. **1**, 1749–4885 (2007).
30. 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 J. Phys. **11**, 075003 (2009).
31. S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. **37**, 1008–1010 (2012).
32. 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," Opt. Express **19**, 10632–10639 (2011).
33. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photon. **7**, 378–381 (2013).
34. A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, "Fully automated entanglement-based quantum cryptography system for telecom fiber networks," New J. Phys. **11**, 045013 (2009).
35. Recommendation ITU-T G.694.2, Spectral grids for WDM applications: CWDM frequency grid (2003).
36. Recommendation ITU-T G.694.1, Spectral grids for WDM applications: DWDM frequency grid (2012).
37. C. A. Brackett, "Dense wavelength division multiplexing networks: principles and applications," IEEE J. Sel. Areas Commun. **8**, 948–964 (1990).

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

38. P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," Electron. Lett. **33**, 188–190 (1997).
39. 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 *Optical Fiber Communication Conf.* (IEEE, 2006), p. 3.
40. H. Rohde, S. Smolorz, A. Poppe, and H. Huebel, "Quantum key distribution integrated into commercial WDM systems," in *Optical Fiber Communication Conf.* (IEEE, 2008), pp. 1–3.
41. 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 J. Phys. **11**, 105001 (2009).
42. B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through dense wavelength division multiplexing network," New J. Phys. **12**, 18 (2010).
43. 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 J. Phys. **11**, 045012 (2009).
44. P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New J. Phys. **12**, 063027 (2010).
45. 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," Phys. Rev. X **2**, 041010 (2012).
46. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
47. IEEE, IEEE standard for local and metropolitan area networks: overview and architecture (2002).
48. 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," J. Lightwave Technol. **24**, 2311–2317 (2006).
49. R. Ramaswami, K. Sivarajan, and G. Sasaki, *Optical Networks: A Practical Perspective*, 3rd ed. (Morgan Kaufmann, 2009).
50. 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," J. Lightwave Technol. **22**, 2582–2591 (2004).
51. B. Korzh, N. Walenta, R. Houlmann, and H. Zbinden, "A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator," Opt. Express **21**, 19579–19592 (2013).
52. H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932–5935 (1998).
53. L. Tian and H. Wang, "Optical wavelength conversion of quantum states with optomechanics," Phys. Rev. A **82**, 053806 (2010).
54. C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R. T. Thew, "Heralded photon amplification for quantum communication," Phys. Rev. A **86**, 023815 (2012).
55. 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. Dallmann, "Impact of spontaneous anti-Stokes Raman scattering on QKD+DWDM networking," in *17th Annual Meeting of the IEEE Lasers and Electro-Optics Society* (IEEE, 2004), pp. 491–492.
56. R. Runser, T. Chapuran, P. Toliver, M. Goodman, and J. Jackel, "Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems," in *Optical Fiber Communication Conf.* (IEEE, 2005), p. 3.
57. 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," Opt. Express **17**, 13326–13334 (2009).
58. J. 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," Proc. SPIE **7681**, 76810Z (2010).
59. N. Walenta, "Concepts, components and implementations for quantum key distribution over optical fibers," Ph.D. thesis, Faculté des Sciences de l'Université de Genève (2012).
60. D. Subacius, A. Zavriyev, and A. Trifonov, "Backscattering limitation for fiber-optic quantum key distribution systems," Appl. Phys. Lett. **86**, 011103 (2005).
61. Corning: SMF-28e+ LL optical fiber, http://www.corning.com/.
62. Flyin Optronics: splitter, circulators, CWDM filters and 1310/1550 WDM multiplexers, http://www.flyinoptronics.com/.
63. Polatis: optical switch Series 6000, http://www.polatis.com/datasheets/series-6000-192x192-low-loss-optical-switch.pdf.
64. LG Nortel WPF 1132C (32-channels AWG).
65. V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," Phys. Rev. Lett. **100**, 200501 (2008).

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

1. Introduction

Quantum key distribution allows two distant parties to grow a secret key: an initial shared secret key can be made arbitrarily large while avoiding any information leakage. This is a information theoretic secure scheme based on the laws of quantum mechanics. The price to pay for such a high level of security is the usage of a symmetric key protocol with point-to-point connections [1]. Both parties have to be connected through a quantum and a classical but authenticated channel, typically implemented by dedicated optical fiber links. The technology is mature enough for commercialization [2–6], and long-term practical settings have already been tested [7–9]. However, taking this concept to a network setup results in the need to use a completely separated optical infrastructure for QKD [10–14] which considerably increases its cost. Sharing an already deployed network and as much commercial technology as possible is then a must for the widespread adoption of QKD as a mainstream security technology.

Nowadays, most telecom networks have adopted the optical paradigm [15]. The use of passive optical technology is attracting interest in these networks since the absence of active components in the optical pathway, such as amplifiers or electro-optical converters, allows for a more robust and reliable network [16]—albeit at the cost of some flexibility. From the quantum perspective this means that a unique, uninterrupted optical path can be set between two users and then used as quantum channel, i.e. quantum states can be transmitted in the network without being disrupted. Therefore, it opens the way for integrating QKD systems in commercial telecom networks; this has been a recurring issue in the last years [17–27]. It should be further mentioned that the discussed technology is mainly found in networks up to a metropolitan area scale (e.g. access networks and metro backbones), which in turn are the perfect market for QKD: they serve final users and the losses are compatible with the budget and key rate of actual QKD systems [28–34].

Furthermore, wavelength division multiplexing (WDM) [35, 36] is becoming a dominant technology in standard telecom networks. This allows to share efficiently a common optical infrastructure among multiple users [37]. Ideally, a QKD system could communicate in these networks using a dedicated wavelength (i.e. a channel) for its quantum signal. Unfortunately, the transmission of single-photon pulses in a fiber together with strong, classical signals (carrying $\approx 10^7$ photons per pulse) is disturbed by the noise generated by the latter. The coexistence of quantum and classical channels is thus limited to just a few of them [23, 38–45], especially when they operate in the same spectrum band.

The objective of this work is to devise a technologically realistic and cost-effective QKD network, able to overcome the major roadblocks in the way towards a broader acceptance of QKD technology. The network design is inspired by the technologies and topologies of commercial telecom networks in order to use existing deployed infrastructures (e.g. dark fibers) and commercial components, such that the deployment and running costs are as low as possible and remain competitive with other high security network services. To this end, QKD devices are wavelength multiplexed in order to share resources. This includes quantum and classical signals, the latter being either generated for the stabilization of the quantum channel or for other QKD purposes like key distillation or encryption. Communications between QKD devices are routed using passive optical components in contrast to trusted repeaters [11]. However, this fully passive version only works with static QKD links. In the case that an any-to-any scheme is required, optical switches must be added for dynamic routing. Finally, a network prototype based on the proposed model has been designed and deployed for testing purposes. The present approach focuses on prepare-and-measure QKD schemes that fall into two main classes according to the standard classification [46]: discrete variables QKD and distributed phase-reference pulse QKD. Its extension to other QKD schemes such as continuous variable QKD and entangled photon-pairs QKD might be possible but lies beyond the scope of the present work.

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

The paper is organized as follows. Sec. 2 reviews the architecture and principle of operation of modern metropolitan optical networks. In Sec. 3 we discuss the proposed multiplexing scheme and the modifications required on the network nodes in order to use quantum signals. A prototype of a metropolitan QKD network is described and characterized in Sec. 4. Finally, we summarize the discussion and outline some future improvements in Sec. 5.

2. Metropolitan optical network

Metropolitan networks aim to cover the area of cities, with a typical span from a few to several tens of kilometers [47]. A common architecture of a metropolitan optical network (MON) foresees a division into core and access networks, as depicted in Fig. 1. It should be noted that, actually, the design and topologies in a MON could be more elaborated due to, for instance, external constraints, limited resources, or to the growing needs of the carrier company. However, for the sake of clarity we will stick to the network architecture just outlined as a typical one, denoting it as a *canonical* MON.

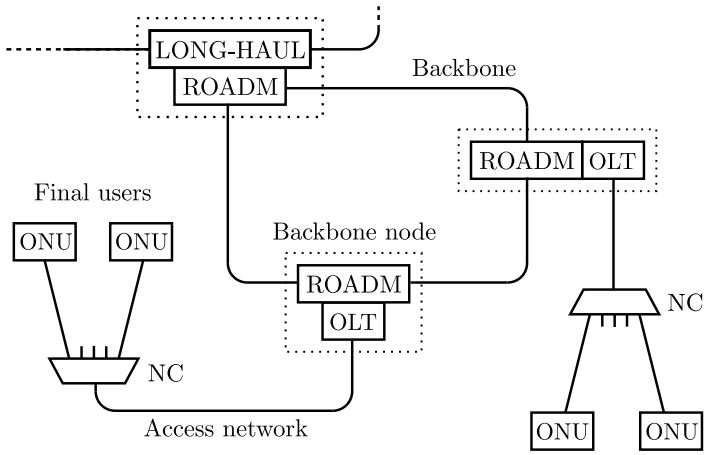

Fig. 1. Typical architecture and topology used in the *canonical* metropolitan optical network considered in this work. A core network, the backbone, with the highest capacity links set up in a ring, is connected with the final users through one-to-many passive access networks. The network component (NC, typically an splitter or multiplexing device) is usually located near the users (optical network units or ONUs) in order to minimize the amount of non-shared fiber used. The backbone uses (reconfigurable) optical add and drop modules, (R)OADM, to add or drop different signals to/from the access networks. In order to drive the access network and translate between its protocol and the one running in the core, an optical line terminator (OLT) is used. This usually means electro-optical conversion, which is disruptive for QKD. Finally, the backbone can be connected to other rings or long-haul networks.

In MONs, signals are commonly multiplexed using two well-known approaches: time-division multiplexing (TDM) and wavelength-division multiplexing (WDM). WDM has the advantage of allowing the simultaneous transmission of signals over a single fiber by using different wavelengths (channels), thus increasing the total communication bandwidth. In this work we focus only on this second approach. In addition, the wavelength will be also used to address different users over a particular path.

The standardized use of WDM defines a grid of channels, each with a central wavelength, uniformly arranged in the optical spectrum. Depending on the spectral distance between adjacent channels, WDM can be coarse WDM (CWDM) or dense WDM (DWDM). CWDM is

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

composed of 18 channels spaced from 1270 to 1610 nm and each occupying 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 100 GHz (or multiples) down to 12.5 GHz (0.8-0.1 nm) to accommodate from 40 up to hundreds of channels [48].

2.1. Access network

An access network follows a point-to-multipoint topology to connect many final users to the core using a simple fiber infrastructure of a few tens of kilometers [49]. They are typically deployed in the so-called fiber-to-the-home (FFTH) architectures with cables containing multiple optical fiber strands and using passive optical technology (i.e. passive optical networks or PON). In a PON, an optical line terminator (OLT), with direct access to the backbone, is connected through a single fiber to a network component (NC) with N outputs, which in turn is connected through a non-shared fiber to N optical network units (ONU) located at the user's premises. The NC is assumed to be close to the ONUs, thus reducing the amount of non-shared fiber used. Depending on the multiplexing technology used, communications between a particular ONU and the OLT, and vice versa, are addressed either using a specific wavelength or time slot (WDM or TDM, respectively) that differentiates it from its neighbors.

In a typical TDM-based access network (e.g. Gigabit-capable PON or GPON), a beam splitter is used as the NC to connect multiple users. This introduces 3 dB of losses each time the number of users is doubled. Hence, a network of 32 users has a minimum of 15 dB losses in the NC. Instead, in a WDM-based approach (e.g. WDM-PON), the splitter is replaced by a wavelength multiplexer. This is typically an arrayed waveguide grating (AWG), which has less insertion losses than the splitter (e.g. a 32-channels AWG has ≈ 3 dB). Moreover, losses do not grow by much when adding more channels. This allows to increase the number of users while maintaining the same overall loss budget. Another key advantage of the AWG that will be used in the present approach is its cyclic behavior: through each output port, not only a single wavelength can be used, but also its periods in the upper and lower spectrum. Despite not being standardized, the common usage is to take advantage of this characteristic and use two spectrum bands to separate downstream and upstream signals [50].

2.2. Core network: backbone

Different access networks are connected through a core network or backbone that in a MON is typically a ring. A first-level backbone is composed of M nodes covering all the metropolitan area, where each backbone node is connected to the OLT of one or more access networks. Signals within the ring are wavelength multiplexed and a (reconfigurable) optical add-drop multiplexer, (R)OADM, is used at the backbone node to add and drop different channels, i.e. add or extract wavelengths to/from the ring. The connection between core and access networks typically includes an electro-optical conversion, since the protocols and technologies can be very different. However, when the backbone and the access network are both based on optical technology and WDM, they can also be directly connected in the optical domain, thus opening the possibility to support quantum communications. This allows for a realistic network where QKD emitters can connect to different receivers (even if different QKD protocols are used [51]).

Furthermore, a ROADM can also connect the core to a long-haul network in order to reach distant networks. However, we will not consider here this scenario, since the distance in these settings exceeds the loss budget of actual QKD systems.

3. Multiplexing QKD systems in a MON

The main thrust underlying the scheme above comes from the need to reduce cost while maximizing network throughput, resiliency and flexibility. In the same spirit, we will use WDM

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

technology as a base to construct a QKD network. The creation and stabilization of a quantum channel is a challenging task that imposes strong requirements on the infrastructure. Quantum channels are easily degraded because of photon absorption or stray photons coming from classical signals in the same fiber. Moreover, technologies that could overcome these problems, like quantum repeaters, are still in their infancy [52–54]. Hence, the communication must follow a direct optical path, with always the same wavelength and within the loss budget of the QKD system.

The objective of the proposed network is to provide an easy to deploy and maintain infrastructure, supporting many non-interfering quantum channels. By sharing the infrastructure among many users, QKD becomes more price-competitive and increases its potential market share. To this end, the network is designed to use in a shared way the very costly dark fiber that is already deployed and as much commercially available optical equipment as possible. It is to be noted that, in most settings, the cost of hiring or deploying from anew a dark fiber offsets by a long margin the cost of the QKD devices themselves. To limit the interference with classical communications signals, we define in principle the QKD network only for QKD purposes, i.e. at first only quantum and *service* signals will be allowed. By service signals, we mean the classical ones used to keep the QKD devices working (interferometer stabilization, synchronization, etc.). In this first approach, a pair of QKD devices only need a quantum channel and a service channel, both directed from emitter to receiver, in order to establish a quantum link. After studying the restrictions imposed by the service channels in Sec. 4, we will discuss the possibilities of adding further channels such as the ones for the classical key distillation protocols in QKD, for cipher-text transmission, or even for purely classical communications unrelated to the purposes of the QKD equipment.

3.1. Bands structure and channel plan

In comparison with classical signals, quantum signals are extremely weak. Even with a QKD system working at a 1 GHz rate, the power difference is ≈ 70 dB. Therefore, the noise generated by classical signals drastically impedes quantum transmission by reducing their signal-to-noise ratio (SNR). In order to avoid this problem, instead of placing all signals together in the same band, we separate them spectrally as already discussed in previous works [19, 38, 41, 55, 56]. In particular, we define a *service band* at the S, C and L bands ($\approx$ 1500-1600 nm), and a *quantum band* at the O band (1260-1360 nm). The distance between channels in the same band will depend on the specific ITU grid used for the implementation. It might not seem an optimal choice to move the quantum signals to the O band since fiber losses are slightly bigger (≈ 0.1 dB/km more), but actually the main source of losses in a MON comes from components such as splitters, filters, multiplexers, switches, etc., and they are similar across the bands (see Table 1). Henceforth, we will use the optical loss as the reference value when comparing different proposals instead of the distance. Beyond having well separated wavelengths for the quantum and classical signals, the motivation behind this choice is the ability to use existing DWDM commercial equipment for the classical service signals, which is backed by a mature industry. For example, a possible implementation of the schema could use standard and readily available small form-factor pluggable transceivers for the classical signals in the DWDM 100 GHz grid in the C band that simply do not exist in the O band. These would be very expensive to commercially manufacture without the high market demand that drove the development in the C band. At the same time, the manufacturing of QKD equipment can be carried out in the O band as it is in the C band. QKD components such as single-photon detectors [2] or adequate lasers for the attenuated single photon sources with similar performance exist in both bands. Of course, the opposite choice: classical signals in the O Band and quantum in the C could be possible and it is just a straightforward modification of the proposed network, but we think that the cost of the

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

equipment would favor the present choice in most designs. On the other hand, since putting the quantum channel in the O band introduces more losses, the measurements in the present paper could be considered, from a secret key-rate performance perspective, as a worst case between the two possible choices.

We will assume a MON where QKD systems are placed at the access networks end-user nodes, as if they were ONUs. In order to distribute the channels among them, we slice the quantum and service band in as many AWG-periodic subbands as there are access networks, and then we assign a pair of quantum and service subbands to each access network. In this way, each QKD device from a QKD system (emitter or receiver) gets a quantum channel and its AWG-periodic service channel. This means that a pair of QKD devices will have available four channels (two in each direction) to run the QKD protocol, although not all are used in our first approach for the service channels. Figure 2(a) shows the schematic spectrum resulting from this approach. Therefore, the selection of a certain pair of wavelengths by a QKD device will also select a specific access network and, within that network, a specific QKD device. This addressing mechanism also allows an easy filtering of unwanted signals at the receivers side.

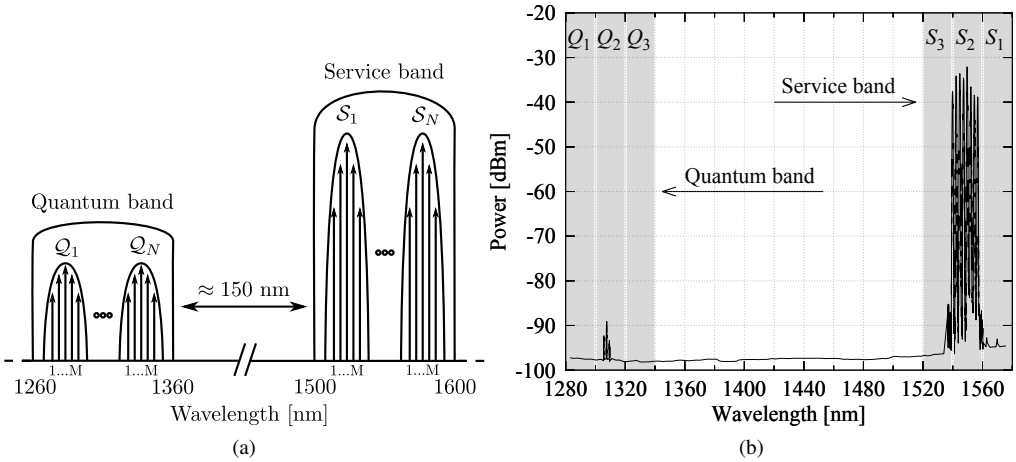

Fig. 2. (a) Spectrum of the proposed wavelength-multiplexing scheme. The spectrum is divided in two bands, quantum and service, separated well enough to minimize noise in the quantum band. The first band is located in the O band (13xx) and is used to transport the quantum channel. The second, mainly at the C band (15xx), carries the *service* channels needed to keep the quantum channel and cryptographic protocol working. Each of the two bands is divided in N subbands, named here $Q_{1...N}$ and $S_{1...N}$, for quantum and service, respectively. A pair of quantum and service subbands will correspond to an access network. Each subband carries M channels, represented here as arrows. Channels are chosen in an ITU grid and periods of the AWG. Subbands are selected such that the corresponding wavelengths in the quantum and service band are in the same period, hence both will come out together in the same AWG port. (b) Experimental spectrum of the network prototype. To check the behavior of the network prototype, two signals were fed into the quantum and service subbands Q2 and S2. The subband structure is clearly seen. The different number of channels seen in both bands are due to the input signals used for the test. For a complete description, see Sec. 4.

The pairs of quantum and service channels must be routed identically to the same device. To this end, we take advantage of the cyclic behavior of the AWG. For our experimental test bed, we have characterized the periodicity of a standard, telecommunication grade, 100 GHz 32-channels AWG using three tunable lasers to cover the whole 1260-1620 nm range. A given

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

wavelength was fed to the common port and an optical spectrum analyzer was used to measure the output port. In Fig. 3 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 that separates the quantum from the classical signals and is not used in the proposal. The figure clearly shows the periodicity used to route the corresponding pairs of quantum and service bands to the same destination. We define as a *periodic set* the set of channels that can be used through each output port of the AWG.

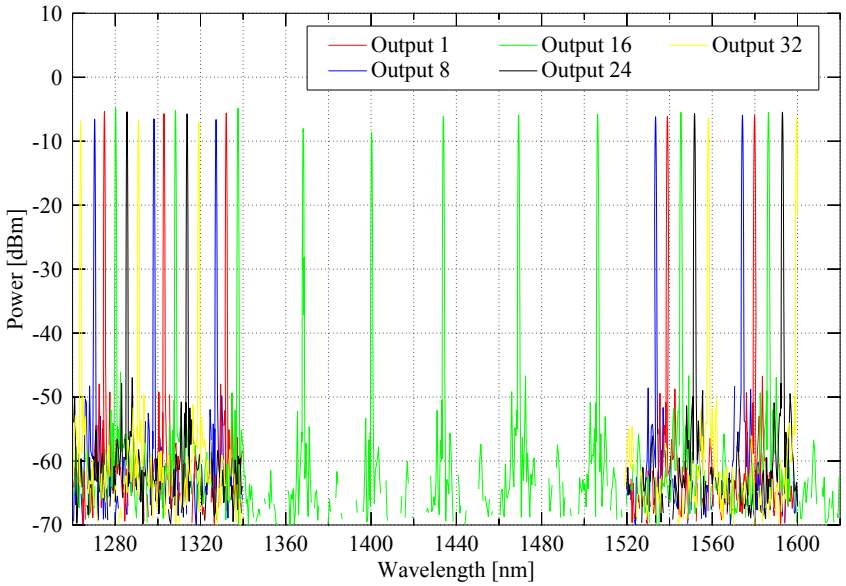

Fig. 3. Experimental data of the cyclic behavior of a 100 GHz 32-channels AWG, as the one used in the network prototype, in the range 1250-1620 nm. Only outputs 1, 8, 16, 24 and 32 are shown, and only output 16 is presented over the whole range. Channels from the same periodic set have the same color.

3.2. Simplified network

Using this approach, it is straightforward to build a simplified two access networks MON, as depicted in Fig. 4. In this case, the backbone is just a fiber running from one access network to the other. A wavelength tunable QKD emitter —one that can use any channel in the quantum band and the corresponding periodic one for the service band— located behind one of the AWGs could address any QKD receiver located in the other AWG just by changing the pair of wavelengths, and vice versa. The AWG imposes that both QKD devices must be connected to the same output port of their respective AWGs, since ports only allow to pass wavelengths in the same periodic set. This is easily solved by adding an $M \times M$ switch in front of the emitter's AWG. This switch is the only active element in the network. On the other hand, optical switches do not spoil the quantum signal and have very low losses. With this modification, the network is an all-to-all, wavelength addressable and dynamically reconfigurable network, since any QKD emitter can communicate with any receiver at any time by using the appropriate channel and setting the switch accordingly. This network is, however, directional; all emitters have to be located in one access network and all the receivers in the other. If a switch is also added to the

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

receiver's side AWG, this limitation no longer exists and QKD emitters/receivers can be freely mixed and located at any port of any of the two access networks.

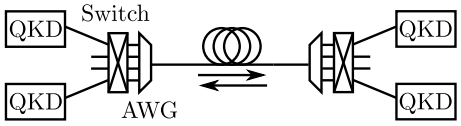

Fig. 4. Simplified network with two WDM-PON access networks. Only one switch is actually needed to allow a wavelength tunable QKD emitter to use any port of the AWG, and thus communicate in an all to all configuration with any receiver on the other AWG. If a switch is used on each side, as depicted, then emitters and receivers can be freely mixed in both access networks. See text.

3.3. Backbone nodes and full QKD-MON

In order to extend this network to a realistic MON, we have to be able to connect more than two access networks. As described in Sec. 2, this is done in classical communications using (R)OADMs. In our case, we would need special OADMs able to add and drop simultaneously pairs of bands located in different parts of the spectrum. This has to be done for any subband and in the appropriate periodical sets, introducing the minimal amount of losses as possible and without disrupting the quantum channel. Commercial equipment is not designed to do this, hence we need to devise a dedicated one.

There are several possible designs that can be adapted to different scenarios. Here we adopt a particular one (see Fig. 5) that has low losses and that is easy, reliable and cheap to build. All components used are standard and commercially available, thus able to pass the quality and availability tests required in a real-world deployment. They are also passive. In addition to the already mentioned benefits, the use of passive components in the OADMs has a clear advantage: all paths are always available and no action is required by an external participant to switch between them. As it can be seen in the figure, when the signals enter the OADM, two band-pass filters drop the quantum and service subbands assigned to the access network through the filtered port. These subbands are routed downstream using circulators and they are coupled using a 1310/1550 WDM multiplexer before they reach the AWG in the access network. In the upstream direction, a 1310/1550 WDM mux separates the signal into quantum and service bands. 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 injected into the ring no matter which subband they belong to. The key aspect of this OADM is the passband width of the components, since it will determine the specific wavelengths and width of the bands and subbands, hence the addressing and number of channels. Moreover, note that OADMs give a directionality to the backbone network. Hence, the backbone must be a closed ring in order to guarantee communications among all access networks.

The splitter is the component that introduces most losses. These can be reduced by changing the splitting ratio. It can be optimized depending on the number of OADMs that have to be crossed. 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, although this is at the expense of increasing the losses in other paths.

Figure 6 shows the result of these modifications: an all-optical QKD-MON based on WDM technology with simultaneous, dynamic, all-to-all communications capability where QKD emitters and receivers are freely mixed in any access network. Colored dots are used to il-

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

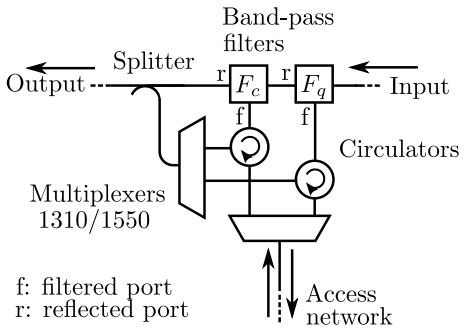

Fig. 5. Backbone node: OADM designed for the QKD-MON. Built out of common network components, it drops the quantum and service subbands from the ring's signal (input) to the access network, and adds any channel coming from the access network, no matter which subband it belongs to, to the ring (output).

lustrate a pair of wavelengths within a periodic set: one color represents one wavelength in the quantum band and the corresponding in the service band. As an example, it is shown how multiple communications are performed simultaneously. The scheme is non blocking in the sense that QKD devices in different access networks (e.g. the ones at the bottom and at the right) can also address devices in a third access network (top) that is simultaneously being used from the other two networks. OLTs have been removed: they are no longer needed since no conversion of any kind needs to be done and they would disrupt the quantum channel. This means that all upstream or downstream signals go straight to the backbone ring or access network, respectively. Note that there is no short path that links directly two QKD systems in the same access network. There are simple local solutions to this problem. For instance, using a larger switch allows to create return paths (i.e. connect them again to the switch) with the free ports in the side of the AWG.

The losses of the network are shown in Table 2. They are calculated using the theoretical values of the components used in their construction. For mere illustrative purposes, we also 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 [28,57,58], allows a QKD-MON with 3-4 OADMs and a span of 15-20 km. Although there are QKD systems with a loss budget over 40 dB [29–31], we do not consider them practical in real world networks, since they are based on superconducting detectors that need cryogenic temperatures to work. Note that the network scheme remains valid even if QKD technology improves, since a higher loss budget can be directly interpreted as adding new backbone nodes or longer fibers.

One-way QKD systems [28–31, 57, 58] can be used directly in this network, one example could be a system running the coherent-one way (COW) protocol. The most recent implementation of a COW system [59] uses a quantum channel (emitter to receiver) together with two classical channels (one in each direction) that carry the service signals and the distillation protocol communication via TDM (in Sec. 4, this advanced approach to the service channel is discussed). Time multiplexing a wavelength in the presented network does not pose any problem and the scheme works flawlessly without modifications. Moreover, the COW system can tolerate delays between quantum and classical signals, such as those originating from the small differences in path that can occur in our OADM node. The only requirements to adapt a COW system to the presented network architecture 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.

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

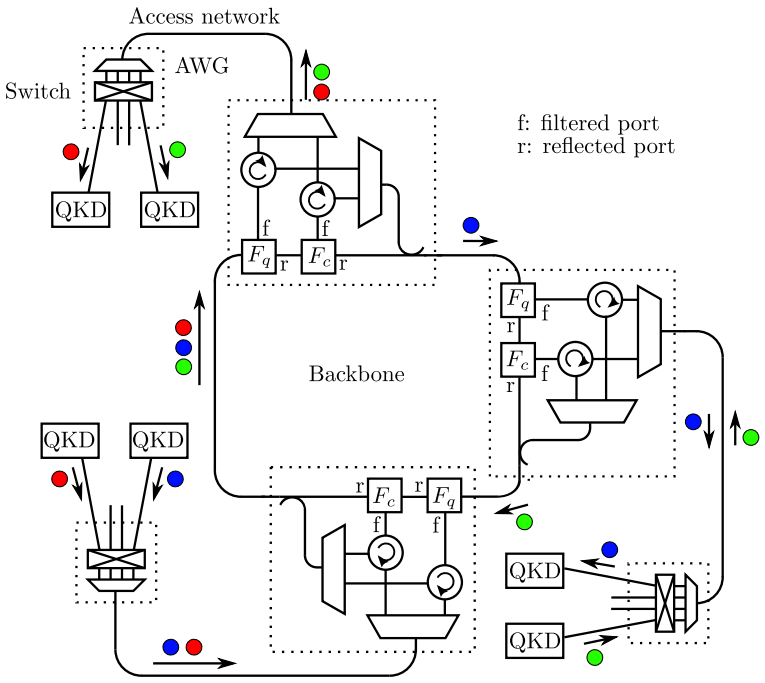

Fig. 6. Proposed QKD-MON with three access networks. Colored dots are used to illustrate the communication over different paths. Each colored dot represents a pair of wavelengths: one in the quantum band and the corresponding periodic one in the service band that would come out of the same output port of the AWG. The main network components are represented in dashed-line boxes. These devices can be built with out of the shelf commercial components. Note how one access network can communicate simultaneously with the others in a non-blocking way: communications can be performed simultaneously since the network operates employing wavelength multiplexing.

Regarding the maximum number of users that the network can serve, it depends on the width of the spectrum bands, subbands and DWDM channel spacing chosen. If CWDM is used for the subbands (passband of ≈ 13 nm) and a 100 GHz grid, extension of the corresponding ITU DWDM grid, for the 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 in the shortest wavelengths and by the need of having the quantum and service, classical signals well separated to avoid interference in the longest wavelengths. Four CWDM channels fit in the wavelength plan without problems. The second term is the passband of the CWDM channel over the DWDM channel spacing in nanometers. Since 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 although, in practice, mismatches between the specifications of network components (e.g. CWDM channels and the cycles of the AWG), and the noise in the quantum channel coming from the classical service signals will set the specific limit for a given choice. The noise increases the number of erroneous detections in the single photon detectors and can increase the quantum bit error rate (QBER) to the point of precluding any key exchange. These photons are generated mainly by three physical phenomena: Raman scattering, four-wave mixing

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

(FWM) and crosstalk due to imperfect devices. However, we can eliminate the last two since, due to the separation between quantum and service bands, no signal generated by FWM from the service band will fall within the quantum band [43]. Likewise, strong service signals that could produce too much crosstalk due to insufficient isolation in the devices can be easily filtered because they are also in other band. The only phenomenon that could spoil the quantum signals is Raman scattering, but then a band separation of approx. 150 nm is enough to attenuate it considerably [55, 60], as we will see in the next section.

Table 1. Losses of typical optical network components. Values are from commercial models available in the market [61–64] that are used for the test-bed in Sec. 4.

Device	Passband	Losses
Single-mode fiber	C band	0.18 dB/km
Single-mode fiber	O band	0.32 dB/km
Connectors	—	0.2 dB/pair
1×2 Splitter	$1270-1350\&1510-1590$ nm	3.6 dB
1×32 Splitter	$1270-1350\&1510-1590$ nm	16.5 dB
4×4 to 192×192 Switch	—	1 dB
Circulator	$1280-1340$ nm	0.8 dB
Circulator	$1520-1580$ nm	0.8 dB
CWDM filter	≈ 13 nm	$0.4-0.6$ dB
1310/1550 WDM mux	$1260-1360\&1460-1560$ nm	0.5 dB
32-ch AWG DWDM mux	100 GHz	3 dB

Table 2. Calculated losses for the main network modules of the QKD-MON (according to Table 1). Using these theoretical values, we estimate the losses of different full optical paths in terms of OADMs and fiber length.

Network component	Losses (quantum)	Losses (service)
32-ch AWG	3 dB	3 dB
Switch	1 dB	1 dB
OADM (add)	5.4 dB	5.4 dB
OADM (pass)	4.8 dB	4.8 dB
OADM (drop)	1.7 dB	2.3 dB
10-km path and 2 OADMs	18.1 dB	17.5 dB
15-km path and 3 OADMs	24.7 dB	23.2 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

4. Network prototype

The QKD-MON depicted in Fig. 6 has been implemented using the components detailed in Table 1. The test bed network is a full-featured quantum metropolitan optical network, 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. 7. It crosses all network components in order to connect access networks 1 and 3. Thus, it corresponds to the worst case scenario in terms of losses and generated noise.

The three access networks are connected by a backbone using single mode fiber with a total length of approx. 16 km. Optical channels are implemented using two spectrum bands (de-

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

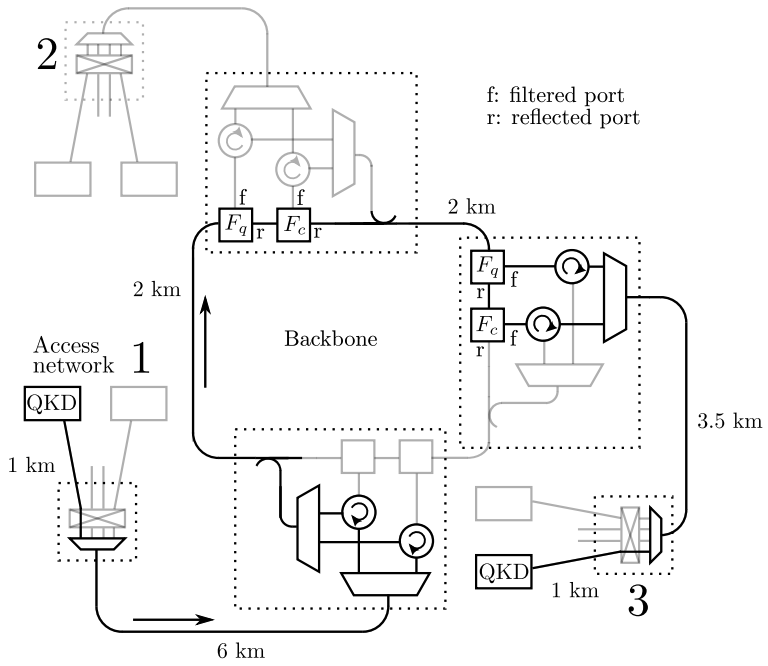

Fig. 7. QKD-MON test bed: Network prototype with three OADMs built following the design in Fig. 6. The total length of the fiber is approx. 16 km, a typical span for metro area. A relatively long fiber is used in the access network 1 to generate a high amount of Raman scattering, more than the average for access networks. Overlaid in black is the worst case path in the test bed with respect to losses and generated noise, hence this is the set-up used to perform the measurements.

fined by the spectrum bandwidth of the components used at the OADM): 1280-1340 nm for the quantum channels and 1520-1580 nm for the service ones. Two subbands are assigned to each access network: 1280-1300 nm and 1560-1580 nm for the quantum and service channels, respectively, of the access network 1; 1300-1320 nm and 1540-1560 nm to the access network 2; and 1320-1340 nm and 1520-1540 nm to the access network 3. Note that CWDM is used in the backbone for routing subbands, and channels within a subband are redistributed in the access network using a 100 GHz 32-channels DWDM AWG multiplexer. This is a bonus for the practical implementation, since industrial grade components are readily available.

The test bed network 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 optical spectrum analyzer to measure the peak power of both signals at different points of the network, including the received signals at the end (i.e. the full optical path). The results, given in Table 3, are consistent with the calculated theoretical values (Table 2). In a further working test, the band-subband structure depicted in Fig. 2(a) is reproduced. Multiple QKD devices communicating with the access network 2 are simulated using broad-band lasers and an attenuator for the quantum channels. The results are shown in Fig. 2(b). The difference in the number of quantum and service channels is due to the different width of the lasers used for each band.

Once the network prototype has been checked successfully, we want to find the maximum input power of the service band that does not disrupt the quantum transmission. The critical

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

Table 3. Measured losses in the quantum and service band for the OADMs and for the full optical path in the QKD-MON test bed (see Fig. 7).

Device	Losses (quantum)	Losses (service)
32-ch AWG	2.34 dB	2.45 dB
OADM (add)	5.98 dB	4.91 dB
OADM (pass)	5.7 dB	5.8 dB
OADM (drop)	1.83 dB	2.24 dB
Full optical path	23.15 dB	20.64 dB

power is reached when the noise produced by the service signals in a quantum channel together with the intrinsic noise of the single-photon detectors (SPD) used in the QKD yield a QBER equal to the threshold (11% if we assume that a BB84 with one-way communications is used). In case the power is below the critical value, a QKD link could be established whenever an appropriate QKD system is used, i.e. one able to withstand the 20-30 dB losses [28, 57, 58]. The power threshold also allows to estimate the maximum number of QKD devices that can operate simultaneously. Using again the full optical path, we have performed several measurements of the forward and backward noise in order to simulate different network configurations (e.g. emitters and receivers mixed together in the same access network). For the forward noise, measurements are carried out at the smallest wavelength separation between quantum and service bands allowed by the channel plan, which is approx. 180 nm (1340 to 1520 nm). This should produce the highest noise levels possible. As a comparison with the schemes where all signals are placed in the same spectral region, the forward noise at the service band is also measured (1530 nm). In both setups, an SPD [2] 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 service 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). In this way we can simulate scenarios with a different number of QKD devices. Finally, we measure the backward noise in a quantum channel by moving the SPD and WDM multiplexer also to the access network 1. The measured noise per 1 ns gate in a quantum channel is presented as a function of the input power in the service band for all three scenarios in Fig. 8 (note that the intrinsic noise of the SPD has been subtracted). The figure also depicts the noise (dark count rate) of an actual QKD system [58] and the expected detection rate of quantum signals. The probability of detecting an emitted single photon is calculated as $1-\exp(-\mu\tau\eta)$, where μ is the mean photon number, τ is the transmittance and η is the quantum efficiency of the SPD. Therefore, we can estimate the QBER as the ratio of erroneous detections measured with the SPD over the total number of detections. This measurement includes contributions from the dark count rate and the noise generated by the service signals. Calculated values of the QBER of several representative points of the experiment are also shown.

As expected, the forward noise in the service band is higher than in the quantum band. Although the forward noise in the service band is not relevant for QKD operation, it highlights the importance of separating quantum and service bands in the spectrum. The results are consistent with previous findings [23,43–45], where only a few attenuated classical channels could be transmitted in the same band without disrupting the quantum channel. Also as expected, the backward noise in the quantum band becomes the limiting factor. This is because Raman forward-scattered photons have suffered higher losses (filtering and fiber attenuation integrated over the whole network path). This is something to take into account when a non-directional network is used, since then QKD emitters and receivers can be mixed in the same access network. In this test bed, it is seen that, even with approx. $+2$ dBm power for the service band,

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

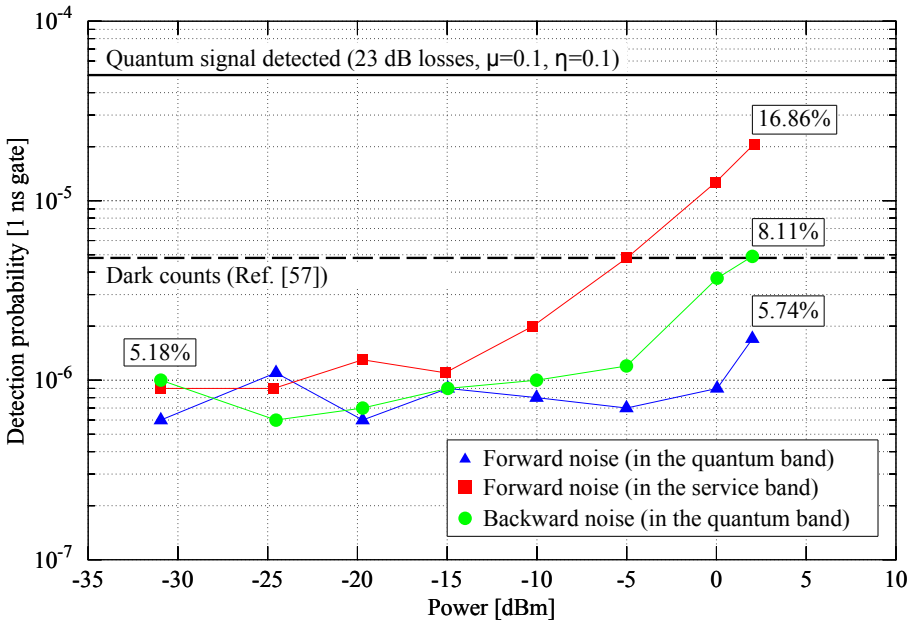

Fig. 8. Noise measurement done using the setup in Fig. 7. A laser signal centered at 1520 nm and with power ranging from -30 to $+2$ dBm is fed at the access network #1. The forward noise produced in a quantum channel (1340 nm, triangles) is measured using a SPD at the access network #3. The backward noise (circles) is also measured by connecting the SPD to the access network #1. This allows assessing the amount of interference that would reach a QKD receiver coming from an emitter in the same AWG. As a further check, we also measure the forward noise in the service band (1530 nm, squares). To facilitate the comparison, values are normalized considering 1 ns gates. Besides, a quantum signal (mean photon number, $\mu = 0.1$, and detector's quantum efficiency, $\eta = 0.1$) detected at the access network #3 and the dark count rate of an SPD [58] are also presented. Using these data, a rough estimation of the QBER is shown for multiple points.

an actual QKD system [58] can successfully establish a QKD link since the QBER estimation is below the threshold. This overall power for the service band would allow for more than 32 simultaneous service channels of -13 dBm without disrupting the quantum channels. For example, in this case, the QBER would increase from 4.37% with no service channel to 5.1% with only one and to approx. 5.74% with all 32 channels being used at the same time. Note that the minimum power in the classical channel has to be chosen carefully to grant a good reception of the service signals. With -13 dBm, even in the worst case (highest losses) path, the receiving power of the service channel 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} [45]. Less conservative estimates, using shorter gates at the SPDs (e.g. 100 ps [58]), will reduce the noise considerably and thus allow for more service channels or higher data rates.

Modes of network operation

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 be highly desirable to go beyond and use the rest of the time for key distillation and/or cyphering. To distil a key, a bidirectional communication is required since classical data has to be sent from the receiver to the emitter. However, note that

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

the backbone ring is directional: a signal originated in the receiver cannot be propagated back to the emitter using the same path. To do this, a signal traveling along the other part of the ring has to be used. Therefore, the receiver has to use a service channel assigned to the emitter. Since, by design, every device in the network has a pair of channels assigned, there is no extra addressing required for these *return channels*; they are already located in the channel plan. However, 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 [65], the switching time is not a problem. However, if a simultaneous return channel is necessary, this can be easily taken into account. For instance, in a static version of the network, all channels (i.e. quantum, service and return) can be configured to belong to the same periodic set. 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, however it is not a technical problem since this is a short distance and most installations include spare fibers that could be used for this purpose.

5. Conclusions

We have presented a quantum metropolitan network that is, in contrast to existing QKD networks, specifically designed to share infrastructure and use existing optical components in an attempt to make QKD a more cost-competitive technology and lower the barriers to a wider market adoption. We also show that the new modules needed can be built out of inexpensive, industrial grade and readily available components, without introducing unacceptable losses. The scheme is based on wavelength division multiplexing and addressing, whereby multiple QKD devices are simultaneously connected for transmitting quantum and classical signals. The architecture is a conventional one in metropolitan optical networks, comprising backbone and access networks, although these two segments are directly connected to provide uninterrupted optical paths between all users; a must in order to support a quantum channel. The network allows all to all QKD links and uses standard commercial WDM technology: CWDM for the backbone and DWDM for the access. Except the switches on the user side, needed only if all-to-all dynamic routing is required, the rest of the network is purely passive. This would potentially allow for a cheap, easy and reliable deployment.

The scheme is limited by the loss budget of actual QKD systems ($\approx$ 20-30 dB), but, as discussed above, this is enough for a backbone ring of 20 km with three access networks. This would allow to cover interesting regions in a city and its surroundings. The measurements performed on a prototype network demonstrate that it is capable of supporting at least 32 simultaneous QKD links, each one with a pair of a quantum and a service channel, whereby the latter can support traffic of up to 1.25 Gbps classical signals. This traffic could include key distillation communication or even cipher text transmission. Classical channels for other purposes could also be included when not all of the possible QKD links are installed. The estimate assumes 1 ns detector gates: more channels and a higher throughput would be possible if last generation, sub-ns gated detectors are used. We introduced the scheme with discrete, one-way QKD systems but it could, in principle, be extended to entangled pairs and continuous variables, although then the limits could possibly vary. We plan to address in near future the extension of the present scheme to cover all main QKD realizations.

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014

Acknowledgments

This work has been partially supported by projects QUITEMAD, *Comunidad Autónoma de Madrid*, and Quantum Hybrid Networks, *Ministerio de Economía y Competitividad*, Spain. GAP acknowledges financial support from NCCR-QSIT. AIT acknowledges support by the project QKD-Telco: Practical Quantum Key Distribution over Telecom Infrastructures, within the FIT-IT programme funded by the *Austrian Federal Ministry for Transport, Innovation and Technology* (BMVIT) in coordination with the *Austrian Research Promotion Agency* (FFG). The authors also thank P. Corredera for his assistance regarding the characterization of the AWG, and M. Soto and Telefónica I+D for the loan of the OSA, EDFA and fiber prototype network used in this work.

#195939 - $15.00 USD Received 16 Aug 2013; revised 22 Nov 2013; accepted 4 Dec 2013; published 16 Jan 2014