Secure Optical Networks Based on QKD and Weakly Trusted Repeaters

David Elkouss[a], Jesus Martinez-Mateo[b] and Alex Ciurana[b] and Vicente Martin[b]

[a]Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid
[b]Facultad de Informática, Universidad Politécnica de Madrid

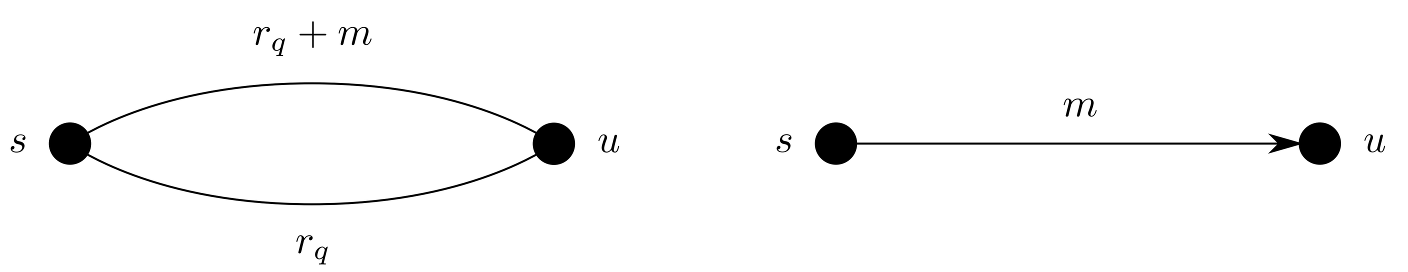
POLITÉCNICA

Introduction

Point-to-point QKD devices have reached a mature industrial state; however, these devices are limited in distance since losses and noise in the communication severely hinder the weak quantum signal. To overcome this limitation, intermediate nodes (i.e. repeaters) are used. Both, quantum [1] and trusted [2], classical, repeaters have been proposed in the QKD literature, but at the moment only the latter can be implemented. We introduce an alternative solution based on network codes and partial trust of the intermediate nodes.

Weakly Trusted Repeaters

Network coding is a paradigm where the nodes, instead of simply forwarding the incoming flows through the outgoing paths, distribute a function of the inputs. We consider a network where every two nodes are connected via a QKD link. This restricts eavesdropping to the intermediate network nodes; only a curious router can gain access to network messages.

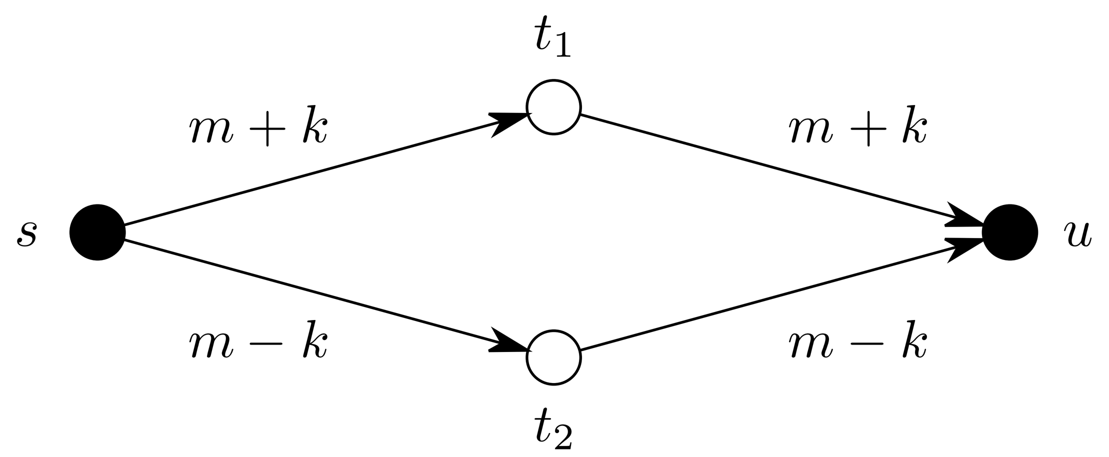


Physical (left) and logical representation (right) of a QKD link.

Let $\mathcal{W}$ stand for the set of eavesdroppers. Every $w \in \mathcal{W}$ receives the messages traversing a collection of nodes B_w and targets a subset of the source message M_w. A network code is admissible over this *eavesdrop network* model if it verifies the so-called secure and decodable conditions [3]:

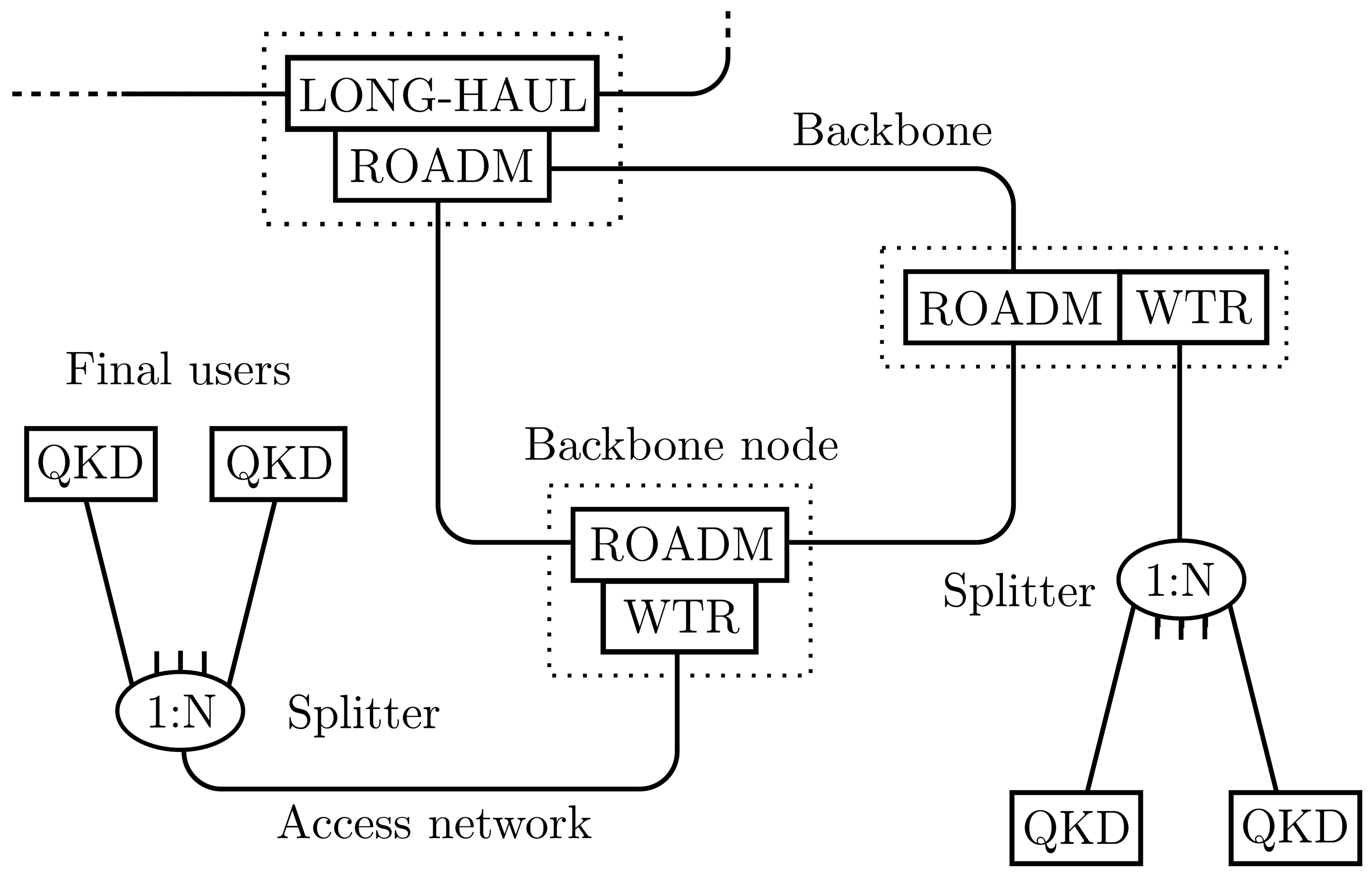
$$H(M_w|U) = 0 \text{ and } H(M_w|B_w) = H(M_w)$$

Example:



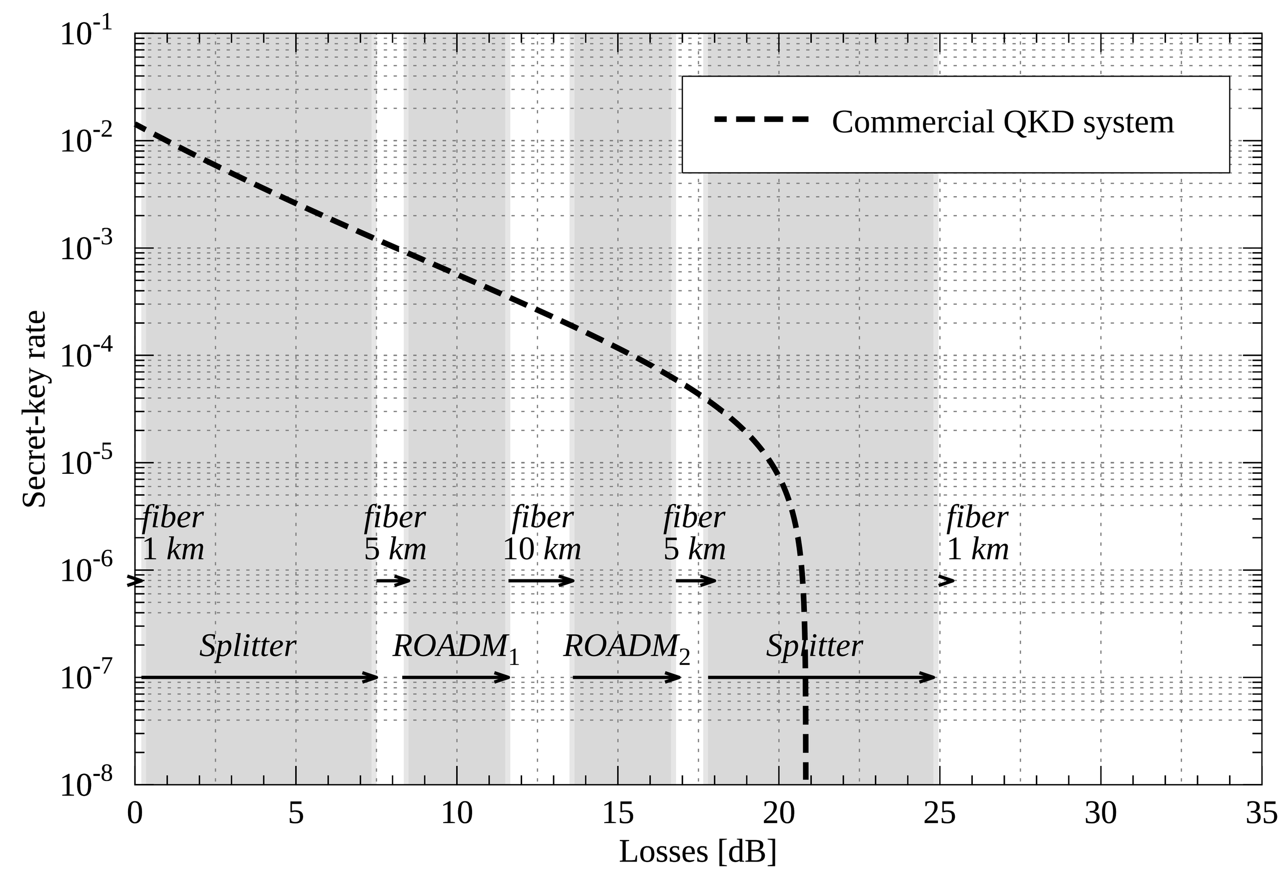
Explicit code for a toy network; ($B_{w_1} = \{t_1\}$ and $B_{w_2} = \{t_2\}$).

Metropolitan Optical Network



Main components and architecture of a metropolitan optical network

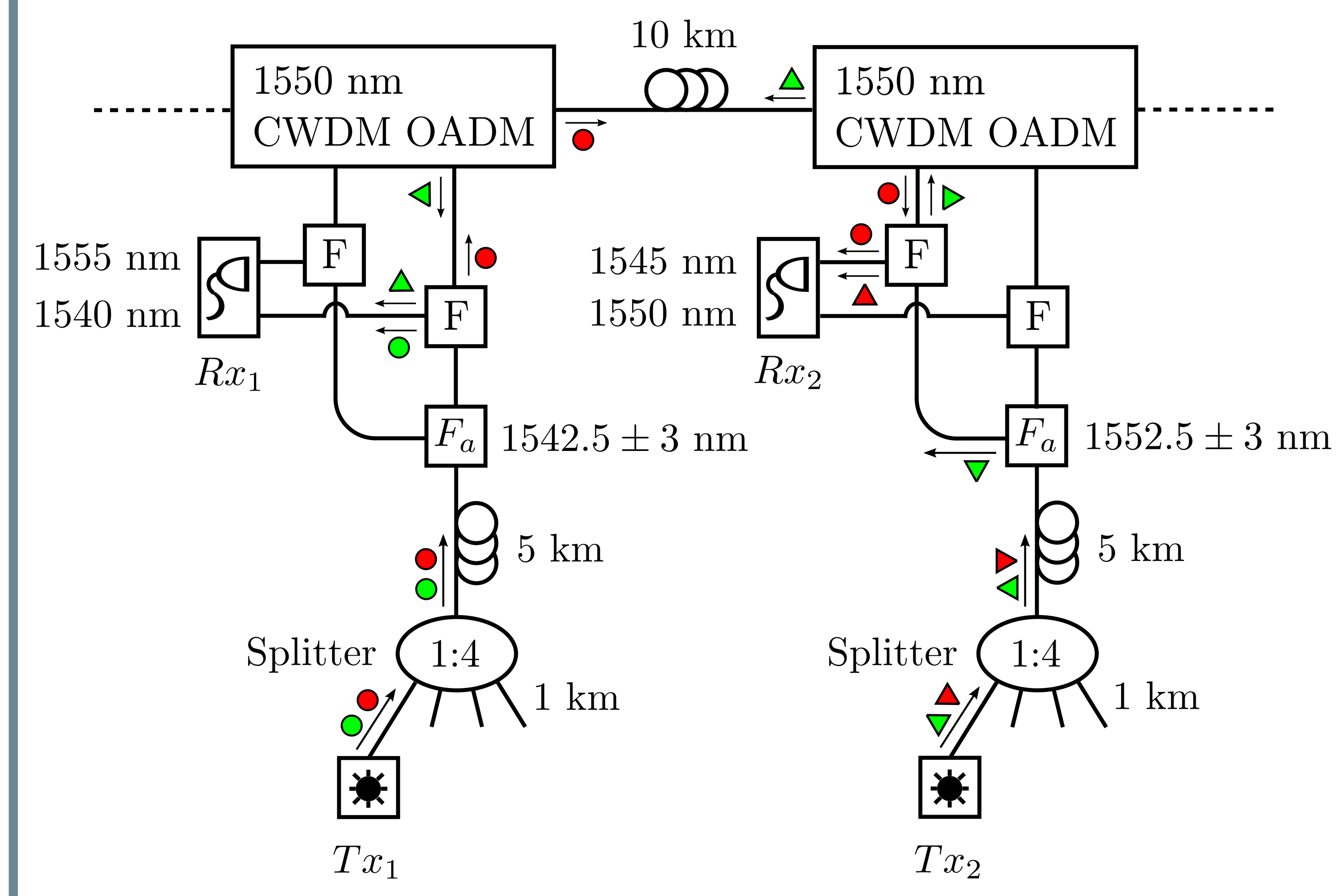
In order to communicate securely over a metropolitan optical network, a QKD link has to be created among any two final users. Since transmission losses do not allow to directly exchange a QKD key among two different access networks, weakly trusted repeaters are placed in the middle, alongside the ROADMs at the immediate backbone node and at its closest neighbors. With this configuration, each user has several outgoing links.



The figure compares 1) the secret key rate of a commercial QKD device with 2) the losses experienced traversing the different components of a metropolitan optical network.

Network Prototype

A specific network prototype for the quantum layer is presented to show the viability of the WTR paradigm, i.e., we discuss the placement and logical connections between of the nodes. It works under the wavelength-addressing paradigm: a wavelength is assigned to each receiver (Rx) of the WTRs. At the backbone node, passive optical components (filters and OADMs) are used to route the signals to the correct receiver. Hence, the transmitters (Tx) of the QKD systems only have to emit at the correct wavelength. The QKD keys exchanged between adjacent nodes in the logical network are later used to cypher the classical communications between the same nodes.



Communications between emitters and receivers are represented using colored circles (from $Tx1$) and triangles (from $Tx2$). The color indicates the wavelength. There are two different paths joining $Tx1$ with $Tx2$, e.g. via $Rx1$ or $Rx2$.

References

[1] H. J. Briegel, W. Dür, J. I. Cirac and P. Zoller. Quantum Repeaters: The role of imperfect local operations in quantum communication, in *Physical Review Letters*, vol. 81, no. 26, pp. 5932–5935, 1998.

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

[3] N. Cai and T. Chan. Theory of secure network coding, in *Proceedings of IEEE*, vol. 99, no. 3, pp. 421–437, 2011.

[4] D. Elkouss, J. Martinez-Mateo, A. Ciurana and V. Martin. Secure optical networks based on QKD and weakly trusted repeaters, in *Journal of Optical Communications and Networking*, vol. 5, no. 4, pp. 316–328, 2013.