Entanglement Distribution and Secret Key Sharing In Optical Networks

Muneer Alshowkan, Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

Communicating a quantum state remotely is possible by Remote State Preparation. Sender Alice create a pure state known to her and help the receiver Bob to securely prepare the state remotely instead of sending the physical quantum state. To successfully perform this protocol the sender and the receiver must share Einstein-Podolsky-Rosen (EPR) state and have access to an authenticated classical channel. The sender and the receiver must be sharing an entangled bit for each state the sender wishes to prepare at the receiver's location. In this paper we introduce a protocol to create and distribute the required entangled pairs between the communicating parities. A trusted source of EPR states will provide the necessary entangled states required to the sender and the receiver. The distributed EPR state will be used between the communicating parties to create secret keys by using remote state preparation protocol. The proposed protocol will provide unconditional security and any attacking attempt will be discovered due to the disturbance in the states.

Optical Fiber Network

Optical Fiber Network: is a type of data communication networks where the transmission medium is an optical fiber. Optical fiber is thin strands of glass or plastic behaves like a waveguide. A waveguide is a structure that allow the propagation of electromagnetic waves such as light.

Metropolitan Optical Network

Optical Access Network

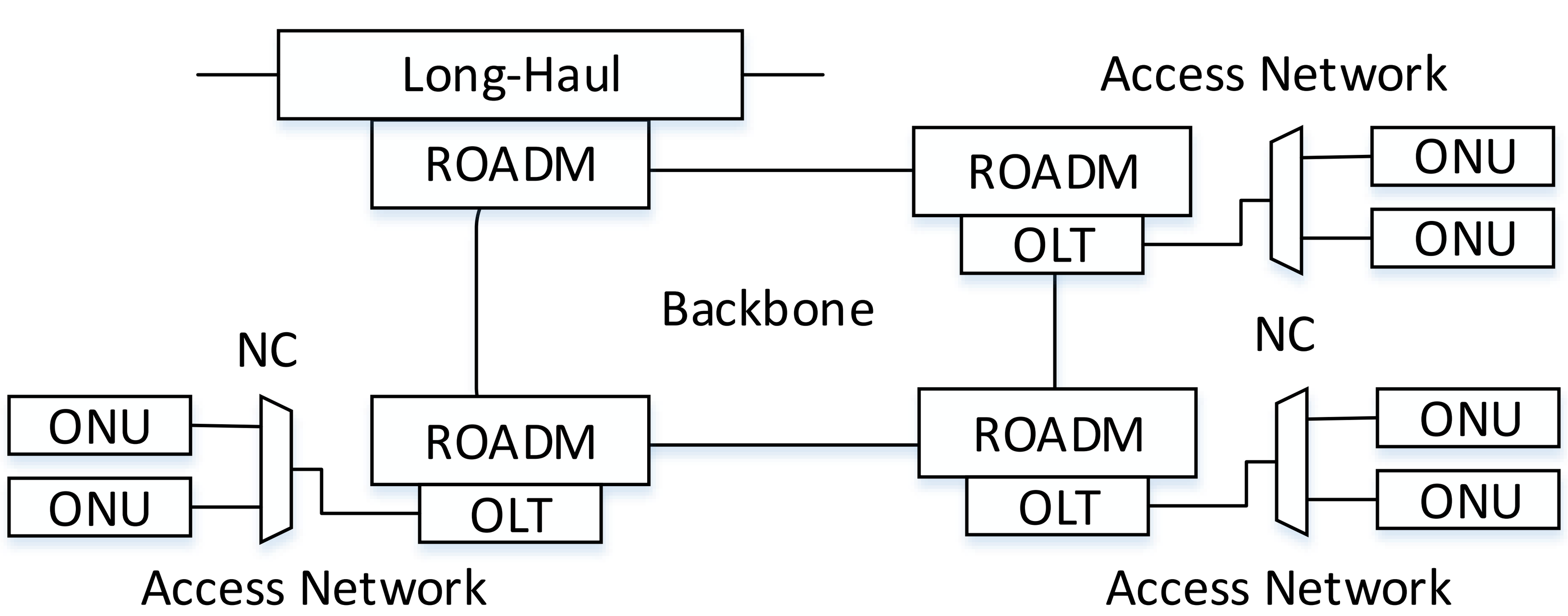

Fig 1: canonical metropolitan optical network

Quantum Cryptography

Quantum cryptography depends on the laws of quantum mechanics for sending and receiving data using quantum states such as atoms, photons or molecules.

Quantum Entanglement:

A pair of particles share the same properties, measurement on one particle determines the value of the other particle even if they are spatially separated. Fig 2 shows the process to create entangled pair of photons, each photon in a different wavelength.

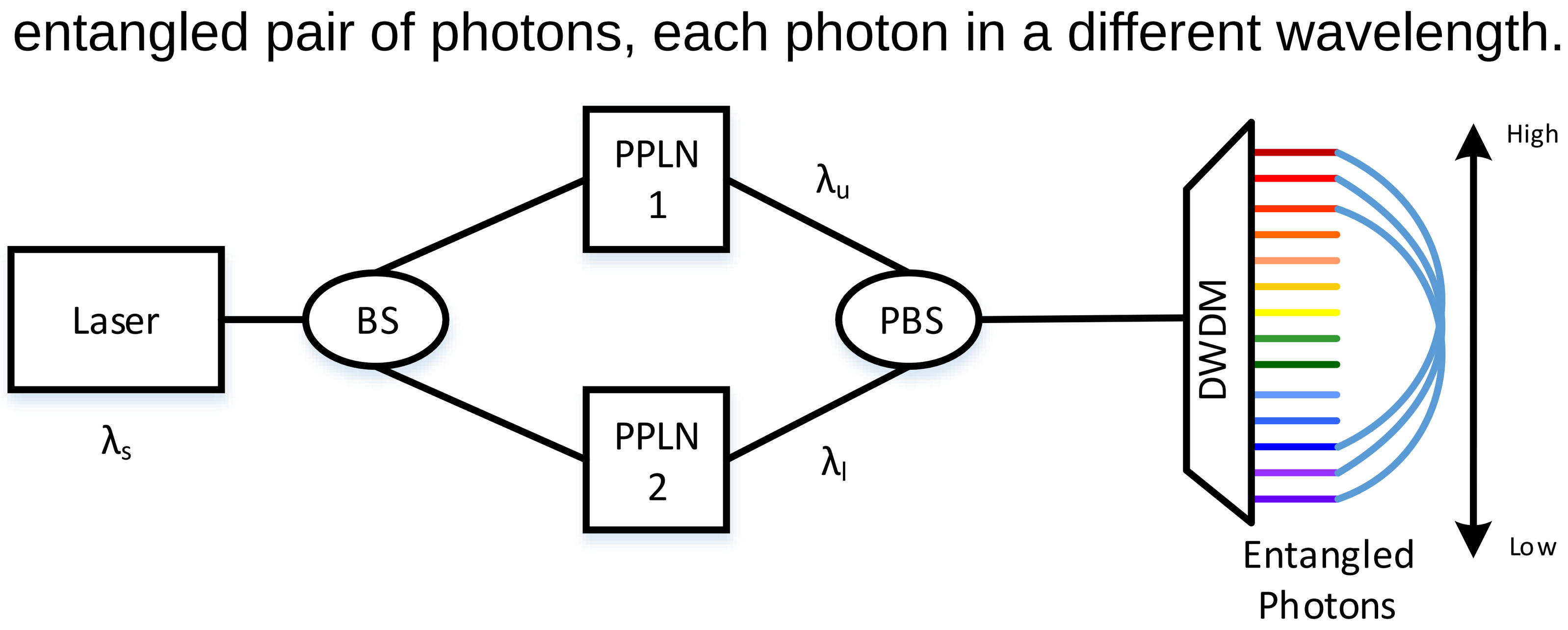

Fig 2: parametric down conversion to create entangled photons

Design for the access network

EPR source will be required in the access network to distribute the entangled pairs through the optical fiber links. Also, classical channel will be needed to for key distillation. Separation and guarding between quantum signal and classical signal is essential to avoid classical channel to disturb the quantum channel fig 3.

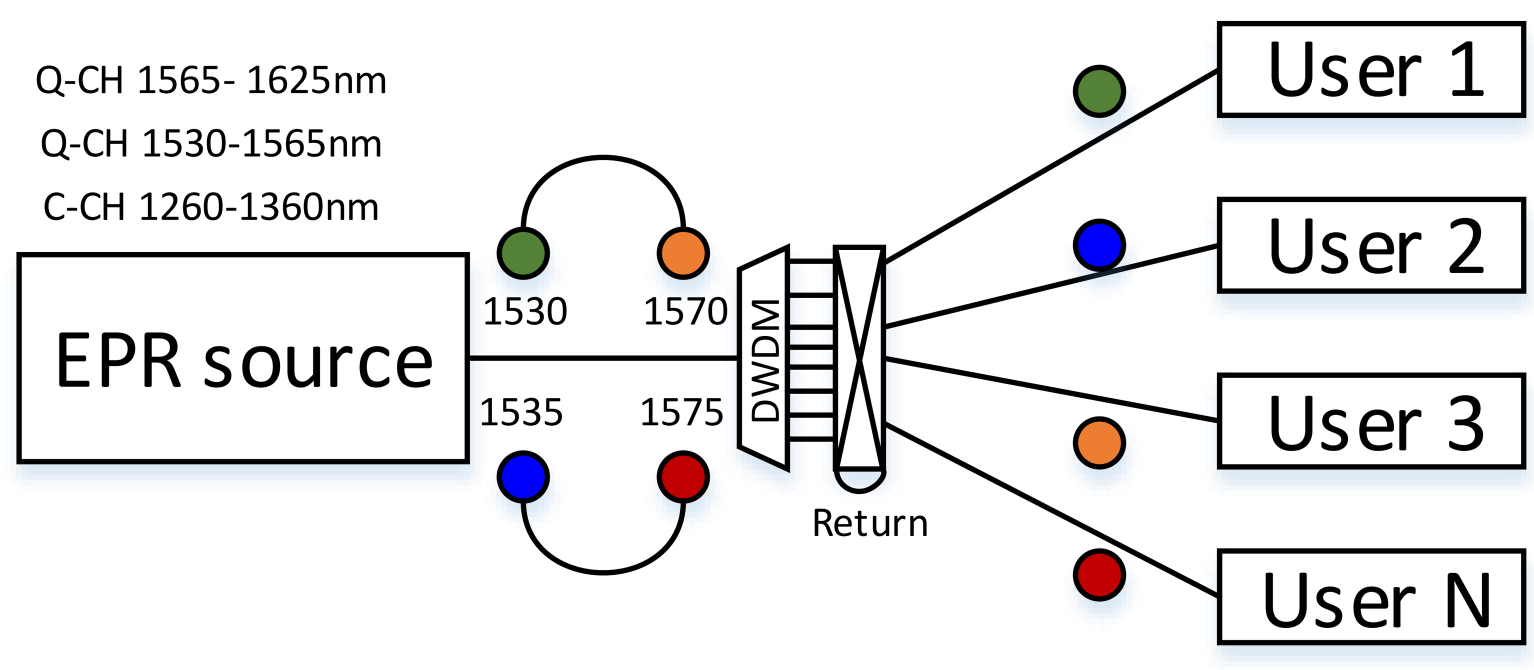

Fig 3: Access network containing quantum and classical channel

Design for metropolitan optical network

Distributing the entangled pairs from the central EPR source. The EPR source distribute the entangled pairs in the access networks and between them based on the assigned wavelength fig 4.

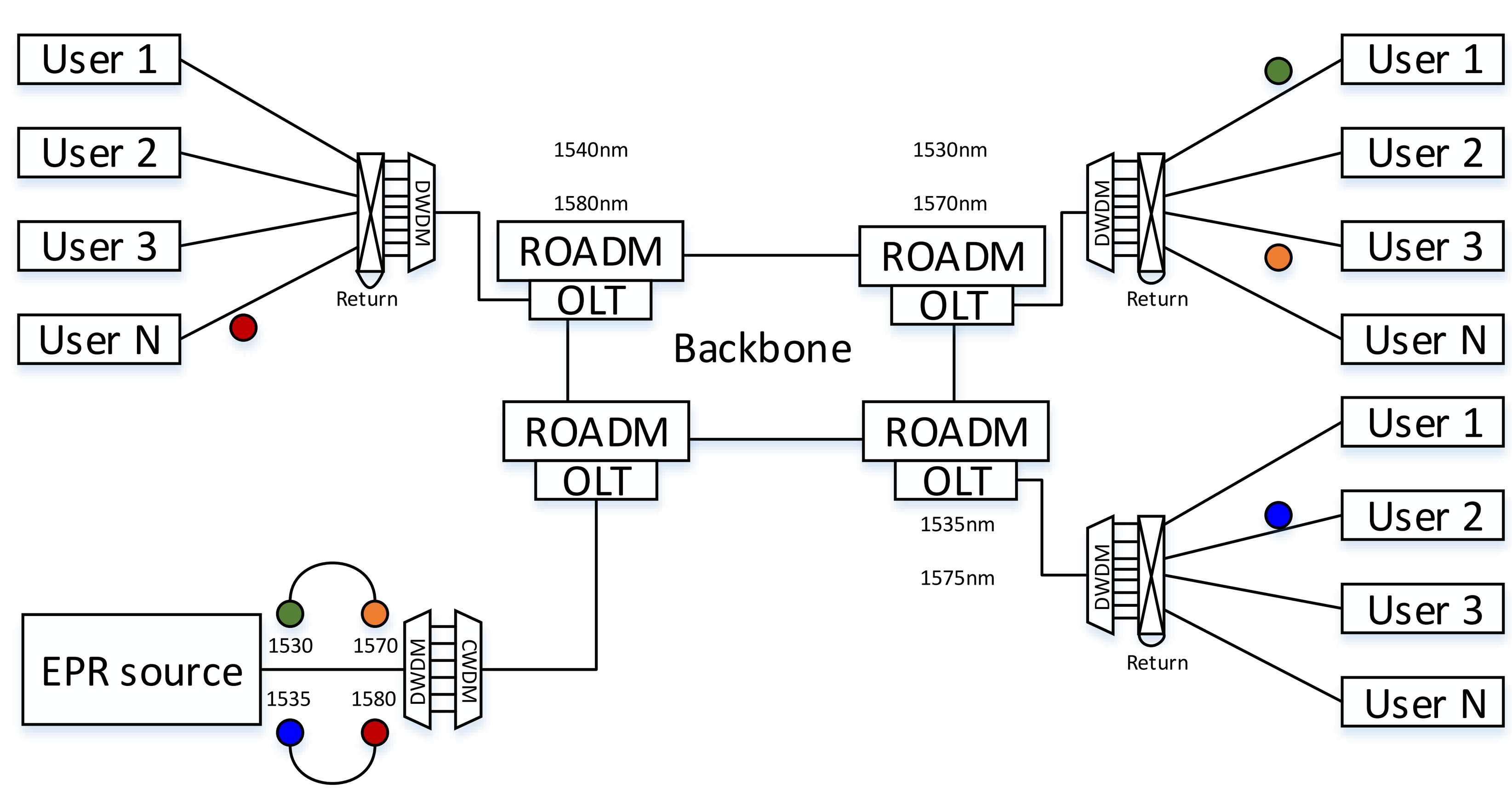

Fig 4: Entangled pairs distribution in the metropolitan network

Sharing the Secret key

After the entanglement source create the maximally entangled state from basis $\{|\Psi^{\mp}\rangle, |\Phi^{\mp}\rangle\}$ and send the entangled photons to the sender and the receiver.

$$|\Psi^{-}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B),\ |\Psi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$

$$|\Phi^{-}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B),\ |\Phi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

The sender and the receiver now can perform the remote state preparation. The sender create a state and measure it in one of the basis $|\Psi\rangle$ or $|\Psi \perp\rangle$ Von Neumann measurement on their qubit. The result will indicate to the sender if the receiver entangled bit will be in the correct state or not. If stat in the correct state the sender will inform the receiver by sending one classical bit to perform the appropriate quantum gate.

References:

1- S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. DeMicheli, et al., "PPLN waveguide for quantum communication," The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics, vol. 18, pp. 155-160, 2002.

2- A. Ciurana, V. Martin, J. Martinez-Mateo, B. Schrenk, M. Peev, and A. Poppe, "Entanglement Distribution in Optical Networks," Selected Topics in Quantum Electronics, IEEE Journal of, vol. 21, pp. 1-12, 2015.