Deterministic And Efficient Three-party Quantum Key Distribution

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

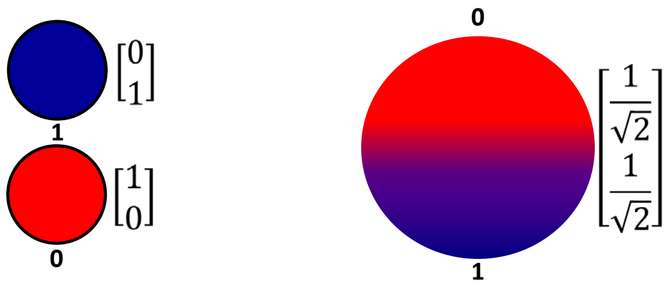
Abstract

The field of quantum computing is based on the laws of quantum mechanics, including states superposition and entanglement. Quantum cryptography is amongst the most surprising applications of quantum mechanics in quantum information processing. Remote state preparation allows a known state to a sender to be remotely prepared at a receiver's location when they prior share entanglement and transmit one classical bit. A trusted authority in a network where every user is only authenticated to the third party distributes a secret key using quantum entanglement parity bit, controlled gates, ancillary states, and transmit one classical bit. We also show it is possible to distribute entanglement in a typical tele-com metropolitan optical network.

Key Idea, Hypothesis And Specific Problem

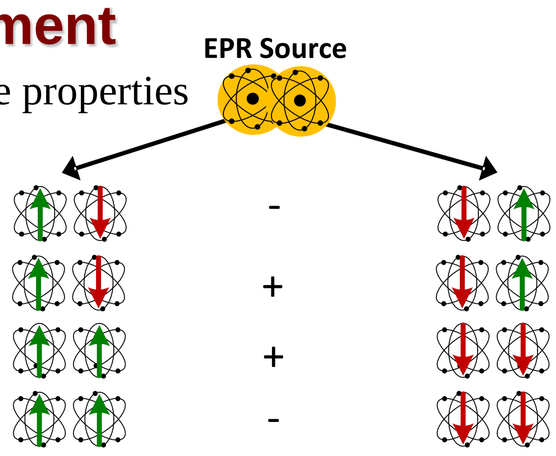
Quantum Cryptography, Quantum key distribution. Quantum teleportation consumes two cbits and ebits. Remote state preparation consumes one cbit. Key distribution between untrusted parties by secure and efficient secret key establishment. Also, entanglement distribution in an optical network. Consumes one cbit on average for each qubit by Finding a secure and efficient entanglement-assisted three-party quantum key distribution protocol. In addition, how to distribute entanglement in a typical telecom metropolitan optical network.

Conventional And Quantum Computing



Quantum Entanglement

Pair of particles share the same properties

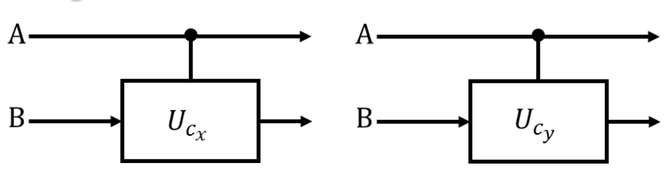


Bell States:

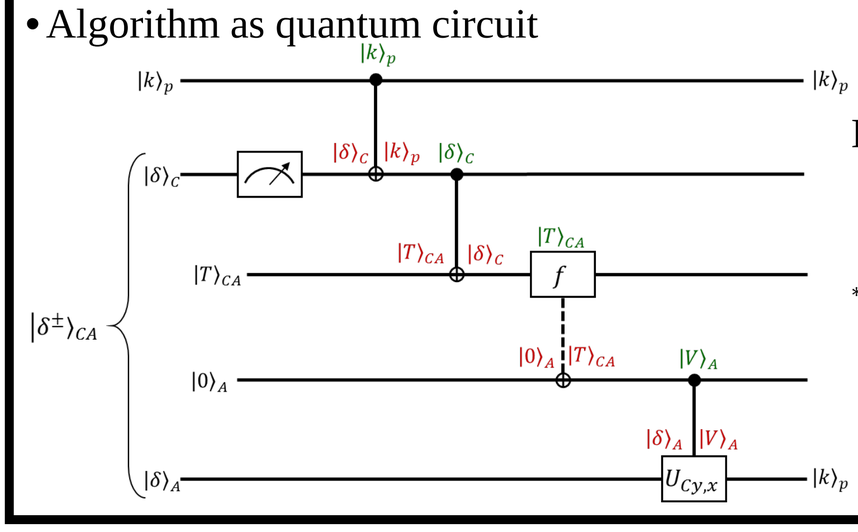
$$|\Psi^-\rangle = |0\rangle|1\rangle - |1\rangle|0\rangle$$
$$|\Psi^+\rangle = |0\rangle|1\rangle + |1\rangle|0\rangle$$
$$|\Phi^+\rangle = |0\rangle|0\rangle + |1\rangle|1\rangle$$
$$|\Phi^-\rangle = |0\rangle|0\rangle - |1\rangle|1\rangle$$

Efficient Quantum Key Distribution

- Pre-shared EPR parity bits
  For $|\Psi^{\pm}\rangle = |T\rangle_{Cx} = |1\rangle$
  For $|\Phi^{\pm}\rangle = |T\rangle_{Cx} = |0\rangle$
- Ancillary qubits
  For Alice $|0\rangle_A$
  For Bob $|0\rangle_B$
- Controlled-U Gates
- Algorithm as quantum circuit



$$Uc_x = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad Uc_y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix}$$



Intrinsic Efficiency

$$\eta = \frac{q_s}{q_u + b_t}$$

$* q_s$qubits $* q_u$ ebits $* b_t$ cbits

$$\frac{2}{4+1} = \frac{2}{5}$$

Entanglement Distribution in Optical Network

Contains: Backbone network; Backbone nodes; Access network
Centralized EPR source: Classical signals; Quantum signals
Simultaneous transmission of classical and quantum signals

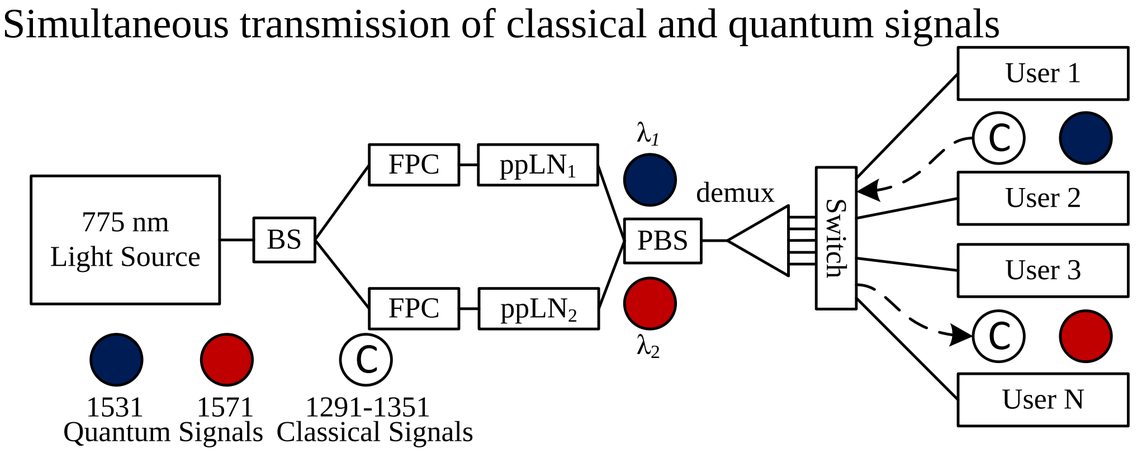


Fig 1. Entanglement distribution in an access network

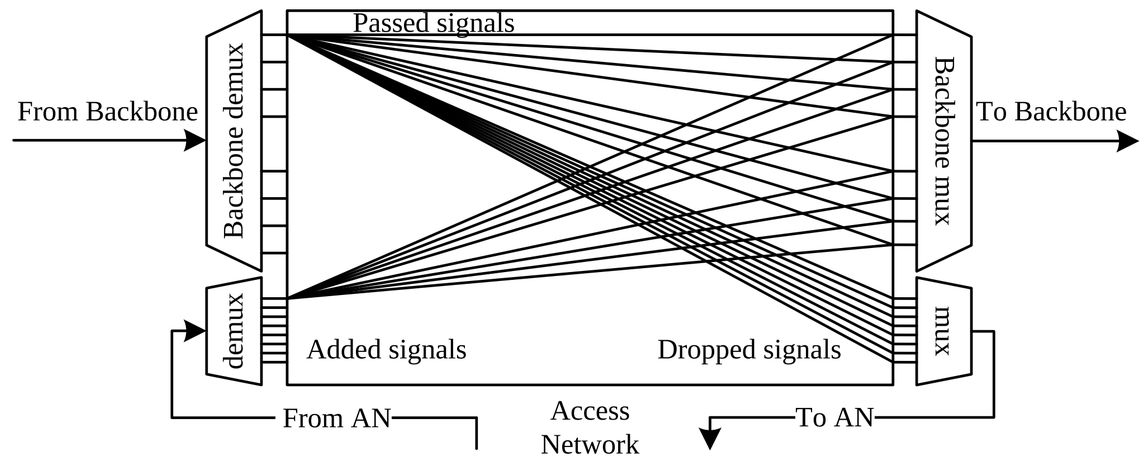


Fig 2. Design of the backbone node (ROADM)

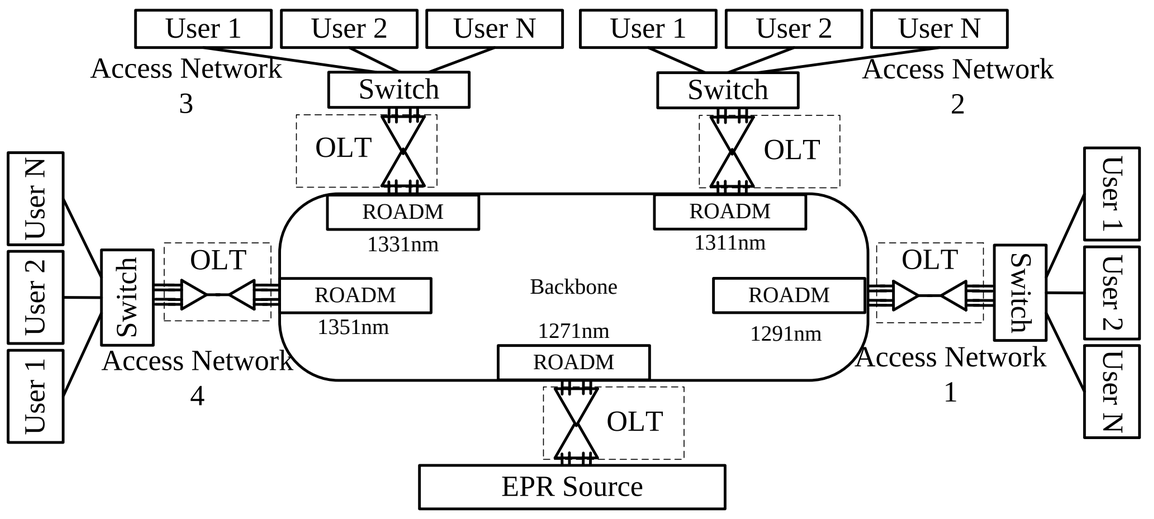


Fig 3. The architecture of the metropolitan optical network (MON)

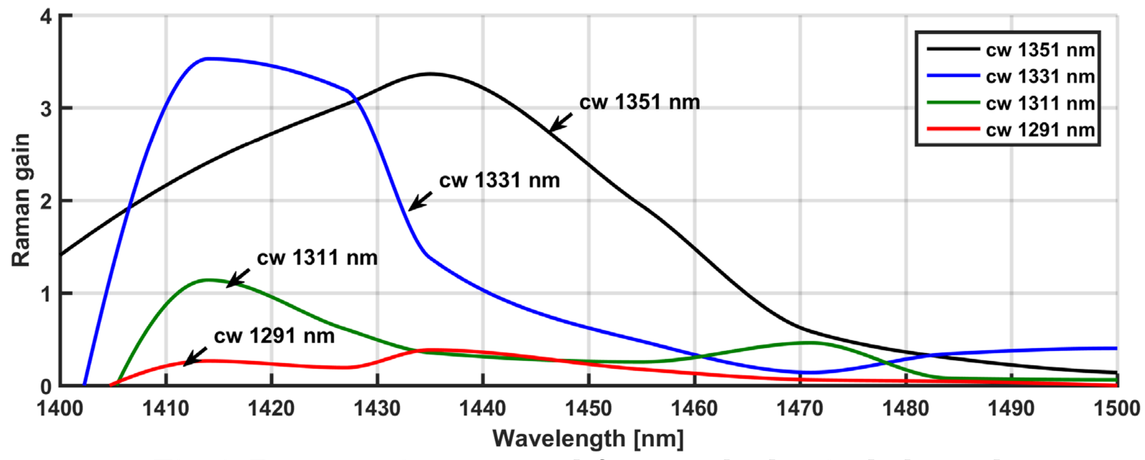


Fig 4. Raman gain generated from each classical channel

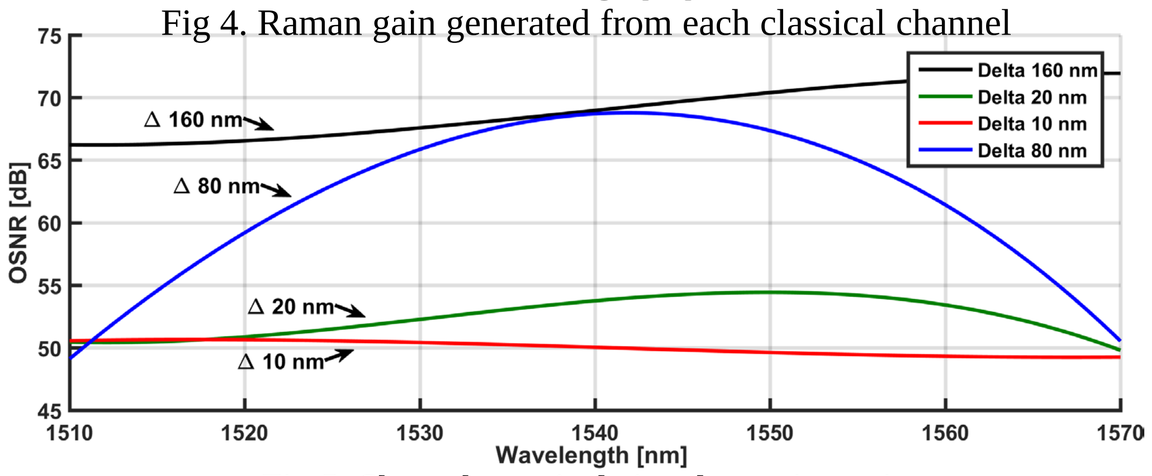


Fig 5. Show the optical signal to noise ratio

References:

1- C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci., vol. 560, no. P1, pp. 7–11, Dec. 2014.

2- A. Ciurana, et al, "Entanglement Distribution in Optical Networks," IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 37–48, May 2015.