DETERMINISTIC AND EFFICIENT THREE-PARTY QUANTUM KEY DISTRIBUTION

Muneer Alshowkan, Khaled Elleithy

Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT, USA

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 telecom metropolitan optical network.

KEY IDEA AND HYPOTHESIS

- Quantum Cryptography
- Quantum key distribution
- Quantum teleportation consumes two cbits and ebits
- Remote state preparation consumes one cbit
- Key distribution between untrusted parties
- Secure and efficient secret key establishment
- Entanglement distribution in an optical network

DOMAIN AND THE SPECIFIC PROBLEM

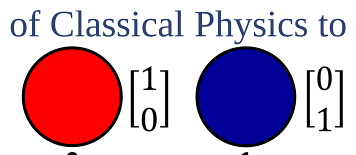
- Domain: Quantum key distribution
- Specific Problem:
- Finding a secure and efficient entanglement-assisted three-party quantum key distribution protocol
- How to share secret keys between two untrusted to each other parties?
- The problem of distributing entanglement in typical telecom metropolitan optical network
- How can we have a centralized EPR source to creates and distributes entanglement to users in different access networks
- Is it possible to create a dynamic network using reconfigurable optical add/drop multiplexers to serve the multiple users in different access networks?
- Can classical and quantum signal reliably travel in the same optical fiber?

METHODOLOGICAL APPROACH

- Using the formal methodological approach to create a three-party quantum key distribution
- Design simulate optical network architecture for entanglement distribution in a metropolitan optical network

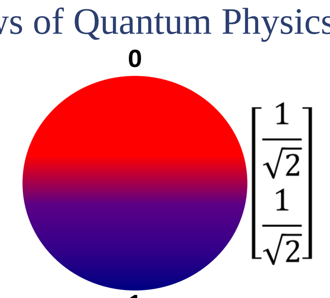
CONVENTIONAL AND QUANTUM COMPUTING

- Conventional Computing
  - Systems depend on laws of Classical Physics to perform calculations.



$\begin{bmatrix}1\\0\end{bmatrix}$ $\begin{bmatrix}0\\1\end{bmatrix}$

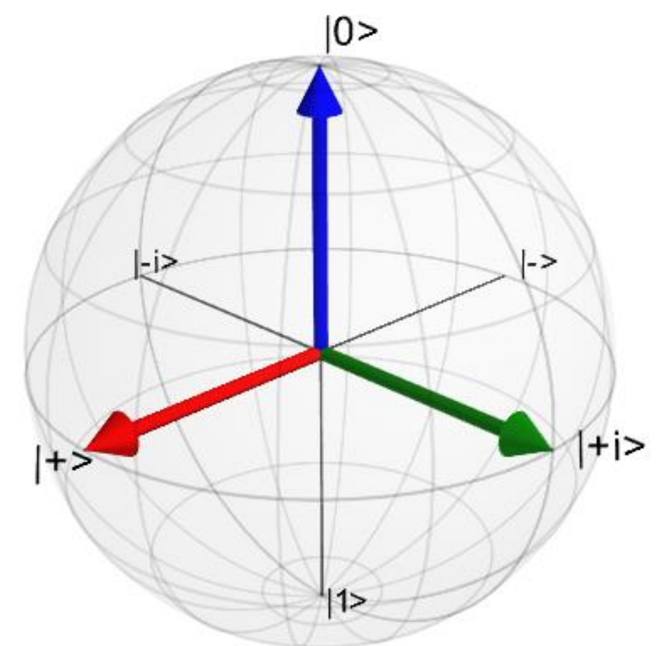
- Quantum Computing
  - Systems depend on the laws of Quantum Physics to perform calculations



$\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix}$

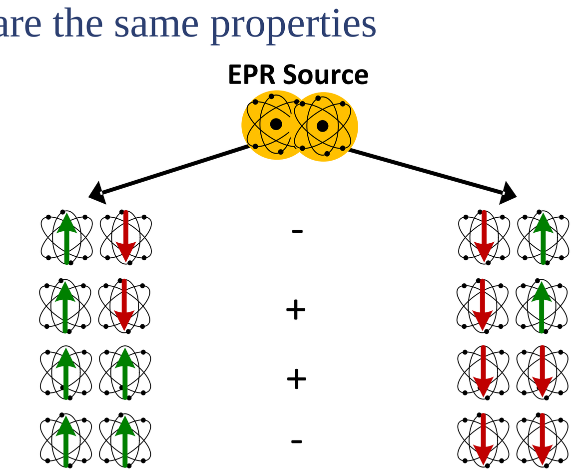
QUBITS AND QUANTUM BASES

- Qubit is linear combination
  - $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Computational Basis:
  - $|0\rangle = cos\,\theta|0\rangle + sin\theta|1\rangle$
  - $|1\rangle = cos\,\theta|0\rangle - sin\theta|1\rangle$
- Qubit Basis:
  - $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$
  - $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- Qubit Basis:
  - $|+i\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$
  - $|-i\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$



QUANTUM ENTANGLEMENT

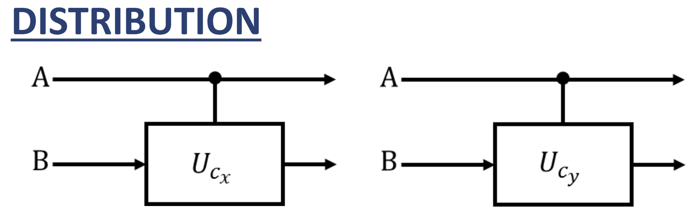
- Describe a pair of particles share the same properties
- Bell States/EPR Pairs:



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

DETERMINISTIC AND EFFICIENT THREE-PARTY 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



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

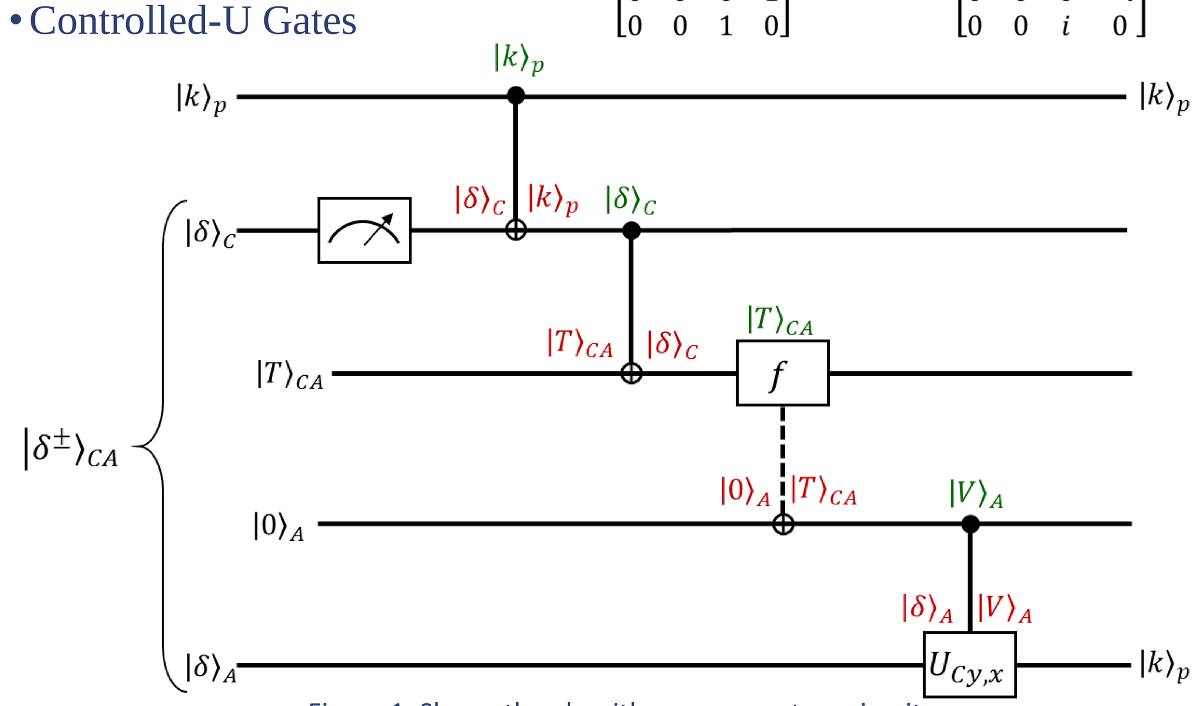


Figure 1. Shows the algorithm as a quantum circuit

- Intrinsic efficiency

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

$* \; q_s$ qubits $\quad * \; q_u$ ebits $\quad * \; b_t$ cbits

Table 1. Comparing the performance to the literature

Protocol	Operations	Qubit/Type	ebit/Type	cbit	η
Ref. [44]	2-Proj M, 2-U. Op	2-Eq	6-Triparatite	2	1/4
Ref [42]	1-Proj M, 2-U. Op	2-Eq	6-Triparatite	2	1/4
Ref [51]	1-Proj M,1-BSM, 3-U. Op	2-Eq	6-GHZ	3	2/9
Ref [45]	2-Proj M, 3-U. Op	2-Eq	6-GHZ	2	1/4
Ours	1-Proj on 2-P M, 2-U. Op	2-Eq	4-EPR	1	2/5

Quantum Entanglement Distribution for Secret Key Establishment in Metropolitan Optical Networks

- Entanglement Distribution in MON
  - Backbone network
  - Backbone nodes
  - Access network
- Centralized EPR source
  - Classical signals
  - Quantum signals
- Simultaneous transmission of classical and quantum signals
  - Four-Wave mixing
  - Raman scattering

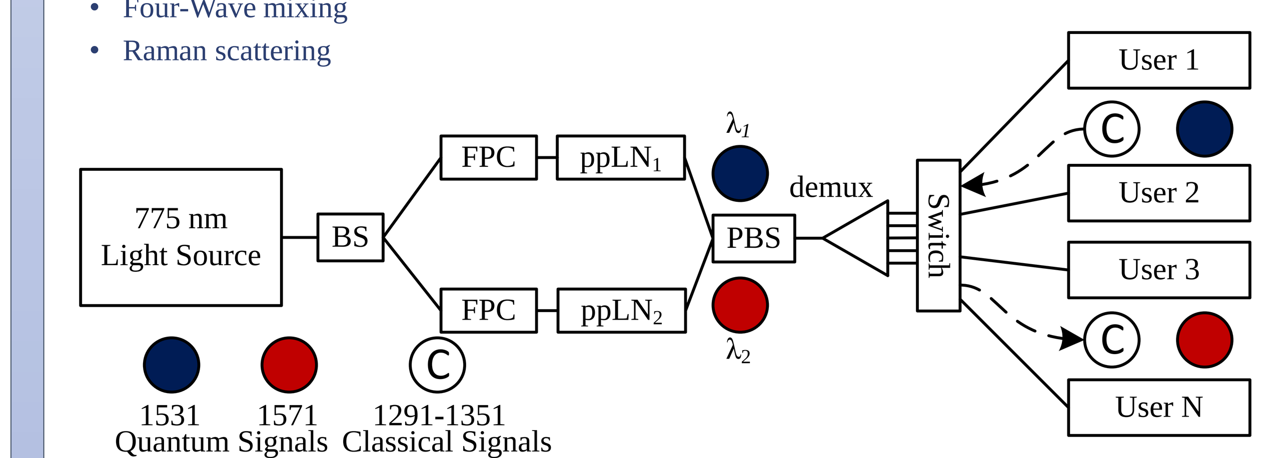


Figure 2. Entanglement distribution in an access network

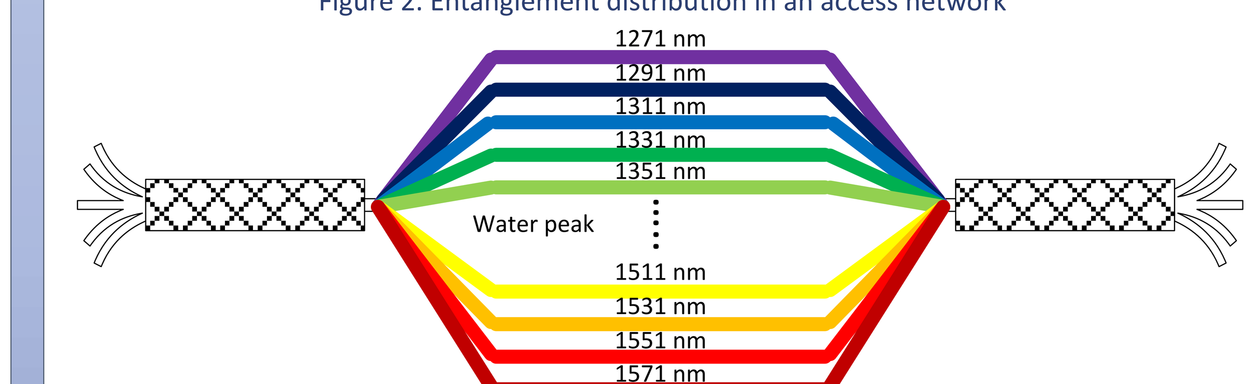


Figure 3. The range of classical and quantum channels

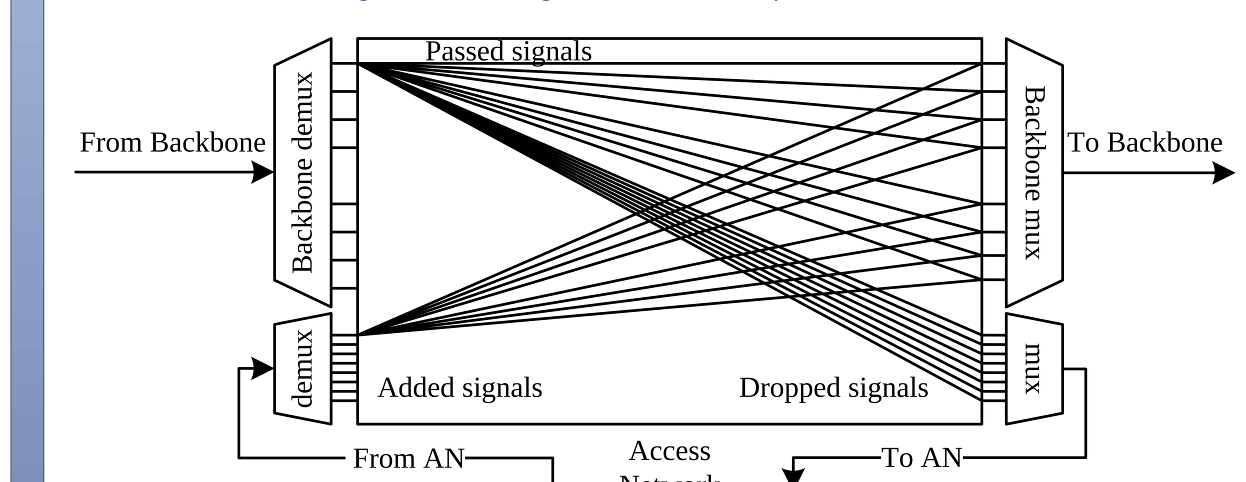


Figure 4. Design of the backbone node (ROADM)

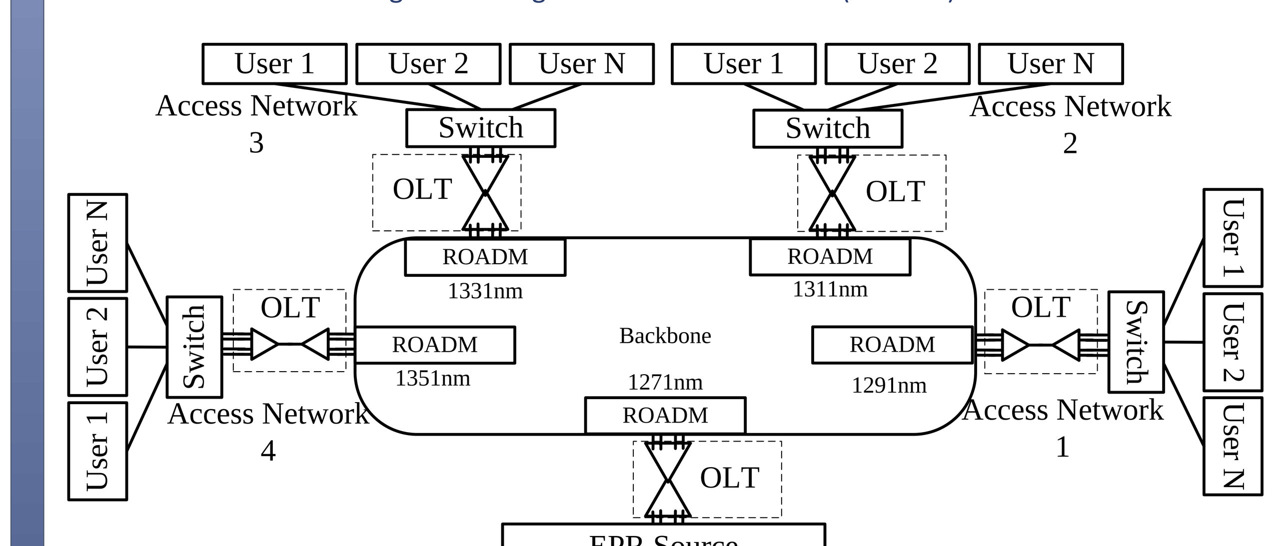


Figure 5. The architecture of the metropolitan optical network (MON)

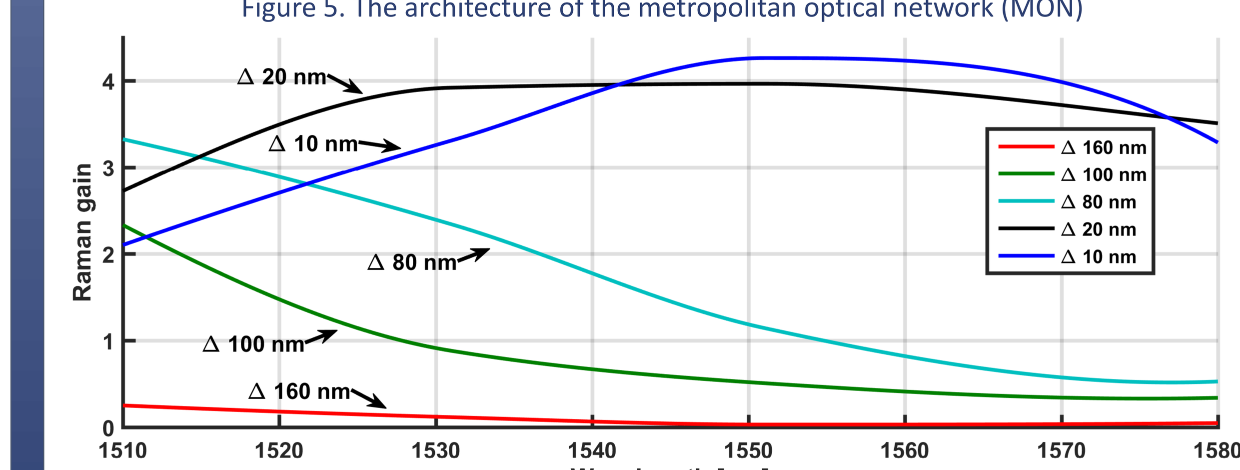


Figure 6. Raman gain in various spacing settings

RESULTS

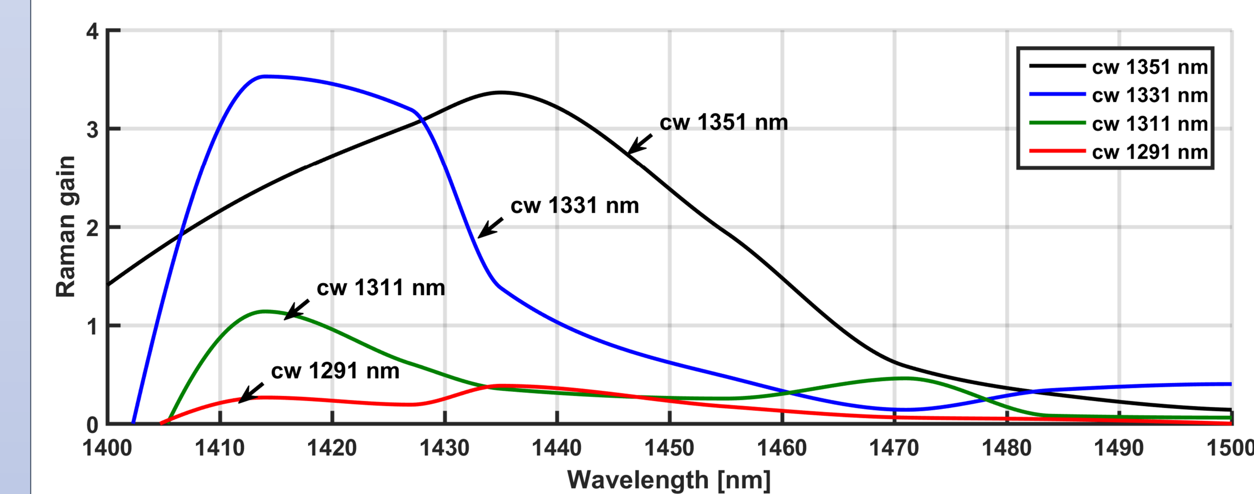


Figure 7. Raman gain generated from each classical channel

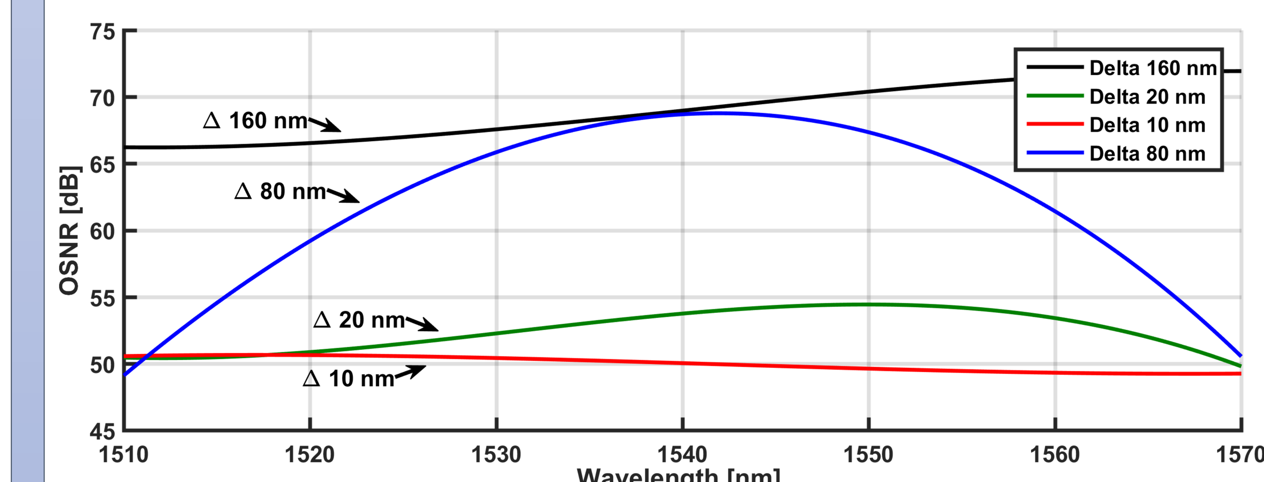


Figure 8. Show the optical signal to noise ratio

CONCLUSION

- Deterministic and efficient three-party QKD
- The protocol uses:
  - Two maximally entangled states
  - One two-particles von Neumann.
- Introduced the parity bit
- Introduced ancillary
- Introduced the U_{cx} and U_{cy} gates
- The protocol is exact and deterministic
- Compared related protocols
- Distributes a key of d qubits by $2d$ entangled pairs and d cbits
- Quantum entanglement distributing entangled in MON
- Centralized entanglement source serves the entire network
- Wavelengths that correspond to channels in the CWDM
- Dynamic entanglement distribution:
  - Drop
  - Pass
  - Add
- Simultaneous transmission of classical and quantum signals
- Increased the number of access networks

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell system technical journal, vol. 28, pp. 656-715, 1949.

[2] 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.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical review letters, vol. 67, pp. 661, 1991.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete on a quantum computer," SIAM journal on computing, vol. 26, pp. 1484-1509, 19logarithms97.

[5] 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, Mar. 1993.

[6] M. Alshowkan and K. Elleithy, "Quantum mutual authentication scheme based on Bell state measurement," in IEEE Long Island Conference (LISAT), Long Island, pp. 1-6, 2016.

[7] A. Ciurana, V. Martin, J. Martinez-Mateo, B. Schrenk, M. Peev, and A. Poppe, "Entanglement Distribution in Optical Networks," IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 37–48, May 2015.

[8] M. Alshowkan and K. Elleithy, "Quantum Entanglement Distribution for Secret Key Establishment in Metropolitan Optical Networks," in IEEE International Conference (NAS), Long Beach, pp. 1-8, 2016.