Multi-User Quantum Communication Networks

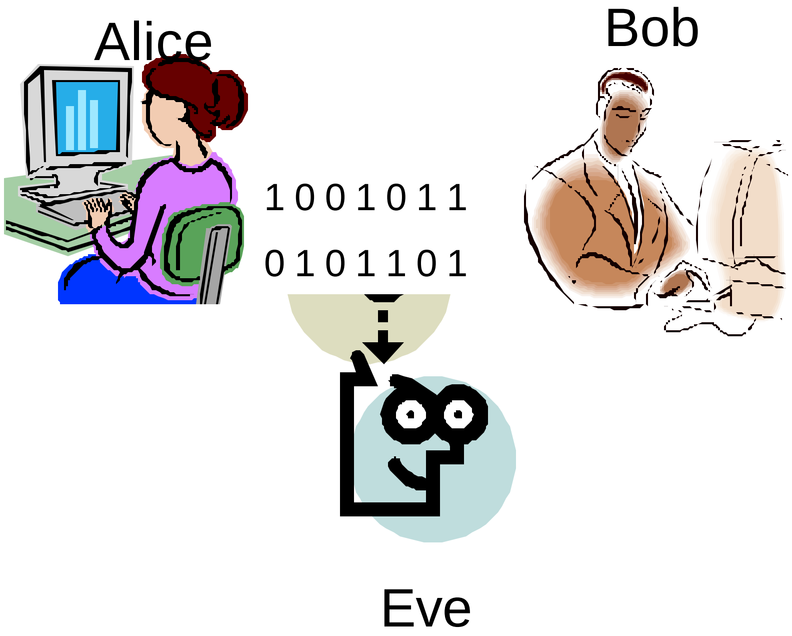
Bing Wang, Patrick Kumavor, Craig Beal, Susanne Yelin*

Electrical & Computer Engineering Department, University of Connecticut, Storrs, CT 06269

***Physics Department, University of Connecticut**

Quantum Key Distribution

- Traditional 128bit (mathematical) public key encryption are highly susceptible to decryption by powerful computers
- Perfect Encryption is possible with Vernam Cipher, (aka One Time Pad)
- Quantum Key Distribution: Secure distribution of encryption keys possible using quantum bits, or Qubits
- Security of QKD is independent of computing power.
- Security of QKD based on fundamental Quantum Mechanical principles: the uncertainty principle and the no-cloning theorem.
- Any attempt to eavesdrop will be immediately detected.



Encryption

Alice

Message:	1 1 0 0
Key:	1 0 1 0
Encrypted Message:	0 1 1 0
Key:	1 0 1 0
Decrypted Message:	1 1 0 0

Eve

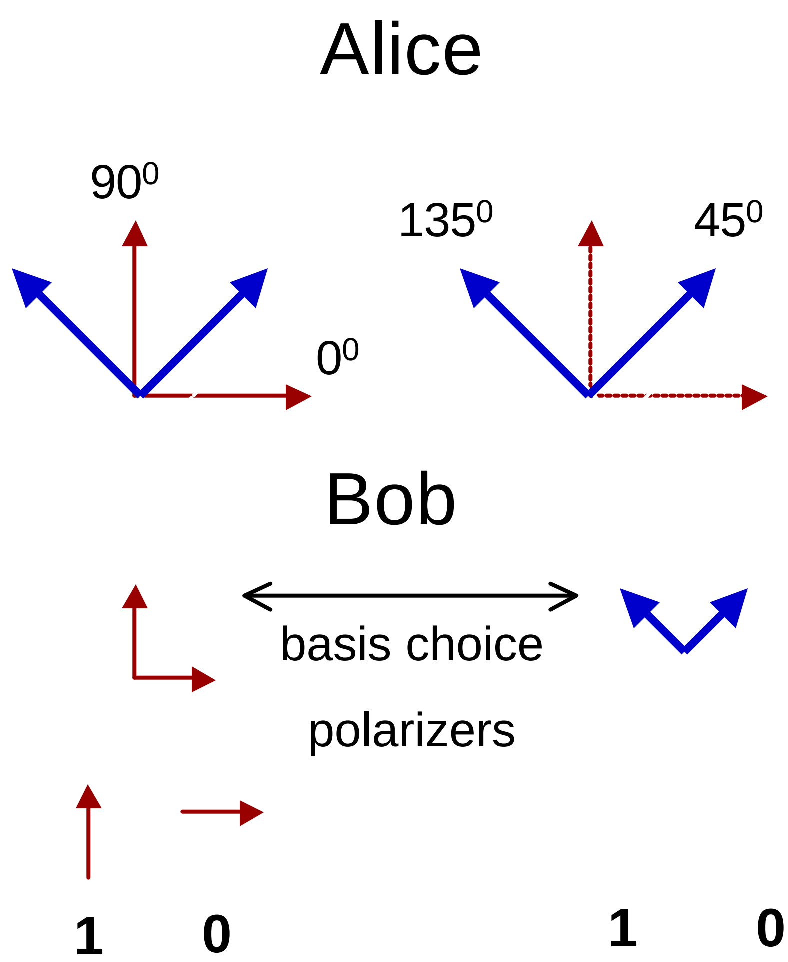
Bob

If key only used ONCE (One Time Pad), then encryption is secure, but…….

Problem of Key Distribution

Quantum Key Distribution

- QKD transmits photon in two non-orthogonal basis sets, such as Polarization or Phase
- Polarization: "Alice" transmits in [0,1] in 1st basis as 0 & 90^0 and [0,1] in 2nd basis as 45^0 & 135^0
- "Bob" chooses the between the two basis randomly. Bob's choice will coincide with Alice's in 50% of the time
- After photons are sent, Alice and Bob communicate over public channel on which basis was used.
- Bob keeps qubits detected using same basis



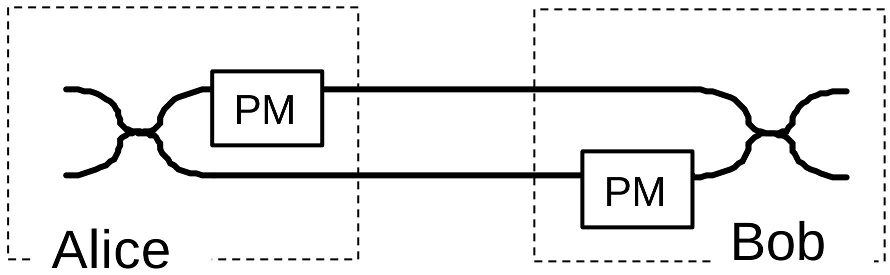
Quantum Key Distribution

- !! Alice does NOT send quantum encryption key to Bob !!
- The key is created when Bob and Alice decides on their basis choice AFTER the qubit photons are transmitted.
- Eavesdropper Eve cannot know which basis to use because it's decided AFTER transmission.
- If Eve taps the channel, the quantum bit error rate, or QBER, will increase significantly, alerting Alice and Bob of Eve's presence.
- Phase encoded QKD uses interferometer instead of polarized light and polarizers

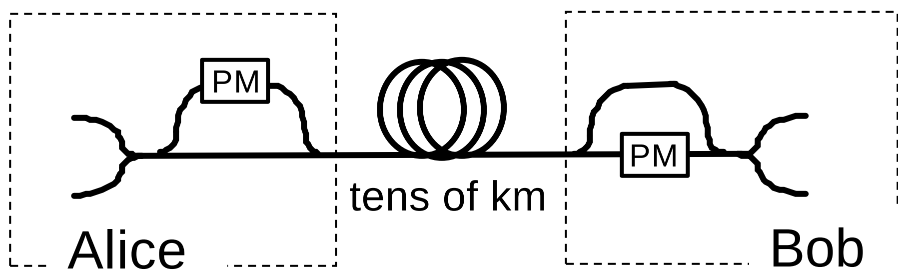
Phase Encoded QKD

- Phase encoded QKD uses interferometers
- Phase encoded QKD more practical in optical fiber systems due to polarization mode dispersion (PMD) in fiber.
- First demonstrated using a collapsed Mach-Zehnder optical fiber interferomter

Mach-Zehnder Interferometer



Collapsed Mach-Zehnder Interferometer



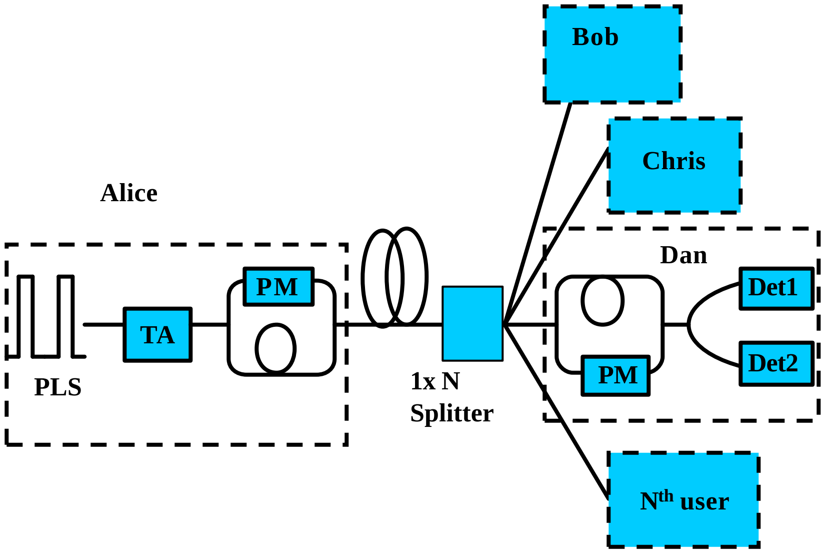
Current efforts in quantum key distribution

- Present QKD research focuses on
  - New quantum protocols
  - Free-space implementation
  - Compatibility with existing state-of-the-art optical network communication technologies
- Current efforts include
  - Research groups: University of Geneva, Los Alamos National Lab, IBM research, Northwestern University
  - Start-up companies: MagiQ Technologies Inc, id-Quantique
  - Telcordia Technologies (working with Los Alamos), focuses on having 1.3mm quantum channels and 1.55mm classical optical communications on same fiber
  - BBN Technologies (Darpa funded), has multi-user testbeds, linking Harvard, Boston University, and BBN
  - ***Special section at OFC 2005 dedicated to Quantum Information.***
  - ***Our work published in Jan 05 issue of Journal of Lightwave Technology***

QKD with network topologies

- Network topologies to be compared are
  - Passive star
  - Optical ring based on Sagnac interferometer
  - Wavelength-routed
  - Wavelength-addressed bus
- Single photon source approximated by highly attenuated coherent laser light
- Single photon detectors are avalanche photodiodes that are gated and operating in Geiger mode
- Alice encodes the transmitted photons using her phase modulator
- Bob measures photons with his phase modulator and single photon detectors
  - He assigns each detector with a bit value (0 or 1)
  - Knowing the phase shift he applies, he can infer from the detector that fired the phase shift and consequently the bit value Alice sent

Passive star network topology

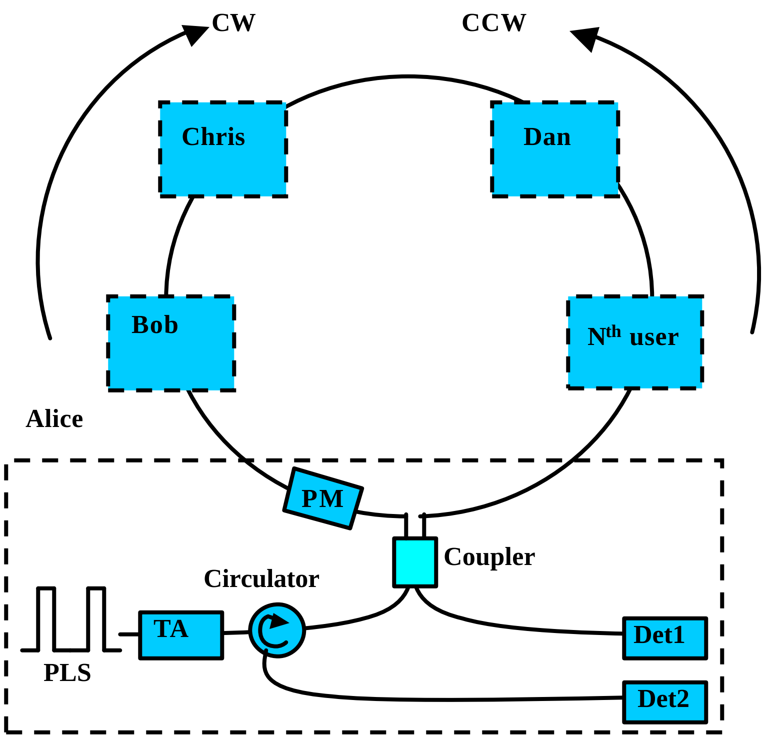


PLS- Pulsed laser source
PM- Phase modulator
TA- Tunable attenuator
Det- Detector

- Passive star network connecting four users first demonstrated by Townsend [2]
- Alice equipped with PLS, TA, and PM
- Each end-user equipped with PM and two Det
- Alice is linked to other users via a 1xN splitter
- Photons are randomly routed to one user at a time since they are indivisible
- “Distance” is defined as the total fiber length spanning Alice and any of the users

[2] P.D Townsend, Nature, 385, 47, (1997)

Optical ring network topology

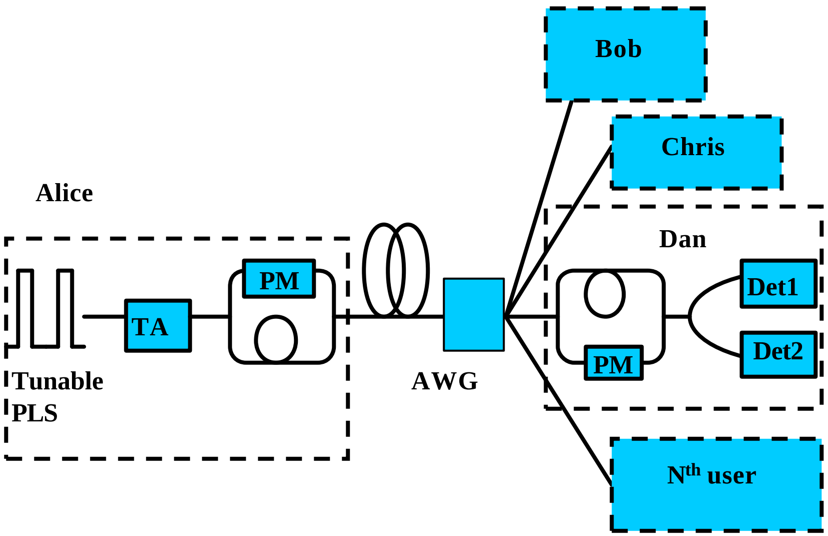


PLS- Pulsed laser source
PM- Phase modulator
TA- Tunable attenuator
Det- Detector
cw (ccw)-clockwise (counter clockwise)

- A two-user QKD system based on optical fiber Sagnac interferometer has been demonstrated by Nishioka et al. [3]
- Alice has PLS, TA, circulator, coupler, and PM
- Each end-user equipped with a PM
- Alice's circulator directs photons to the fiber loop and they traverse in both the cw and ccw directions
- Upon exiting loop, photons that take left turn are directed by circulator to Det2; those that take right go to Det1
- There is a control mechanism so that only one user can modulate photon at a time
- "Distance" is defined as the length of fiber loop

[3] T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, IEEE Photonics Technology Letters, 14, 576 (2002)

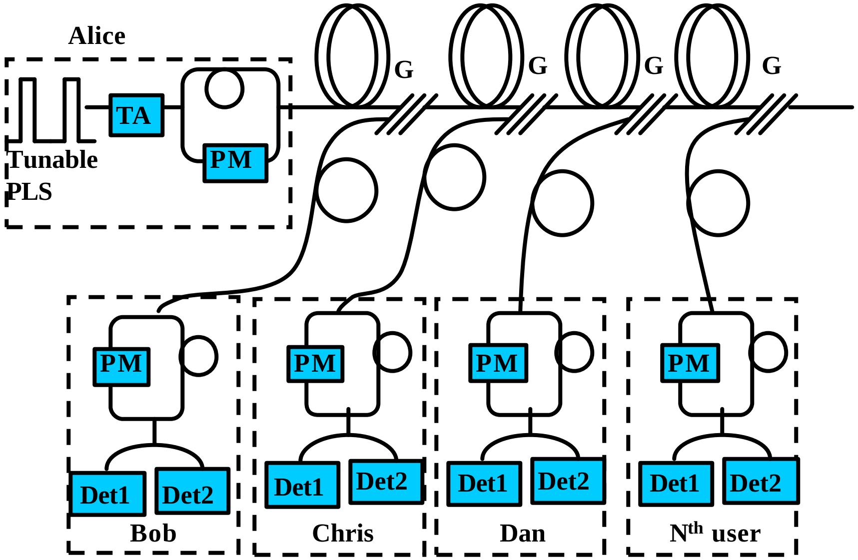
Wavelength-routed network topology



- Alice's end consist of wavelength-tunable PLS, TA, and PM
- Each end-user has PM and two Det
- Network users each apportioned a separate wavelength channel
- Alice communicates with users via the AWG by tuning her laser to the corresponding wavelength
- "Distance is defined as the total fiber length spanning Alice and any user

PLS- Pulsed laser source
PM- Phase modulator
TA- Tunable attenuator
Det- Detector
AWG- Arrayed waveguide grating

Wavelength-addressed bus network



PLS- Pulsed laser source
PM- Phase modulator
TA- Tunable attenuator
Det- Detector
G- Fiber bragg grating

- Alice's end is made up of tunable PLS, TA, and PM
- End-users each have PM and two Det
- Every user assigned a separate wavelength channel
- Each G is designed to match the wavelength of each user and reflects photons with wavelength corresponding to intended recipient, but otherwise transmits it
- Alice communicates with a particular user by tuning her laser to the wavelength designated for that user and sending the photon
- "Distance" is defined as total fiber length between Alice's and the end-users' ends

Quantum bit error rate (QBER)

- Quantum bit error rate (QBER)
  - $$QBER = (mThP_{opt} + P_{dark})/(mTh + 2P_{dark})$$

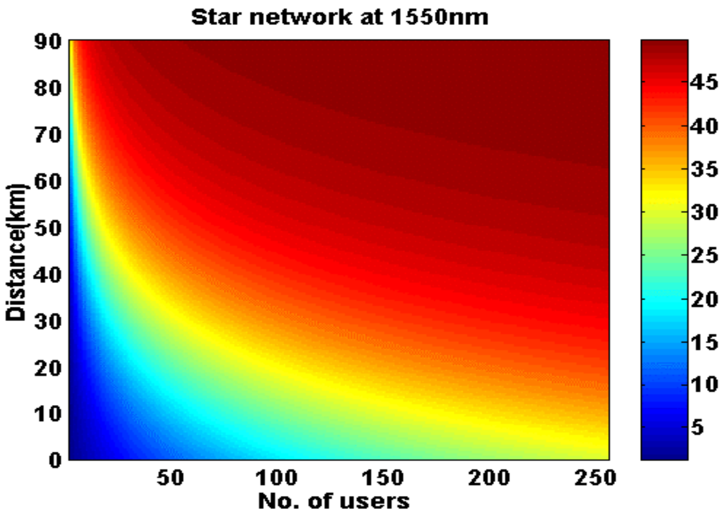
m - mean photon number
T - transmission coefficient of link
h - detector efficiency
P_{opt} - probability of photon going to wrong detector
P_{dark} - dark count probability
f - repetition frequency

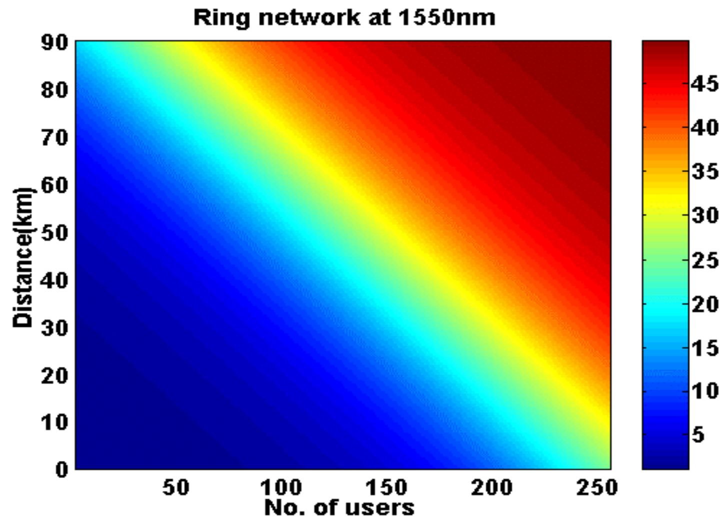
- Network topologies are compared using analysis of their QBER
- High QBER values result in decreased total number of keys available for encrypting data
- Networks with QBER > 15% vulnerable to eavesdropping

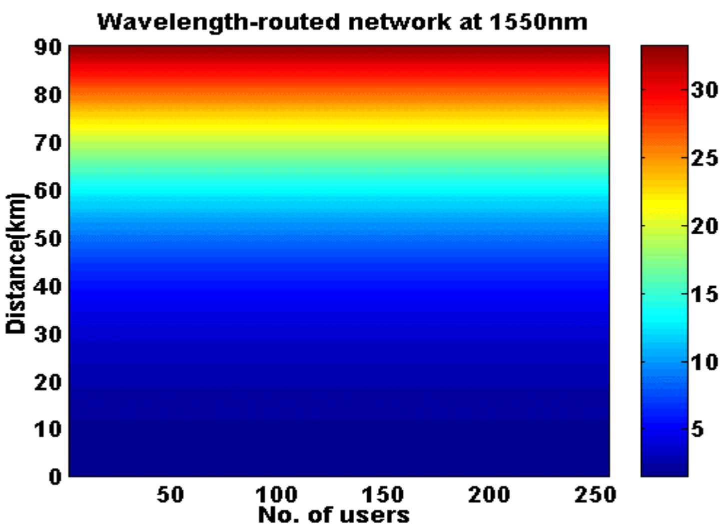
For secure communication, QBER < 15%

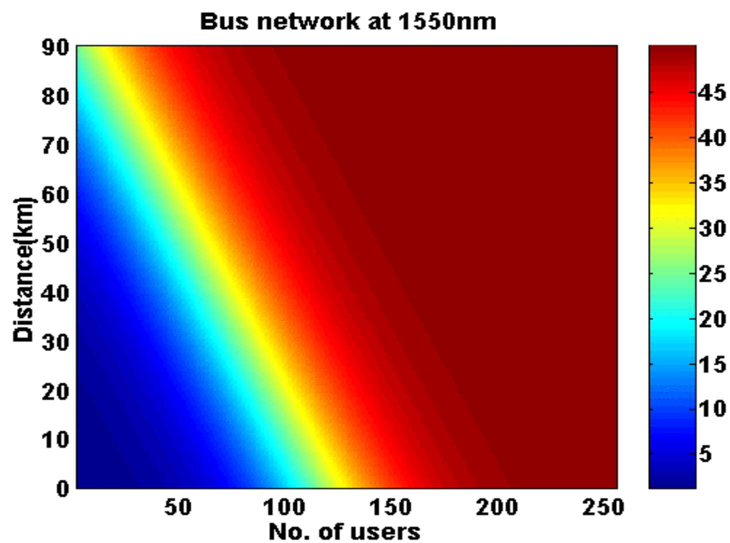
***"Quantum Cryptography" Nicholas Gisin, Reviews of Modern Physics, January 2002.**

Comparison of the four networks @ 1550nm

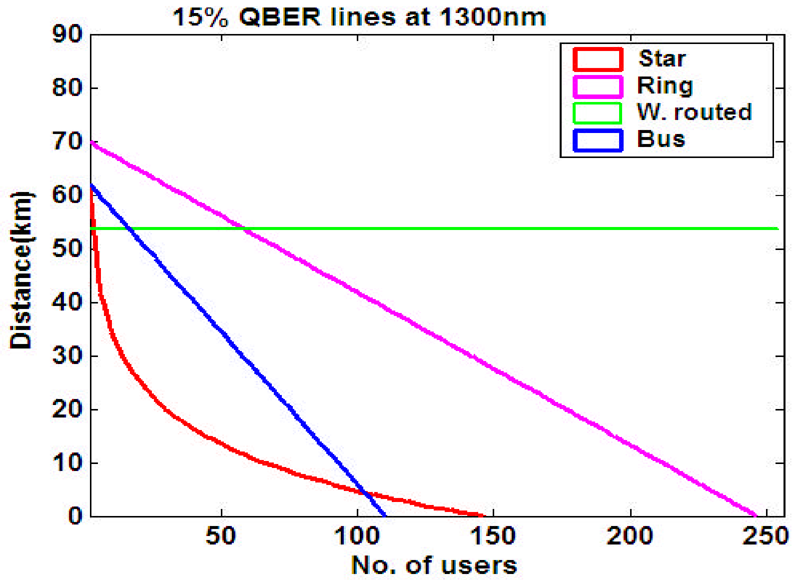








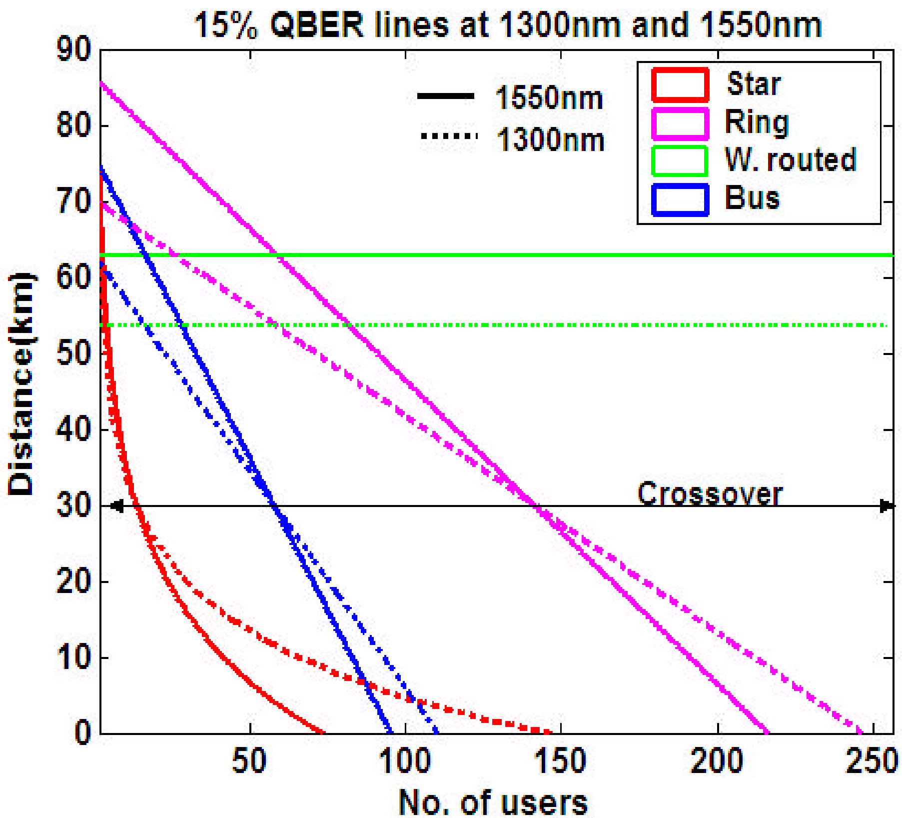
Comparison of topologies at 1300nm



	Maximum distance for secure communication (km)			
No. of users	Star	Ring	W. routed	Bus
1,2	60,54	70	54	62
3-17	28-54	65-70	54	54-62
18-59	12-28	54-65	54	30-54
60-102	5-12	42-54	54	5-30
103-128	2-5	34-42	54	0-5

Maximum distance available for secure key distribution with number of users on network

Comparison of topologies at 1300nm and 1550nm



Maximum distance for secure communication vs. number of users at wavelengths of 1550nm and 1300nm

- 1300nm and 1550nm lines cross each other at distance of 30km (crossover)
- Distances > crossover distance ⇒ QKD at 1550nm better
- Distances < crossover distance ⇒ QKD at 1300 nm better
- For wavelength-routed network, 1300nm and 1550nm lines do not cross each other (parallel lines); QKD at 1550nm is always better than QKD at 1300nm
- This mainly has to do with assumptions in fiber-loss and detector effeciency in the model

Conclusions

- Star network
  - 1xN splitter acts as 1/N attenuator and hence not suited for large networks
  - Easy to implement
- Ring network
  - Definition of “distance” limits actual (point-to-point) distance between users
  - Not affected by phase and polarization fluctuations
  - Easily configured to accommodate more users
- Wavelength-routed network
  - Size of network limited by AWG bandwidth channel
  - AWG loss approximately uniform with number of wavelength channels and hence number of users on network. Best suited for networks with large users
- Bus network
  - Grating inserted into network for every user added makes system more lossy and hence not suitable for large networks
  - Easily configured to accommodate more usersAcknowledgement

Conclusions

- Simulations assumes present COTS device technology
  - Present work on single photon detector can increase quantum efficiency
  - Single photon generator, (Number or Fock state generators) can increase mean photon number from $\mu = 0.1$ to $\mu = 1$, adding 10dB margin
- Theoretical work
  - Quantum repeaters still theoretical. Many many years until a usuable networking device
- Main interests
  - Those that require a future proof encryption scheme
    - **Present state of the art encryption vulnerable to near-future computers capable of peta-flop calculations**
    - **Adversaries can store data for 10-20 years, until such computers are available**
  - Financial community
  - Government and Defense applications
- Acknowledgement
  - NSF-ITR and ARO for research funding