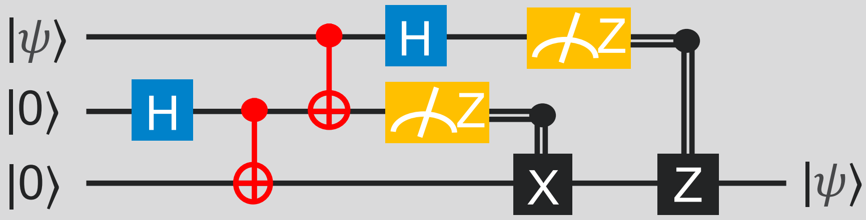
ARGONNE QUANTUM COMPUTING TUTORIAL

Argonne NATIONAL LABORATORY

INTRODUCTION TO QUANTUM NETWORKING

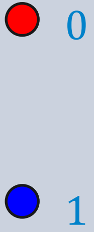
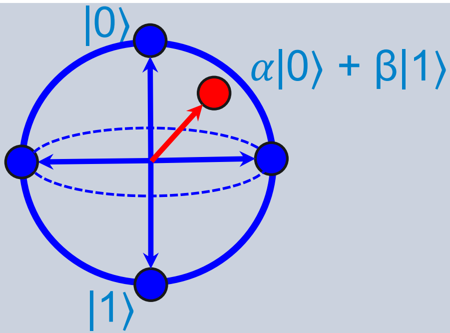


MARTIN SUCHARA

Argonne National Laboratory
msuchara@anl.gov

December 11, 2018
Lemont, IL

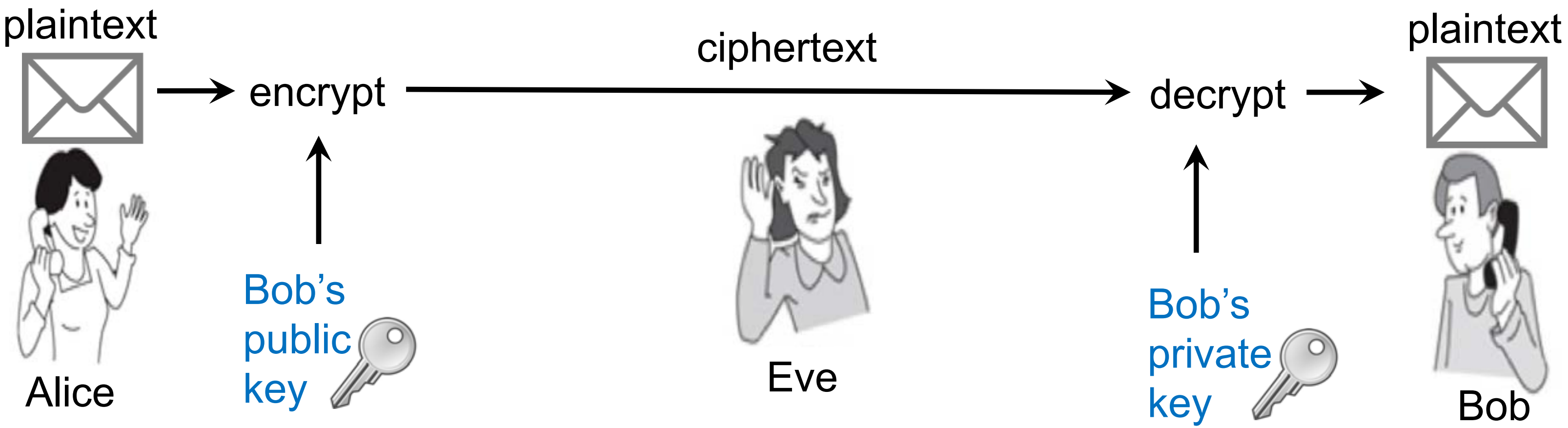
QUANTUM TECHNOLOGIES ARE A BIG THREAT AND OPPORTUNITY FOR NETWORK SECURITY

Classical bit:	Qubit:	Multi-qubit systems:
		2 qubits: $\alpha\|00\rangle + \beta\|01\rangle + \gamma\|10\rangle + \delta\|11\rangle$ 3 qubits: $\alpha\|000\rangle + \beta\|001\rangle + \gamma\|010\rangle + \delta\|011\rangle + \varepsilon\|100\rangle + \zeta\|101\rangle + \eta\|110\rangle + \theta\|111\rangle$

- Quantum computing uses the rules of quantum mechanics to manipulate quantum information
  - Exponential speedup for some computational problems
  - Allows secure information transmission on telecommunication fiber

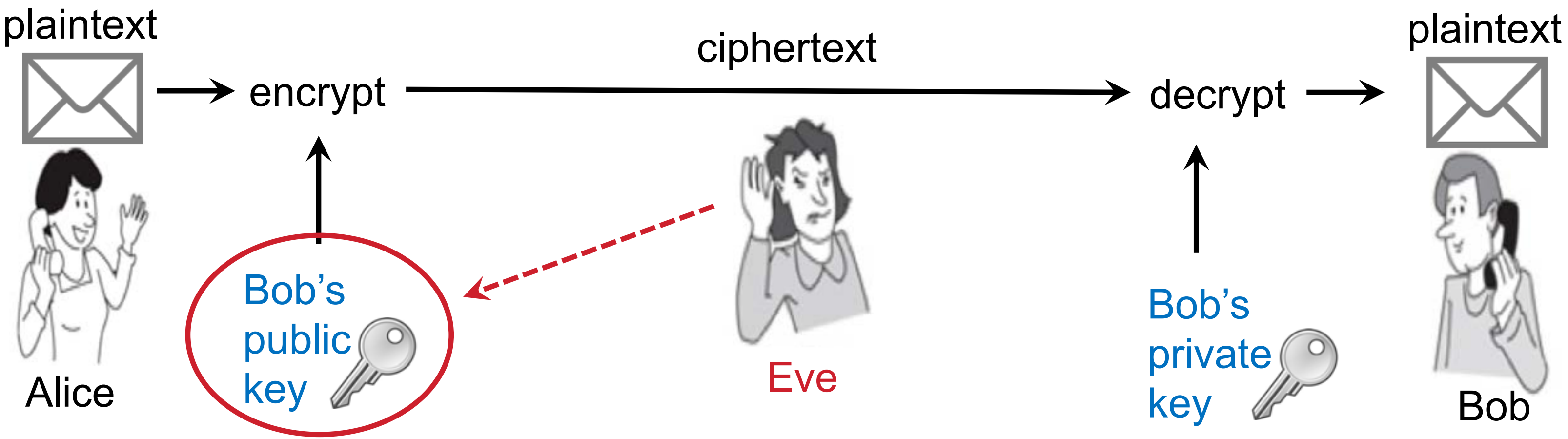
PUBLIC KEY CRYPTOGRAPHY

- No need for Alice and Bob to share a common secret
- Bob conveys his public key in a public communication and Public Key Infrastructure (PKI) ensures that they key belongs to Bob
- Cryptographic protocols: RSA, DSA, DH, ECDH, ECDSA, etc.



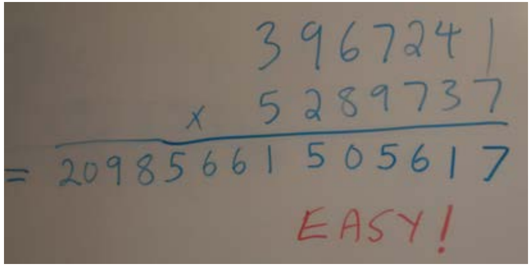
SHOR'S FACTORING ALGORITHM BREAKS PUBLIC KEY CRYPTOGRAPHY

- In 1994 Peter Shor at AT&T Labs discovered a quantum factoring algorithm with exponential speedup that breaks all major public-key cryptosystems
- Algorithm can be used to factor integers and solve discrete logarithm problem

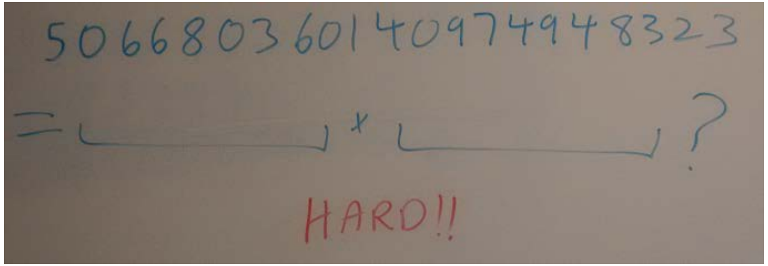


SHOR'S FACTORING ALGORITHM

- Old paradigm:

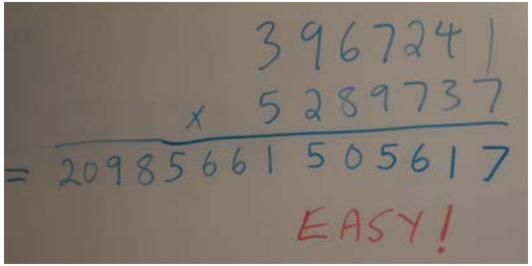


Encrypting is easy

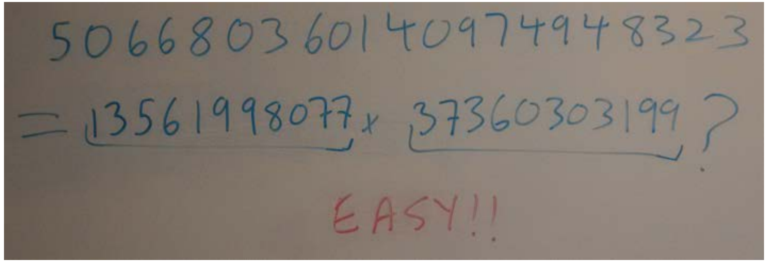


Codebreaking is hard

- Quantum paradigm:



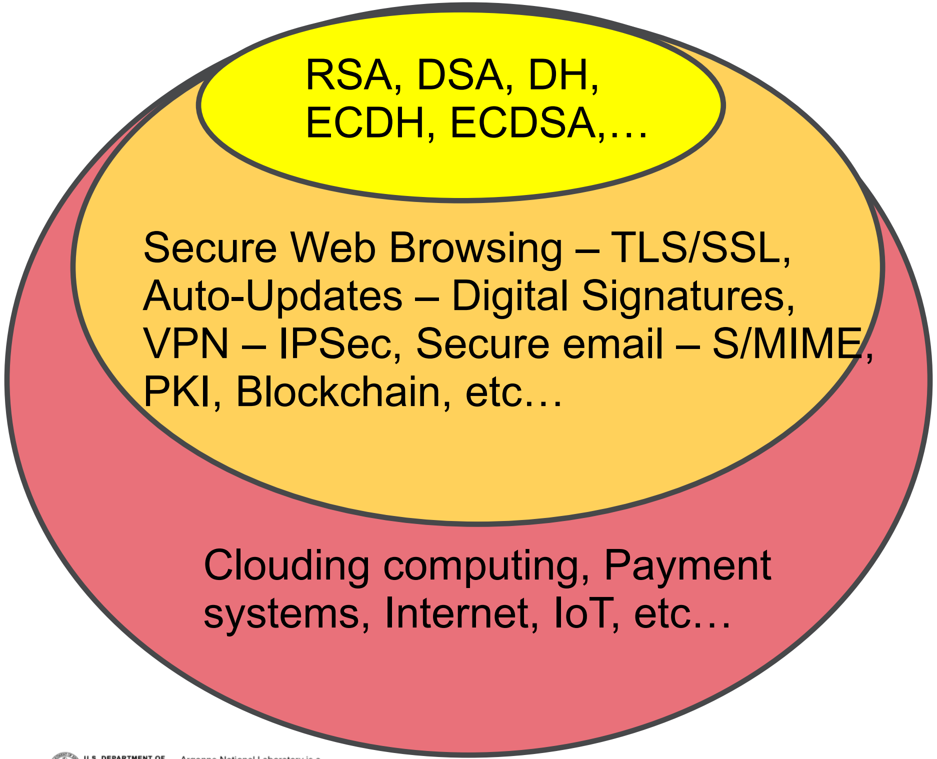
Encrypting is easy



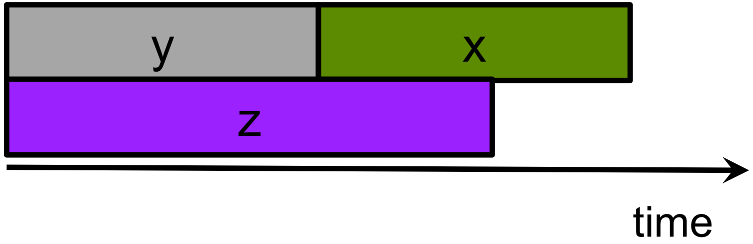
Codebreaking is **easy!**

DO WE NEED TO WORRY?

What will be affected:



- Security shelf-life: ***x years***
- Time to re-tool the existing infrastructure: ***y years***
- How long to build a large-scale quantum computer: ***z years***
- "Theorem": If **x** + **y** > **z**, then worry



M. Mosca: e-Proceedings of 1st ETSI Quantum-Safe Cryptography Workshop, 2013

WHAT IS ‘z’?

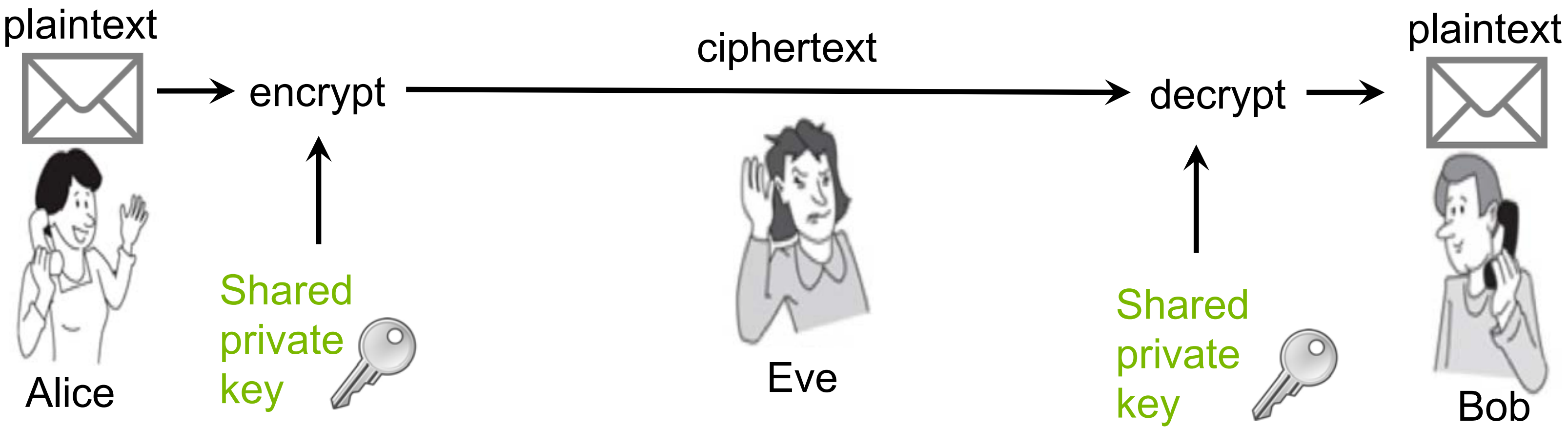
- Michele Mosca [Oxford, 1996]: *“20 qubits in 20 years”*
- Microsoft Research [October 2015]: *”Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade”*
- Michele Mosca ([NIST, April 2015], [ISACA, September 2015]): *“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”*
- Michele Mosca [London, September 2017]: *“1/6 chance within 10 years”*
- Simon Benjamin [London, September 2017]: *Speculates that if someone is willing to “go Manhattan project” then “maybe 6-12 years”*

WHAT CAN WE DO NOW?

- NSA will discontinue the use of public-key cryptosystems such as RSA, DH and DSA for classified information.
- **Alternatives:**

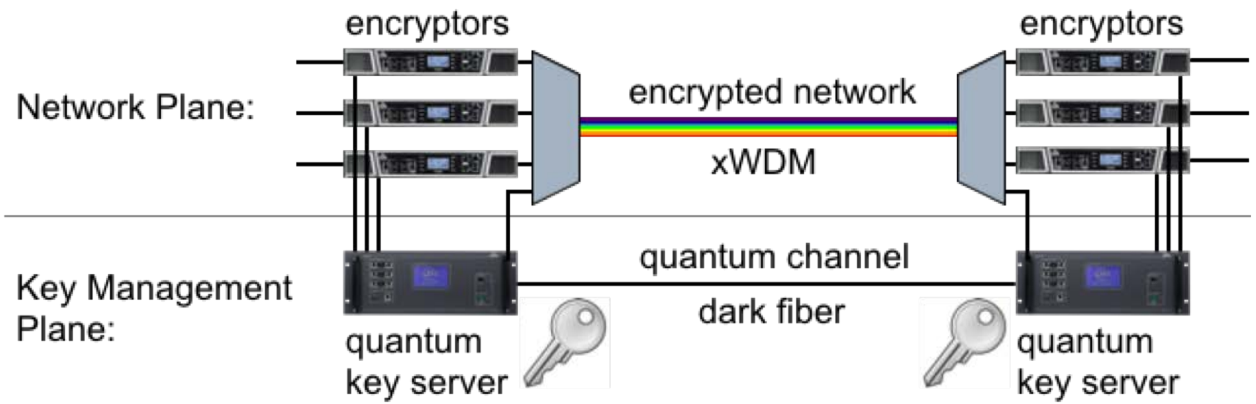
→ **use private-key cryptography**

→ **develop new cryptographic tools**



QUANTUM KEY DISTRIBUTION NETWORKS

- Distributes secret key securely for use with private-key cryptography, offers "perfect" security guarantee



Beijing-Shanghai QKD Backbone

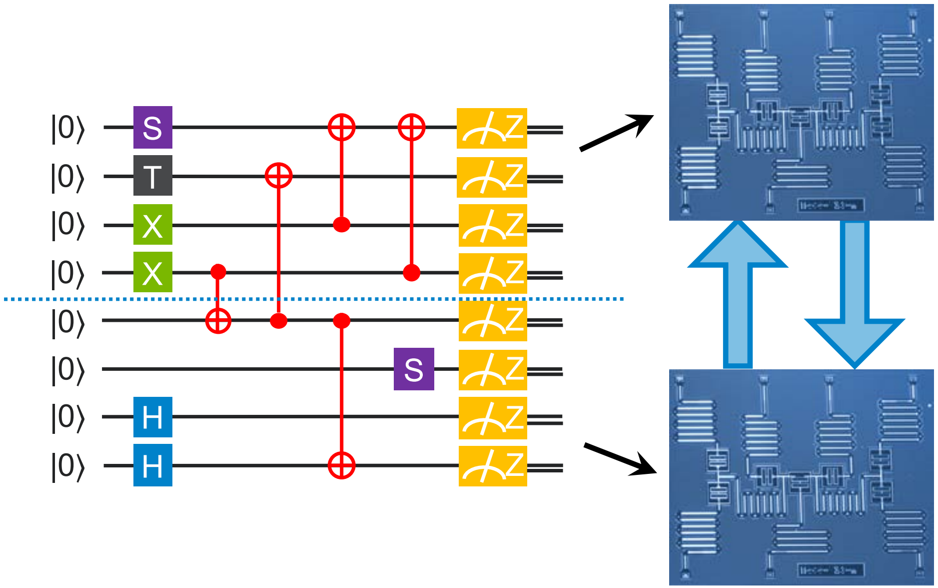
SwissQuantum Network

Tokyo QKD Network

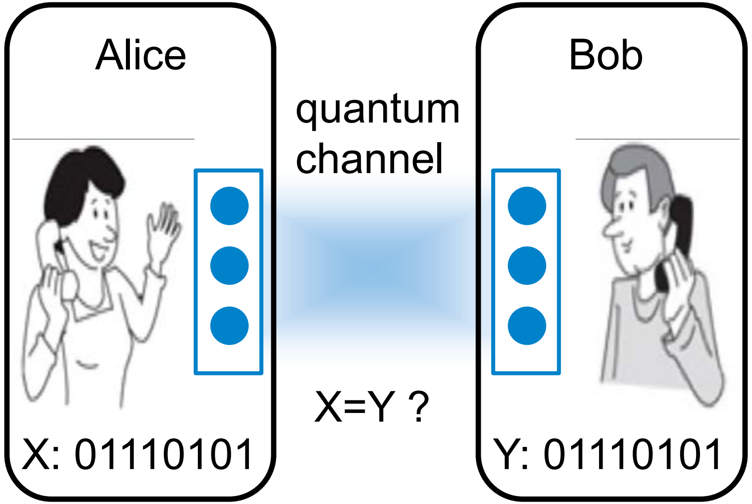
Battelle QKD Network, Columbus, OH

QUANTUM NETWORK APPLICATIONS: DISTRIBUTED COMPUTATION

- Connecting small quantum processors allows solving larger problems:



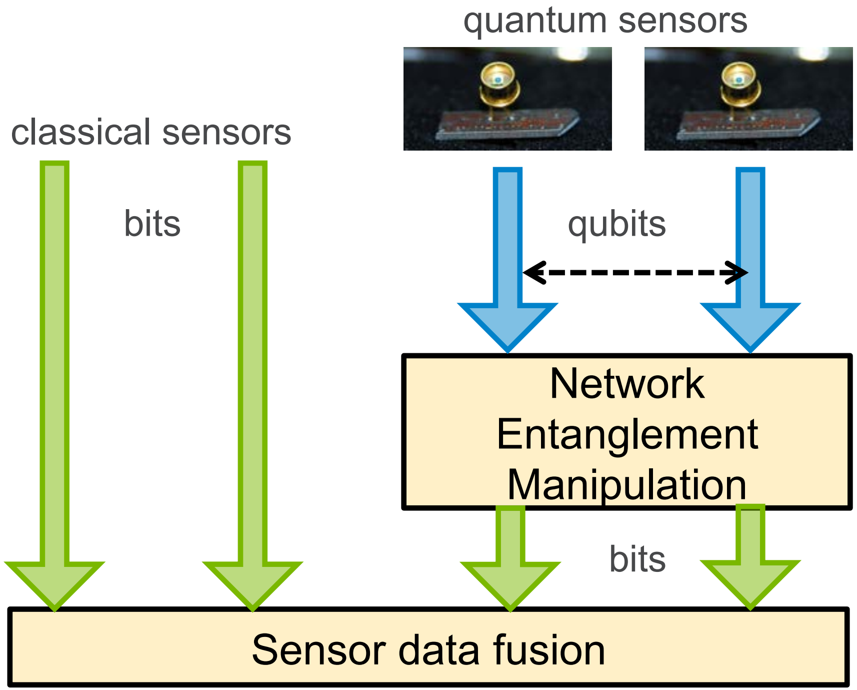
- Some distributed problems can be solved with exponential speedup:



Promise: Hamming distance n/2 or 0

QUANTUM NETWORK APPLICATIONS: SENSING

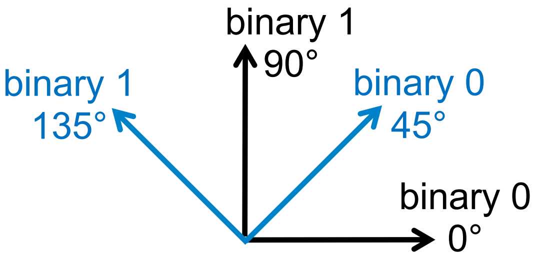
- Quantum sensing uses individual particles (photons, electrons) as sensors in measurements of forces, gravitation, electric fields etc.
- Heisenberg’s uncertainty principle limits the precision; precision is enhanced by shifting the uncertainty to another variable (known as a squeezed state)
- Networked sensors exploit entanglement



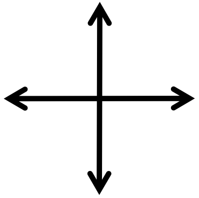
QUANTUM KEY DISTRIBUTION NETWORKS

BB84 PROTOCOL – BENNETT & BRASSARD, 1984

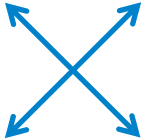
- Goal: exchange secret keys with perfect security
- Works by encoding secret bits in the polarization state of a photon



photon polarization



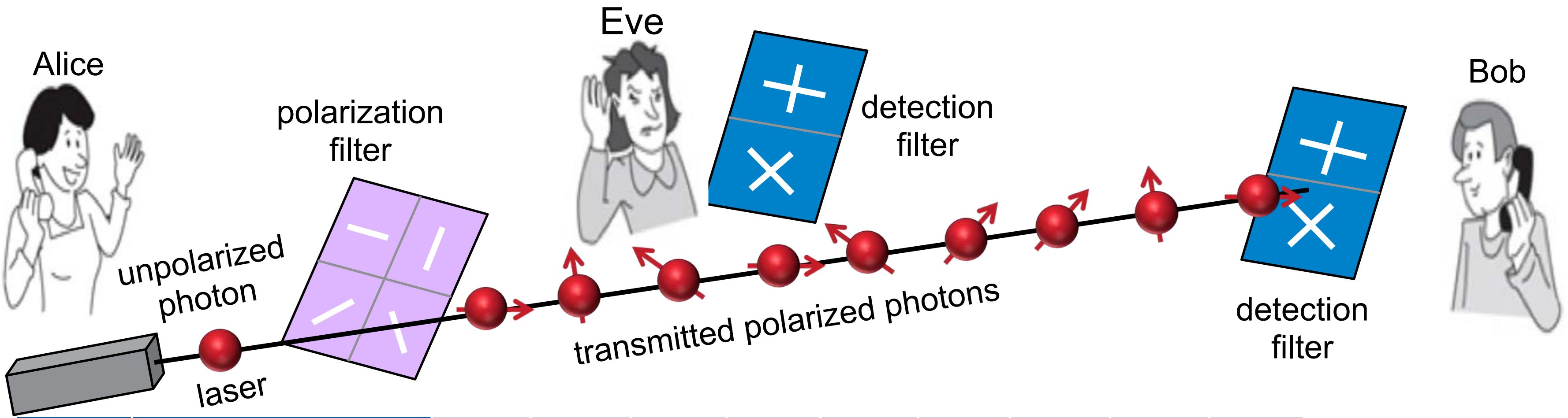
rectilinear basis



diagonal basis

	Measurement in + basis:	Measurement in x basis:
0 encoded in + basis	0	0 or 1 with probability 50%
1 encoded in + basis	1	0 or 1 with probability 50%
0 encoded in x basis	0 or 1 with probability 50%	0
1 encoded in x basis	0 or 1 with probability 50%	1

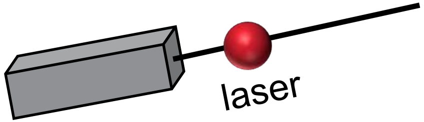
BB84 PROTOCOL – BENNETT & BRASSARD, 1984



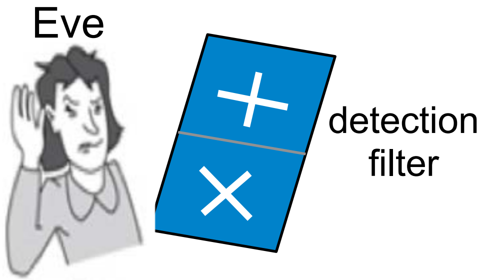
Step 1	Alice’s bit	0	1	1	0	1	0	0	1	0
Step 2	Alice’s random basis	+	+	x	+	x	x	x	+	+
Step 3	Alice’s polarization	→	↑	↖	→	↖	↗	↗	↑	→
Step 4	Bob’s random basis	+	x	x	x	+	x	+	+	x
Step 5	Bob’s measurement	→	↗	↖	↗	↑	↗	↑	↑	↗
Step 6	Public discussion	Determine which bases match and only retain the corresponding bits								
Step 7	Shared secret key	0		1			0		1	

WHY IS THE BB84 PROTOCOL SECURE

- Initial security assumptions:
  - No photon loss and attenuation on the fiber
  - Accurate lasers capable of emitting single photons



- What can Eve do? At best she can choose + or x basis at random and measure some photons
  - Correct measurement basis is not publicly known until after photons are received by Bob
  - If wrong basis is chosen photons are corrupted with 50% probability



- Alice and Bob must compare a few random key bits and make sure they match
  - If checking m bits probability of detecting an eavesdropper is $1 – (3/4)^m$

- BB84 guarantees key confidentiality but does not solve problem with availability
  - Eve may still cut the fiber

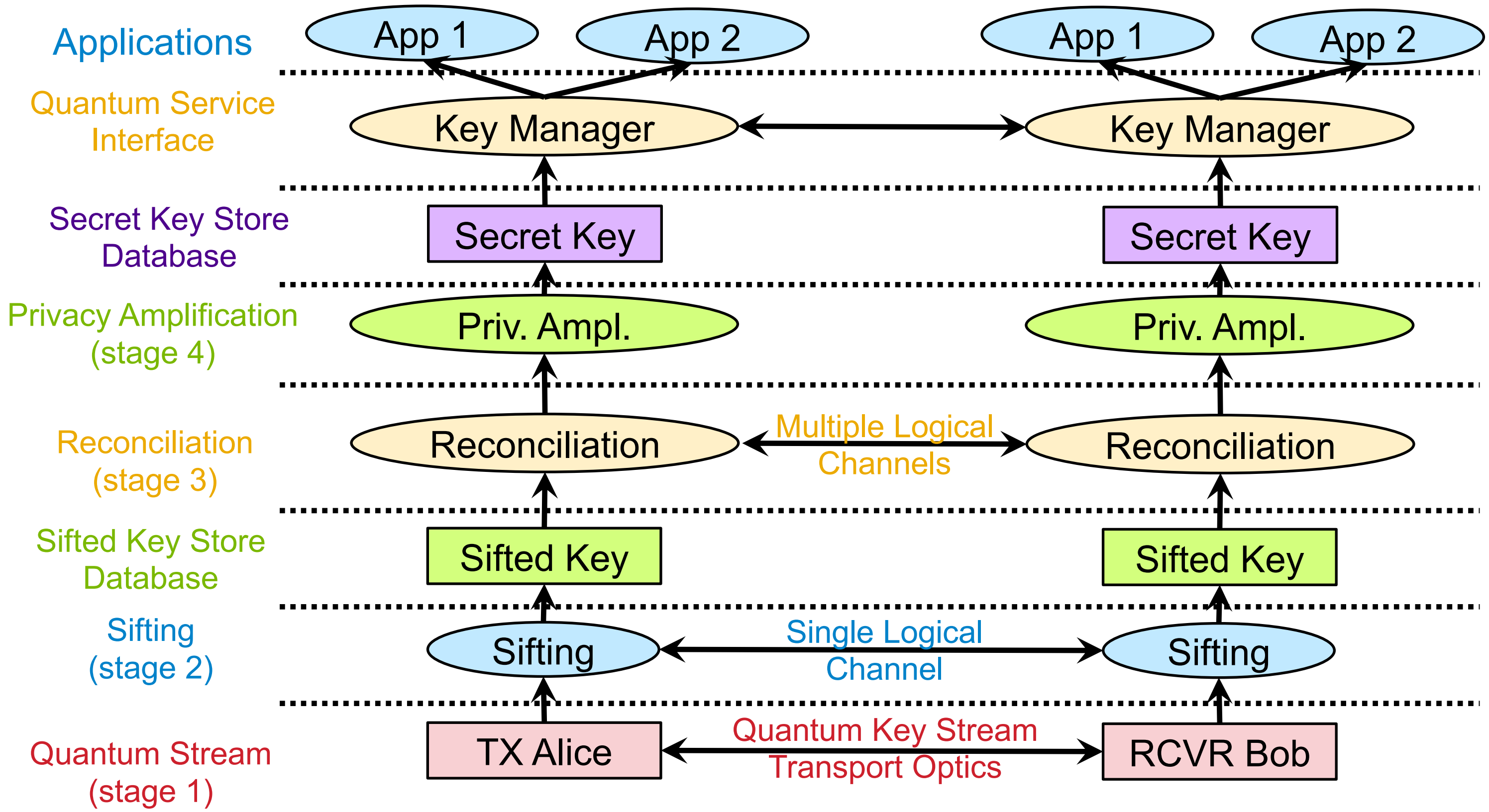
AVOIDING PHOTON SPLITTING ATTACKS

- Lasers have Poisson statistics and may emit multiple photons
- Scarani, Acin, Ribordy and Gisin resolved this in the SARG04 protocol
  - First 5 steps are the same as for BB84
  - Alice does not directly announce her bases but rather announces a pair of non-orthogonal states, one of which she used to encode her bit
  - If Bob used the correct basis, he will measure the correct state
  - If he chose incorrectly, he will not measure either of Alice's states and he will not be able to determine the bit

QKD server from ID Quantique

Random number generator from ID Quantique

THE QKD PROTOCOL FLOW



U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

Argonne NATIONAL LABORATORY

THE CASCADE PROTOCOL

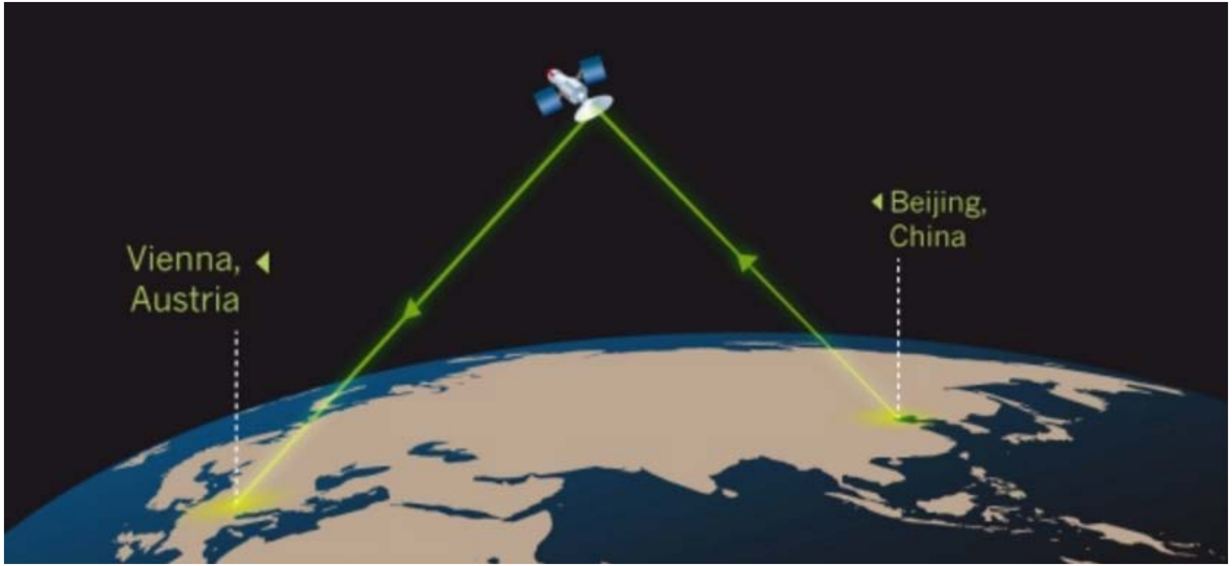
G. Brassard and L. Salvail: Advances in Cryptology: Eurorypt 93.

- Goal: correct errors that occurred due to photon loss or attenuation and make sure that the resulting keys are consistent
- Must be able to perform secret key reconciliation by using public discussion on the classical channel
- Most well-known is the CASCADE protocol
  - Run iteratively, number of passes depends on estimated error probability and number of errors
  - Strings divided into blocks of k_i bits and the blocks double in size in each step
  - Initial block size is $k_1 \approx 0.73/e$ where e is the error probability estimate
  - Must be followed by privacy amplification

<table>
<tr><td>01001011</td><td colspan="2">0101110</td><td>0100100</td><td>1101001</td><td>0110101</td><td>1110010</td></tr>
<tr><td>01001011</td><td>0101</td><td>1111</td><td colspan="2">0100101101001</td><td colspan="2">0110101110011</td></tr>
<tr><td colspan="2">0100101 0100</td><td></td><td colspan="4">0100101101000110101110010</td></tr>
</table>

SATELLITE QKD NETWORKS

- Entanglement based QKD: crystal in the satellite produces a pair of entangled photons that remain entangled after separation
- Lower photon loss in vacuum allows communication over great distances



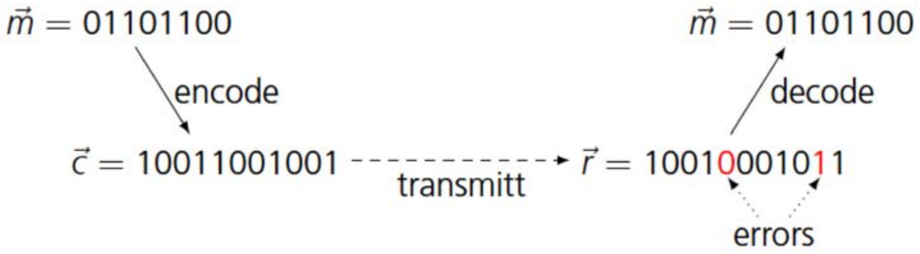
- QUESS satellite also dubbed Micius was launched by China on August 16, 2016
- Record entanglement distribution between ground stations >1,200 km apart
- Plans to connect Vienna and Beijing

ALTERNATIVE: POST-QUANTUM CRYPTOGRAPHY

- Post-quantum crypto replace traditional public-key crypto
  - Software solution relies on hardness of some problems
  - Demonstrated by Google and Microsoft to secure TLS

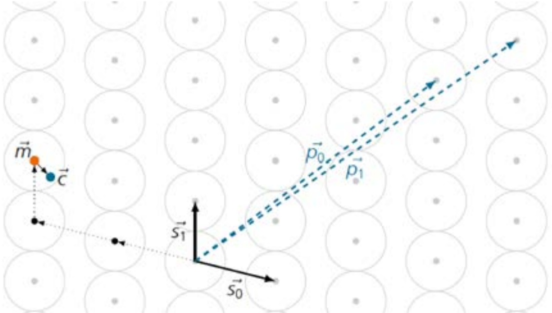
- Each family is based on different mathematical problems that are hard to solve both with traditional computers as well as quantum computers
- They differ in efficiency, e.g., in the size of public and private keys, sizes of cipher texts and key-exchange messages, and computational cost, their maturity, and the amount of trust in their strength
- In general post-quantum schemes require more resources compared to traditional cryptography

POST-QUANTUM CRYPTOGRAPHY EXAMPLES



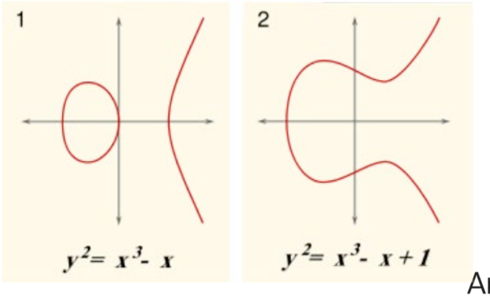
1. Code-Based Cryptography

- Use error-correcting codes
- Hard to decode a random linear code
- Size of key between 1MB and 4MB



2. Lattice-Based Cryptography

- Hard to find the shortest vector in a high dimensional lattice
- New Hope was implemented by Google in Chrome
- Some lattice-based cryptosystems were broken

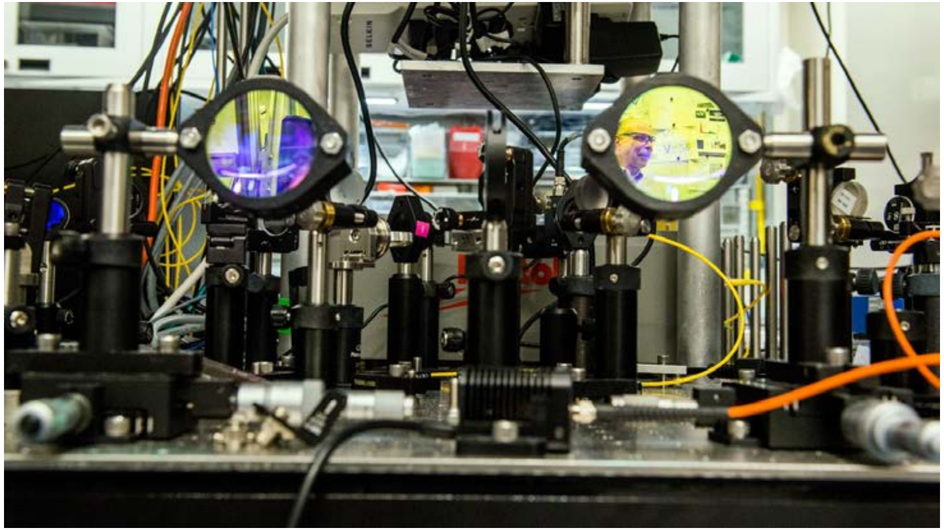


3. Supersingular Elliptic Curve Isogeny Cryptography

- Based on operations between different elliptic curves, enables a Diffie-Hellman like key exchange
- Proposed in 2006, not yet ready for adoption

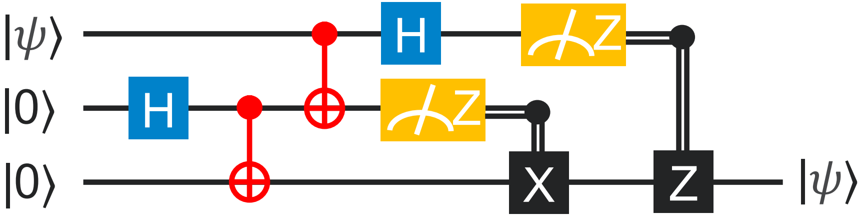
QUANTUM TELEPORTATION NETWORKS

QUANTUM TELEPORTATION



Optical table demonstrating the principles of quantum teleportation in the Awschalom Lab (University of Chicago and Argonne)

- Quantum teleportation allows transmission of quantum states between two network hosts
- Much more general than QKD networks
- Requires distribution of entangled particles followed by classical communication
- Was demonstrated experimentally

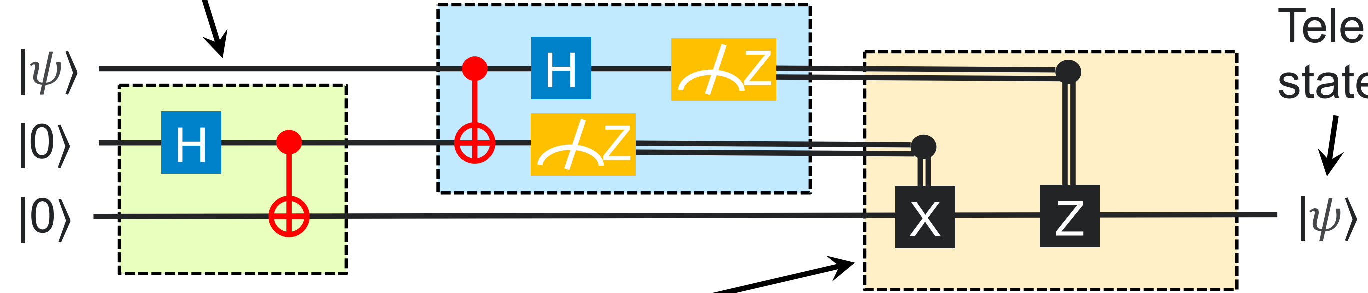


HOW THE TELEPORTATION CIRCUIT WORKS

Bell measurement determines which of the 4 Bell states the 2 qubits are in: $|\psi_0\rangle=|00\rangle+|11\rangle$, $|\psi_1\rangle=|01\rangle+|10\rangle$, $|\psi_2\rangle=|00\rangle-|11\rangle$, or $|\psi_3\rangle=|01\rangle-|10\rangle$

Bell state preparation prepares the maximally entangled state $|00\rangle + |11\rangle$

Input state

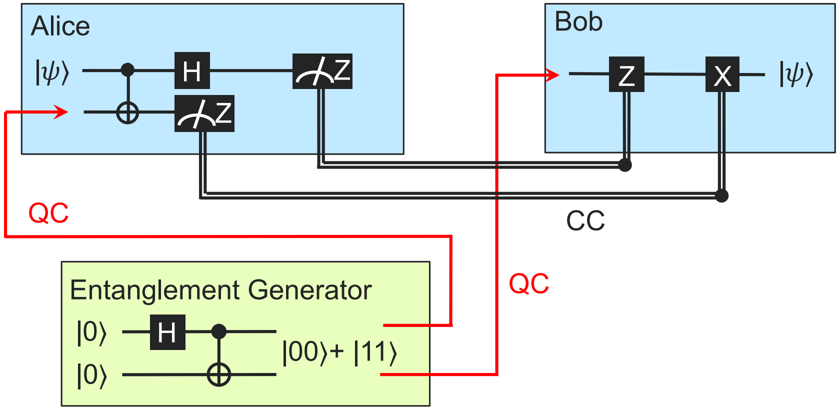


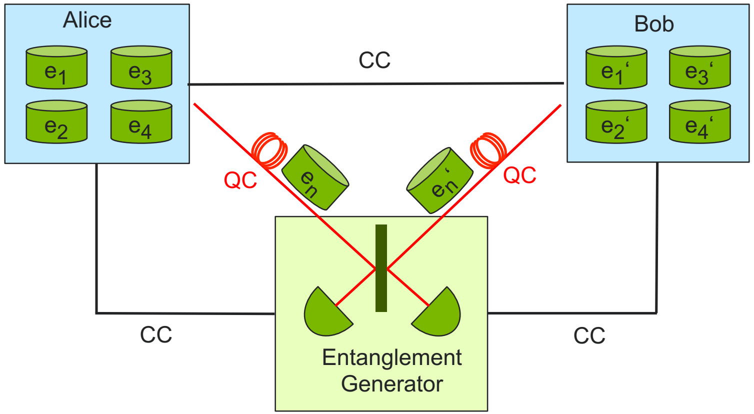
Teleported state

Clasically controlled bit flip and phase flip operation

Teleports quantum information, not matter

QUANTUM TELEPORTATION NETWORKS

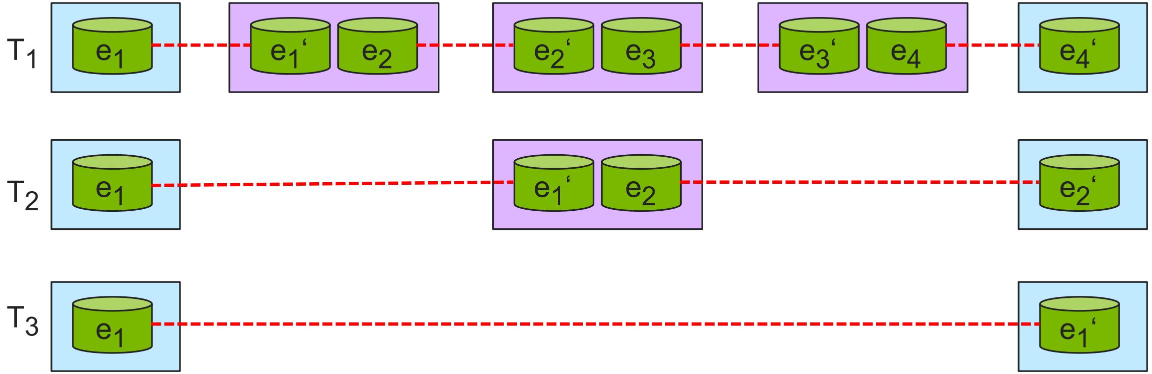




- Teleportation of quantum state $|\psi\rangle$ from Alice to Bob uses a quantum channel (QC) and a classical channel (CC)
- Teleportation does not communicate faster than speed of light. Why?

- Entangled photons are generated anddistributed to network hosts
- Photons must be tracked at the individual particle level, requiring a great level of coordination

ENTANGLEMENT SWAPPING

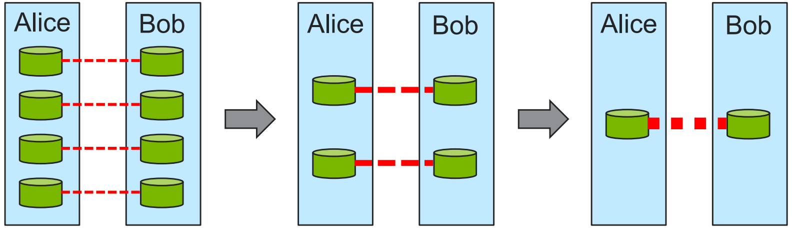


- Produces long-distance entanglement
- Challenges: needs accurate tracking of entangled photons, accurate timing and / or quantum memories

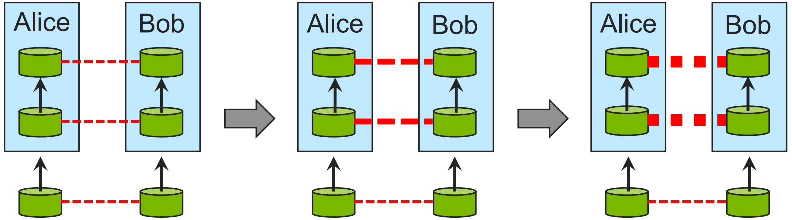
- Create entanglement in individual links and store in quantum memories
- Then connect these links through entanglement swapping (using quantum teleportation)

ENABLING RELIABLE COMMUNICATION

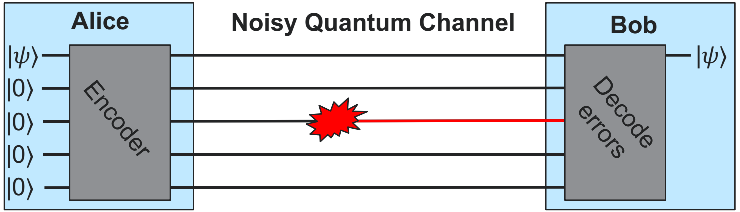
- Entanglement purification – uses n weakly entangled pairs to distill a high-quality entangled pair:



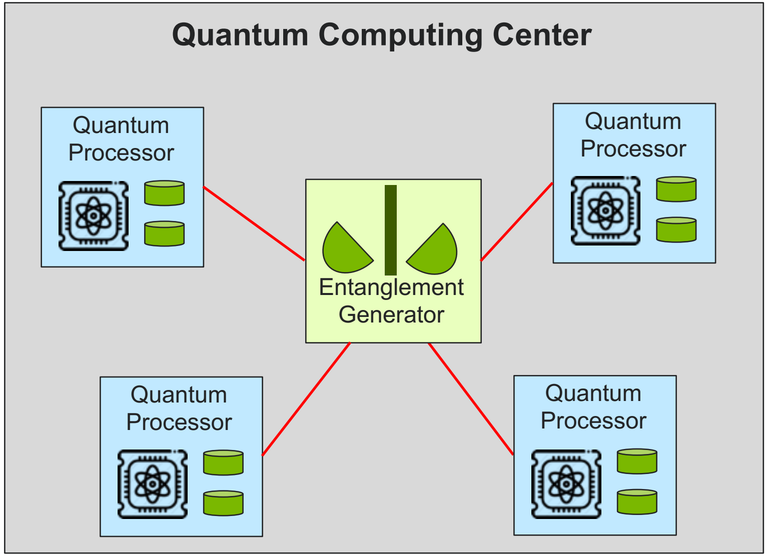
- Entanglement pumping – gradually improves entanglement quality by using additional weakly entangled pairs:

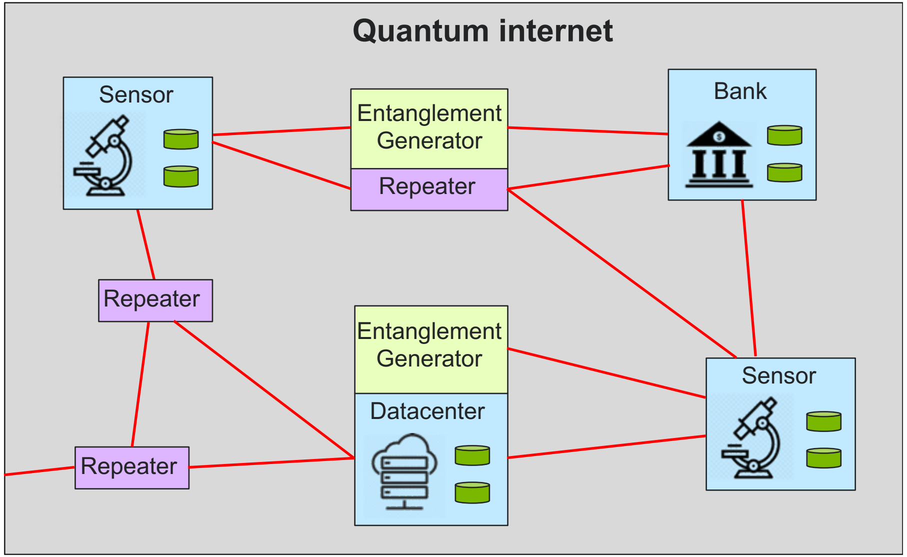


- Error correction – encodes the transmitted states into multiple qubits and no entanglement is required:



TELEPORTATION NETWORK APPLICATIONS





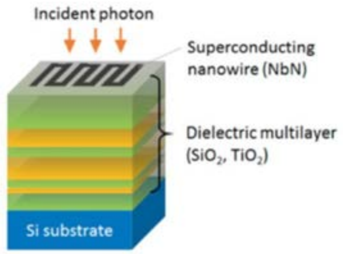
Local area quantum network – repeater nodes are not needed. Network must provide high throughput and low latency.

The quantum internet – applications require long-distance communication. Bandwidth, latency and security requirements vary. Multiple repeaters and entanglement generators are used.

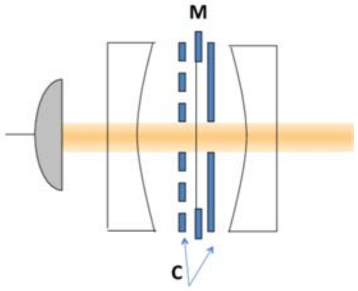
BUILDING A QUANTUM TELEPORTATION NETWORK IN THE CHICAGO AREA

ARGONNE-FERMILAB QUANTUM NETWORK

- Experimental realization of quantum teleportation at telecom wavelength using optical fiber
- Experiment requires:
  - Communication on dedicated dark fiber near telecommunication wavelength ~1532 nm
  - Entanglement generation
  - Single photon detection
  - Precise coordination and timing
- Future extensions driven by technology:
  - Quantum memories will allow building a quantum repeater
  - Frequency conversion and transduction

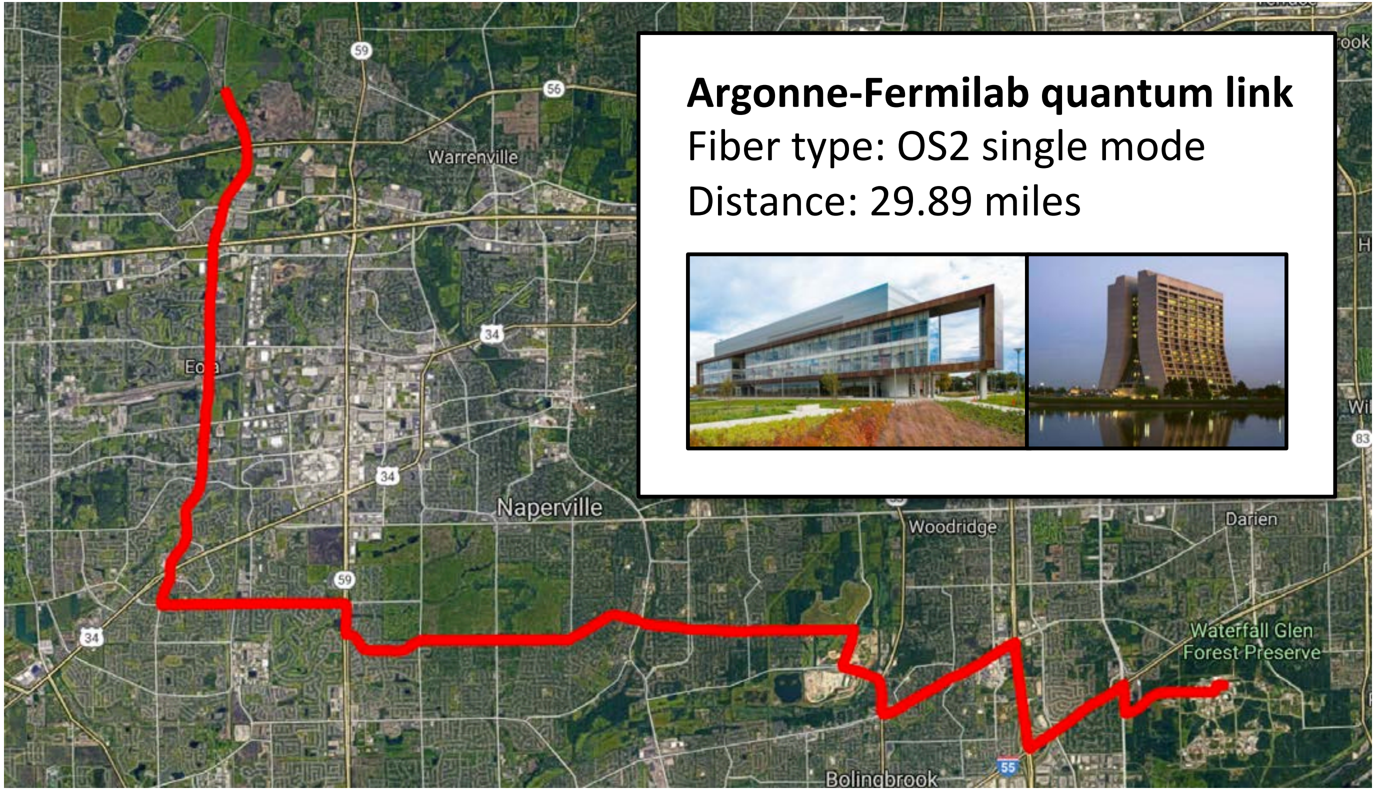


Superconducting nanowire single photon detector



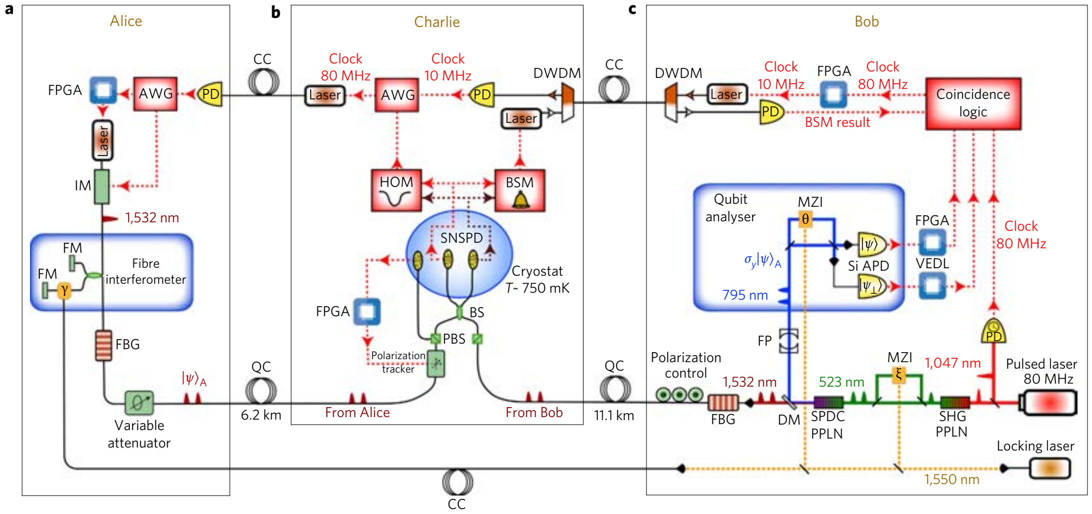
Fabry-Perot cavity used to create entanglement

THE ARGONNE-FERMILAB QUANTUM LINK



Argonne-Fermilab quantum link
Fiber type: OS2 single mode
Distance: 29.89 miles

FERMILAB QUANTUM NETWORK



- Alice prepares laser pulses in various time-bin qubit states psiA> = alpha* |e> + beta * |l> where |e> and |l> denote early and late temporal modes
- Bob creates a pair of 1532nm and 795nm entangled photons
- Alice sends qubits to Charlie who performs a Bell state measurements to teleport the qubits to Bob

AWG - arbitrary waveform generators
BS - beamsplitter
BSM - Bell-state measurement
CC - classical channel
DM - dichroic mirror
DWDM - dense-wavelength division multiplexers
FBG - fibre Bragg grating
FM - Faraday mirrors
FP - Fabry-Perot cavity
FPGA - field-programmable gate-arrays
HOM - Hong-OuMandel dip
IM - intensity modulator
MZI - Mach-Zehnder interferometer
PBS - polarizing beamsplitters
PD - photo diodes
QC - quantum channel
SHG PPLN - periodically poled lithium-niobate crystal
Si APD - silicon avalanche photodiodes
SPDC PPLN - spontaneous parametric down-conversion
SNSPD - superconducting nanowire single photon detectors
VEDL - variable electronic delay-line

THANK YOU!