# Quantum Communications Beyond QKD

## Colin P. Williams

Jet Propulsion Laboratory,
California Institute of Technology, Pasadena, CA 91109-8099
Email: Colin.P.Williams@jpl.nasa.gov, Tel: (818) 393 6998

# Overview

- **QKD is practical, but is it significant?**
  - Pros and cons of QKD
- **What else might you do with quantum information?**
  - What's new about quantum information?
  - What does it allow us to do that we can't do otherwise?
  - Can we beat Shannon bound on data compression?
  - Can we improve network communications?
  - Could quantum communications help us make quantum computers?

# Pros and Cons of QKD

## Pros

- **In principle, QKD can be unconditionally secure**
- **QKD ensures long-term confidentiality of information**
  - Immune to technological advances in computers and algorithms
  - Diplomatic and military communications (historical security needed)

## Cons

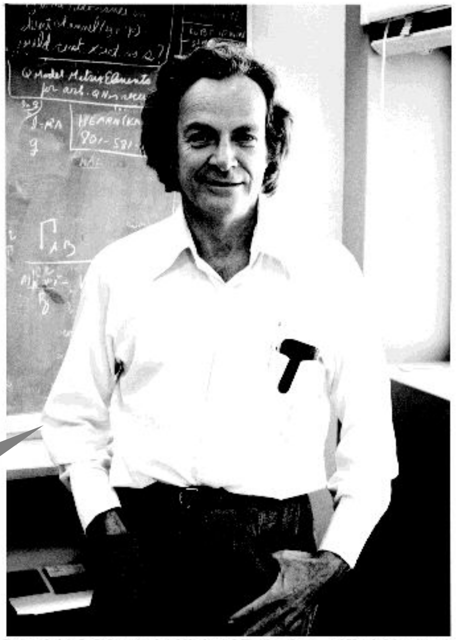
- **In practice, to be truly secure, QKD needs authenticated channel**
  - Otherwise vulnerable to "man-in-the-middle" attacks
- **In practice, to be truly secure, should use keys in a One Time Pad**
- **Real hardware is imperfect**
  - Imperfections can introduce loopholes
- **Limited range in fiber until quantum repeaters arrive**

- **Channel security isn't the whole story**
  - Humans/trusted insiders (blackmail, bribery, corruption)
  - Economic impact greater for "denial-of-service" type attacks
  - Existence of other quantum cryptographic primitives impeded by lack of an unconditionally secure quantum bit commitment protocol

# What’s different about Quantum Information?

# Quantum Information is Weird

- **"Commonsense" properties of information**
  - *Bits are 0s or 1s*
  - *Bits can be copied perfectly*
  - *Reading a bit does not change its value*
  - *Reading the bit values of part of a memory register does not affect the other bit values*
  - *You can always negate a bit*
  - *You cannot compress n-bit messages beyond their Shannon bound*
- **For qubits, these assumptions are *false*!**

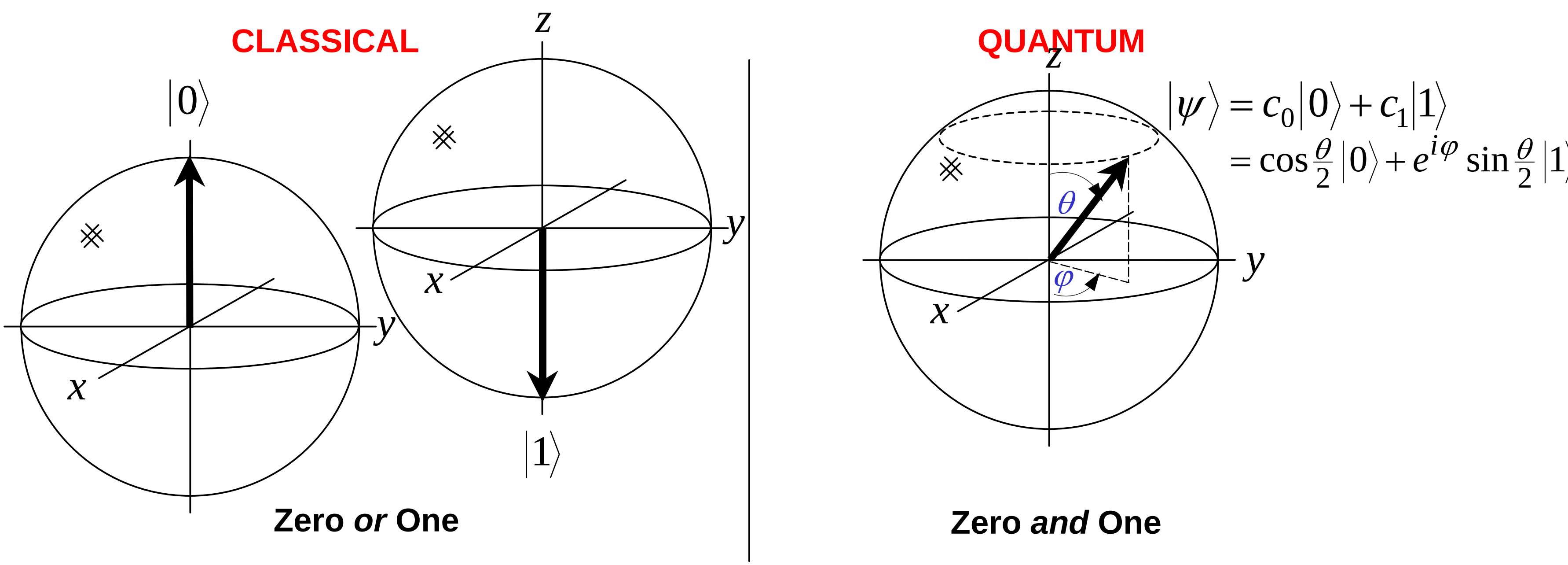




***"Because nature isn't classical dammit!"***
**Richard Feynman**

# From Bits to Qubits

- **Use 2-state quantum systems for bits (0s and 1s) e.g. polarized photons**




- **A qubit can exist in a *superposition* state** $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ **s.t.** $|c_0|^2 + |c_1|^2 = 1$

# Entangled Qubits

- **Quintessential quantum property of qubits**
  - State of one qubit linked with that of another
- **Entangled state, e.g.,**

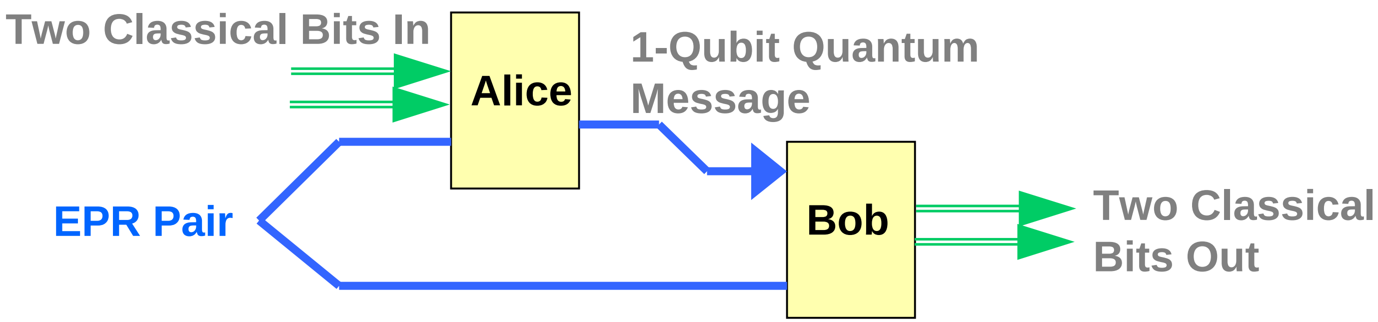
$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) \neq |\psi\rangle_A|\phi\rangle_B$$

- **Initially, neither "A" nor "B" has a definite bit value**
- **But measuring bit value of "A" determines that of "B" and vice versa**
- **Effect appears to propagate instantaneously independent of**
  - Distance between "A" and "B"
  - Nature of intervening medium
  - Recent experiments bound speed to > 10,000 c (Gisin, Geneva)

# What else can you do with Quantum Communications?

# Beyond Shannon Data Compression

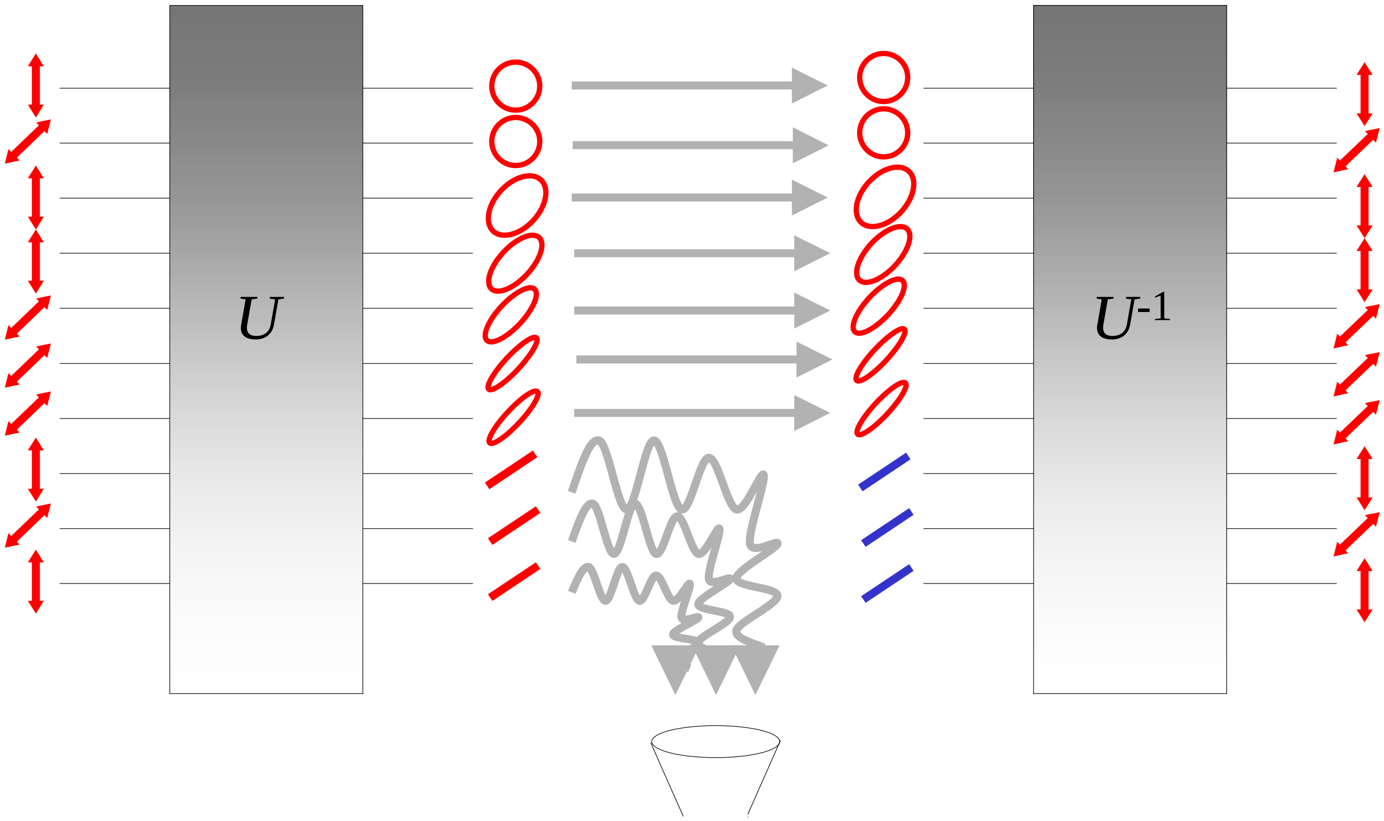
- **Factor of $\times 2$ compression beyond Shannon bound *at communication time***
  - If one can create, distribute and store entangled qubits error free




- **Improve data throughput at times of peak load by distributing entanglement when traffic is below network capacity**
- **Needs shared prior entanglement to work!**

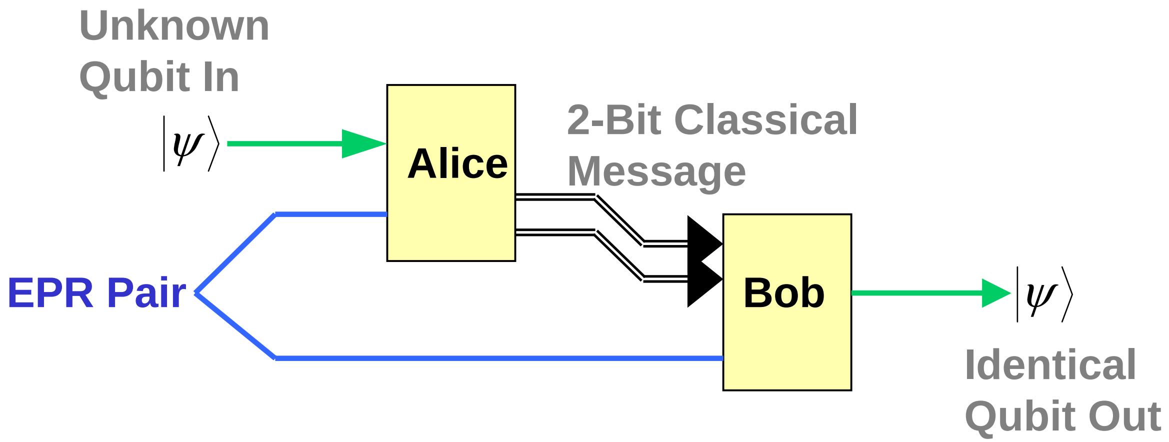
# Without Prior Entanglement?

- **Can we beat the Shannon bound without prior entanglement?**
- **Depends**
  - If bits are encoded in orthogonal quits … no
  - If bits are encoded in non-orthogonal qubits … yes



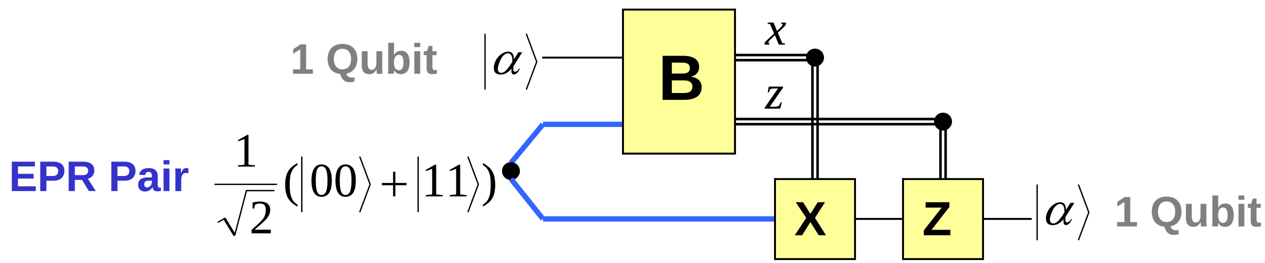
# We Can Teleport Quantum Information

- Use EPR pair and 2 classical bits to send 1 qubit
- Original state of qubit need not be known to Alice or Bob



# Teleportation in Detail

- **Single qubit** $|\alpha\rangle = a|0\rangle + b|1\rangle$ **and EPR pair** $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- **Measure** $|\alpha\rangle$ **and one qubit of** $|\psi\rangle$ **in Bell basis** $|0x\rangle + (-1)^z|1\bar{x}\rangle$

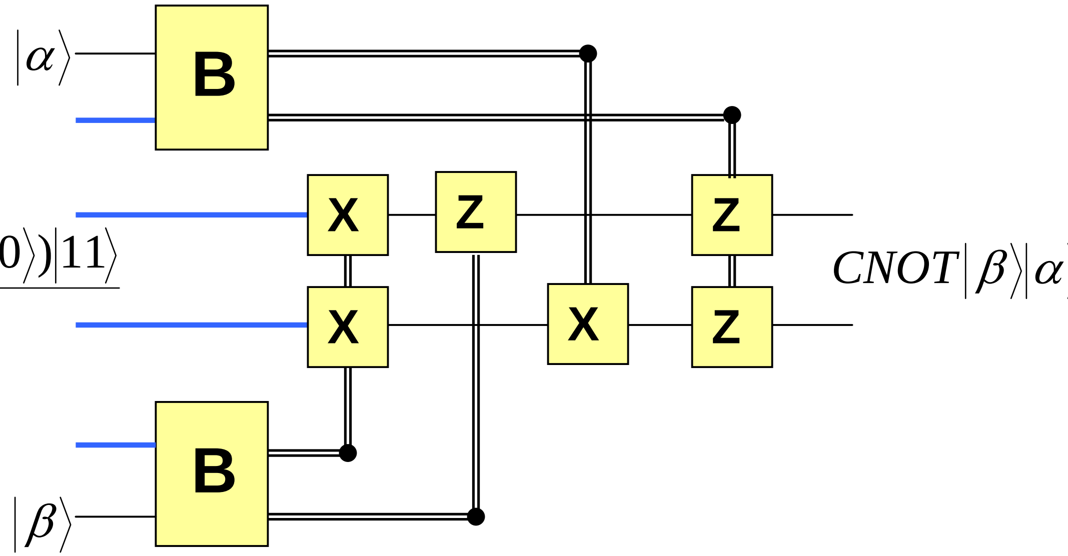



- **Giving uniformly distributed classical result "*x z*"**
- **Just after B, output qubit is** $|\alpha\rangle$ **except for additional 1-qubit gate op.**
  - *I (identity), X, Y, or Z*
  - *Determined by value of classical bits x and z in "x z"*
- **Therefore reverse the appropriate Pauli operator to re-construct** $|\alpha\rangle$

# Is Teleportation Useful?

- **Can make a CNOT gate via teleportation**

$$|\chi\rangle = \frac{(|00\rangle + |11\rangle)|00\rangle + (|01\rangle + |10\rangle)|11\rangle}{\sqrt{2}}$$



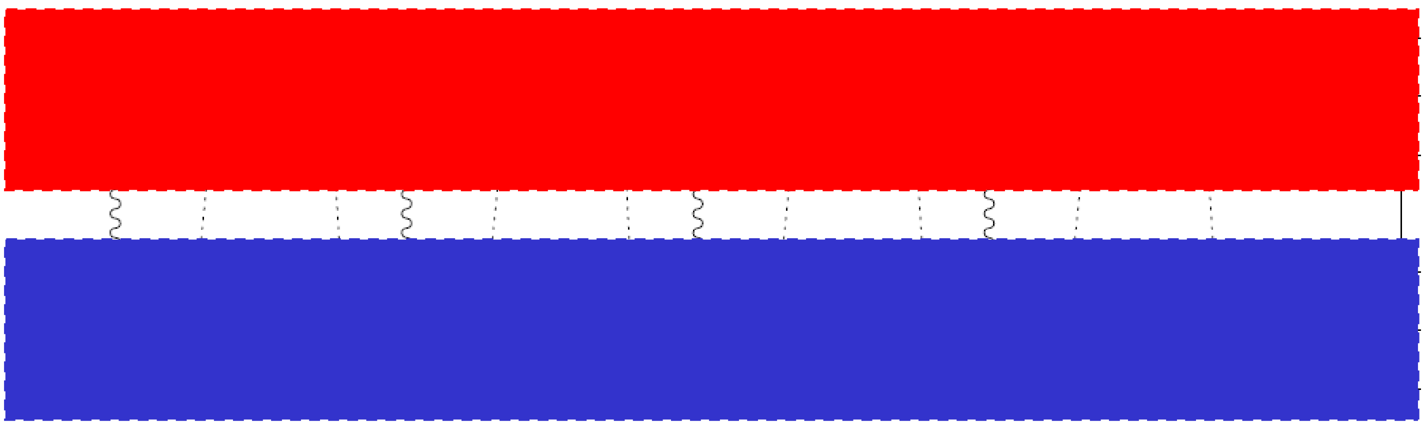

- **Can make $|\chi\rangle$ from a pair of GHZ states**
  - **The GHZ state is a 3-qubit entangled state** $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

- **Hence teleportation, GHZ states and Bell basis measurements can be used as a basis for universal quantum computation**

# Quantum Communications for Making Quantum Computers?

# Distributed Quantum Computers

- **Beating the wiring crunch?**
  - –Many few-qubit quantum processors connected by a quantum network
  - –Will necessitate development of means to coherently convert flying qubits to static qubits



A 4-qubit QFT distributed over two 2-qubit processors. Source: Yimsiriwattana/Lomonaco, quant-ph/0403146.

-Needs ability to create, distribute, and store entangled qubits without error

# Conclusions

- **There's more to quantum communications than QKD!**
- **What's new about quantum information?**
  - Entanglement, non-determinism, superpositions of bits
- **What does it allow us to do that we can't do otherwise?**
  - Beat the Shannon bound at communication time
    - Perhaps relieving network congestion at peak times
  - Teleportation of information
  - Compression of quantum information
- **Could quantum communications help us make quantum computers?**
  - Yes
  - Quantum communications offer alternative requirements for achieving universal quantum computers
    - Fixed entangled states, Bell measurements and teleportation
  - Quantum communications allows distributed quantum computing
    - Perhaps relieving the wiring jam!