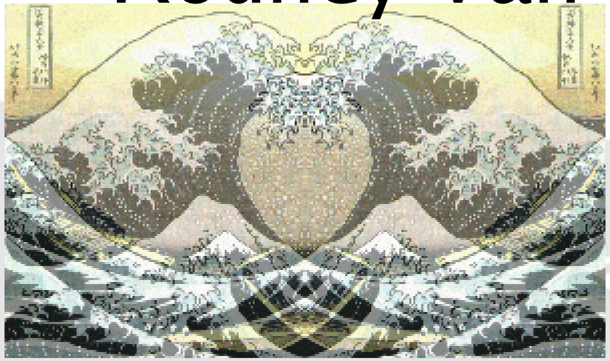
Applications of an Entangled Quantum Internet

Conference on Future Internet Technologies

Seoul, Korea

June 20, 2008

Rodney Van Meter (Keio) (rdv@sfc.wide.ad.jp)



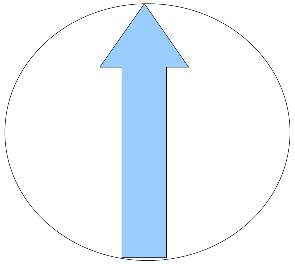
Byung-Soo Choi (Ewha Woman's University)

KEIO 150
Design the Future

Outline

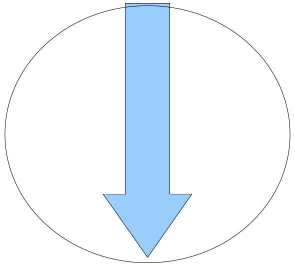
- Quantum Key Distribution (QKD)
- Extending QKD: switching and trusting
- Quantum Repeaters
- What would a *distributed* quantum system be good for?
- What problems do we have to solve to get there?

What's a Qubit?

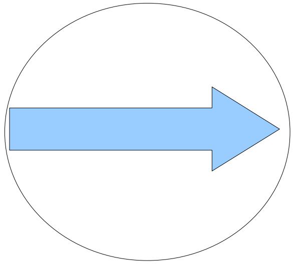


= |0>

A qubit has two states that can be 0 and 1, such as horizontal and vertical polarization of a photon, or up and down spin of an electron.



= |1>



What is this?

= |0> + |1>

A qubit can be in a superposition of both states at once!

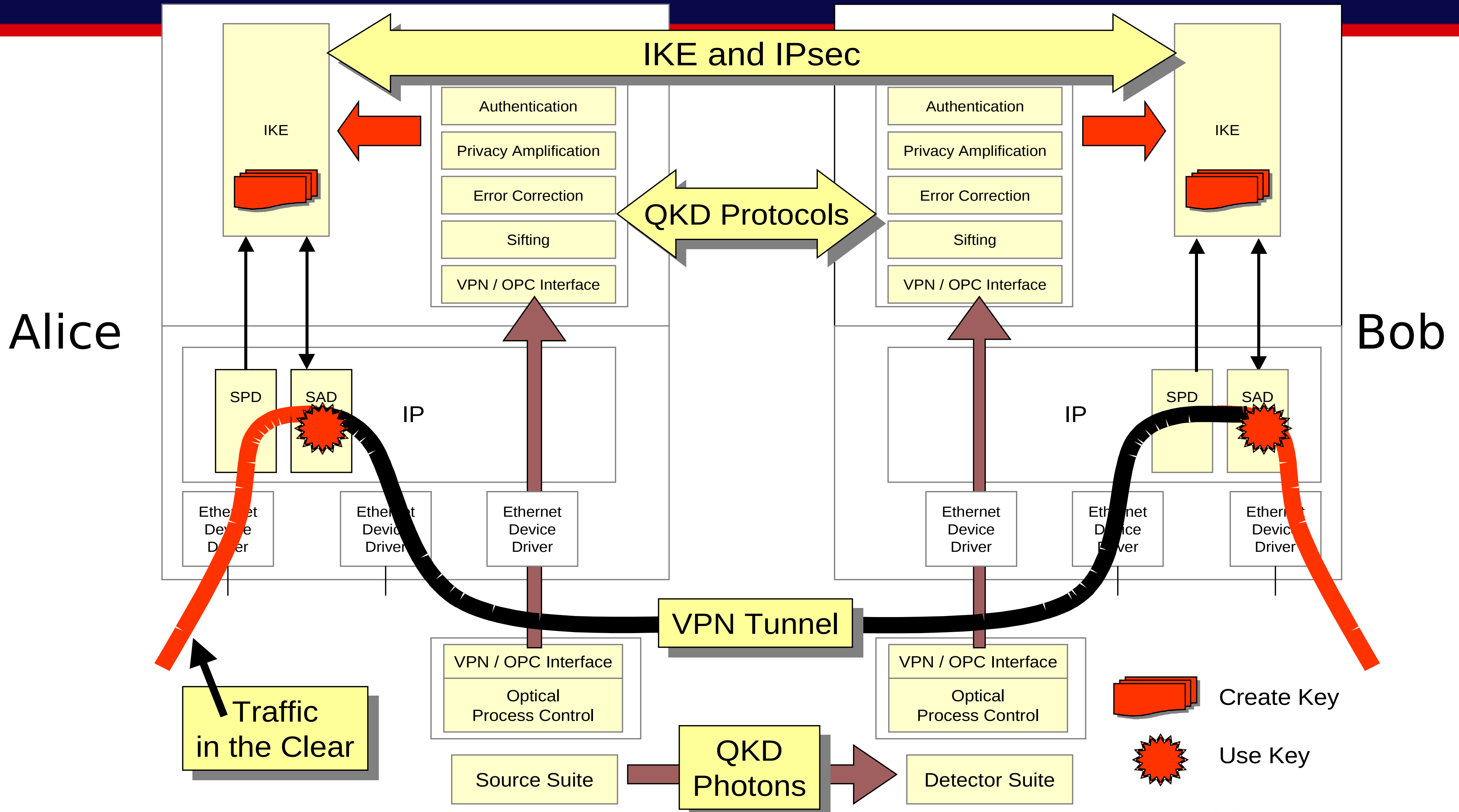
Quantum Key Distribution

- “Tamper-evident” generation of shared random numbers
- Ideal use: generate bit stream for one-time pad
  - Mostly, too slow for that
- Use as Diffie-Hellman replacement
- Still requires classical authentication

Quantum Key Distribution

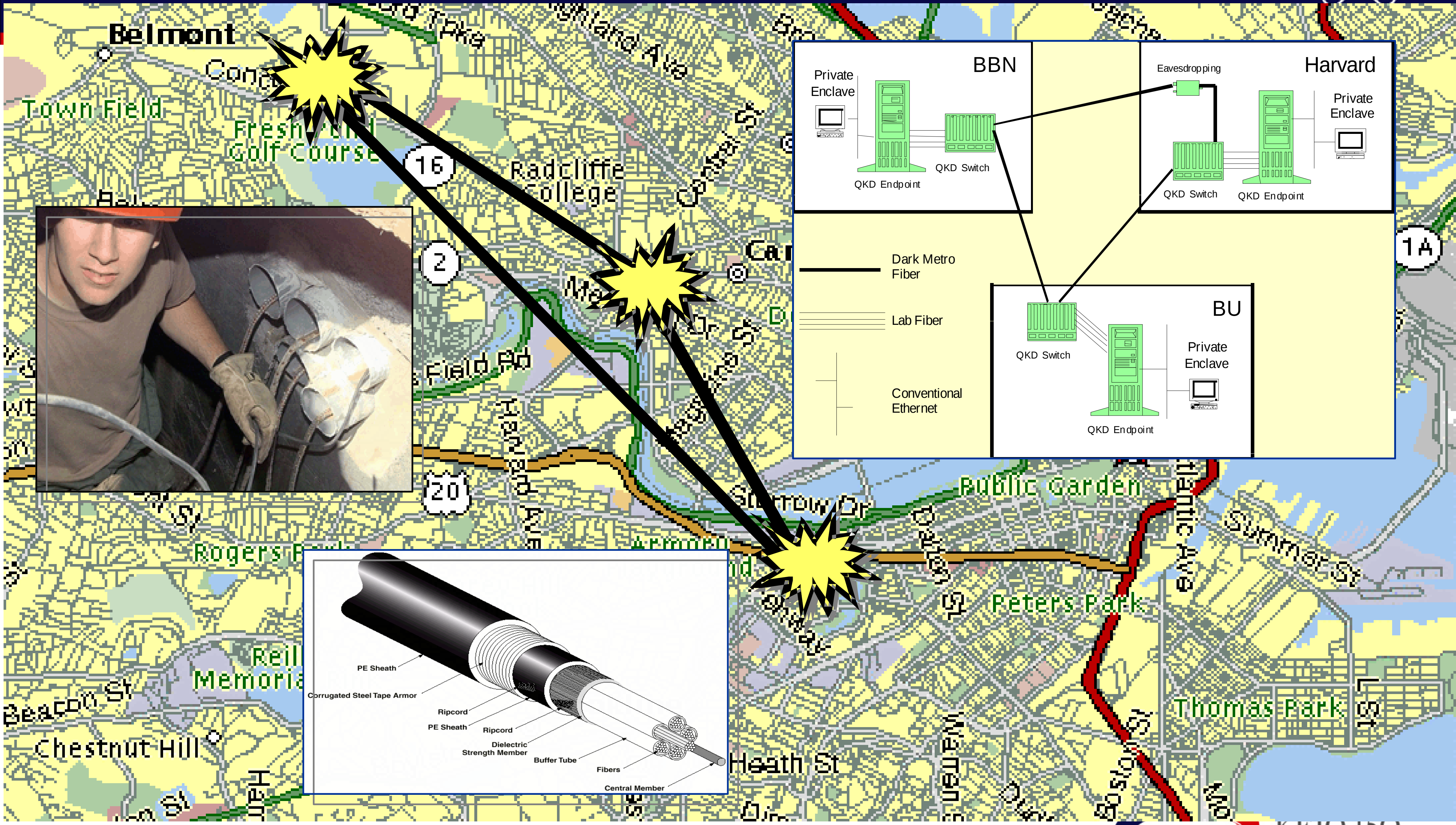
- Basic use is <150km, dedicated point-to-point fiber, no amplifiers
- Can be optically switched & multiplexed w/ other data
- Longer distance requires:
  - trusting intermediate nodes, or
  - entanglement-based **quantum repeaters**
- Everything but repeaters in actual use now (thanks, Chip Elliott!)

Putting It All Together



slide from Elliott, BBN

The DARPA Quantum Network

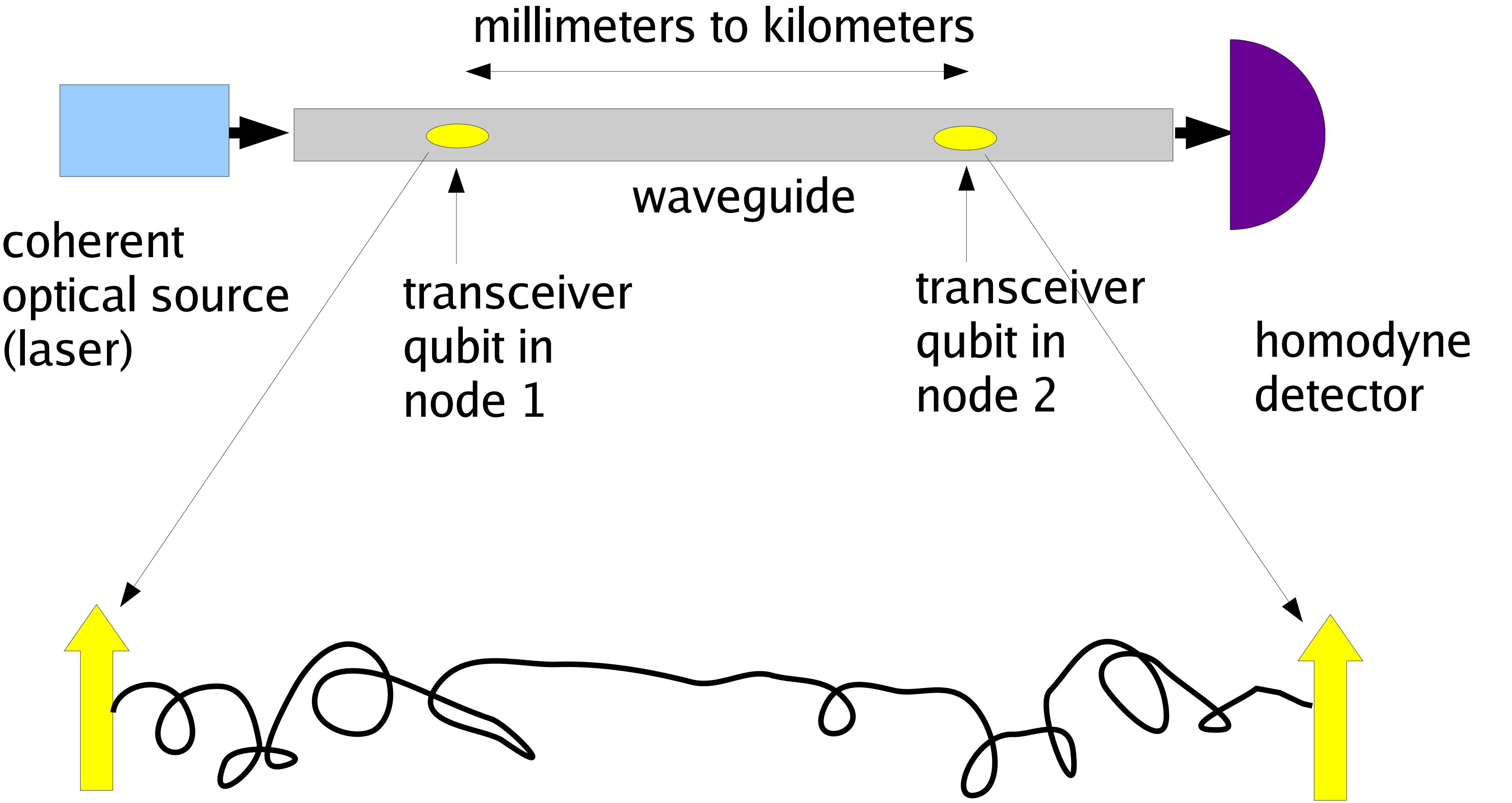


slide from Elliott, BBN

Going the Distance

- Longer distance requires:
  - trusting intermediate nodes, or
  - entanglement-based **quantum repeaters**
- Quantum repeaters are *not* amplifiers
- Repeaters use **teleportation**
- Teleportation requires **entangled** states known as **Bell pairs**

Network Link Technology (Qubus)



Munro, Nemoto, Spiller, New J. Phys. 7, 137 (2005)

Teleportation

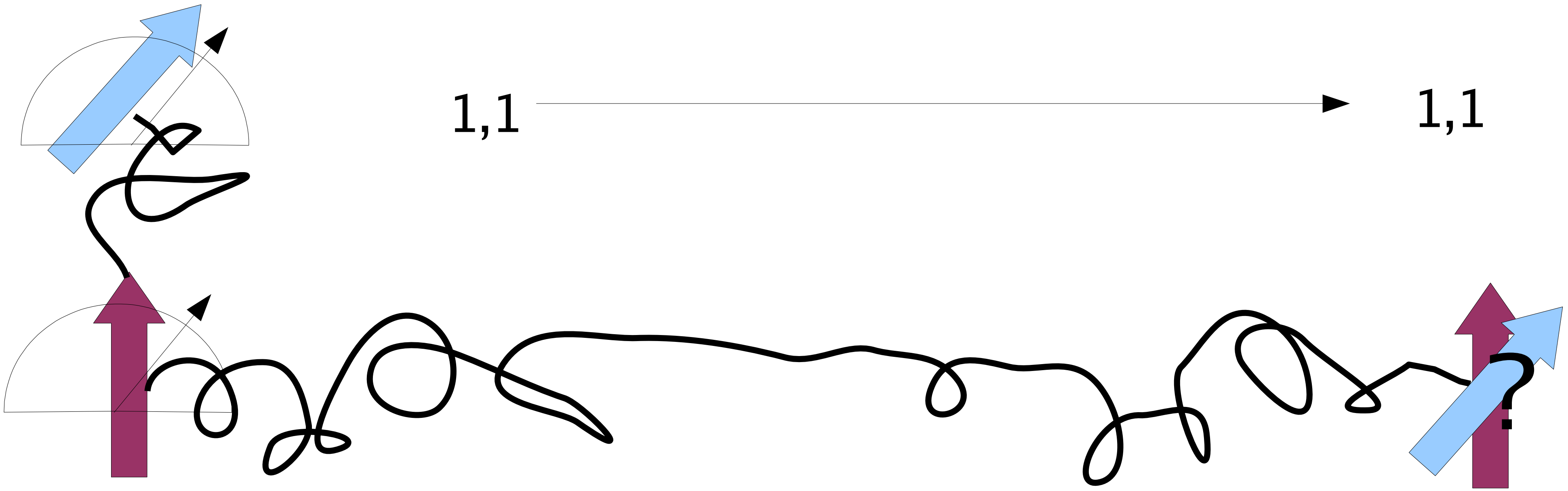
1) Start with an EPR pair, and the qubit to be sent

2) Entangle locally at the source

3) Measure both qubits at source

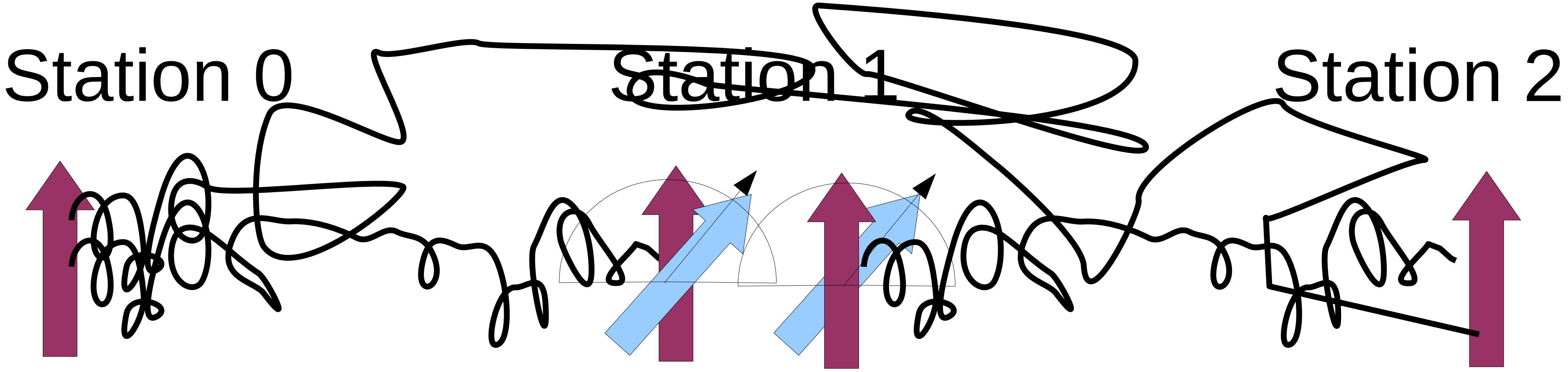
4) Transmit classical results to destination

5) Local operations recreate original qubit



Bennett et al., Phys. Rev. Letters 70, 1993

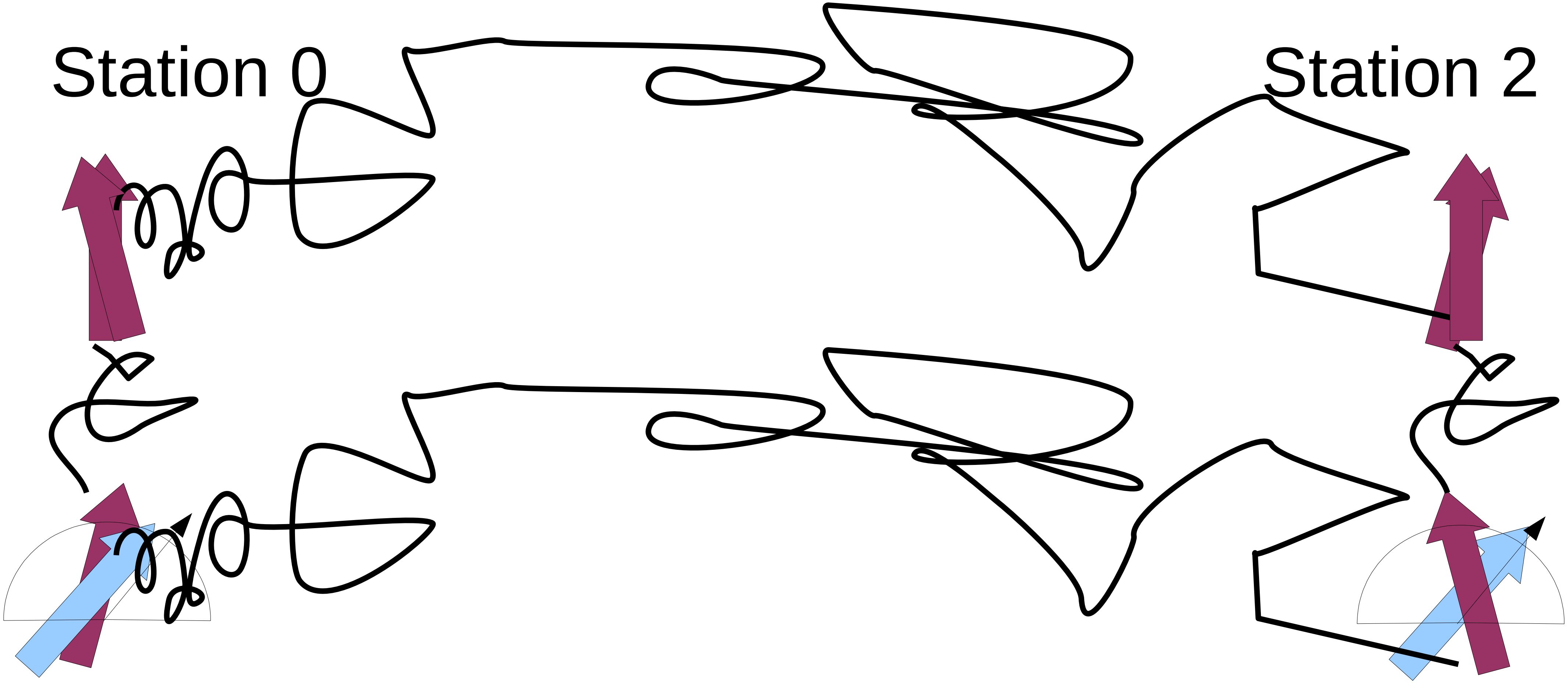
Quantum Repeater Operation



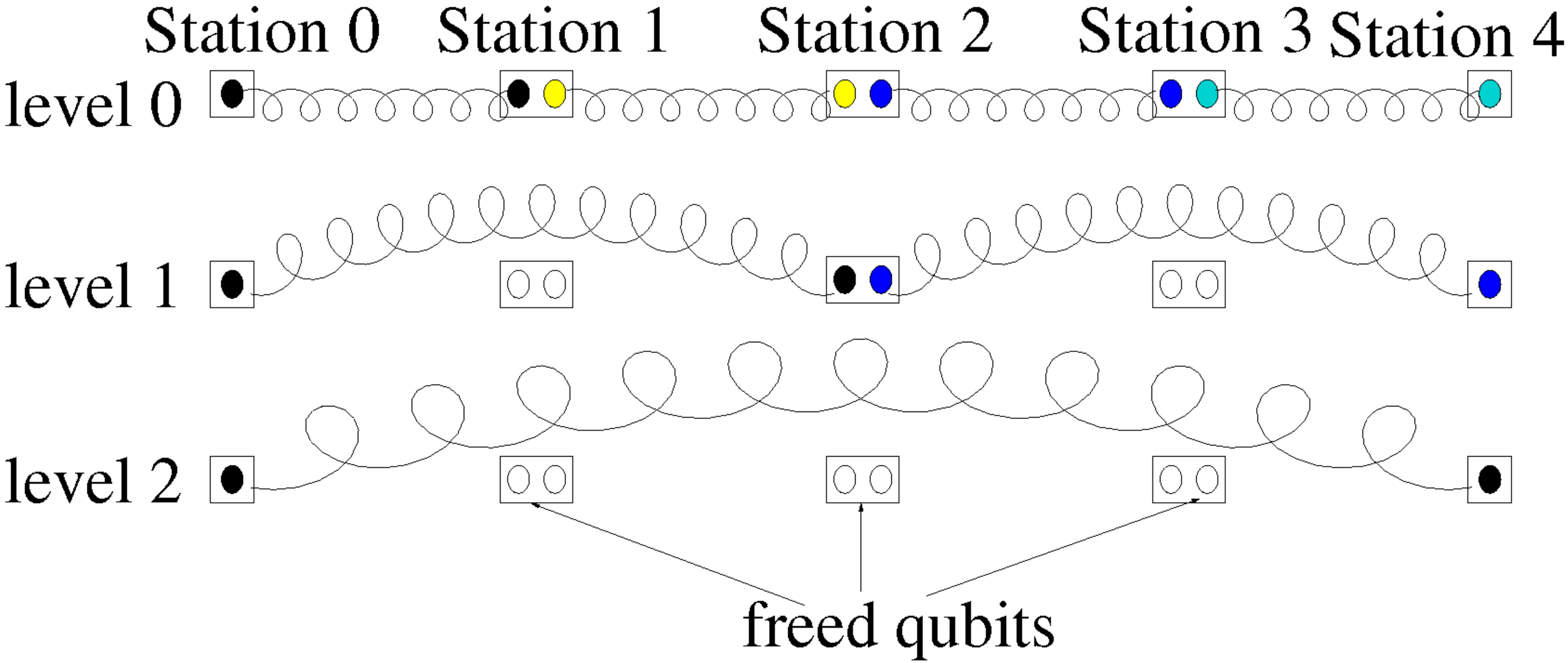
Bell State Measurement

Called *entanglement swapping*.
Fidelity declines; you must *purify* afterwards

Purification

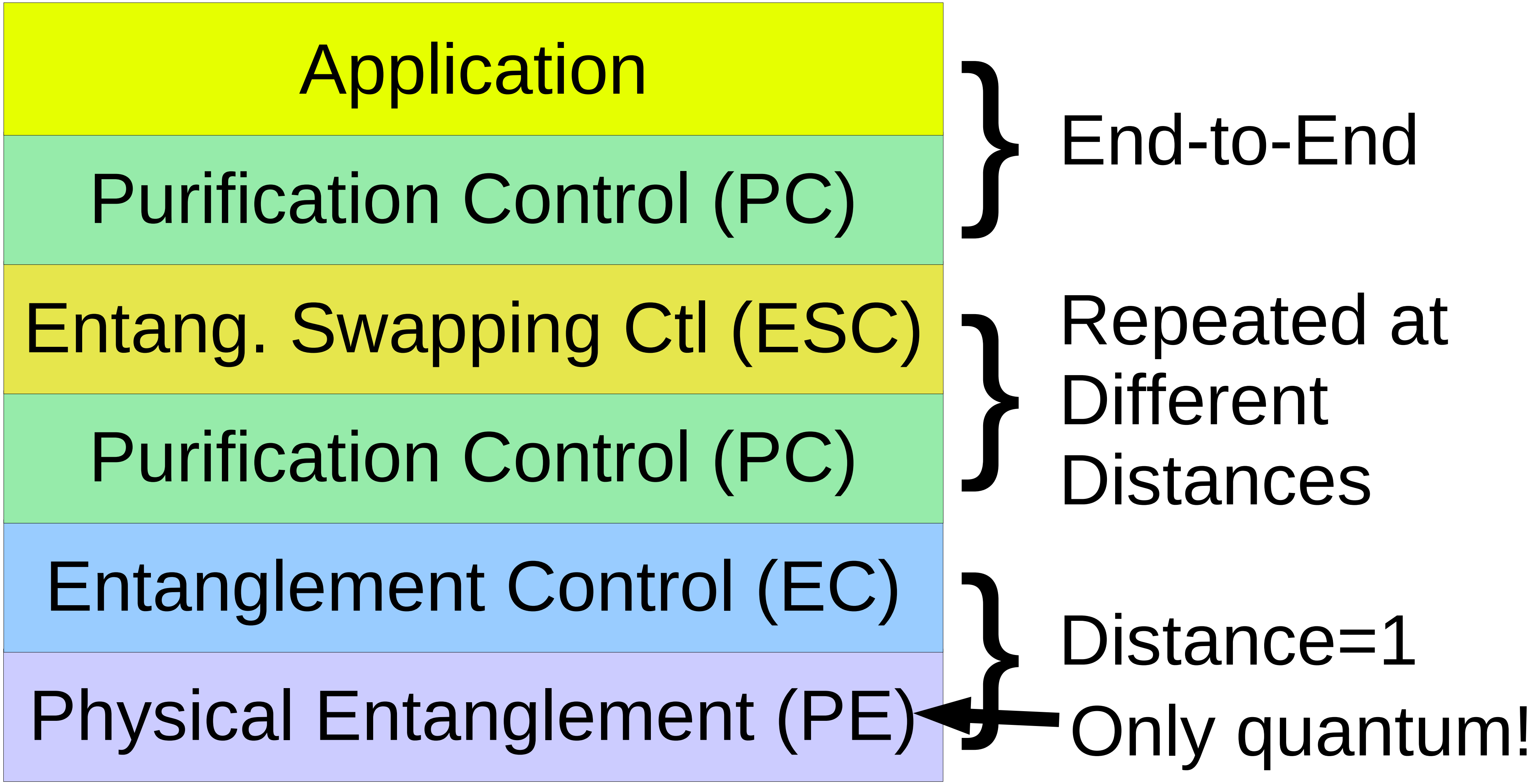


Nested Entanglement Swapping



Destination

Repeater Protocol Stack



Application

Purification Control (PC)

Entang. Swapping Ctl (ESC)

Purification Control (PC)

Entanglement Control (EC)

Physical Entanglement (PE)

End-to-End

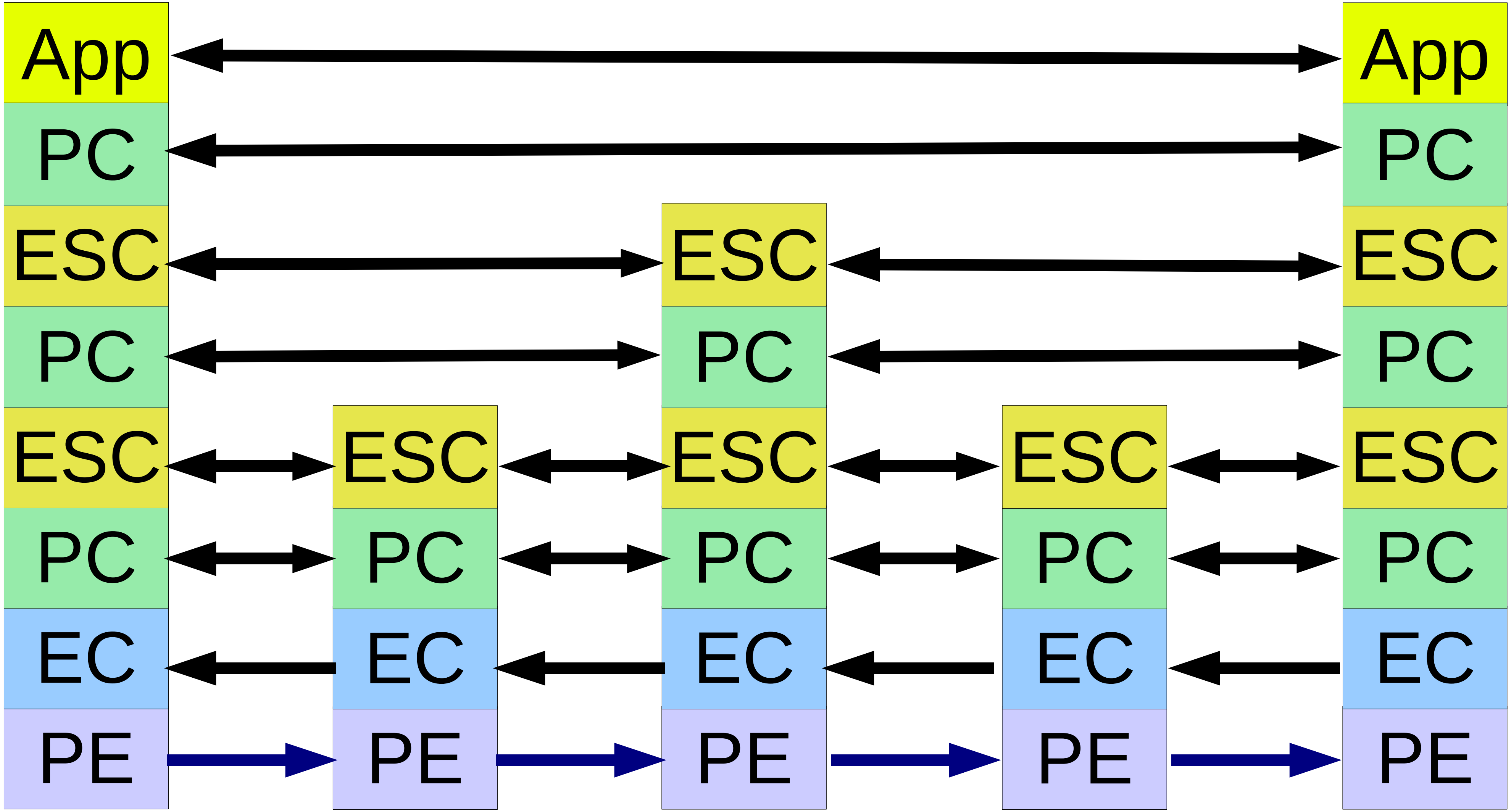
Repeated at Different Distances

Distance=1

Only quantum!

Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear)

Four-Hop Protocol Interactions



Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear)

What about *Distributed* QC?

- Two types: those that use entanglement, and those that don’t
- Quantum key distribution can be done either way
- Entanglement can be either a *digital* resource, or a *gyroscopic* reference

Long-Distance Entanglement: Digital Uses

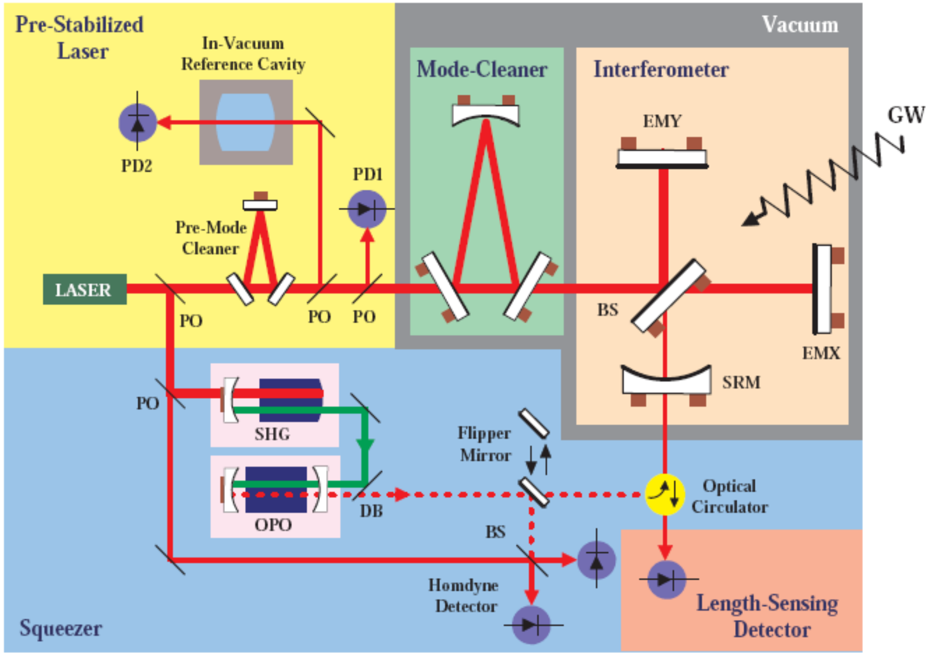
- Quantum Key Distribution
- Distributed leader election
- Same as classical distrib. systems: connect
  - People
  - Machines
  - Data/databases

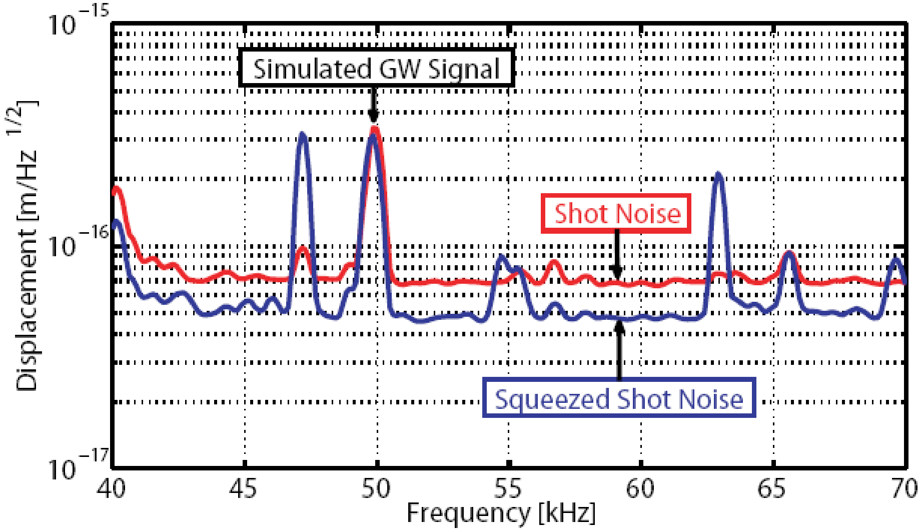
  ...that are in distant locations

Gyroscopic (Physical) Uses

- Entanglement can also be used to improve precision of measurements
  - Phase/timing
  - Directional information
- Better atomic clocks
- Quantum imaging

Gravity Waves?





From Goda *et al.*, *Nature Physics*, 2008.

GW detector using “squeezed” states.

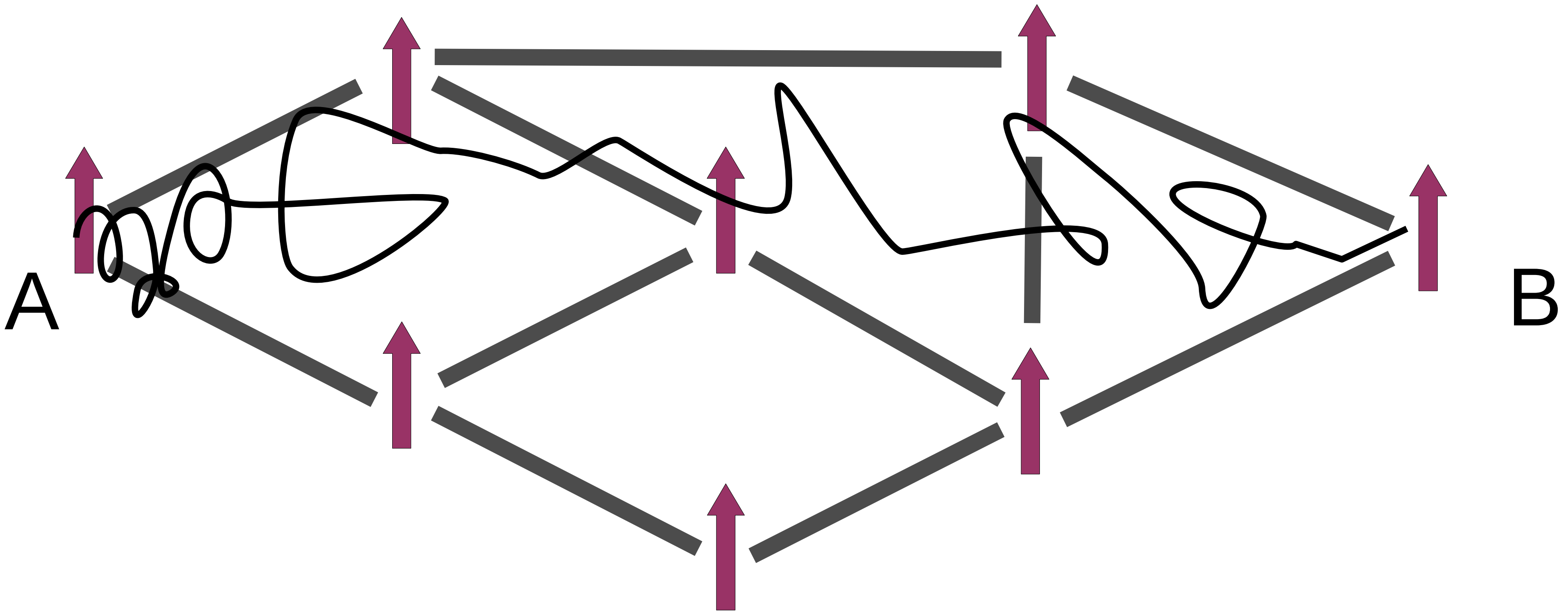
Squeezed states are non-classical, but not entangled; can they be created using entanglement?

Does long-distance entanglement help?

Problems to Solve

- Well, repeaters don’t work yet… (QKD does)
- **Lots** of networking problems:
  - Routing of “messages”
  - Resource management in networks
  - Protocol design
  - Network Coding (Net. Info. Flow)
  - Effective use of wide-area, large-scale entanglement

Routing

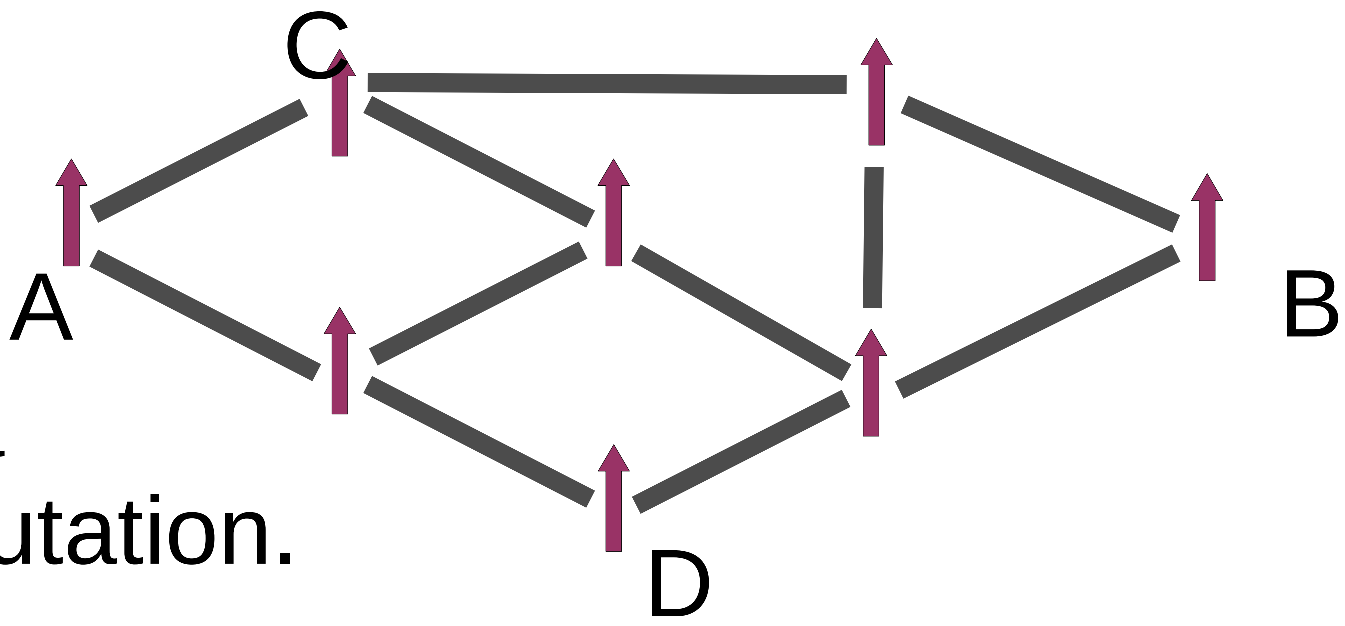


Simple.

...but we don’t yet know the cost metric.

Resource Management (QoS?)

A<->B & C<->D want to talk.



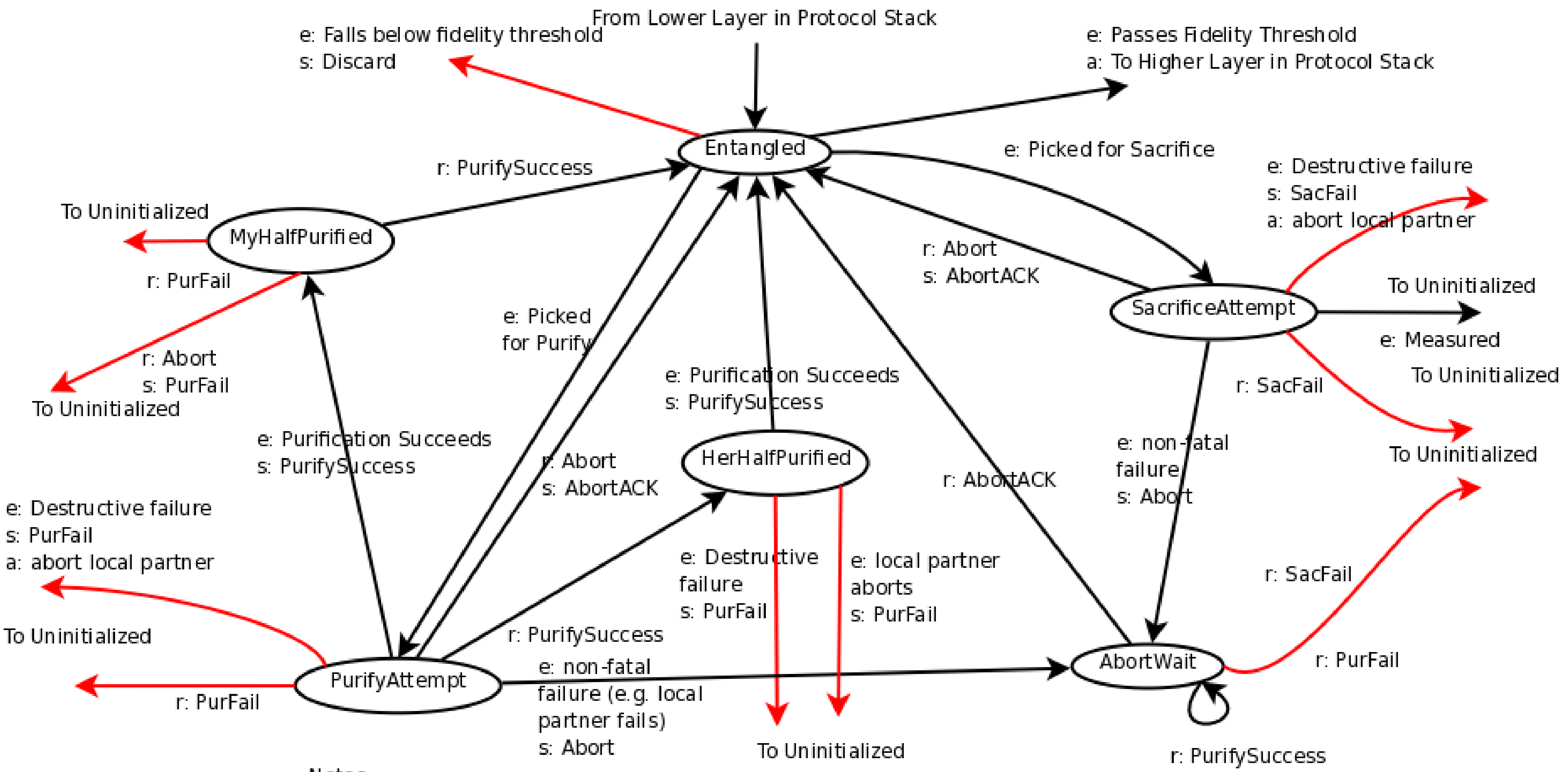
Remember, it's a *distributed* computation.

Worse, fragile quantum memory means there is a *hard real time* component.

==>requires *circuit switching*???
(bottleneck likely is memory per node)

Protocol Design

Purification Control (PC) Protocol State Machine v5



Notes:
MyHalfPurified sends a "PurFail" when it receives "Abort", because they've crossed in the network.
"Discard" transitions not detailed. All states can discard, send a "Discard" message, and go back to "Uninitialized" (in EC layer). Epoch gets incremented, and all old msgs discarded after that. "Abort" with an old epoch should be responded to with "Discard", I think.
I think there are still one or two holes in the coordination between the purifying and sacrificed partners.

Legend:
r: received message
e: local event
s: message sent
a: local action

Conclusions

- Entangled Quantum Internet will be buildable (eventually)
- Digital applications include quantum key distribution, leader election, simple connection of distributed resources
- Gyroscopic uses include possible “Big Science” projects like gravity wave observatories
- ...and there are lots of fun networking problems before we get there

AQUA: Advancing Quantum Architecture

http://www.sfc.wide.ad.jp/aqua/

with thanks to

Chip Elliott,

Kohei M. Itoh, Thaddeus Ladd,

Kae Nemoto, Bill Munro,

Gerard Milburn, C. Walker, Min Yun