Networking Problems in Using Quantum Repeaters

Rodney Van Meter

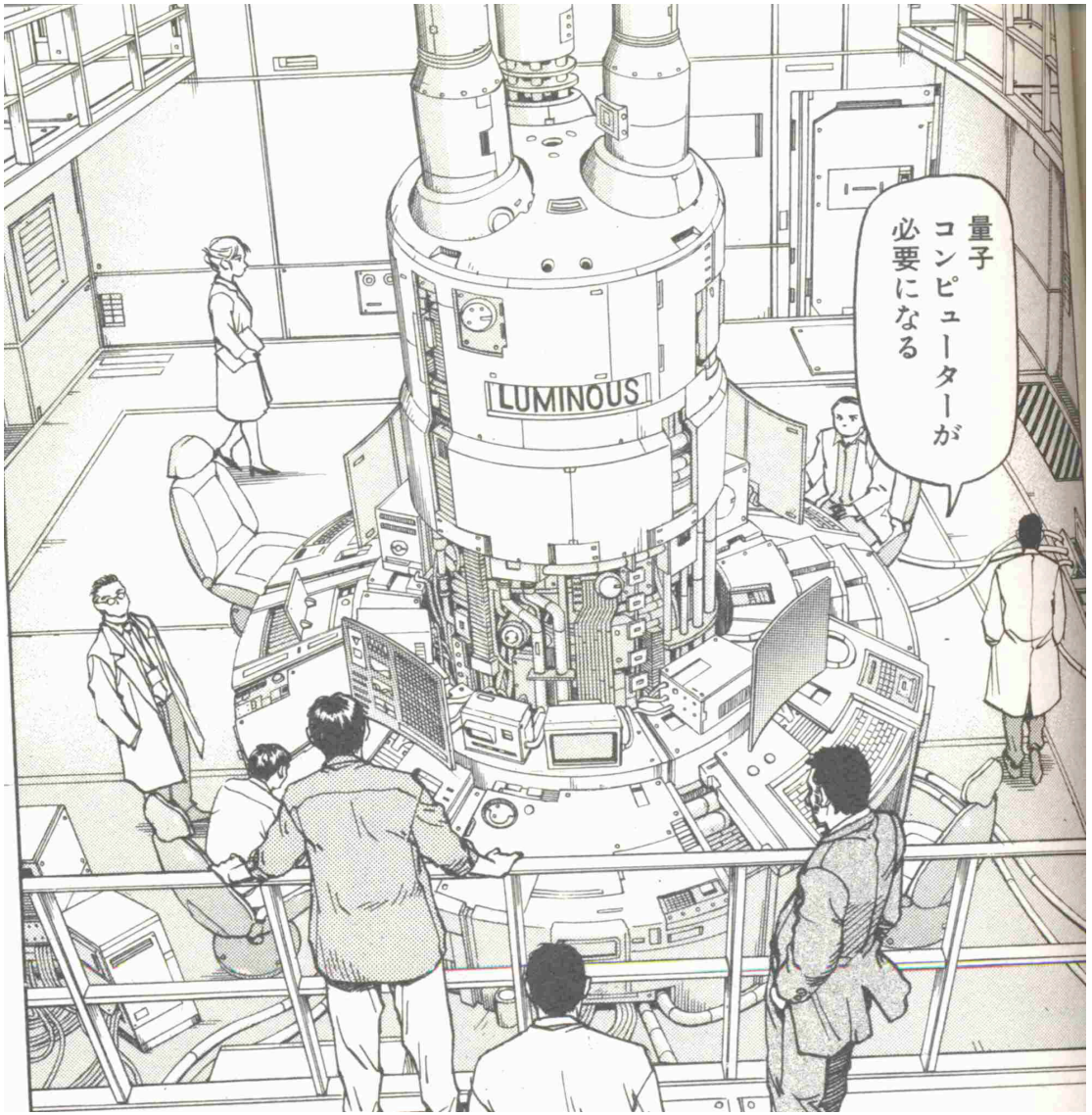
MAUI, 2009/4/16

rdv@sfc.wide.ad.jp

http://www.sfc.keio.ac.jp/~rdv/

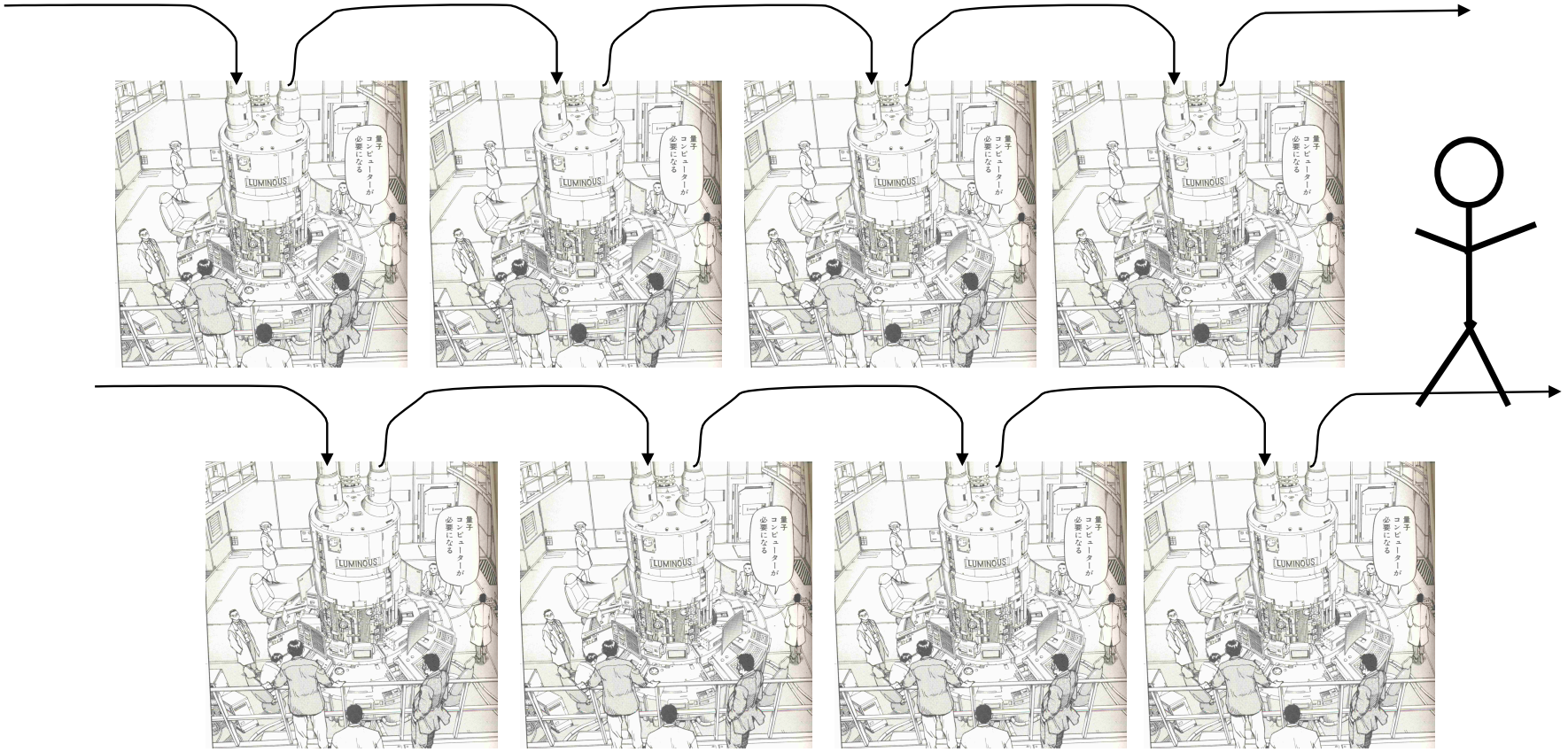
KEIO 150
Design the Future

Assume a Quantum Computer Like This...



KEIO 150
Design the Future

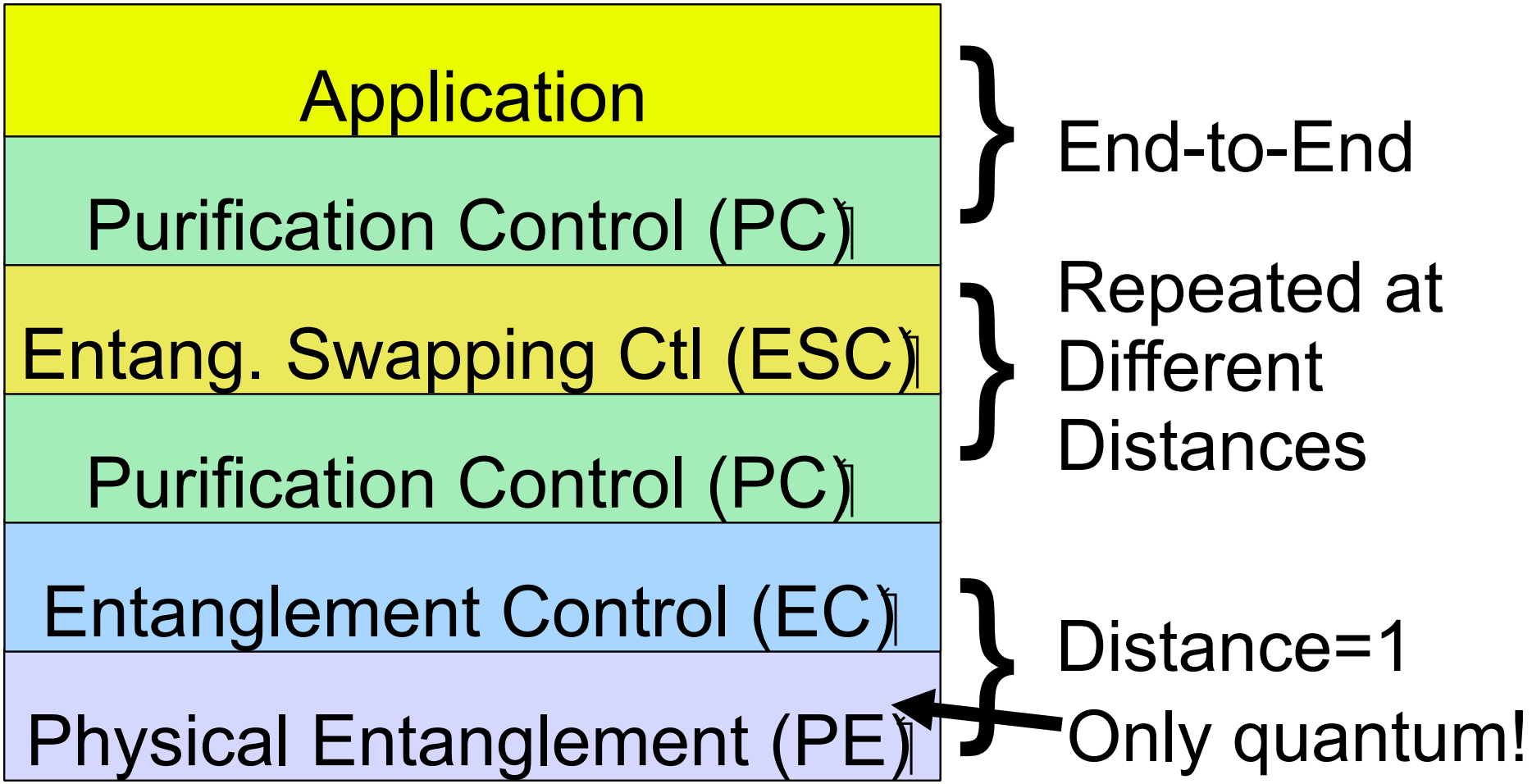
I want to Build a Distributed Quantum System Like This



Laboratory-sized quantum multicomputer or transcontinental network, either one!

KEIO 150
Design the Future

Repeater Protocol Stack



Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear), quant-ph:0705.4128

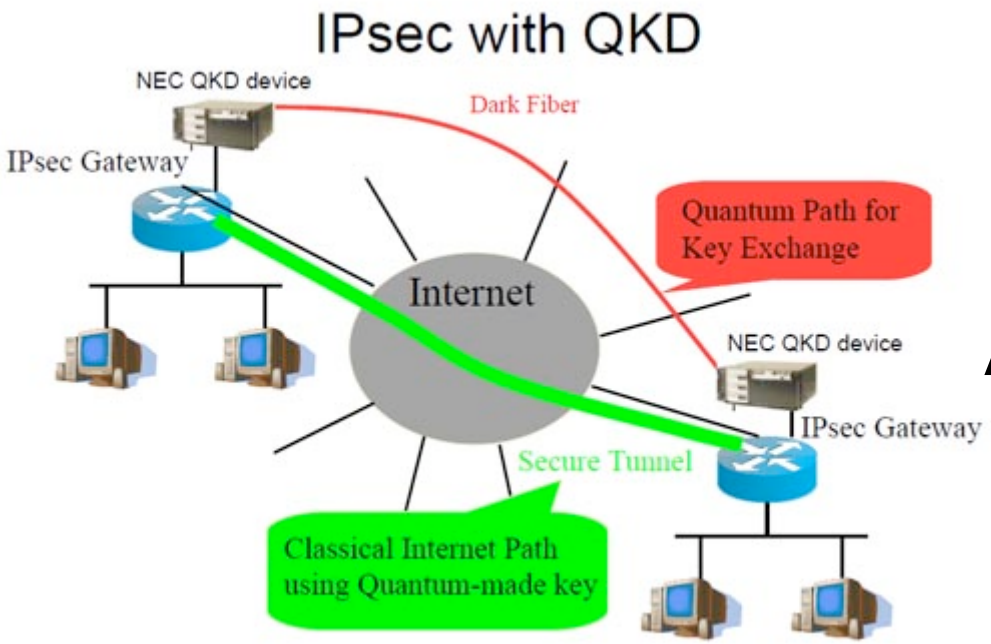
KEIO 150
Design the Future

Outline

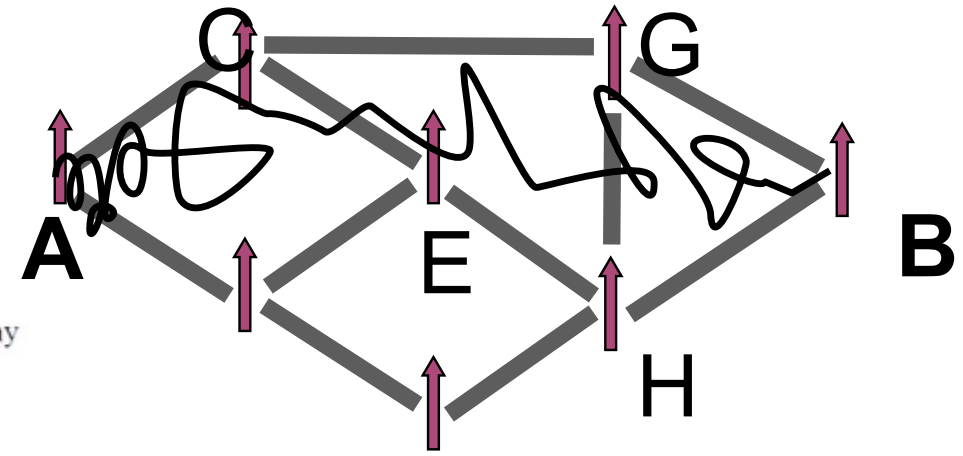
- Two types of quantum networks
- IPsec with QKD
  - IPsec with QKD
  - US & European efforts
  - Open problems & plans
- Repeaters
  - Basic concepts
  - Our recent results
  - Open problems & plans

Two Types of Quantum Networks

Unentangled Networks



Entangled Networks

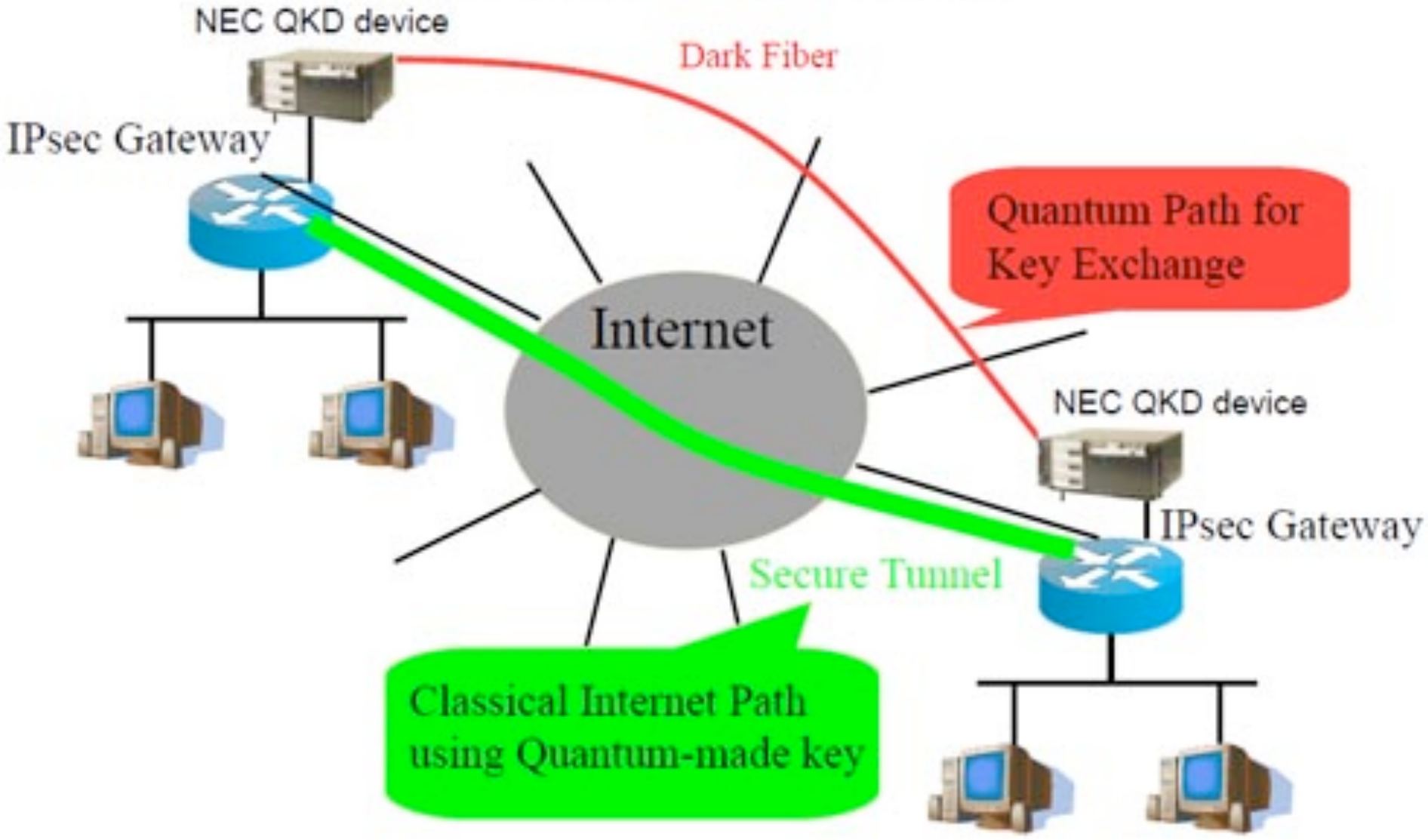


KEIO 150
Design the Future

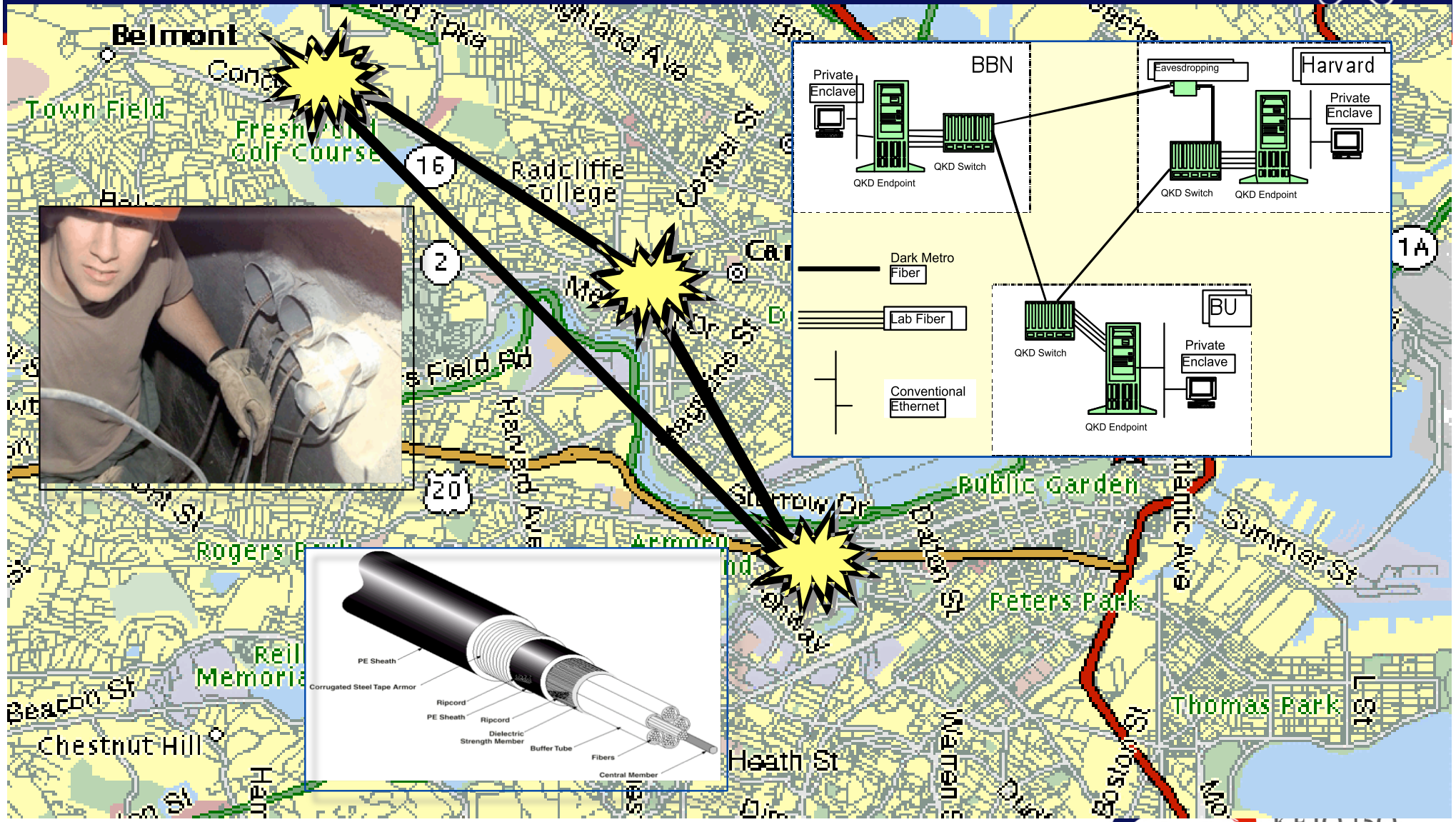
Quantum Key Distribution (QKD)

- Creates a *shared, random secret* between two nodes
- Uses physical effects to guarantee that key has not been observed
- Requires authenticated classical channel
- Limited to <150km per hop

IPsec with QKD



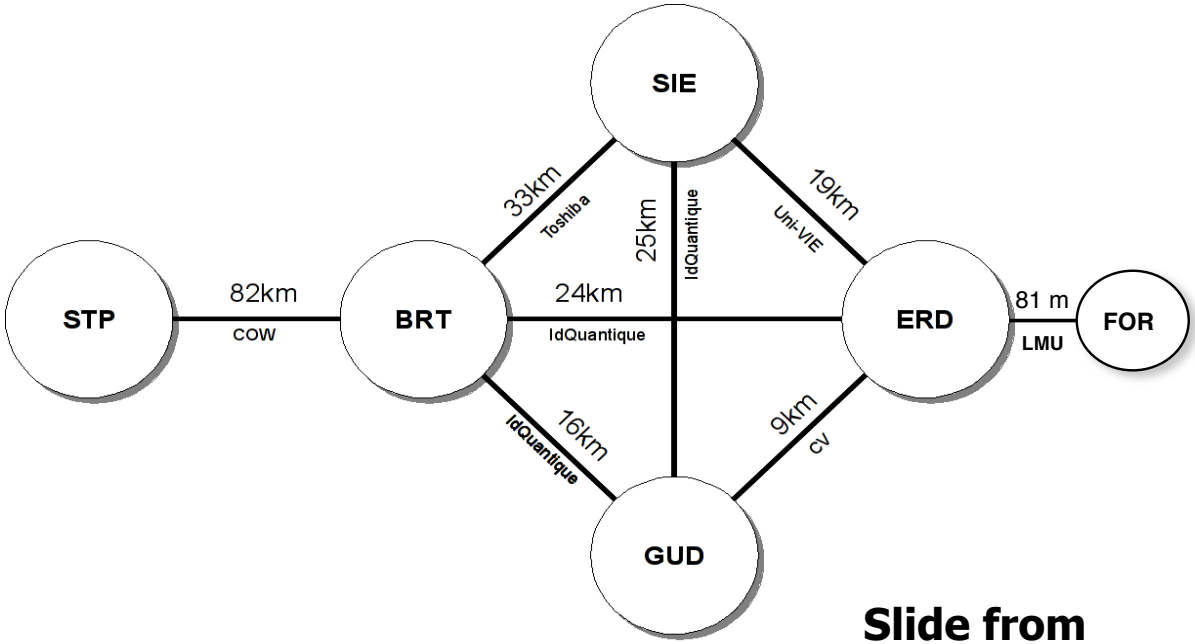
The DARPA Quantum Network



slide from Elliott, BBN

KEIO ISC
Design the Future

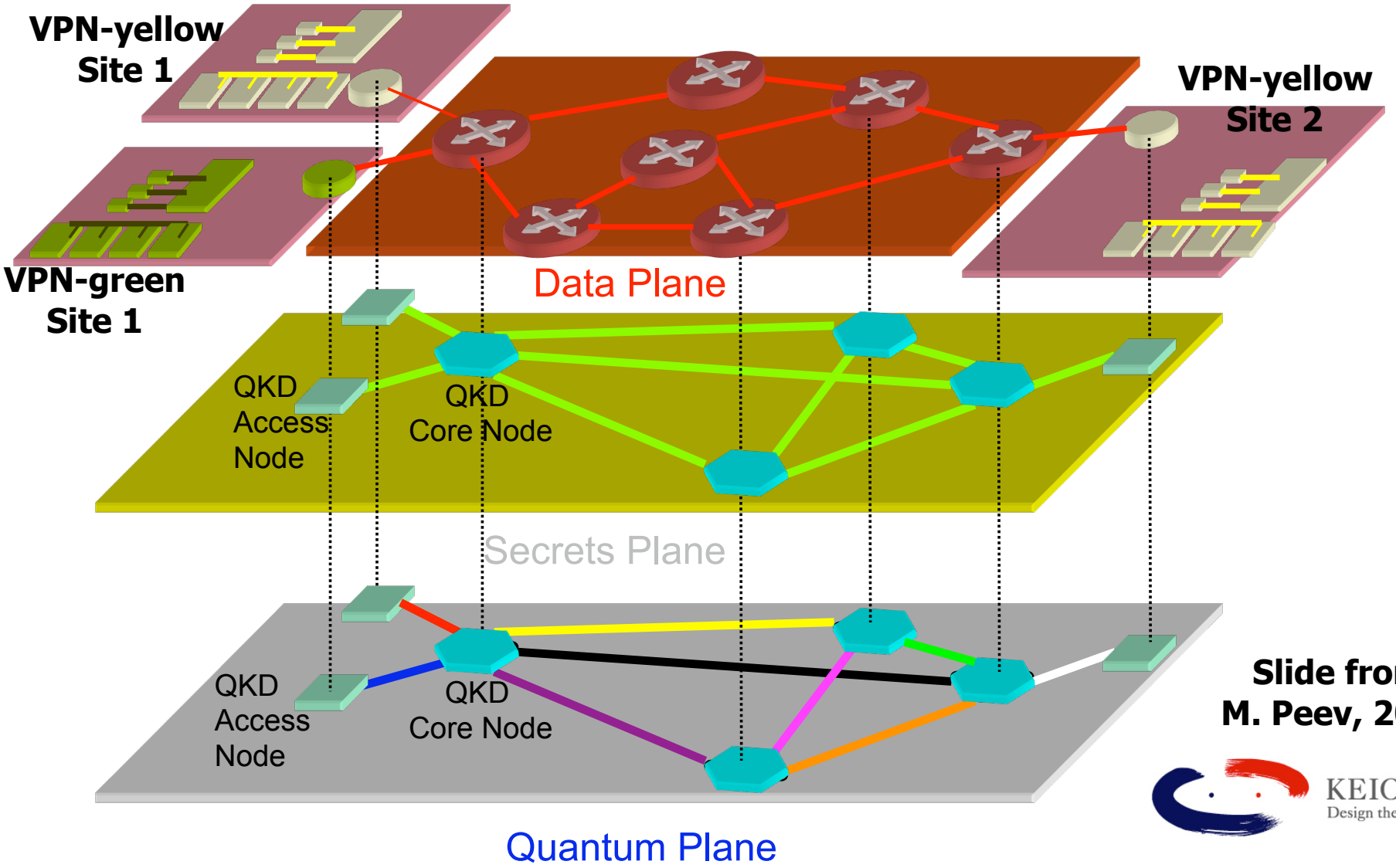
SECOQC Prototype – principle layout



Slide from M. Peev, 2008

KEIO 150
Design the Future

A Trusted repeater QKD-Network: Abstract Architecture (SECOQC, Europe)



Slide from M. Peev, 2008

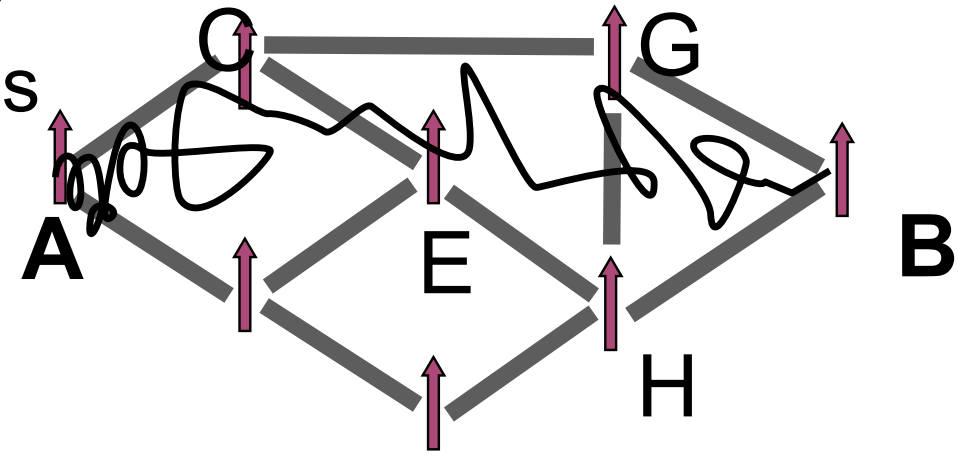
KEIO 150
Design the Future

QKD with IPsec Plans

- Test over raw fiber, Yagami<->K2
- Use key for one-time pad
- Work w/ NEC, BBN & ITU to standardize
- Write experimental I-D on IKE changes
- Take to IETF in Hiroshima?

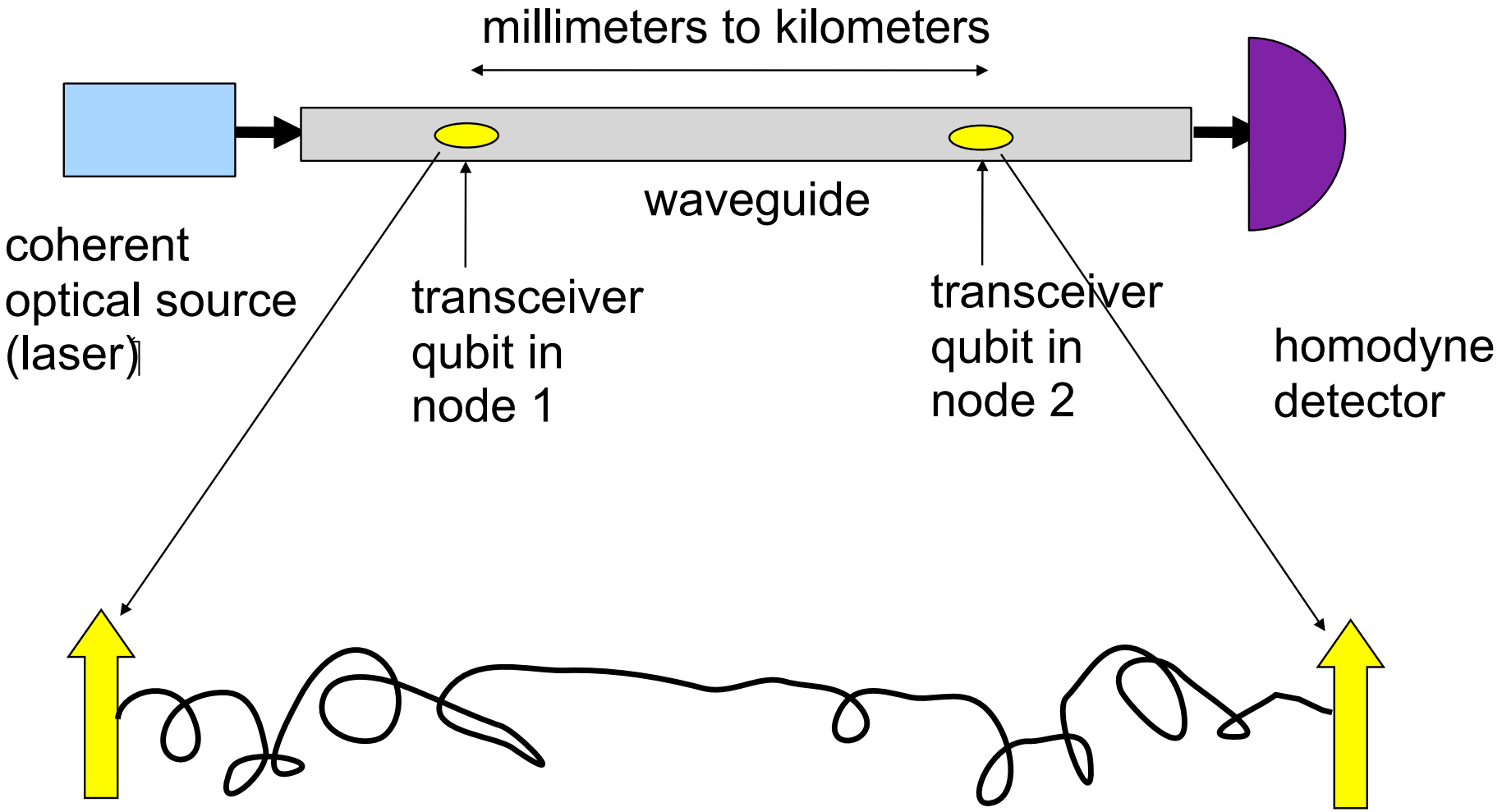
Outline

- Two types of quantum networks
- IPsec with QKD
  - IPsec with QKD
  - US & European efforts
  - Open problems & plans
- **Repeaters**
  - **Basic concepts**
  - **Our recent results**
  - **Open problems & plans**



KEIO 150
Design the Future

Network Link Technology (Qubus)

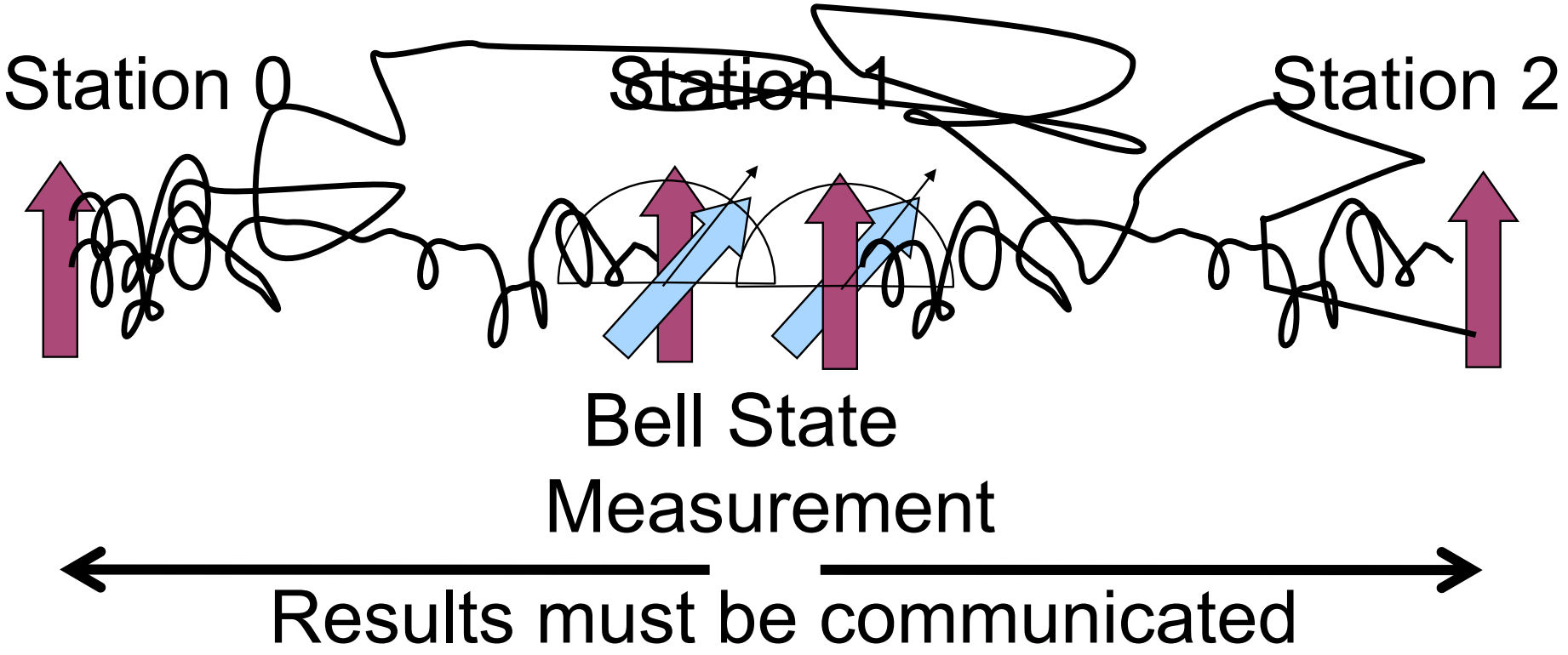


Munro, Nemoto, Spiller, New J. Phys. 7, 137 (2005)

Ladd et al., NJP 8, 184 (2006)

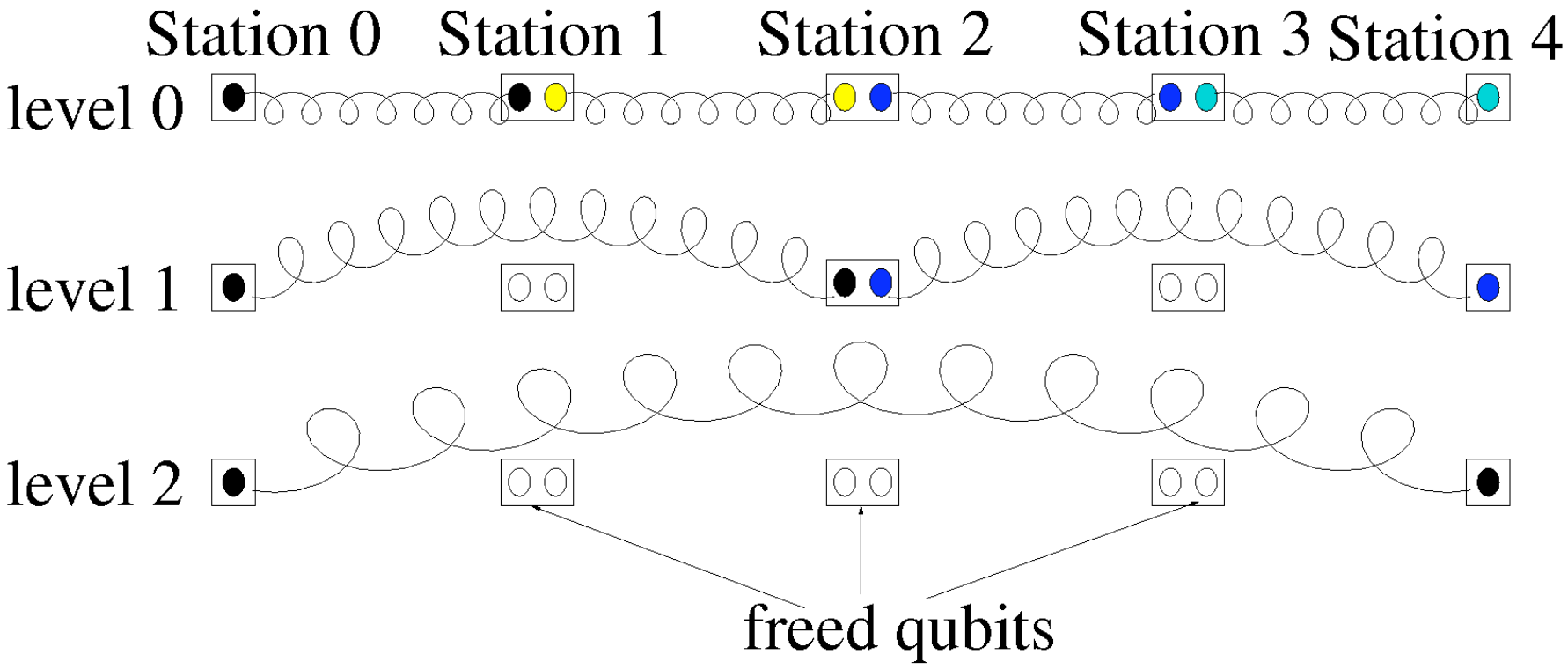
KEIO 150
Design the Future

Quantum Repeater Operation: Entanglement Swapping



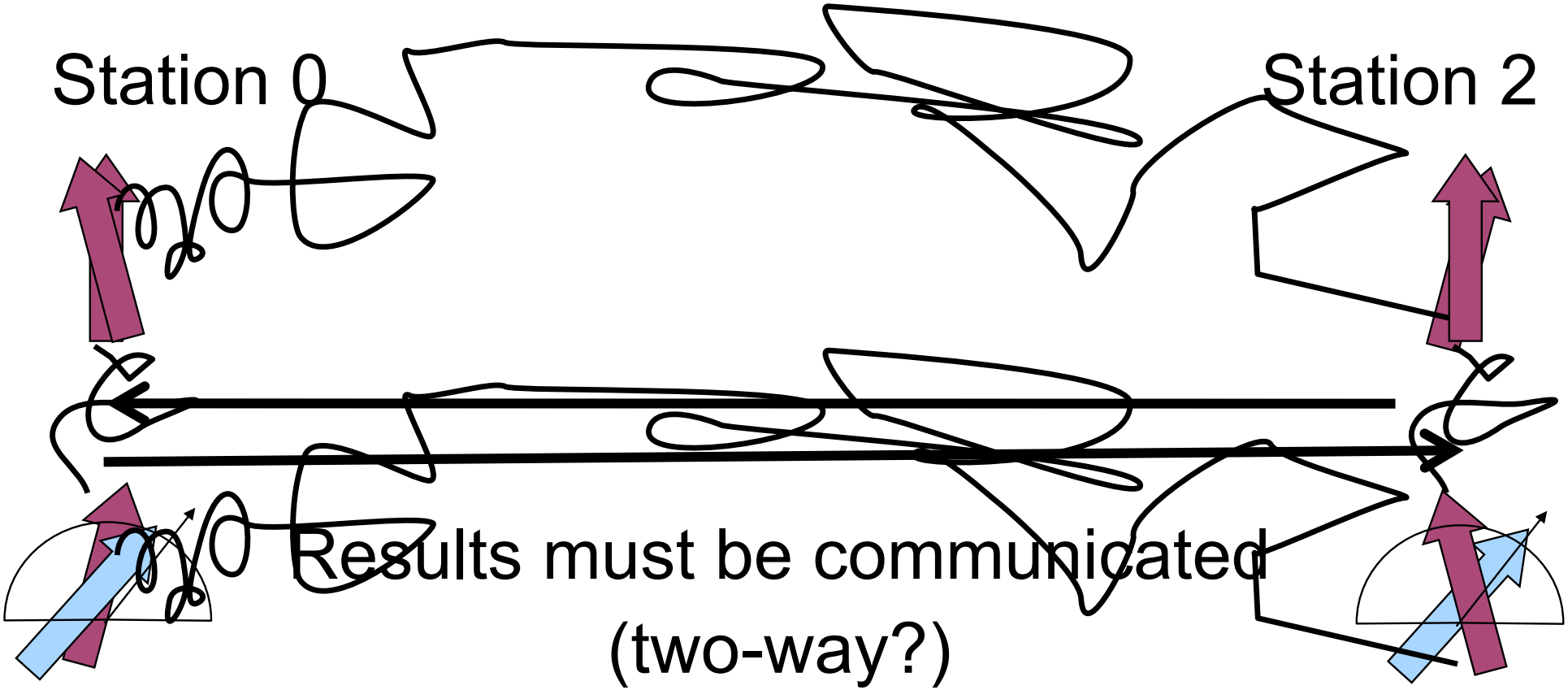
Fidelity decreases; you must *purify* afterwards

Nested Entanglement Swapping



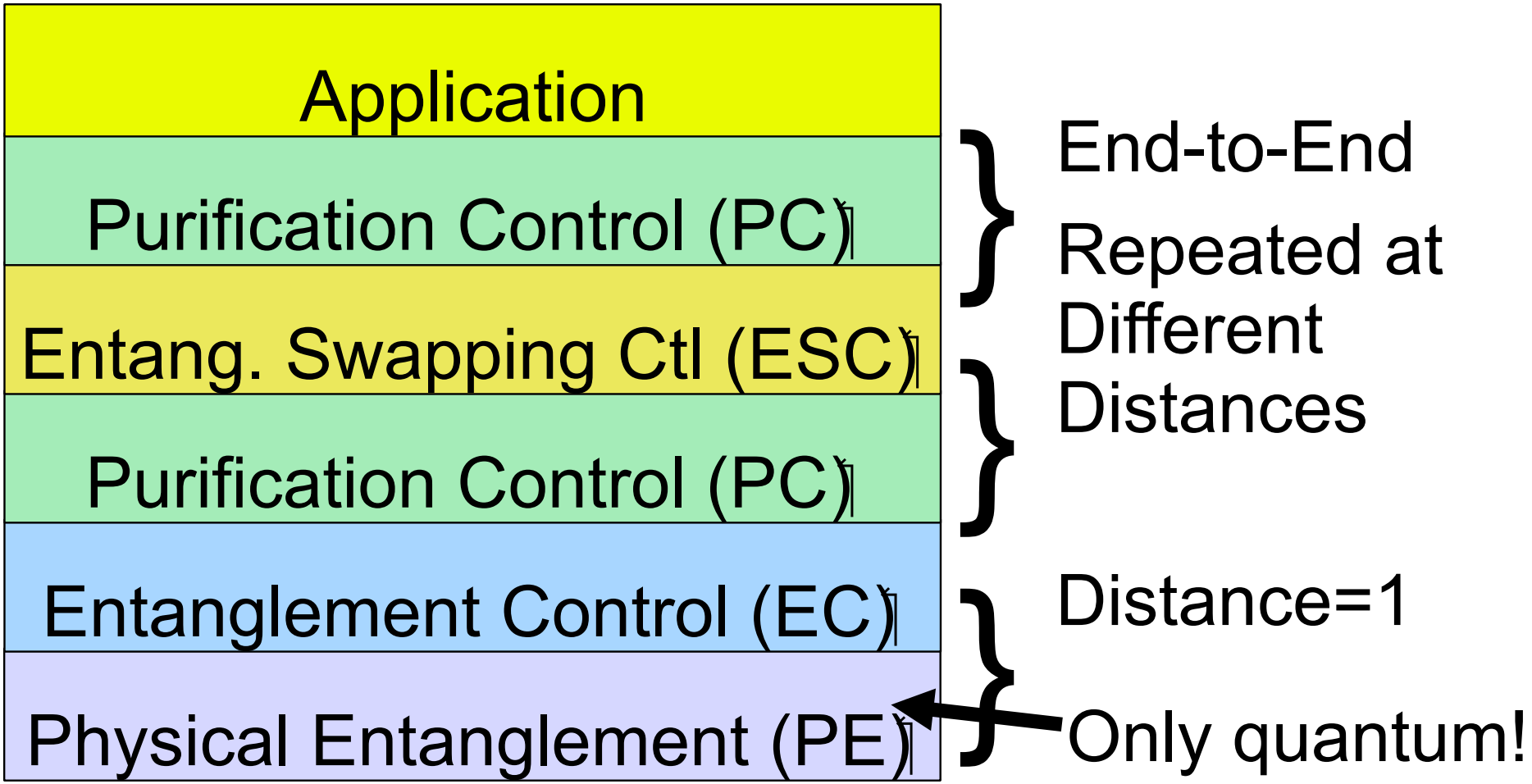
KEIO 150
Design the Future

Purification



KEIO 150
Design the Future

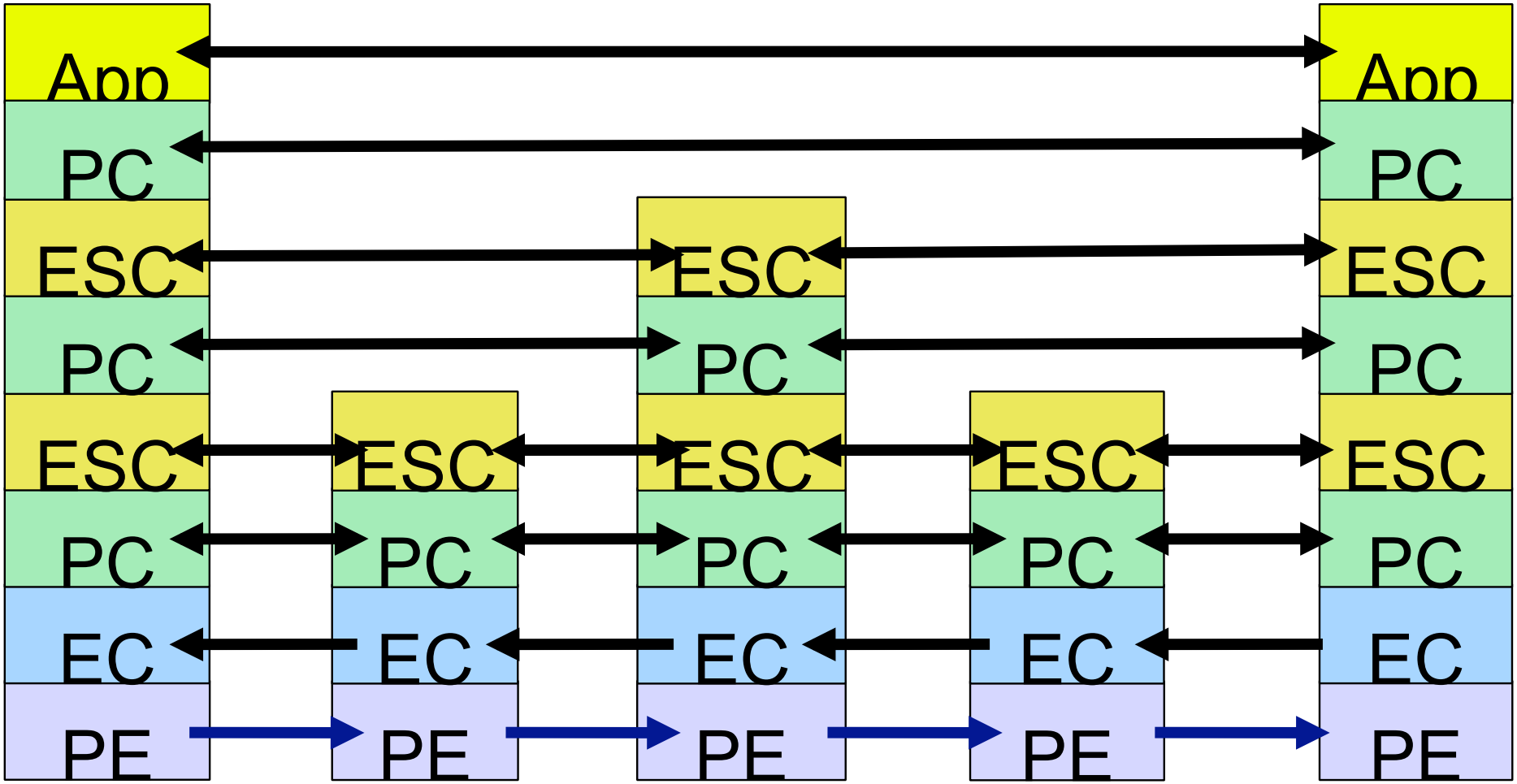
Repeater Protocol Stack



Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear), quant-ph:0705.4128

KEIO 150
Design the Future

Four-Hop Protocol Interactions



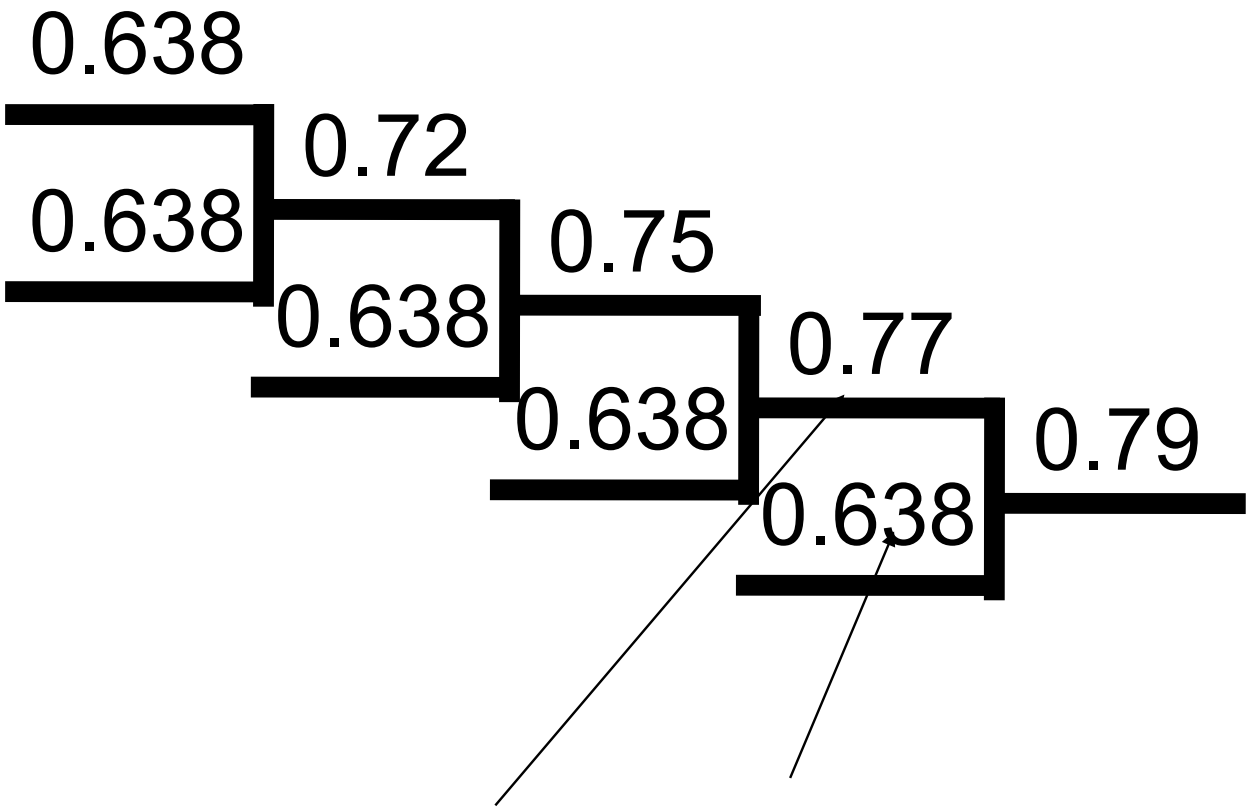
Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear)

The Repeater's Jobs

Entanglement swapping & purification, which require:

- A little bit of quantum communication
- Quantum memory
- Local quantum operations (gates & measurements)
- Lots of decision making (both local and distributed)
- Lots of classical communication

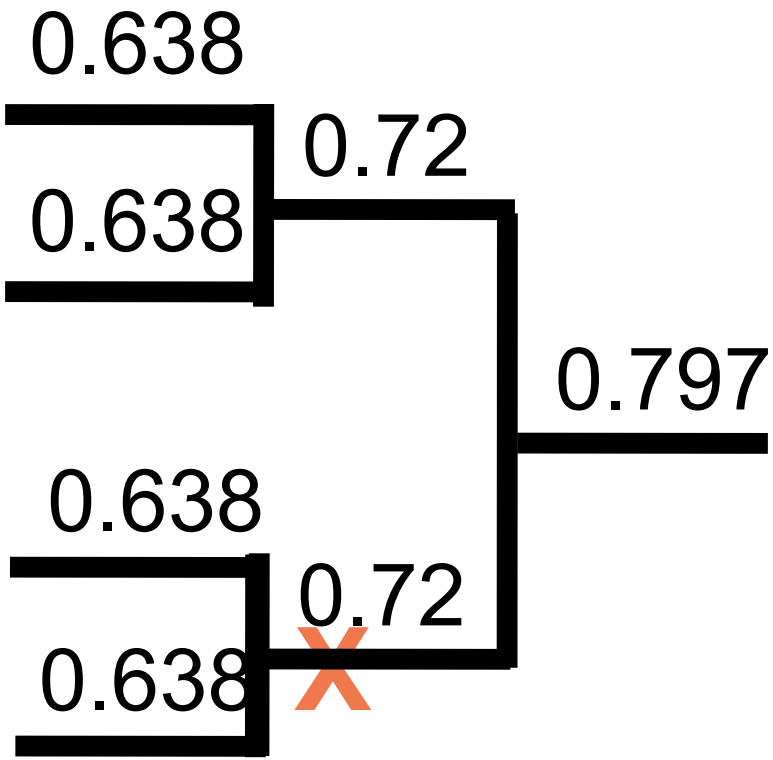
Entanglement Pumping



Ineffective w/ large fidelity difference

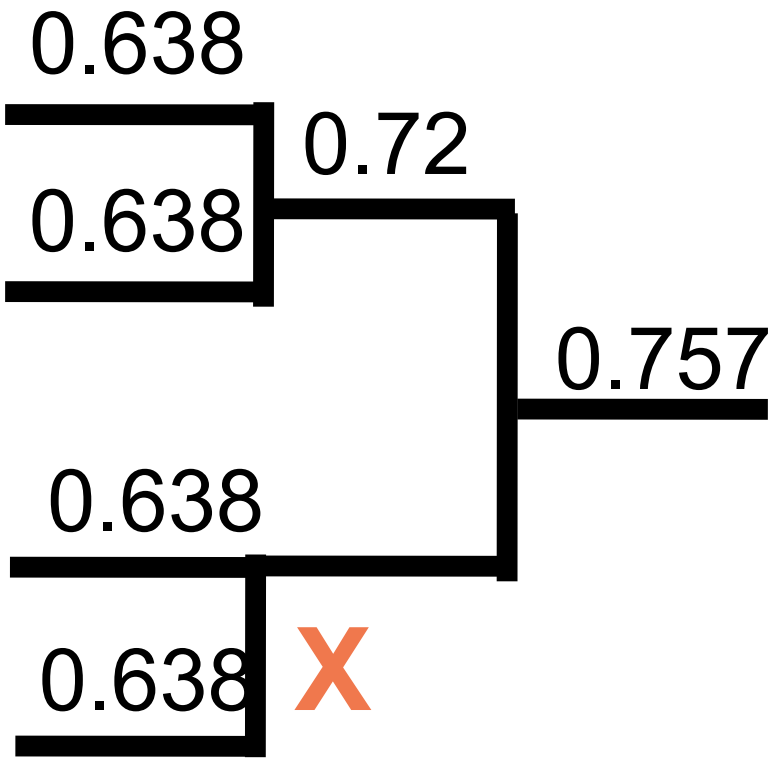
KEIO 150
Design the Future

Symmetric Purification



Problems:
Exact matching can require long waits.
Not realistic when memory effects (decoherence) considered.
Can deadlock if resources are limited.

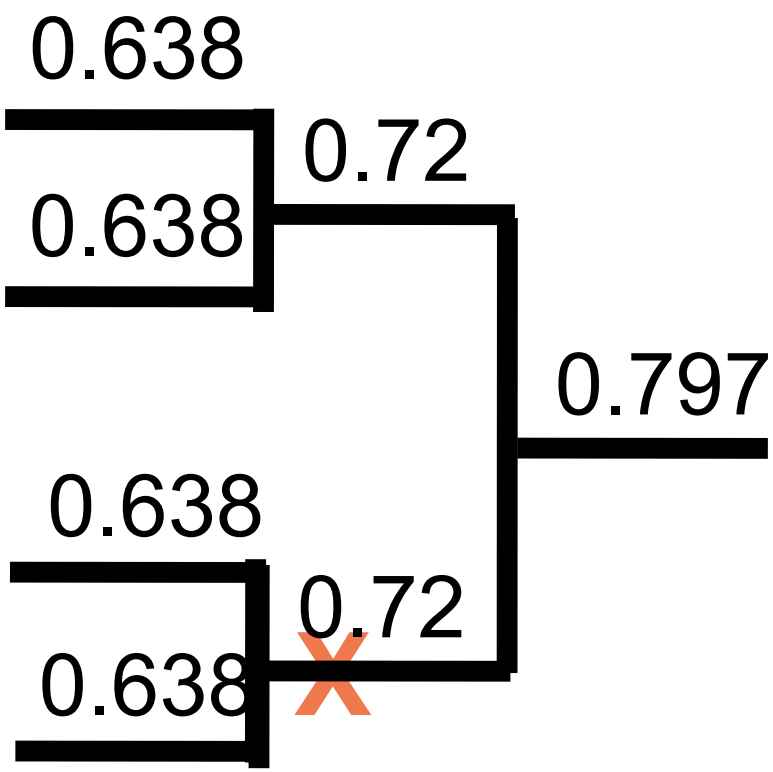
Greedy Purification



Doesn’t wait for anything, uses whatever’s available.

Works well w/ large number of qubits per repeater.

Banded Purification

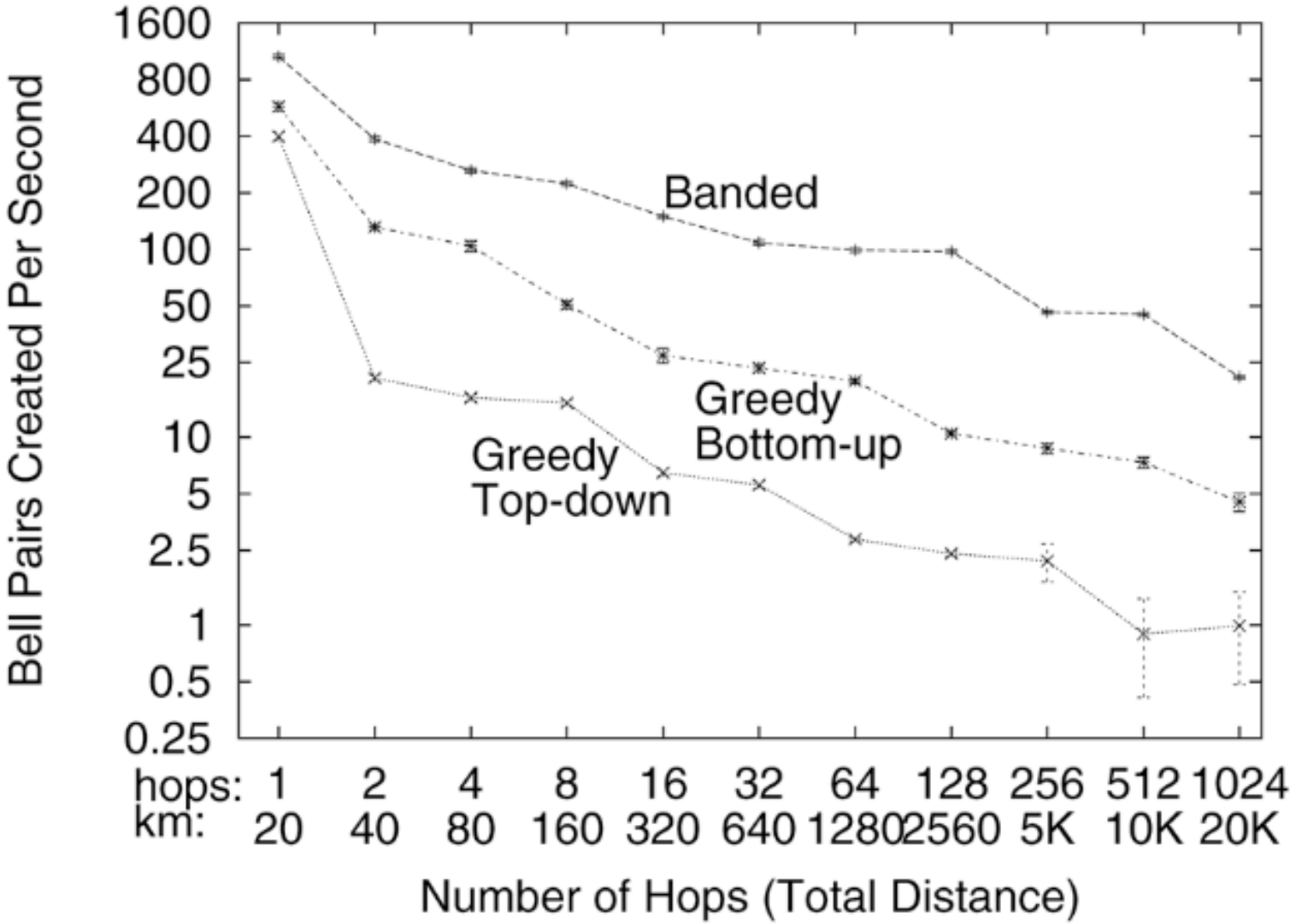


Large gains in throughput.
Moderate # qubits (5-50).
Avoids deadlock.
Realistic memory model.
Simple to implement in real time (even in HW).
Probably not optimal, but probably close.

Divide fidelity space into multiple *bands*
e.g., above & below 0.70

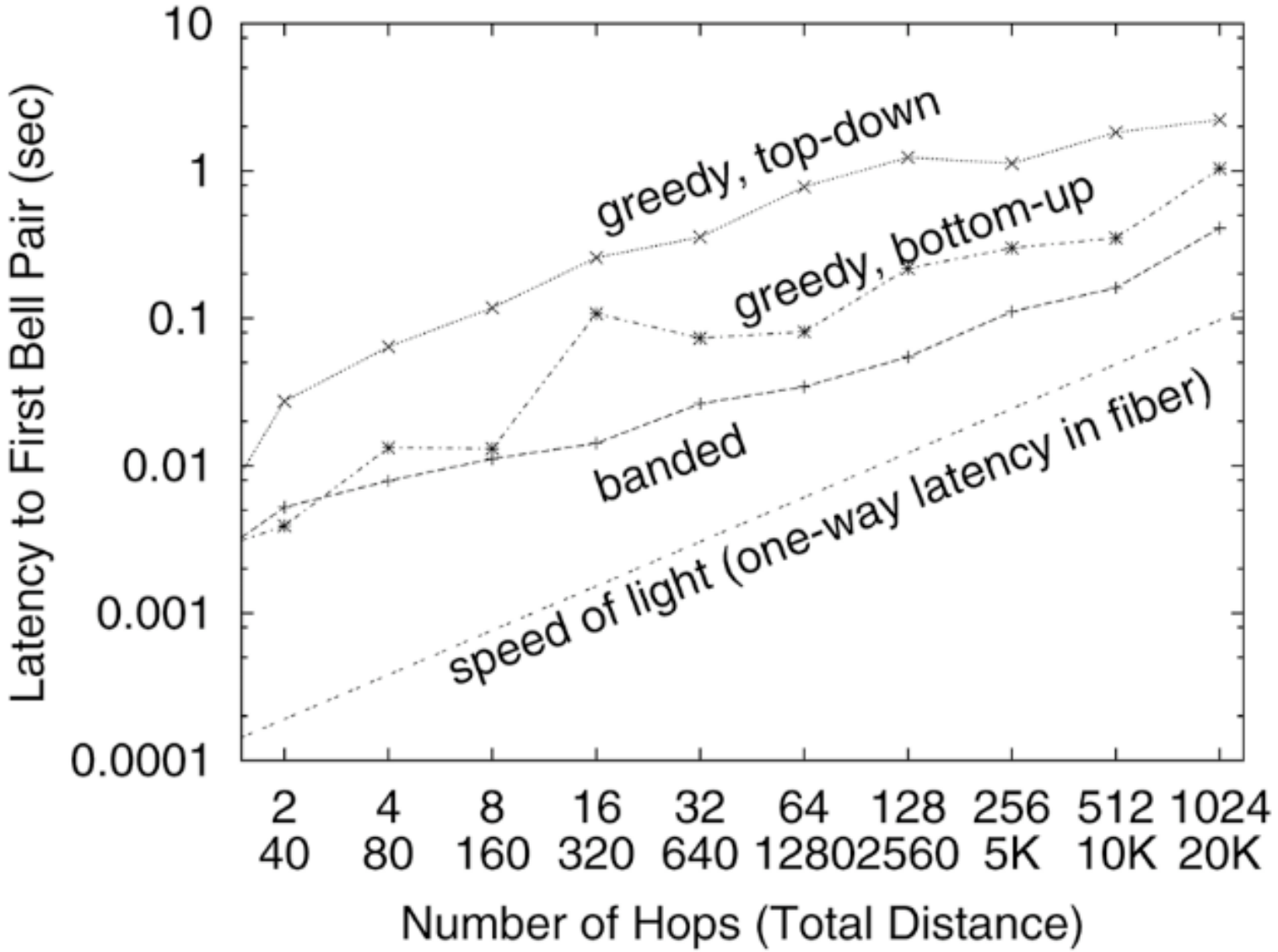
KEIO 150
Design the Future

Banded Purification Performance



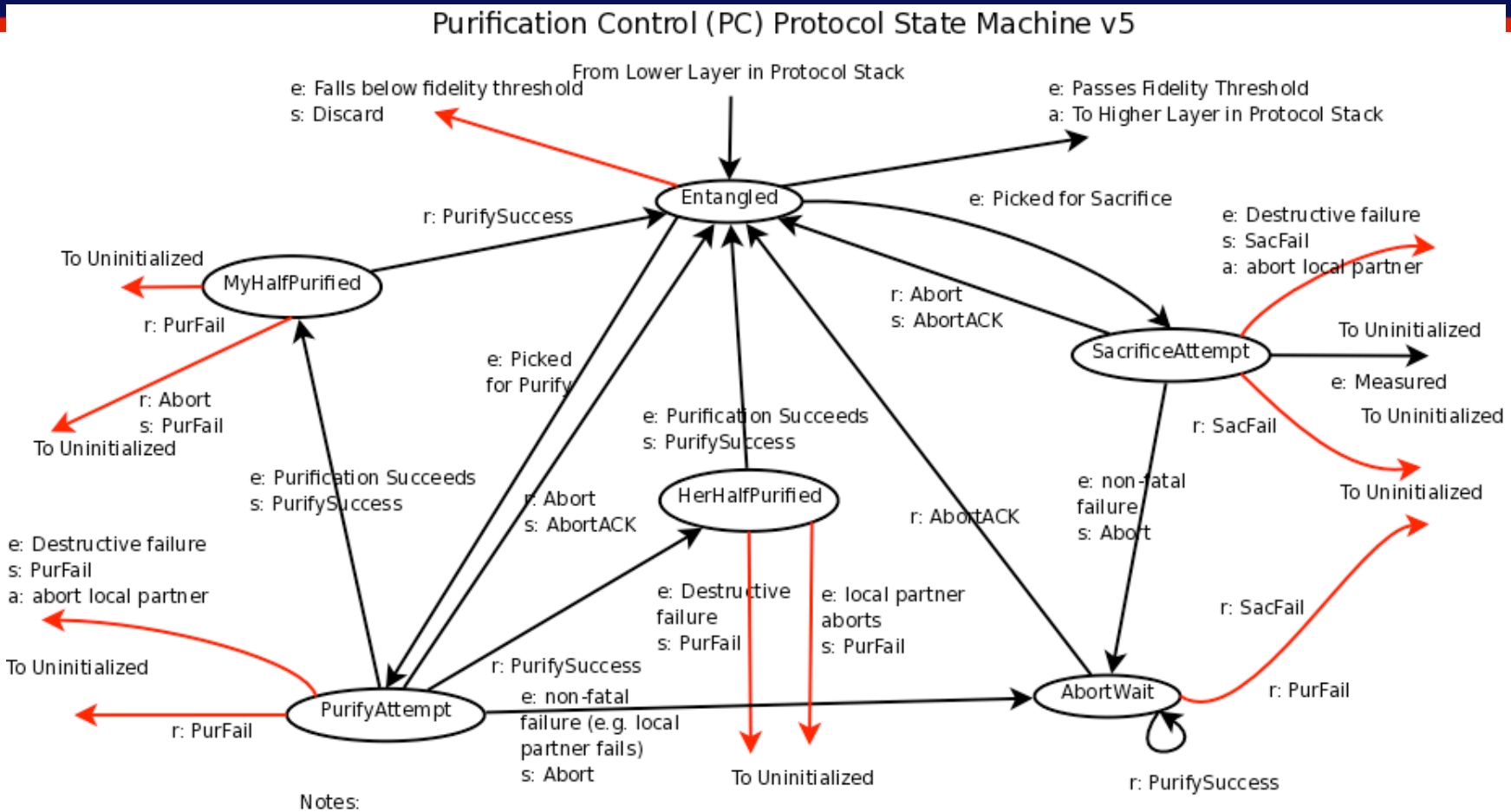
Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear), quant-ph:0705.4128

Banded Purification Latency

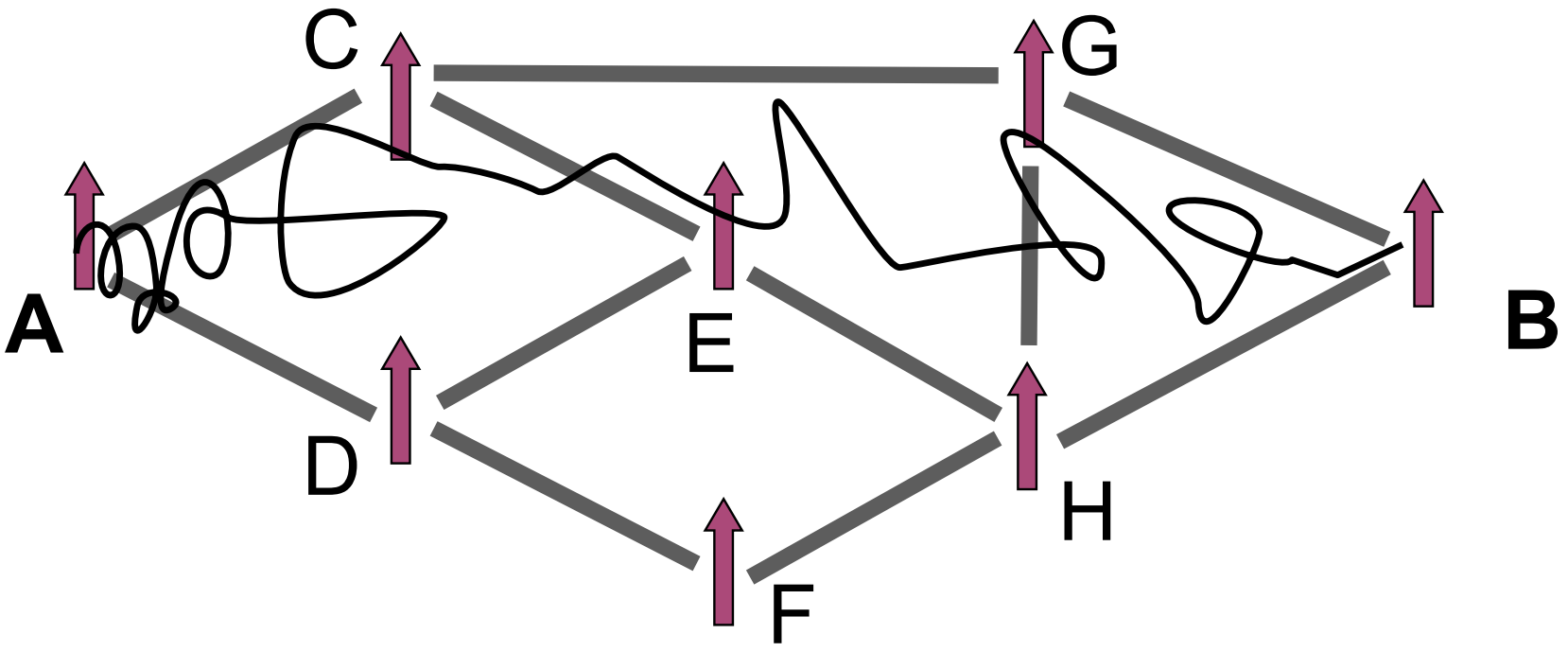


Van Meter *et al.*, IEEE/ACM Trans. on Networking, Aug. 2009 (to appear), quant-ph:0705.4128

Protocol Design



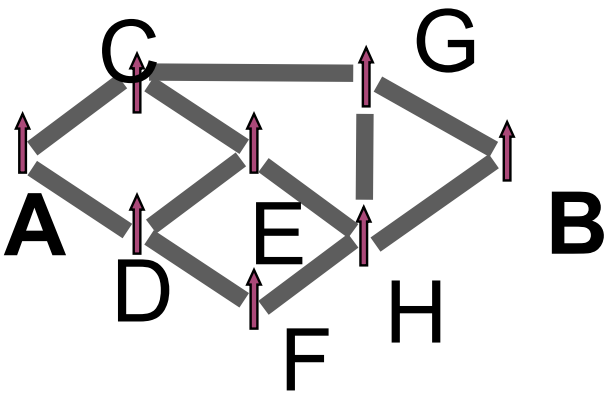
Routing



Simple: use Dijkstra's Shortest Path First.

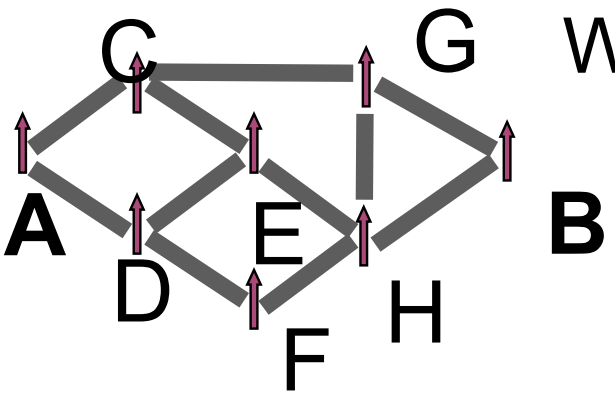
...but we don't yet know the cost metric.

A Different Meaning of "Which Path?"



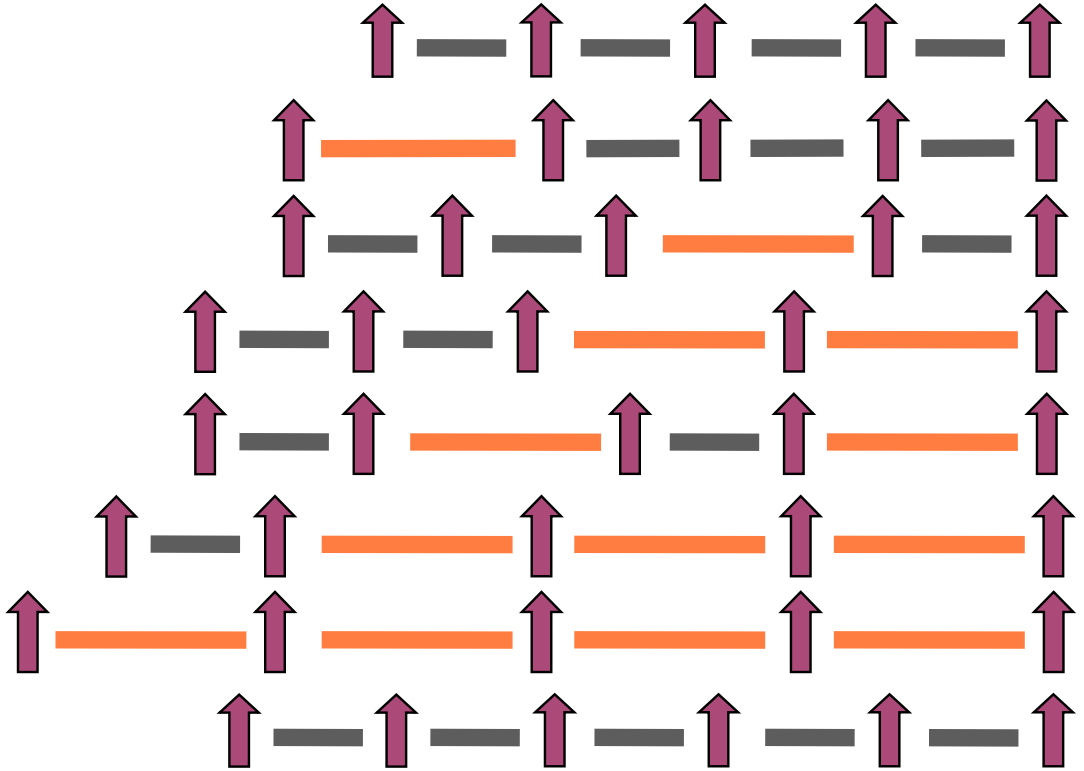
3 hops: ACGB
4 hops: ACGHB
ACEHB
ADEHB
ADFHB
5 hops: ACEHGB
ADEHGB
ADECGB
ADFHGB
6 hops: ACECGHB
7 hops: ADFHECGB
ACEDCHGB

But What is Distance?



What if hops are not homogeneous?

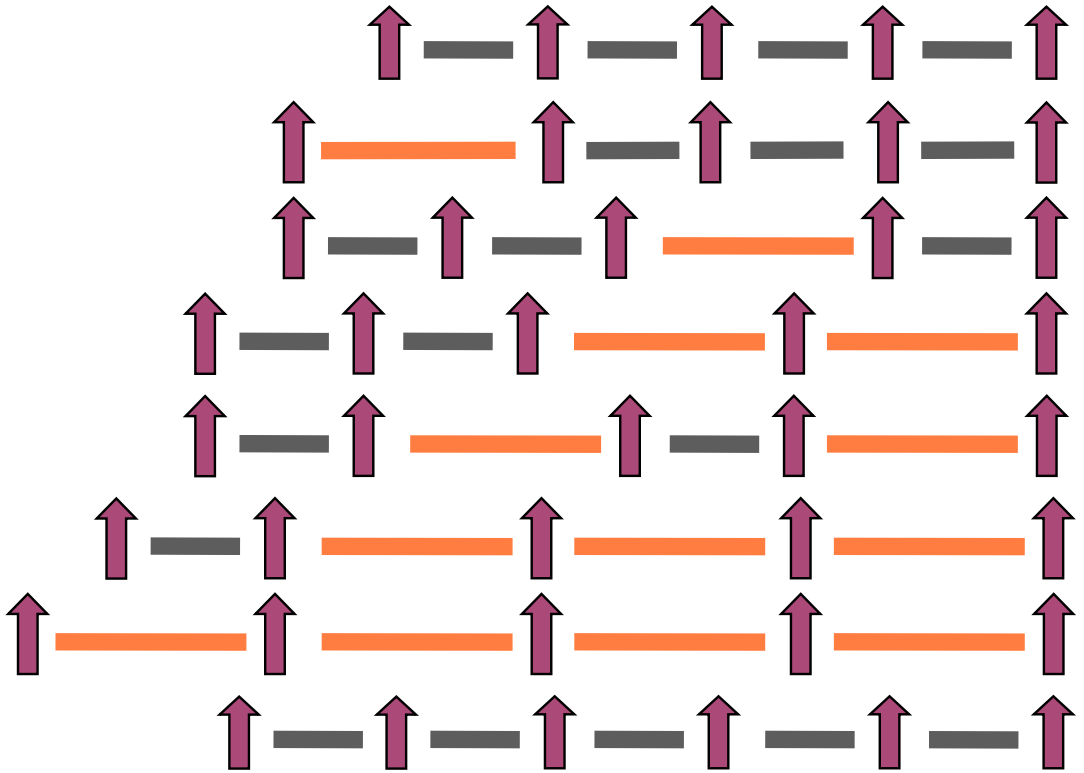
Are 2^n-1 hops,
2^n hops,
and 2^n+1 hops
significantly different?



KEIO 150
Design the Future

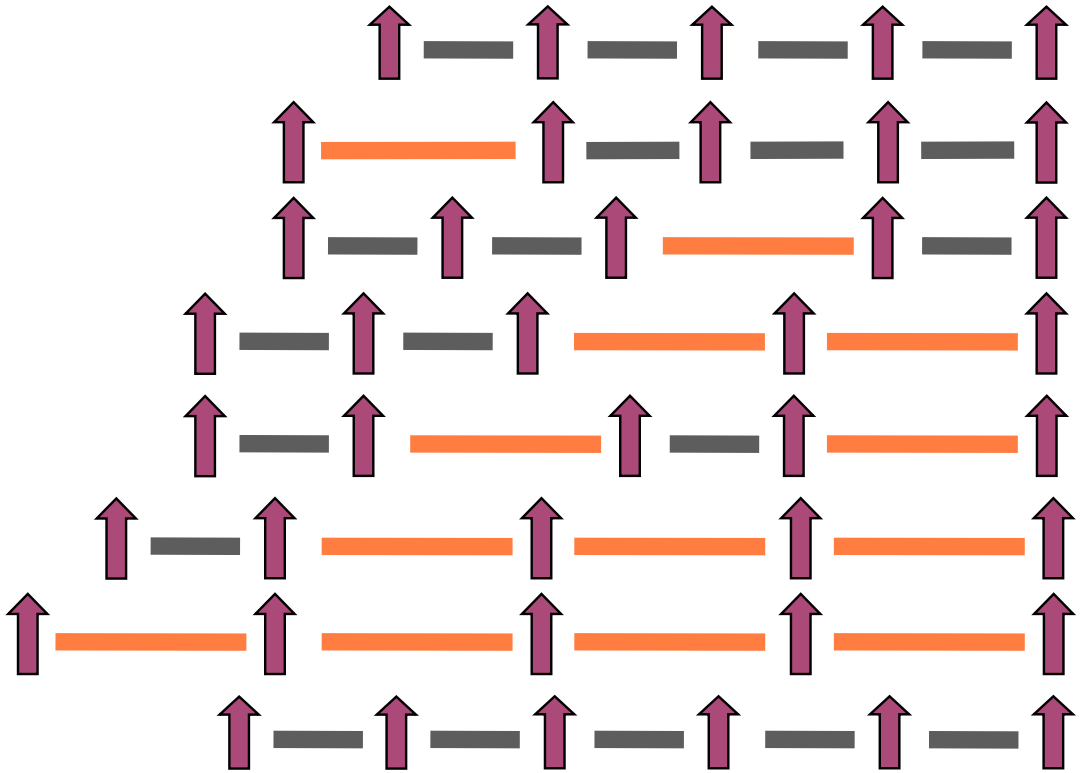
How Do We Order These?

- How does *number* of links matter?
- Does *number* of **weak** links matter?
- Does *position* of weak link matter?
- Is cost **additive?**
- At this logical level, is this technology-independent?



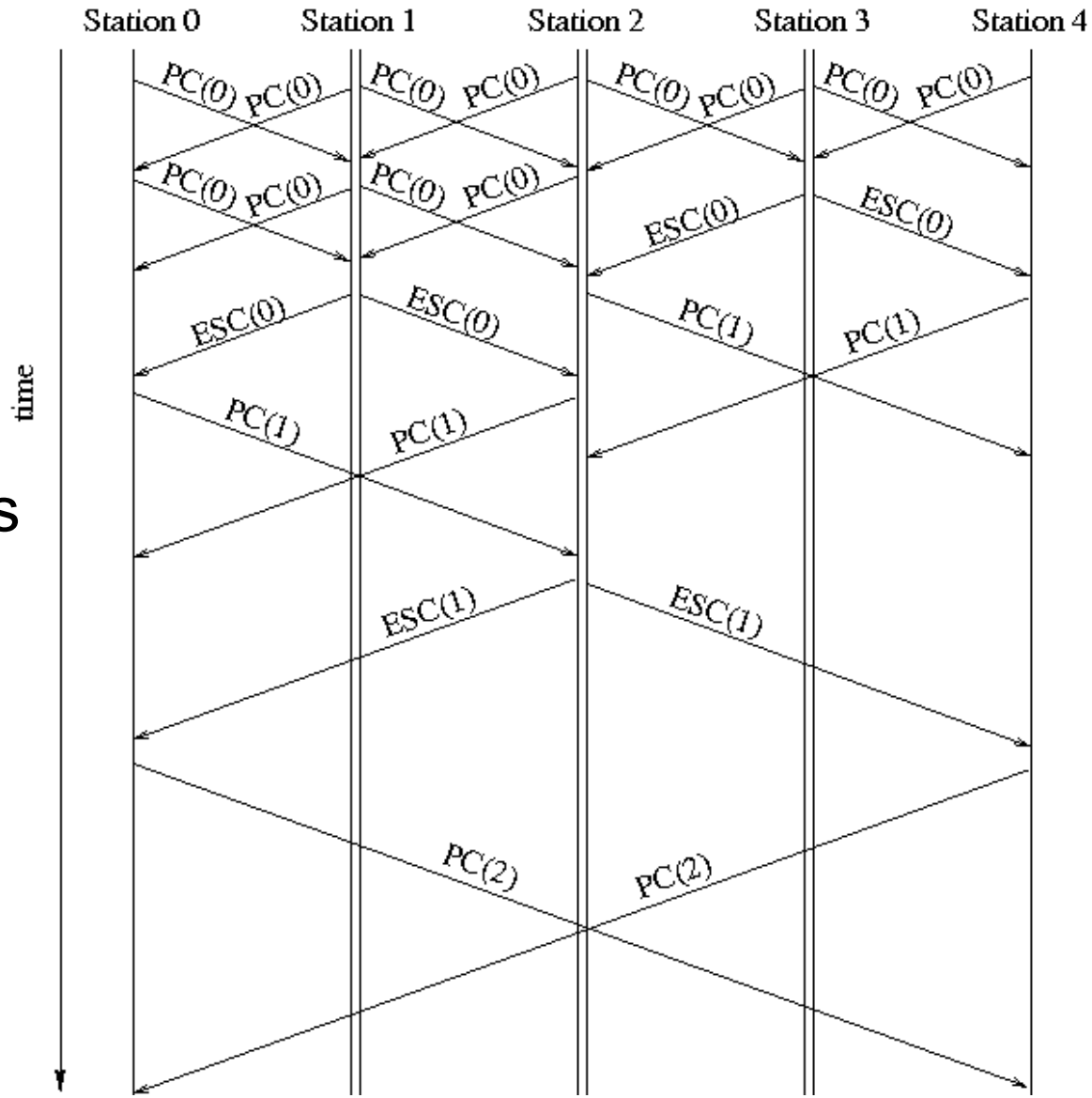
Other Problems

- Defining swap points
- Static or dynamic?
- Avoiding leapfrog
- Avoiding deadlock
- Minimizing waits for classical messages

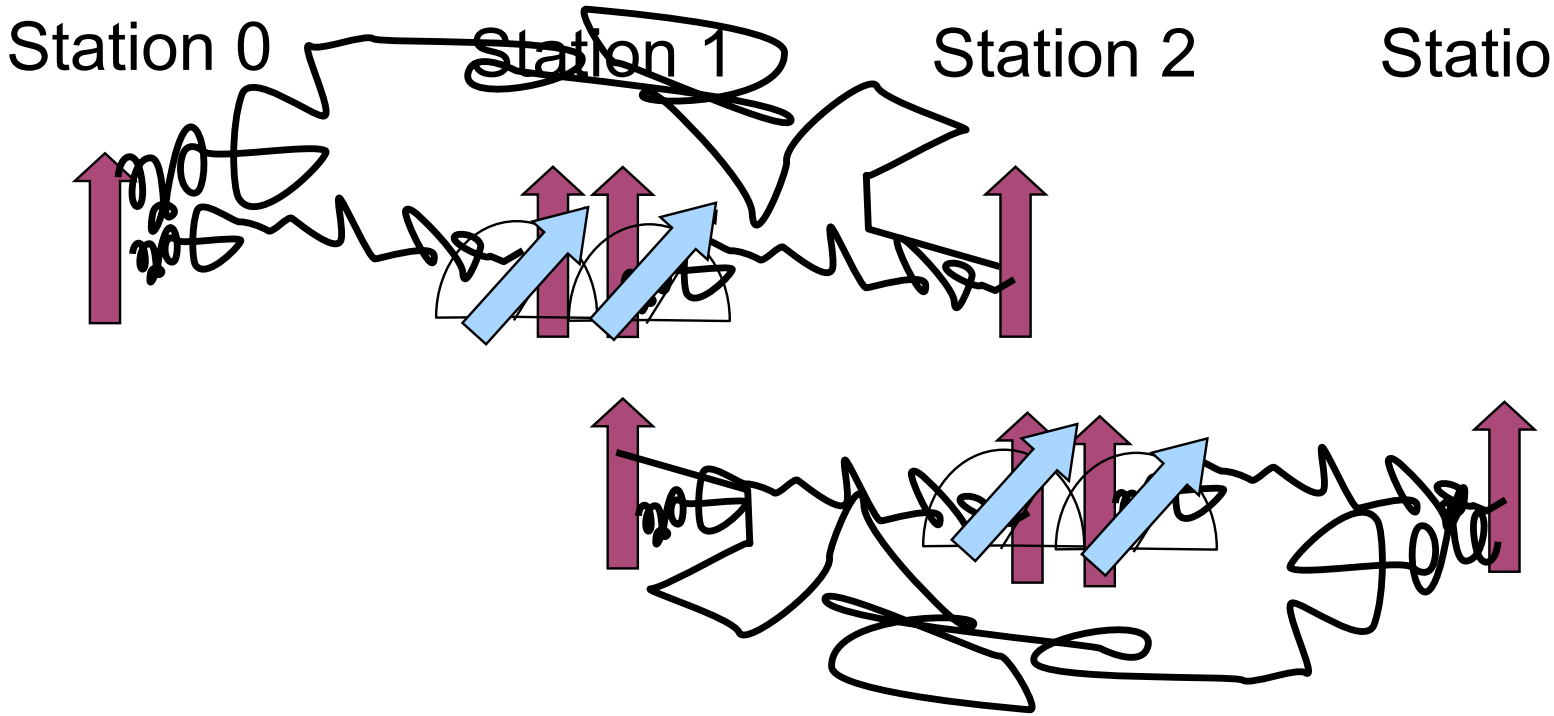


Other Problems

- Partial messaging sequence
- Can this be made more efficient?
- Due to memory degradation, gains will be better than linear



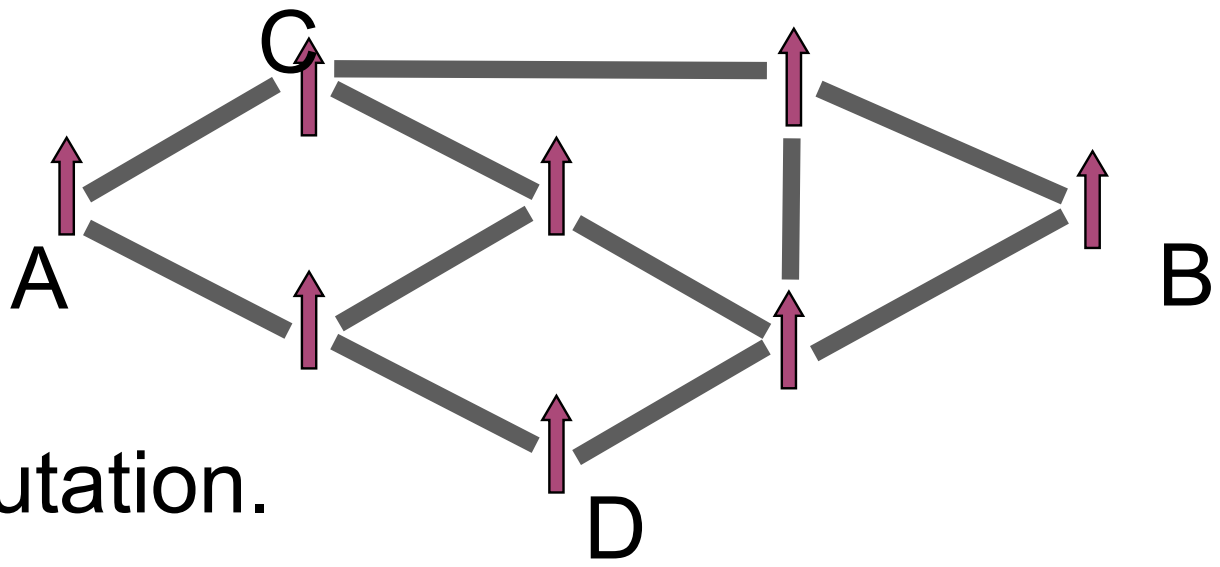
Leapfrog



KEIO 150
Design the Future

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)

Open Repeater Problems

- Well, repeater HW doesn’t work yet...
  - Sims of “weak links” mostly functional
  - Establishing swapping points
  - More dynamic behavior
  - Non-power-of-two hops
  - Finish & publish protocol state machine

Open Complex Network Problems

- Coding partially done
  - Using graphviz file format
  - Routing not done
  - Workload generator needs work
  - QoS / resource allocation not implemented
- Visualization of networks
- Investigate graph states & quantum network coding
- More detailed workload definition

Milestones for JSPS

- Define a cost metric
  (figure out if it's additive!)
- Define a path selection algorithm
- Define test cases
- Simulate that set of test cases
- Extend to topologically complex networks
- Create static visualizations

Food for Thought

- When will first *Science* or *Nature* paper appear *using* a quantum computer, but not *about* the quantum computer?
- That is, when will a quantum computer ***do*** science, rather than ***be*** science?
- Answers from quantum researchers range from “less than five years” to “more than forty years”

Thanks

Thanks to Thaddeus Ladd, Bill Munro and Kae Nemoto (coauthors on much of this work), as well as Austin Fowler, Jim Harrington, Kohei Itoh, Agung Trisetyarso, Byung-Soo Choi, Shota Nagayama, and Takahiko Satoh

And funding from NICT, MEXT, NSF, the Mori Fund at Keio, and now **JSPS** for funding.

KEIO 150
Design the Future

AQUA: Advancing Quantum Architecture