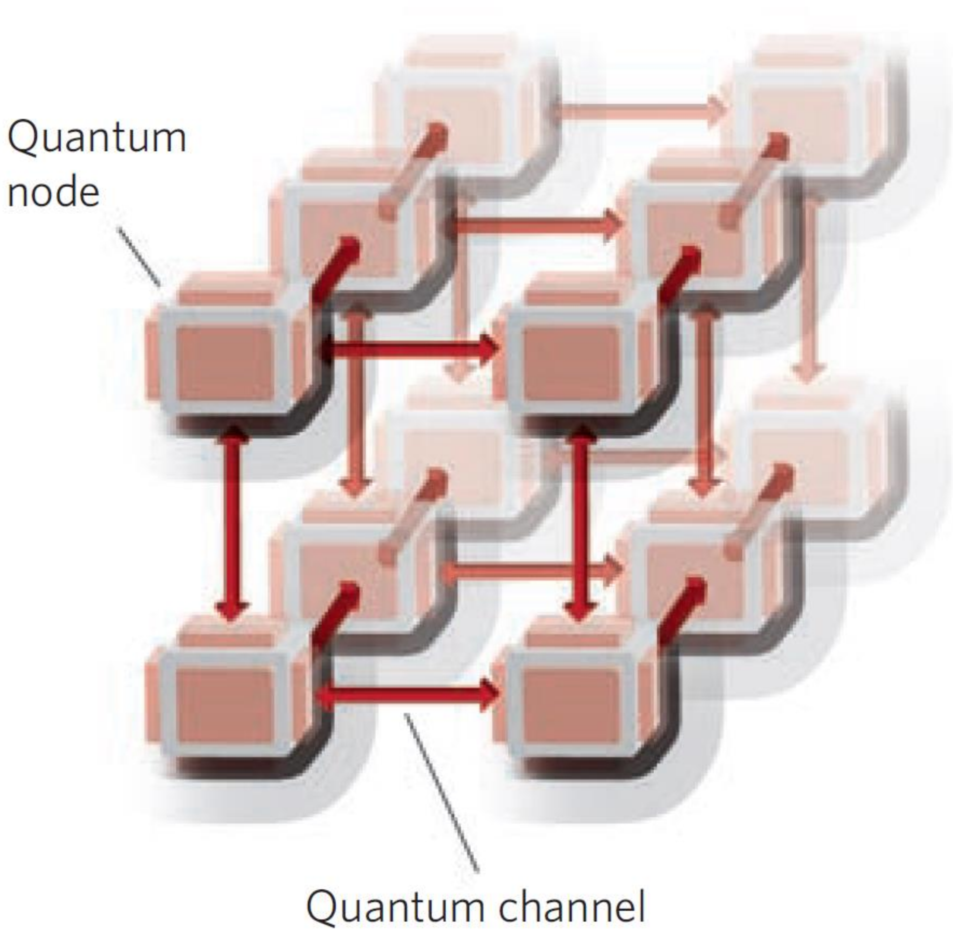
Tutorial on Quantum Repeaters
Rodney Van Meter & Tracy Northup

@IRTF, 2019/3/25

Outline

- What’s a quantum network? (tl;dr version)
- Applications: Why quantum networks?
- Basic terminology & concepts
- Basic mathematical notation
- Basics of entanglement
- Teleportation
- Implementation
- Repeaters: rationale, concepts & generations
- Final thoughts: learning more & getting involved

Quantum networks: the vision



- Quantum nodes at which information is stored and processed.
  - » atoms
- Quantum channels for information transport.
  - » photons

H. J. Kimble, *Nature* 453, 1023 (2008)

Two kinds of quantum networks

<u>Unentangled Networks</u>

Good only for quantum key distribution (QKD), which aids ***longevity of secrecy*** … encrypted informa… classical networ… Very limited distan… satellite possible!).

Weak in multi-hop settings, better for point-to-point.

Easier (still not easy) to build.

<u>Entangled Networks</u>

Good for many purposes:

- crypto functions including QKD
- …ecision sensor networks
- …g quantum computers
- …um Internet.

…stance using *quantum* …).

Strong in networked settings.

Hard to build.

Actually a series of steps from here to there (Wehner, Elkouss, Hanson)

Entanglement （量子もつれ）

Even if they
are far apart!

“Measure” this one and find its value…

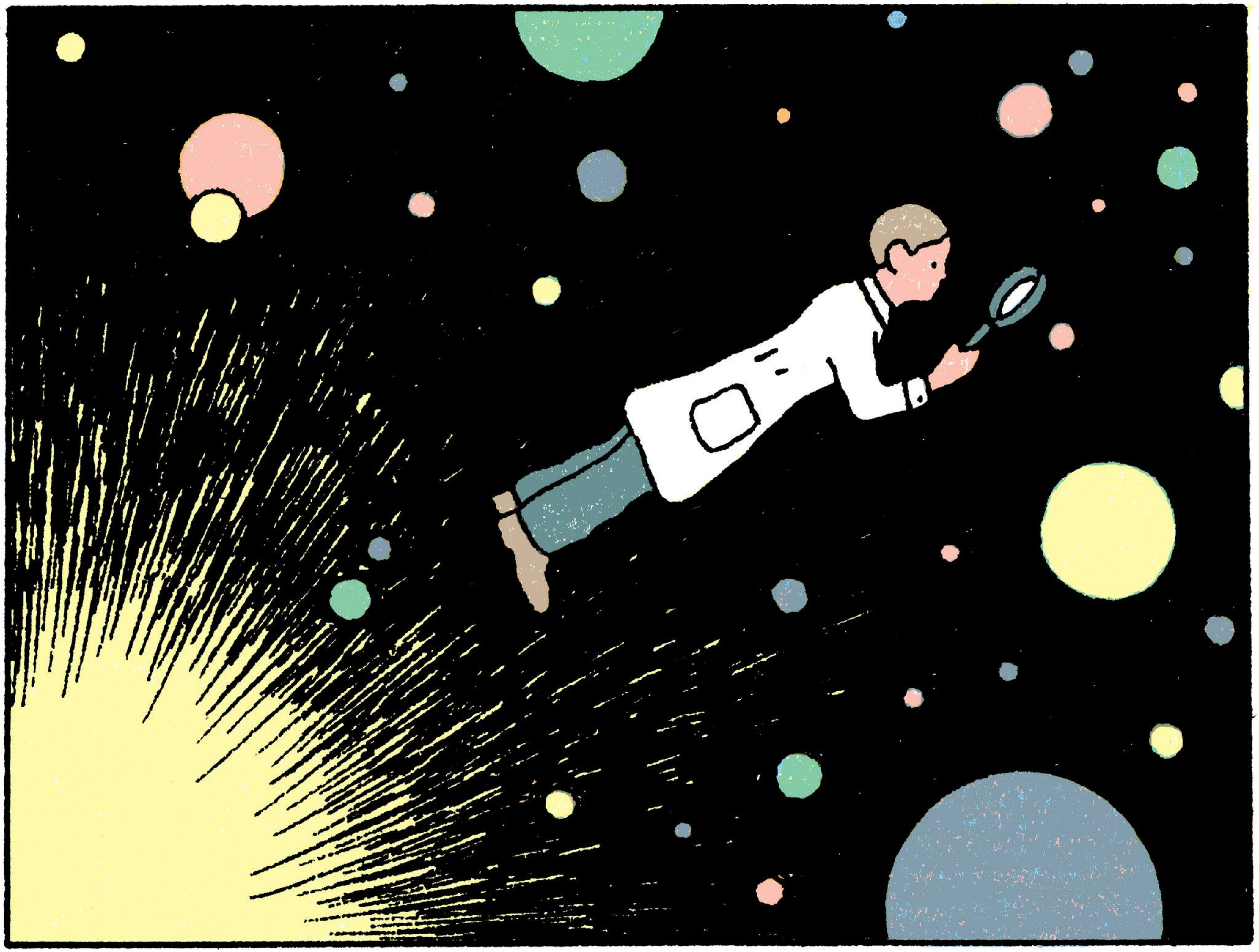
and you’ll also know what this one is

The New York Times

SundayReview

Is Quantum Entanglement Real?

NOV. 14, 2014



Physics Vol. 1, No. 3, pp. 195–200, 1964 Physics Publishing Co. Printed in the United States

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†
Department of Physics, University of Wisconsin, Madison, Wisconsin

(*Received* 4 *November* 1964)

I. Introduction

THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no "hidden variable" interpretation of quantum mechanics is possible. These attempts have been examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly non-local structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

The job of a quantum repeater network is…

- …to make end-to-end entanglement (modulo some arguments about temporal matters).
- And, **entanglement is a consumable resource**, so we have to make lots of it.

So the job of a quantum repeater is…

- 1) to make base-level entanglement over a physical link
- 2) to couple entangled links along an end-to-end path to meet the applications' needs
- 3) to monitor and manage errors
(purification, QEC, or both)
- 4) to participate in the management of the network

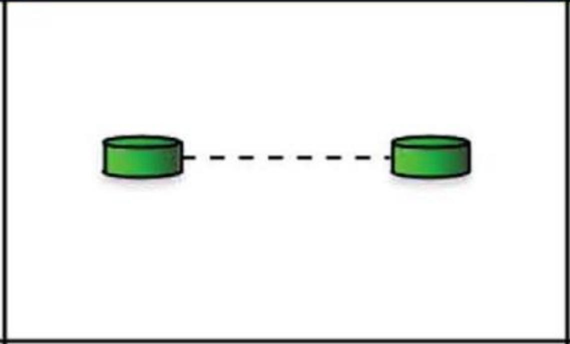
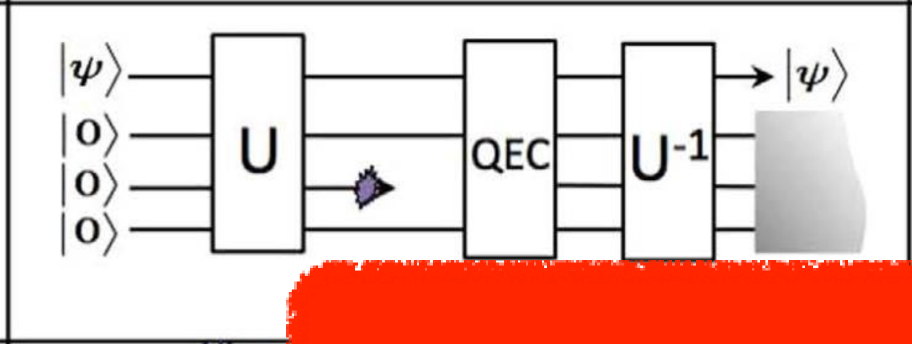
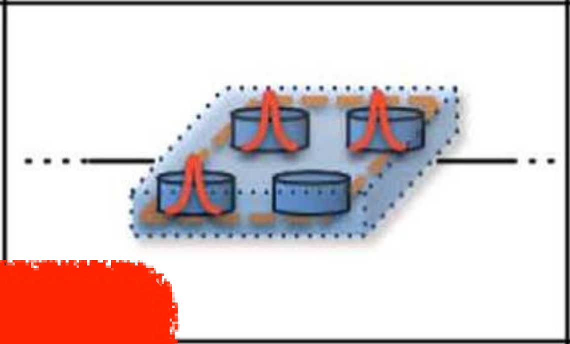
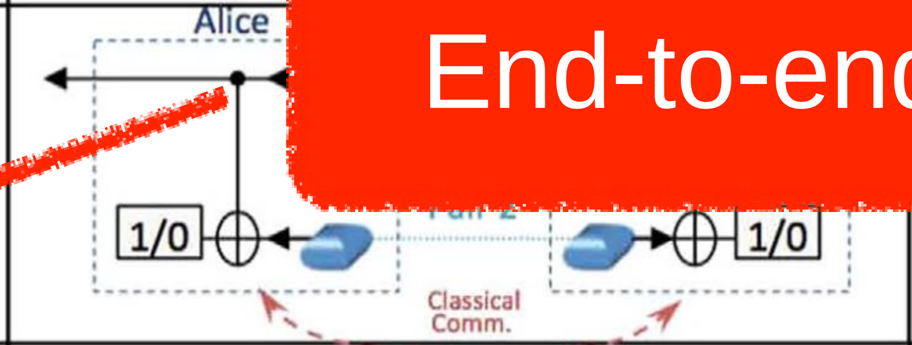
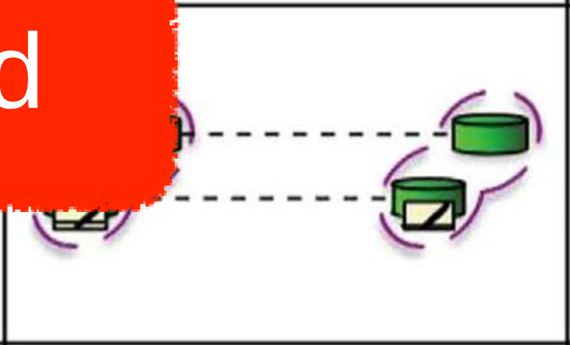
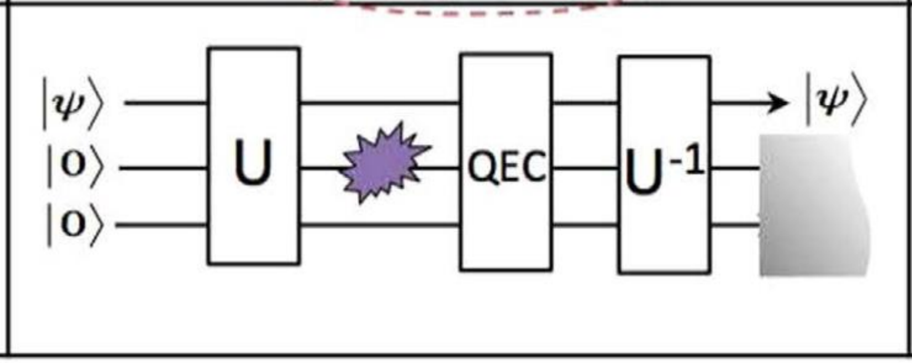
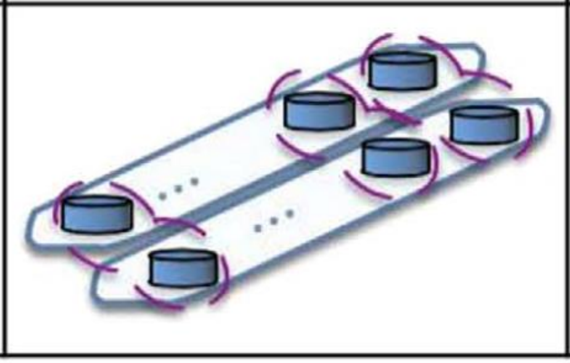
And the job of a Quantum Internet is…

To do all of this:

- across *heterogeneous* networks (both physically and logically)
- in an environment with *minimal trust* between networks
  - no knowledge of the internals of autonomous networks
  - possible presence of malicious nodes

Link level

End-to-end

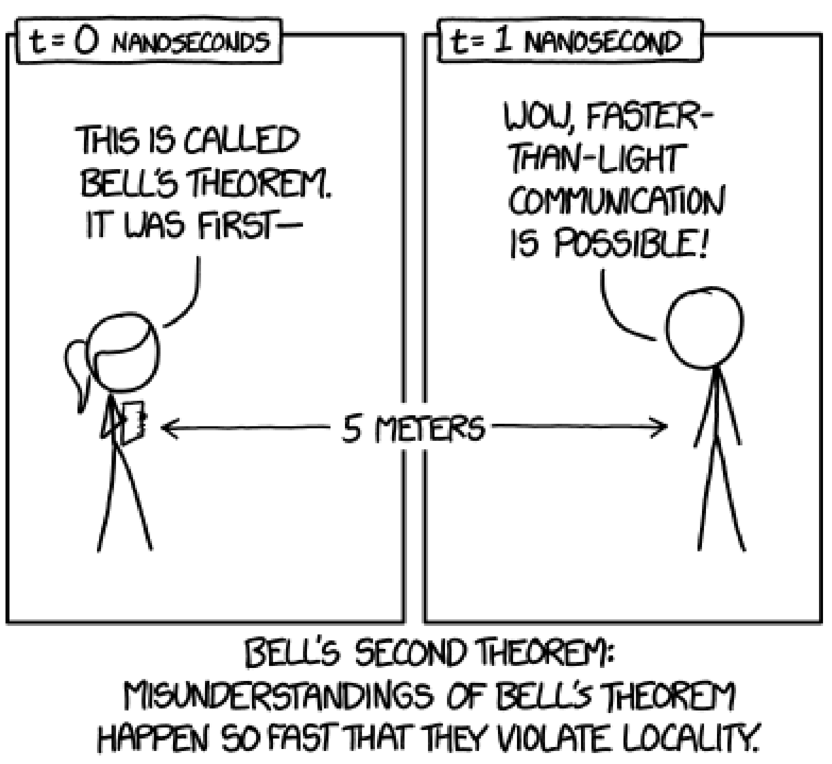
Errors	Approaches	Examples	Schematics	1G	2G	3G
Loss Error	Heralded Entanglement Generation (HEG)			✔	✔	
	Quantum Error Correction (QEC)					✔
Operation Error	Heralded Entanglement Purification (HEP)			✔		
	Quantum Error Correction (QEC)				✔	✔

Elements: Remotely entangled qubit; Flying qubit (photons); CNOT gate; Qubit in an encoded block; Measurement (X/Z); Teleportation-based Error Correction

http://www.nature.com/articles/srep20463

Good for & not good for

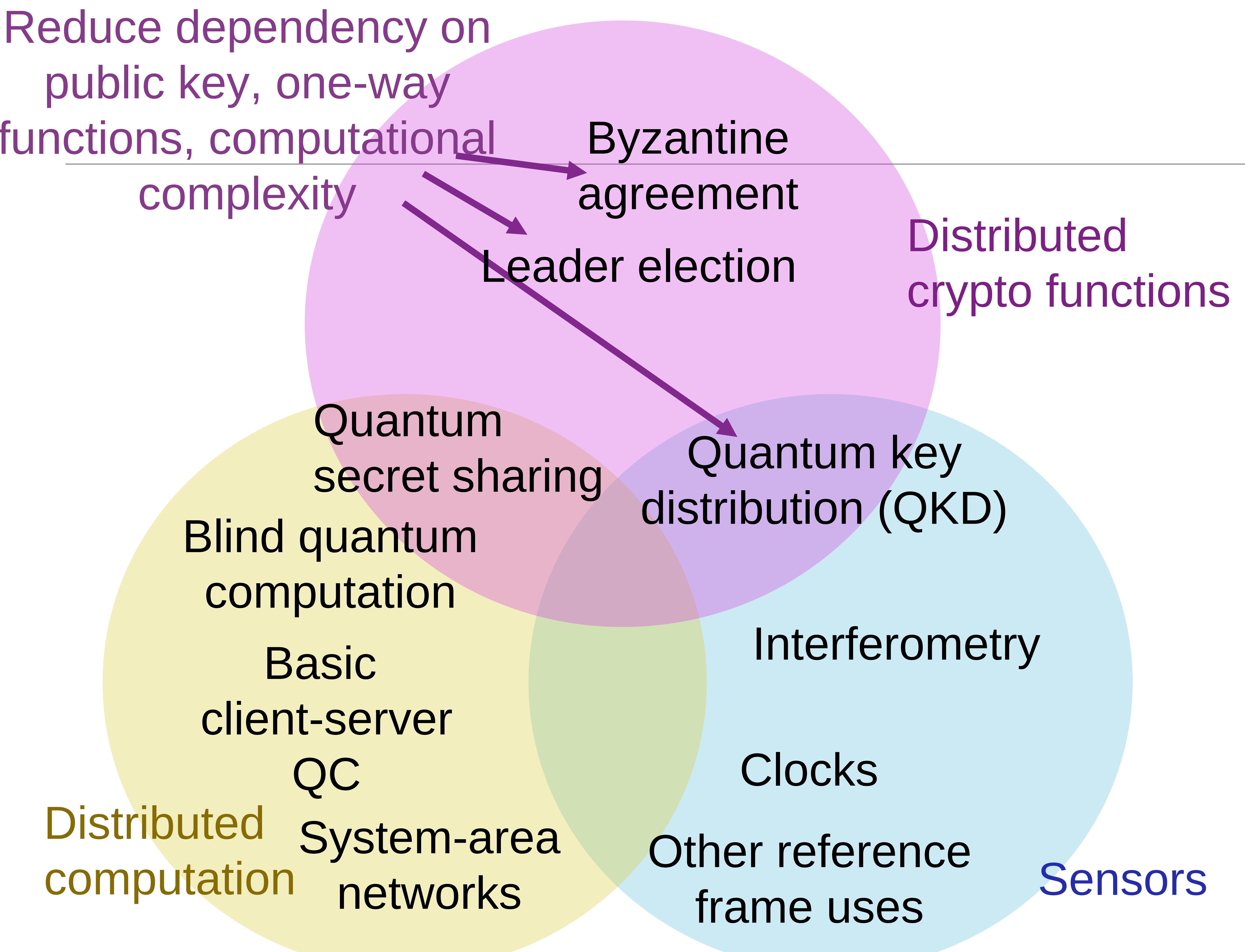
Quantum networks are about *new capabilities,* not some path to huge communication bandwidth. Reduced # of communication rounds (asymptotically, theoretically), higher precision, scalability of distributed quantum systems, etc.



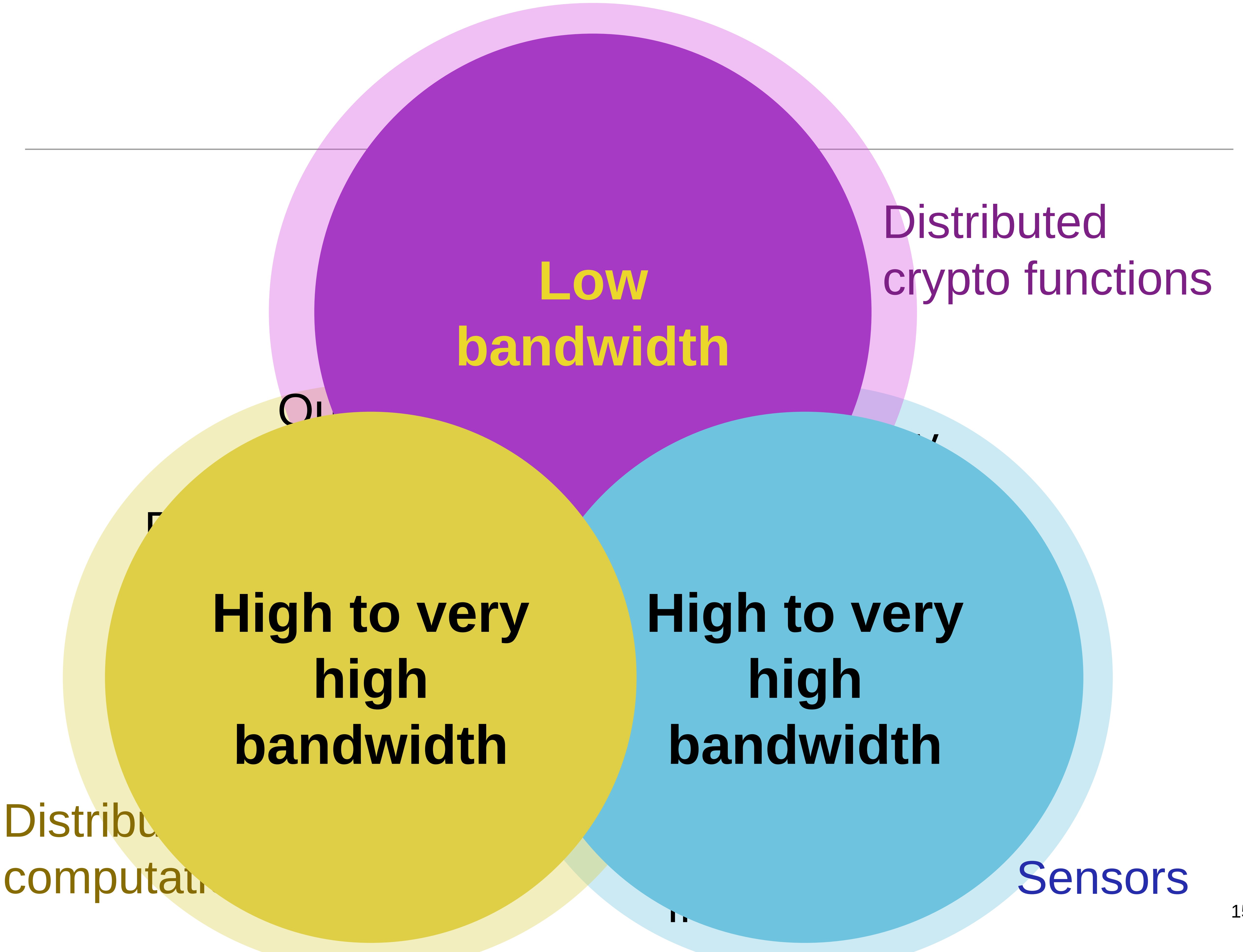
No faster-than-light communication!

You can each get shared, secret random numbers upon *measuring* shared, entangled states, but that doesn't give you the ability to send messages.

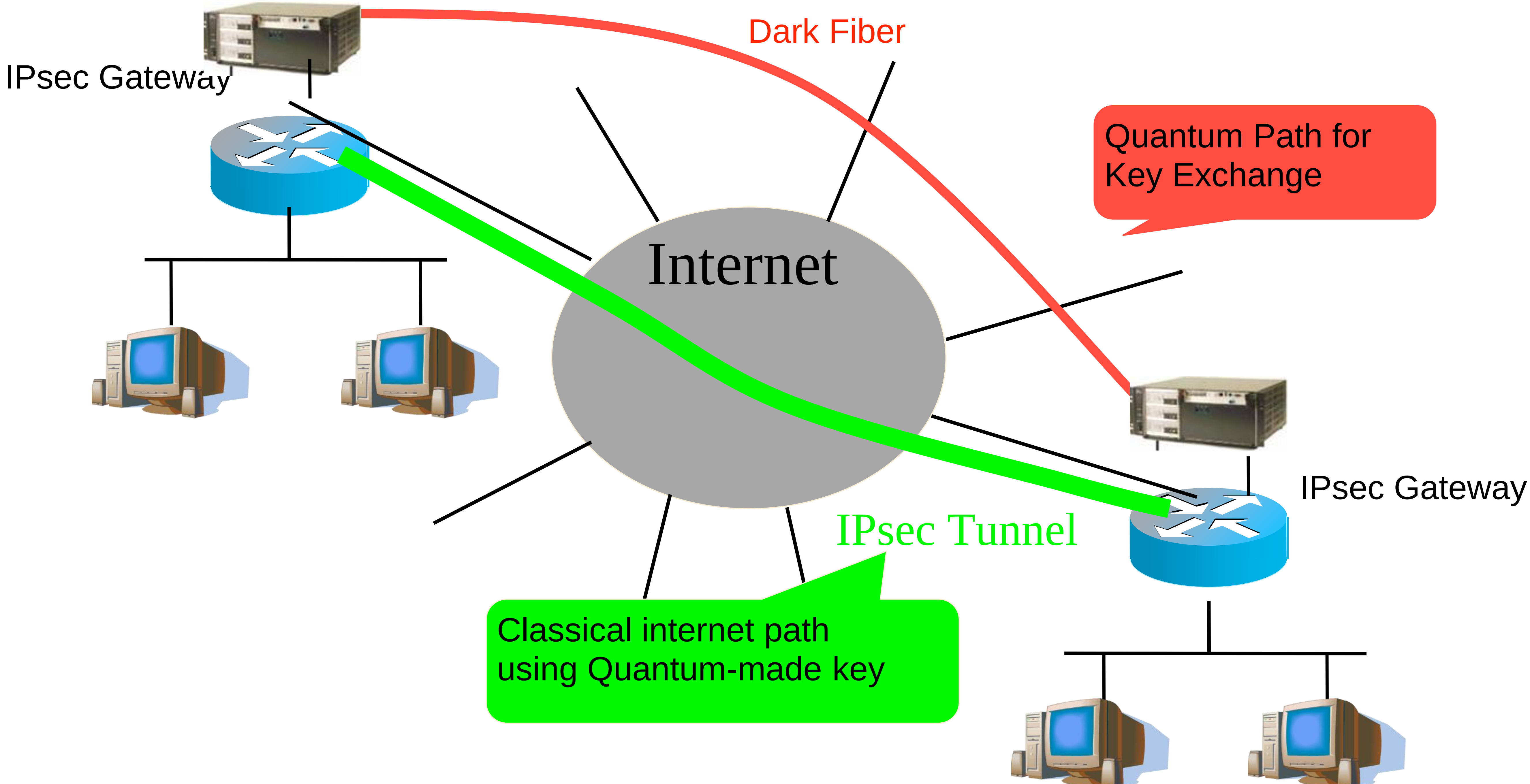
Why quantum networks?
Introduction to applications



Reduce dependency on public key, one-way functions, computational complexity
Byzantine agreement
Leader election
Distributed crypto functions
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Interferometry
Basic client-server QC
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors

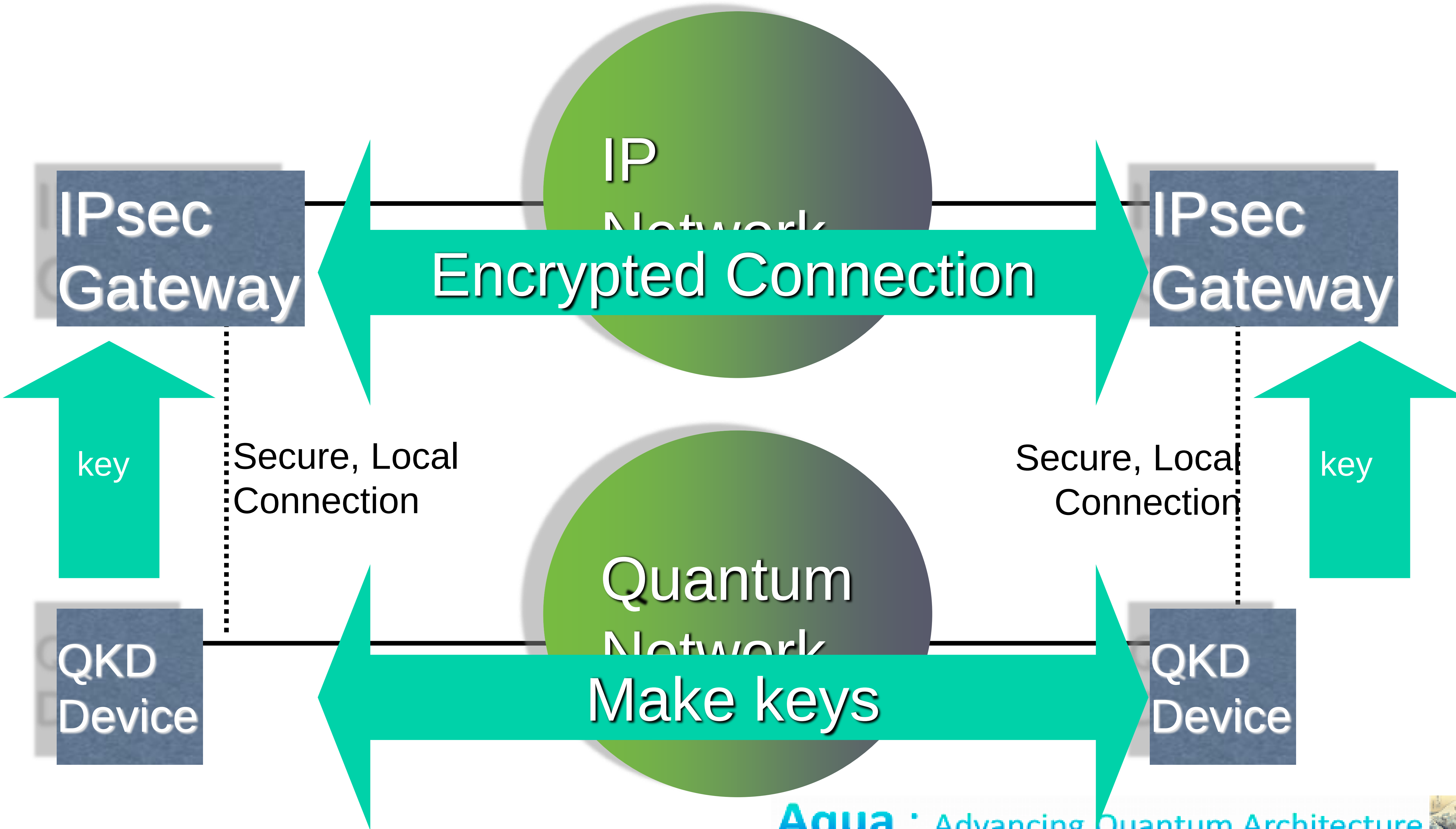

Low bandwidth
Distributed crypto functions
High to very high bandwidth
High to very high bandwidth
Sensors

IPsec with QKD: Quantum-protected campus-to-campus connection

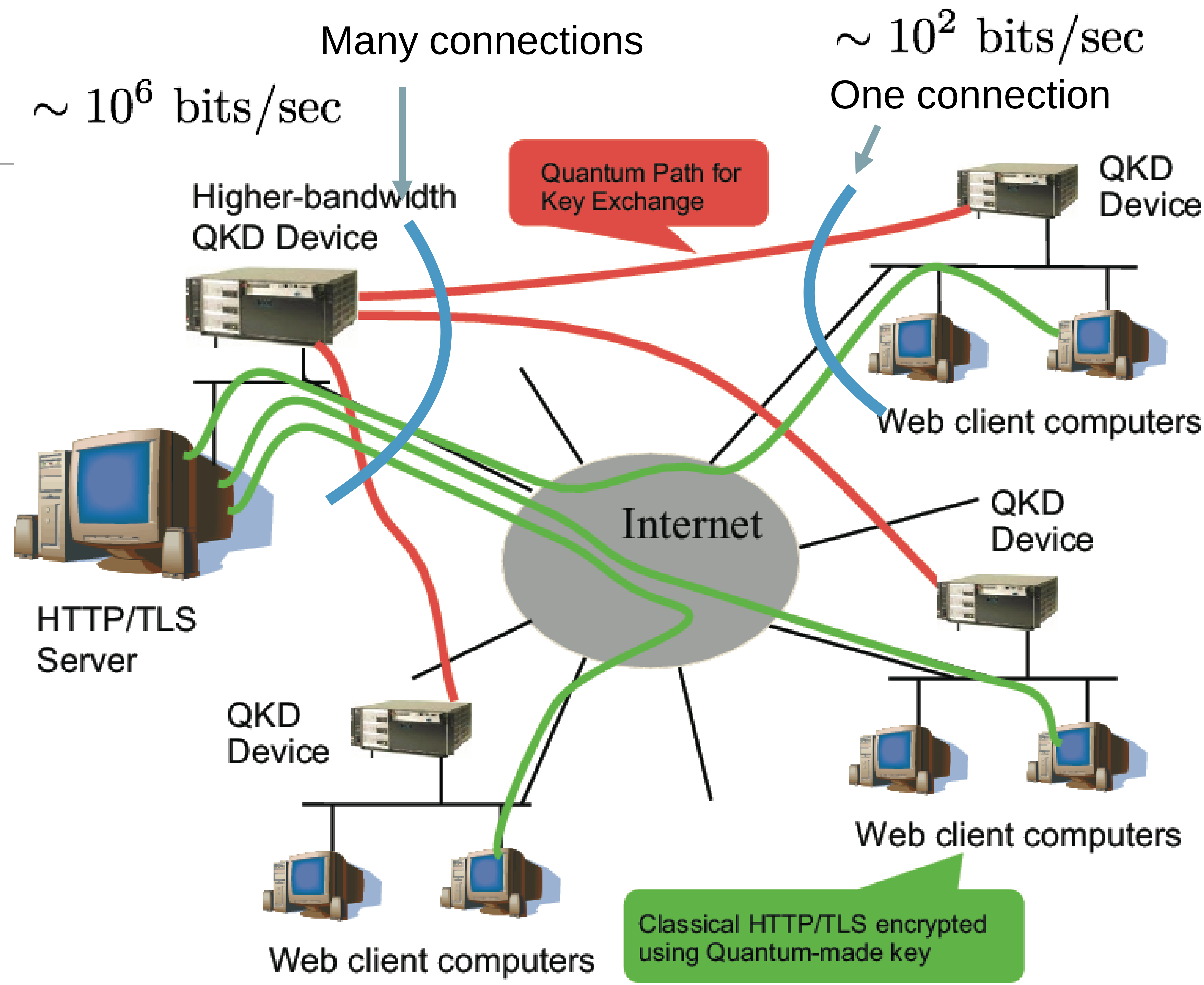


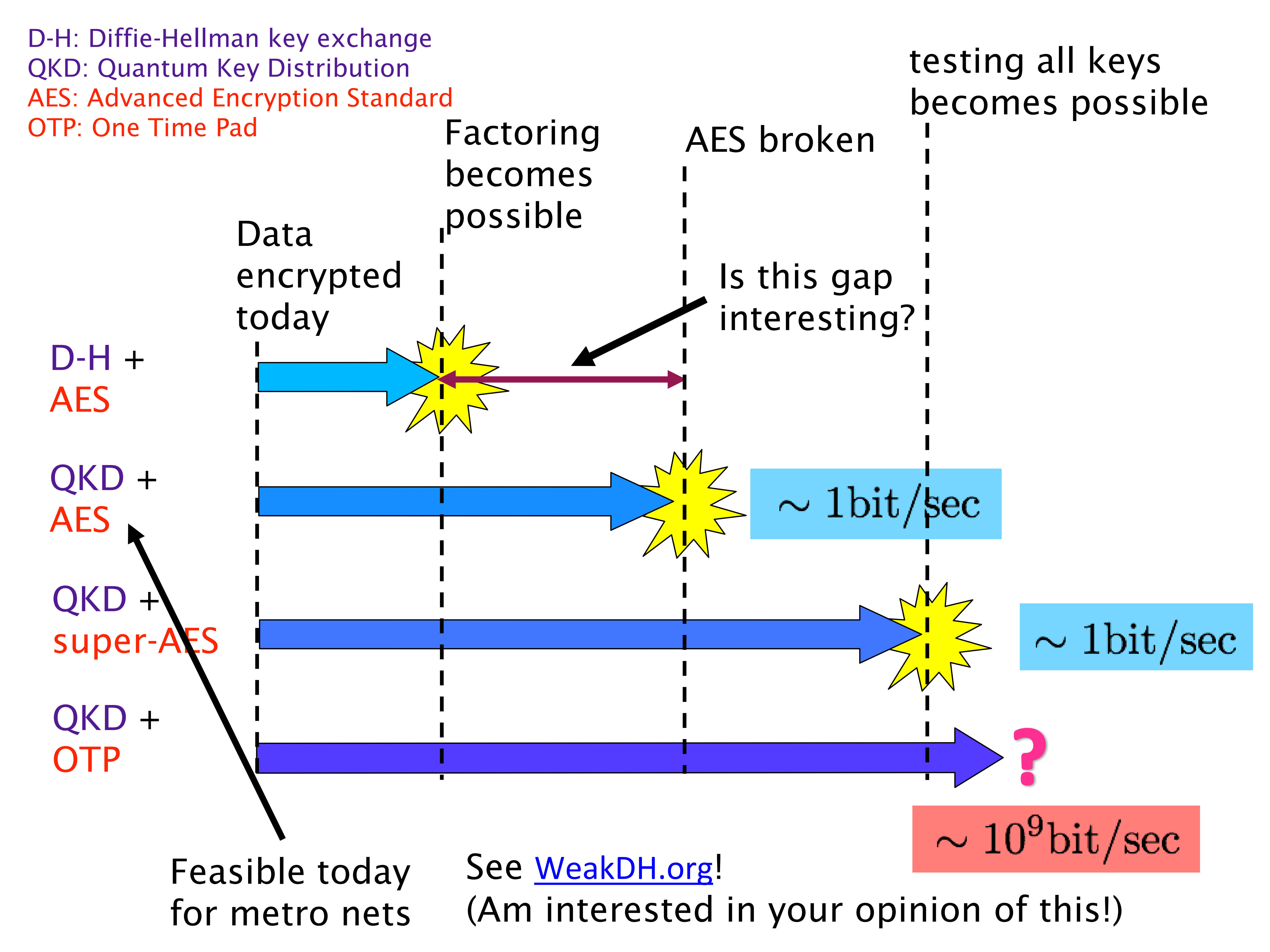
draft-nagayama-ipsecme-ike-with-qkd-01.txt, 2014/10

IPsec with QKD



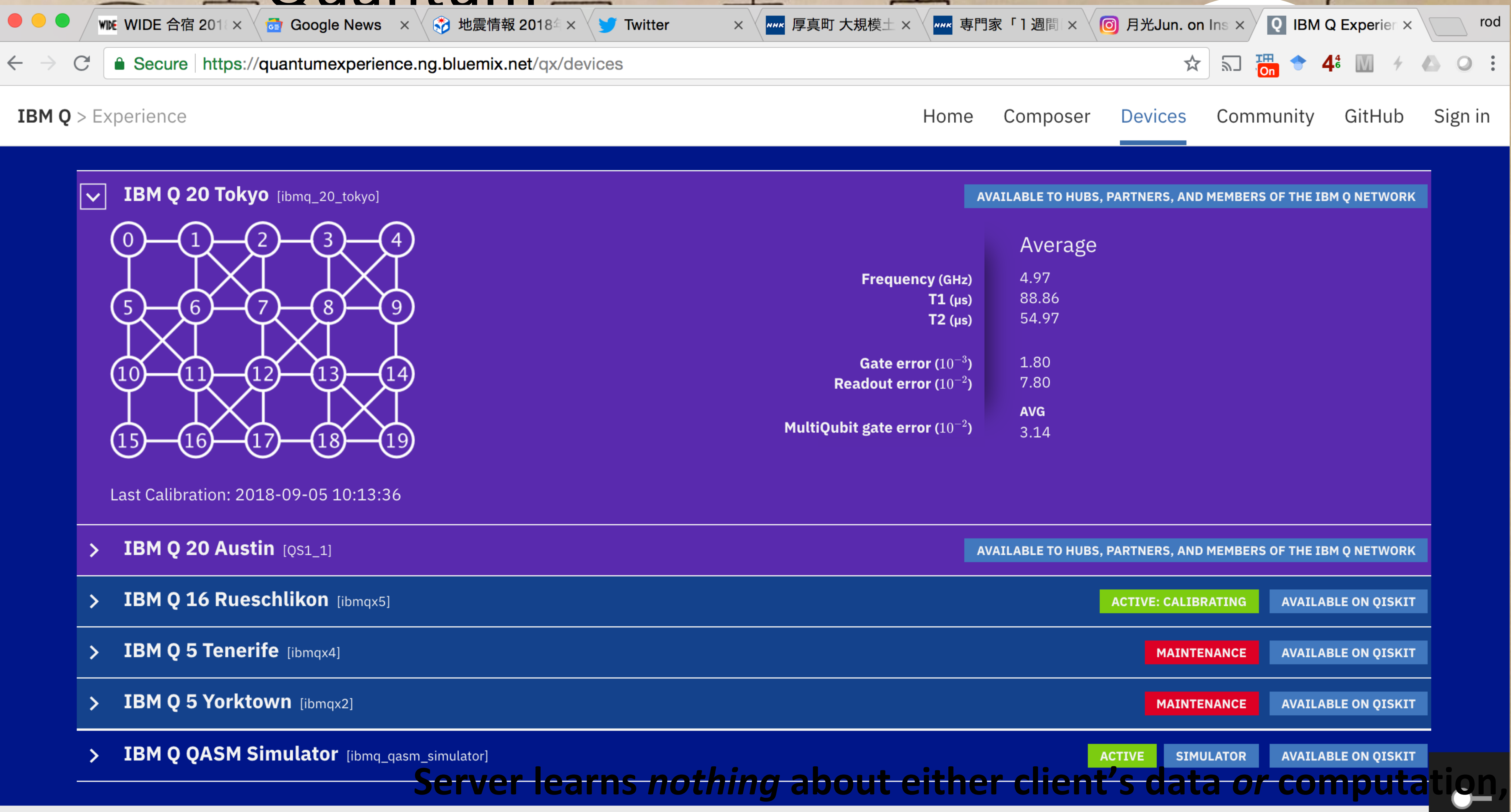
TLS with QKD:
Quantum-protected web/e-commerce

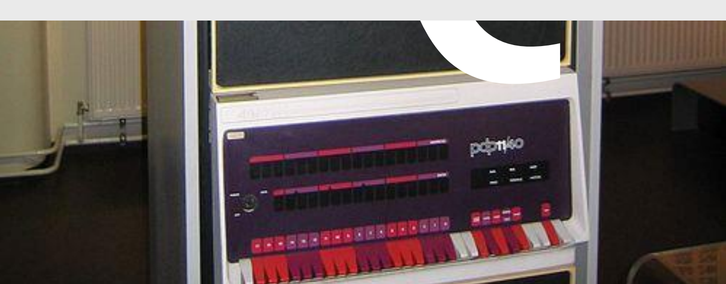



D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad
testing all keys becomes possible
Factoring becomes possible
AES broken
Data encrypted today
Is this gap interesting?
D-H + AES
QKD + AES
$\sim 1\mathrm{bit/sec}$
QKD + super-AES
$\sim 1\mathrm{bit/sec}$
QKD + OTP
?
$\sim 10^9\mathrm{bit/sec}$
Feasible today for metro nets
See WeakDH.org!
(Am interested in your opinion of this!)

Blind Computation: Secure Quantum

ARPA NETWORK, LOGICAL MAP, MAY 1973





Server learns *nothing* about either client's data *or* computation, except upper bound on computation size. (cf. classical homomorphic encryption) (Broadbent et al.)

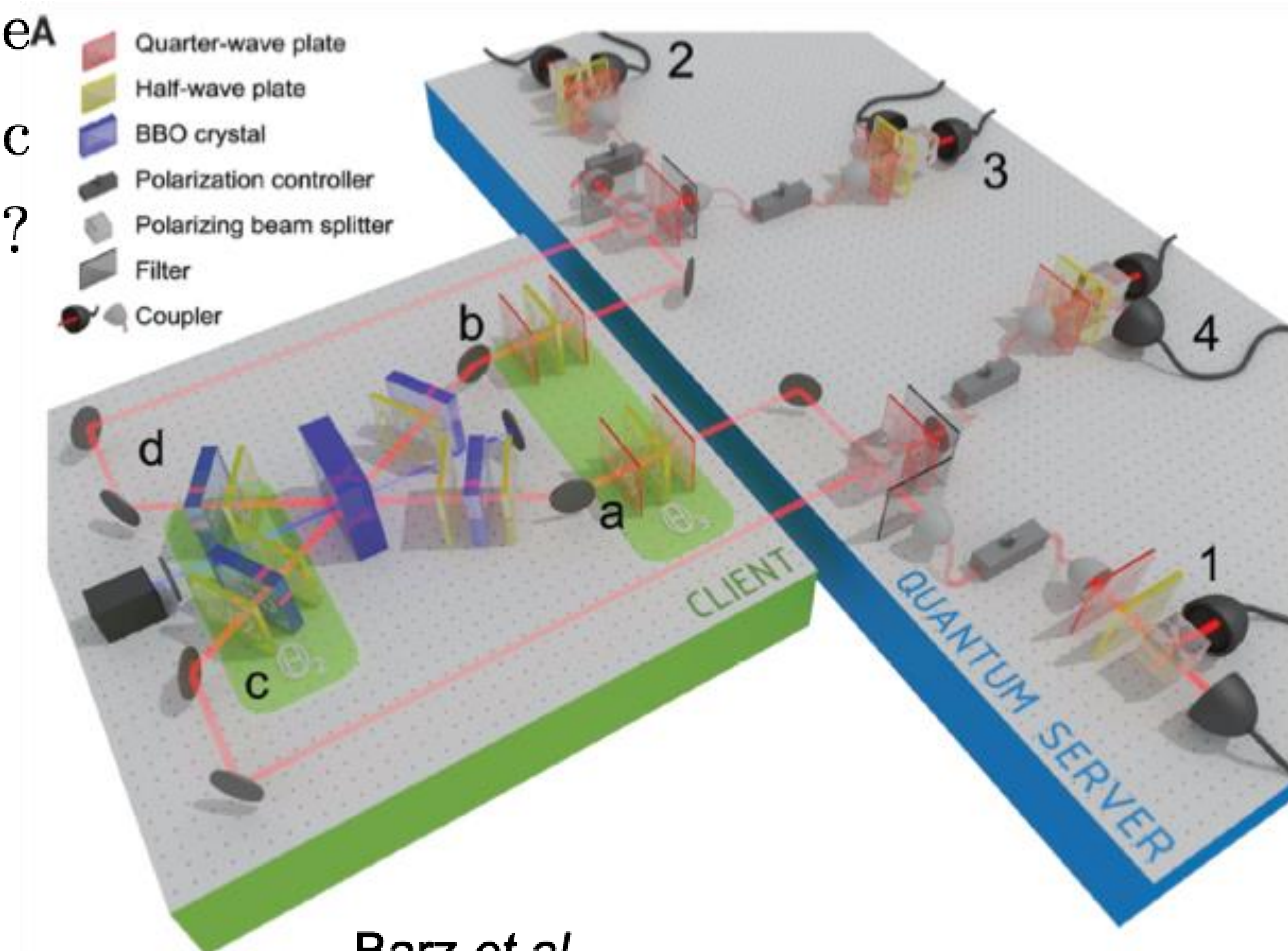
Distributed QC: blind computing

Maybe

$\sim 10^{10}$ Bell pairs/sec

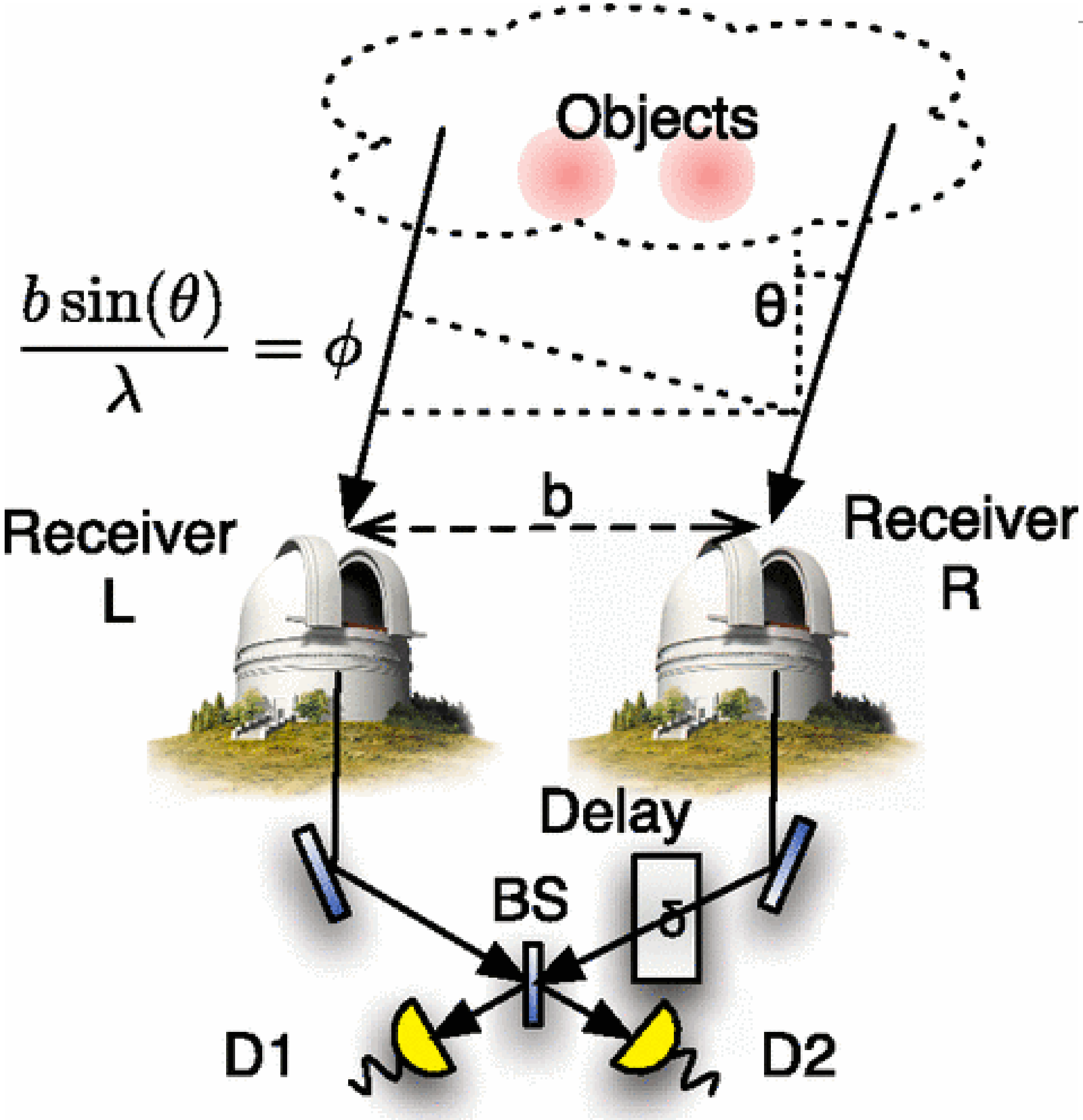
for FT Shor?

- A platform for secure distributed quantum computation, not an “application” per se.
- Assumes MBQC as programming model.



Barz *et al.*, *Science* 335 (2012)

Sensors: Interferometry



$$\frac{b\sin(\theta)}{\lambda} = \phi$$

$$\sim 10^{11}\ \text{Bell pairs/sec}$$

DOI: http://dx.doi.org/10.1103/PhysRevLett.109.070503

Oh, yeah, and communication complexity

arXiv.org > quant-ph > arXiv:quant-ph/0101005

Quantum Physics

Quantum Communication Complexity (A Survey)

Gilles Brassard

(Submitted on 1 Jan 2001)

Exponential Separation of Quantum and Classical Communication Complexity

Ran Raz
ranraz@wisdom.weizmann.ac.il,
Department of Applied Mathematics,
Weizmann Institute,
Rehovot 76100, ISRAEL

Exponential separation for one-way quantum communication complexity, with applications to cryptography

Dmitry Gavinsky*
IQC, University of Waterloo

Julia Kempe†
School of Computer Science
Tel Aviv University

Iordanis Kerenidis†
CNRS & LRI
Univ. de Paris-Sud, Orsay

Ran Raz‡
Faculty of Mathematics
Weizmann Institute

Ronald de Wolf§
CWI
Amsterdam

arXiv.org > quant-ph > arXiv:1605.07372

Quantum Physics

Exponential Communication Complexity Advantage from Quantum Superposition of the Direction of Communication

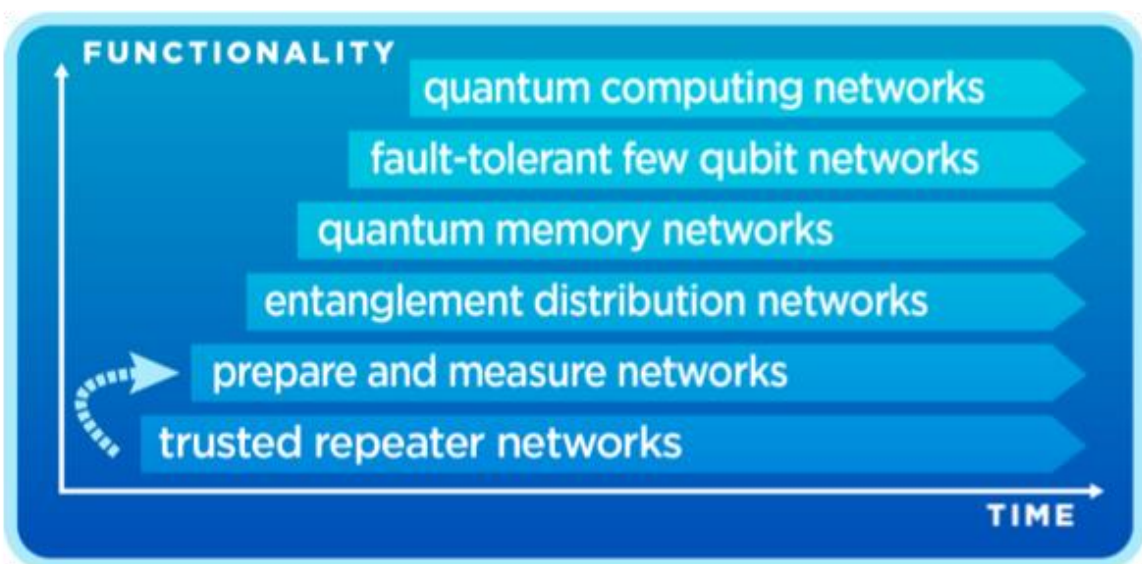
Philippe Allard Guérin, Adrien Feix, Mateus Araújo, Časlav Brukner

(Submitted on 24 May 2016 (v1), last revised 9 Sep 2016 (this version, v2))

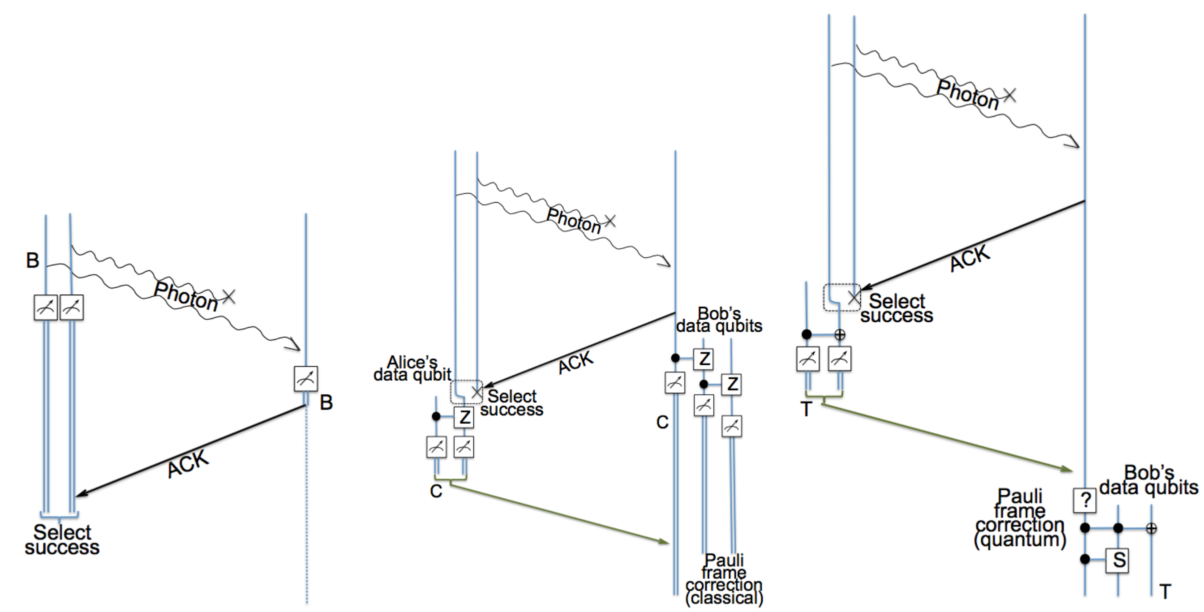
For some abstract tasks, theoretically can be exponentially fewer rounds of communication. I don’t know much about this, but see Raz STOC 1999; arXiv:quant-ph/0101005; arXiv:quant-ph/0611209; arXiv:1605.07372; and a few others.

Technical demands

Some of these require only the ability to measure an inbound photon at the end nodes, others require ability to entangle your local memory at the few-qubit level. True distributed computing (e.g. blind) requires lots of high-fidelity memory.



Wehner, Elkouss, Hanson, *Science*, 2018



(a) B class (b) C class (c) T class

FIG. 2: Timing for application classes over a single forward-propagating link.

rdv et al., arXiv:1701.04586

Basic terminology & concepts

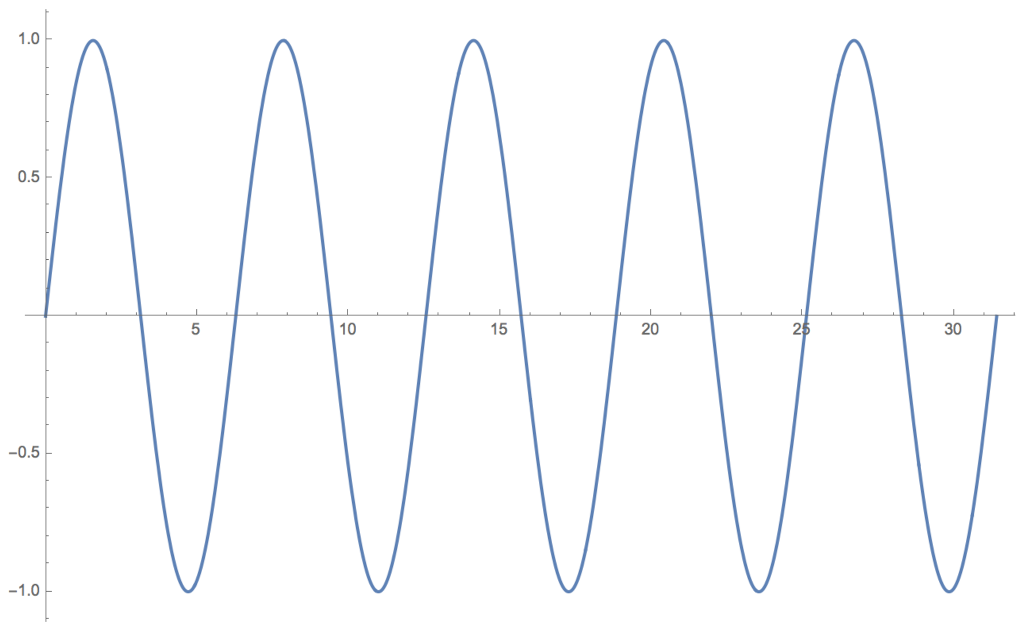
Seven Key Concepts for Quantum Computing

- **Superposition**
- **Interference**
- **Entanglement**
- **Unitary (reversible) operation**
- **Measurement**
- **No-cloning theorem**
- **Decoherence**

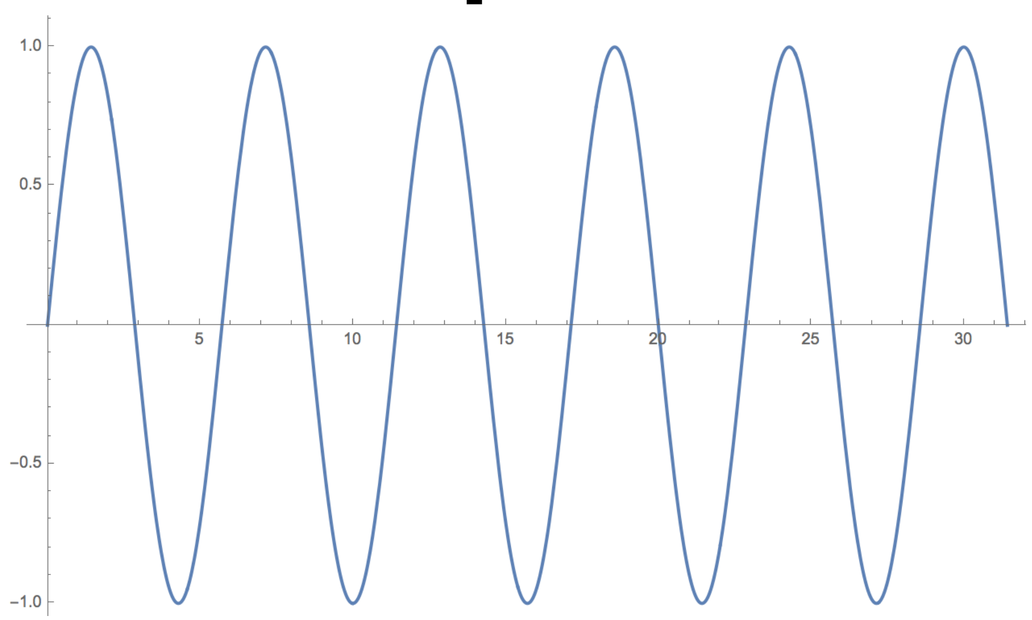
(Abbreviated) Glossary

- **Quantum amplitude**: represented by a complex number, the “amount” of the quantum wave function in a particular state
- **Pure state:** A quantum state whose preparation process did *exactly* what it was supposed to (no noise, no errors, no decay). n.b.: might be in superposition, might be entangled. Fidelity = 1.0.
- **Mixed state:** A quantum state with noise, errors, decay. Fidelity < 1.0.
- **Entangled state:** A multi-qubit quantum state whose qubits can’t be described independently, only in the context of all the qubits.
- **Bell pair:** A canonical two-qubit entangled state. There are four types, can be interconverted, and also can be used as a *basis set* for describing two-qubit states.

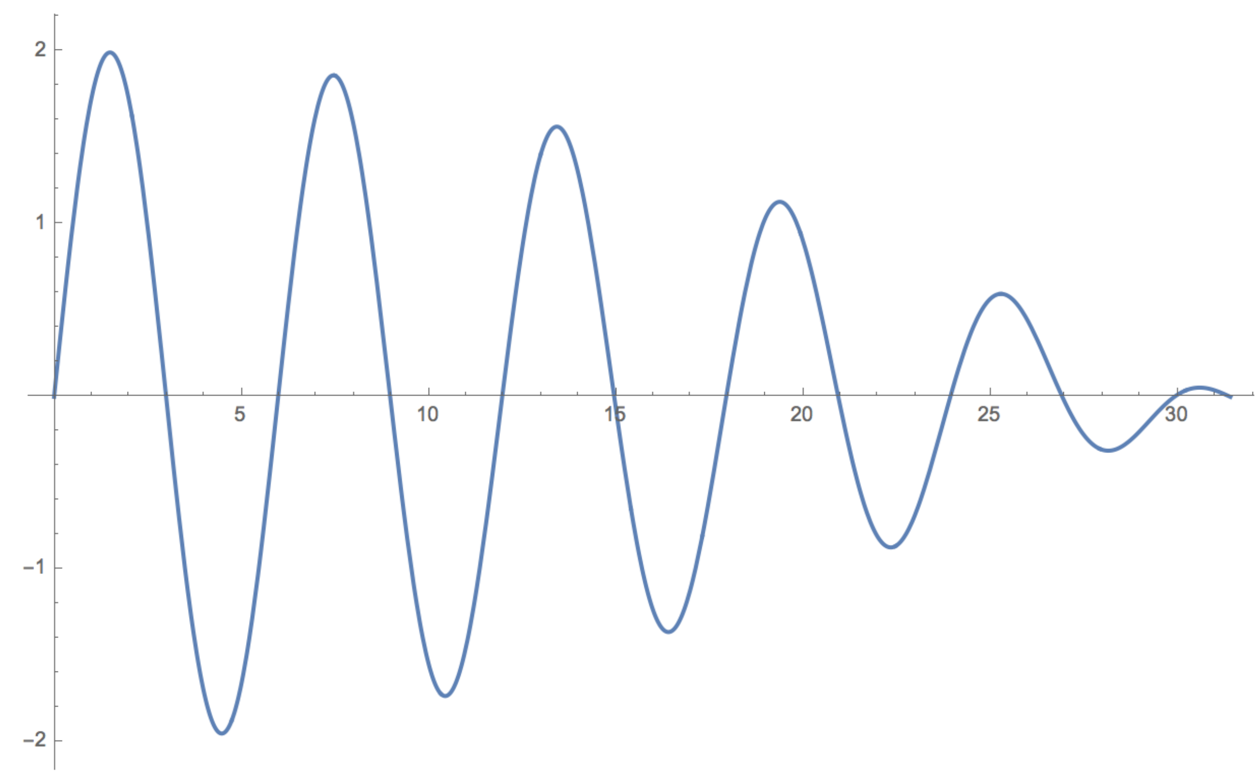
Superposition: Quanta Behaving Like Waves



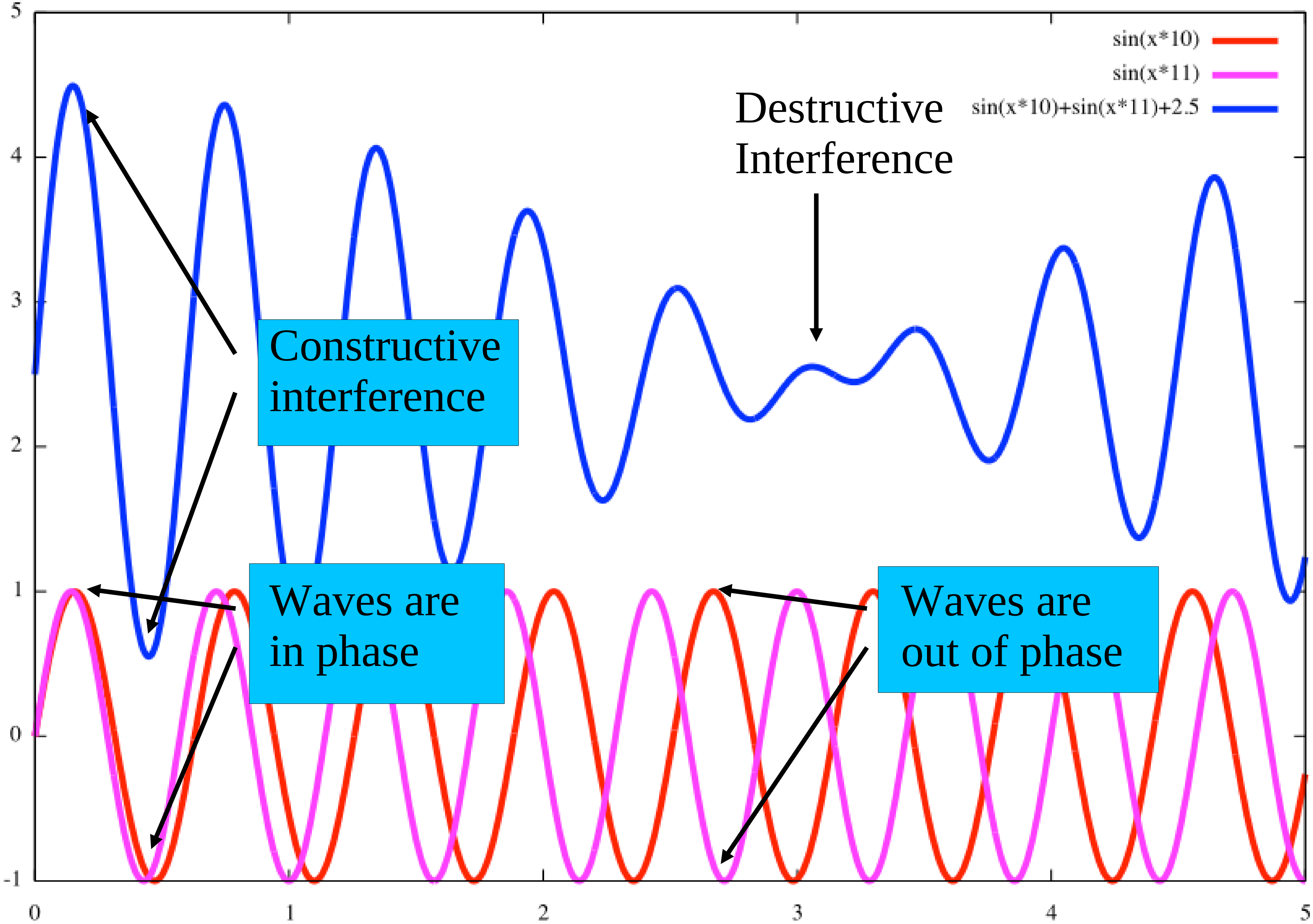
+



=



Interference ／干渉／ การทับซ้อน



Basic mathematical notation (see extensive appendix for more)

Dirac's Bra-ket Notation

ket

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = ?$$

Dirac's Bra-ket Notation

ket

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} =? \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} =?$$

Dirac's Bra-ket Notation

bra

ket

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \equiv \langle 0|$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \equiv \langle 1|$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}\langle 0| + \frac{1}{\sqrt{2}}\langle 1|$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\begin{bmatrix} \alpha & \beta \end{bmatrix} =?$$

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} =?$$

State Vector for Two & Three Qubits

$$|\psi\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \begin{matrix} \leftarrow \text{amplitude of } 00 \\ \leftarrow \text{amplitude of } 01 \\ \leftarrow \text{amplitude of } 10 \\ \leftarrow \text{amplitude of } 11 \end{matrix}$$

$$|\psi\rangle = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

There are 2^*n* elements in the state vector for *n* qubits.
Each amplitude is a complex number.

Prob. of measuring *i* is $|\alpha_i|^2$

Normalization requires $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

No-cloning theorem

- In general, independent (unentangled) copy of a quantum state cannot be made.
- This theorem is important for cryptographic communication with quantum computation.

try to copy $|\psi\rangle$ and $|\phi\rangle$ to $|s\rangle$:

U is virtual gate which copy the input first qubit to the second

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

$$(\langle s| \otimes \langle\phi|)U^{-1}U(|\psi\rangle \otimes |s\rangle) = (\langle\phi| \otimes \langle\phi|) \otimes (|\psi\rangle \otimes |\psi\rangle)$$

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

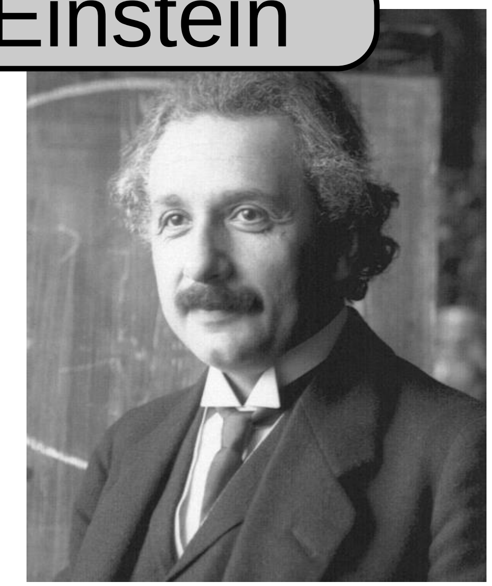
$$\langle\phi|\psi\rangle = 0, 1$$

Then, $|\psi\rangle$ is same or orthogonal.

Basics of entanglement: Bell pairs & nonlocality

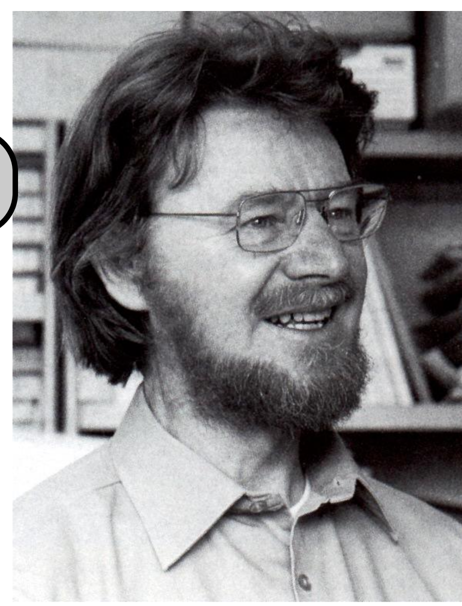
Nonlocality - the arguments

Einstein



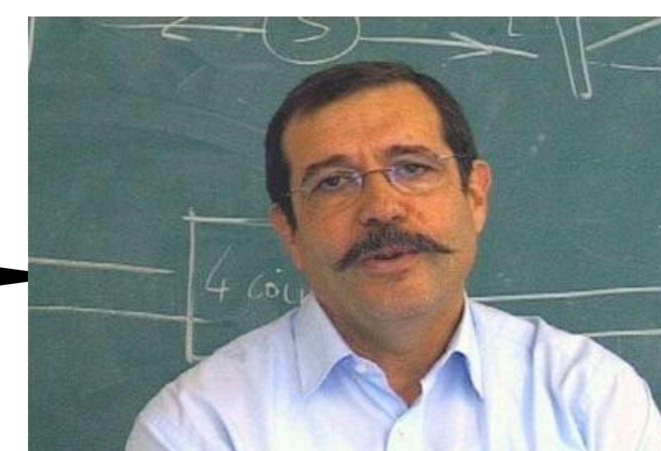
Either quantum mechanics is nonlocal, or it is incomplete (secret plans)

J.S.Bell



Even if it is incomplete, it is still nonlocal!

Aspect



No local hidden variable theory can explain my experiment.

The EPR argument

Einstein, Podolsky, and Rosen asked: is quantum mechanics complete? Before we measure a system, does it have a definite state?

> “If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.”

The EPR argument

Preconditions of the argument:

1. Locality: no immediate signaling.

2. Each measurement generates a single result.

QM is either nonlocal OR incomplete.

Bell's arguments

Bell wondered if adding in hidden variables really saves QM from being nonlocal.

Bell derived an inequality that any local hidden variable theory must satisfy.

He then showed that there are some quantum states that can violate this inequality.

So quantum mechanics cannot be described with a local hidden variables theory.

That’s all well and good in theory, but…

Experimentally, Bell inequality violations have been measured convincingly in many settings.

Since 2015: In three experiments, in ways that close all loopholes that (most) people take seriously…

Note: There are many Bell-type inequalities.
Most famous: Clauser-Horne-Shimony-Holt (CHSH).

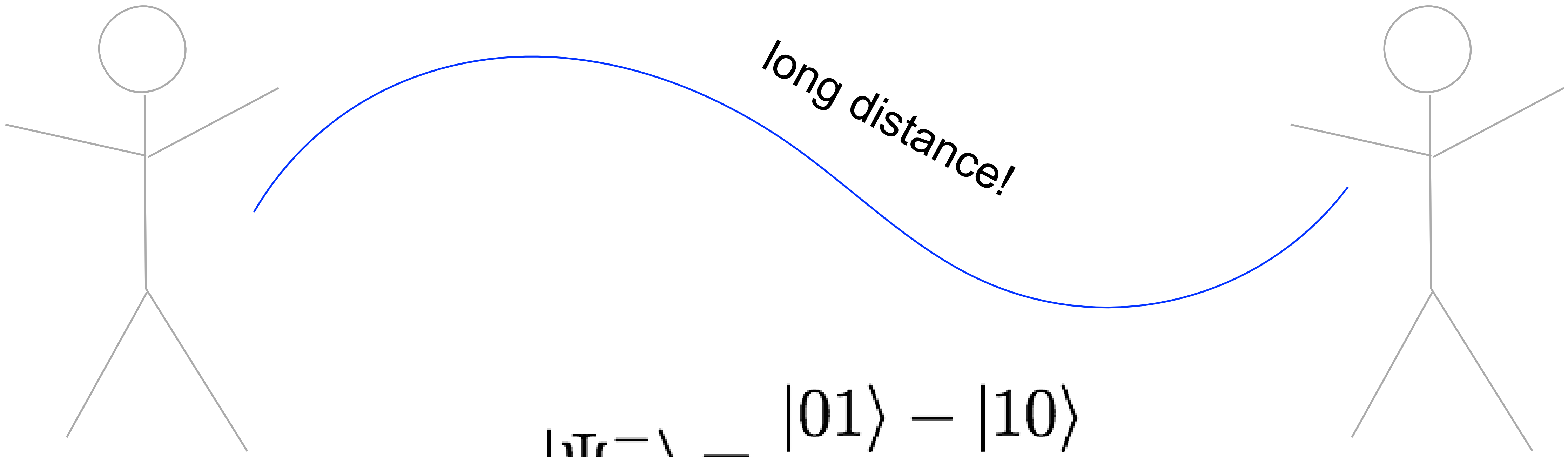
The Bell states

$$|\Phi^+\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \qquad |\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Bell states are entangled states.
That is, they can’t be written as separable states (“product states”).
(These four can also be used as a *basis set* to rewrite any two-qubit state.)

Bell states are a resource for quantum communication and computation.



$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Bell pairs can be used to generate secret keys.

If two people share a Bell pair,
one can send a quantum state to the other.

The no-signaling theorem

Can we use quantum nonlocality to send a signal faster than light?

NO - it is a mathematical consequence of quantum mechanics that even if it is nonlocal, quantum systems cannot signal each other.

Consequences for quantum computing

INFORMATION CANNOT TRAVEL FASTER THAN THE SPEED OF LIGHT

(probably)

Entangled states can appear to be signaling each other, but really they cannot.

Always look for the classical communication channel...

Teleportation

Teleportation

- Yet another concept discovered by Charles Bennett & co.

- Moves a quantum *state* from one location to the qubit.

PHYSICAL REVIEW LETTERS

VOLUME 70 29 MARCH 1993 NUMBER 13

Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2],[3] Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]

[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*

[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*

[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]

[4] *Department of Physics, Technion–Israel Institute of Technology, 32000 Haifa, Israel*

[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*

(Received 2 December 1992)

Teleportation

- Yet another concept discovered by Charles Bennett & co.

- Moves a quantum *state* from one location to another, not the physical carrier of the qubit.

Alice

Bob

So, how do we do this?

The Bell Basis

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} : X_A X_B, Z_A Z_B$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} : -X_A X_B, Z_A Z_B$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} : XX, -ZZ$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} : -XX, -ZZ$$

Stabilizers
(won’t be discussed in this tutorial; unlikely to come up, but if they do, ask us later)

Our Data Qubit

Single-qubit state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha^2| + |\beta^2| = 1$$

Measure 0 w/ prob. $|\alpha|^2$

One-qubit operations

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

What happens to our state after applying those ops:

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

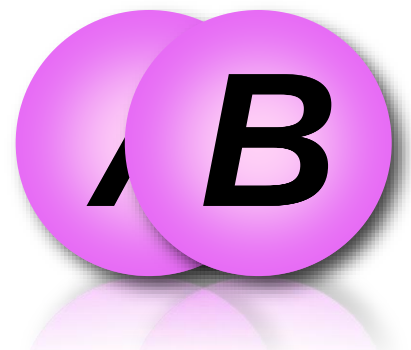
$$X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$$

$$ZX|\psi\rangle = \beta|0\rangle - \alpha|1\rangle$$

Teleportation Operations

Bell pair creation

Bell State Measurement

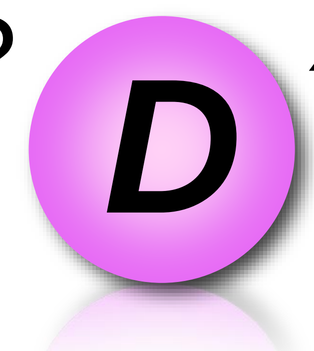


0 **1**

$$|\Phi^+\rangle = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

Z?

X?



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Alice

Bob

Implementation

How can I make my own Bell pair?

Need: two-level quantum systems in which to encode information.

Wish list:

- easy to entangle with each other
- easy to measure (in different bases)
- both of those processes: fast & accurate
- minimal information loss (through interaction with the environment)
- transportable
- identical

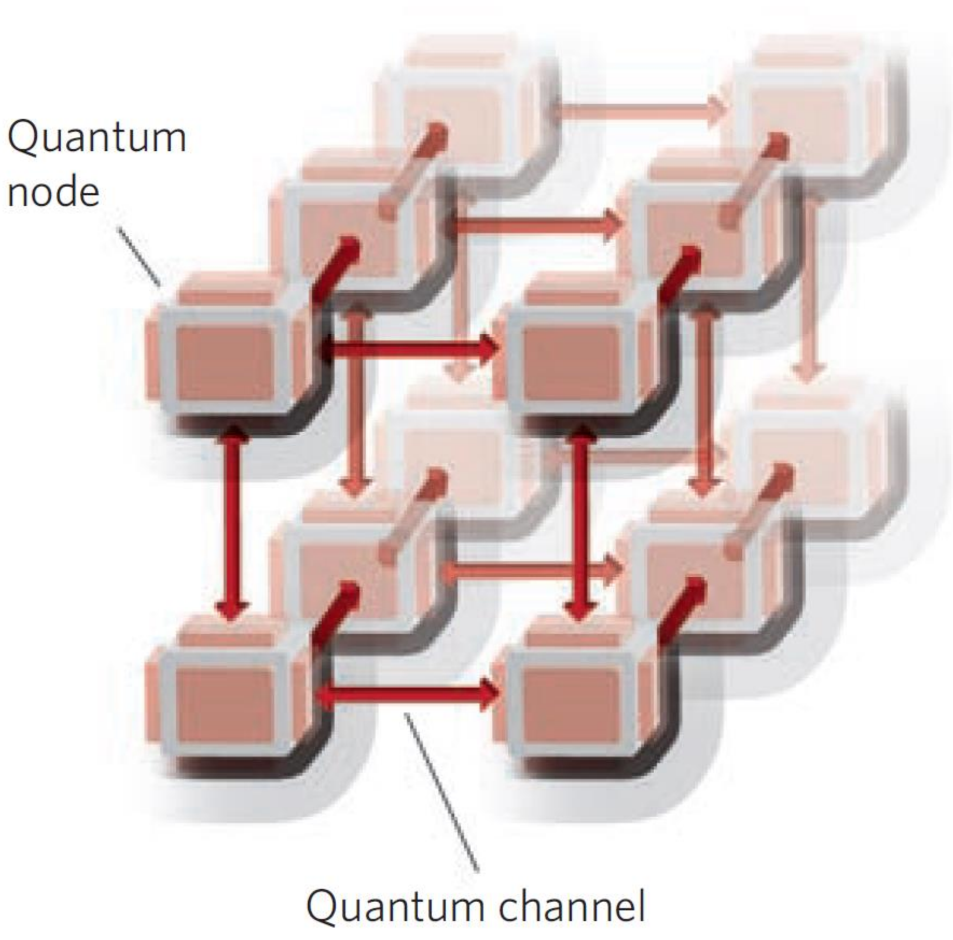
Spoiler alert: there's no perfect TLS.

…so the best choice depends on the application.

Some favorites:

- photons
  - we have: lasers, optical fibers, wave plates & detectors…
  - how do you get just one? what if you want it to stay in one place?
- atoms
  - controlled interactions with lasers & microwaves; storage & processing
  - require sophisticated laboratories; not going anywhere
- artificial atoms
  - properties can be tailored; scalable fabrication
  - are they really identical? are there only two levels?
  - also not going anywhere…

Quantum networks: the vision



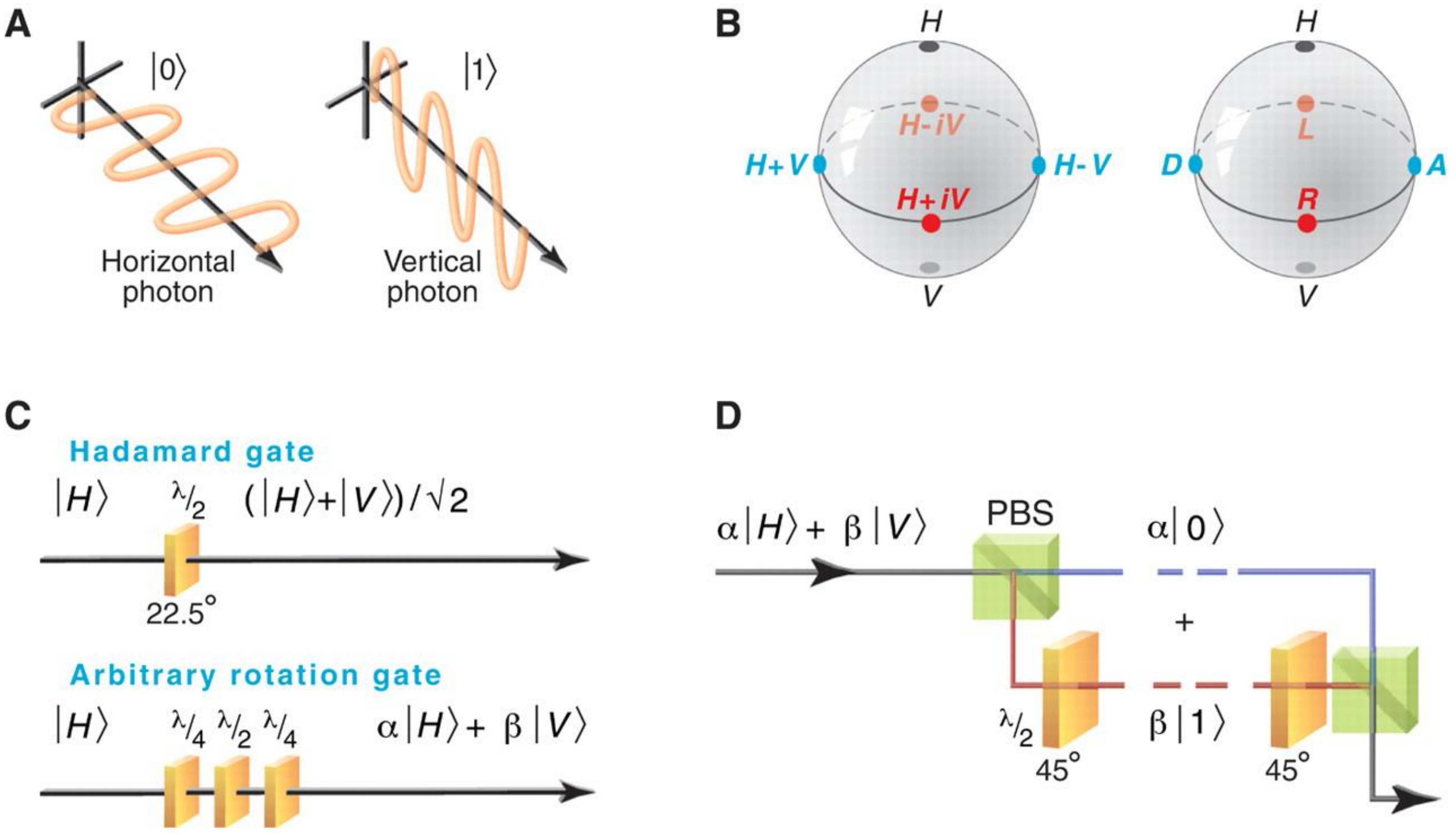
- Quantum nodes at which information is stored and processed.
  - » atoms
- Quantum channels for information transport.
  - » photons

H. J. Kimble, *Nature* 453, 1023 (2008)

Photons

encode 0 and 1 in…

- polarization
- time bin
- number
- path

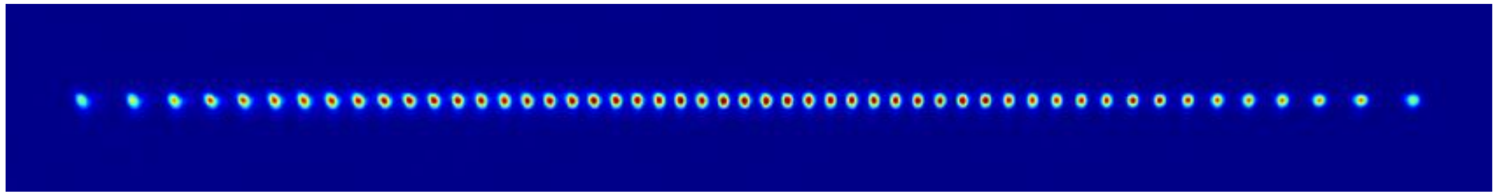


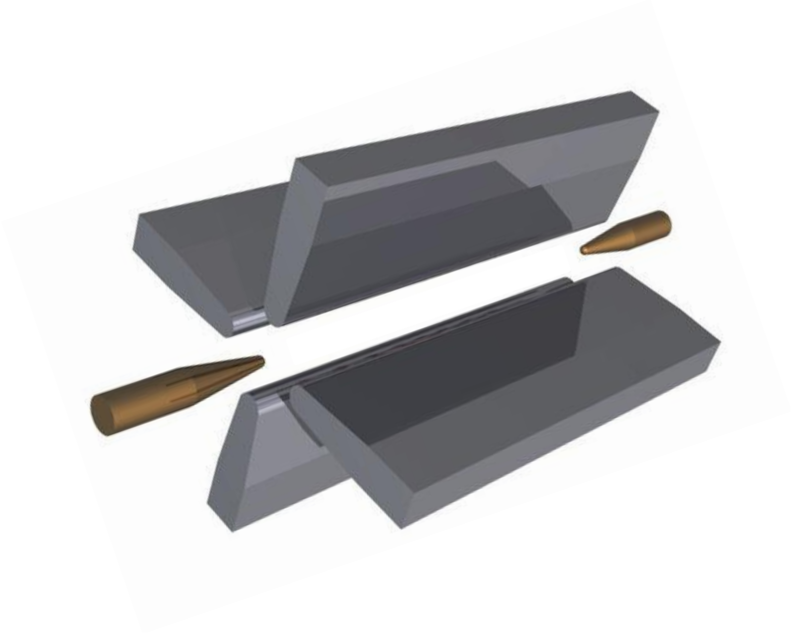
J. L. O'Brien, Science 318, 1567 (2007)

Atoms

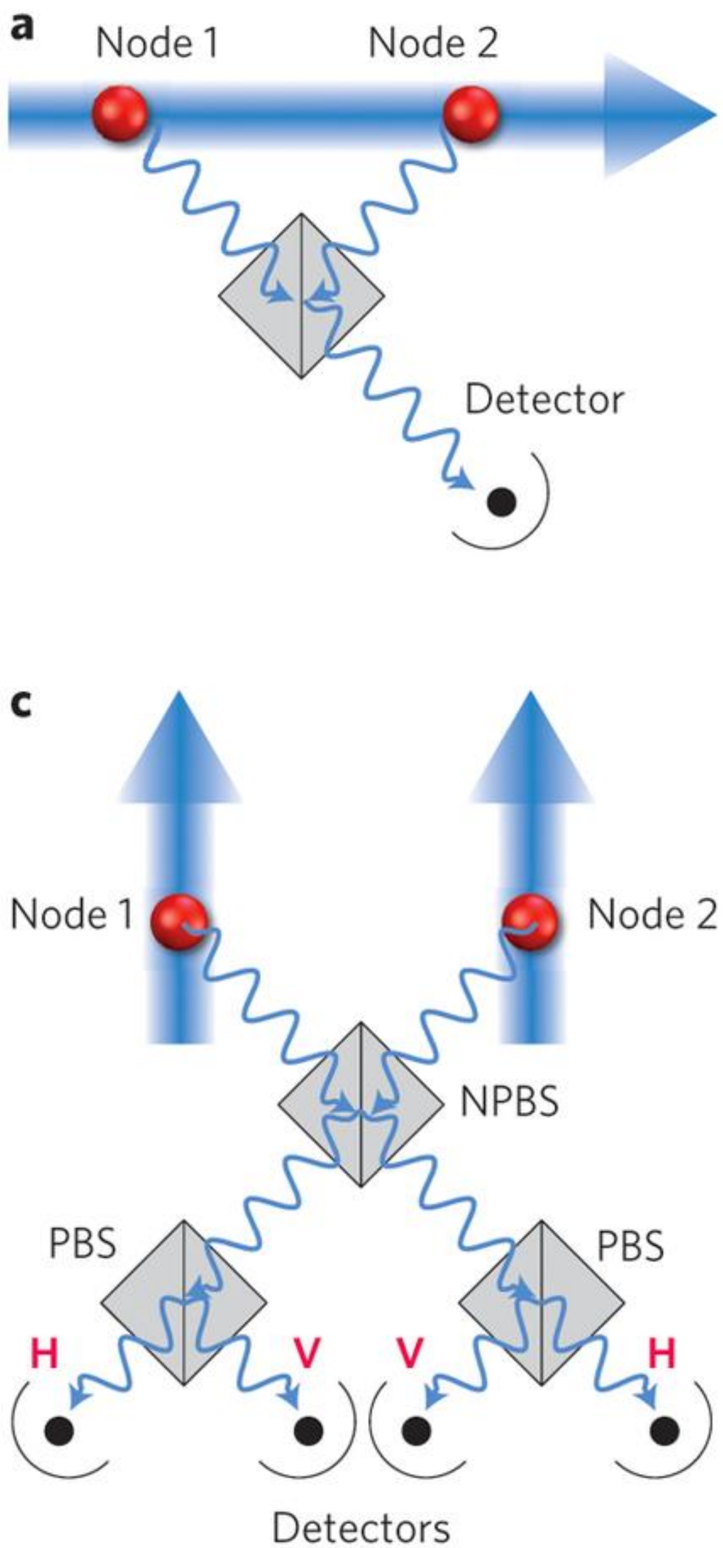
identify two electronic states!

- how long do they live?
- are they addressable with lasers? microwaves?
- are they sensitive to environmental fluctuations?





Generating remote entanglement, probabilistically



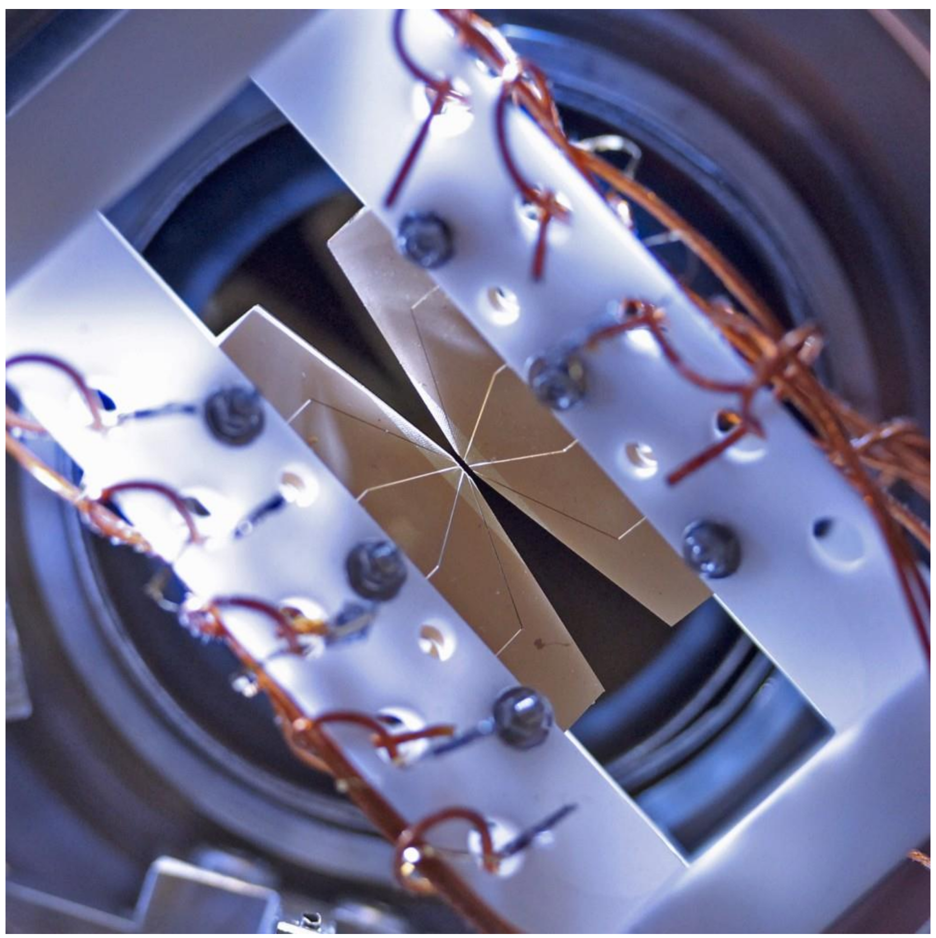
- Each atom emits a photon (or not).
- The atom's state depends on whether or not it emitted a photon (a), or the photon polarization (b).
- The detectors can't tell which atom the photon(s) came from.
- Detection projects the atoms into an entangled state.

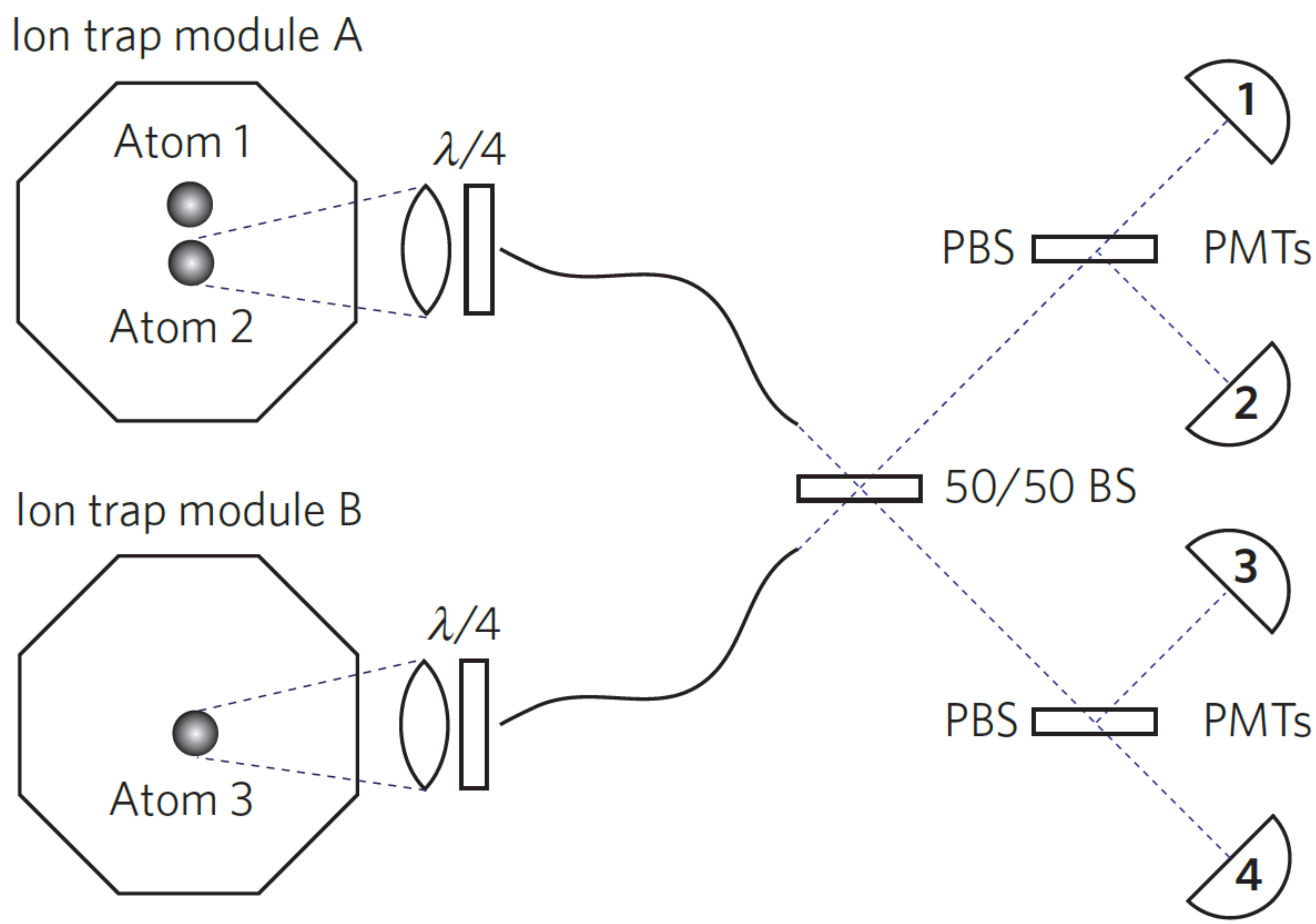
T. Northup and R. Blatt, *Nature Photon.* 8, 356 (2014)

Entangling remote $^{171}Yb^{+}$ ions

Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)
D. L. Moehring et al., *Nature* **449**, 68 (2007)
D. Hucul, *Nat. Phys.* **11**, 37 (2015)



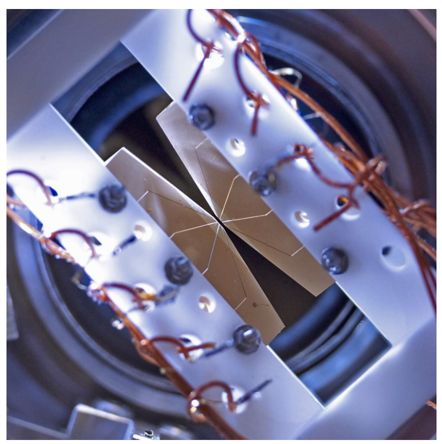


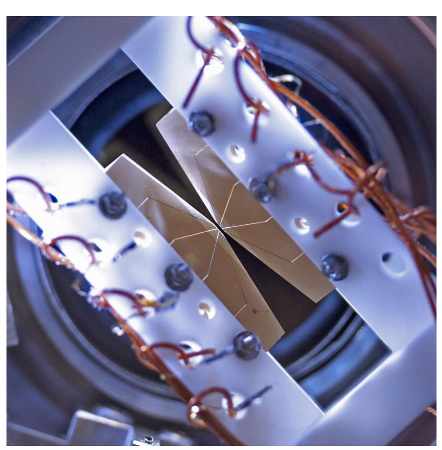
http://iontrap.umd.edu/research/ion-photon-quantum-networks/

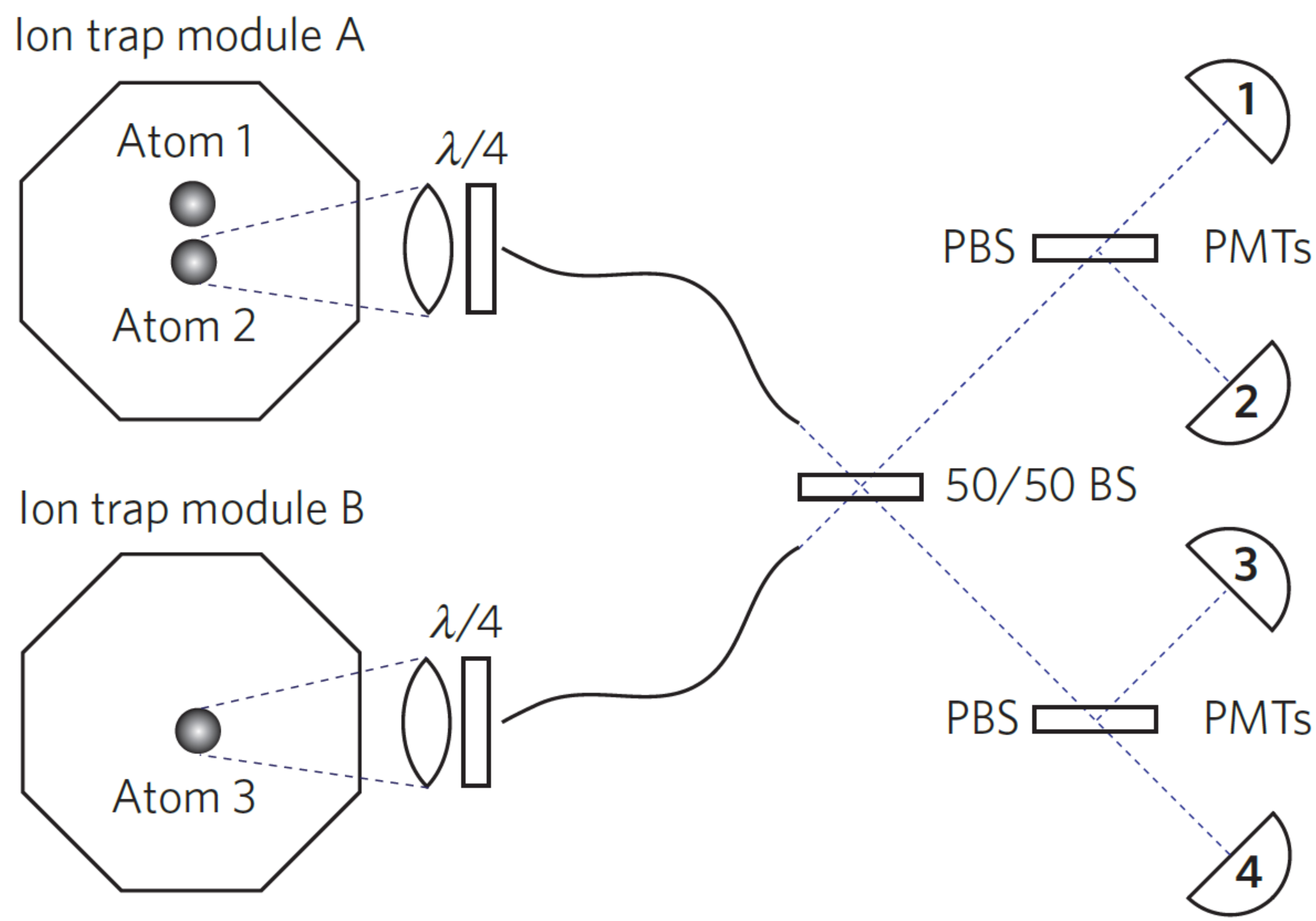
Entangling remote $^{171}Yb^{+}$ ions

Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)
D. L. Moehring et al., *Nature* **449**, 68 (2007)
D. Hucul, *Nat. Phys.* **11**, 37 (2015)







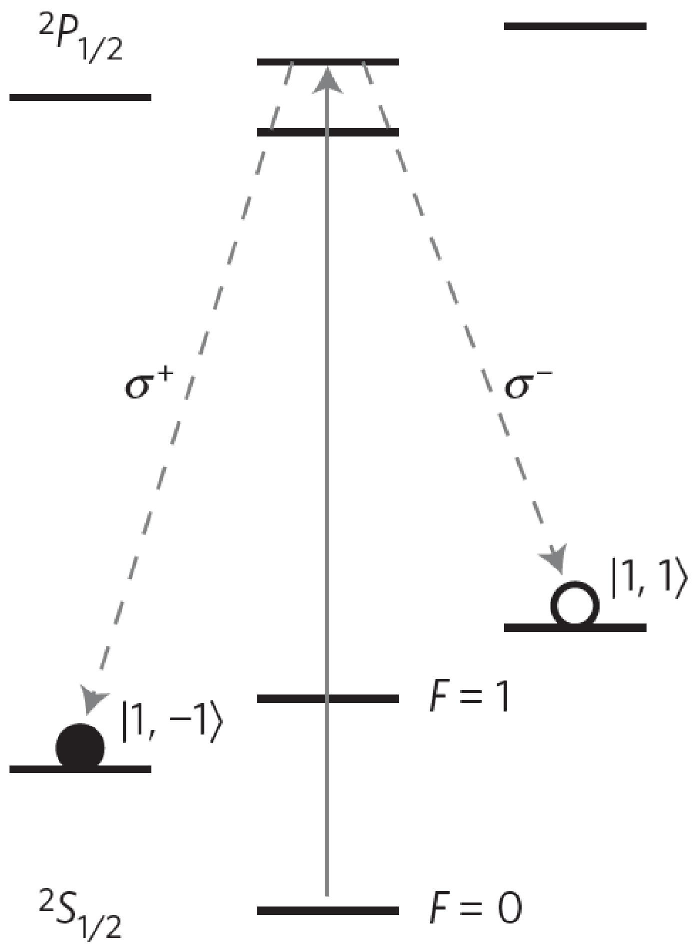
Entangling remote $^{171}Yb^{+}$ ions

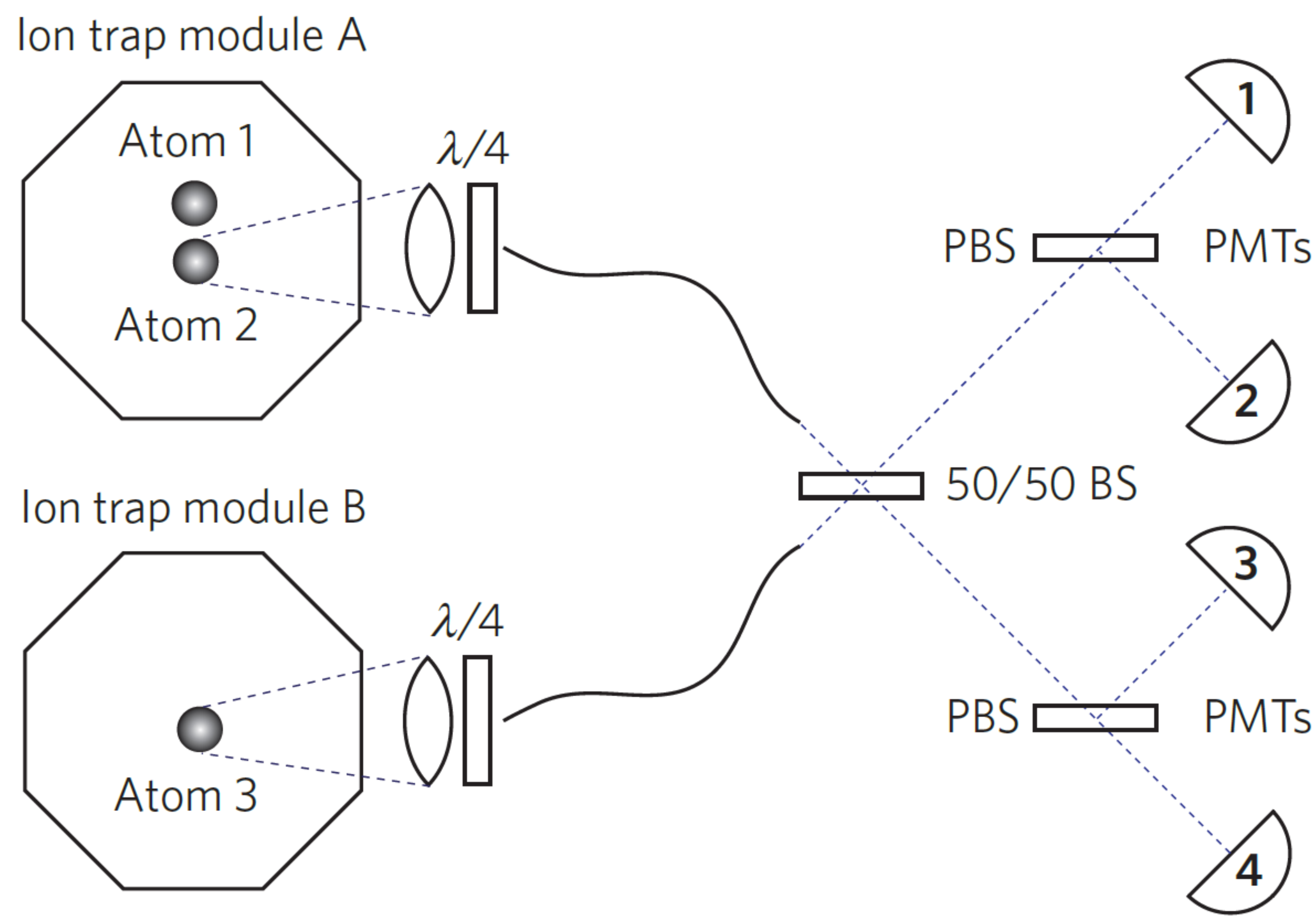
Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)

D. L. Moehring et al., *Nature* **449**, 68 (2007)

D. Hucul, *Nat. Phys.* **11**, 37 (2015)





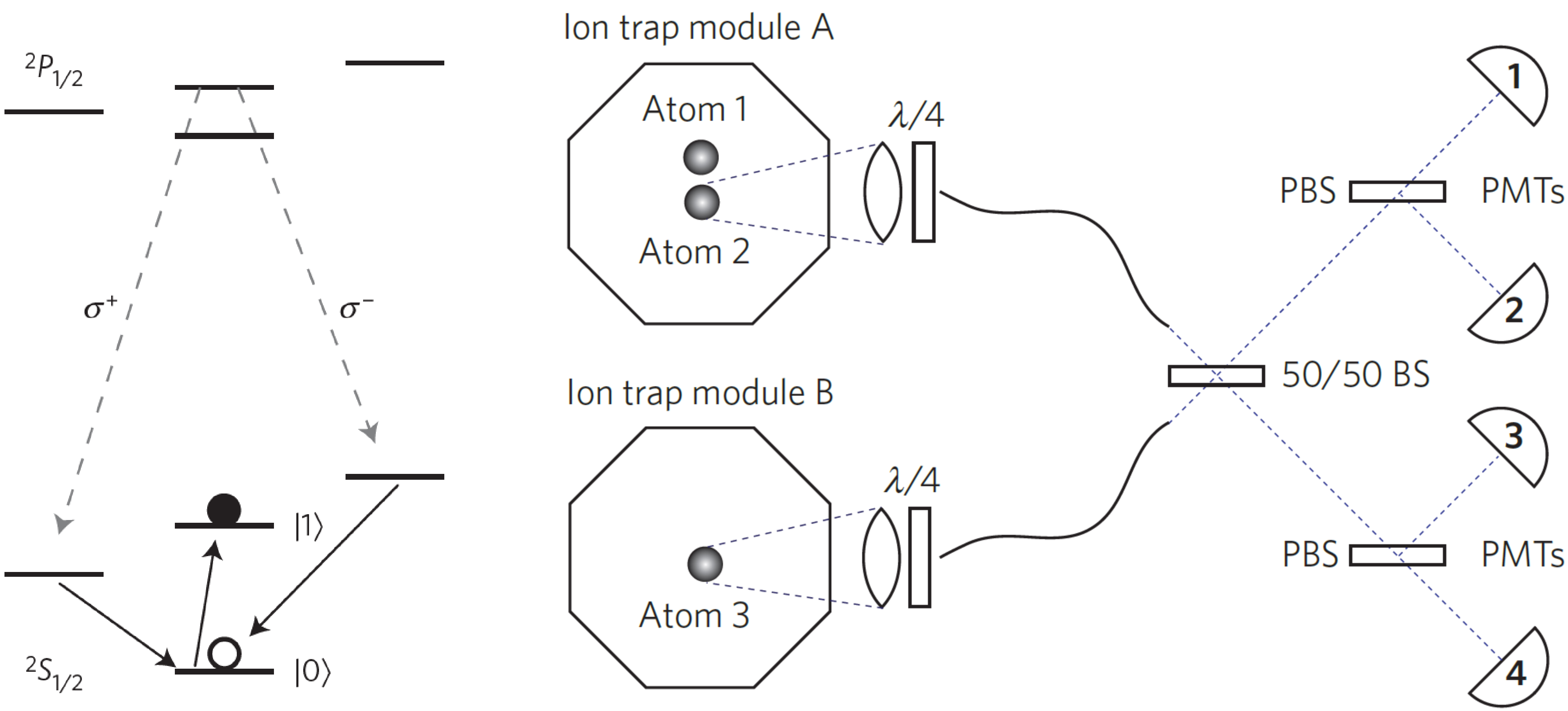
Entangling remote $^{171}Yb^{+}$ ions

Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)

D. L. Moehring et al., *Nature* **449**, 68 (2007)

D. Hucul, *Nat. Phys.* **11**, 37 (2015)



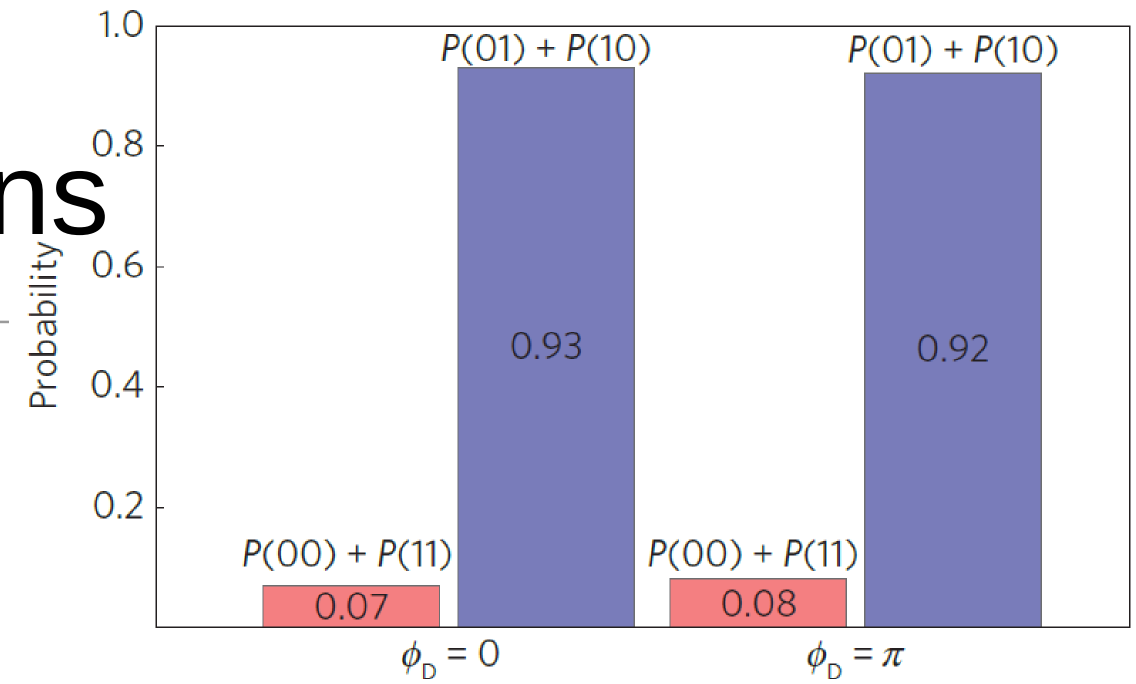
Entangling remote $^{171}Yb^{+}$ ions

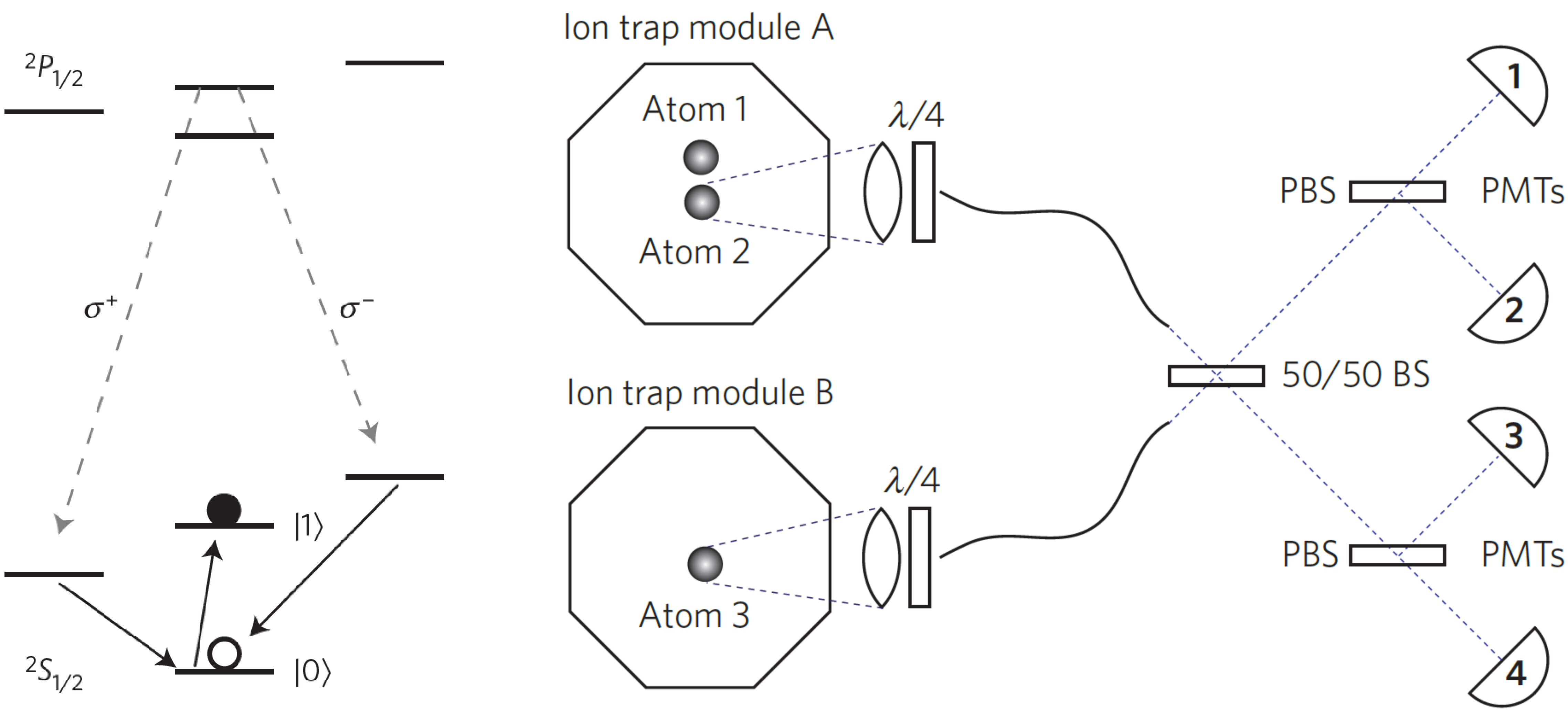
Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)

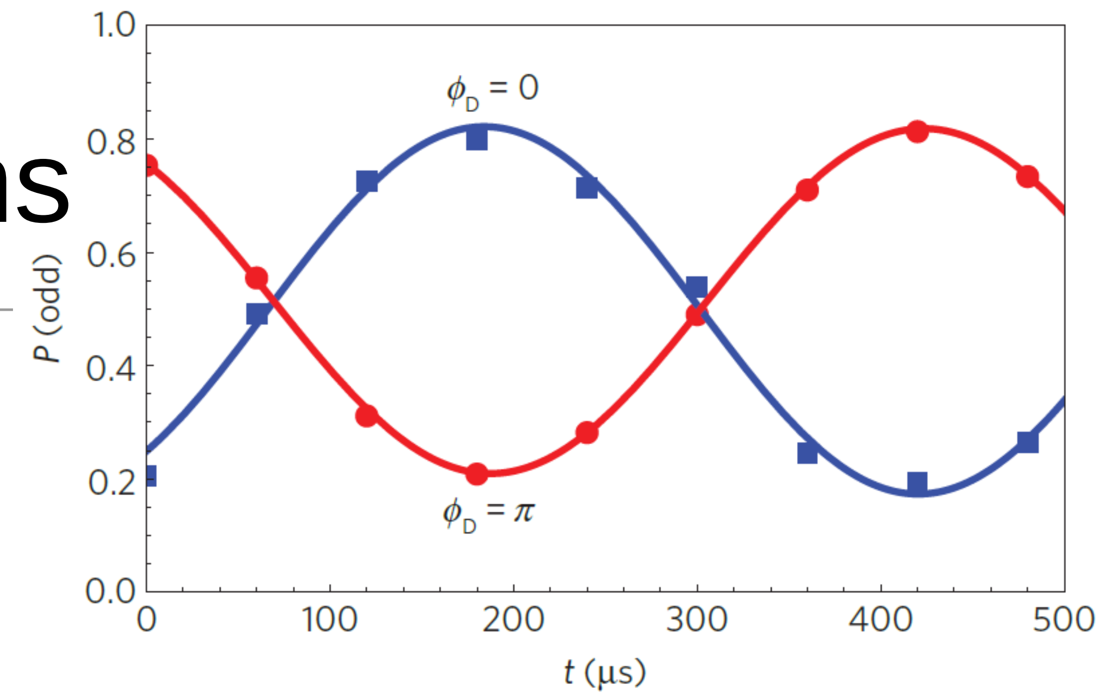
D. L. Moehring et al., *Nature* **449**, 68 (2007)

D. Hucul, *Nat. Phys.* **11**, 37 (2015)





Entangling remote $^{171}Yb^{+}$ ions

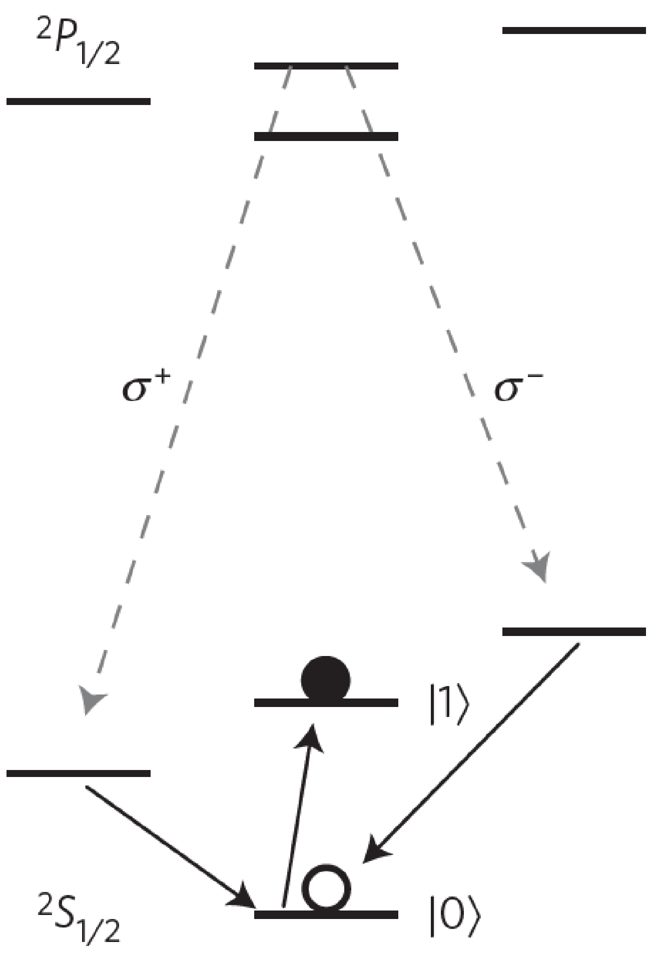


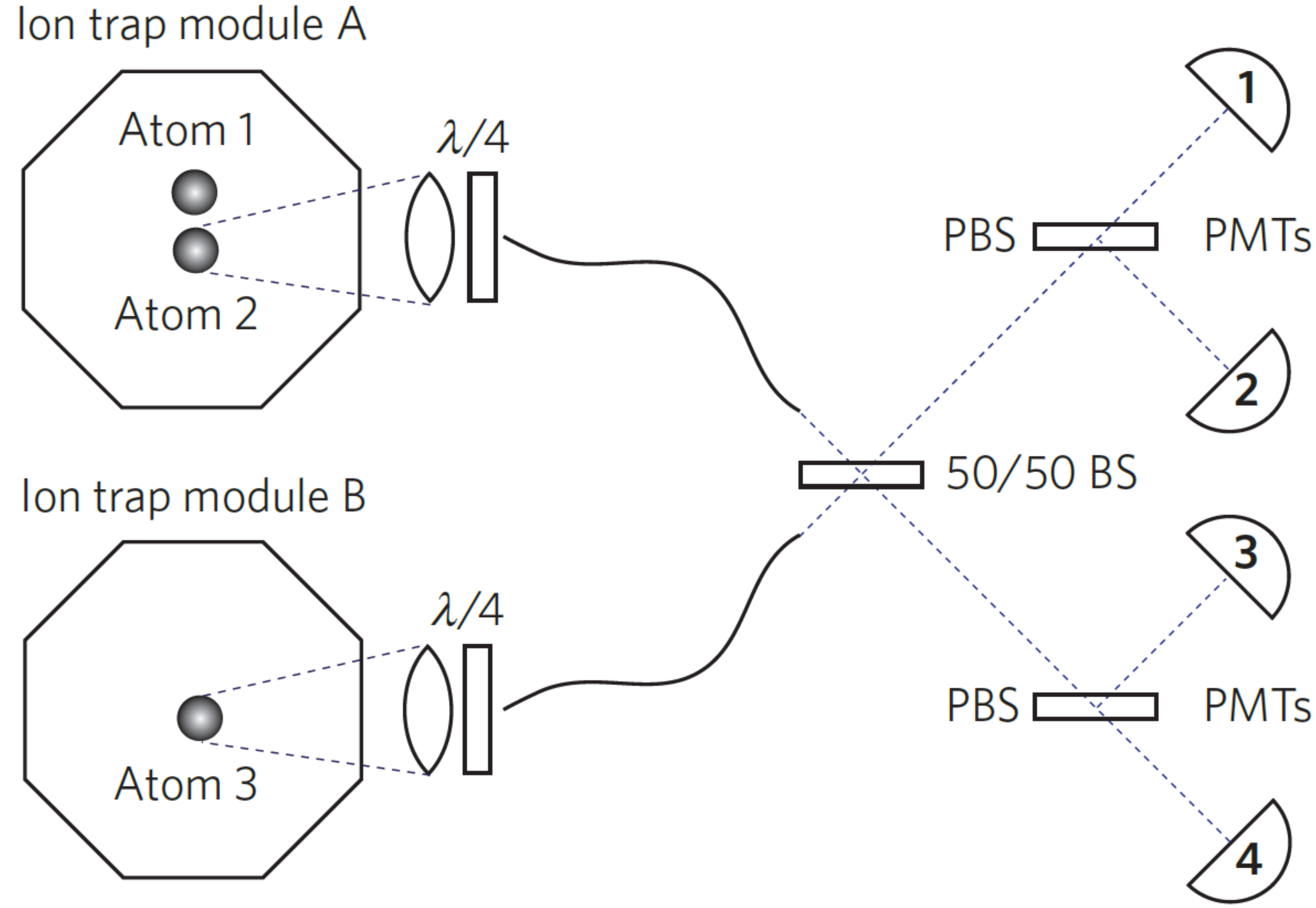
Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)

D. L. Moehring et al., *Nature* **449**, 68 (2007)

D. Hucul, *Nat. Phys.* **11**, 37 (2015)





Entangling remote $^{171}Yb^{+}$ ions

state fidelity

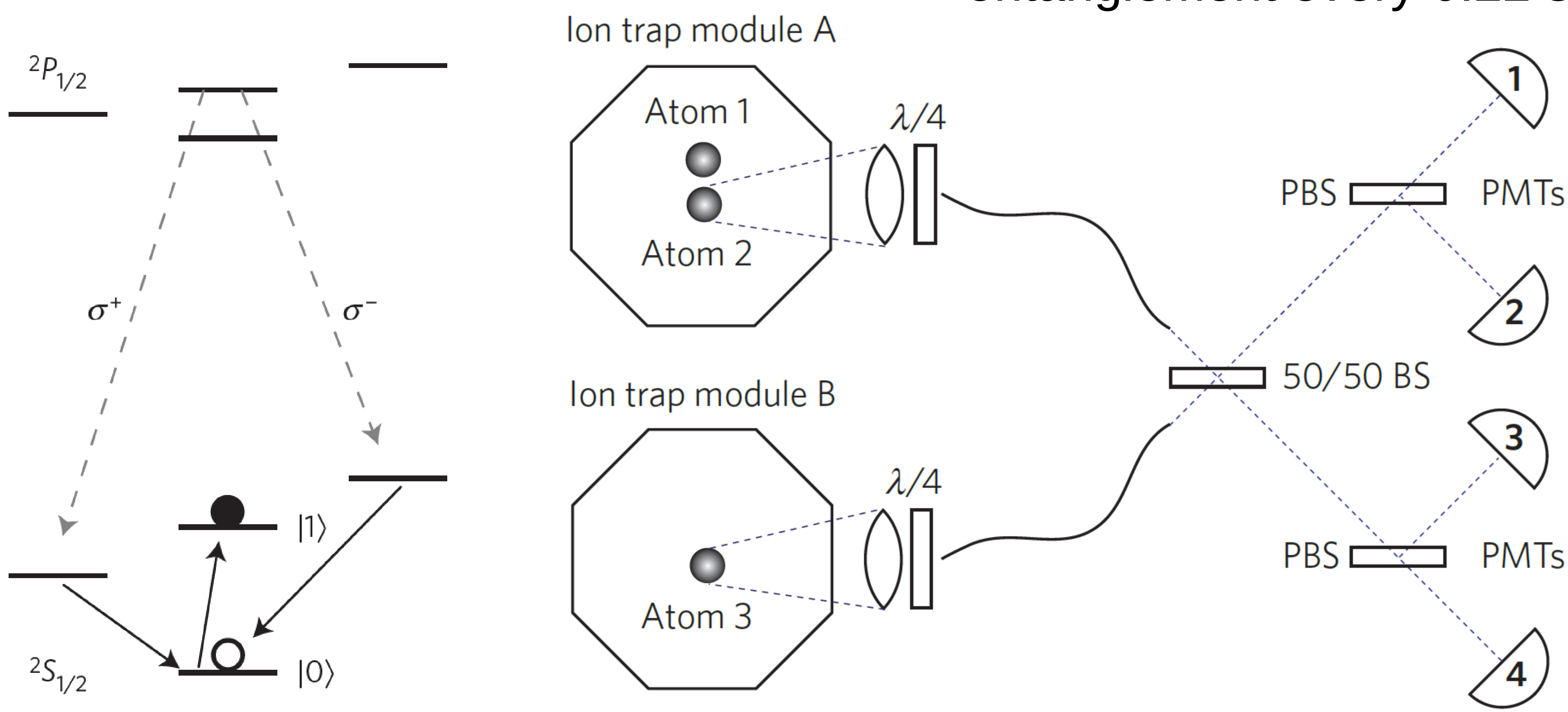
$$F \equiv |\langle \psi_{\mathrm{ideal}} | \psi_{\mathrm{exp}} \rangle|^2$$

Monroe group, University of Maryland / JQI

B. B. Blinov, *Nature* **428**, 153 (2004)
D. L. Moehring et al., *Nature* **449**, 68 (2007)
D. Hucul, *Nat. Phys.* **11**, 37 (2015)

here: fidelity = 78(3)%
(classical bound: 50%)

entanglement every 0.22 s



Remote entanglement has been shown in a handful of experimental systems

- atomic ensembles
  C. W. Chou et al., Nature 438, 828 (2005)
- neutral atoms
  J. Hofmann et al., Science 337, 72 (2012)
- NV centers
  H. Bernien et al., Nature 497, 86 (2013)
- superconducting qubits
  A. Narla et al., Phys. Rev. X 6, 031036 (2016)
- quantum dots
  A. Delteil et al., Nat. Phys. 12, 218 (2016)

state of the art: two-node experiments

Repeaters:
rationale, concepts & generations

So the job of a quantum repeater is…

- 1) to make base-level entanglement over a link
- 2) to couple entangled links along an end-to-end path to meet the applications' needs
- 3) to monitor and manage errors (purification, QEC, or both)
- 4) to participate in the management of the network

Conceptual Hardware

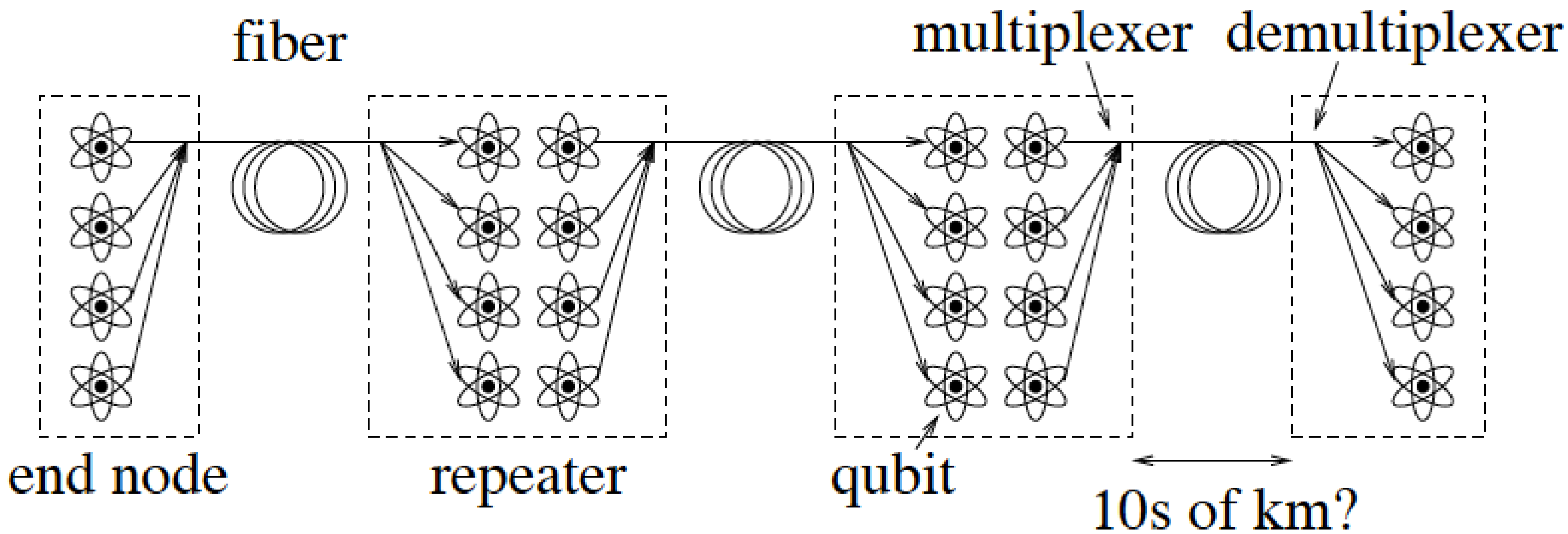
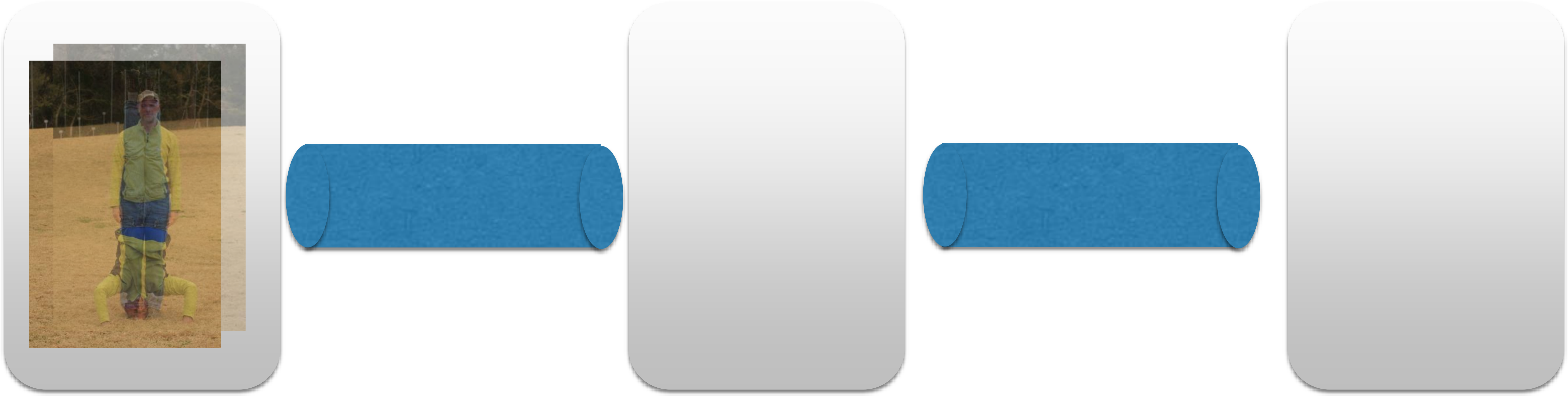


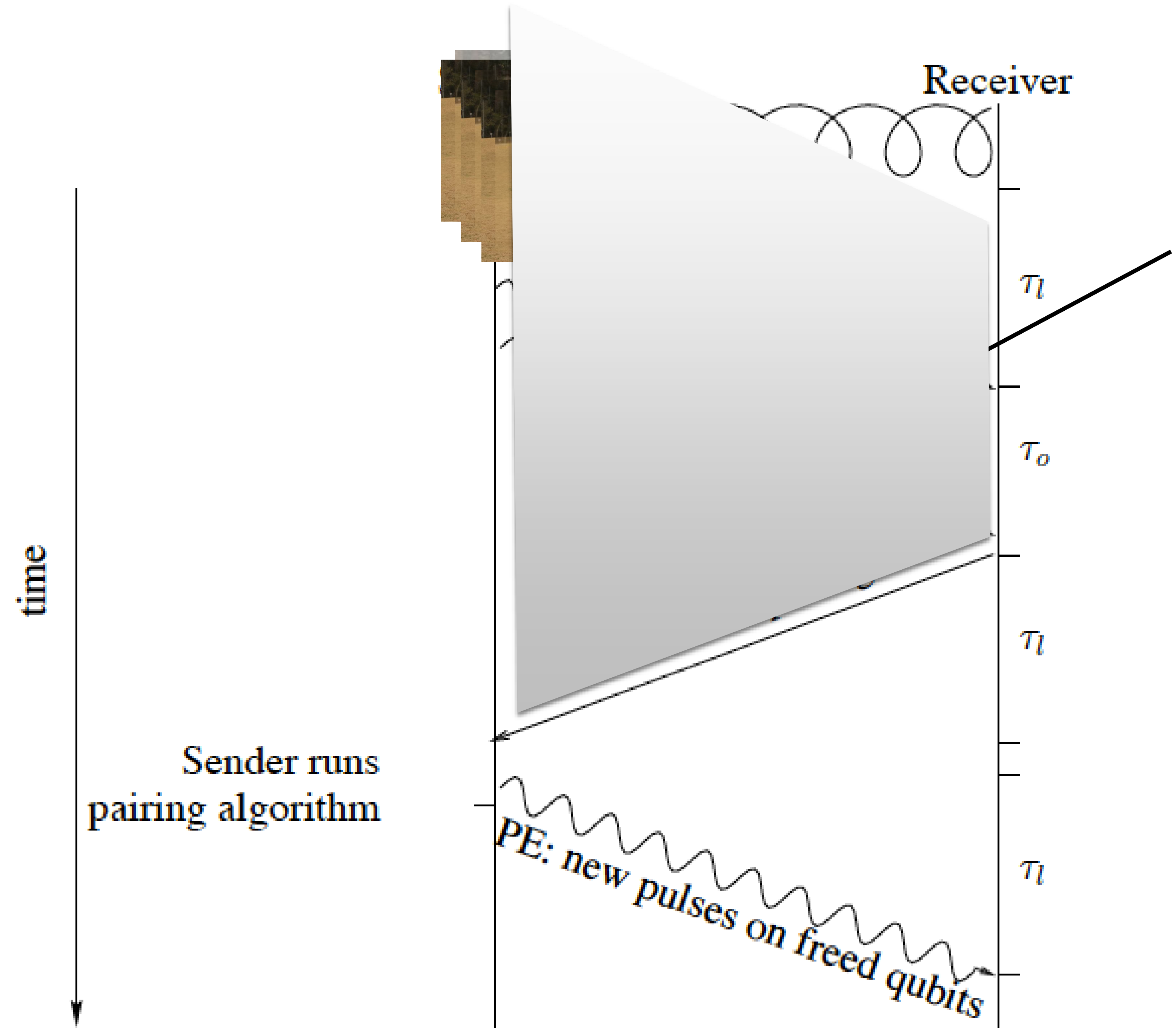
Figure 10.1: Generic view of the hardware of a line of repeaters. Qubit memories are represented by the atom symbol, regardless of physical device type.

(There are also all-optical approaches, with no static buffer memory.)

Store-and-Forward?



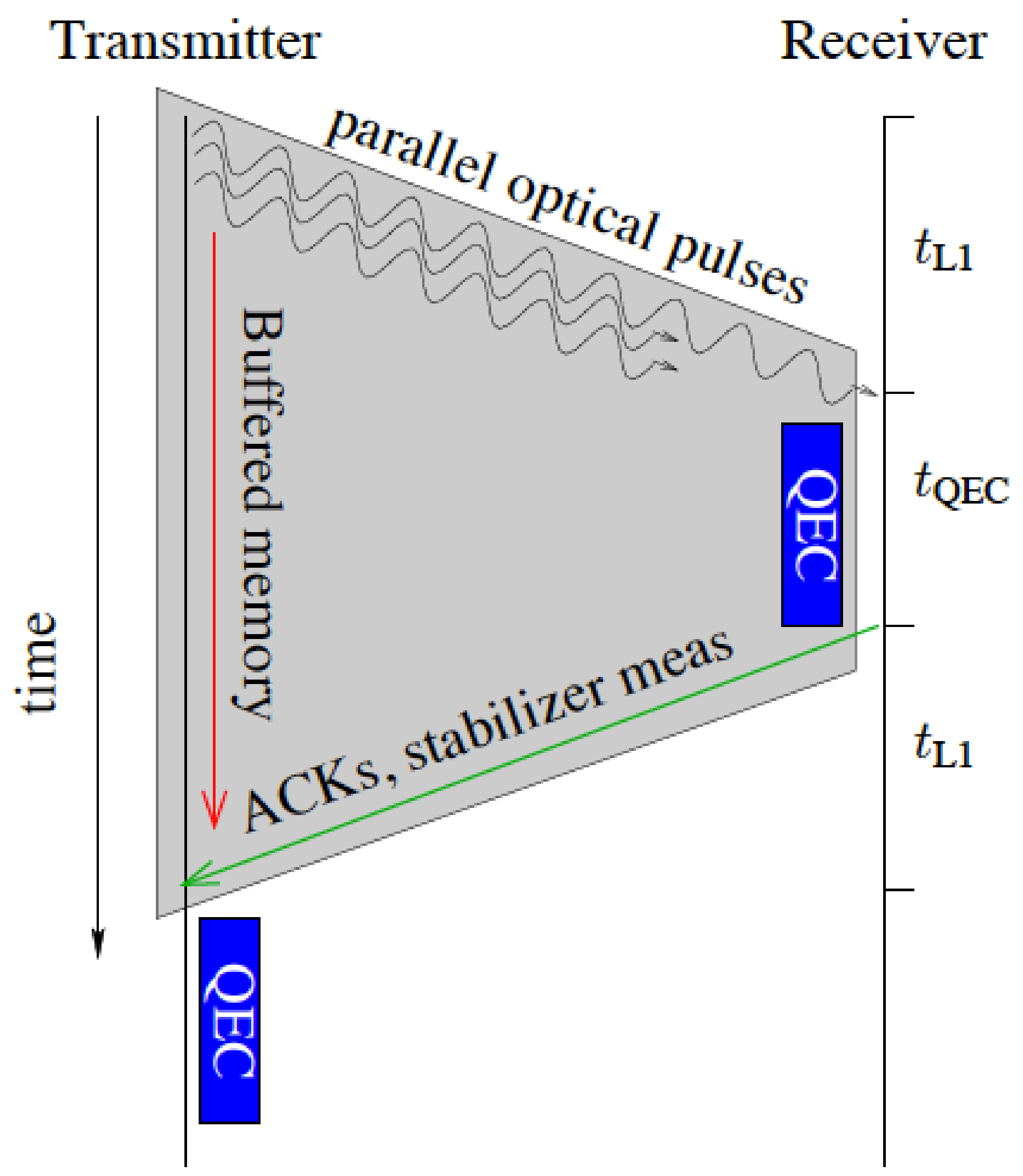
Direct Transmission Pretty Clearly Doesn't Work...



Loss in channel always too high

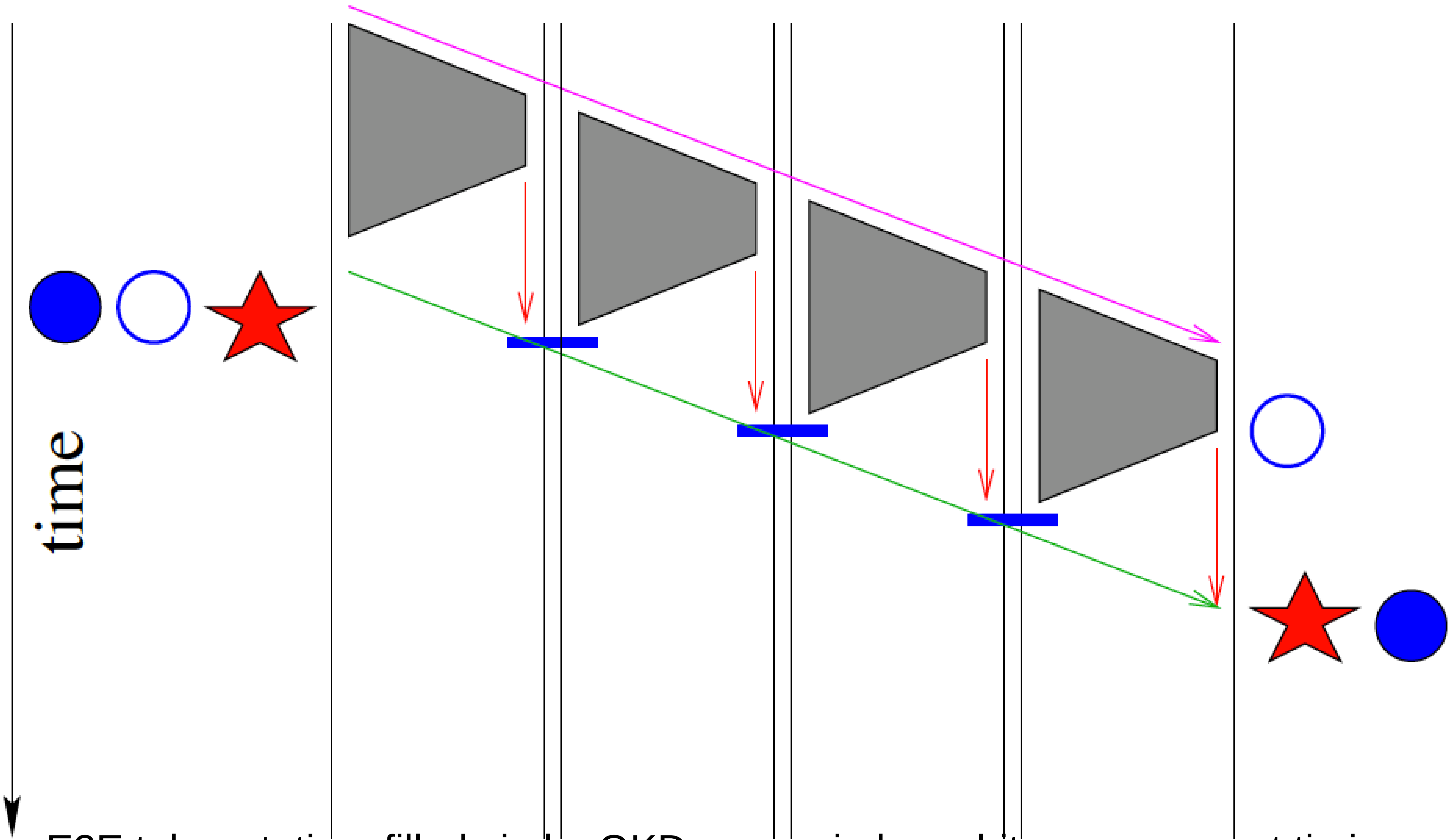
Must use acknowledged link layer, build generic Bell pair, then teleport

Timing Trapezoids



So Why Doesn't Hop-by-Hop Teleportation Work?

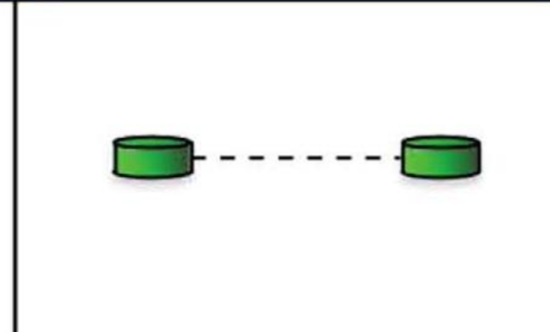
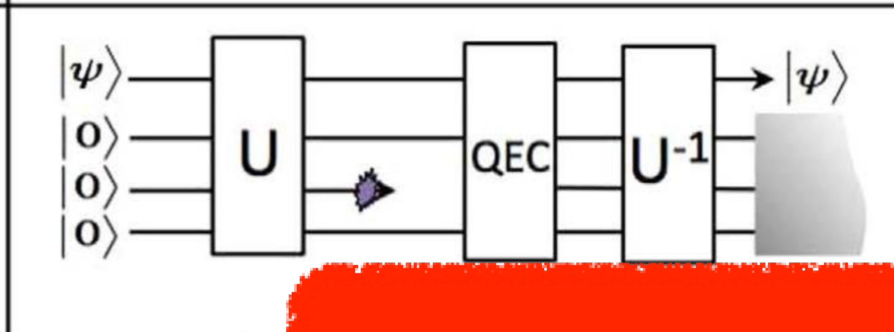
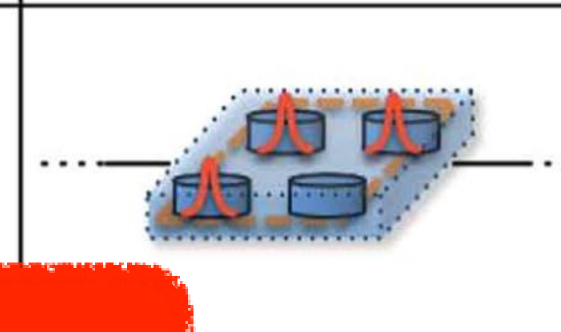
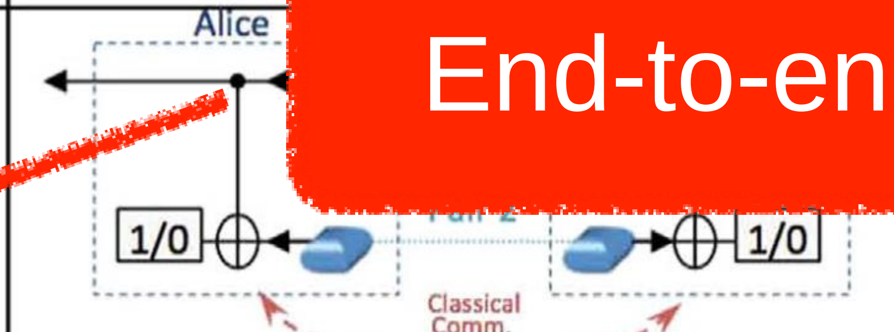
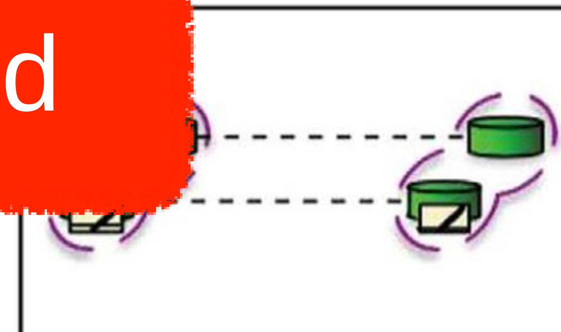
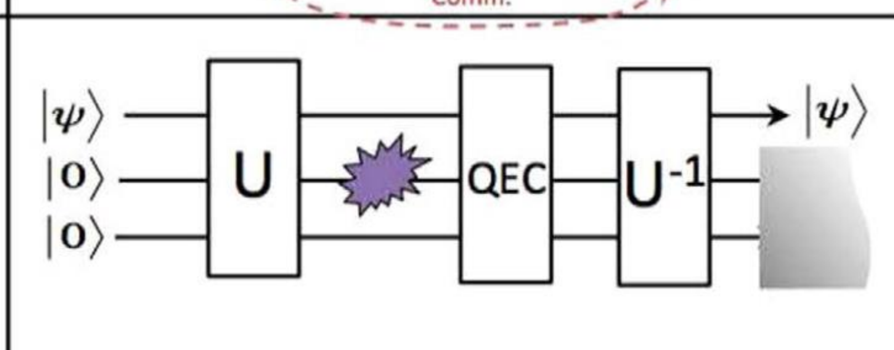
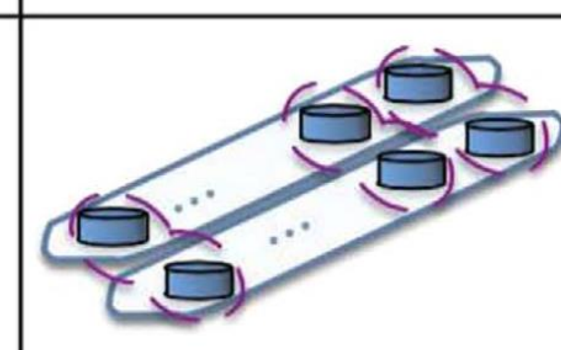
Long memory times, swapping (local xfer) fidelity



Star: E2E teleportation; filled circle: QKD; open circle: qubit measurement timing
blue bar: entanglement swapping

Link level

End-to-end

Errors	Approaches	Examples	Schematics	1G	2G	3G
Loss Error	Heralded Entanglement Generation (HEG)			✓	✓	
	Quantum Error Correction (QEC)					✓
Operation Error	Heralded Entanglement Purification (HEP)			✓		
	Quantum Error Correction (QEC)				✓	✓

Elements: Remotely entangled qubit; Flying qubit (photons); CNOT gate; Qubit in an encoded block; Measurement (X/Z); Teleportation-based Error Correction

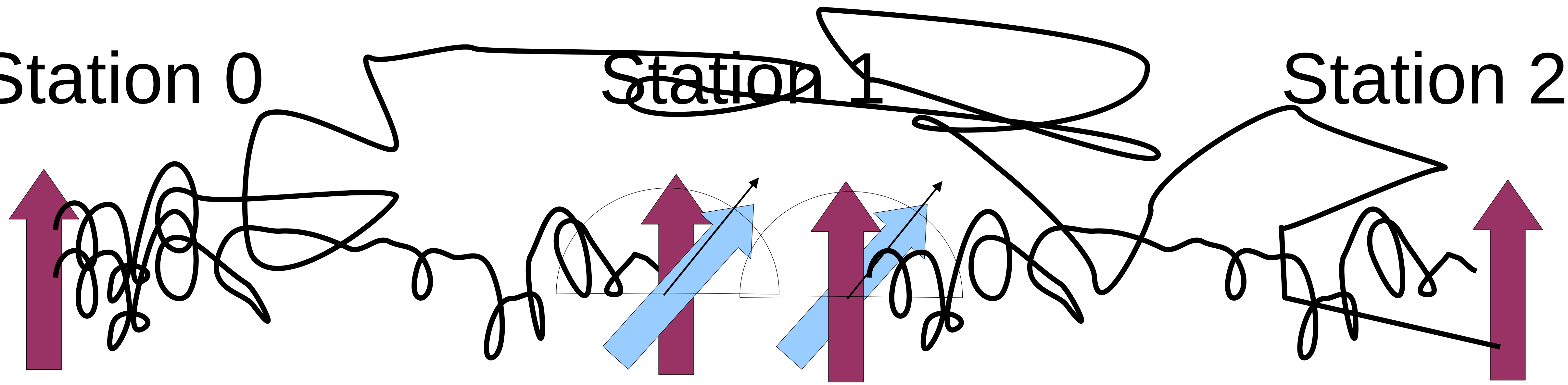
http://www.nature.com/articles/srep20463

Five Repeater Schemes

- 1G: Purify and swap over ACKed links: truly a distributed computation (Dur & Briegel, Lukin, others; since 1998)
- 2G: Error Correction over ACKed links
  - CSS quantum error correction & entanglement swapping (Jiang (Lukin) *et al.*, 2009)
  - Surface code quantum error correction, sort of but not quite swap (Fowler *et al.*, 2010)
- 3G: Error Correction over no-ACK-needed links: store-and-forward
  - Quasi-asynchronous (Munro *et al.*, 2010)
  - Memoryless (Munro *et al.*, 2012)

Quantum Repeater Operation

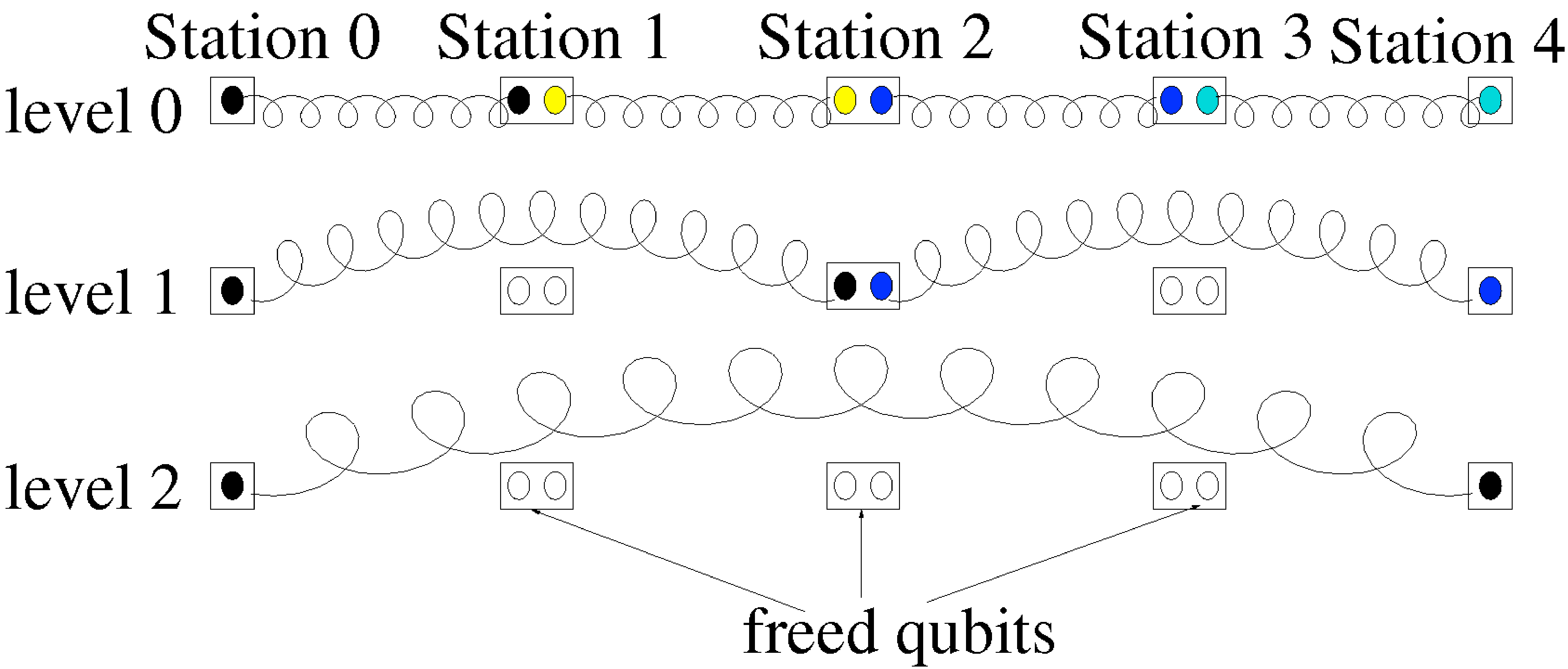
Station 0 Station 1 Station 2



Bell State
Measurement

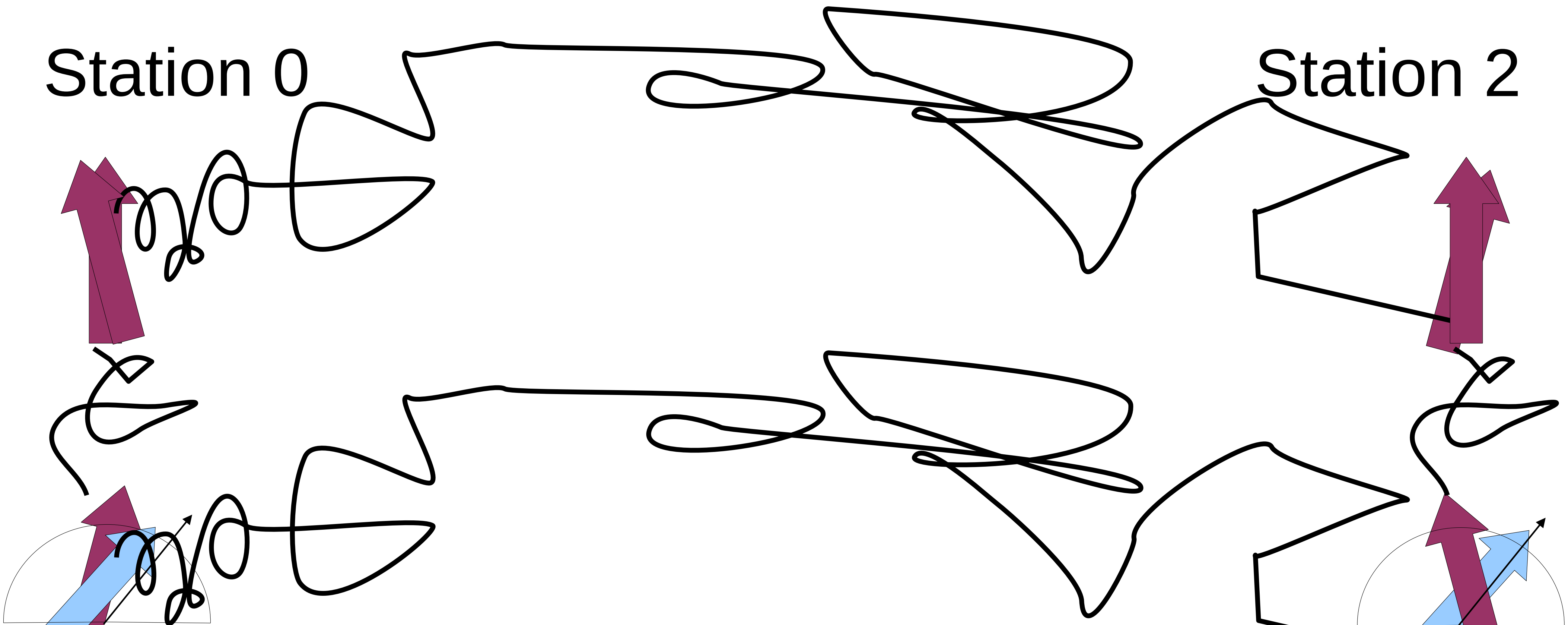
Called *entanglement swapping*.
Fidelity declines; you must *purify* afterwards

Nested Entanglement Swapping



Dur & Briegel, many others

Purification: Error Detection



Two entangled states used:
one used as a *test tool* to test an assertion about the other.
The test tool is destroyed in the process.
On success, confidence in the tested state (fidelity) improves.
On failure, tested state is discarded.

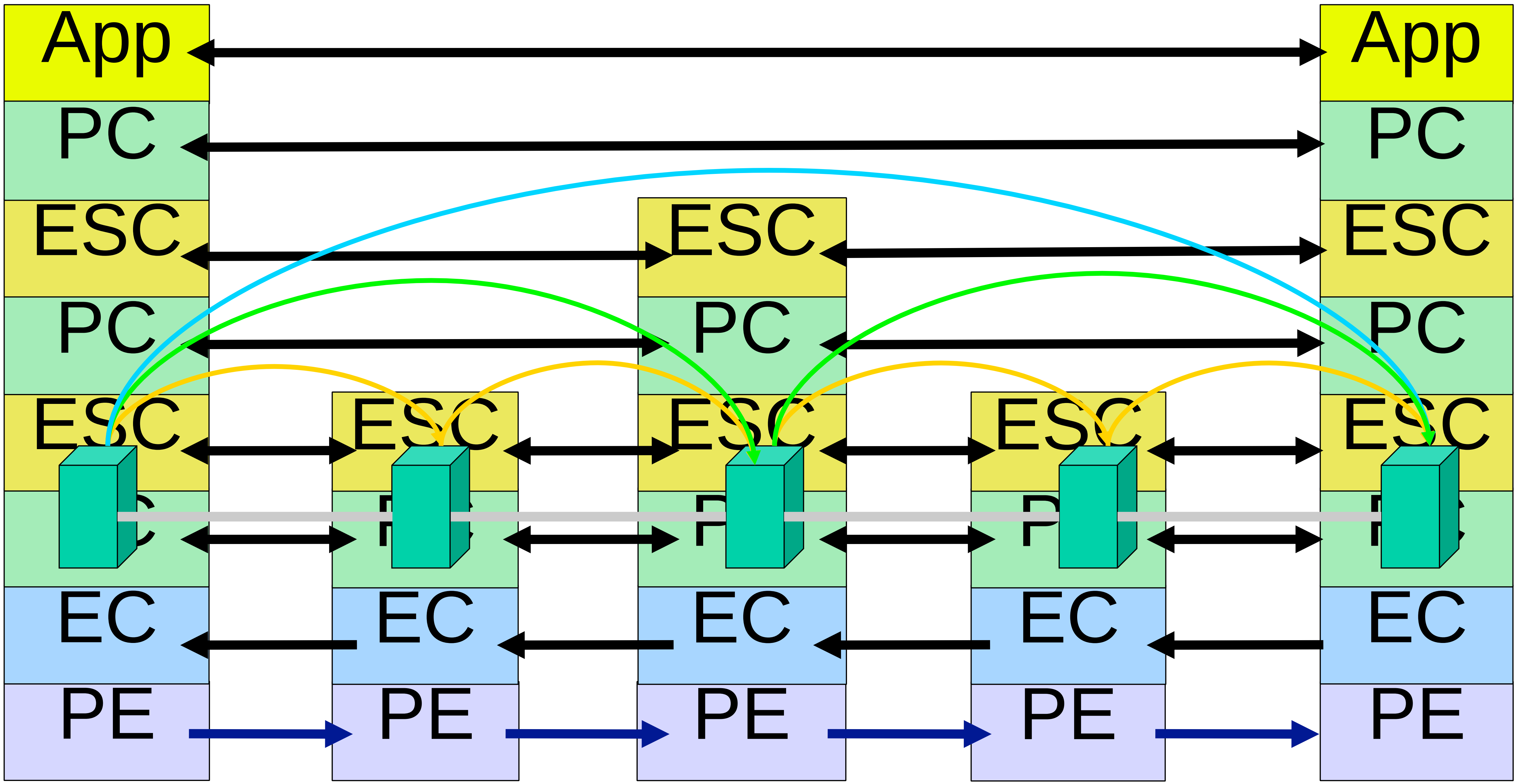
Repeater Protocol Stack

Application	End-to-End
Purification Control (PC)	End-to-End
Entang. Swapping Ctl (ESC)	Repeated at Different Distances
Purification Control (PC)	Repeated at Different Distances
Entanglement Control (EC)	Distance=1
Physical Entanglement (PE)	Distance=1

Only quantum!

Van Meter *et al.*, IEEE/ACM Trans. on Networking, Jun. 2009, quant-ph:0705.4128

Four-Hop Protocol Interactions



2G & 3G are still *far* away

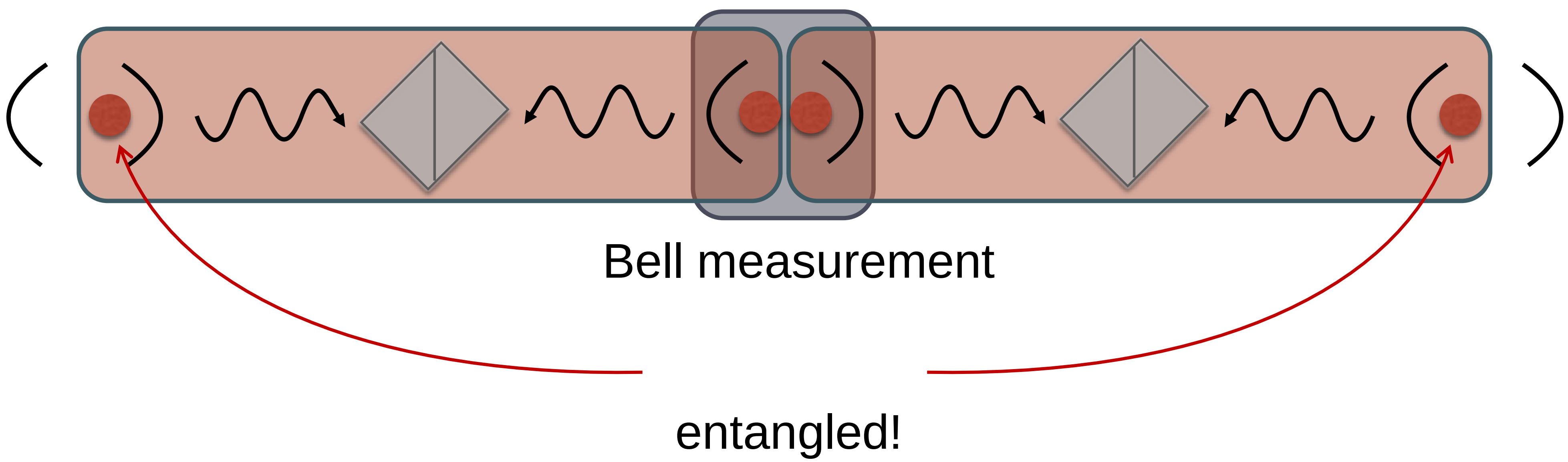
- Even 1G is really hard
  - Entanglement success probability is low, many round trips in protocols, few qubits per node, memory lifetimes are still problematic
  - Getting & keeping a Bell pair to the left at the same time as Bell pair to the right to enable swapping
  - Getting & keeping two Bell pairs for purification
  - Gate errors in both purification and swapping
- 2G: Error Correction over ACKed links
  - Will blow up resource requirements at least 7x, before the probabilistic problems above
  - Gate error rates too high for QEC to work yet
- 3G: Error Correction over no-ACK-needed links (store-and-forward)
  - Prob. 80-93% or better (depending on code) of correctly receiving *each individual photon*

What would the simplest 1G repeater look like?

H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998)

1. Entangle one pair of atoms.
2. Entangle a second pair of atoms.
3. A Bell measurement on the two central atoms entangles the two outermost atoms.

This approach is not scalable because errors accumulate.



What would the simplest 1G repeater look like?

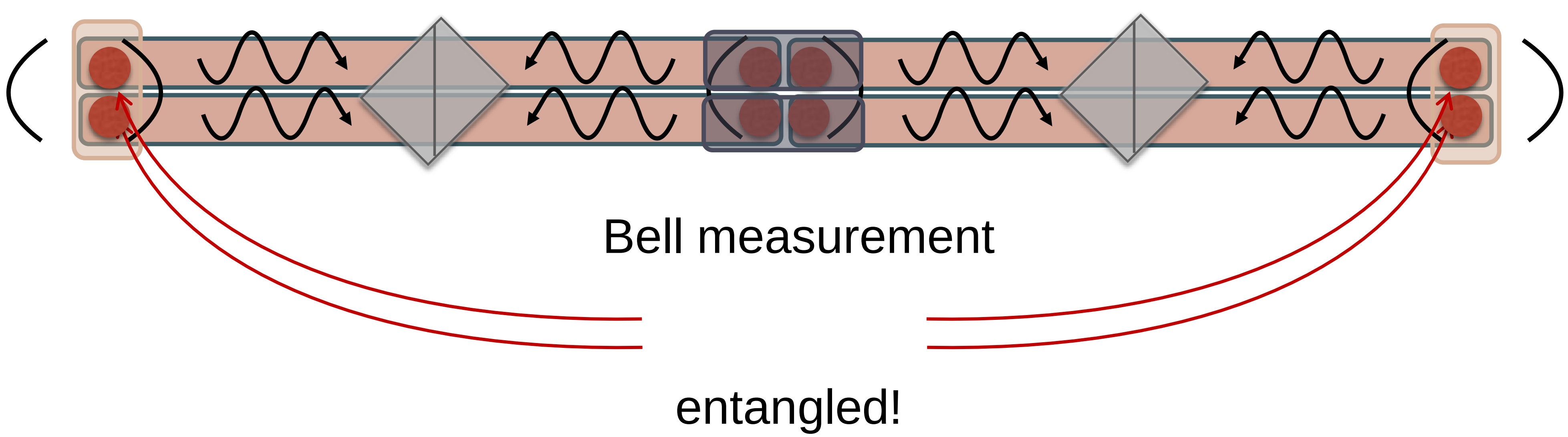
H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998)

Entanglement purification is the key to scalability.

Multiple copies of entangled pairs are reduced to fewer copies with higher fidelity. Requirements: gate operations between local qubits & readout of one qubit.

Quantum repeater = entanglement swapping + purification

Note that we have to wait for classical information to travel from A to B.



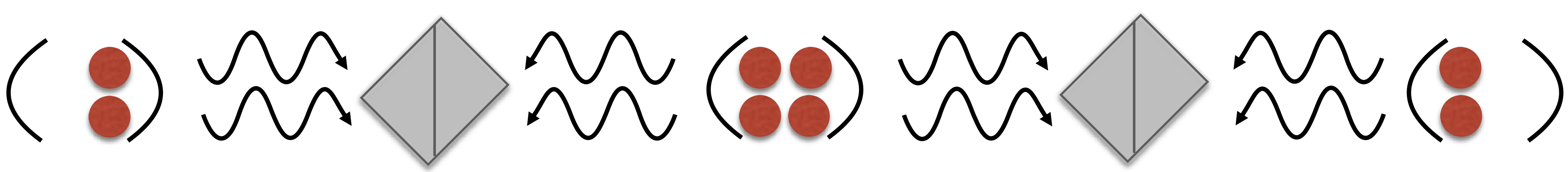
No one has built a quantum repeater yet.

The simplest version:

1. Eight qubits, three nodes
2. Gate operations between qubits for Bell-state measurements and purification.

Closest experiment: entanglement purification with four qubits (two NV centers, two nuclear spins).

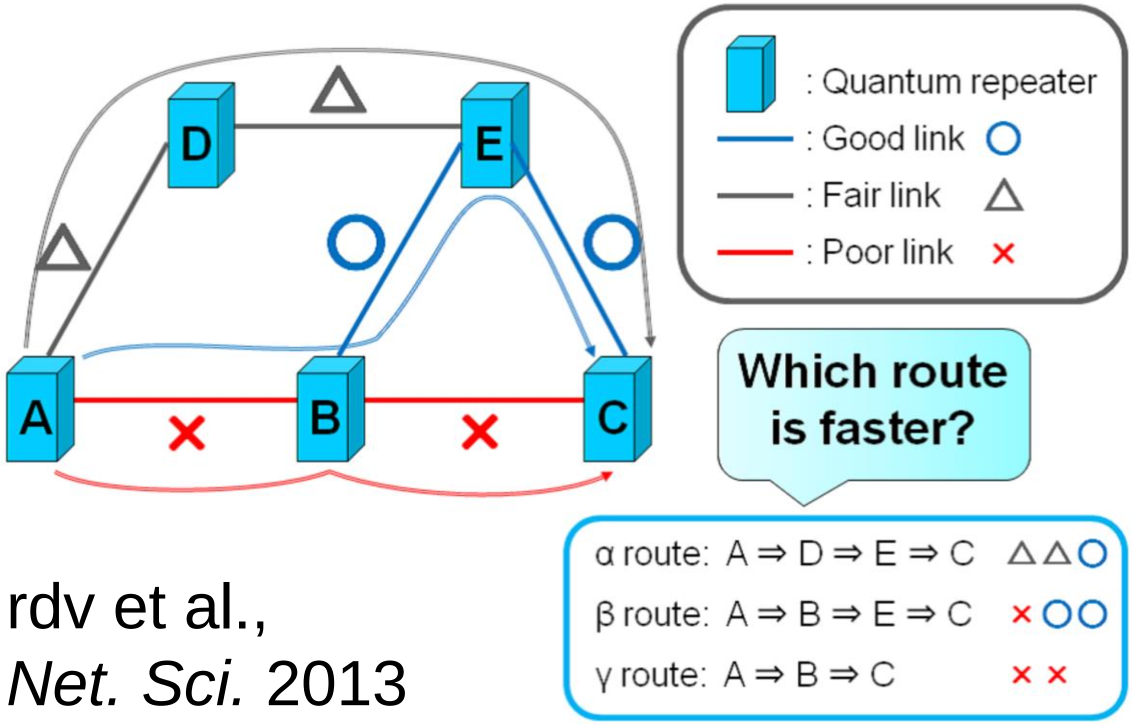
N. Kalb et al., *Science* **356**, 928 (2017)



State of research

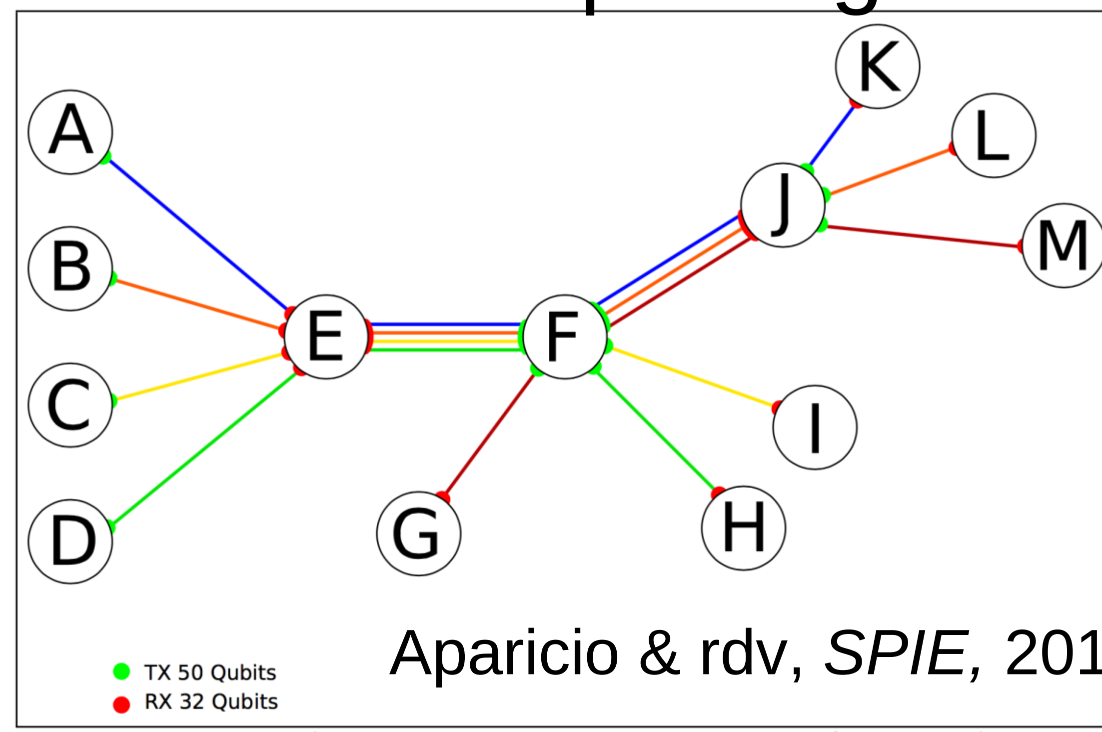
Some networking results from rdv’s group

Routing



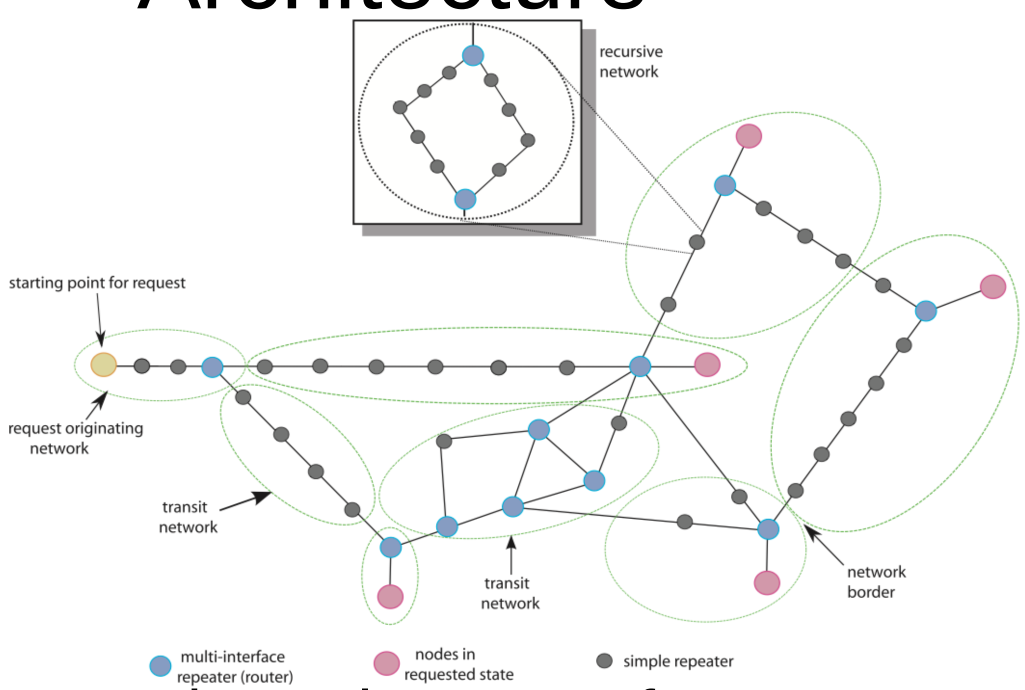
rdv et al.,
Net. Sci. 2013

Multiplexing



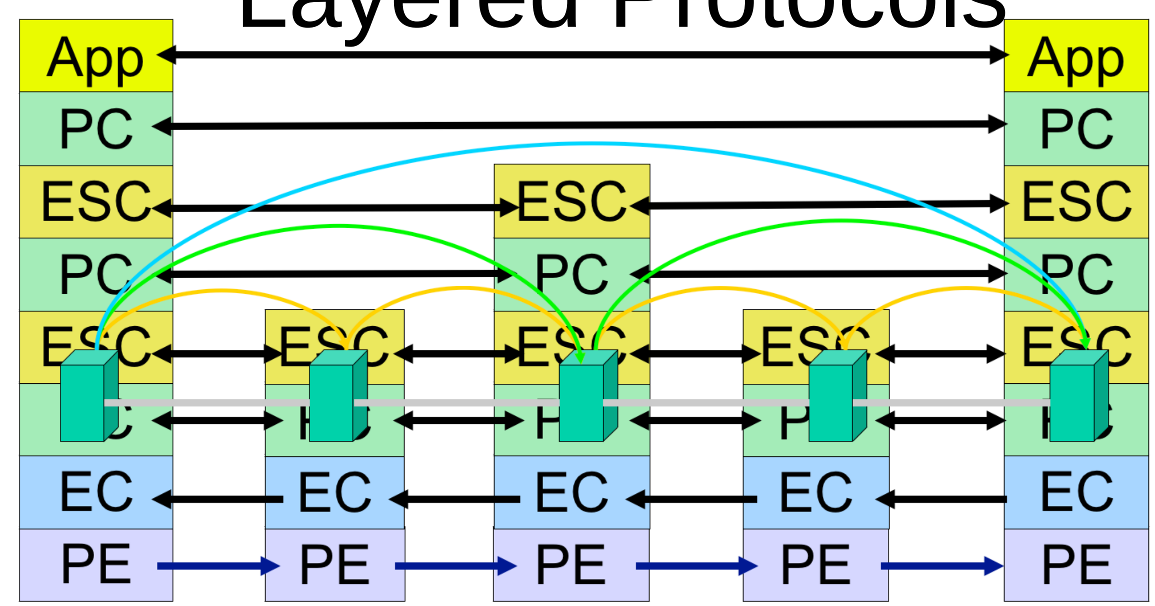
Aparicio & rdv, *SPIE*, 2011

Architecture



rdv et al.,*Prog. Info.* 2013

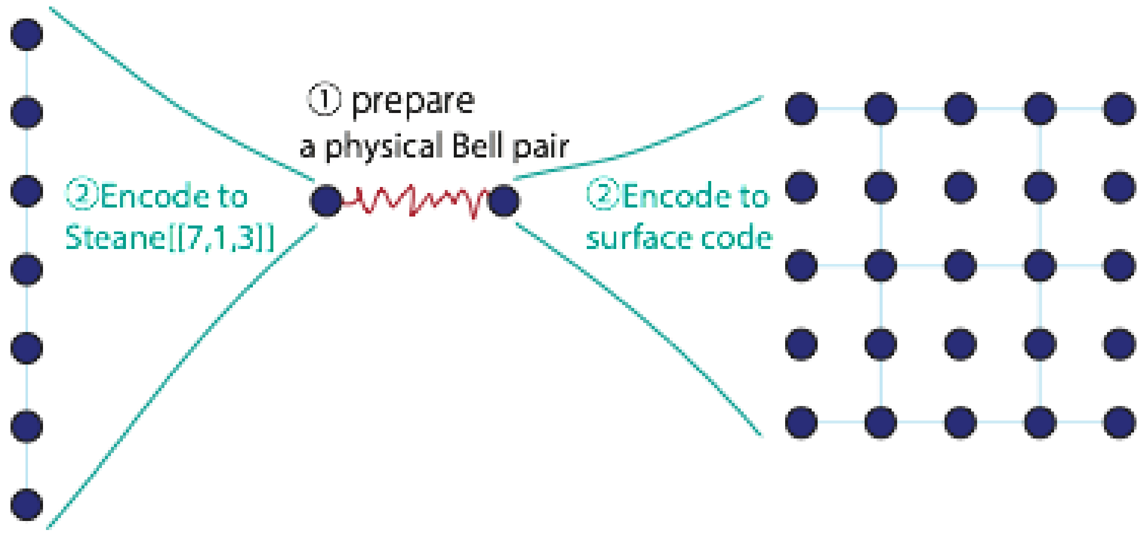
Layered Protocols



rdv et al.,*Trans. Networking*, 2009

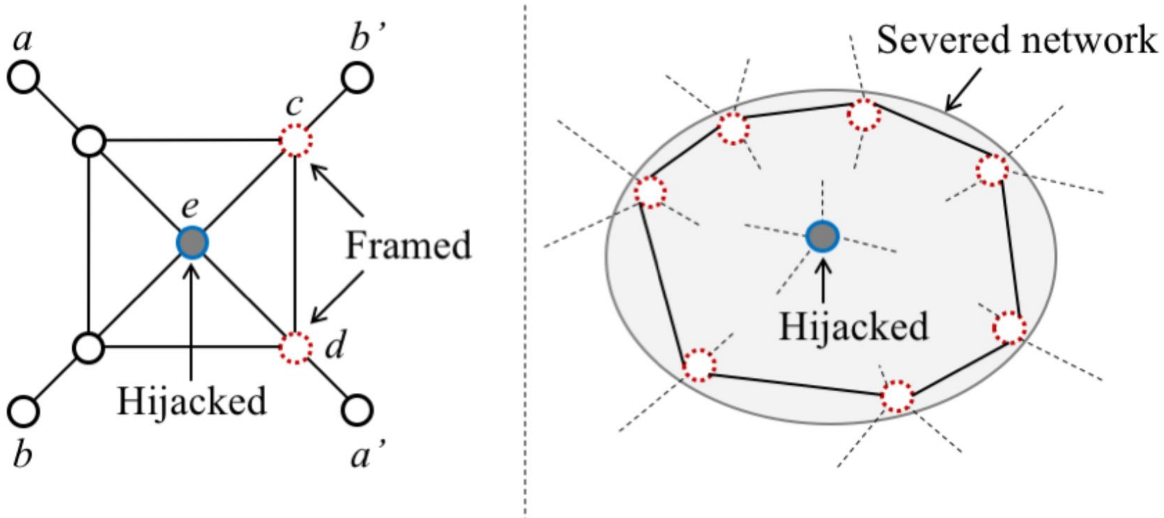
Some networking results from rdv's group

Internetworking



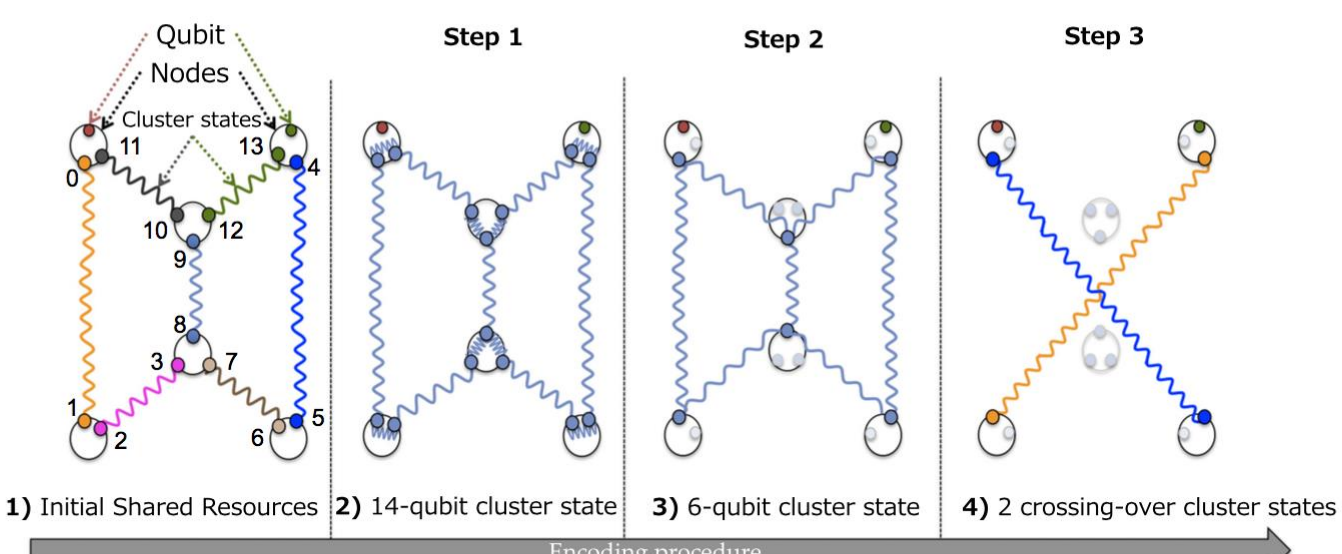
Nagayama et al., Phys. Rev. *A* 2016

Hijacking of a Repeater



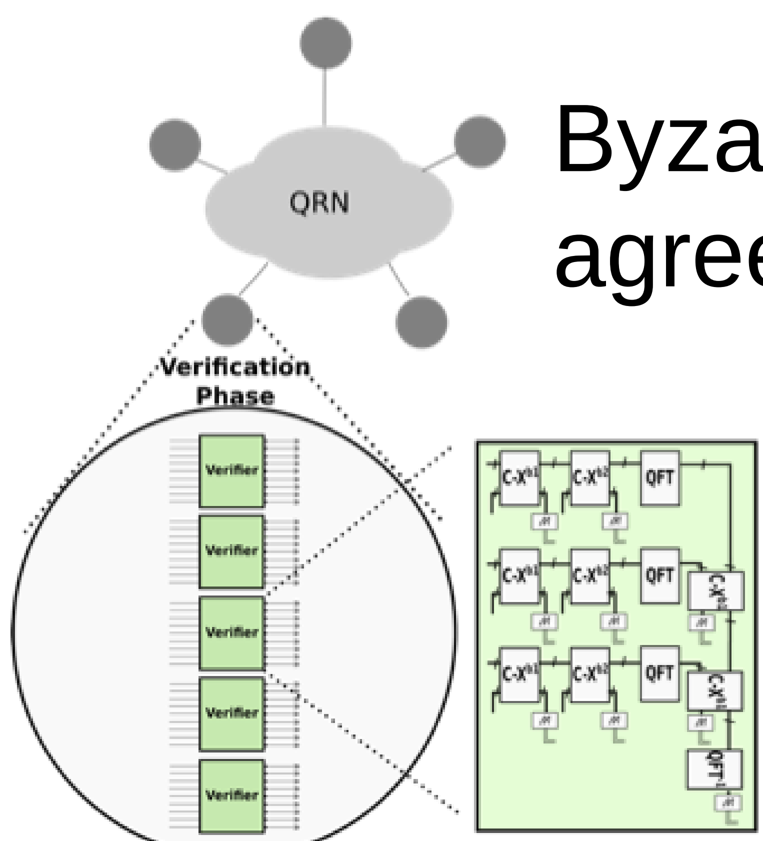
Satoh et al., QST, 2018

Network Coding



Matsuo et al.,*Phys. Rev. A* 2018

Byzantine agreement



Taherkhani et al.,QST, 2017

Stephanie’s group

Quantum internet: A Vision for the road ahead (https://doi.org/10.1126/science.aam9288):
This was presented already in Bangkok. This paper defines stages of quantum networks and what applications can be realized on these.

A Link Layer Protocol for Quantum Networks (will be on arXiv tomorrow!):
Presents a link layer protocol which provides the defines service in https://datatracker.ietf.org/doc/draft-dahlberg-ll-quantum/ together with simulations of performance metrics of a complete implementation of the protocol using a discrete-event simulator.

Parameter regimes for a single sequential quantum repeater (https://arxiv.org/abs/1705.00043):
Assesses the performance of single sequential quantum repeaters using realistic hardware parameters.

Fully device-independent conference key agreement (https://arxiv.org/abs/1708.00798):
Presents security proof for fully device-independent conference key, which task is to distribute a secret key among N parties.

Anonymous transmission in a noisy quantum network using the W state (https://arxiv.org/abs/1806.10973):
Shows how one can perform anonymous transmission using a W state, which in many regimes can tolerate more noise than the more common approach of using a GHZ state.

SimulaQron – A simulator for developing quantum internet software (https://arxiv.org/abs/1712.08032):
Presenting SimulaQron, a simulator intended to be used for development of software for quantum networks.

Final thoughts:
References, learning more & getting involved

Good Repeater References

- Dur & Briegel’s originals, 1990s onwards
- Kimble’s “Quantum Internet” in *Nature,* 2008
- Rodney Van Meter, *Quantum Networking,* Wiley-iSTE 2014
- Takeoka, Guha, Wilde, *Nature Communications*, 2014
  on when repeaters are more effective than simple transmission
- Muralidharan *et al.*, *Scientific Reports*, 2016
  defines 1G, 2G, 3G
- Pirandola, *Nature Communications,* 2017
  extending TGW analysis
- Wehner, Elkouss, Hanson, *Science*, 2018
  roadmap

FutureLearn

Understanding Quantum Computers

Go to course

Upgrade - $59

+ shipping

Edit run

Future Learn

50+

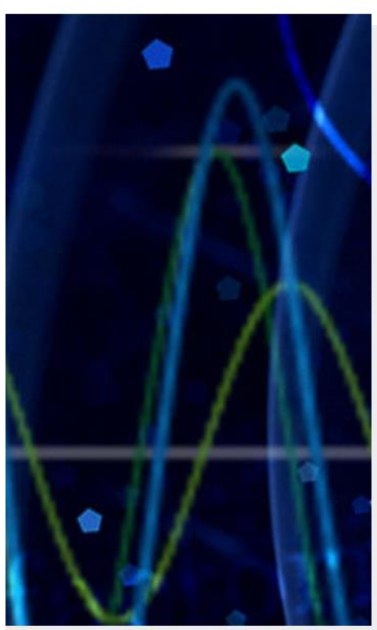
Duration
3 weeks

4 hours
per week

FREE
online course

Upgrade
available

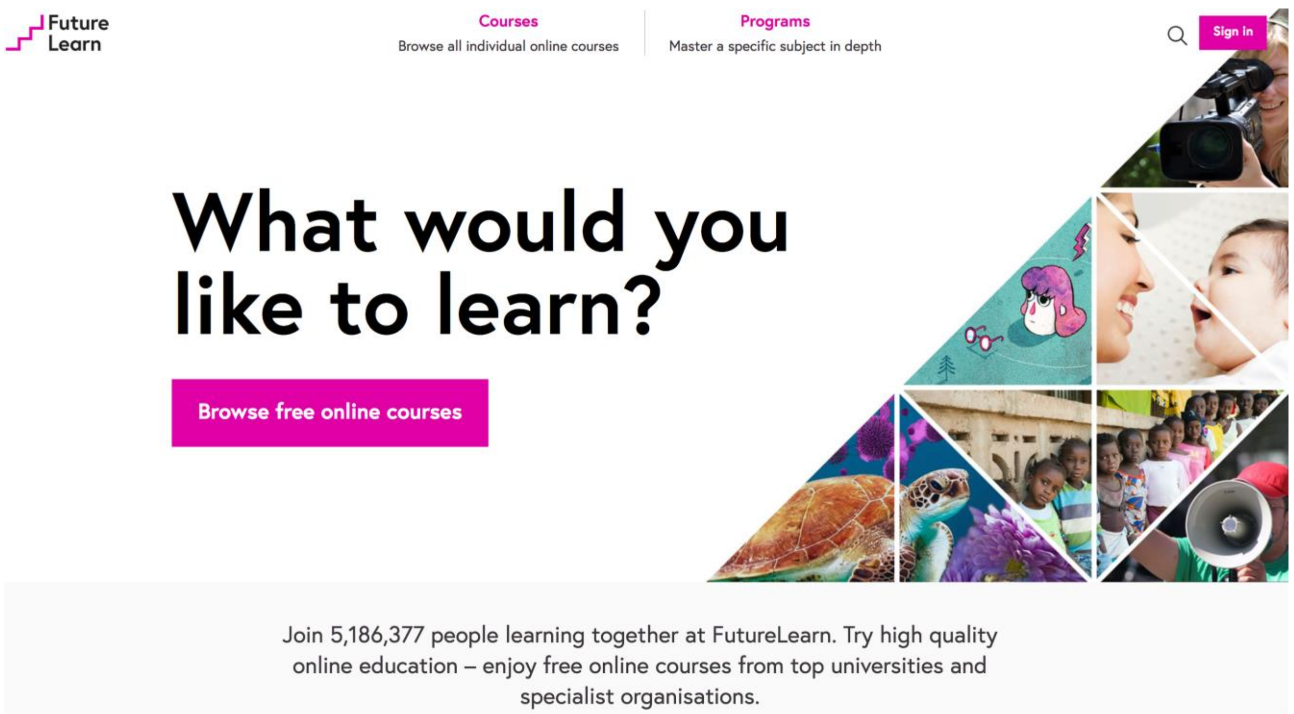
What's this?



View transcript

Download video: standard or HD

Future Learn



Find a course

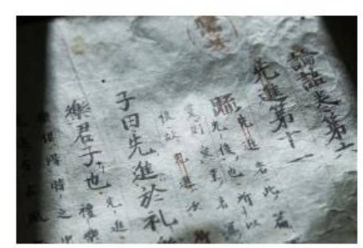
Keio

Search courses

3 RESULTS FOR "KEIO"

AN INTRODUCTION TO JAPANESE SUBCULTURES
KEIO UNIVERSITY
Explore Japanese subcultures and learn about their history from the 1970s to today.
28 Nov | 4 weeks | 4 hours pw | Certificate | More

JAPANESE CULTURE THROUGH RARE BOOKS
KEIO UNIVERSITY
Explore the important roles that books have played in the cultural history of Japan.
9 Jan | 3 weeks | 3 hours pw | Certificate | More



SINO-JAPANESE INTERACTIONS THROUGH RARE BOOKS
KEIO UNIVERSITY
Learn about the role of books in the relationship between the cultures of Japan and China, with this free online course.
6 Mar | 3 weeks | 3 hours pw | Certificate | More

4th run of MOOC (massive open online course) on Quantum Computing includes 日本語の字幕！Starts April 1!

4th run of MOOC will include translation into Thai!

The Quantum Internet and Quantum Computers: How Will They Change the World?

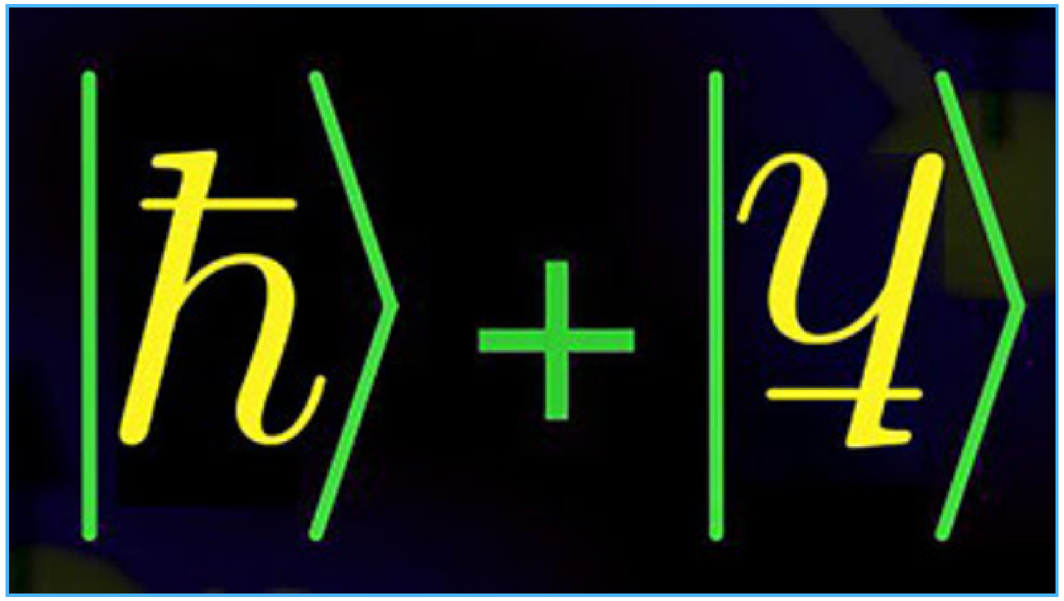
Course Home

2.3.1 What is a quantum internet?

Course subject(s) #MODULE 2: DIVING DEEPER IN THE CONCEPTS OF QUANTUM COMPUTING AND QUANTUM INTERNET

Just like a classical internet a quantum internet consists of computers attached to an internet. In the

Home > All Subjects > Computer Science > Quantum Information Science I, Part 1



Quantum Information Science I, Part 1

Want to learn about quantum bits, quantum logic gates, quantum algorithms, and quantum communications, and know some linear algebra but haven’t yet learned much about quantum mechanics? This is the course for you!

Massachusetts Institute of Technology

Meet the instructors

Isaac Chuang
Professor of Electrical Engineering and Computer Science, and Professor of Physics
Massachusetts Institute of Technology

Peter Shor
Morss Professor of Applied Mathematics and Chair of the Applied Mathematics Committee
Massachusetts Institute of Technology

https://www.edx.org/course/quantum-information-science-i

I R T F

We have created a Research Group (RG) on Quantum Internet inside the Internet Research Task Force (IRTF). Co-chairs are Van Meter (Keio) and Stephanie Wehner (TU Delft).
https://www.irtf.org/mailman/listinfo/qirg

236 list members (as of 2019/3/18)


https://www.wqrn.org
Workshop for Quantum Repeaters and Networks
Top
WQRN
Join us in Japan in 2019
Apply
Committees
Previous WQRNs
FAQ
Contact Us
Workshop for Quantum Repeaters and Networks
n.b.: Dates still tentative
Join us in Japan, Sept. 5-6, 2019
Beginning with dinner on the 4th, ending at breakfast on the 7th.
More details coming soon.
Note that dates are still tentative.

Done!

Any questions you haven't asked yet?

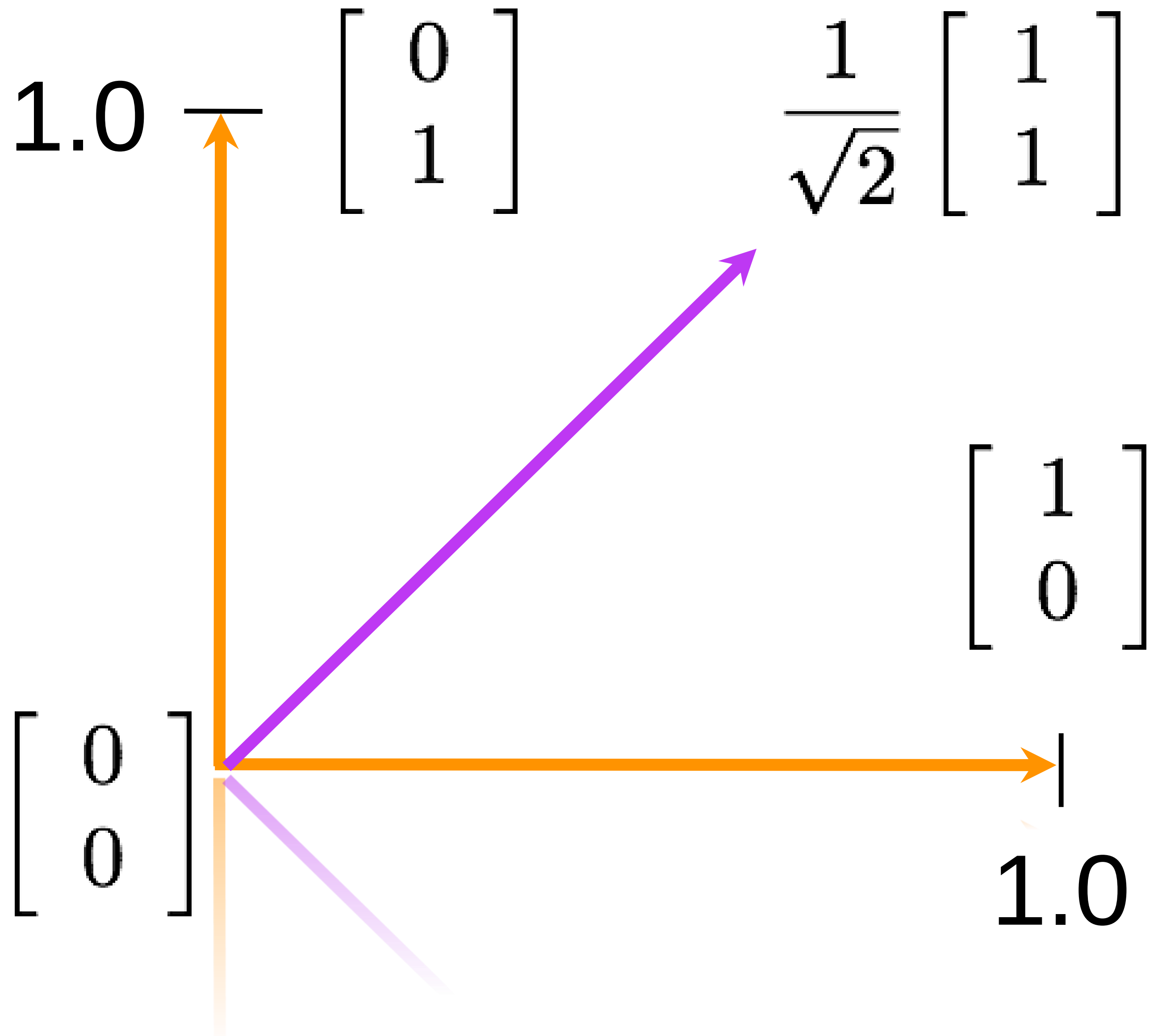
Appendices

- Vectors, Matrices, Dirac’s bra-ket notation, and Complex Numbers
- Quantum States
- Single-Qubit Gates
- Two-Qubit Gates
- Density Matrix
- Teleportation by the numbers

Vectors, Matrices,
Dirac’s bra-ket notation, and
some complex numbers

Vectors

A vector has a direction and a distance. It can be described via a set of coordinates, assuming the vector starts at the origin.



Dirac’s Bra-ket Notation

ket

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = ?$$

Dirac's Bra-ket Notation

ket

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} =? \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} =?$$

Dirac's Bra-ket Notation

bra

ket

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \equiv \langle 0|$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \equiv \langle 1|$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}\langle 0| + \frac{1}{\sqrt{2}}\langle 1|$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\begin{bmatrix} \alpha & \beta \end{bmatrix} =?$$

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} =?$$

Vector Addition

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\psi\rangle + |\phi\rangle = \begin{bmatrix} \alpha + \gamma \\ \beta + \delta \end{bmatrix}$$

$$|\phi\rangle = \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$$

Vector Inner Product

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$\langle\phi|\psi\rangle = \alpha\gamma + \beta\delta$$

$$\langle\phi| = \begin{bmatrix} \gamma & \delta \end{bmatrix}$$

Matrix

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$$

$$B = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

n.b.: It’s more standard to start index at 1, but 0 will be more convenient here.

Matrix Addition

$$A + B = \begin{bmatrix} a_{0,0} + b_{0,0} & a_{0,1} + b_{0,1} & a_{0,2} + b_{0,2} & a_{0,3} + b_{0,3} \\ a_{1,0} + b_{1,0} & a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} & a_{1,3} + b_{1,3} \\ a_{2,0} + b_{2,0} & a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} & a_{2,3} + b_{2,3} \\ a_{3,0} + b_{3,0} & a_{3,1} + b_{3,1} & a_{3,2} + b_{3,2} & a_{3,3} + b_{3,3} \end{bmatrix}$$

Multiplying a vector by a matrix

$$A|\psi\rangle = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$= \begin{bmatrix} a_{0,0}\alpha + a_{0,1}\beta \\ a_{1,0}\alpha + a_{1,1}\beta \end{bmatrix}$$

Complex numbers

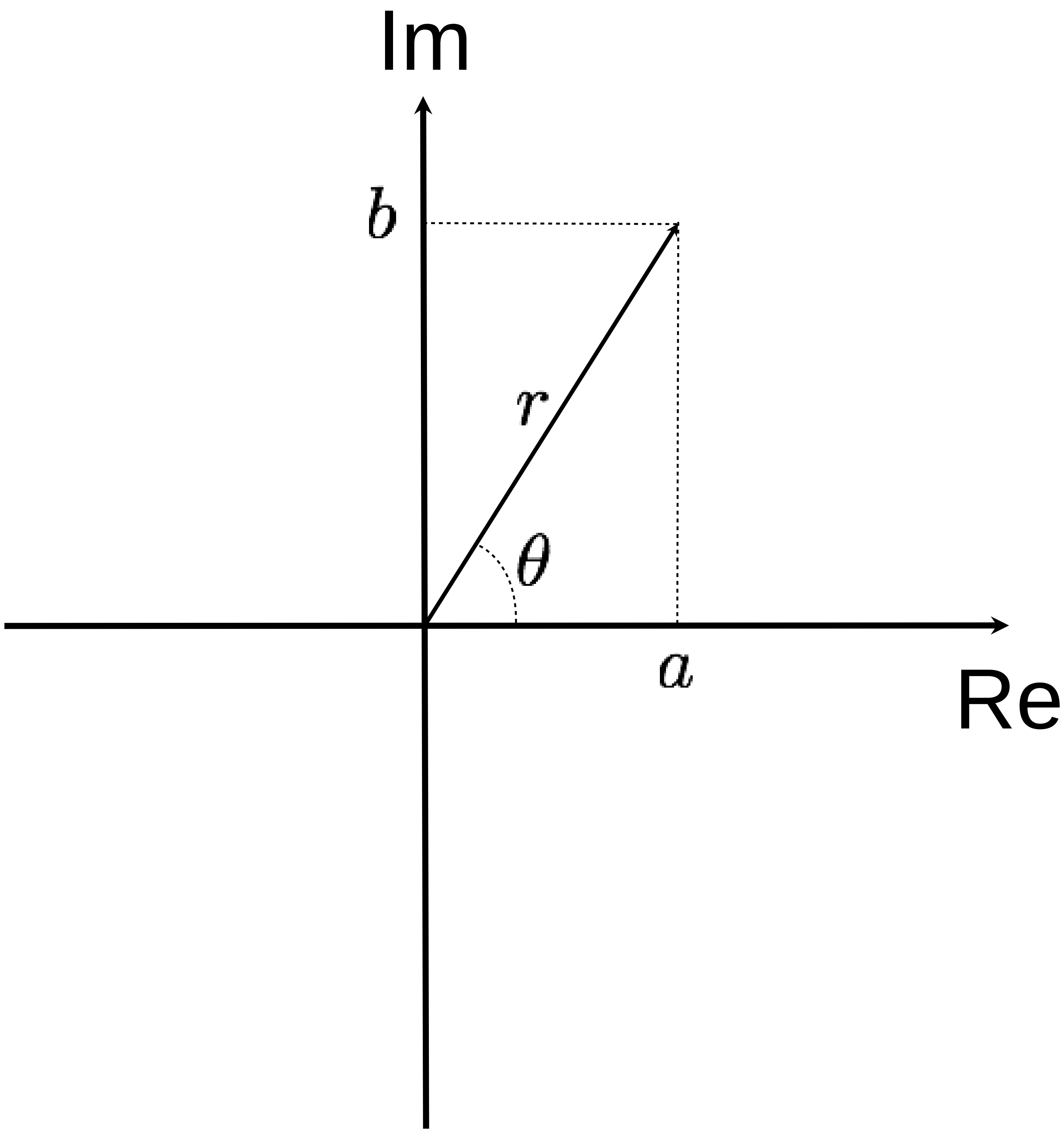
Quantum physics contains complex numbers so that

Quantum information is consist of complex numbers.

$$i = \sqrt{-1}$$

$$\underbrace{a}_{\text{real part}} + \underbrace{bi}_{\text{imaginary part}}$$

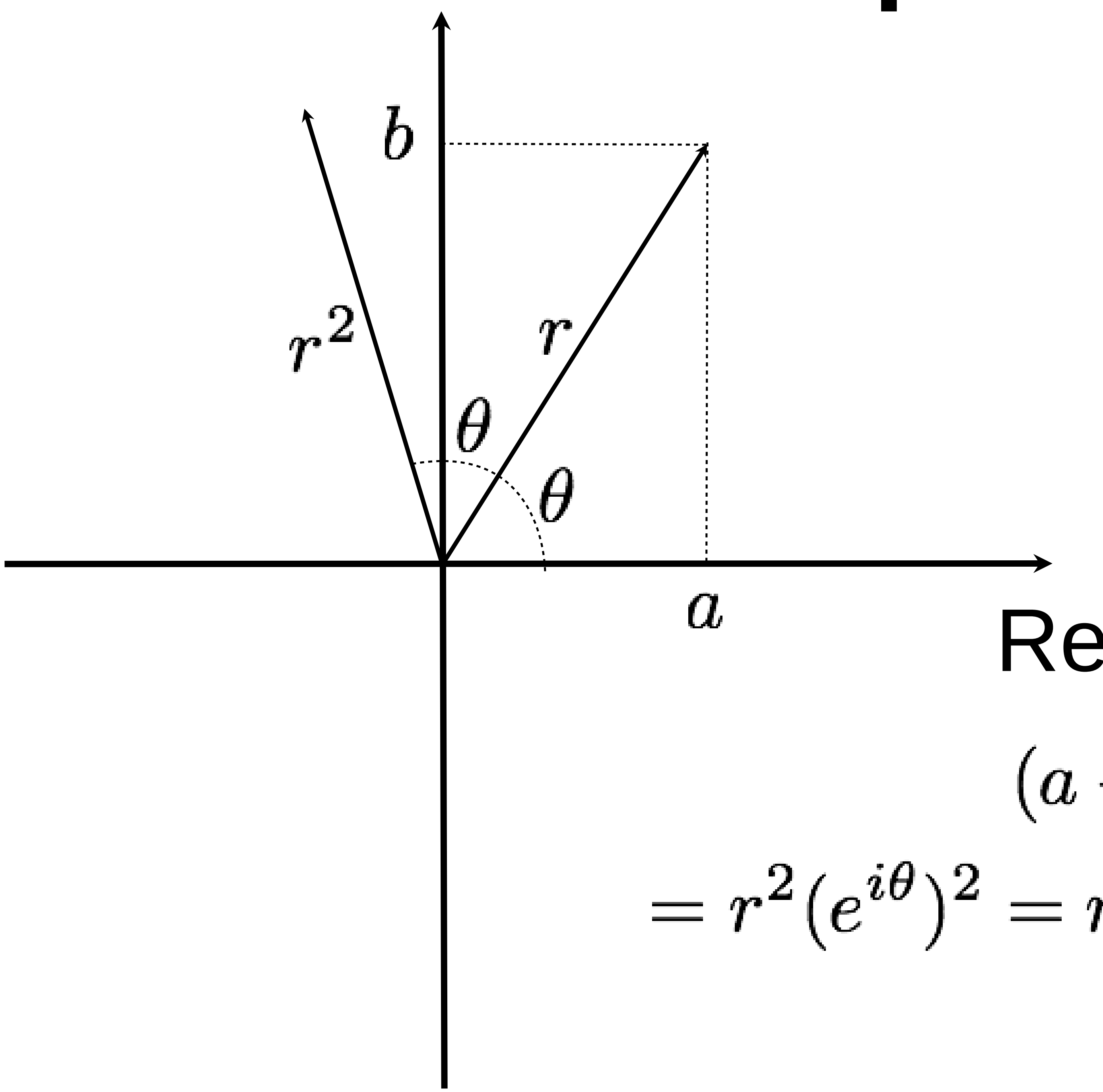
Complex plane



$$a + bi = r(\cos\theta + i\sin\theta)$$
$$= re^{i\theta}$$

Euler's formula

Exponentiating complex numbers



$$a + bi = r(\cos\theta + i\sin\theta)$$
$$= re^{i\theta}$$

Euler's formula

$$(a + bi)^2 = (r(\cos\theta + i\sin\theta))^2$$
$$= r^2(e^{i\theta})^2 = r^2 e^{i2\theta} = r^2(\cos 2\theta + i\sin 2\theta)$$

De Moivre's formula

Complex Numbers in Bra-ket

Earlier presentation wasn't quite complete!

$$|\psi\rangle = \left[\begin{array}{c} \alpha \\ \beta \end{array} \right]$$

$$\langle\psi|\psi\rangle = \alpha\alpha^* + \beta\beta^*$$

$$= a^2 + b^2 + c^2 + d^2$$

$$\langle\psi| = \left[\begin{array}{cc} \alpha^* & \beta^* \end{array} \right]$$

$$\alpha = a + ib$$

$$\alpha^* = a - ib$$ complex conjugate

$$\beta = c + id$$

$$\beta^* = c - id$$

Vector Outer Product

$$|\psi\rangle\langle\phi| = \begin{bmatrix} \alpha\gamma^* & \alpha\delta^* \\ \beta\gamma^* & \beta\delta^* \end{bmatrix}$$

Same thing as tensor!

...what's a tensor?

Tensor Product

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \qquad B = \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix}$$

$$A \otimes B = \left(\begin{array}{cc} a_{0,0} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} & a_{0,1} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} \\ a_{1,0} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} & a_{1,1} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} \end{array} \right)$$

Tensor Product

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$I \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

$$H \otimes H = ?$$

Quantum States

Writing quantum states

To write a quantum state we use a **ket vector**:

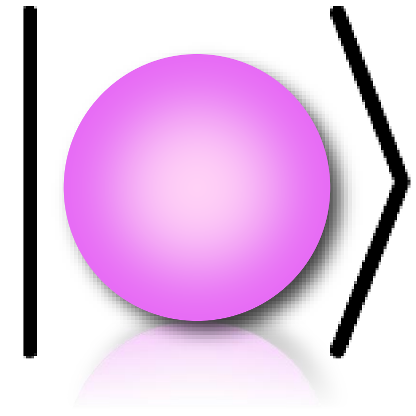
$$|A\rangle$$

This is “the state of system A”.

We can put many things inside kets...

Writing quantum states

To write a quantum state we use a **ket vector**:



We can put many things inside kets...

Writing quantum states

To write a quantum state we use a **ket vector**:

$$|\psi\rangle$$

We can put many things inside kets...

Writing quantum states

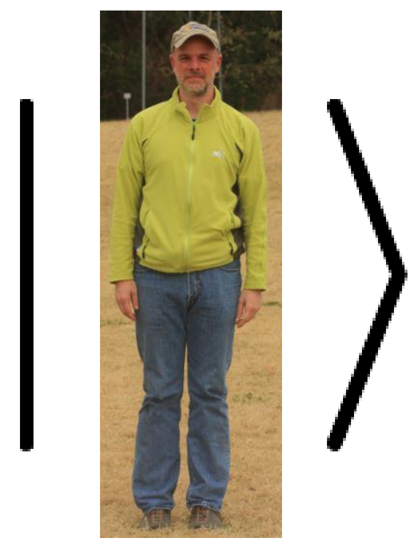
To write a quantum state we use a **ket vector**:

$$|\uparrow\rangle$$

We can put many things inside kets...

Writing quantum states

To write a quantum state we use a **ket vector**:



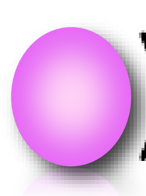
We can put many things inside kets...

Writing quantum states

Ket vectors tell us the probability of measuring the state.

Suppose we just have two outcomes: 0 and 1.

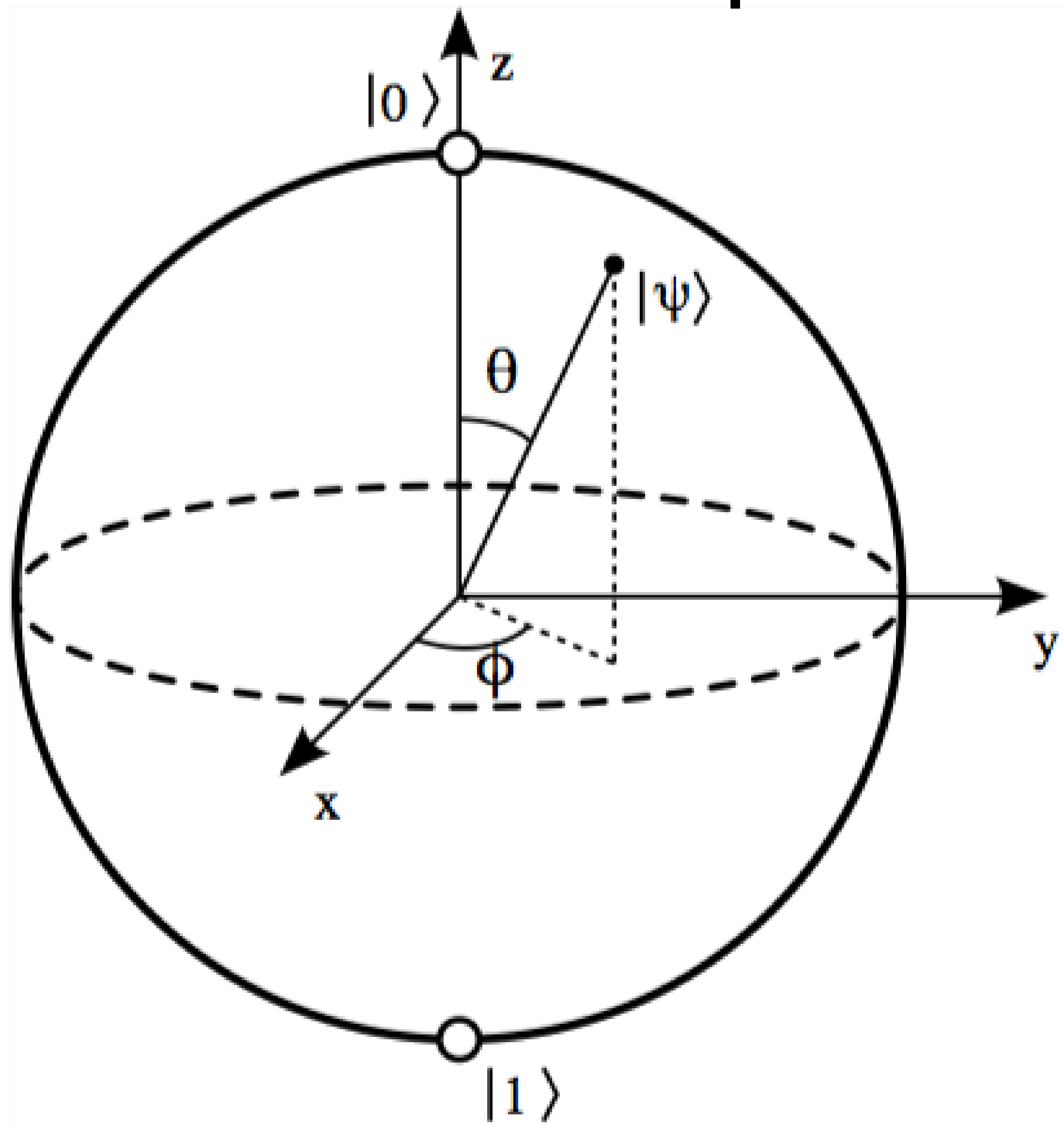
A ket vector for the system could be written

$|$$\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$

What does this mean?

Bloch Sphere

$|0\rangle$ is up here



Question: Where are

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

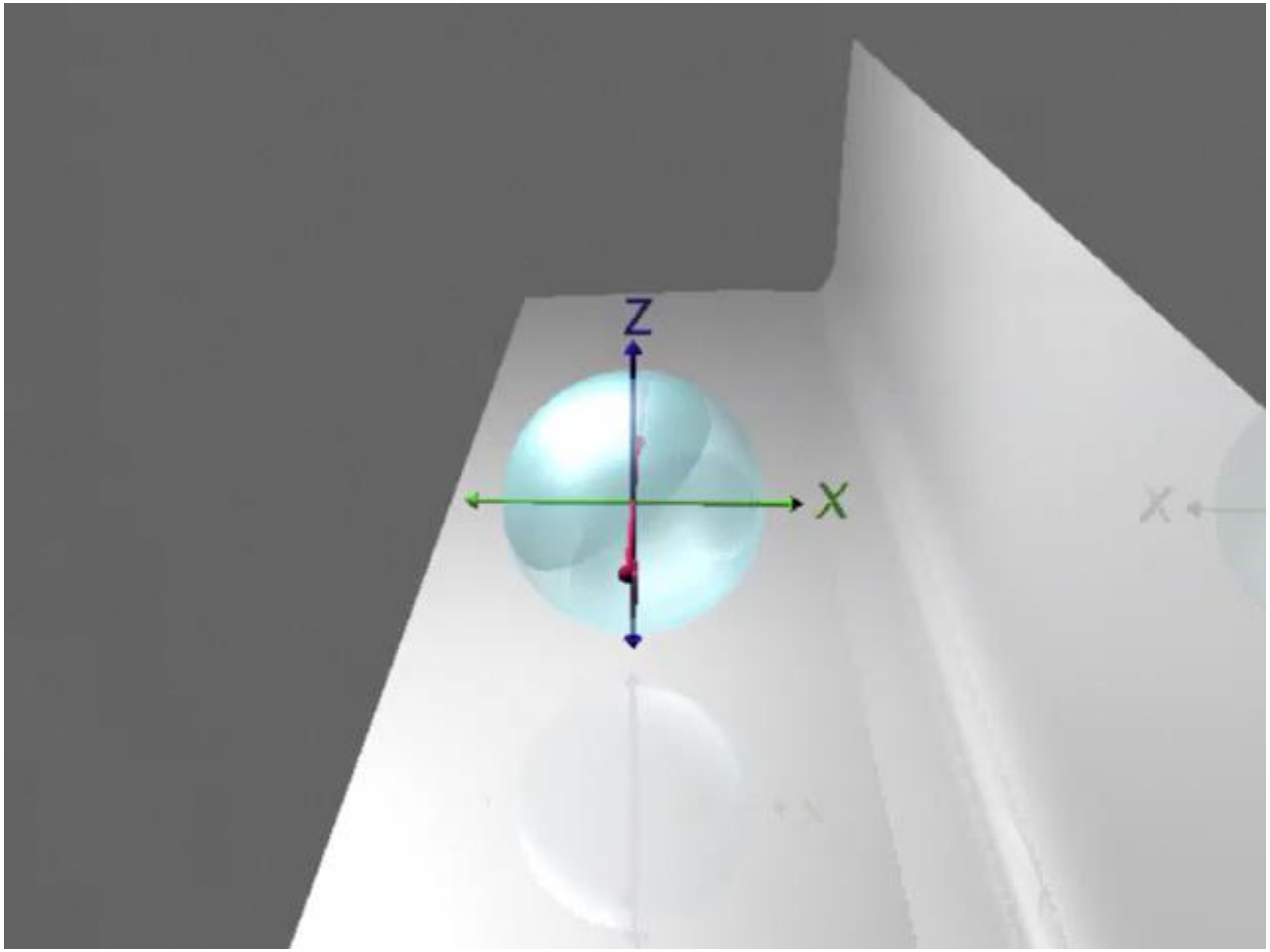
$$\frac{|0\rangle + i|1\rangle}{\sqrt{2}} \qquad \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

Note: This is not (usually) directly relatable to something physical!

$|1\rangle$ is down here

Image from Wikipedia

Bloch Sphere



Phase

Phase, then, is position about the vertical axis on the Bloch sphere.
You can’t touch it, see it, smell it, taste it, or hear it.
It doesn’t “mean” anything.

...but you can calculate using it.

The *Z* Gate

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Question: What does this do to this state?

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Question: What does this do to any observation or measurement we make?

Multiple Qubits: Hilbert Space is a Very Big Place

n qubits can be in 2^n possible states: 000..00, 000..01, 000..10, ..., 111...10, 111..11

In fact, it can be in a superposition of all of those states at once:

$$|\psi\rangle = \sum_{i=0}^{2^n} \alpha_i |i\rangle$$

State Vector for Two & Three Qubits

$$|\psi\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \begin{matrix} \leftarrow \text{amplitude of } 00 \\ \leftarrow \text{amplitude of } 01 \\ \leftarrow \text{amplitude of } 10 \\ \leftarrow \text{amplitude of } 11 \end{matrix}$$

Question: How many elements are there in an *n*-qubit state vector?

$$|\psi\rangle = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

Hilbert Space

Each element of the state vector is a *basis vector*. The total set is *Hilbert space*, and it grows exponentially with the number of qubits!

n.b.: Each individual qubit has two states, or two basis vectors, but they are *multiplicative* when combined -- adding a qubit *adds dimensions* to the total size of our space!

$$|\psi\rangle = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

Bell States: Our First Important Multi-Qubit States

$$|\Phi^+\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \qquad |\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

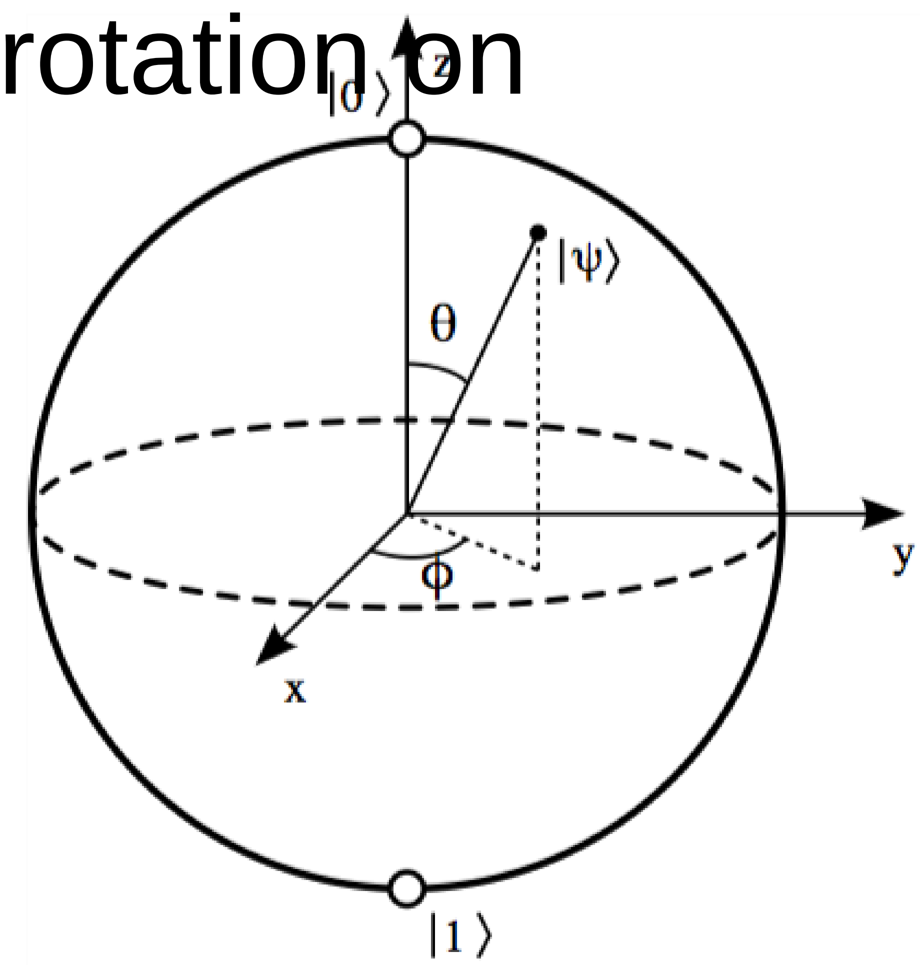
$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Critical for quantum communication

Foundation for tests of entanglement
(CHSH inequality, a little later)

Quantum gates

- All quantum gates are unitary.
- What’s unitary?
  - said simply, reversible rotation on Hilbert space



Simple single-qubit gates

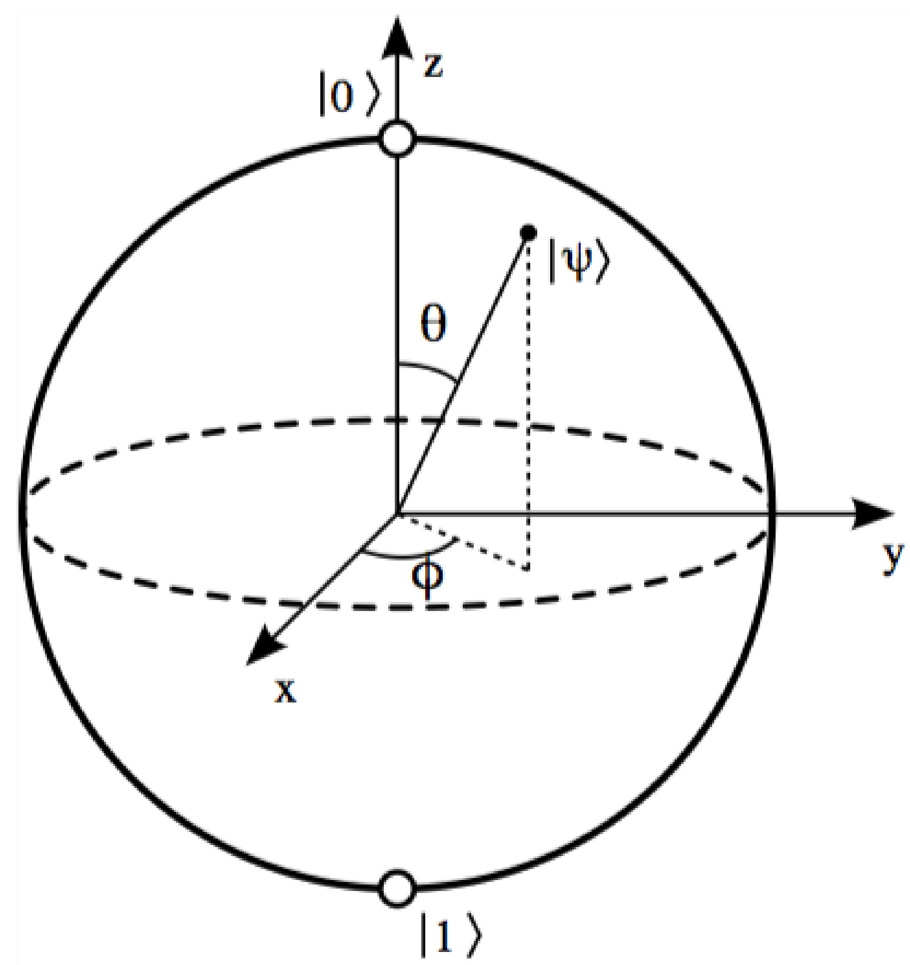
X gate, Z gate

- X gate
  - rotation around X axis

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Z gate
  - rotation around Z axis

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

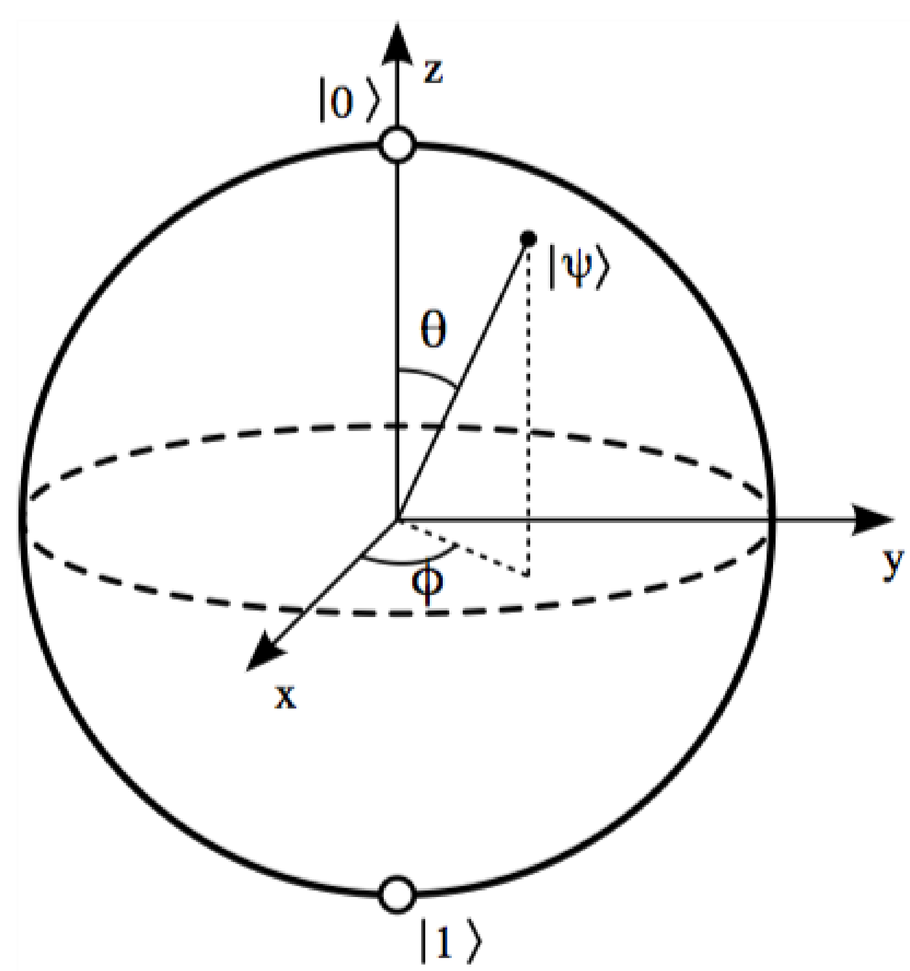


Y gate

- rotation around Y axis

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$i \times X \times Z = ?$$



Global phase

- Global phase does not affect quantum state.

$$|\phi\rangle = e^{i\theta}(a|0\rangle + b|1\rangle)$$

$$= (e^{i\theta}a|0\rangle + e^{i\theta}b|1\rangle)$$

$$|e^{i\theta}a|^2 = |a|^2$$

$$|e^{i\theta}b|^2 = |b|^2$$

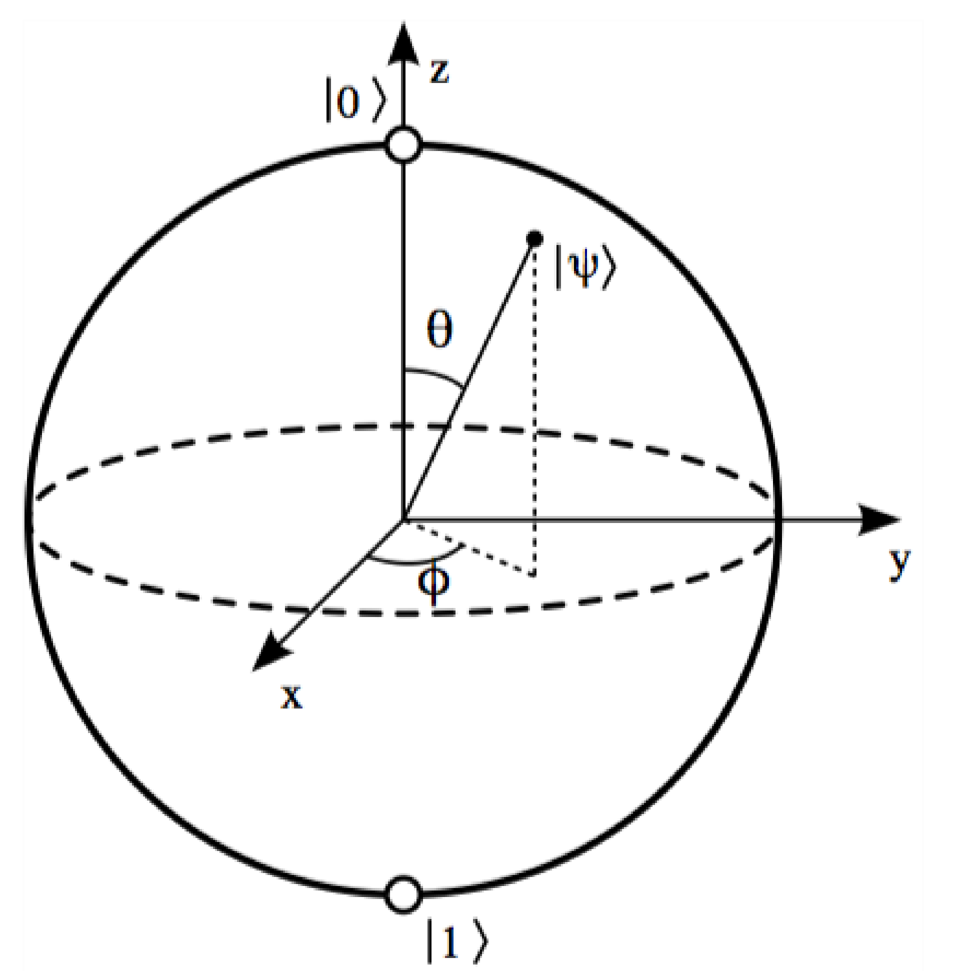
($\because$ $e^{i\theta}$ is rotation whose norm is 1 around origin,
it does not change the distance from the origin)

Y gate

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- rotation around Y axis

$$i \times X \times Z =?$$

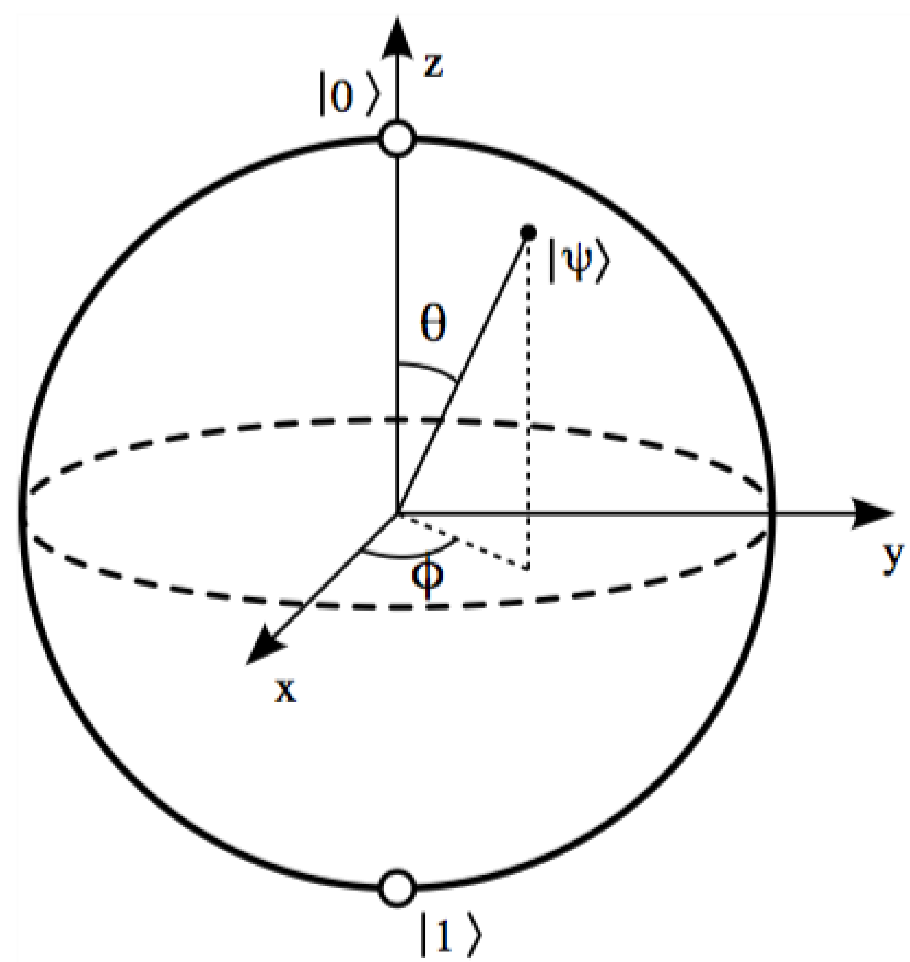


Y gate

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- rotation around Y axis

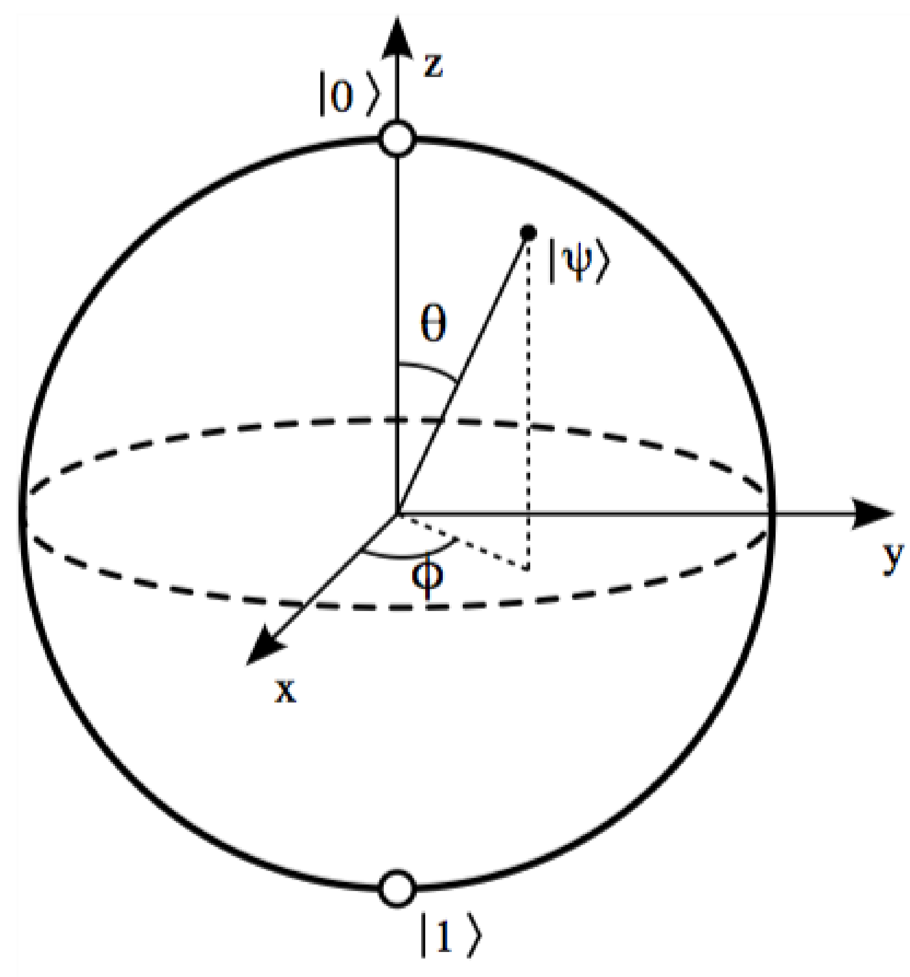
$$i \times X \times Z = i \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$= i \times \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$



Y gate

- rotation around Y axis $$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$
- can be created by multiplying X and Z

$$i \times X \times Z = i \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$= i \times \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$



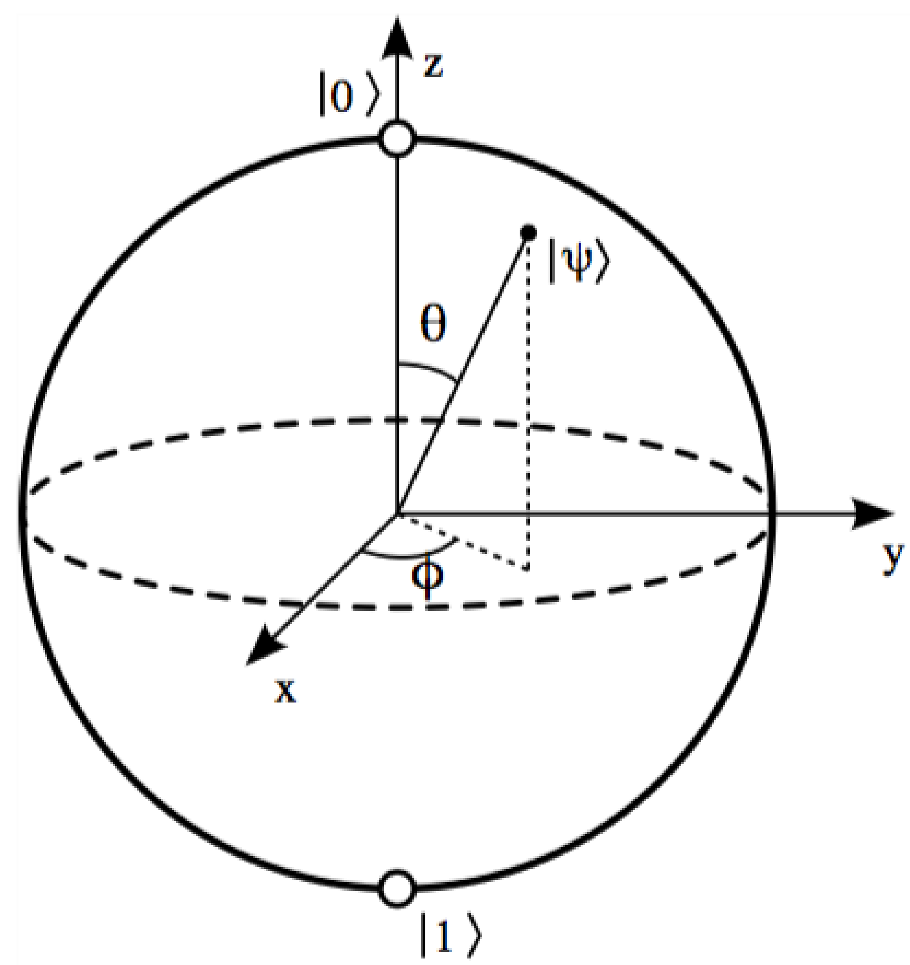
Pauli gates

- X, Y, Z are called the Pauli matrices (Pauli gates), which are the most basic gates.

I gate

- I gate
  - Identity gate, which does not change quantum state

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



H gate

- H gate exchanges the relationship between X axis and Z axis

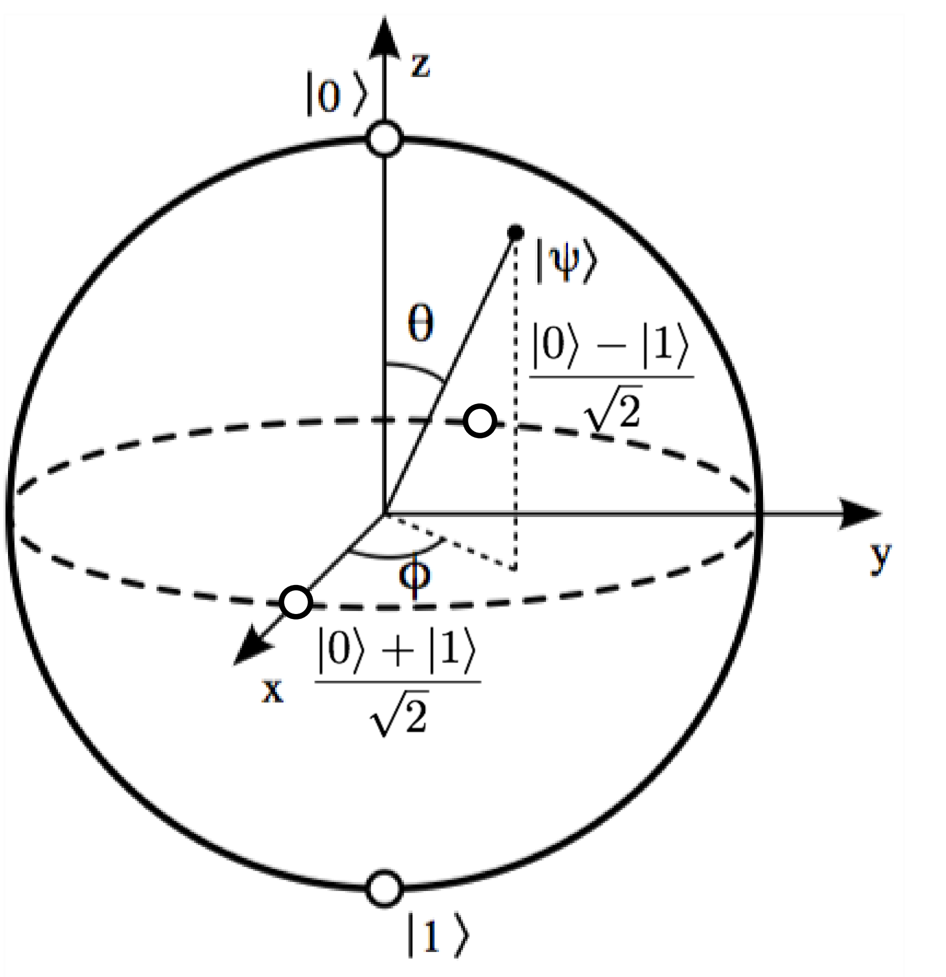
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H \times |0\rangle = ?$$

$$H \times |1\rangle = ?$$

$$H \times \frac{|0\rangle + |1\rangle}{\sqrt{2}} = ?$$

$$H \times \frac{|0\rangle - |1\rangle}{\sqrt{2}} = ?$$



H gate

- H gate exchanges the relationship between X axis and Z axis

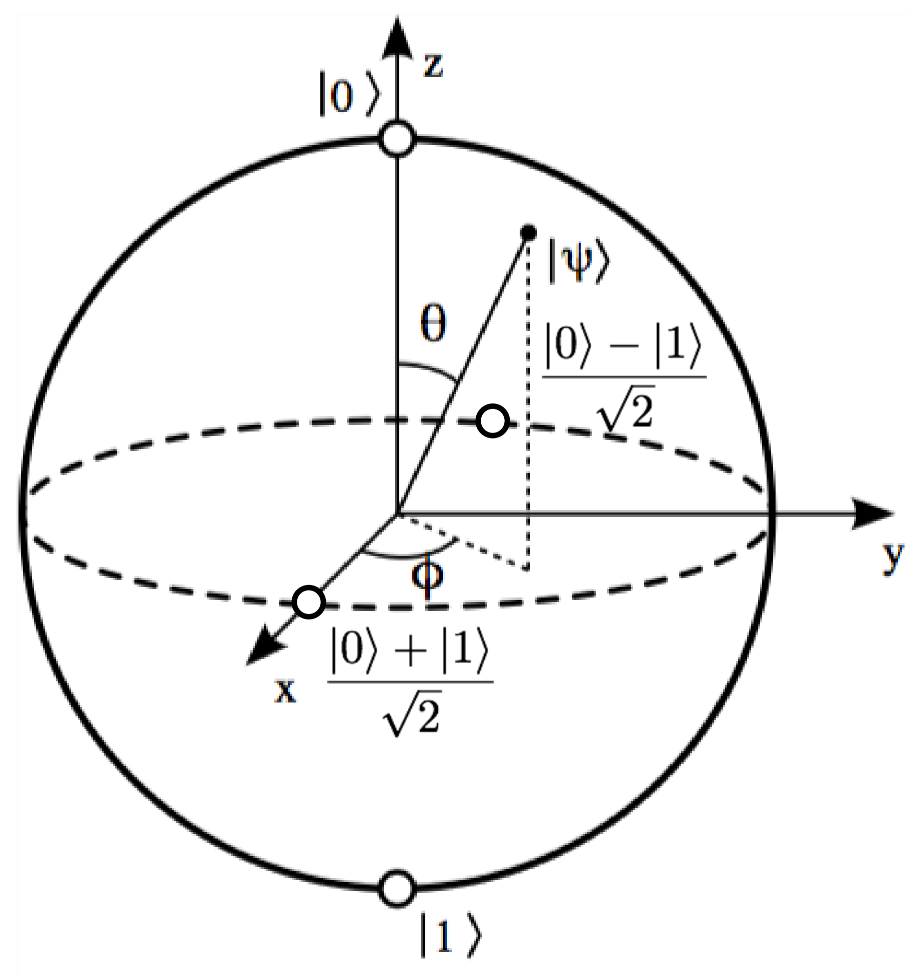
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

$$H \times |0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H \times |1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$H \times \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix} = |0\rangle$$

$$H \times \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix} = \begin{pmatrix}0\\ 1\end{pmatrix} = |1\rangle$$



Simple two-qubits gates

Controlled NOT (CNOT)

- In fact, it is more correct to call controlled X
- If the first qubit is 1, the second qubit gets X
  - the first qubit is control qubit
  - the second is target qubit

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

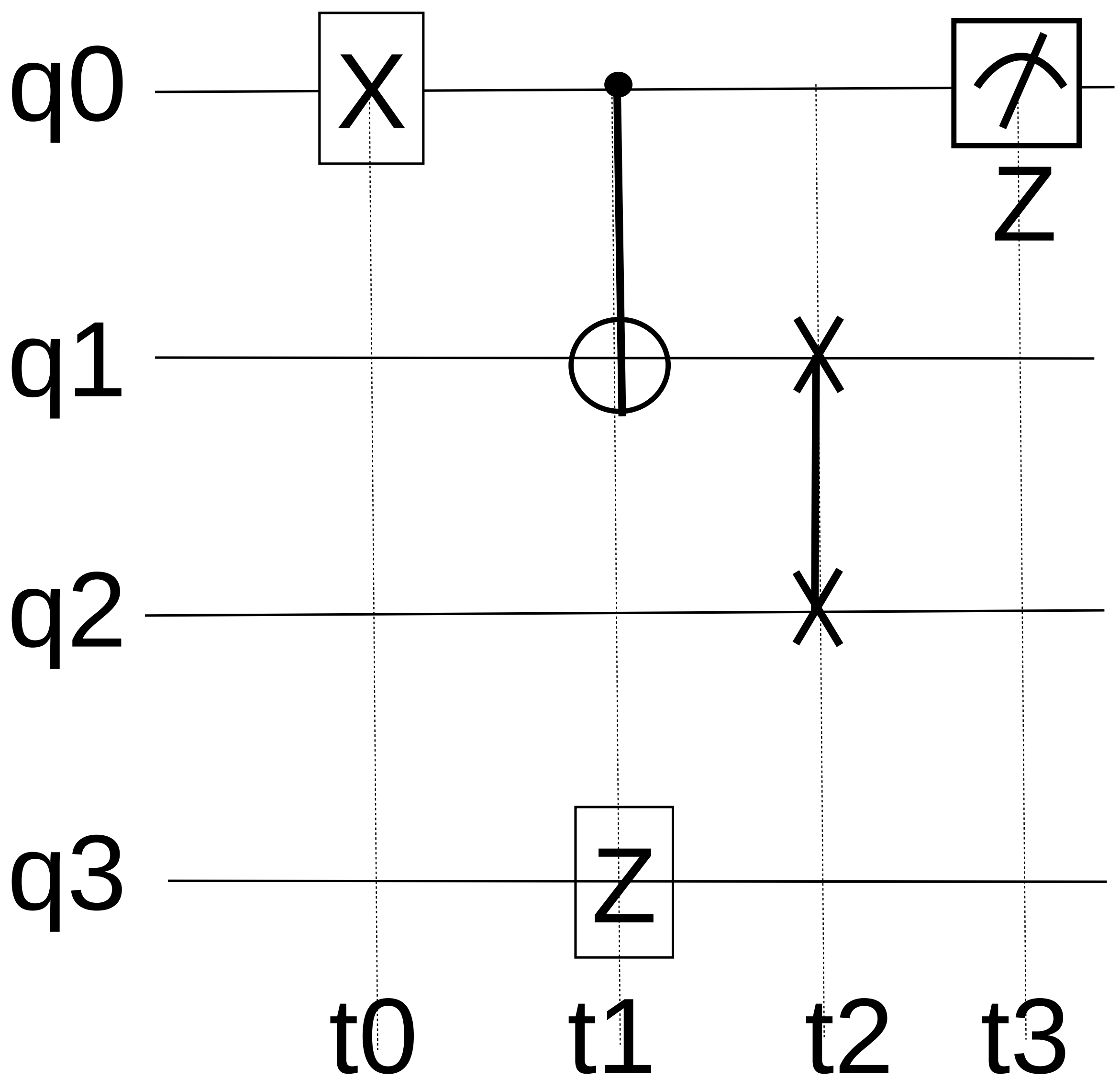
Controlled NOT (CNOT)

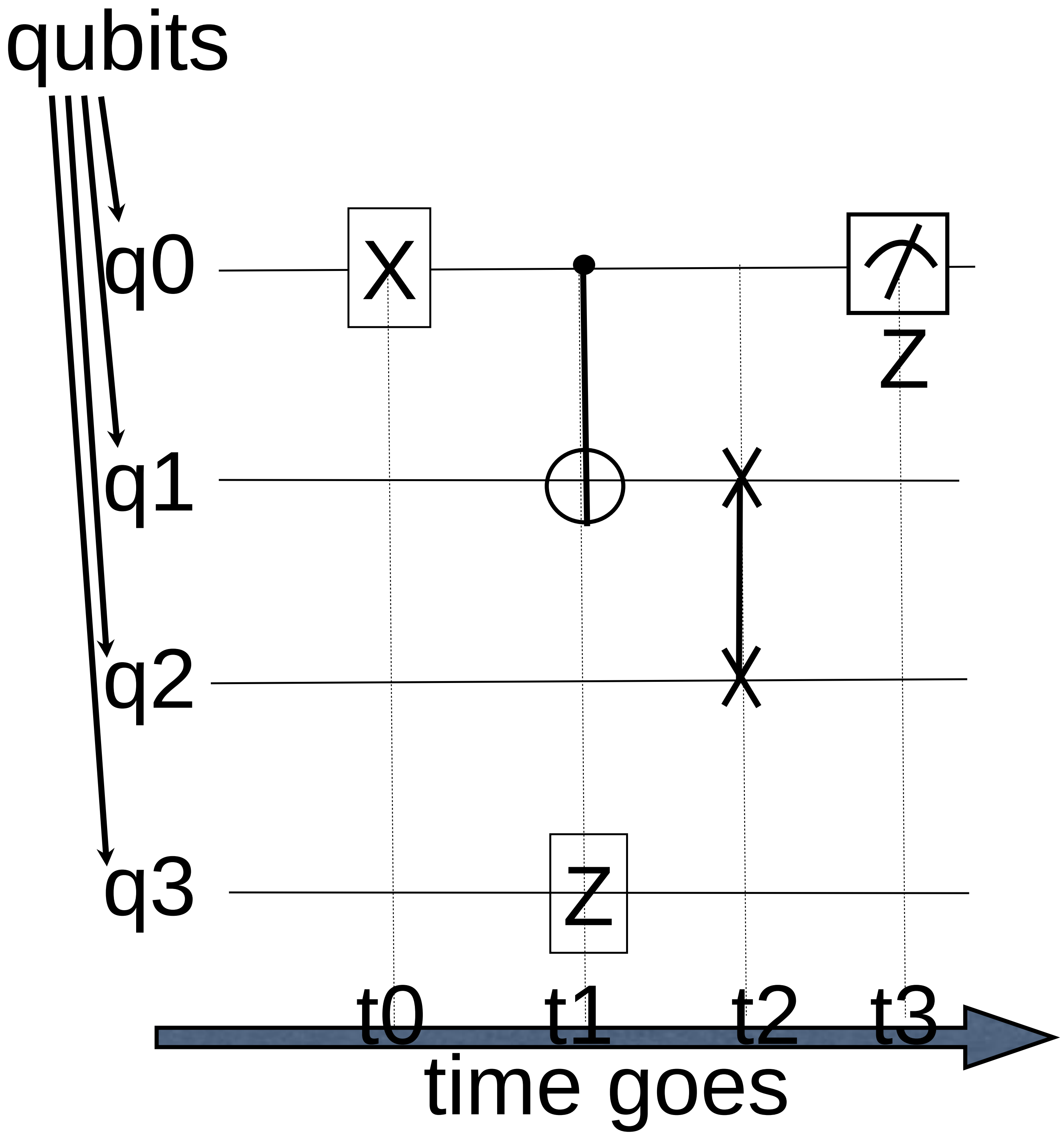
- two qubit state

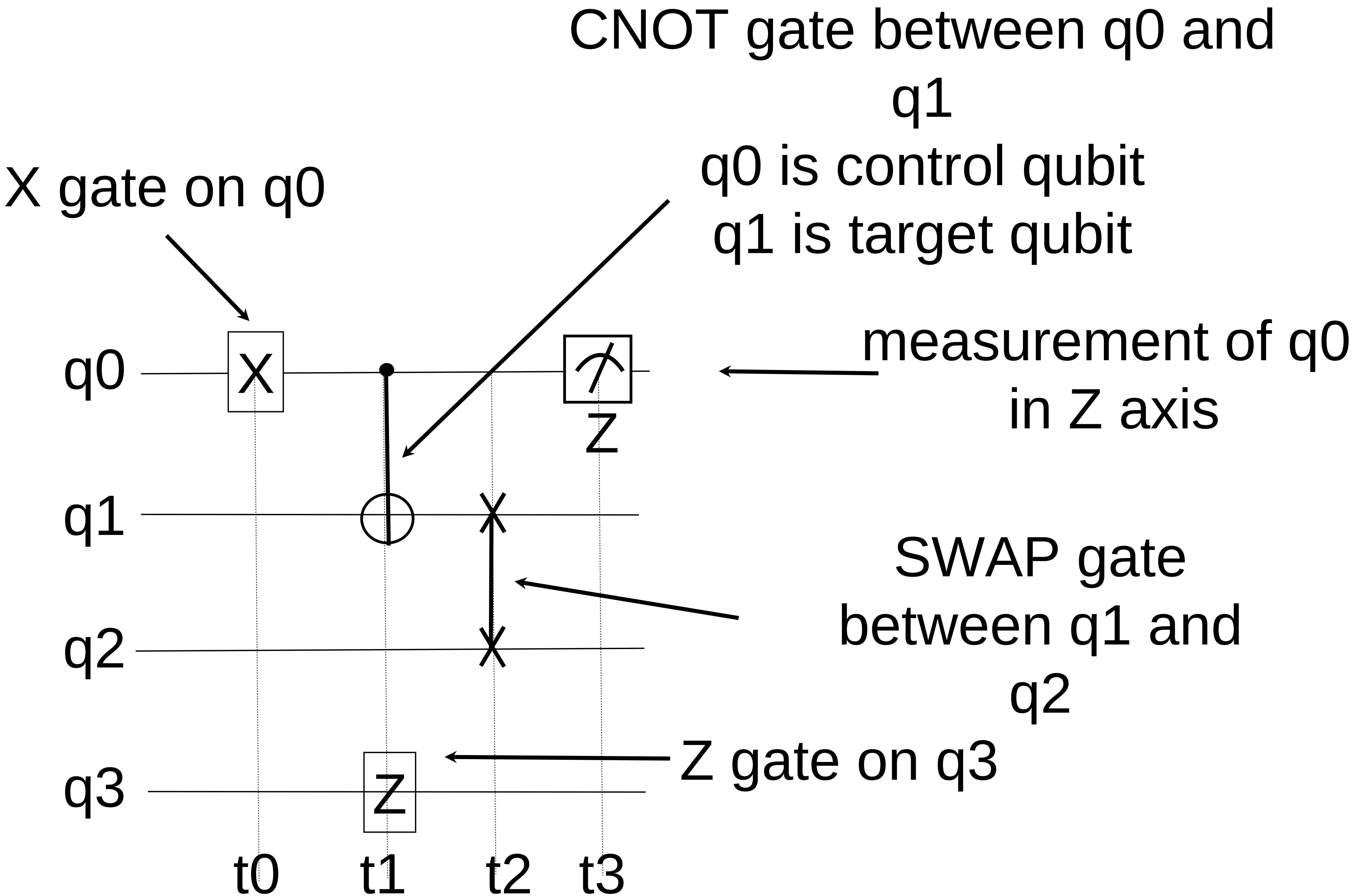
$$\begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix} \Rightarrow \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

$$CNOT \times \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}$$

Circuit notation


q0
q1
q2
q3
X
Z
Z
t0
t1
t2
t3


qubits
q0
q1
q2
q3
X
Z
Z
t0
t1
t2
t3
time goes


CNOT gate between q0 and q1
q0 is control qubit
q1 is target qubit
X gate on q0
q0
X
measurement of q0, in Z axis
Z
q1
SWAP gate between q1 and q2
q2
Z gate on q3
q3
Z
t0
t1
t2
t3

Density Matrix Representation

Pure vs. mixed states

When A is part of a larger superposition, we need to know the state of **both A and B** to fully know the state of A.

If we **do not have access** to the state of B, then we have **lost information about A**.

Pure vs. mixed states

If we **do not have access** to the state of B, then we have **lost information about A**.

If we have **full information** about A then we say "A is in a **pure state".**

If we **do not** have full information about A then "A is in a **mixed state".**

Note: we can have full information about a superposition! $|+\rangle$ is still a "pure state".

Pure vs. mixed states

Pure states (full information) are written as state vectors, $|\Psi\rangle$.

How do we write mixed states, where we have lost some of the state information?

...

Representing mixed states

Representing mixed states

Density matrices let us deal with **uncertainty in the quantum state**.

This uncertainty comes about because the state we want is part of a larger superposition, which we do not have access to.

Density matrices record the **probability of measurement outcomes**.

Representing mixed states

Look again at the state

$$|AB\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

We can write the state of A using the **density matrix** ρ_A :

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Representing mixed states

$$|AB\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Probability of measuring "0"

Probability of measuring "1"

So **diagonal elements always add up to 1**.

Representing mixed states

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We find the probabilities of other measurements by **changing the basis**.

Let’s find the probability of measuring “+” or “-” given this density matrix for the state.

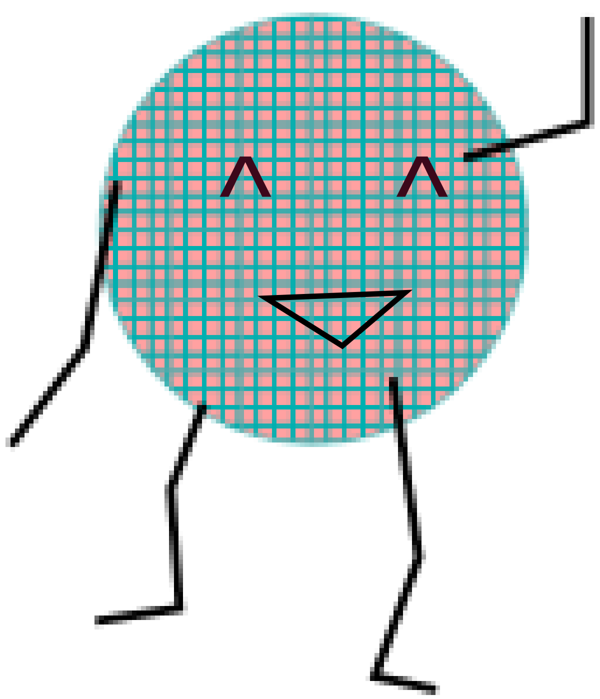
Representing mixed states

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Let’s find the probability of measuring “+” or “-” given this density matrix for the state.

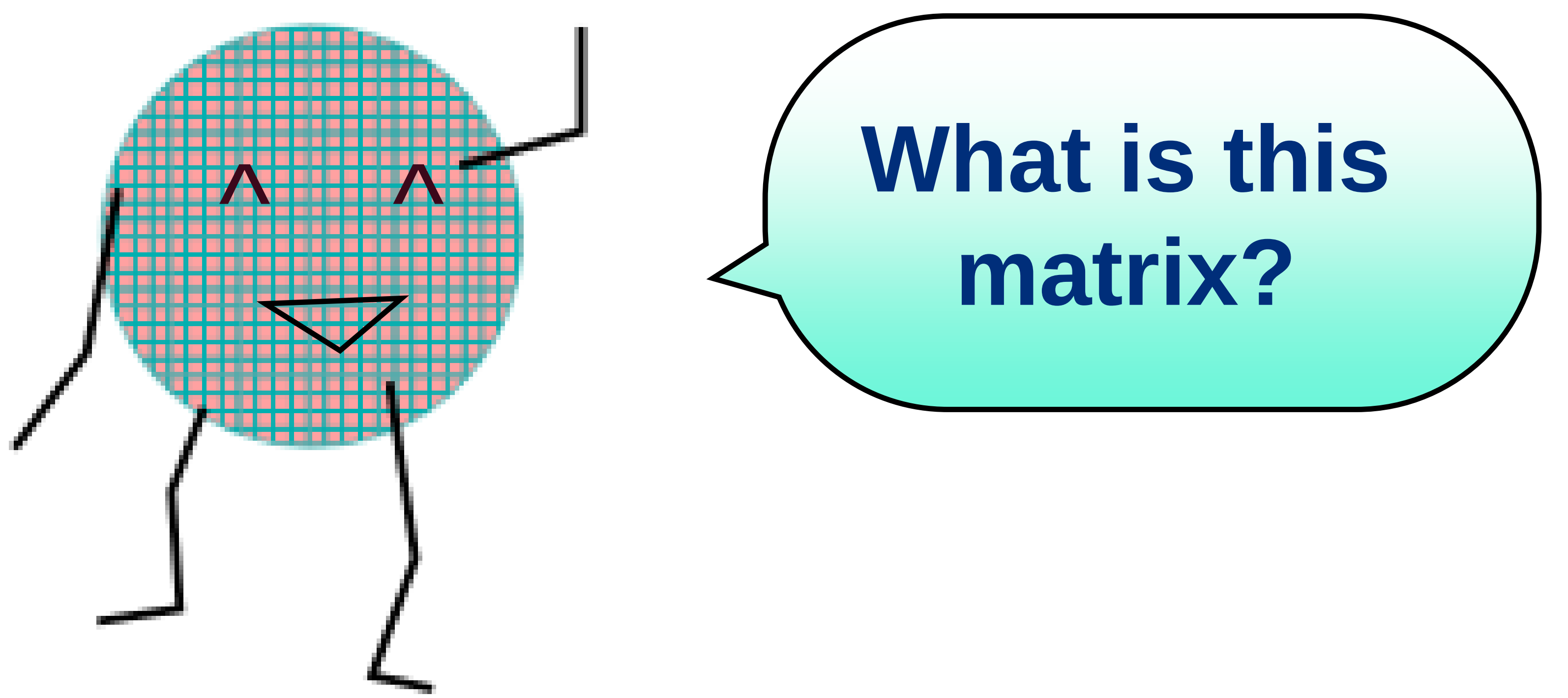


Which operator transforms us to the {|+>,|->} basis?

Representing mixed states

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\rho_A^{Hadamard} = H\rho_A H$$



Representing mixed states

$$\rho_A = \frac{1}{2}\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right) \qquad H = \frac{1}{\sqrt{2}}\left(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}\right)$$

$$\begin{aligned}\rho_A^{Hadamard} &= H\rho_A H \\ &= \frac{1}{2}\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right)\end{aligned}$$

So prob(0) = prob(1) = prob(+) = prob(-) = 0.5

Representing mixed states

We have see n:
The density matrix gives **probabilities of measuring the basis states**.

We calculate the probabilities for different measurements by **transforming into the basis of that measurement**.

Now: how do we **calculate** a density matrix?

Calculating density matrices

Now: how do we **calculate** a density matrix?

The elements in a density matrix represent **“projection operators”:**

$$\rho = \begin{pmatrix} |0\rangle\langle 0| & |1\rangle\langle 0| \\ |0\rangle\langle 1| & |1\rangle\langle 1| \end{pmatrix}$$

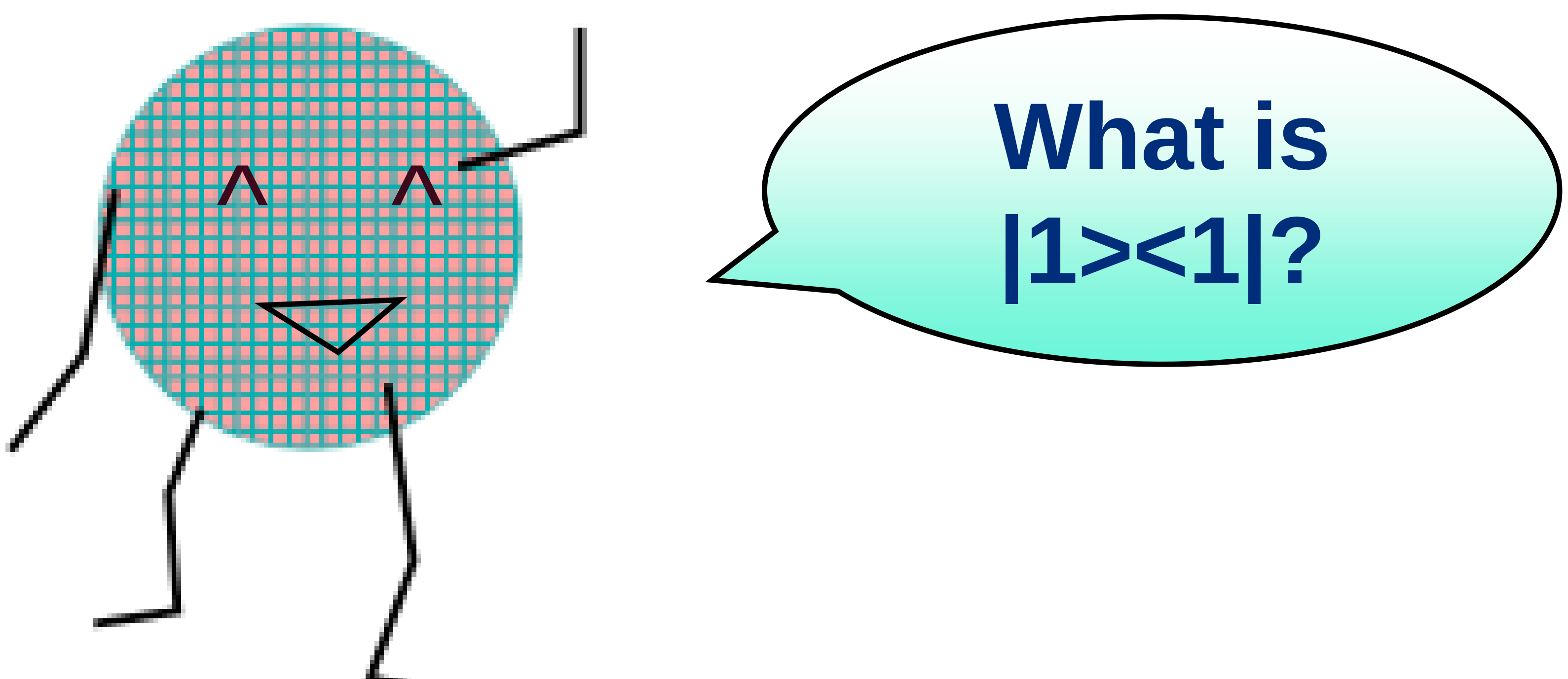
So

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

Calculating density matrices

$$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$



Calculating density matrices

$$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0,1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Calculating density matrices

$$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) = \begin{pmatrix} 1 & \mathbf{0} \\ 0 & \mathbf{0} \end{pmatrix}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0, 1) = \begin{pmatrix} \mathbf{0} & 0 \\ \mathbf{0} & 1 \end{pmatrix}$$

Pure vs mixed states again

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

A **pure state** is represented as a density matrix by a **single** projection operator in some basis,

Pure: $$\rho = |\Psi\rangle\langle\Psi|$$

A **mixed state** is represented as a density matrix by a **sum** of projection operators:

Mixed: $$\rho = \sum_i |\psi_i\rangle\langle\psi_i|$$

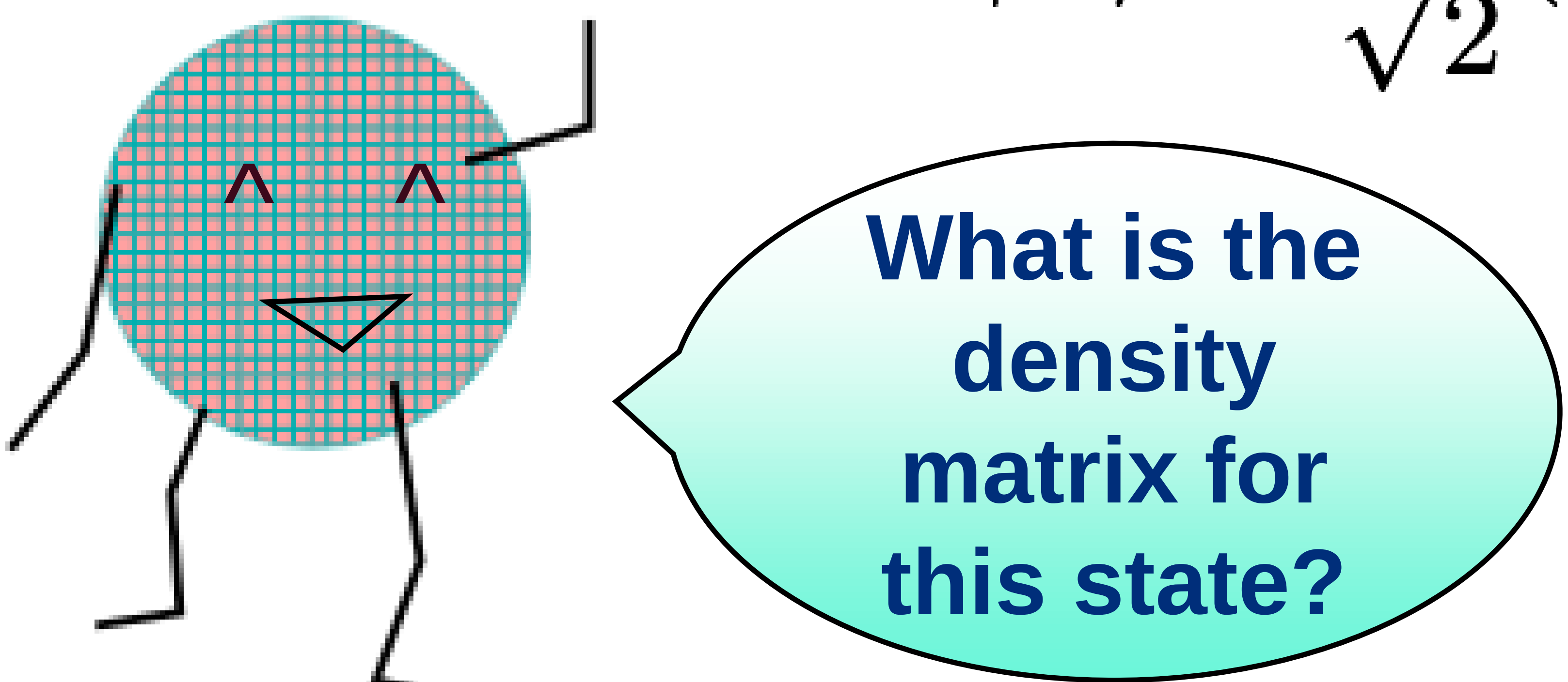
Calculating density matrices

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Pure: $\rho = |\Psi\rangle\langle\Psi|$

Mixed: $\rho = \sum_i |\psi_i\rangle\langle\psi_i|$

Let's look at the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$



Calculating density matrices

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Pure: $\rho = |\Psi\rangle\langle\Psi|$ Mixed: $\rho = \sum_i |\psi_i\rangle\langle\psi_i|$

Let's look at the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Calculating density matrices

Let's look at the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Probability of measuring "0"

Probability of measuring "1"

Diagonal elements are probabilities, and must sum to one!

Off-diagonal elements are called "quantum coherences"

Calculating density matrices

So is this the same thing? Still 50/50…

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

This is just a classical random variable, *not* a superposition!

Representing mixed states

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\rho_A^{Hadamard} = H\rho_A H$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0|$$

50/50 superposition state taken back to 0!

Representing mixed states

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{aligned} \rho_A^{Hadamard} &= H\rho_A H \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

So prob(0) = prob(1) = prob(+) = prob(-) = 0.5!

Summary so far

A system in a mixed state is represented by a **density matrix** rather than a **state vector**.

A pure state $|\Psi\rangle$ has a density matrix $|\Psi\rangle\langle\Psi|$

A mixed state is a sum of pure-state density matrices, $\rho = \sum_i |\psi_i\rangle\langle\psi_i|$

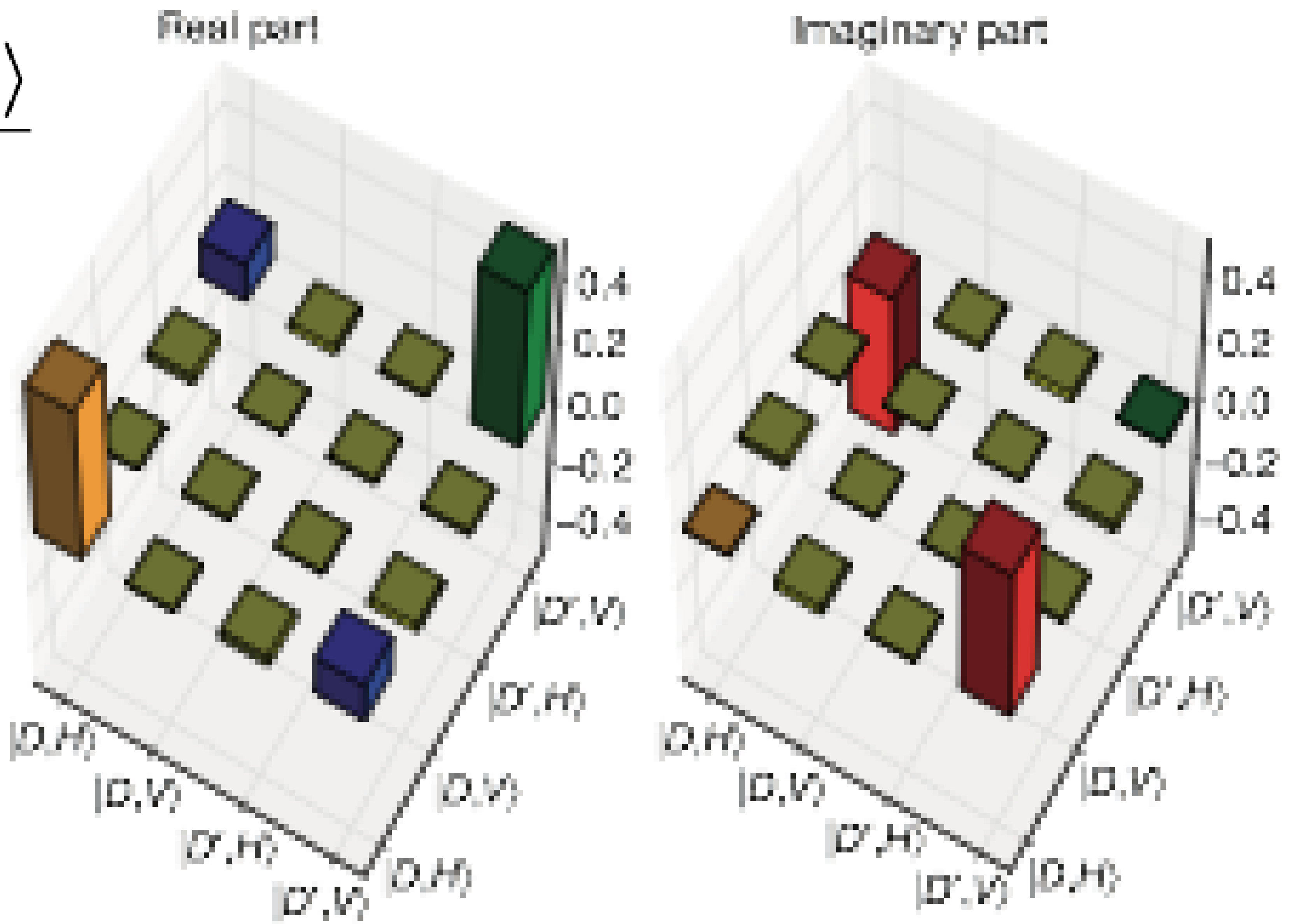
Still to answer: if we have a many-qubit pure state, how can we calculate the density matrices of the individual mixed qubit states?

For example: Experimental Results

$$\frac{|DH\rangle + e^{i\pi/4}|D'V\rangle}{\sqrt{2}}$$

$$F = 0.974 \pm 0.02$$

D and D’ are states of the ion, and H and V are horizontal and vertical polarization of the photon



A. Stute *et al., Nature* 482, 485 (2012)

Teleportation by the numbers

Teleportation By the Numbers (or Symbols)

$$|\psi\rangle_D = \alpha|0\rangle_D + \beta|1\rangle_D \quad |\Phi^+\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

$$\begin{aligned}
|\psi\rangle_D|\Phi^+\rangle_{AB} &= (\alpha|0\rangle_D + \beta|1\rangle_D) \otimes \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}} \\
&= \frac{1}{2}|\Phi^+\rangle_{\boxed{DA}}|\psi\rangle_{\boxed{B}} \\
&\quad + \frac{1}{2}|\Phi^-\rangle_{DA}Z|\psi\rangle_B \\
&\quad + \frac{1}{2}|\Psi^+\rangle_{DA}X|\psi\rangle_B \\
&\quad + \frac{1}{2}|\Psi^-\rangle_{DA}ZX|\psi\rangle_B
\end{aligned}$$

Rewrite (just algebra!) treating DA as a pair

and B as a solo qubit

Teleportation By the Numbers (or Symbols)

$$|\psi\rangle_D|\Phi^+\rangle_{AB} = (\alpha|0\rangle_D + \beta|1\rangle_D) \otimes \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

$$= \frac{1}{2}\boxed{|\Phi^+\rangle_{DA}}\boxed{|\psi\rangle_B}$$

$$+ \frac{1}{2}\boxed{|\Phi^-\rangle_{DA}}\boxed{Z|\psi\rangle_B}$$

$$+ \frac{1}{2}\boxed{|\Psi^+\rangle_{DA}}\boxed{X|\psi\rangle_B}$$

$$+ \frac{1}{2}\boxed{|\Psi^-\rangle_{DA}}\boxed{ZX|\psi\rangle_B}$$

BSM collapses state to *one* of these terms, and tells us which

Leaves something *related* to original *D* on *B*

Question: How do we fix it up?