AQUA

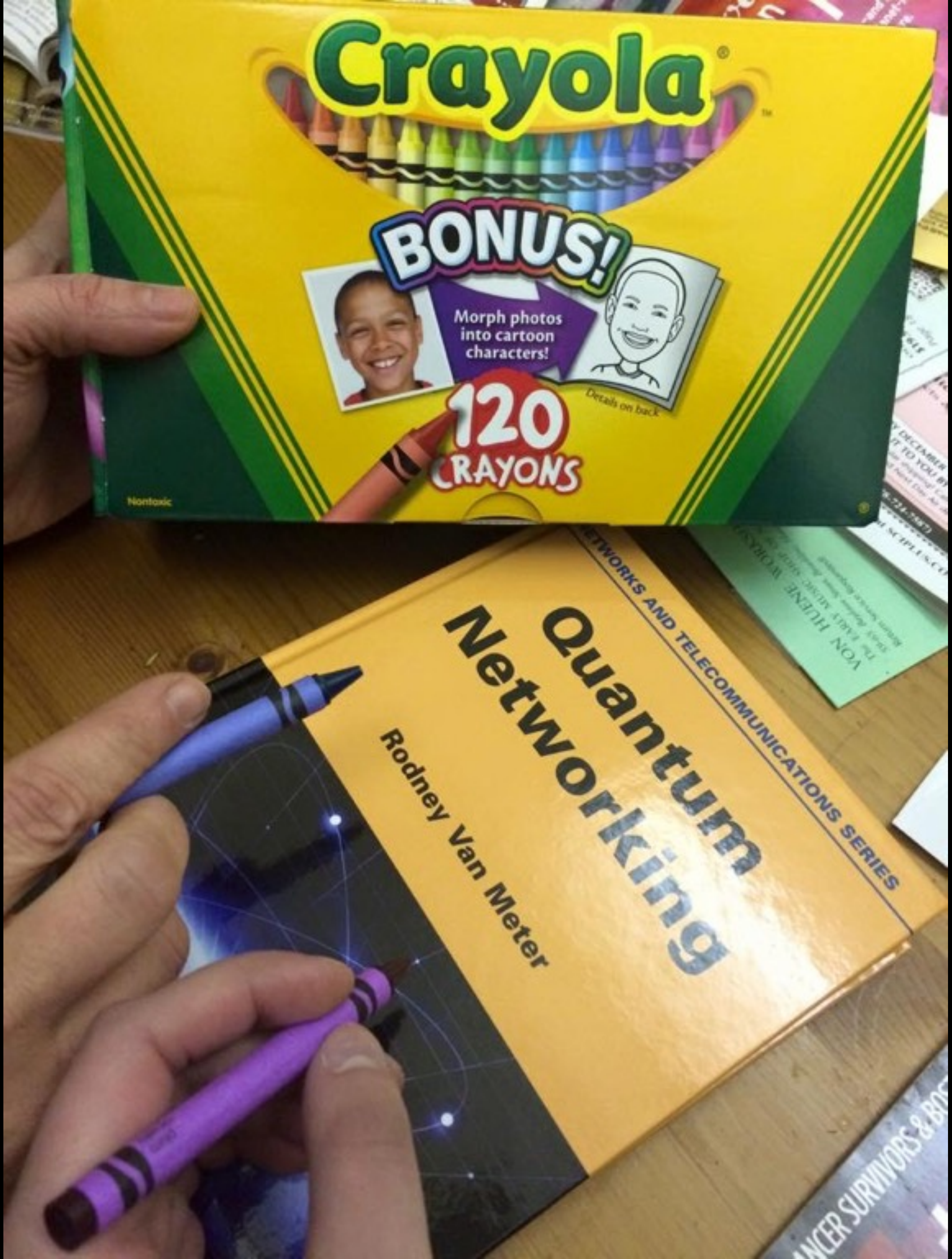
Advancing Quantum Architecture

The Quantum Internet
ザ・量子インターネット

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

Rodney Van Meter
Keio University
@IIJ
2017/5/23

funding provided by:


Crayola
BONUS!
Morph photos into cartoon characters!
Details on back
120 CRAYONS
Nontoxic
ETWORKS AND TELECOMMUNICATIONS SERIES
Quantum Networking
Rodney Van Meter

The Quantum Information Technology Industry

(Over the last couple of years, it has become possible to talk about this.)

"My team has created a very innovative solution, but we're still looking for a problem to go with it."

"...there's a market, there's a hunger for these devices."

Chris Monroe, University of Maryland

http://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one

nature International weekly journal of science

Commercialize early quantum technologies

Masoud Mohseni, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy & John Martinis

03 March 2017

Masoud Mohseni, Peter Read, Hartmut Neven and colleagues at Google's Quantum AI Laboratory set out investment opportunities on the road to the ultimate quantum machines.

Subject terms: Quantum physics • Technology

http://www.nature.com/news/commercialize-early-quantum-technologies-1.21583

- “We contend that short-term returns are possible with the small devices that will emerge **within the next five years**”
- “three commercially viable uses for early quantum-computing devices: **quantum simulation**, **quantum-assisted optimization** and **quantum sampling**. Faster computing speeds in these areas would be commercially advantageous in sectors from artificial intelligence to finance and health care.”

Big Labs


THE STACK
NEWS | DIRECTORY | WEBINARS | WHITE PAPERS | VIDEOS
CLOUD
DEFAULT
IBM claims to be launching Quantum Computing in the cloud
Martin Anderson Mon 6 Mar 2017 10.43am
IBM


techviral
Microsoft Is Developing Its Own Quantum Computer And OS
November 25, 2016
Shares
Microsoft
Quantum Computer
Microsoft is Developing Its Own Quantum Computer And OS


Google

Quantum Computing Startups

D:WAVE
The Quantum Computing Company™

Applied Quantum Technologies

rigetti

QxBranch

qci

CAMBRIDGE
QUANTUM
COMPUTING
LIMITED

Quantum Circuits, Inc.

Quantum Networking (QKD) Startups

MagiQ

(1999 ~)

id Quantique

(2001 ~)

SeQureNet

A Quantum Key to Network Security

(2009 ~)

Quintessence labs

(2008 ~)

Qubitekk

NATURE | NEWS

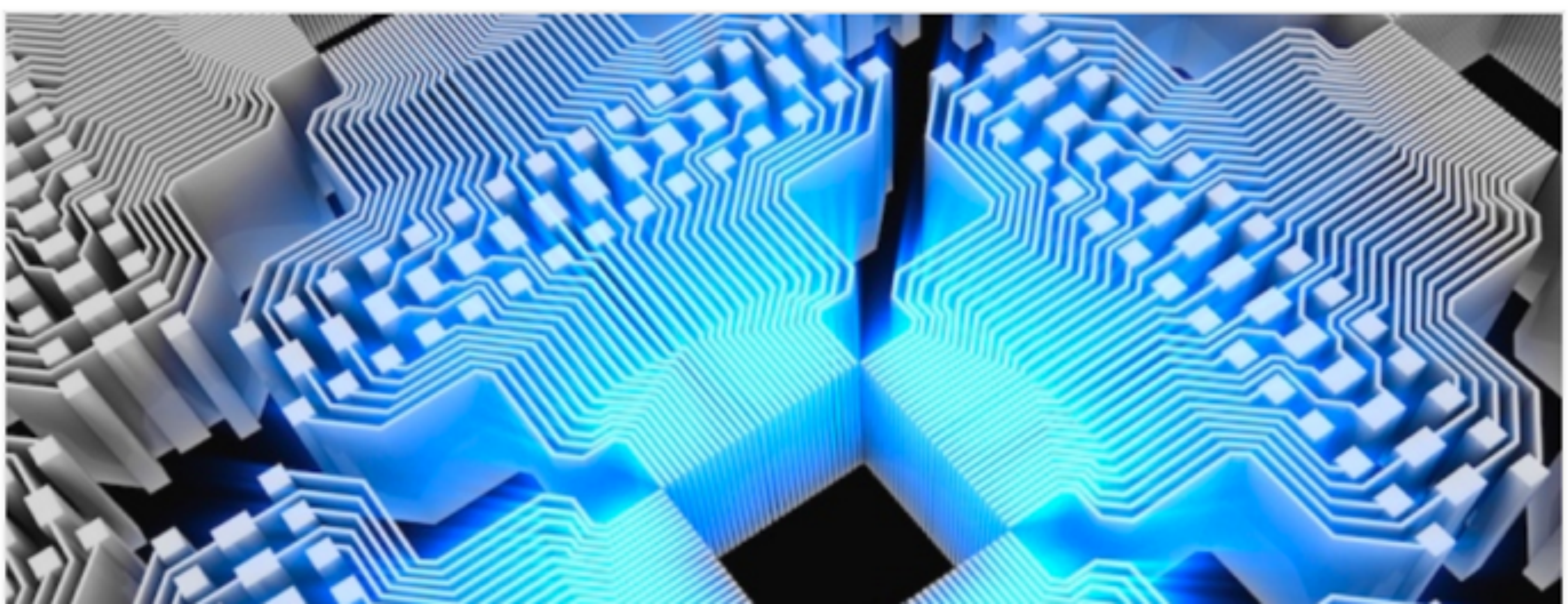
Europe plans giant billion-euro quantum technologies project

Third European Union flagship will be similar in size and ambition to graphene and human brain initiatives.

Elizabeth Gibney

21 April 2016 | Updated: 26 April 2016

PDF | Rights & Permissions



WIDE

UNIVERSITY of York

New Hub to make quantum leap in secure communications

Posted on 26 November 2014

Leading researchers from UK universities and industry have come together in a unique collaboration to exploit fundamental laws of quantum physics for the development of secure communication technologies and services for consumer, commercial and government markets.

Led by the University of York, the project consortium has bid successfully for Government funding to be one of four hubs in the EPSRC's new £155m National Network of Quantum Technology Hubs announced today by Greg Clark, Minister of State for Universities, Science and Cities.

The new hubs are the centre-piece of the £270 million investment in the UK National Quantum Technologies Programme announced by the Chancellor in the 2013 Autumn Statement.

The £24m five-year project involves eight universities - Bristol, Cambridge, Heriot-Watt, Leeds, Royal Holloway, Sheffield , Strathclyde and York - each of which will

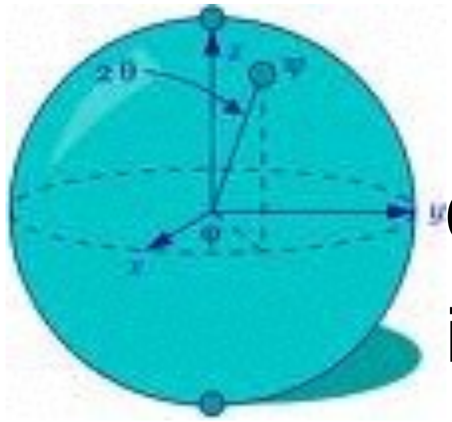
Outline

- Quantum Information Technology Industry:
  - Why should I be excited?
- Background:
  - interference, entanglement & teleportation
- Applications of quantum networks
- Lines of repeaters
- Networks & internetworks of repeaters

Quantum computing in 2 slides (1)

Current computers use **bits**, 0 and 1, as the fundamental unit of information to store and process.

Physically, a transistor either conducts current ("1") or it doesn't ("0"). The laws of physics that govern transistors determine the logical flow of information in a computer.



Quantum computers use **qubits** as the basic information unit.

Quantum computing in 2 slides (2)

A qubit can be in a state that is both 0 and 1 at the same time:

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

SUPERPOSITION

Two or more qubits can be correlated more strongly than bits can:

$$\alpha|01\rangle + \beta|10\rangle$$

ENTANGLEMENT

The focus of our research into quantum computing is to exploit the logic of entanglement and superposition to create **quantum technologies**.

One Particle (One Photon, One Electron)

Two possible states:

One Particle (One Photon, One Electron)

Two possible states:

One Particle (One Photon, One Electron)

Two possible states:

$$|\uparrow\rangle$$

$$|0\rangle$$

One Particle (One Photon, One Electron)

Two possible states:

$$|\uparrow\rangle$$

$$|0\rangle$$

One Particle (One Photon, One Electron)

Two possible states:

$$|\uparrow\rangle \quad |\downarrow\rangle$$

$$|0\rangle \quad |1\rangle$$

Superposition & Measurement

Superposition & Measurement

We can create a state that's partially up, partially down

Superposition & Measurement

We can create a state that's partially up, partially down

"Measure" it and find its value…

KEIO 150 Design the Future

Superposition & Measurement

We can create a state that's partially up, partially down

"Measure" it and find its value…

Superposition & Measurement

We can create a state that's partially up, partially down

"Measure" it and find its value...

50/50 chance of each outcome

KEIO 150
Design the Future

Superposition & Measurement

We can create a state that's partially up, partially down

"Measure" it and find its value...

50/50 chance of each outcome

...destroys the superposition!

Making Entanglement (one of many ways)

Making Entanglement (one of many ways)

Start with one qubit, put it in superposition

Making Entanglement (one of many ways)

Start with one qubit, put it in superposition

bring in a second qubit

Making Entanglement (one of many ways)

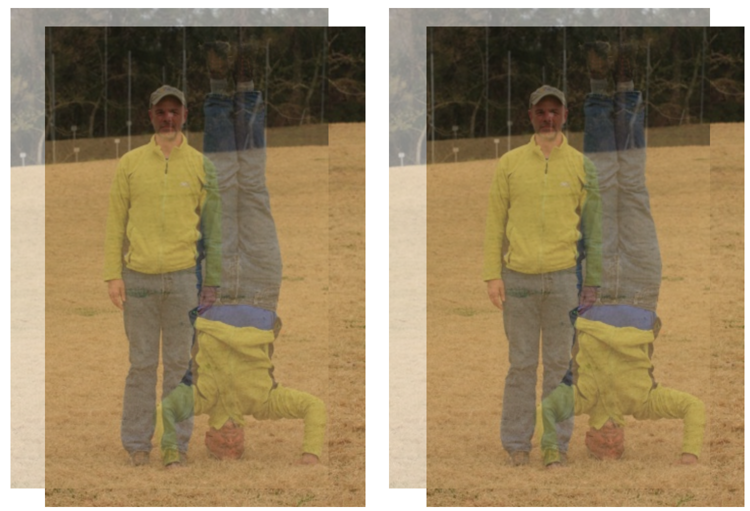
Start with one qubit, put it in superposition

bring in a second qubit

Entangle them!

(very dependent on qubit type)

Measuring Entanglement



Measuring Entanglement

Measuring Entanglement

“Measure” this one and find its value…

(50/50 chance of up & down)

and you’ll also know what this one is

Measuring Entanglement

Even if they are far apart!

"Measure" this one and find its value…

(50/50 chance of up & down)

and you'll also know what this one is

KEIO 150
Design the Future

Two Qubits, Four States

Just like two classical bits, we can have four possible combinations

Two Qubits, Four States

$|\uparrow\uparrow\rangle$

Just like two classical bits, we can have four possible combinations

Two Qubits, Four States


$$|\uparrow\uparrow\rangle$$

$$|\uparrow\downarrow\rangle$$


Just like two classical bits, we can have four possible combinations

Two Qubits, Four States

$|\uparrow\uparrow\rangle$

Just like two classical bits, we can have four possible combinations

$|\uparrow\downarrow\rangle$

$|\downarrow\uparrow\rangle$

Two Qubits, Four States

$$|\uparrow\uparrow\rangle$$

Just like two classical bits, we can have four possible combinations

$$|\uparrow\downarrow\rangle$$

$$|\downarrow\uparrow\rangle$$

$$|\downarrow\downarrow\rangle$$

Entanglement

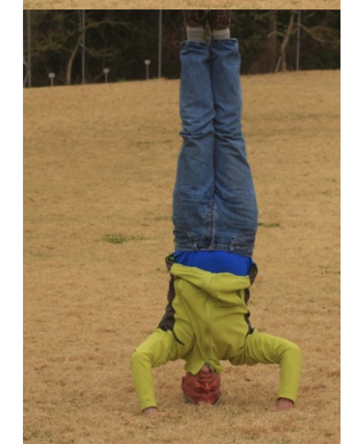
Entanglement

If this:

Entanglement




If this:

or this:


Entanglement

If this:

but never the other two combinations...

or this:

Entanglement

If this:

$$\frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}}$$

or this:

Entanglement

If this:

$$\frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

or this:

Entanglement

If this:

ENTANGLEMENT!

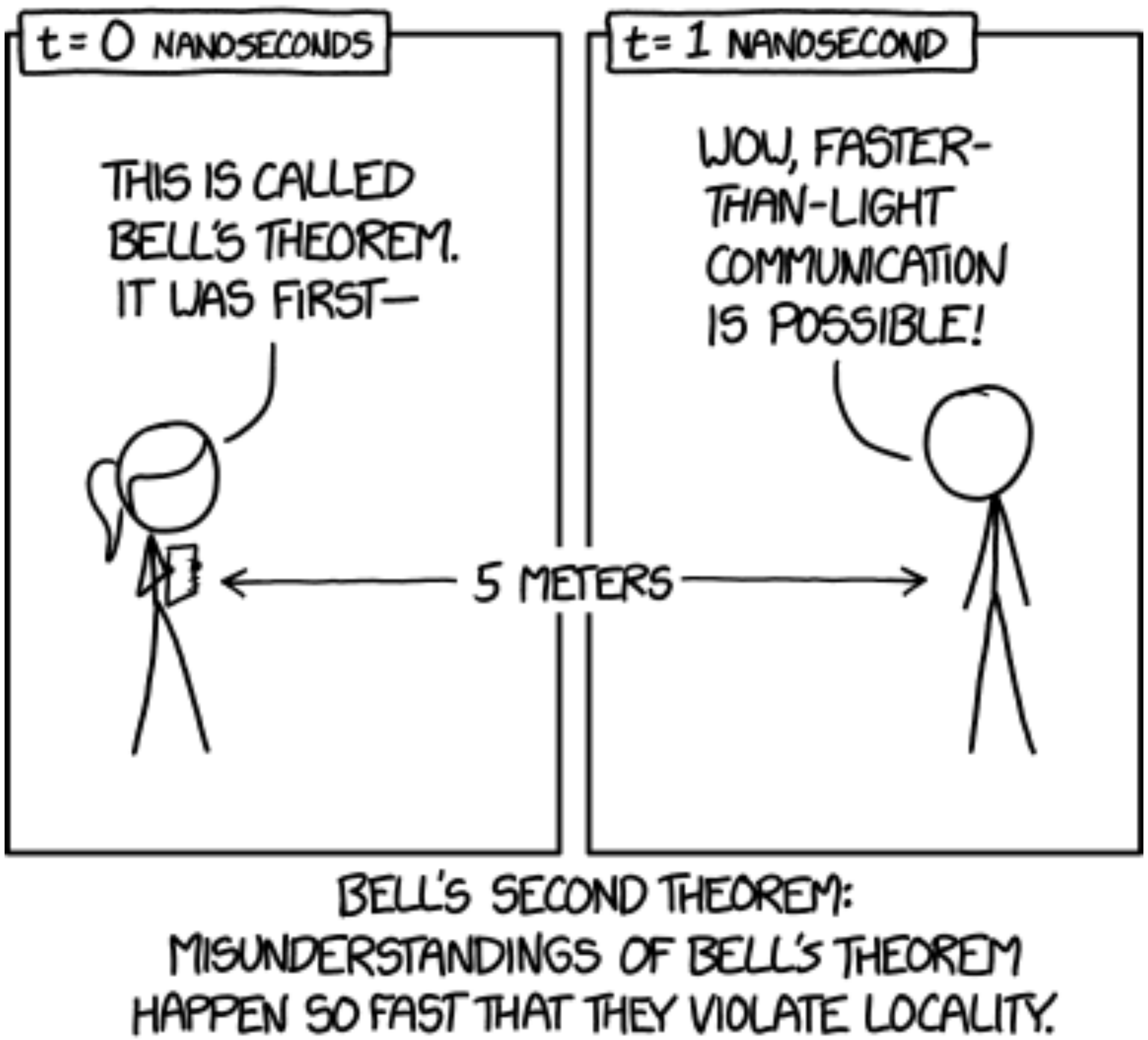
They are random but not independent.

$$\frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

or this:

EIO 15O
sign the Future

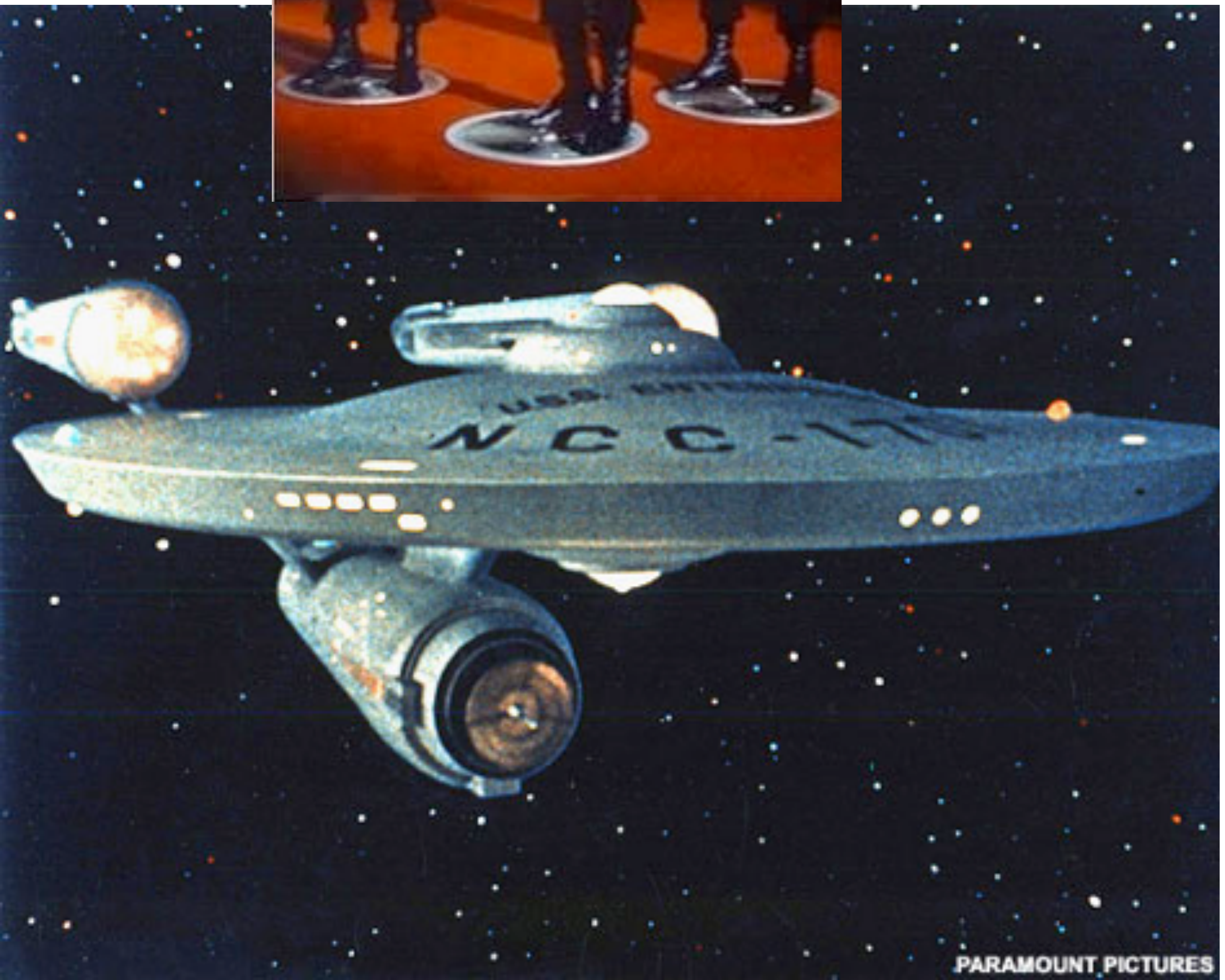
But No Faster-Than-Light Communication



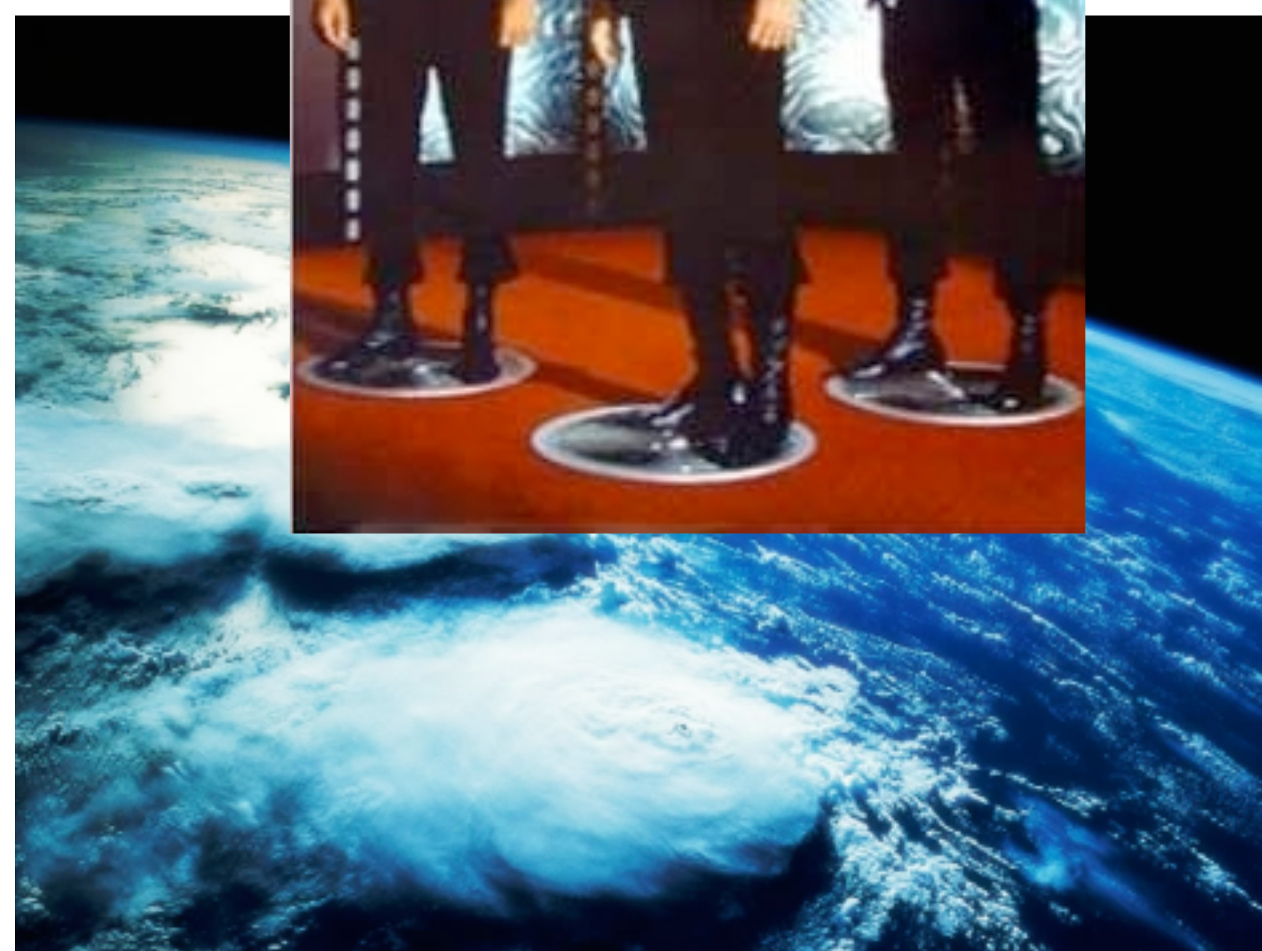
Nope!

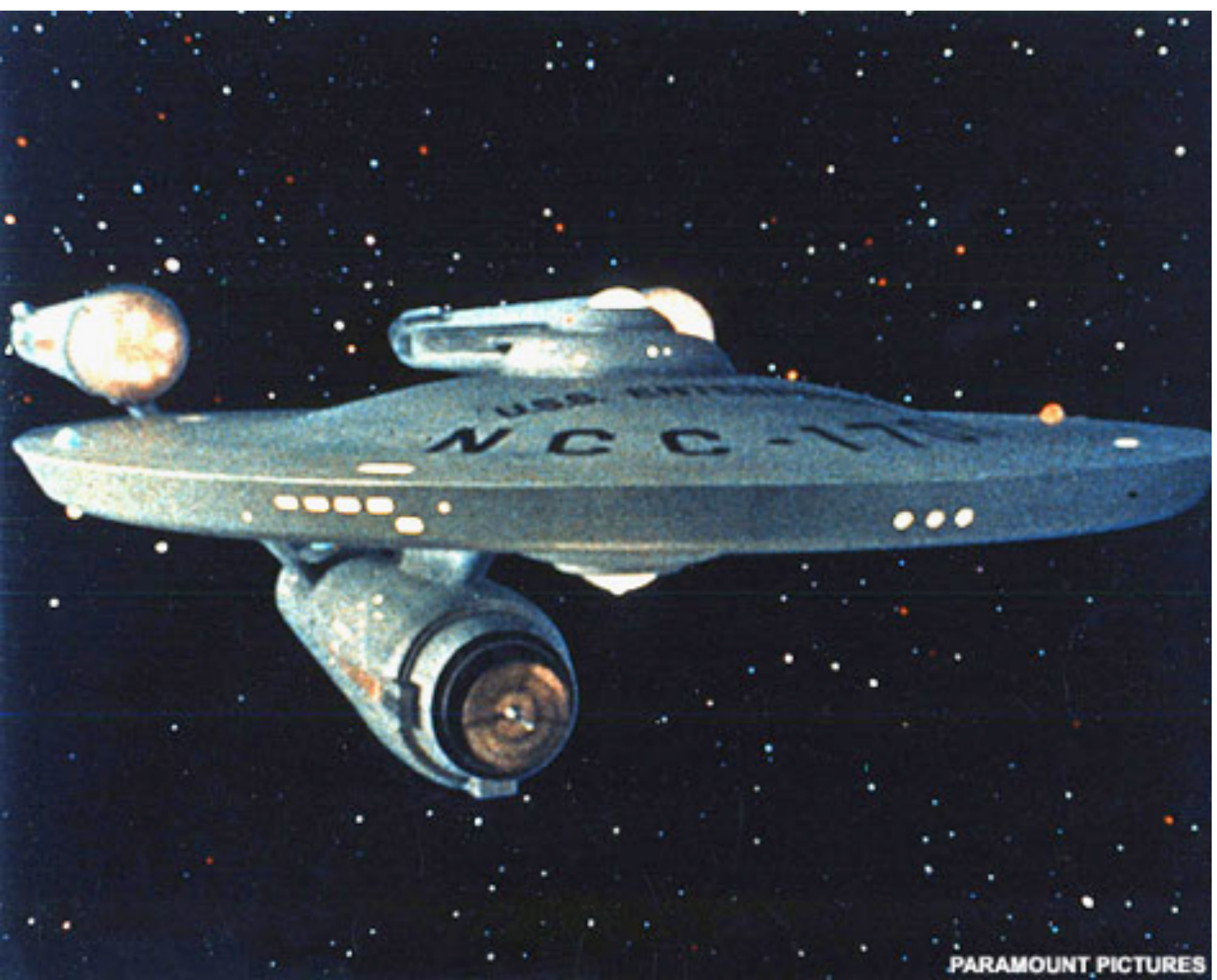
You can each get shared, secret random numbers upon *measuring* shared, entangled states, but that doesn't give you the ability to send messages.

Teleportation

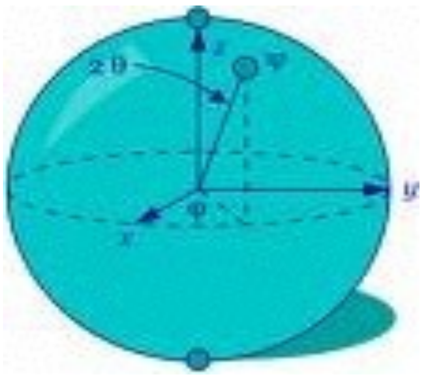


Teleportation

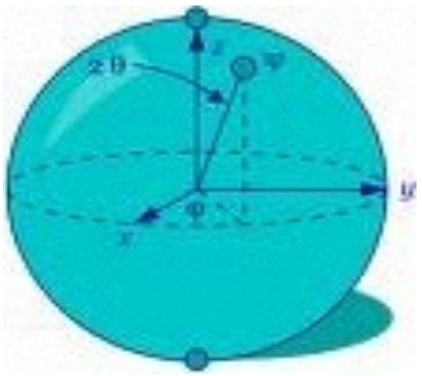




Quantum teleportation: Information, not Objects



Quantum teleportation: Information, not Objects



Quantum teleportation: Information, not Objects

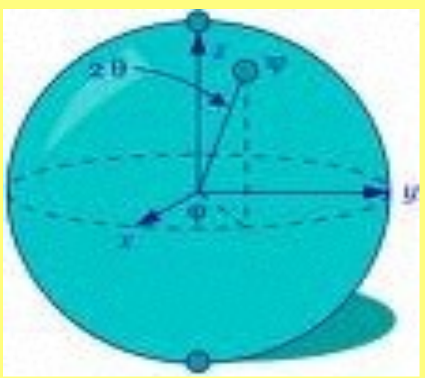
Alice

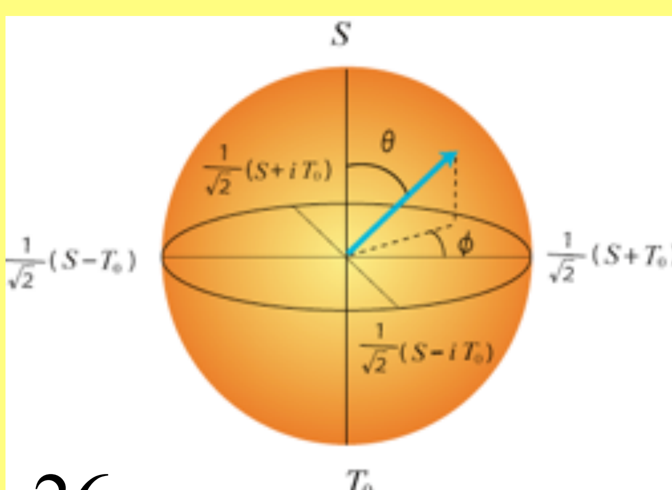
Bob

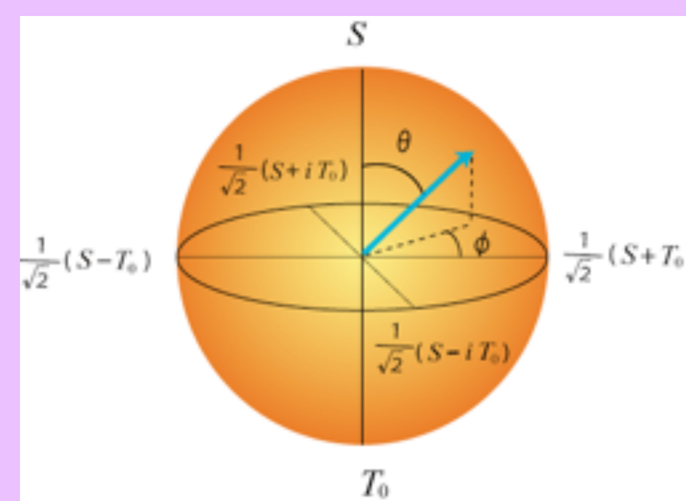
Quantum teleportation: Information, not Objects

Alice

Bob



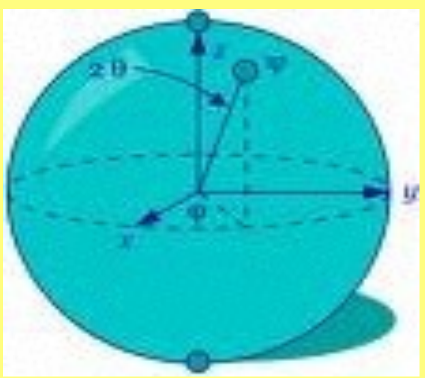




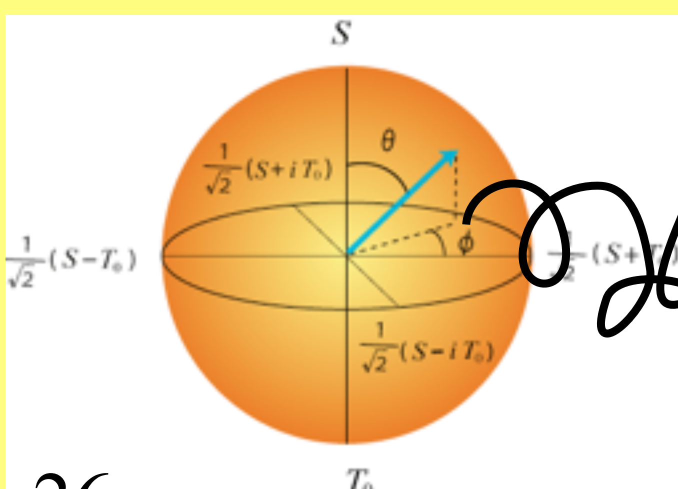
Quantum teleportation: Information, not Objects

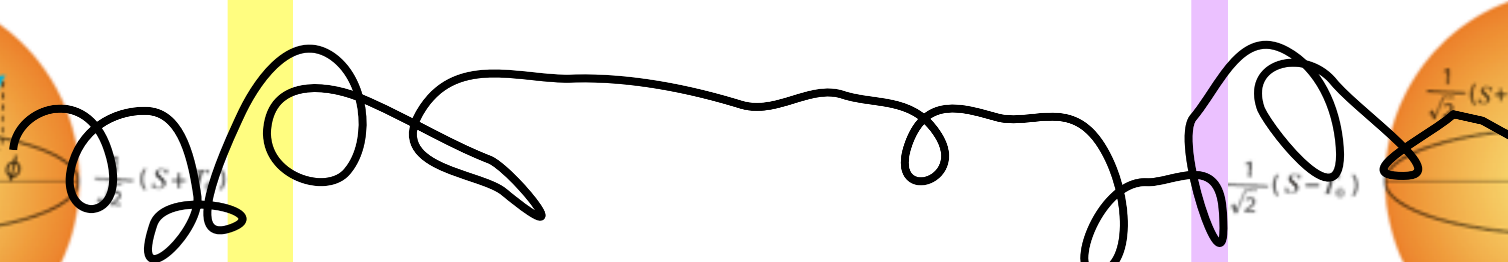
Alice

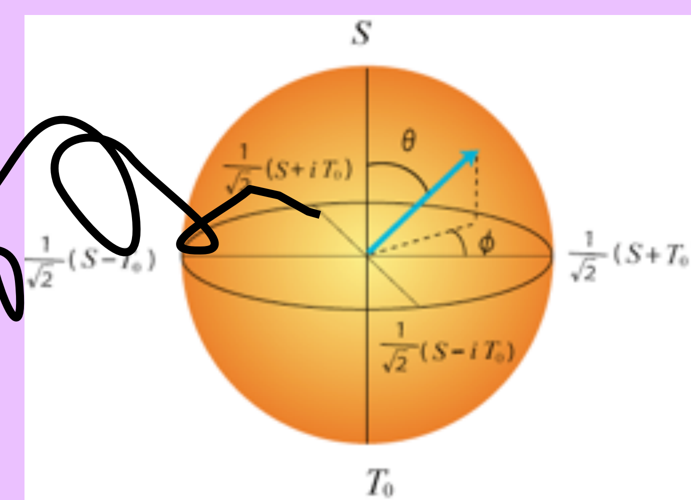
Bob



Use Entanglement



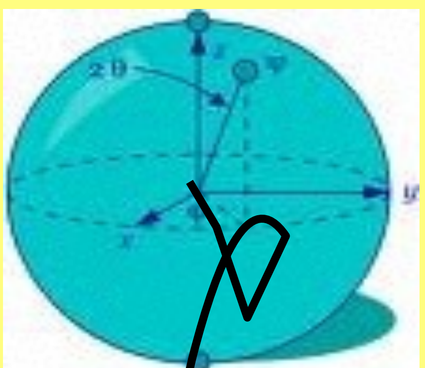




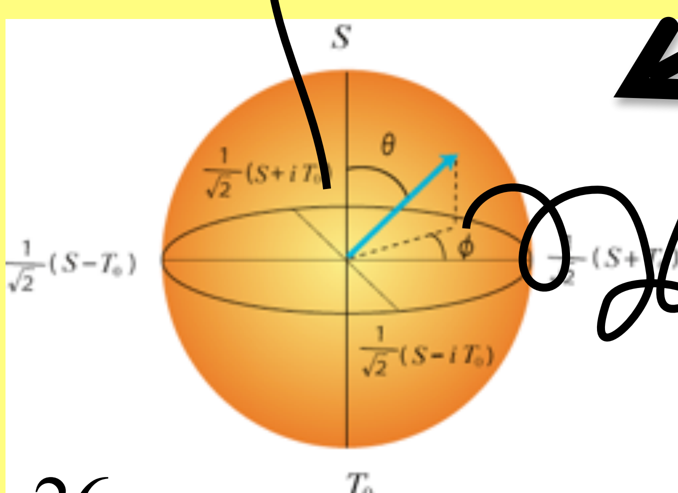
Quantum teleportation: Information, not Objects

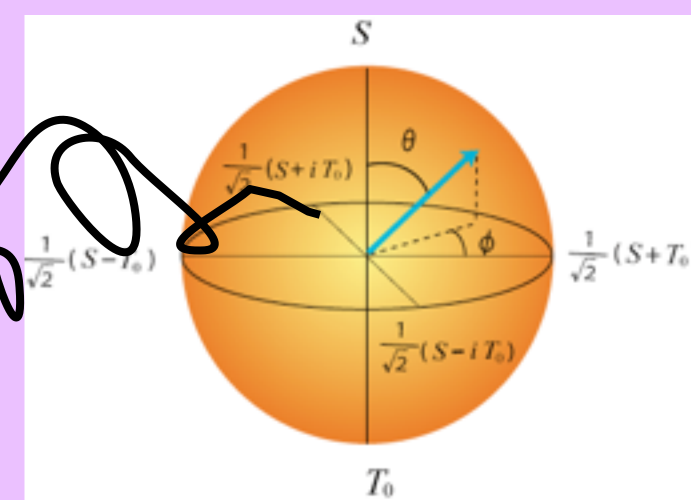
Alice

Bob



Local Quantum Operations

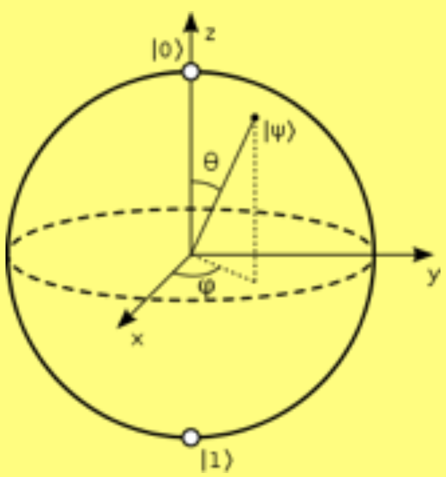




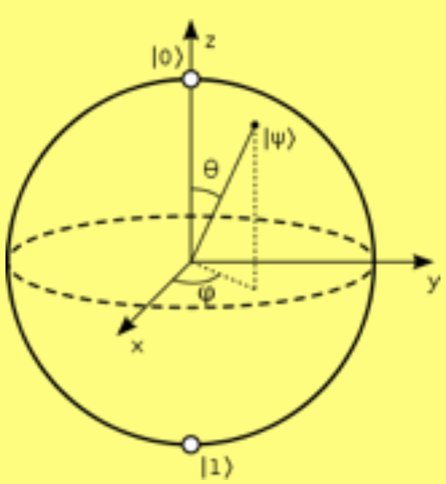
Quantum teleportation: Information, not Objects

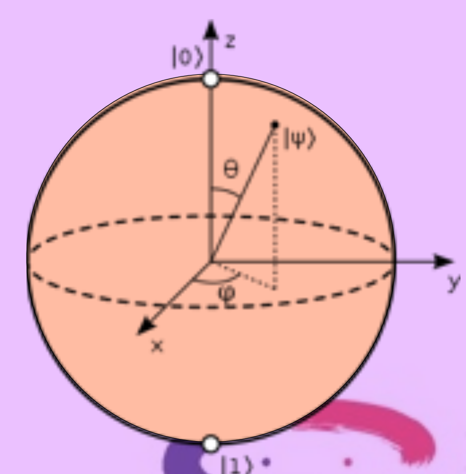
Alice

Bob



Local Quantum Operations

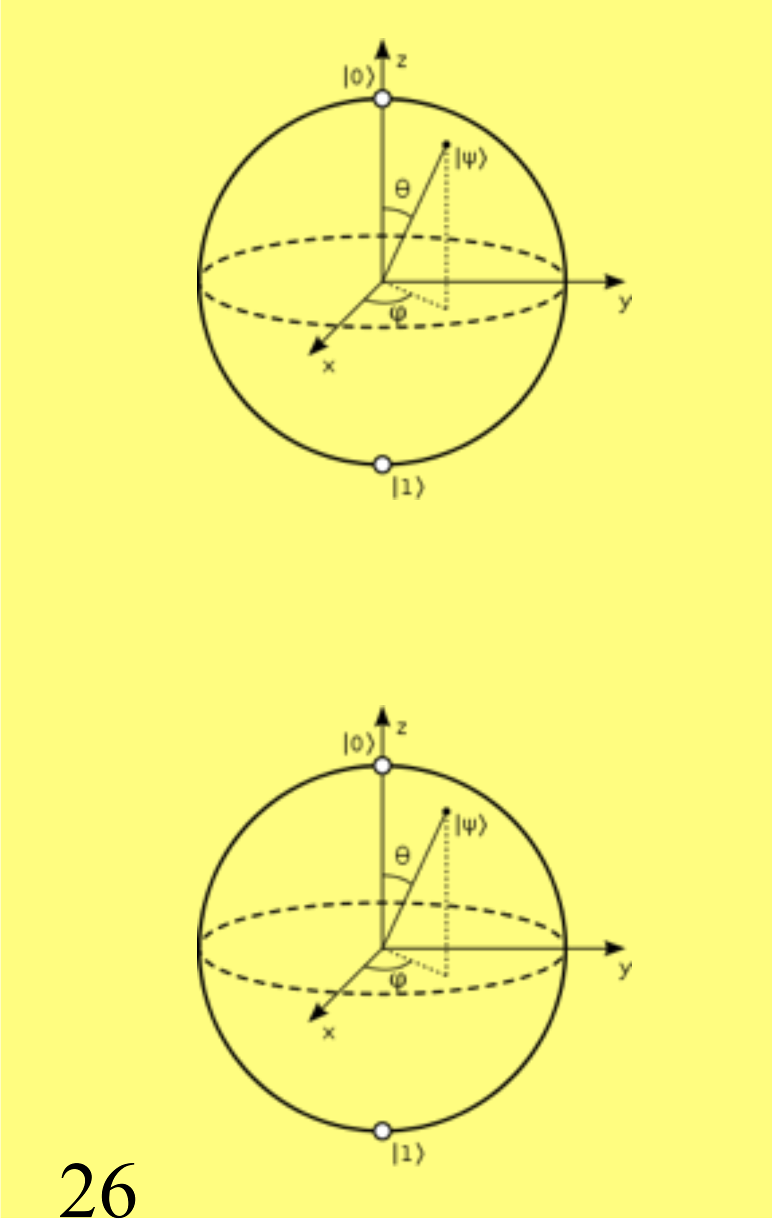


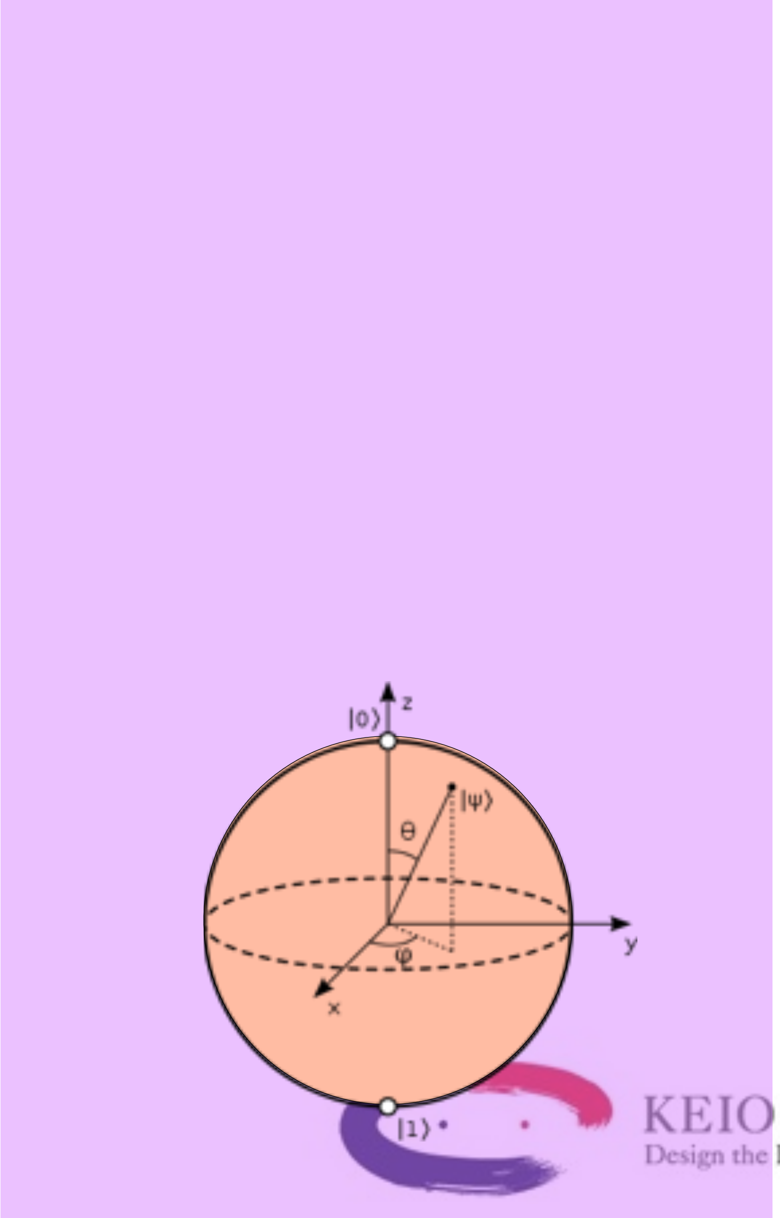


Quantum teleportation: Information, not Objects

Alice

Bob

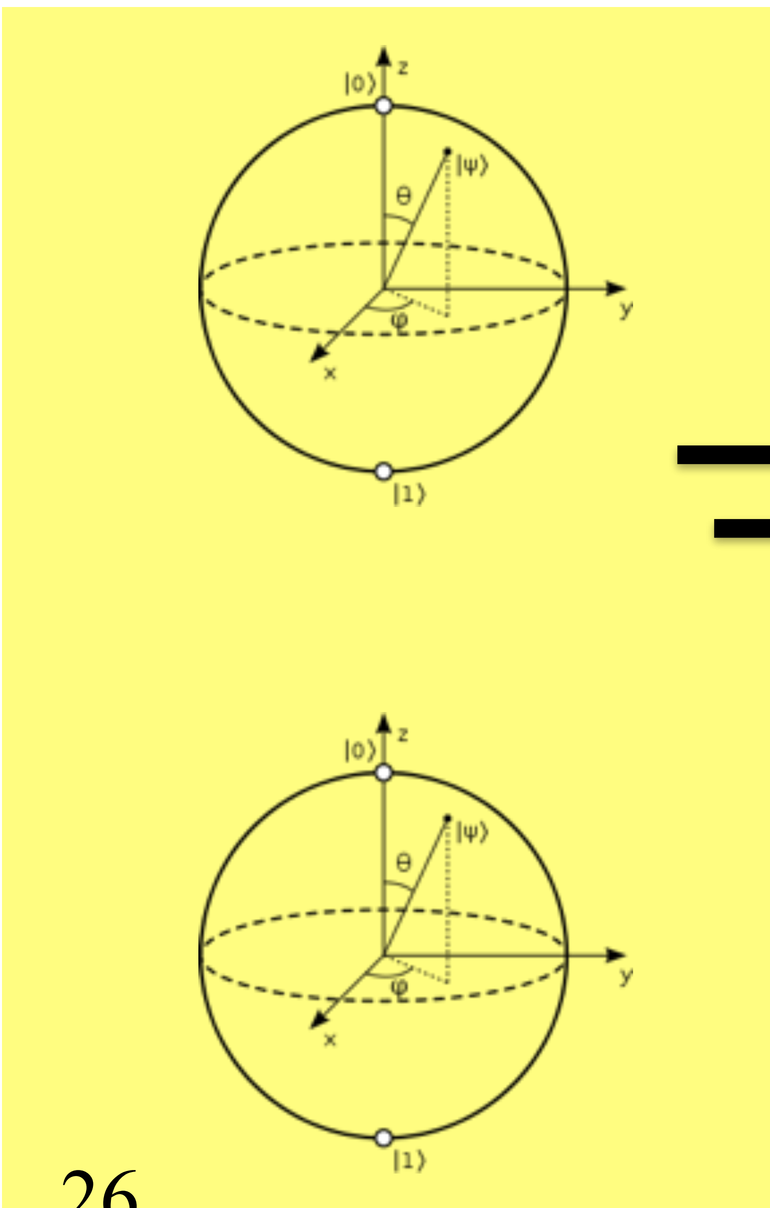




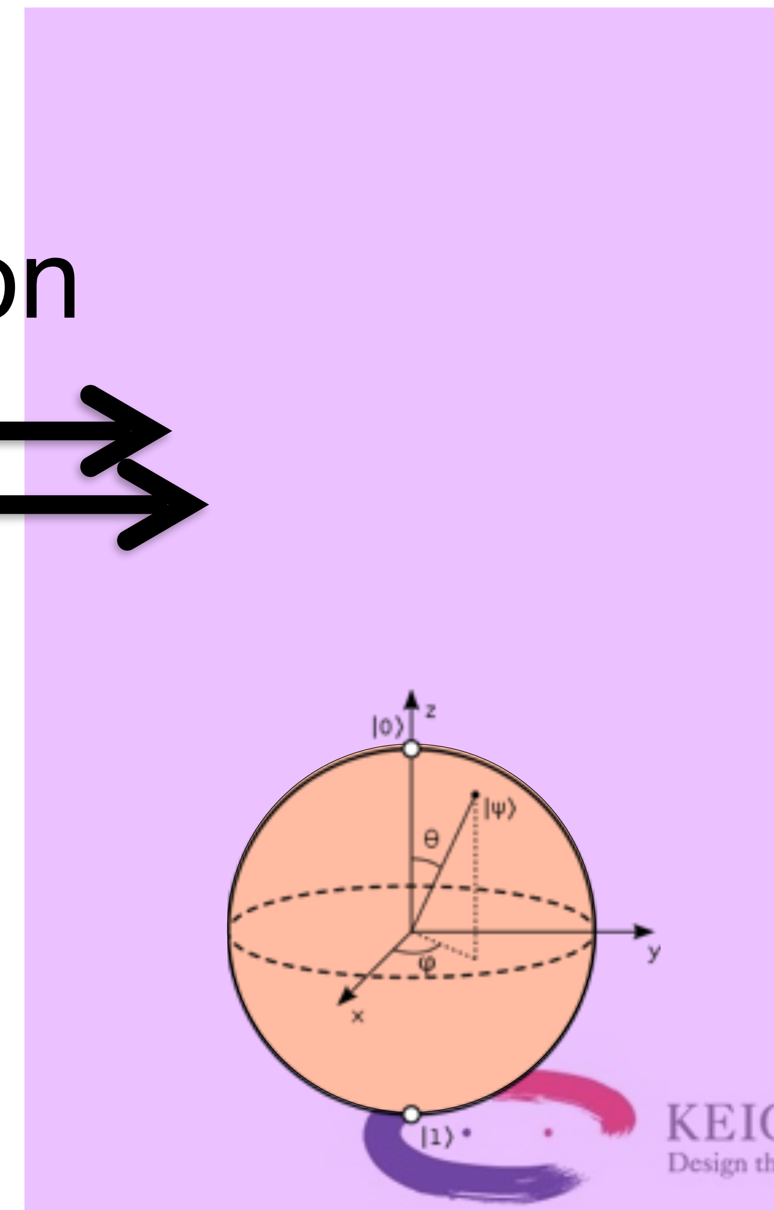
Quantum teleportation: Information, not Objects

Alice

Bob

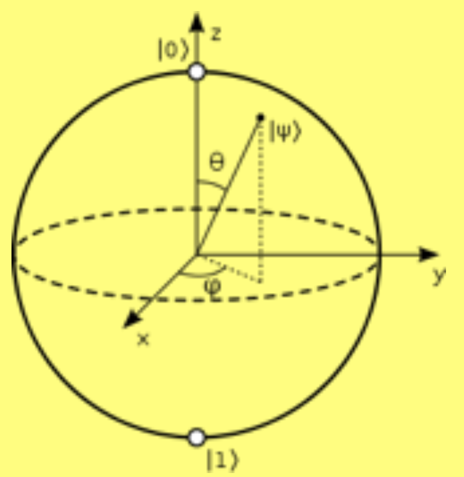


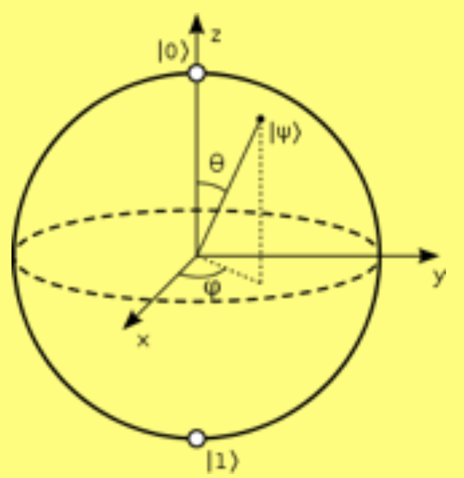
Classical Communication



Quantum teleportation: Information, not Objects

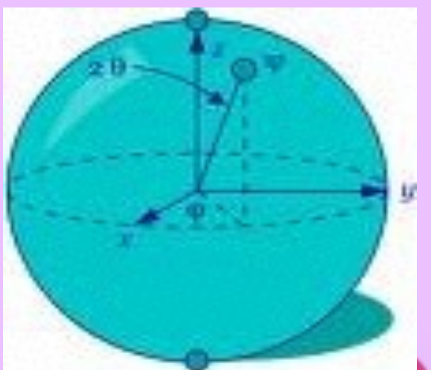
Alice





Bob

and Local Q Ops to Recreate Original



The New York Times

SundayReview

Is Quantum Entanglement Real?

NOV. 14, 2014

Physics Vol. 1, No. 3, pp. 195–290, 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)

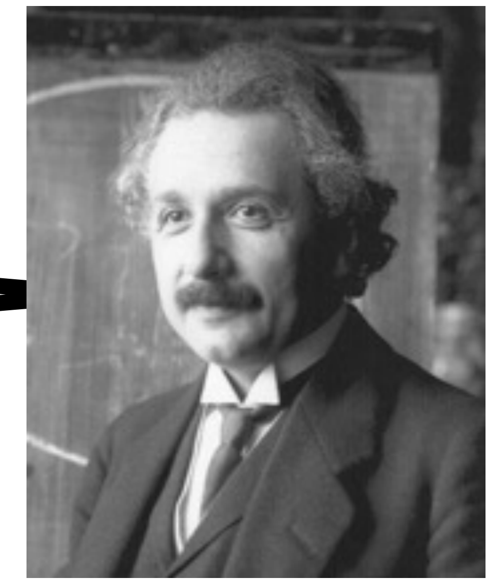
I. Introduction

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 nonlocal structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

Nonlocality - the arguments

Nonlocality - the arguments

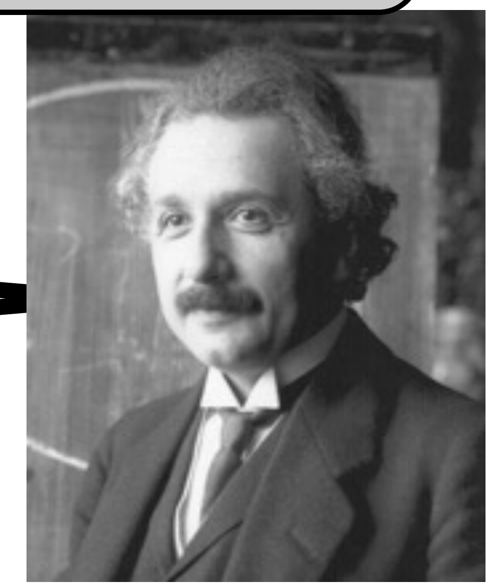
Hang on, quantum mechanics as written down requires things far apart to behave like they have faster than light communication?!?



Nonlocality - the arguments

Hang on, quantum mechanics as written down requires things far apart to behave like they have faster than light communication?!?

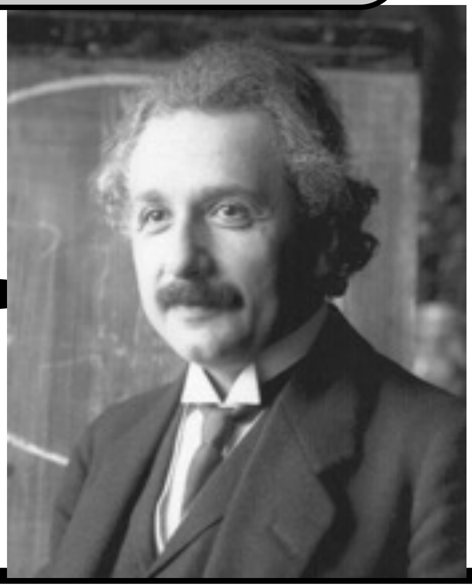
Einstein



Nonlocality - the arguments

Hang on, quantum mechanics as written down requires things far apart to behave like they have faster than light communication?!?

Einstein

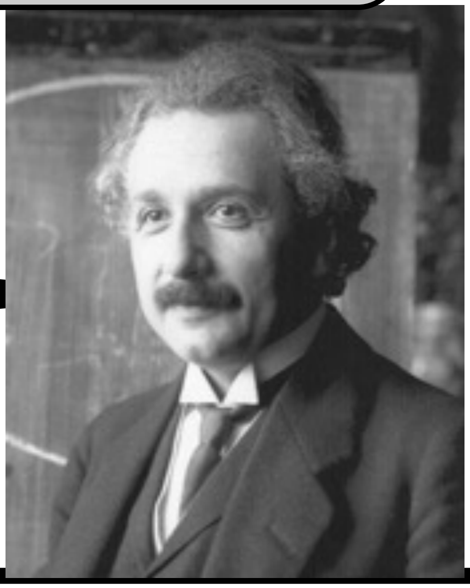


There's a way to statistically test this.

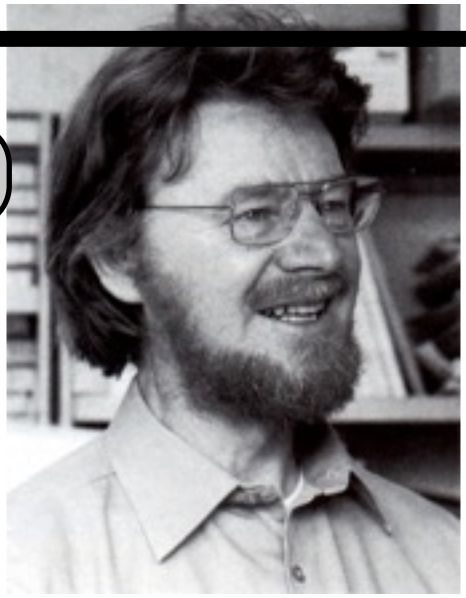
Nonlocality - the arguments

Hang on, quantum mechanics as written down requires things far apart to behave like they have faster than light communication?!?

Einstein



J.S.Bell

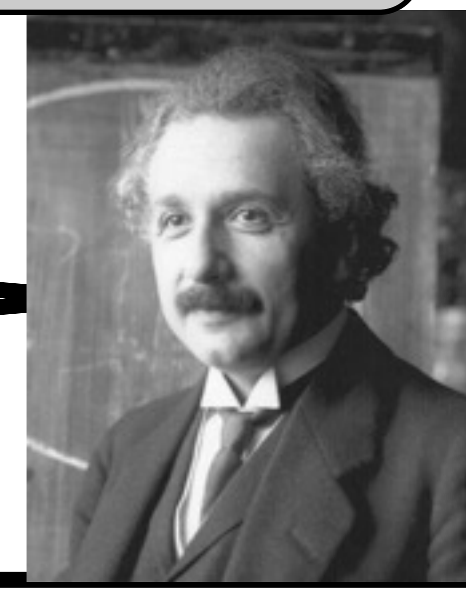


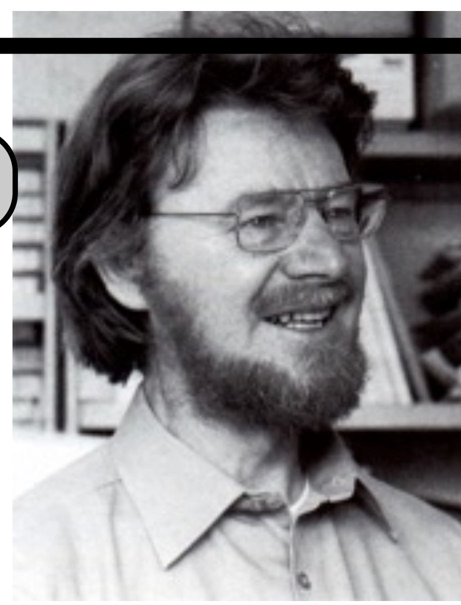
There's a way to statistically test this.

Nonlocality - the arguments

Hang on, quantum mechanics as written down requires things far apart to behave like they have faster than light communication?!?

Einstein





J.S.Bell

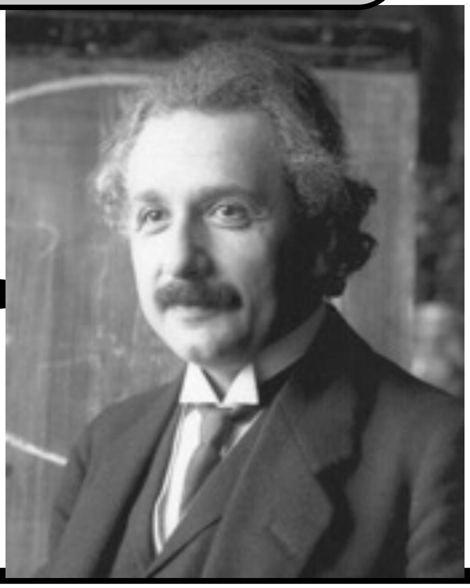
There’s a way to statistically test this.

I tested it!

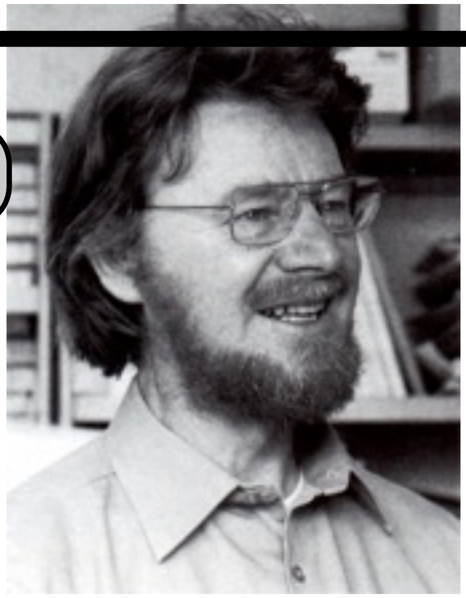
Nonlocality - the arguments

Hang on, quantum mechanics as written down requires things far apart to behave like they have faster than light communication?!?

Einstein



J.S.Bell



There's a way to statistically test this.

Aspect

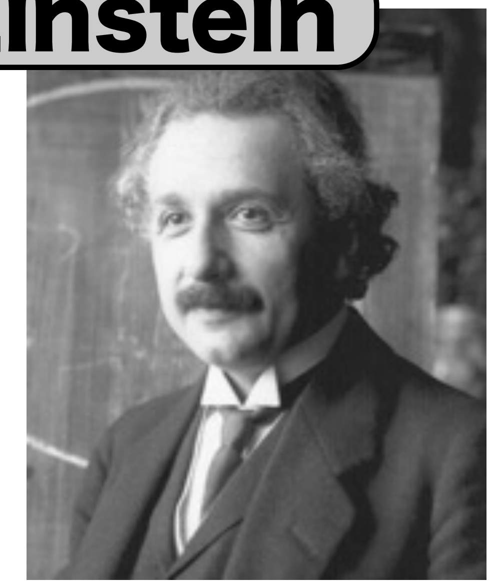
I tested it!

Nonlocality - the arguments

Nonlocality - the arguments

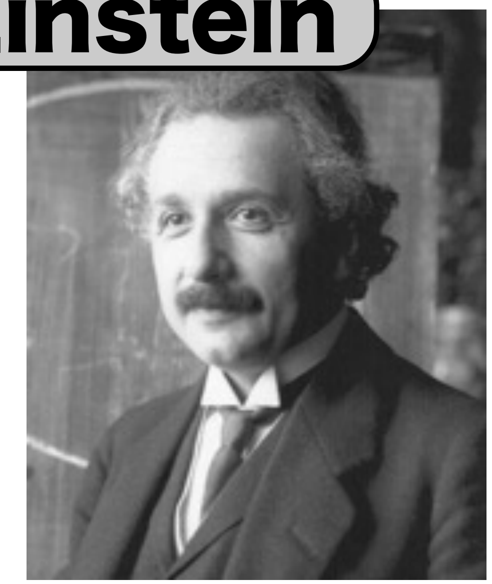
Either quantum mechanics is nonlocal, or it is incomplete (secret plans)

Einstein



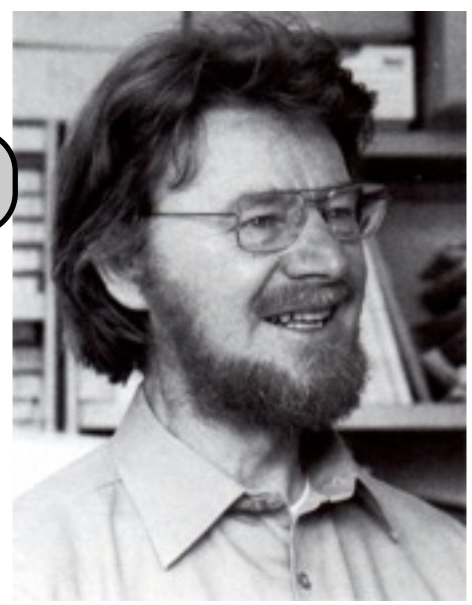
Nonlocality - the arguments

Einstein



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

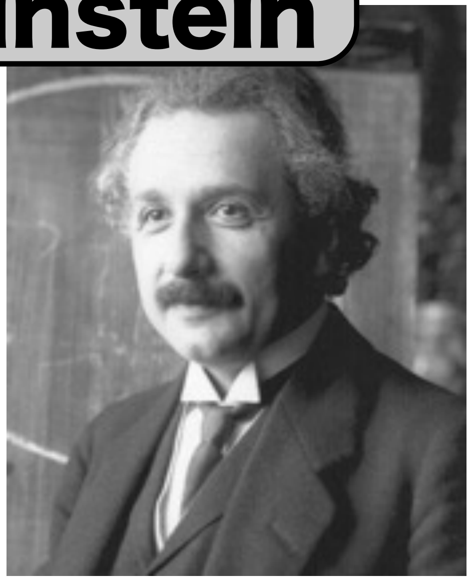
J.S.Bell



Even if it is incomplete, it is still nonlocal!

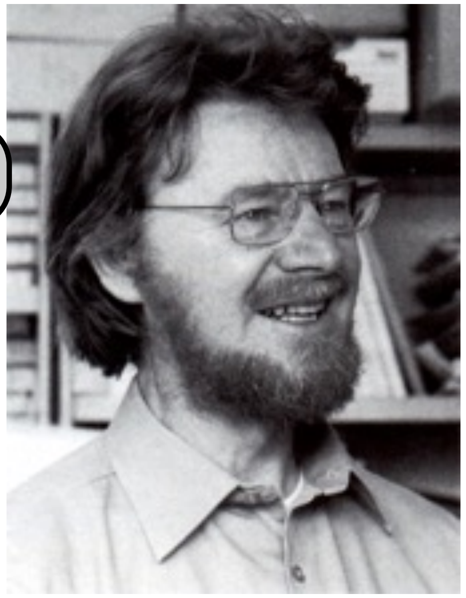
Nonlocality - the arguments

Einstein



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

J.S.Bell

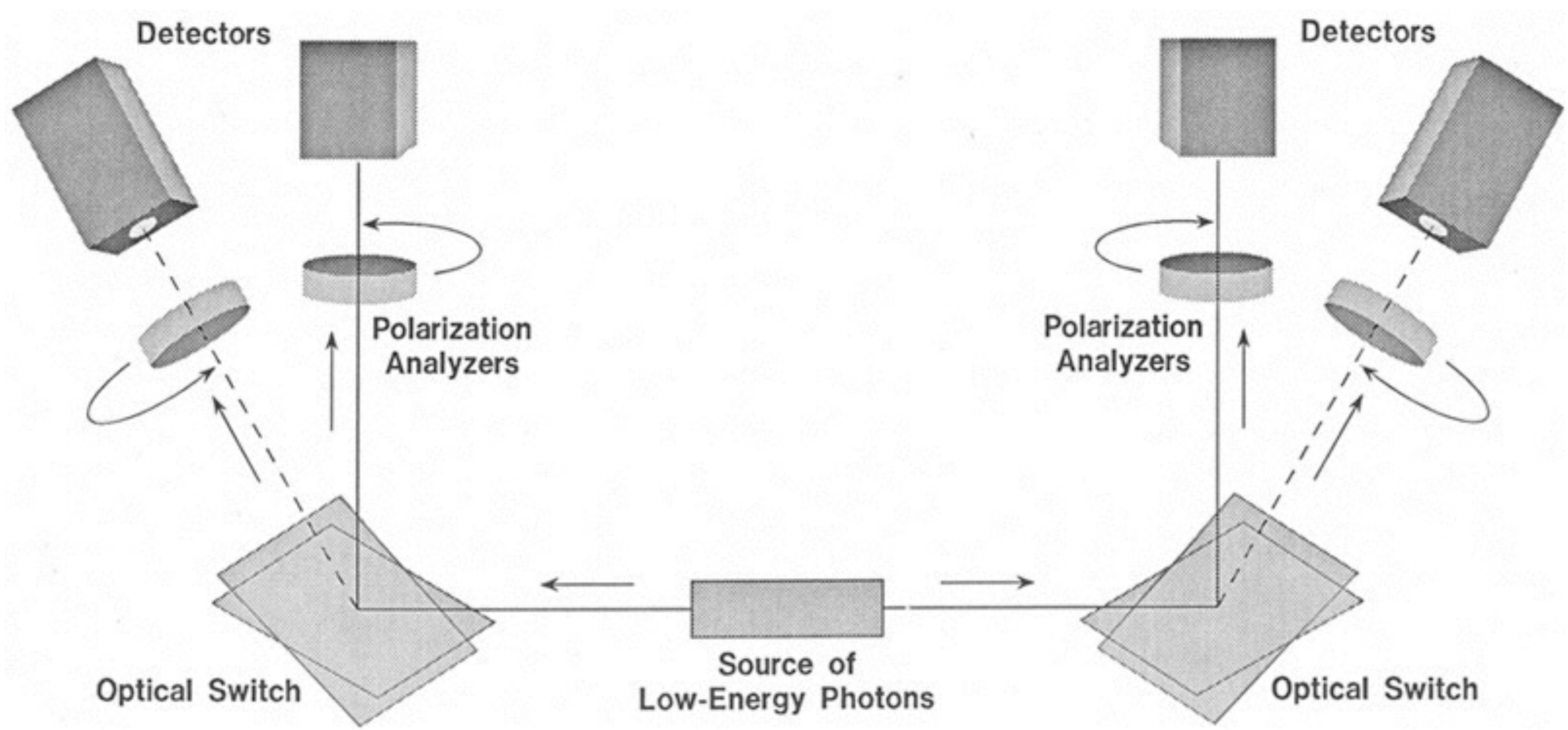


Even if it is incomplete, it is still nonlocal!

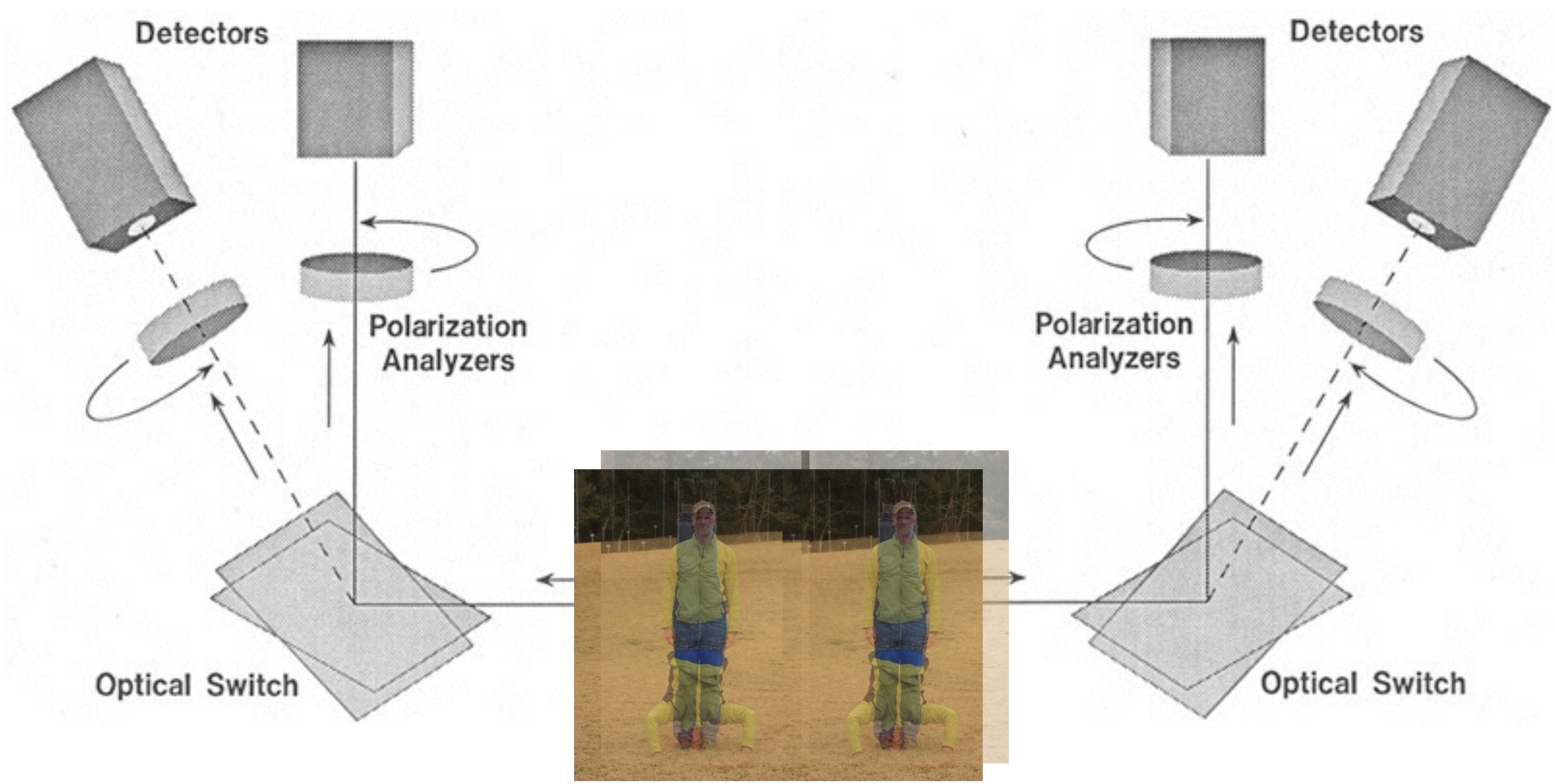
Aspect

No local hidden variable theory can explain my experiment.

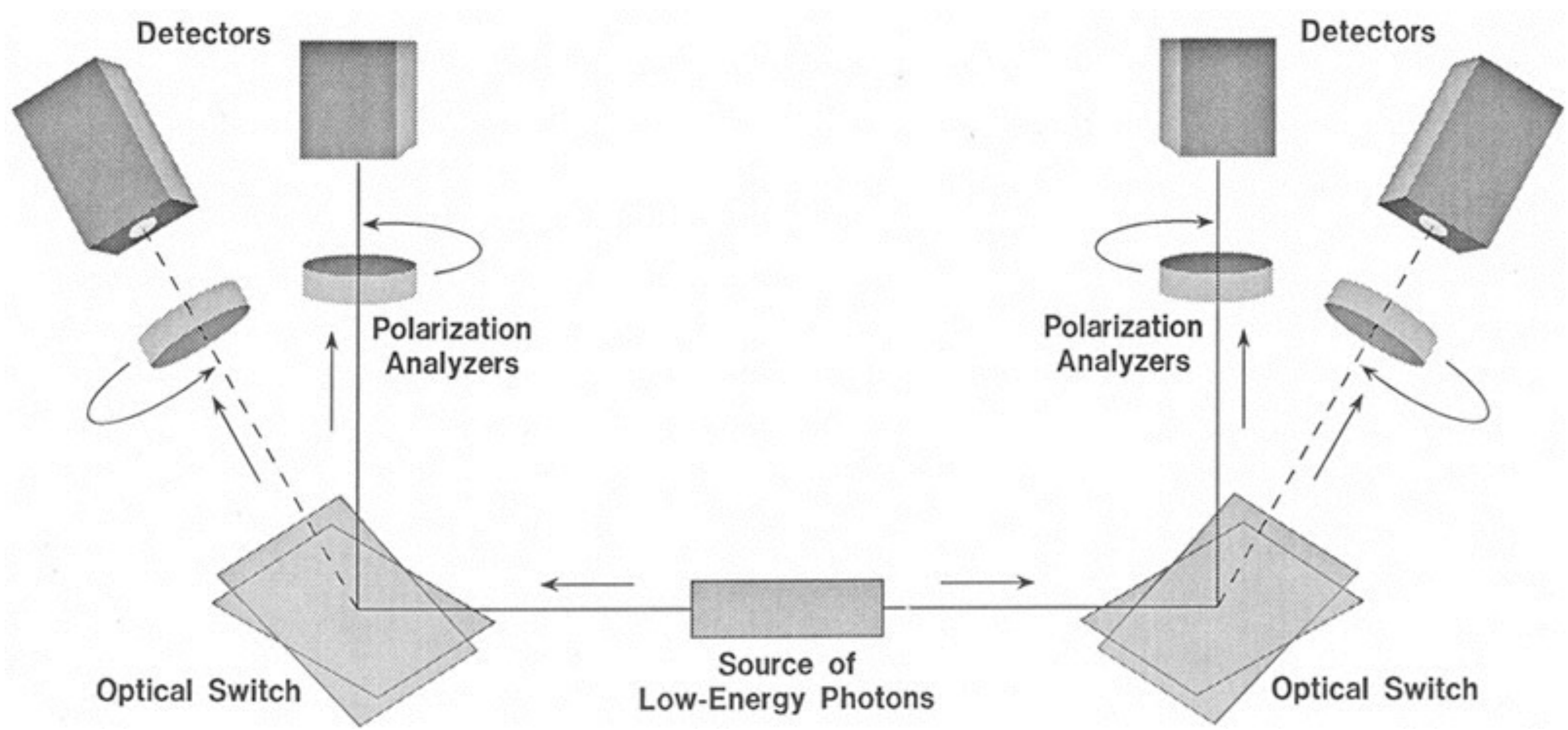
The Aspect experiments



The Aspect experiments



The Aspect experiments



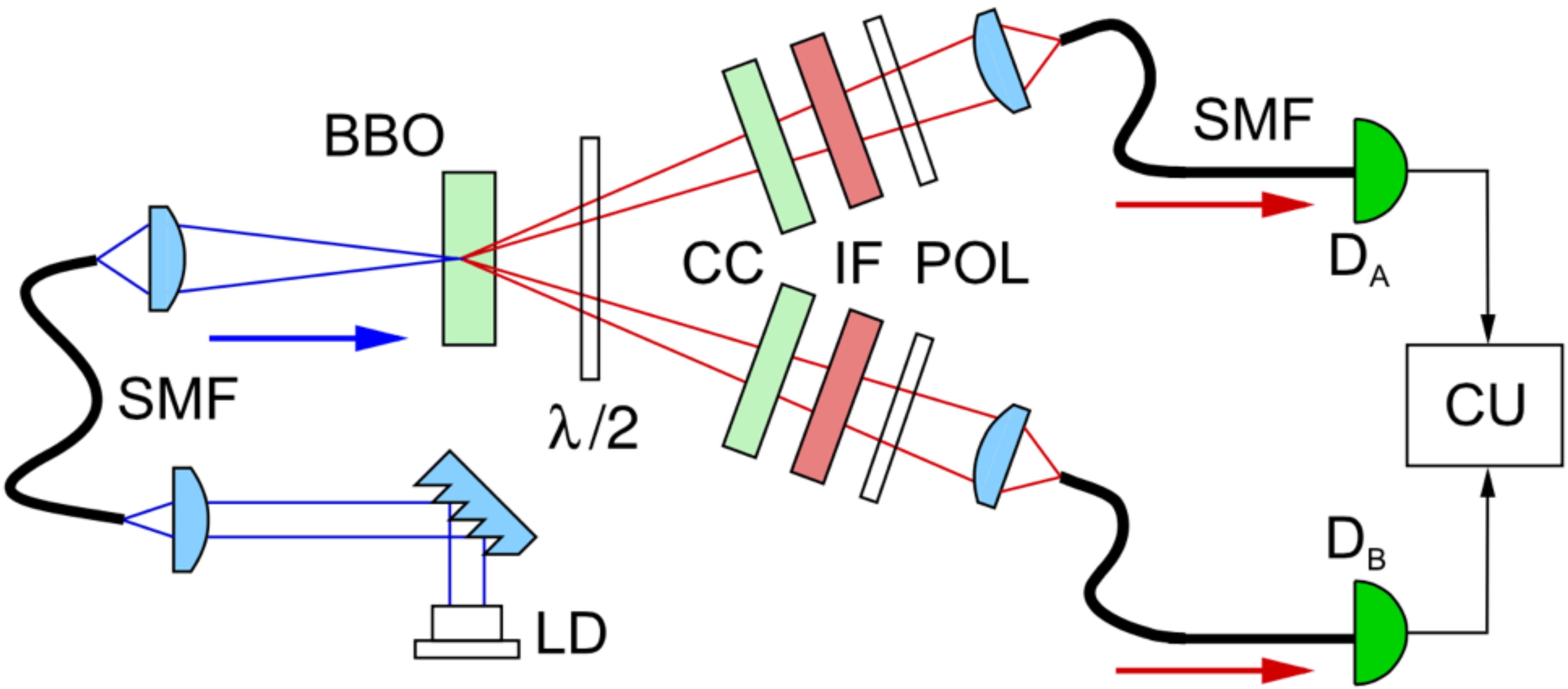
Recent Bell Inequality Violation Experiments

- Four major research groups have announced results in testing Bell's theorem in 2015.
- Pop science reports:
  - Delft group: http://phys.org/news/2015-08-loopholes-entanglement-bell-inequality.html
  - Vienna group: http://phys.org/news/2015-11-big-quantum.html
  - Singapore group: http://www.eurekalert.org/pub_releases/2015-11/cfqt-ere110915.php
  - UNSW group: http://www.gizmag.com/advance-programmable-silicon-quantum-computers/40420/
- btw, the Wikipedia article is a reasonable list of Bell inequality violations going back three decades:
  https://en.wikipedia.org/wiki/Bell_test_experiments

Recent Bell Inequality Violation Experiments

- Technical papers:
  - Hanson group, Delft:
    http://www.nature.com/nature/journal/v526/n7575/full/nature15759.html
    http://arxiv.org/abs/1508.05949
  - Zeilinger group, Vienna: Giustina et al.
    http://arxiv.org/abs/1511.03190
    - (related: http://www.pnas.org/content/early/2015/10/27/1517574112, http://www.pnas.org/content/early/2015/10/28/1517007112)
  - Kurtsiefer group, Singapore:
    https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.115.180408 or
    http://arxiv.org/abs/1506.01865
  - Morello group, University of New South Wales (Kohei M. Itoh, Keio, collaborating):
    http://www.nature.com/nnano/journal/vaop/ncurrent/full/nnano.2015.262.html

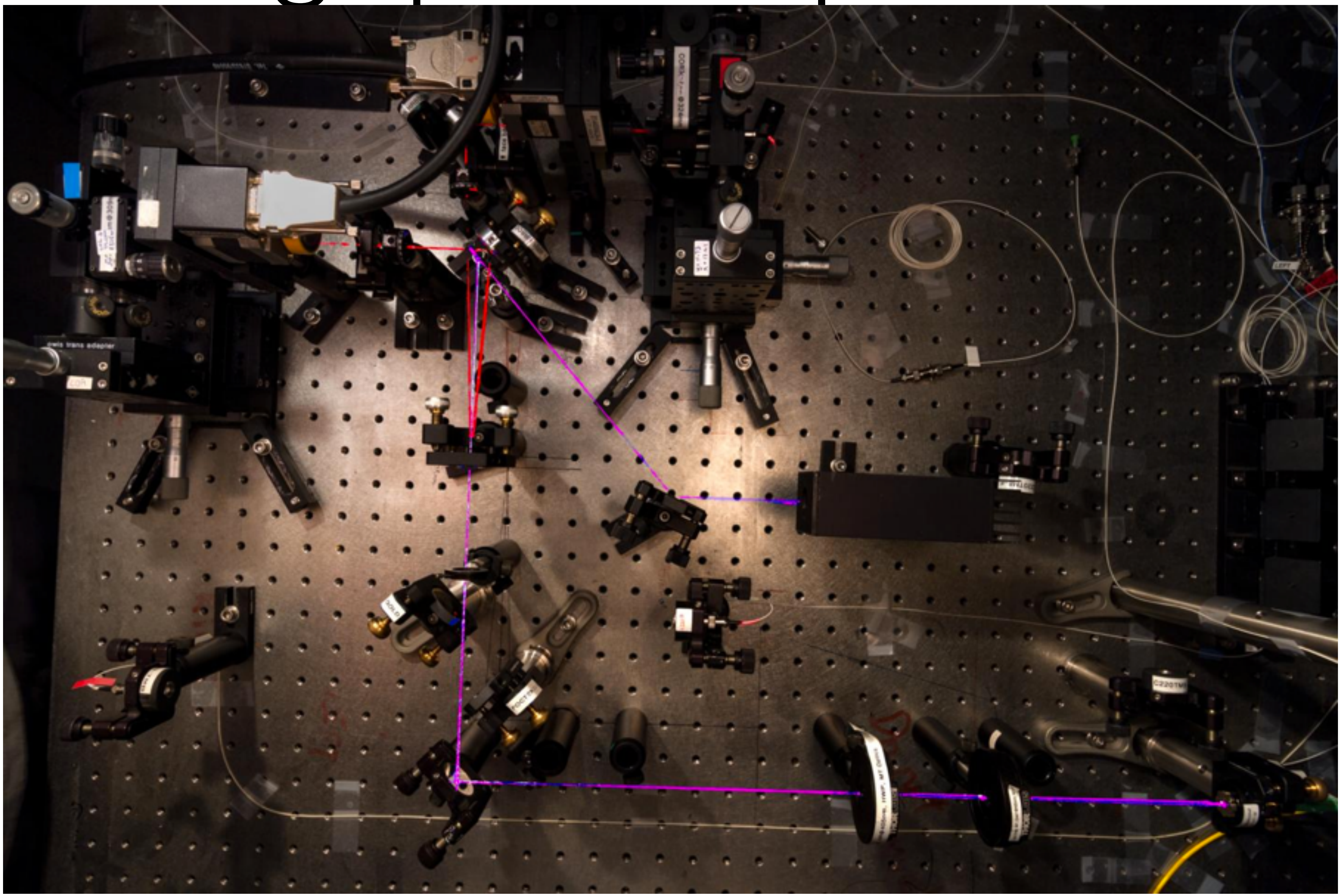
Singapore Experiment



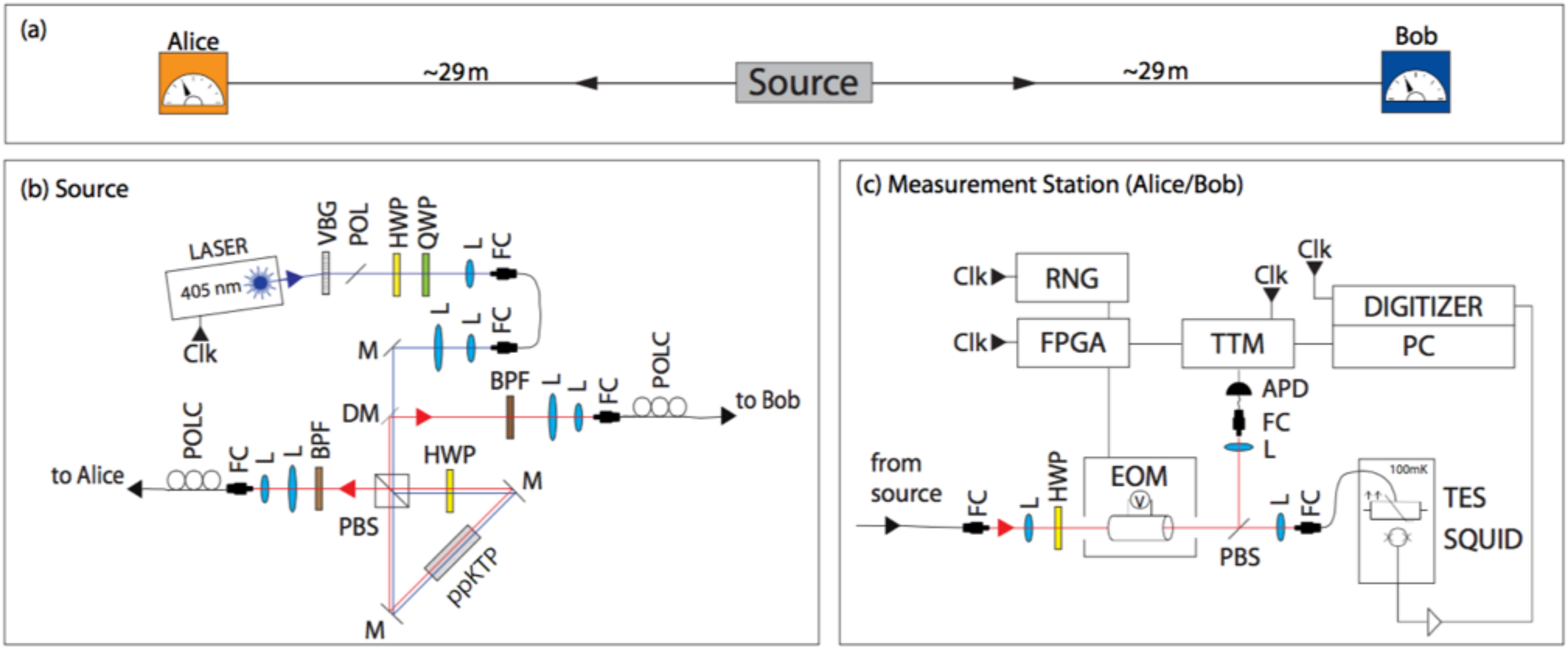
Poh *et al.*, *Phys. Rev. Letters* 115, 180408, 2015

Super-precise statistical test of Bell inequality

Singapore Experiment



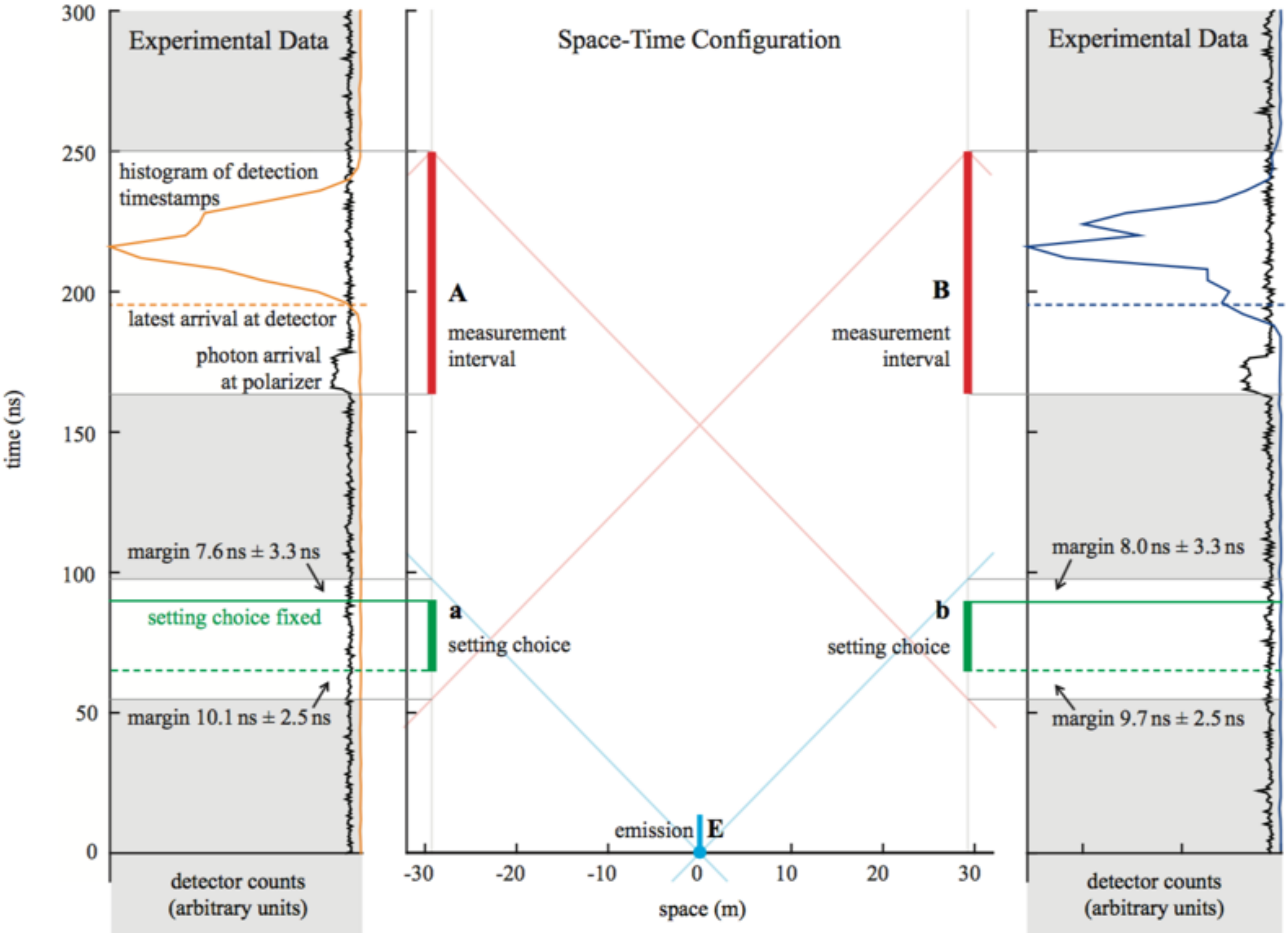
Vienna Experiment



Closing timing loopholes (strengthening the proof)

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.115.250401 arXiv:1511.03190

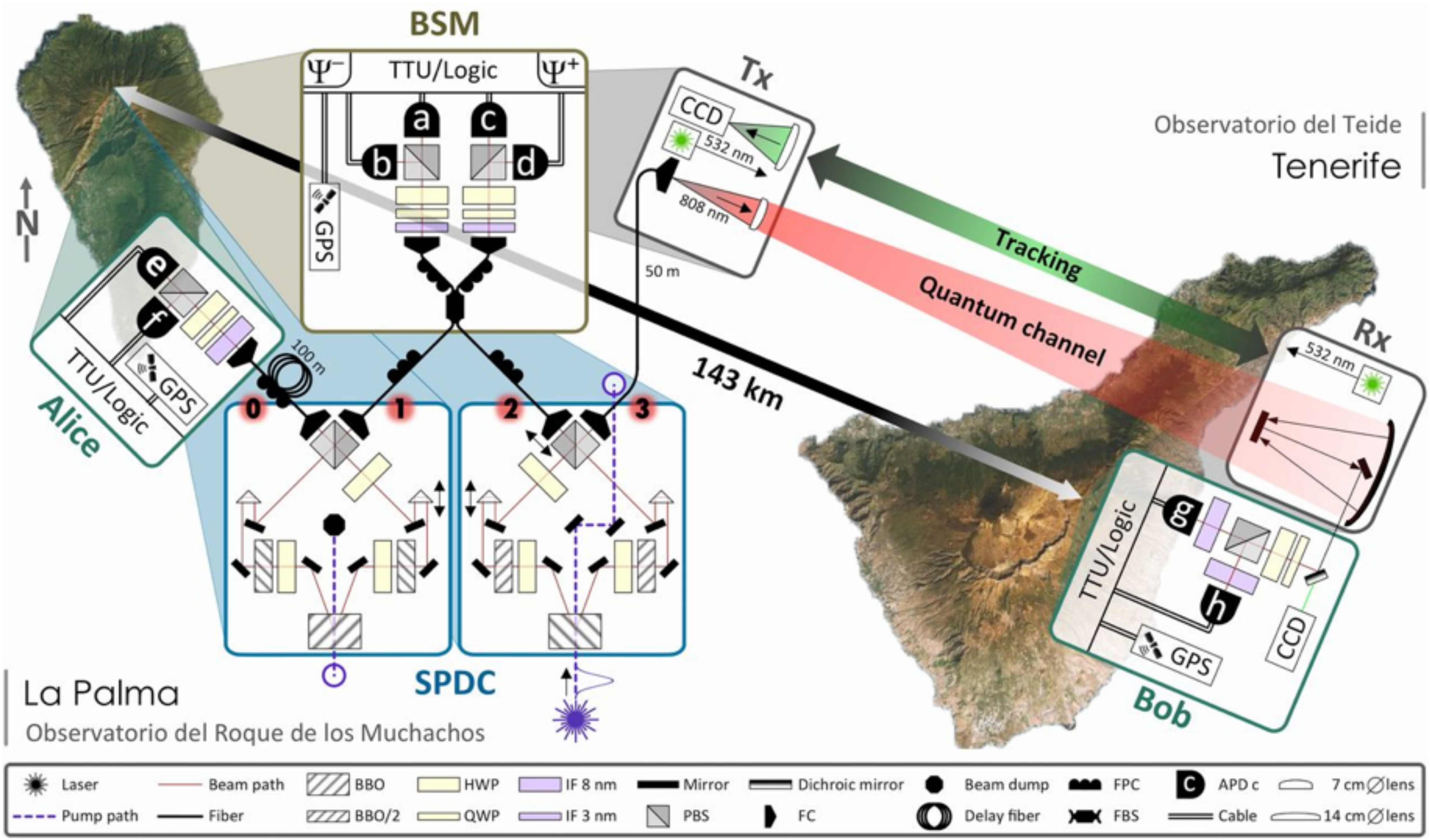
Vienna Experiment



arXiv:1511.03190

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.115.250401

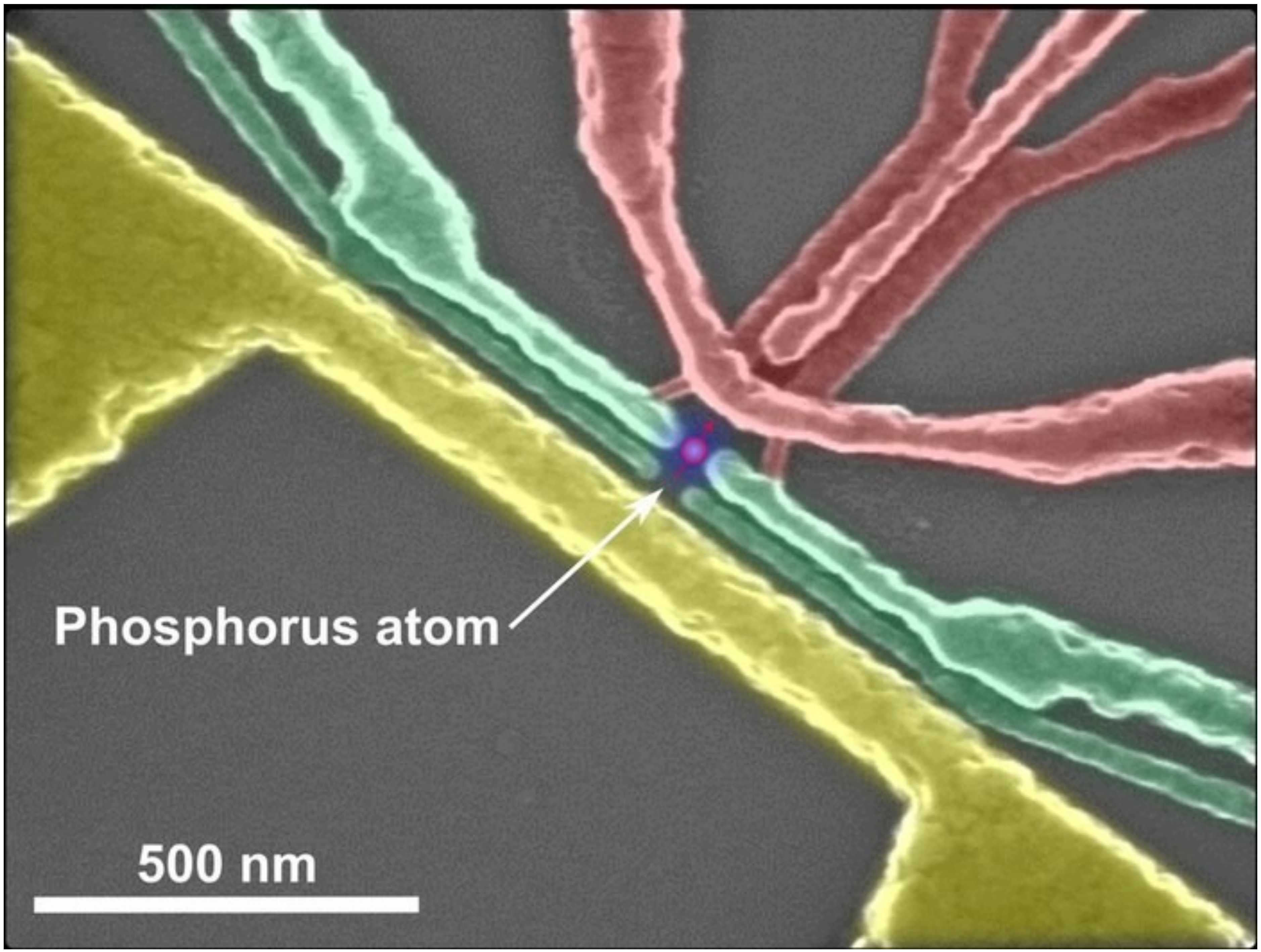
Vienna Experiment #2



Gaining distance and linking two entangled states together!

http://www.pnas.org/content/112/46/14202

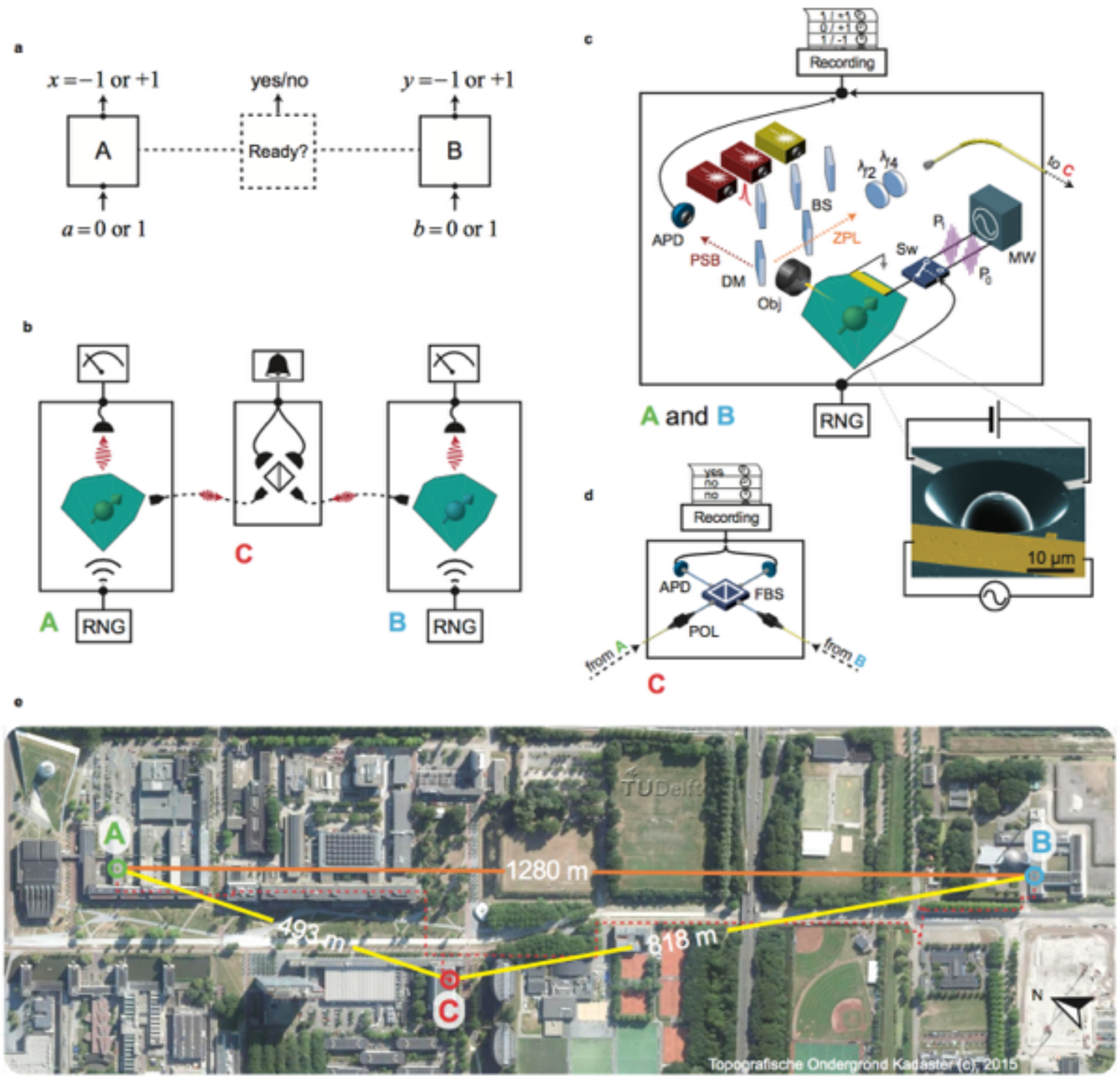
UNSW Experiment



First Bell inequality between two solid-state qubits in a device

http://www.nature.com/nnano/journal/vaop/ncurrent/full/nnano.2015.262.html

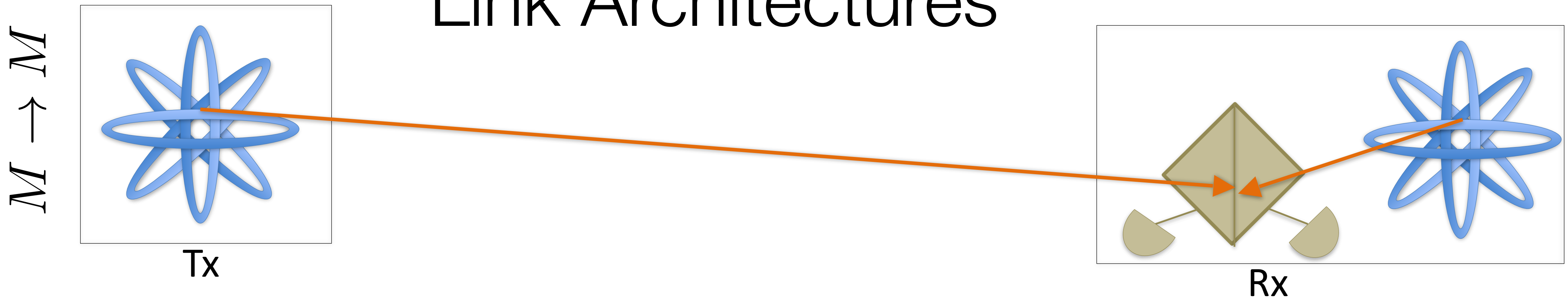
Delft Experiment



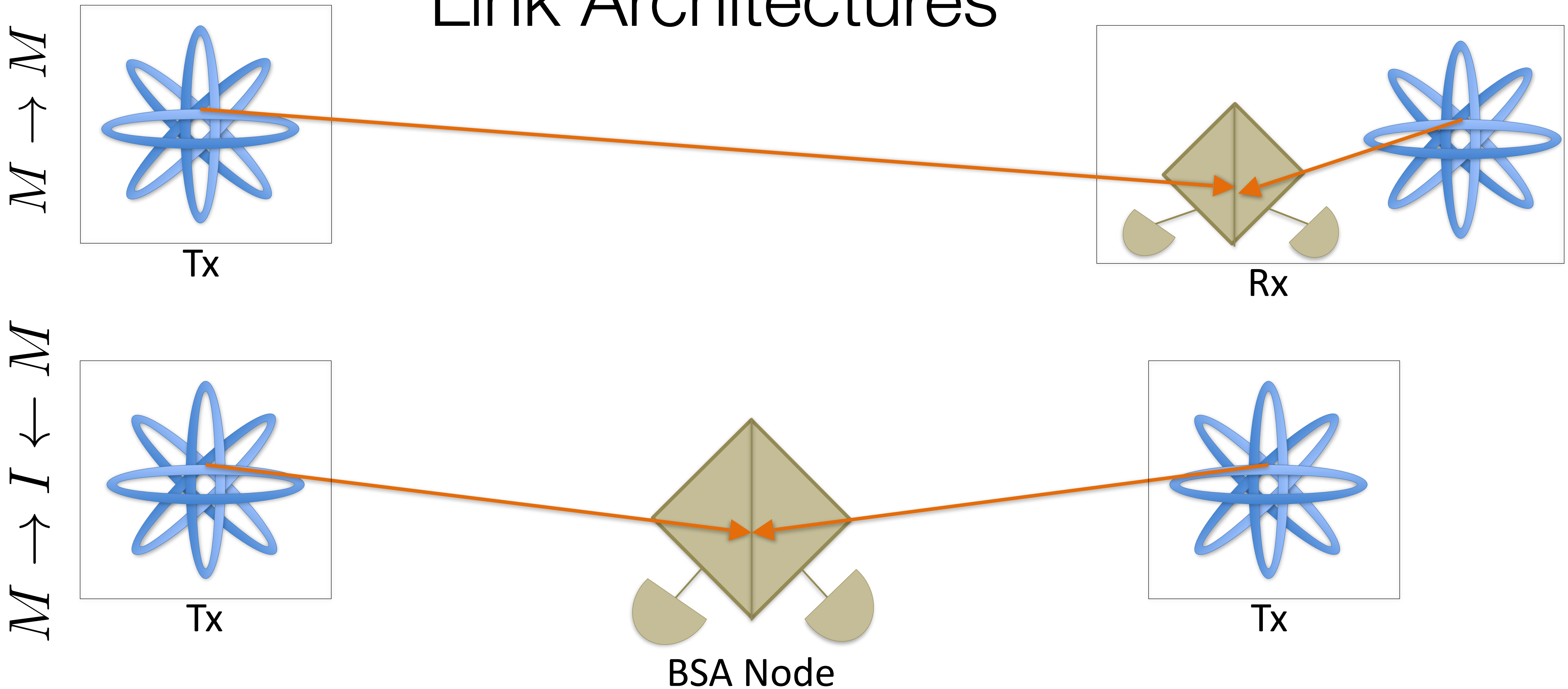
Over 1.3 km using solid-state memories (small pieces of diamond engineered to hold a single extra electron, known as NV centers)

Hensen *et al.*, *Nature,* 29 Oct. 2015

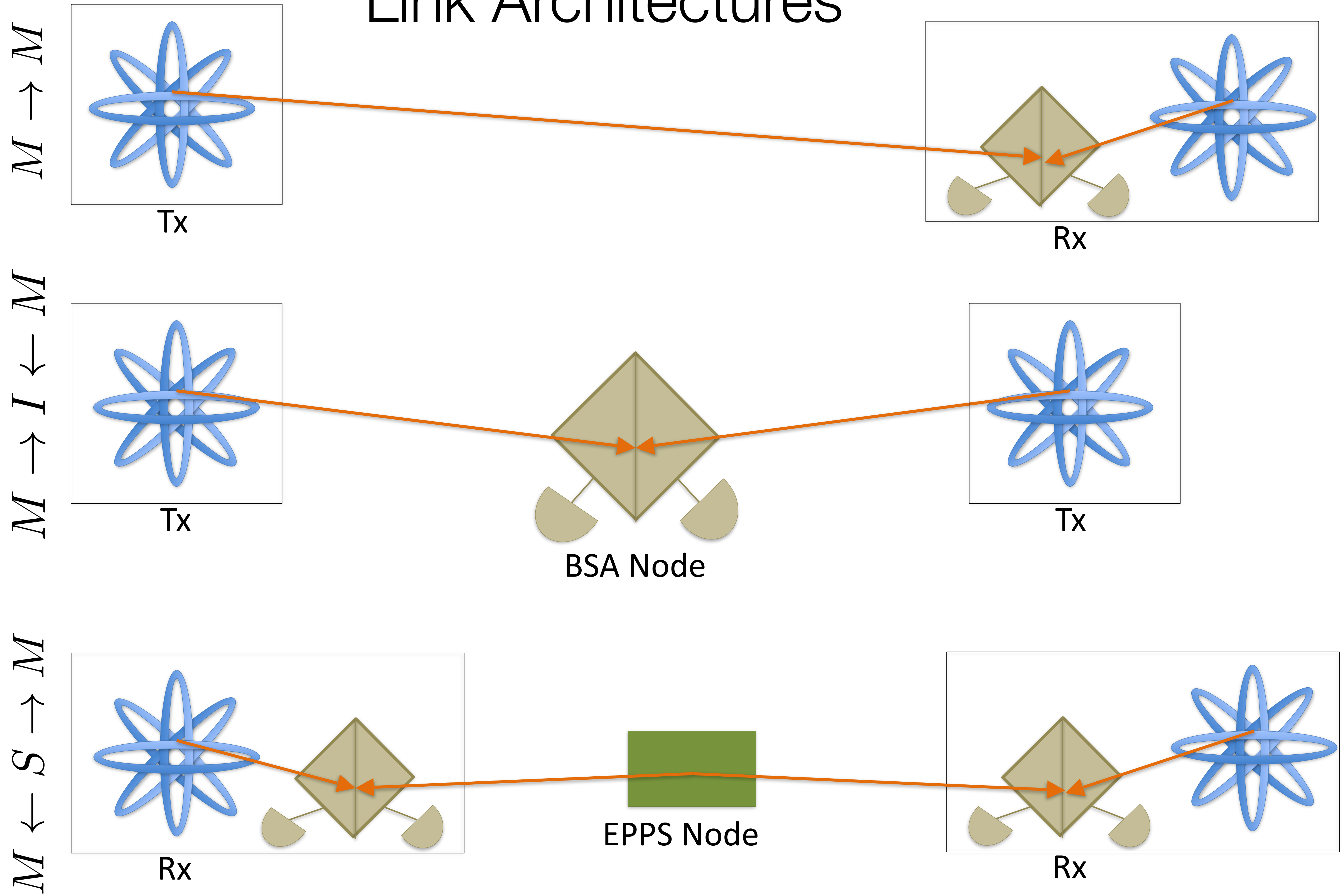
Link Architectures



Link Architectures



Link Architectures



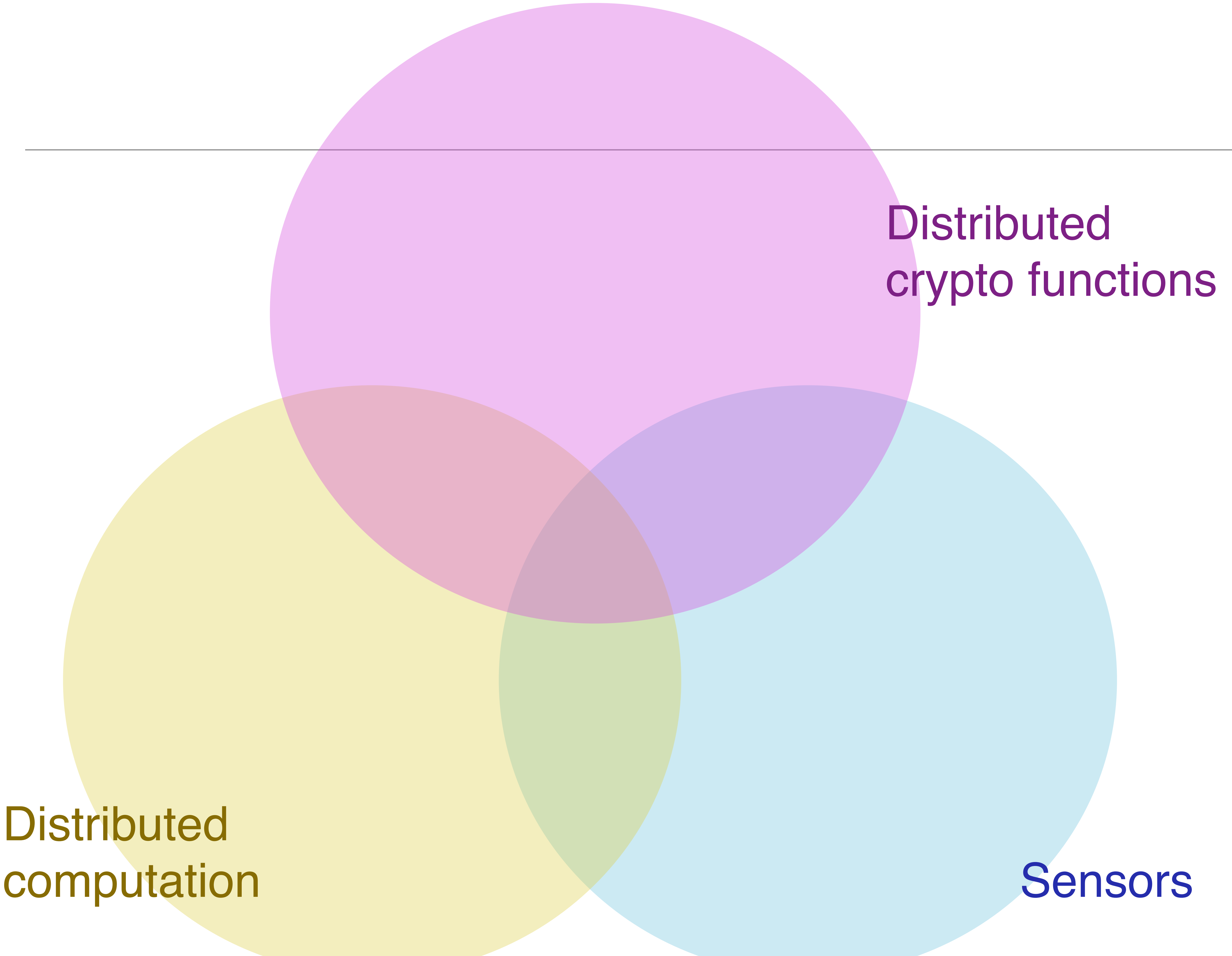
https://qz.com/760804/chinas-new-quantum-satellite-will-try-to-teleport-data-outside-the-bounds-of-space-and-time-and-create-an-unbreakable-code/

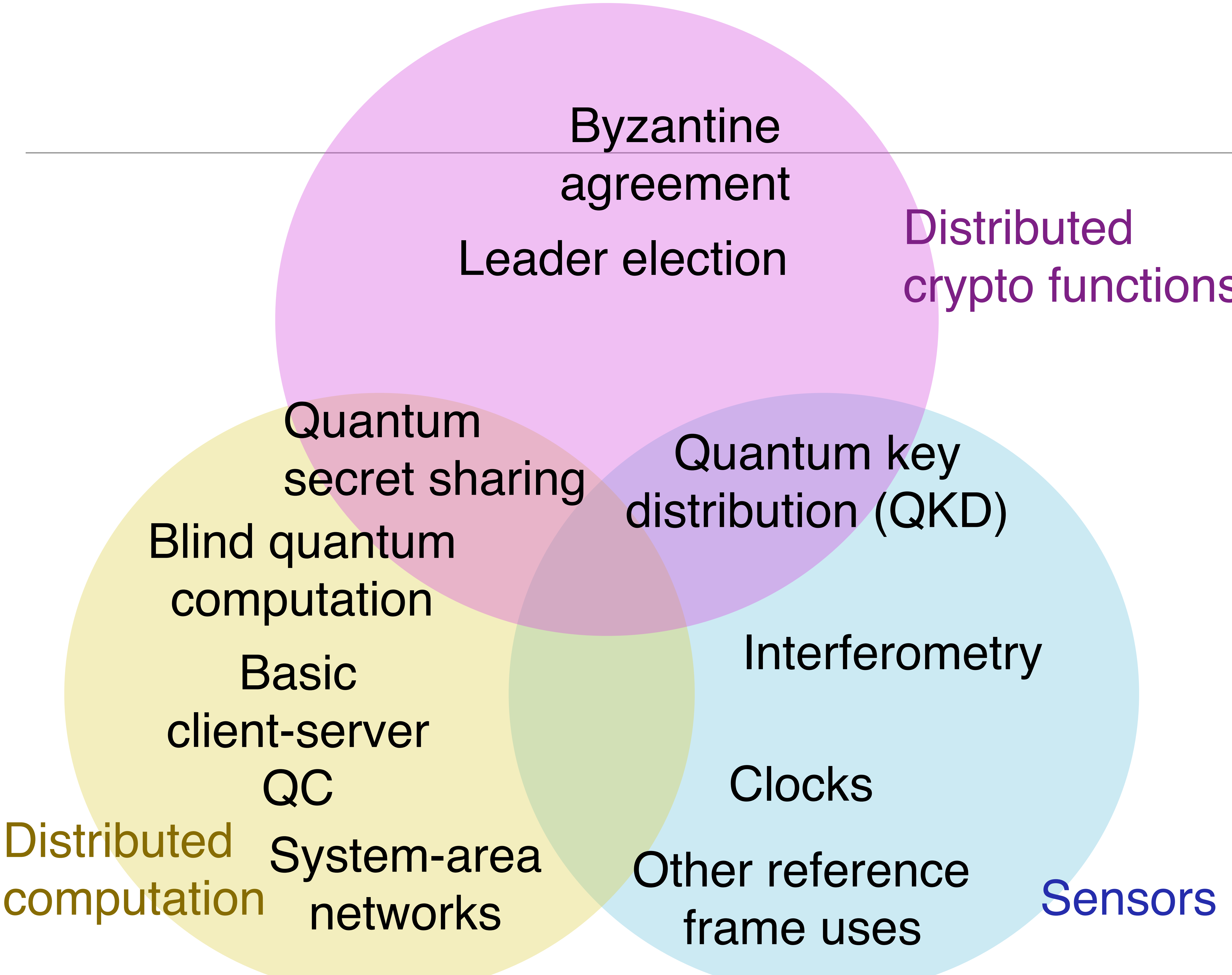
So the job of a quantum repeater network is…

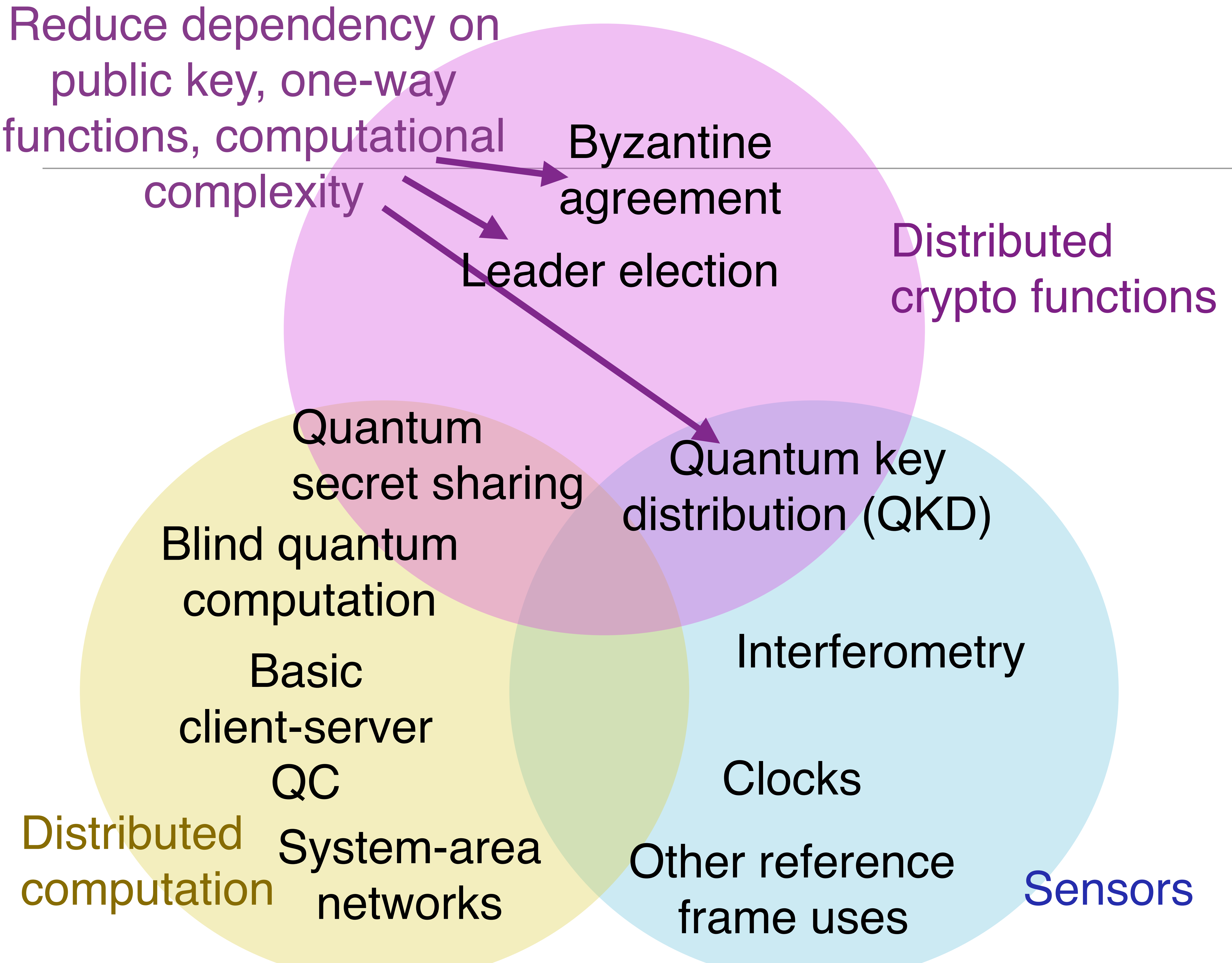
- …to make that entanglement.
- (And, it's a ***consumable resource***, so we have to make lots of it.)
- But what can we do with it if we have it?
—> Well, obviously, test quantum theory!
But what else?

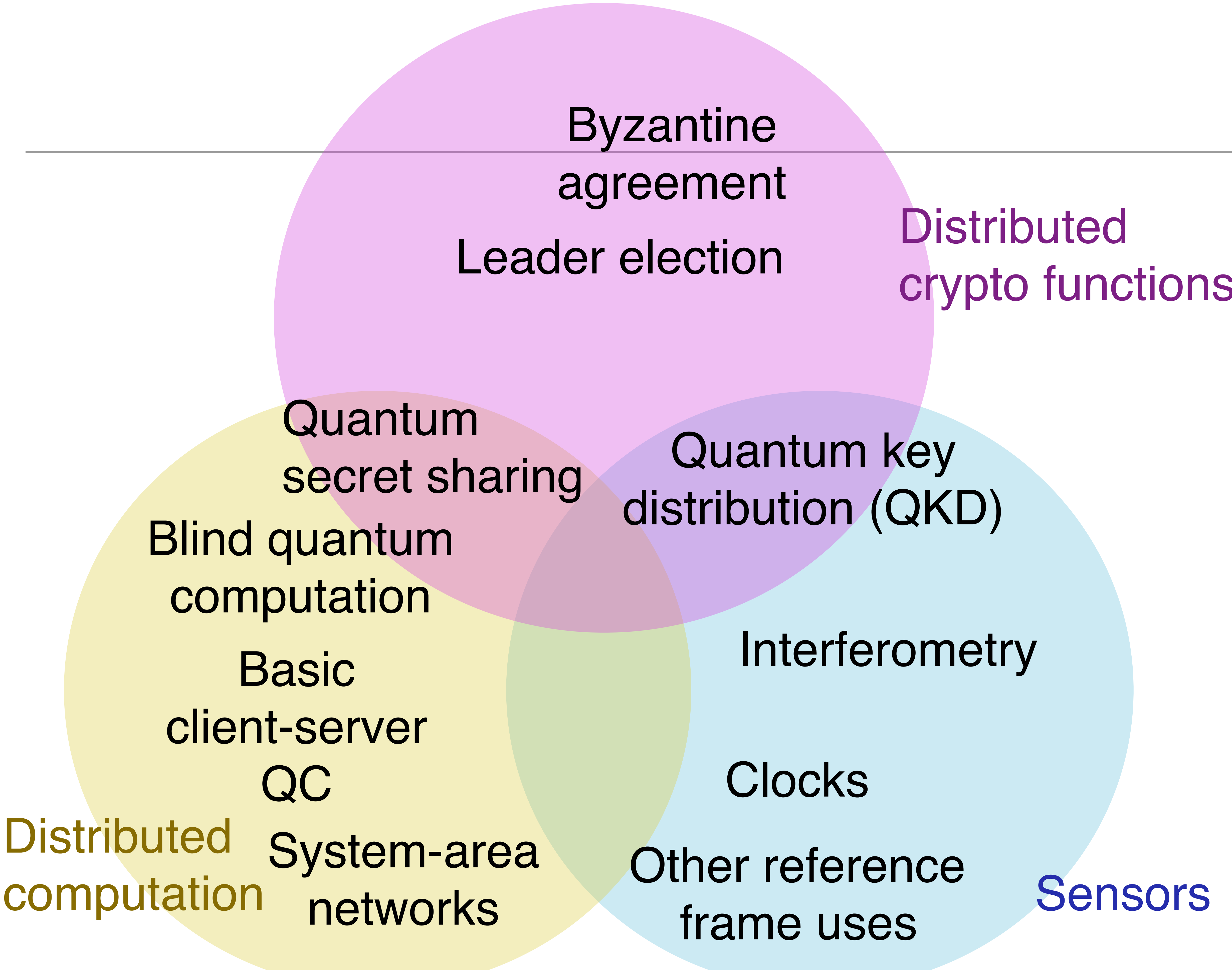
Outline

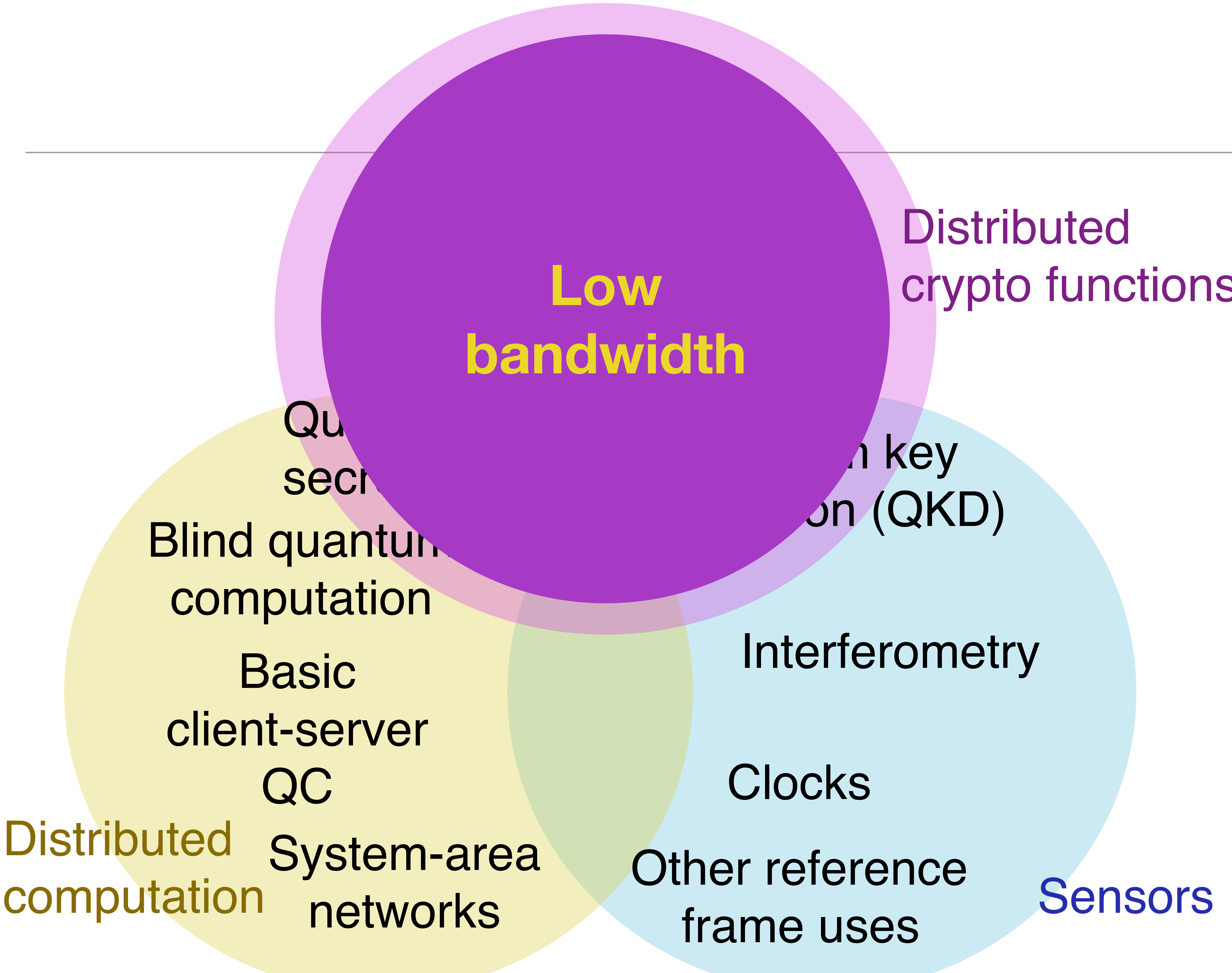
- Background: entanglement & teleportation
- **Applications of quantum networks**
- Lines of repeaters
- Networks & internetworks of repeaters

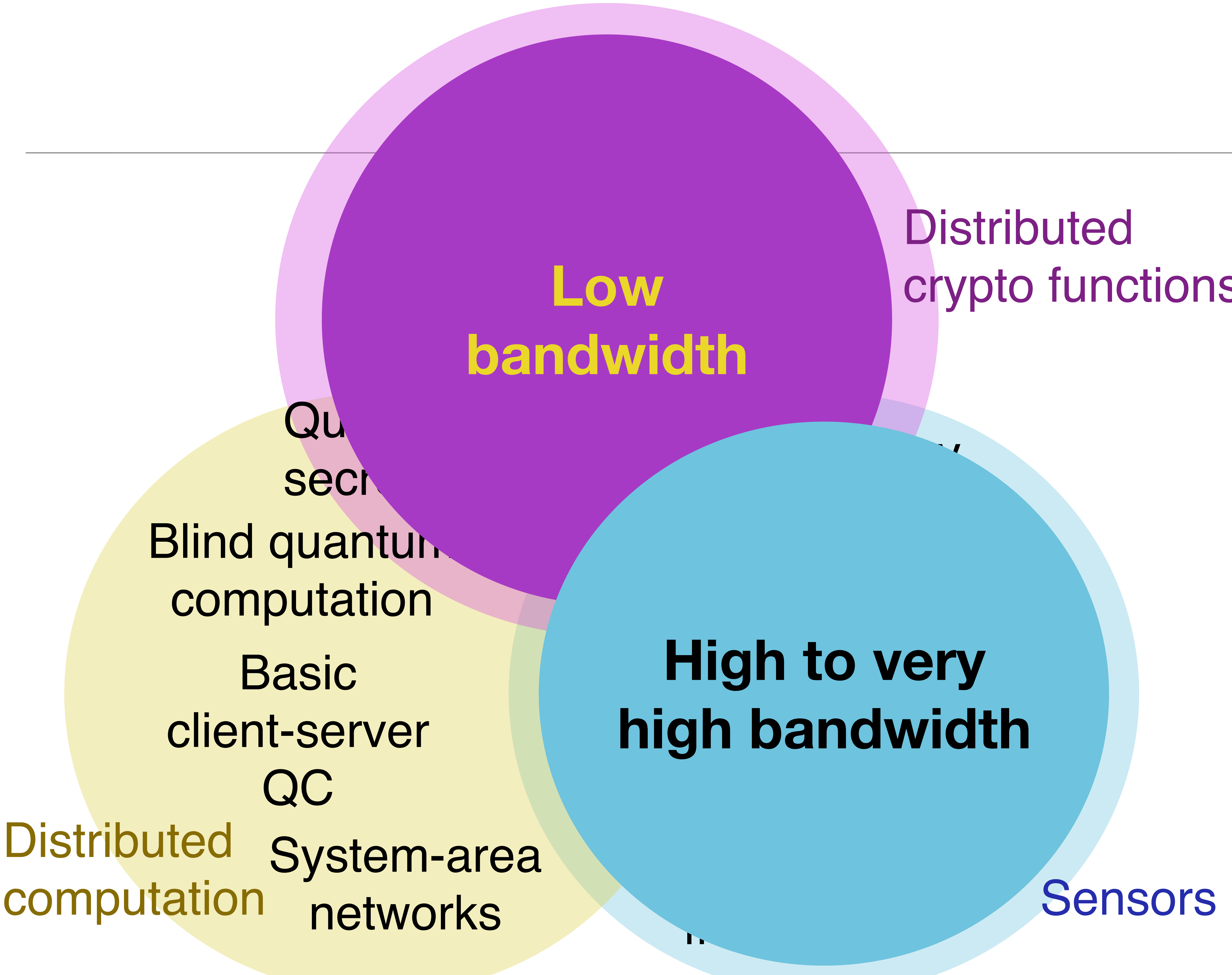

Distributed
crypto functions
Distributed
computation
Sensors

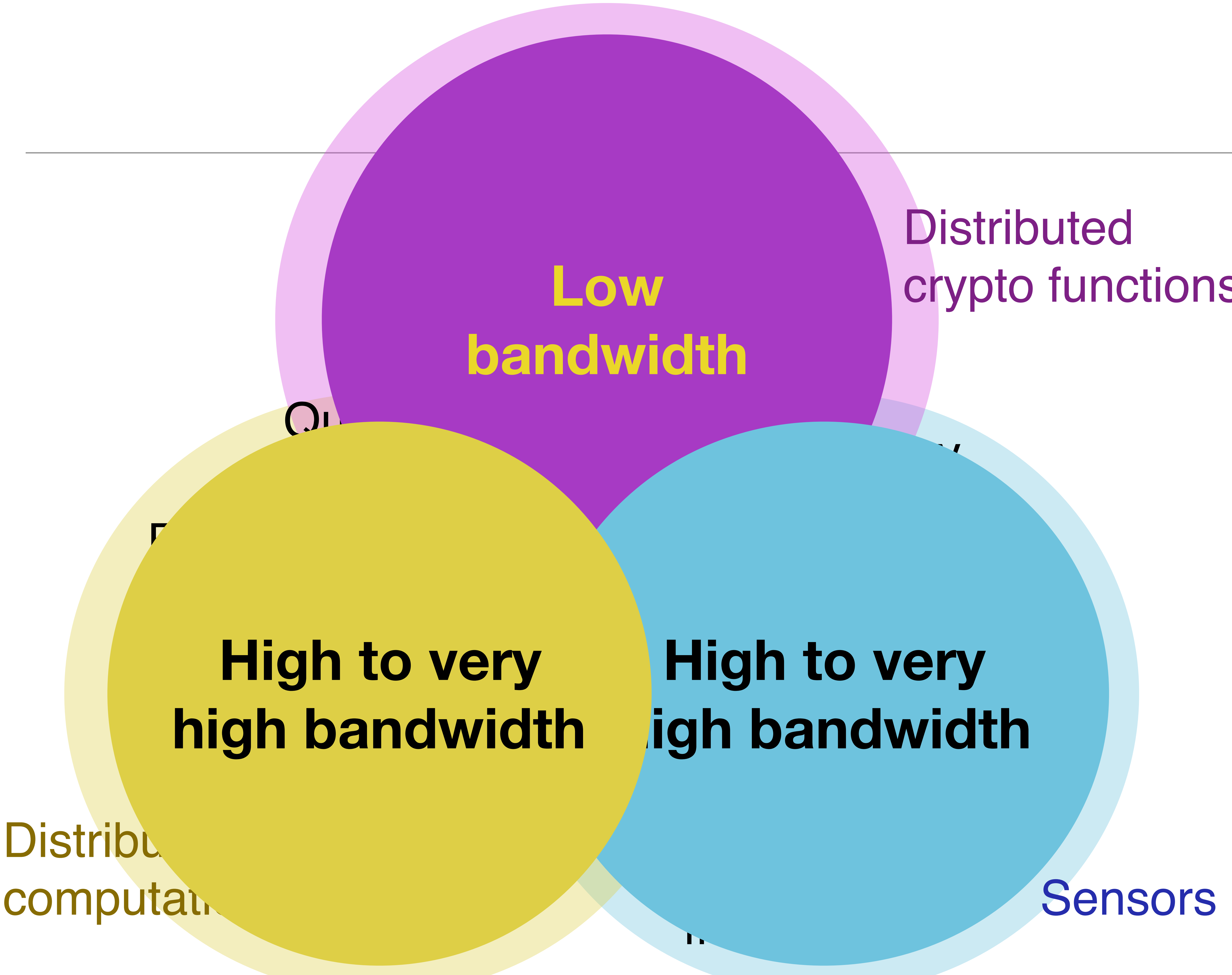

Byzantine agreement
Leader election
Distributed crypto functions
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors


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
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors

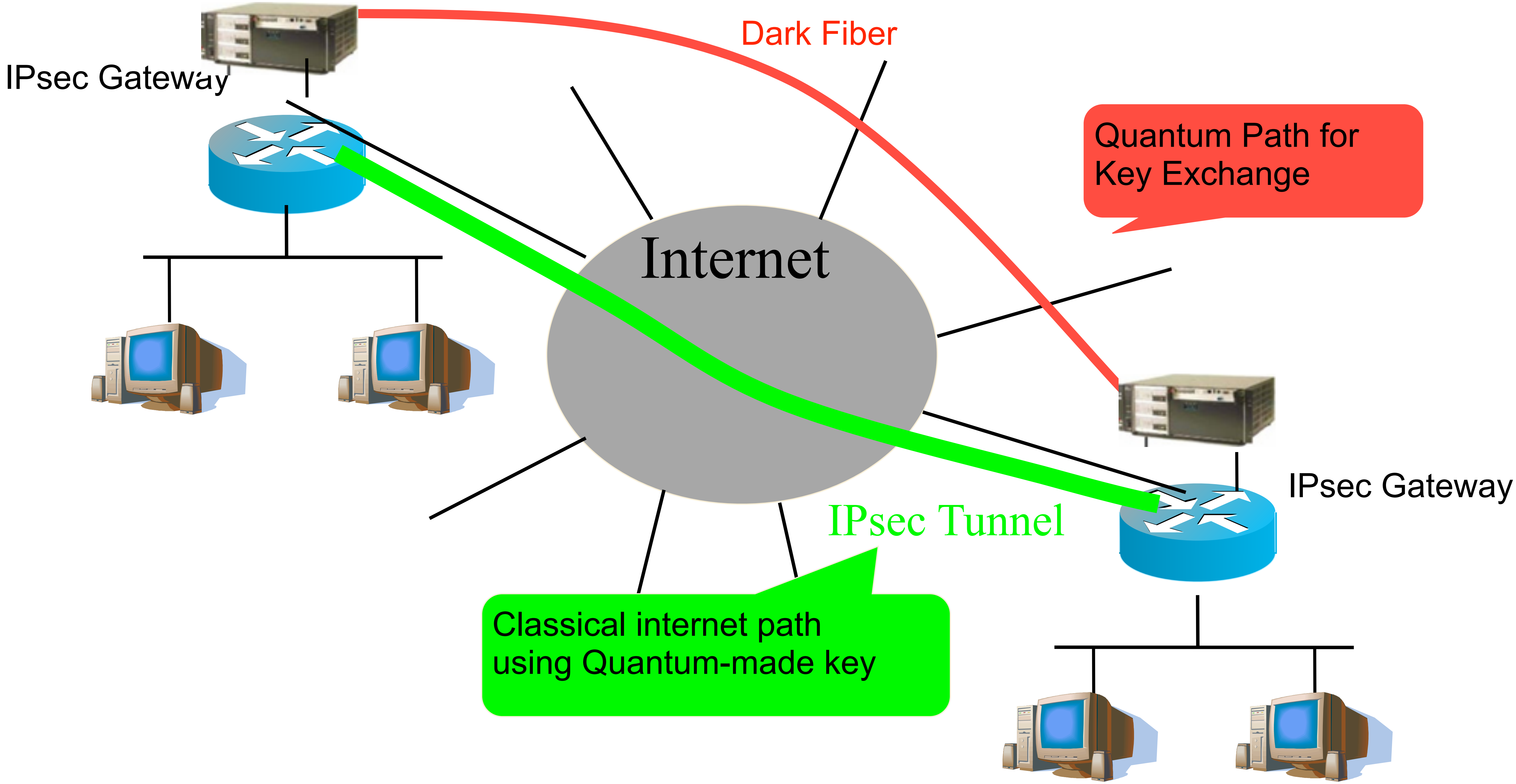

Byzantine agreement
Leader election
Distributed crypto functions
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors


Low
bandwidth
Distributed
crypto functions
Qu
secr
n key
on (QKD)
Blind quantum
computation
Basic
client-server
QC
System-area
networks
Distributed
computation
Interferometry
Clocks
Other reference
frame uses
Sensors


Low
bandwidth
Distributed
crypto functions
Blind
computation
Basic
client-server
QC
Distributed
computation
System-area
networks
High to very
high bandwidth
Sensors

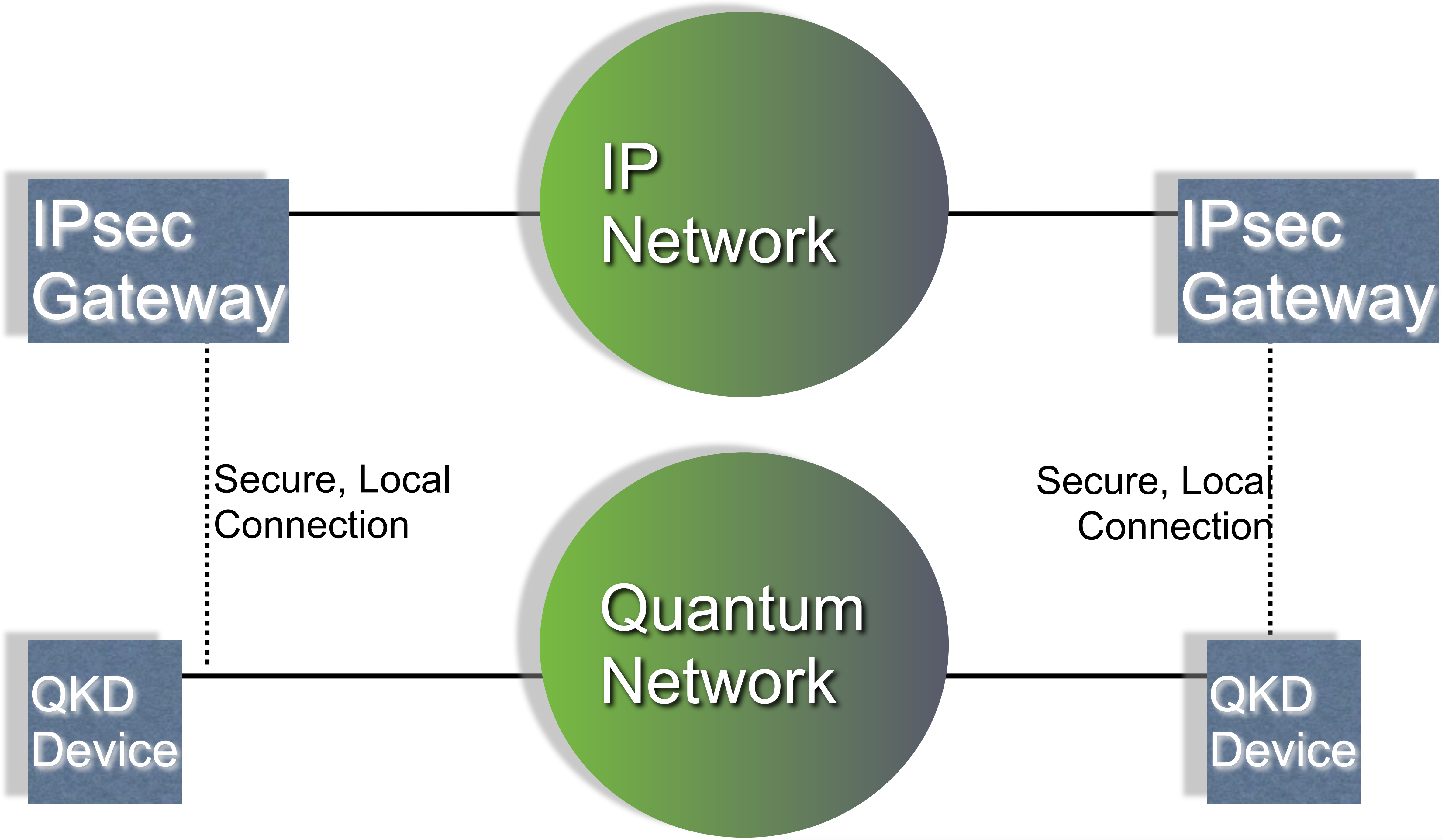

Low
bandwidth
High to very
high bandwidth
High to very
high bandwidth
Distributed
crypto functions
Distribu
computati
Sensors

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

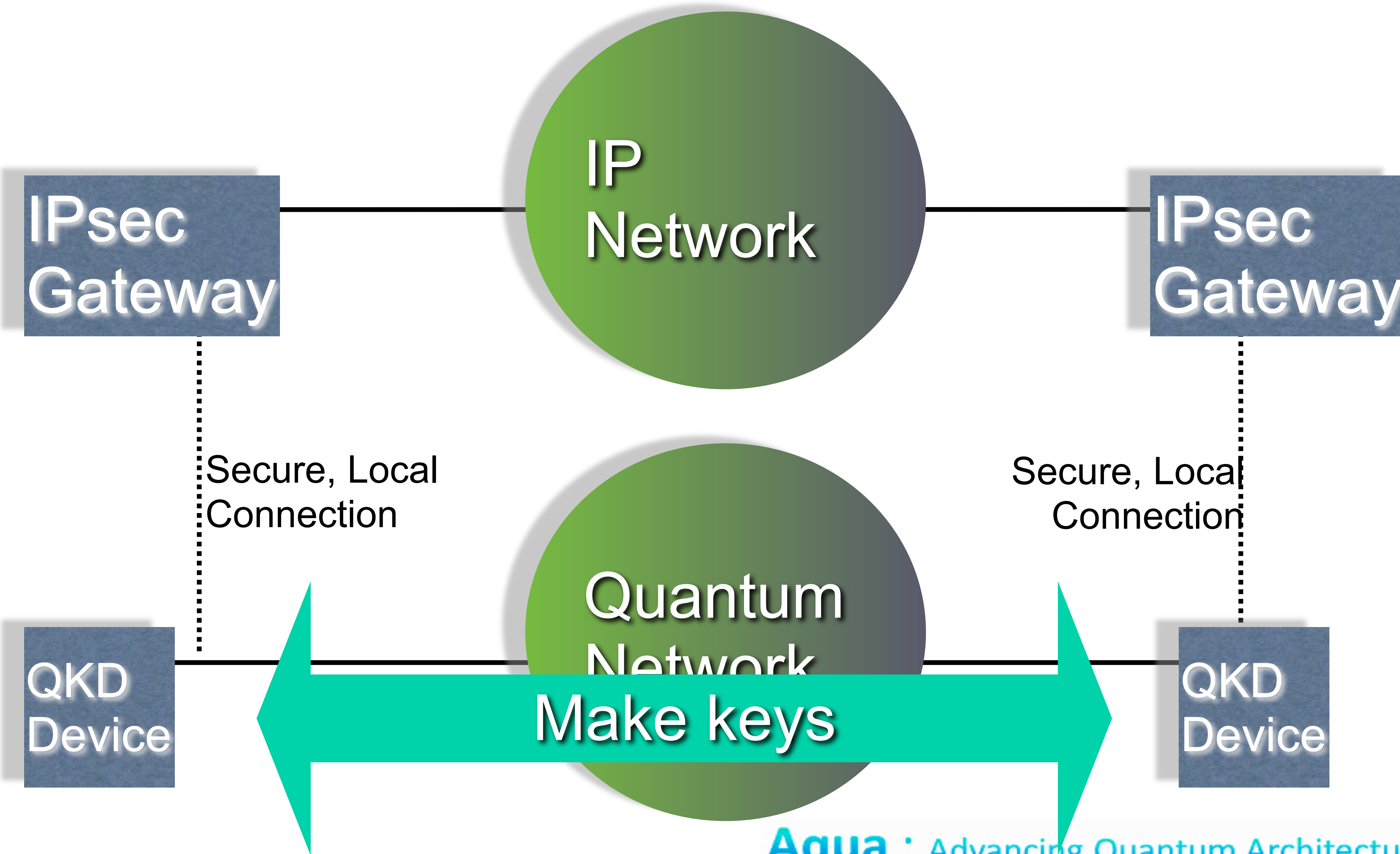


draft-nagayama-ipsecme-ike-with-qkd-01.txt, 2014/10

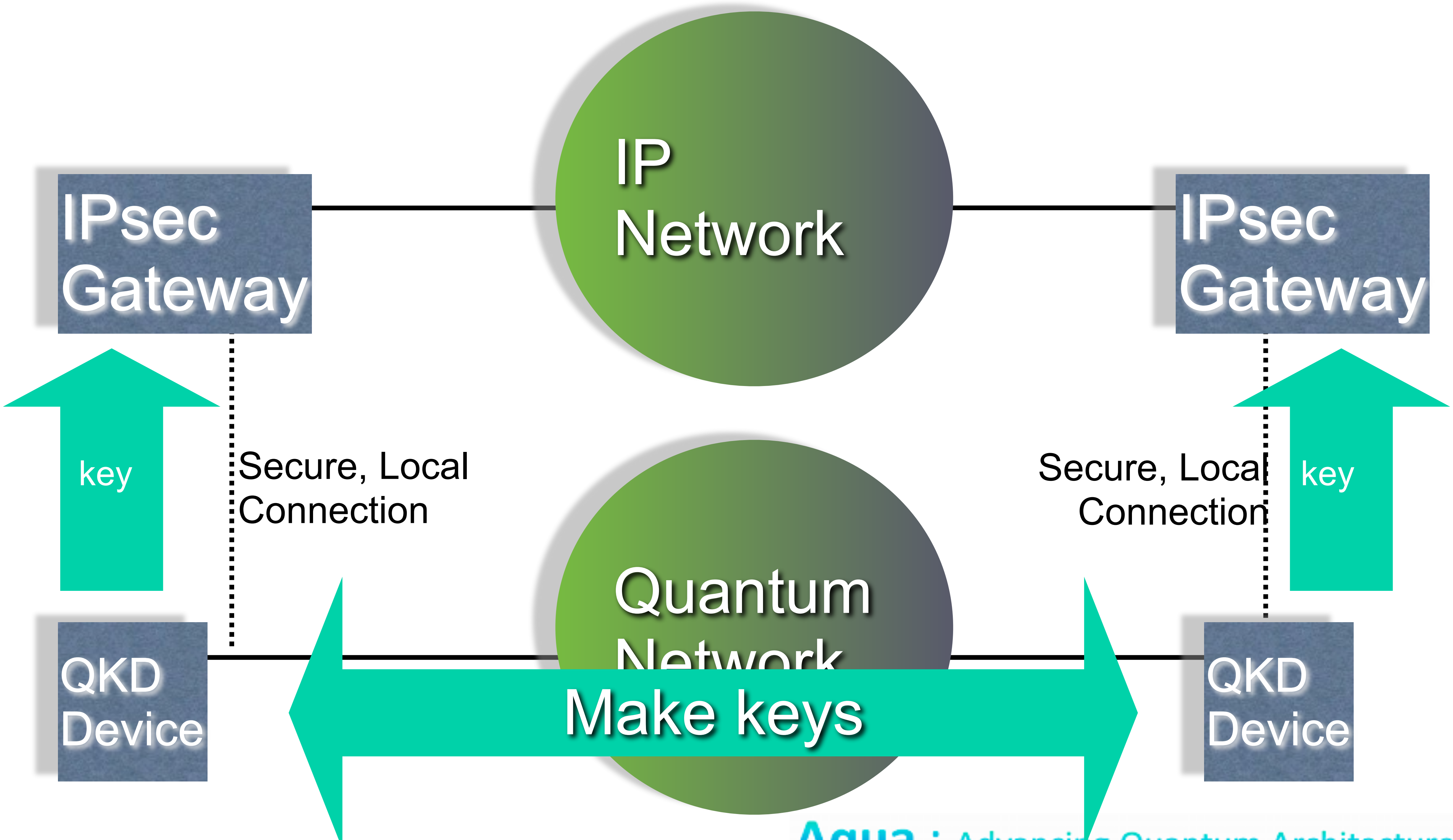
IPsec with QKD



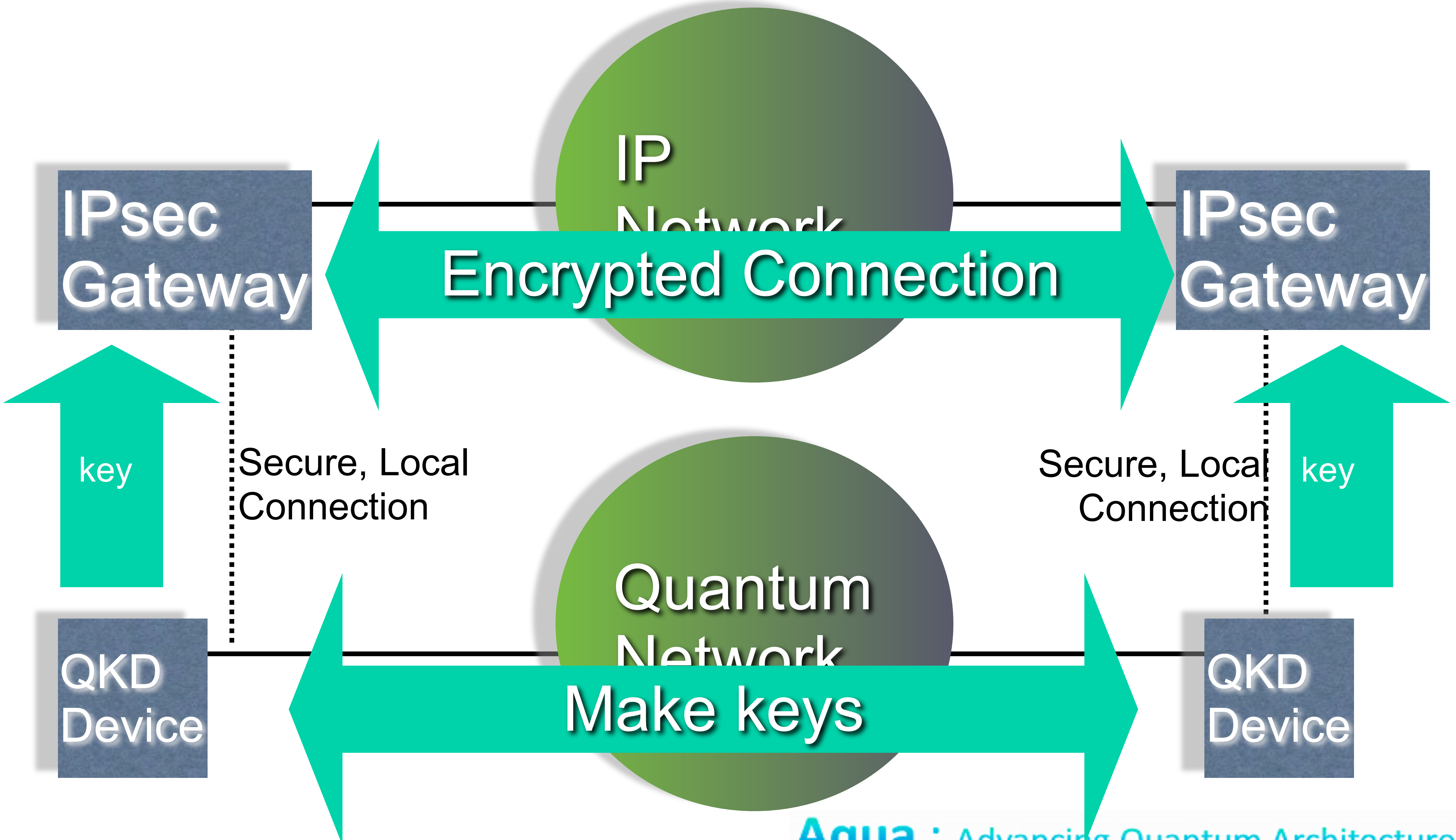
IPsec with QKD



IPsec with QKD

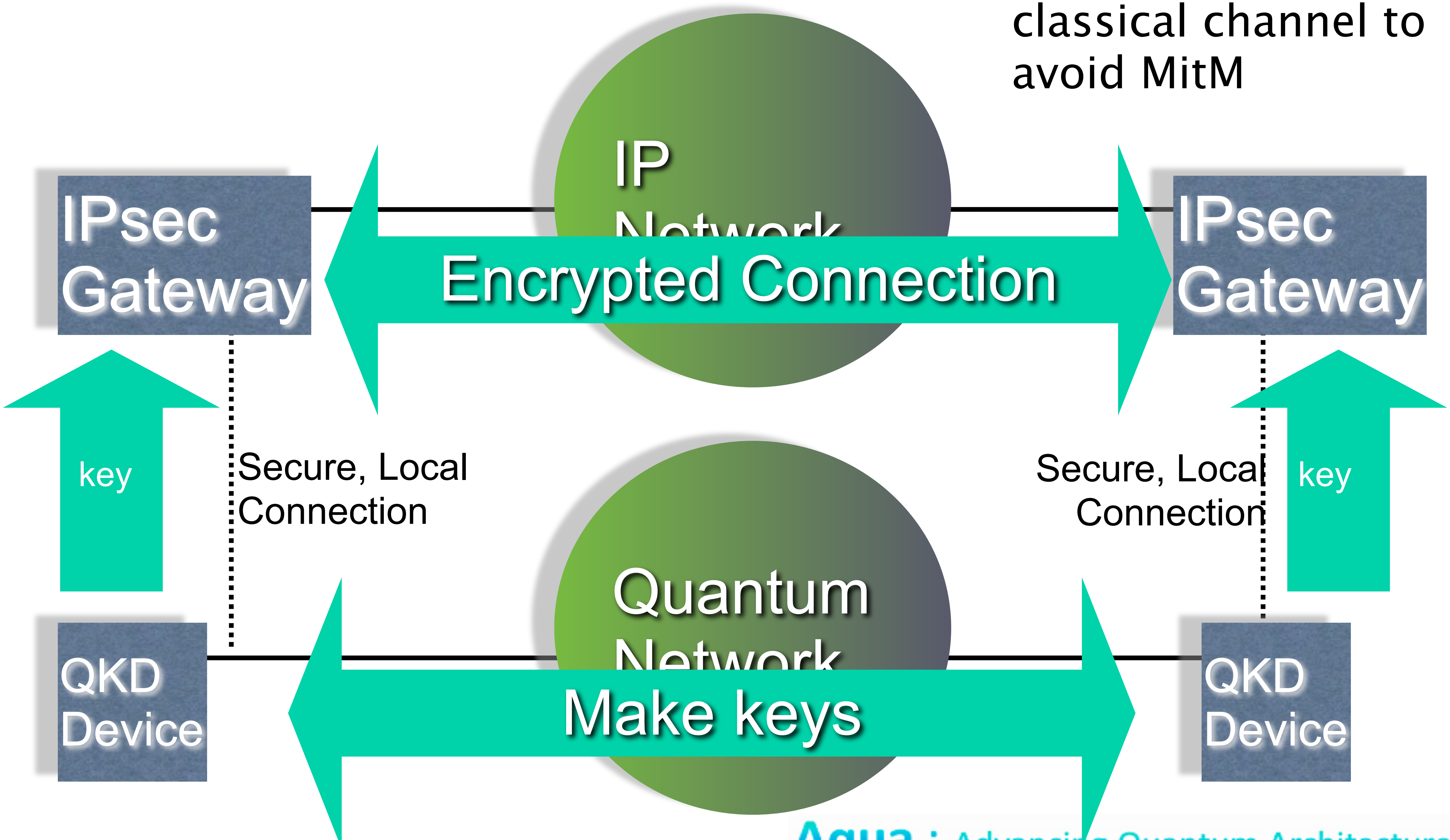


IPsec with QKD



IPsec with QKD

n.b.: QKD requires an authenticated (but not secret) classical channel to avoid MitM



D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

D-H +
AES

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

D-H + AES

QKD + AES

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

D-H + AES

QKD + AES

QKD + super-AES

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

D-H +
AES

QKD +
AES

QKD +
super-AES

QKD +
OTP

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

Data encrypted today

D-H + AES

QKD + AES

QKD + super-AES

QKD + OTP

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

Factoring becomes possible

Data encrypted today

D-H + AES

QKD + AES

QKD + super-AES

QKD + OTP

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

Factoring becomes possible

AES broken

Data encrypted today

D-H + AES

QKD + AES

QKD + super-AES

QKD + OTP

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

Data encrypted today

Factoring becomes possible

AES broken

testing all keys becomes possible

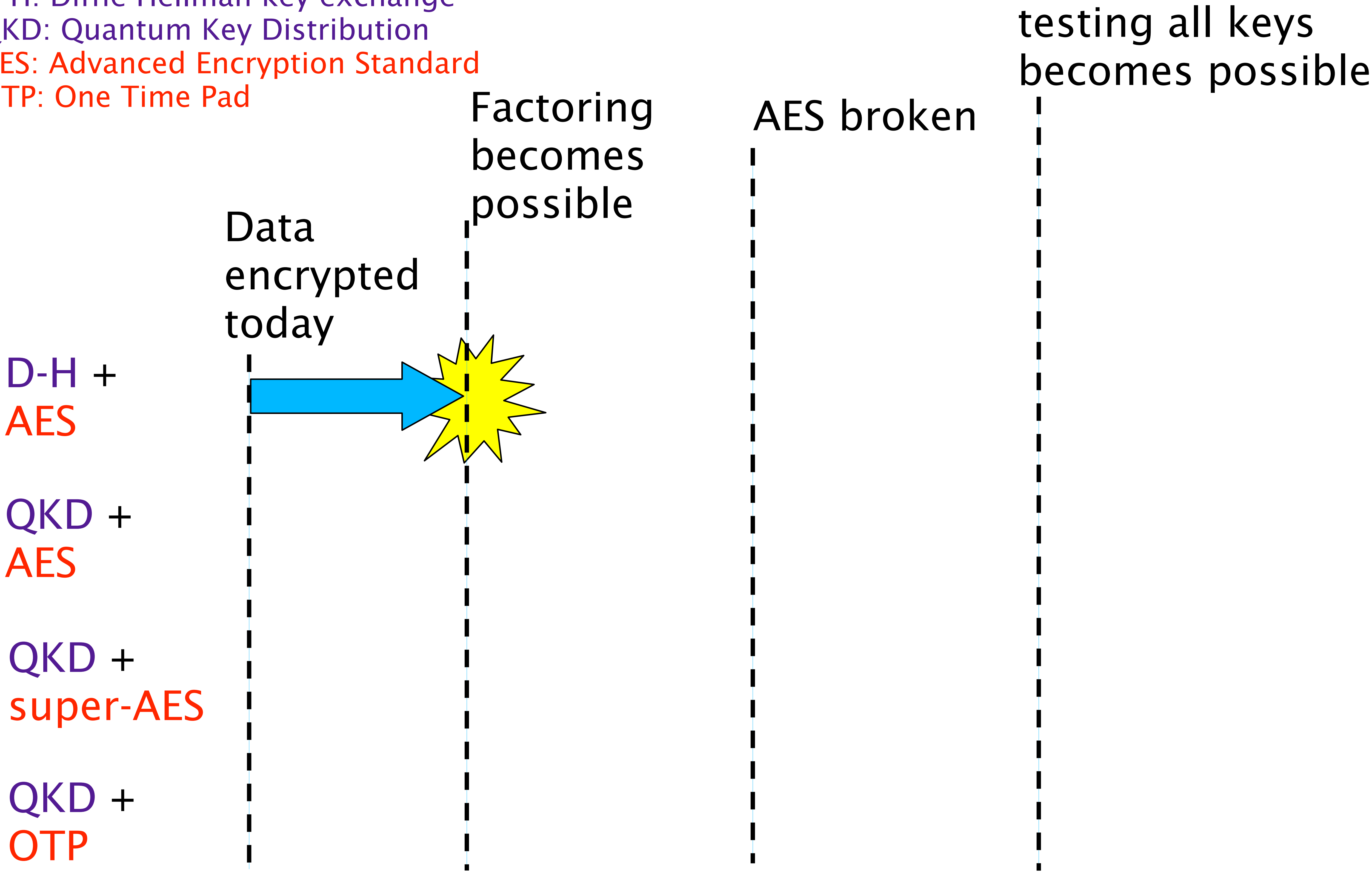
D-H + AES

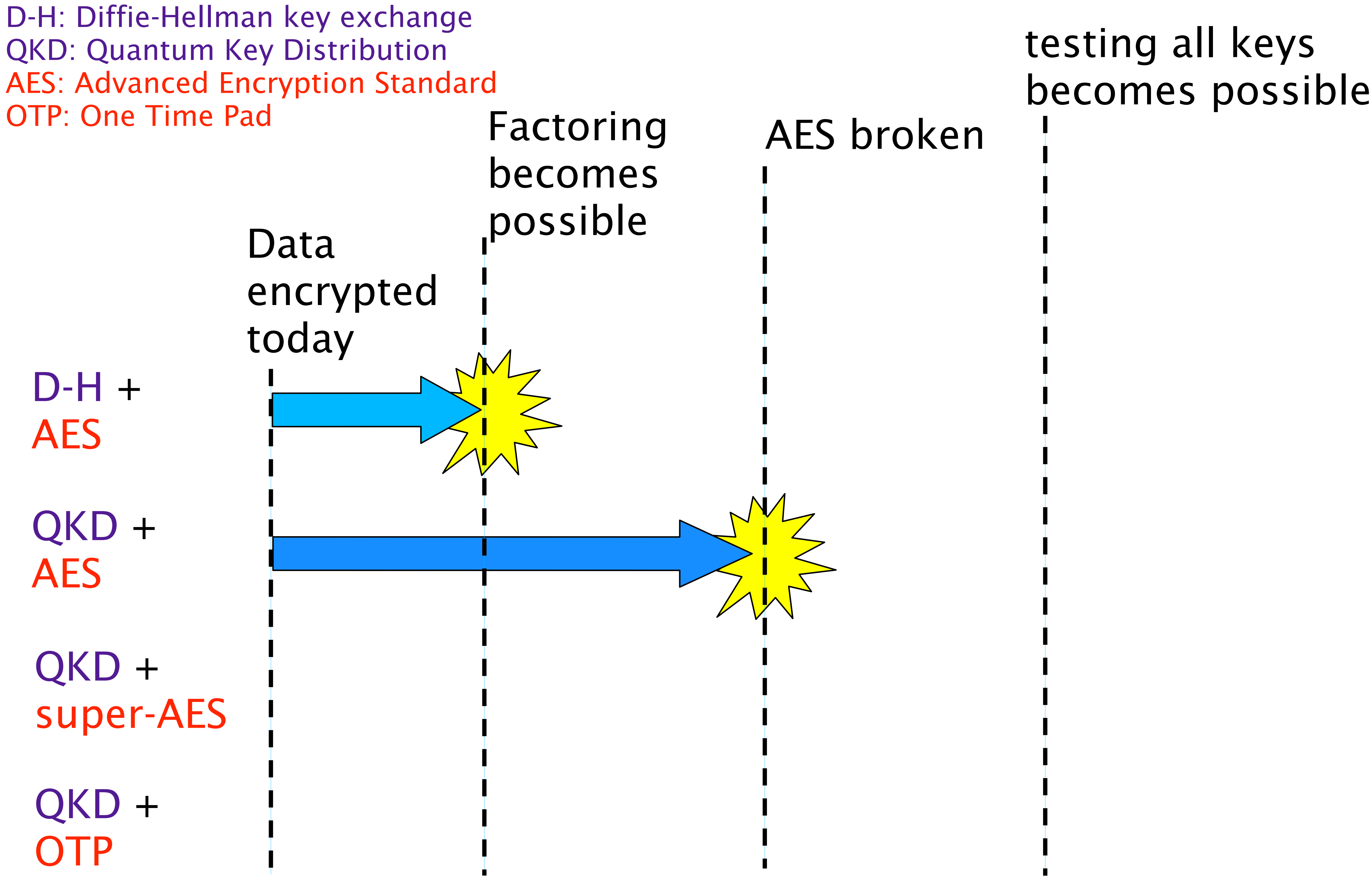
QKD + AES

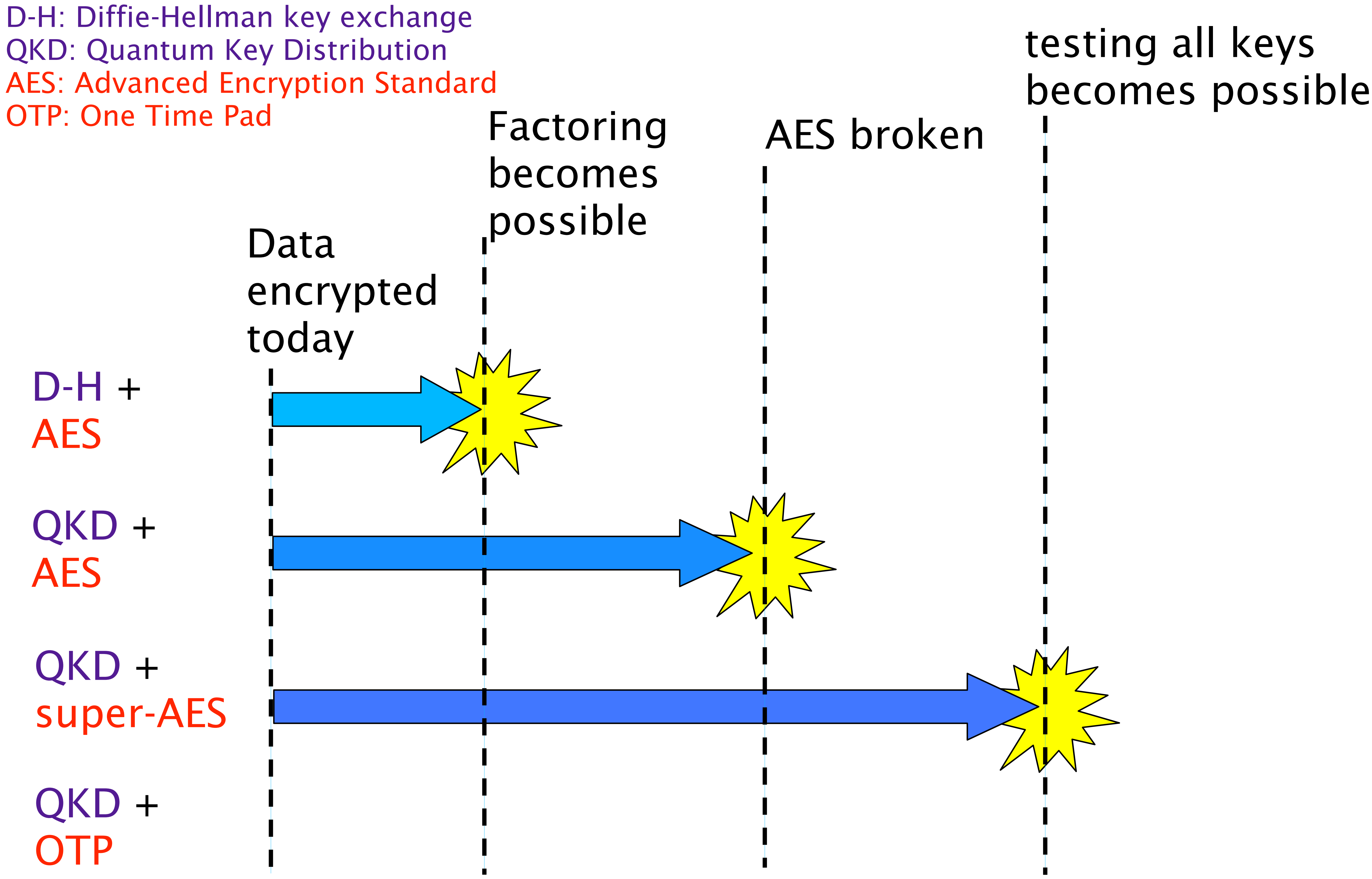
QKD + super-AES

QKD + OTP

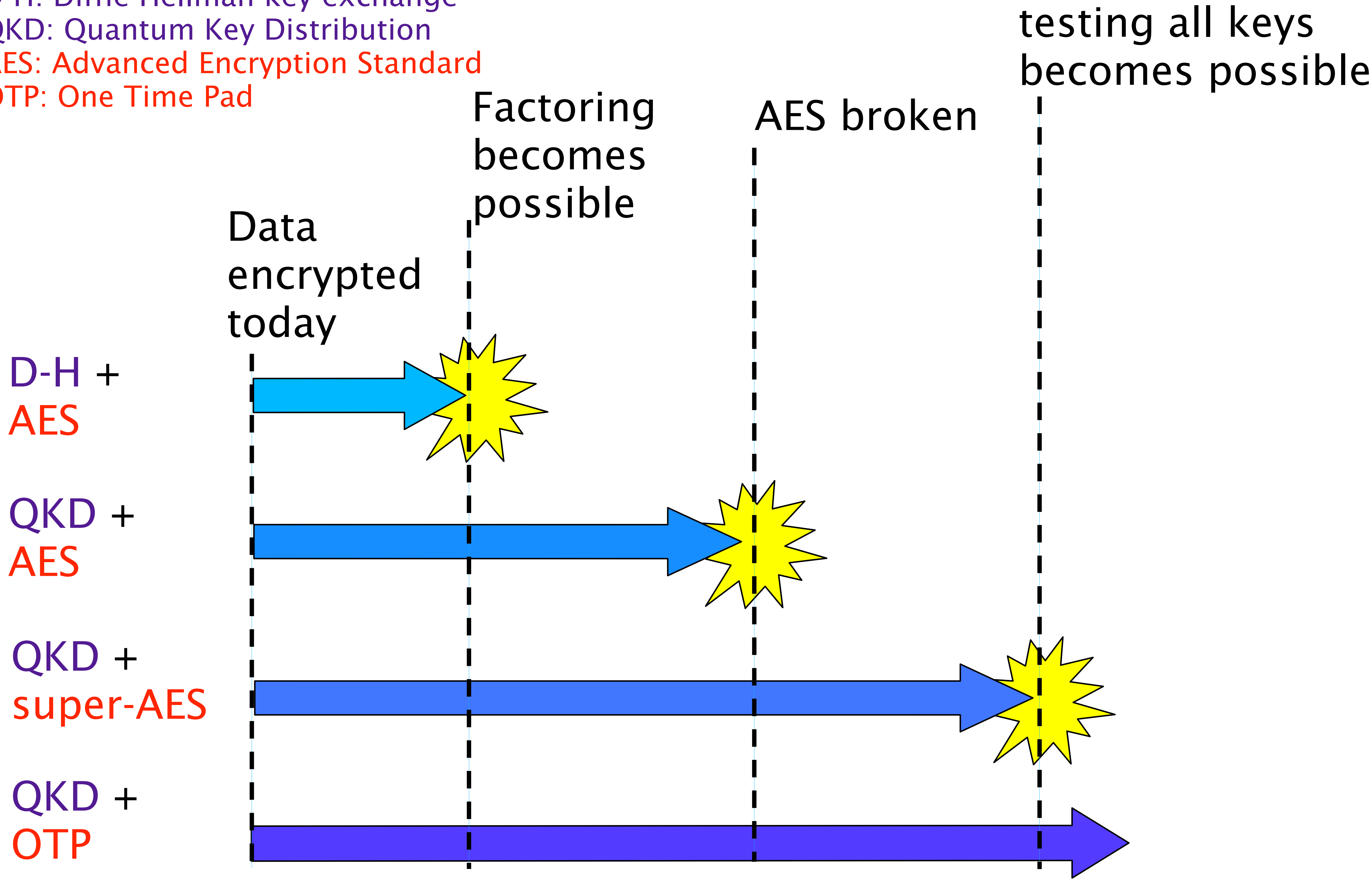
D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

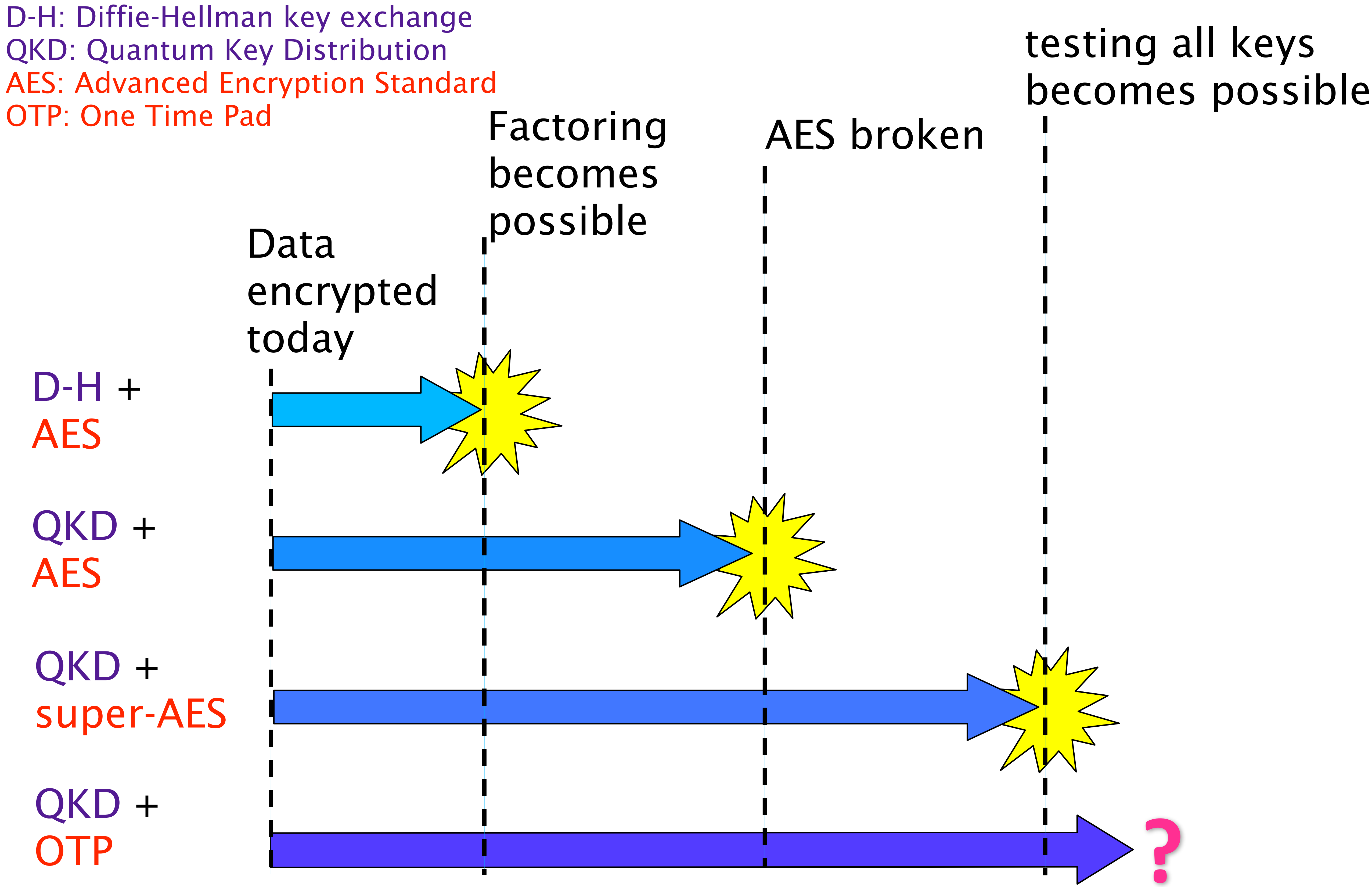



D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad
testing all keys becomes possible
Factoring becomes possible
AES broken
Data encrypted today
D-H + AES
QKD + AES
QKD + super-AES
QKD + OTP

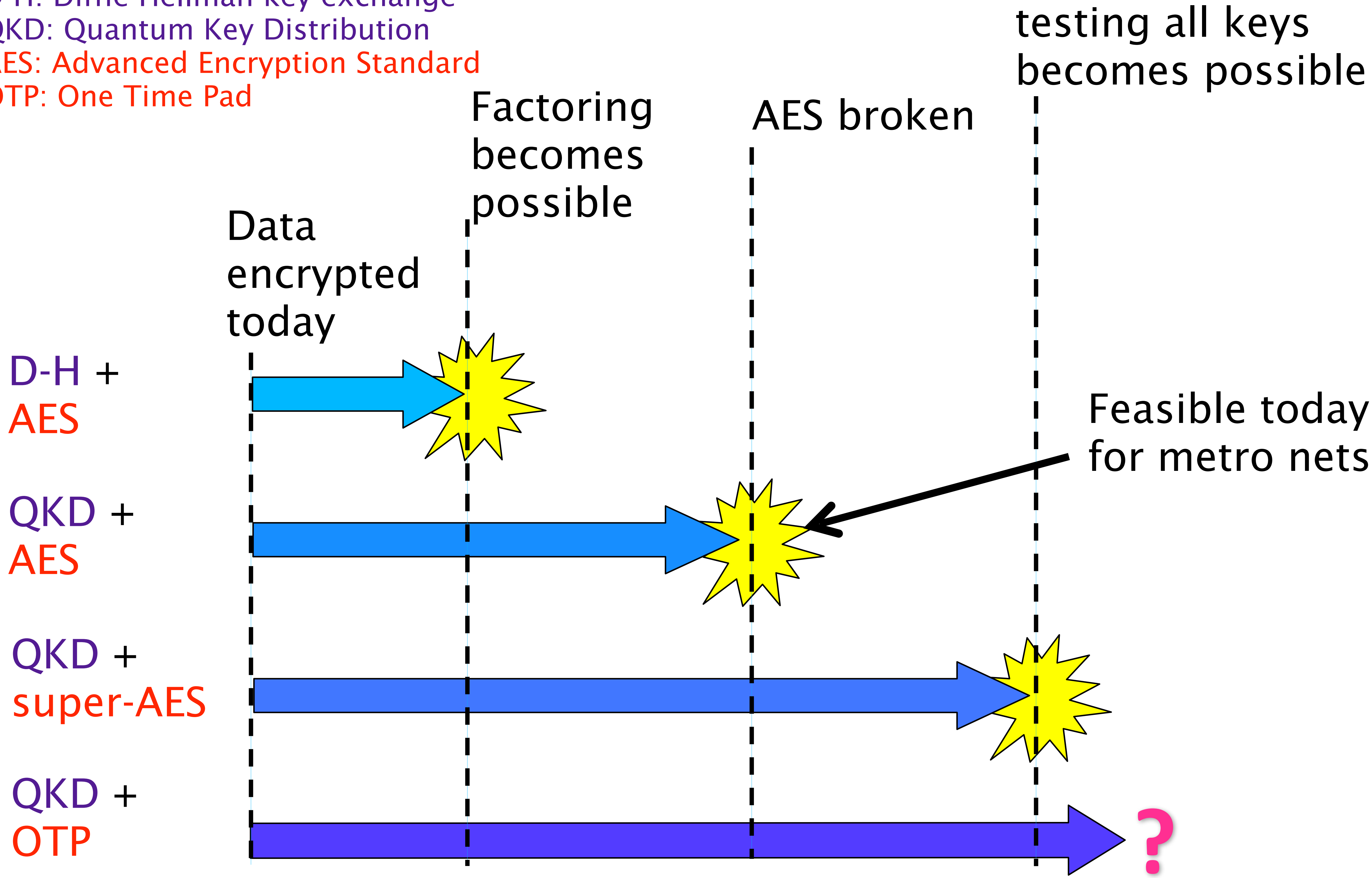

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad
testing all keys becomes possible
Factoring becomes possible
AES broken
Data encrypted today
D-H + AES
QKD + AES
QKD + super-AES
QKD + OTP

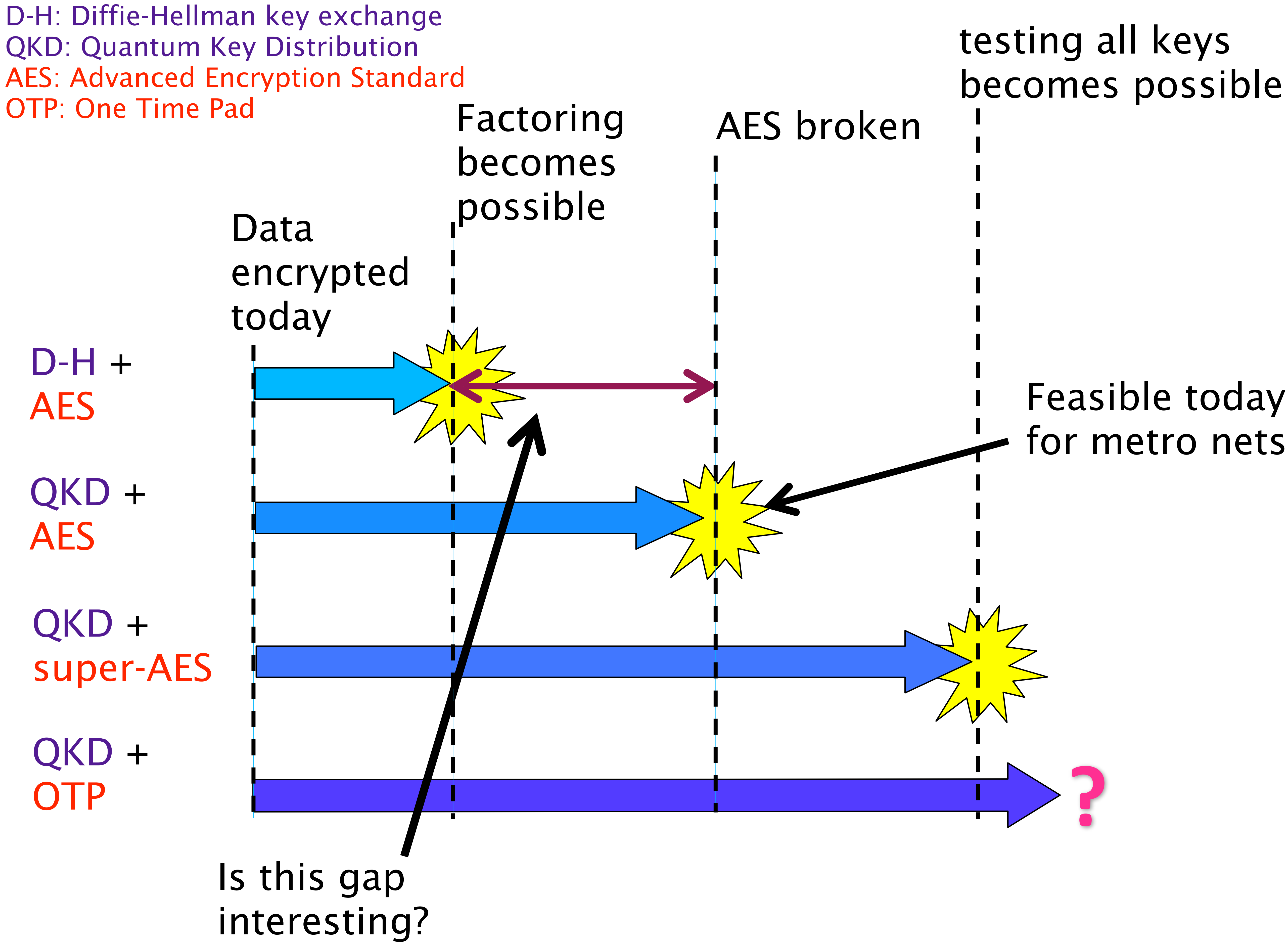
D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad



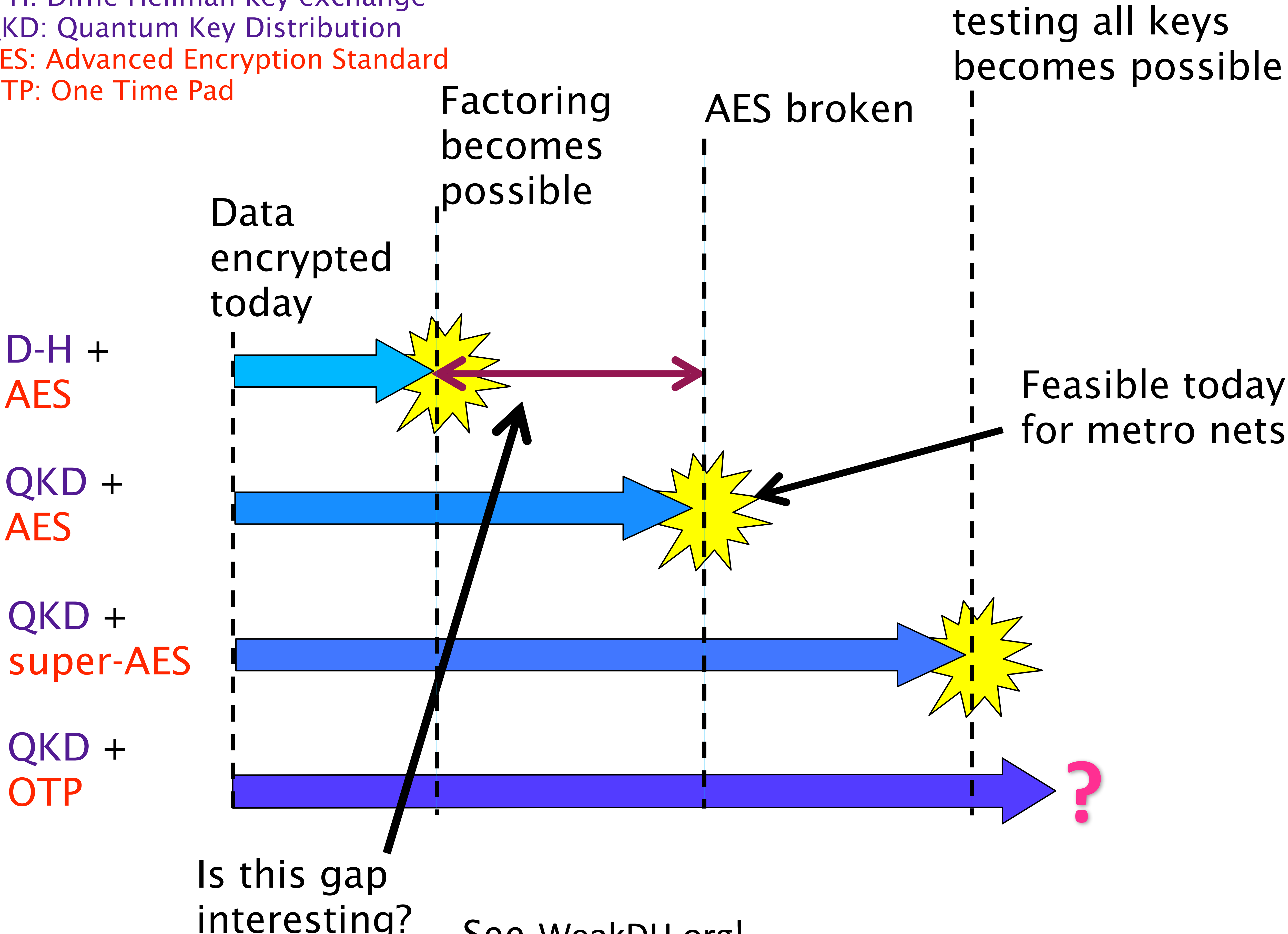

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad
Data encrypted today
Factoring becomes possible
AES broken
testing all keys becomes possible
D-H + AES
QKD + AES
QKD + super-AES
QKD + OTP
?

D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad

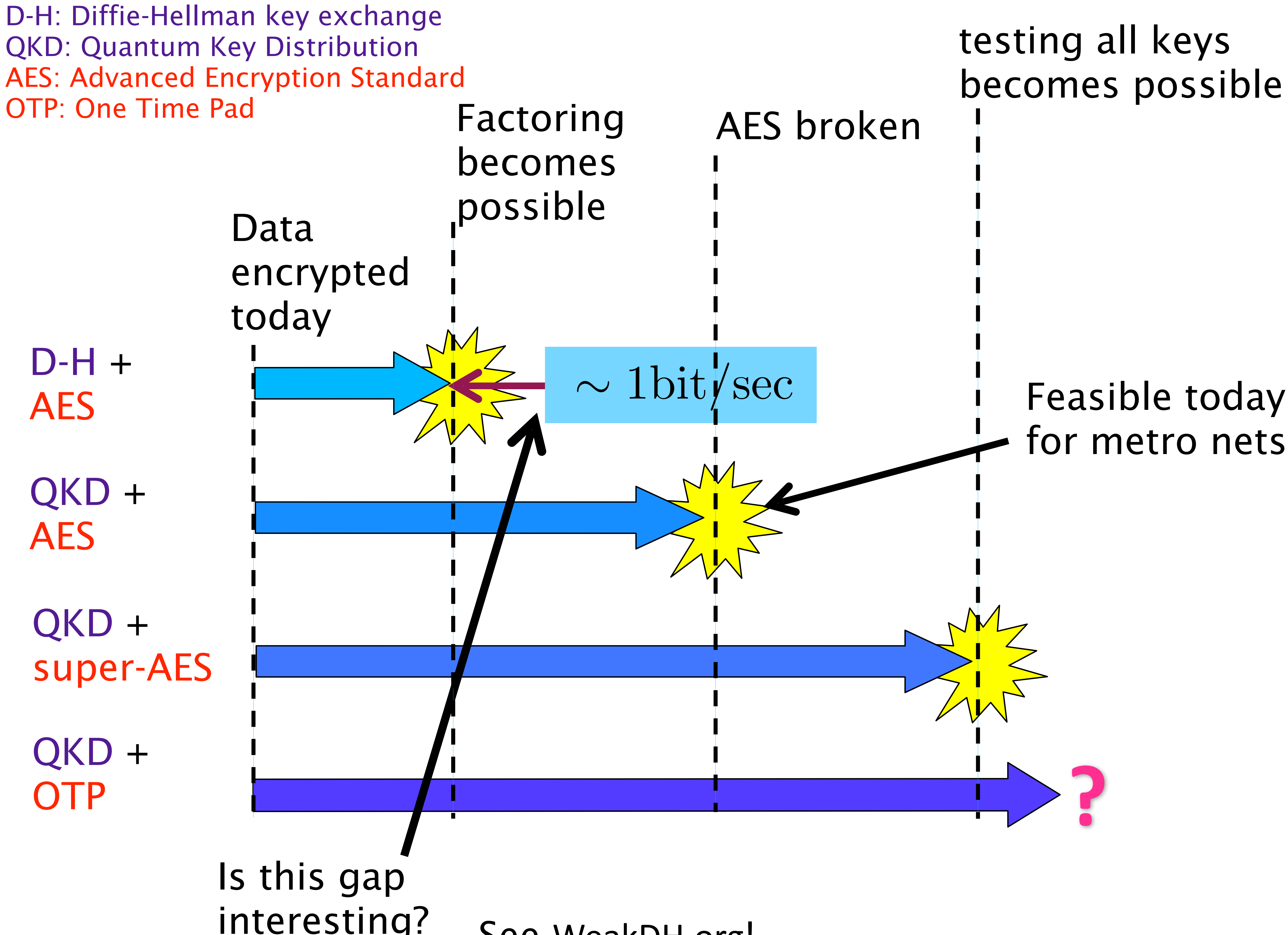



D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad
testing all keys becomes possible
Factoring becomes possible
AES broken
Data encrypted today
D-H + AES
QKD + AES
QKD + super-AES
QKD + OTP
Feasible today for metro nets
?
Is this gap interesting?

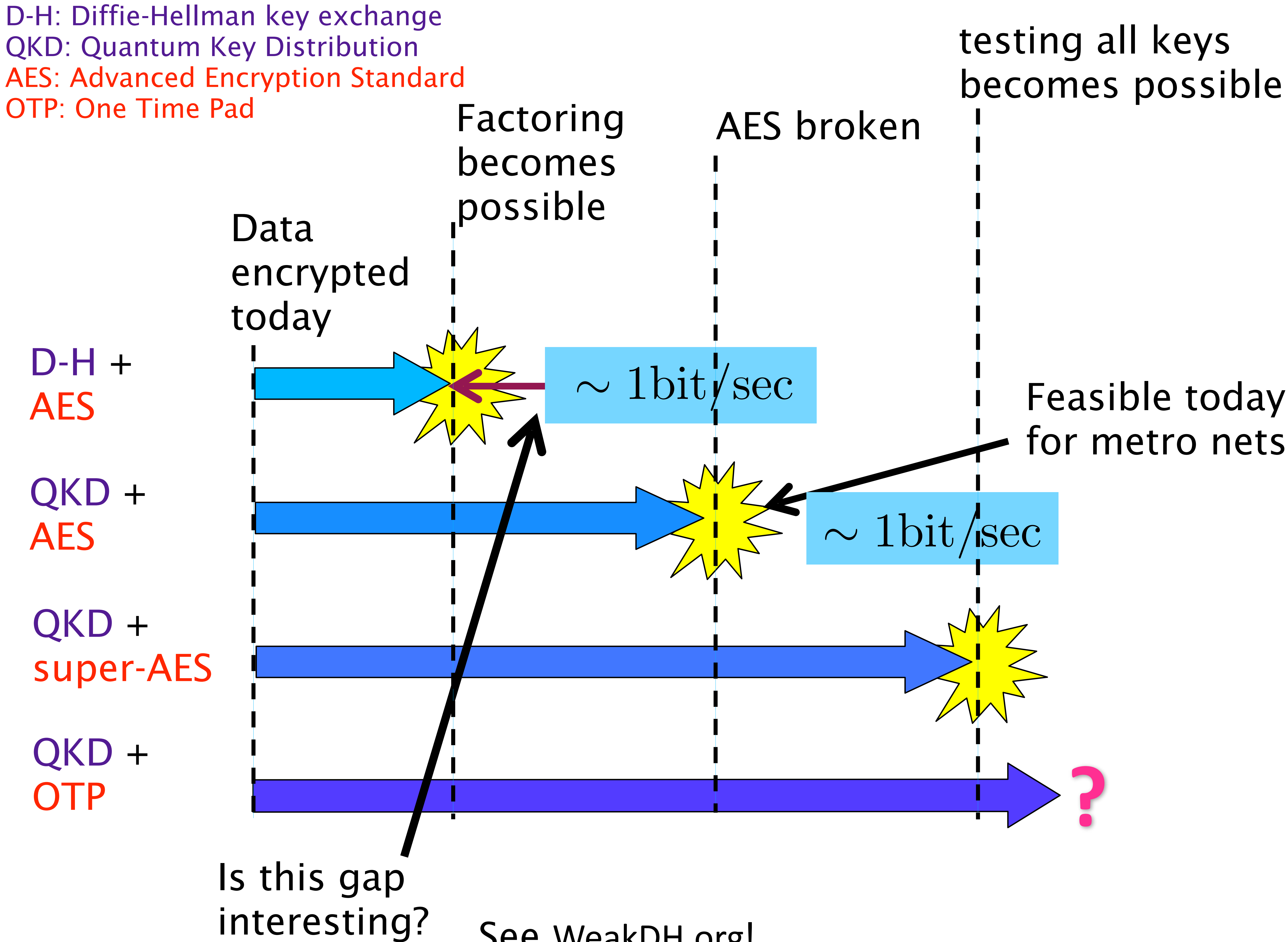
D-H: Diffie-Hellman key exchange
QKD: Quantum Key Distribution
AES: Advanced Encryption Standard
OTP: One Time Pad



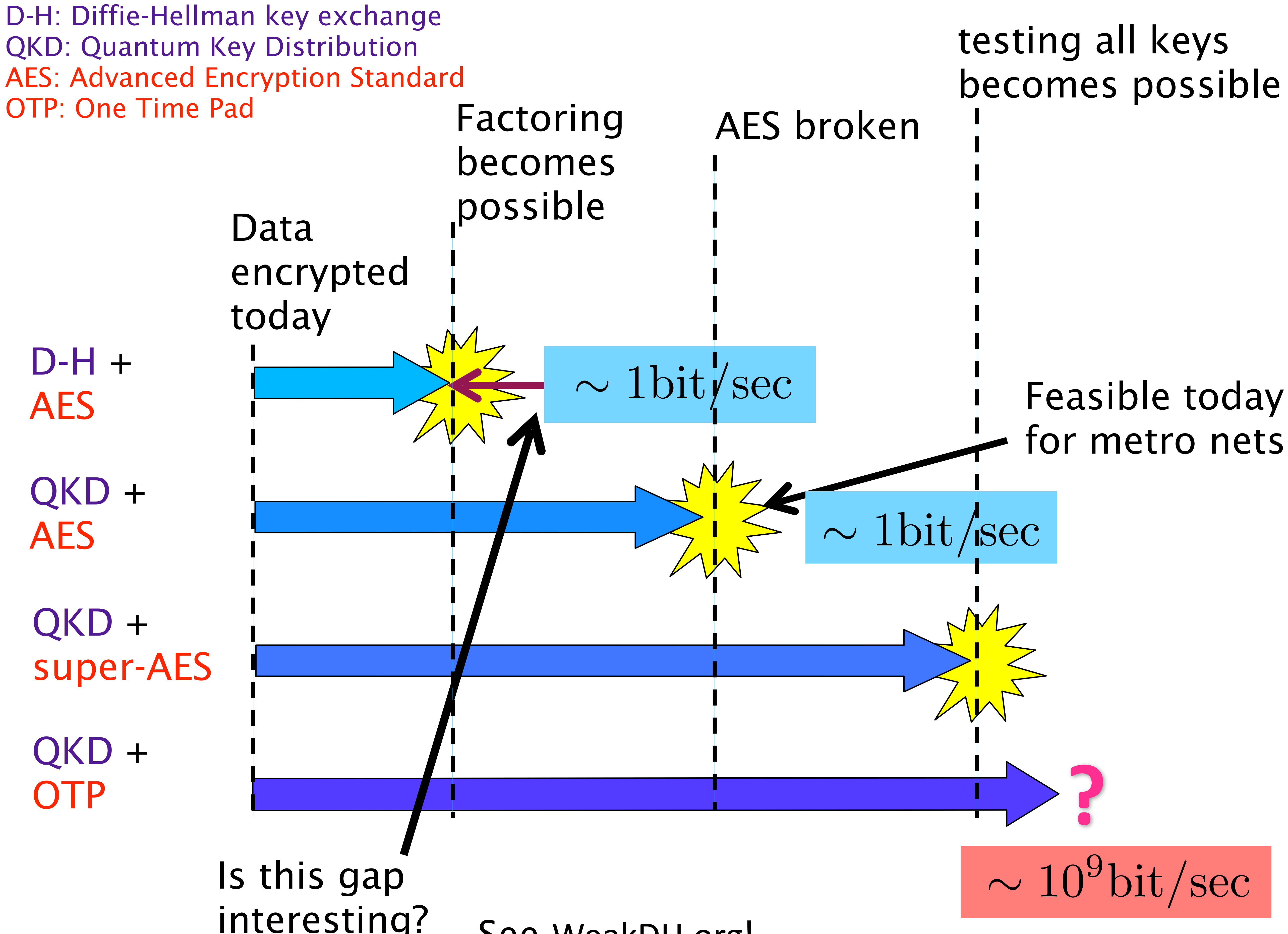
See WeakDH.org!
(Am interested in your opinion of this!)



See WeakDH.org!
(Am interested in your opinion of this!)



See WeakDH.org!
(Am interested in your opinion of this!)



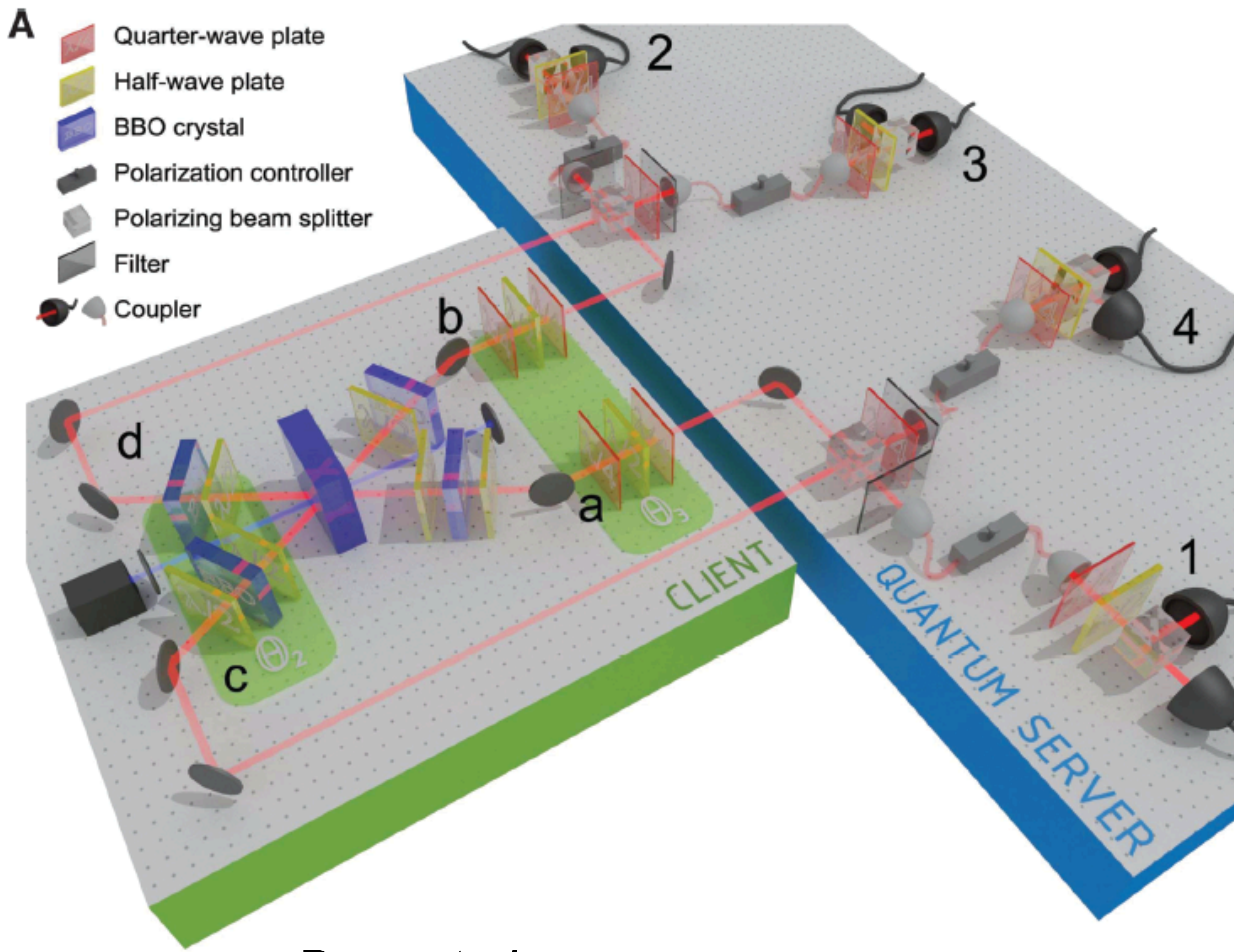
See WeakDH.org!

(Am interested in your opinion of this!)

Distributed QC: blind computing

A platform for secure distributed quantum computation, not an “application” per se.

Assumes MBQC as programming model.

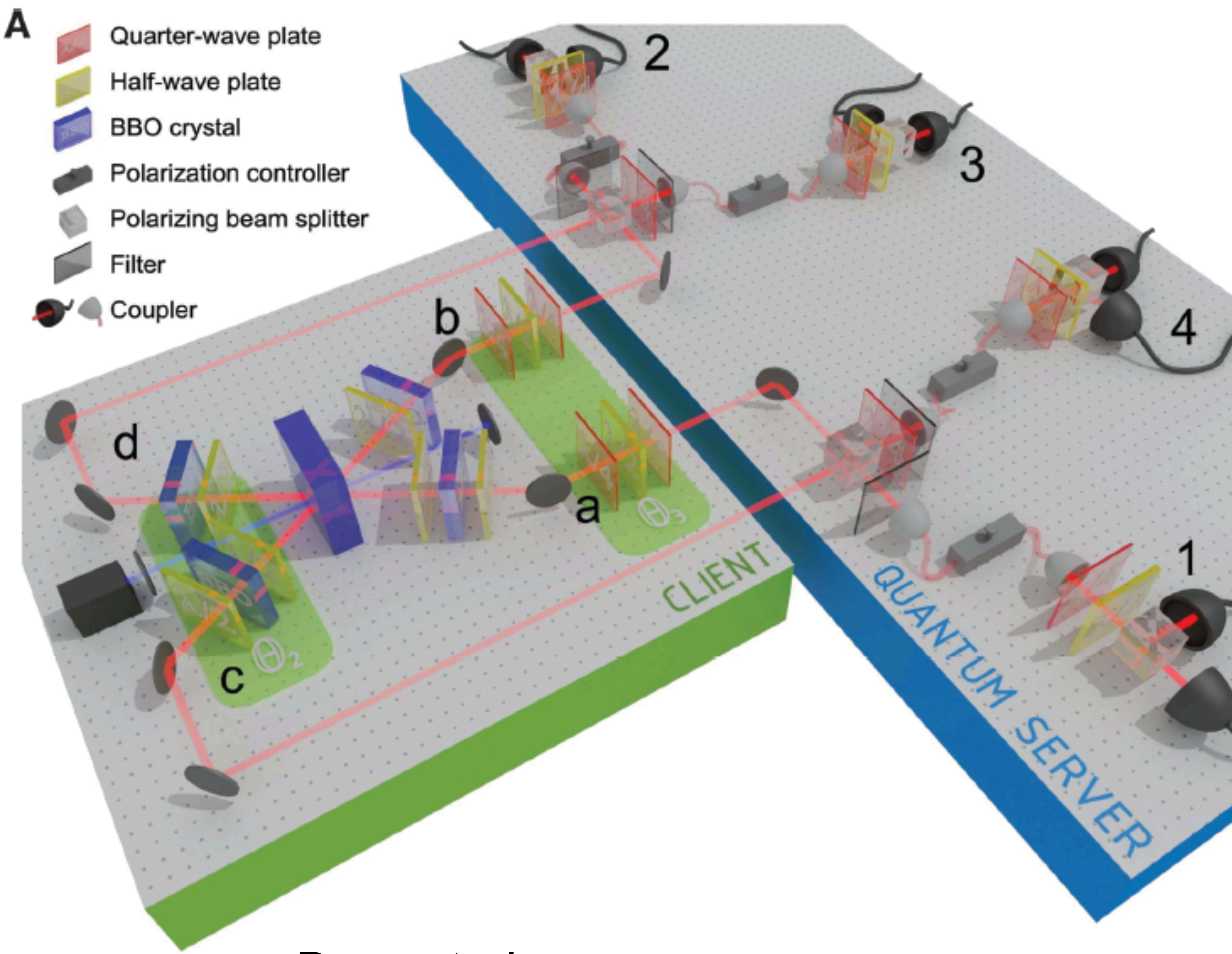


Barz *et al.*, *Science* 335 (2012)

Distributed QC: blind computing

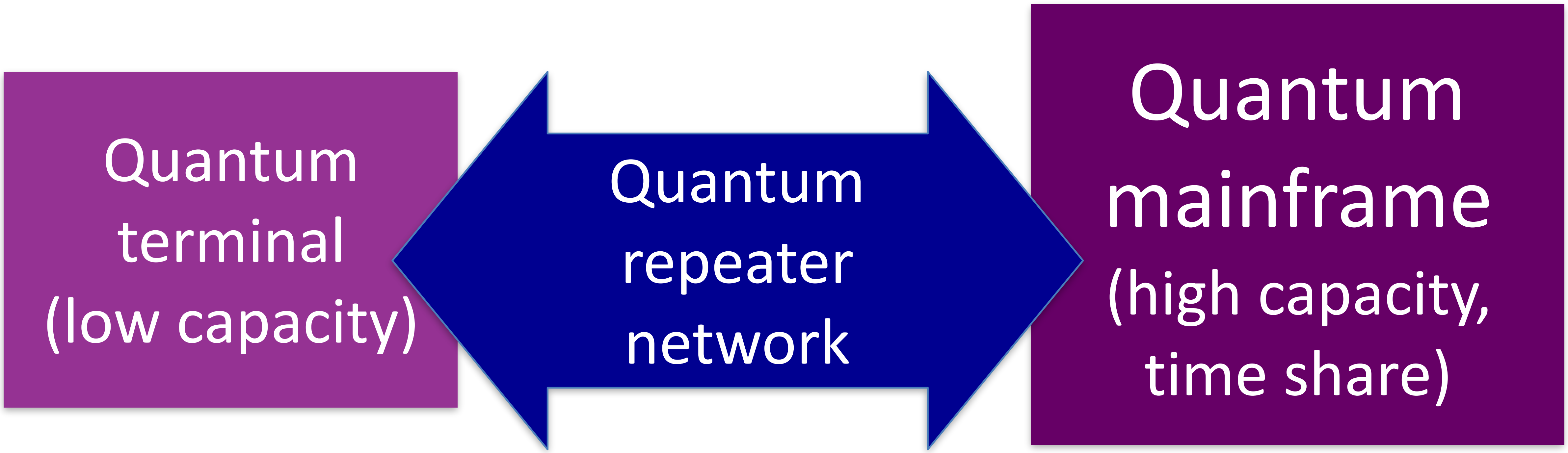
Maybe $\sim 10^{10}$ Bell pairs/sec for FT Shor?

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



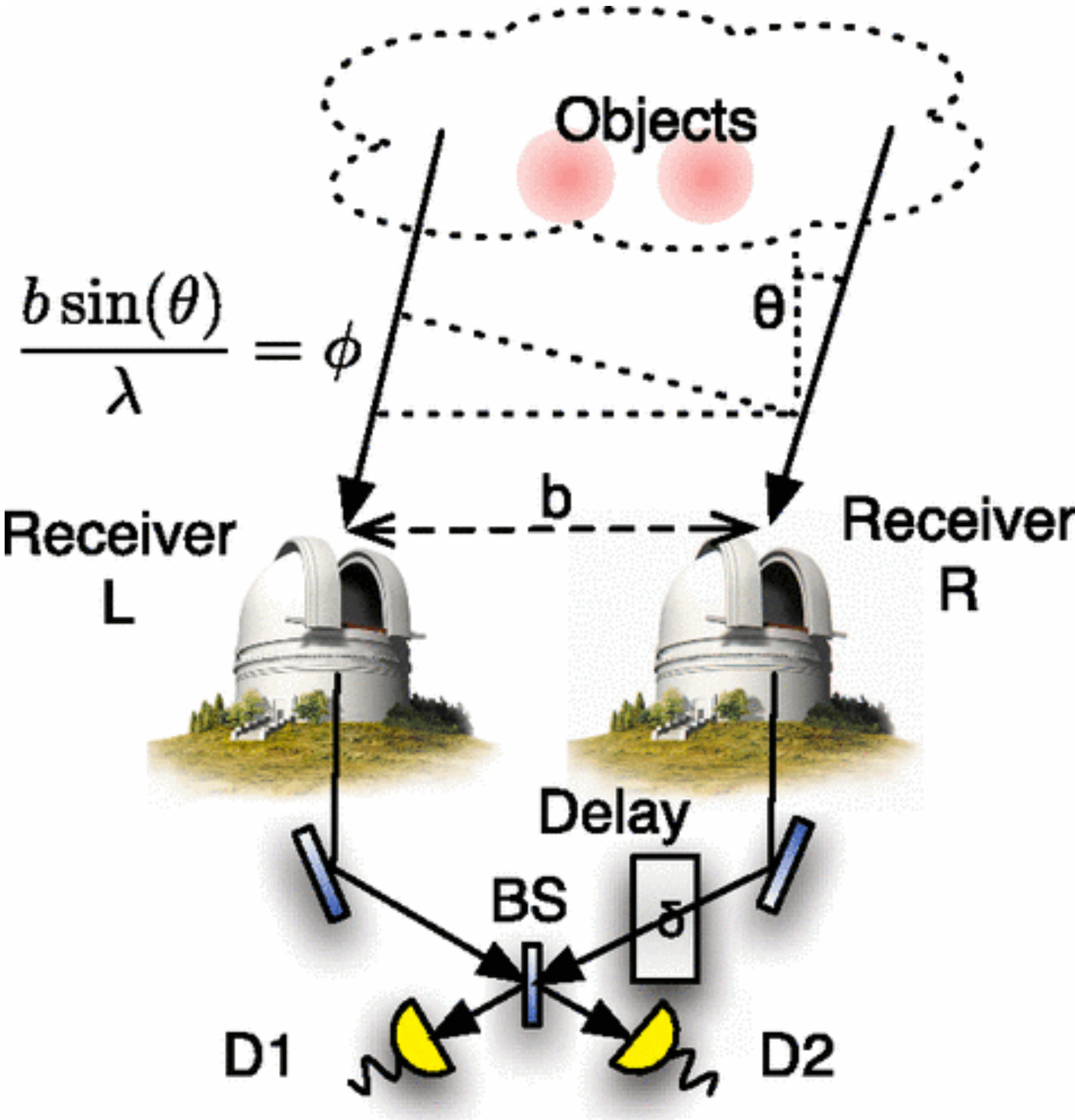
Barz *et al.*, *Science* 335 (2012)

Blind Computation: Secure Quantum Time-Sharing



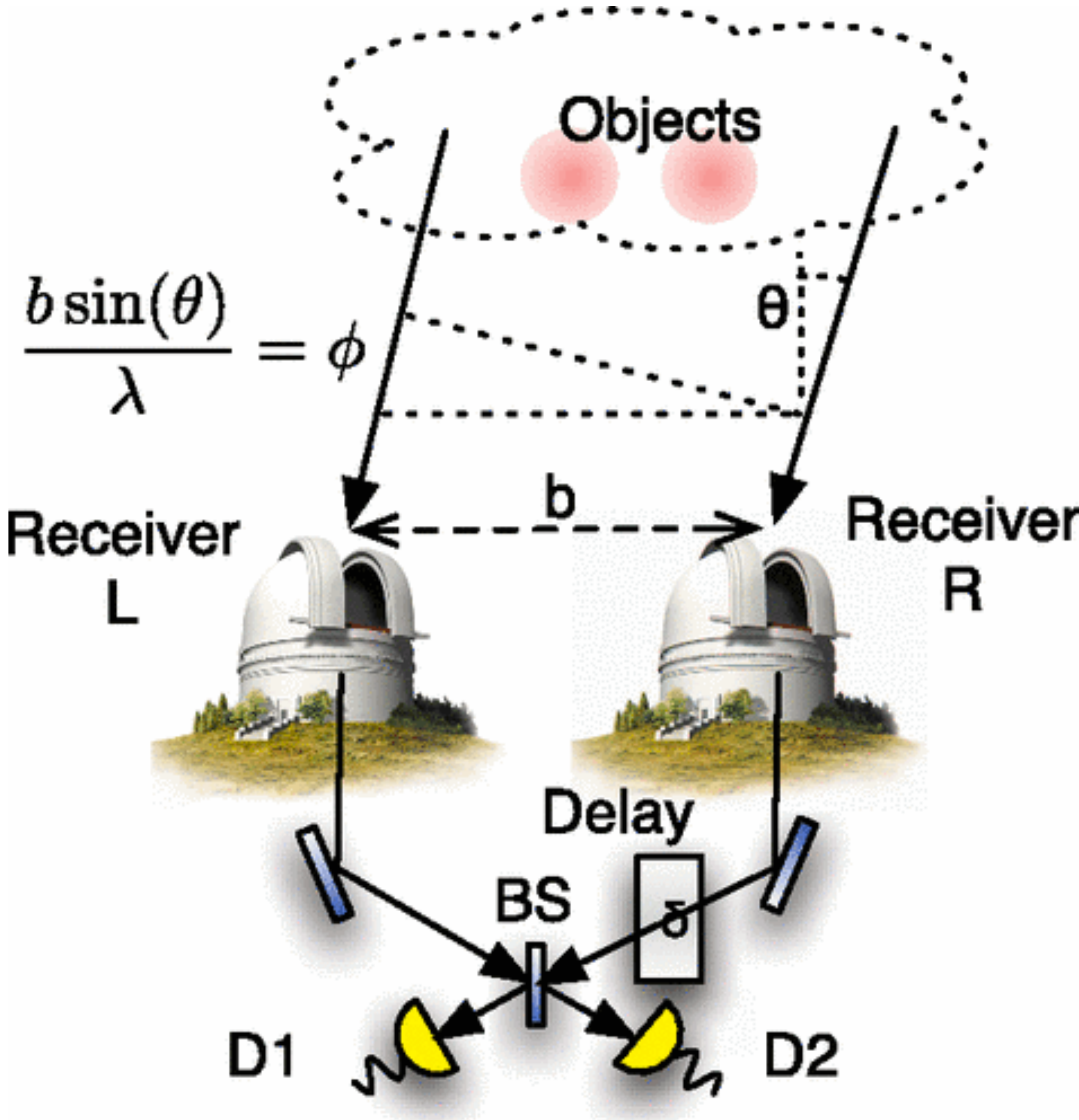
Server learns *nothing* about either client's data *or* computation, except upper bound on computation size. (cf. classical homomorphic encryption)

Sensors: Interferometry (干渉計)



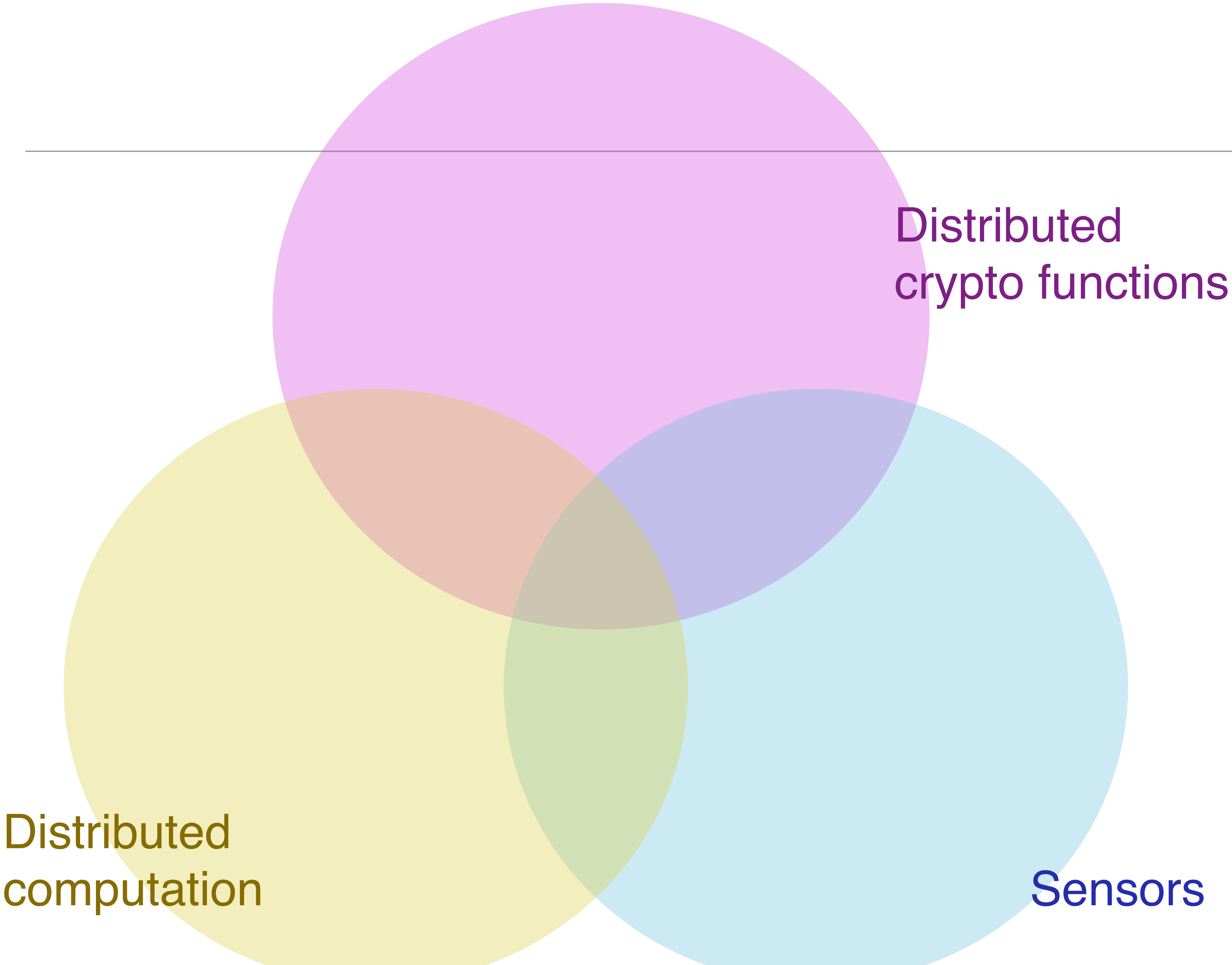
DOI: http://dx.doi.org/10.1103/PhysRevLett.109.070503

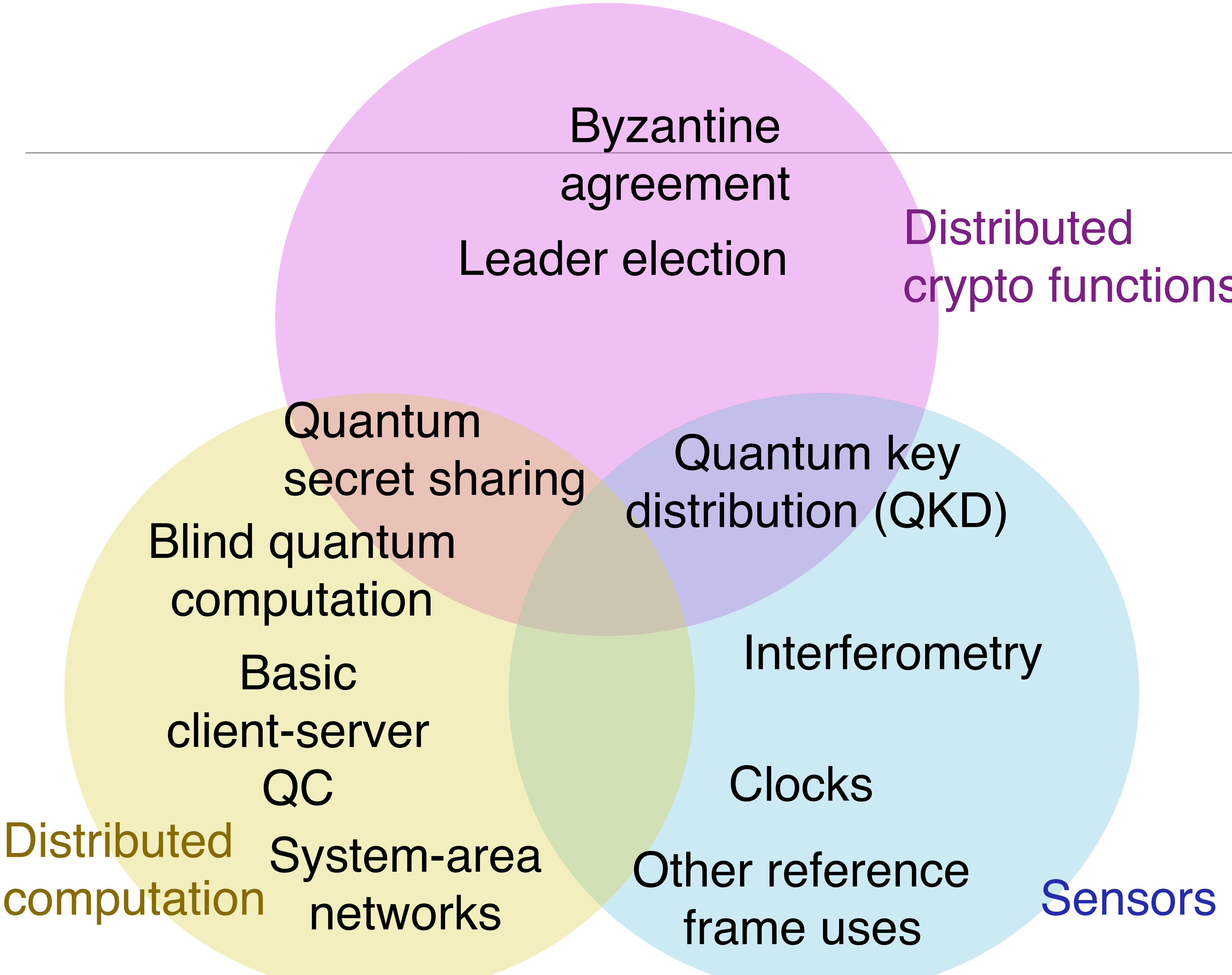
Sensors: Interferometry (干渉計)

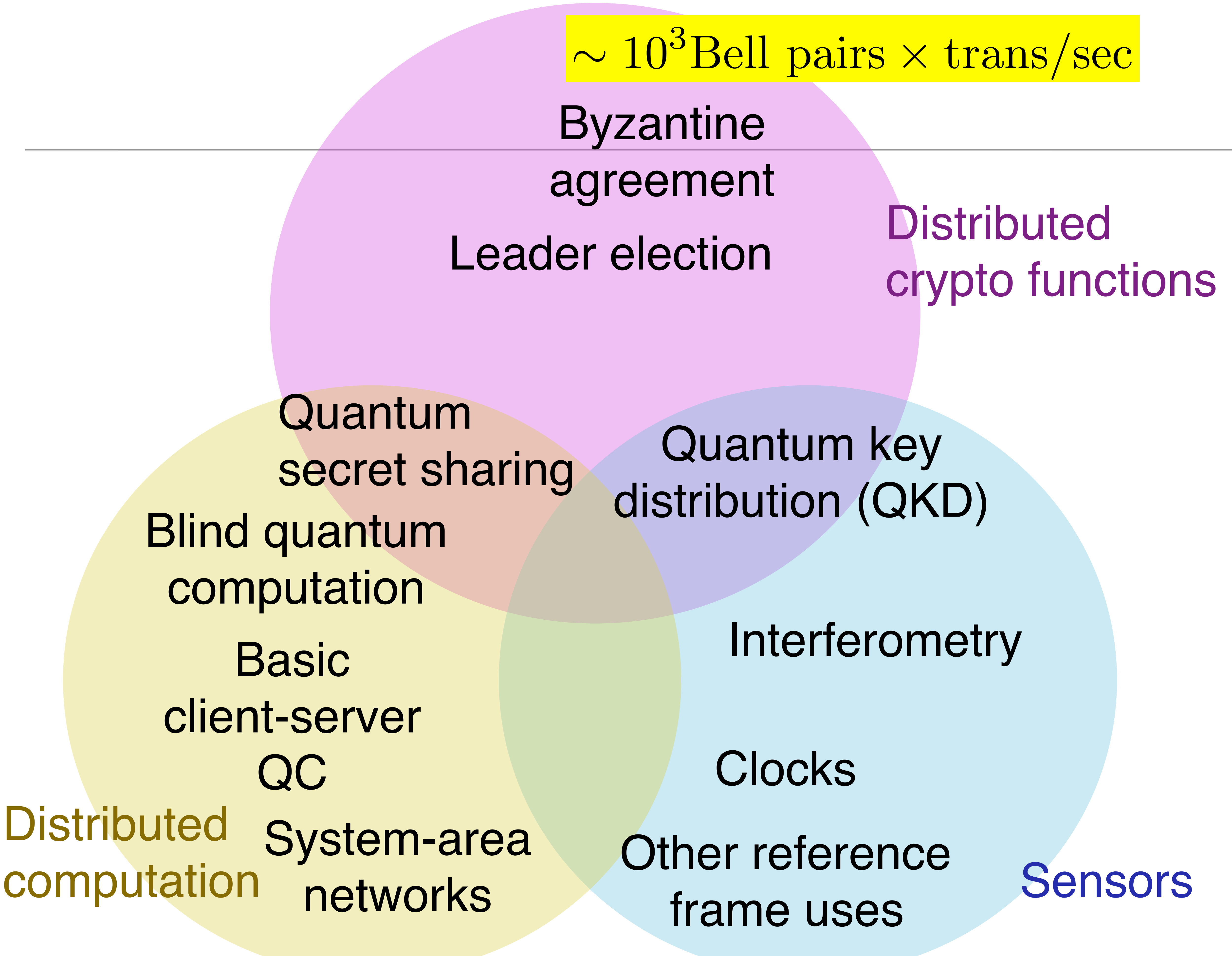


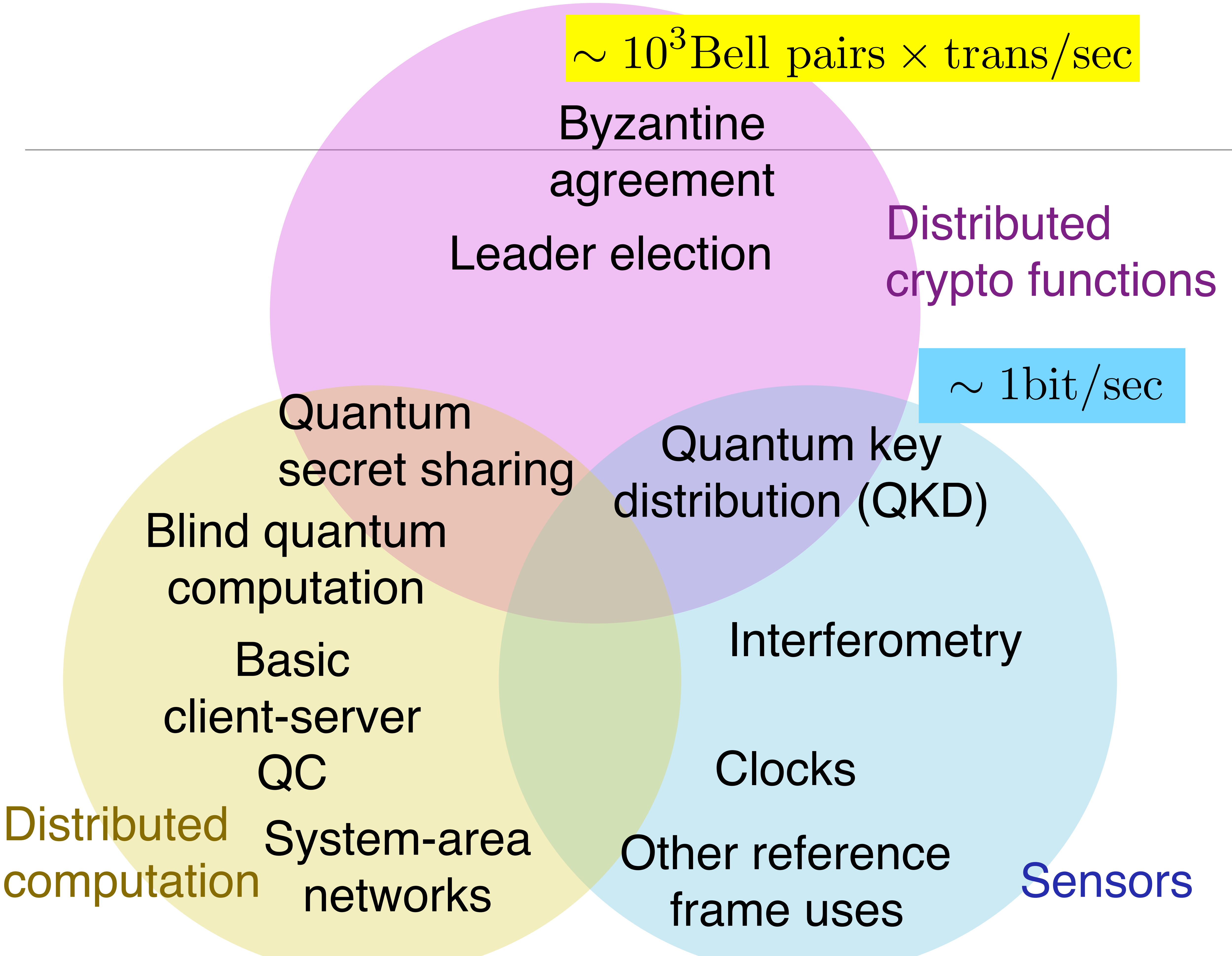
$\sim 10^{11}$ Bell pairs/sec

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

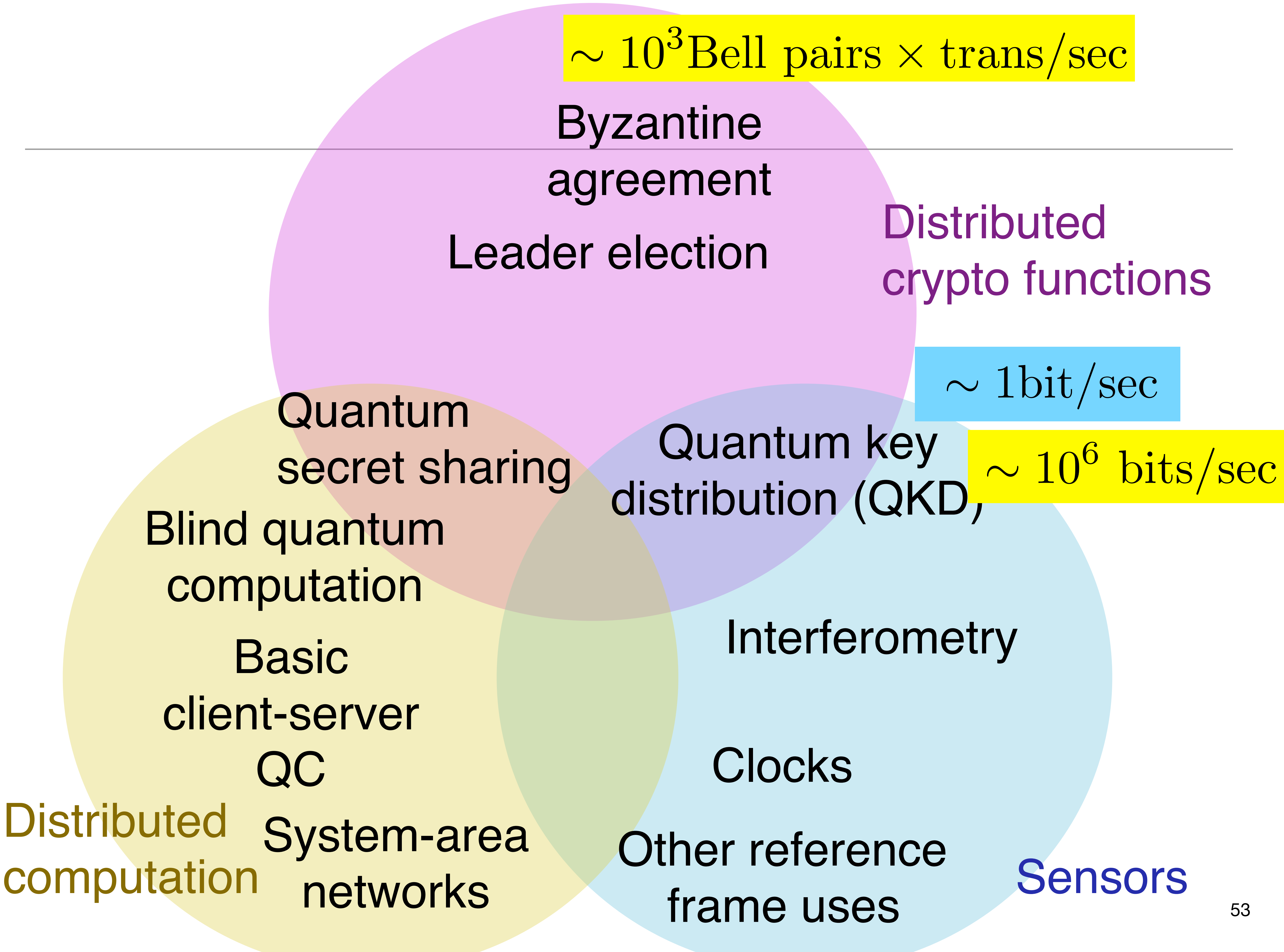

Distributed
crypto functions
Distributed
computation
Sensors

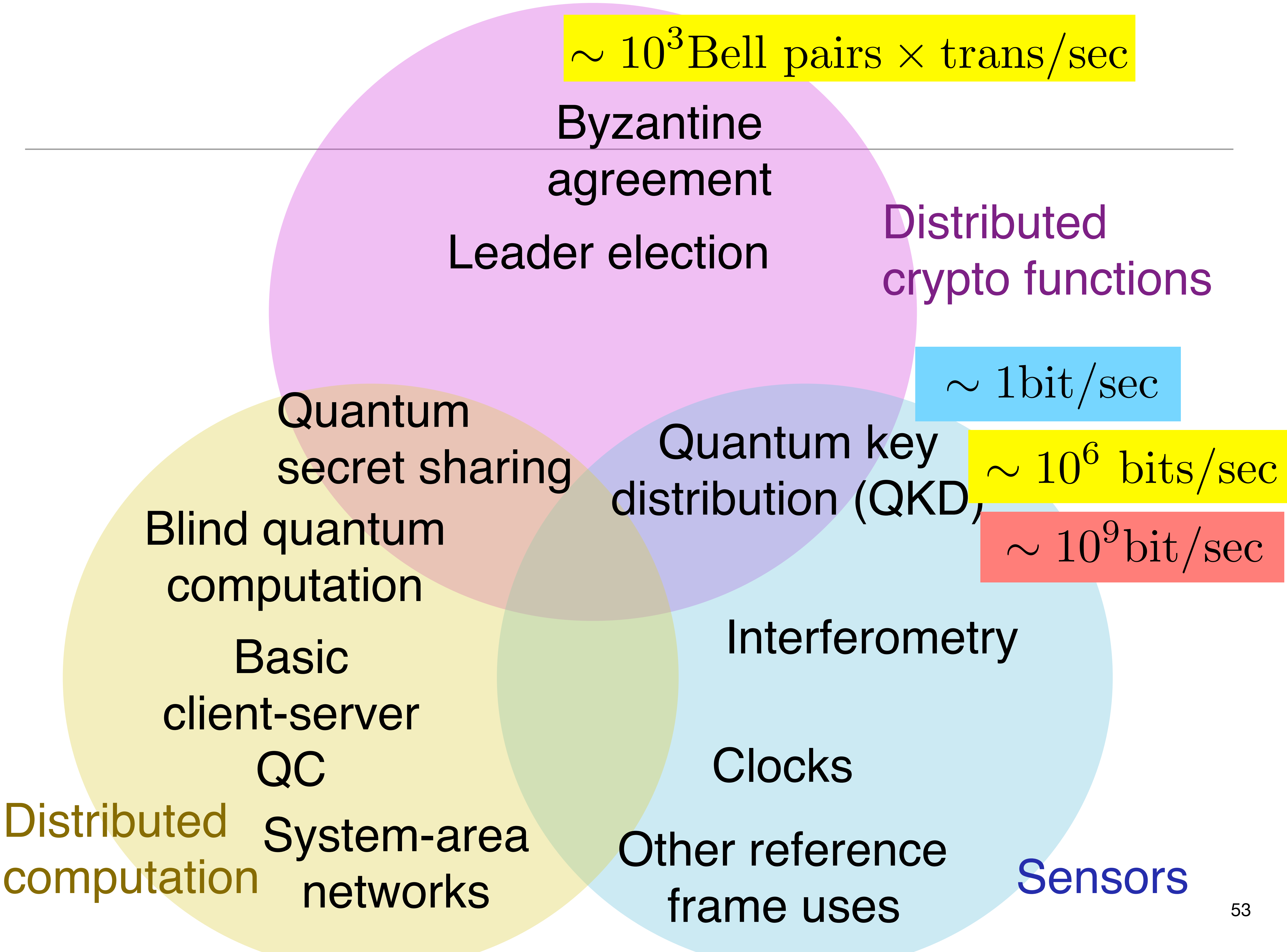

Byzantine agreement
Leader election
Distributed crypto functions
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors


$\sim 10^3 \text{Bell pairs} \times \text{trans/sec}$
Byzantine agreement
Leader election
Distributed crypto functions
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors

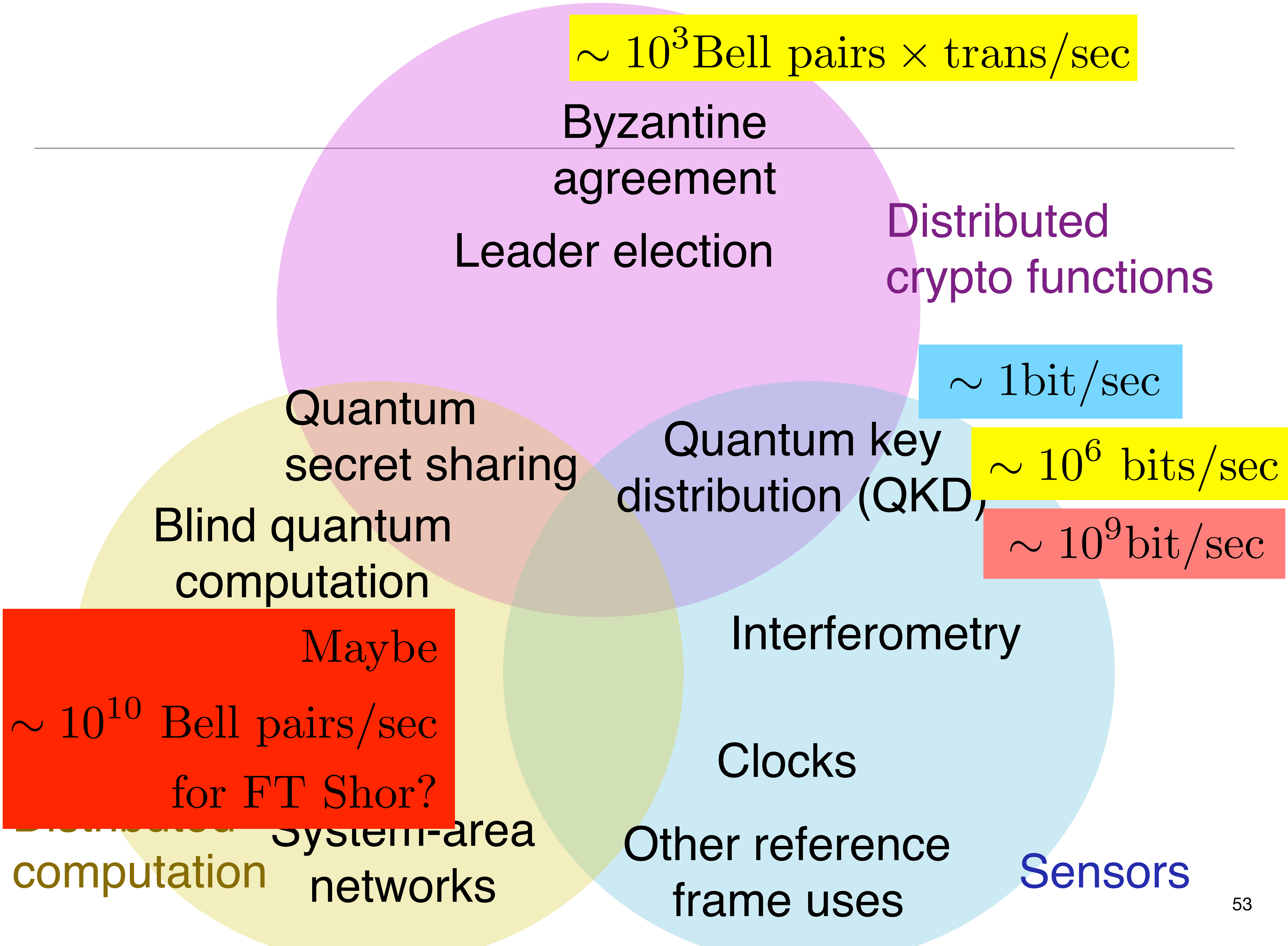


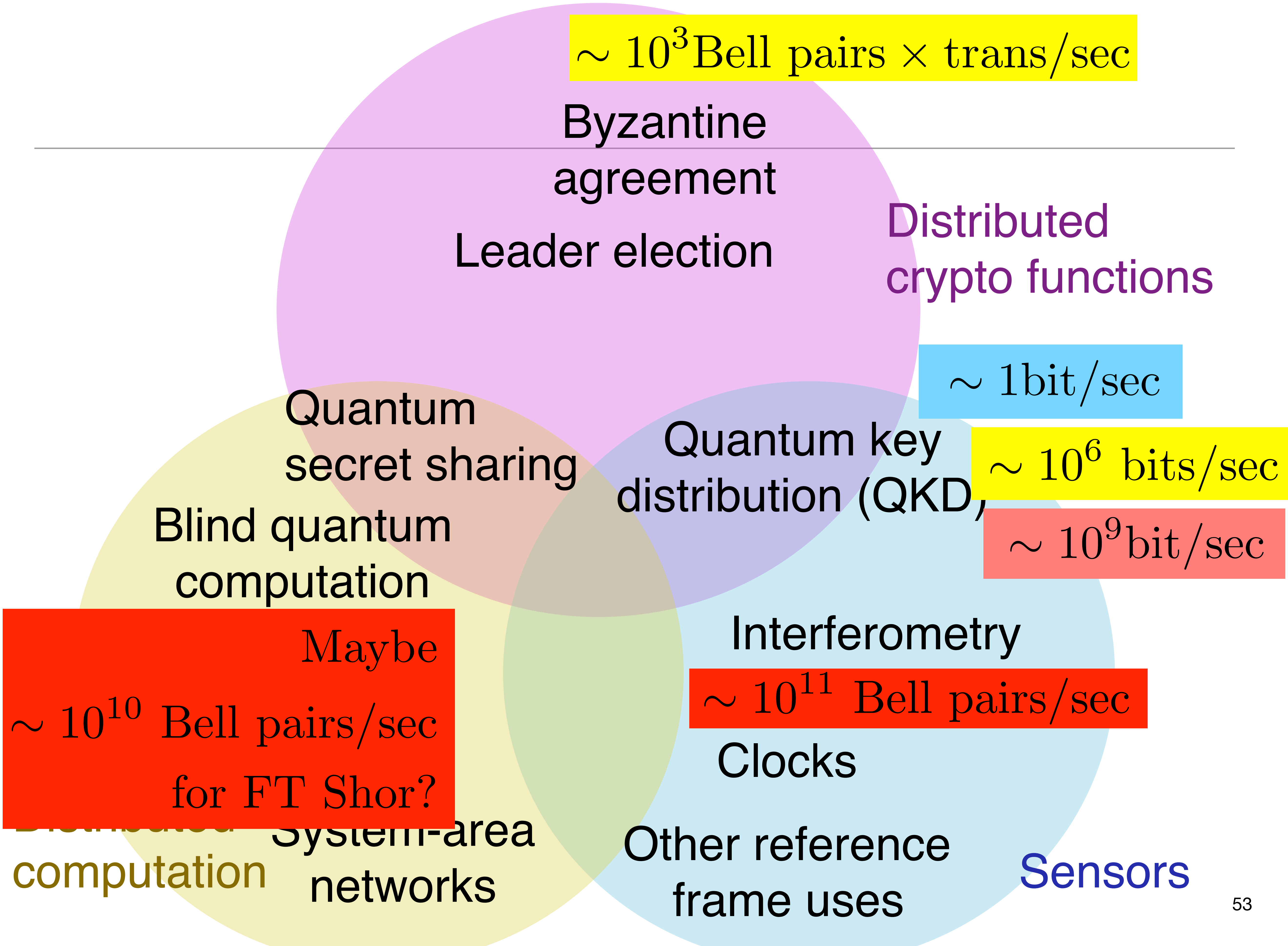
$\sim 10^3 \text{Bell pairs} \times \text{trans/sec}$
Byzantine agreement
Leader election
Distributed crypto functions
$\sim 1\text{bit/sec}$
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors


$\sim 10^3$Bell pairs $\times$ trans/sec
Byzantine agreement
Leader election
Distributed crypto functions
$\sim$ 1bit/sec
Quantum secret sharing
Quantum key distribution (QKD)
$\sim 10^6$ bits/sec
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors



$\sim 10^3 \text{Bell pairs} \times \text{trans/sec}$
Byzantine agreement
Leader election
Distributed crypto functions
$\sim 1\text{bit/sec}$
Quantum secret sharing
Quantum key distribution (QKD)
$\sim 10^6$ bits/sec
$\sim 10^9\text{bit/sec}$
Blind quantum computation
Basic client-server QC
Interferometry
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors


$\sim 10^3$ Bell pairs $\times$ trans/sec
Byzantine agreement
Leader election
Distributed crypto functions
~ 1 bit/sec
$\sim 10^6$ bits/sec
$\sim 10^9$ bit/sec
Quantum secret sharing
Quantum key distribution (QKD)
Blind quantum computation
Maybe
$\sim 10^{10}$ Bell pairs/sec
for FT Shor?
Interferometry
Clocks
System-area networks
computation
Other reference frame uses
Sensors



$\sim 10^3$Bell pairs $\times$ trans/sec
Byzantine agreement
Leader election
Distributed crypto functions
$\sim$ 1bit/sec
Quantum secret sharing
Quantum key distribution (QKD)
$\sim 10^6$ bits/sec
$\sim 10^9$bit/sec
Blind quantum computation
Maybe
$\sim 10^{10}$ Bell pairs/sec
for FT Shor?
Interferometry
$\sim 10^{11}$ Bell pairs/sec
Clocks
Distributed computation
System-area networks
Other reference frame uses
Sensors

Entanglement is Independent of Distance

Entanglement is Independent of Distance

...provided we have high-fidelity transmission, memory, and operations

Entanglement is Independent of Distance

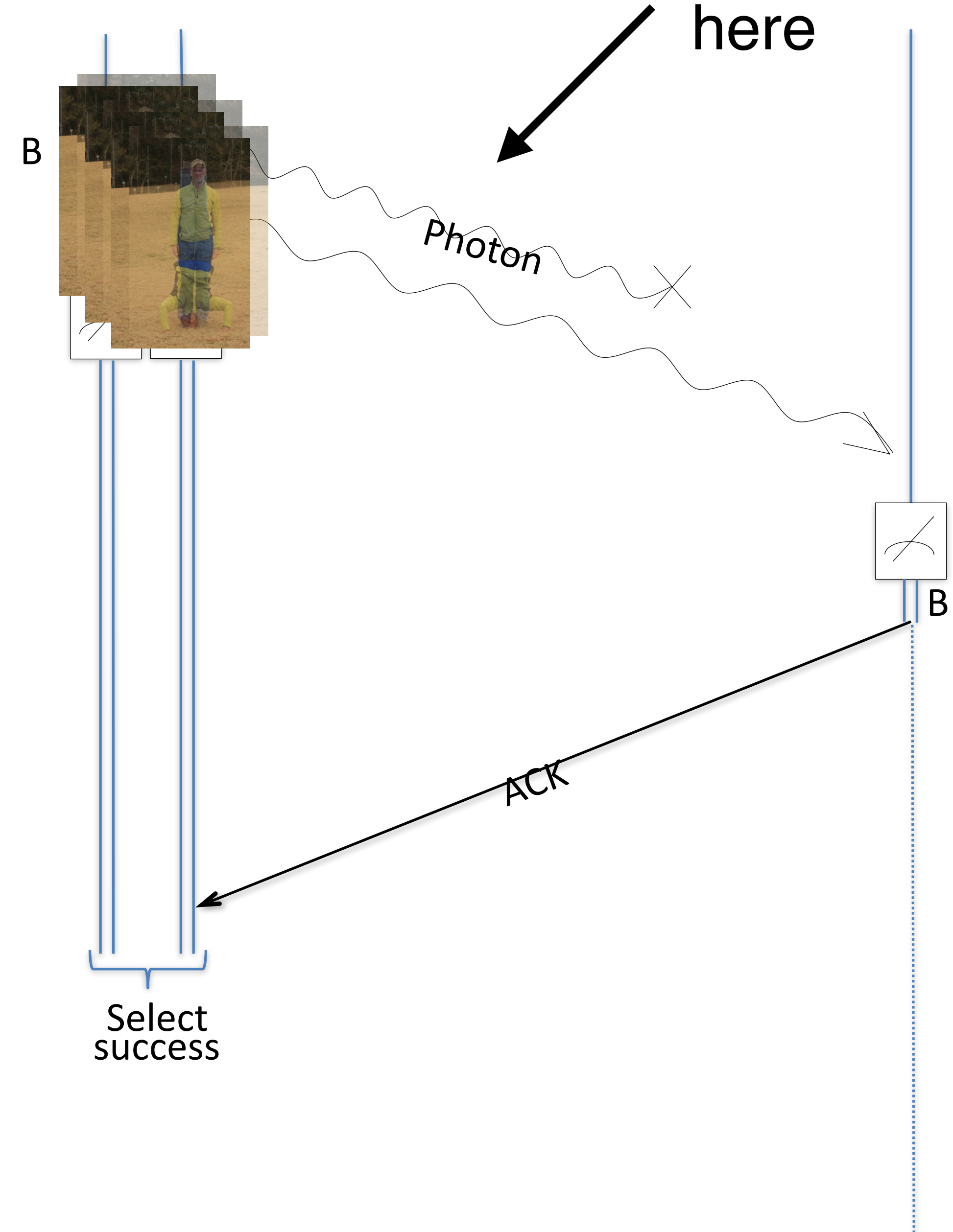
...provided we have high-fidelity transmission, memory, and operations

…so that’s what quantum repeater networks are all about.

Losing Photons Affects When We Can Use Info

Losing photons here

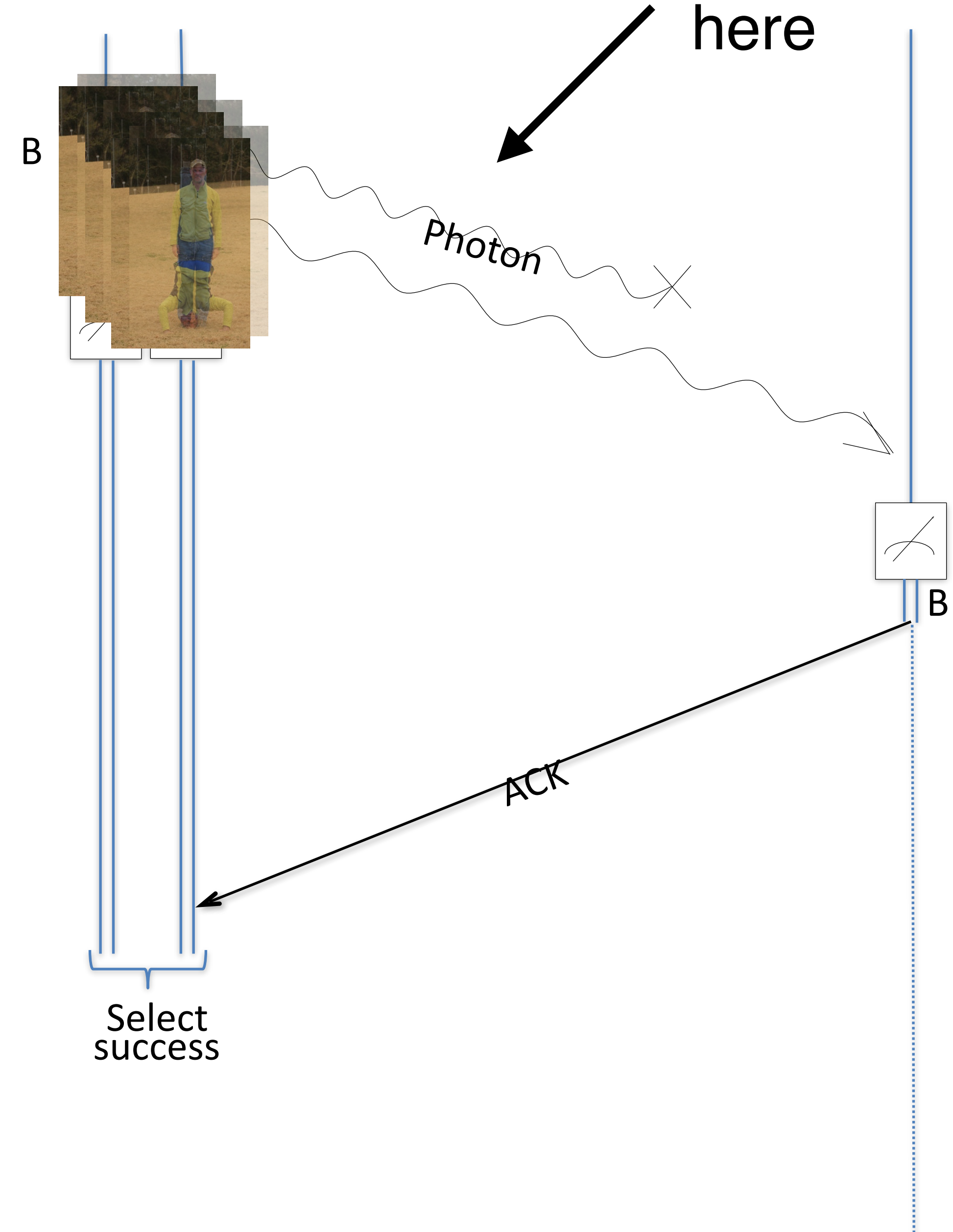
Double lines are *classical* information



Losing Photons Affects When We Can Use Info

Losing photons here

Double lines are *classical* information

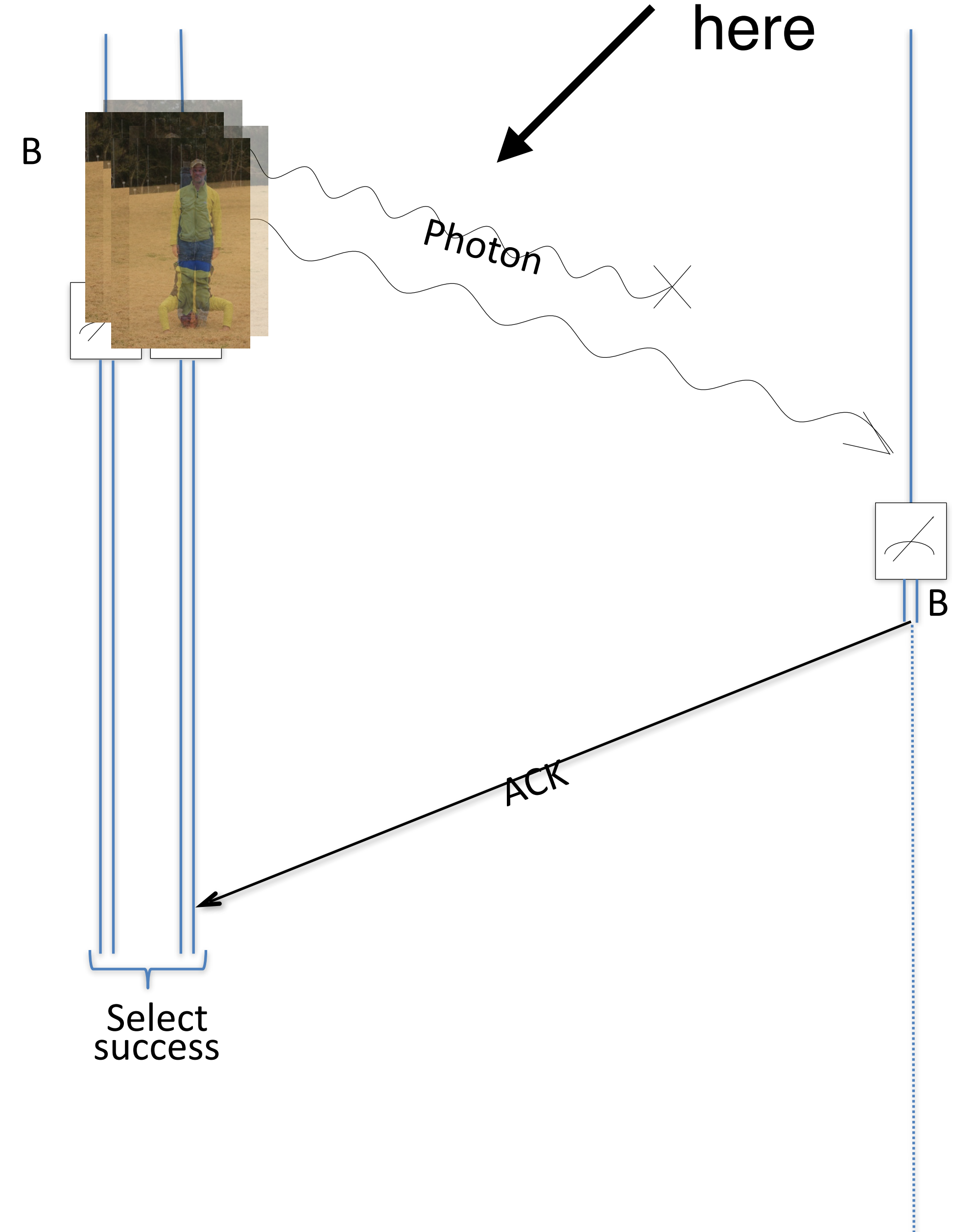


B (Bell) class:
Bell inequality violations, quantum key distribution (QKD)
no quantum buffering
all classical post-selection

Losing Photons Affects When We Can Use Info

Losing photons here

Double lines are *classical* information

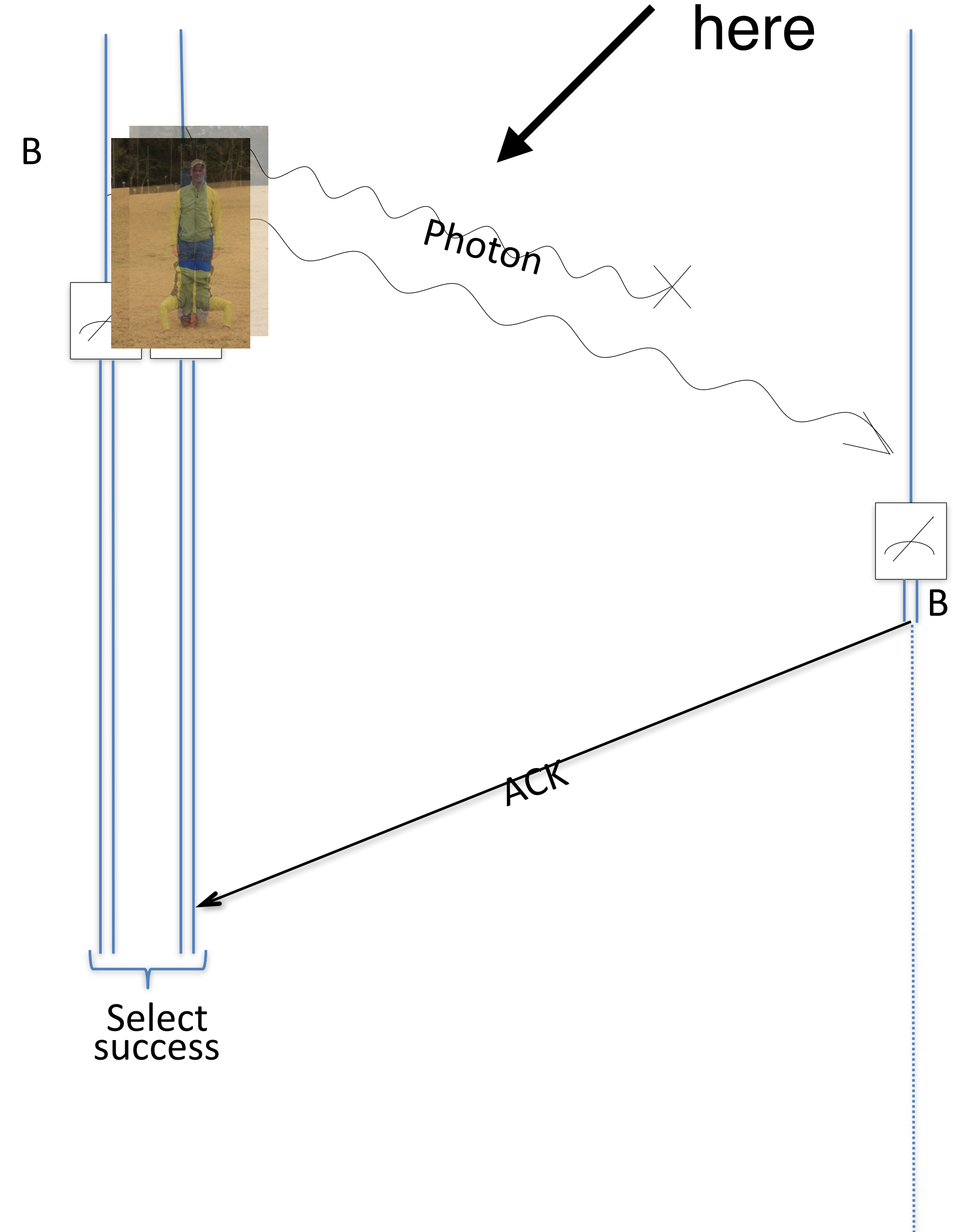


B (Bell) class:
Bell inequality violations, quantum key distribution (QKD)
no quantum buffering
all classical post-selection

Losing Photons Affects When We Can Use Info

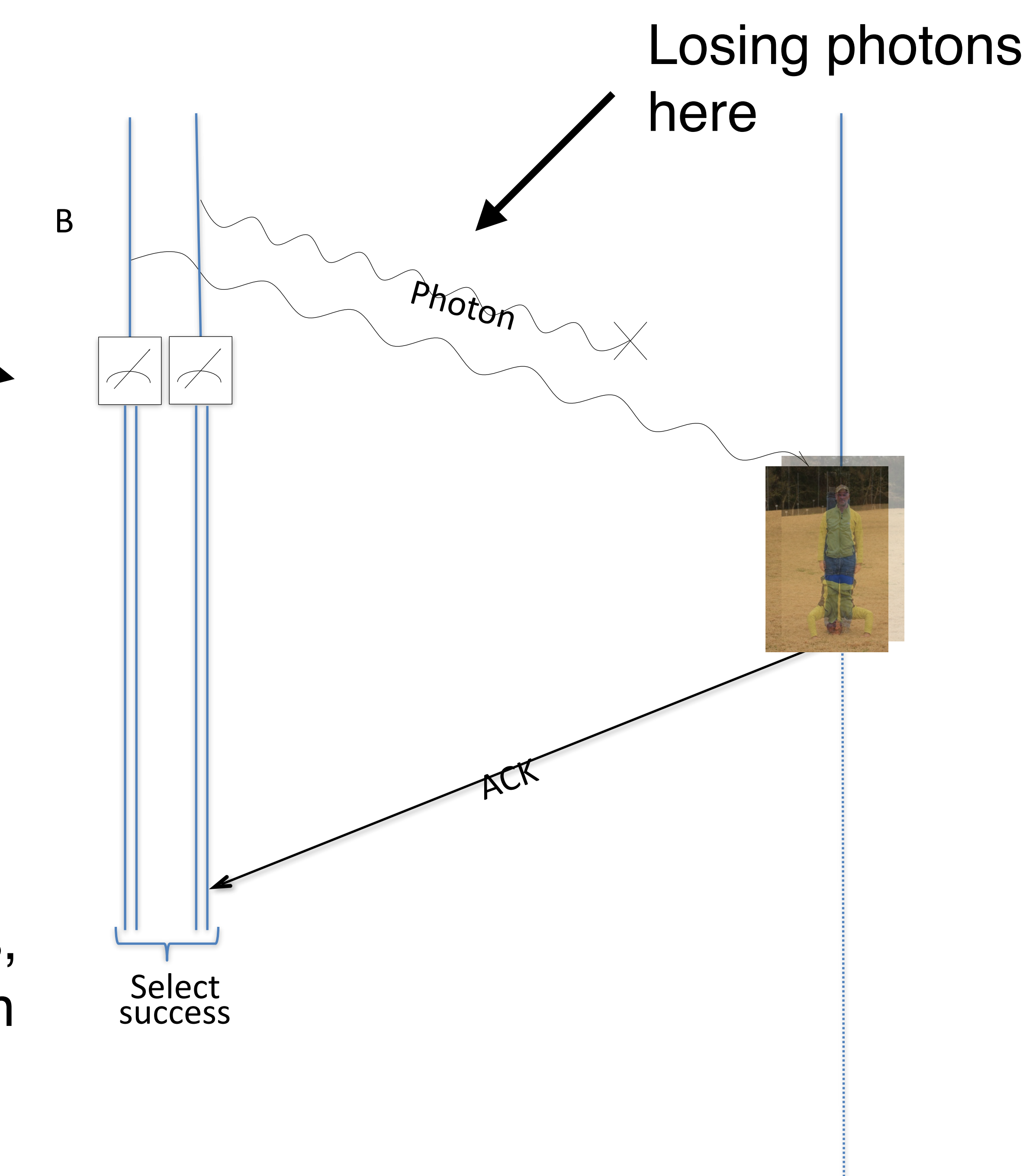
Losing photons here

Double lines are *classical* information



B (Bell) class:
Bell inequality violations, quantum key distribution (QKD)
no quantum buffering
all classical post-selection

Losing Photons Affects When We Can Use Info



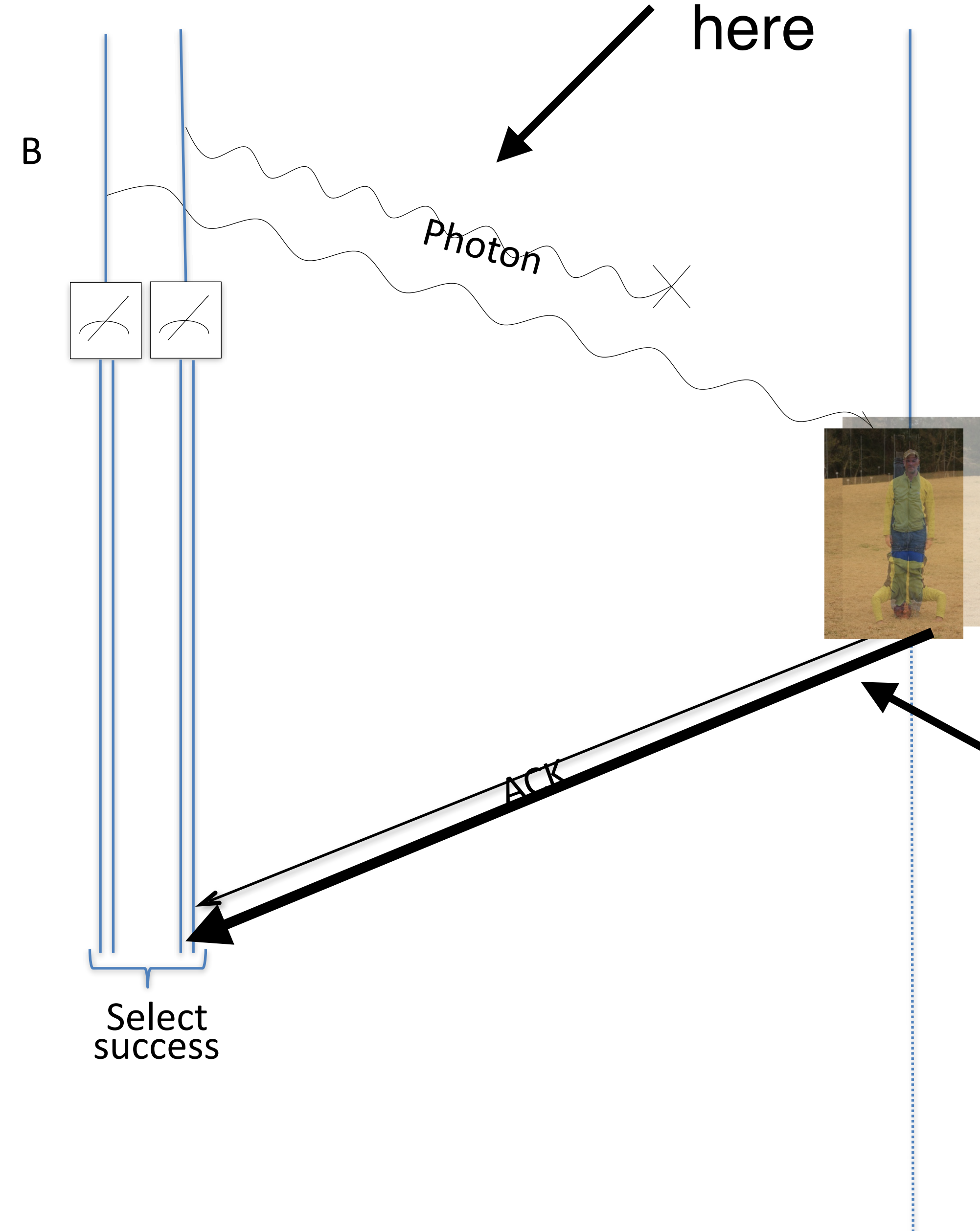
Double lines are *classical* information

B (Bell) class:
Bell inequality violations, quantum key distribution (QKD)
no quantum buffering
all classical post-selection

Losing Photons Affects When We Can Use Info

Losing photons here

Double lines are *classical* information



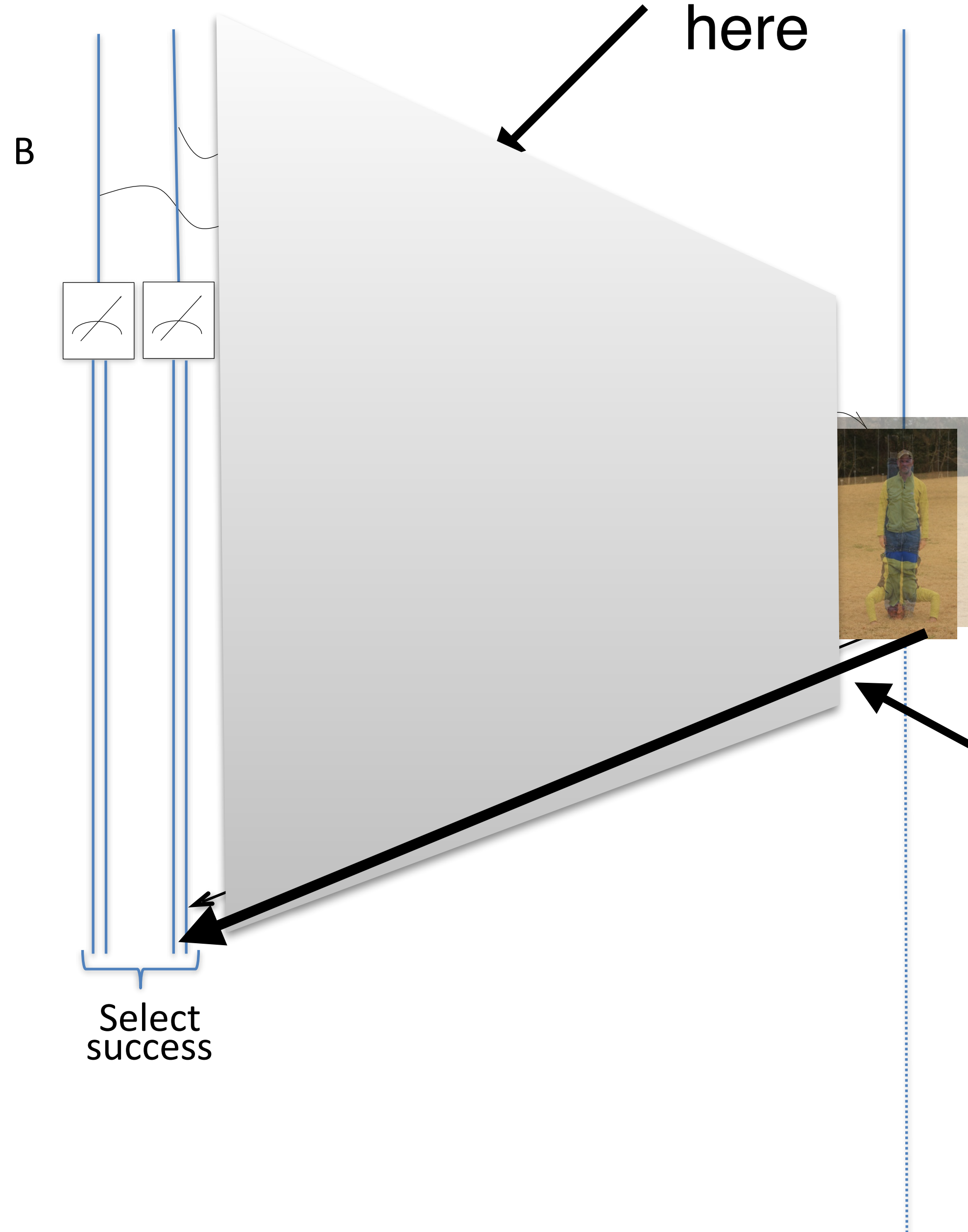
ACKing what we got

B (Bell) class:
Bell inequality violations, quantum key distribution (QKD)
no quantum buffering
all classical post-selection

Losing Photons Affects When We Can Use Info

Losing photons here

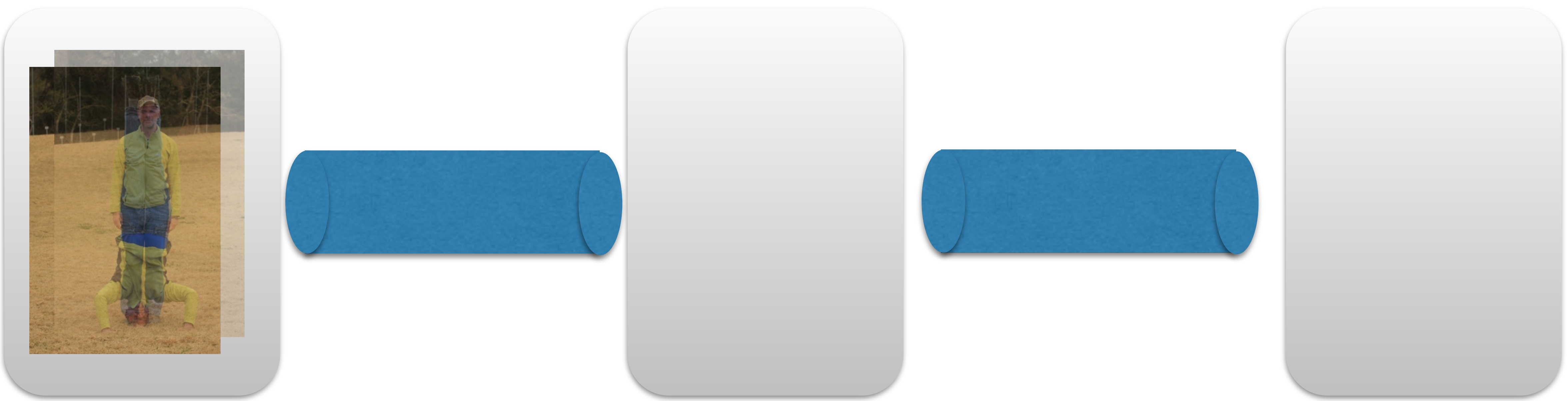
Double lines are *classical* information



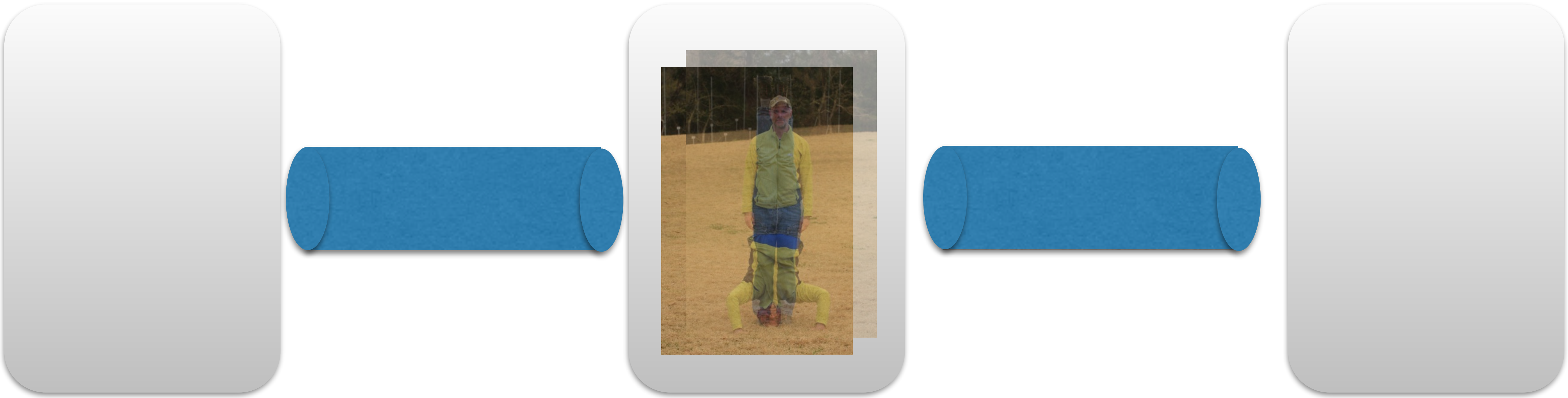
ACKing what we got

B (Bell) class:
Bell inequality violations, quantum key distribution (QKD)
no quantum buffering
all classical post-selection

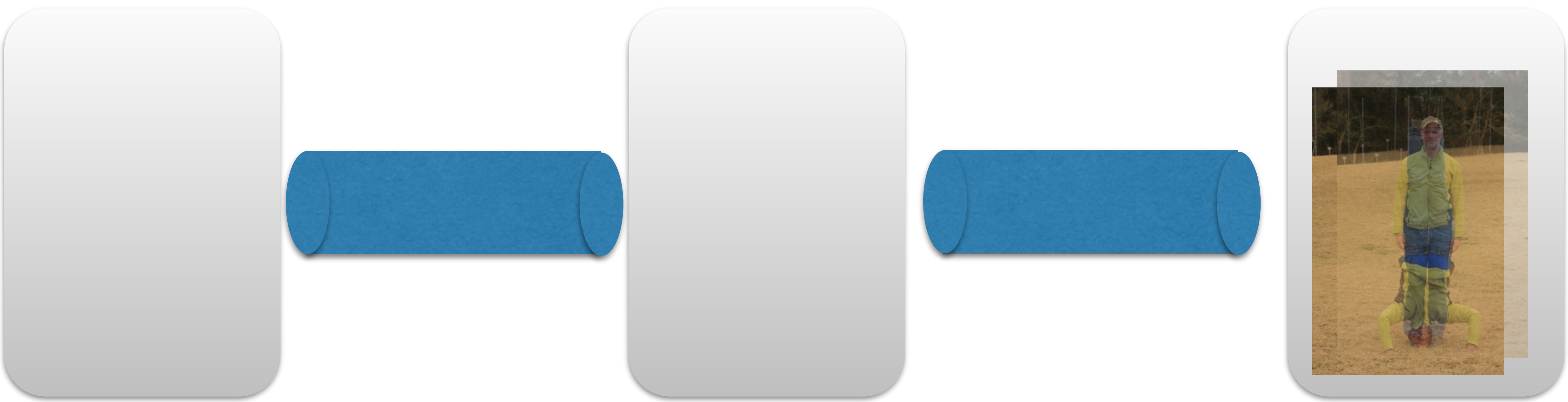
Store-and-Forward?



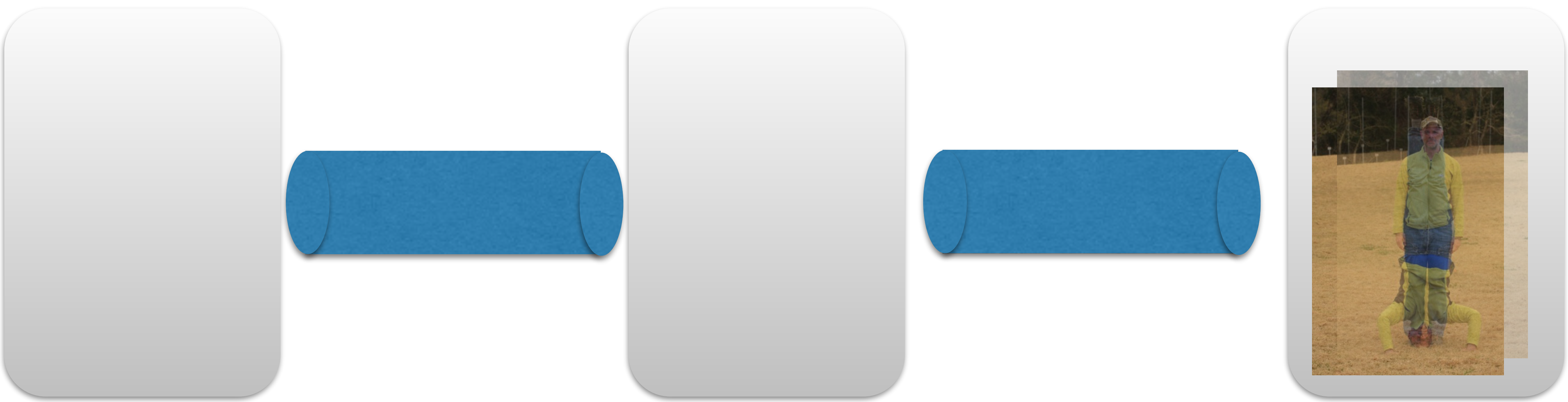
Store-and-Forward?



Store-and-Forward?



Store-and-Forward?



1) photon loss

Problems: 2) local operation errors

3) memory errors

So We Build Repeaters: Conceptual Hardware

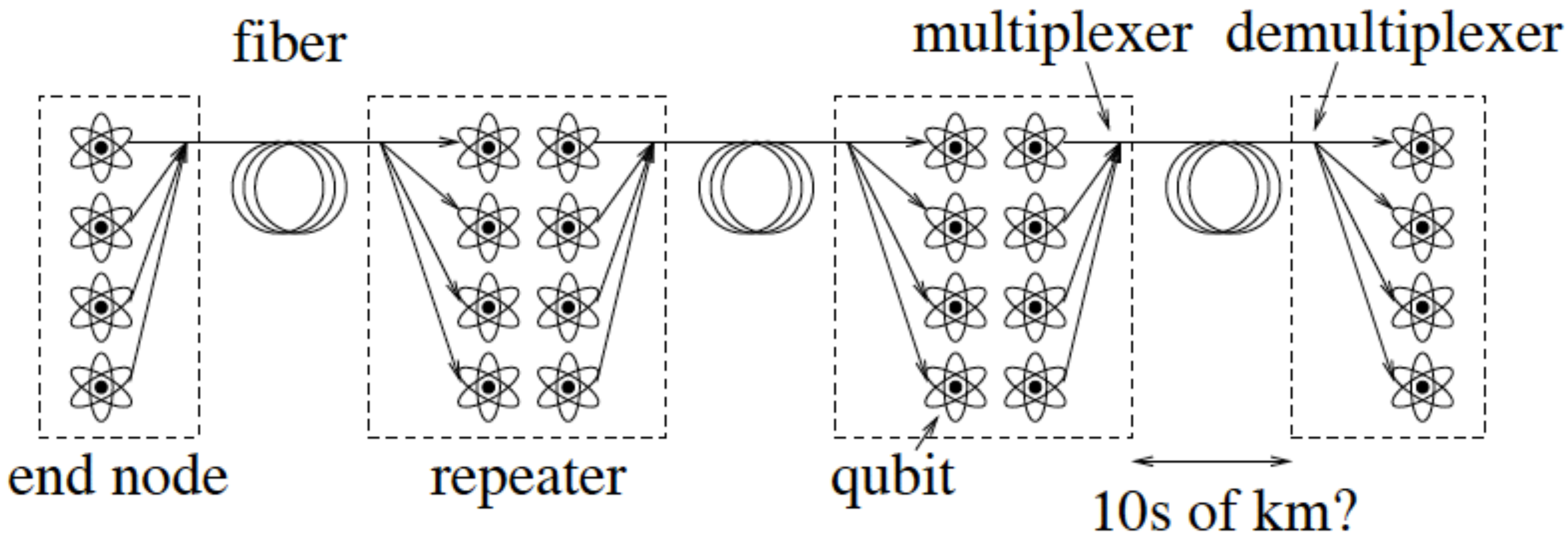


Figure 10.1: Generic view of the hardware of a line of repeaters. Qubit memories are represented by the atom symbol, regardless of physical device type.

Tasks of a Quantum Repeater

Tasks of a Quantum Repeater

1. To make basic entanglement over a distance (e.g., over fiber or free space)

Tasks of a Quantum Repeater

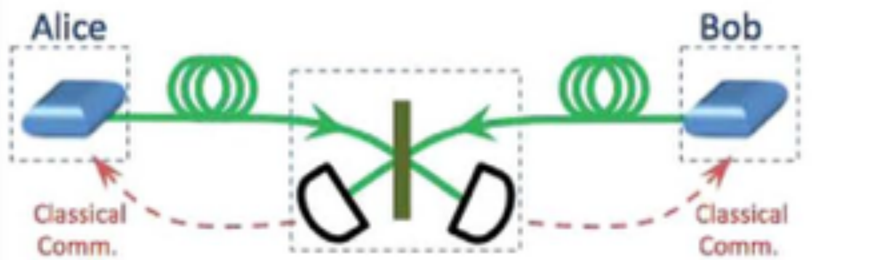
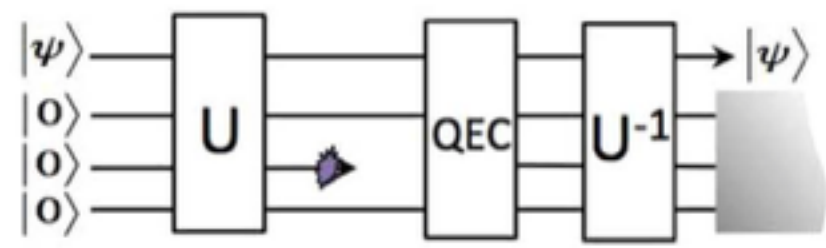
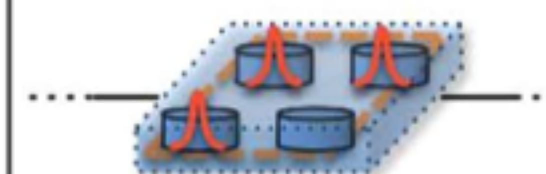
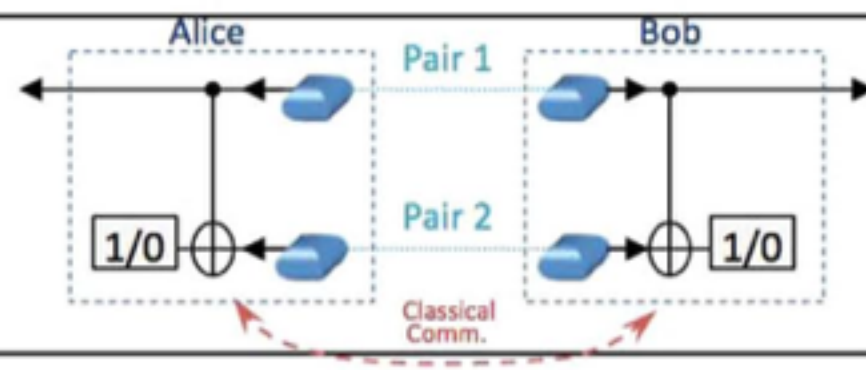
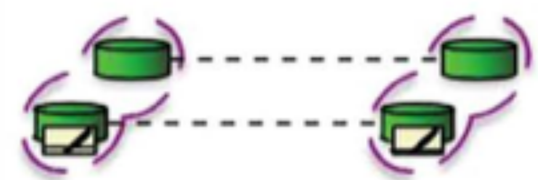
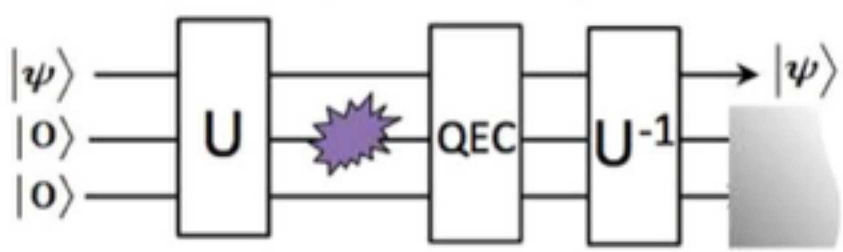
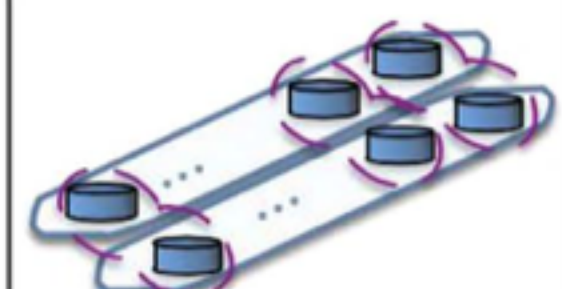
1. To make basic entanglement over a distance (e.g., over fiber or free space)
2. To manage errors
   - Loss of photons
   - Gate errors
   - Memory errors

Tasks of a Quantum Repeater

1. To make basic entanglement over a distance (e.g., over fiber or free space)
2. To manage errors
   - Loss of photons
   - Gate errors
   - Memory errors
3. To *extend* entanglement across multiple hops

Tasks of a Quantum Repeater

1. To make basic entanglement over a distance (e.g., over fiber or free space)
2. To manage errors
   - Loss of photons
   - Gate errors
   - Memory errors
3. To *extend* entanglement across multiple hops
4. To be part of a *network:*
   - *Route* through a network
   - *Manage resources* (time, memory, photons, …)
   - To be secure; *etc.*

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

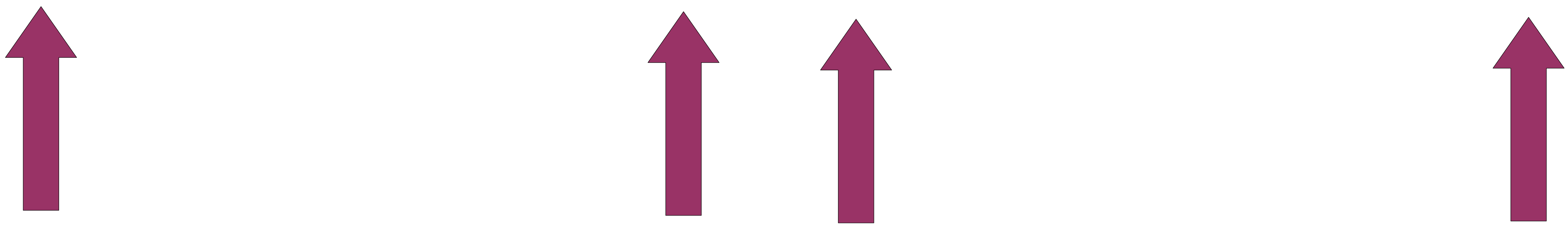
http://www.nature.com/articles/srep20463

Repeater Schemes

- **1G: Purify and swap**
  (Dur & Briegel, Lukin, others; since 1998)
- 2G & 3G: CSS quantum error correction
  (Jiang (Lukin) *et al.*, 2009)
- 2G & 3G: Surface code quantum error correction
  (Fowler *et al.*, 2010)
- 2.5G: Quasi-asynchronous
  (Munro *et al.*, 2010)
- Memoryless
  (Munro *et al.*, 2012)
- All Optical
  (physical layer w/ implications for architecture)

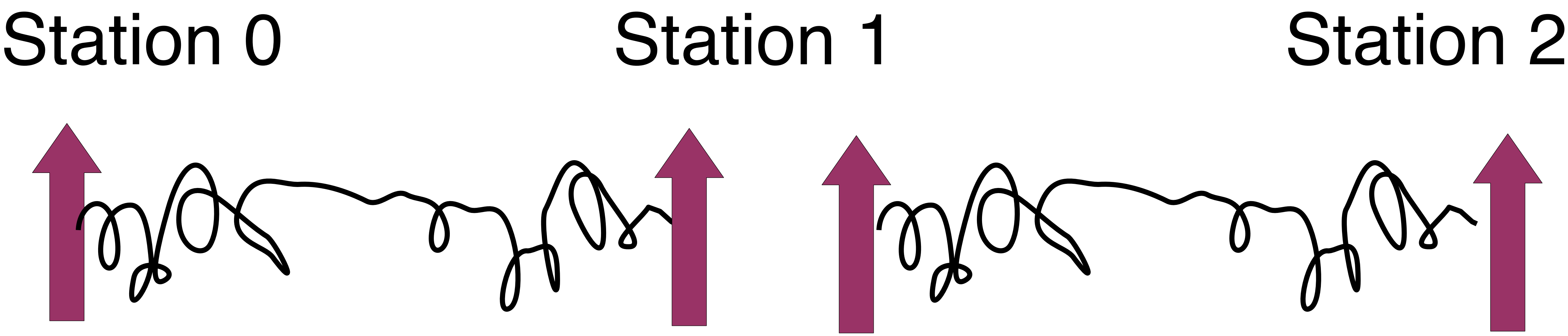
Lengthening Entanglement

Station 0 Station 1 Station 2

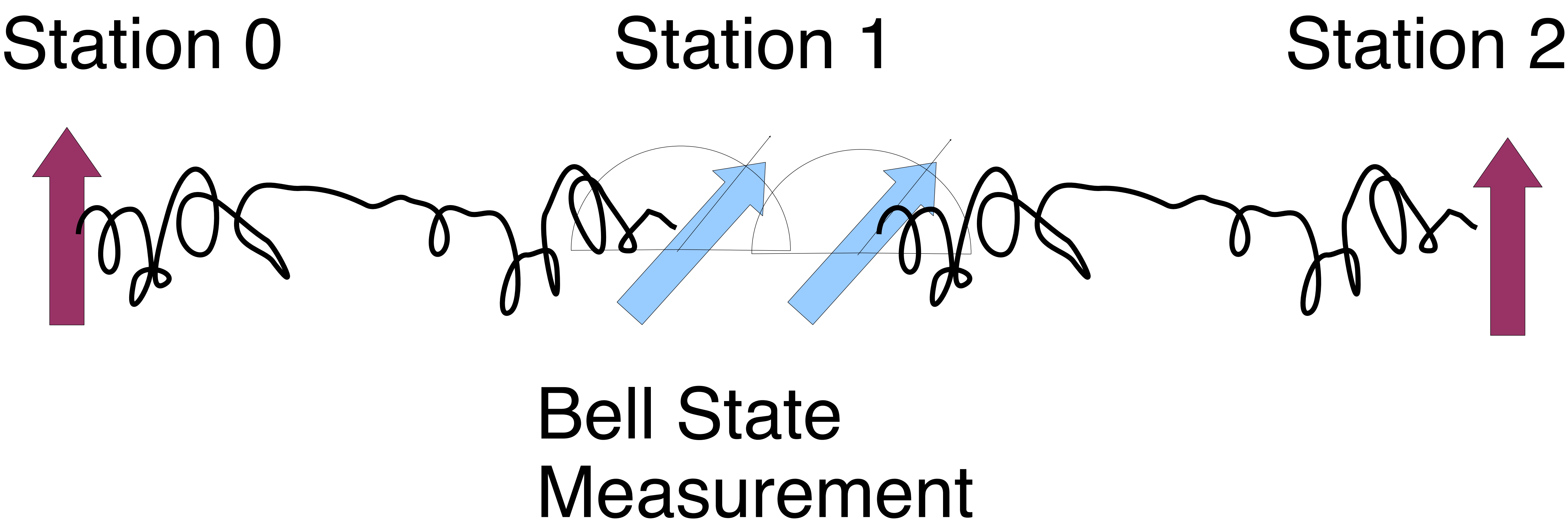


KEIO 150
Design the Future

Lengthening Entanglement

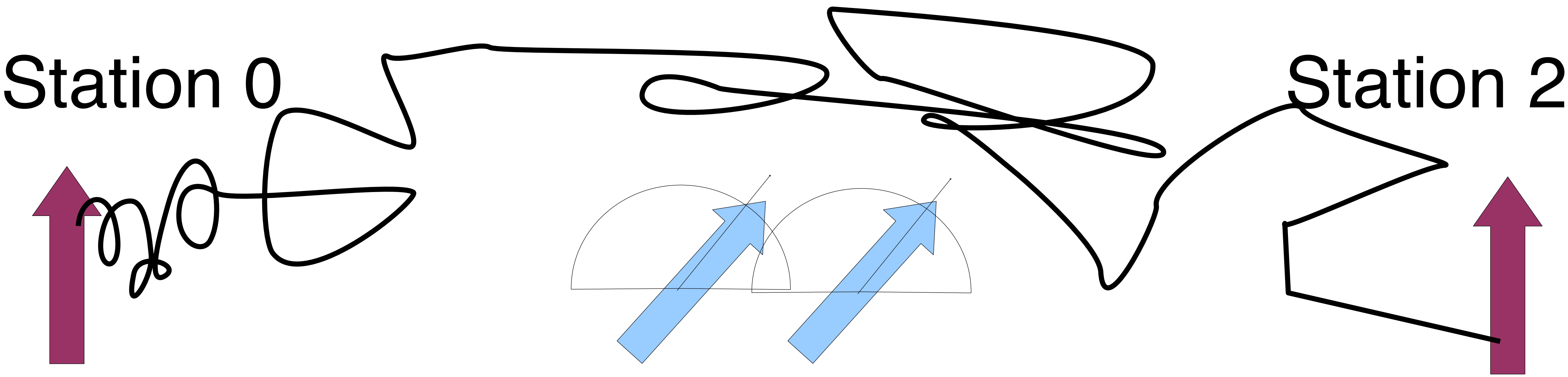


Lengthening Entanglement



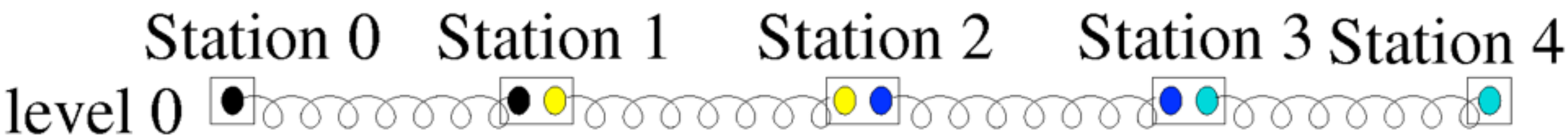
KEIO 150 Design the Future

Lengthening Entanglement



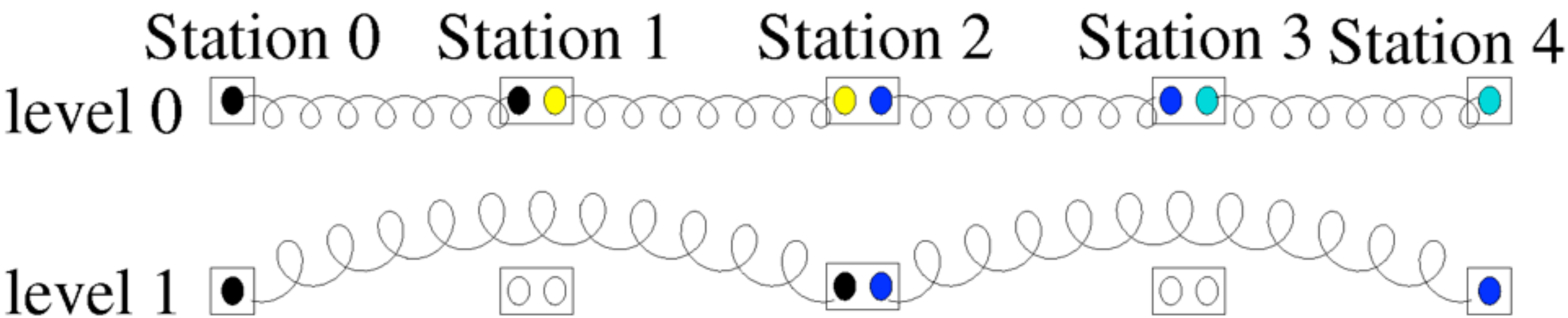
Called *entanglement swapping*.
Fidelity declines; you must *purify* afterwards

Nested Entanglement Swapping



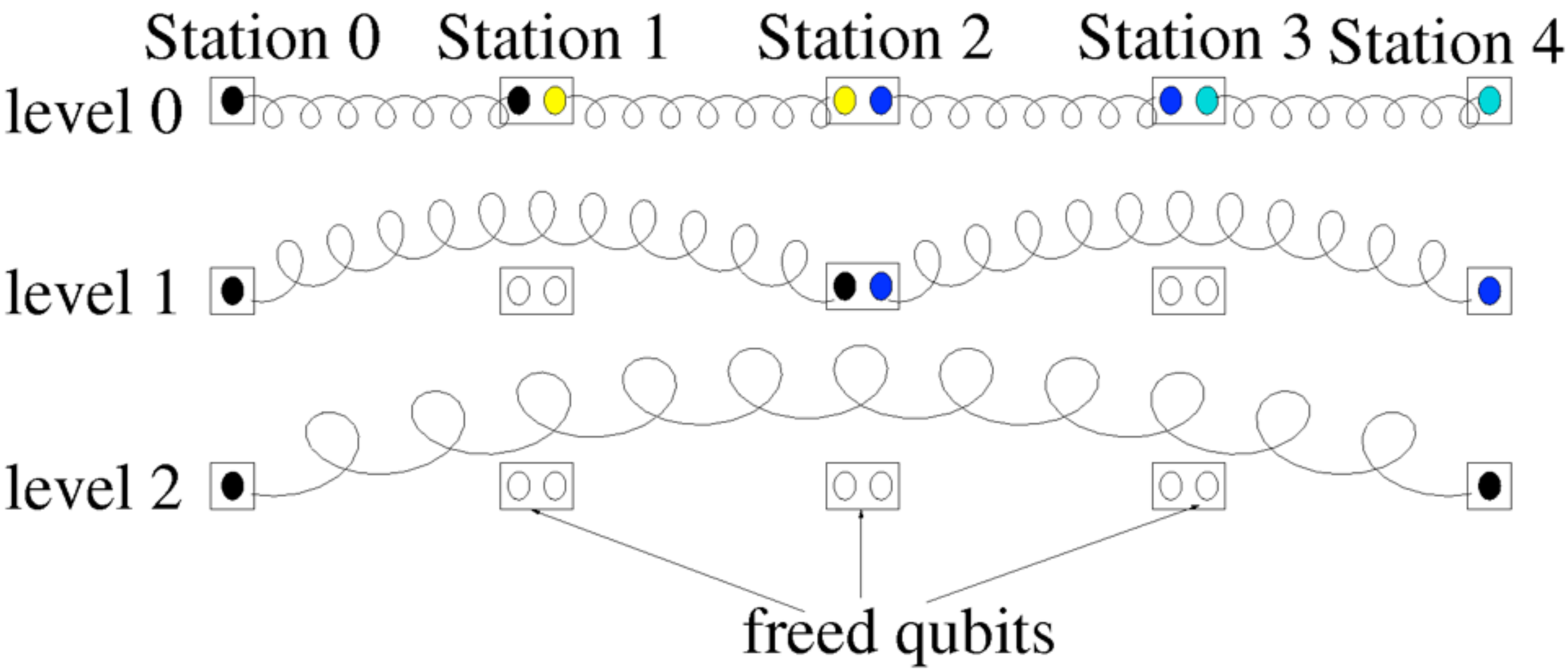
Dur & Briegel, many others

Nested Entanglement Swapping



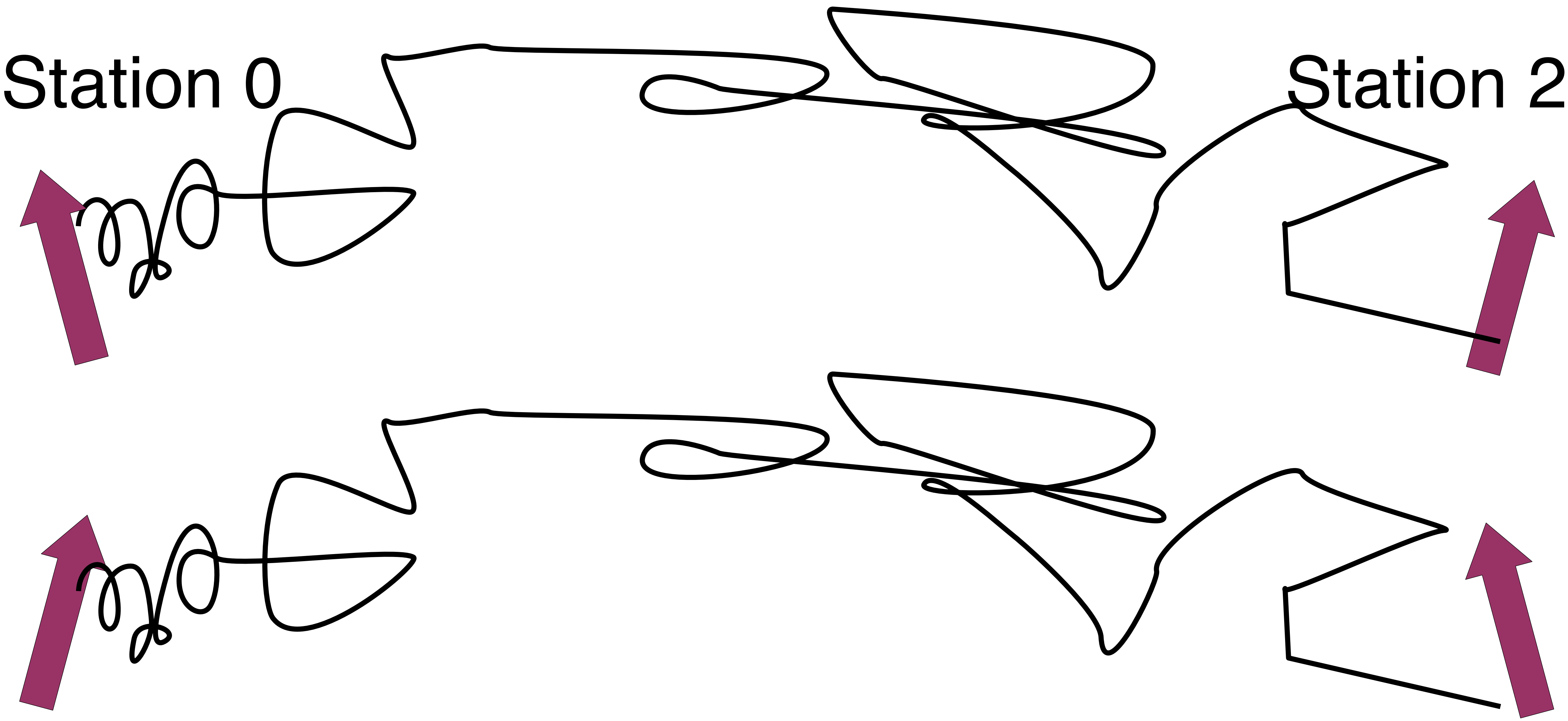
Dur & Briegel, many others

Nested Entanglement Swapping

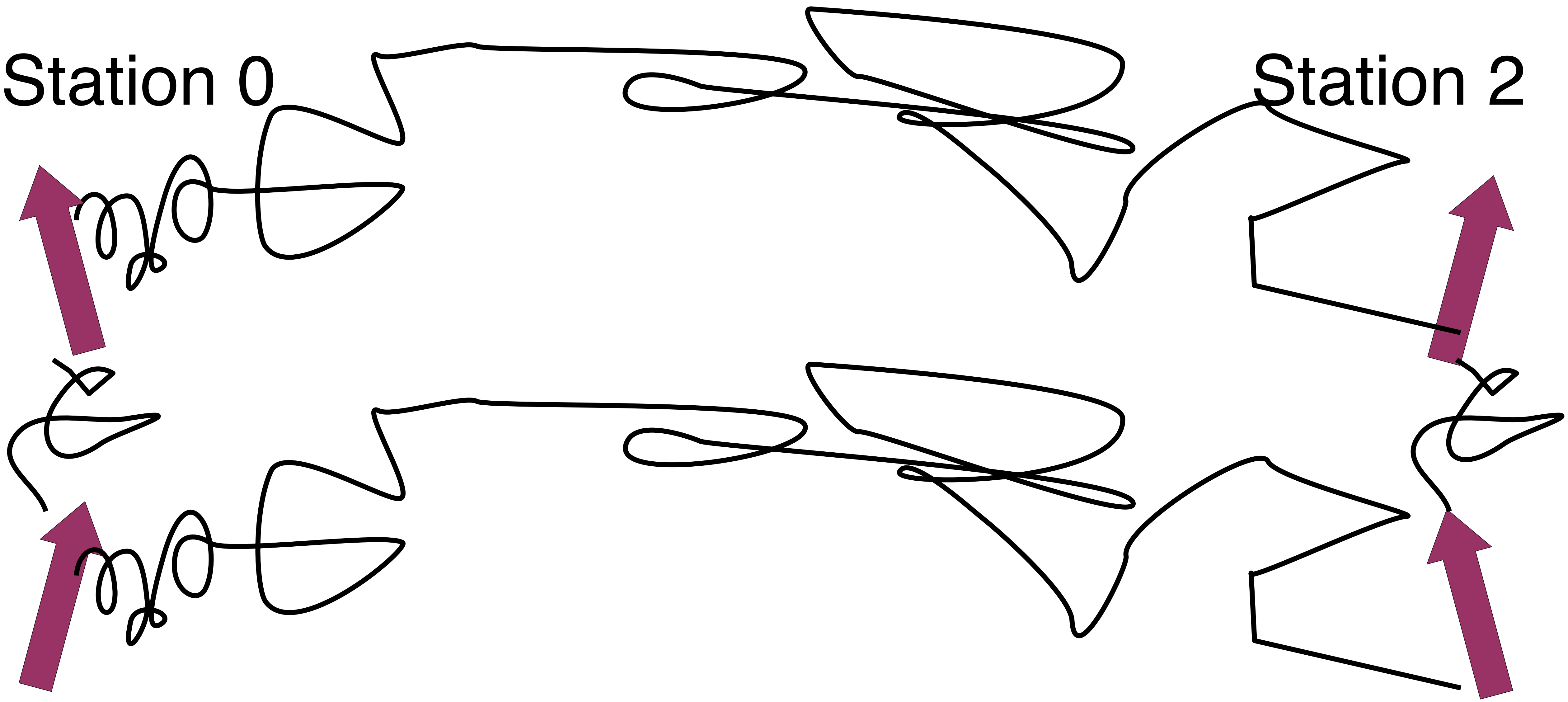


Dur & Briegel, many others

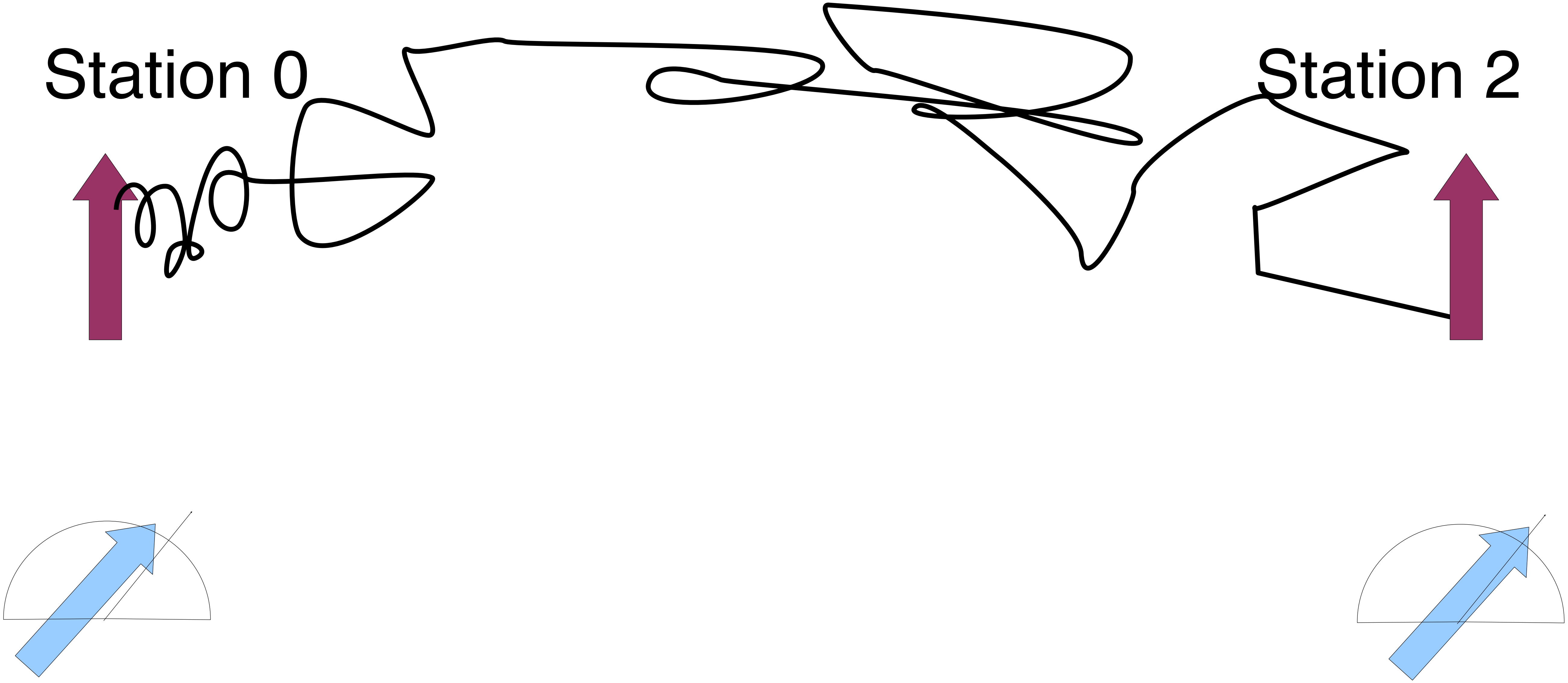
2-EPP: Purification



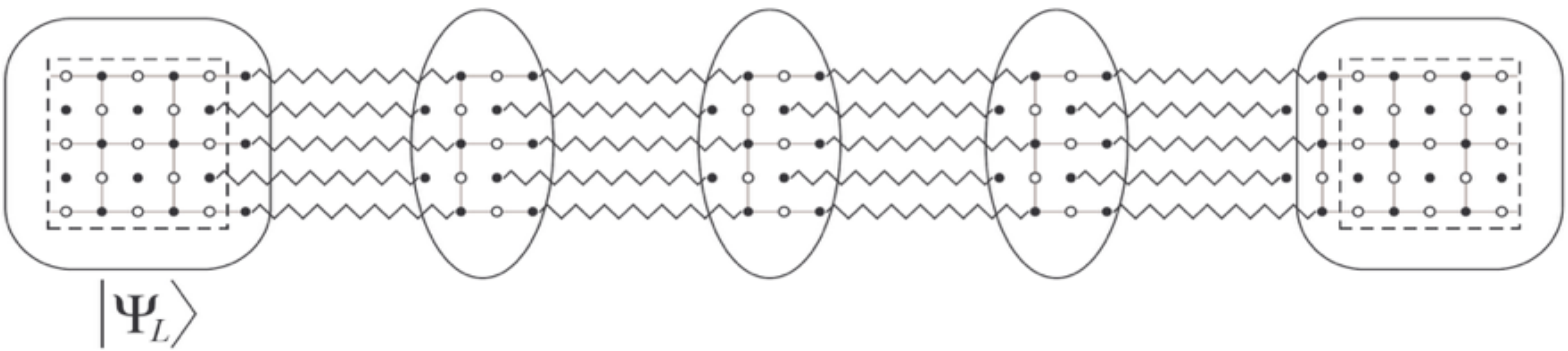
2-EPP: Purification

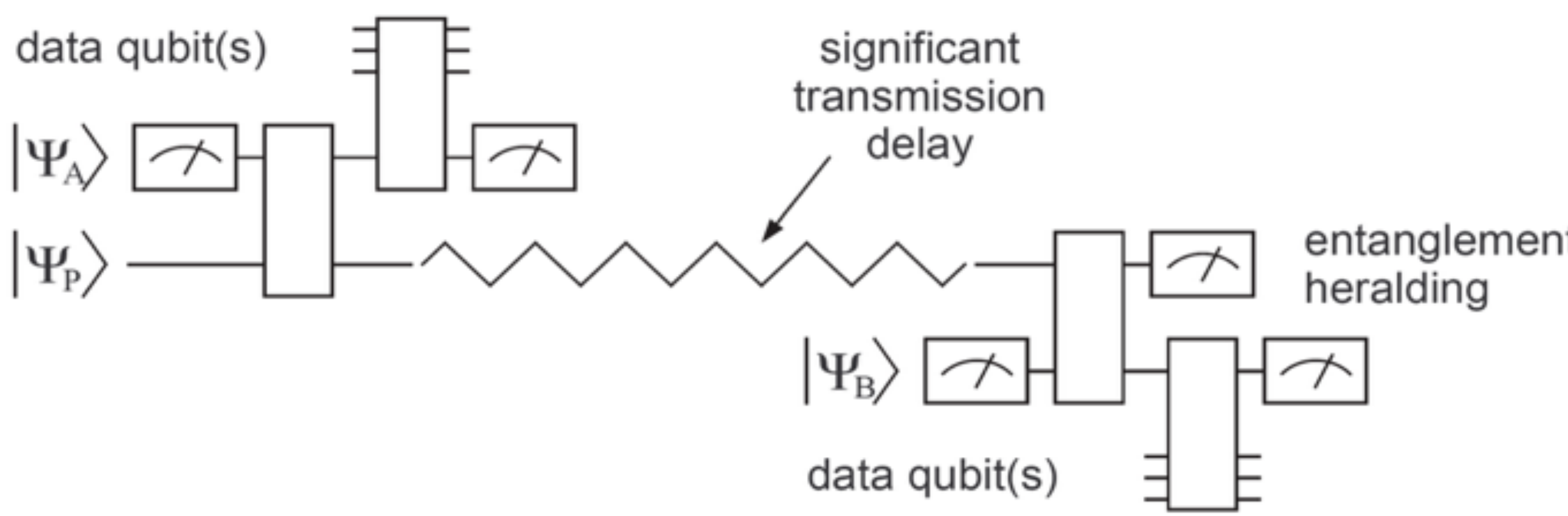


2-EPP: Purification

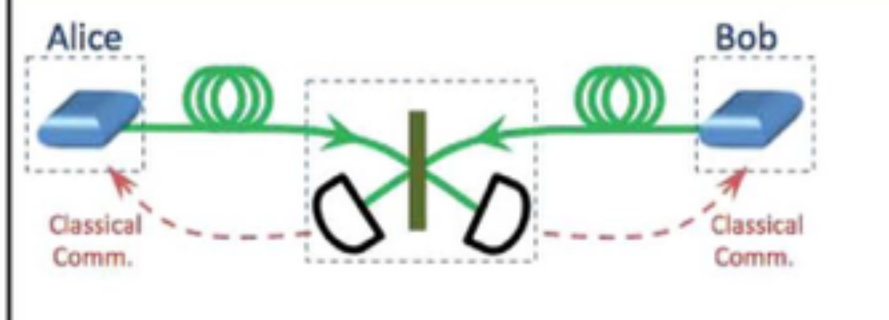
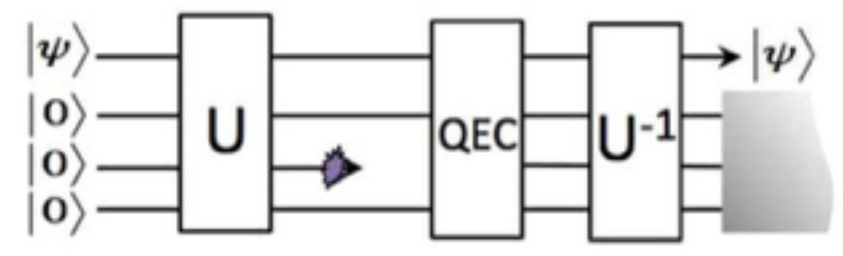
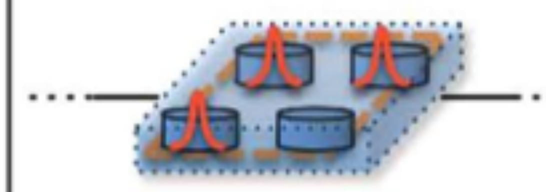
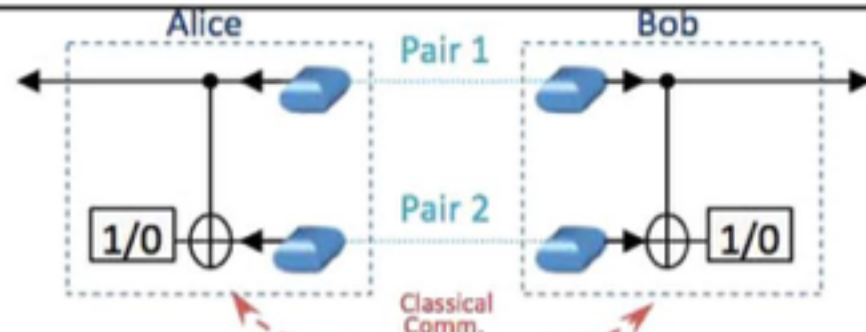
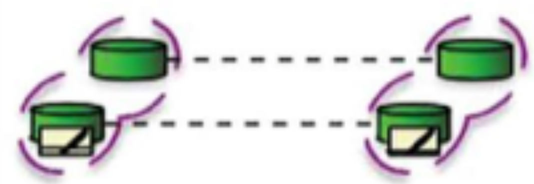
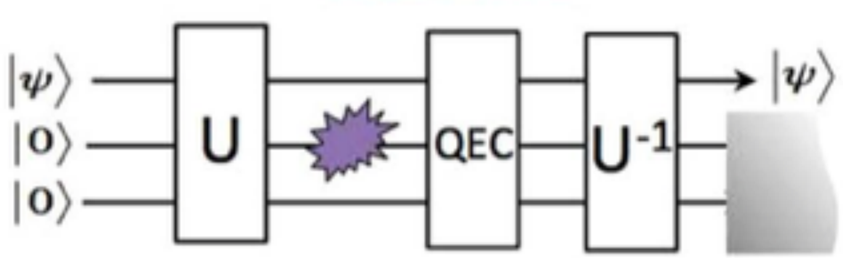
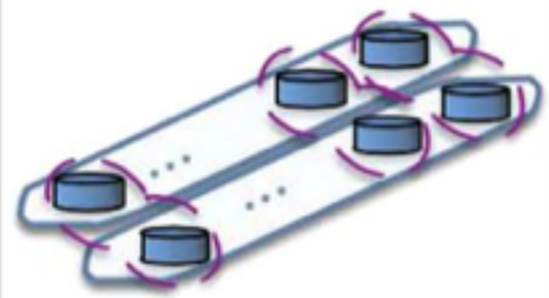


1-EPP: Surface code quantum communication





Fowler *et al., PRL* 104, 2010

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

Learning More

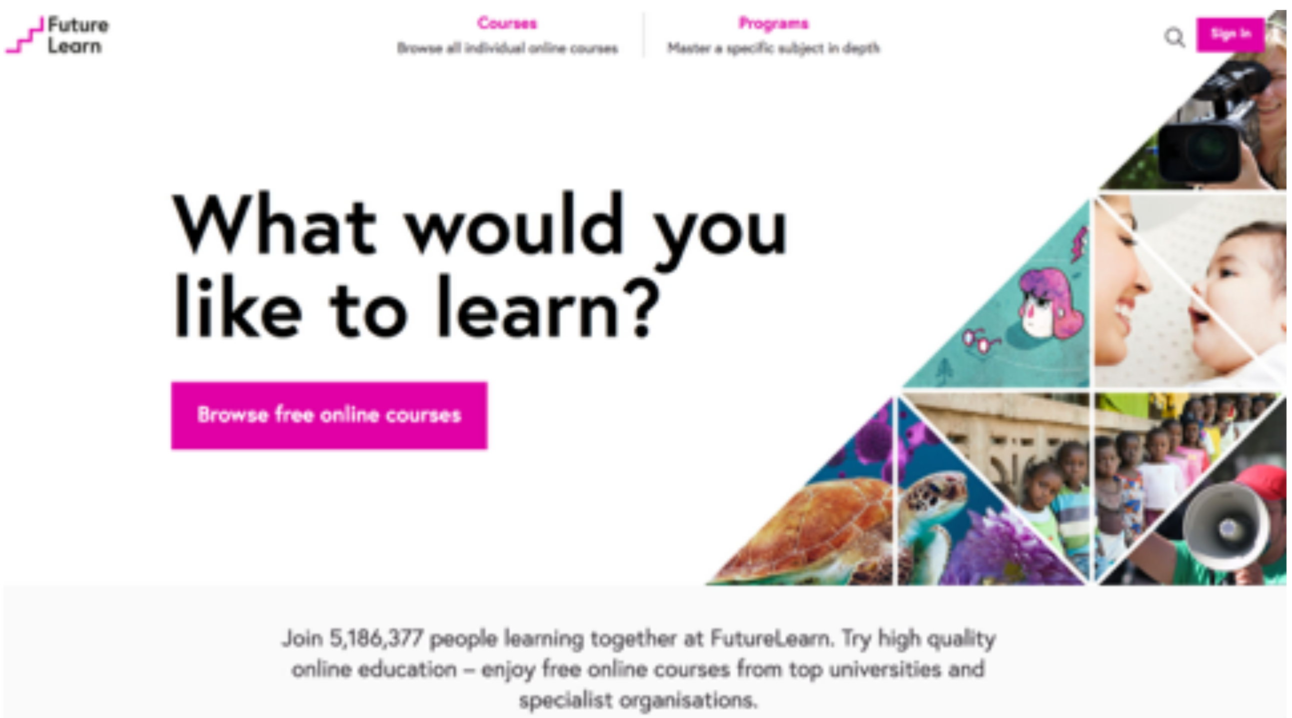
(Many good references in both 英語 and 日本語; here are a few of our own recent ones.)

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

MOOC (massive open online course) on Quantum Computing tentatively scheduled for Fall 2017

DUKE UNIVERSITY | PRATT

Home Program Travel Info Apply

Next meeting this September (2017)
in Europe

Welcome

The organizing committee is pleased to invit … Repeaters and Networks, to be held at the historic Asilo … acific Grove, CA, May 15-17, 2015.

The 1998 proposal introducin … rofile efforts on vital components needed to establish a mu … eaters utilize quantum entanglement, quantum memories, … ors and quantum teleportation to dramatically enhance both th … ication. Various experimental schemes have been propos … y experimental efforts are working towards the realizati … ogress, significant challenges remain, first in proof- of-p … evelopment of practical systems adequate for deployment in

… ing the active research community together to discuss the progress, … directions for quantum repeaters and networks. We invite researchers … technologies and system integration, protocols for connecting repeaters across ne … gh fidelity, architectures for large-scale networks, and applications of distributed quant … ement.

Important Dates

Application Deadline:
Extended until February 13, 2015

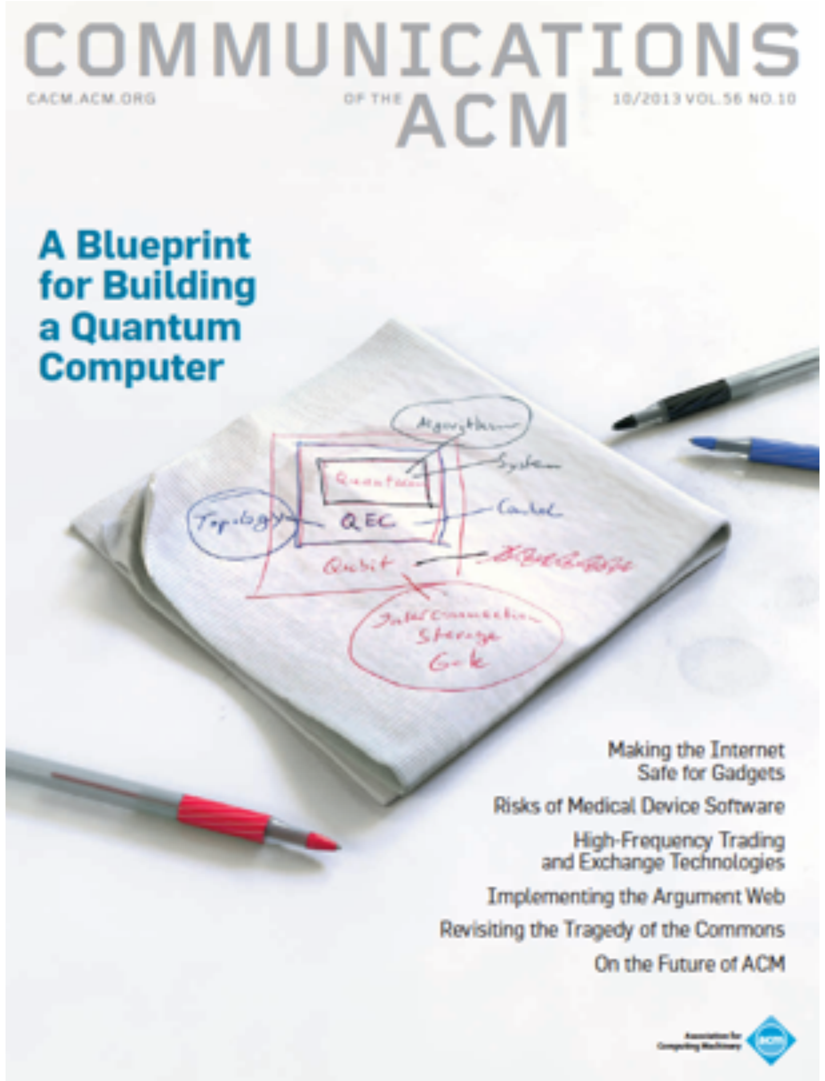
Notification to Attend:
February 20, 2015

Registration Deadline:
March 13, 2015

Hotel Reservation Deadline:
March 31, 2015

May 15-17, 2015

Asilomar Conference Grounds
800 Asilomar Avenue
Pacific Grove, California, USA



QUANTUM COMMUNICATIONS

Designing Quantum Repeater Networks

Rodney Van Meter and Joe Touch

Abstract

Quantum networks generate distributed entangled state or relocate quantum state, uniquely ensuring eavesdropper detection or reaching agreement more quickly than their classical counterparts. These capabilities rely on the composition of link and multihop mechanisms into a coherent system, with particular attention to managing errors in and loss of delicate quantum states. This article explores quantum networking in terms of fundamental network architecture principles, and explains where and how it diverges from its classical counterparts. It discusses engineering principles that ensure robust and interoperable communication by introducing new protocol layers to support quantum sessions, and considers how these layers interact with quantum link mechanisms to support user-level quantum-enabled applications.

to *teleport* data rather than transmit it. The discovery of quantum teleportation and quantum error management led to the development of quantum repeaters. These quantum repeaters are the core of a quantum network architecture because they relay data between potentially different link technologies, just as Internet routers do in classical networks. Other quantum router functions, such as path determination and routing exchange, use classical methods adapted with quantum-related metrics and constraints.

Very little work has been done to date on quantum repeater network architectures, but a half dozen approaches to repeater communication sessions have been proposed [4–9]. Each of these approaches can be organized into a protocol stack in the spirit of the OSI seven-layer model. We focus on the relationship between the session architecture and the restrictions imposed by the physical technologies, and the

Found Phys (2014) 44:819–828
DOI 10.1007/s10701-014-9807-z

Quantum Computing's Classical Problem, Classical Computing's Quantum Problem

Rodney Van Meter

Received: 7 January 2014 / Accepted: 7 May 2014 / Published online: 4 June 2014

Abstract Tasked with the challenge to build better and better computers, quantum computing and classical computing face the same conundrum: the success of classical computing systems. Small quantum computing systems have been demonstrated, and intermediate-scale systems are on the horizon, capable of calculating numeric results

Quantum Networking and Internetworking

Rodney Van Meter

Abstract

Quantum networks build on entanglement and quantum measurement to bring new capabilities to communication systems. Quantum physical effects can be used to detect eavesdropping, to improve the shared sensitivity of separated astronomical instruments, or to create distributed states that will enable numerical quantum computation over a distance using teleportation. Because quantum data is fragile and some quantum operations are probabilistic, errors and distributed calculations must be managed aggressively and perhaps cooperatively among nodes. Solutions to these problems will have both similarities to and differences from purely classical networks. Architectures for large-scale quantum networking and internetworking are in development, paralleling theoretical and experimental work on physical layers and low-level error management and connection technologies. With unentangled quantum networks already deployed, entangled networks may appear within the next few years and will form a vibrant research topic in the coming decade.

Teleportation is a magic word, exotic and evocative, but it has been appearing in serious technical literature with increasing frequency. Both theoretically fascinating and experimentally demonstrated, teleportation is the key to quantum networks [1, 2]. When used in discussions about quantum information, teleportation refers not to Captain Kirk stepping into a machine on the starship Enterprise,

scopes [3], high-precision clock synchronization, and quantum forms of distributed tasks such as leader election, Byzantine agreement [4], and coin flipping. Quantum and classical networks and computing systems will hybridize, allowing applications to select the most efficient mechanism for accomplishing a particular function.

Modern work on quantum communications can be said to

The Path to Scalable Distributed Quantum Computing

Rodney Van Meter, Keio University Shonan Fujisawa Campus
Simon J. Devitt, RIKEN Center for Emergent Matter Science

Researchers are fabricating quantum processors powerful enough to execute small instances of quantum algorithms. Scalability concerns are motivating distributed-memory multicomputer architectures, and experimental efforts have demonstrated some of the building blocks for such a design. Numerous systems are emerging with the goal of enabling local and distributed quantum computing.

Increasingly, quantum computers and networks are expanding already astonishing classical computing and communication capabilities.[1,2] As the sidebar "Key Concepts in Quantum Computing" describes, quantum computing has six underlying concepts. Each concept is simple, but collectively they imply that classical computation is incomplete and that quantum effects can be used to efficiently solve some previously intractable problems.

In the 1980s and 1990s, researchers developed several quantum algorithms and laid the foundation of quantum computational complexity, but they did not fully grasp the process of creating new quantum algorithms. From the early 2000s, researchers have begun to more deeply understand this process, which has caused an explosion of proposed quantum computing algorithms (http://math.nist.gov/quantum/zoo) in areas ranging from quantum chemistry to astrophysics to matrix operations relevant to machine learning.[3] Some algorithms offer only a polynomial speedup over competing classical algorithms; others offer super-polynomial speedups in asymptotic complexity. However, in many cases, studies have not yet investigated the algorithm's interaction with quantum computer architecture to determine constant factors, fidelity demands, and resource requirements. In short, the required size, speed, and fidelity of a commercially attractive quantum computer remain open questions.

Experimental groups are now fabricating quantum processors powerful enough to execute small instances of quantum algorithms and demonstrate quantum error correction (QEC) that extends the lifetime of quantum

Summary

Summary

1. Quantum computing and networking are *happening:* there are applications, hardware, an ecosystem.

Summary

1. Quantum computing and networking are *happening:* there are applications, hardware, an ecosystem.
2. Network applications: crypto functions, sensor networks, distributed quantum computing (encrypting time sharing).

Summary

1. Quantum computing and networking are *happening:* there are applications, hardware, an ecosystem.
2. Network applications: crypto functions, sensor networks, distributed quantum computing (encrypting time sharing).
3. Photon loss, memory are implementation challenges.

Summary

1. Quantum computing and networking are *happening:* there are applications, hardware, an ecosystem.
2. Network applications: crypto functions, sensor networks, distributed quantum computing (encrypting time sharing).
3. Photon loss, memory are implementation challenges.
4. Much *networking* work to be done.

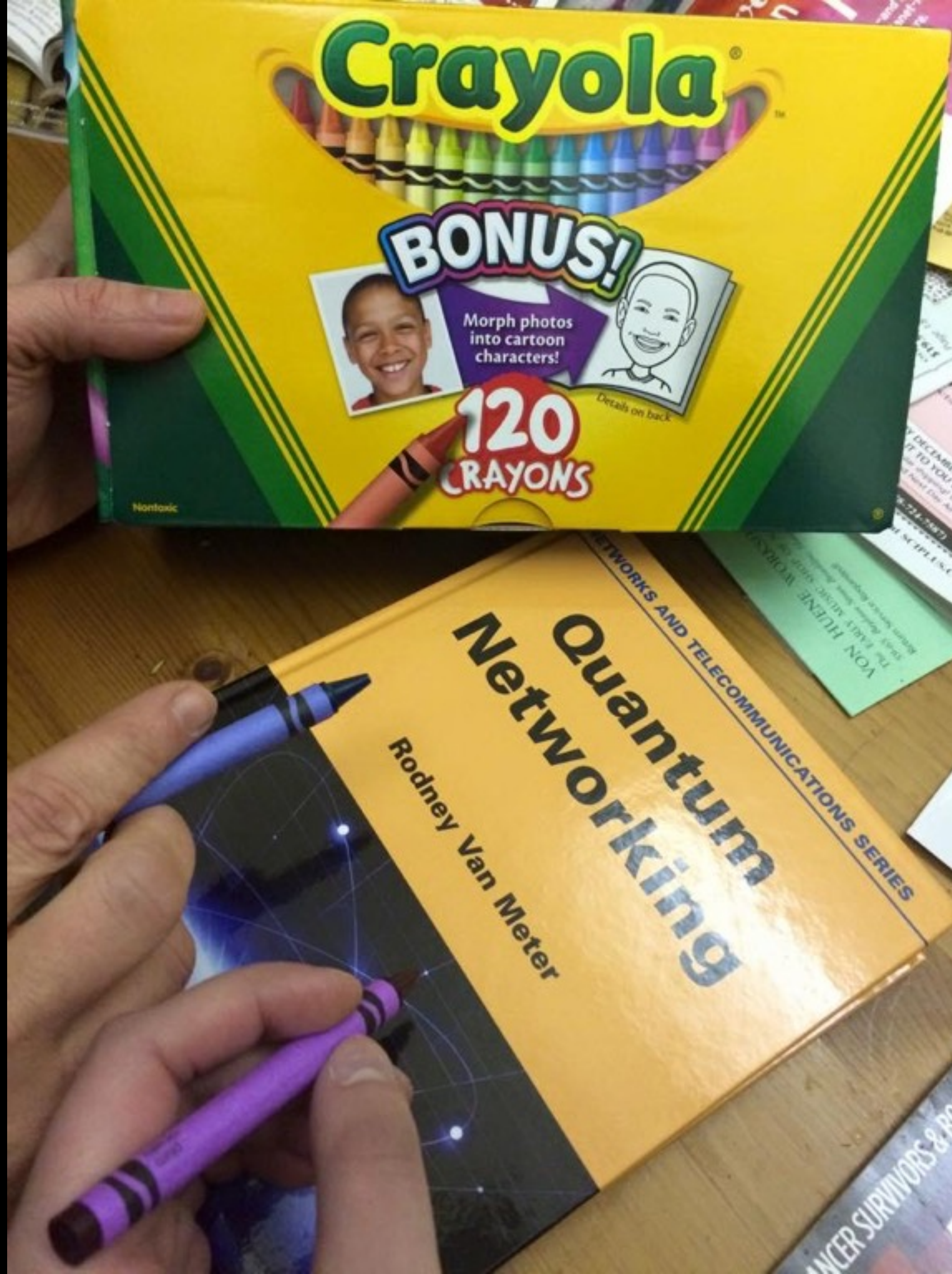
Summary

1. Quantum computing and networking are *happening:* there are applications, hardware, an ecosystem.
2. Network applications: crypto functions, sensor networks, distributed quantum computing (encrypting time sharing).
3. Photon loss, memory are implementation challenges.
4. Much *networking* work to be done.
5. It's all a great deal of fun, come join us!


Google
HA
FA
O(n)







Crayola
BONUS!
Morph photos into cartoon characters!
Details on back
120 CRAYONS
Nontoxic
NETWORKS AND TELECOMMUNICATIONS SERIES
Quantum Networking
Rodney Van Meter