Vision for a QIRG: Quantum Internet Research Group

Rodney Van Meter
(rdv@sfc.wide.ad.jp or rdviii practically everywhere else)
Stephanie Wehner
(s.d.c.wehner@tudelft.nl)

Two kinds of quantum networks

<u>Unentangled Networks</u>

Good only for quantum key distribution (QKD), which aids ***longevity of secrecy*** of encrypted information on classical networks.

Very limited distance (but 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
- high-precision sensor networks
- connecting quantum computers into a Quantum Internet.

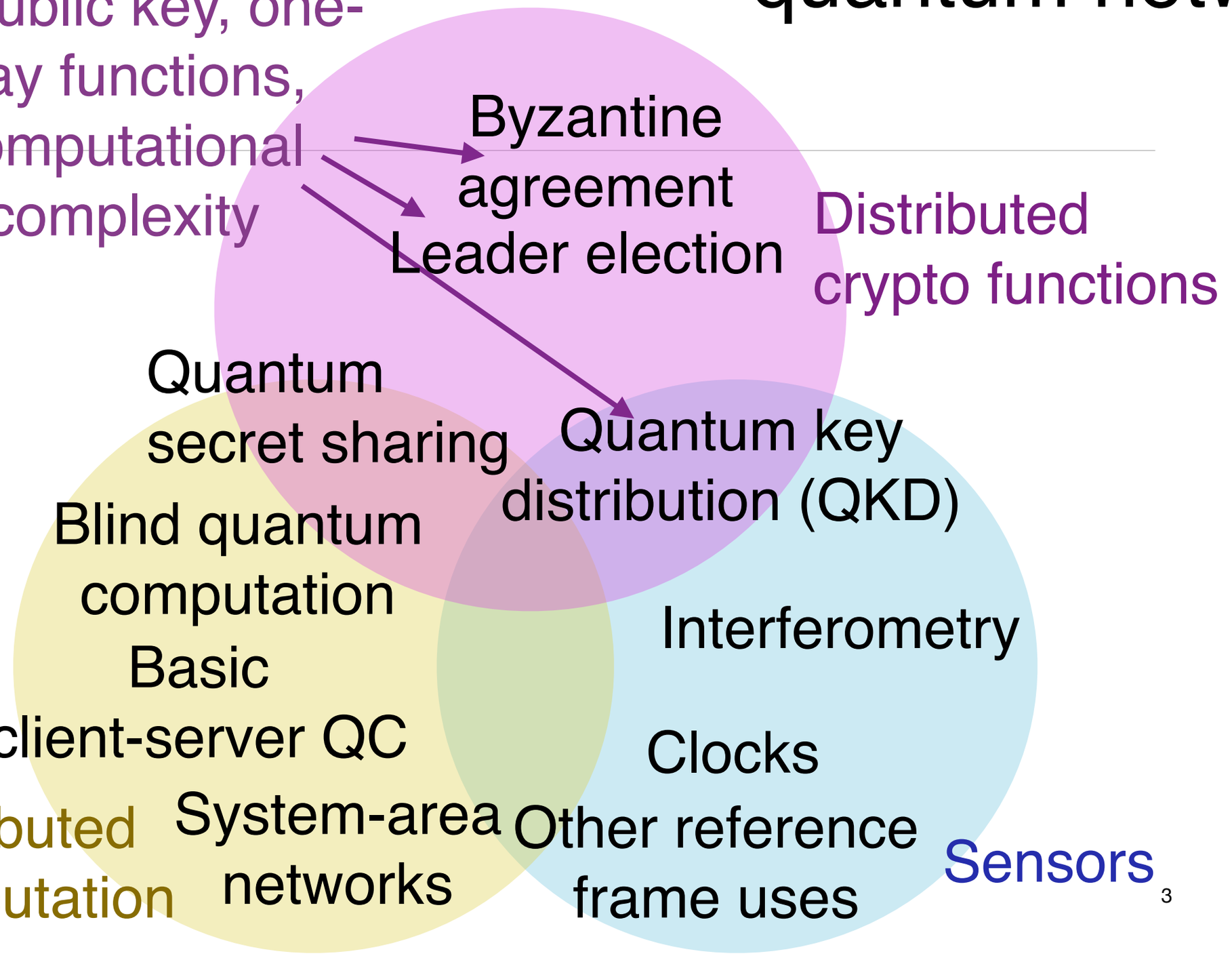
Unlimited distance using *quantum repeaters*.

Strong in networked settings.

Hard to build.

Uses for a quantum network

Reduce dependency on public key, one-way functions, computational complexity



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 (logical operation) inaccuracies
   - Memory decay
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.*

Quantum startups

More than 50 startups now, many created in the last year: some hardware, some software, some networking (primarily quantum key distribution, QKD).

MagiQ (1999 ~)

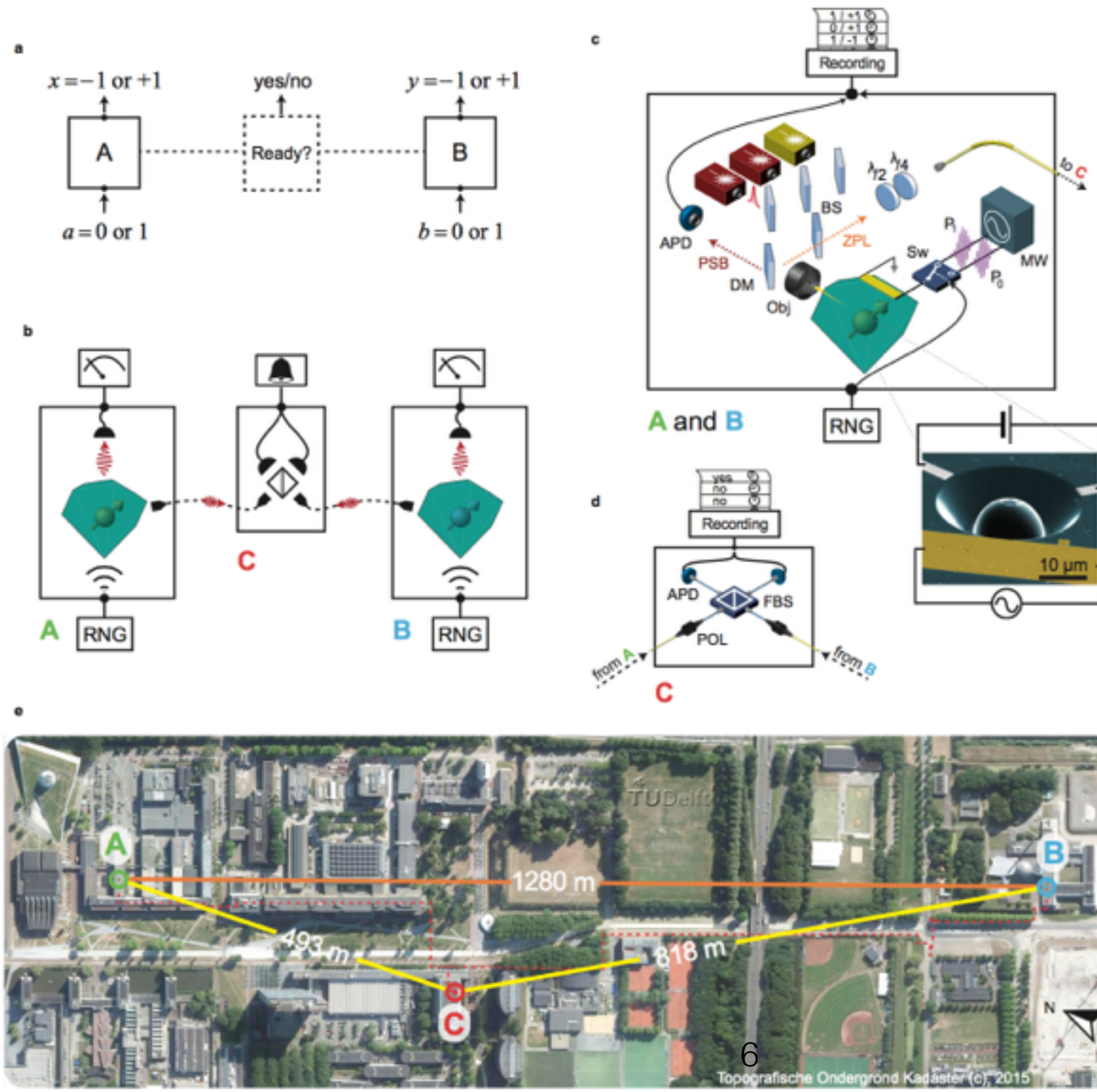
id Quantique (2001 ~)

labs Quintessence (2008 ~)

SEQURENET A QUANTUM KEY TO NETWORK SECURITY (2009 ~)

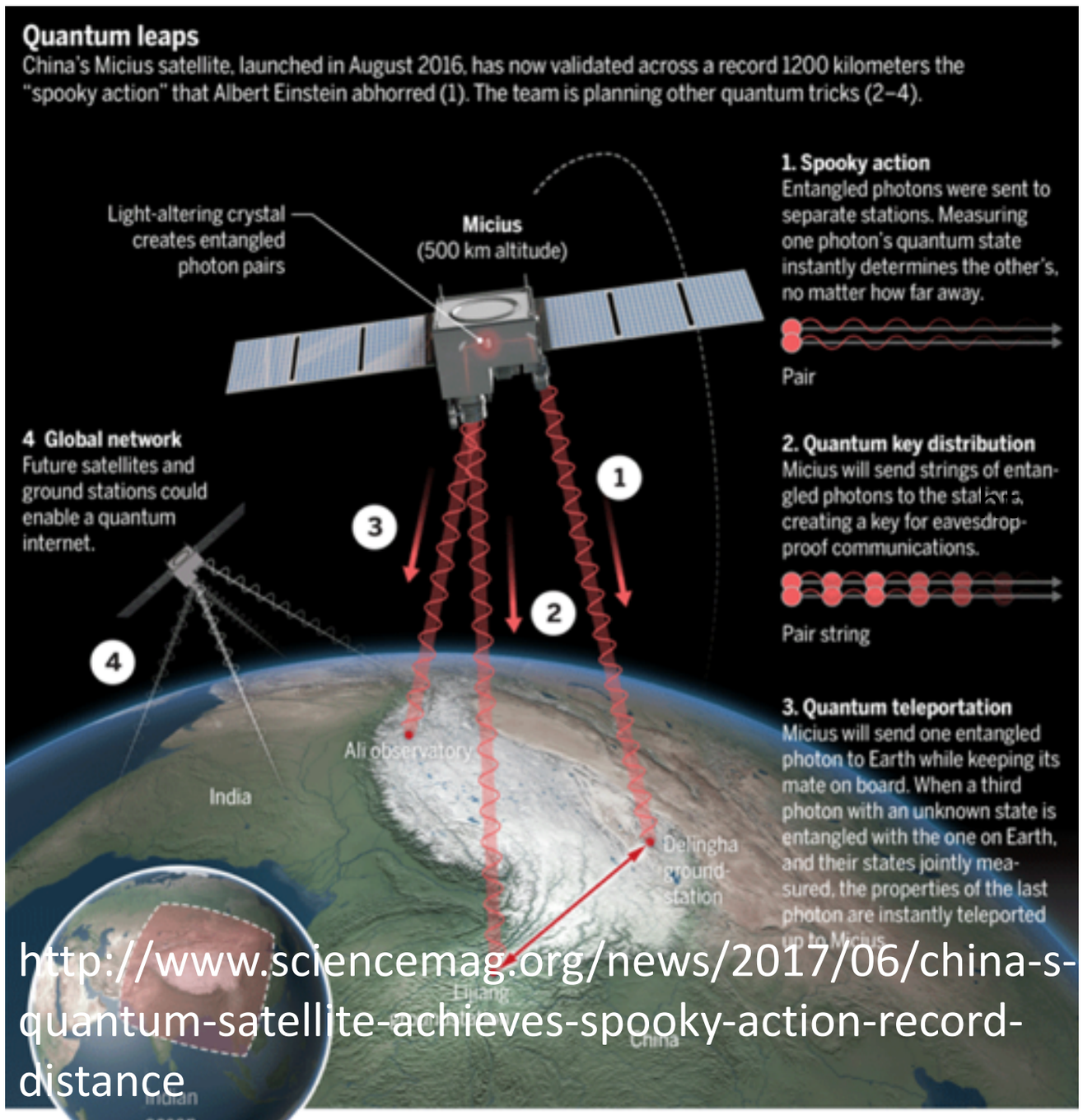
Qubitekk

Delft experiment: 2 nodes

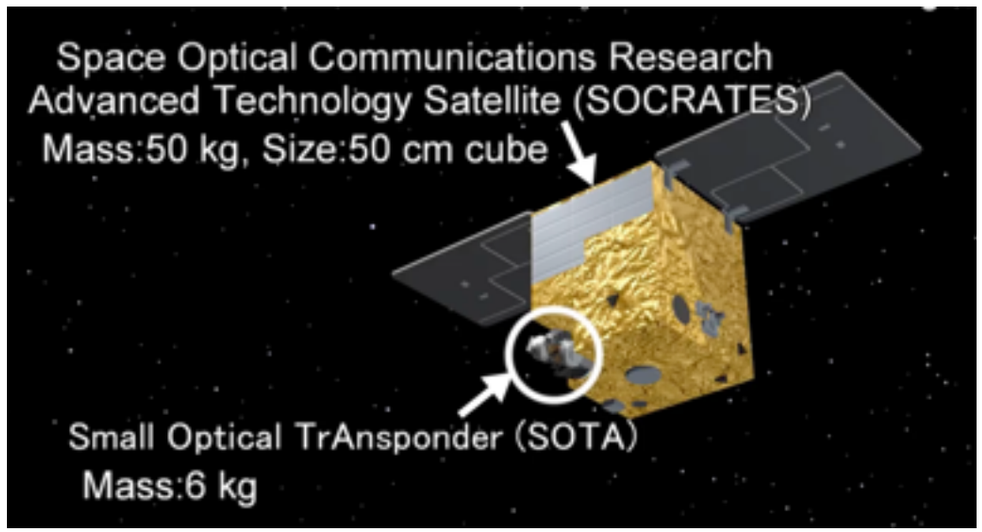


Hensen *et al.*, *Nature,* 29 Oct. 2015

QKD & entanglement distribution via satellite



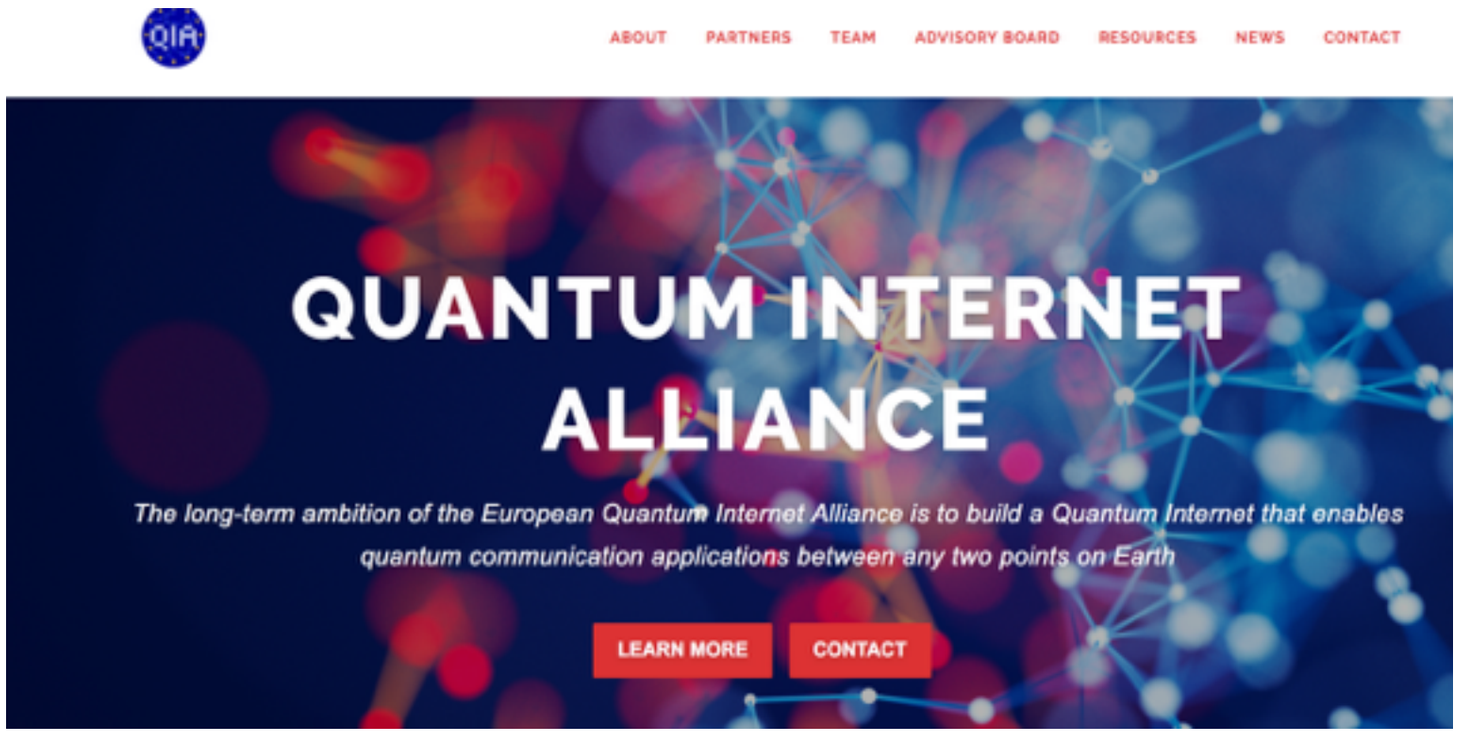
http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance



://www.nict.go.jp/en/press/2017/07/11-1.html

Also experiments from Canada, Singapore and elsewhere

European Quantum Internet effort

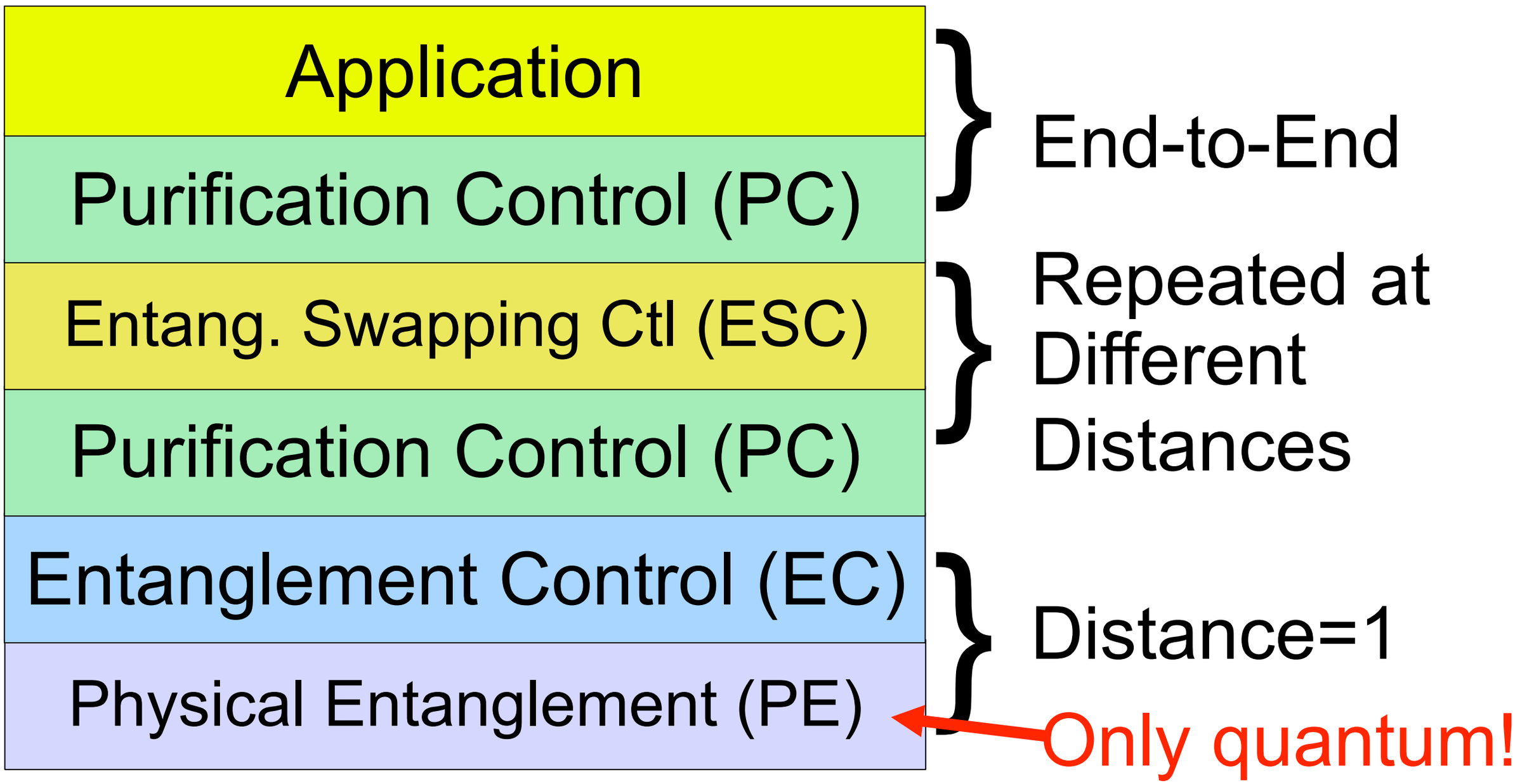


http://quantum-internet.team/

The European quantum technologies flagship programme

http://iopscience.iop.org/article/10.1088/2058-9565/aa6aca/meta

Repeater protocol stack requires networking expertise



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

QIRG

- Classical protocols & architecture for:
  - routing
  - connection setup
  - resource management
  - inter-network interoperability
  - security
  - guaranteeing robustness & consistency
  - app APIs (what's a quantum socket?)

https://www.irtf.org/mailman/listinfo/qirg

Qirg -- Quantum Internet (proposed) RG

About Qirg — English (USA)

Work toward a Quantum Internet is well underway in physics laboratories and in theory groups. The next step is network engineering. Some of the problems we hope to address include:

* routing: there are a number of proposals, including a couple in the last six months or so, and which routing schemes are appropriate for which circumstances needs to be assessed
* resource allocation: some of the routing proposals seem to be including a notion of the dynamic traffic on the network, but this distinction needs to be defined clearly
* connection establishment: what does a request look like (semantics more than syntax) as it propagates across the network?
* interopeability: given than different networks are currently being designed and built, how do we ensure a long-lived internetwork develops?
* security: are quantum repeater networks inherently more or less vulnerable in operations than classical networks?

There are also other problems:

* applications for a Quantum Internet: by far the most important on the agenda is figuring out what we would *do* with a Quantum Internet, including what data rates and fidelities are required (otherwise, there is no market for a QI)
* multi-party states and multi-party transfers such as network coding: rather than simple, independent point-to-point transfers, how can we create and use more complex states?

But perhaps two of the most important things that can be done as a *community* are:

* There is a taxonomy of 1G, 2G, 3G repeaters, created by Muralidharan, Jiang and others
* Wehner and Elkhouss have created a great roadmap of milestones for quantum networks

Discussing, perhaps enhancing, publicizing and endorsing such roadmaps/taxonomies might be a good starting point.

To see the collection of prior postings to the list, visit the Qirg Archives or Qirg MHonArc Archives.

Using Qirg

To post a message to all the list members, send email to qirg@irtf.org.

You can subscribe to the list, or change your existing subscription, in the sections below.

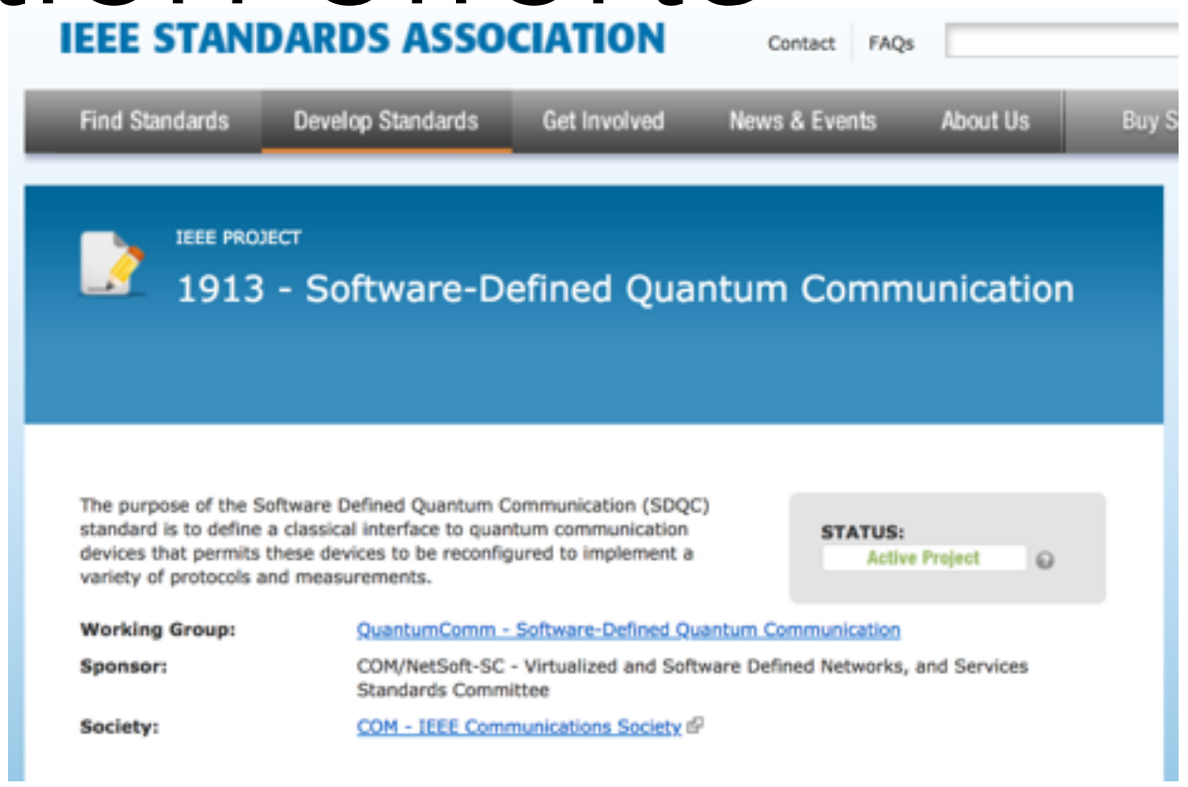
Subscribing to Qirg

Subscribe to Qirg by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a private list, which means that the list of members is not available to non-members.

- https://www.irtf.org/mailman/listinfo/qirg

Some QKD-oriented standardization efforts

ETSI effort on quantum key distribution (QKD)



IEEE P1913, Software-Defined Quantum Communication

Also, of course, methods for out-of-band key management for IPsec!

Join us!

- Suggest a prettier name?
- Discuss charter
- Tentative plan is to meet 3x/year:
  - 1 @IETF
  - 1 @quantum conference
    (QCrypt or WQRN, most likely)
  - 1 virtual

universität innsbruck

EN Staff login Search Quicklinks

Studies Research Connect About u

2nd Workshop for Quantum Repeaters and

2nd Workshop for Quantum Repeaters and Networks

Home

We are pleased to invite you to the Second Workshop for Quantum Repeaters and Networks, to be held in Seefeld, Austria, Sept. 25-26, 2017.

The first workshop, held in 2015 in Pacific Grove, California, brought together a diverse international group of researchers f
fruitful weekend of talks and discussions. At this second workshop, we look forward to continuing these discussions, w
focus on recent progress, challenges and new possible directions emerging in our community. We invite research
key enabling technologies and system integration, protocols for connecting repeaters across network links wit
architectures for large-scale networks, and applications of distributed quantum entanglement.

We've arranged the technical sessions around four themes, with the goals of quantum networks, fig
technologies, and paths to scalability; please see the Speakers & Program page for details. There

We encourage you to apply and hope to see you in Seefeld in September.

Next meeting 2019
in Japan (date & location TBD)

DUKE UNIVERSITY | PRATT

Home Program Travel Info Apply

Welcome

The organizing committee is pleased to invite you to the first Workshop for Quantum Repeaters and Networks, to be held at the historic Asilomar Conference Grounds in beautiful Pacific Grove, CA, May 15-17, 2015.

Important Dates

Application Deadline:
Extended until February 13, 2015

Notification to Attend:
February 20, 2015

References: Recent Bell Inequality Violation Experiments

- Three major research groups announced important 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/

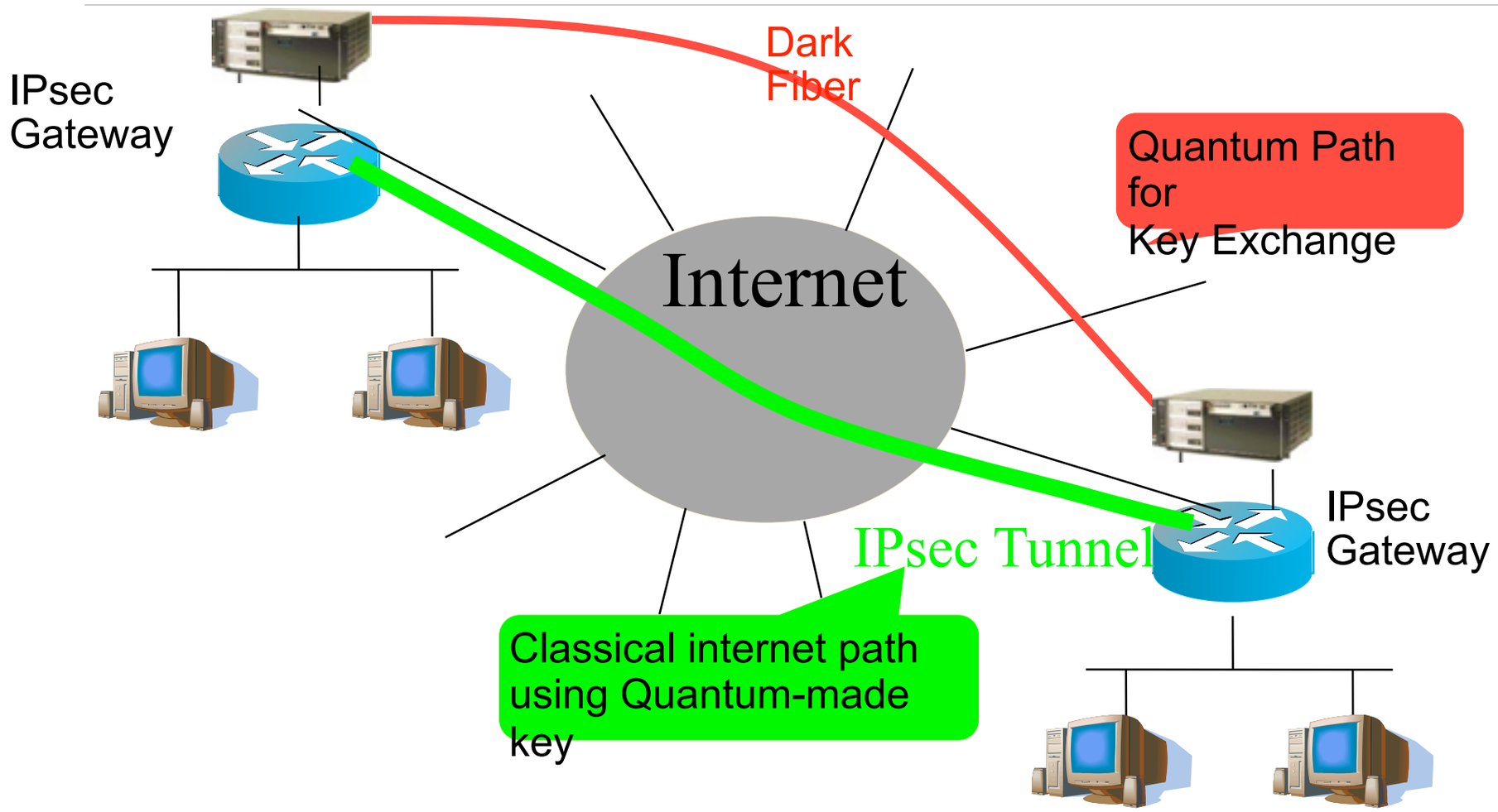
- The Wikipedia article is a reasonable list of Bell inequality violations going back three decades: https://en.wikipedia.org/wiki/Bell_test_experiments

References: Quantum repeaters

- Briegel, Dür, Cirac & Zoller, *Phys. Rev. Letters* 81, 5932, 1998
  https://arxiv.org/pdf/quant-ph/9803056
- 2,177 things that reference the above
- Van Meter, *Quantum Networking*, Wiley-ISTE, 2014

Backup Slides

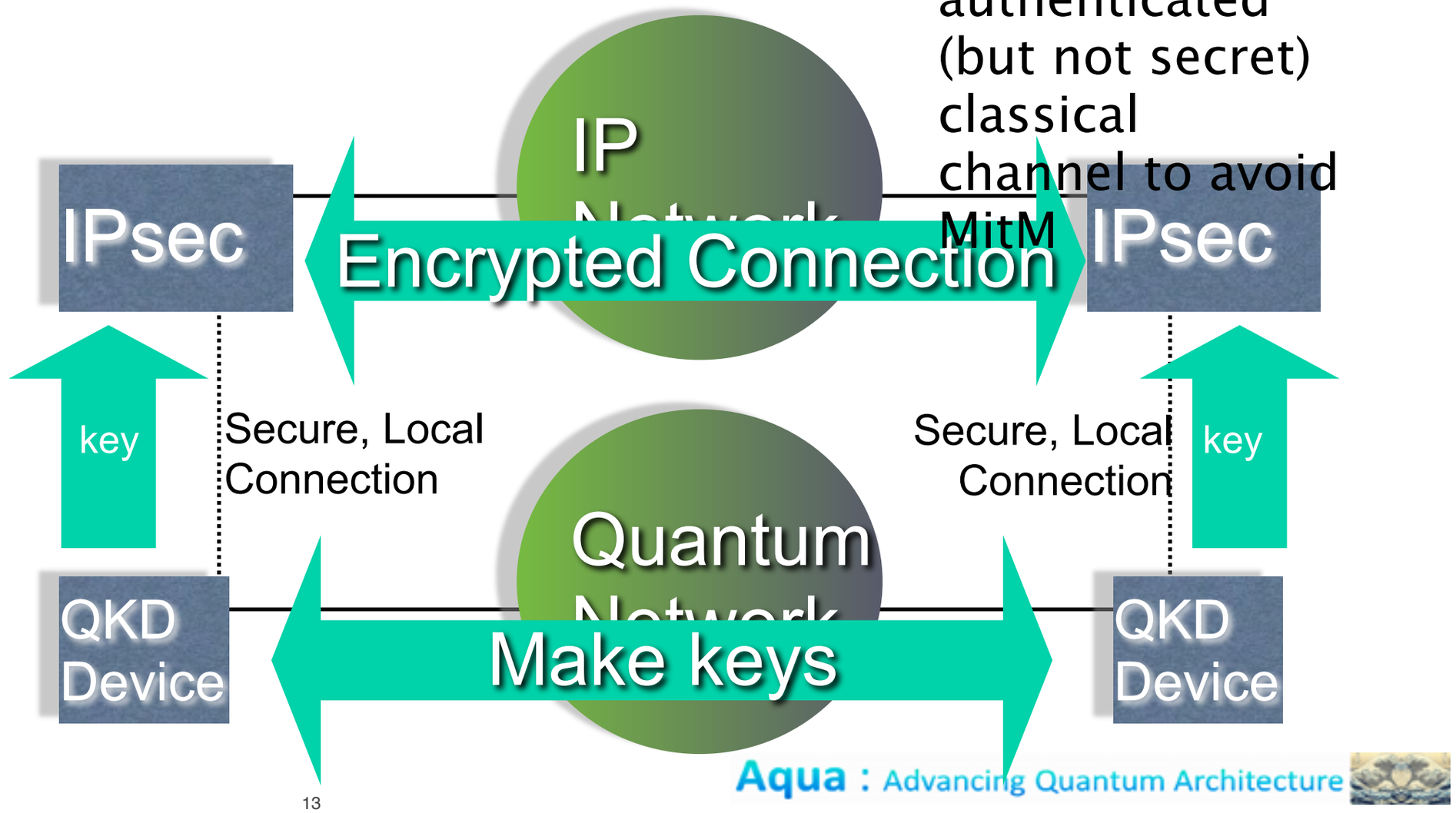
IPsec with QKD: Quantum-protected campus-to-campus connection



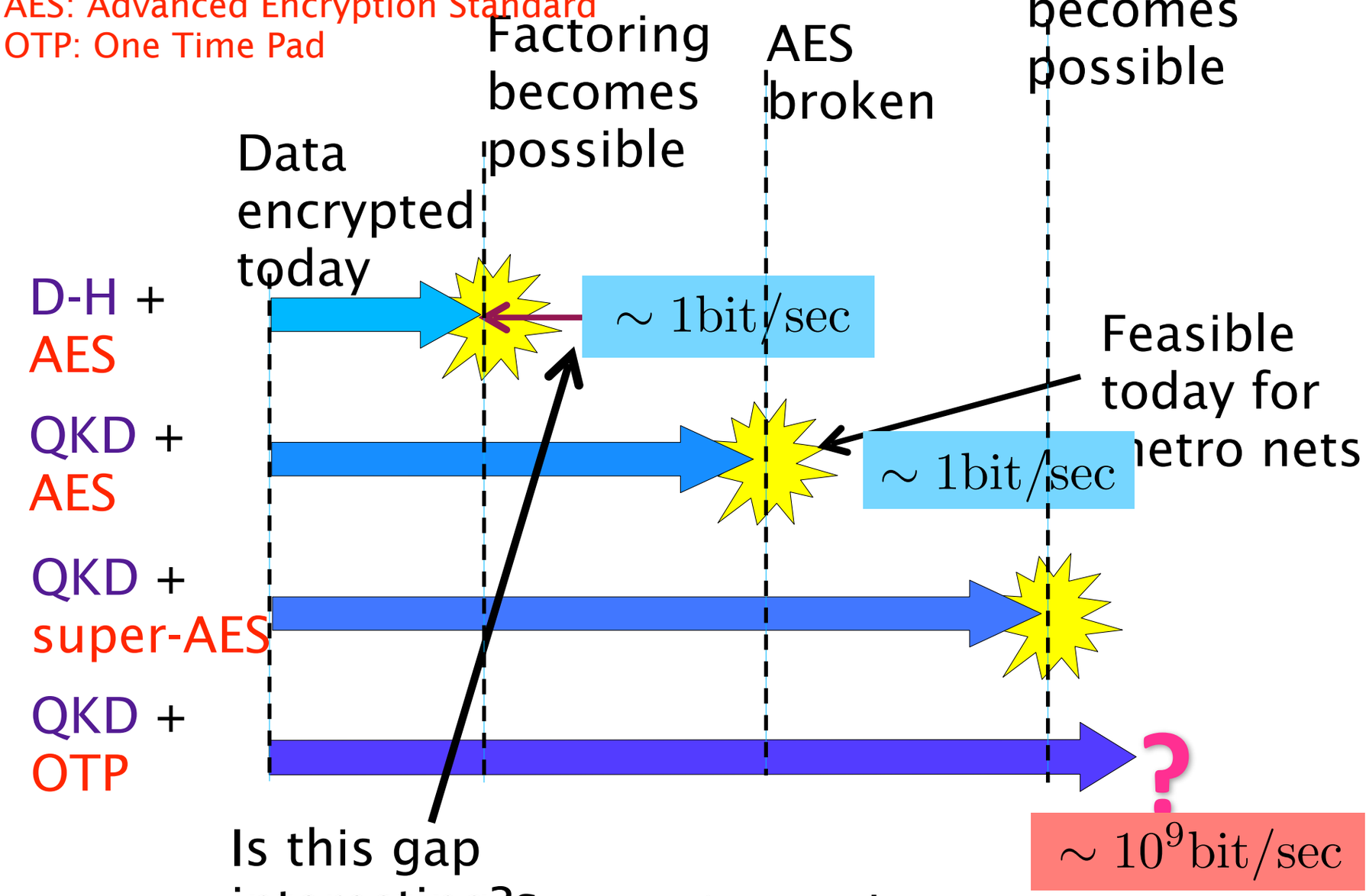
draft-nagayama-ipsecme-ike-with-qkd-01.txt, 2014/10

IPsec with QKD

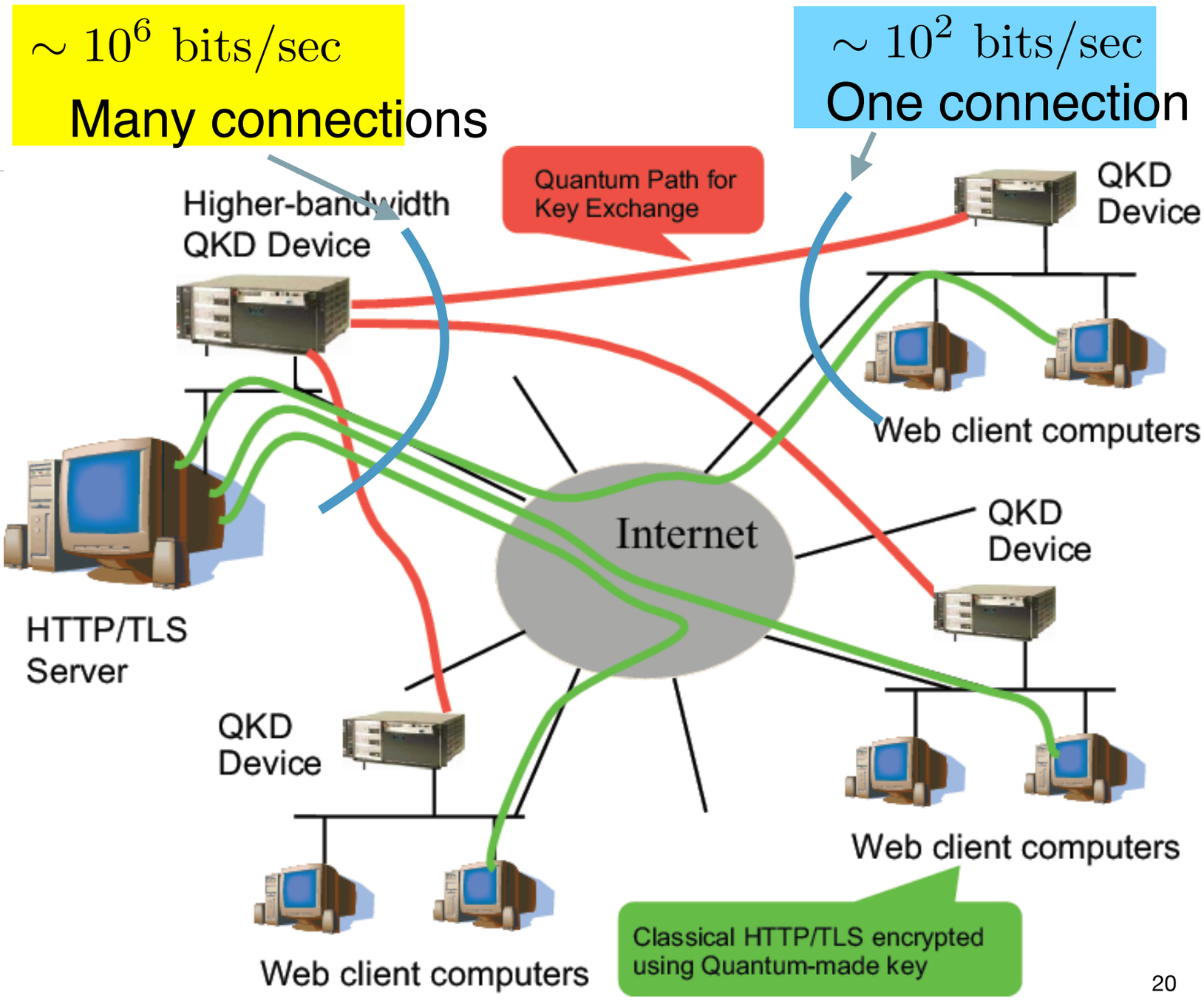
n.b.: QKD requires an authenticated (but not secret) classical channel to avoid MitM



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



TLS with QKD:


$\sim 10^6$ bits/sec
Many connections
$\sim 10^2$ bits/sec
One connection
Higher-bandwidth
QKD Device
Quantum Path for
Key Exchange
QKD
Device
Web client computers
Internet
QKD
Device
HTTP/TLS
Server
QKD
Device
Web client computers
Web client computers
Classical HTTP/TLS encrypted
using Quantum-made key

Four-Hop Protocol Interactions