

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

Unentangled Networks

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.

Entangled Networks

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

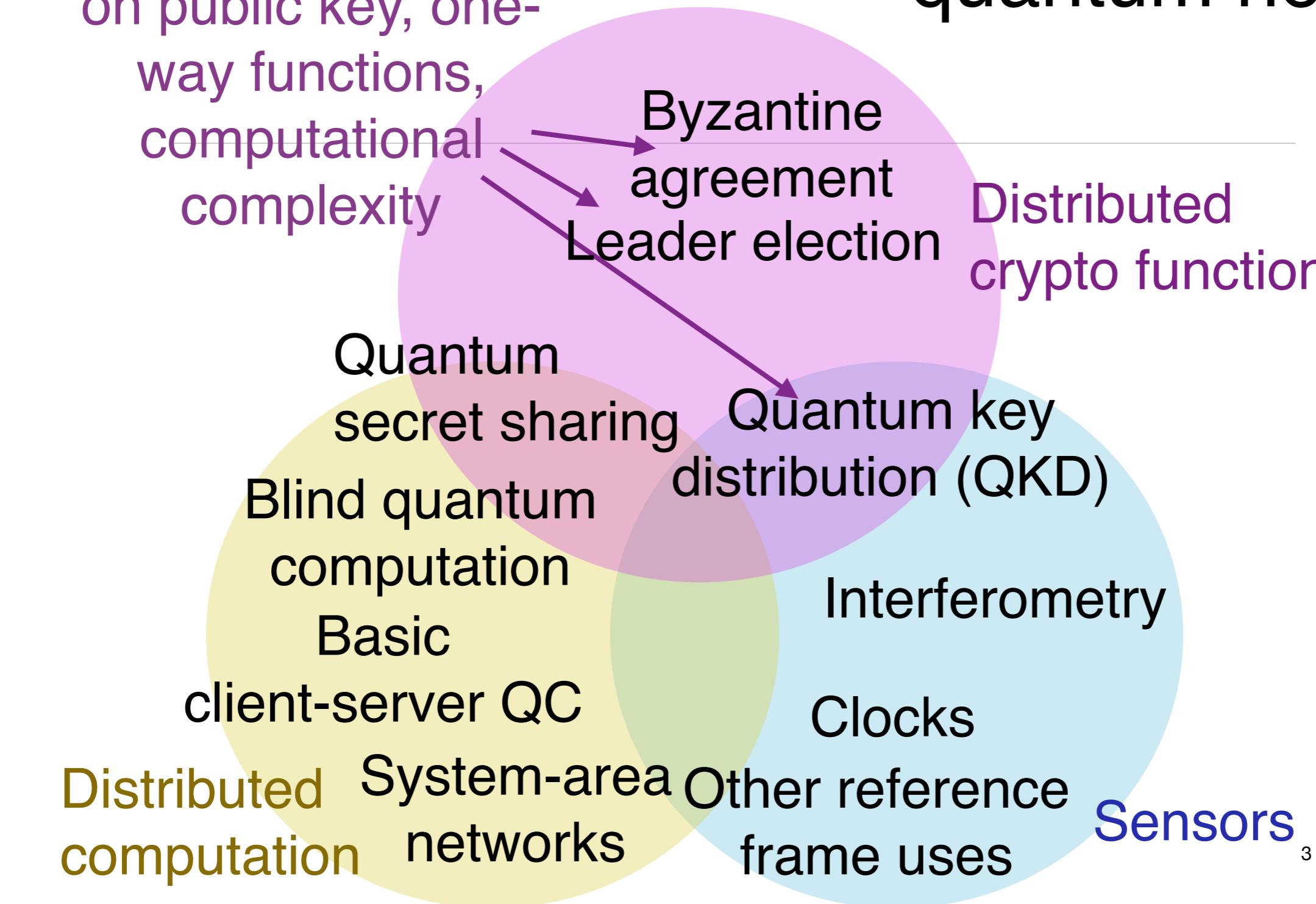
Reduce dependency on public key, one-way functions, computational complexity

Distributed computation
Basic client-server QC
System-area networks

Quantum key distribution (QKD)
Interferometry
Clocks
Other reference frame uses

Distributed crypto functions

Byzantine agreement
Leader election



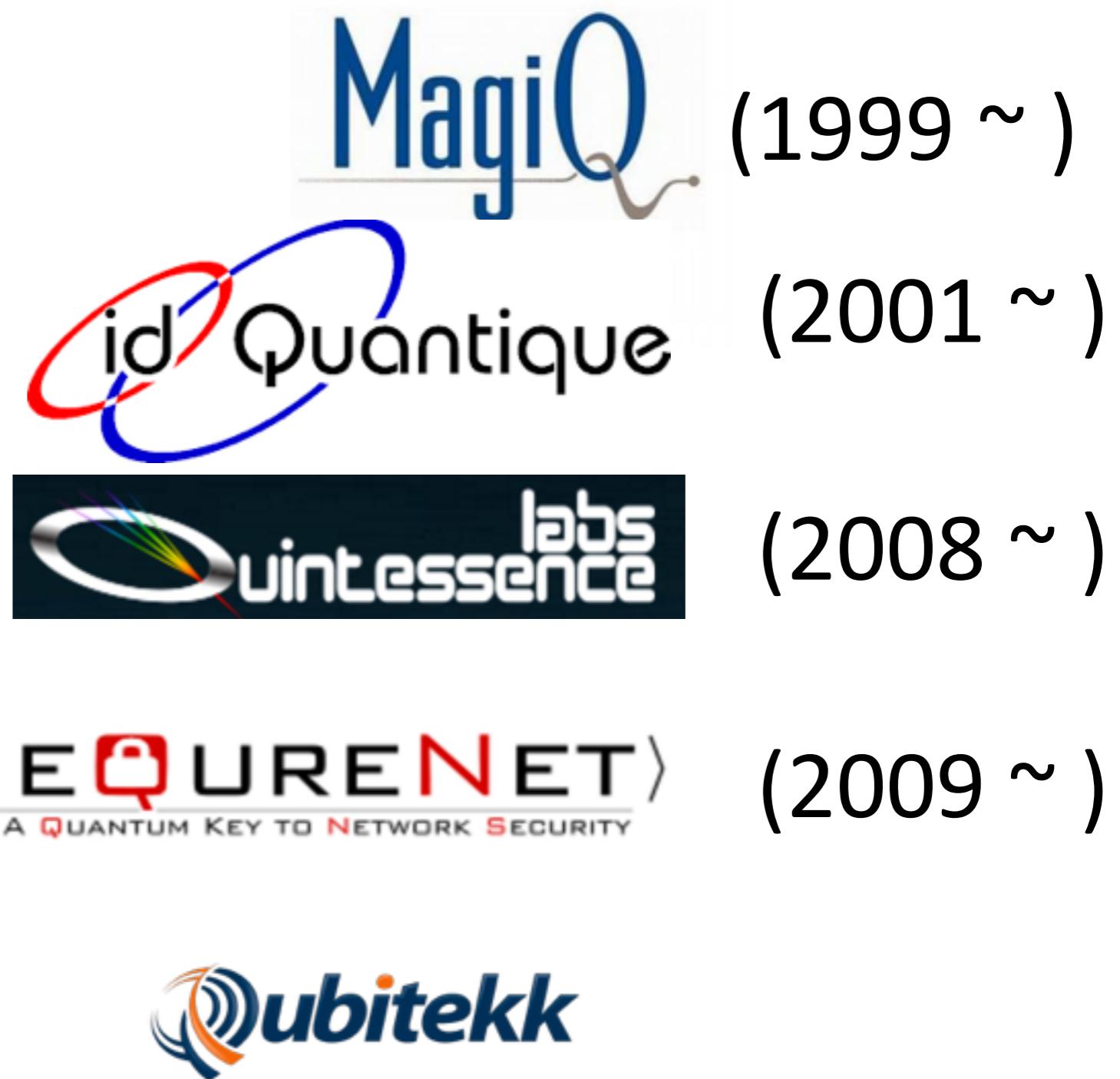
Sensors³

Tasks of a Quantum Repeater

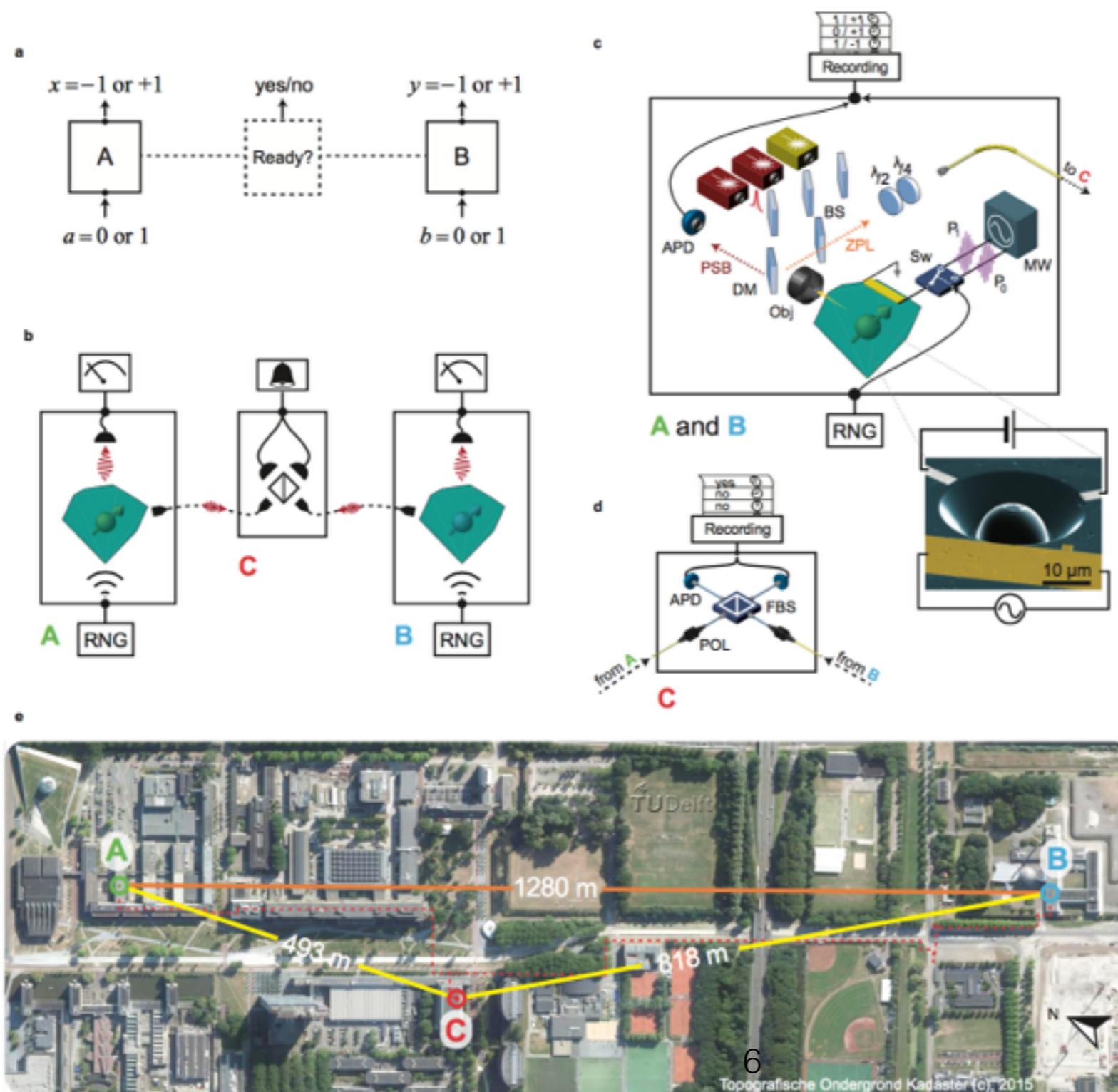
1. To make basic entanglement over a distance
(e.g., over fiber or free space)
2. To manage errors
 - Loss of photons
 - Gate (logical operation) inaccuracies
 - Memory decay
3. To *extend* entanglement across multiple hops
4. To be part of a *network*:
 - *Route* through a network
 - *Manage resources*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

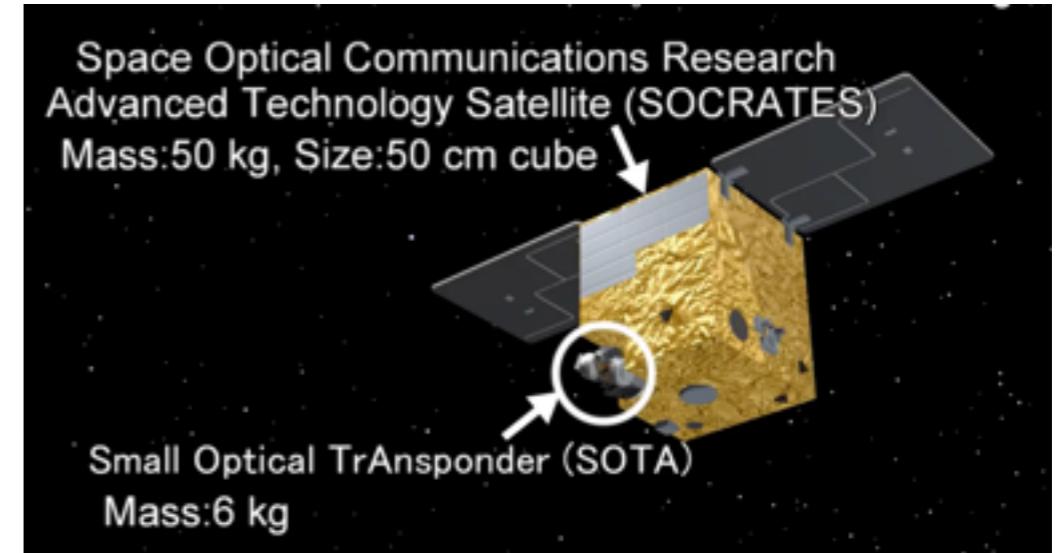
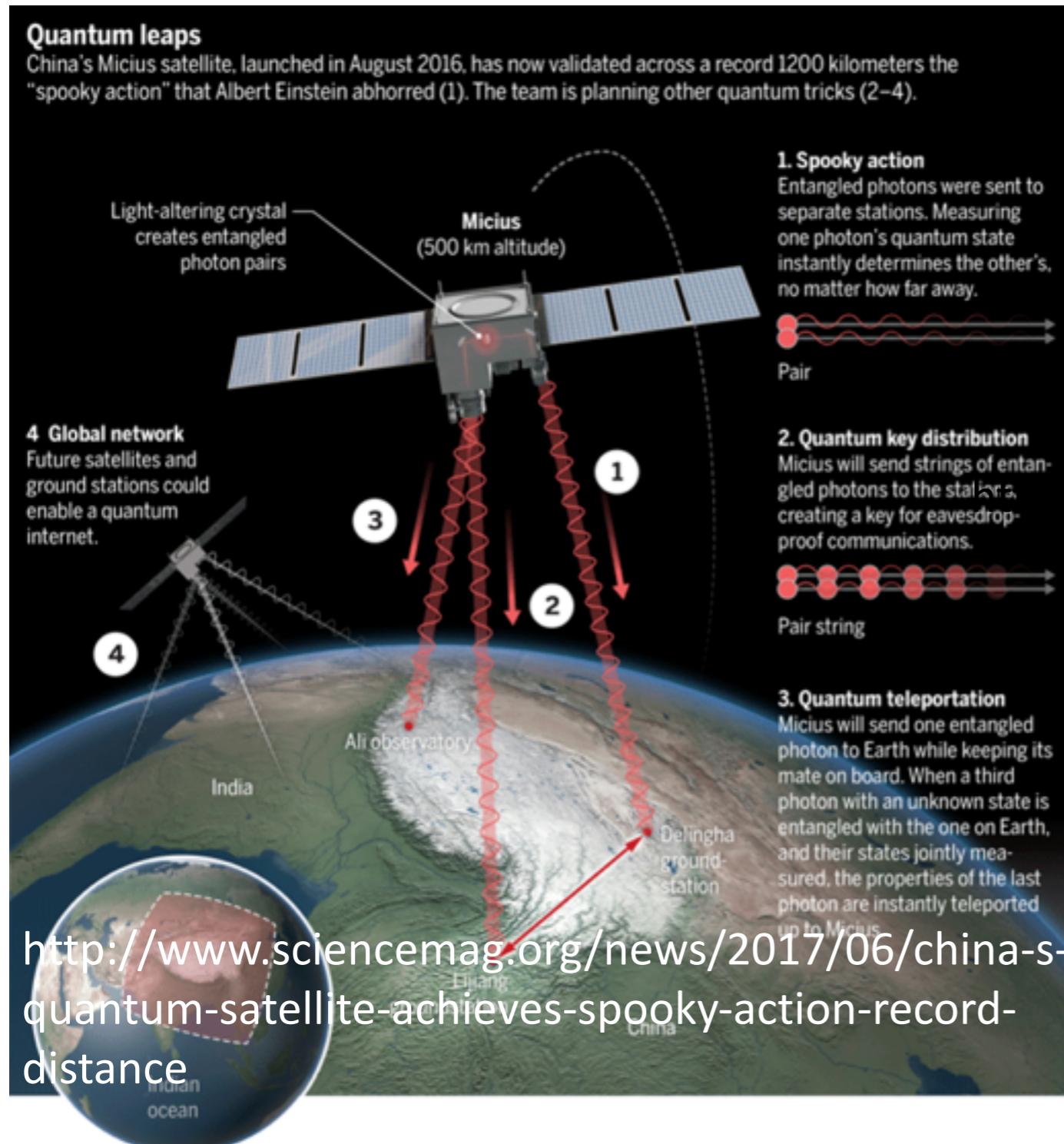


Delft experiment: 2 nodes



Hensen et al., Nature, 29 Oct. 2015

QKD & entanglement distribution via satellite



[://www.nict.go.jp/en/press/2017/07/11-1.html](http://www.nict.go.jp/en/press/2017/07/11-1.html)

Also experiments from Canada, Singapore and elsewhere

European Quantum Internet effort

The screenshot shows the homepage of the European Quantum Internet Alliance. At the top left is the QIA logo. Below it is a navigation bar with links: ABOUT, PARTNERS, TEAM, ADVISORY BOARD, RESOURCES, NEWS, and CONTACT. The main title "QUANTUM INTERNET ALLIANCE" is prominently displayed in large white letters against a dark blue background featuring a network of red and blue dots. Below the title is a subtitle: "The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth". At the bottom are two red buttons: "LEARN MORE" and "CONTACT".

<http://quantum-internet.team/>

IOPscience Journals Books Publishing Support Login Search IOPscience

Quantum Science and Technology

PERSPECTIVE

The European quantum technologies flagship programme

Max F Riedel¹, Daniele Binoi², Rob Thew³ and Tommaso Calarco¹

Published 23 June 2017 • © 2017 IOP Publishing Ltd

Quantum Science and Technology, Volume 2, Number 3

Focus on Quantum Cryptography and Quantum Networking



References Citations

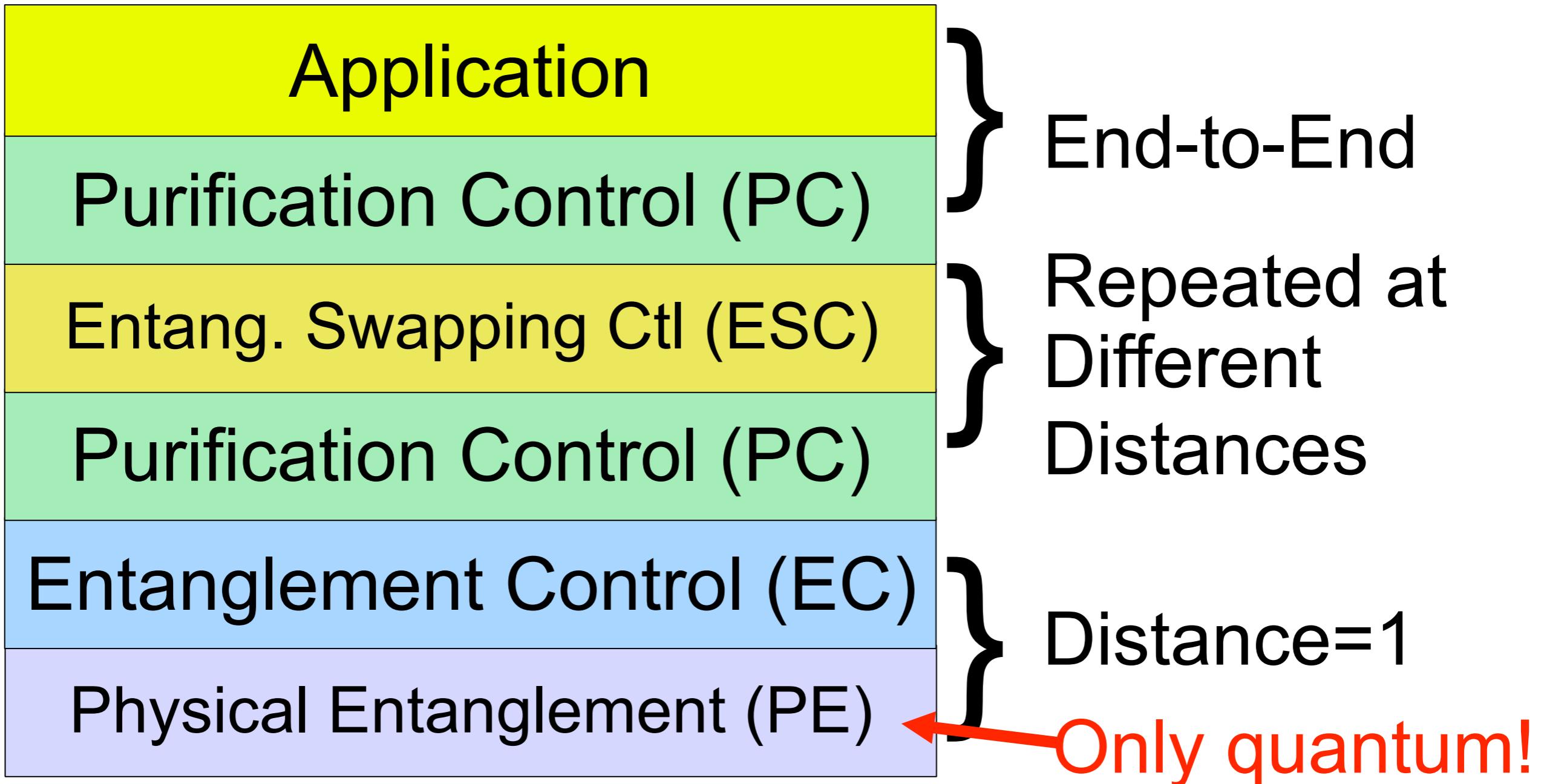
+ Article information

Abstract

Quantum technologies, such as quantum communication, computation, simulation as well as sensors and metrology, address and manipulate individual quantum states and make use of superposition and entanglement. Both companies and governments have realised the high disruptive potential of this technology. Consequently, the European Commission has announced an ambitious flagship programme to start in 2018. Here, we sum up the history leading to the quantum technologies flagship programme and outline its envisioned goals and structure. We also give an overview of the strategic research agenda for quantum communication, which the flagship will pursue during its 10-year runtime.

The European quantum technologies flagship programme

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>

The screenshot shows a web browser window with the URL <https://www.irtf.org/mailman/listinfo/qirg> in the address bar. The title bar reads "Qirg -- Quantum Internet (proposed) RG". The page content is as follows:

About Qirg

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?
- * interoperability: 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 Elkhoury 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.

Some QKD-oriented standardization efforts

The screenshot shows the ETSI website's navigation bar with links for Standards, Technologies & Clusters, Membership, News & Events, and Contact. Below the navigation is a search bar and a menu with Website, Standards, and a magnifying glass icon. The main content area is titled "Quantum Key Distribution" under the "Technologies & Clusters" section. It includes a sidebar with "Clusters" and "Technologies" sections, and a main content area with an introduction about the EC FP6-project SECOQC and a diagram showing four steps: Plan, Meet, Agree, and Publish.

The screenshot shows the IEEE Standards Association website's navigation bar with links for Find Standards, Develop Standards, Get Involved, News & Events, About Us, and Buy Standards. The main content area is titled "IEEE PROJECT" and "1913 - Software-Defined Quantum Communication". It includes a status box indicating "Active Project", a description of the purpose of the standard, and details about the Working Group, Sponsor, and Society involved.

ETSI effort on quantum key distribution (QKD)

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

IEEE P1913, Software-Defined Quantum Communication

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

2nd Workshop for Quantum Repeaters and Networks

2nd Workshop for Quantum Repeaters and Networks

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 for a fruitful weekend of talks and discussions. At this second workshop, we look forward to continuing these discussions, with a focus on recent progress, challenges and new possible directions emerging in our community. We invite researchers working on key enabling technologies and system integration, protocols for connecting repeaters across network links with novel 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, figure-of-merit technologies, and paths to scalability; please see the [Speakers & Program](#) page for details. There will also be time for poster presentations.

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



A large, diagonal, semi-transparent yellow banner runs across the top right of the page, containing the text "Next meeting 2019 in Japan (date & location TBD)".

WORKSHOP FOR QUANTUM REPEATERS AND NETWORKS

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

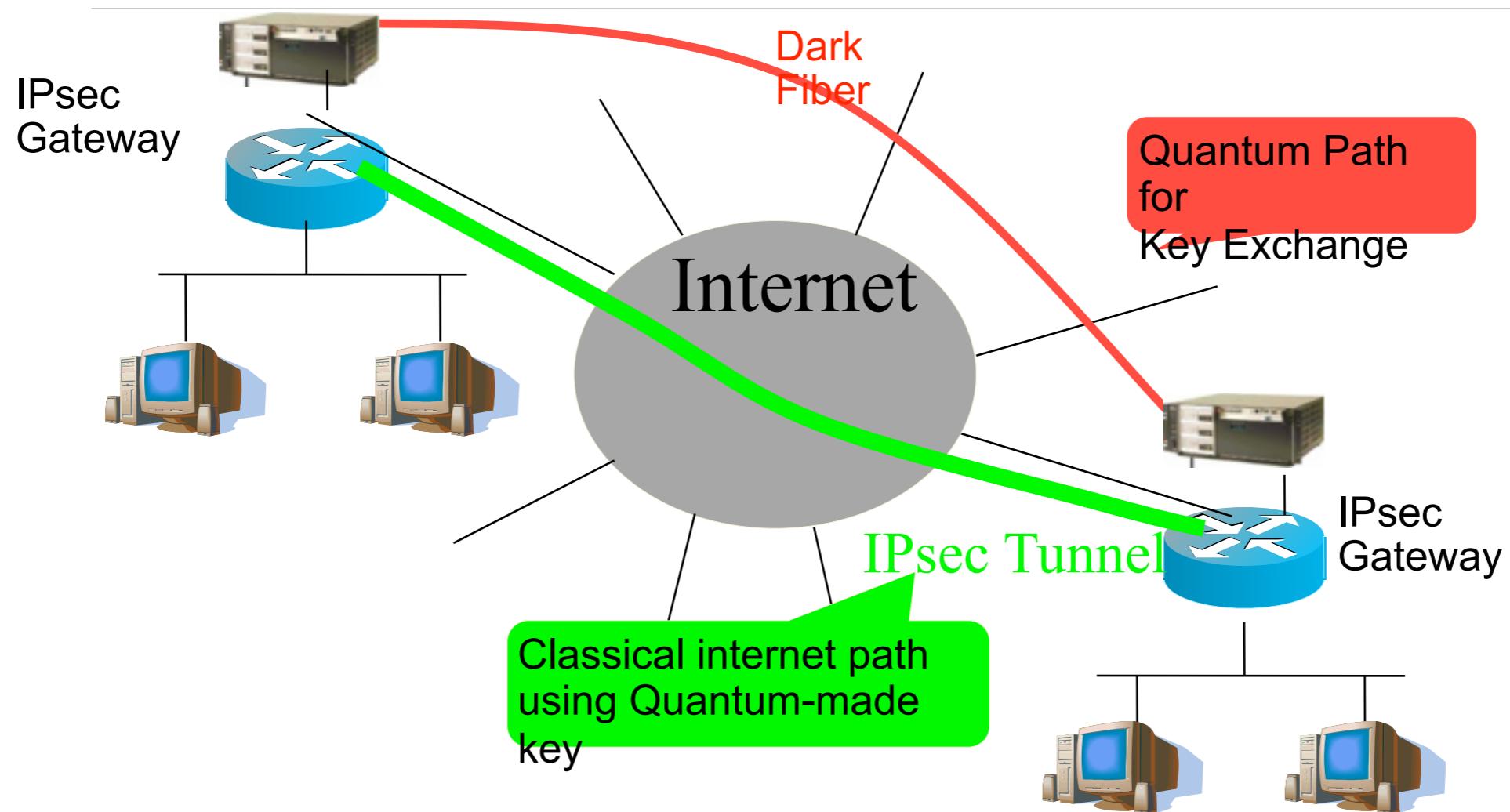
- Three major research groups announced important results in testing Bell's theorem in 2015.
- Pop science reports:
 - Delft group: <http://phys.org/news/2015-08-loopholes-entanglement-bell-inequality.html>
 - Vienna group: <http://phys.org/news/2015-11-big-quantum.html>
 - Singapore group: http://www.eurekalert.org/pub_releases/2015-11/cfqte-re110915.php
 - 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

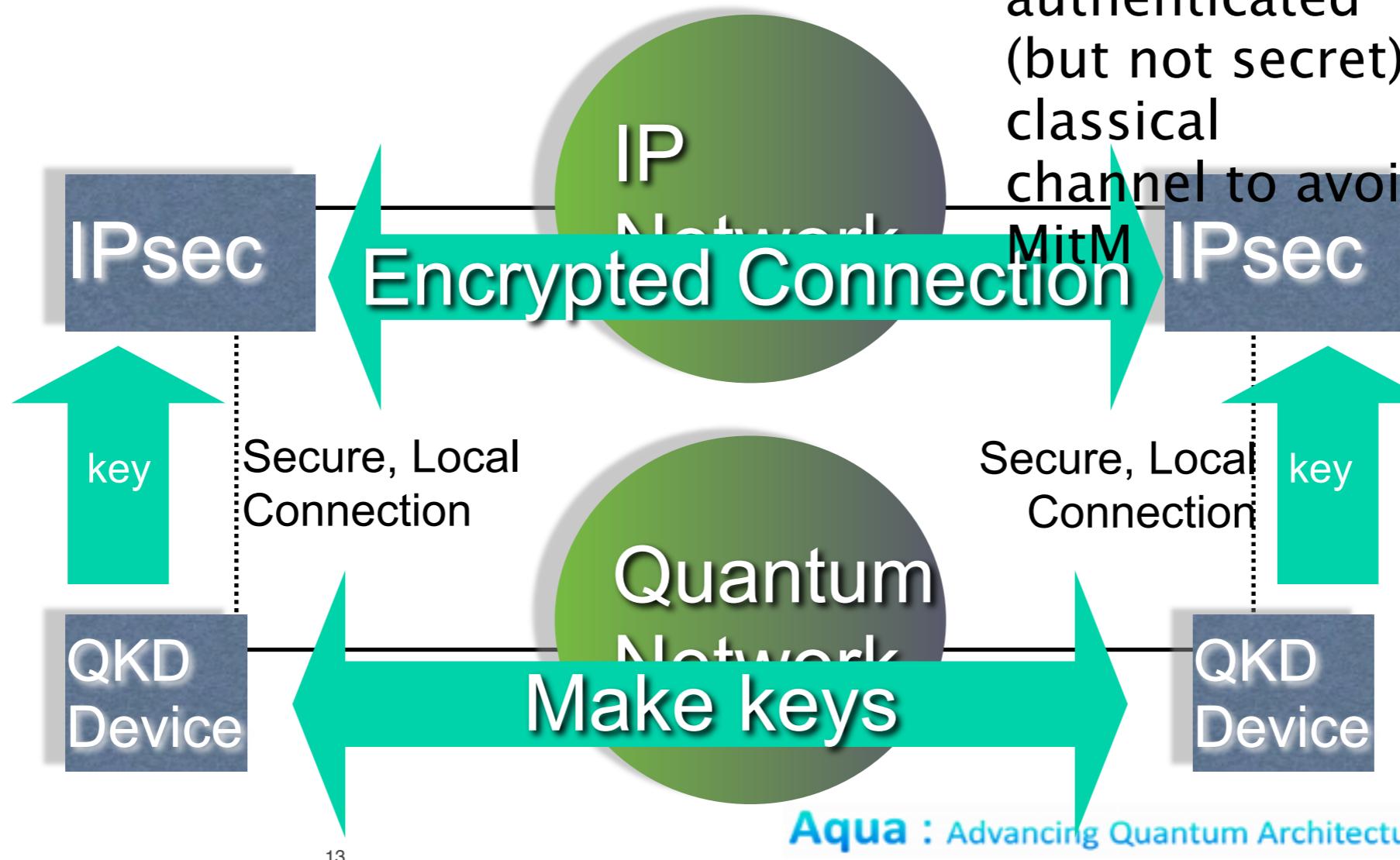


2014/10/gayama-ipsecme-ike-with-qkd-01.txt,

IPsec with QKD



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

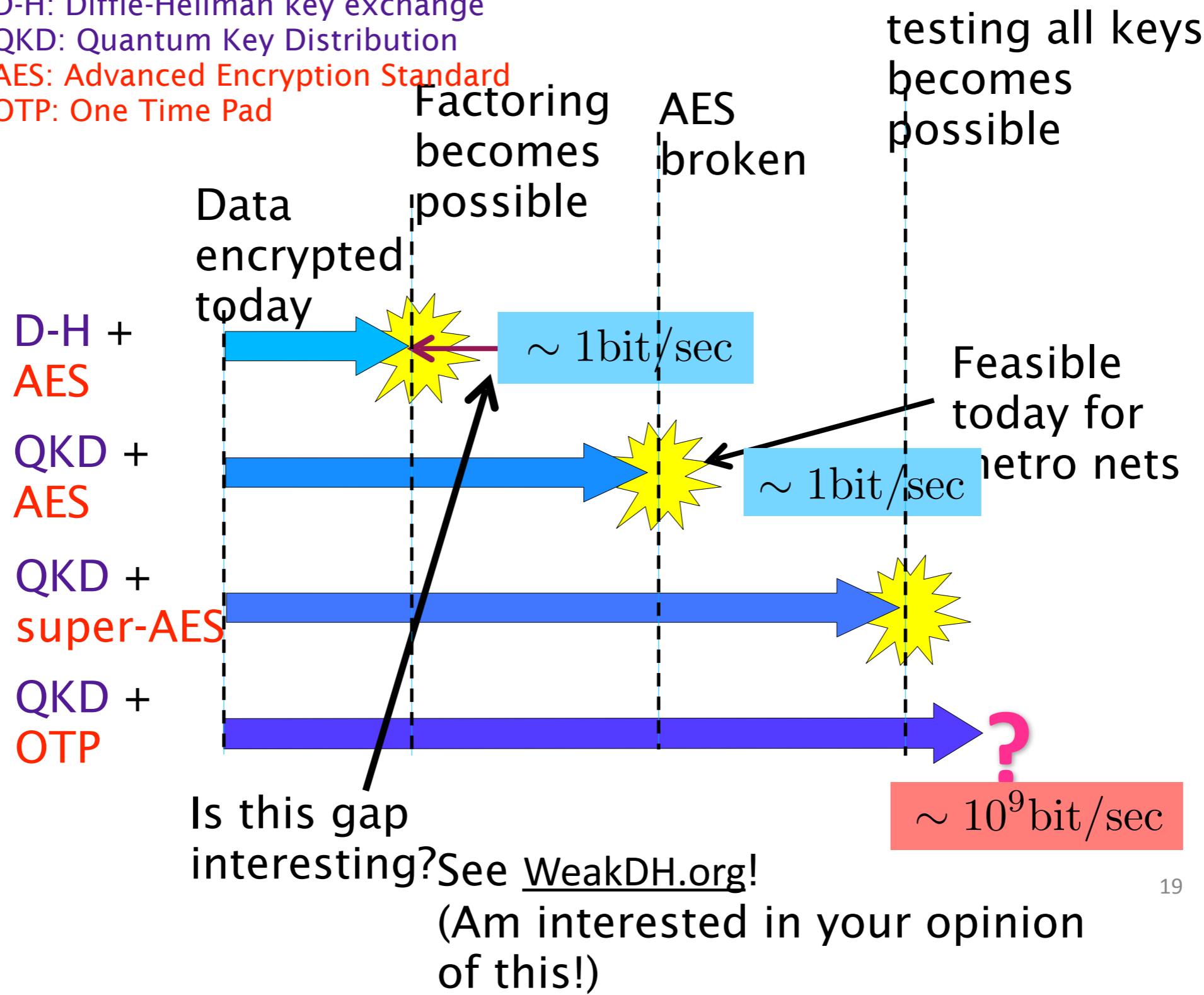


D-H: Diffie-Hellman key exchange

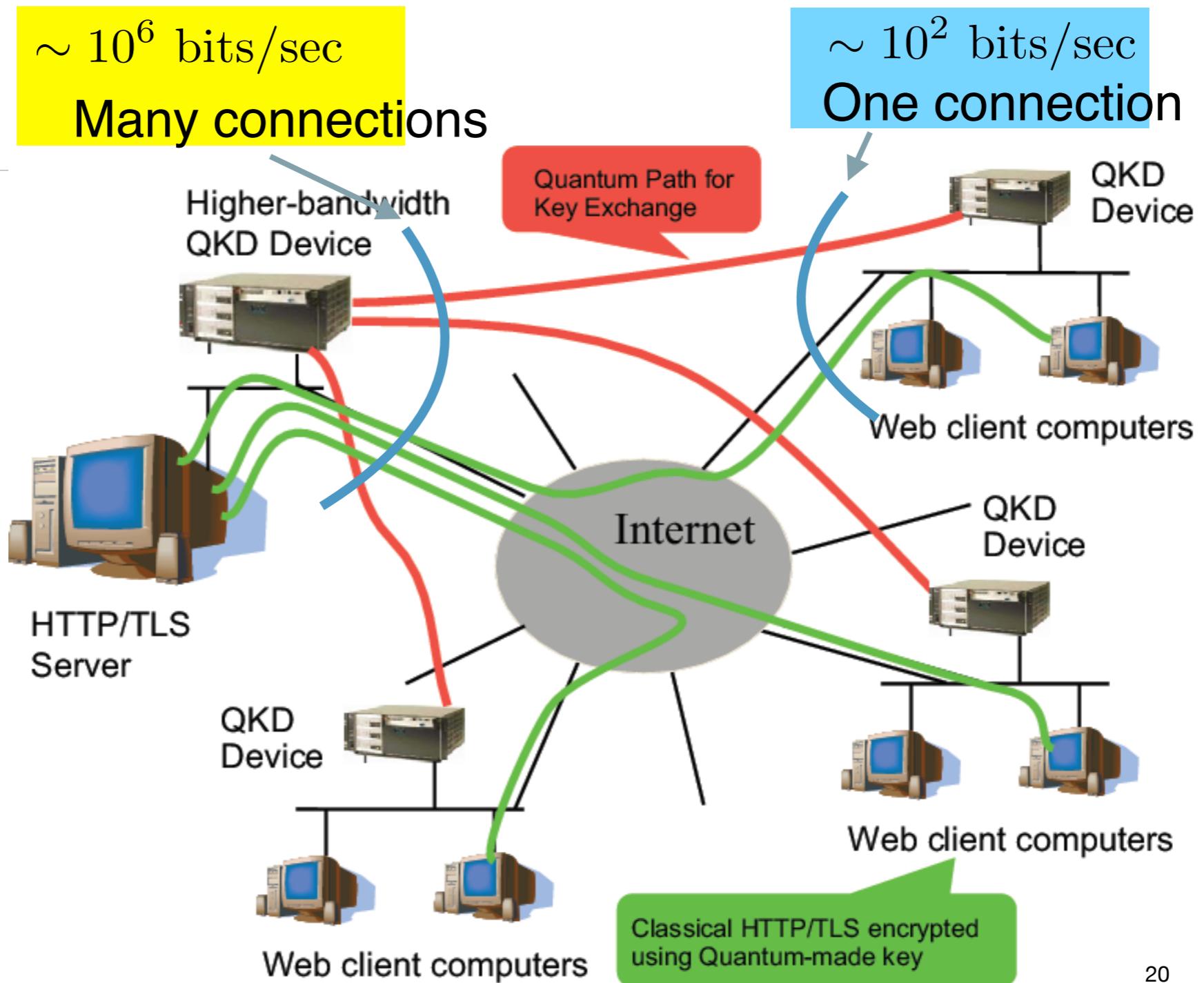
QKD: Quantum Key Distribution

AES: Advanced Encryption Standard

OTP: One Time Pad



TLS with QKD



Four-Hop Protocol Interactions

