ADVA™ Optical Networking

Quantum-safe data center interconnects

A practitioner’s guide

Jörg-Peter Elbers

OIDA Executive Forum 2019 – Panel 4: Commercial QKD & Encryption

Why do we care?

Data center A

Data center
interconnect (DCI)

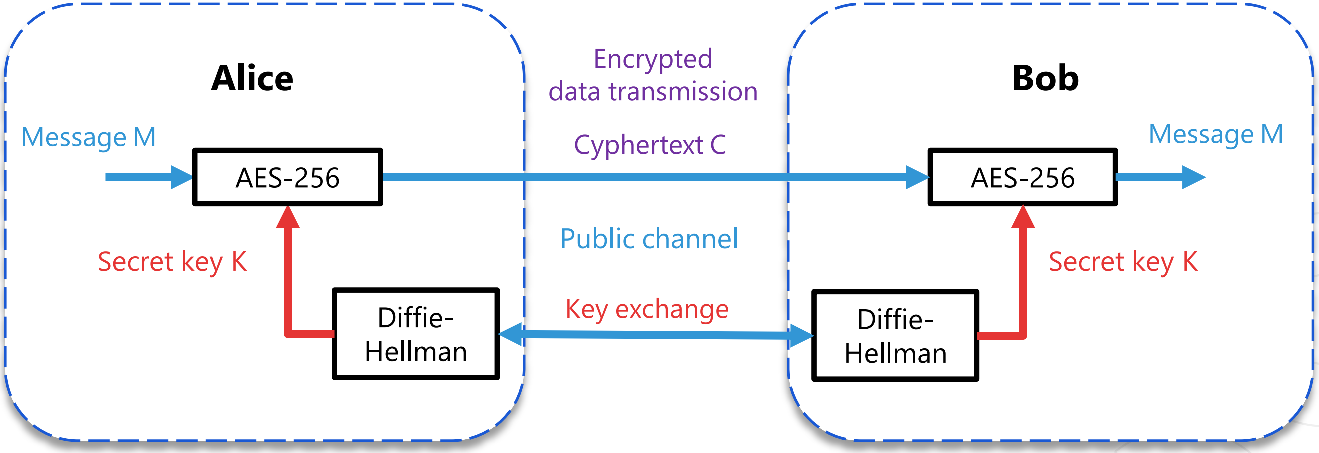
Fiber tapping devices

DWDM interception devices
10..100 Gb/s, direct detect & coherent

Data center B

Intercepting data center traffic is easy and can reveal a vast amount of critical data.

What can we do?



Alice

Message M

AES-256

Secret key K

Diffie-Hellman

Encrypted data transmission

Cyphertext C

Public channel

Key exchange

Bob

Message M

AES-256

Secret key K

Diffie-Hellman

On-the-fly encryption *secures* data communication over *insecure* channels.

What changes with quantum computers?

Data center A

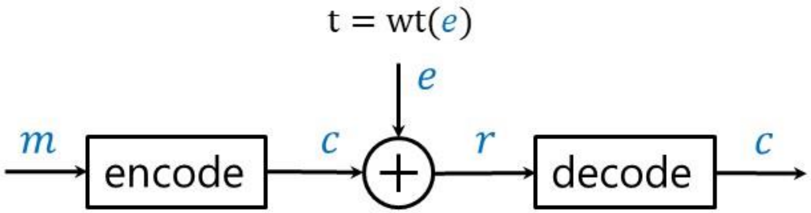
Adversary's recipe

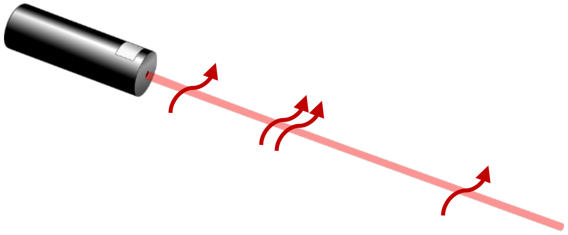
1. Intercept data communication
2. Store intercepted data
3. Use quantum computer to break key exchange protocol
4. Retrieve encryption keys
5. Decrypt data

Data center B

Quantum computers put secrecy of encrypted data communication at risk.

How can we make the key exchange quantum-safe?





Post-quantum cryptography (PQC)

- Provides computational security
- Is based on hardness of math problems
- Works on any communication channel
- Requires endpoint protocol access only
- Is independent of optical layer

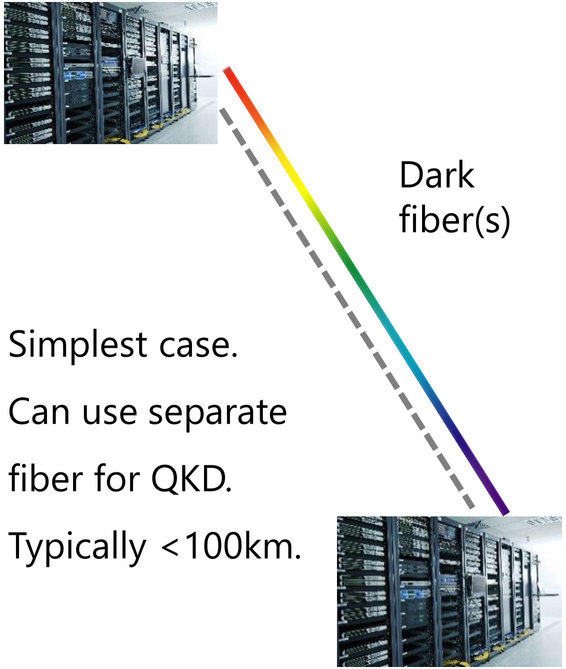
Quantum-key distribution (QKD)

- Provides information-theoretic security
- Is based on laws of quantum physics
- Needs optical fiber or free-space channel
- Requires access to physical infrastructure
- Depends on optical link performance

Note: Security is only as strong as the weakest link in the chain.

What are practical DCI deployment scenarios?

Metro DCI link

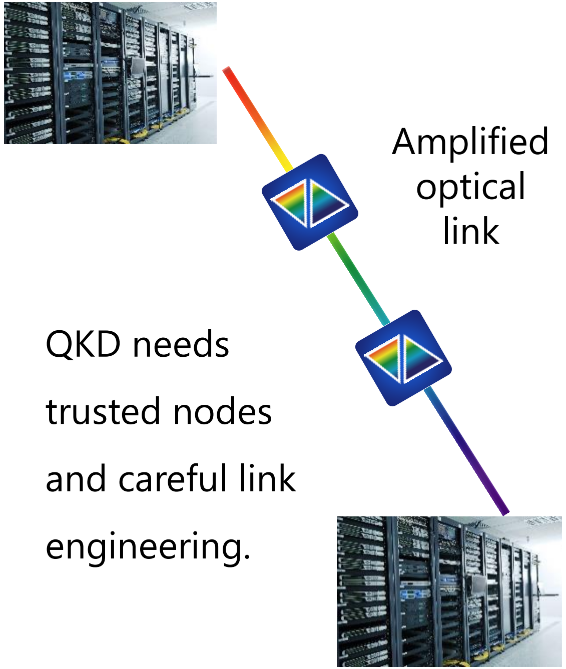


Simplest case.

Can use separate fiber for QKD.

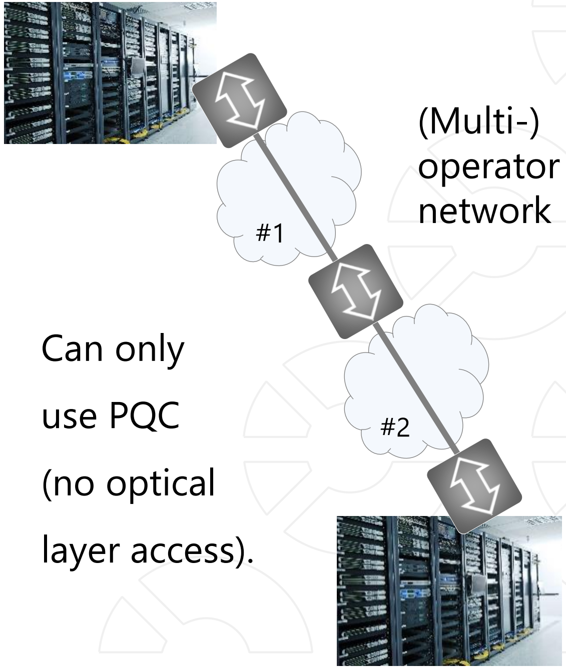
Typically <100km.

Long-haul DCI link



QKD needs trusted nodes and careful link engineering.

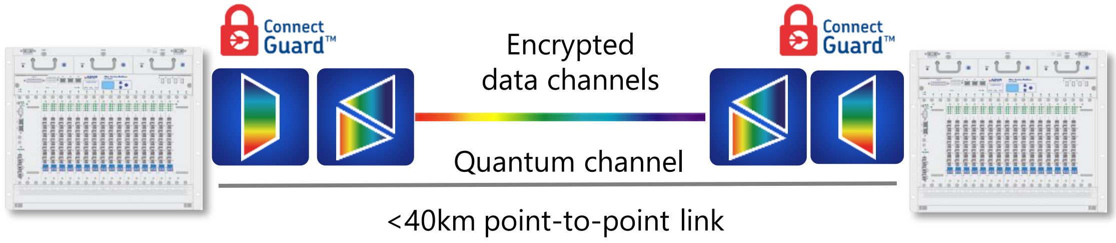
DCI via layer 1 VPN



Can only use PQC (no optical layer access).

Some quantum-safe deployment examples

Financial institution

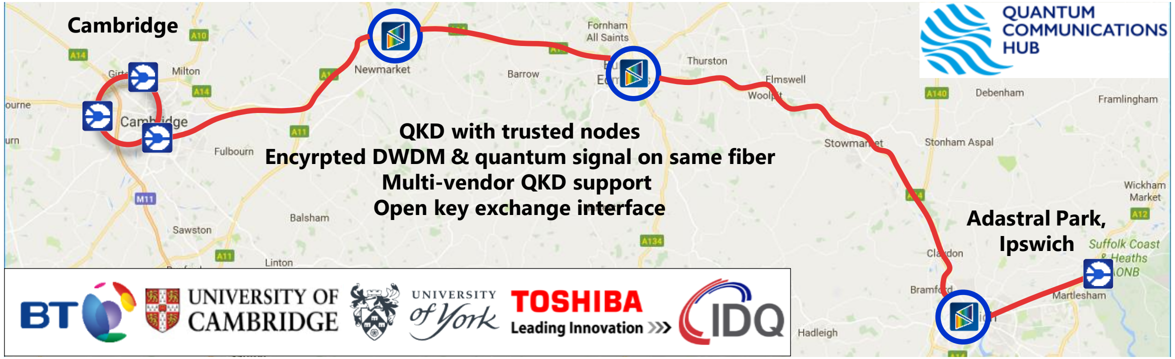


Encrypted data channels

Quantum channel

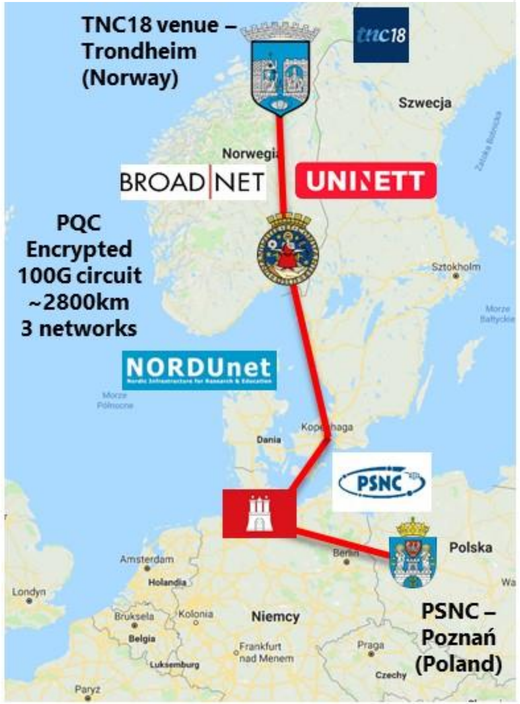
<40km point-to-point link

UK regional network



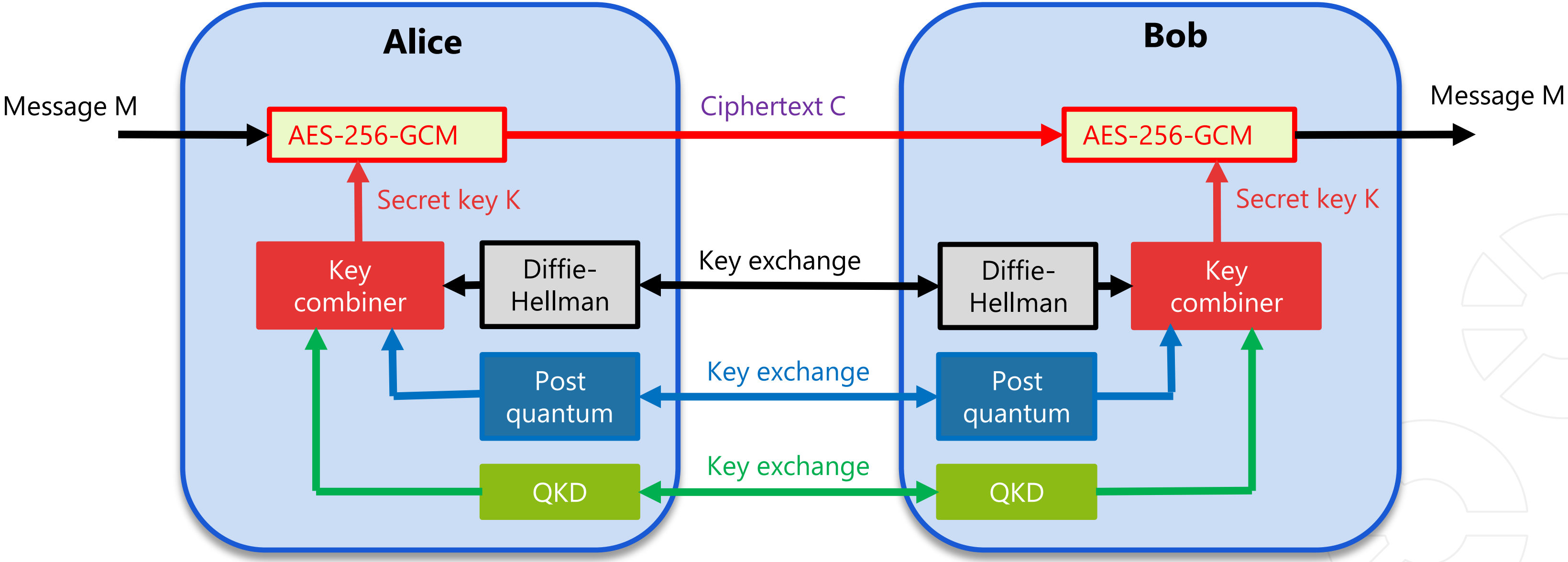
QKD with trusted nodes
Encyrpted DWDM & quantum signal on same fiber
Multi-vendor QKD support
Open key exchange interface

EU research network



PQC Encrypted 100G circuit ~2800km 3 networks

Do I need to decide for one key exchange scheme?



Key exchange schemes can be combined to provide robust quantum-safe solutions.

ADVA™
Optical Networking

Thank you

jelbers@advaoptical.com

IMPORTANT NOTICE

ADVA Optical Networking is the exclusive owner or licensee of the content, material, and information in this presentation.
Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.

The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA Optical Networking shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.