Building the Quantum Network Testbed in Eindhoven

SURF – Research on Optical Network

Chigo Okonkwo

Motivation

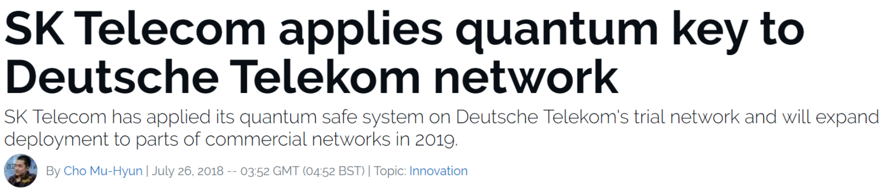
- Encryption is an essential part of an information centric society
- A layer of protection is required to shield confidential data from exposure to attacks (or from those the information is not intended for)
- Symmetric Cryptography: The most secure and widely employed for data transmission confidentiality and integrity.
- Challenges: How to securely share the keys between concerned parties, from Alice to Bob (without Eve receiving)

Motivation

- Current key distribution approaches include RSA, Diffie-Hellman and ECC which rely on symmetric key exchange
- Increasing plethora of increasing machine-to-machine and 5G device comms.
- Publicly exchanged of key ciphers are fundamentally mathematical calculations which are simple to compute
  - Vulnerable to weak random number generators
  - New attack strategies/vectors
  - Advances in Computational power (e.g. RSA-129 was broken with distributed computing)

- Major Scare Tactic Alert: Information transmitted today can be stored for decryption when quantum computers are mature.

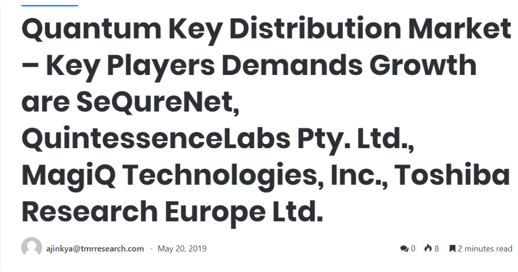
Explosion of QKD testbed activity



SK Telecom applies quantum key to Deutsche Telekom network

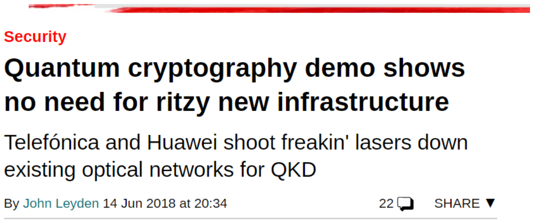
SK Telecom has applied its quantum safe system on Deutsche Telekom's trial network and will expand deployment to parts of commercial networks in 2019.

By Cho Mu-Hyun | July 26, 2018 -- 03:52 GMT (04:52 BST) | Topic: Innovation



Quantum Key Distribution Market – Key Players Demands Growth are SeQureNet, QuintessenceLabs Pty. Ltd., MagiQ Technologies, Inc., Toshiba Research Europe Ltd.

ajinkya@tmrresearch.com · May 20, 2019 0 8 2 minutes read

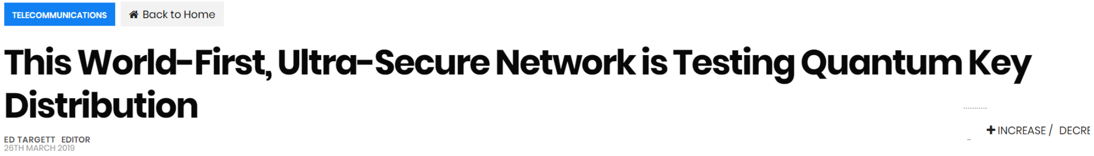


Security

Quantum cryptography demo shows no need for ritzy new infrastructure

Telefónica and Huawei shoot freakin' lasers down existing optical networks for QKD

By John Leyden 14 Jun 2018 at 20:34 22 SHARE ▼

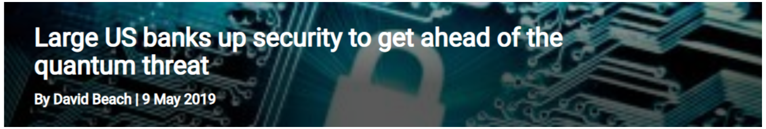


TELECOMMUNICATIONS Back to Home

This World-First, Ultra-Secure Network is Testing Quantum Key Distribution

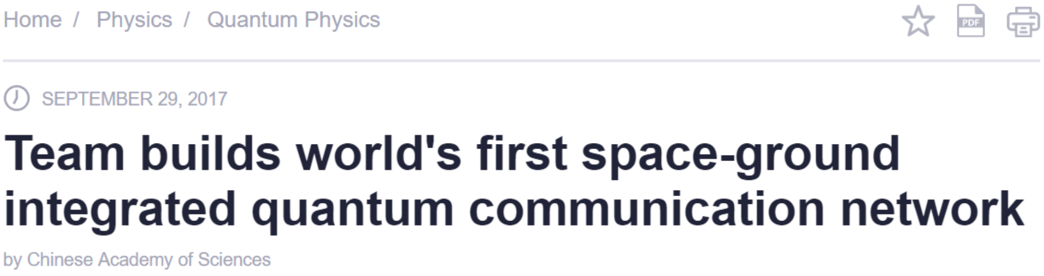
ED TARGETT EDITOR
26TH MARCH 2019

+INCREASE / DECRE



Large US banks up security to get ahead of the quantum threat

By David Beach | 9 May 2019



Home / Physics / Quantum Physics

SEPTEMBER 29, 2017

Team builds world's first space-ground integrated quantum communication network

by Chinese Academy of Sciences

Motivation for QKD testbed

- QKD works only when there is no difference between theoretical devices and their practical implementation e.g. single photon sources/detectors
  - Measurement device independent (MDI-QKD) and decoy-state QKD

- Validation of long established Security Proofs

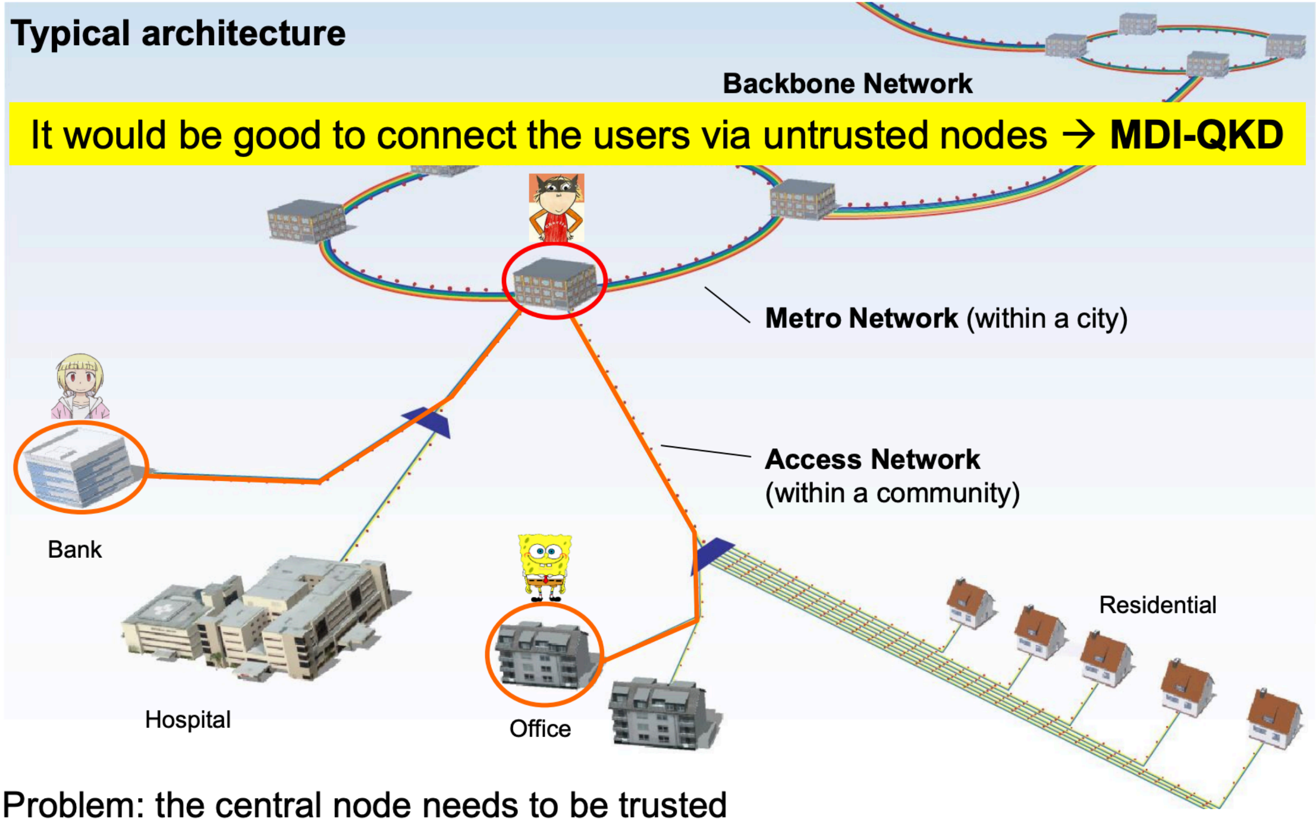
- QKD is limited to short transmission distances and optical networks span trans-oceanic and over continental terrestrial networks
  - Long distance -> decoherence and high channel losses (current records are 500km)
  - Key rates -> after 1000km drops to 0.3 photons per 100 years!
  - Quantum repeaters are being developed in the long-term but trusted relays can be employed

- Push towards deployment of multi-vendor Quantum security in the field

- Development and testing of Photonic Integrated transmitters and receivers (e.g. integrated single photon sources and detectors)

- Verification of QKD protocols

Long distance QKD



It would be good to connect the users via untrusted nodes → **MDI-QKD**

Problem: the central node needs to be trusted

Source: TREL 2018

Current experimental QKD Networks and Activity

Austria: SECOQC in Vienna

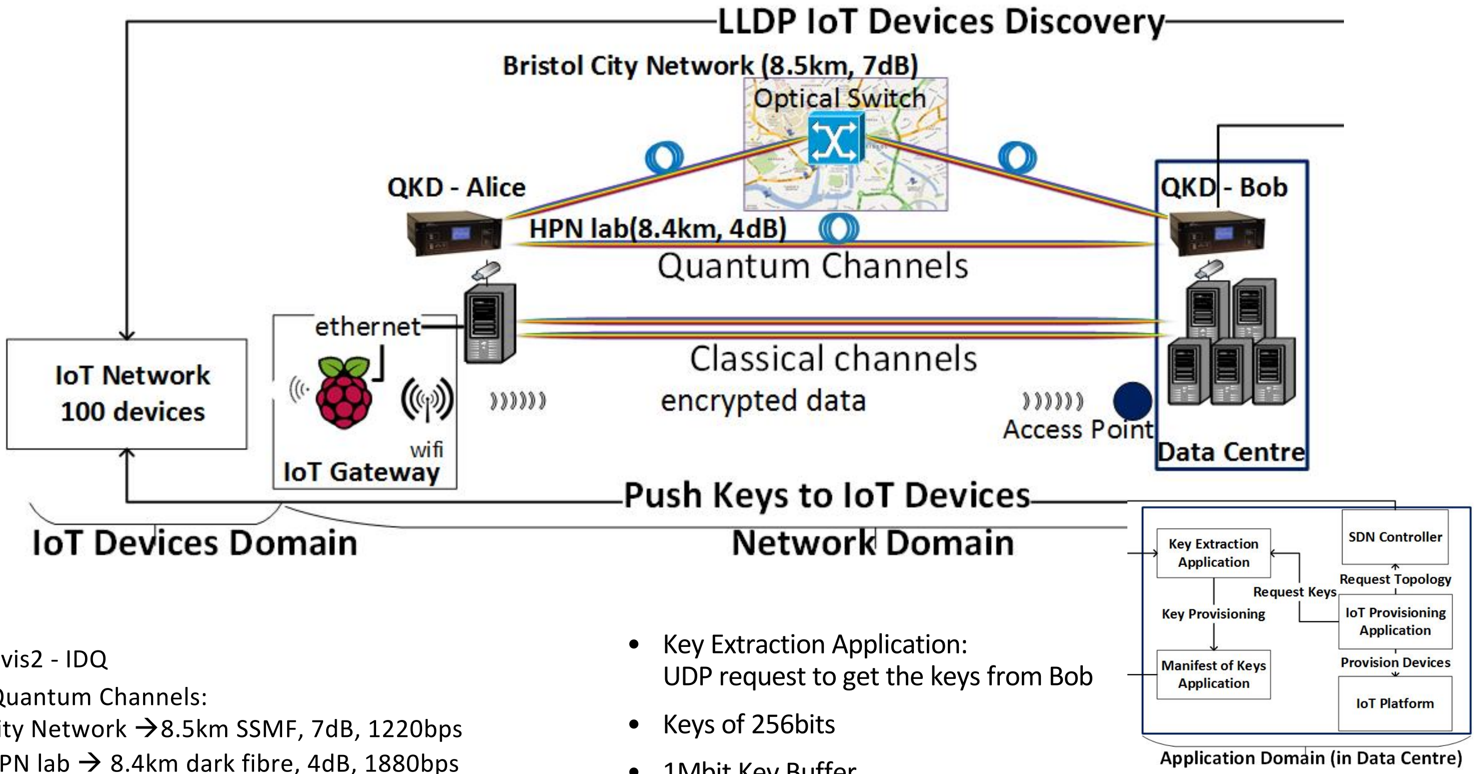
United Kingdom: University of Bristol, Toshiba, ADVA, BT

China: Bejing to Shanghai Backbone QKD Networks

South Korea: KREONET, recently SK Telecom/IDQuantique

Japan: Tokyo QKD Network (NICT, Mitsubishi, Toshiba etc)

United Kingdom: Bristol Quantum Testbed - IOT

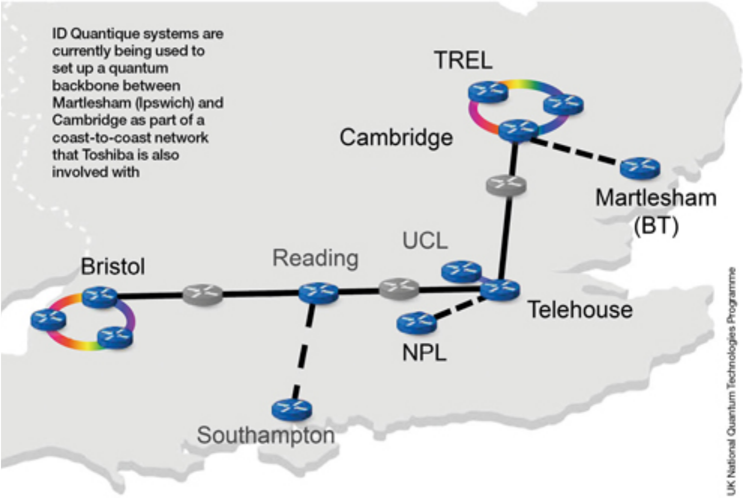


- Clavis2 - IDQ
- 2 Quantum Channels:
  - City Network →8.5km SSMF, 7dB, 1220bps
  - HPN lab → 8.4km dark fibre, 4dB, 1880bps

- Key Extraction Application:
  UDP request to get the keys from Bob
- Keys of 256bits
- 1Mbit Key Buffer

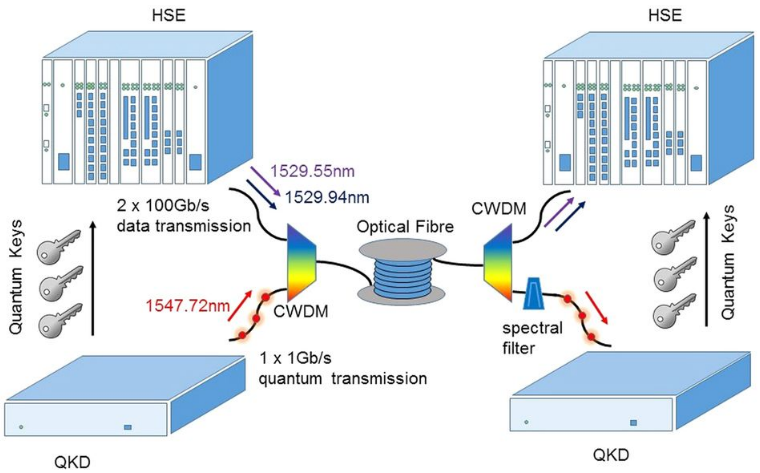
Source: University of Bristol

United Kingdom: UK Quantum Network (UKQNtel)



ID Quantique systems are currently being used to set up a quantum backbone between Martlesham (Ipswich) and Cambridge as part of a coast-to-coast network that Toshiba is also involved with

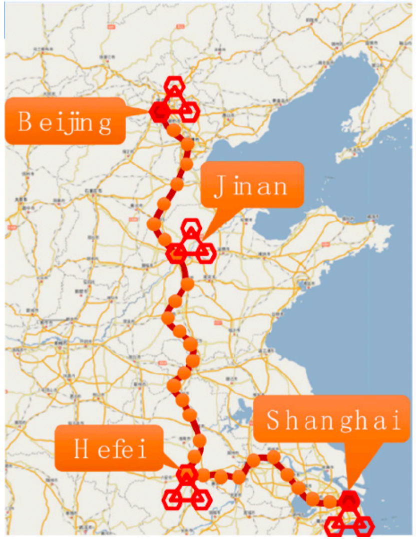
UK National Quantum Technologies Programme



125km using trusted nodes (BT research nodes)
Collaboration between TREL, University of Cambridge, UCL, ADVA and IDQuantique within the £120M Quantum Hub initiative
Modified BB-84 protocol – T12

Source: Toshiba and BT

China: QKD backbone



7600km
2500km

World’s longest quantum secure backbone network (2000km)
32 nodes in total, the backbone connects 4 Metropolitan areas with connection to 8-10 nodes each, different Topologies and QKD protocols
Satellite based QKD exploiting low attenuation and faster propagation in air and in vacuum achieving >1200km with key rates 1kbps

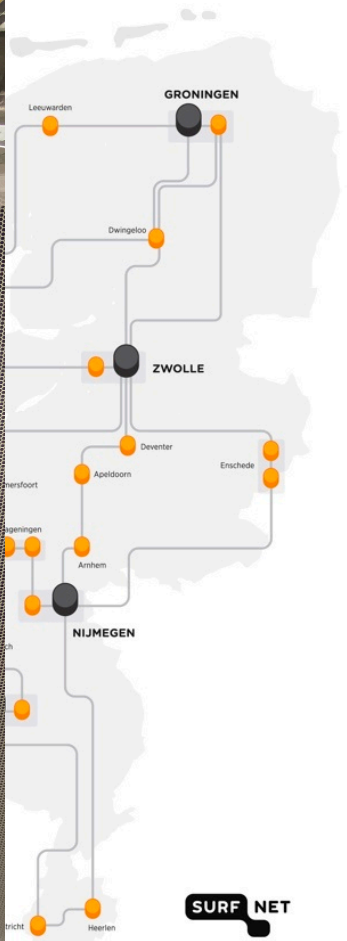
Source: Optics Express
Vol. 26, No. 18 | 3 Sep 2018

Dutch Quantum Technology Ecosystem

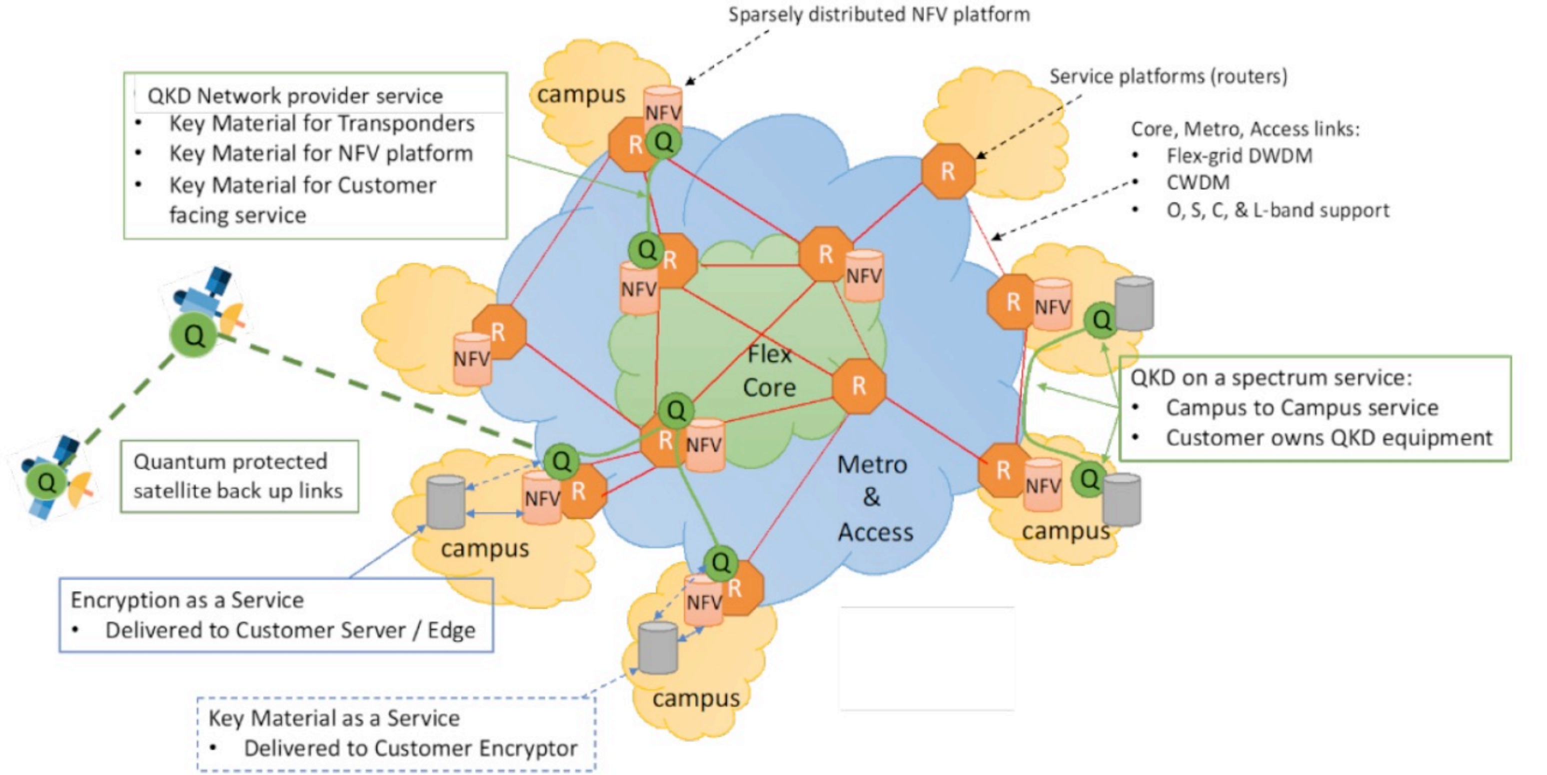
QuSoft – Quantum simulators and software
QuTech – Quantum Technologies
QT/e Eindhoven –Security Proofs, Integrated Quantum Sources, Optical Systems, Development of Attack Vectors, Post Quantum techniques
Microsoft – Quantum Computing
Twente – Quantum Secure Authentication
SURFNet – QKD as a service

SURFNET – Du Provider

- 100 Optical Node
- 100Gbit/s Optical
- Interconnecting r
- Interconnecting R



Vision: QKD as a service



Sparsely distributed NFV platform

Service platforms (routers)

Core, Metro, Access links:
- Flex-grid DWDM
- CWDM
- O, S, C, & L-band support

QKD Network provider service
- Key Material for Transponders
- Key Material for NFV platform
- Key Material for Customer facing service

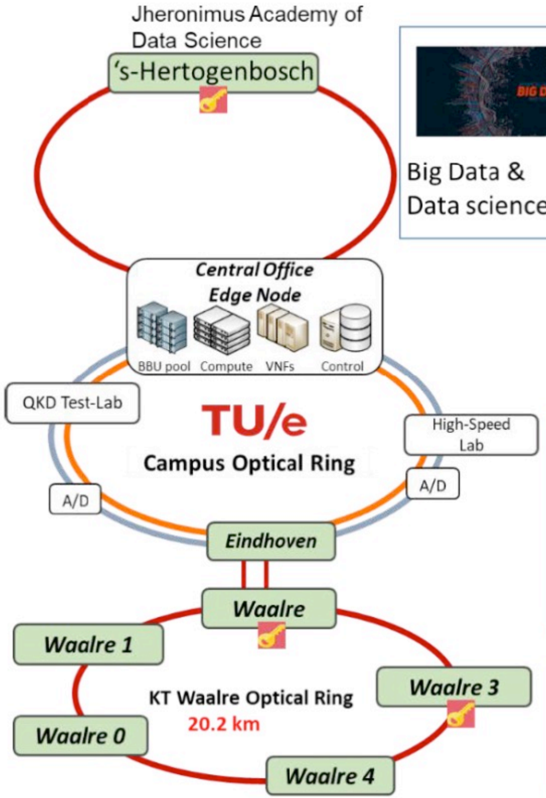
QKD on a spectrum service:
- Campus to Campus service
- Customer owns QKD equipment

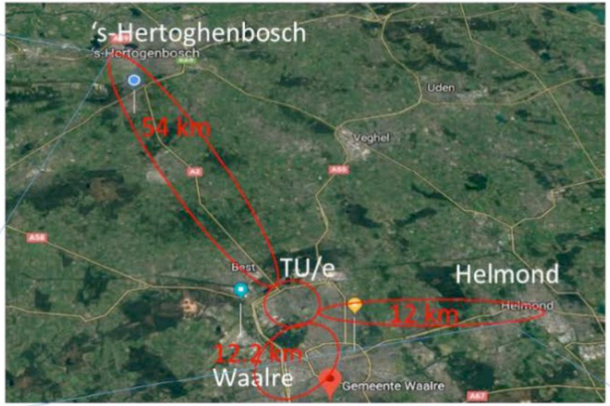
Quantum protected satellite back up links

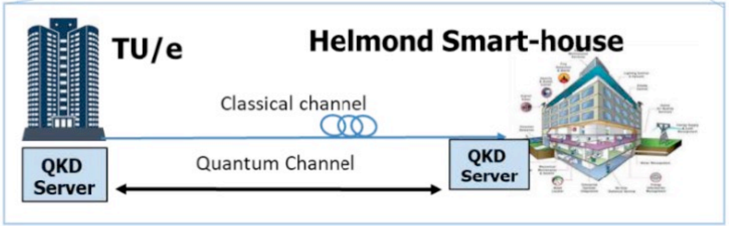
Encryption as a Service
- Delivered to Customer Server / Edge

Key Material as a Service
- Delivered to Customer Encryptor

Eindhoven – eQKDNet

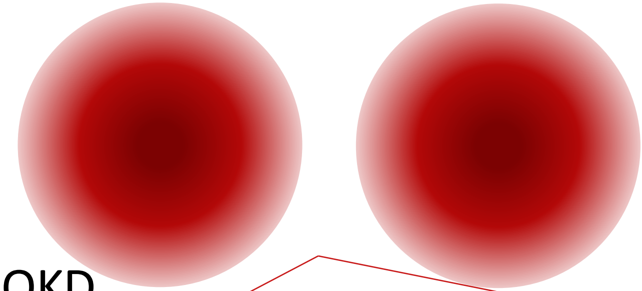






Continuous Variable Quantum Key Distribution

Continuous Variable States



Discrete Variable States

CV-QKD

Pros

☺ Can be implemented with conventional coherent communication hardware.

☺Can use integration techniques used for conventional coherent communication.

☺WDM compatibility.

- ☺ Spectral filtering with local oscillator

CV-QKD

Cons

☹ Security proofs less mature compared to DV-QKD.

☹ Reconciliation process complex.

- ☹ Especially forward error correction.

☹ Currently, transmission reach not as good as DV-QKD (in dedicated fibers).

TU/e

Multiplexing Techniques

Wavelength Division Multiplexing.
Most straightforward and can (to some extent) use the exist network architecture.
Problem: ASE noise and nonlinear noise (more on this in the following slides!)

Mode multiplexing in few- or mulitmode-fibers [1].

Spatial multiplexing in multicore fibers [2].

Time division multiplexing.

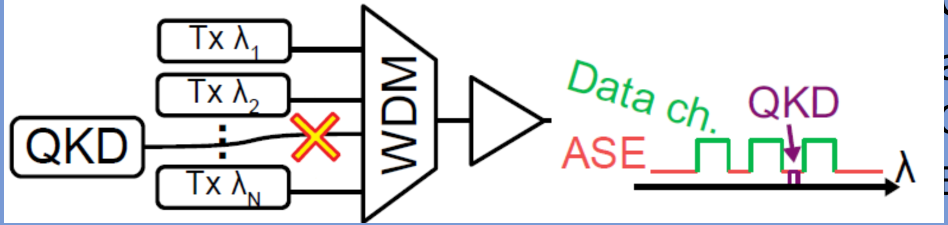
Simultaneous transmission of classical and CV-QKD states. (Displaced by the modulation) [3].

[1] J. Carpenter et al., “Mode multiplexed single-photon and classical channels in a few-mode fiber, Optics Express, vol. 21, no. 23, pp. 28794–28800, 2013.

[2] T. A. Eriksson et al. “Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission." IEEE Photonics Technology Letters 31.6 (2019): 467-470.

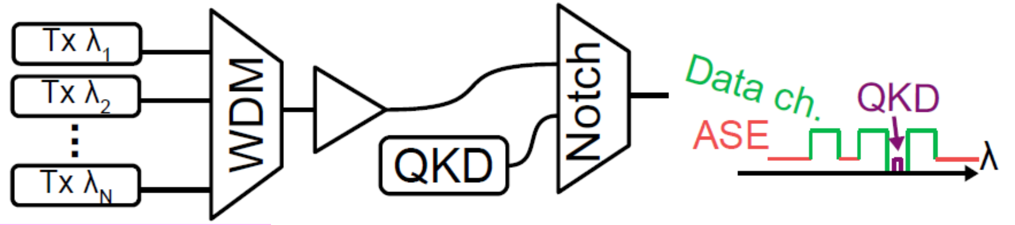
[2] R. Kumar, et al. "Experimental demonstration of single-shot quantum and classical signal transmission on single wavelength optical pulse." *Scientific reports* 9.1 (2019): 11190.

Multiplexing with Coherent WDM Channels



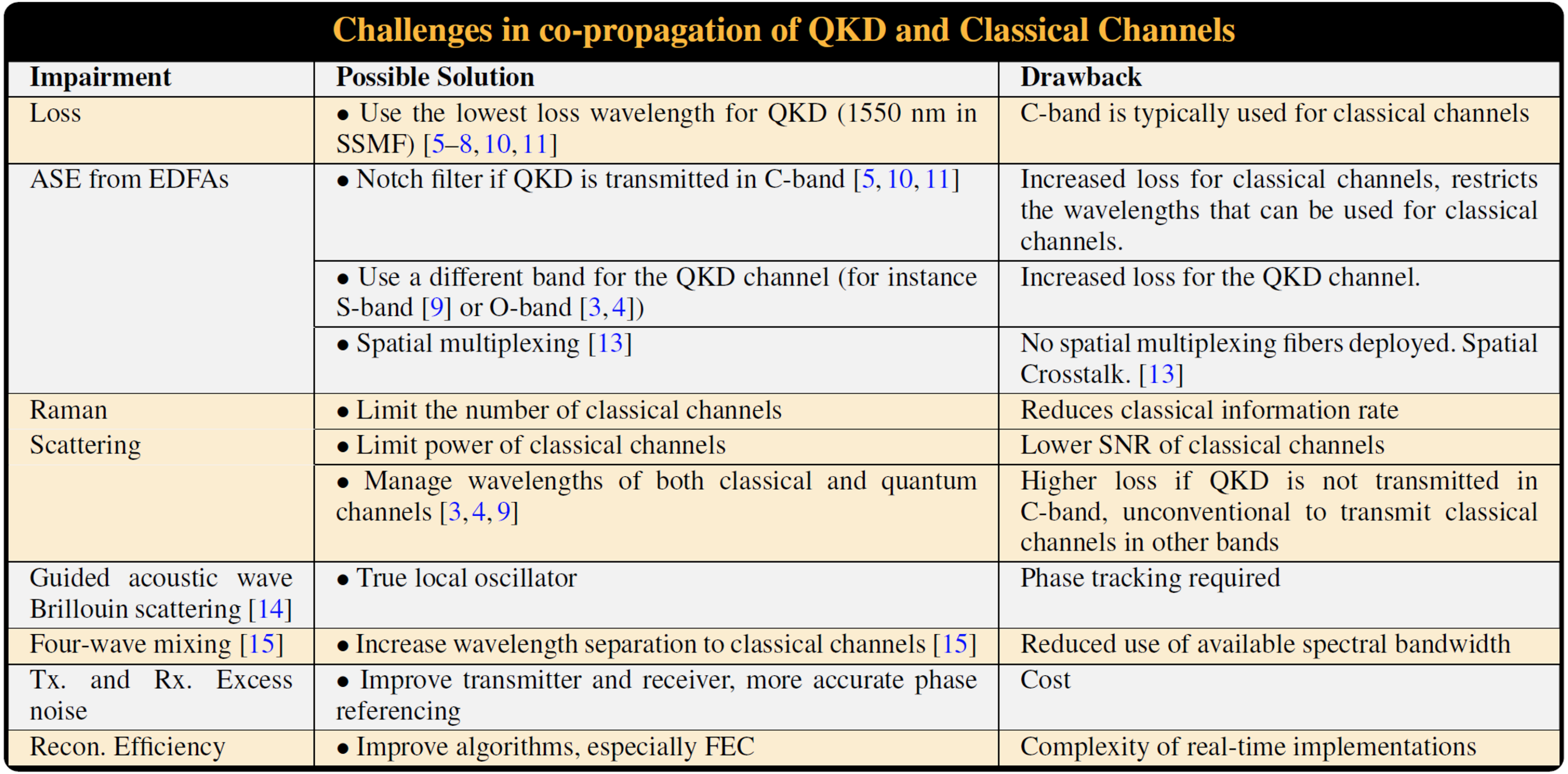
Conventional WDM systems use EDFAs after multiplexing.

QKD cannot use a port of the multiplexer since the EDFA destroys the quantum state.



- For multiplexing, a second stage is needed that removes ASE noise from the EDFA.
  - Will affect the architecture of the classical channels.

Challenges to deploying QKD



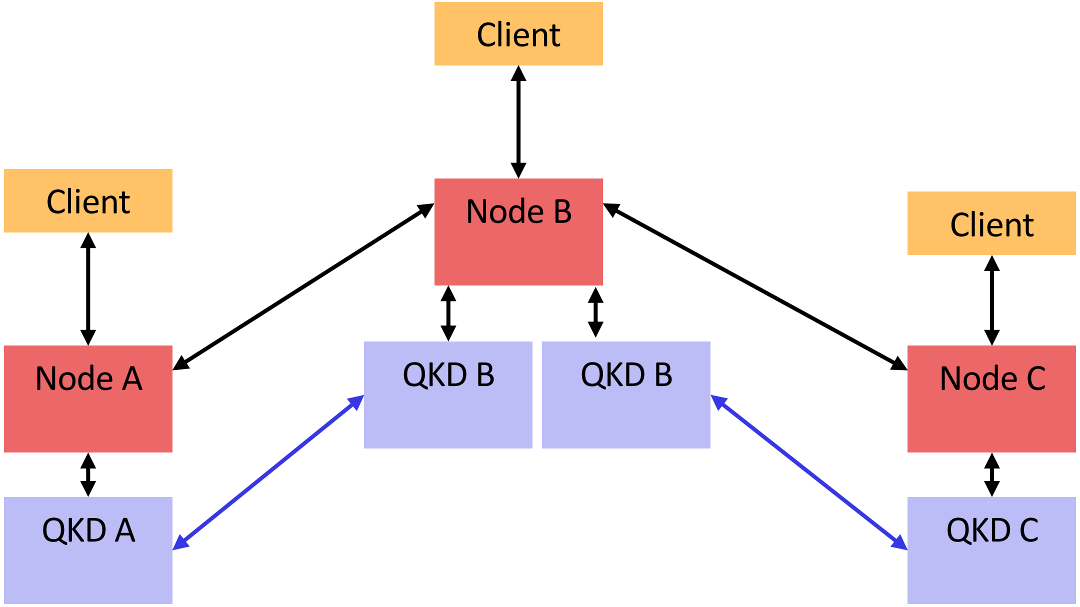
Challenges in co-propagation of QKD and Classical Channels

Impairment	Possible Solution	Drawback
Loss	• Use the lowest loss wavelength for QKD (1550 nm in SSMF) [5–8, 10, 11]	C-band is typically used for classical channels
ASE from EDFAs	• Notch filter if QKD is transmitted in C-band [5, 10, 11]	Increased loss for classical channels, restricts the wavelengths that can be used for classical channels.
	• Use a different band for the QKD channel (for instance S-band [9] or O-band [3, 4])	Increased loss for the QKD channel.
	• Spatial multiplexing [13]	No spatial multiplexing fibers deployed. Spatial Crosstalk. [13]
Raman Scattering	• Limit the number of classical channels	Reduces classical information rate
	• Limit power of classical channels	Lower SNR of classical channels
	• Manage wavelengths of both classical and quantum channels [3, 4, 9]	Higher loss if QKD is not transmitted in C-band, unconventional to transmit classical channels in other bands
Guided acoustic wave Brillouin scattering [14]	• True local oscillator	Phase tracking required
Four-wave mixing [15]	• Increase wavelength separation to classical channels [15]	Reduced use of available spectral bandwidth
Tx. and Rx. Excess noise	• Improve transmitter and receiver, more accurate phase referencing	Cost
Recon. Efficiency	• Improve algorithms, especially FEC	Complexity of real-time implementations

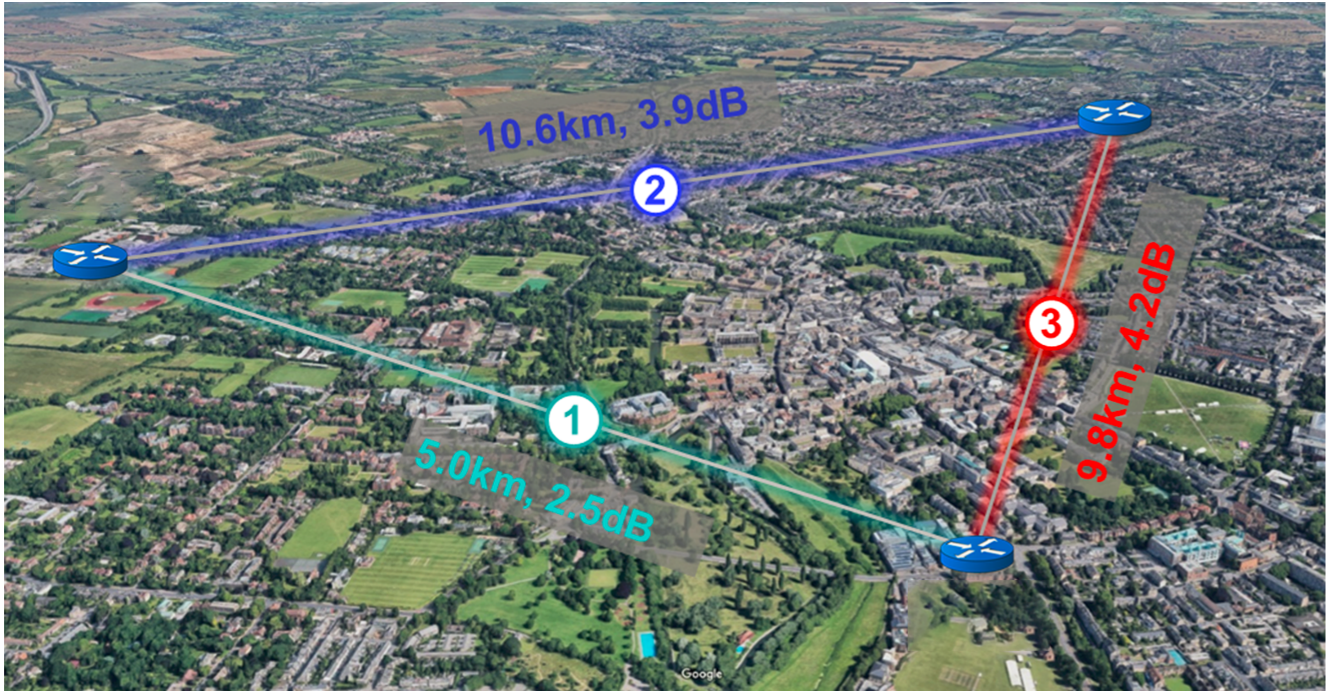
Networking Layer

- Point-to-point -> network
- Client interface

Networking software ->

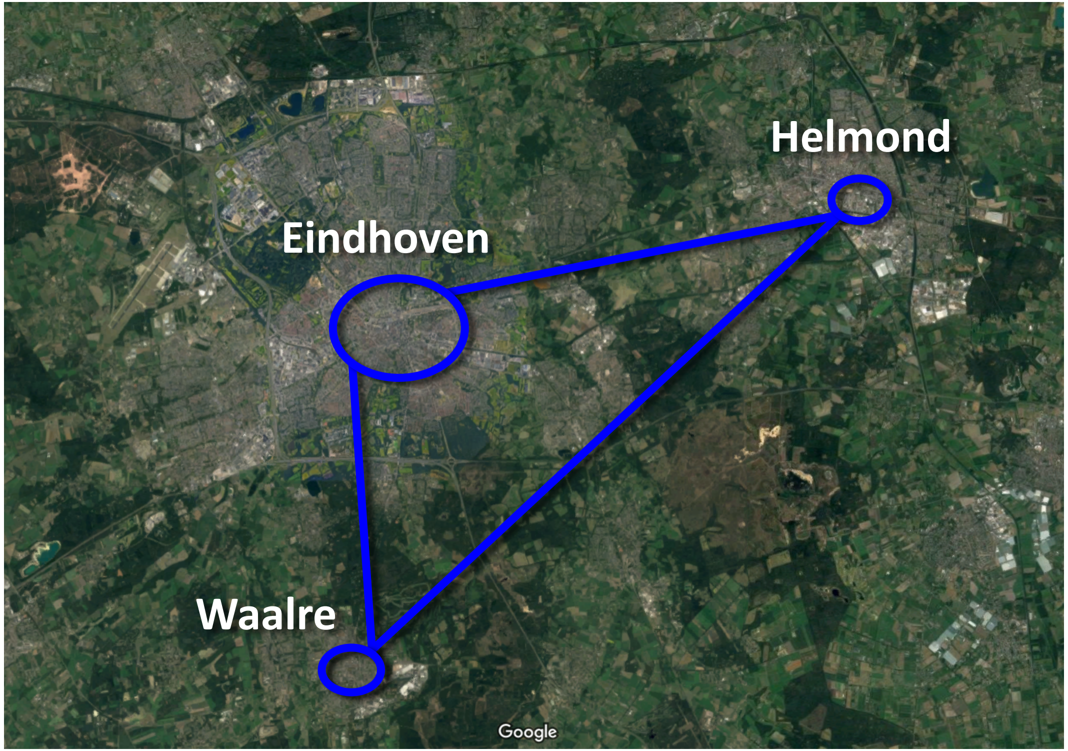


Cambridge Quantum Network



Dynes, J.F., Wonfor, A., Tam, W.W.S. *et al.* Cambridge quantum network

Eindhoven QKD Network Testbed



T. R. Raddo *et al.* "Quantum Data Encryption as a Service on Demand: Eindhoven QKD Network Testbed"

New networking software

Motivation for new networking software

Toshiba & ID-Quantique

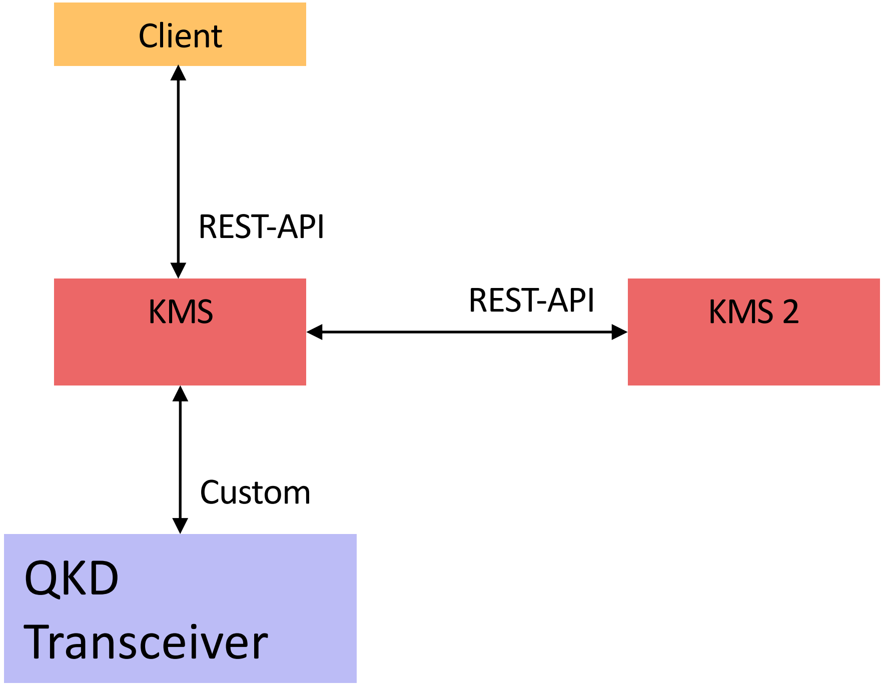
- Costly
- Closed source
- Incompatible

New software

- Open source
- Modular
- Customized testing

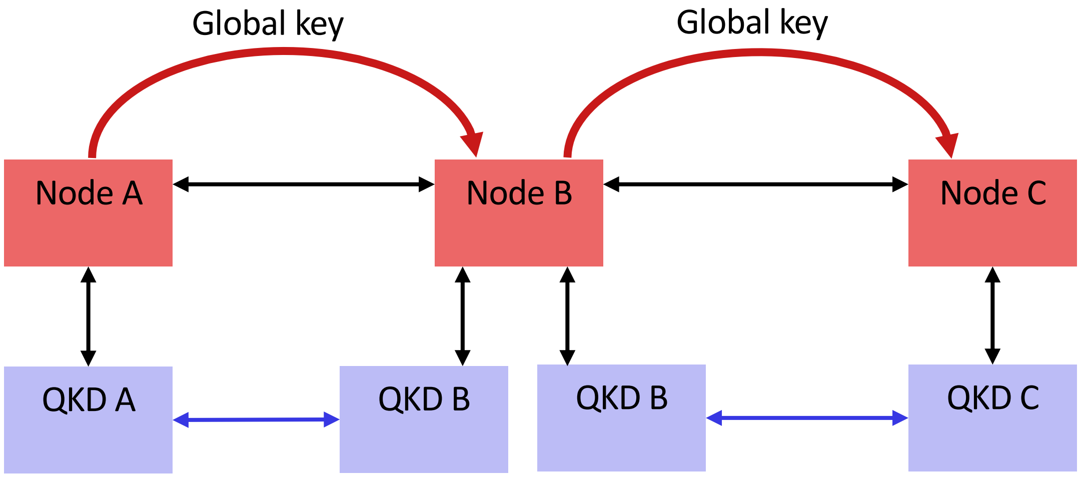
Networking layer implementation

- Python
- Flask
  - REST-API
- Easily modifiable
- modular

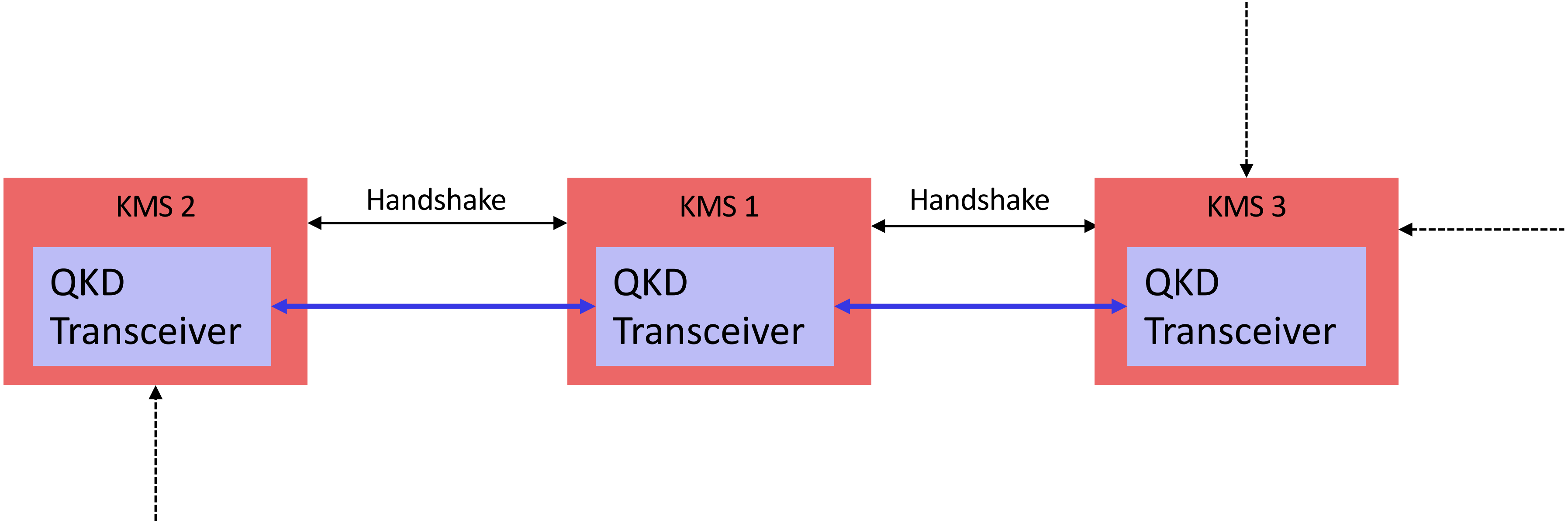


Key exchange

Global key ⊕ secure key

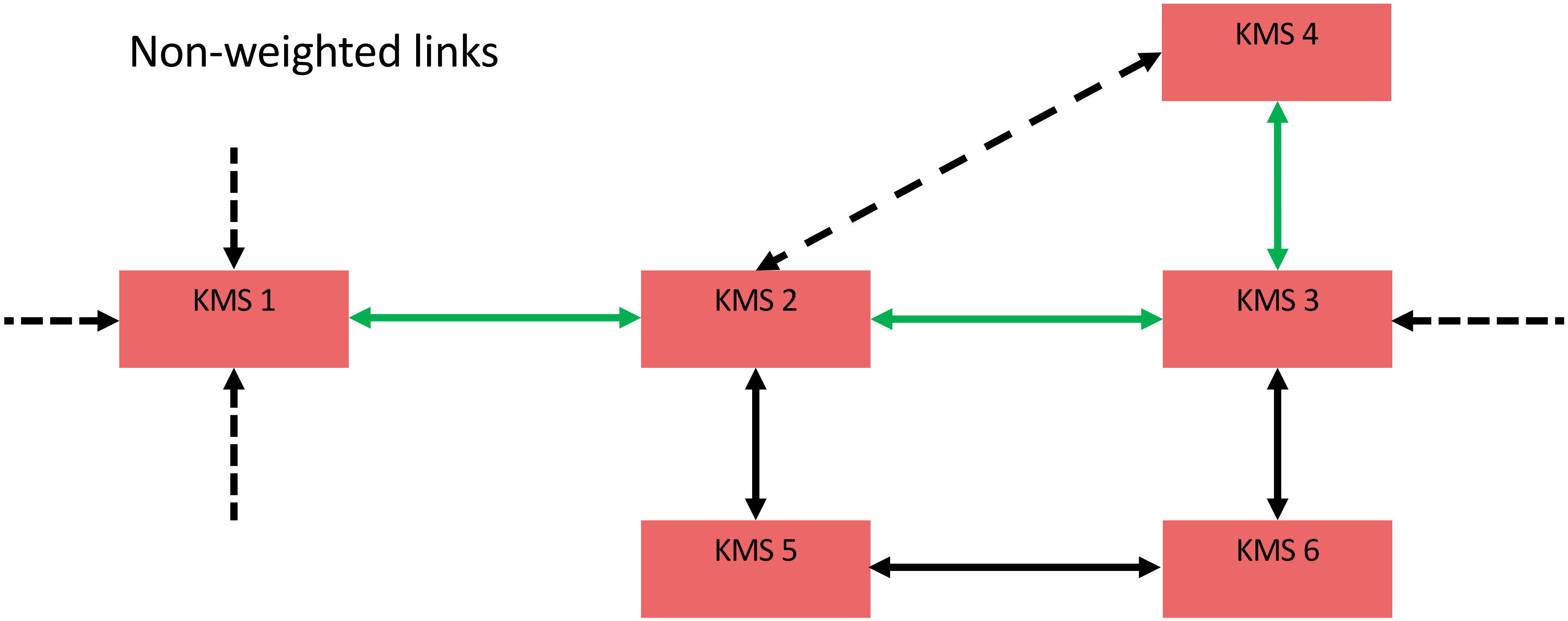


Network creation



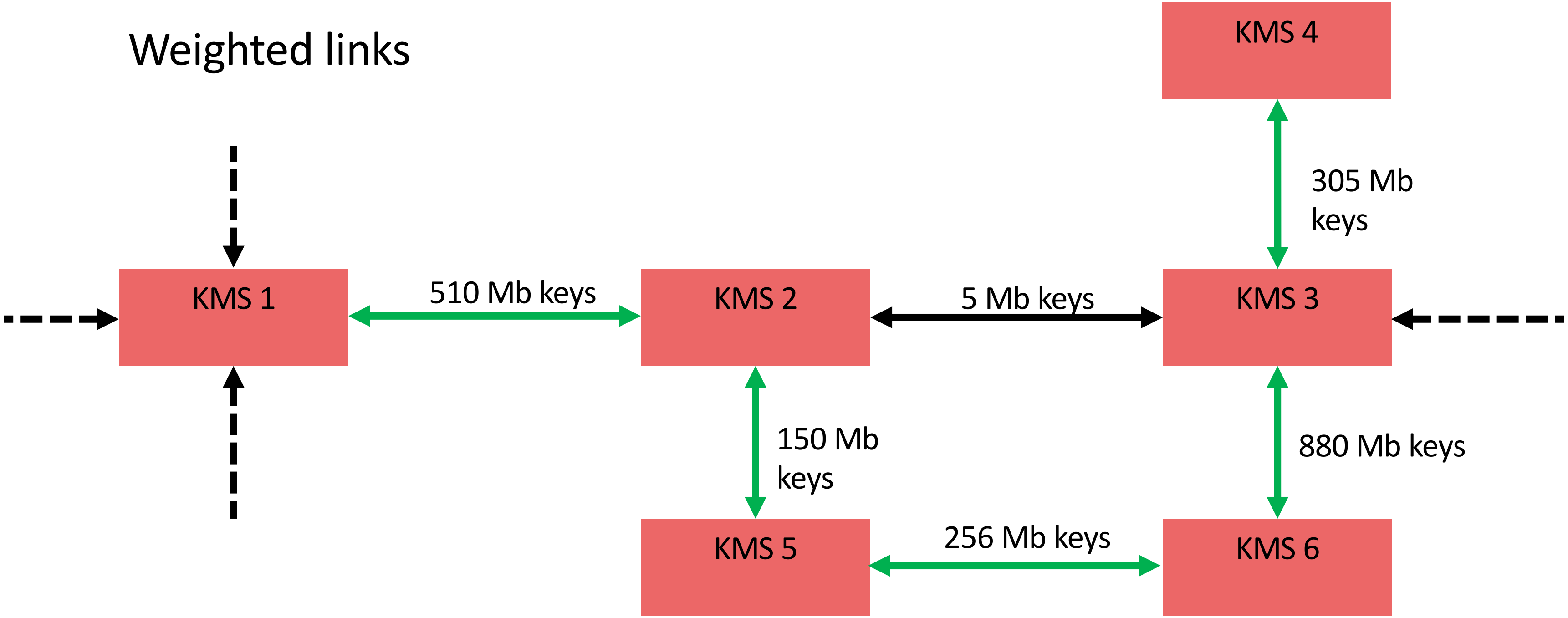
Routing

Non-weighted links



Routing

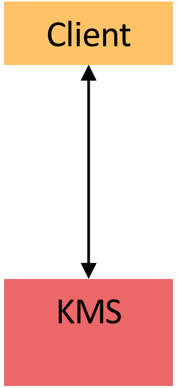
Weighted links



Client interface

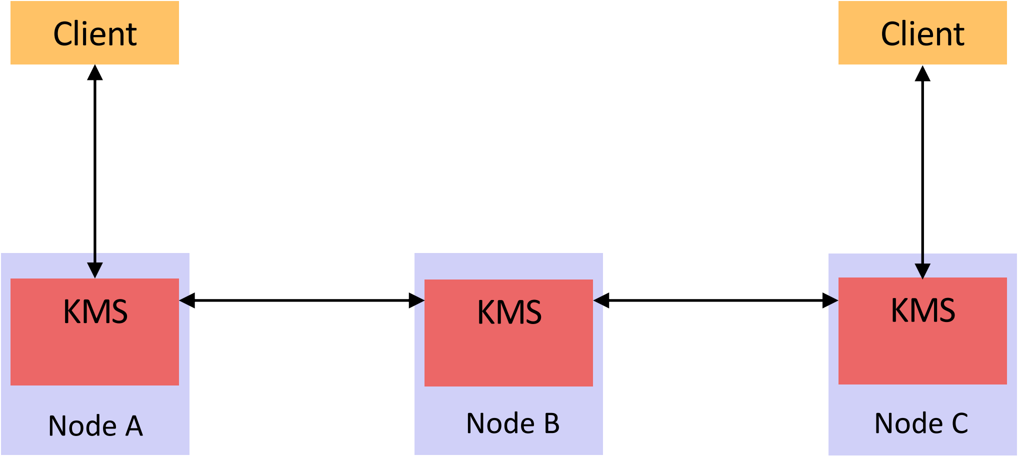
ETSI standards:

https://{KMS_hostname}/api/v1/keys/{Client_ID}/enc_keys

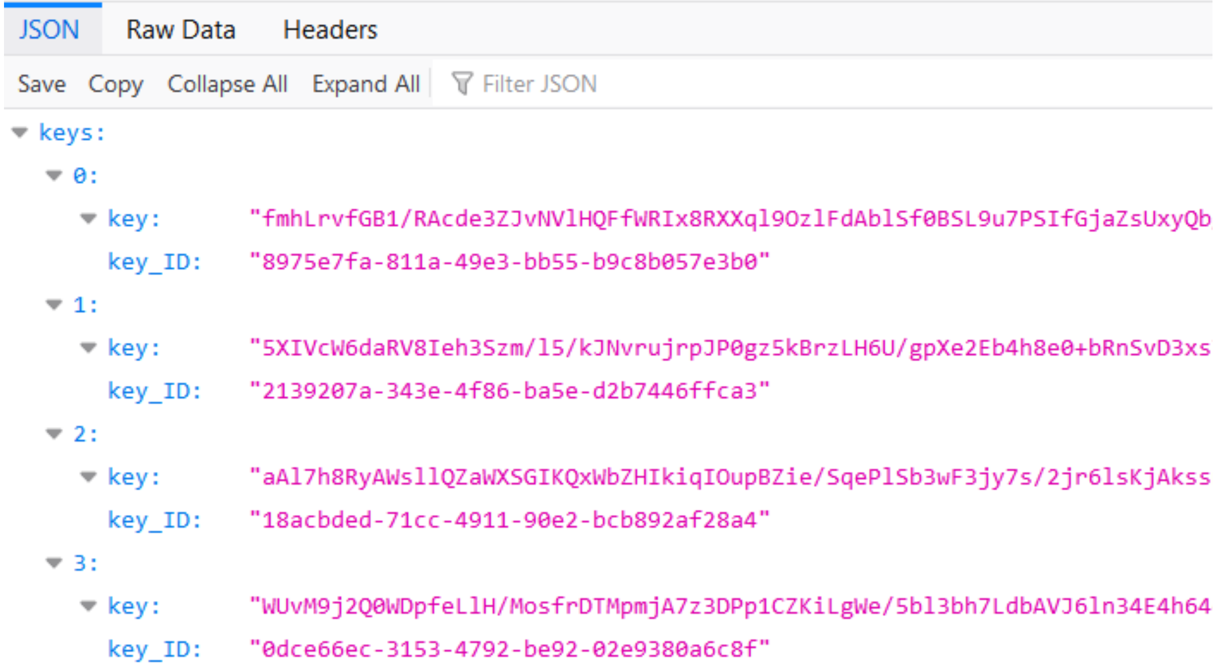


Testing setup

Ubuntu servers in rack



Testing Key distribution



```
▼ keys:
  ▼ 0:
    ▼ key:     "fmhLrvfGB1/RAcde3ZJvNVlHQFfWRIx8RXXql9OzlFdAblSf0BSL9u7PSIfGjaZsUxyQb
      key_ID:  "8975e7fa-811a-49e3-bb55-b9c8b057e3b0"
  ▼ 1:
    ▼ key:     "5XIVcW6daRV8Ieh3Szm/l5/kJNvrujrpJP0gz5kBrzLH6U/gpXe2Eb4h8e0+bRnSvD3xs
      key_ID:  "2139207a-343e-4f86-ba5e-d2b7446ffca3"
  ▼ 2:
    ▼ key:     "aAl7h8RyAWsllQZaWXSGIKQxWbZHIkiqIOupBZie/SqePlSb3wF3jy7s/2jr6lsKjAkss
      key_ID:  "18acbded-71cc-4911-90e2-bcb892af28a4"
  ▼ 3:
    ▼ key:     "WUvM9j2Q0WDpfeLlH/MosfrDTMpmjA7z3DPp1CZKiLgWe/5bl3bh7LdbAVJ6ln34E4h64
      key_ID:  "0dce66ec-3153-4792-be92-02e9380a6c8f"
```

Testing results

- Broadcasting and handshaking
- Automatic network creation
- Routing
- Key exchange
- Client connection

Conclusion

- Ongoing work to deploy a QKD over optical infrastructure
- QKD field lab to support research
- Modular
- Vendor independent
- Full network layer