QKD – PRINCIPLES AND NETWORKS

Andreas POPPE
Center for Digital Safety & Security
AIT Austrian Institute of Technology
Vienna, Austria

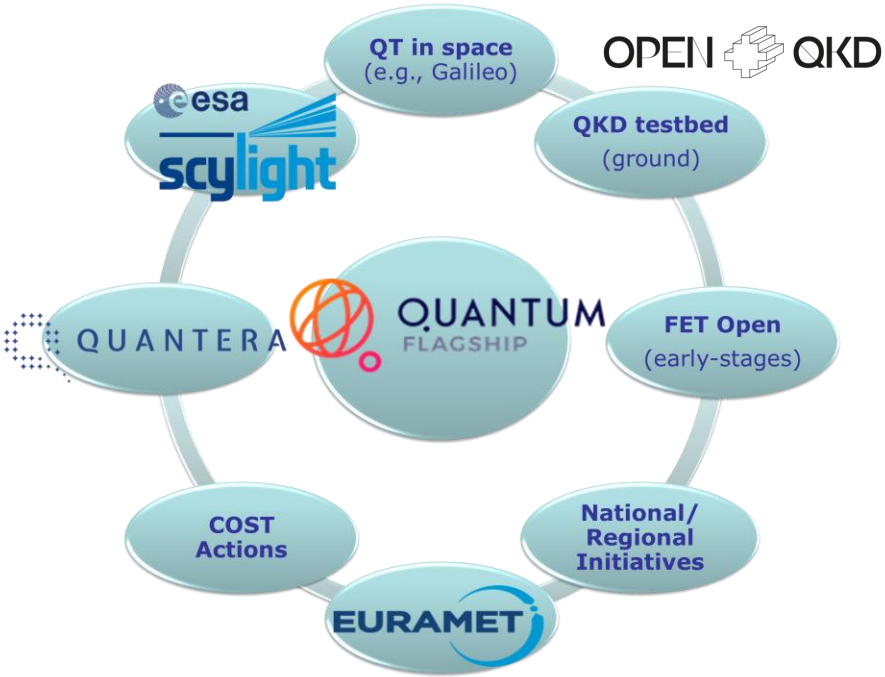
andreas.poppe@ait.ac.at

OUTLINE

1. Quantum eco-system in Europe + Motivation
2. QKD protocols
3. Trusted node paradigm
4. Future network planning
5. OpenQKD (slide set 2)

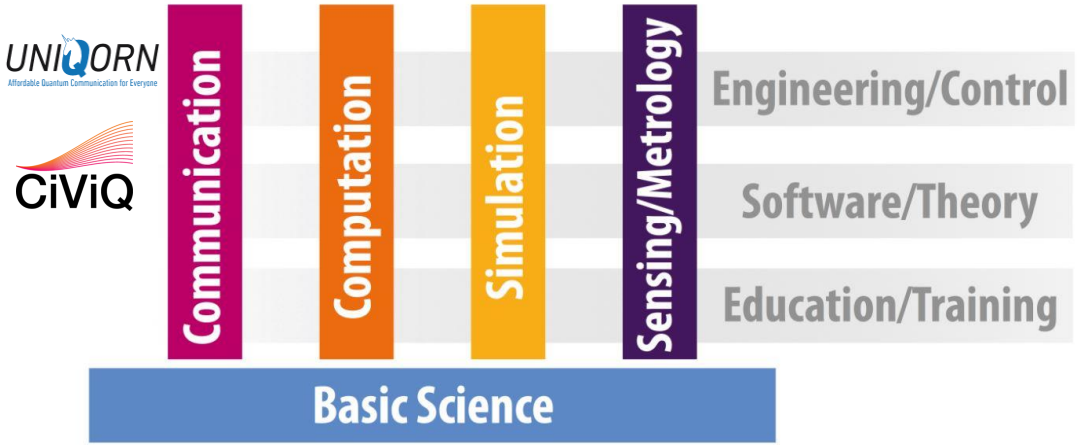
OUTLINE

1. **Quantum eco-system in Europe + Motivation**
2. QKD protocols
3. Trusted node paradigm
4. Future network planning
5. OpenQKD (slide set 2)



EU Quantum Technologies Flagship 2018 - 2028

The Quantum Flagship is a 10 years program initiated by EU with 1000M€ funding



https://ec.europa.eu/digital-single-market/en/news/intermediate-report-quantum-flagship-high-level-expert-group

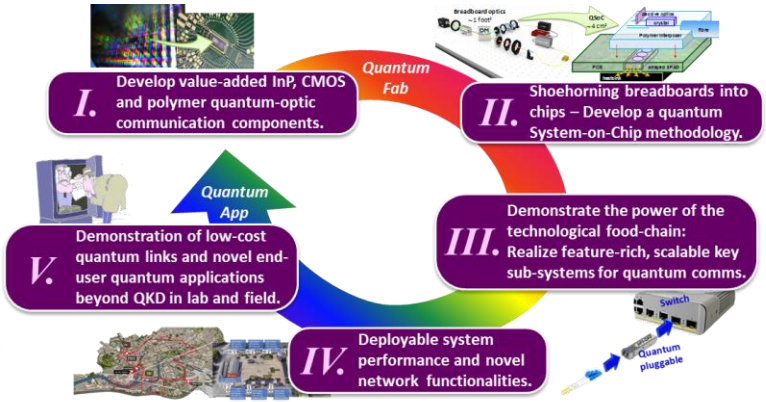
SHAPING EUROPEAN QT FLAGSHIP PROJECTS

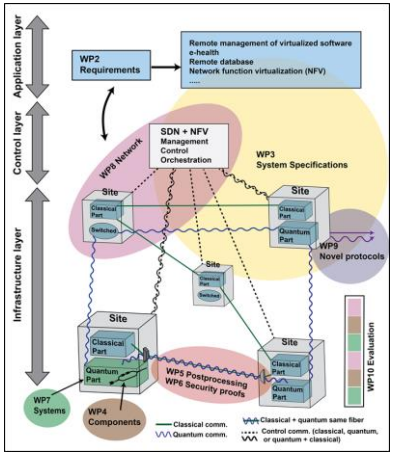
AUSTRIAN INSTITUTE OF TECHNOLOGY

UNIQORN

Affordable Quantum Communication for Everyone

Coordinated by AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY





CiViQ

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY partner

Telecom networks require enhanced security

Flexible and inexpensive QKD systems that can be **integrated into modern telecom infrastructures**

Continuous Variable QKD Technology (CV-QKD)

Consortium of 21 partners: 4 Research Institutes, 7 Universities, 2 SMEs, and 8 large companies

EU QT-Flagship project CiViQ

For further industrialization, the EU wide CV-QKD community grouped together to form a consortium with up to now 21 partners.

Common motivation: Transfer similarities of coherent communication schemes to the quantum domain.

The goal is to open a radically novel avenue towards flexible and cost-effective **integration of** Continuous-Variable **quantum communication** technologies **into** emerging optical **telecommunication networks**.

Specifications, use-cases, requirements

Next generation integrative ***Networks***

Components

CV-QKD systems

Next generation systems and advanced protocols

Validation, benchmarking of CV-QKD systems of use-cases in networks

21 partners with

- 10 universities and research centers
- 8 industrial partners incl. SMEs + large enterprises
- 3 telecom providers

from

8 EU-countries and Israel:

Optical Platform for Integration

- Prospective QKD devices will be an optional card that can also seamlessly be integrated
- Standard high-end telecom devices
- Co-integration of QKD with >100 Gb/s channels
- AES-256 encryptor including adequate key interface
- Option to force key exchange in the encryptor from parts of seconds to never

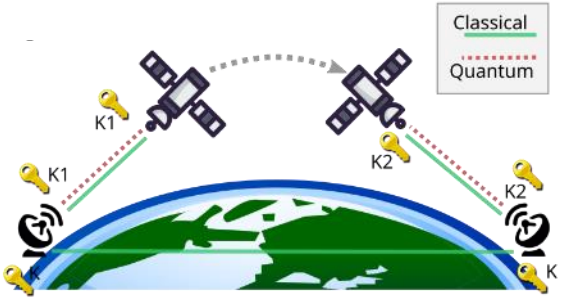
EUROQCI: A EUROPEAN QUANTUM INTERNET

QUANTUM COMMUNICATION INFRASTRUCTURE (EuroQCI)

Build and **deploy** in the next decade a certified secure pan-European end-to-end QCI for **cyber-security services**

EuroQCI

- Terrestrial QKD network
- Satellite based QKD network



Phase 1: Quantum Secured Network

Phase 2: Quantum Information Network

Strengthen European autonomy in:

- Cyber Security
- Quantum Technologies
- High Performance Computing

ADVANTAGES OF QKD

AUSTRIAN INSTITUTE OF TECHNOLOGY

Long – term Security

- Forward secrecy
- Guaranteed safety for decades
- Medical and biometric data

ITS – secure Encryption

- Combination of QKD and one-time pad
- Governments
- Military

Dynamic Keys

- Fast renewal of keys
- 1Tbit of AES encryption per key
- Critical infrastructure

OUTLINE

1. Quantum eco-system in Europe + Motivation
2. **QKD protocols**
3. Trusted node paradigm
4. Future network planning
5. OpenQKD (slide set 2)

Quantum Key Distribution protocols

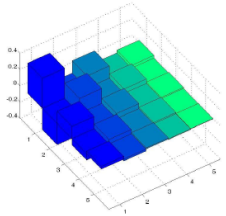
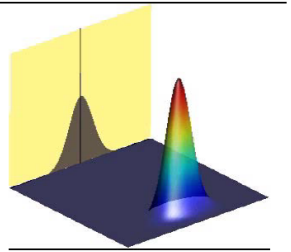
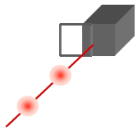
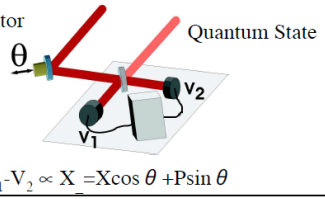
- Discrete Variable QKD (DV-QKD)
  - Prepare-and-measure
  - Encoding in phase and polarization
  - Many other protocols than BB84
- Entanglement based protocols
  - Heralded photons with pair source
  - Polarization encoding
- Distributed phase-reference protocols
  - Differential phase shift
  - Continuous one-way
- Continuous Variable protocols (CV-QKD)
  - Discrete modulation
  - Gaussian modulation

Overview of this schemes:
V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009)

More recent review:

E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan “Practical challenges in quantum key distribution,” *npj Quantum Information* **2**, 16025 (2016)

Discrete vs. Continuous Light

Light is :	Discrete Photons	Continuous Wave
We want to know :	their Number & Coherence	its Amplitude & Phase (polar) its Quadratures X & P (cartesian)
We describe it with :	Density matrix $\rho_{n,m}$ 	Wigner function W(X,P) 
We measure it by :	Counting: APD, VLPC, TES... 	Demodulating : Homodyne Detection  V_1-$V_2 \propto X_\theta = X\cos\theta + P\sin\theta$
« Simple » States	Fock States	Gaussian States

Philippe Grangier

Laboratoire Charles Fabry de l'Institut d'Optique,
UMR 8501 du CNRS, 91127 Palaiseau, France

Principles of QKD

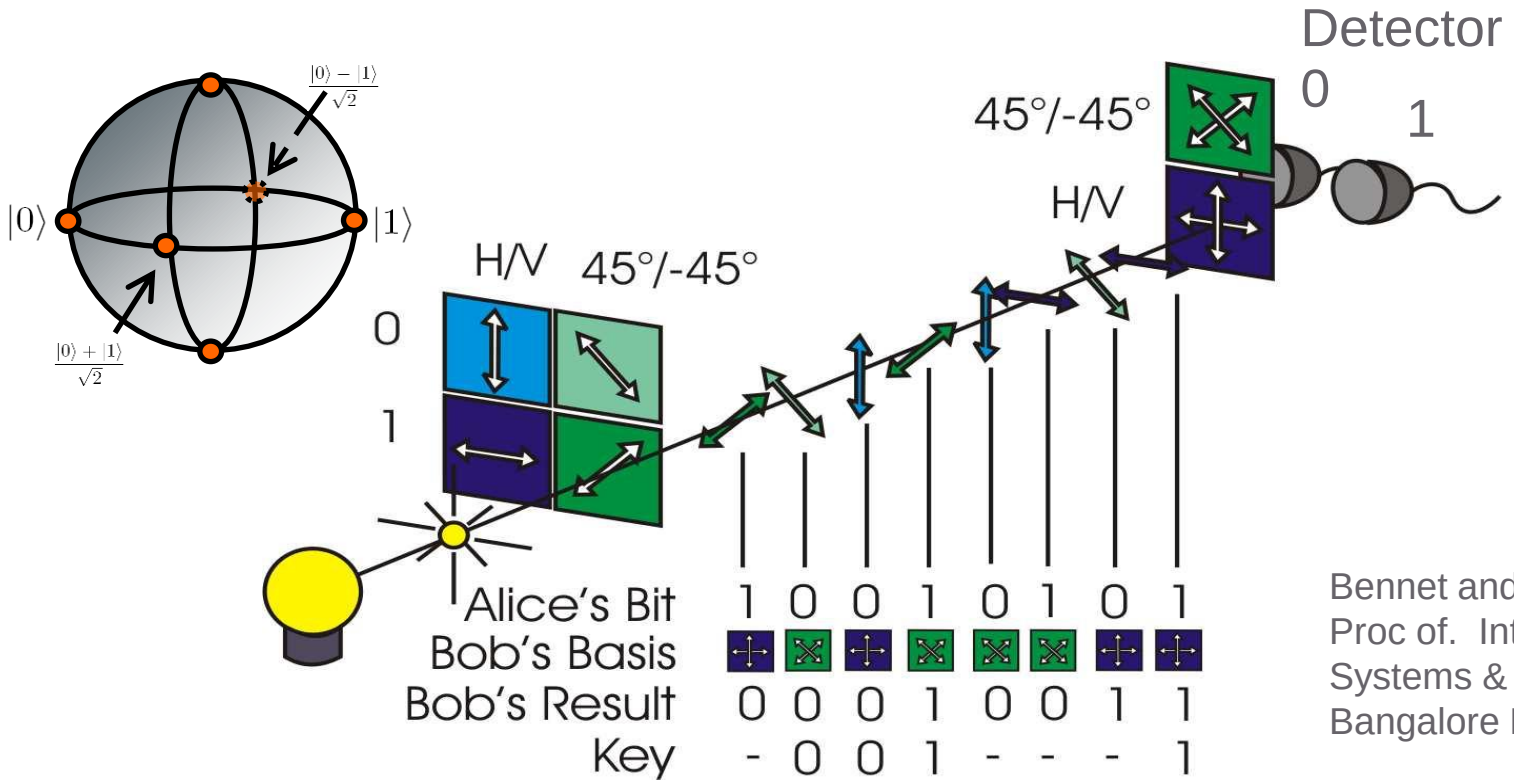
Quantum channel with non-commuting quantum observables, usually „polarization“, „phase“, now also orbital angular momentum → **DV-QKD**

Eve can easily listen-in / copy classical data without being detected

Continuous Variable **CV-QKD** protocol:

- Non-commuting observables are the quadratures I and Q (X and P)
- Coherent states (<5 photons) are modulated in phase & amplitues
- Detection is performed with shot-noise limited homodyne detectors

Historic BB84 protocol



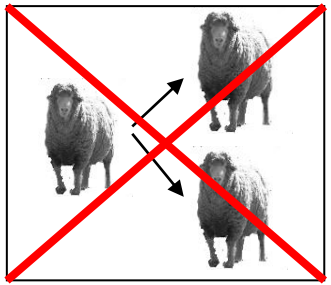
Bennet and Brassard
Proc of. Int.Conf. Computers, Systems & Signal Processing, Bangalore India 175 (1984)

Detecting an adversary in the quantum channel

Alice prepares qubits and send them to Bob

- Intercept – Resend attack
- Cloning Attack: Eve tries to „amplify“ single qubit

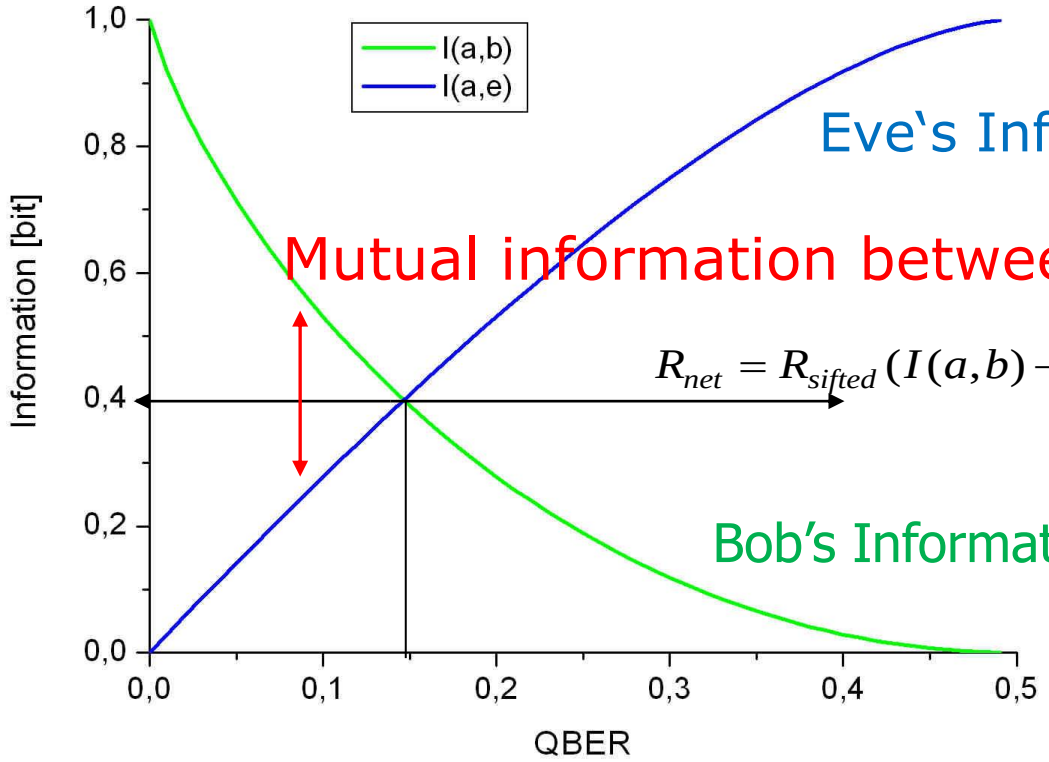
  Quantum world: No-Cloning Theorem !!!!



Whatever Eve does: Laws of physics prevent her to extract information without disturbing the qubits!

Alice and Bob must evaluate the errors on the quantum line to shorten the key and remove the information revealed to the eavesdropper completely

Individual attacks on a DV-QKD system



Eve's Information

Mutual information between Alice and Bob

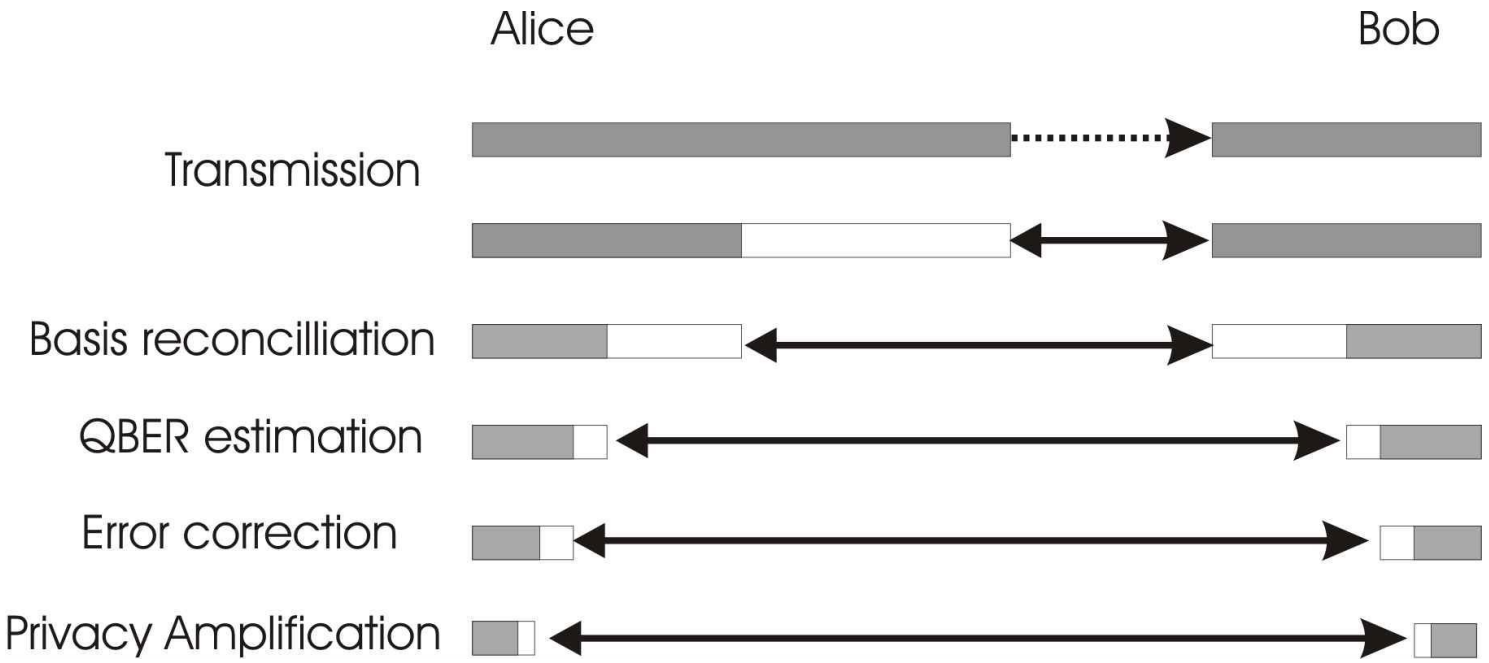
$$R_{net} = R_{sifted}\,(I(a,b) - I(a,e))$$

Bob's Information

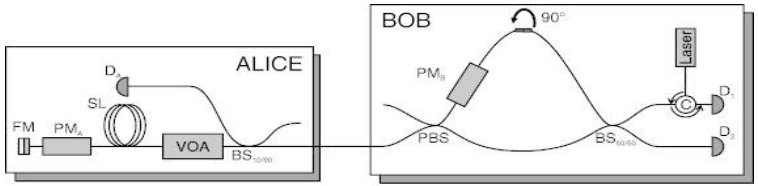
$$QBER = \frac{\text{false counts}}{\text{all counts}}$$

Reconciliation steps

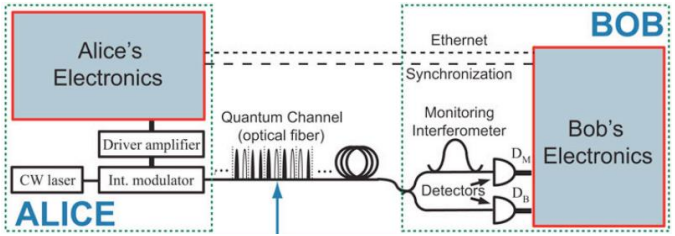
to transfer measurements into a key



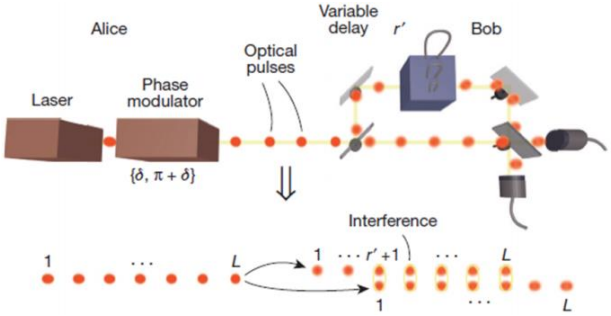
Different successful realizations of DV-QKD



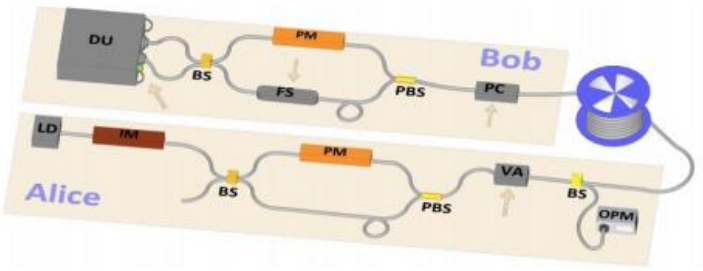
IdQuantique (Geneva), N. J. of Phys. 11 (‘09)



Geneva U., Opt. Expres 17 (‘09)



Tokyo U., Sasaki T. et al, Nature 509 (‘14)



Toshiba, Lucamarini M. et al,Opt. Expres 21 (‘13)

Commercial QKD devices today

- QuantumCTek (China):
  Quantum gateway with high number of deployments, polarization encoding

- IdQuantiqe (Swiss): first commercial product (Datacenters, Banks, etc.), requires dark fibre for quantum channel

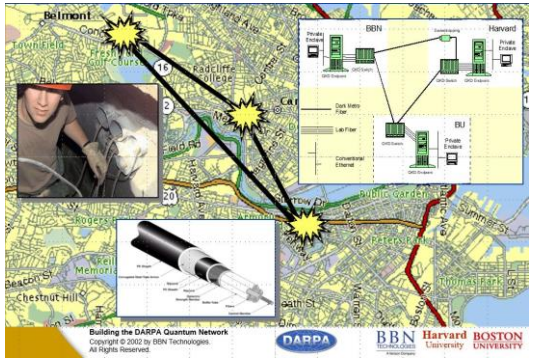
- Toshiba QKD (Japan, UK): System- boxed, standalone, high-rate system
  still under development, UK Quantum Hub

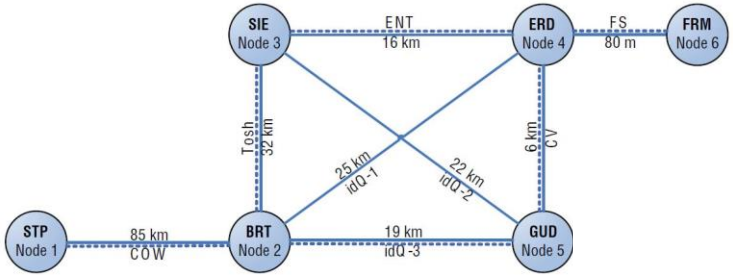
OUTLINE

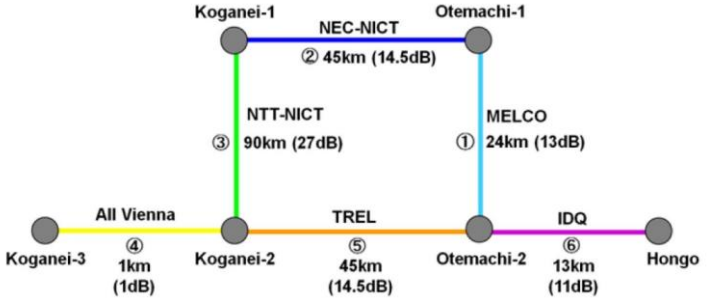
1. Quantum eco-system in Europe + Motivation
2. QKD protocols
3. **Trusted node paradigm**
4. Future network planning
5. OpenQKD (slide set 2)

QKD Networks

DARPA Network 2002 SECOQC Network 2008 Tokyo Network 2010







Chip Elliott, NJP 4, 46 (2002) M. Peev et al., NJP **11**, 75001 (2009) M. Sasaki et al., Opt Exp. **19**, 143962 (2011)

All these demonstrations show interoperability of QKD-links from different vendors. Unfortunately they all failed to trigger attention from telecoms to start (massive) deployment, because the functionalities demonstrated there (switching, trusted repeaters) could not be mapped to deployed infrastructures.

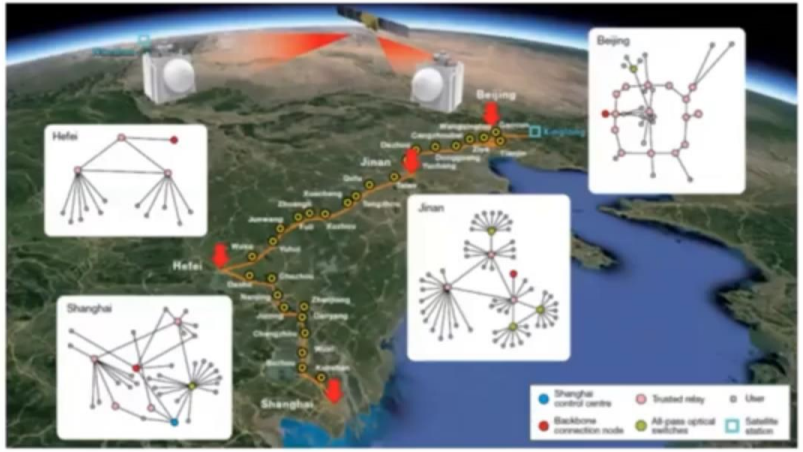
Towards a Quantum Communication Infrastructure

Practical testbed deployment is crucial for
interoperability, maturity, network integration aspects and topology, use case benchmarking, standardization of interfaces

Y.-A. Chen *et al.*, Nature 2021

Trusted node networks
SECOQC QKD network, 2008
South Africa, Swiss, Tokyo,
UK QC Hub networks
China 2000 km backbone network, including satellite link

LEO Micius: downlink QKD, uplink quantum teleportation, entanglement-based QKD



Networks with untrusted nodes for end-to-end security

Quantum repeaters, long-term and efficient quantum storage beat direct transmission, improve rates, develop network and protocol stack

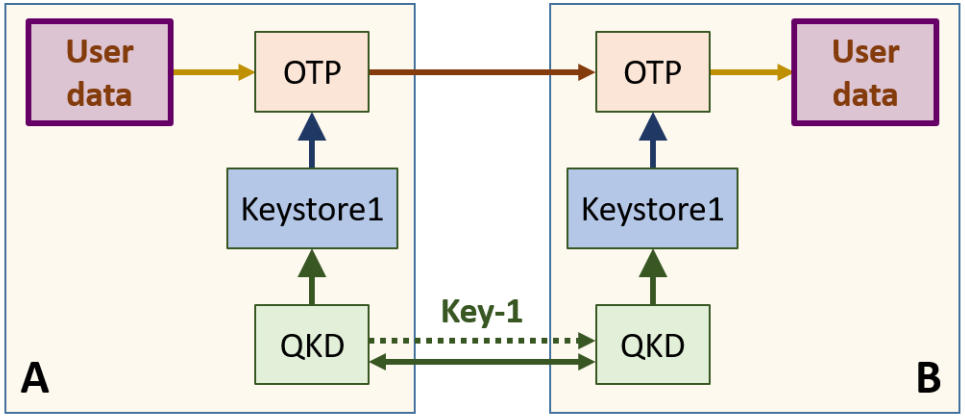
European Commission

esa

EuroQCI

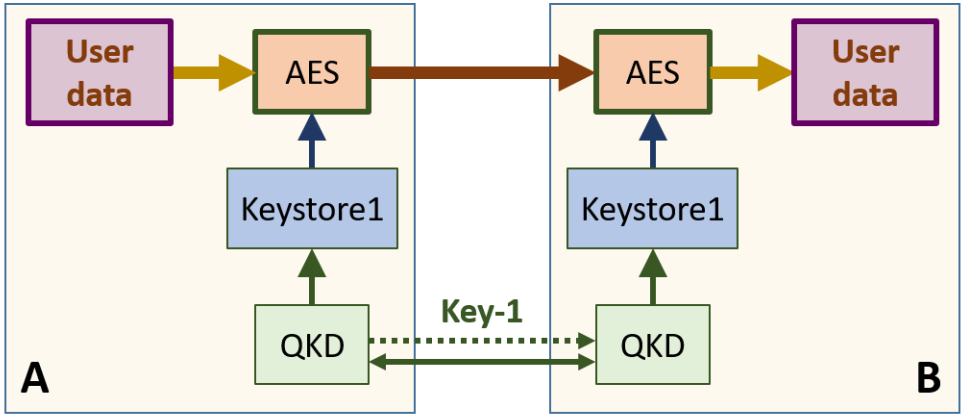
Trusted node paradigm – building block OTP

- Fundamental building block
- OTP… One Time Pad
- Locations A and B are connected by a **low**-speed data connection and QKD-link
- Equal rates for User data and Key-1



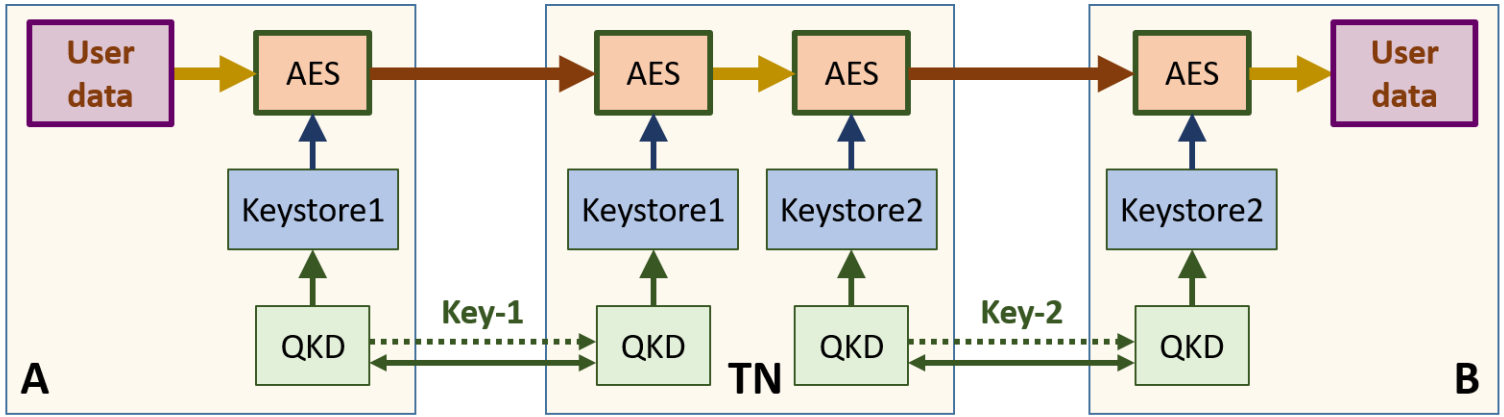
Trusted node paradigm – building block AES

- Fundamental building block
- AES… Advanced Encryption Standard
- Locations A and B are connected by a **high**-speed data connection and QKD-link
- Key-1 to refresh secret AES key



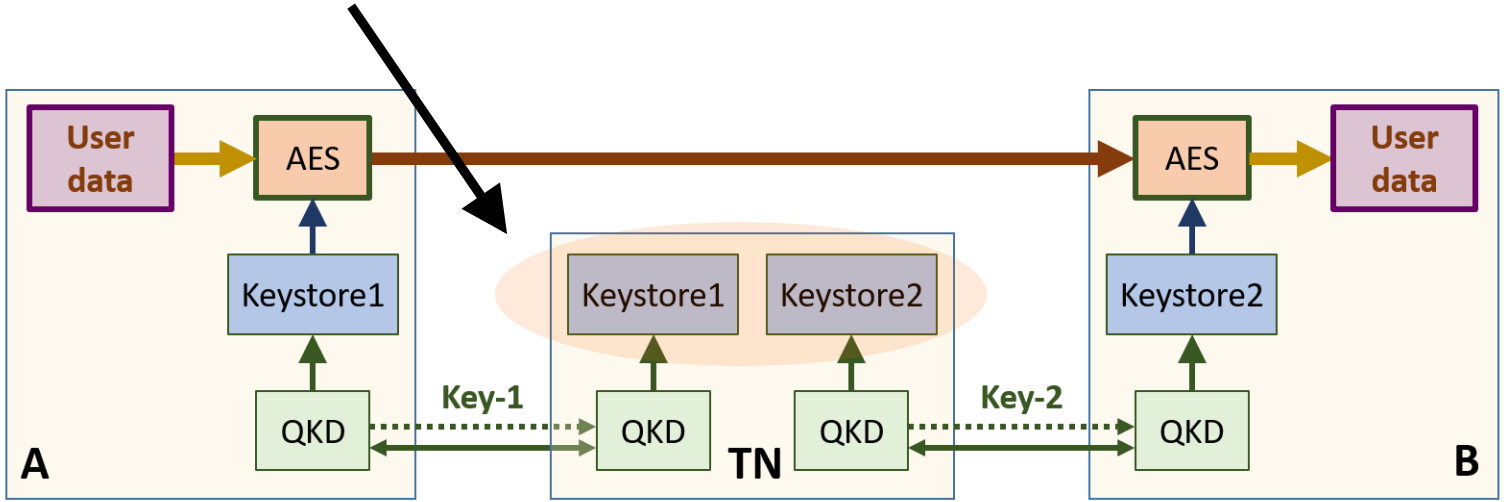
Trusted node paradigm – linear chain

- Locations A and B are connected by building blocks to increase distance
- Network arguments: Linear chain to star shape network
- “Full-blown” trusted node. **TN need perform full functionalities** (full encryption and decryption in TN).
- User data need and QKD-links same fibers, satellite-connection?



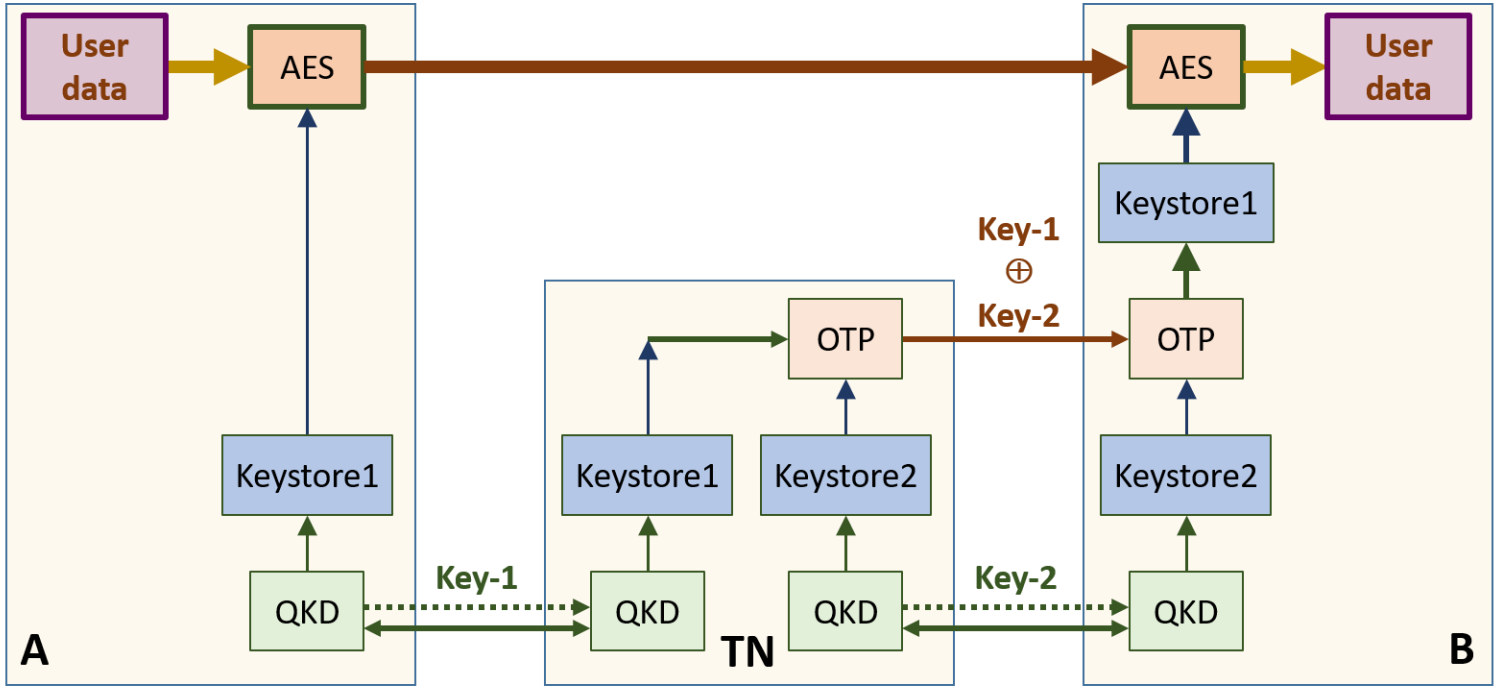
Trusted node paradigm – end-to-end security

- User data is not interrupted, totally different route is possible (satellite)
- Node has full key, therefore “**Trusted node**”
- AES-keys need to be the same on both ends
- QKD-network is about to generate end-to-end-keys



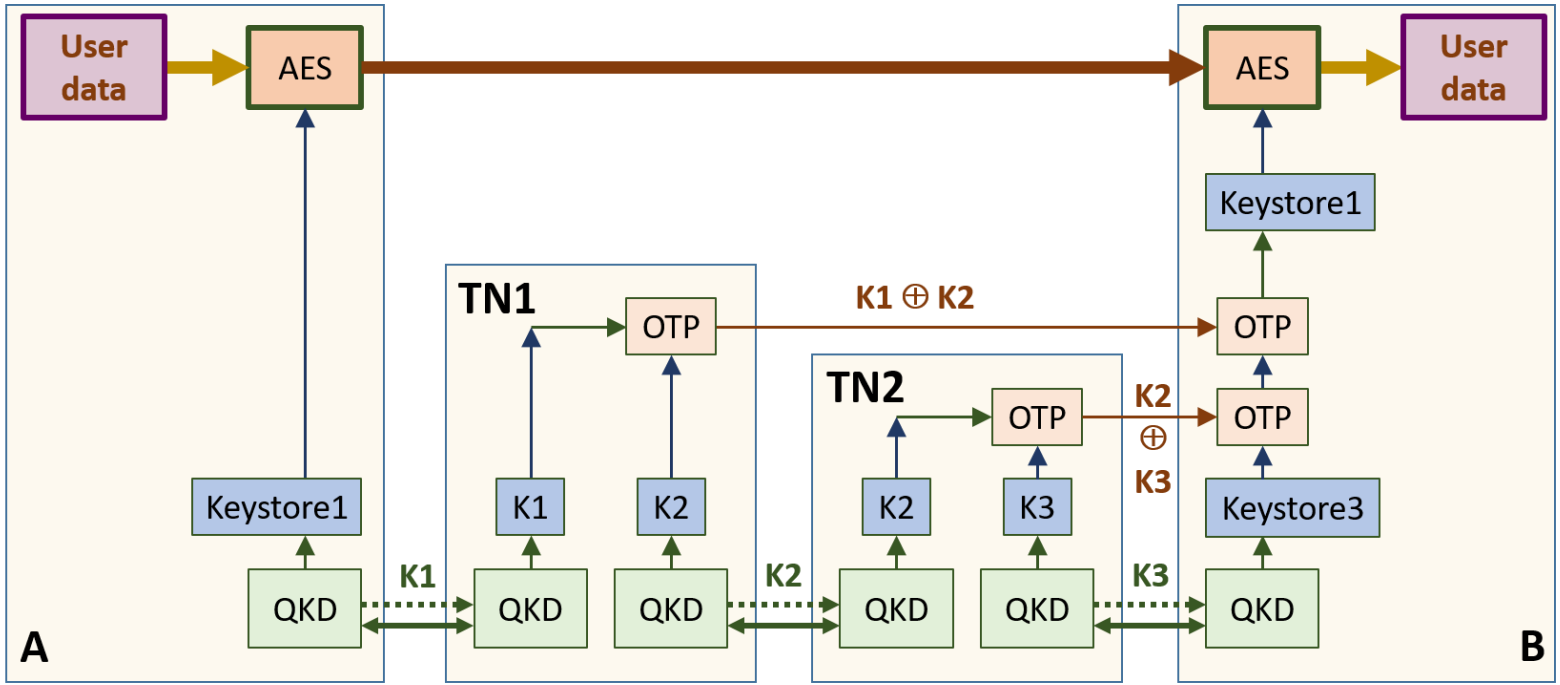
Trusted node paradigm – XORing of keys

- Secure Key-1 by Key-2, lowest rate is limiting



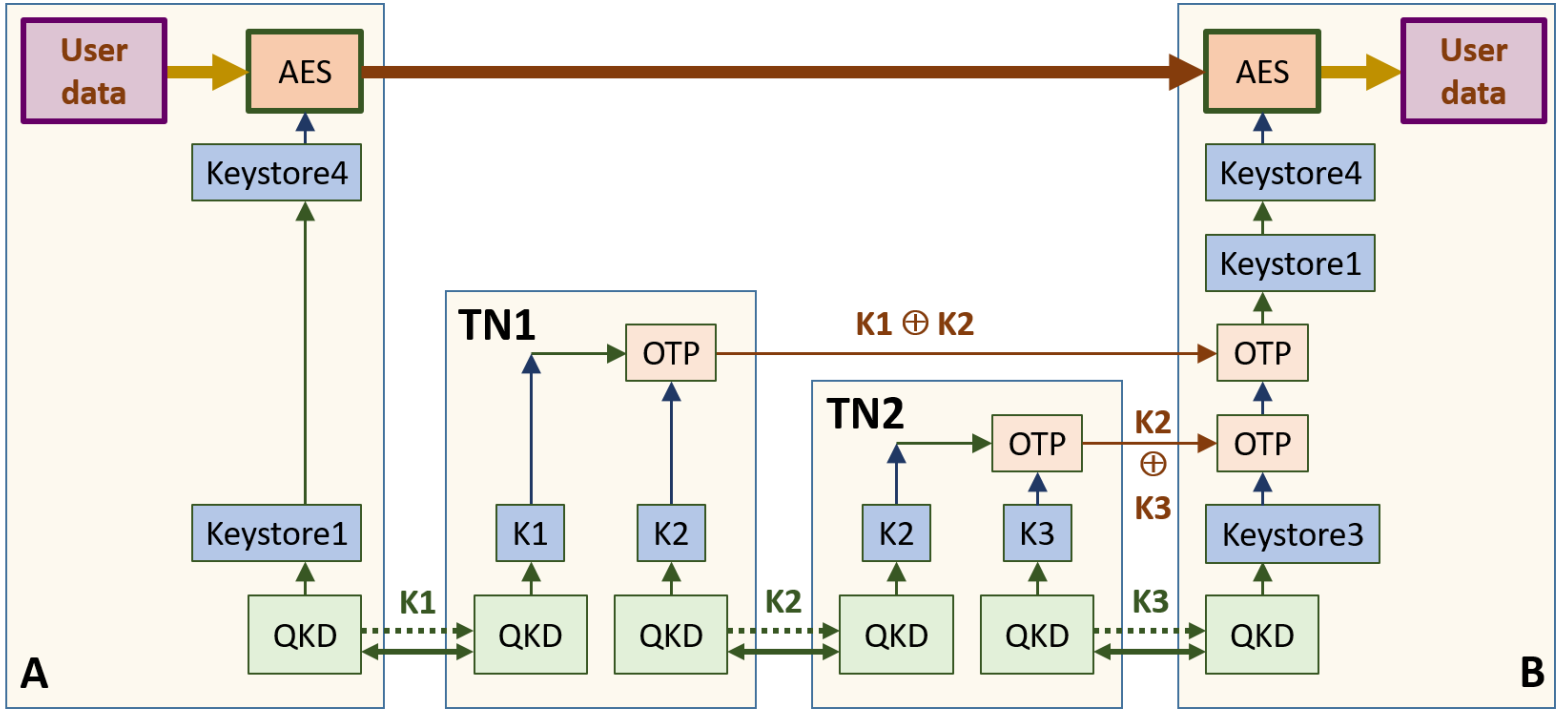
Trusted node paradigm – it gets complicated fast

- More intermediate TNs are possible



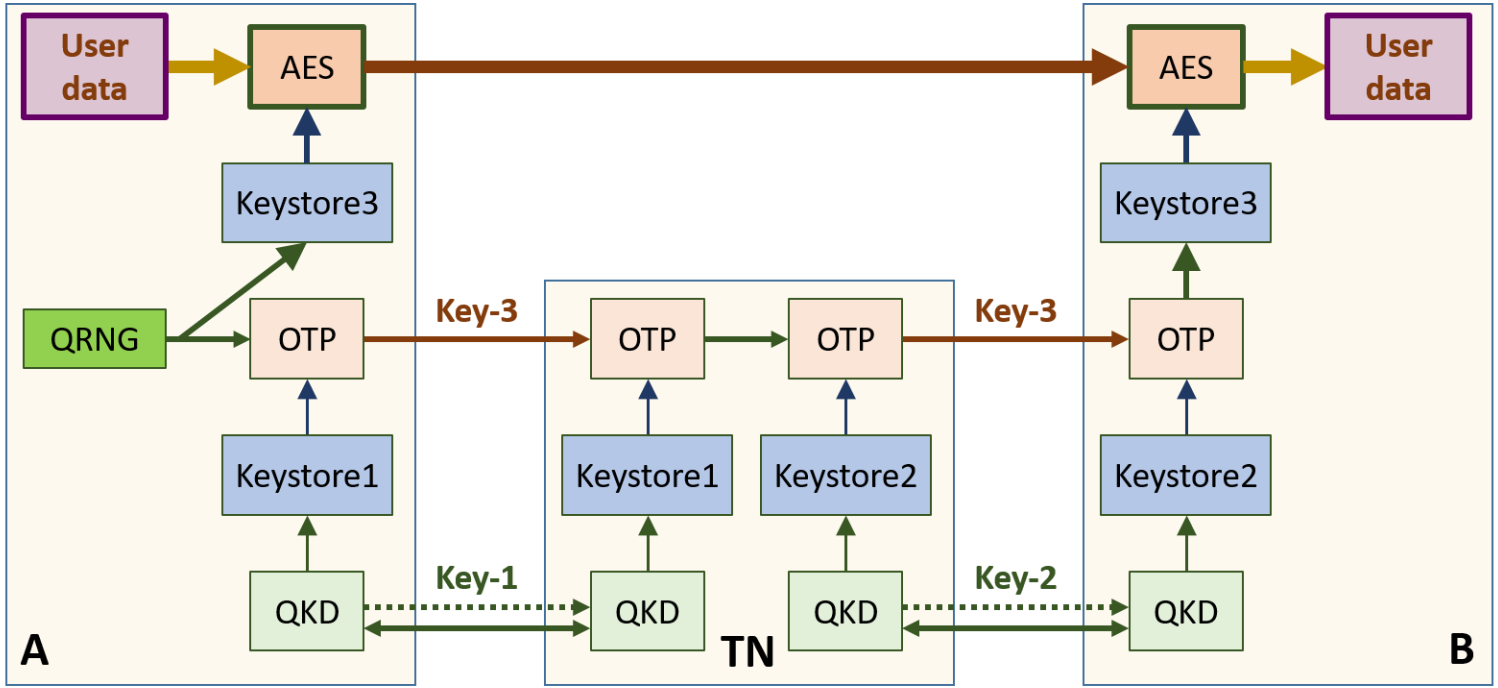
Trusted node paradigm

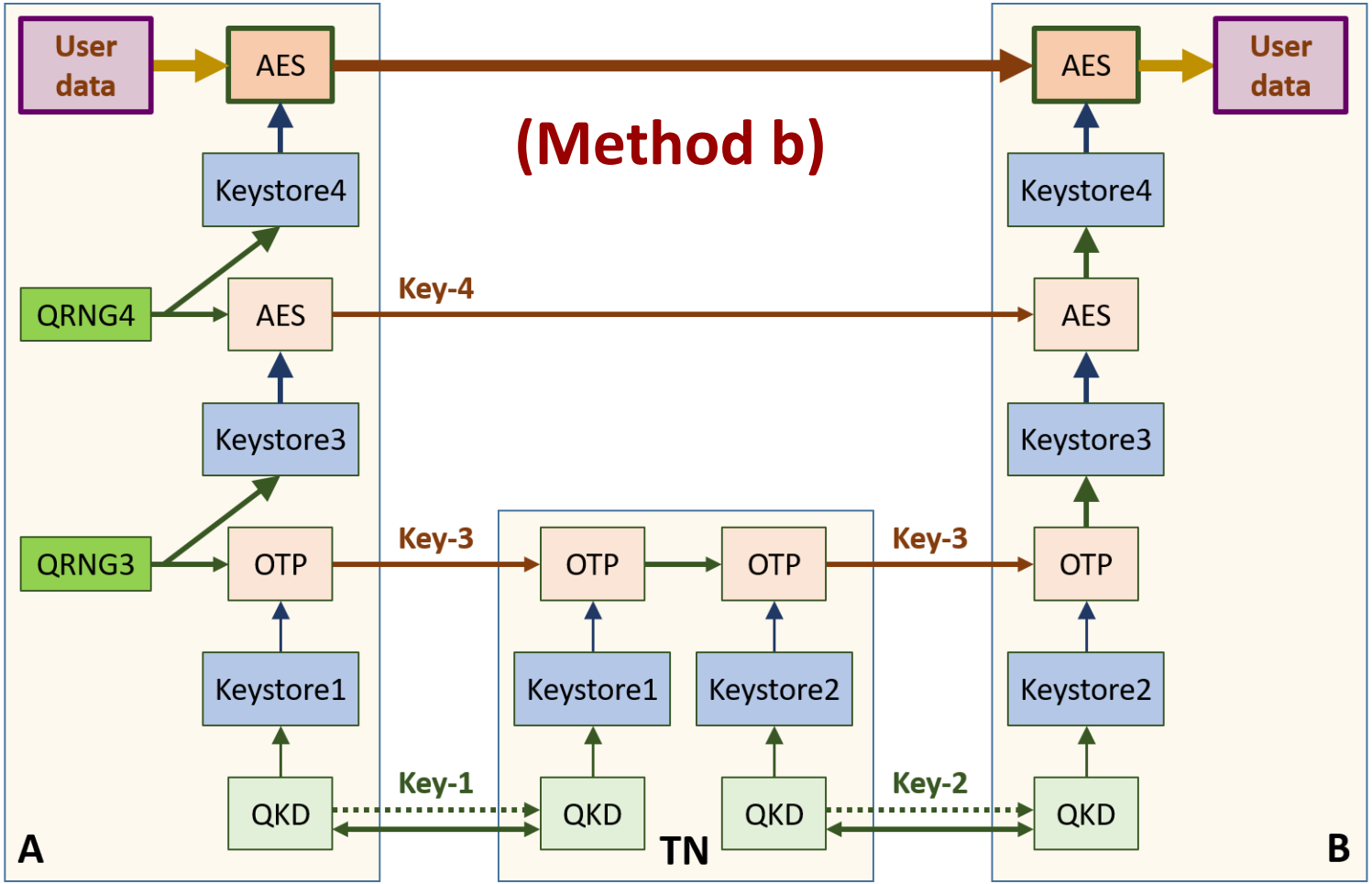
- Keystore 4 can be fed by different QKD routes/paths through the networks



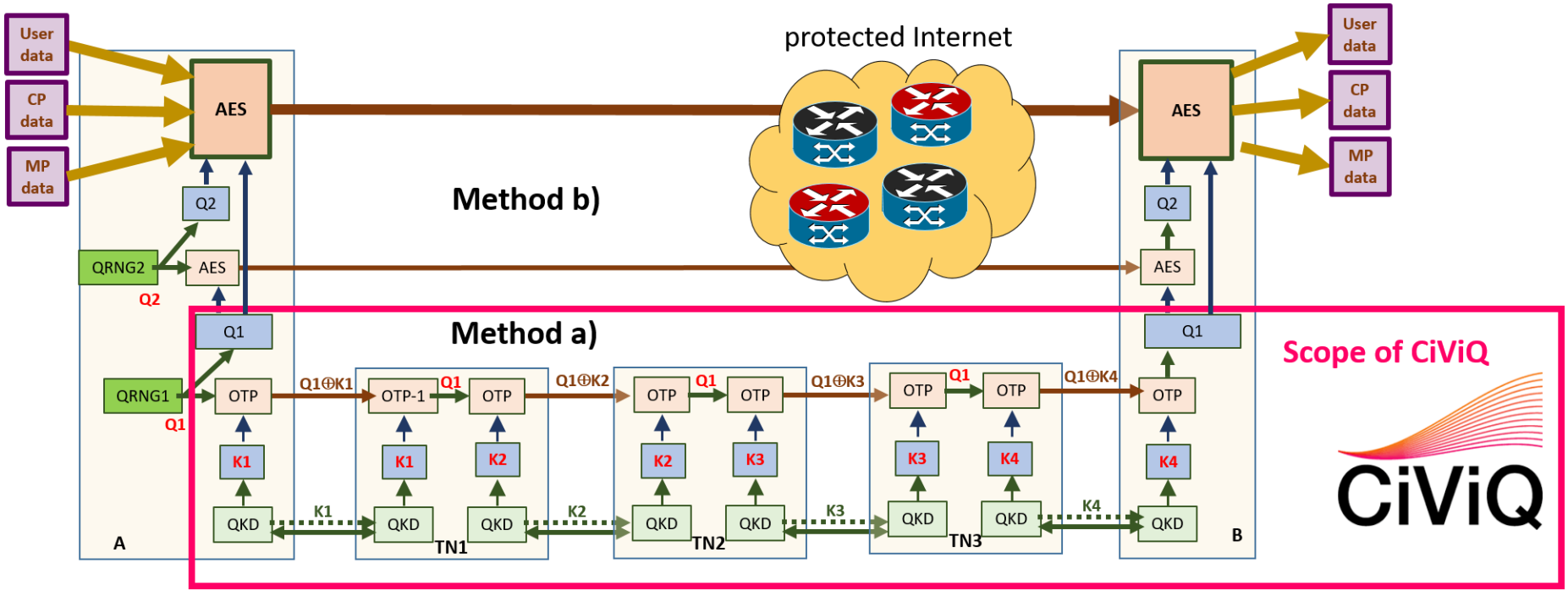
Trusted node paradigm (Method a)

- QRNG as a source for AES-keys, like low-rate user data fundamental block




User data
AES
AES
User data
(Method b)
Keystore4
Keystore4
QRNG4
AES
Key-4
AES
Keystore3
Keystore3
QRNG3
OTP
Key-3
OTP
OTP
Key-3
OTP
Keystore1
Keystore1
Keystore2
Keystore2
Key-1
Key-2
QKD
QKD
QKD
QKD
A
TN
B

Trusted node paradigm



OUTLINE

1. Quantum eco-system in Europe + Motivation
2. QKD protocols
3. Trusted node paradigm
4. **Future network planning**
5. OpenQKD (slide set 2)

ICTON 2019 We.B5.1

CiViQ

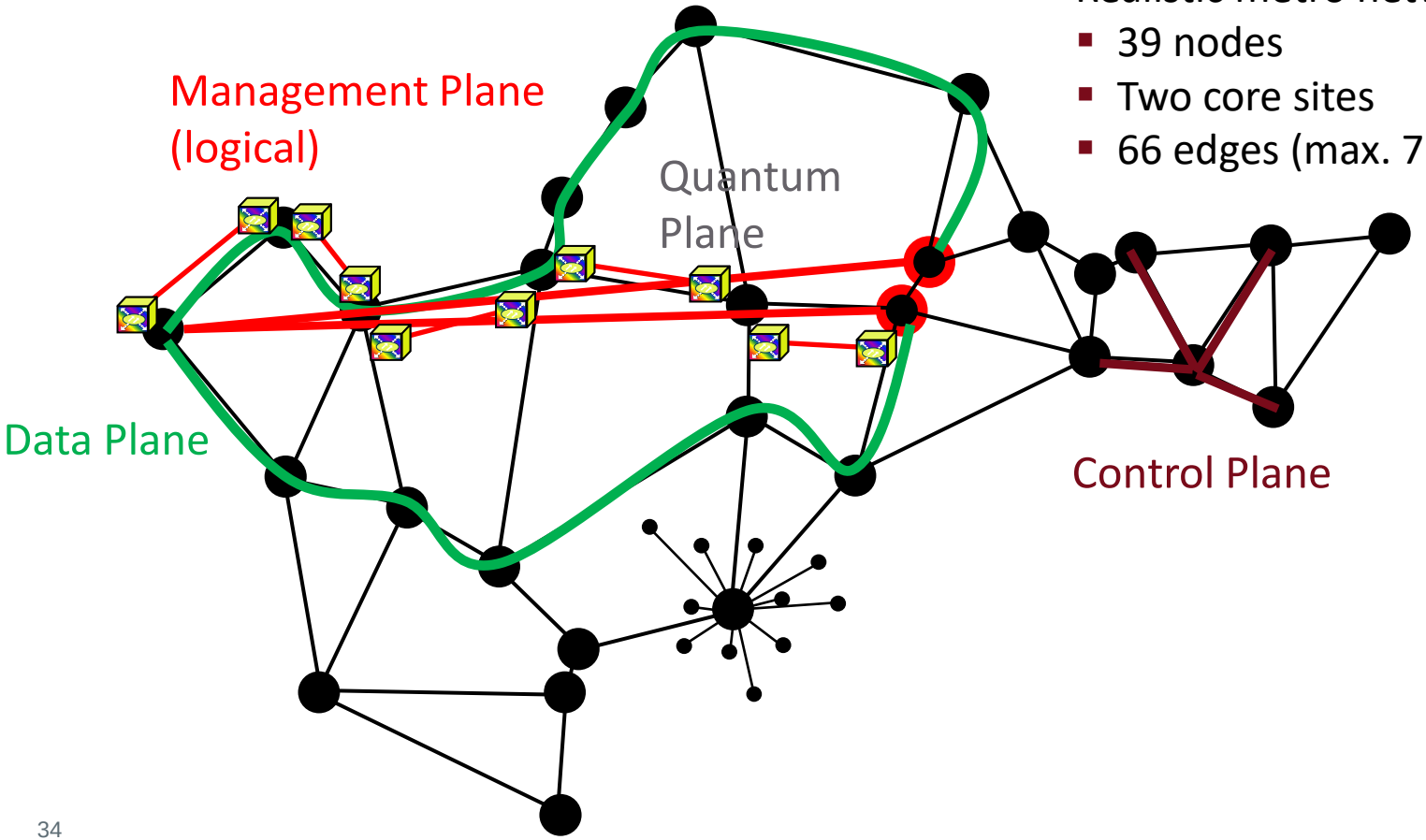
Simulation of a Real-World Driven Reference QKD-Network

Andreas Poppe[1], Matthias Gunkel[2], Felix Wissel[2], Paul Schilder[2], Martin Franzke[2], and Momtchil Peev[1]

[1]Optical and Quantum Communications Laboratory, Munich Research Centers, European Research Institute, Huawei Technologies Düsseldorf GmbH, Munich, Germany

[2]Fixed Mobile Engineering Deutschland, Deutsche Telekom Technik GmbH, Darmstadt, Germany

Reference Network scenario

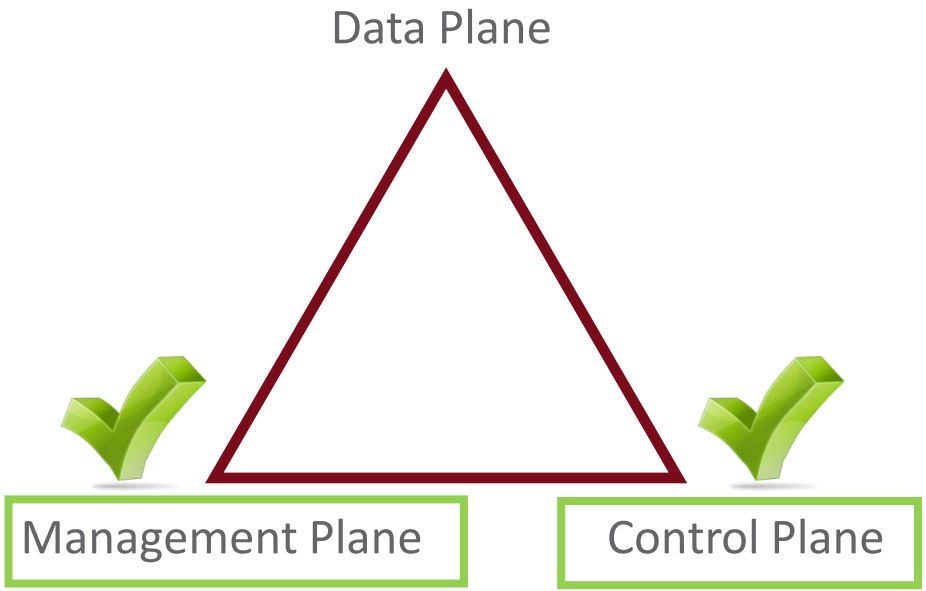


Realistic metro network

- 39 nodes
- Two core sites
- 66 edges (max. 72.4km)

Traffic Categories

no primary focus,
but maybe long-term goal!



Requirements	Traffic type		
	Management plane	**Control plane**	**Data plane**
Topology	Centralized	Next neighbor	Any to any
Average traffic volume	Low, < 1Gbit/s	Very low, few kbit/s (rare peaks)	e.g. several 100Gbit/s or even beyond
Security primarily required for…	Confidentiality Authentication Integrity	Authentication Integrity	Confidentiality
QKD replacing software-based key distribution	Feasible	Feasible	Questionable
Quantum keys used as One-time-pad	Not feasible	Feasible	Not even considered
AES-256 key refresh time*	**≈100 seconds**	**≈ 1hour … 1day**	**≈1-10s /100G channel**
Key rate in NW	**several 10kbit/s**	**few 10bit/s**	**up to multiple Mbit/s per node**

* in case of AES-GCM mode

Network assumptions & Optimization goal

- All nodes require some key material
- All nodes might act as trusted nodes
- Goal: minimum cost
  - N nodes require at least N-1 QKD edges
    - Resilience not yet studied
    - No parallel QKD systems; no node bypassing
- Design Methodologies
  - Integer Linear Programing (ILP)
  - Heuristic designs
    - Minimum Spanning Tree (MST)
    - Single-Source Shortest Path Tree (SS-SPT)
- Question: What is the **maximum minimum key rate** deliverable for the management plane scenario?

Model of QKD links:

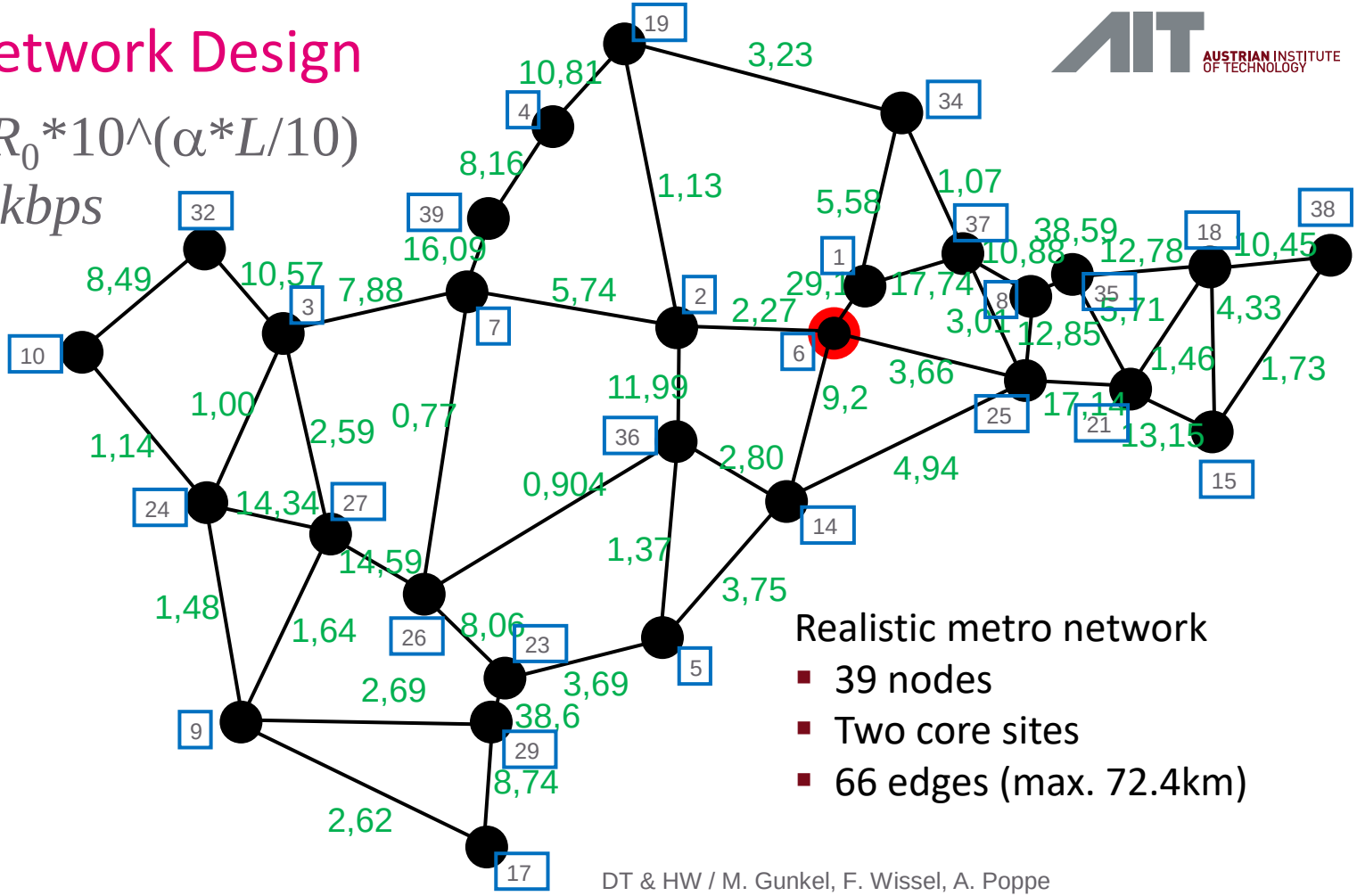
$$R(L) = R_0 * 10\text{^}(\alpha * L/10)$$

$$R_0 = 50kbps$$

QKD Network Design

$R(L) = R_0 * 10^{(\alpha * L/10)}$

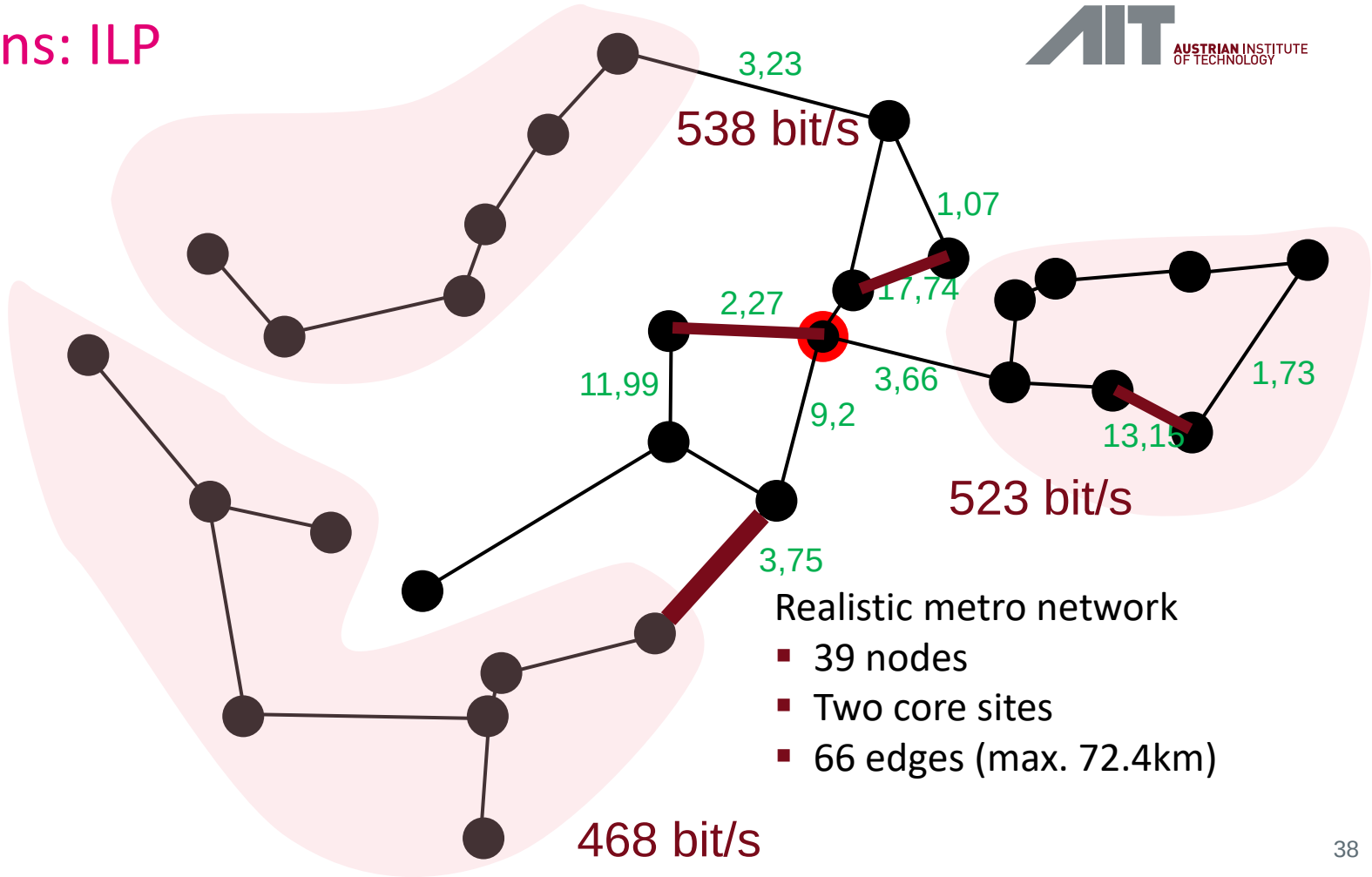
$R_0 = 50kbps$



Realistic metro network

- 39 nodes
- Two core sites
- 66 edges (max. 72.4km)

Solutions: ILP

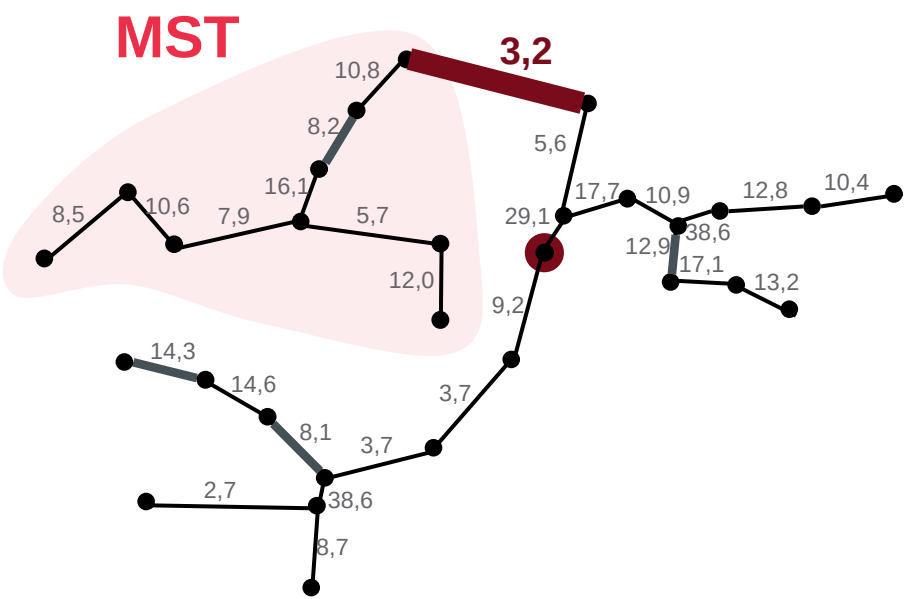


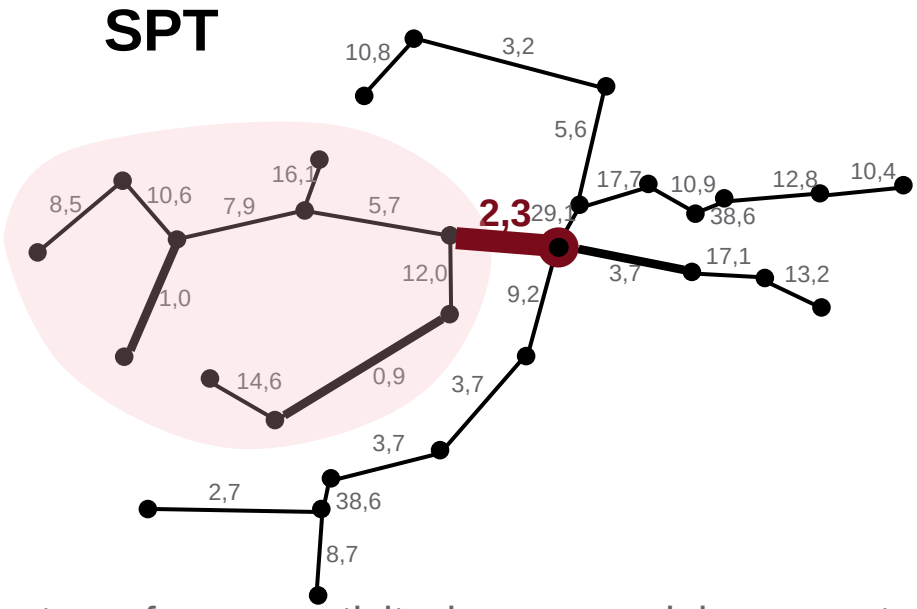
Realistic metro network

- 39 nodes
- Two core sites
- 66 edges (max. 72.4km)

M. Franzke

Solutions: Heuristic designs





- All methods achieve same number of QKD systems for connectivity, i.e. same minimum costs.
- Minimum Spanning Tree (MST) prefers shorter edges than Shortest Path Tree (SPT) and provides a 50% higher minimum key material throughput to leaf nodes:
  - MST: 0.355 kbit/s SPT: 0.23 kbit/s

OUTLINE

1. Quantum eco-system in Europe + Motivation
2. QKD protocols
3. Trusted node paradigm
4. Future network planning
5. **OpenQKD (slide set 2)**

Open European Quantum Key Distribution Testbed

Andreas Poppe

Center for Digital Safety & Security
AIT Austrian Institute of Technology
1210 Vienna, Austria

andreas.poppe@ait.ac.at

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857156.

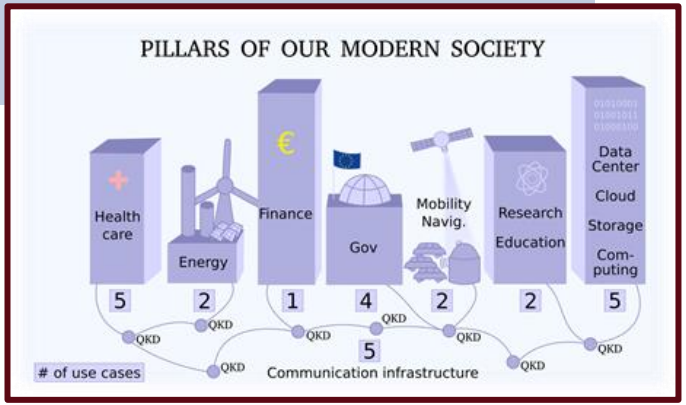
Coordinated by: AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

EU PROJECT OPENQKD

- **European QKD Testbed Infrastructure**: Sep. 2019 – Aug. 2022
- AIT Coordinator - 38 Partner, 18 M€

- **16 Testbeds and National Demo Sites:** Vienna, Madrid, Berlin, Poznan, Paris, Delft, Cambridge, Athens, Geneva, Padua, etc
- **Initial 32 QKD use-cases (UC):** Critical infrastructure, Telekommunication, Smart Grid, Health services, Cloud Services, Inter-governmental communication, High Performance Computing, Financial Services, etc.
- **Already 17 UC added** by existing and new partners

- More than 30 QKD systems in field deployments
- Free-space und simulation of satellite QKD
- Open calls to attract external partners



OPENQKD eco system

- QKD supplier
- QKD R&D partners
- QKD network developers
- Suppliers of network encryption
- Fiber infrastructure operators
- Telecom operators
- Aerospace and satellite industry
- Standardisation institutes
- Early adopters

OPENQKD OBJECTIVES

- Experimental testing platform
- Cooperation with end-users to demonstrate real world applications
- Demonstrate high maturity of technology, Kick-start European QKD industry
- Standardisation of interfaces
- Pilot for pan-European quantum communication infrastructure

Wide spectrum of partners

- Telco operators
- QKD developers
- Suppliers of classical network equipment (encryption)
- End-users
- Academic groups

USE-CASES IN TESTBEDS

Vienna

- Encryption between governmental agencies
- Academic network backbone
- Inter-government cross border link
- Distributed cloud storage secured by ITS QKD

Poznan

- High Performance Computing
- Healthcare
- e-Government
- Banking
- Police
- Time signal reference distribution

Madrid

- Network security and attestation
- Critical infrastructure protection
- QKD as a cloud service
- Security in e-health services
- Quantum cryptography for B2B & 5G networks
- Self-healed network management

Berlin

- Critical infrastr. protection (telecom network)
- Post Quantum - QKD Hybrid
- QKD key management for Hardware Security Modules
- Modular QKD Network Architectures
- Client, Network and Data Center Applications

QKD enabled ICT security

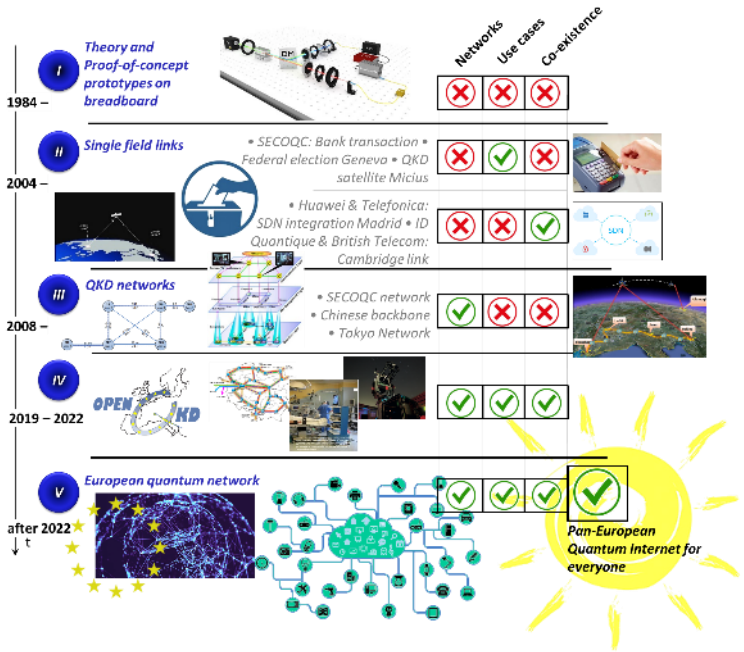
Quantum Key Distribution

- a technology offering security in the quantum age
- so far only isolated demos on technological level
- slow take up and low visibility due to lack of understanding and risk-aversion

Need an integrated approach to

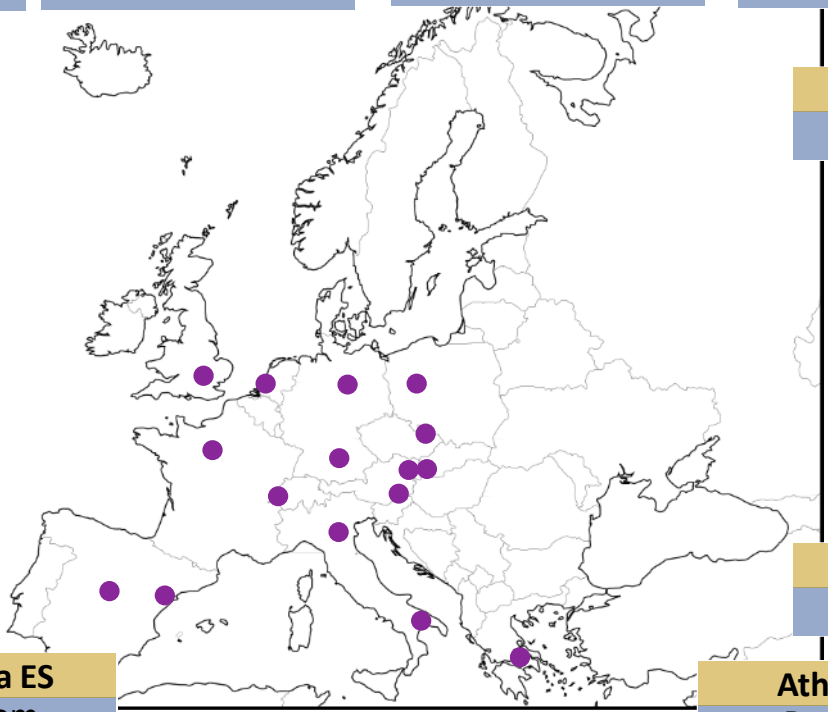
- ✓ Raise awareness of QKD in security applications
- ✓ Demonstrate seamless integration into current networks and security architectures
- ✓ Show the benefit of QKD for a wide range of real world use-cases
- ✓ Involve whole supply chain from manufacturers to end-users
- ✓ Set standards for large scale deployment opportunities

Realised in OPENQKD



16 OPENQKD test sites

Large geographic reach-out



Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

Bratislava CZ
Government

Cambridge UK
Data Centers

Ostrava CZ
High Perf. Comp.

Paris FR
Academic network

Graz AT
Healthcare

Geneva CH
Smart Grid

Padua IT
Free-space QKD

Oberpfaffenhofen DE
Satellite QKD

Matera IT
Satellite QKD

Barcelona ES
Video Com

Athens GR
Data Com

16 OPENQKD test sites

Graz AT
Healthcare

MEDICAL USE CASE IN GRAZ

Use case:

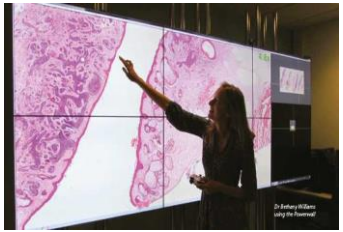
- ❑ Secure storage and retrieval of medical data
- ❑ Secret sharing (data at rest) and QKD (data in transit)

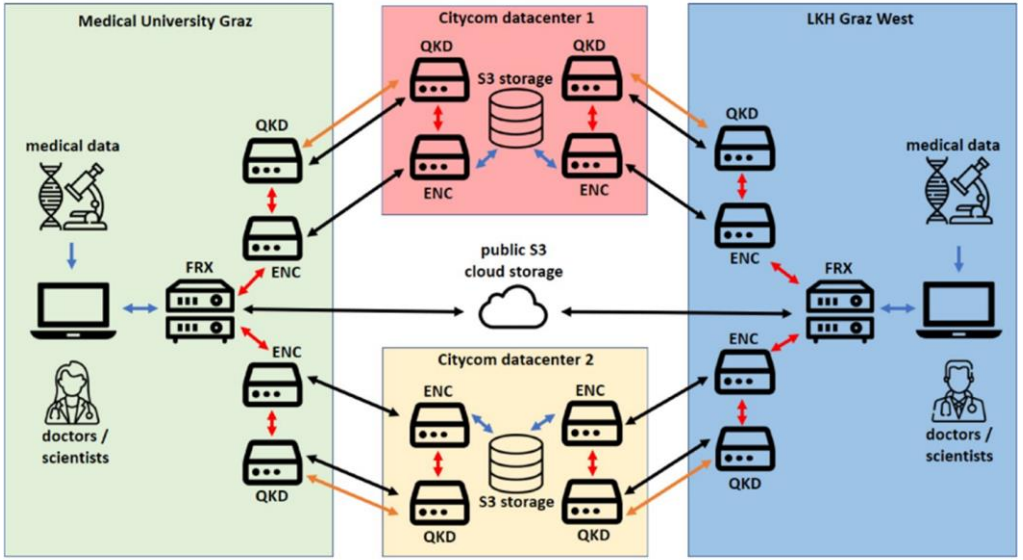
Devices:

- ❑ 4 QKD links (IDQ)
- ❑ 4 pairs of layer-2 encrytors (ADVA)
- ❑ 2 secret sharing devices (fragmentiX)

Fiber infrastructure:

- ❑ 4 fiber links (9 – 20 km) between hospitals and data centers

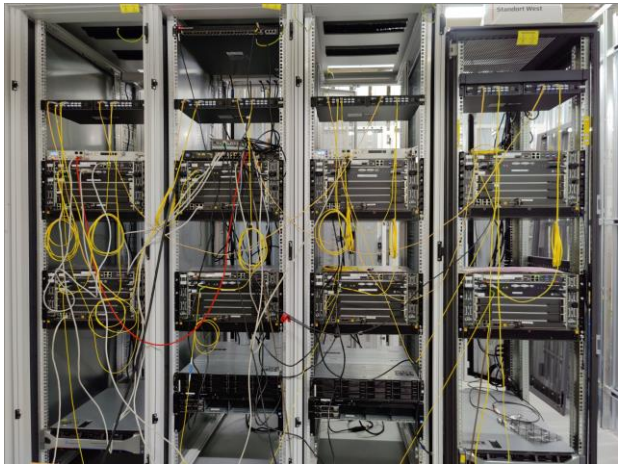




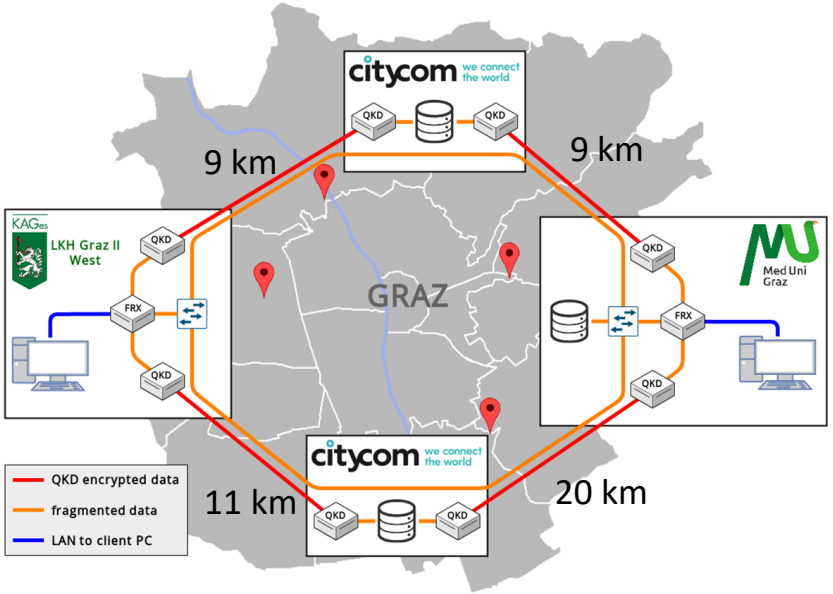
MEDICAL USE CASE IN GRAZ

Deployment started in Graz:

- ❑ Test of 4 QKD links (IDQ) completed under realistic conditions
- ❑ Fiber infrastructure characterized
- ❑ Interface to encryptors (ADVA) implemented

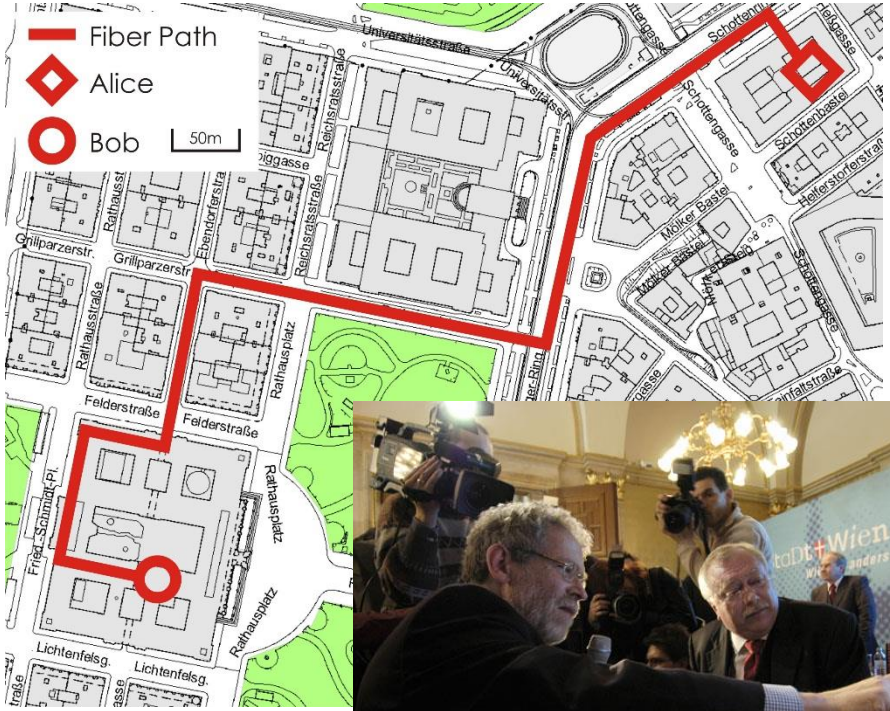


Dry-run of optical network



Geographic layout of network nodes

QKD demonstrations 2004 and 2017



Let’s stay entangled …

Send an email to alice@openqkd.eu or bob@openqkd.eu

Follow us https://twitter.com/openqkd | @openqkd

Connect with us www.linkedin.com/in/openqkd | OPENQKD Project

Find information https://openqkd.eu/ (2nd round of Open Calls in 06.2021)

Thank You!