tnc25
Brighton, UK | 9-13 JUNE 2025
BRIGHTER TOGETHER

Institute of Mathematics and Computer Science
University of Latvia

On Quantum-Secure Layer 3 (IP) and Layer 2 Networking

(and a bit of Layer 4)

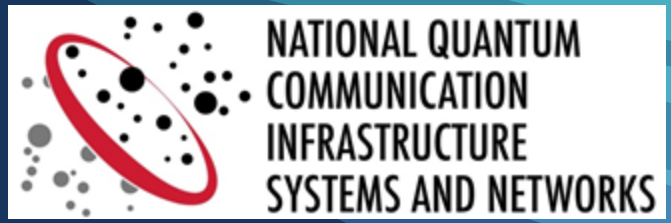
Sergejs Kozlovičs, Rihards Balodis, Ināra Opmane

TNC25 @ Brighton, UK

June 11, 2025

Co-funded by
the European Union

GÉANT



IMCS UL
Institute of Mathematics and Computer Science of University of Latvia

Founded:
1959

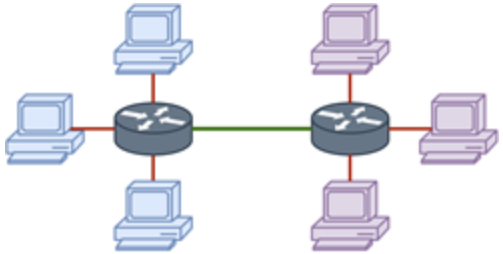
Now:
One of the largest and most influential research institutions in Latvia, EU

Formerly:
The Latvia Computing Center

IMCS UL: Latvian/Baltic/European Internet

1990-ties:

- IMCS UL connects Latvia to the global Internet



August, 1990:
first e-mail via a
modem connection

October, 1992:
Riga-Tallinn permanent link,
2400 bits/second

Before 2000-ties:

- IMCS UL actively cooperated with DANTE and NORDUNET, and partnered with the TEN34 (19 countries) and BaltNet projects

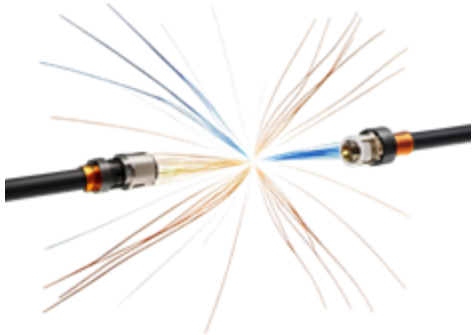
Since 2000-ties:

- IMCS UL has been a partner in all GÉANT projects GN1/2/3/4
  Latnet/Sigmanet (part of IMCS UL) is a long-term GÉANT partner
- IMCS UL is is a partner now (we maintain a GÉANT node)

IMCS UL: Quantum Connections

2019, and 2020-ties:

- IMCS UL introduces the very first quantum communication Channels in Latvia



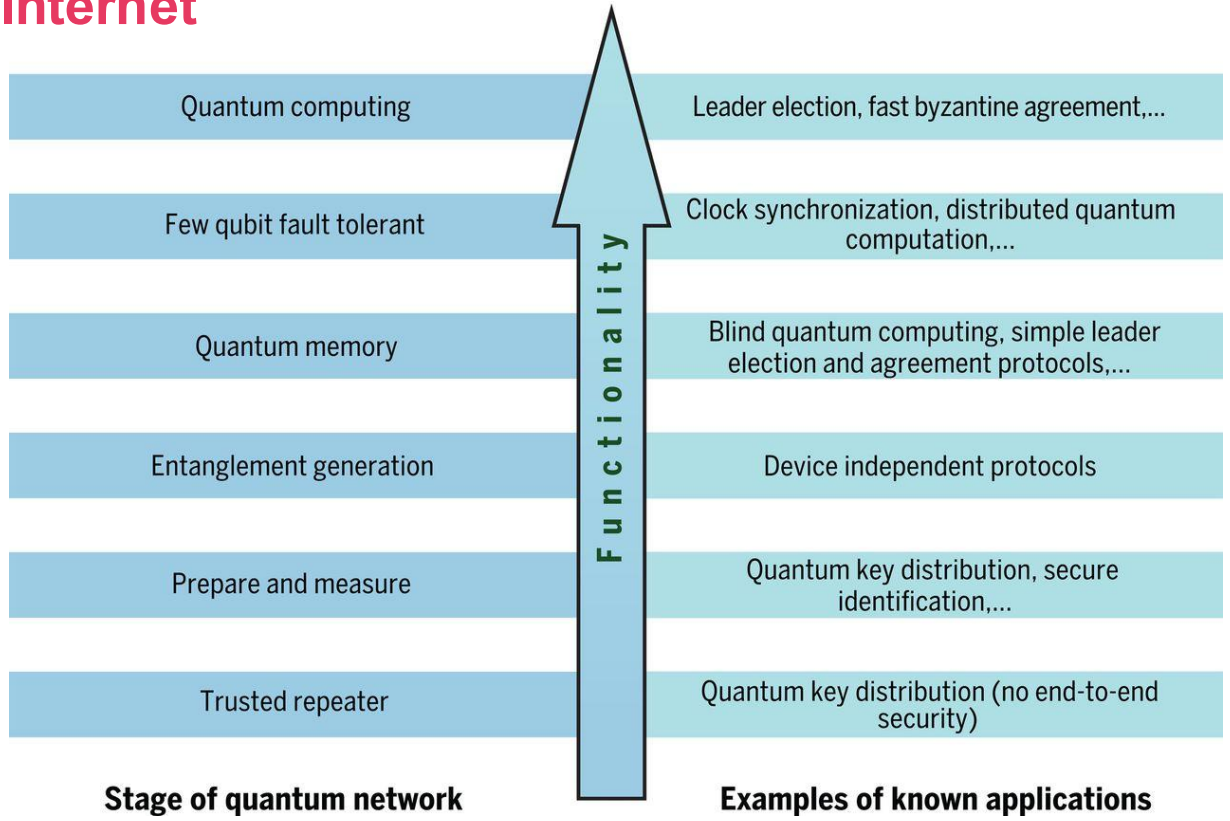
2019:
the first in-lab quantum link

2021:
the first metropolitan-scale link in Riga (33km), with partners

Since 2023:

- Conventional telecommunications industry partners (LVRTC, TET, ECO) turn towards quantum communications

Towards the Quantum Internet

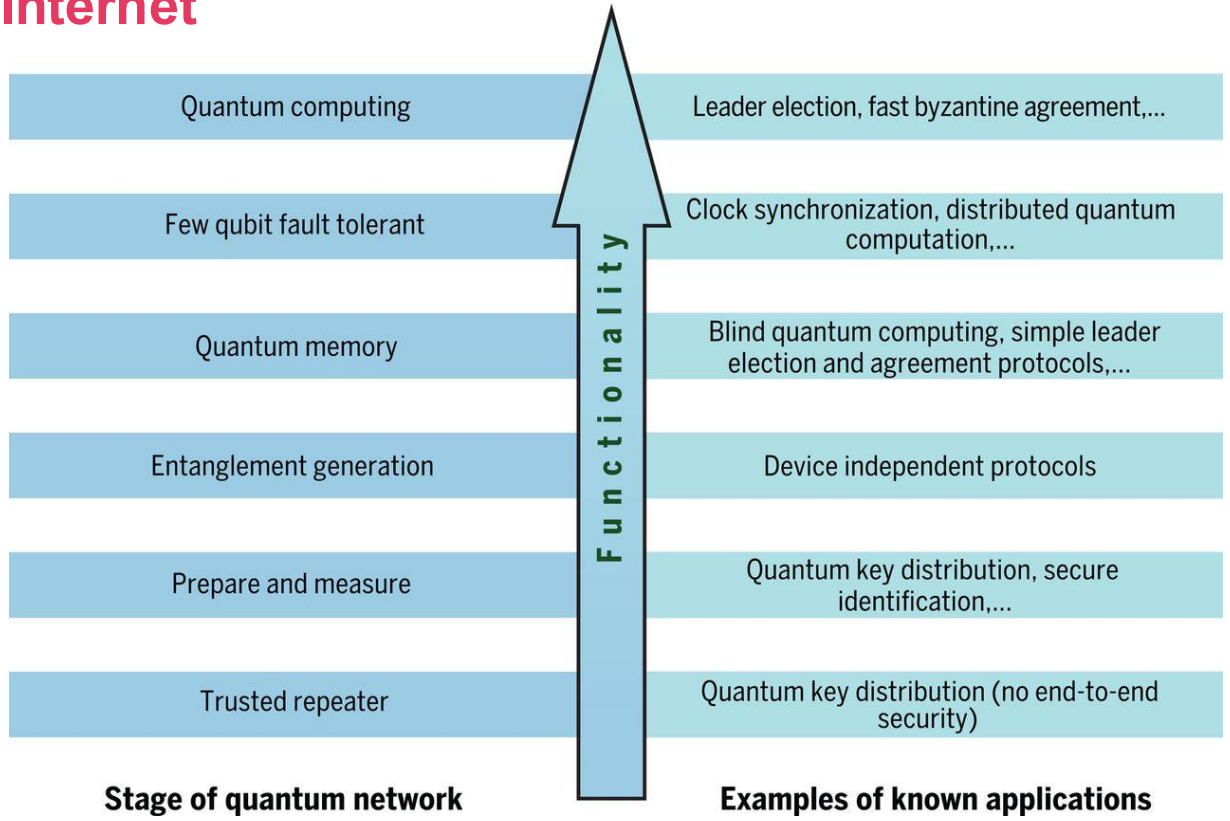


Stephanie Wehner *et al.* Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018)

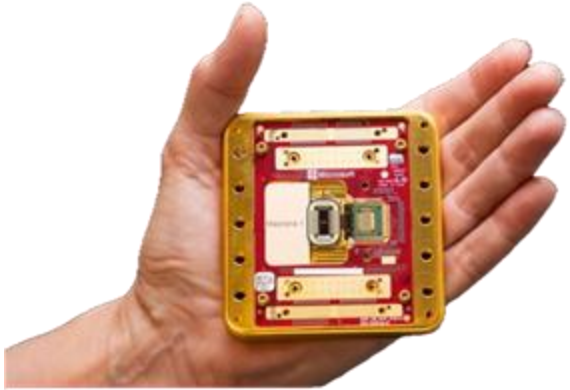
Towards the Quantum Internet

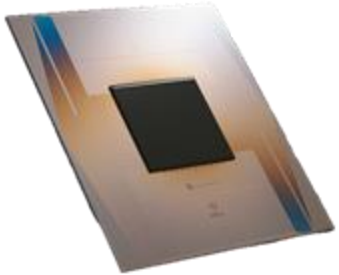
The Quantum Internet can wait
(entanglement distribution, distributed quantum computing...)

Quantum-secure key exchange cannot wait!



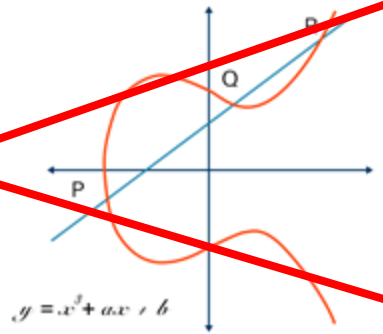
The Quantum Threat





TLS 1.3 and below

TLS



ECC,
RSA,
...

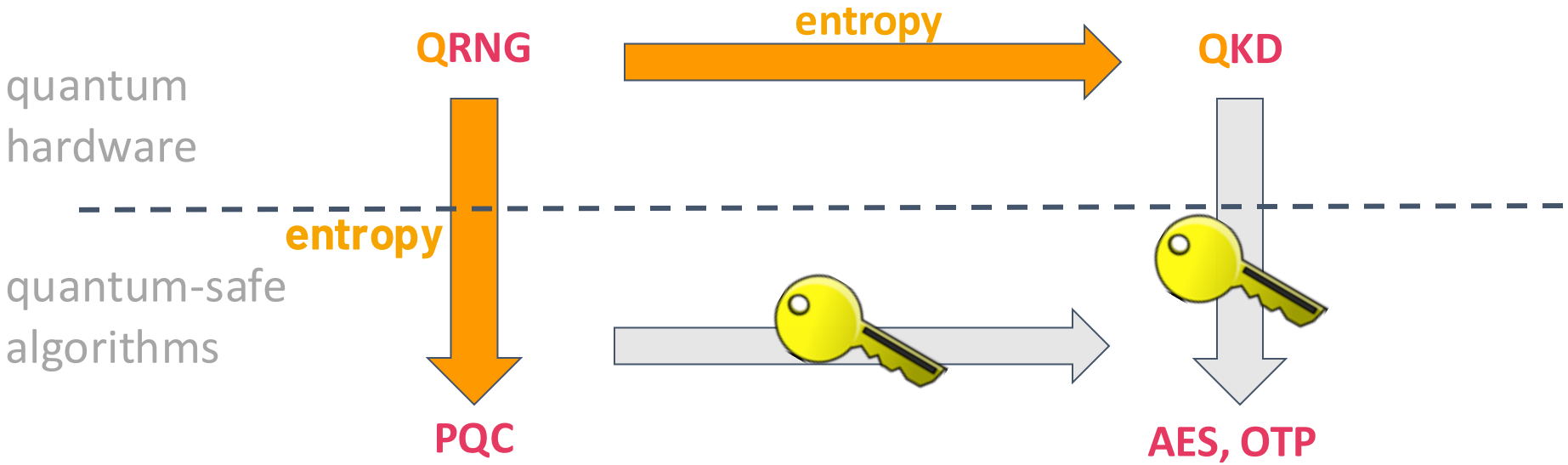
Harvest Now, Decrypt Later

Most quantum-vulnerable algorithms should be:

- deprecated by 2030 and
- disallowed by 2035.

[NIST Internal Report, NIST IR 8547, “Transition to Post-Quantum Cryptography Standards”]

Our Motto: Fight Quantum with Quantum!



considered quantum-safe
(believed to be hard problems for the quantum computer)

considered quantum-safe
(AES: limited speedup by Grover's search; OTP is information-theoretically secure)

QRNGs: Quantum Random Number Generators

Each **QKD** device must have one.

QRNGs are essential for **PQC** algorithms:

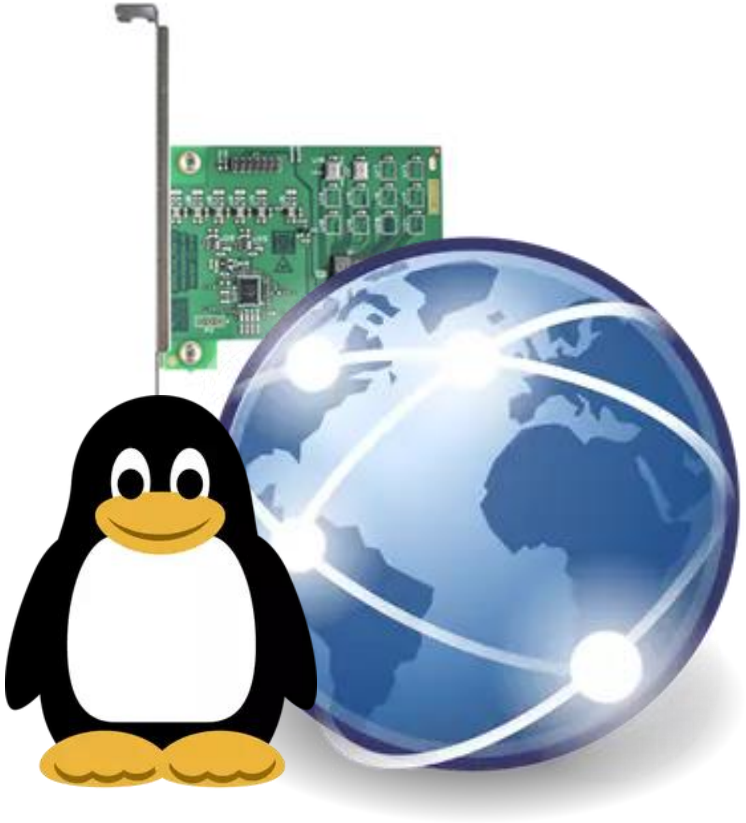
- uniform bitstring sampling
- nonces
- seeds
- salt...

Quantum Random Number Generators utilize **inherently random** quantum processes (nuclear decay, photon behaviour, quantum vacuum fluctuations)

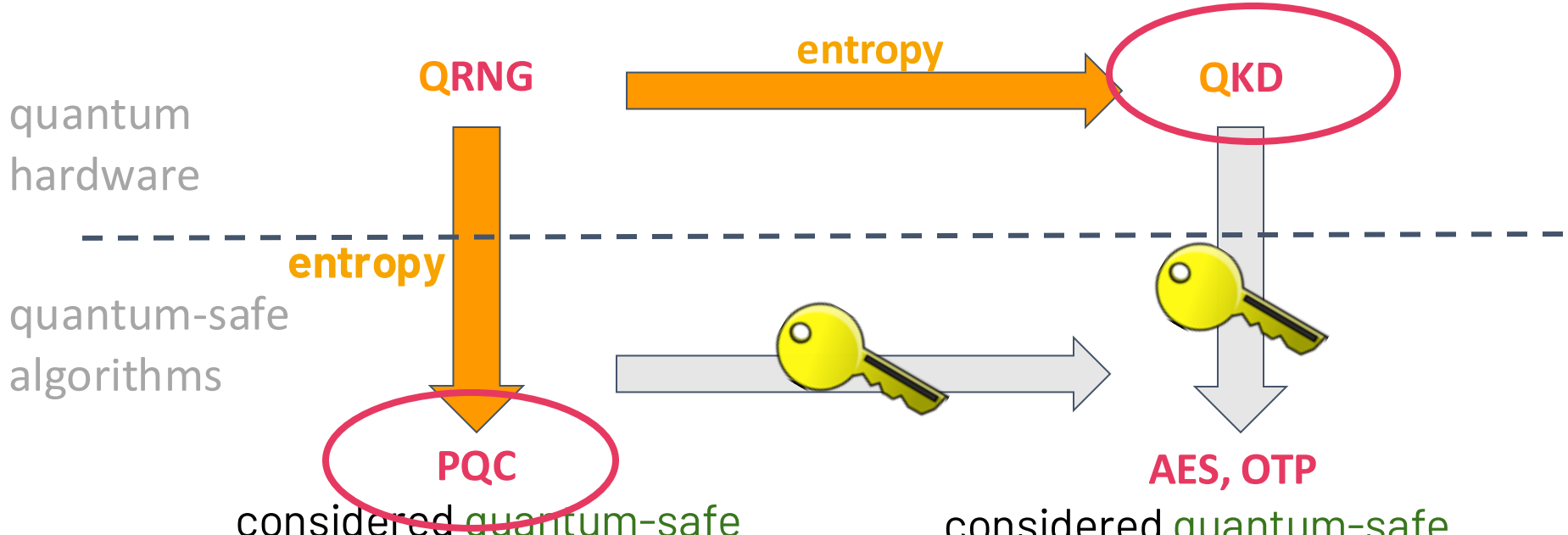
Our QRNG as a Service

We developed:

- QNRG as a Service (qrng.lumii.lv), 2022
  the first QRNG service secured with PQC
- Linux kernel module (/dev/qrandom0 simulation)
- Windows DLL with Detours (non-open-source)
- D-Bus QRNG service
- OpenSSL3 provider



Our Motto: Fight Quantum with Quantum!



considered quantum-safe
(believed to be hard problems for the quantum computer)

considered quantum-safe
(AES: limited speedup by Grover's search; OTP is information-theoretically secure)

QKD vs. PQC

QKD	PQC
Perfect Forward Secrecy	**Vulnerabilities can be found** in the future Have to withstand the test of time
Information-Theoretically Secure	**Not Information-Theoretically Secure**
Non-breakable unless Quantum Mechanics are false	**Believed** to be quantum-safe Breakable with unlimited computational power
Expensive: devices *and* infrastructure needed	Operates on **existing Internet infrastructure**
Difficult to configure and maintain	**Integrates** well into existing software and **Public Key Infrastructure (PKI)**
No authentication	Provides **Authentication** and Encryption (AE)

The Four-Wheel Drive Engine Model (Hybrid!)

GÉANT + QKD: The Problem

Infinera DTN-X optical equipment over dark fibre

- **Dark fibre** is good for quantumness!

But: Optical Transport Network (OTN) switching…

- Optical **routing/switching is a problem**,
  since we cannot copy an unknown quantum state

GÉANT + QKD: The IDEA!

QKD as a Service

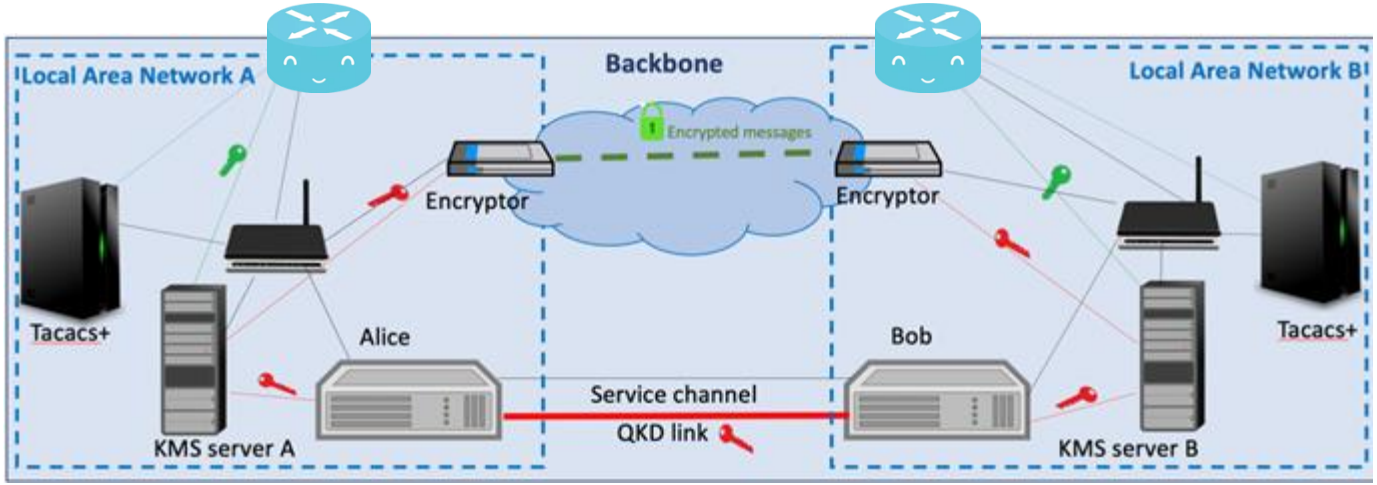
“WP6 Task 1 is currently reviewing network support requirements for Quantum Technology and quantum key distribution/exchange (**QKD/QKE**) technology in order to consider its applicability **as a service** for use by the GÉANT community.”

[NETDEV: https://wiki.geant.org/display/NETDEV/QT]

Our Solution #1: the Backbone

Replace your cable with our backbone!

We offer a network segment (trunk) secured with quantum keys.

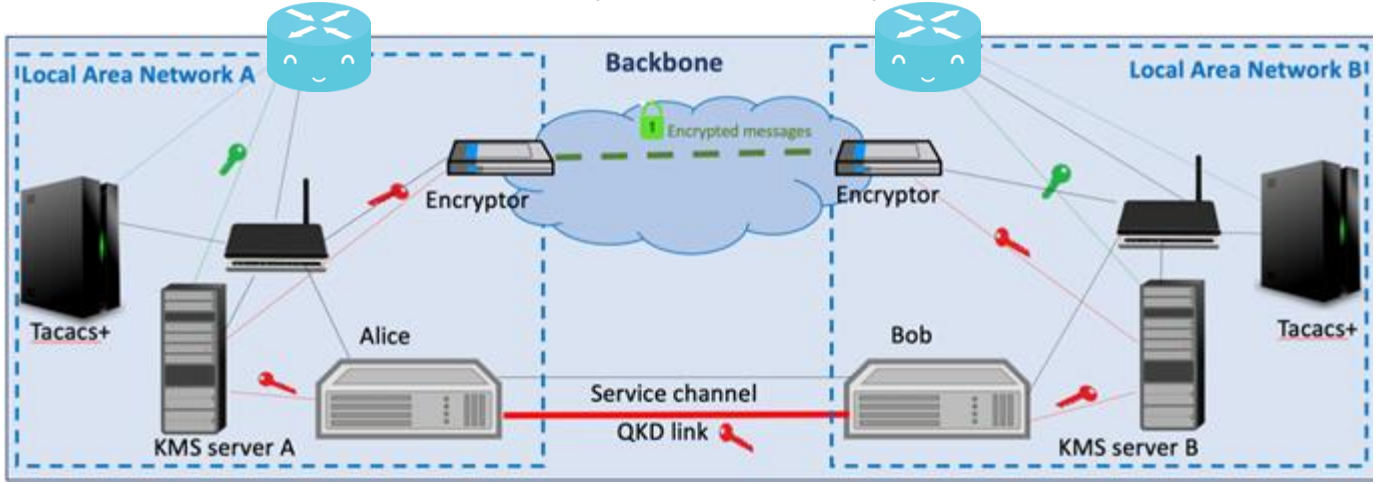


Our Solution #1: the Backbone

Can be implemented via:

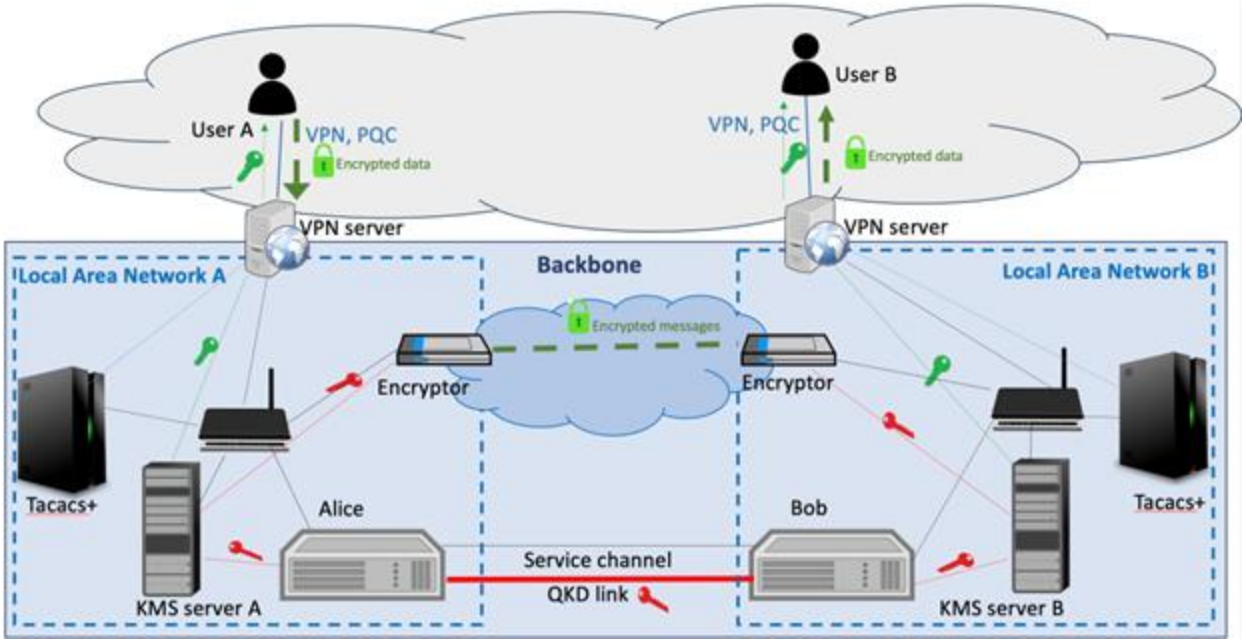
- L2 encryptors with QKD support (Centauris)
- L3 routers/firewalls with QKD support (Cisco, Juniper)

certified devices!
preferrably, with PQC support



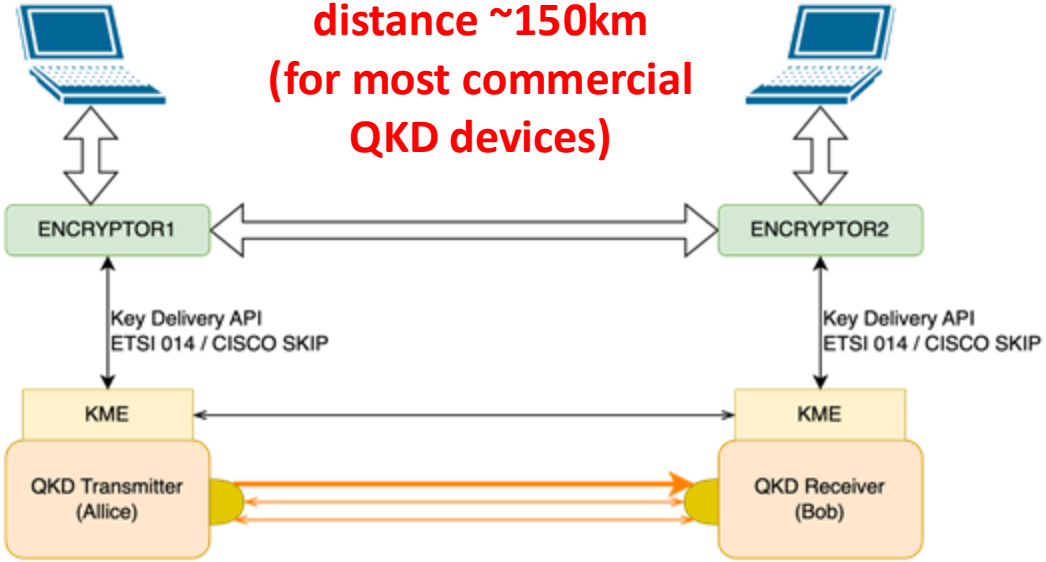
Our Solution #2: Access via PQC VPN

L2/L3 VPN:
classical
and PQC

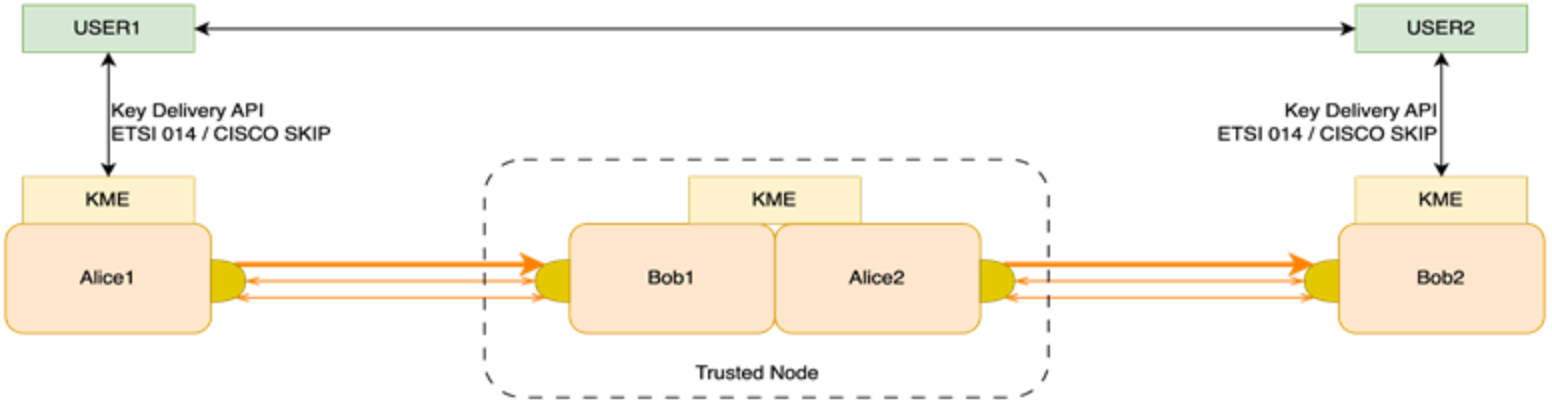


One More Problem, Sorry ☹

PROBLEM:
distance ~150km
(for most commercial QKD devices)



Trusted Nodes



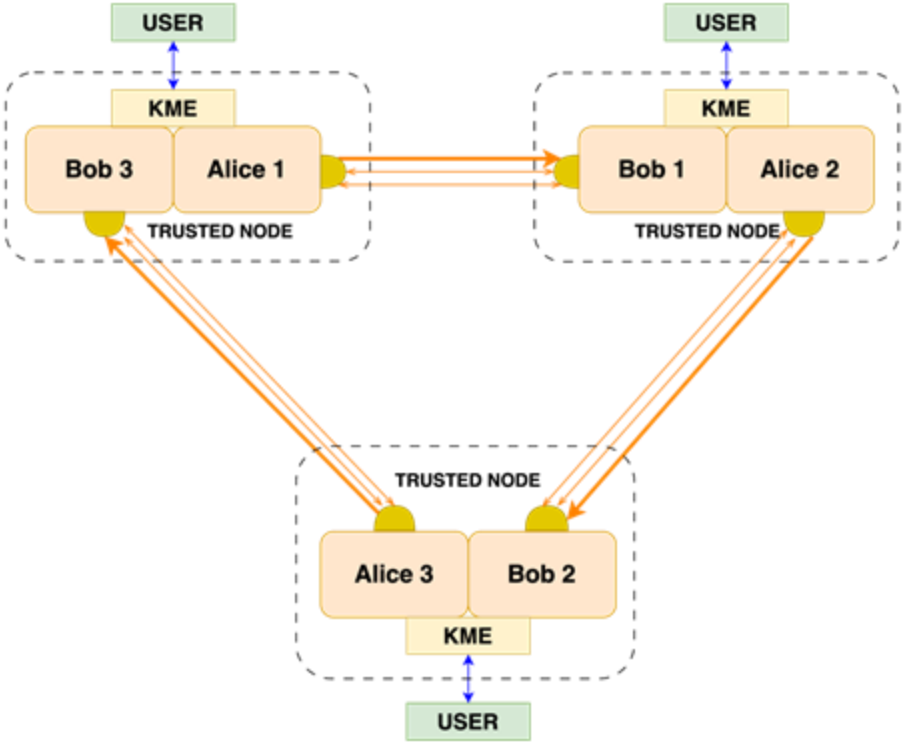
Complex Topologies

In the LatQN project, we are implementing the "triangle" topology between different partners in Latvia

=> latqn.eu

(part of EuroQCI)

- **Key Relay** algorithms are needed
- We have to **sacrifice some QKD keys** for that (a precious resource!)



The research is supported by the European Union, project No. 101091559 "Development of experimental quantum communication infrastructure in Latvia (LATQN)".

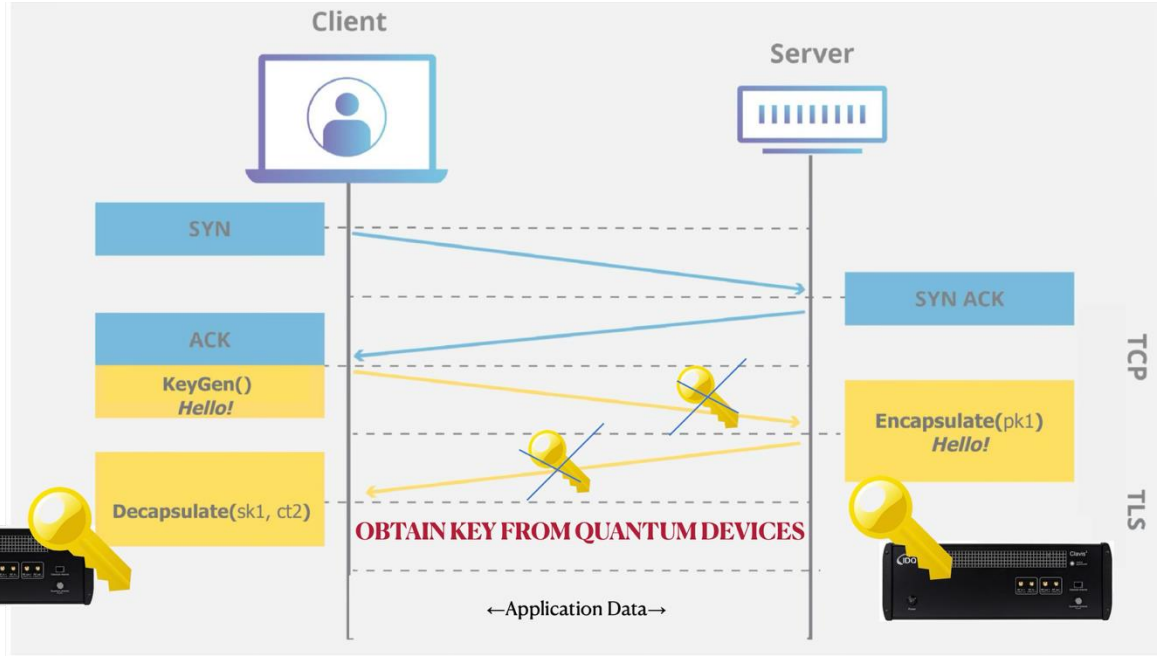
EuroQCI =
European
QKD "Internet"


How to provide QKD as a Service for end users without L2/L3 hardware or VPN software?

Our Solution #3: TLS (Layer 4) Integration

We developed a library (Java and native) that implements TLSv1.3 secured with quantum keys

- We replace TLS Key Exchange with an abstract Key Encapsulation Mechanism, KEM (like in PQC)
- “Quantum KEM” does not exchange keys but obtains them from quantum devices



Our Solution #3: TLS (Layer 4) Integration

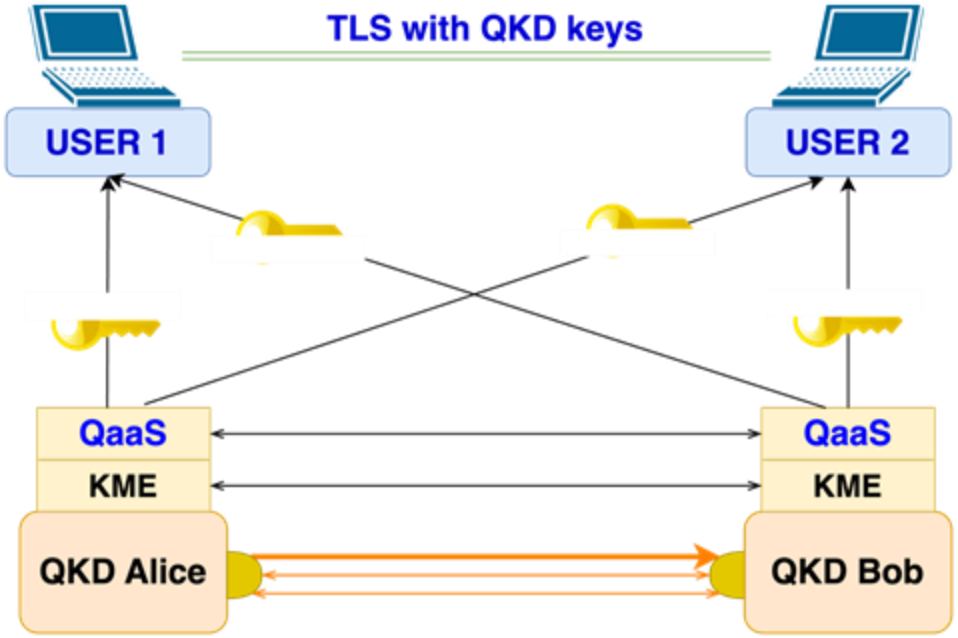
“Quantum KEM” implementations:

- Direct ETSI QKD GS 014
- Direct CISCO SKIP
- Our original double-secure Butterfly Protocol

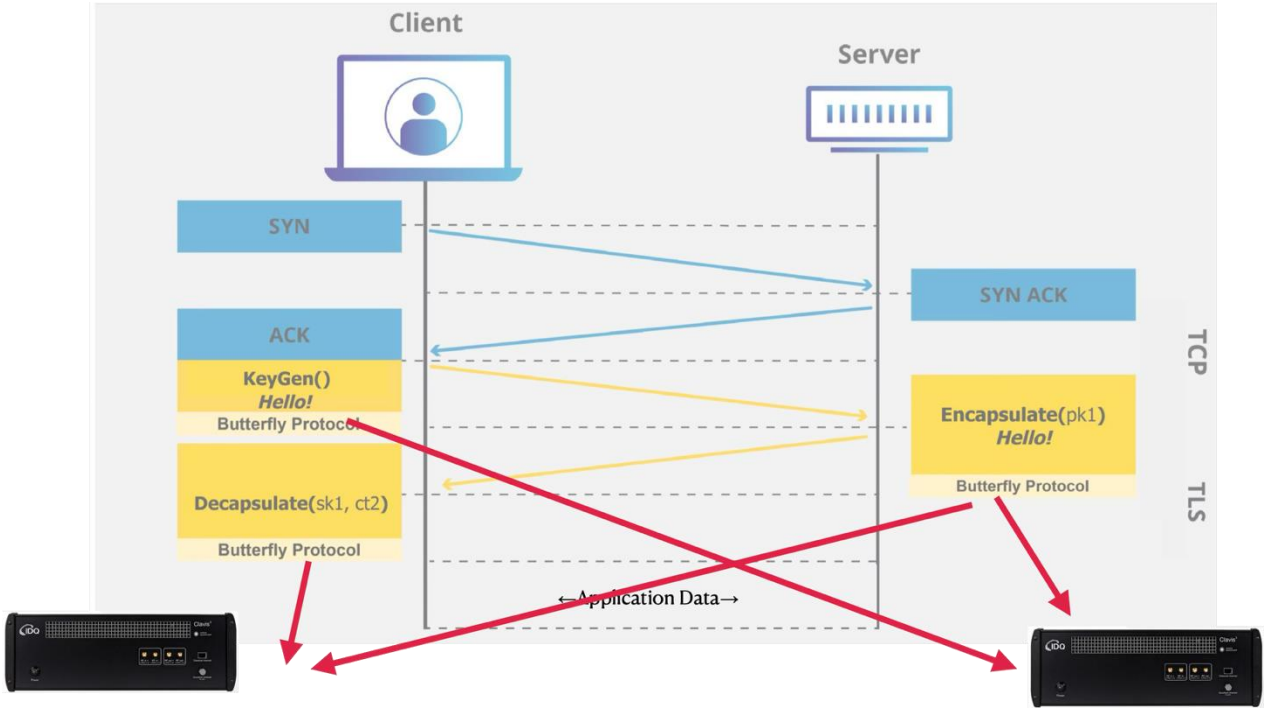
Our Double-Secure Butterfly Protocol

qkd.lumii.lv

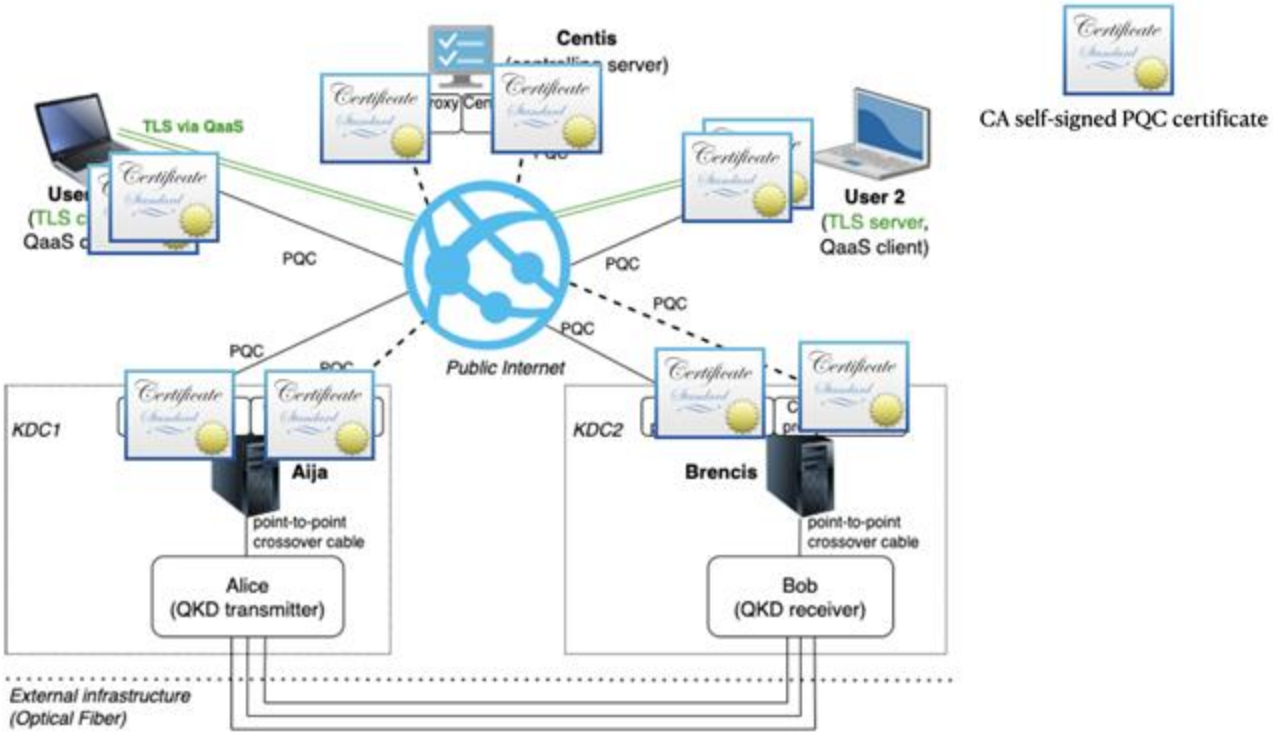
QKD as a Service via our Butterfly Protocol with TLSv1.3 integration



Butterfly Protocol as KEM in TLSv1.3



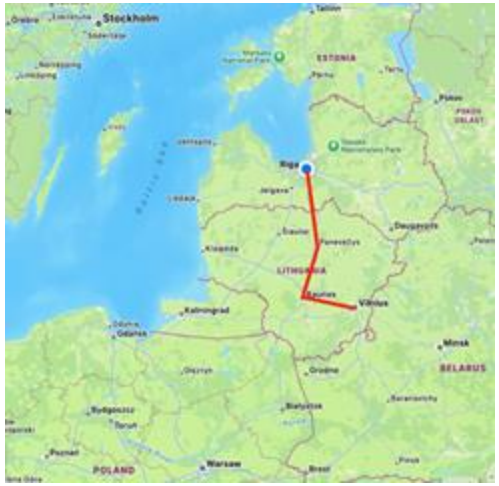
Please do not take technology for granted!



Further Projects

Lat-LitQN:

- Riga (LV) - Kaunas (LT) - Vilnius (LT)
- with the ability to connect to Poland



Quantum Shield for Data:

- Quantum-Secure Access to the Cloud
- Quantum-Secure Backups for Data

Satellite QKD?

Satellites could help establish long-distance QKD without the need for trusted nodes.

Entanglement-based protocols can be utilised (although quantum memory is required in some cases).

We and the satellites:

- During 1997-1999, IMCS UL operated an international satellite channel between IMCS UL (LV) and Crawford Communications (US)
- During the Lat-LitQN project, we are going to do research on QKD via satellites

Huttner, B., Alléaume, R., Diamanti, E. *et al*. **Long-range QKD without trusted nodes is not possible with current technology.** *npj Quantum Inf* 8, 108 (2022). https://doi.org/10.1038/s41534-022-00613-4

Thank you

Any questions?

sergejs.kozlovics@lumii.lv

imcs@lumii.lv

Co-funded by the European Union