EuroQCI : vers une infrastructure de communication quantique sécurisée en Europe

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

Paris Centre for Quantum Technologies

Sécurité numérique à l'ère quantique : opportunités et défis

Programme de Transfert au Campus Cyber

25 juin 2024

Quantum communication

Quantum communication is the art of transferring quantum information between distant locations

Encoding on properties of quantum states of light
Propagation in optical fibre or free-space channels
Information processing in network nodes (processors, sensors, memories)

Security
Untrusted network users, devices, nodes

Efficiency
Optimal use of communication resources

Applications
Demonstrate provable quantum advantage in security and efficiency for communication and information processing tasks

Quantum network stages and applications

QKD, coin flipping, digital signatures

Secret sharing, device independence, anonymous communication

Quantum money, secure multiparty computing, election, agreement

Blind, distributed quantum computing and sensing

Mature technology

Early commercial systems

Proof-of-principle

Trusted nodes and switching

Entanglement distribution

Quantum memories

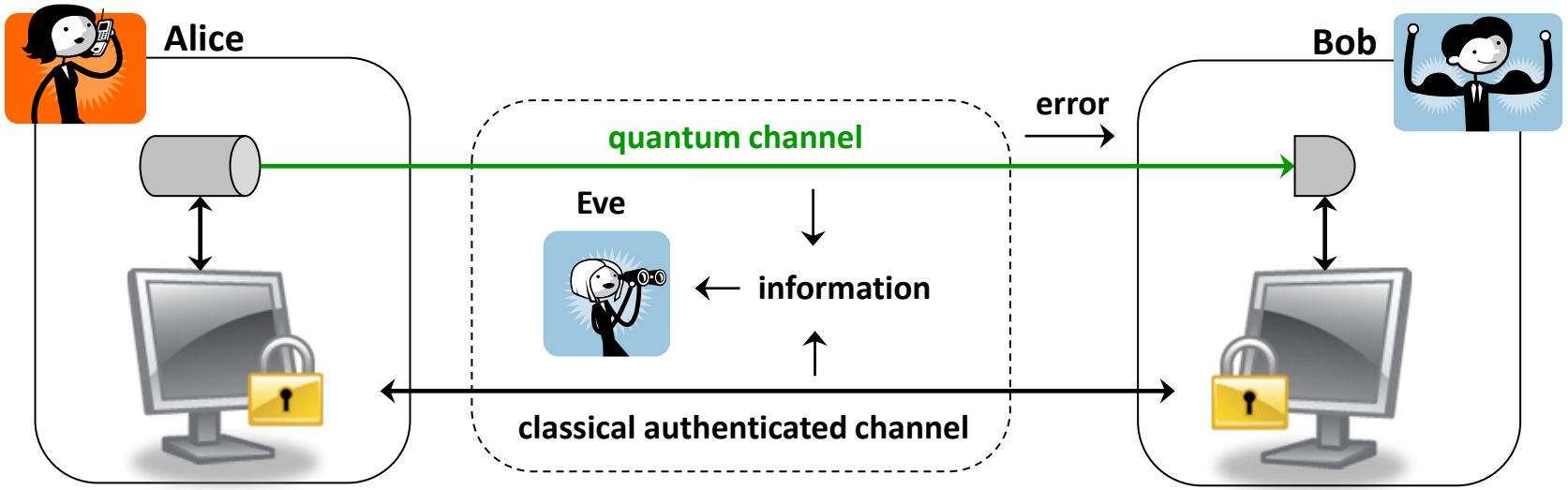
Quantum processors

Present

Time

Quantum-safe cryptography

Thanks to the fundamental principles of quantum physics (no cloning theorem, superposition, entanglement and nonlocality), it is possible to detect eavesdropping on the communication link

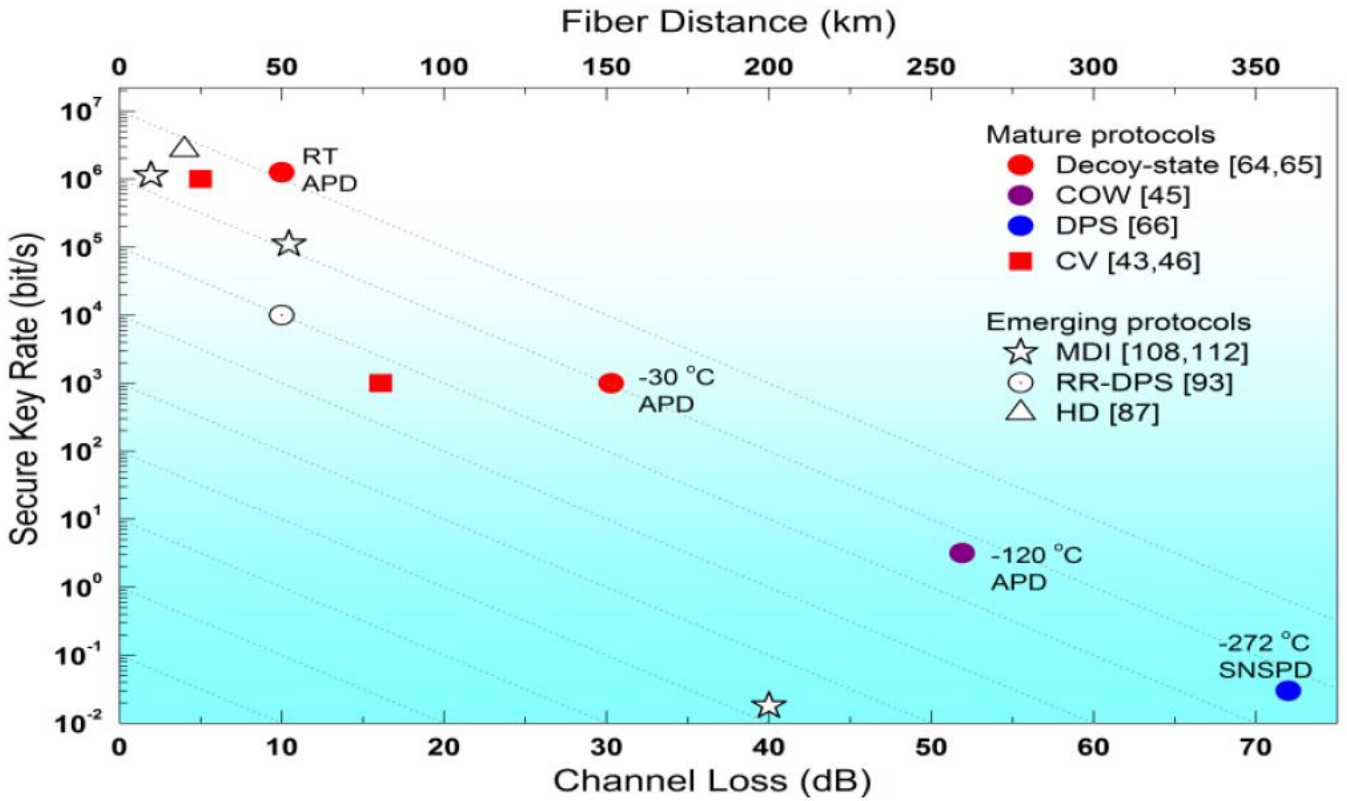


Authentication	Key agreement	Message encryption
e.g. with pre-shared keys, post-quantum or ITS digital signatures	e.g. with post-quantum or **QKD** (ITS) replacing vulnerable asymmetric algorithms	e.g. with AES or one-time pad (ITS)

Hybrid QKD and computational (post-quantum) schemes offer practical security-in-depth and advantage with respect to key dependency

QED-C publication: QKD: Part of a Defense-in-Depth Security Strategy, May 2024

QKD in practice



Performance of point-to-point, prepare-and-measure fibre-optic QKD systems

ED *et al.*, npj Quantum Information 2016

Fundamental limits in rate and range
Quantum signals cannot be amplified without noise

Security definition: $\frac{1}{2}\left\|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\right\|_1 \leq \varepsilon$ for any $\rho_{A^n B^n E}$

Towards device independence: If Alice and Bob share nonlocal correlations less assumptions on devices

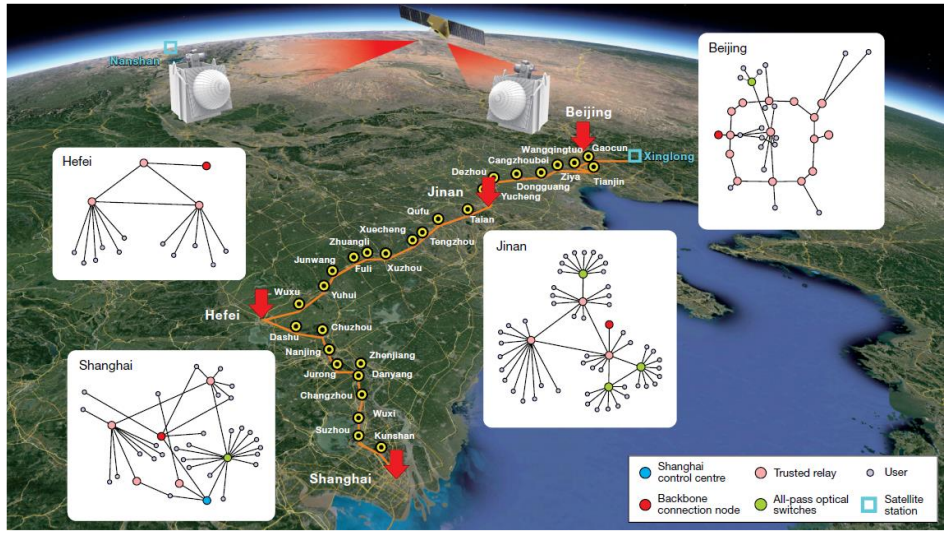
Practical security: Deviation from security proof may lead to side-channel attacks

BSI report: Implementation attacks against QKD systems, November 2023

Trusted-node networks

To counter inherent range limitation due to optical fiber loss → terrestrial and satellite-based networks

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



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

Mesh type networks with point-to-point links using currently available technology

SECOQC QKD network, 2008
Swiss Quantum Network, 2011
Tokyo QKD network, 2015
China integrated terrestrial-satellite network

If the distance between Alice and Bob exceeds the range of the system:

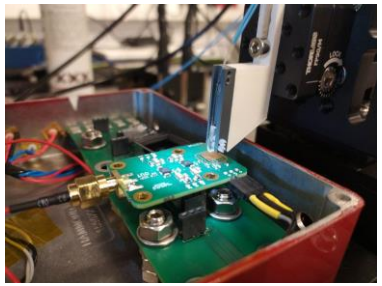
Alice-R: key1, R-Bob: key2, R: key1⊕key2 → Bob: key2⊕(key1⊕key2) = key1

Quantum secure network technology targets

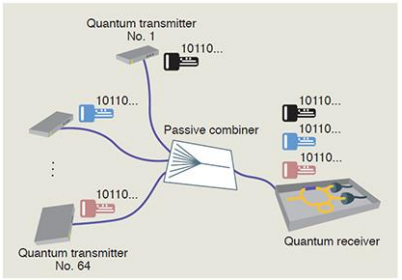
QKD offers a fundamental functionality and has a pilot role in the TRL ladder for quantum communication networks

Demonstrate that it can work

at large scale
cost-effective & small form factor

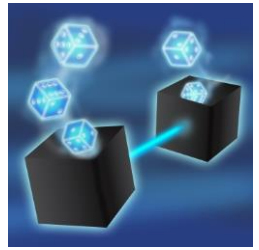


over real-world networks
coexistence and key management



for real-world security
QKD+PQC & hardware evaluation

with minimal trust assumptions
(semi) device independence



Demonstrate compelling functionalities beyond QKD with provable quantum advantage

Secure multi-party computation

Long-term secure storage

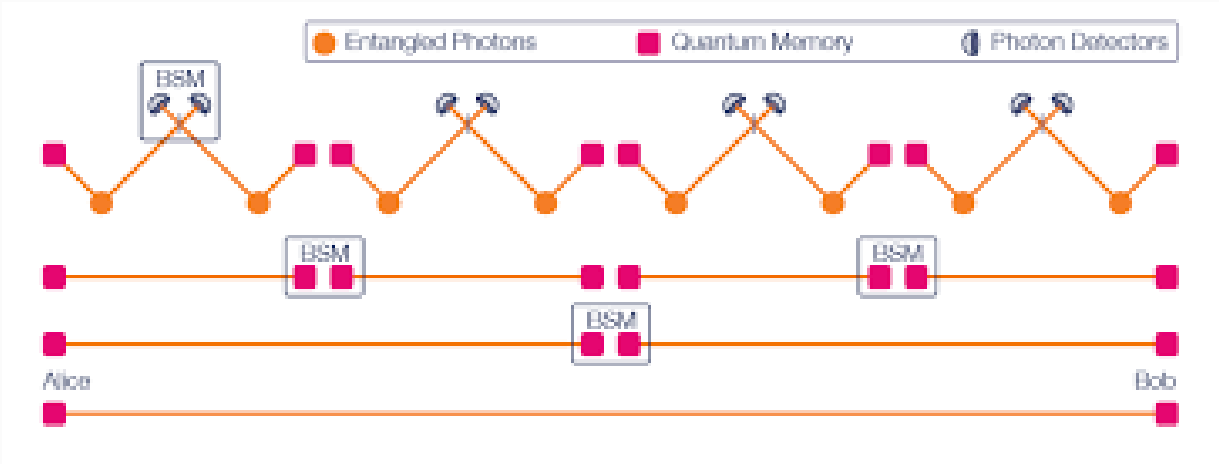
Unforgeable quantum cryptograms

Secure distributed quantum metrology and sensing

Entanglement-based networks

Create efficiently end-to-end entangled resources with quantum repeaters and quantum memories

Fundamental for interconnecting devices via teleportation over long distances, **alleviate need for trust in intermediate nodes**



Technological challenges despite significant progress

→ trade-offs in critical benchmarks (efficiency, storage time), entanglement rate, range,…

→ development of network architecture for the quantum internet

QUANTUM INTERNET ALLIANCE

FRANCE 2030

Target performance with multiplexing techniques: **repeater link with 50 bit/s over 50 km, >97% fidelity**

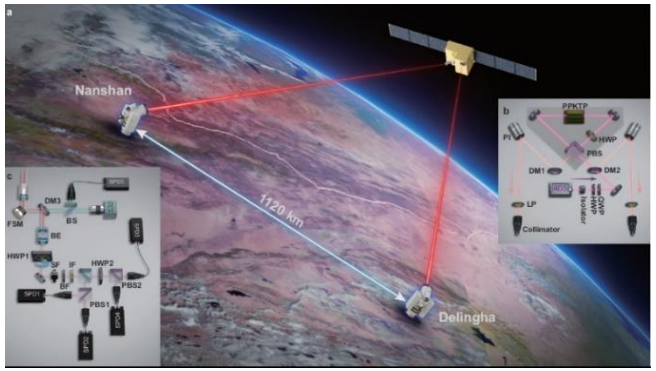
Full network stack for target use cases in server-client scenario

Satellite quantum communication

They alleviate the need for long chains of trusted nodes or quantum repeaters
Terrestrial and space networks work together and can be fallback options

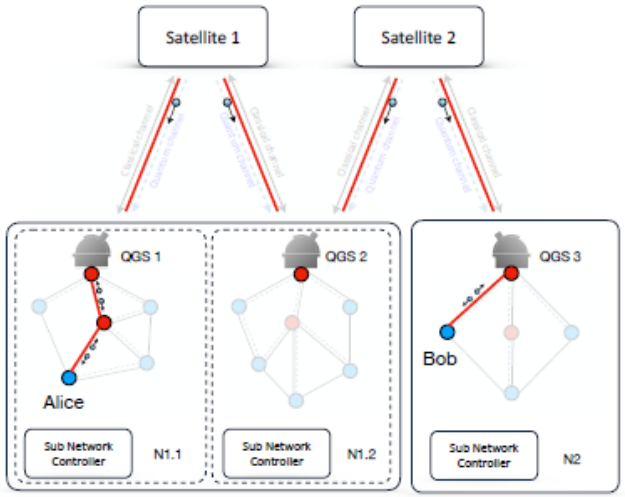
Micius: first satellite equipped with quantum technologies

- ✓ 1200 km down-link QKD
- ✓ Videoconferencing across the globe in trusted node satellite model
- ✓ Up-link quantum teleportation
- ✓ Entanglement-based QKD over 1120 km



J. Yin *et al.*, Nature 2020

First European quantum satellites planned for 2026



L. de Forges de Parny *et al.*, **Satellite-based Quantum Information Networks: Use cases, Architecture, and Roadmap**, Commun. Phys. 2023

Trade-offs between losses, divergence, pointing, telescope size, atmospheric turbulence, adaptive optics, visibility time, detector efficiency,…

Large-scale deployment efforts

QUANTUM

QSN PARTNERSHIP — Resources and applications for quantum secure networks

QIA QUANTUM INTERNET ALLIANCE — Enabling the quantum internet

Boost production facilities in Europe
Design satellite payloads
Support fundamental research

Technological capabilities →

← Deployment possibilities

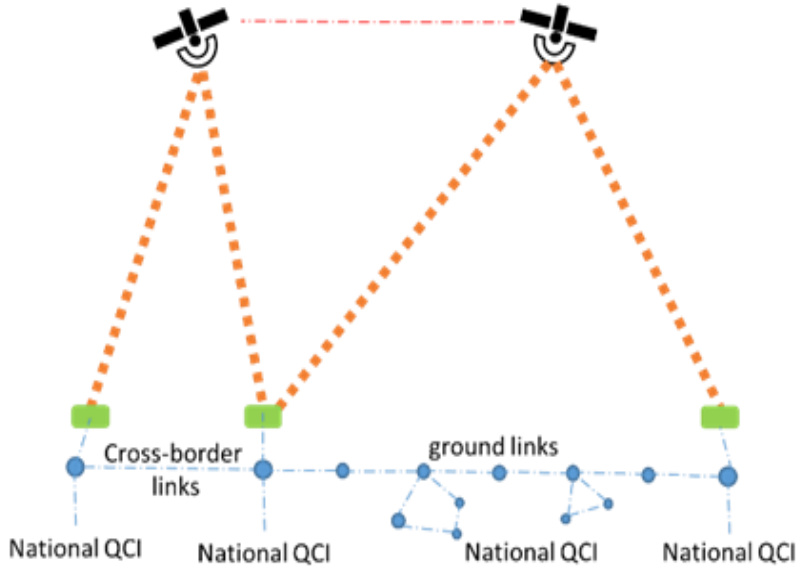
EuroQCI

Architecture studies
Industrial QKD systems
National deployments in all MS
Testing and validation
Cross-border links
Eagle-1 & SAGA satellite programmes

An operational integrated satellite and terrestrial system spanning the whole EU for ultra-secure exchange of cryptographic keys

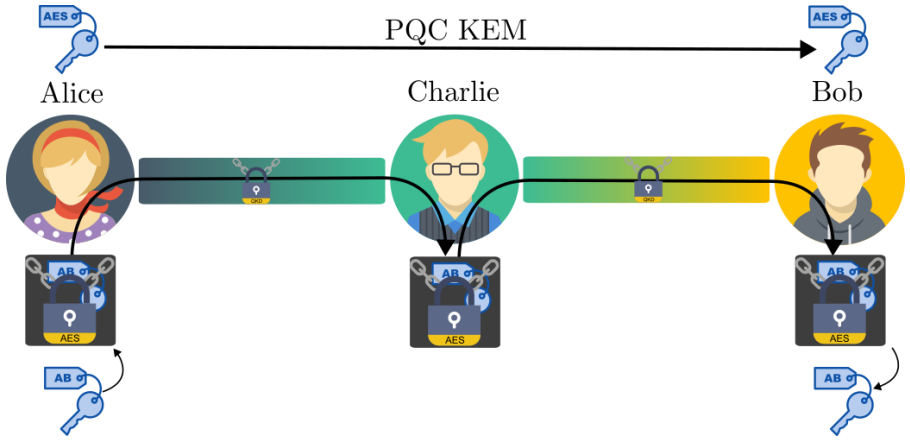
Integrated into IRIS², the EU Secure Connectivity Programme

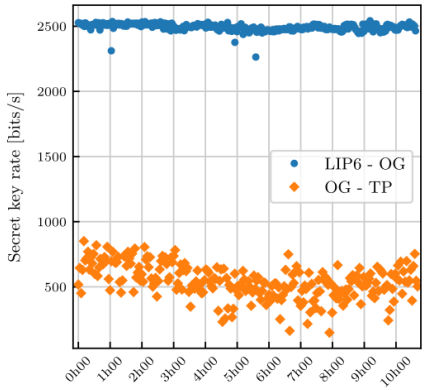
China → trusted nodes, integration with PQC, satellite-terrestrial link integration
South Korea → governmental services
US → entanglement distribution
UK → dynamic network routing, advanced functionalities
Japan, Singapore, Canada,…

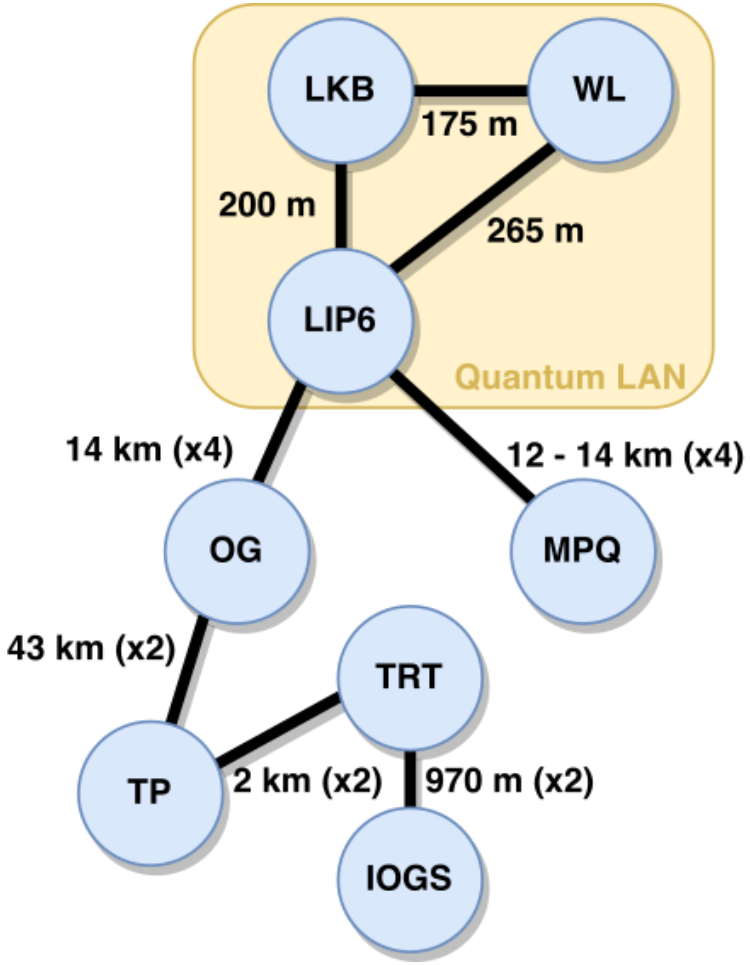


Paris testbed deployment and FranceQCI

Benchmarking with commercial systems
Efficient PQC-secured trusted-node QKD exchange







Deployment of CV-QKD prototype

exail

Entanglement distribution

Deployment of quantum memory link
Neutral atom technology with record high storage-and-retrieval efficiency

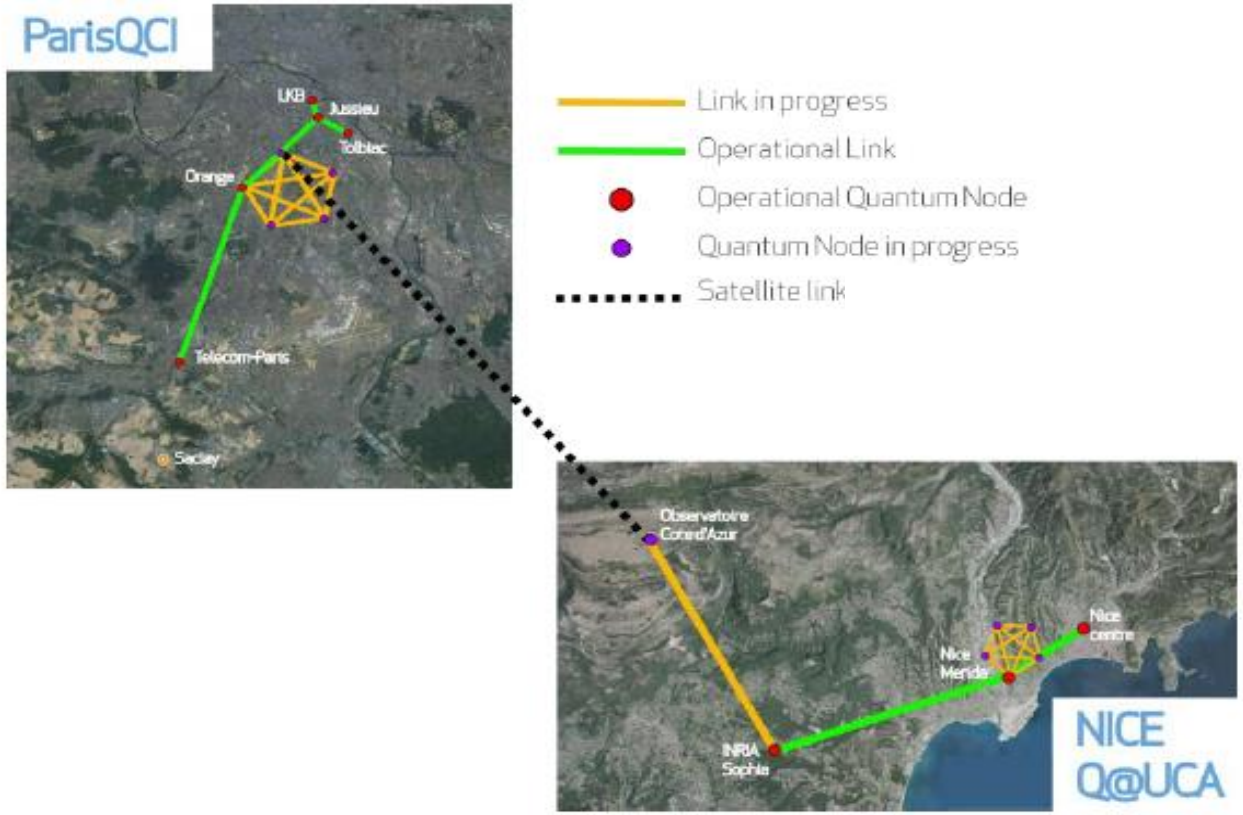
Welinq

Long term secure storage with QKD

VeriQloud

Y. Piétri *et al.*, QCrypt 2024

Paris testbed deployment and FranceQCI



Interface of Nice testbed with Optical Ground Station of the Côte d'Azur Observatory

Key takeaways

Significant progress in recent years

High-TRL QKD systems deployed in moderate-scale testbeds all over the world with strong security assumptions (trusted end users, mostly trusted intermediate nodes)

Milestone satellite quantum communication experiments

Low-TRL implementations of other quantum cryptographic functionalities

Low-TRL quantum memory devices and elementary repeater links

What are the next barriers to overcome for scale up and wide use in global quantum networks?

Relax security assumptions on users and nodes

Enhance performance and increase TRL while also providing agility and versatility in large-scale testbeds

Integrate with computational (post-quantum) cryptography and standard networks

Enrich functionalities with demonstrated quantum advantage

Certification and standardization across all quantum technology pillars

Thank you!