Communications Quantiques

10 Mars 2022 – Journées Partenaires Entreprise

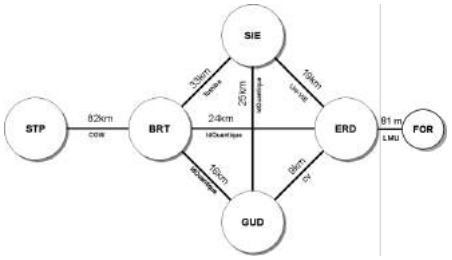
Romain Alléaume
Télécom Paris – Institut Polytechnique de Paris

romain.alleaume@telecom-paris.fr

Telecom Paris at the forefront of R&D in Quantum Key Distribution, over the past 15 years

First European QKD network (Vienna, 2008)

SECOQC



INSTITUT d'OPTIQUE GRADUATE SCHOOL

cnrs

THALES

TELECOM ParisTech

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

CV-QKD Technology

Record distance of 100 km (2012)

First Commercial System (SeQureNet)

Collaborative projects with key actors (2008-2017)

ANR

Network and Cryptography (FREQUENCY)

Implementation Sec, Q hacking (Q-CERT, ETSI)

Multiplexing (Quantum WDM)

Quantum Networks (QCALL)

AIT Austrian Institute of Technology

TOSHIBA Leading Innovation

IDQ

University of Cambridge

University of Waterloo | IQC Institute for Quantum Computing

清華大學 Tsinghua University

NICT 情報通信研究機構 National Institute of Information and Communications Technology

TELECOM Paris

Telecom Paris, (IQA+GTO) partner of 2 projects from the Quantum Technology Flagship, since 2018

Continuous Variable Quantum Communication

European Quantum Technology Flagship Project: 2018-2021

21 Partners, 3 years, 10 M€ budget

Q Comm R&D, Telecom Manufacturers, Network Operators

OPENQKD

European QKD Testbed

European Quantum Technology Flagship Project: 2019-2022

38 Partners, 3 years, 15 M€ budget

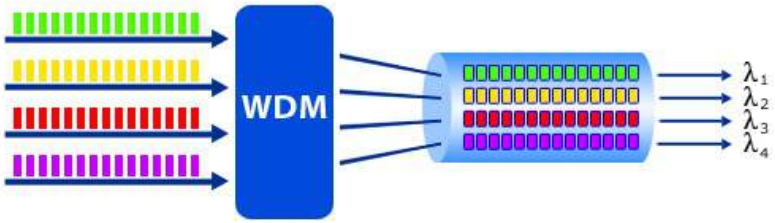
QKD and Encryption Suppliers, Telecom and Aeorospace industry, Standardization bodies, QKD and Network R&D, Early Adopters

➔ 16 Test Sites **(incl. Paris)** Use-case demonstrations, Standards

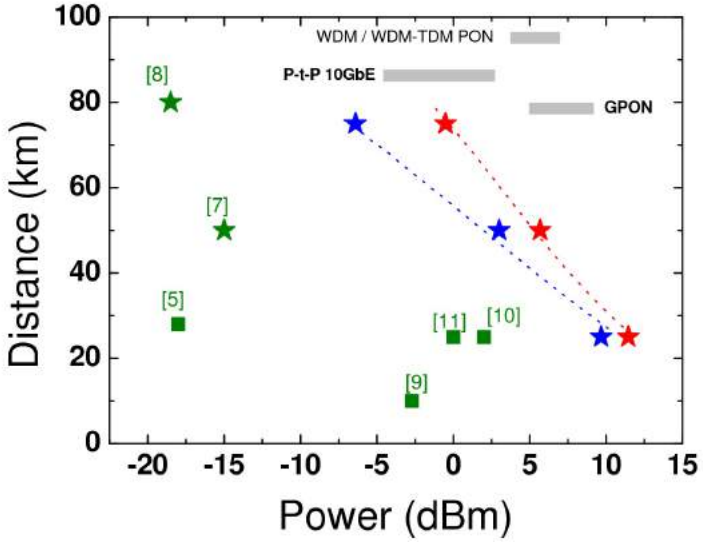
➔ ***Precursor of Euro QCI***

Telecom-grade Quantum Communications

WDM integration of CV-QKD

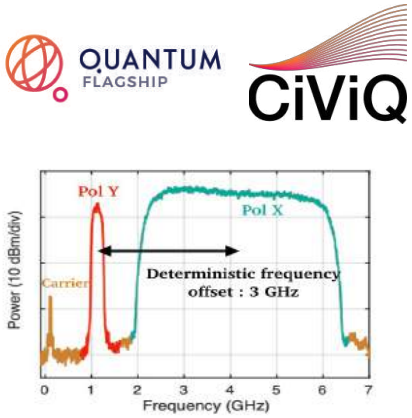


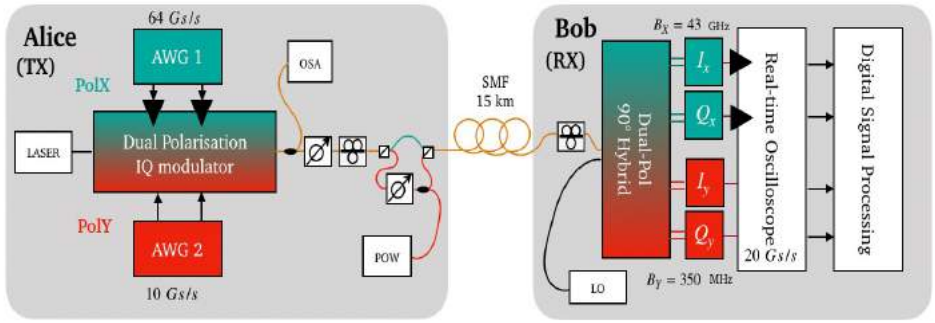
R. Kumar, H. Qin and RA
Coexistence of continuous variable QKD with intense DWDM classical channels. New Journal of Physics, 17(4), 043027. (2015).

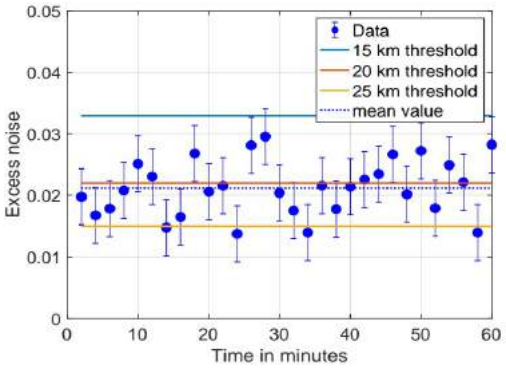


CV-QKD strong WDM coexistence (10 dBm @ 25 km) favored by coh detection

Convergence with classical coherent comm systems



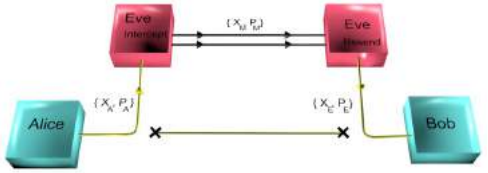


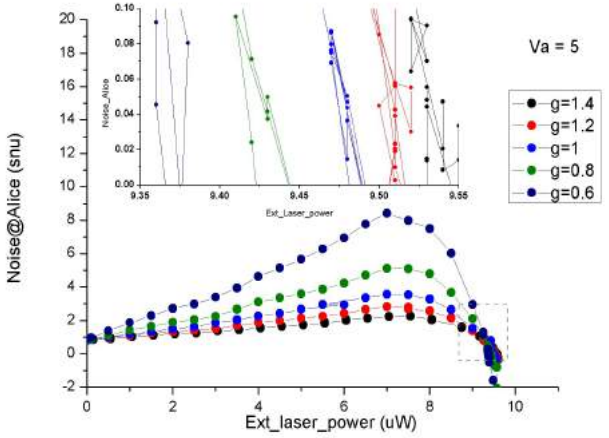


R. Aymeric, C.Ware, Y. Jaouën and RA, Symbiotic joint operation of quantum and classical coherent communications, OFC 2022

Build Certified QKD (Q Hardware) Implementations

From Quantum Hacking …





- *Hao Qin, Rupesh Kumar, and RA, Q hacking: Saturation attack on practical CV-QKD, Phys. Rev. A **94**, 012325. (2016)*
- R. Kumar, F. Mazzoncini, H. Qin, R. Alléaume, *Experimental vulnerability analysis of QKD based on attack ratings*. Scientific reports, 11(1), 1-12 (2021).
- F. Mazzoncini et al., *QKD Attack Rating: Prioritizing is the key to Practical Security,* **Contributed talk at Qcrypt, August 2021**

…to Security Evaluation and Certification

ETSI QKD Industry Standardization Group

International group of experts (academics & industry)

&

OPENQKD (Flagship project 2019-2022)

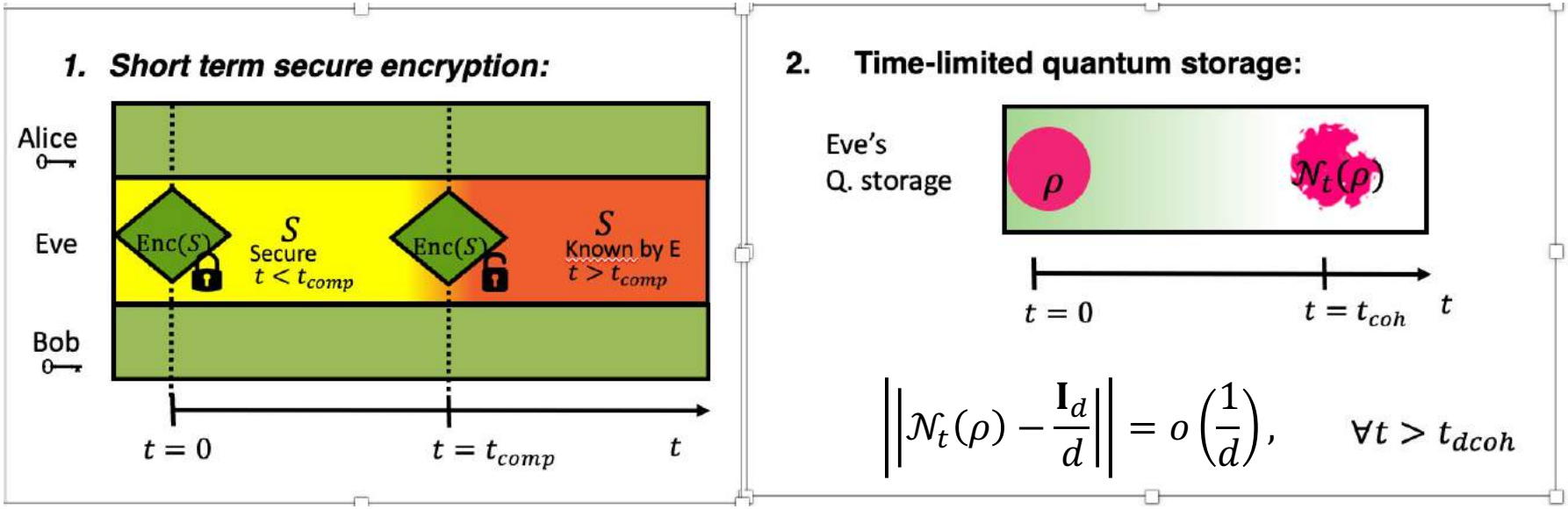
- Quantum Hacking
- Protection Profile for QKD

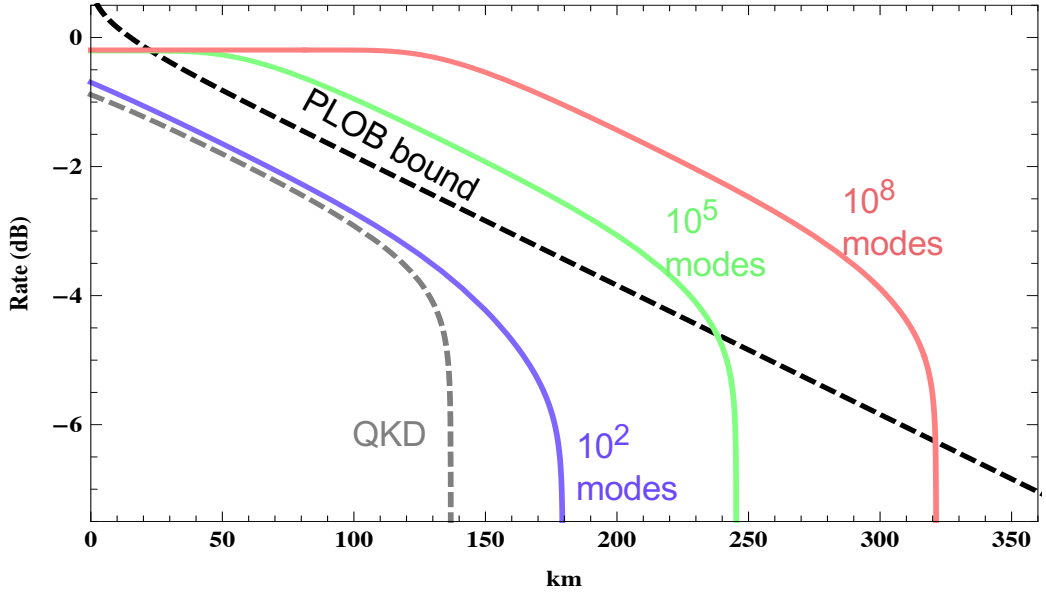
➔ **Towards Quantum Hardware Security (next Flagship phase)**

Hybridize quantum and computational cryptography

Quantum Computational Timelock

New Security Model





3 Patent Applications **EP**15305017.4 **WO**2016110582

arXiv:2004.10173

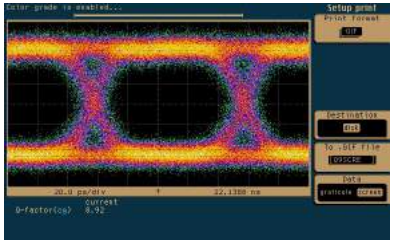
Nilesh Vyas, RA, *Everlasting secure key agreement from the quantum computational timelock*, **Contributed Talk at ICQOM 2021**

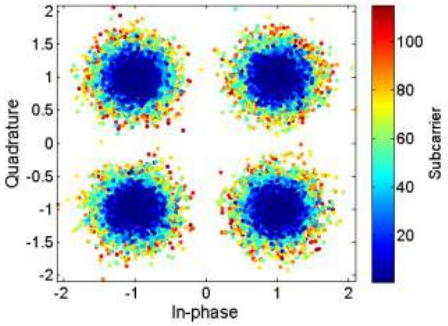
Secure KD with >> 1 photons / ch use

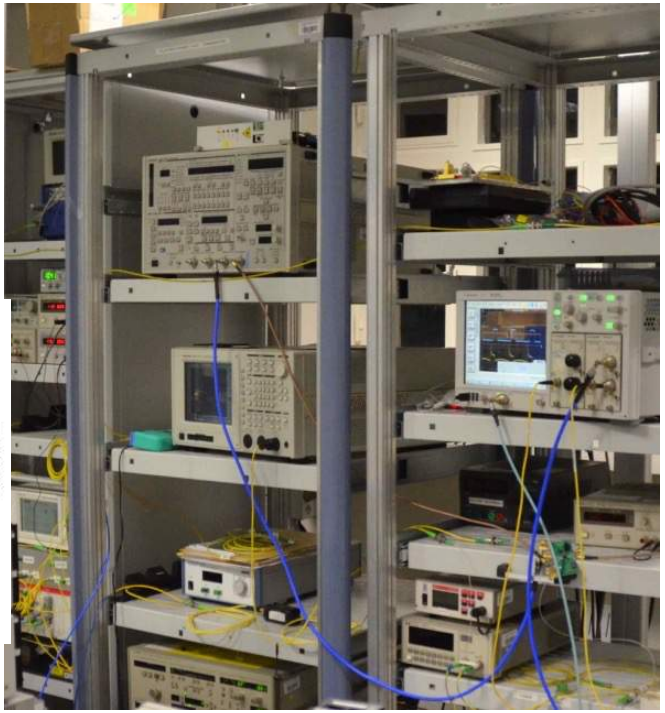
➔ Longer reach & Higher rates than QKD

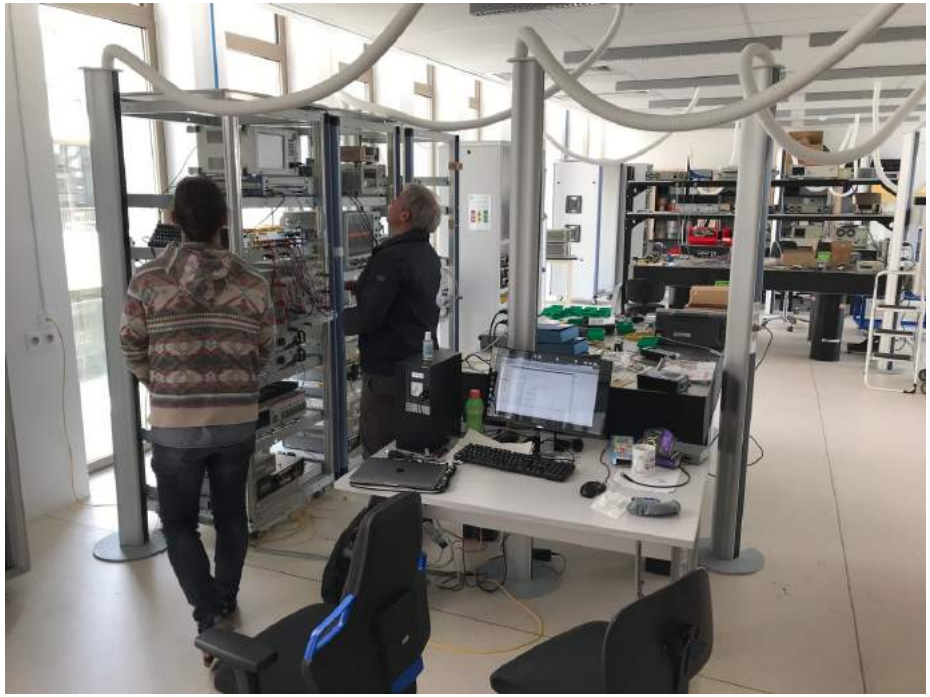
TELECOM Paris

Q Communication over a state-of-the-art optical communication platform









Collaboration avec équipe GTO - Telecom Paris (Yves Jaouen, Cédric Ware)

Plateforme 40 Gb/s à l'état de l'art + détecteurs cohérents « quantiques »

TELECOM Paris

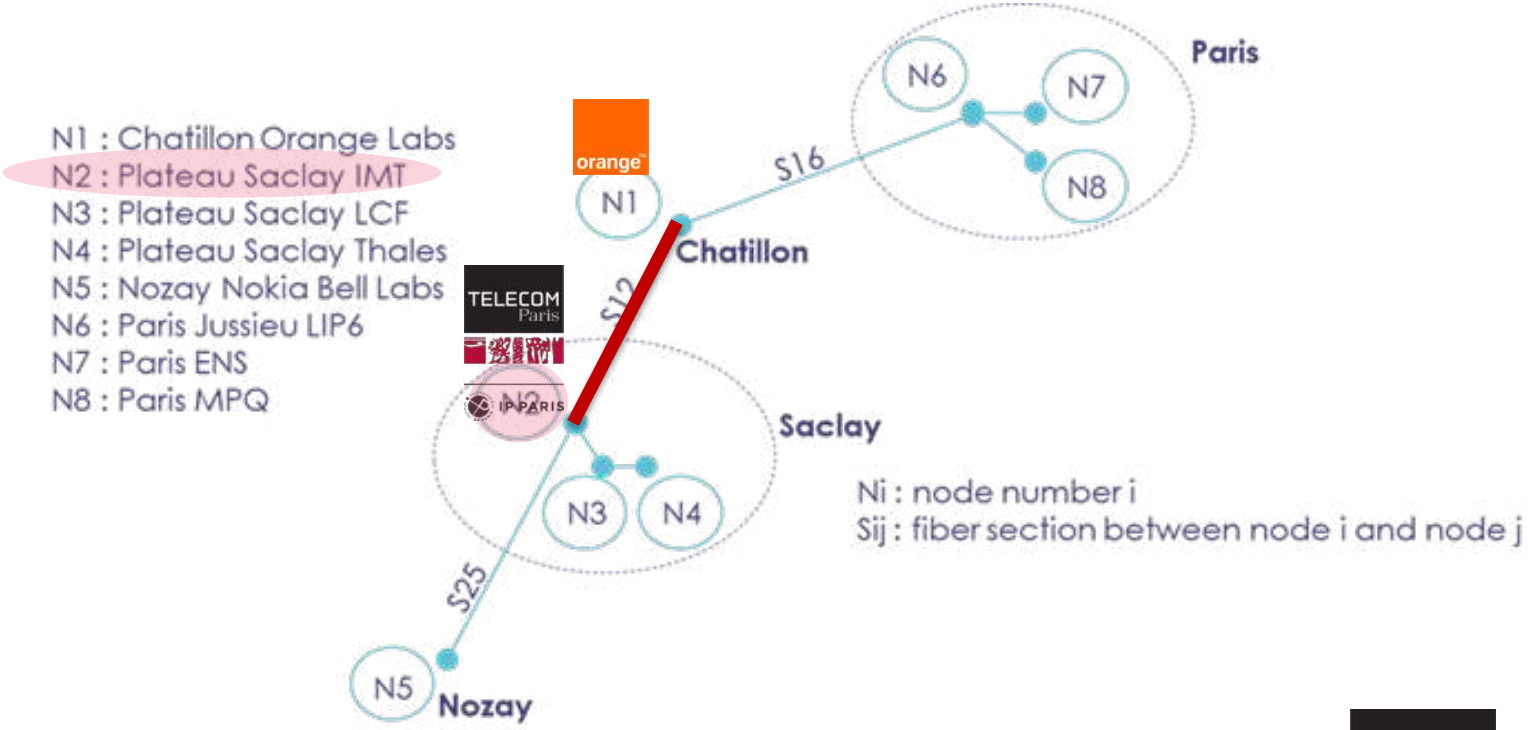
ParisRegionQCI: Deployment of a Quantum Communication Network in Paris Region

ParisRegionQCI 2021-2023
Projet Région IDF, mostly industry
Orange (Coord), Thales, Nokia, Kets, Quandela, VeriQloud, IOGS, LIP6, Telecom Paris.

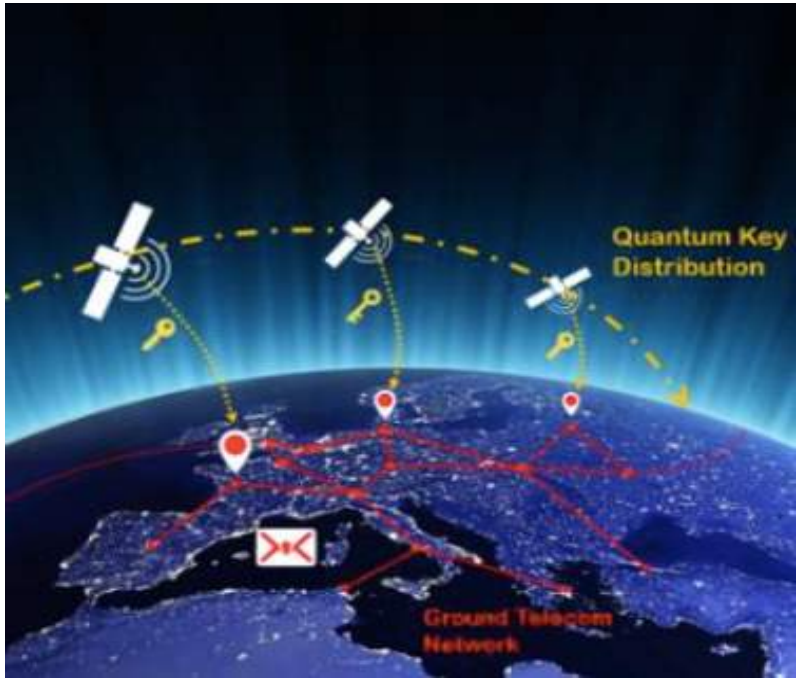
ParisQCI: 2021-2024
Projet SIRTEQ SYNERGIE
mostly academic (Q Internet)
LIP6 (coord), MPQ, LKB, C2N, LCF, Telecom Paris.

OR-TP link deployed in Sept 2021

→ *First step towards national French Q network in EuroQCI*



European Quantum Communication Infrastructure (EuroQCI)



Projet Initié par la Commission Européenne en 2019

Vise le déploiement d'une **Infrastructure pan-européenne** publique **de communications quantiques** (terrestre + satellitaire) à l'horizon 2030

Ratifié par les 27 pays européens (EU27)

Implication importante de Télécom Paris

- ***2019-2022: Etudes de faisabilité, QOSAC, QSAFE***
- ***2022: Digital Europe Program ➔ FranceQCI***

Conclusion

- **Recherche Quantique @ Télécom Paris**
  - Recherche reconnue internationalement
  - Forte activité européenne: QT Flagship, EuroQCI
  - Dimension fondamentale + technologique (brevets)

- **Nouvelles Opportunités**
  - Collaborations industrielles
  - Innovation et valorisation, Création Start-up
  - **Emplois pour les ingénieurs de l'IMT**
    - **Programme Quantum Engineering (integrated M2)**