Formation des Futurs Ingénieurs Quantiques

Cycle Quantique de la Fondation Télécom
Deuxième Petit Déjeuner - 10 Avril 2019

Romain Alléaume

Cet exposé:

Communications Quantique, Cryptographie Quantique

&

Parcours d' Ingénieurs Quantiques formés à Télécom ParisTech

Paul Jouguet

Raja Yehia

Emilien Lavie

Raphaël Aymeric

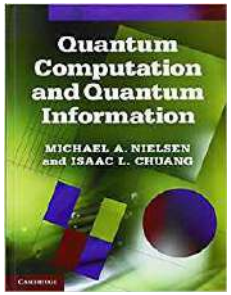
Enseignements Quantiques à Télécom ParisTech

Première année:

- Cours: Bases de la Mécanique Quantique, Semi-conducteurs
- Projet Applicatif Final. 2 semaines à temps plein (Juin), autour de l'ordinateur quantique d'IBM accessible par le Cloud.
  Programmation d'un vrai (!) ordinateur quantique

Deuxième année:

Cours d'introduction à l'information quantique
et à l'algorithmique quantique



Troisième année: Programme QEng

Programme de 6 mois, de type « Access PhD »
en Quantum Engineering

- Tutorat en Information Quantique
- Calcul Quantique
- Cryptographie quantiques [Master AFP-MPRI]
- Communications quantiques [Master LOM]
- 1 Projet de recherche encadré (4 mois à mi-temps)



Equipe enseignante
I. Zaquine, R. A. , F. Miatto

Contexte: Industrialisation des Technologies quantiques

Quantum Technology Flagship Européen, 2018-2028, 1 B€

Vise au développement industriel des technologies quantiques

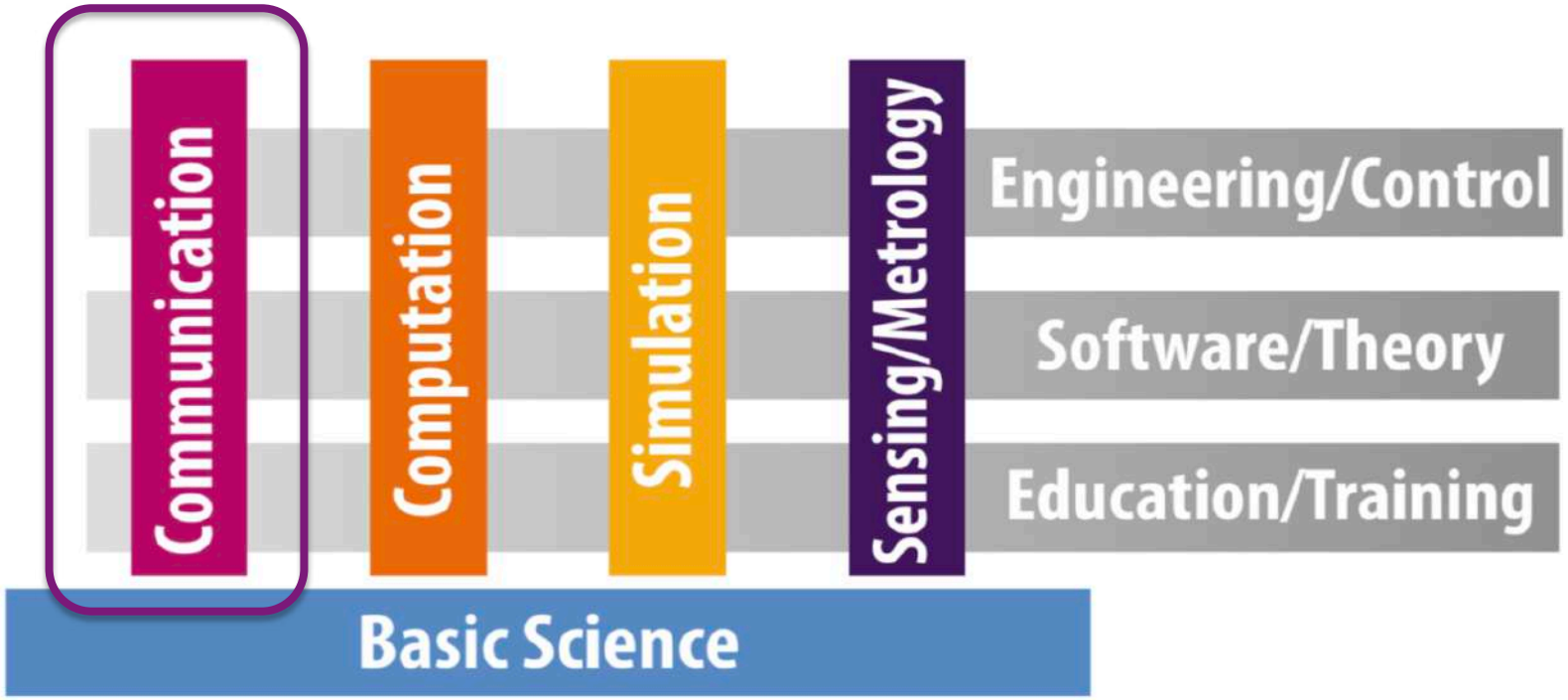
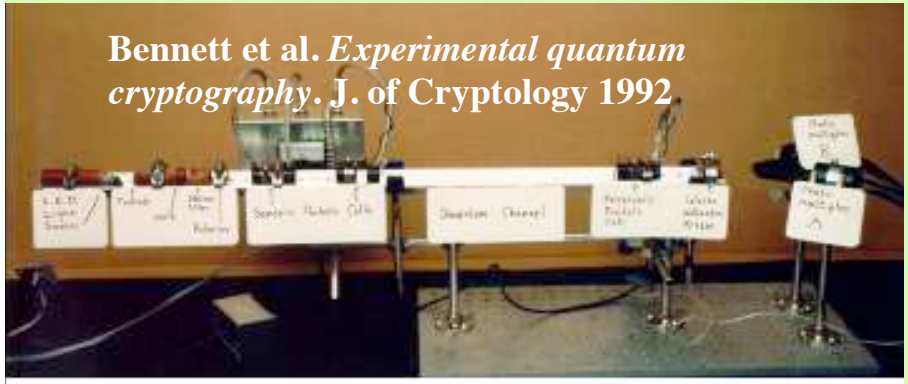


Figure: Structure of the Strategic Research Agenda

Investissements publics et privés importants à l'échelle mondiale: US, CN, DE, UK, CAN, AUS, DK, PL, etc…

Main application of Q Communication today: Quantum Key Distribution

Early 90's: Pionneering work in USA and UK



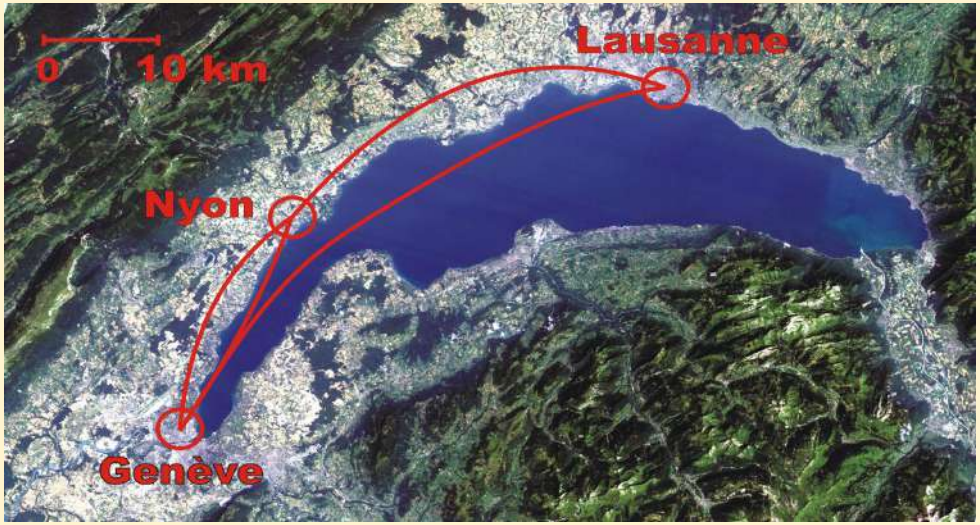
Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

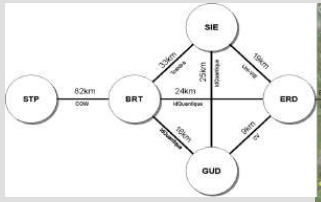
Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

1995-2005: Mastering telecom fibers

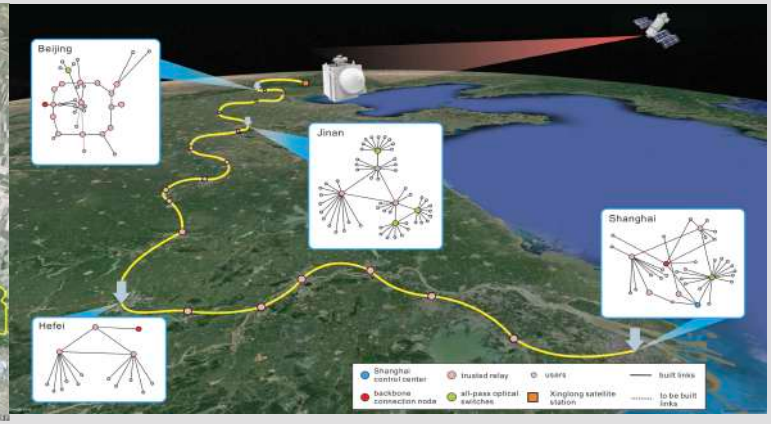


2005 -2019: Real-world QKD deployment and industrialization

2008 First European QKD Network Vienna

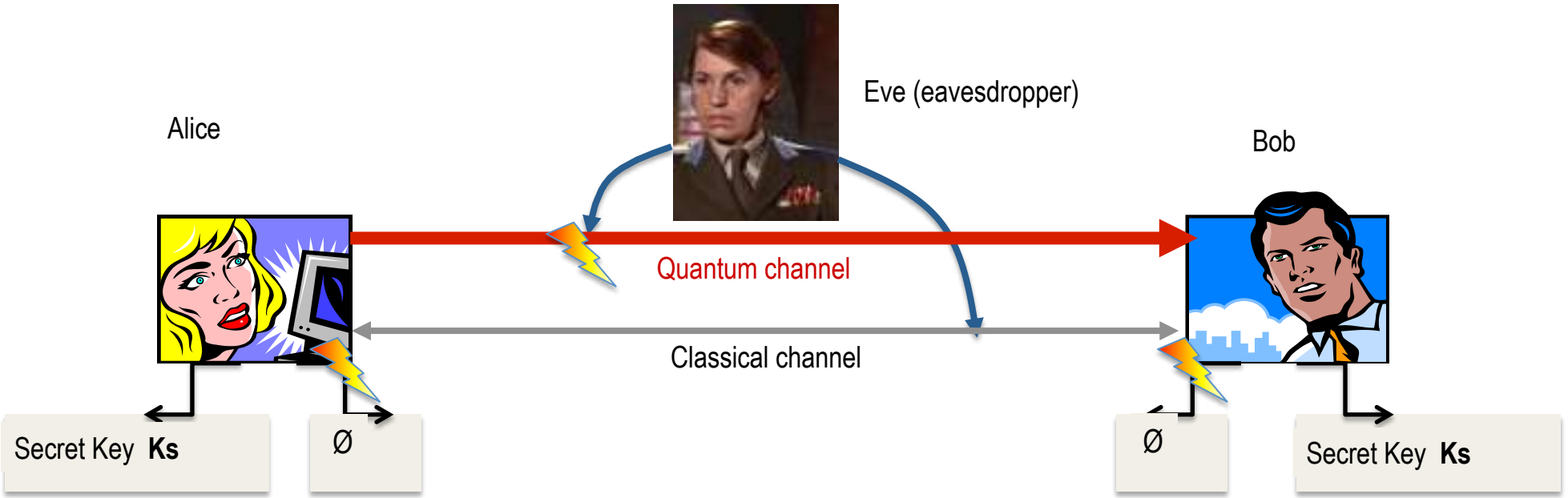


SECOQC



2016-18: Micius Satellite & Chinese 2000 km QKD network

Distribution quantique de clés (QKD):



- Sensibilité qubit à la mesure => espionnage détectable
- **Sécurité « inconditionnelle »**
  - Pas d'hypothèse sur puissance attaquant
  - « Future-proof »

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Prix au Concours National de Création d'Entreprises Innovantes en 2007 et 2008

Spin-off de Telecom ParisTech
Cœur activité: 2010-2014

Nicolas Aliacar - Gérant, co-founder
Polytechnique
+ MBA Collège des Ingénieurs

Romain Alléaume - co-founder
ENS Ulm, PhD Quantum Optics
Telecom ParisTech Associate Professor

Sébastien Kunz-Jacques – CTO
ENS Ulm, PhD Crypto
Laboratoire cryptologie de l'ANSSI

Paul Jouguet - R&D and Sales
PhD and Master Sc, TelecomParisTech
Master in Probabilities (Paris VII)

Développe des produits QKD commerciaux (software & hardware)
IP agreements with Thales, CNRS (IO), Telecom ParisTech

Recherche partenariale avec leaders internationaux

- ANR International France – Canada FREQUENCY
- IAPP France - Suisse Q-CERT

SeQureNet main achievements

Cygnus: First CVQKD commercial system launched in sept 2012 at Singapore (QCRYPT 12)

Targeted markets:
R&D and Industrial integration
Open system (at hardware and software level), designed for scientist and engineers
Targeted partnerships: QKD deployments

- High security encryption in optical networks (military, government, telco, cloud)
- WDM integration tests

2013: First Commercial system bought by NICT Tokyo
➔ Part of the QKD showcase at QCRYPT 2015

2014: Reconciliation software licenses sold to several institutions

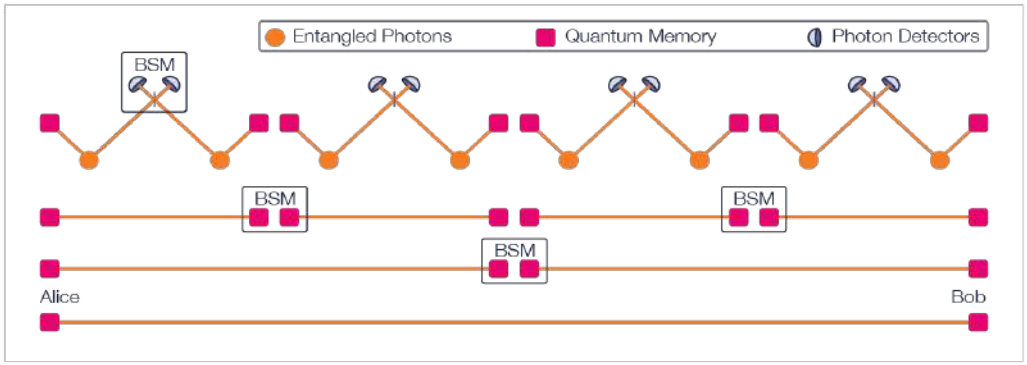
Research work recognized at international level
7 peer-reviewed papers in international journals
(Nature Photonics, PRA, Optics Express, QIC)
More than 20 invited / contributed talks including best student paper award at QCRYPT 12

-Long distance demonstration of CVQKD
Nature Photonics 7, 378 (2013)

-1 Patent on Secure shot-noise calibration

- Collaborations with international leaders

Long-term vision for Q networks: Quantum Internet



2020 planned demo:
Early network of Entangled Q memories

Raja Yehia

QEng program 2017

Master thesis 2018
QuTech Delft

Currently: PhD @ LIP6
Sorbonne Université

Quantum Internet Alliance
Flagship Project

Implementation Security of Quantum Key Distribution

Emilien Lavie

QEng program 2017

Master thesis 2018
CQT Singapour

Currently: PhD
CQT Singapour

Problématique :
Q Hacking

Solutions:

Certification des implémentations
Protocoles Q Crypto « Device-Independent »

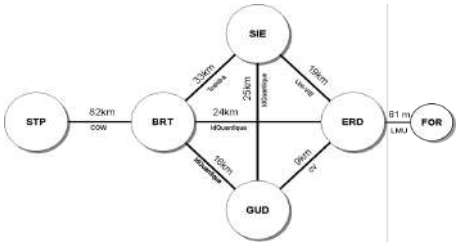
Méthodes numériques pour (MDI)-QKD

Pour en savoir plus
https://www.youtube.com/watch?v=OEkdknqUIII

2005-2019 Telecom ParisTech joue un rôle de premier plan dans le développement de la technologie QKD

Premier réseau QKD européen (Vienne, 2008)

SECOQC



INSTITUT d'OPTIQUE GRADUATE SCHOOL

cnrs

THALES

TELECOM ParisTech

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Technologie CV-QKD :
Record de distance : 100 km (2012)
Premier système commercial (SeQureNet)

Projets collaboratifs avec acteurs internationaux clés (2008-2021)

Réseaux et cryptographie (NC ANR
Sécurité des implémentations, Q hacking (Q-CERT, ETSI)
Multiplexage optique (Quantum WDM)
Réseaux Quantiques (QCALL)
Comm Quantiques CV (CIVIQ)
Tested QKD (OPENQKD)

QUANTUM FLAGSHIP

QUANTUM FLAGSHIP

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

IDQ

UNIVERSITY OF CAMBRIDGE

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

TOSHIBA Leading Innovation

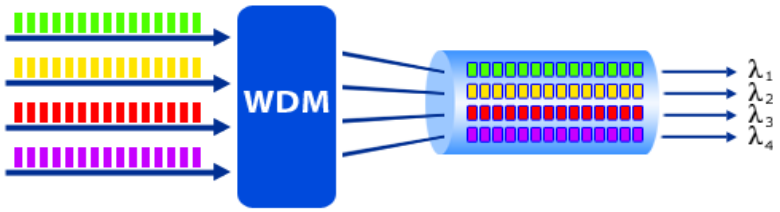
清華大學 Tsinghua University

NICT 独立行政法人 情報通信研究機構 National Institute of Information and Communications Technology

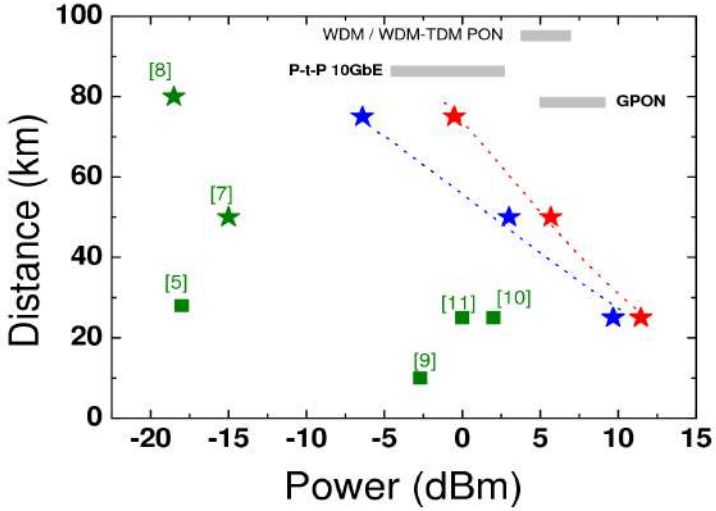
Towards Telecom-grade Quantum Communications

advantage of CV-QKD in terms of integration

WDM integration of CV-QKD



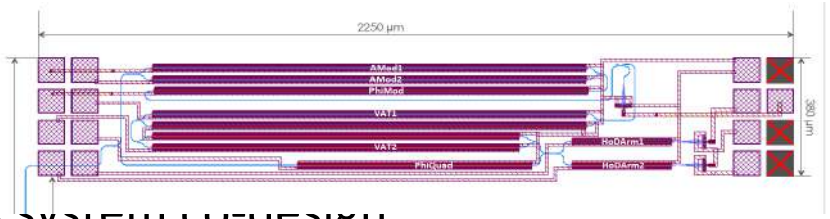
R. Kumar, H. Qin and RA
Coexistence of continuous variable QKD with intense DWDM classical channels. New Journal of Physics, 17(4), 043027. (2015).



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

Smaller and Cheaper systems

- Photonic integration
- Classical and Quantum communications system co-design



Persechino M et al, QIPC 2015

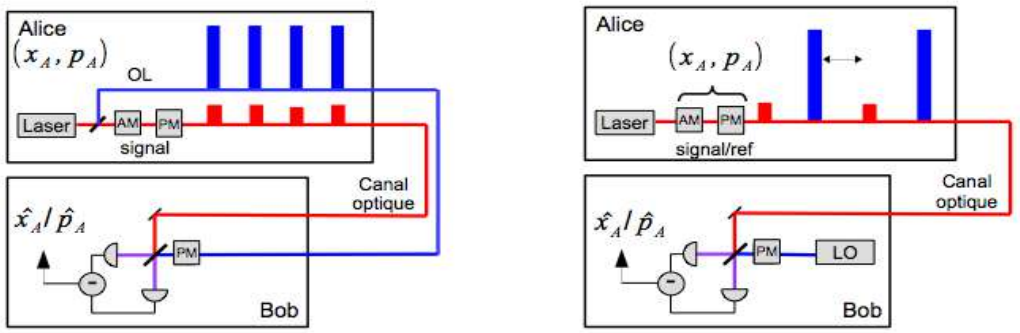
Adrien Marie and Romain Alléaume
Self-coherent phase reference sharing for continuous-variable quantum key distribution
*Phys. Rev. A **95**, 012316, (2017)*

Towards Telecom-Grade QKD: *System design and security*

Coherent Q Com System Design

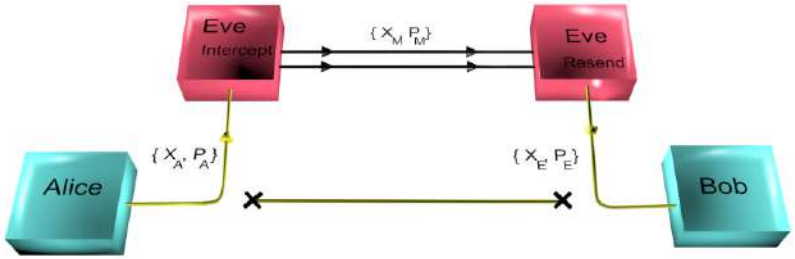
"Local'' Local oscillator
with affordable laser / modulator

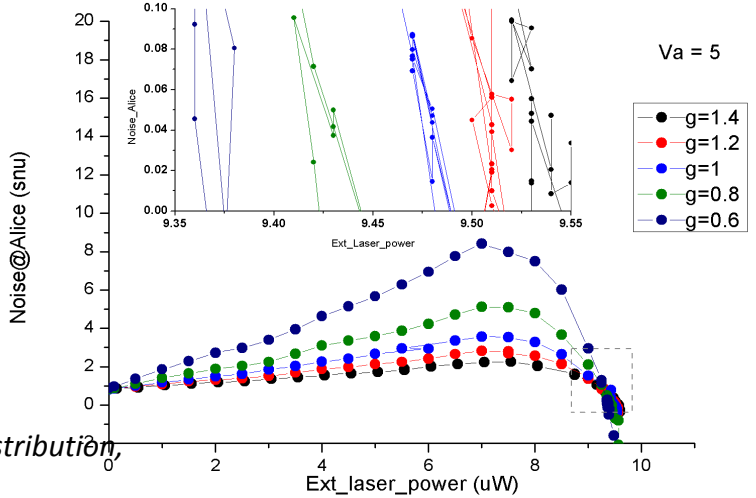
➔ *Convergence with classical coherent comm systems*



Adrien Marie and RA
*Self-coherent phase reference sharing for continuous-variable quantum key distribution Phys. Rev. A **95**, 012316, (2017)*

Implementation security





Hao Qin, Rupesh Kumar, and Romain Alléaume
*Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, Phys. Rev. A **94**, 012325. (2016)*

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

ICFO

Palacký University Olomouc

NOKIA Bell Labs

Mellanox TECHNOLOGIES

T

TELECOM ParisTech

Une école de l'IMT

POLITÉCNICA "Engineering the future"

INTERNATIONAL CAMPUS OF EXCELLENCE

NEXTWORKS ENGINEERING FORWARD

UNIVERSITY of York

DTU

HUAWEI

VLC PHOTONICS

orange

cnrs

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Inria inventors for the digital world

coriant

MPL Max Planck Institute for the science of light

Fraunhofer Heinrich-Hertz-Institut

QUSIDE

Telefónica

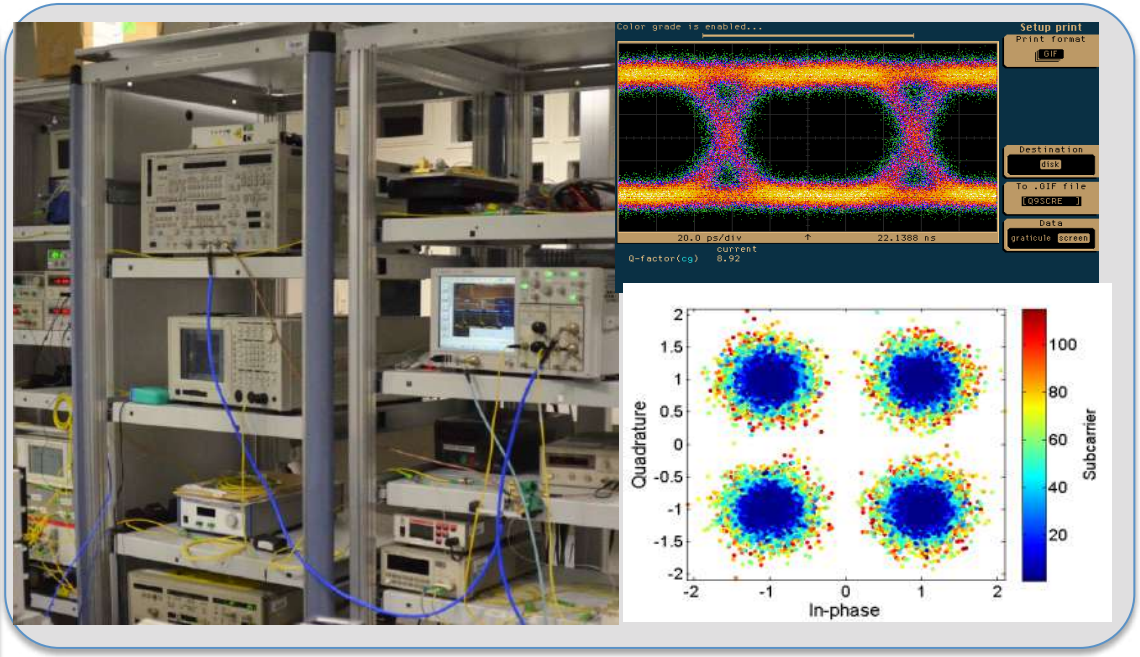
Convergence communications cohérentes classiques et quantiques

Raphaël Aymeric

QEng program 2018

Master thesis 2018
IQC Waterloo

Currently: PhD @
Telecom ParisTech

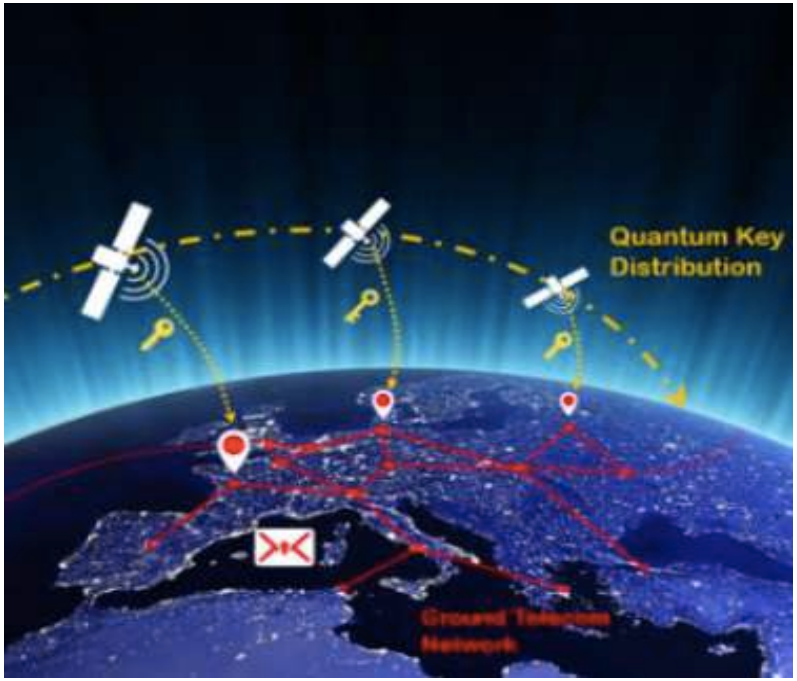


Plateforme communications optiques ultra haut débits

Ongoing PhD at Telecom ParisTech (Supervisors: R. Alléaume, Cédric Ware)

- **Protocols and Security proofs**
- C/Q Coherent Communication System Design & Signal Processing
- Classical / Quantum Communication Co-Propagation (WDM)

Projet Européen de « Quantum Communication Infrastructure »



Initié par la Commission Européenne

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

Opportunité exceptionnelle pour les futurs ingénieurs quantiques

R&D Tech Quantique -- Sécurité / Défense -- Photonique, Télécom

MERCI !