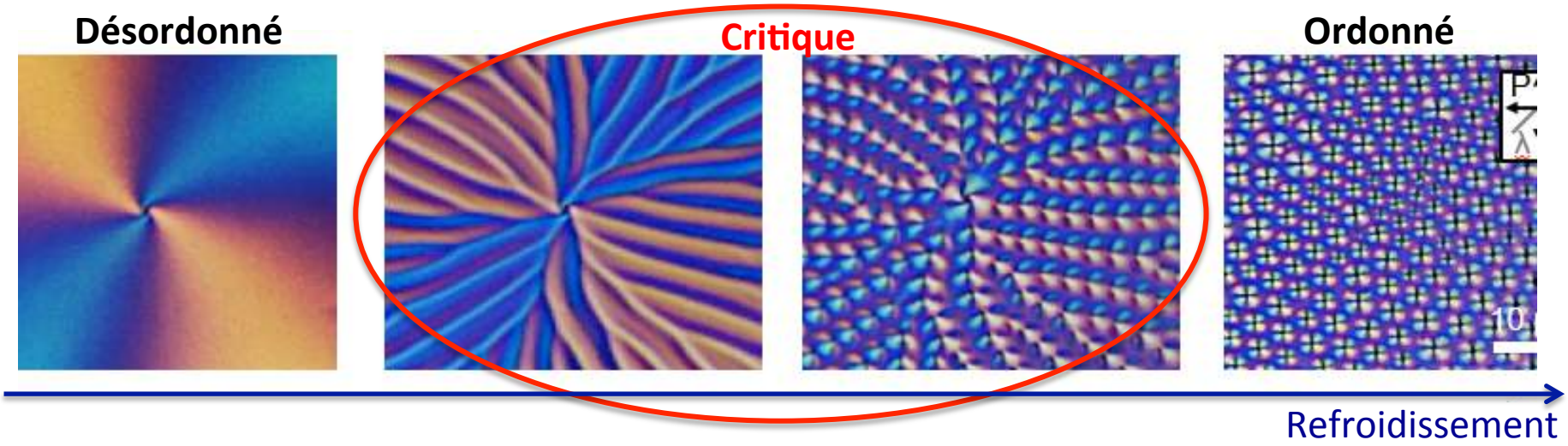
Développement Industriel de la Cryptographie Quantique : Défis et Opportunités

French Photonics Days – Bordeaux – 4 Avril 2019

Romain Alléaume

Industrialisation des technologies quantique: point critique ?



Transition Critique

- Corrélations à grande distance
- Instabilité
- Complexité

Industrialisation Technologies Q

- Recherche fonda. / Technologies / Industriels / Invest. publics et privés
- Risque
- Caractère structurant (DeepTech) Importance Stratégie

Industrialisation QKD: retour d'expérience sur SeQureNet

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Spin-off Telecom ParisTech

TELECOM ParisTech

2008-2009 | 2010-2014 | 2015-2017

Création → Cœur de l'activité R&D → Act. réduite → Fermeture

2012, Cygnus: Premier système commercial de cryptographie quantique à variables continues

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

2008-2009 : Création – Formation Equipe

Equipe

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

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

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

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

Conseil Scientifique

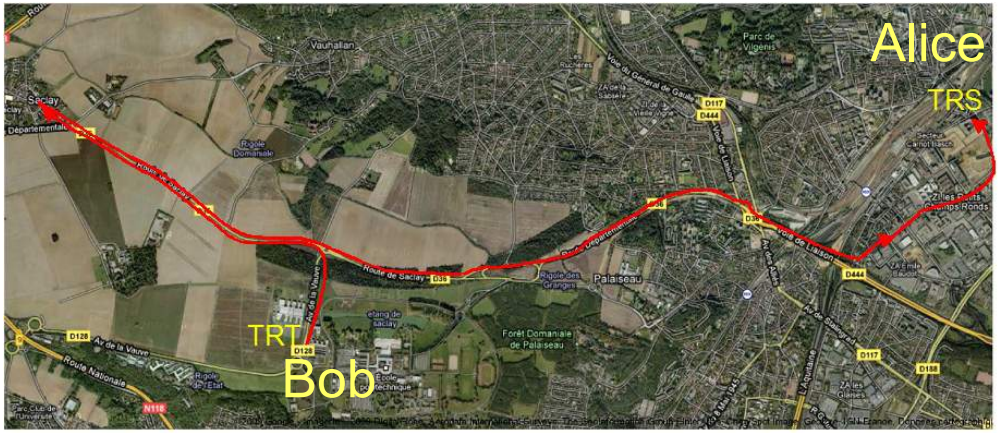
Philippe Grangier
Dir Recherche CNRS – Institut d'Optique
Co-inventor of CVQKD

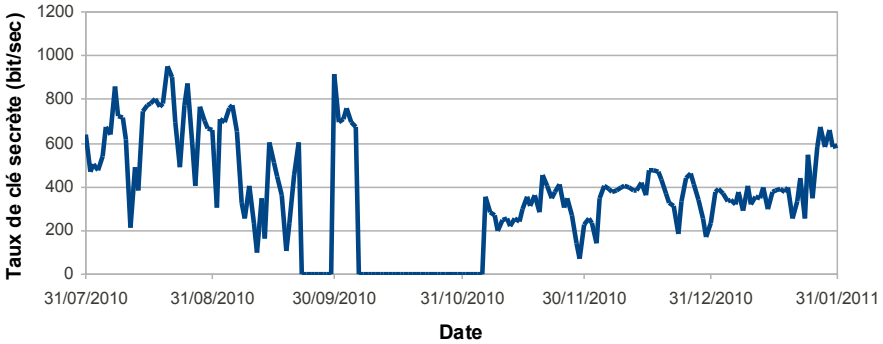
Jean-François Roch
Professeur et Dir adoint de l'ENS Cachan
Quantum optics expert

Michel Riguidel
Professeur émérite à Telecom ParisTech
Network security expert

2010 : 6 months deployment (SEQURE project)

- Fiber link: Thales R&T (Palaiseau) to Thales Raytheon Systems (Massy), 18 km
- **CV-QKD Technology**
- 17.7 km, 5.6 dB





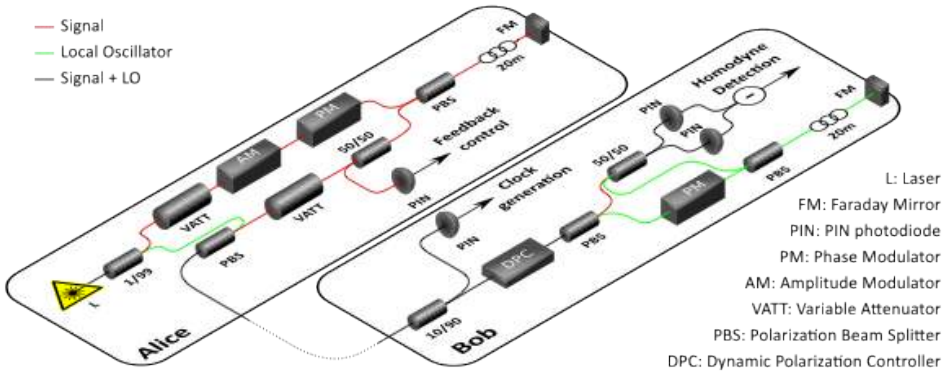
Deployment realized by

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

2010-2014 : Improvements + Industrialization of CV-QKD

- **Starting Point: Secoqc / SEQURE CVQKD demonstrator**

- **Modifications of the optical design**
  - Clock recovery (Alice-Bob synchronization)
  - Removed one amplitude modulator (on Alice side)
  - 1 MHz repetition rate



- **Software fully rewritten (C)**
  - New feedback control loops
  - Improved procedures for parameter estimation
  - Original (inventive) algorithms for phase stabilisation, synchronization,
  - Well separated of functionnalities
  - Clean management of scheduling

  ➔ High system stability

  ➔ Evolutionary system

- **New algorithms for reconciliation**
  - Highly efficient LDPC codes on GPU
  - Fast privacy amplification

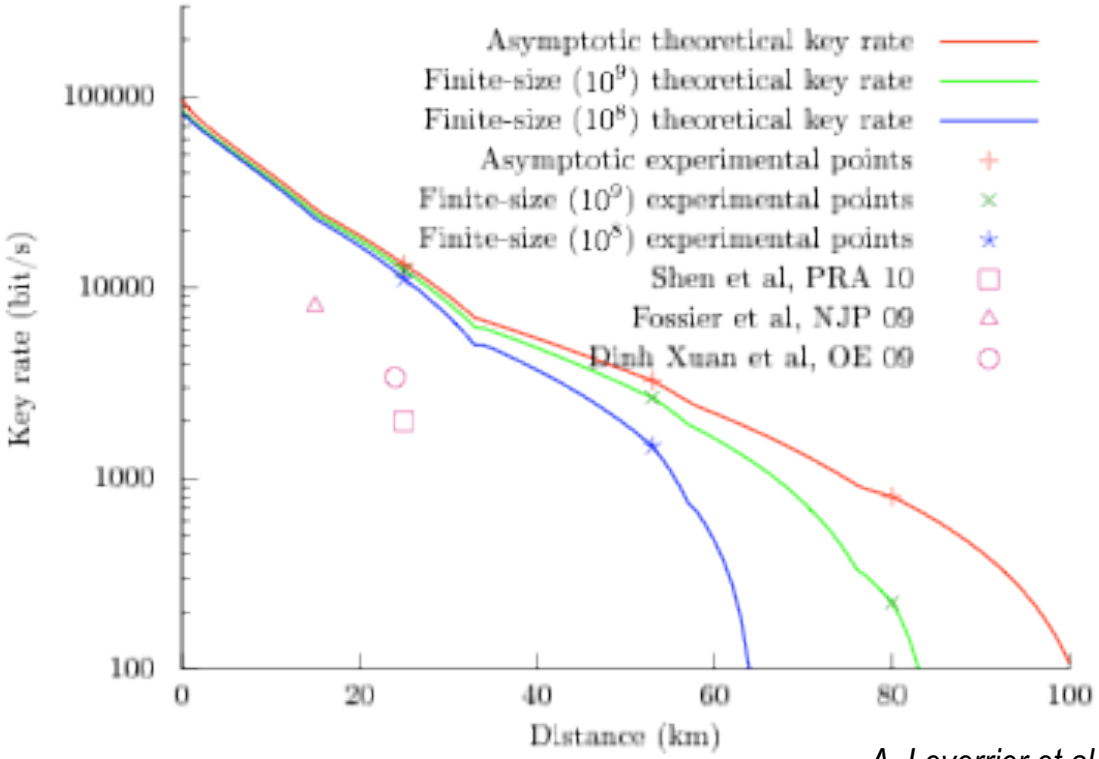
  ➔ Larger distances

SEQURENET

A QUANTUM KEY TO NETWORK SECURITY

Performance: a giant step ahead

- **Long distances (> 80 km) reachable thanks to a breakthough in CV reconciliation**
  - Channel Virtualisation (A. Leverrier) => virtual channel close to binary modulation BIAWGN
  - Very efficient LDPC codes for the BIAWGN, even at low SNR



SeQureNet system performance clearly outperforms previous results

80 km, including finite-size effects and uncertainty on calibrated values

$\varepsilon = 10^{-10}$

Security proof:
Collective Attacks + Finite size

A. Leverrier et al. Phys. Rev. A 81, 062343 (2010)
Paul Jouguet et al., Nature Photonics 7, 378 (2013)

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

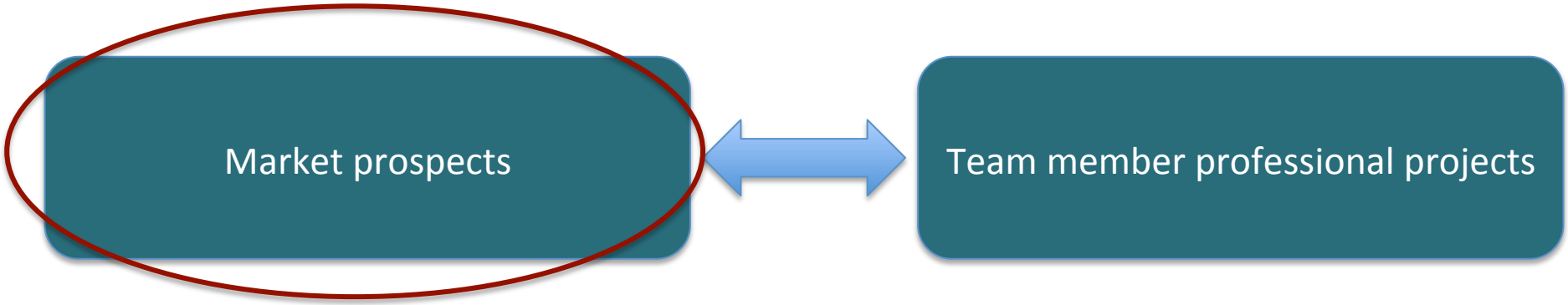
Research work recognized at international level
7 peer-reviewed papers in international journals (Nature Photonics, PRA, Optics Express, QIC)
More than 20 invited / contributed talks including best student paper award at QCRYPT 12

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

-1 Patent on Secure shot-noise calibration

- Collaborations with international leaders

« But why did you stop the activity then ? »



Marché de la QKD: Dynamique et Verrous

Marché QKD déjà existant et en forte croissance de 2016 à 2019

- 2000 km Trusted node QKD network + Micius satellite in China
- Activity and Products developped by Toshiba, British Tel., Adva, IdQuantique
- SeQureNet had a commercial activity (FR, JP, USA, CN)
- SK Telecom and Deutsche Telekom Quantum Alliance (Feb 2017)
- QuantumXChange launches commercial QKD service in NYC-Boston

Dominé par activités de R&D (publiques et privés) en QKD

Rôle clé des invest. publics stratégiques en Chine, Corée, UK, DE

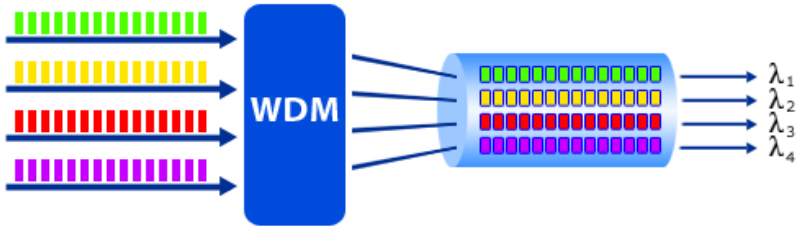
Comment faire croitre le marché de la QKD et accélérer son industrialisation ?

- Défi1 : Photonique quantique - Coût et Intégration
- Défi2: Intégration cryptographique

Défi1 : Vers une QKD certifiée et intégrée dans réseaux télécom

Avantages technologiques pour la CV-QKD

Intégration ds réseaux optiques

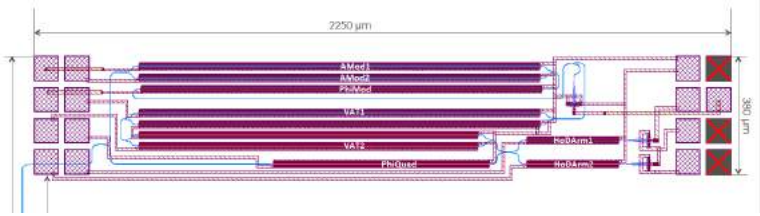


Rupesh Kumar, Hao Qin, Romain Alléaume,
Coexistence of continuous variable QKD with intense DWDM classical channels. New Journal of Physics, 17(4), 043027. (2015).

Sécurité implémentations QKD

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

Baisser les coûts des systèmes



Persechino M et al, QIPC 2015

- Photonic integration
- Convergence between classical and quantum communications

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

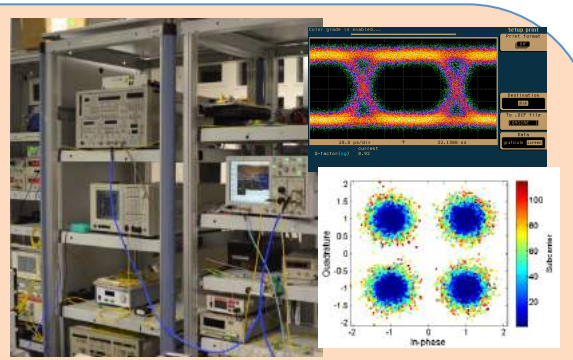
Continuous Variable Quantum Communication

European Quantum Technology Flagship Project: 2018-2021

21 Partners, 3 years, 10 M€ budget

Q Comm R&D, Telecom Manufacturers, Network Operators

- **CV Q communication system design: theory and experimental validation**
  - Convergence, LLO design, Signal Processing
  - WDM compatibility
- **CV-QKD protocols and security**
  - Side-channels analysis and c-measures
  - Standards and certification
- **Flexible / Secure Q PHY-layer**
  - Network Integration & Demonstrations (SDN)
- **Photonic integration of components and systems**



Défi2 : Améliorer l'intégration cryptographique de la QKD

Dissensus entre cryptographie « classique » (computationnelle) et cryptographie quantique

K. G. Paterson, F. Piper, R.Schack Quantum cryptography: A practical information security perspective eprint.iacr.org/2004/156.pdf

R. Alléaume, et al. (23 co-authors), Using quantum key distribution for cryptographic purposes: A survey. Theor. Comput. Sci. 560: 62-81 (2014) (secoqc white paper 2007)

D. Stebila, M. Mosca, N. Lütkenhaus, N. The case for Quantum Key Distribution, Quantum Communication and Quantum Networking, 283-296. (2010)

NCSC position paper on QKD www.ncsc.gov.uk/information/quantum-key-distribution, Oct 2016

Elements d'analyse

☺ **QKD** permet de réaliser la **distribution de clé crypto** avec **avantage fondamental** par rapport à crypto computationnelle: information-theoretic security.

➔ **permet sécurité à long-terme des communications**

😐 QKD pas un service de sécurité « en soi »: doit être combiné

☹ Ne peut pas être déployé partout, Limitations sur Performance/ Coût

Message

Q Crypto ne remplace pas la Crypto Computationnelle

Best when combined (cf security belt / airbag)

Quels usages et quels marchés pour la QKD ?

There is a market for quantum-enhanced Layer 2 Link Encryption (IdQuantique, Toshiba, Quintessence Labs, QuantumCTek and Chinese QKD network, and etc…).

⇒ How large ? Is it really quantum crypto killer application ?

Other q crypto use cases

Long-term secure storage
(proactive secret sharing)
J Buchman et al. eprint.iacr.org 2016/742

Quantum-enhanced key management

Physical layer security (PUFs, QRNG)

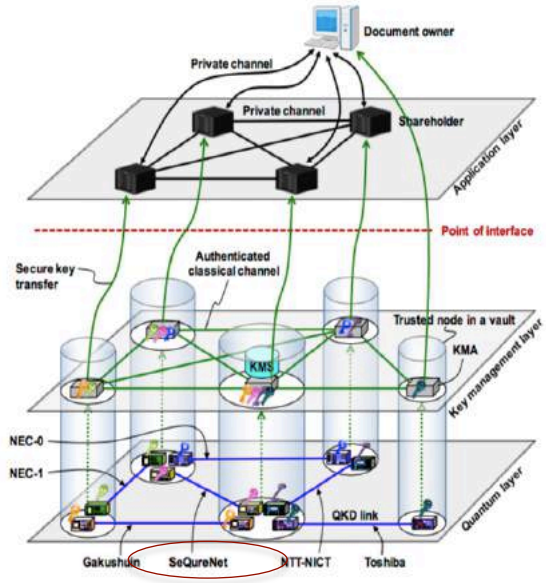
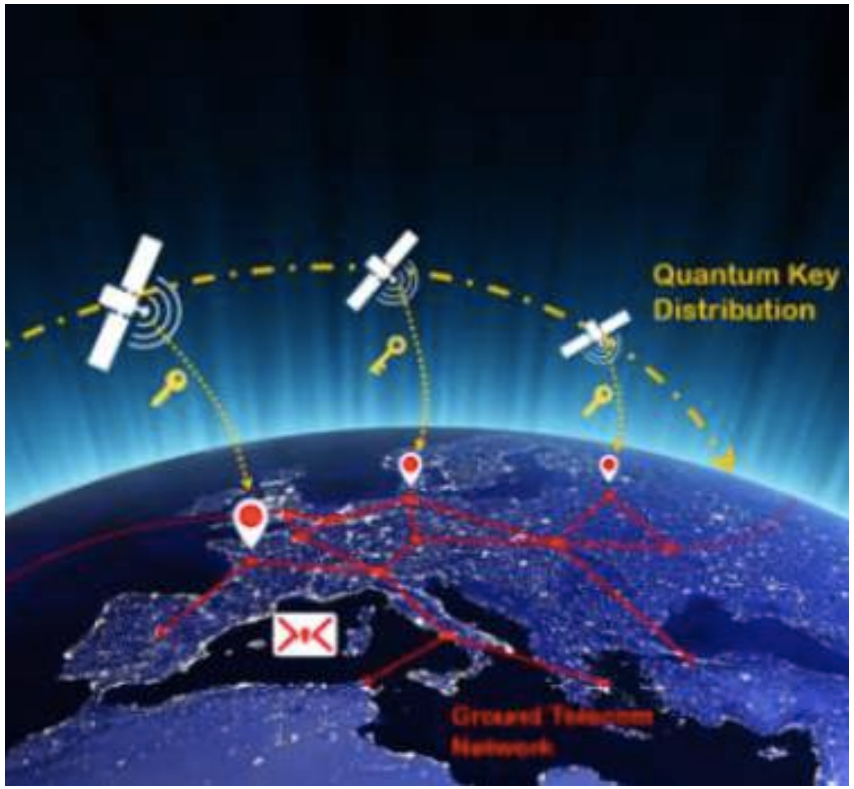


Figure 4: The secret sharing scheme supported by the Tokyo QKD Network.

Facteur de croissance essentiel pour le marché QKD :
Collaboration renforcée entre Académiques et Industriels des domaines Crypto/ Sécurité et Crypto Quantique

Projet Européen de « Quantum Communication Infrastructure »



Initié par la Commission Européenne

Vise le déploiement d'une **infrastructure pan-européenne**, et publique, **de communications quantiques** (terrestre + satellitaire)

à l'horizon 2030

Secteurs pertinents pour QCI:

Techno quantiques -- Sécurité / Défense -- Photonique, Télécom

➔ *Nombreux acteurs clés et atouts scientif & industriels en France*

➔ *Opportunité exceptionnelle pour accélérer / coordonner les efforts.*