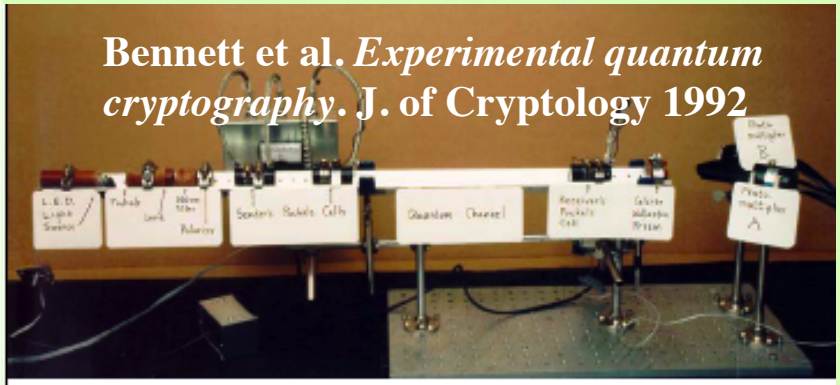
Présentation des activités de recherche « quantiques » au sein de Telecom ParisTech
9 Juin 2010

Romain Alléaume
Maitre de Conférences
Télécom ParisTech
Département Informatique et Réseaux

Déploiement de la distribution quantique de clés pour la sécurisation des réseaux, industrialisation et enjeux fondamentaux

Systèmes QKD : maturation de la technologie dans les laboratoires depuis 1984 et l'idée initiale de Bennett et Brassard (protocole BB84)

USA, UK: Expériences pionnières dans les années 90



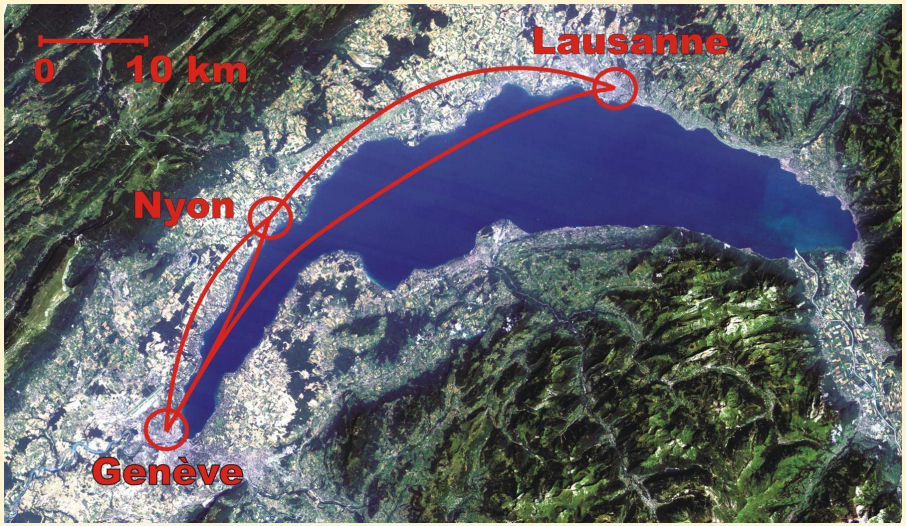
Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

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.

Années 2000-2004 : le basculement sur fibre optique télécom, déploiement hors du labo

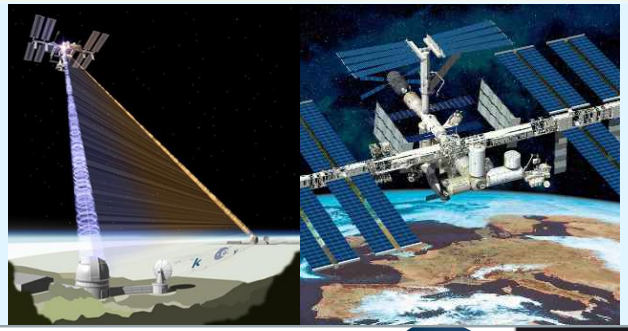


Frontières pour la QKD

- Améliorer les performance des liens
- déploiement sur des réseaux de communication

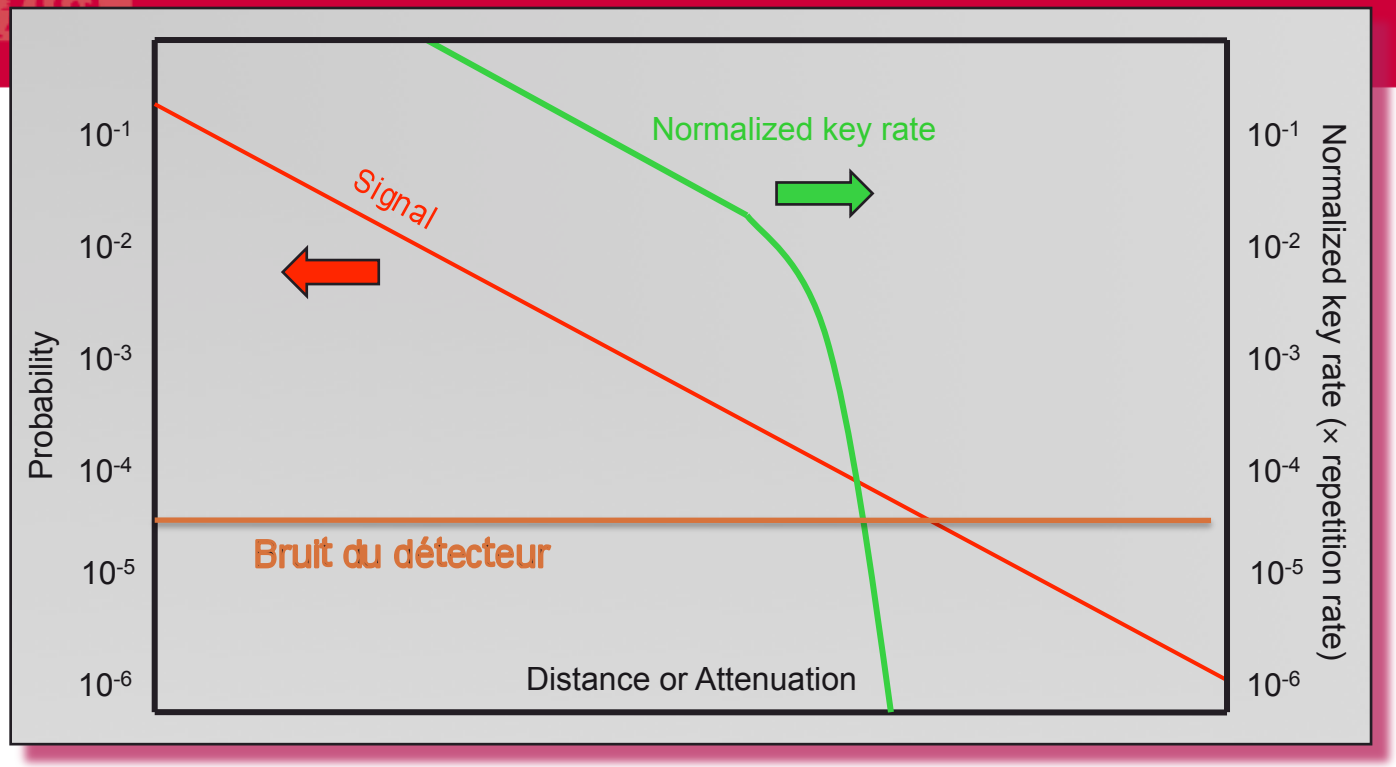
SECOQC

- L'espace cf projet Space-QUEST :



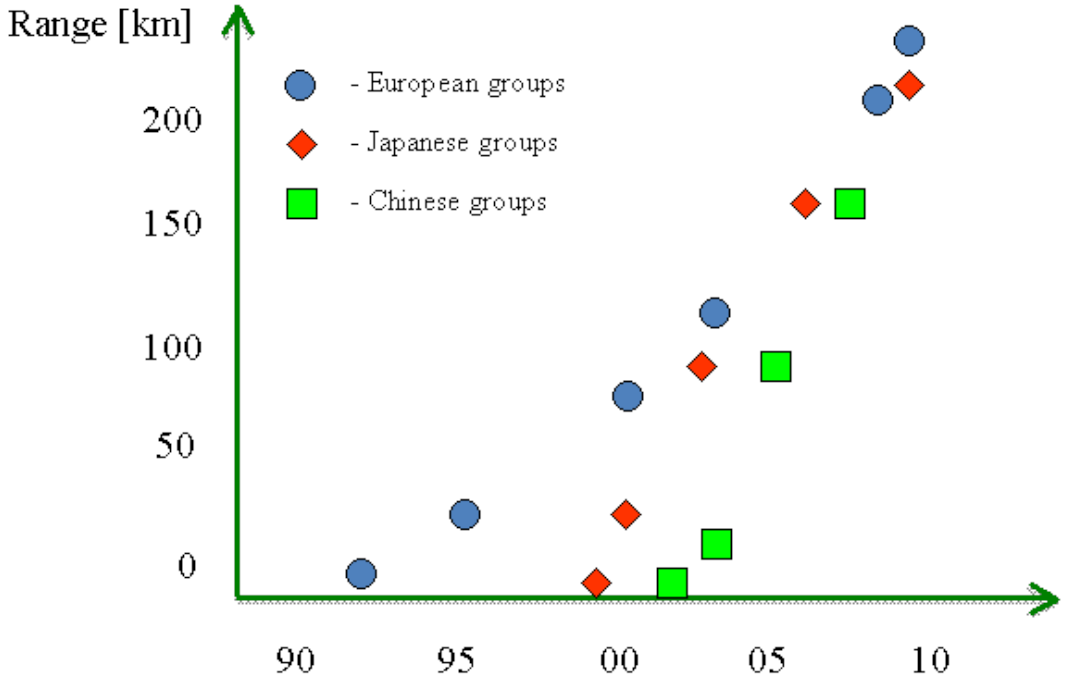
cnrs TELECOM ParisTech

Performance d'un lien QKD

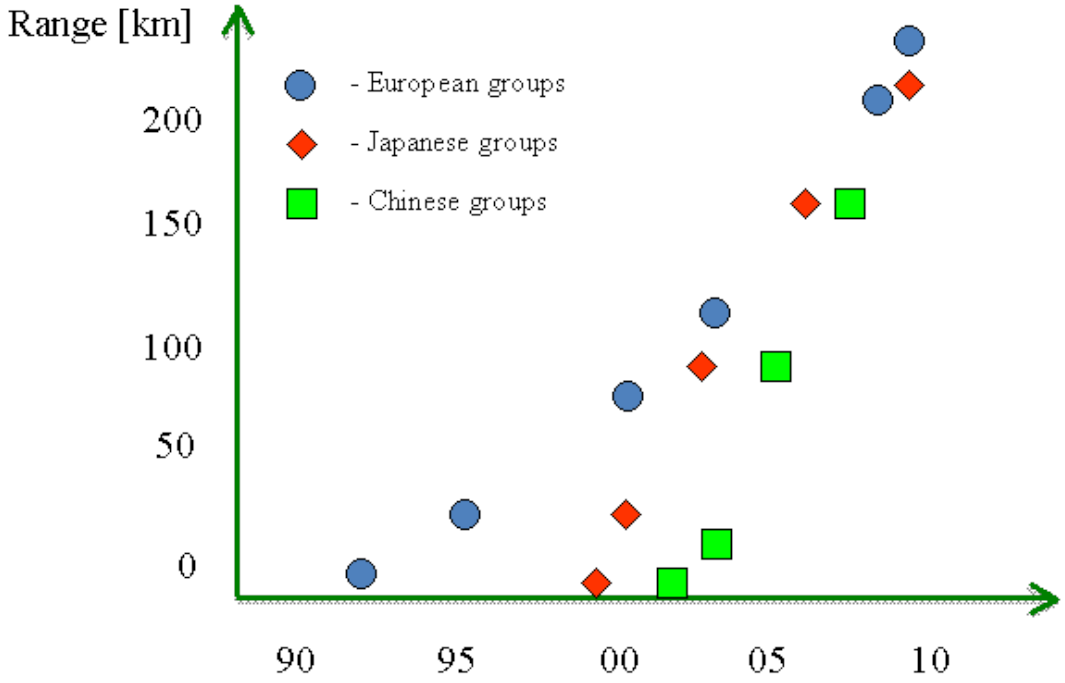


- La métrique est le nombre de bits de clé par seconde
- Le débit en clé diminue avec la distance, l'atténuation
  - Le niveau du signal diminue exponentiellement avec l'atténuation
  - Le niveau du bruit du détecteur est lui constant
- Le taux d'erreur est assimilé à l'espion et le taux de clé s'effondre quand signal ~ bruit

QKD en voie d'industrialisation => Course technologique pour la performance des liens

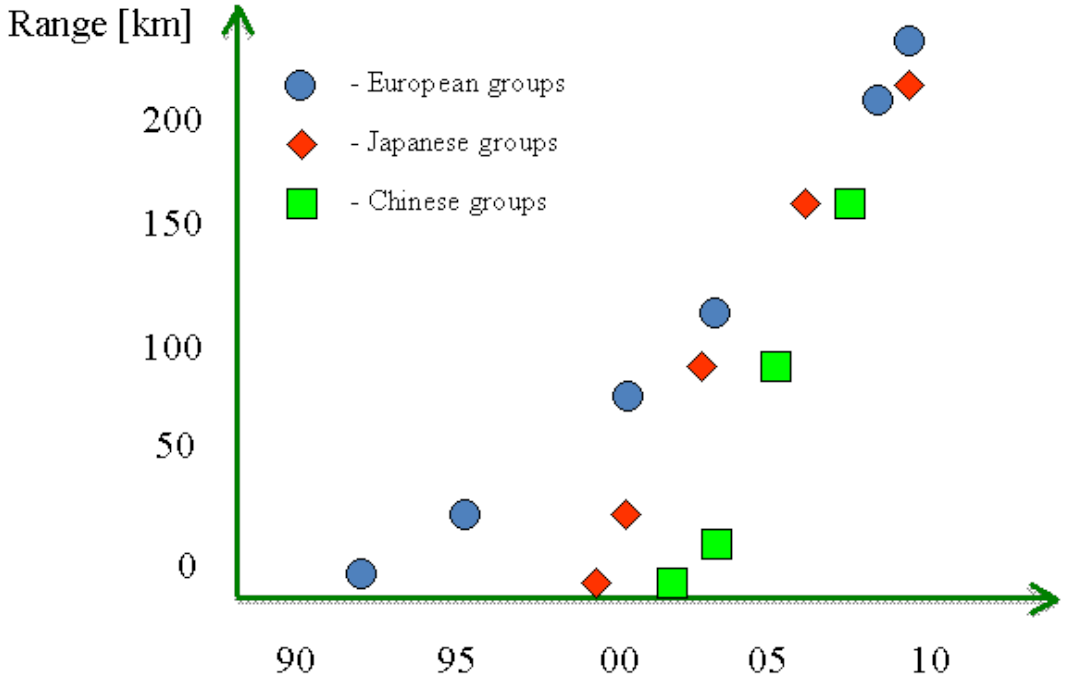


QKD en voie d'industrialisation => Course technologique pour la performance des liens



Intérêt majeur des protocoles inventés dans la thèse d'Anthony Leverrier : grande distance accessible, avec hardware plus simple => Axe de travail pour équipe IQ + SeQureNet

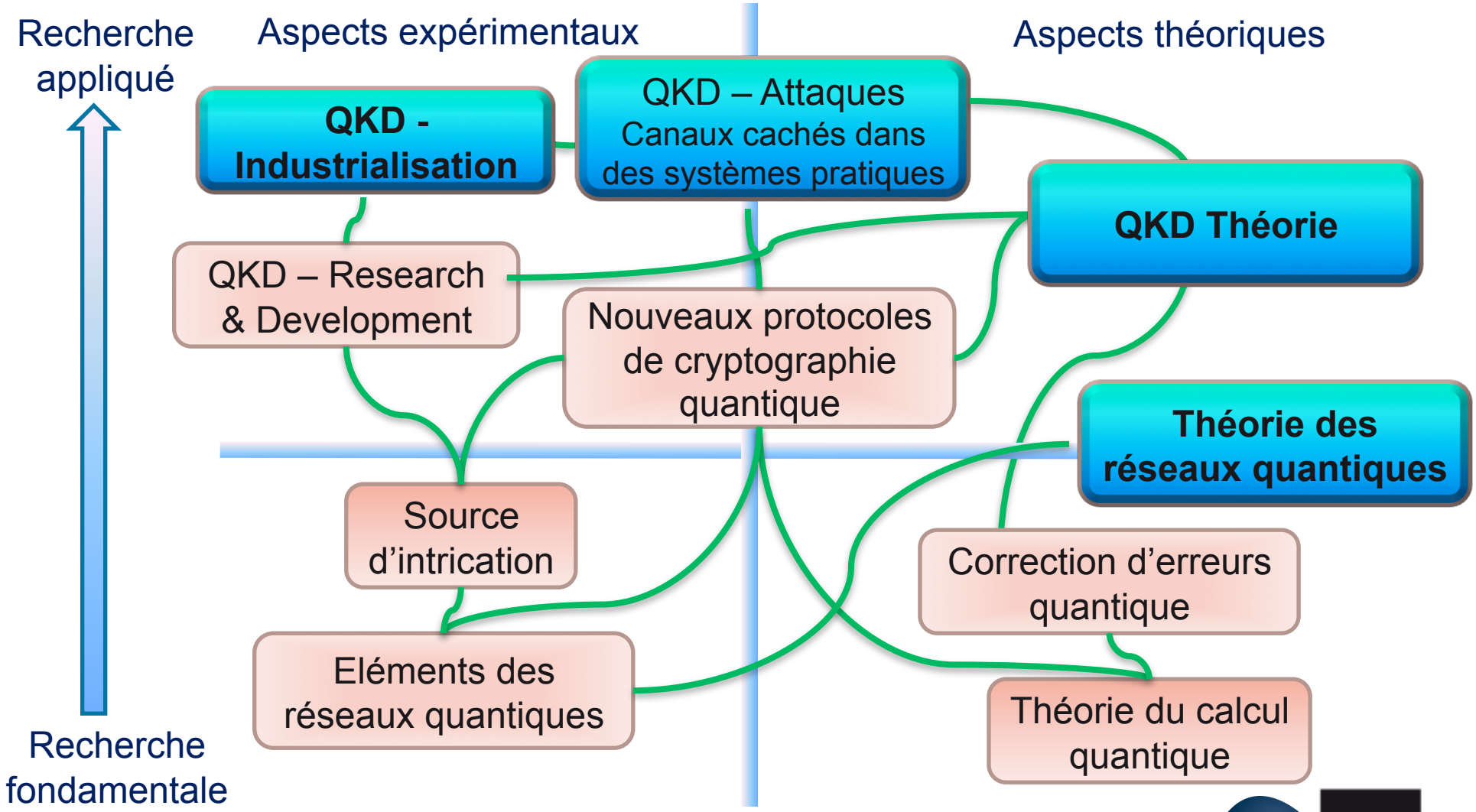
QKD en voie d'industrialisation => Course technologique pour la performance des liens



Intérêt majeur des protocoles inventés dans la thèse d'Anthony Leverrier : grande distance accessible, avec hardware plus simple => Axe de travail pour équipe IQ + SeQureNet

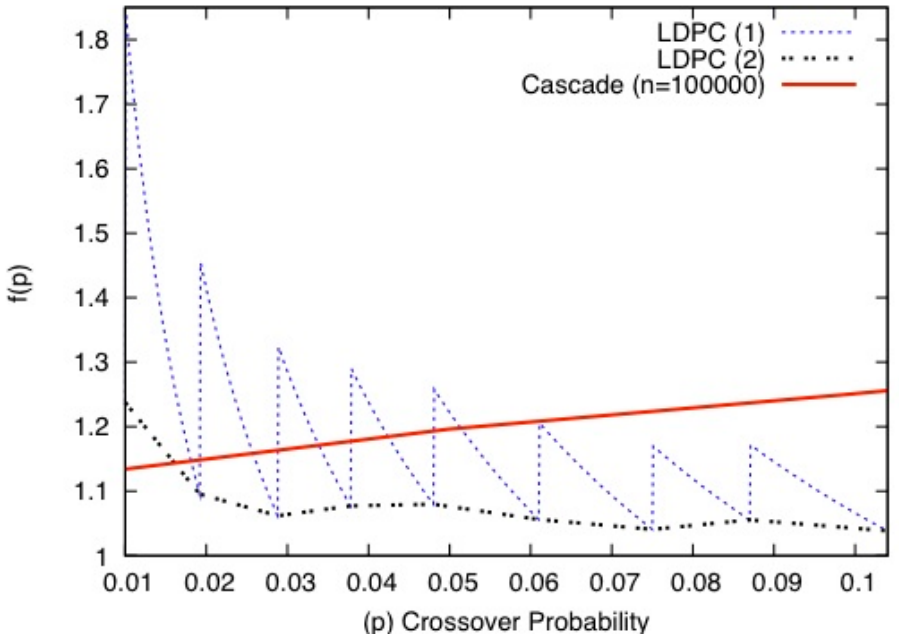
- Cependant, l'amélioration des performance n'est pas la seule métrique
  - Sécurité des implémentations QKD (attaques)
  - Usage / standardisation de la QKD
  - Optimisation du déploiement (topologie, coût, compatibilité avec réseaux optiques)

Choix pour cet exposé : la distribution quantique comme technologie télécom



Performance des liens QKD : Projet ANR Prospiq et distillation de clé

- Amélioration des codes correcteurs d'erreurs utilisés dans la distillation de clé : Utilisation de LDPC, optimisé pour le BSC
  - *D. Elkouss, A. Leverrier, R. Alléaume, J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution", International Symposium on Information Theory, ISIT, 2009*
  - Développement d'une pile logicielle intégrée et fonctionnelle
  - Démonstration (2010) de QKD avec source de photons uniques « industrielle » (Quantum Victoria), collaboration: ENS Cachan, EADS

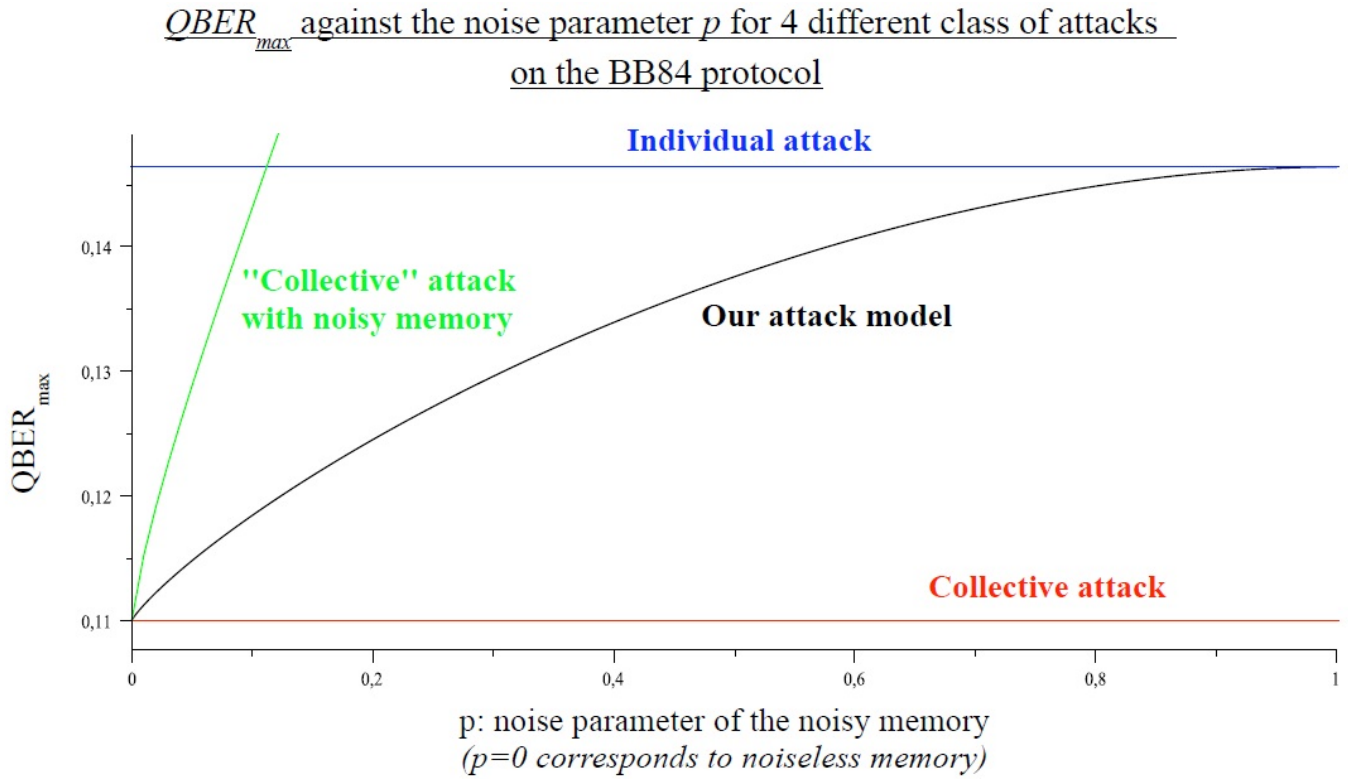


Projet ANR SEQURE : Intégration d'un lien quantique avec chiffeur commercial

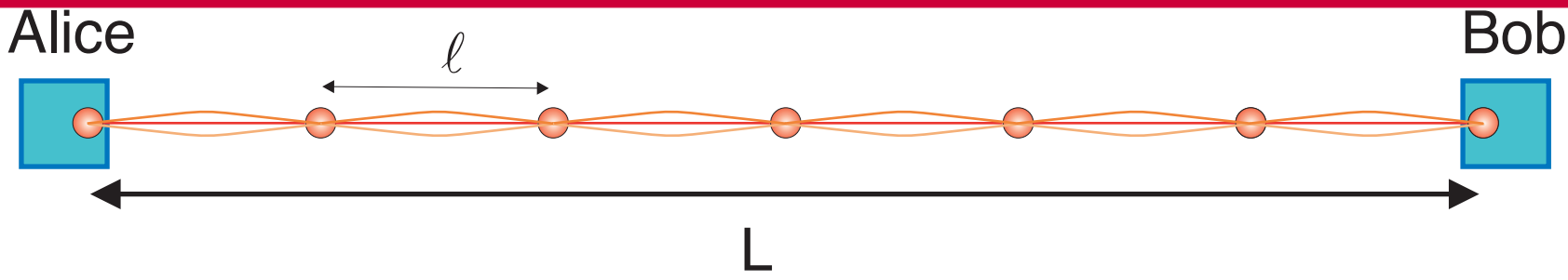
- Développement d'une interface logicielle dédiée (collaboration Thales Communications)
- SeQureNet : mise en place d'un démonstrateur sur réseau réel (avec système CVQKD)
- Collaboration sur la technologie CVQKD avec Institut d'Optique (Philippe Grangier, et Thales Research and Technology (Thierry Debuisschert)

Performance des liens QKD : importance du travail théorique (protocoles, preuves, modèmes de sécurité)

- **Cf protocole 4 états Anthony Leverrier**
- **Travail actuel : Modèle de sécurité et performances en cryptographie quantique, contre espion avec des limitations « physiques réalistes »**
  - Exemple : mémoire quantique bruitée, thèse Aurélien Bocquet



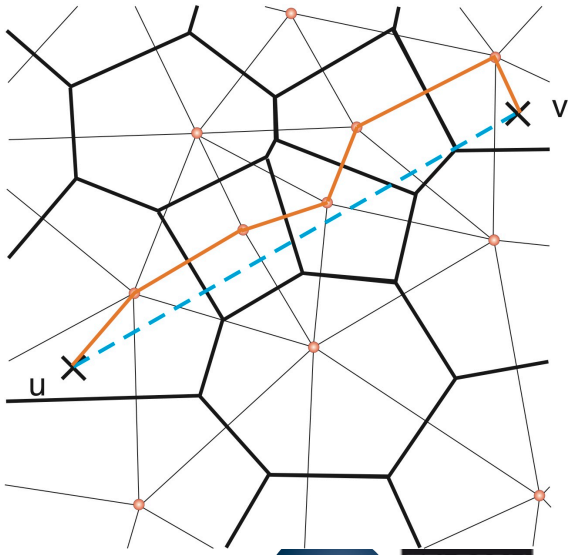
Optimisation topologique d'un réseau QKD : coût de déploiement comme métrique - implications



Modèle simple: chaîne unidimensionnelle

Cost function $$\mathcal{C} = C_{QKD}\,\frac{L}{l}\,\frac{R_T}{R(l)} = C_{QKD}\,\frac{L}{l}\,\frac{R_T}{R_0}e^{l/\lambda_{QKD}}$$

Optimum (coût minimum) $$l_{opt1D} = \frac{10}{\alpha\, ln(10)} \equiv \lambda_{QKD}$$



Généralisation à des modèles de réseaux 2D, étudiés avec les outils de géométrie stochastique
Topological optimization of quantum key distribution networks
R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus
New Journal of Physics, 11, 075002 (2009)

Plateforme Sécurité Quantique

Plate-forme expérimentale d'évaluation, d'attaque, de développement de contre-mesures et de certification de crypto-systèmes quantiques

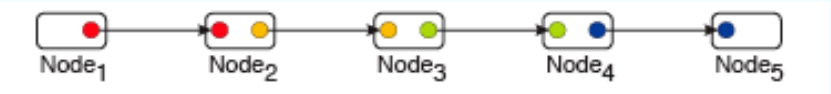
Permettre une évaluation crypto rigoureuse des systèmes quantiques indispensable pour les applications industrielles en sécurité (analogie avec industrie des cartes à puces)

- Mise en commun de moyens avec TSI/TOS (salles sous-sol bâtiment C)
- Asset majeur dans les projets collaboratifs dans lesquels nous sommes engagés
  - FREQUENCY, Q-CERT, CRYQ,
  - Standardisation de la QKD au sein de l'ETSI ISG, contacts avec l'ANSSI

(2004-2008) SECOQC La cryptographie quantique est étendue aux réseaux, permettant d'échanger des clés secrètes sur de grandes distances, avec des protocoles standardisés

Le concept: Trusted QKD network

Permet d'étendre la sécurité inconditionnelle sur des distances arbitrairement grandes.

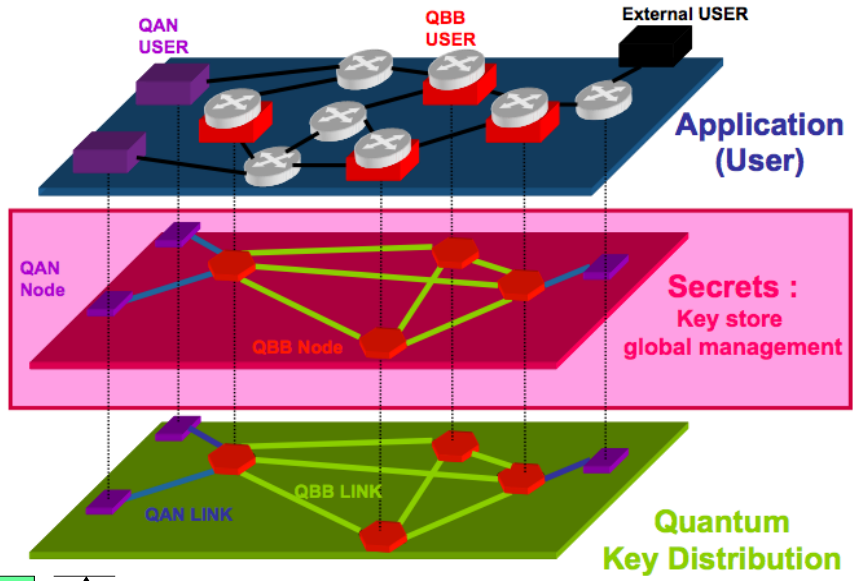


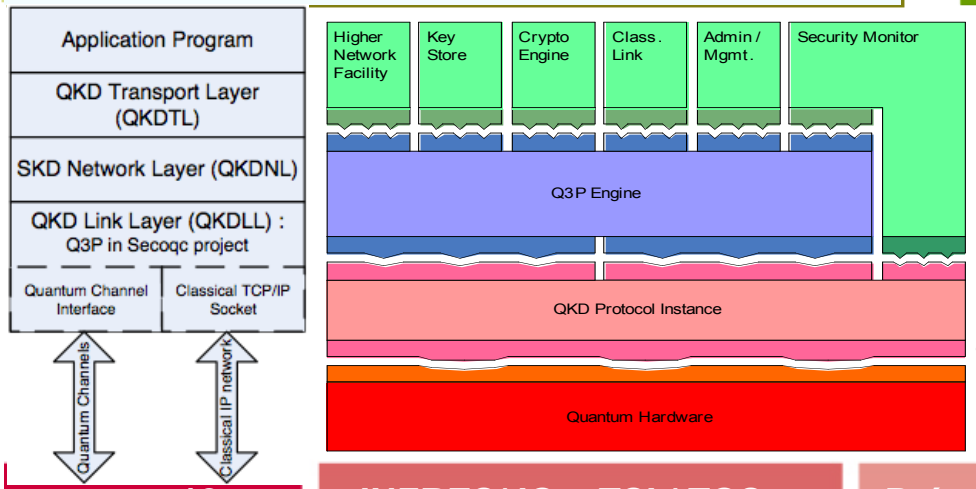
A chaque «hop», le message (clé de session) est déchiffré puis chiffré, en one-time-pad, avec une nouvelle clé QKD locale. $C_i = M \oplus K_{local,i}$

M apparaît en clair dans chacun des noeuds

⇨ Les nœuds doivent être de confiance

Une Architecture originale





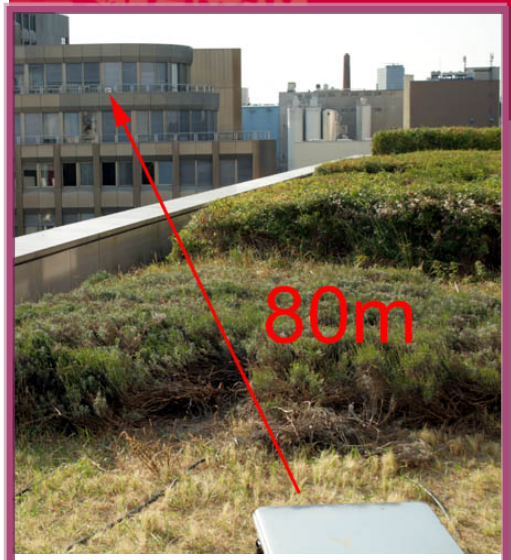
M. Dianati, R. Alléaume , M. Gagnaire, X Shenn, Journal of Security and Communication Networks 2008 quant-ph/ 0610202

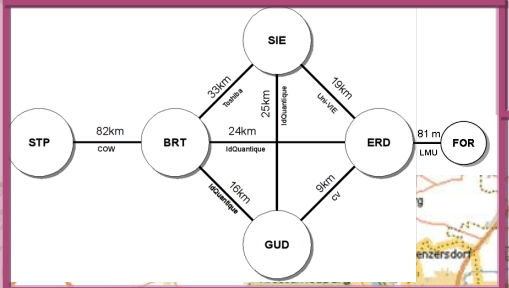
***Standardized** node architecture and interfaces between QKD devices and QKD network applications+*

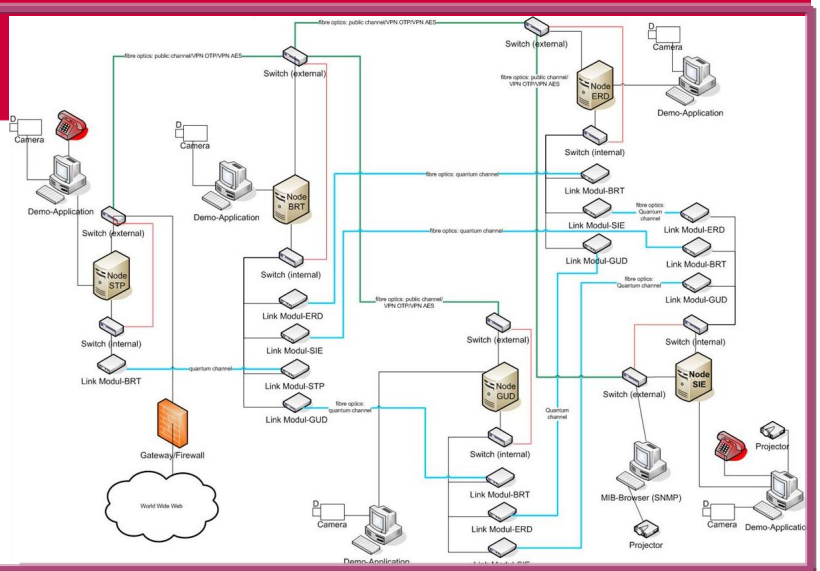
***Standardized** set of original nertwork protocols*

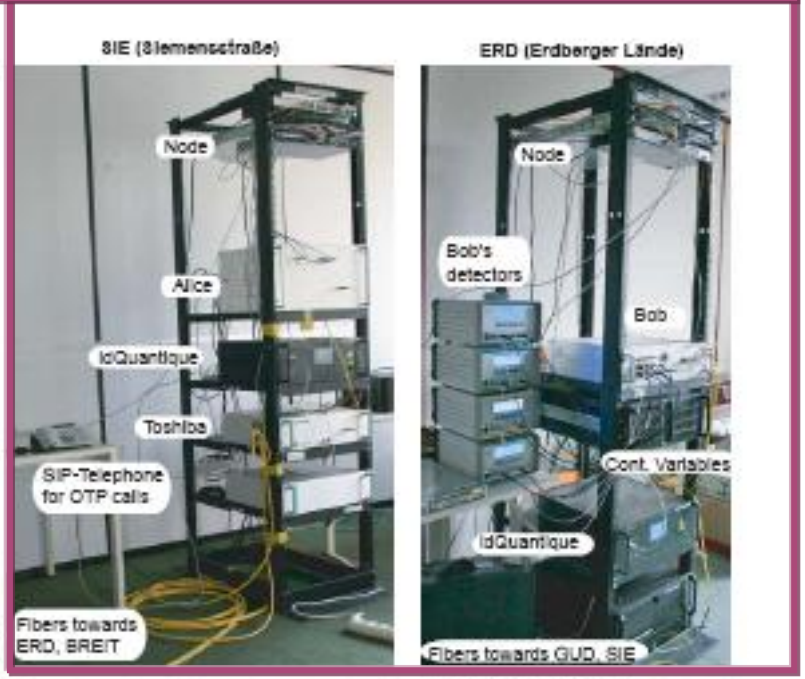
STANDARDISATION au niveau EUROPEEN (QKD ISG au sein de ETSI, depuis oct 2008)

Déploiement du premier réseau QKD européen

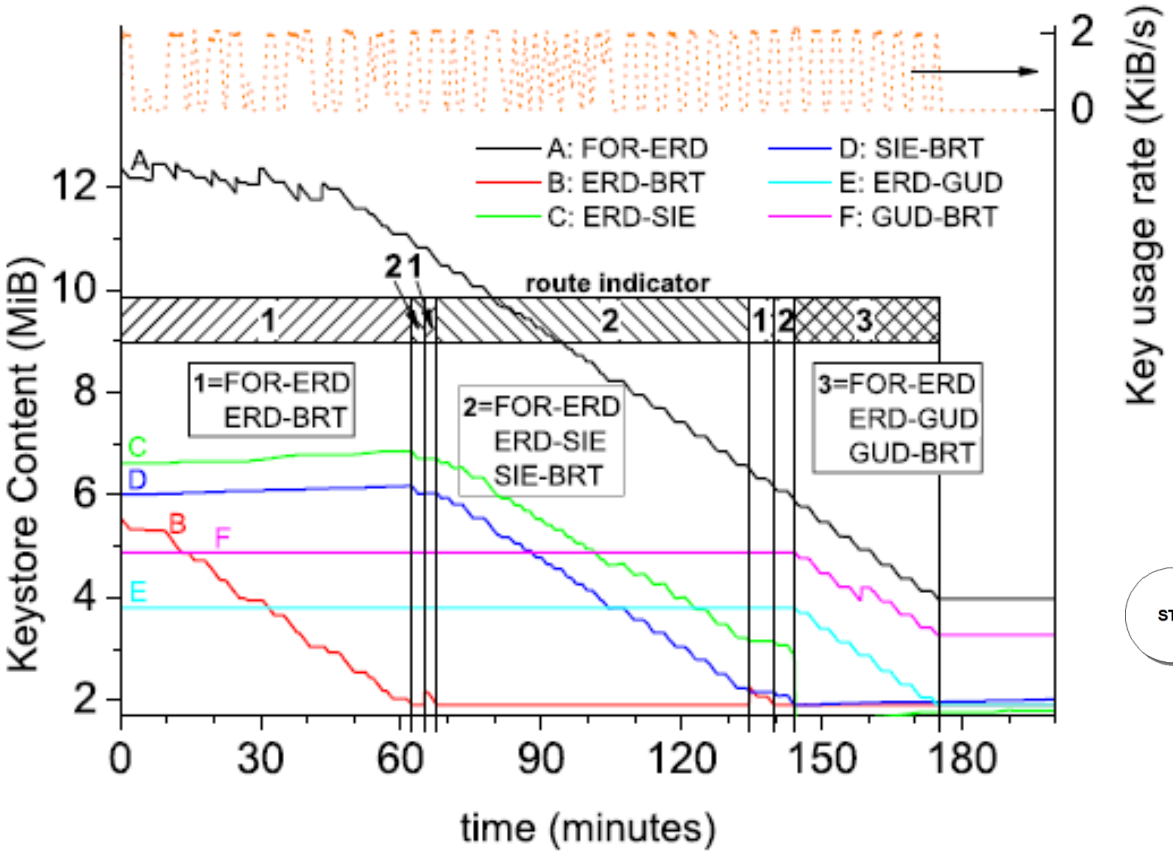


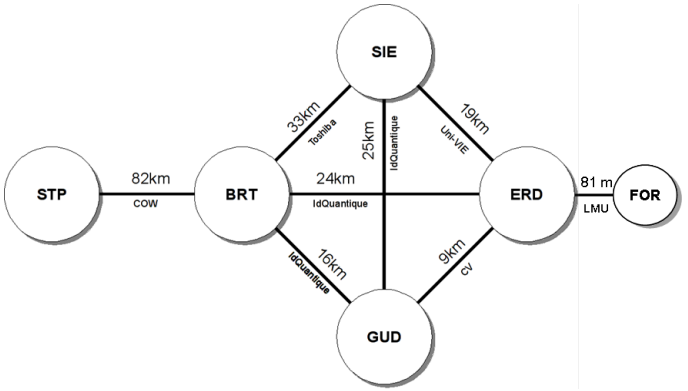






Réseau QKD SECOQC : Résilience par la redondance





SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

spin-off de Télécom ParisTech, créée en mai 2008

Intégration de la distribution quantique de clé dans des infrastructures de haute sécurité

- **Compétences en Cryptographie, Développement logiciel, Sécurité**
  - Avance technologique issue des projets SECOQC et SEQURE
  - Travaux à la source d'une norme européenne (QISG, ETSI)
  - Propriété intellectuelle sur combinaison QKD + chiffreur (partenariat Thales Com)

- **Stratégie de développement**
  - Valorisation de la PI accumulée par le groupe de recherche (notamment brevets)
  - Développement d'applications cryptographiques dédiées
  - Participation au développement du laboratoire d'évaluation et d'attaques (Q-CERT, FREQUENCY)

- **Marchés visés**
  - 1/ Défense - marchés gouvernementaux
  - 2/ Télécoms, Grands comptes et Banques

oséo Pour financer et accompagner les PME

ministère délégué à la recherche

Prix aux Concours National en 2007 et 2008

cnrs TELECOM ParisTech

Composition actuelle de l'entreprise (hors conseil scientifique)

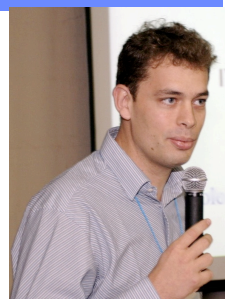
Nicolas Aliacar

Gérant et Co-fondateur

- **32 ans, X +** MBA
- **Expérience d'audit interne et de création d'entreprise**

Romain Alléaume

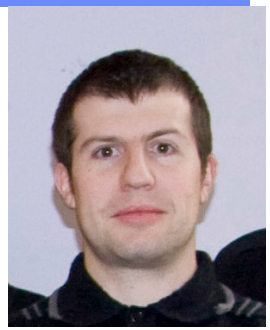
Conseiller Scientifique et Co-fondateur



- **32 ans, ENS Ulm + PhD**
- **Ing. Corps des Mines**
- **Maître de conférences à Télécom ParisTech**

Sebastien Kunz-Jacques

Directeur Technique



- **32 ans, ENS Ulm + PhD Cryptologie**
- **Ing. Corps des Mines**
- **Ancien ANSSI**
  - Evaluation robustesse de la cryptographie gvt. / indus.
  - Conseil aux industriels pour certification de mécanismes cryptographiques

Paul Jouguet

Ingénieur R&D

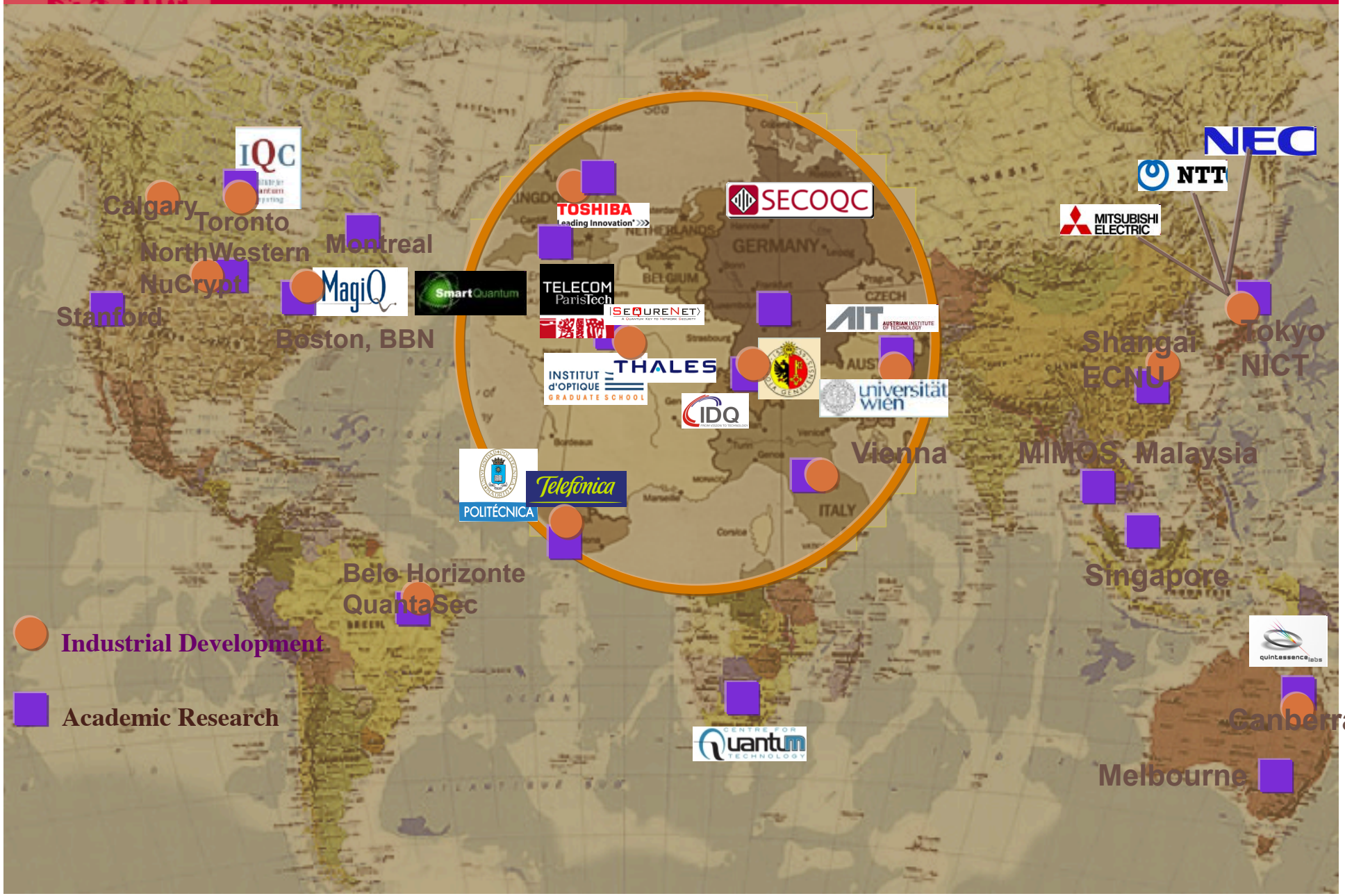
- **25 ans, Ingénieur TPT**
- **MSc Modélisation Aléatoire (Paris VII)**
- **Doctorant CIFRE**
- **Ancien Trésorier de la Junior Entreprise de TPT**

CONCLUSIONS - PERSPECTIVES

Mise en place d'une équipe complémentaire, avec des synergies fortes entre nos thèmes de recherche

- Véritable travail en équipe sur la quasi-totalité des thématiques évoquées
- Positionnée sur des thématiques actuelles, présentant des enjeux forts pour la communauté scientifiques, et pour lesquels on peut afficher des points différenciant
  - Théorie / expérience / intégration / développement industriel en QKD
  - Optique quantique et photons intriqués
  - Codes correcteurs comme outil de référence (crypto, calcul quantique)
  - Réseaux quantiques

SECOQC, ETSI ISG, FREQUENCY… : des connexions avec les pôles internationaux de références en information quantique



Enjeux – Perspectives

- **Mener à bien les projets engagés !**
  - Travail expérimental au sein du labo d'attaque débutera en juillet 2010
  - Kick-off FREQUENCY juin 2010
  - Kick-off Q-CERT juillet 2010

- **Matérialiser le virage industriel de la QKD par de nouveaux partenariats – nouveaux projets**
  - Problématique réseaux optiques => équipementier télécom
  - Problématique Sécurité / Crypto => DGA (collaboration SeQureNet)

- **Tenter de tirer partie, à travers les collaborations privilégiées entretenues avec les leaders français du domaine, de l'appel d'offre labo d'excellence**