



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



Equipe Information Quantique (INFRES)

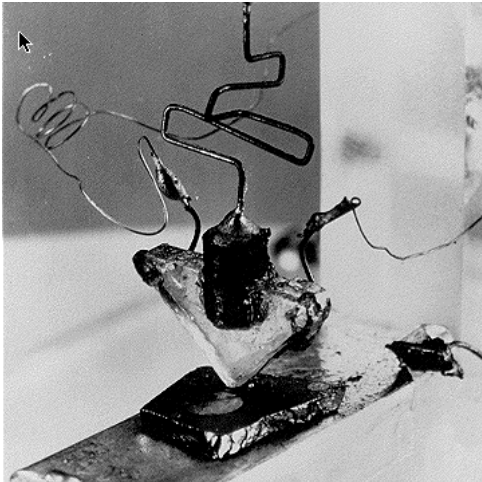
Equipe Traitement Optique du Signal (TSI)

Présentation et positionnement scientifique du projet

Bilan administratif

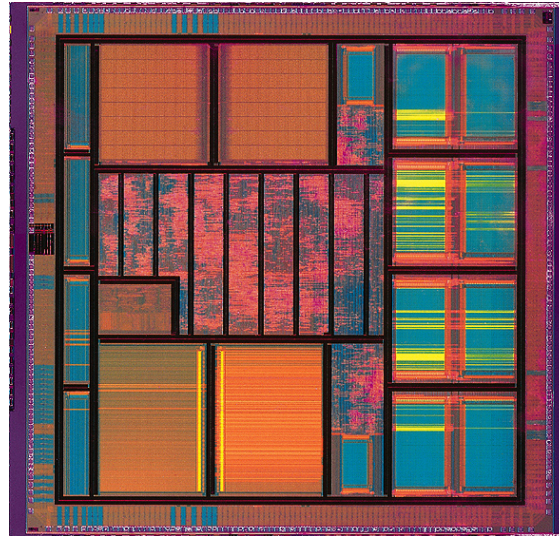


Pourquoi développer une activité en information quantique à TPT ?

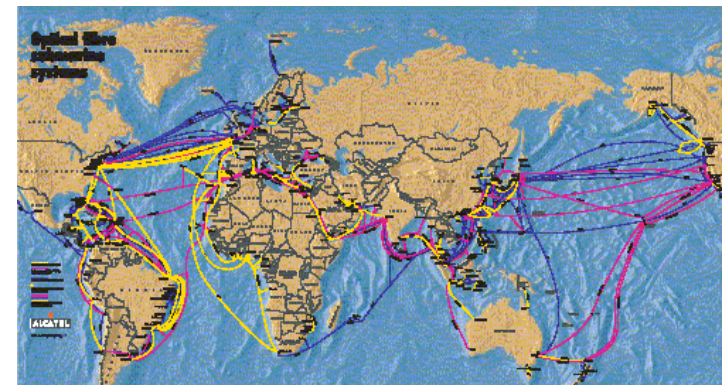


Transistor

Circuits intégrés



Laser



Physique quantique, une des théories scientifiques majeures du 20^{ème} siècle
→ fondement de la ***couche physique*** de la société de l'information

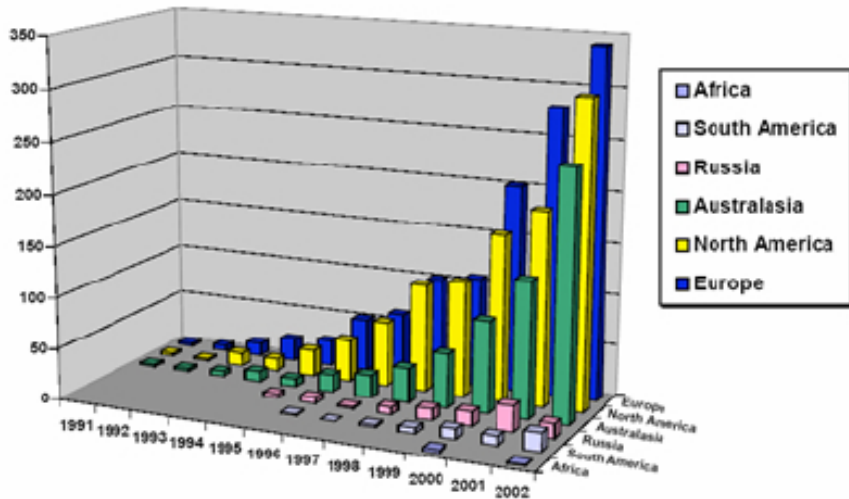
L'information Quantique : une révolution du traitement de l'information (communications mais aussi calcul)



« L'information quantique représente un renouveau radical des technologies de l'information, encore plus différent des technologies actuelles que nos ordinateurs ne sont différents du boulier »

William D. Phillips, Prix Nobel de Physique 1997

Un domaine en pleine effervescence au niveau international



Number of publications

In Quantum Information Processing and Communications, in peer-reviewed journals (per year, per geographic zone)

Source QUIPROCONE -> QIPC strategic report 2005

Des investissements majeurs dans les pays les plus dynamiques

- Canada (IQC Waterloo/ RIM) + Calgary + Montreal
- USA (MIT, Caltech, Stanford, DARPA...)
- Singapour National University
- Japon (NICT, NII, Toshiba)
- Chine (Key State Laboratory Heifei)
- Australie (Canberra, Brisbane)
- Europe tient la corde (un de ses domaines d'excellence, cf attribution ERC)



Historique du développement de la thématique Information Quantique à TPT : 2004-2007

- Lancement d'un séminaire interne d'introduction au domaine qui connaît un succès certain, avec 10 séances en 2004-2005
- 2005 : soutien du LTCl et décision d'un investissement exceptionnel: projet Kantik
- Au niveau Infres –TSI (avant tout TSI): Réalisation d'une source de photons intriqués, article BUP.
- Structuration d'un enseignement commun et de projets de recherche autour de l'optique quantique, optique non linéaires, photons intriqués (idée d'interfaces).
- Rôle structurant à INFRES du projet européen SECOQC, travaux et collaborations avec les leaders européens du domaine. Reconnaissance à travers le travail mené (nomination steering committee, editing author du white paper SECOQC, etc..).
- En parallèle à SECOQC développement d'une activité théorique en information quantique: Capacité zéro-erreur quantique, Sécurité de la QKD (Anthony Leverrier), optimisation topologique des réseaux QKD, Codes correcteurs pour la QKD

2007-2009 : capitalisation sur les premiers succès, extension de l'équipe, accroissement du rayonnement

- 2 Candidature CNRS en 2008, signe de l'attractivité d'un projet d'une équipe d'information quantique à TPT.
- 2007 Obtention du projet ANR SEQUIRE : vers l'industrialisation de la QKD (collaboration Thalès et Institut d'Optique)
- 2008 Succès de la démonstration internationale SECOQC => vers des standards européens à partir des protocoles spécifiés à TPT (ETSI QKD ISG).
- Réflexion autour des perspectives industrielles de la QKD + lauréat Concours, Création Entreprise Innovante (2007-2008) => **création de SeQureNet (2008)**
- **2 recrutements CNRS en 2009: Eleni Diamanti, CR2, (classée 2^{ème}, 08), Damian Markham, CR1 (classé 3eme, 07)**
- Obtention d'e-QUANET en 2009
- Succès de la thèse d'Anthony Leverrier, renforcement de la collaboration avec Philippe Grangier (7 papiers acceptés / publiés, 1 brevet,)
- Début de la thèse d'Aurélien Bocquet (CER) : Nouveaux modèles de sécurité en cryptographie quantique
- Lancement de QuPa : Cycle de conférence sur l'information quantique à Paris

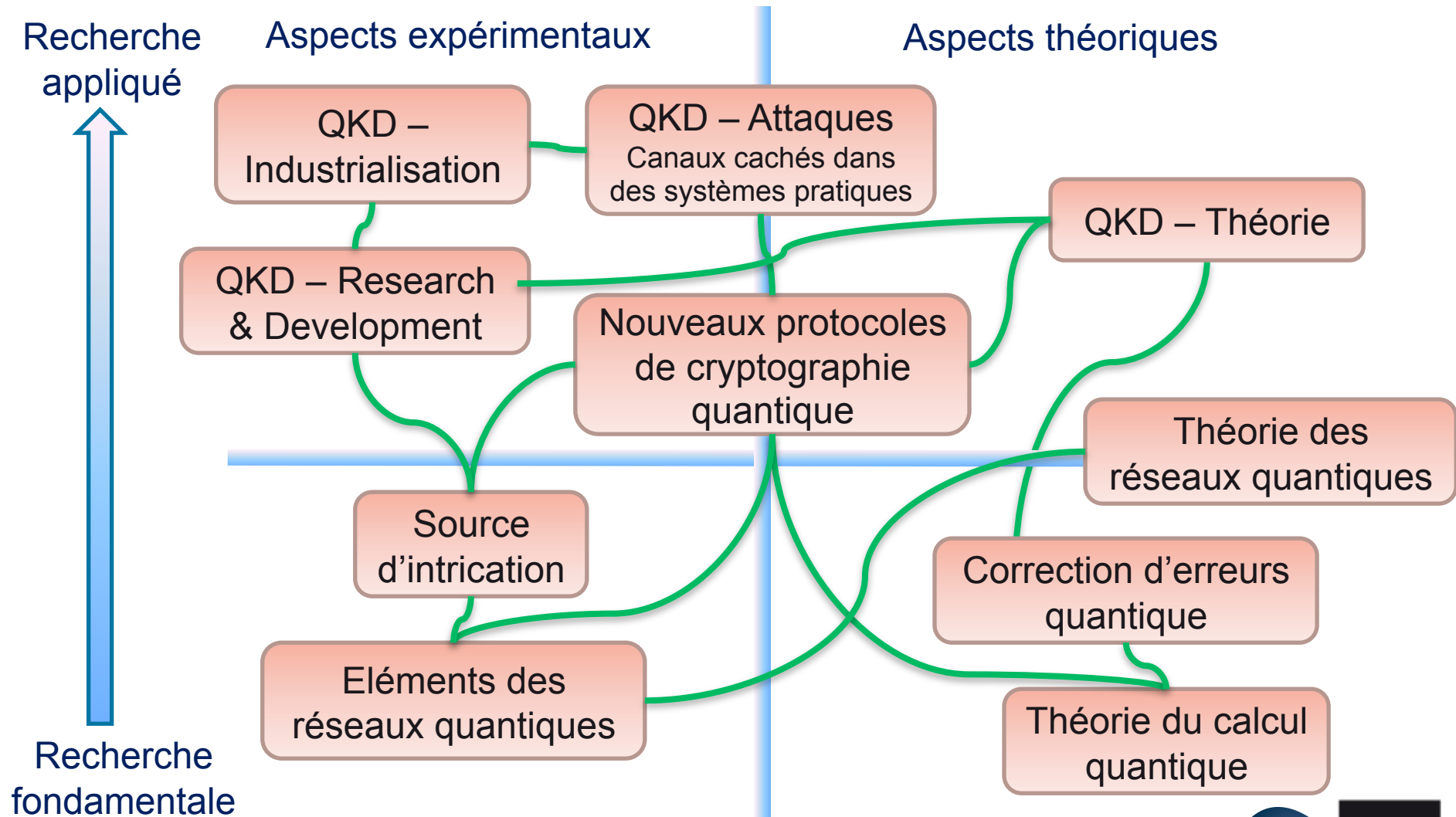
2009- 2010 : succès dans les appels à projet, mise en œuvre d'un projet scientifique ambitieux et structuré

- 2009 : 3 succès à des réponses à AAP sélectifs
 - ANR Blanc internationale FREQUENCY : Fundamental Research on Networks and Cryptography – Collaboration avec les équipes canadiennes en pointe au niveau internationale en information quantique / cryptographie quantique (IQC, Calgary, Montreal)
 - Projet européen Industry- Academia Partnership Pathway Q-CERT : collaboration avec IdQuantique et Université de Genève autour de la certification de systèmes QKD de nouvelle génération
 - AAP SESAME (Region Ile de France) : Projet « Sécurité Quantique » => financement d'une plateforme expérimentale pour les attaques et le développement de contre-mesures
- Mise en place de la plateforme Sécurité Quantique
- Arrivée de doctorants, post-docs (Anne Marin, Zizhu Wang, Sara Felloni), grâce au soutien de l'Institut Télécom (Futur et Ruptures) et du département INFRES (Carnot)
- Structuration de la valorisation d'éléments de PI à travers SeQureNet

Equipe Infres / Information Quantique + SeQureNet (janvier 2010)

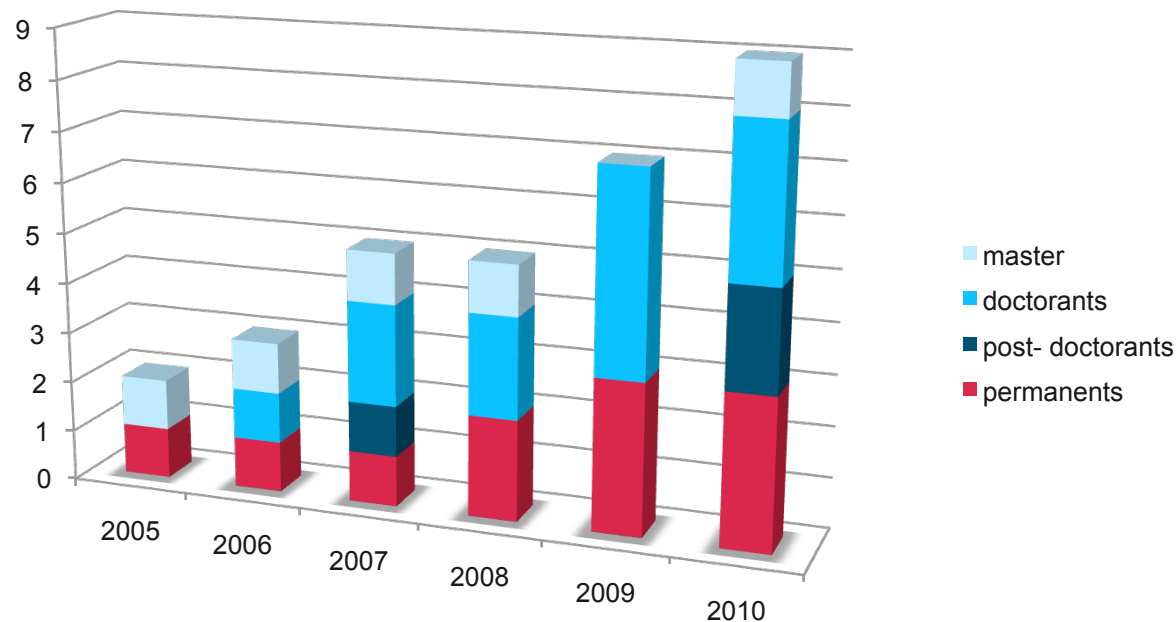


Vue d'ensemble de notre recherche





Bilan chiffré Infres / IQ : Personnel



Un développement dynamique, dont les facteurs clés de succès sont la capitalisation sur les collaborations scientifiques de premier plan (projet européen SECOQC), le soutien du CNRS, le soutien du LTCI / Institut Télécom



Bilan chiffré INFRES / IQ : Contrats et Ressources

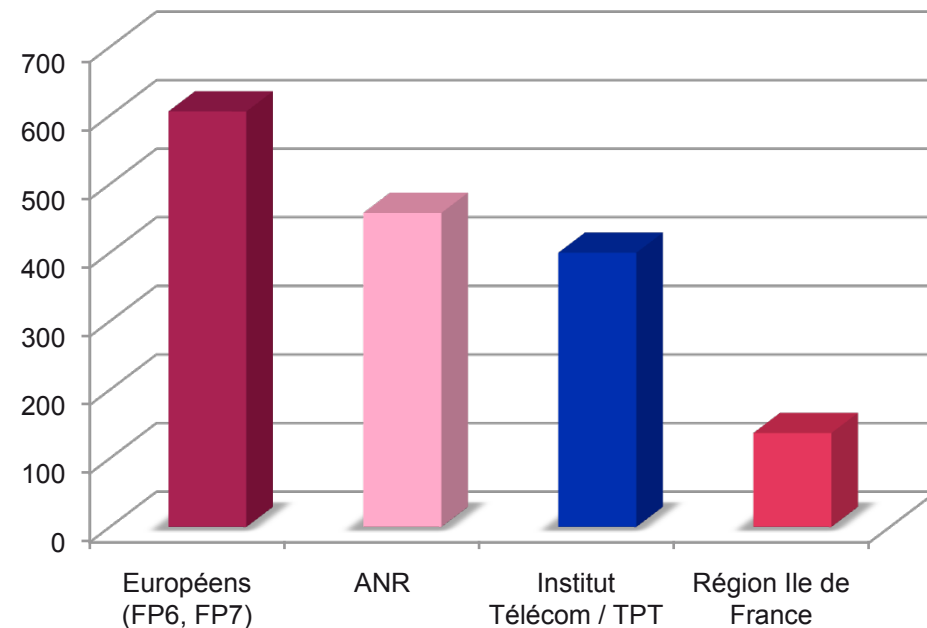
- SECOQC, Projet Européen Intégré FP6, Trust & Security, 438 k€ (avr. 2004 - oct. 2008)
- PROSPIQ, Projet ANR PNANO, 83 k€ (jan. 2007 - juin 2010).
- SEQUIRE, Projet ANR SeSUR, 125 k€ (jan. 2008 - dec. 2010).
- COCQ, Projet ANR Domaines Emergents, 68 k€ (jan. 2009 - dec. 2011).
- CRYQ, Projet ANR Jeunes Chercheurs, 45 k€ (2009-2011)
- SESAME Sécurité Quantique, 447 k€ en dépenses d'équipement (2008-2010)
 - Prêt d'équipement lien CVQKD (Institut d'Optique) : 50 k€
 - 60 k€ financement sur contrats TSI + 60 k€ de prêts
 - 100 k€ financement sur contrats INFRES (SECOQC, SEQUIRE)
 - 75 k€ financement Dir Recherche
 - 80 k€ financement Institut Telecom
 - 137 k€ financement région Ile de France
- FREQUENCY, Projet ANR Blanc International, 159 k€ (janv 2010-déc 2012)
- Q-CERT, Projet européen IAPP, 168 k€ (juill 2010- juin 2013)
- Q-PRIM (Post-doc futur et Ruptures) : 45 k€ (2010-2011)
- 1 bourse de thèse Carnot INFRES (Zizhu Wang, 2009-2012), 1 bourse de thèse Futur et Rupture (Anne Marin 2009-2012)

Bilan chiffré INFRES / IQ : Contrats et Ressources

[Données consolidées depuis 2005]



Européens (FP6, FP7)	606
ANR	458
Institut Télécom / TPT	400
Région Ile de France	137
Externes	1201
Internes (IT / TPT)	400



Capacité à bâtir des collaborations avec des équipes de niveau international
Capacité à trouver des financements pour notre recherche
Soutien de l'Institut Télécom / TPT important et apprécié 😊



Bilan chiffré **INFRES IQ + TSI/ TOS** : Production scientifique (2006 – 2010)

- **Publications dans des revues internationales : 46, avec plus de 800 citations**

2 *Phys. Rev. Lett*

10 *Phys. Rev. A*

6 *New J. Phys.*

6 *Opt. Lett./Opt. Express*

1 chapitre de livre

- **Conférences internationales invitées : 21**

Tropical QKD (Canada), ICQIT, UQCC (Japan), QIPC (Spain), CLEO (USA), QICS (Austria)

- **Conférences internationales avec actes : 20**

- **Présentations et séminaires : plus de 50**

- **Comités de conférences**

GdR Information Quantique: Fondements et Applications, 2010 – 2013

Quantum Africa 2011, CLEO Europe 2011, Post-Quantum Security Models 2010, DQC Summer School 2010, DCM 2010, ICQNM 2008

INFRES IQ + TSI/ TOS :

Liste des publications principales depuis 2006

Physique

- R. Alléaume, F. Roueff, E. Diamanti, N. Lütkenhaus, "Topological optimization of quantum key distribution networks", **New Journal of Physics**, 11, 075002 (2009)
- A. Leverrier, P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with a discrete modulation", **Phys. Rev. Lett.** 102, 180504 (2009)
- D. Markham, B. Sanders, "Graph states for quantum secret sharing", **Phys. Rev. A** 78 042309 (2008)
- A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, P. Grangier, "Multidimensional reconciliation for continuous-variable quantum key distribution", **Phys. Rev. A** 77, 042325 (2008)
- M. Hayashi, D. Markham, M. Muraio, M. Owari, S. Virmani, "Bounds on Multipartite Entangled Orthogonal State Discrimination using Local Operations and Classical Communication", **Phys. Rev. Lett.** 96, 040501 (2006)

Informatique

- L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, T. Länger, "Security of trusted repeater quantum key distribution networks", **Journal of Computer Security** 18(1), 61 (2010)
- E. Kashefi, D. Markham, M. Mhalla, S. Perdrix, "Information Flow in Secret Sharing Protocols", DCM 2009, **EPTCS** 9,87 (2009)
- M. Dianati, R. Alléaume, M. Gagnaire, X. Shen, "Architecture and protocols of the future European quantum key distribution network", **Security and Communication Networks** 1(2), (2008)

Optique

- Q. He, I. Zaquine, R. Frey, R. Andre, G. Roosen, "Efficient Bragg diffraction in thin semiconductor 2D gratings", **Opt. Lett.** 33, 2868 (2008)
- E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low-jitter up-conversion detectors", **Opt. Express** 14, 13073 (2006)
- E. Diamanti, C. Langrock, M. M. Fejer, Y. Yamamoto, H. Takesue, "1.55 μ m photon-counting optical time-domain reflectometry with a single-photon detector based on upconversion in a PPLN waveguide", **Opt. Lett.** 31, 727 (2006)

Equipe TSI/TOS : Problématique

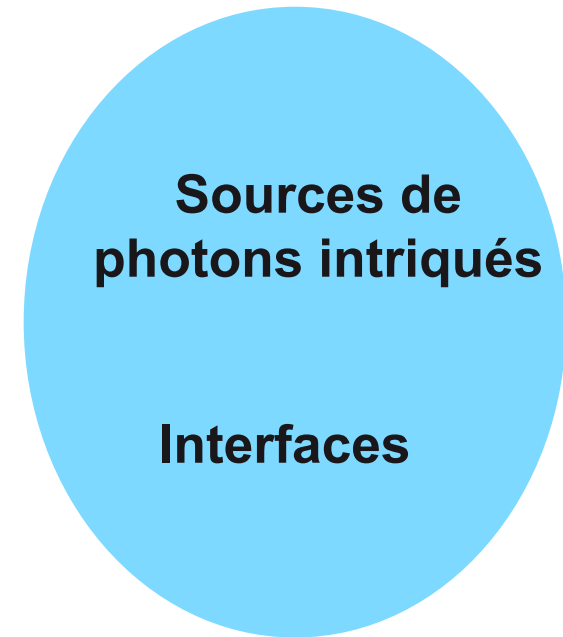
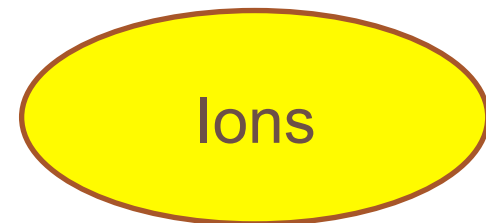
Qubit = système à deux états



Propagation



Traitement



Optique non linéaire



Optique non linéaire pour les communications quantiques

L'équipe :

Jean-Loup Smirr : doctorant

Romain Alléaume

Eleni Diamanti

Robert Frey

Gérard Mouret

Isabelle Zaquine

} permanents

Premiers financements

Acronyme	Sujet	Organisme	Budget / budget total
Kantik 2005	Source de photons intriqués en polarisation à 810nm	CNRS	50/100 k€
J-L. Smirr 2007-2010	Eléments des futurs réseaux de communications quantiques	EDOM Institut TELECOM	Bourse MESR + 3 mois
Y. Menesguen (2007)	Interface de changement de longueur d'onde	Département TSI	Postdoc 8 mois
FRIQ 2007	Fonctions Réseaux pour l'Information Quantique	Institut TELECOM	40/40 k€
IMPROC 2007-2009	Interface Mémoire-PROpagation pour les Communications quantiques Partenaire : LCFIO	Région Il de France C'Nano	35/50 k€
2008	Amplificateur Erbium	Fonds Carnot	30 k€
2008	Fabry-Perot d'analyse spectrale et analyseur de spectre optique	CNRS	25 k€
2008	Détecteur de photons uniques	Département TSI	30 k€



Communications quantiques : premier bilan

- **Mise au point d'une source de photons intriqués en polarisation à 810 nm**
 - Pour l'enseignement (Bulletin de l'Union des Physiciens)
 - Applications à des tests de cryptographie (INFRES)
- **Etudes de faisabilité de l'interface de changement de longueur d'onde**
 - Théorique
 - expérimental
- **Source de photons jumeaux à 1550 nm basée sur la fluorescence paramétrique**
étude du filtrage $\Delta\lambda=100 \text{ nm} \longrightarrow \Delta\lambda=100 \text{ fm}$
- **Obtention du contrat ANR eQUANET avec partenaires prestigieux.**