COMMUNICATIONS QUANTIQUES

INTERVENANT :

Mathias VAN DEN BOSSCHE - Thales Alenia Space

Au programme

- **Communications quantiques**
  - → En deux mots…
  - → Maturité mondiale
  - → Principes stratégiques F

- **Réseaux d'information quantique /QIN**
  - → objectifs : vers une téléportation spatiale
  - → actions en cours : ligne de projets QINSAT
  - → derniers résultats de nos équipes

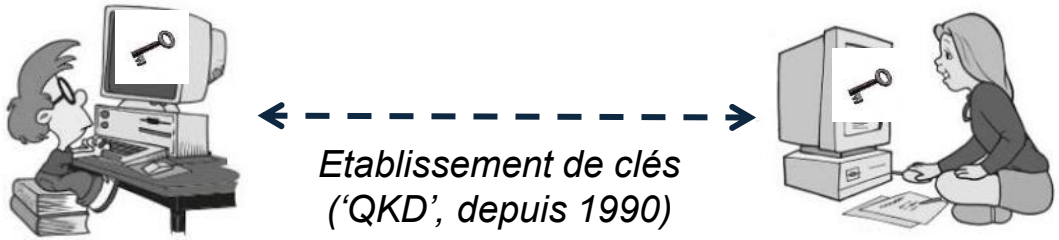
- **Etablissement de clés par voie quantique / QKD**
  - → La question des nœuds de confiance
  - → projets en cours et résultats : UE, ESA, HISPASAT, ASI

COMMUNICATIONS QUANTIQUES : E QU'ES AQUÒ?

Communications: Deux utilisations de la physique quantique

Partager du hasard confidentiel...

…0101010010110101…



Etablissement de clés ('QKD', depuis 1990)

…0101010010110101…

… ou mieux, partager des états

$|\Psi\rangle=\alpha|\uparrow\rangle+\beta|\downarrow\rangle$

téléportation (depuis 1997)

$|\Psi\rangle=\alpha|\uparrow\rangle+\beta|\downarrow\rangle$

Quantum-Secured Networks

Sécurité inconditionnelle

+

Sécurité persistante

+

Défense en profondeur

Quantum-Information Networks

=> Réseaux de

- Calculateurs quantiques
- Capteurs quantiques
- Sécurité en bonus

C'est la priorité F

Etat de l'art mondial

Terrestre

1ere génération sur étagère

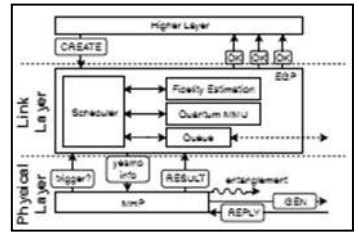
- IDQ/IonQ, Toshiba, Huawei…Thales
- Réseau étendu en…
- Discussi…n sécurité

Mais acceptabilité?
cf dernière partie

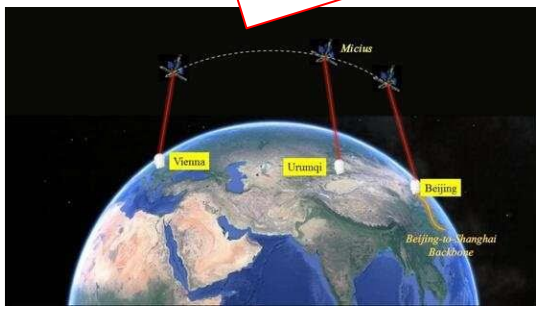
Des réseaux expérimentaux

- Distribution d'intrication SOPHIA-NICE-OCA (F)
- Intrication entre diamants à Delft (NL)
- Intrication de terres rares à Barcelone (E)
- Distribution d'intrication Long Island (US)

Standardiser l'architecture réseau

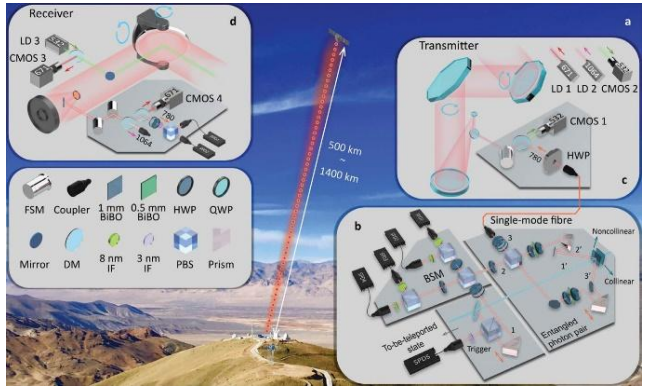


Spatial



Micius (Chine), 2018

Clés établies entre Pekin et Vienne, chiffrement de communications.



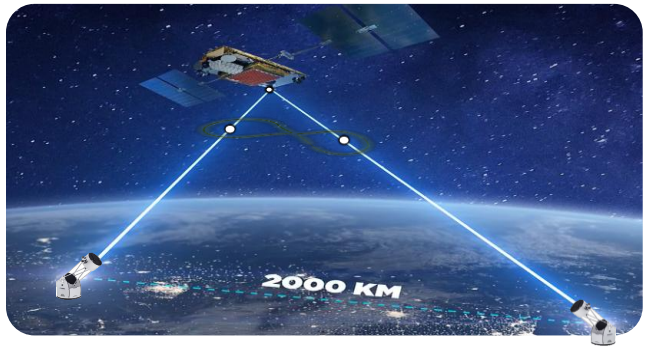
Micius (Chine), 2019

Connecté 2 stations distantes de 1200km grâce à un satellite en orbite basse.

Clés par voie quantique (QKD)

Réseaux d'Information Quantique (QIN)

Stratégie des acteurs en France



Les réseaux d'information quantique (QIN) sont le véritable enjeu

- Performance et résilience des infrastructures de calcul
- Multi-applications, potentialité commerciale de type internet
- Communications sécurisées par construction
- Mais défis significatifs : investissement long terme, retards longs à rattraper (cf. IA en Europe…)

⇒ Prototyper des réseaux sols et leurs connections spatiales dès que possible
⇒ Participer aux forums internationaux pour l'intéropérabilité

L'établissement de clés de chiffrement par voie quantique

- est bien connu de certains acteurs F : U. Nice, Sorbonne, Thales R&T, ADS, eXail, Orange, etc
- intéresse des acteurs européens qui acceptent ses faiblesses temporaires
- partage de nombreuses technologies avec les QIN

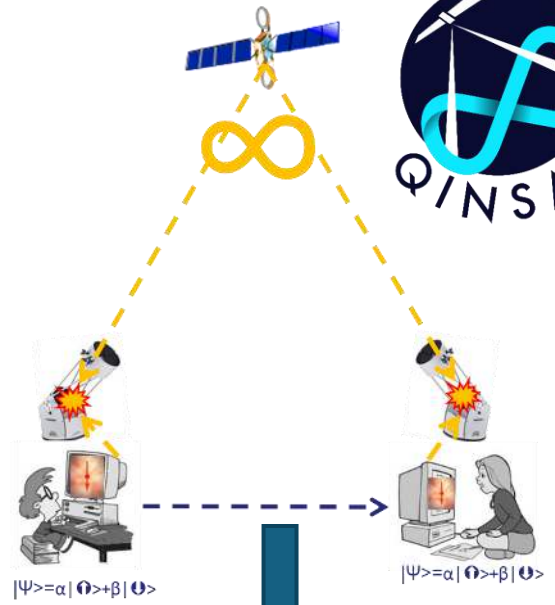
⇒ Répondre présent aux demandes des entités intéressées
⇒ Organiser les synergies pour l'avancée des technologies

RESEAUX D'INFORMATION QUANTIQUE

Vers une téléportation spatiale

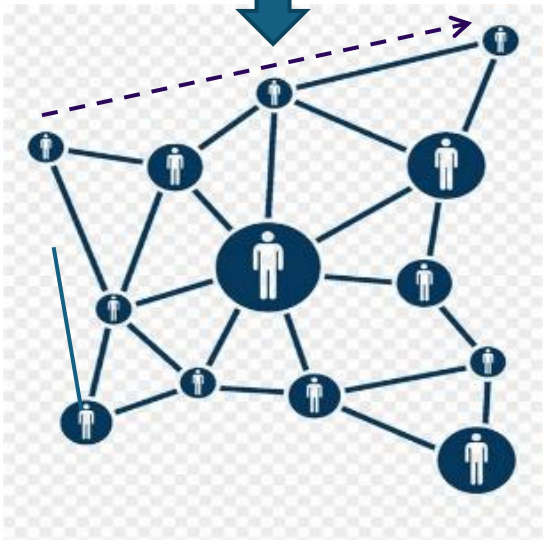
Téléportation d'états

- Transporter de l'information quantique se fait en mettant en œuvre un protocole de *téléportation d'état* (Zeilinger, 1997)
- Il exploite les corrélations entre deux objets quantiques préparés ensemble puis séparés (→ photons intriqués)
- Pour connecter deux stations au sol, distribuer des photons intriqués depuis un satellite en orbite basse

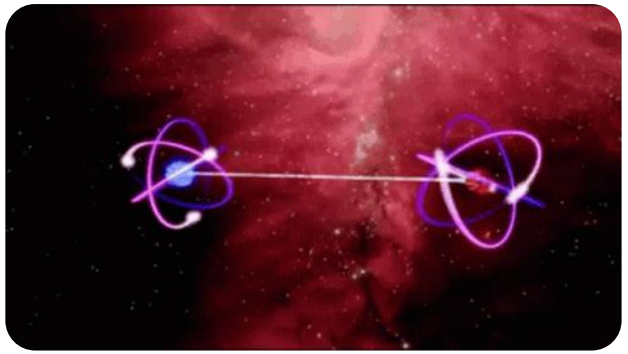


Plan d'action

1. QINSAT :
   - Un satellite qui émet des *paires de photons intriqués*
   - Deux stations 'nœuds spatiaux' pour collecter et *consommer l'intrication*
   - Evaluer les performances, améliorer les solutions
2. Réseau expérimental
   - *Se connecter aux nœuds terrestres* déployés en parallèle
   - *Equiper les stations de mémoires quantiques* pour stocker l'intrication en attendant de communiquer
   - Valider les *protocoles d'opération du réseau* (commutation et routage d'intrication, etc)
3. Proposer un système opérationnel aux fermes de calcul quantique



Les projets passés et en cours

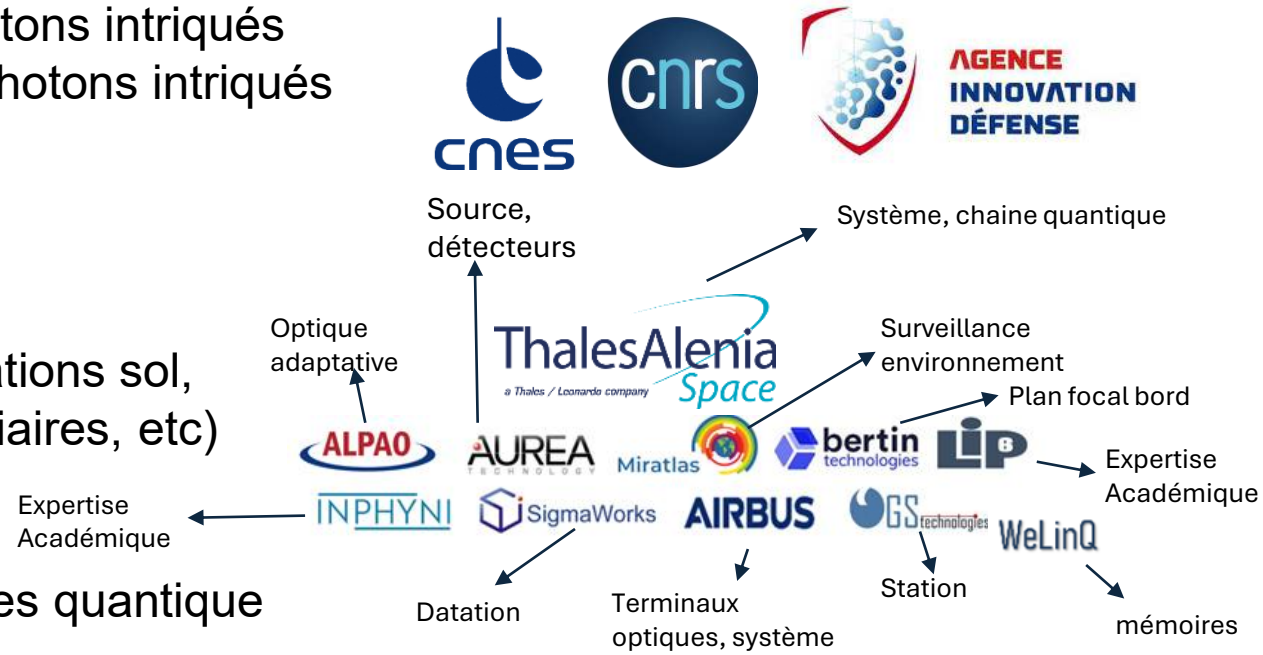


Avancées 2019-2024

- Phase 0 (TAS/CNES): specs utilisateur, architecture globale, rôle du satellite, technologies critiques
- SoluQS (TAS/AID) : prototypage d'une source de photons intriqués
- RouteRIQS (TAS/CNES) :
- ProRIQS (TAS/CNES) : étude et validation de techno pour récepteur sol
- HPEPS (ADS/QTLabs/EU): prototypage source de photons intriqués
- IQPHOS (ADS/AUREA/ESA): prototypage source de photons intriqués

Equipe de France 2022-2025+ : travail en écosystème

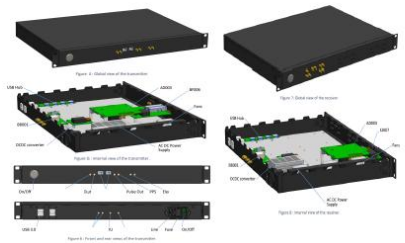
- TeQuanTs (ESA/CNES/TAS/ADS)
  - → architecture plus raffinée (simulation),
  - → maturation technologique (source, optique bord, stations sol, détecteurs, datation / synchronisation, canaux auxiliaires, etc)
  - → Déploiement d'un laboratoire commun au CNES
- QCTM (ESA/ADS): technologie télescope spatial
- QuTechSpace (ADS/QTLabs/ESA): sources photoniques quantique spatiales
- QuantiTag (ESA/TAS) : système de datation embarqué
- Phase A QINSAT (CNES/TAS/ADS):
  - → définition détaillée de la mission
  - → préparation du programme satellite.



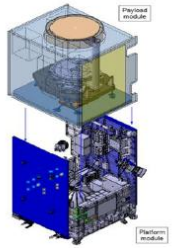
Resultats récents sur les QIN spatiaux

Optical Ground Terminal

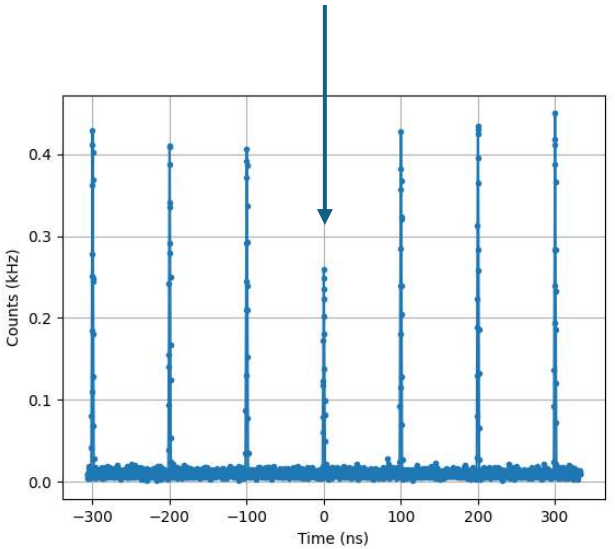
Time-Synchronization



On-Board Optical Terminal



Creux de Hong-Ou-Mandel: nous savons maîtriser l'indiscernabilité des photons



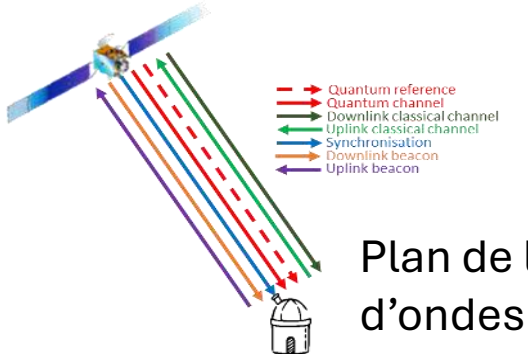
Single Photon Detector

Adaptive Optics

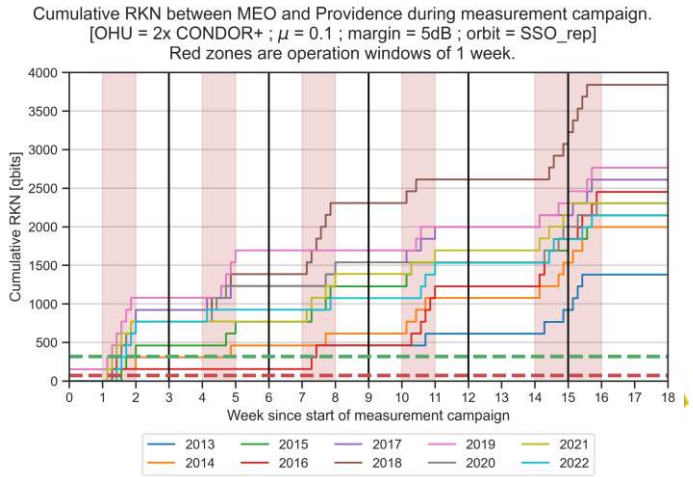
Integrated Sky Monitor

Entangled Photon Source

Premiers matériels développés



Plan de longueurs d'ondes bord-sol



Niveau de service et scenarios météo

ETABLISSEMENT DE CLÉS PAR VOIE QUANTIQUE

La question des ‘nœuds de confiance’

Problème

- Algorithme de Shor - les ordinateurs quantiques vont percer le chiffrement à clés publiques (→ ~~HTTPS~~…)
- Etablir des clés par voie quantique éliminera cette vulnérabilité : à terme solution parfaite, mais…

Protocoles sans intrication

- Simples à mettre en œuvre
- Sécurité par lien, pas de bout en bout
- Nœuds intermédiaires ‘de confiance’ hackables

=> Acceptabilité en question

Protocoles avec intrication

- Nécessitent d’avoir un QIN
- Mais plus de nœud intermédiaire
- Sécurité de bout en bout

=> Acceptabilité techniquement indiscutable

- Peu d’entités connaissent à la fois la sécurité des communications *et* la physique quantique, ce qui explique le buzz sur cette application mal née
- Il existe des algorithmes classiques pour des clés publiques ‘post quantiques’ . Plus gourmands que RSA, sans preuve de sécurité définitive => *solution temporaire*
- Quand les QIN seront déployés, les *clés établies avec de l’intrication* seront la solution.

Les projets passés et en cours

Avancées 2002-2019

- Thales R&T démontre la QKD ‘à variables continues’
- Eutelsat et l’ESA étudient un système spatial
- La stat-up SequreNet se monte puis ferme
- La Commission Européenne Prépare le projet EuroQCI
- L’ESA planifie le volet spatial d’EuroQCI : SAGA

Maquette chaine GEOQKD

Projets Européens

UE

- Deux études de faisabilité EuroQCI (Thales+Deutsche Telekom, Airbus+Orange)
- Développement de boitiers QKD terrestres (Thales+eXail)
- Réseaux expérimentaux : ParisRegionQCI, FranceQCI
- Définition d’un centre européen de test et d’homologation: Petreus, Nostradamus
- Poursuite du projet EU6QCI E2E system

ESA

- 3 phases A/B1 SAGA : TAS-F+OHB, ADS-F, ADS-G, TAS-I
- 1 Phase B2 SAGA TAS-I (TAS-F, ADS, OHB)
- SES: Eagle 1 démonstrateur QKD ADS-TESAT/ADS-NL

HISPASAT : Garbo/GEOQKD TAS-E

ASI : Sequentia TAS-I

=> Possible intégration dans IRIS² phase 2

France 2030 : PEPR Communication quantiques (académiques)

Pour emporter chez vous

- **Communications quantiques sont deux types de services**
  → Les réseaux QIN qui connecteront les ordinateurs quantiques en utilisant de l'intrication
  → Les moyens d'établissement de clés de chiffrement qui utilisent les propriétés quantiques des photons, mais dont la première génération n'est pas entièrement satisfaisante/
  Les satellites sont nécessaires pour les communications longues distance

- **La stratégie des acteurs français est**
  → de s'appuyer sur l'expérience de 25 ans de nos académiques et de certains industriels
  → de se lancer (depuis 2018) dans les QIN qui sont un objectif massif mais très ambitieux
  → d'apporter des solutions de chiffrement aux clients qui le demandent.

- **Avancement en Europe**
  → Soutien de nos agences CNES surtout, mais aussi AID, UE, ESA, HISPASAT, ASI et de nos actionnaires pour monter des projets qui détourent progressivement les sujets à traiter et les solutions adaptées
  → Nous commençons à maitriser en labo les différents aspects de la mise en œuvre spatiale des QIN
  → Nous visons une démonstration d'un lien sol-sol grace à un satellite en orbite basse cette décénnie, puis plusieurs liens en suivant, pour proposer des services vers 2035 aux futures fermes de calcul quantique.