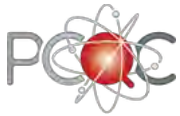
Réseaux de communication quantique

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

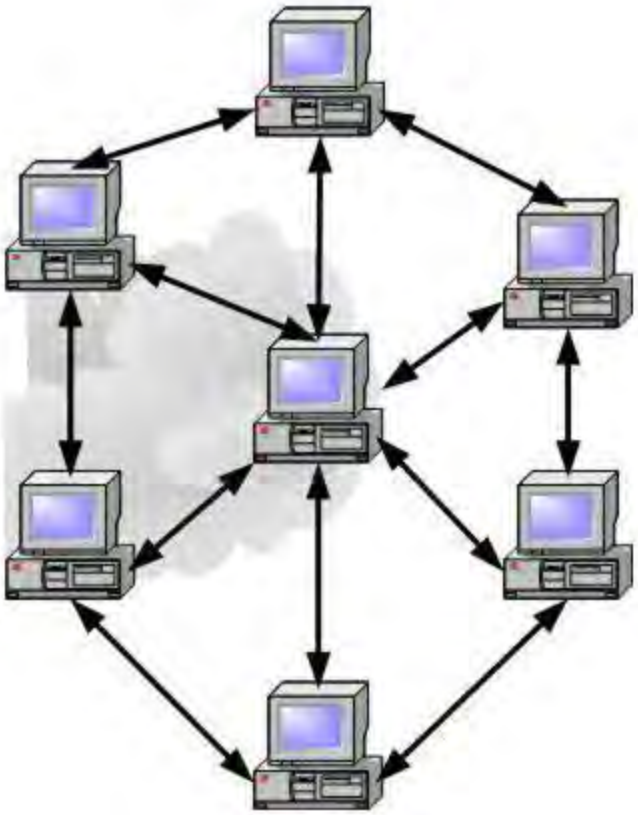
Paris Centre for Quantum Computing



Séminaire, Collège de France, 7 avril 2021

dans le cadre du cours du professeur invité Frédéric Magniez

Réseaux informatiques

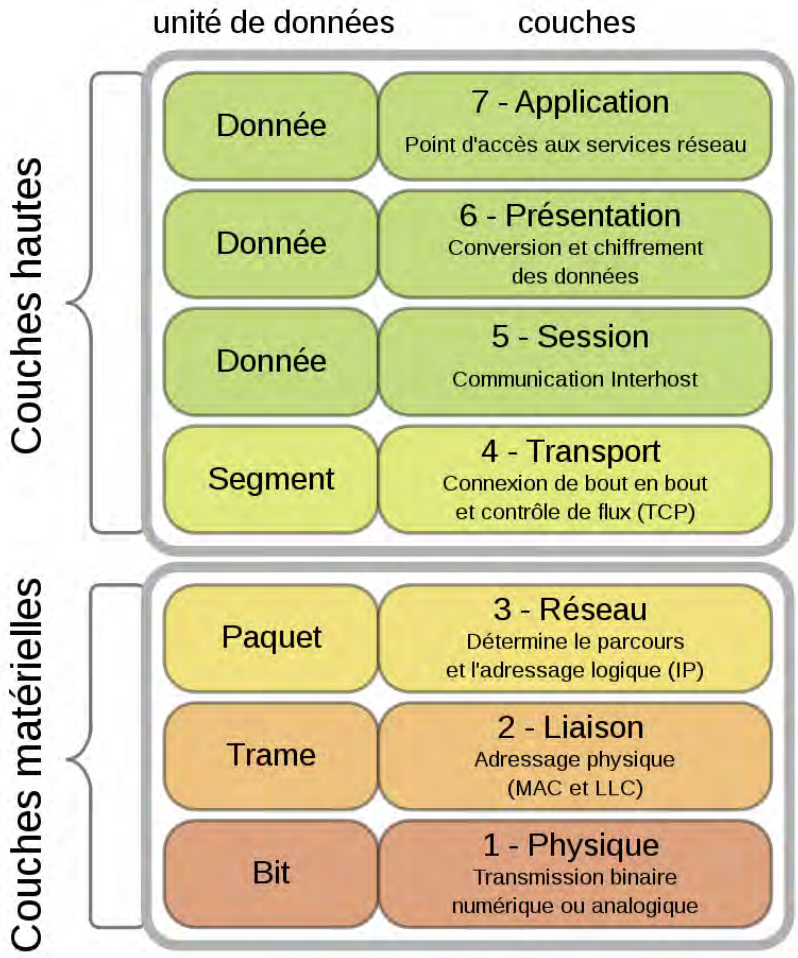


Un **réseau informatique** (en anglais, *data communication network* ou DCN) est un ensemble d'équipements reliés entre eux pour échanger des informations

Une histoire passionnante depuis 1960, entre le réseau Cyclades et ARPANET…

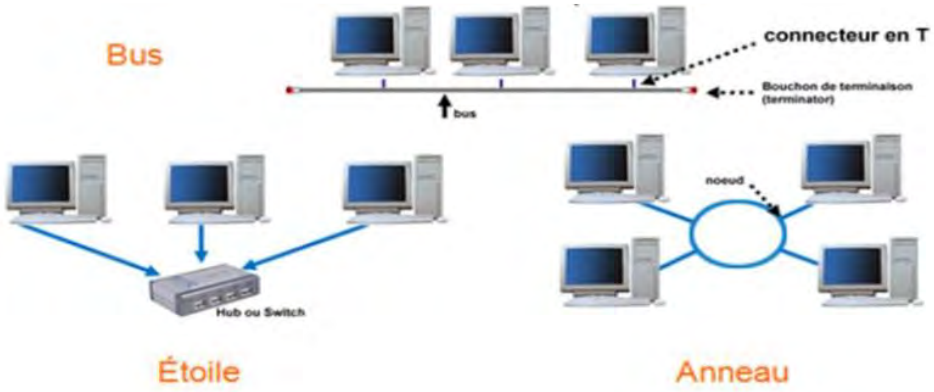
Aujourd'hui, on les utilise pour transférer
des textes (sms),
des données (internet),
des communications vocales (VoIP),
des images (télé),..

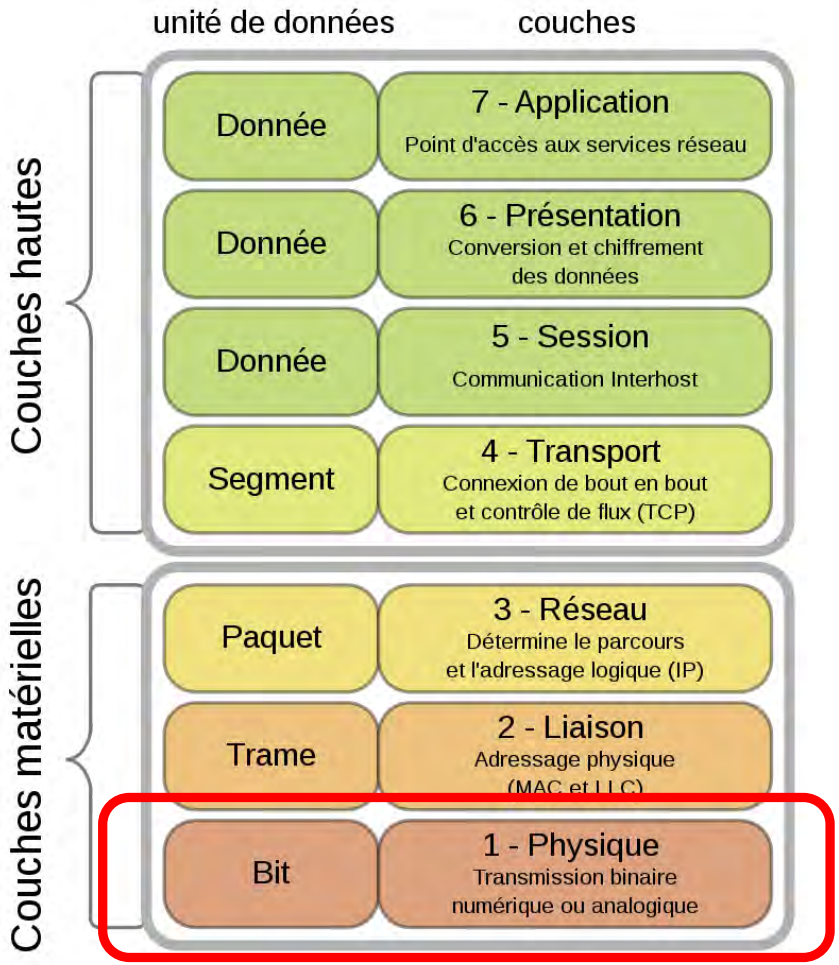
Protocoles et fonctionnalités

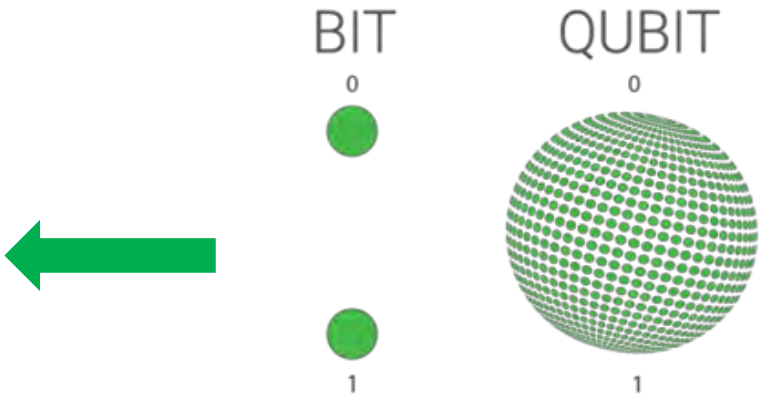


Portée et topologie

Distance entre processeurs	Emplacement des processeurs	Exemple
1 m	Un mètre carré	Réseau personnel
10 m	Une salle	Réseau local
100 m	Un immeuble	
1 km	Un campus	
10 km	Une ville	Réseau métropolitain
100 km	Un pays	Réseau longue distance
1 000 km	Un continent	
10 000 km	Une planète	Internet




unité de données
couches
Couches hautes
Couches matérielles
Donnée
7 - Application
Point d'accès aux services réseau
Donnée
6 - Présentation
Conversion et chiffrement des données
Donnée
5 - Session
Communication Interhost
Segment
4 - Transport
Connexion de bout en bout et contrôle de flux (TCP)
Paquet
3 - Réseau
Détermine le parcours et l'adressage logique (IP)
Trame
2 - Liaison
Adressage physique (MAC et LLC)
Bit
1 - Physique
Transmission binaire numérique ou analogique


BIT
0
1
QUBIT
0
1

Réseaux quantiques

Un **réseau quantique** est un ensemble de **systèmes quantiques** reliés entre eux pour

- échanger des informations
- utiliser les propriétés fondamentales de la mécanique quantique (superposition, intrication, mesure) afin de renforcer des services des réseaux informatiques « classiques » ou d'en créer des nouveaux

Remarques

Les réseaux quantiques n'ont pas vocation à remplacer les réseaux « classiques »

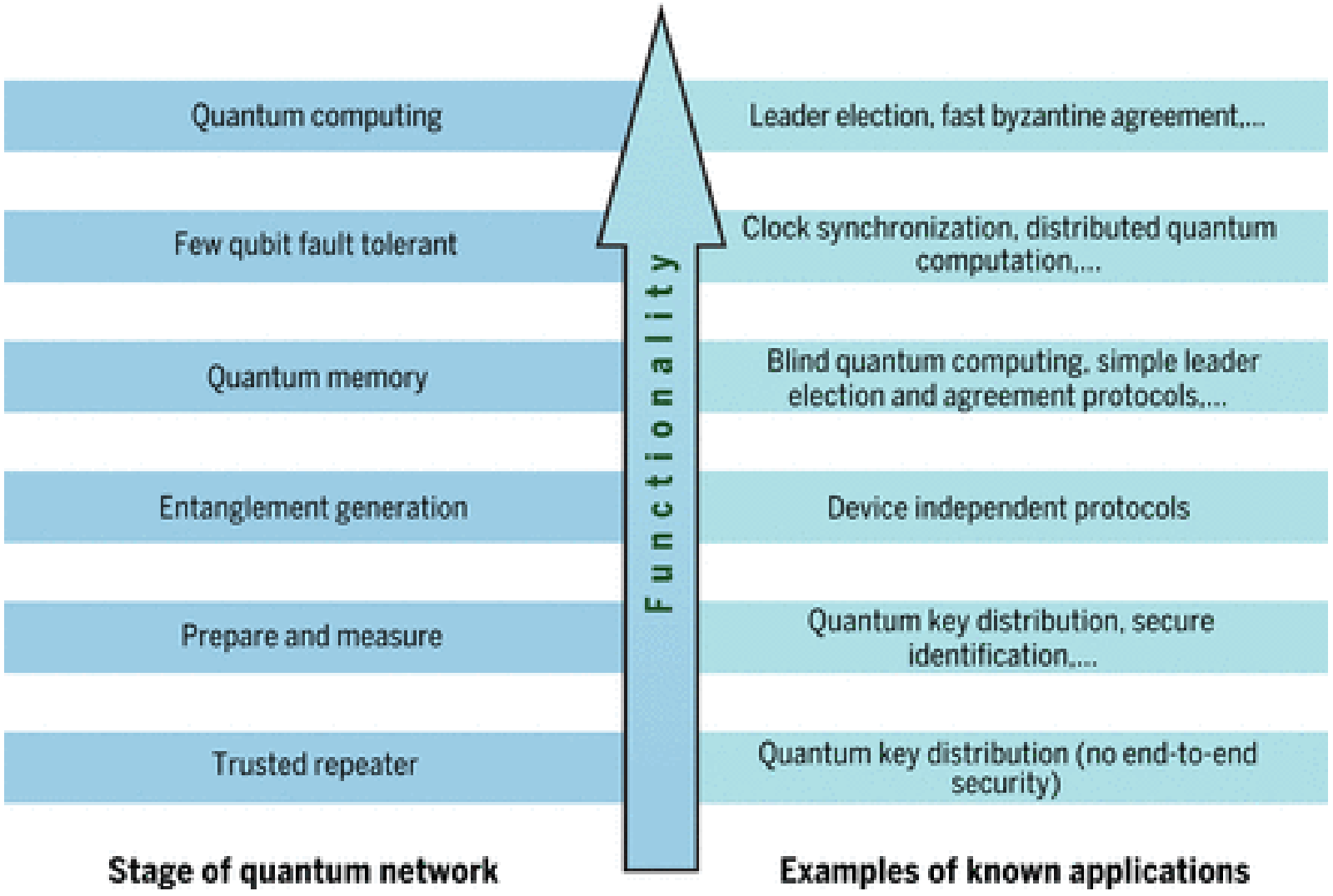
Les systèmes quantiques reliés – les nœuds du réseau – peuvent être des processeurs quantiques, des capteurs quantiques, des mémoires quantiques, ou des « simples » dispositifs de génération ou de mesure d'états quantiques

Les photons – les particules élémentaires qui incarnent l'aspect corpusculaire de la lumière – sont les porteurs idéaux de l'information quantique dans des réseaux de communication quantique

Les canaux de transmission quantique sont la fibre optique ou l'espace libre

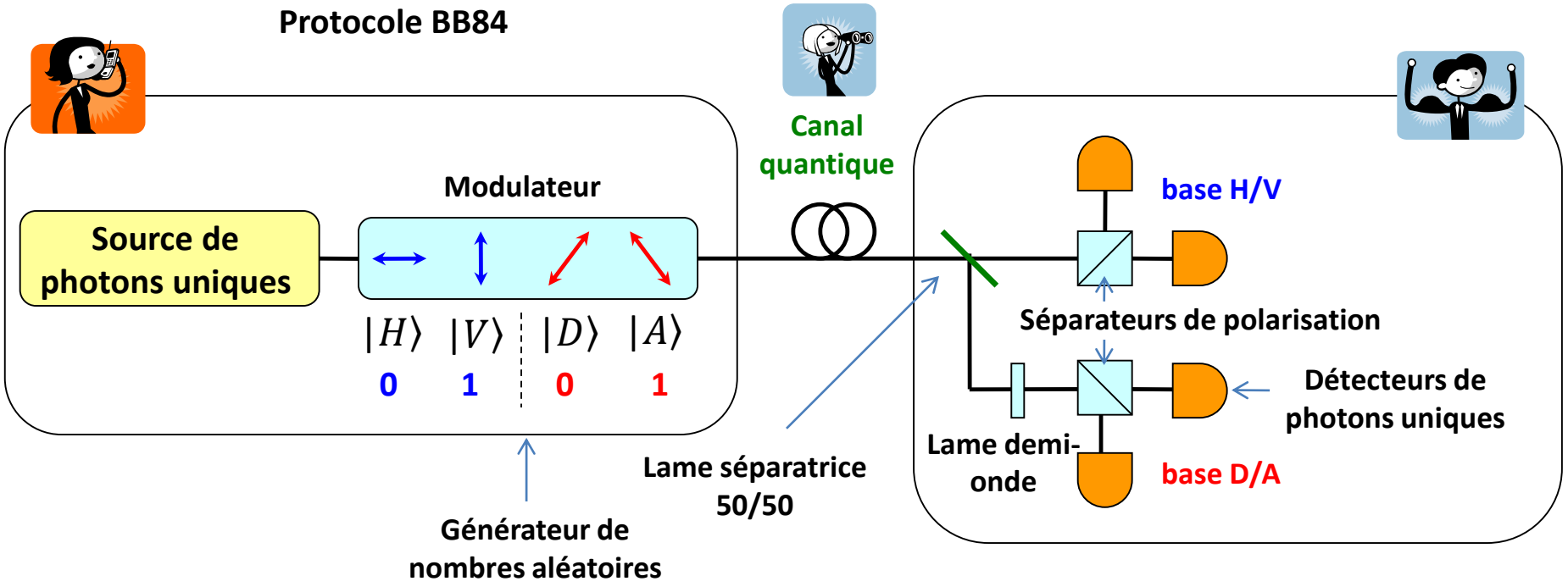
Les applications possibles dépendent de l'étape de développement du réseau quantique

Etapes de développement des réseaux quantiques



S. Wehner *et al.*, Science 2018

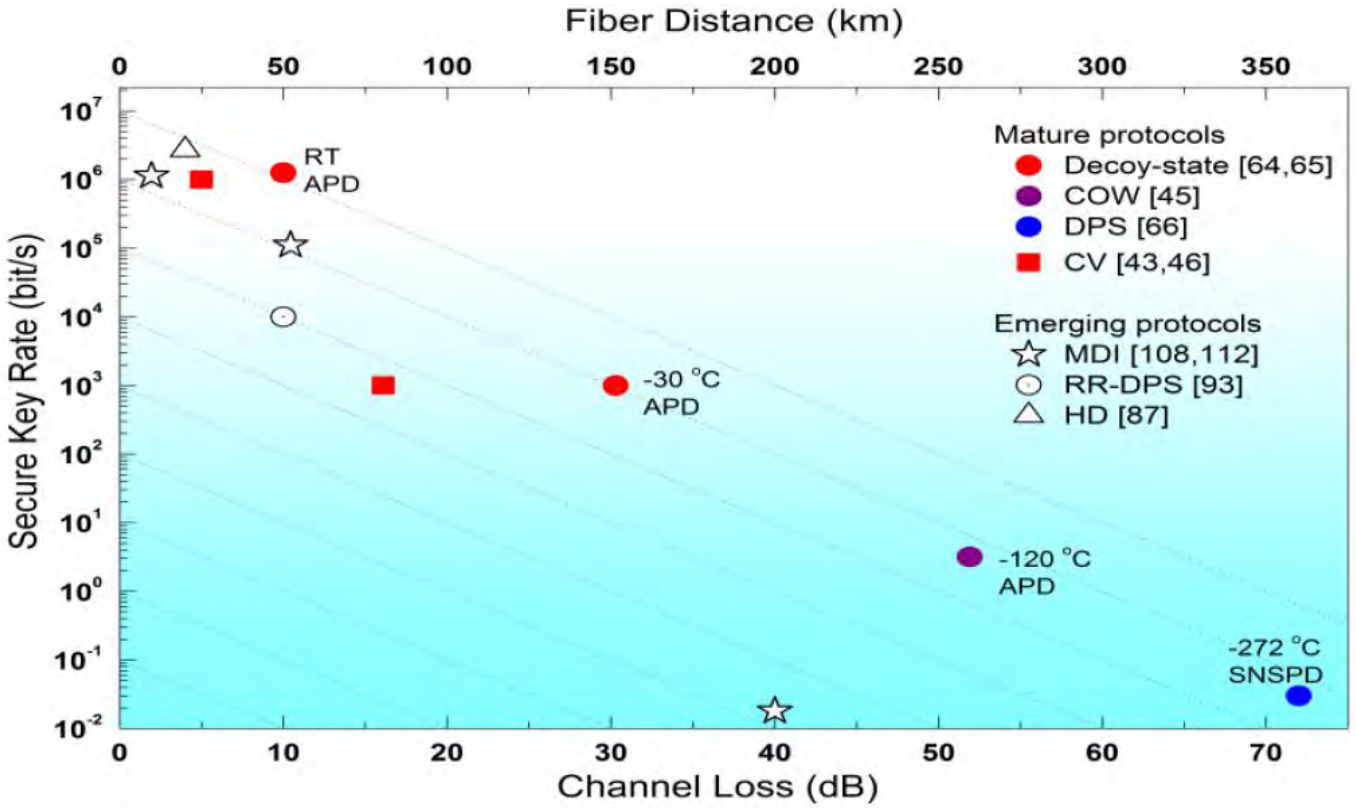
Distribution quantique de clés



Théorème du non clonage: Eve ne peut pas copier les états envoyés par Alice
Principe d'incertitude de Heisenberg: Eve ne peut pas mesurer sur les deux bases

En combinaison avec des protocoles d'authentification et de chiffrement, la distribution quantique de clé (en anglais, *quantum key distribution* ou QKD) permet l'échange des messages secrets avec une sécurité renforcée

Performances pratiques



Performances des systèmes QKD sur des liaisons fibrées point à point

ED, H.-K. Lo, B. Qi, Z. Yuan, npj Quantum Info. 2016

Plusieurs protocoles pour la même fonctionnalité → en réponse à des imperfections

Sécurité: $\frac{1}{2}\left\|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\right\|_1 \leq \varepsilon$ for any $\rho_{A^n B^n E}$

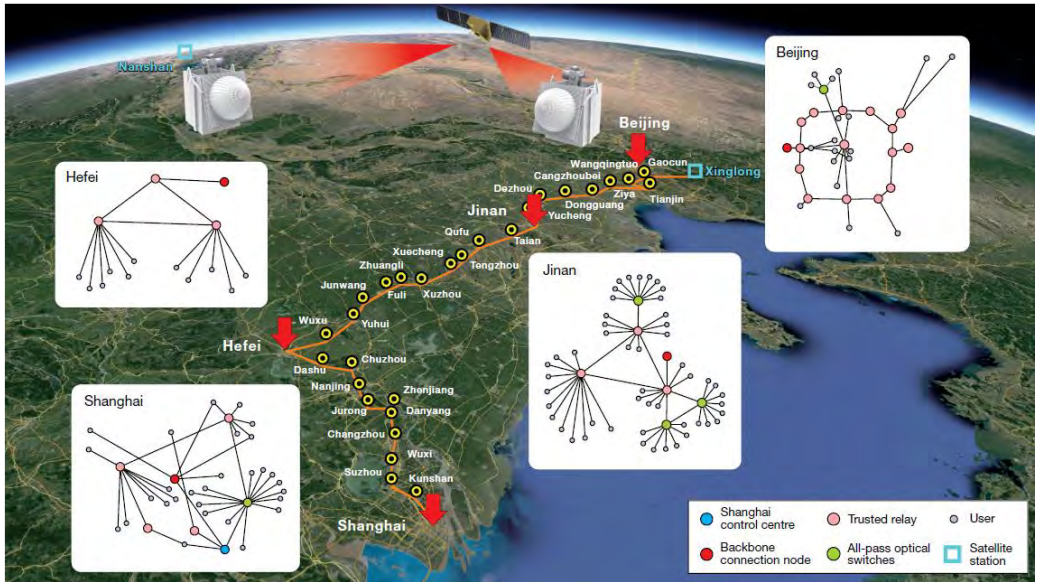
composabilité, effets de taille finie, attaques générales

Limites fondamentales du taux et de la portée

Réseaux avec des répéteurs fiables

Si la distance entre Alice et Bob dépasse la portée maximale du système:

Alice-R: key1, R-Bob: key2, R: key1⊕key2 → Bob: key2⊕(key1⊕key2) = key1



Y.-A. Chen *et al.*, Nature 2021

OPEN QKD

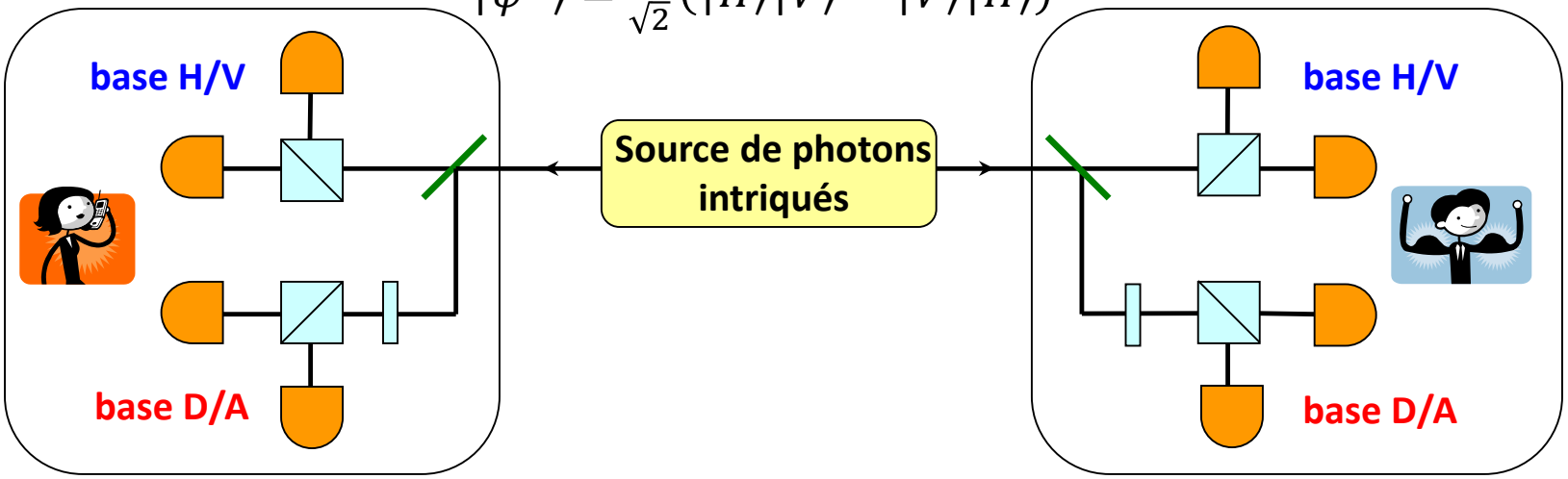
Data centres, réseaux électriques, infrastructures critiques, communications gouvernementales, partage de dossiers médicaux…

S'affranchir des hypothèses

Mot clé: intrication

Protocoles Ekert91, BBM92

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)$$



De tels états donnent lieu à des corrélations non-locales et peuvent violer des inégalités de Bell

Propriété de monogamie:
Si les qubits de Alice et de Bob sont parfaitement corrélés entre eux, ils ne peuvent pas être corrélés avec un troisième qubit

Comment faire propager les états intriqués ?

Les canaux quantiques ont des pertes et sont bruités
- pour transmettre un photon sans absorption, le nombre de répétitions augmente exponentiellement avec la distance
- même quand le photon arrive, la fidélité de l'état transmis décroit exponentiellement avec la distance

$$F = |\langle \varphi_1 | \varphi_2 \rangle|^2$$

Pourquoi on ne peut pas utiliser des amplificateurs comme pour les réseaux de communication classique ?

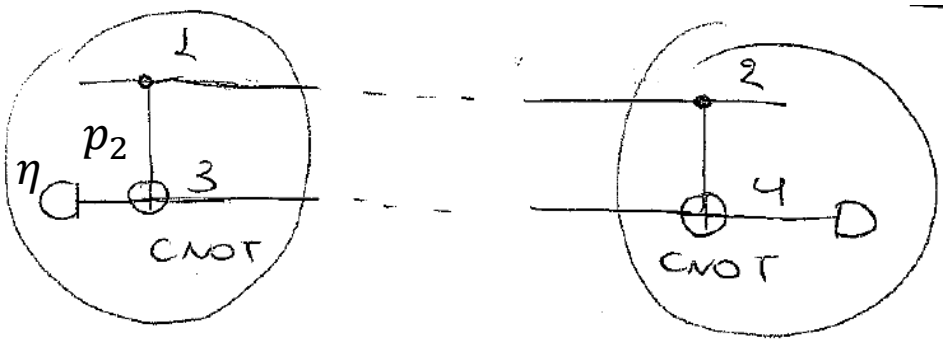
L'amplification introduit du bruit → perte des corrélations

Un répéteur quantique doit
- garantir une bonne fidélité
- utiliser peu de ressources
- tolérer des erreurs d'opération et de mesure réalistes

→ purification d'intrication + échange d'intrication

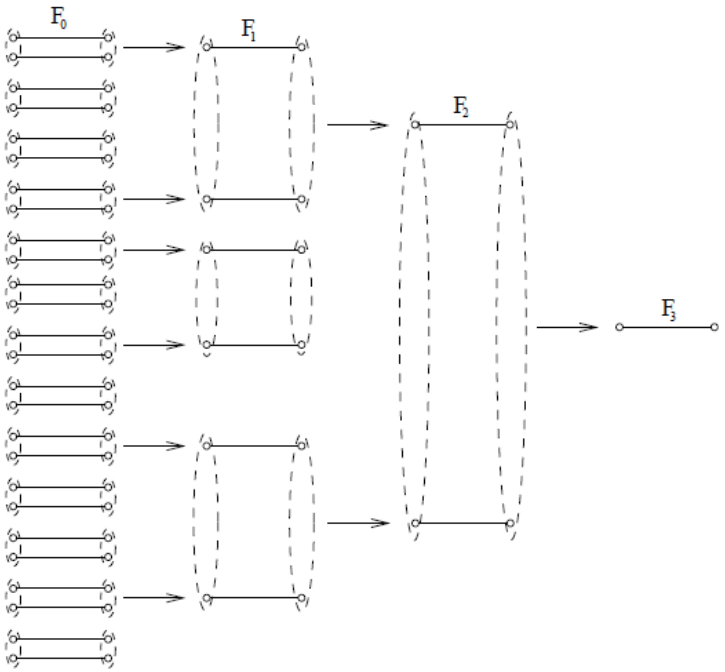
Purification d'intrication

Distillation de paires de meilleure fidélité à partir d'un plus grand nombre de paires imparfaites



$$F' = f(F, p_2, \eta)$$

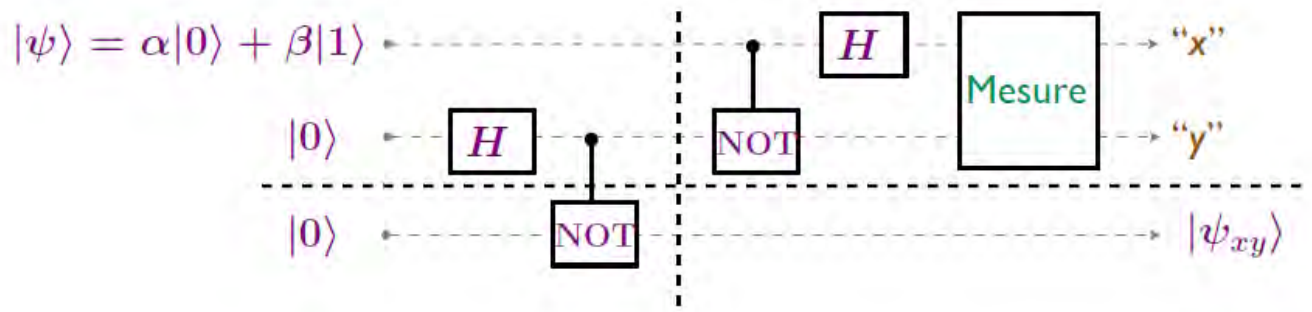
Si $F \in (F_{\min}, F_{\max})$, alors $F' > \mathrm{F}$

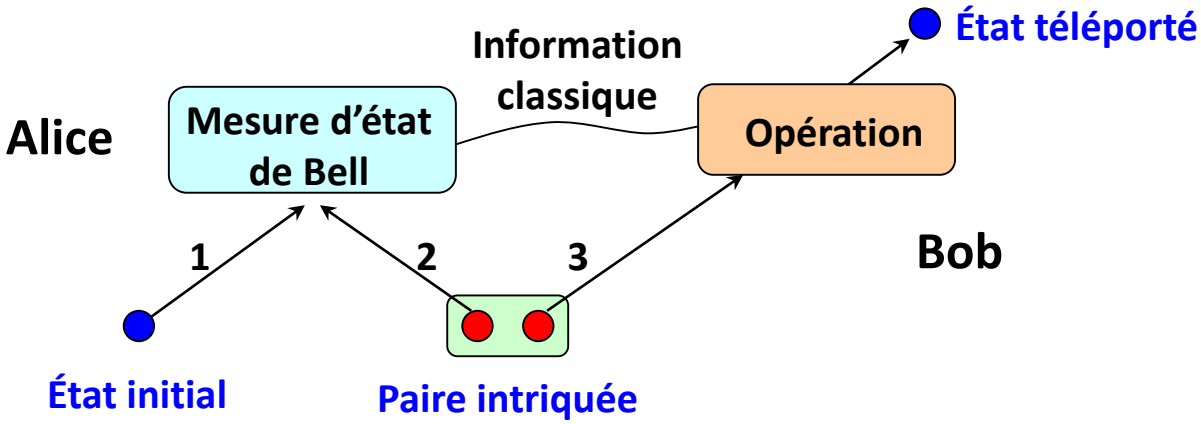


W. Dür *et al.*, Phys. Rev. A 1999

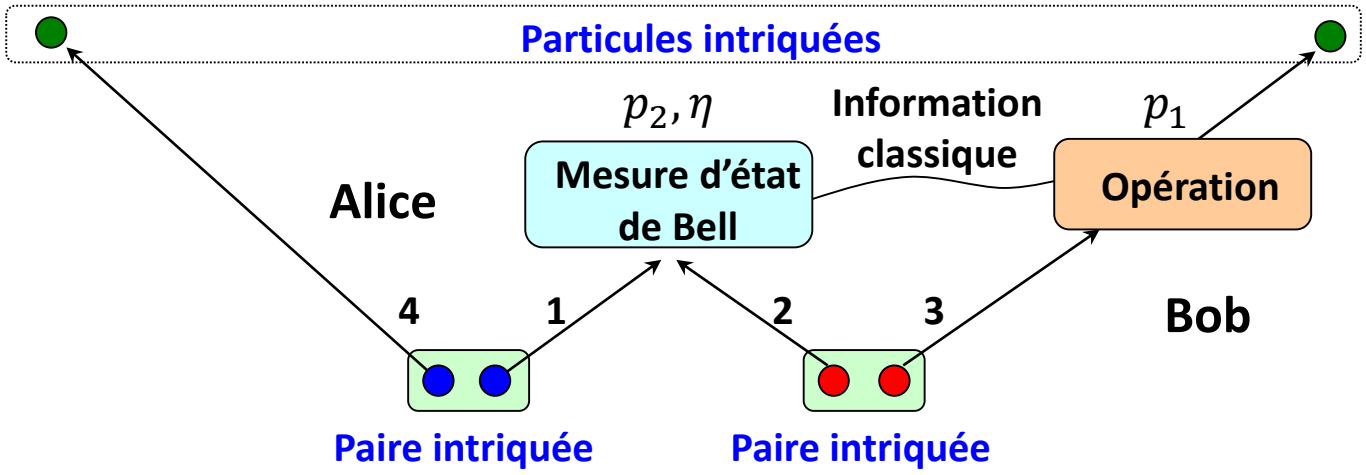
Echange d'intrication

Généralisation de la téléportation quantique permettant d'intriquer des qubits distants

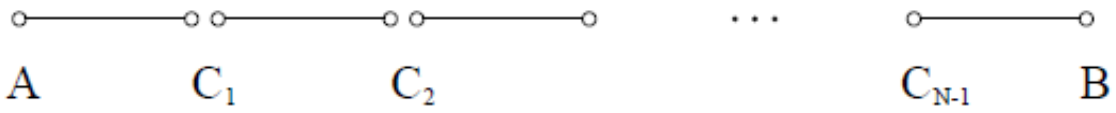




Echange d'intrication



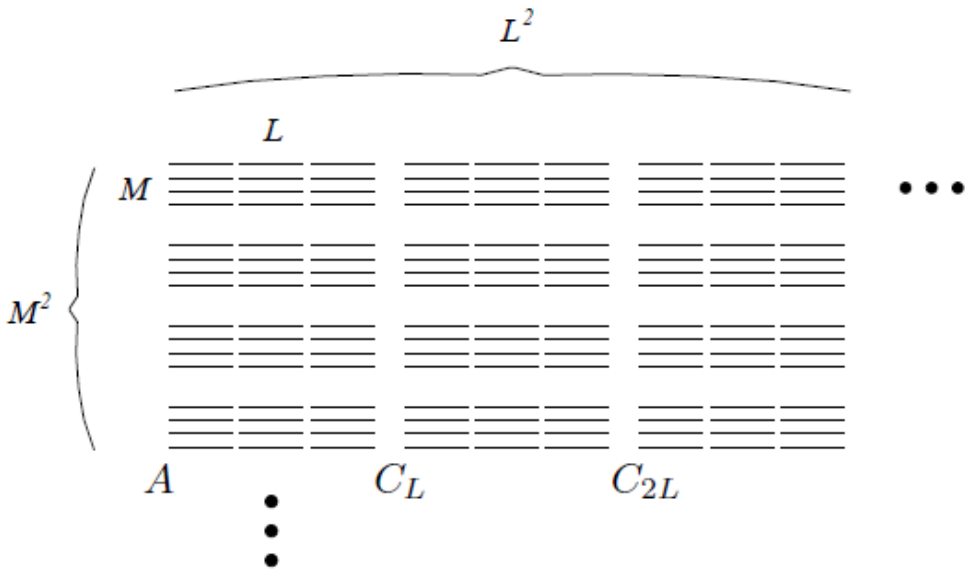
$$F' = f(F, p_1, p_2, \eta) < F$$



$\log_2 N$ connections

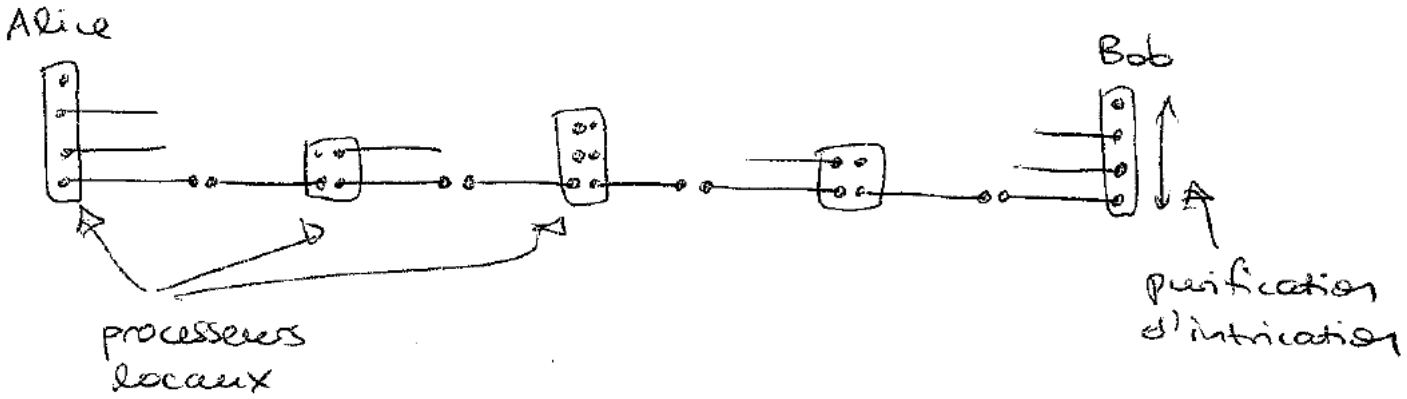
Répéteur quantique

Diviser le canal; connecter, purifier, itérer en respectant les seuils de fidélité



$N^{\log_L M+1}$

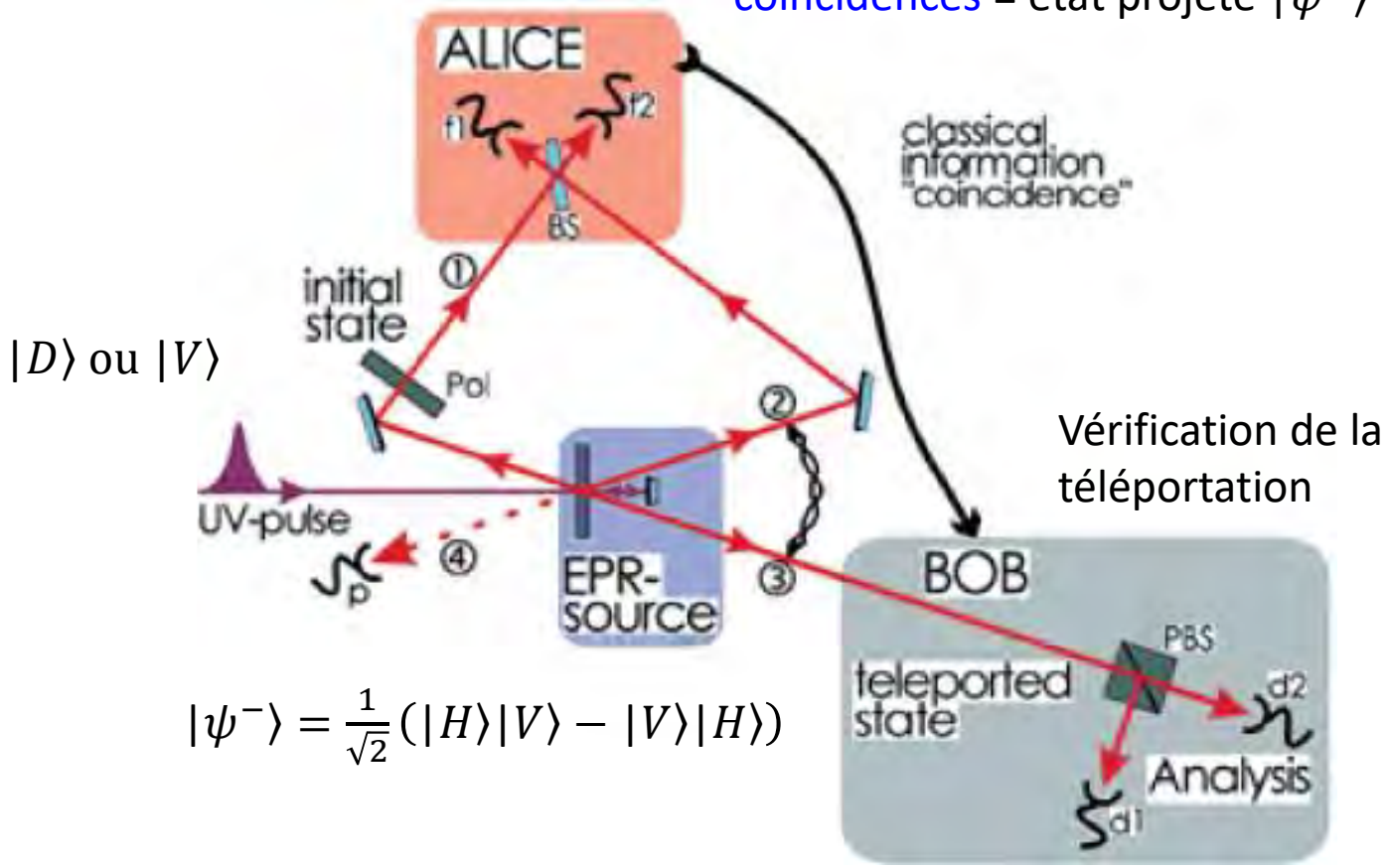
nombre de paires élémentaires



Téléportation quantique en pratique

Première expérience de téléportation quantique
Université de Vienne, 1997

Mesure d'état de Bell *partielle*:
coïncidences = état projeté $|\psi^-\rangle$

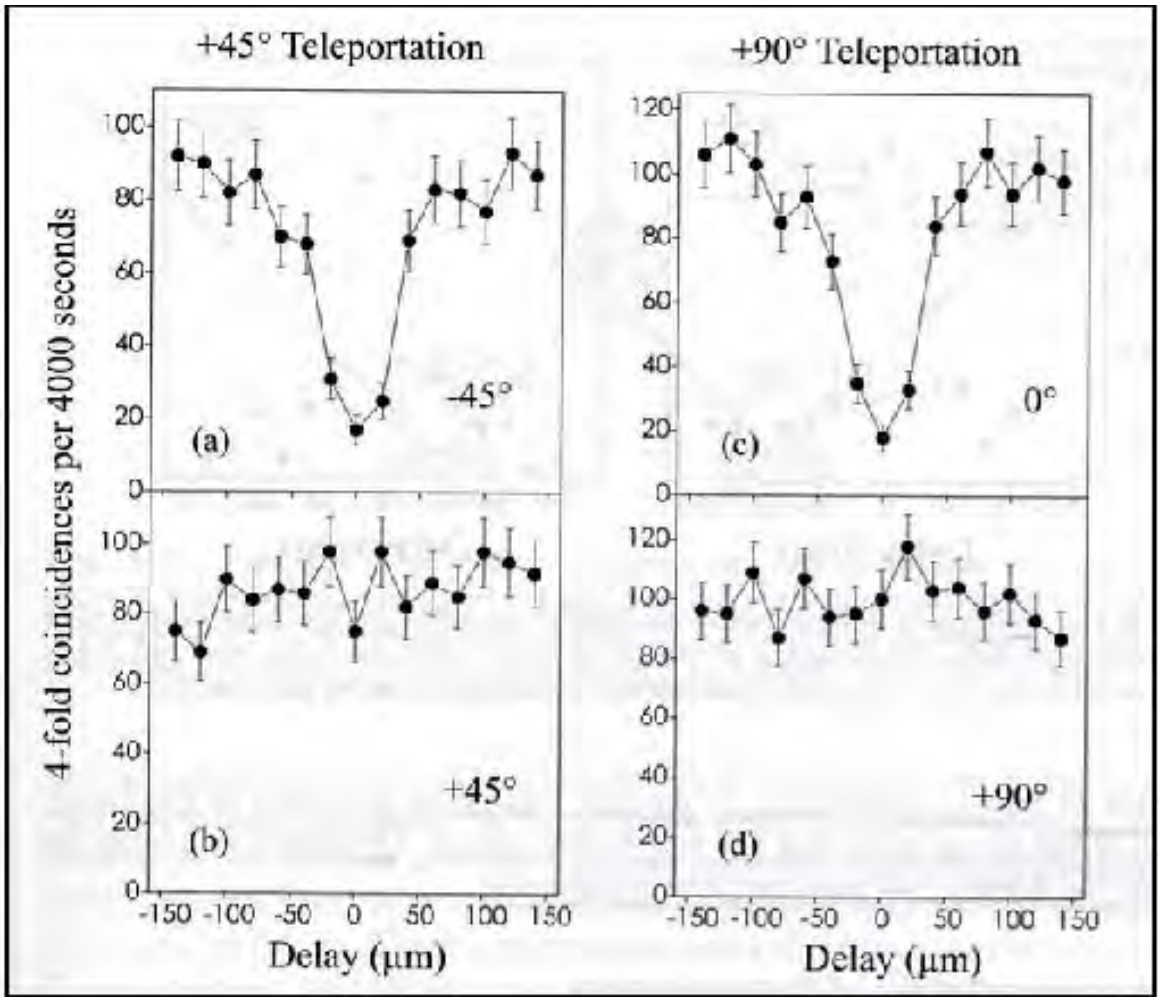


$|D\rangle$ ou $|V\rangle$

Vérification de la téléportation

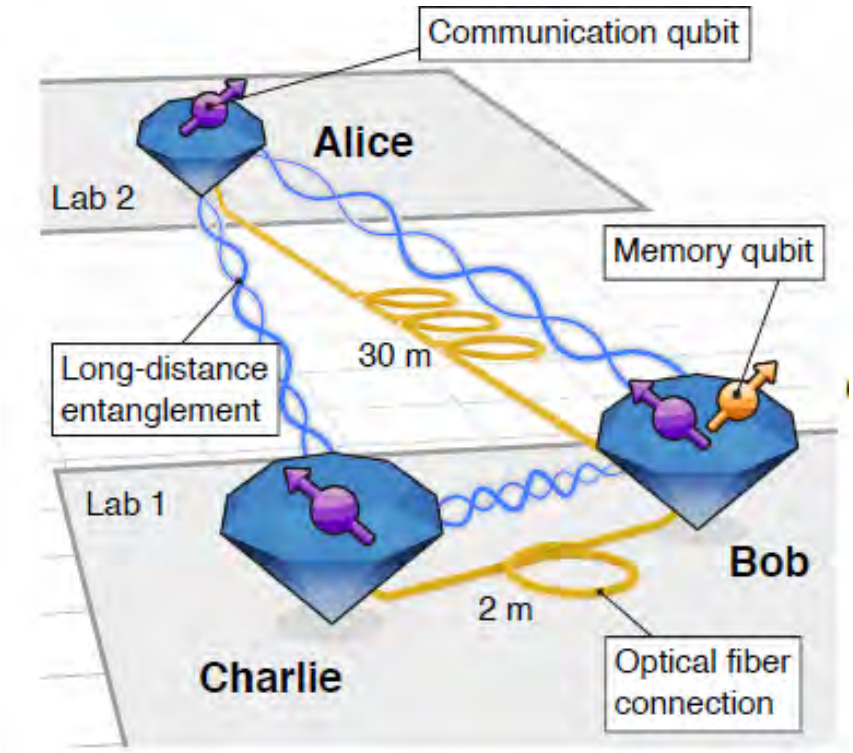
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)$$

Vérification expérimentale



Maintenant protocole complet, Alice et Bob séparé de dizaines ou centaines de kilomètres!

Vers un répéteur quantique



TU Delft, M. Pompili *et al.*, 2021

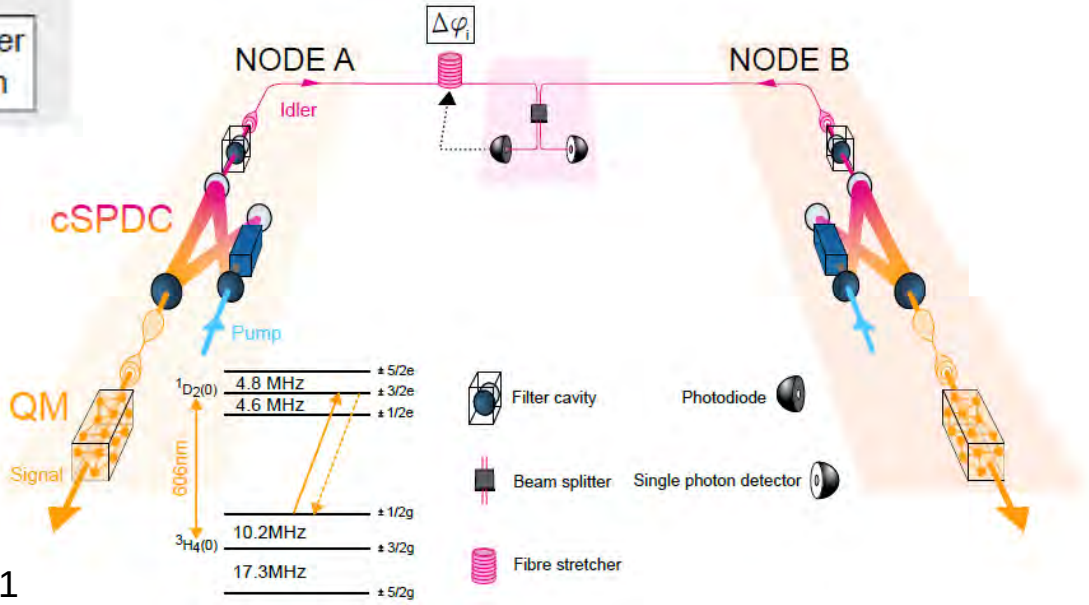
Défis

Durée et efficacité de stockage (record à Paris!), multiplexage

Taux d'intrication

Portée au niveau de réseaux locaux

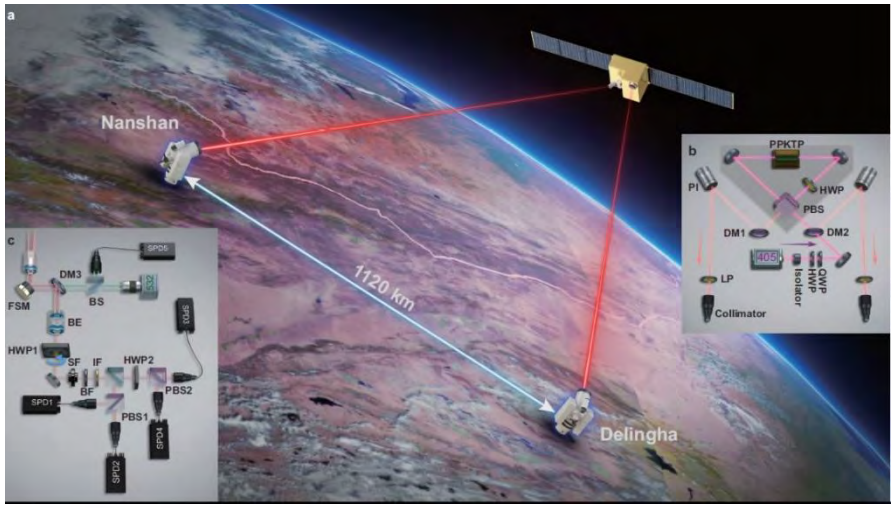
Pile réseau (transport, routage,…) et applications



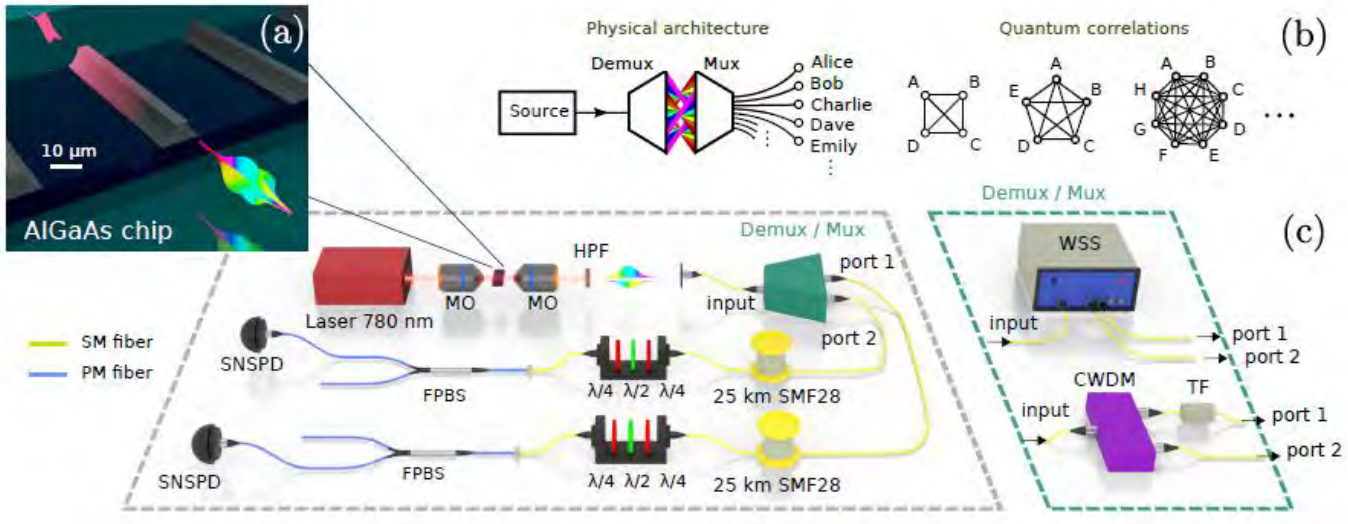
ICFO, D. Lago-Rivera *et al.*, 2021

Applications à échelle intermédiaire

QKD, tirage à pile ou face, monnaie quantique, transmission anonyme,
« communication complexity »,…
Portée au niveau de réseaux métropolitains et longue distance
Démonstration d'un avantage quantique

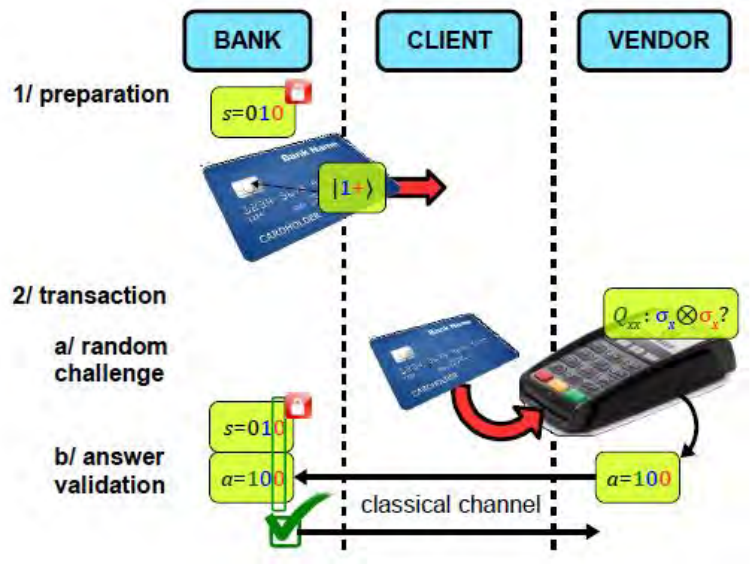


J. Yin *et al.*, Nature 2020



F. Appas *et al.*, 2021

Applications à échelle intermédiaire



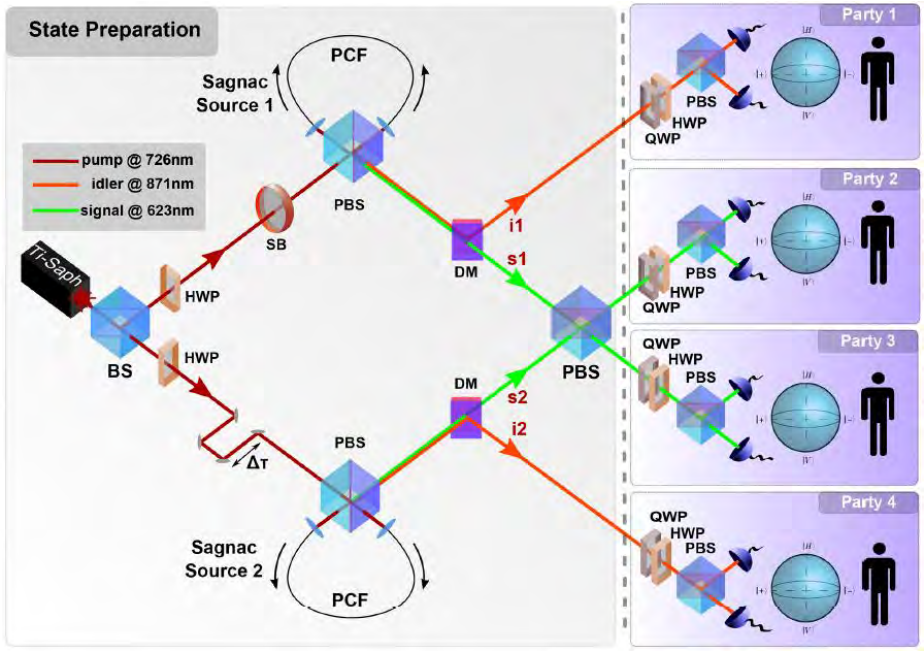
M. Bozzio *et al.*, npj Quant. Inf. 2018

Vérification d'intrication multipartite en présence d'adversaires

Application à la transmission anonyme

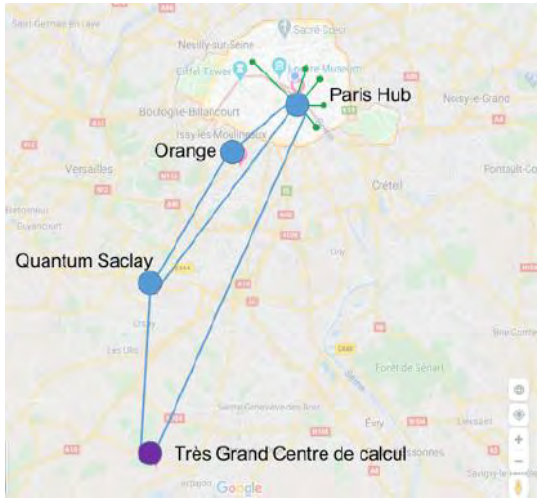
La phase de vérification garantit l'anonymité

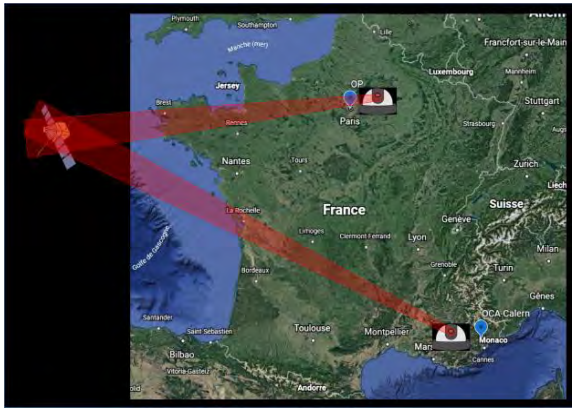
$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$$



W. McCutcheon *et al.*, Nature Commun. 2016

A. Unnikrishnan *et al.*, Phys. Rev. Lett. 2019





Merci!

eleni.diamanti@lip6.fr