Introduction aux communications quantiques

Nicolas Fabre, Maitre de conférences Telecom Paris.

Telecom Paris, nicolas.fabre@telecom-paris.fr

06/12/2024

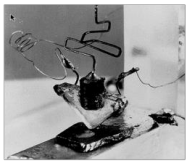
Ce que nous verrons

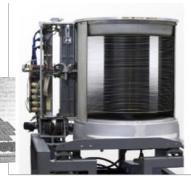
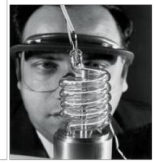
- Introductions aux technologies quantiques.
- Pourquoi utiliser des ressources quantiques dans des protocoles de communication ?
- Distribution de clés quantiques avec des photons uniques polarisés (également appelée DV-QKD). Protocoles BB84, BBM92.
- Post-traitement classique (correction d'erreur, amplification de la confidentialité)

Première révolution quantique

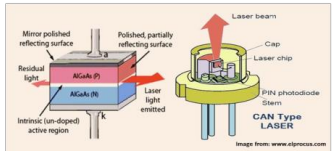
Première révolution quantique

Première révolution quantique: compréhension de la nature à l'échelle microscopique: atomes, molécules, et de l'interaction lumière-matière



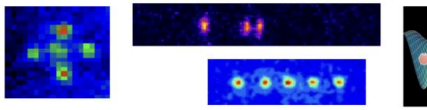



1905-1927 Quantum Physics development	1947 Transistor	1954 Panneau solaire	1956 Hard Disk Drive	1960 Laser	2004 Nanotechnologies	2008+ Smartphone

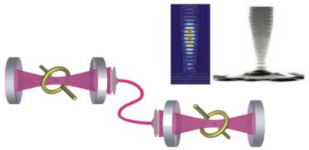


Qu'est ce qu'un système quantique?

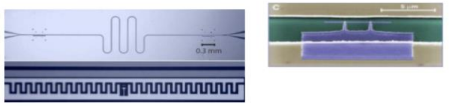
En 1952, Erwin Schrödinger écrit : « *nous ne faisons jamais d'expériences avec un seul électron ou un seul atome... cela entrainerait inévitablement des conséquences ridicules* ».



Manipulation de molécules ou atomes individuels



Production et contrôle de photons uniques

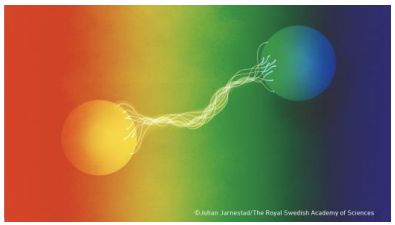


« Boîtes à paires de Cooper »

Chaque photon (ou atome, ou électron...) peut porter un « bit quantique » ou « qubit »

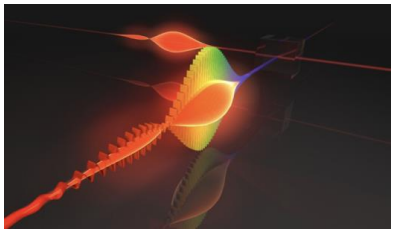
Seconde révolution quantique

Seconde révolution quantique: Exploiter le phénomène de superposition, d'intrication quantique et de la mesure de systèmes quantiques à des fins technologiques (qui n'était pas exploité avant « dans la première révolution quantique)



Intrication quantique:

Corrélation sur les propriétés physiques de deux systèmes quantiques



Superposition quantique

Le photon est à la fois bleu, et rouge et vert...

Seconde révolution quantique

1980's

Scientific Pioneers


R. Feynman


D. Deutsch

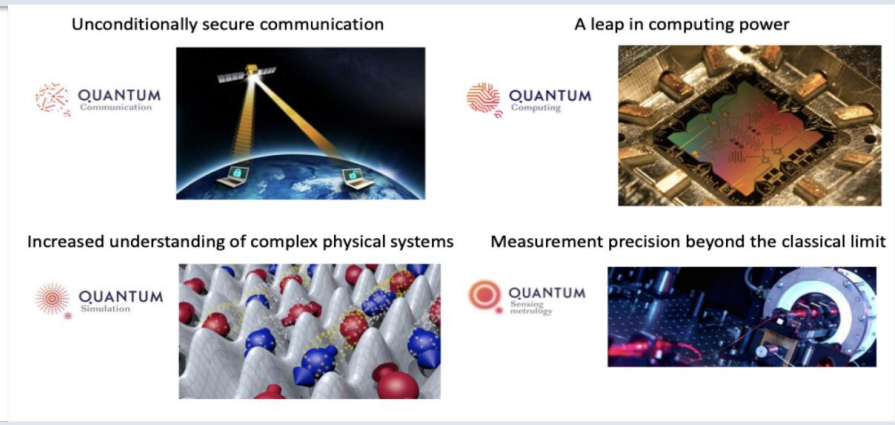

P. Shor


L. Grover


G. Brassard


C. Bennett

Quantum Technologies to **transmit / protect / detect / process** classical or quantum **Information**

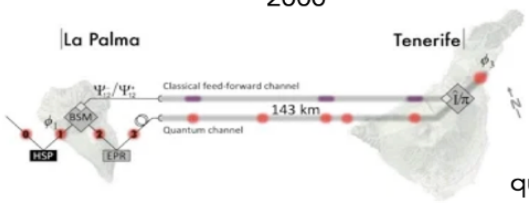


Exploiter le phénomène de superposition, d'intrication quantique et de la mesure de systèmes quantiques à des fins technologiques.

Seconde révolution quantique: n'est pas nouvelle

Premières expériences en communication quantiques

2000

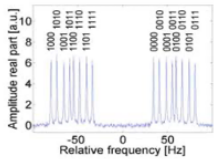


(Également en Suisse en 2001)

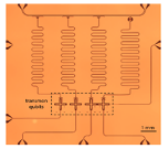
2000

IDQ

Première start-up quantique (quantum random number generator)



Shor Factoring Algo with NMR (2001)

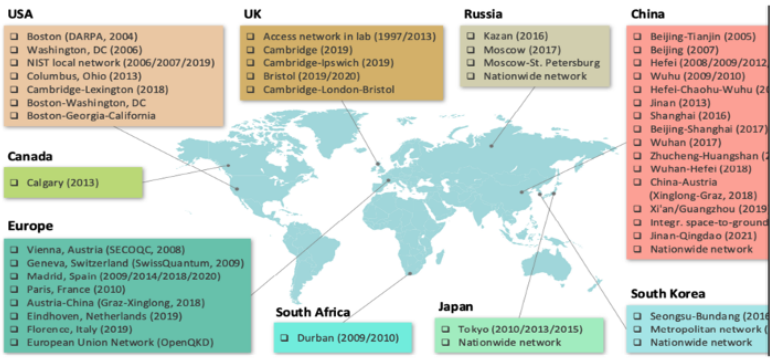


Transmon Qubit (2007)

2008, Quantum network, Vienne

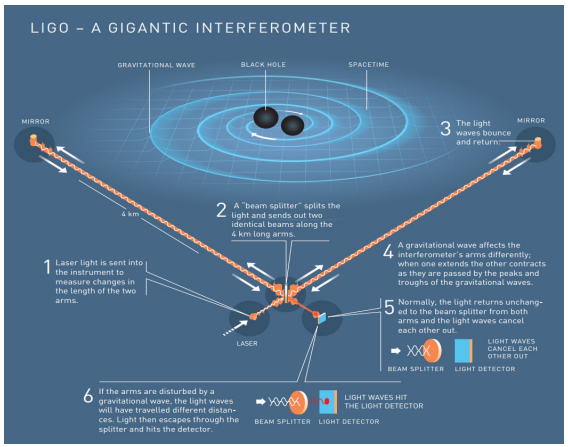
The SECOQC quantum key distribution network in Vienna

M Peev[1,20], C Pacher[1], R Alléaume[2], C Barreiro[3], J Bouda[4], W Boxleitner[1], T Debuisschert[5], E Diamanti[2,6], M Dianati[7], J F Dynes[8], S Fasel[3], S Fossier[2,6], M Fürst[1], J-D Gautier[3], O Gay[10], N Gisin[3], P Grangier[2], A Happe[1], Y Hasani[1], M Hentschel[11], H Hübel[12], G Humer[1], T Länger[1], M Legré[10], R Lieger[1], J Lodewyck[5,6,13], T Lorünser[1], N Lütkenhaus[14,15], A Marhold[10], T Matyus[1], O Maurhart[1], L Monat[10], S Nauerth[3], J-B Page[10], A Poppe[1], E Querasser[1], G Ribordy[16], S Robyr[10], L Salvail[17], A W Sharpe[8], A J Shields[8], D Stucki[1], M Suda[1], C Tamas[1], T Themel[1], R T Thew[3], Y Thoma[3], A Treiber[12], P Trinkler[10], R Tualle-Brouri[2], F Vannel[3], N Walenta[3], H Weier[1], H Weinfurter[18,19], I Wimberger[10], Z L Yuan[8], H Zbinden[3] and A Zeilinger[1,13]

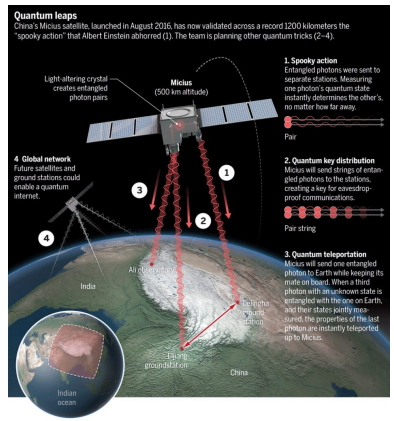


Réalisation majeures des technologies quantiques

What are the most spectacular experiments?



Quantum metrology:
use of squeezed state
in gravitational wave detector



Quantum communications:
Quantum key distribution experiment

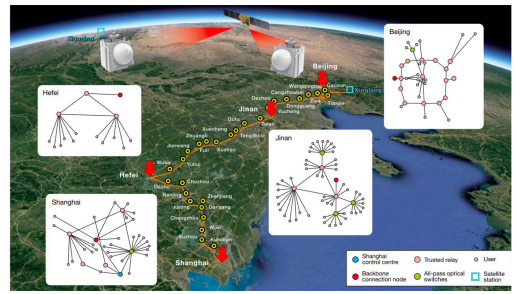
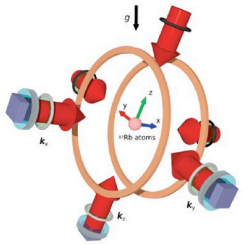


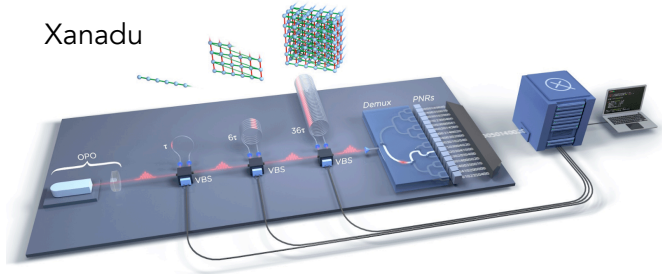
Figure 1. The network consists of four quantum metropolitan-area networks (QMANs) in Beijing, Jinan, Shanghai and Heifei, a backbone fibre link over 2,000 km (orange line) and two ground–satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. The backbone is connected by trusted relays. A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre [3].

Quantum communications:
Quantum network



Quantum metrology: Inertial sensors

Xanadu

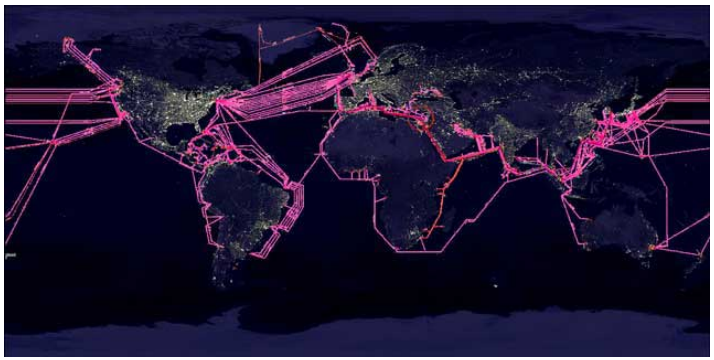


Quantum computing: Sampling experiment
Boson sampling, Gaussian boson sampling

Quantum Computing

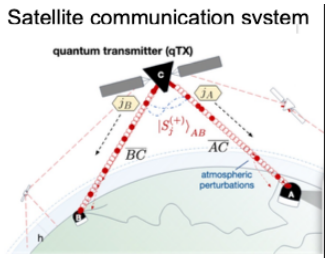
Sommaire

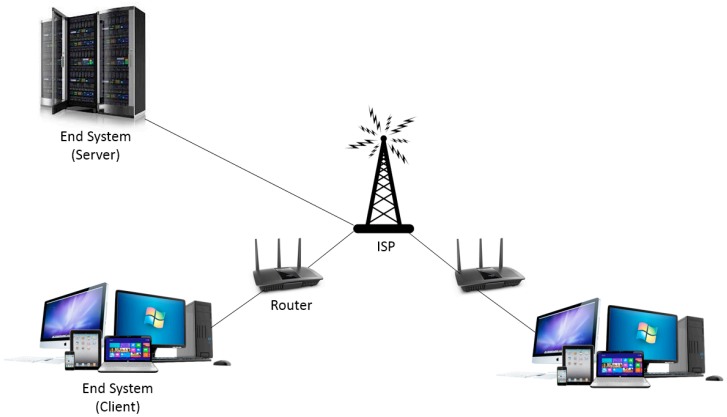
Réseaux classiques

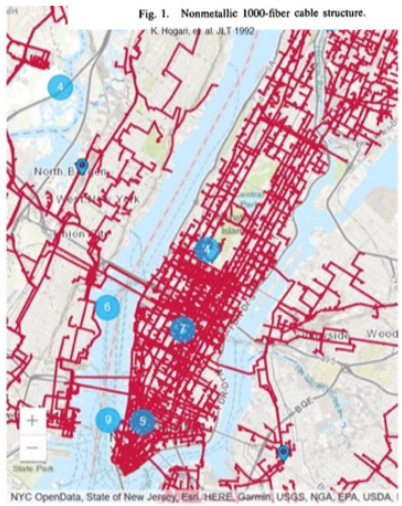


Submarine Fiber Cable Ship

Satellite communication system





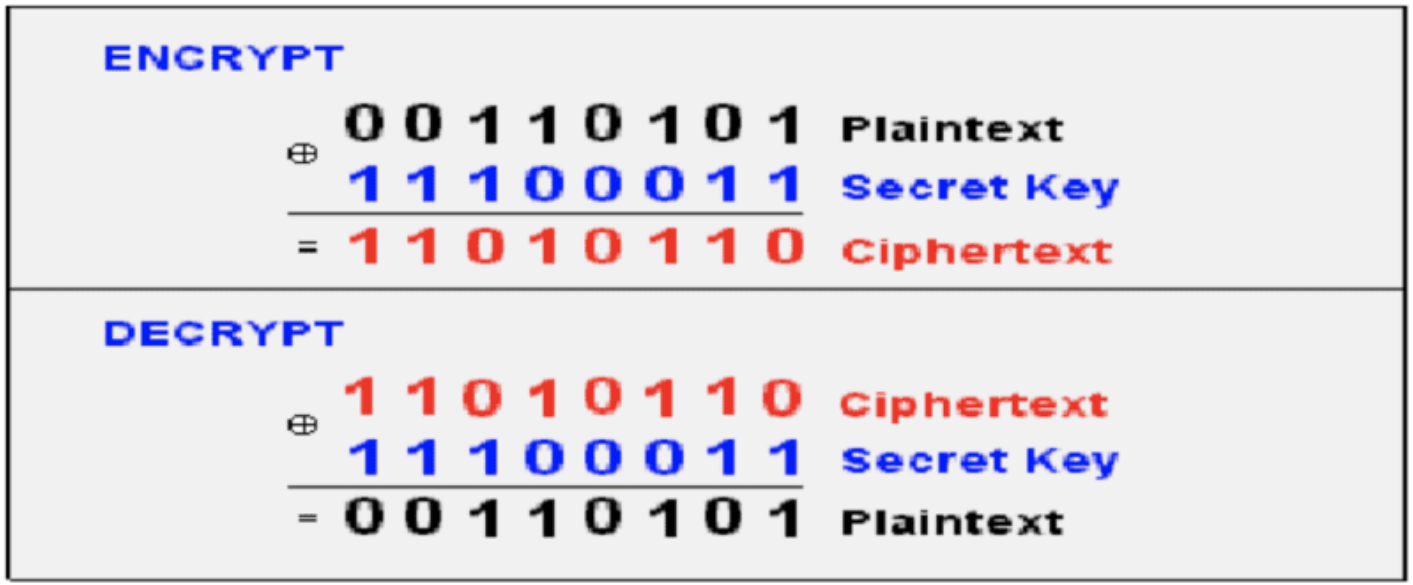


Some pictures from Winter School on Quantum Networks of the Center for Quantum Networks (CQN) and Internet

Definition

Que veut on transmettre à travers un réseau ?

- Image, vidéo, texte...
- Signature digitale, clés de cryptage.



From keyfactor

Expression du problème

Sécurité computationnelle : la sécurité repose sur la difficulté de résoudre un problème computationnellement complexe.

- La sécurité sous-jacente de l'Internet "classique" repose sur des conjectures computationnelles : elle est vulnérable aux piratages et aux écoutes indiscrètes.
- Un ordinateur quantique peut compromettre RSA (factorisation de nombre premier), Diffie-Hellman (discrete logarithm).
- **"Harvest now, decrypt later"** :

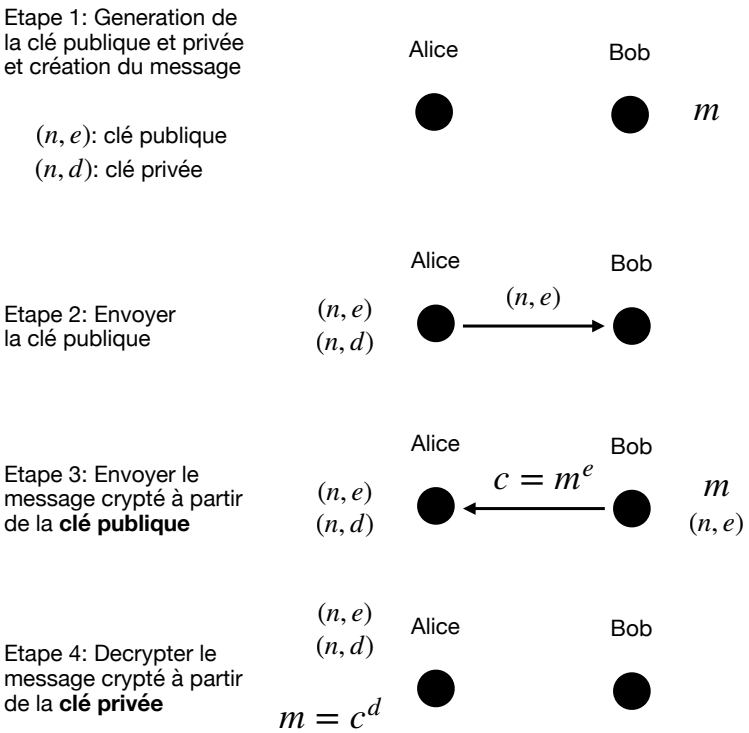
RSA 2048 : quelques mots

(1) Choix de deux nombres premiers distincts, p, q, puis calculer le produit : $n = pq$.
(2) Calcul de la fonciton indicatrice de Euler à partir de deux nombres premiers $\phi(n) = (p-1)(q-1)$
(3) Choisir un entier naturel e premier avec $\phi(n)$ et strictement inférieur à $\phi(n)$.
(4) Calcul de l'inverse de e : $ed = 1 \pmod{(p-1)(q-1)}$.
(5) Génération de la clé publique (n, e) et privée (n, d).

RSA

L'algorithme RSA repose sur le fait qu'il est relativement facile de multiplier deux grands nombres premiers ensemble, mais déterminer les nombres premiers d'origine à partir du résultat (le produit) est computationnellement irréalisable pour des nombres premiers suffisamment grands.

RSA 2048 : quelques mots



Bien noter émetteur, récepteur, clé privée et publique... à chaque schéma de communication, cela peut changer (bien voir la différence avec le one-time pad qui sera utilisé en QKD ensuite).

Expression du problème

RSA

Clé publique : Cette clé est utilisée pour le chiffrement et peut être librement distribuée. La clé publique est dérivée de la clé privée mais il est computationnellement difficile de la retrouver. Clé privée : Cette clé est gardée secrète et est utilisée pour le déchiffrement. Seul le propriétaire de la clé privée devrait y avoir accès. La clé privée est utilisée pour déchiffrer les messages qui ont été chiffrés avec la clé publique correspondante.

Il est important de noter qu'à mesure que les ordinateurs deviennent plus puissants, des longueurs de clé plus importantes sont nécessaires pour maintenir le même niveau de sécurité.

Comment pallier ce problème de sécurité ?

Deux approches : communications quantiques et post-quantum.

• Communication quantique : sécurité basée sur la physique plutôt que sur les mathématiques : sécurité inconditionnelle (en l'absence d'imperfection).

• Cryptographie post-quantique : utilisation d'algorithmes classiques résiliants contre les attaques quantiques et classiques (lattice-based), mais toujours basée sur des "conjectures" pour être sécurisée contre des attaques.

Post-quantum

- Peut être effectué sur les ordinateurs actuels, mais...
- La sécurité n'est pas prouvée.
- Mauvaise mise à l'échelle, et demande un pouvoir computationel considérable.
- Trois candidats post-quantiques ont échoué (compétition du NIST) : en raison de la "conjecture de robustesse" jusqu'à ce qu'une attaque soit conçue. Nouveau standard de août 2024 (trouver le plus petit multiplicateur commun entre différente séquence : on ne sait pas désigner un algorithme classique ou quantique efficace pour cette tache).

Sécurité inconditionnelle

En cryptographie classique, la sécurité repose généralement sur l'hypothèse que certains problèmes mathématiques sont difficiles à résoudre (sécurité computationelle), tels que la factorisation de grands nombres ou le calcul de logarithmes discrets. Cependant, ces hypothèses sont basées sur les limitations des ordinateurs classiques et peuvent être compromises par des ordinateurs quantiques, capables de résoudre ces problèmes beaucoup plus rapidement.

Définition de la sécurité inconditionnelle

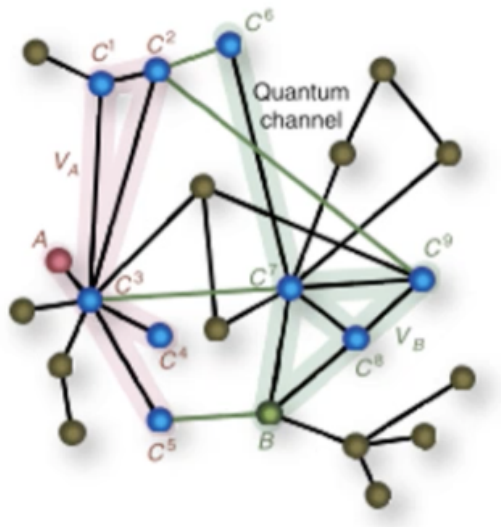
Elle est appelée sécurité inconditionnelle car la sécurité est basée sur les lois de la physique quantique et non sur la complexité computationnelle. La sécurité est garantie même si l'attaquant dispose d'une capacité de calcul infinie, comme c'est le cas avec un ordinateur quantique. Les lois pertinentes sont le théorème de non-clonage et le principe d'incertitude (sécurité de l'information). Exemple : BB84, l'argent quantique (1973).

Sécurité conditionnelle

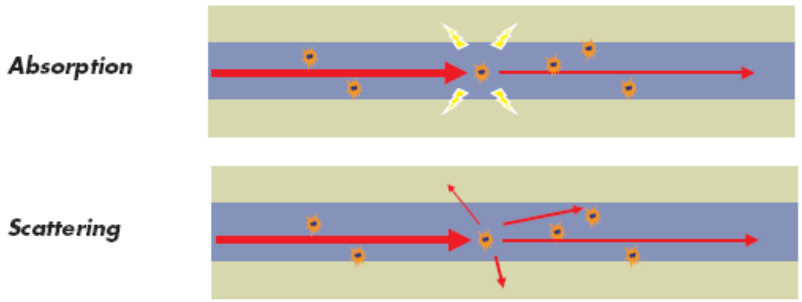
En pratique, atteindre une **sécurité inconditionnelle** dans la communication quantique est difficile car il est toujours théoriquement possible pour une tierce partie de compromettre la clé secrète en utilisant des technologies avancées ou en exploitant des faiblesses dans le protocole de communication.
La **sécurité conditionnelle** est considérée comme moins fiable que la sécurité inconditionnelle, mais elle est souvent utilisée dans les protocoles de communication quantique en raison de sa simplicité de mise en œuvre et de ses performances supérieures en termes de débits de transmission et de distances.

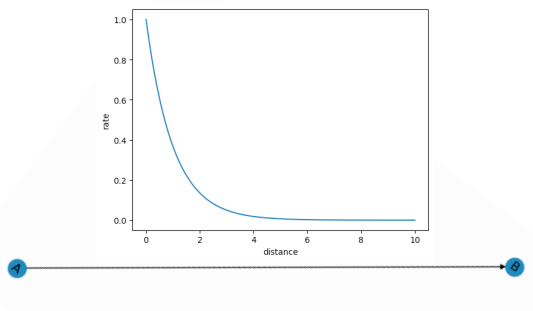
Réseaux quantiques

L'objectif d'un réseau quantique est la transmission et la manipulation de qubits à des emplacements différents.
Un avantage de l'utilisation d'un tel réseau a été démontré en termes de sécurité et d'efficacité.
Nœuds : ordinateur quantique, capteurs, source d'état quantique de la lumière, détecteurs seulement...
Lien : Canal quantique : espace libre, eau, fibre optique



Réseaux quantiques : décohérence et pertes

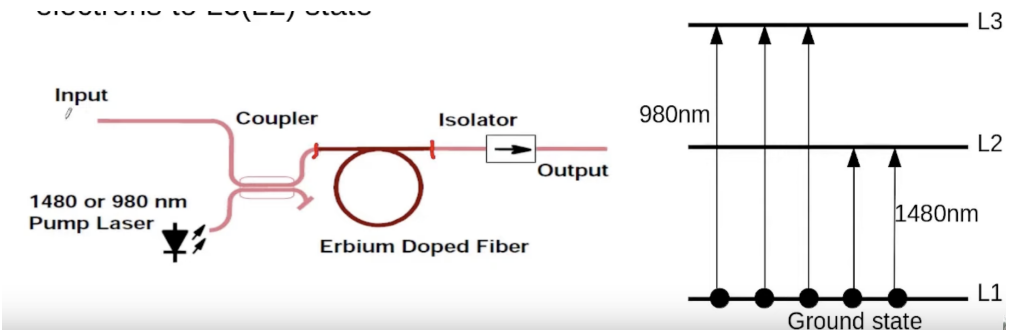


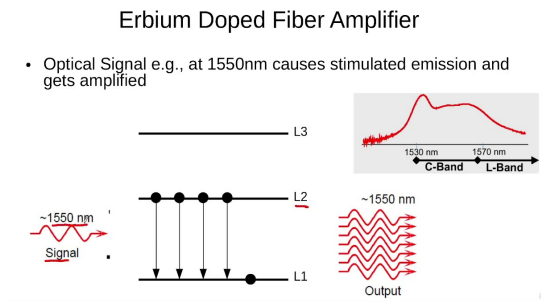


(À gauche) Source : `https://medium.com/@julydd/understanding-of-optical-losses-for-better-data-transmission-3674c0562`
À droite : Décroissance du taux de transmission en fonction de la distance (exponentielle pour la fibre optique, $1/r$ dans l'espace libre).

Réseaux quantiques : décohérence et pertes

→ Comment le problème est résolu avec des réseaux classiques ?
Répéteur à erbium (EDFA) : amplification et copie.





De `https://www.youtube.com/watch?v=muM6ppac-1U&ab_channel=Dr.MoazzamTiwana`

Peut on faire la même chose avec un système classique ?

Réseaux quantiques

Théorème de non-clonage quantique

Il est impossible de produire une copie exacte d'un état quantique inconnu et arbitraire. En d'autres termes, il n'est pas possible de cloner un état quantique sans perturber sa mesure.

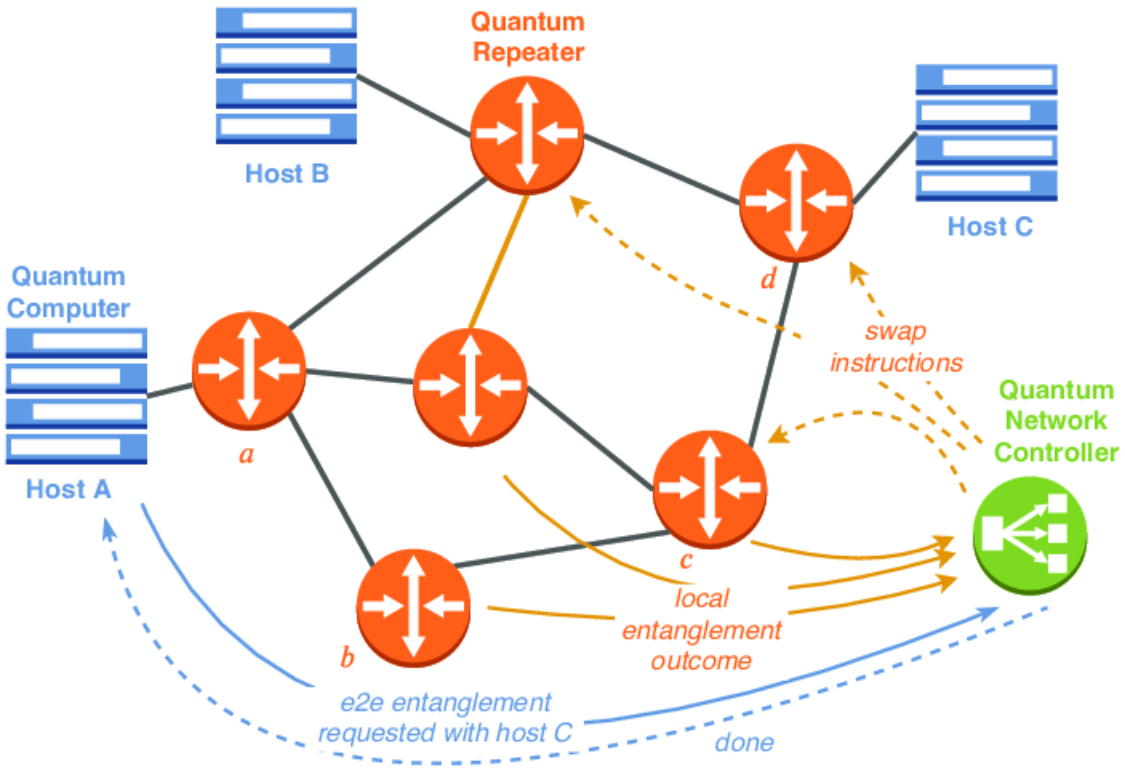
Preuve : L'opération de clonage est décrite par une opération unitaire, qui prend en entrée deux états dans deux chemins spatiaux a, b : celui à cloner $|\psi\rangle_a$ et une ancilla $|E\rangle_b$. Après l'opération de clonage, nous aurions : $\hat{U}|\psi\rangle_a|E\rangle_b = |\psi\rangle_a|\psi\rangle_b$. Cette opération peut s'appliquer à n'importe quel état dans a, elle s'applique donc également à $\hat{U}|\phi\rangle_a|E\rangle_b = |\phi\rangle_a|\phi\rangle_b$. En enchevêtrant ces deux expressions et en utilisant l'unitarité de $\hat{U}$, nous obtenons : $\langle\psi|\phi\rangle = |\langle\psi|\phi\rangle|^2$. Ces états sont soit orthogonaux, soit égaux, ce qui contredit l'hypothèse initiale selon laquelle les états étaient arbitraires.

Composants optiques spécifiques d'un réseau quantique

Il est possible de produire une copie imparfaite (avec une fidélité inférieure à un) : cela introduit du bruit dans le signal qui peut être détecté (perçu comme une attaque).
Amplifier un seul photon : ce n'est plus un seul photon, cela détruit l'information quantique.
Solutions pour transmettre des états quantiques sur de longues distances :

- Nœuds de confiance (vu dans ce cours) ou :
- Mémoires quantiques (non vu dans ce cours)
- Répéteurs quantiques (au cœur : échange d'intrication, non vu dans ce cours)

Composants optiques spécifiques d'un réseau quantique



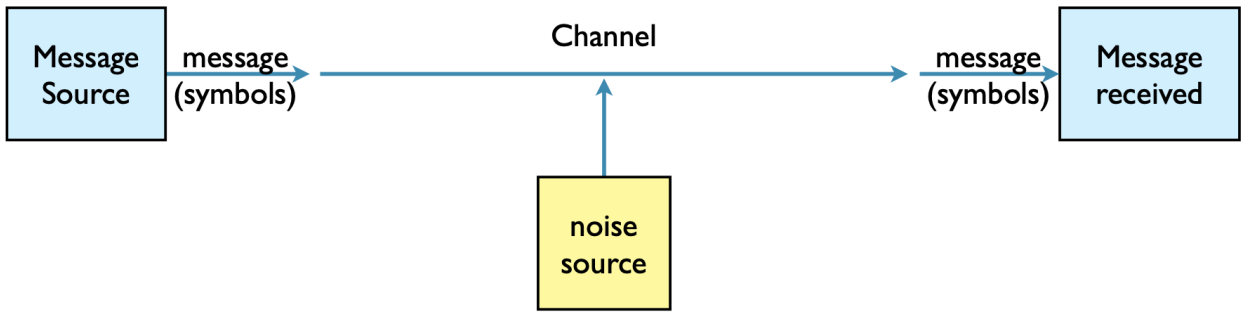
from `https://www.researchgate.net/figure/Quantum-network-architecture_fig1_352621787`.

Recap sur les réseaux quantiques

- Sécurité basée sur les lois de la physique quantique.
- Sécurité inconditionnelle sans imperfections (ce qui est absurde).
- Toujours un risque en matière de sécurité (confiance, imperfections, connaissance de la source/des détecteurs).
- Transmission sur de longues distances : téléportation, échange d'intrication : mémoires quantiques, répéteur quantique.

Sommaire

Schéma de communication



From Winter School on Quantum Networks of the Center for Quantum Networks (CQN)

One-time pad

Crypter un message
https://www.youtube.com/watch?v=gj9mzALyZYg&ab_channel=QuantumVisions

One-time pad

(1) Génération de clé : Une clé aléatoire aussi longue que le message est générée. Cette clé est utilisée une seule fois, d'où le terme "pad jetable".
(2) Chiffrement : Chaque bit ou caractère du message en clair est combiné avec le bit ou caractère correspondant de la clé en utilisant une addition modulaire (généralement XOR, ou exclusif). Cela donne le texte chiffré.

$$\text{Ciphertext}_i = \text{Plaintext}_i \oplus \text{Key}_i$$

(3) Déchiffrement : Pour décrypter, la même clé jetable est utilisée à nouveau avec le texte chiffré pour révéler le texte en clair original.

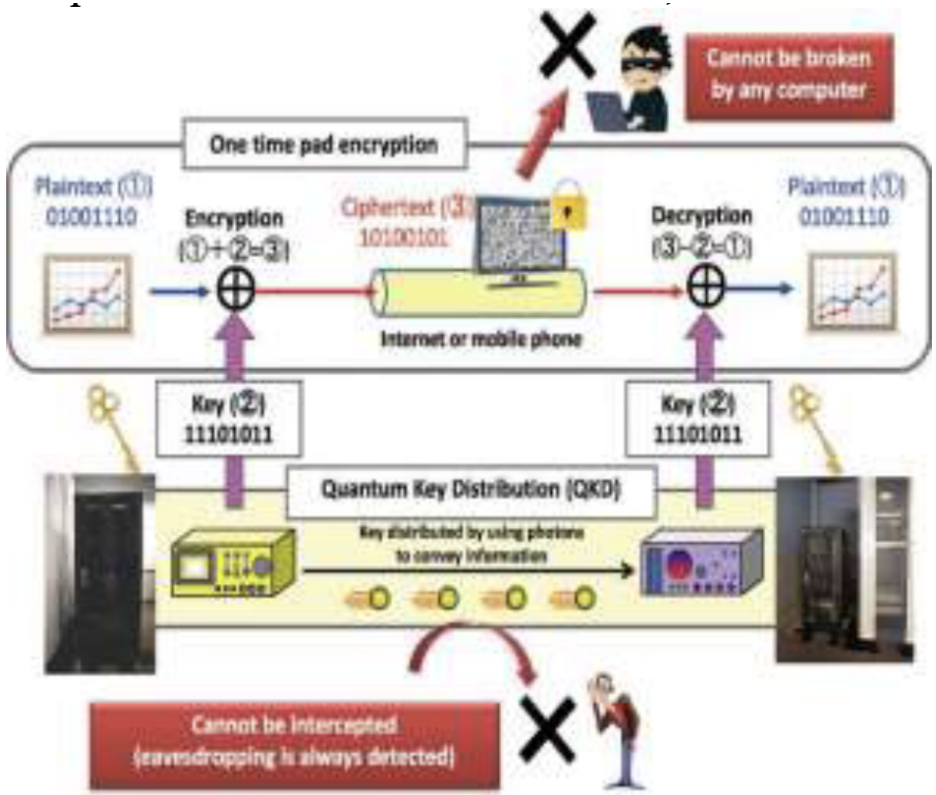
$$\text{Plaintext}_i = \text{Ciphertext}_i \oplus \text{Key}_i$$

- La clé doit être aussi longue que le message.
- La clé doit être véritablement aléatoire et gardée complètement secrète.
- La clé ne doit jamais être réutilisée pour un autre message.

QKD en quelques mots

La QKD remplace l'échange de clés (basé sur la cryptographie à clé publique) dans le but d'établir des clés secrètes. En QKD, la clé est encodée dans le degré de liberté des états quantiques de la lumière. Trois étapes :
- Envoyer la clé
- Mesurer les états quantiques de la lumière, et vérifier à l'aide d'un canal authentifié que la clé n'a pas été interceptée (quantité de bruit introduit par l'attaque)
- Envoyer le message chiffré par la clé (comme dans le cas du "one-time pad")

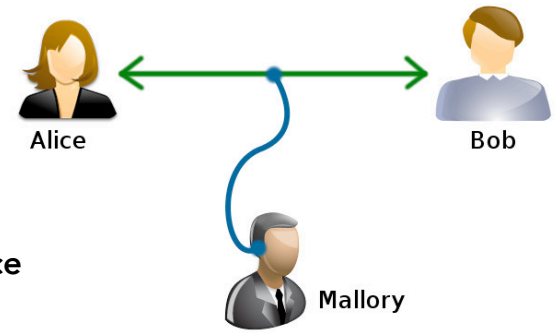
QKD en quelques mots



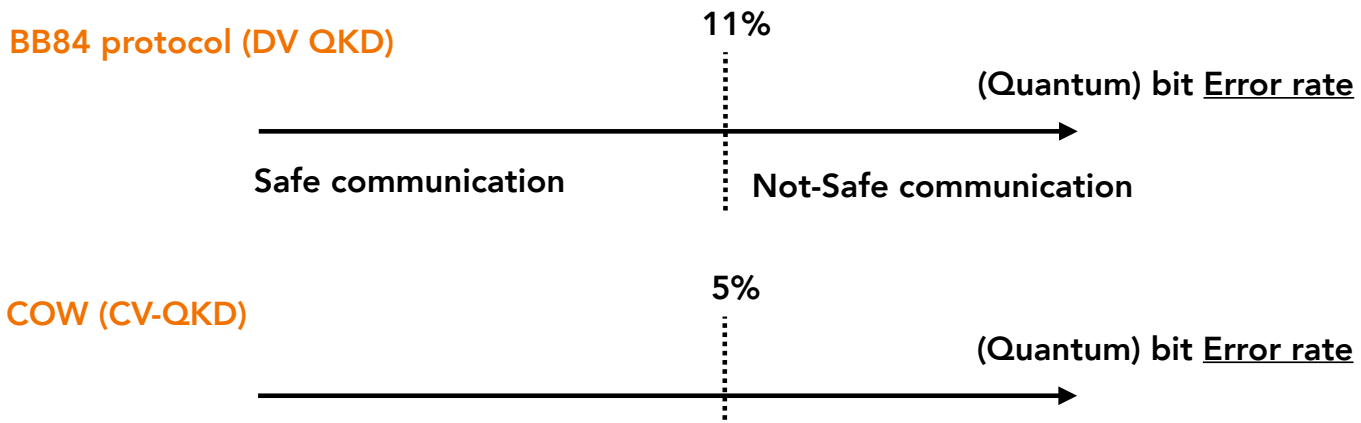
QKD en quelques mots

Alice et Bob veulent partager une clé secrète inconnue de l'attaquant.
Une clé parfaite est une liste de symboles parfaitement corrélés (0 et 1) partagée entre Alice et Bob, sur laquelle Eve n'a aucune information.

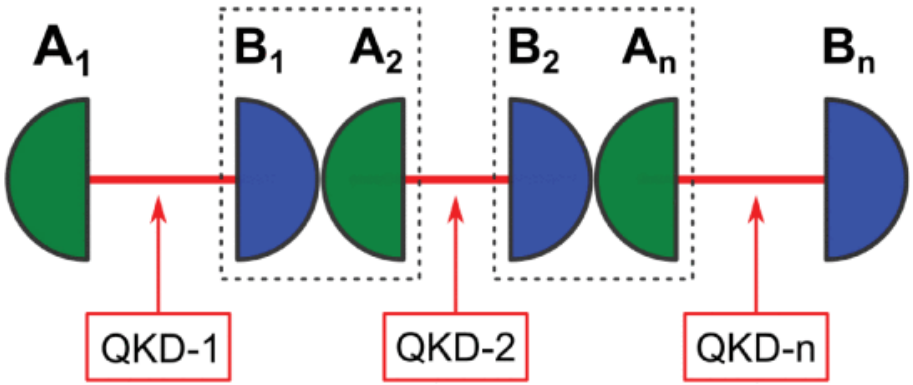
Quantum key distribution in a nutshell



Exchange the key, not the message
If Mallory can extract some information about the key, he will introduce noise that can be detected



Noeud de confiance



https://ieeexplore.ieee.org/document/9405393

(1) Envoyer la clé quantique dans le canal quantique vers le premier nœud, et le message chiffré dans le canal authentifié (OTP)
(2) Effectuer l'opération inverse pour obtenir le message.
(3) Envoyer une autre clé à travers le canal quantique vers le deuxième nœud, et encoder le message avec elle.
(4)...

Etendre la distance de communication

Étendre la distance et éviter la confiance de chacun des noeuds : répéteur quantique (pas dans ce cours).
- construit avec des mémoires quantiques et
- utilisant l'échange d'intrication (entanglement swapping)

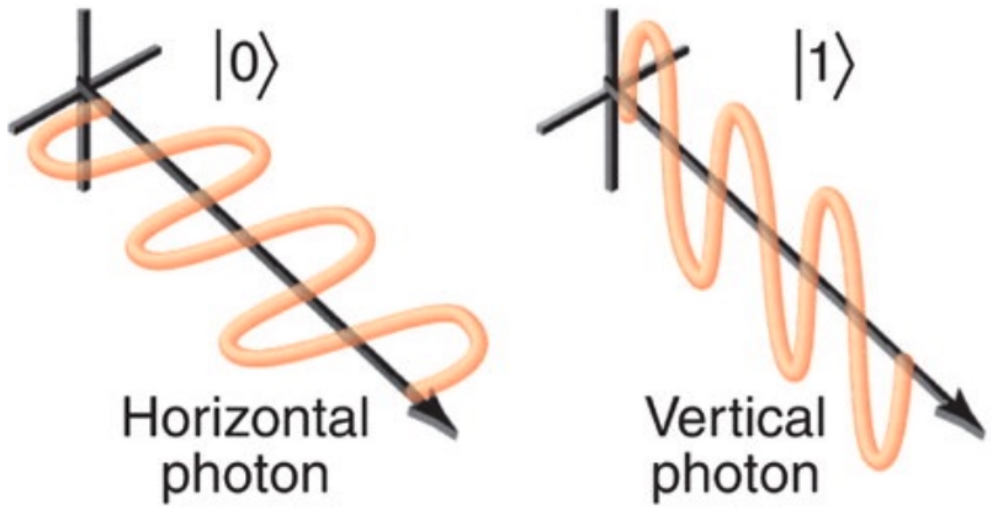
Plusieurs types de mémoires sont en cours de développement (pas encore de répéteur quantique).

Fin du premier cours

Sommaire

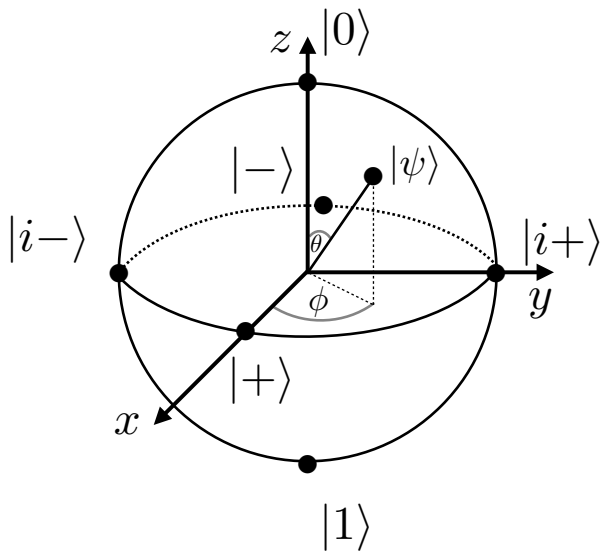
Photon unique

Le parfait vecteur d'information quantique pour les communications quantiques.
- Interagissent peu avec l'environnement
- Produit à la demande
- Difficile à intriquer (mais une paire de photons intriqué est facile à produire)



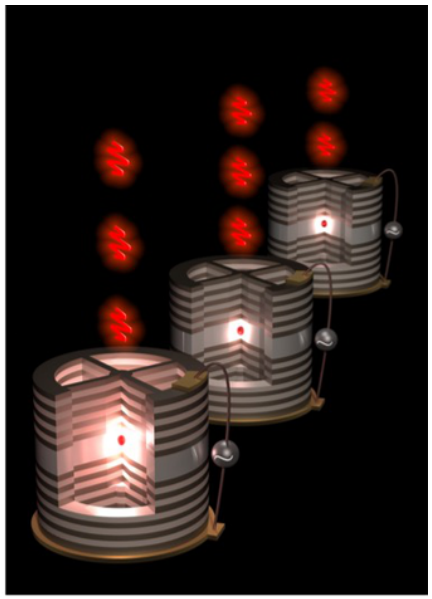
Qubits en polarisation

Base rectiligne : $|0\rangle_+ := |0\rangle$, $|1\rangle_+ = |1\rangle$
Base diagonale : $|0\rangle_\times := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle_\times := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
Ce sont des des bases complémentaires $|_+\langle b|b\rangle_\times| = \frac{1}{\sqrt{2}}$.

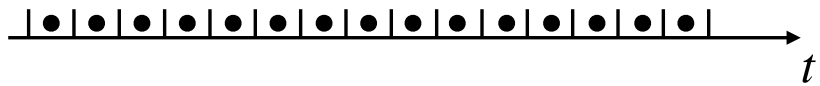


Source de photons uniques

Une source de photons uniques est un dispositif qui émet des photons un par un de manière déterministe à partir d'objets microscopiques tels qu'un atome individuel, un centre coloré dans un cristal ou une boîte quantique dans un semi-conducteur artificiel.
Example : Start-up Quandela : boîtes quantiques (ou centre NV)



Single Photon state

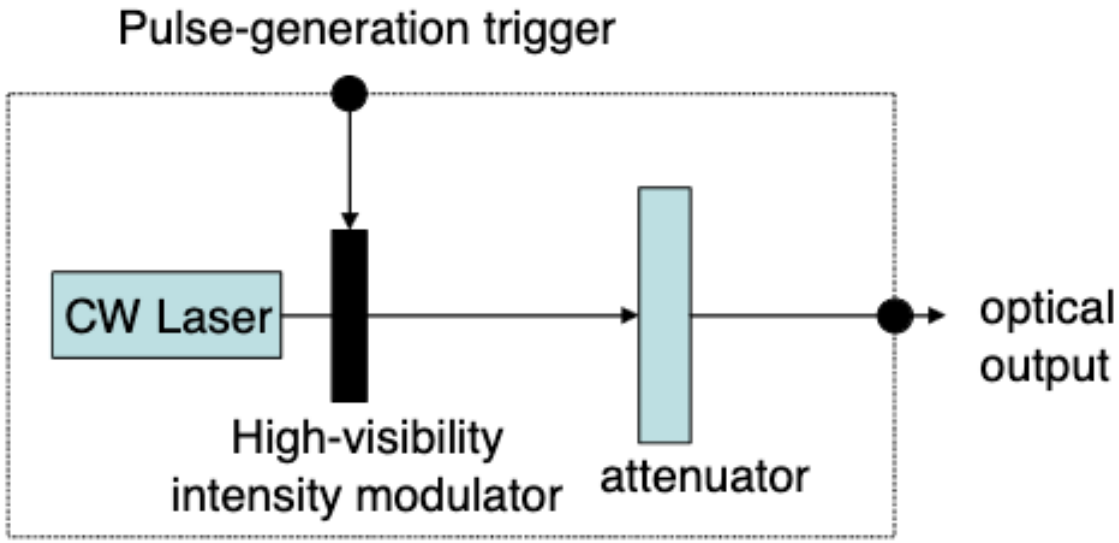


Source de photons unique : en fait...

Utilisation d'états cohérents (laser) atténuées (weak coherent state).

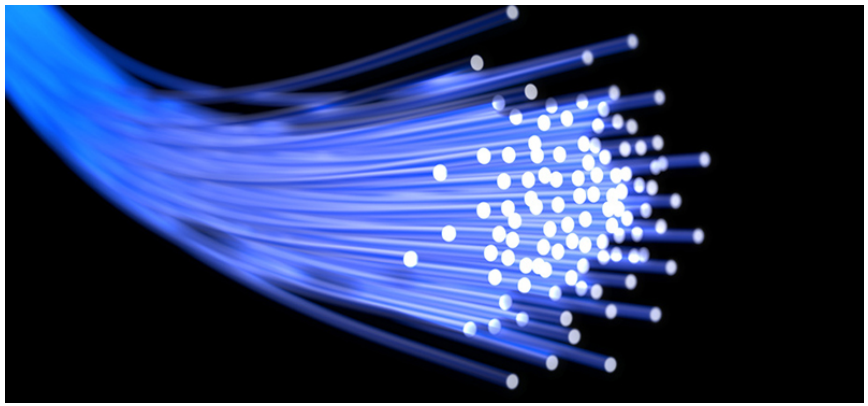
$$|\alpha\rangle = e^{-|\alpha|^2/2}(|0\rangle + \alpha\,|1\rangle + ...) \tag{1}$$

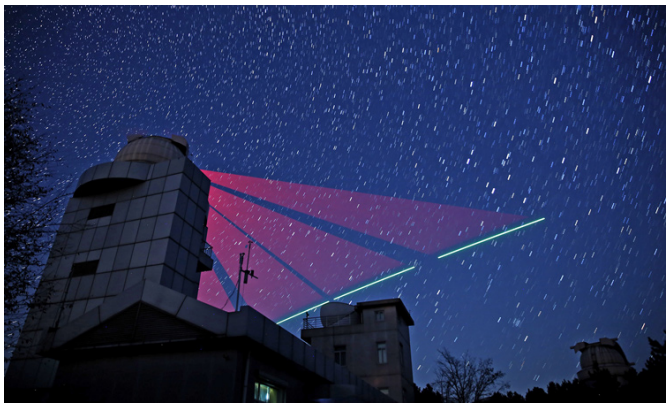
with $\langle\hat{n}\rangle = |\alpha|^2$. Une source de photon unique on-demand est pour le moment couteux (et température cryogénique, et longueur d'onde de 900 nm). Mais plus pour longtemps...



Canal quantique

Fibre optique, atmosphère...





Le canal quantique effectue des opérations logiques sur les états quantiques, induisant donc des erreurs !

Coefficient de transmission

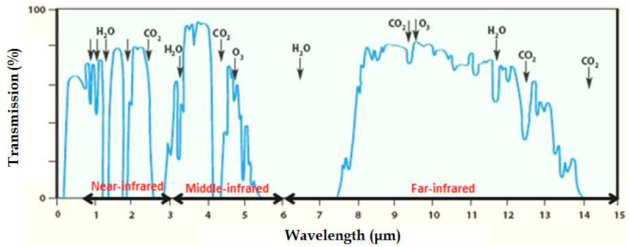


Fig. 27.5. Atmospheric transmission versus wavelength for the UV, visible and infrared bands.

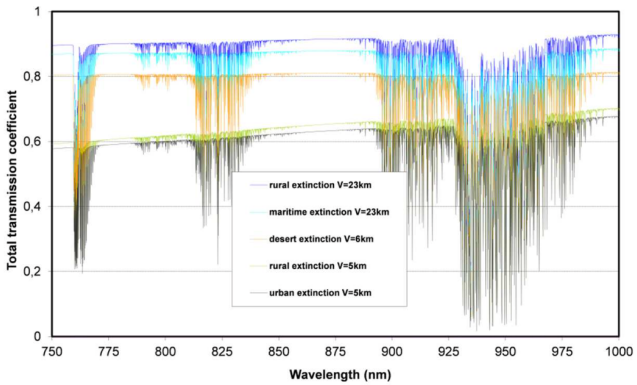
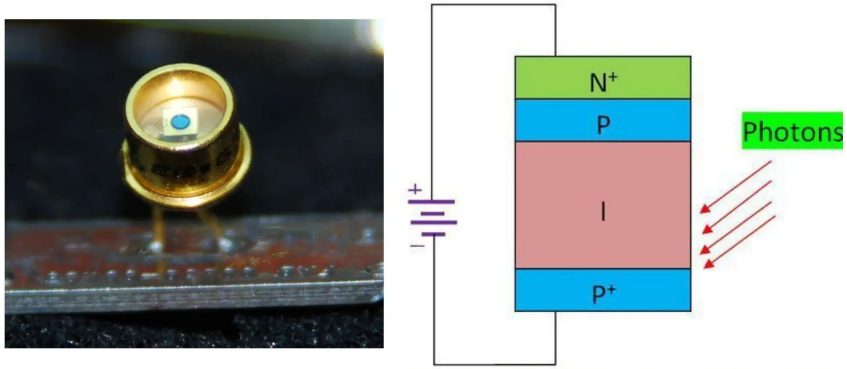


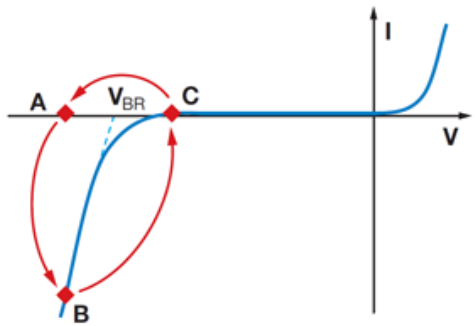
Fig. 27.6. Atmospheric transmission for a 1-km path, at an altitude of 1 m for several locations and visibility ranges.

From Free-Space Quantum Key Distribution, Optical Wireless Communications, 2016 p 589-607

Detecteur de photons uniques à photoavalanche



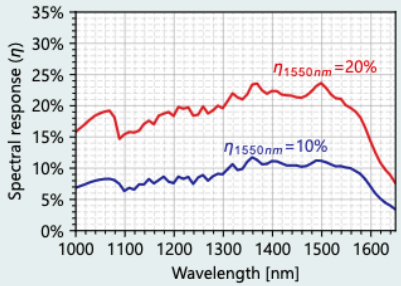
From `https://electricalguide360.com/avalanche-photodiode-or-apds-working-materials-its-uses/?utm_content=cmp-true`



Characteristics of APD

Broadband performance

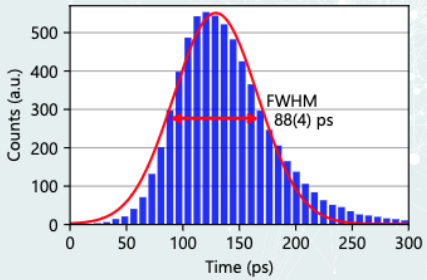
High system detection efficiency (SDE) across a broad range, characterized with equipment carefully calibrated by METAS.



(Above) Spectral response measurement for a typical ID Qube NIR device.

High precision

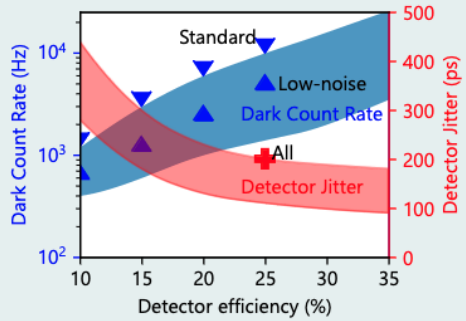
See the best timing resolution with the lowest detection timing jitter.



(Above) Timing jitter measurement of an ID Qube NIR detector at 30% SDE, including all other instrument jitter contributions, recorded with an ID1000 Time Controller.

Low noise

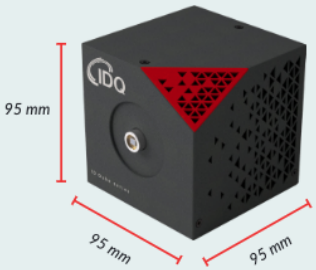
Always few dark counts with our Standard Qube models, and even better with the Low Noise model.



(Above) Dependence of detector noise and timing jitter with SDE. Users have the ability to balance the SDE, noise and precision to best fit their needs.

Compact

The ID Qube's small and compact form factor fits well into your experiments, and ideally suited for applications such as LiDAR, where compactness is key for system integration.

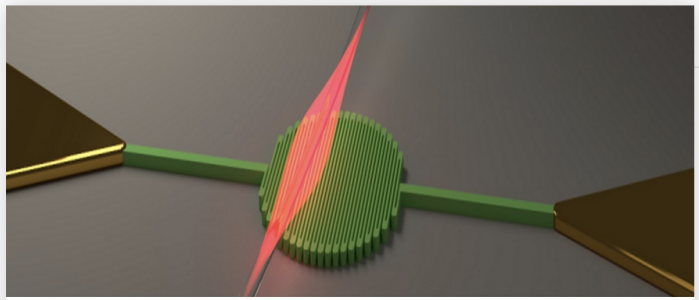


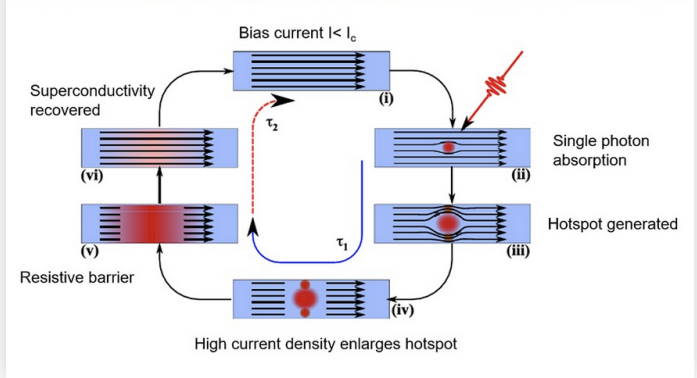
From IdQuantique

Detection : exemple de détecteur de photons uniques

Détecteur de photon unique à nanofils supraconducteurs : ne compte pas le nombre de photons, il fait un clic à chaque détection d'événement..
Un courant constant en dessous du courant critique est appliqué et $T = 2.5$K.
Après l'absorption d'un seul photon, le dispositif est localement à une phase normale, et le courant passe par un dispositif d'amplification où une tension est mesurée.

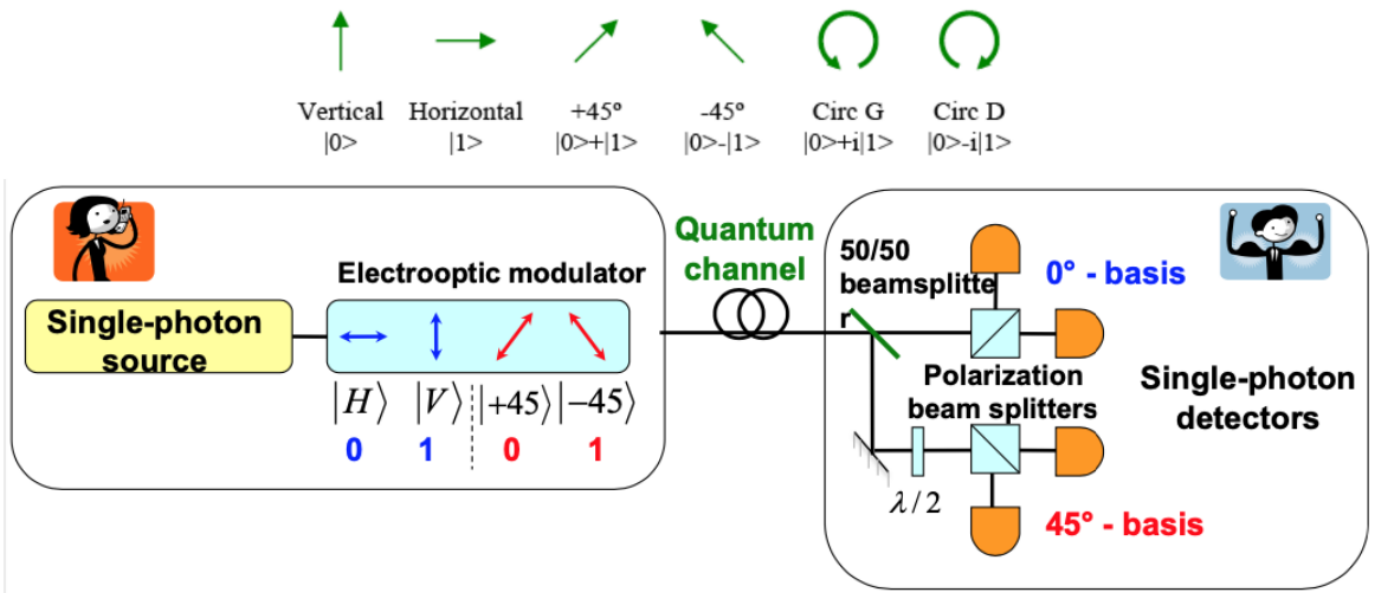
Etat de l'art : $<$ 15 ps timing jitter. From `https://singlequantum.com/technology/snspd/`





BB84 : description du protocole

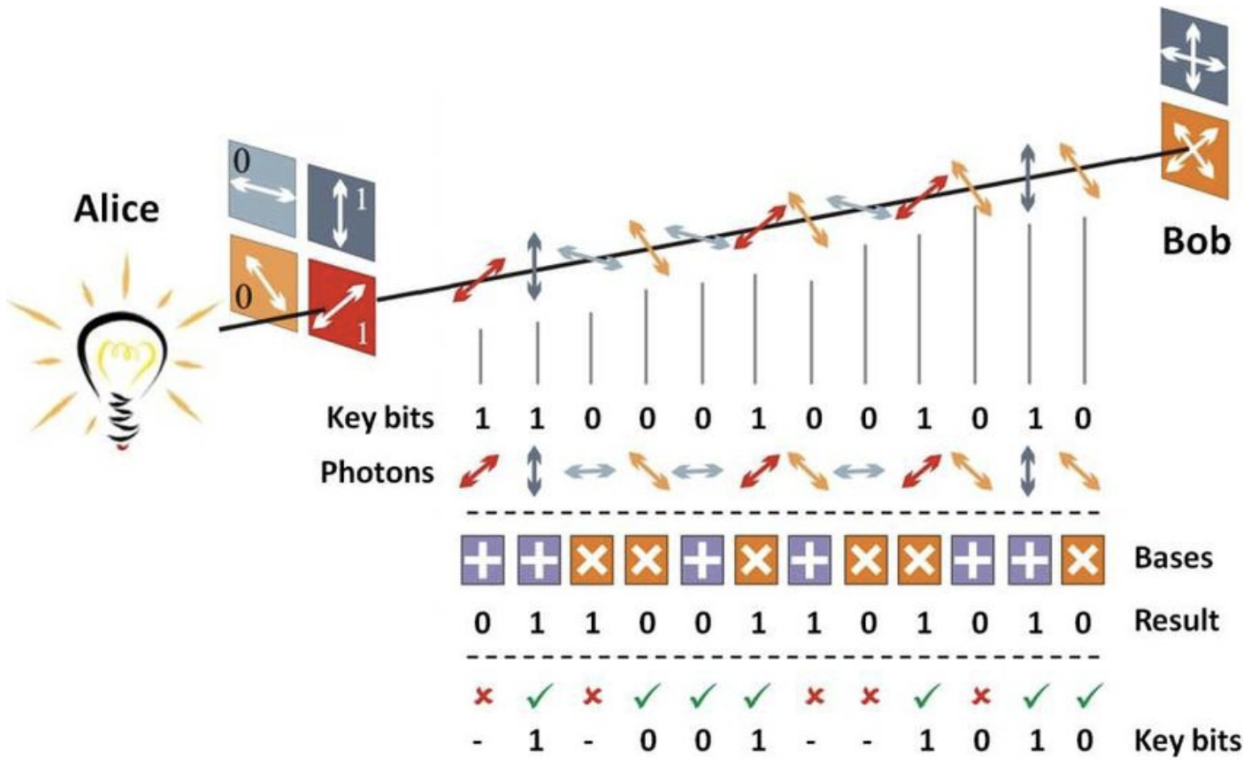
DV-QKD : discrete variable quantum key distribution protocol (utilisation de degrés de libertés discret de photons uniques)
Protocole décrit ici : BB84 (Bennett et Brassard)



BB84 : description du protocole

(1) Alice sélectionne des chaînes aléatoires : les bits $(a_1, ..., a_n)$ et l'orientation de polariseurs $(\alpha_1, ..., \alpha_n)$. Ces deux ensembles déterminent la polarisation de chaque photon unique. Bob choisit également une orientation aléatoire de polariseur $(\beta_1, ..., \beta_n)$.
(2) Alice envoie ses états de photons uniques polarisés.
(3) Bob mesure les photons uniques reçus en utilisant l'orientation de polariseur déterminée par β_i.
(3) Alice et Bob envoient leur orientation (respectivement, base de mesure).
(4) Ils déterminent les intervalles de temps où ils ont la même orientation $\alpha_i = \beta_i$, et génèrent une nouvelle clé (de tri).
(5) Si la longueur de la clé est supérieure à un seuil donné, ils abandonnent le protocole.

BB84 : description du protocole

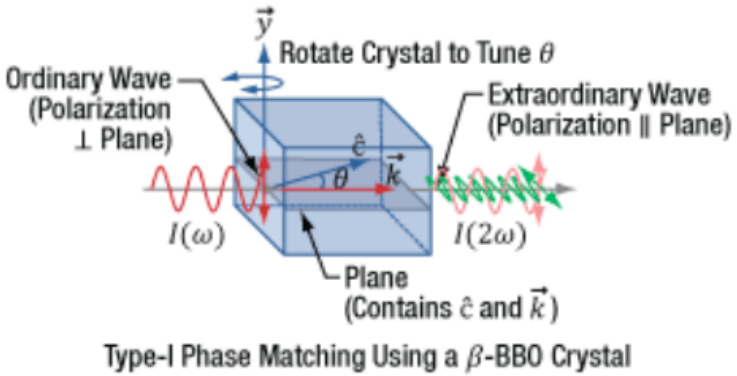


Extrait de Optical Wireless Communications - An Emerging Technology (pp.589-607).

Production de paires de photons intriqués en polarisation

Généré par un processus non-linéaire appelé conversion descendante paramétrique spontanée ou mélange à 4 ondes (à température ambiante)

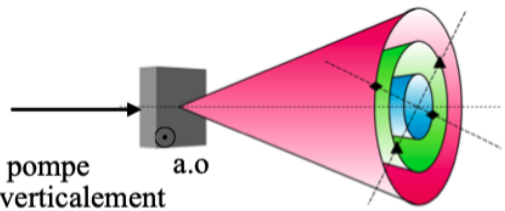
- Effet non-linéaire (effet de conversion paramétrique spontanée)



Type-I Phase Matching Using a β-BBO Crystal

Production de paires de photons intriqués en polarisation

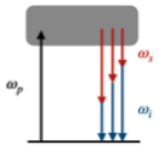
- Effet non-linéaire (effet de conversion paramétrique spontanée) contraint par deux processus:



Laser de pompe polarisé verticalement

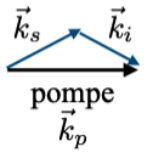
a.o

$$|\psi\rangle = |HH\rangle_{12}$$



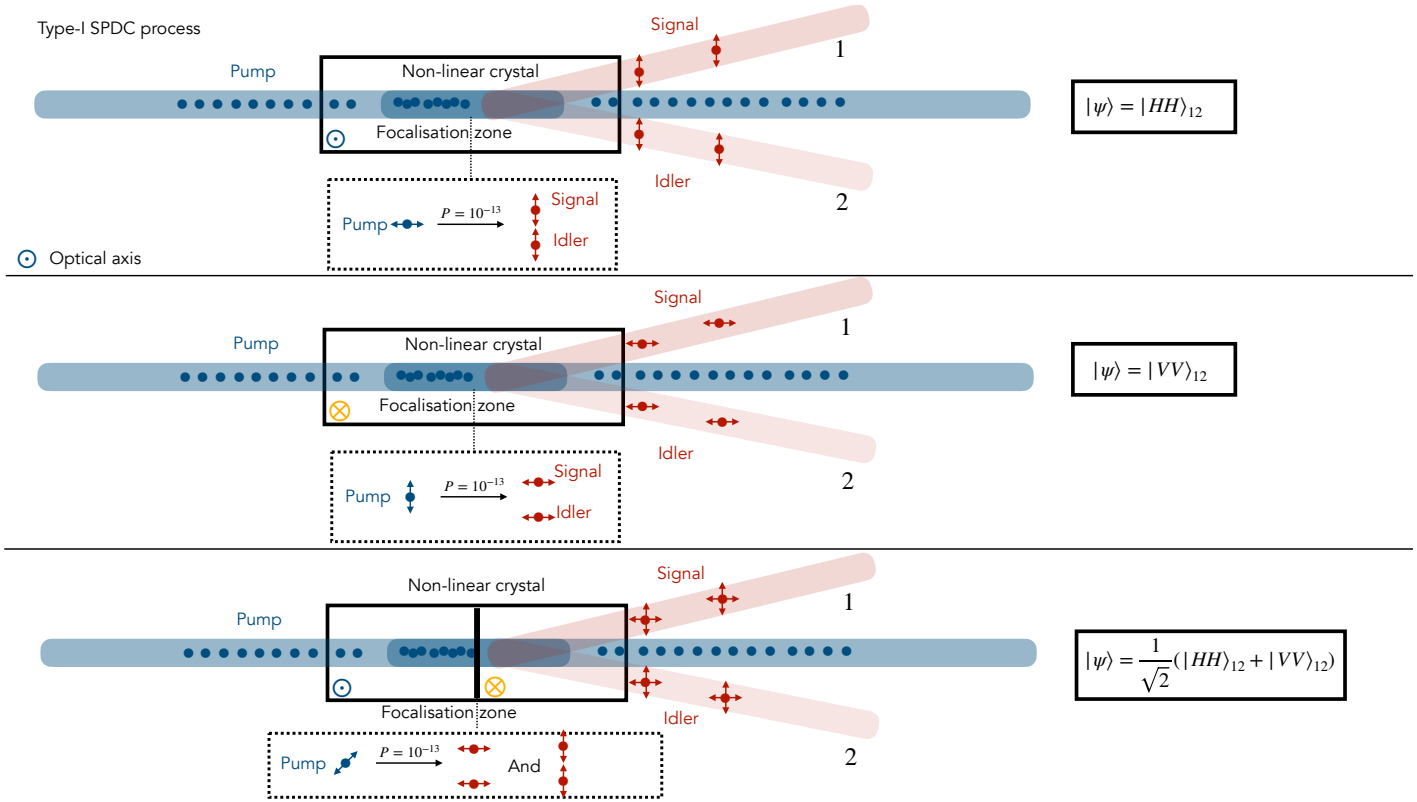
$$\omega_p = \omega_s + \omega_i$$

- Conservation de l'énergie

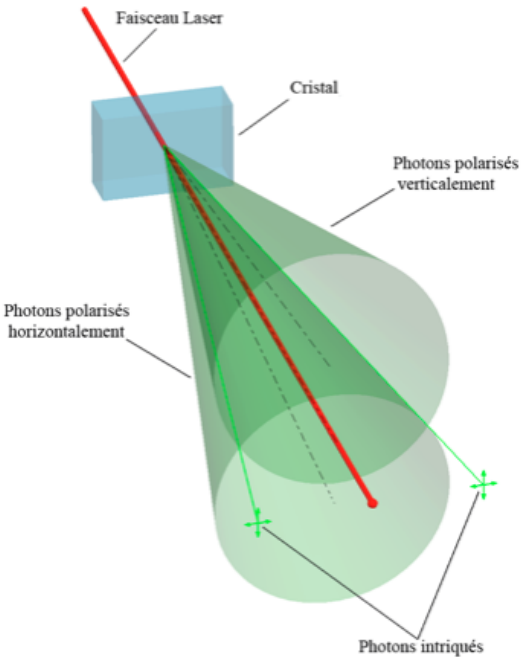


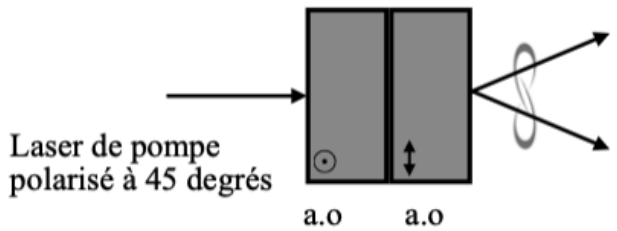
Conservation de l'impulsion

Production de paires de photons intriqués en polarisation



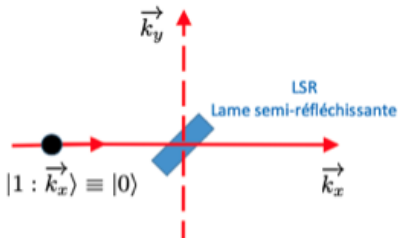
Production de paires de photons intriqués en polarisation





$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |H\rangle_2 + |V\rangle_1 \otimes |V\rangle_2)$$

- Analogue à un photon qui est soit réfléchie, soit transmis



Qutools

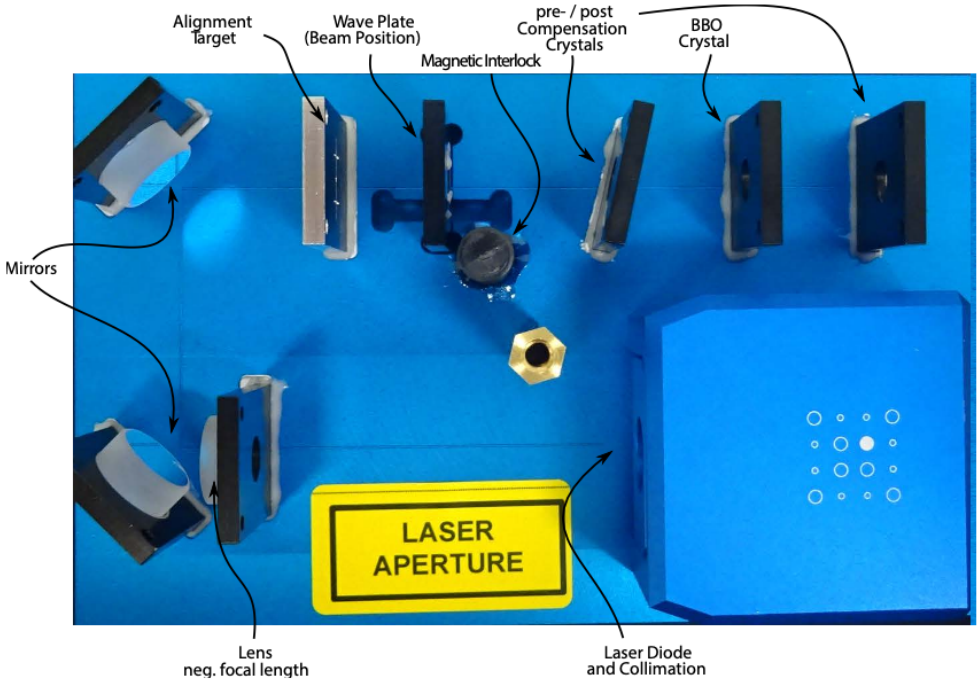
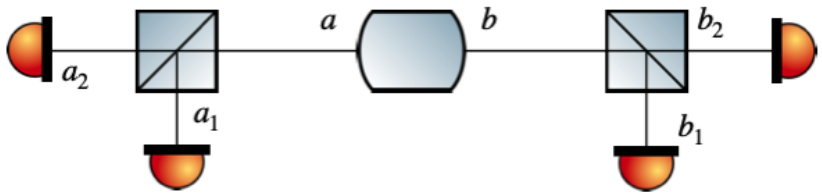


Figure 1.5: Inner details of the pump assembly with the nonlinear crystal.

Production de paires de photons intriqués en polarisation

- Mesures de polarisation de paires de photons

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle_{ab} + |VV\rangle_{ab}).$$

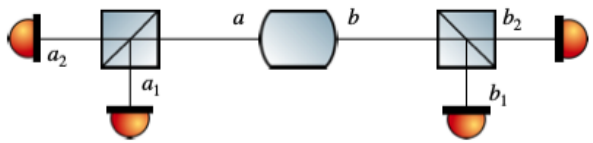


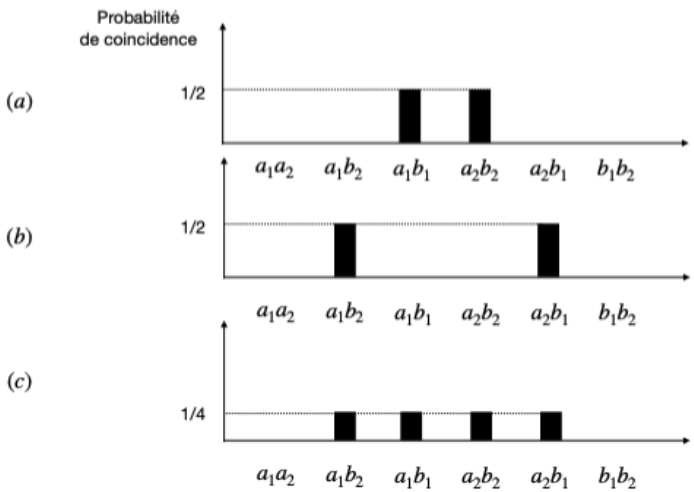
- Après la génération des paires de photons $|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle_{ab} + |VV\rangle_{ab}).$
- Après les cubes séparateurs de polarisation $|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle_{a_1b_1} + |VV\rangle_{a_2b_2})$
- Probabilité de **coincidence:** $P(VV) = P(HH) = \frac{1}{2}$

$$P(HV) = P(VH) = 0$$

Production de paires de photons intriqués en polarisation

- Mesures de polarisation de paires de photons



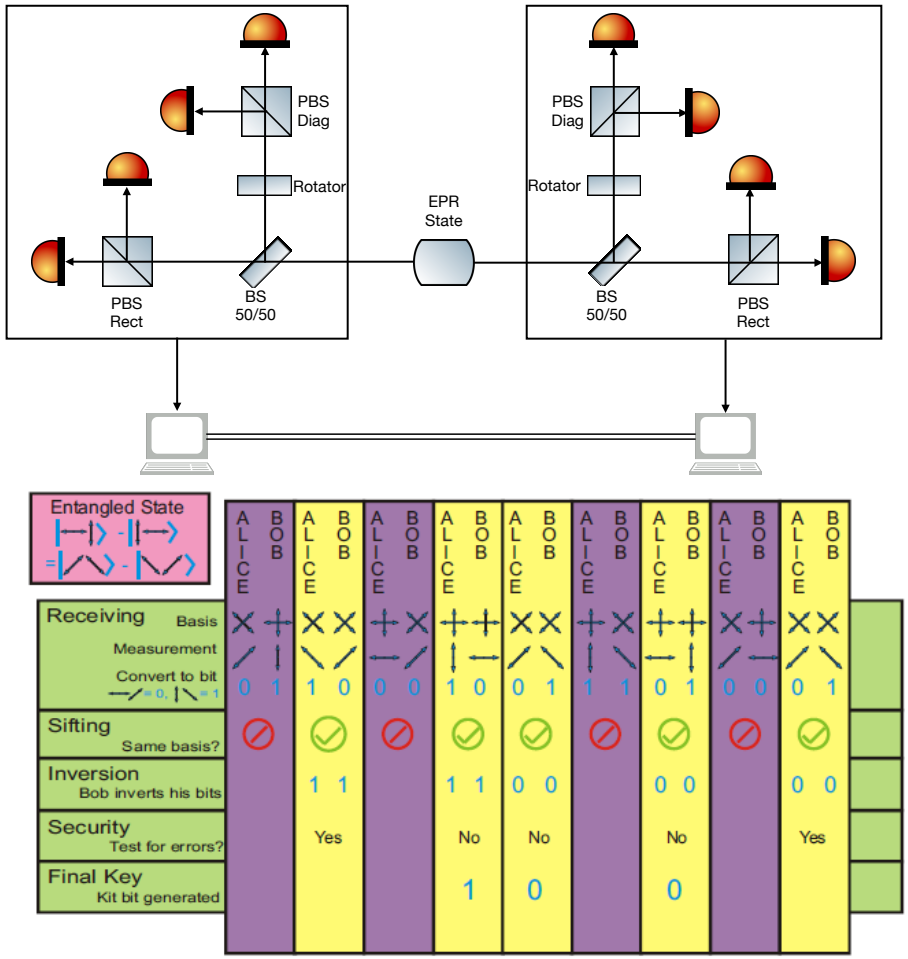


$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle_{ab} + |VV\rangle_{ab}).$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle_{ab} + |VH\rangle_{ab}).$$

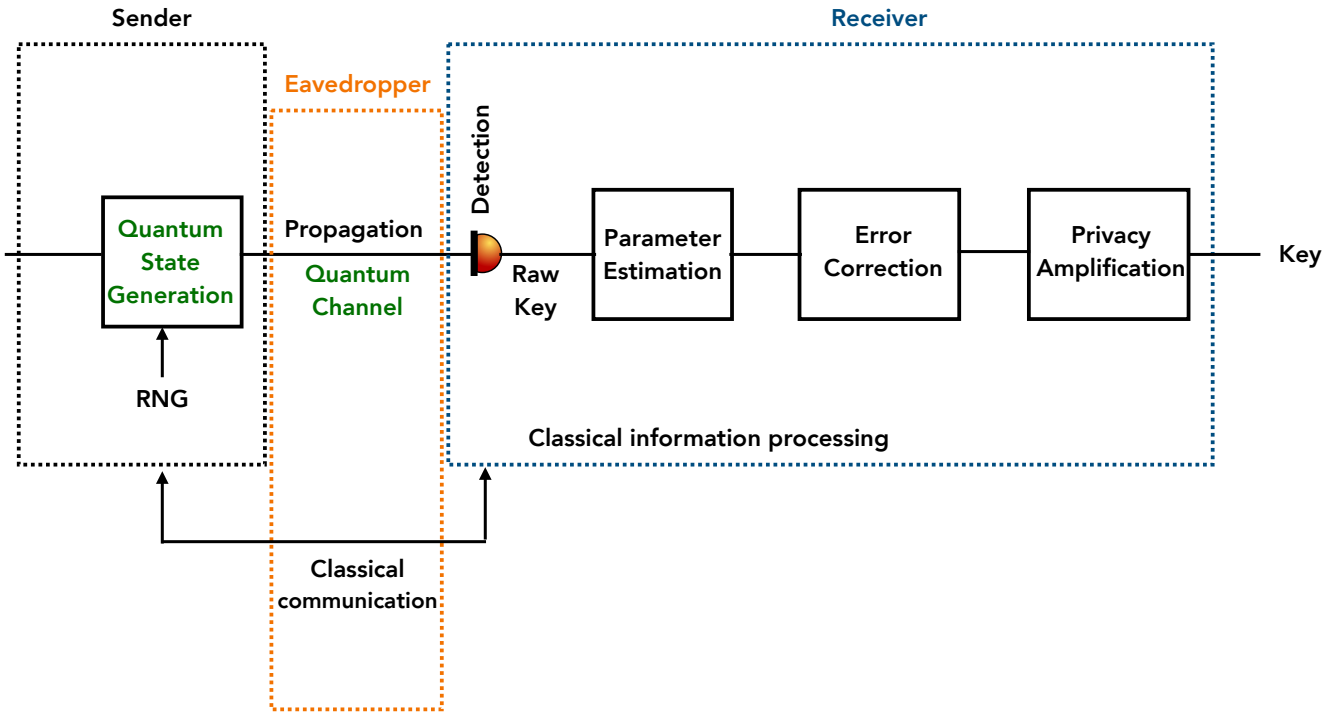
$$|\psi\rangle = \frac{1}{2}(|HH\rangle_{ab} + |HV\rangle_{ab} + |VH\rangle_{ab} + |VV\rangle_{ab}) = \frac{1}{\sqrt{2}}(|H\rangle_a + |V\rangle_a) \otimes \frac{1}{\sqrt{2}}(|H\rangle_b + |V\rangle_b$$

Protocole BBM92



Erven, Chris. (2007). On Free Space Quantum Key Distribution and...

Schéma global



On passe à l'étape de post-processing.

QBER

Le QBER est défini comme le rapport entre les détections erronées sur le nombre total de détections.

QBER

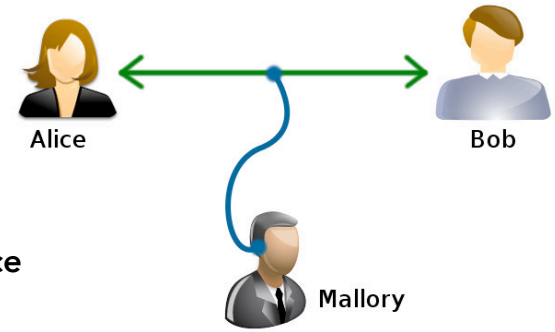
$$\epsilon = \frac{R_{\text{error}}}{\frac{1}{2}R_{\text{raw}} + R_{\text{error}}} \tag{2}$$

Le 1/2 représente la conciliation des bases (sifting) pour le protocole BB84.

Si le QBER dépasse un certain seuil, c'est que la communication a été intercepté. Une attaque donnée introduit un niveau donné de bruit. Même avec des capacités infinies de calcul pour un adversaire, il ne parviendrait pas à se dissimuler.

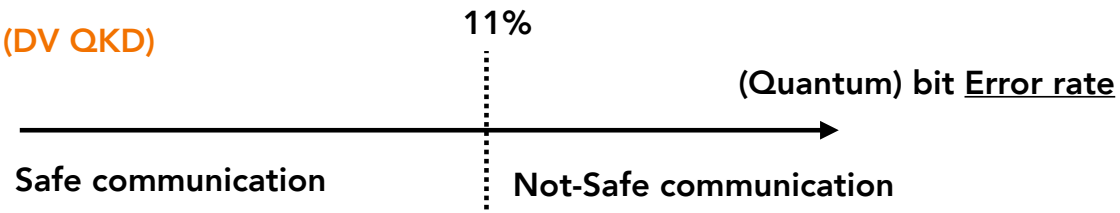
QKD en quelques mots

Quantum key distribution in a nutshell

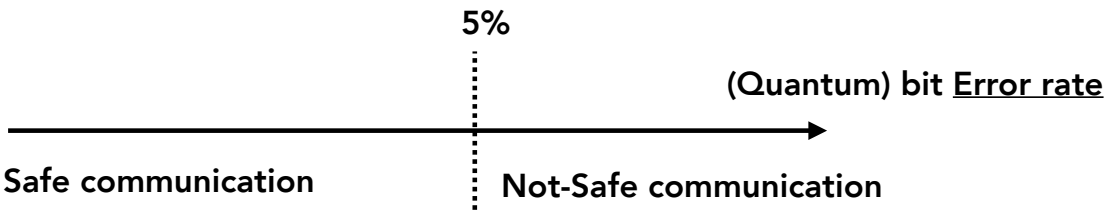


Exchange the key, not the message
If Mallory can extract some information about the key, he will introduce noise that can be detected

BB84 protocol (DV QKD)



COW (CV-QKD)



Estimation de paramètre (QBER)

Que se passe-t-il après le triage ? Estimez le taux d'erreur de la séquence de bits et décidez d'abandonner ou non.
(1) Alice envoie une petite partie de sa séquence à Bob.
(2) Bob calcule le taux d'erreur (voir QBER) avec la séquence qu'il a reçue.
(3) Pour l'ensemble de la séquence, le taux d'erreur quantique (QBER) est censé être le même que celui de l'échantillon (inequalité de Serfling).
(4) Quel est le seuil ?

Classical post-processing (version rapide)

• Correction d'erreur : Une fois que le code de correction d'erreur a été convenu, l'expéditeur peut l'utiliser pour encoder les états quantiques qui doivent être transmis.
Code unidirectionnel : d'Alice à Bob (chaîne supplémentaire pour vérifier son erreur). Difficile, mais à la fois efficace et proche de la limite de Shannon.
Code bidirectionnel : L'information classique est envoyée dans les deux sens. Cette approche se rapproche davantage de la **limite de Shannon**. Il y a des codes qui **délaissent** les erreurs et d'autres qui les **corrigent**.
• Amplification de confidentialité : L'amplification de confidentialité vise à réduire cette vulnérabilité en utilisant des fonctions de hachage et de confusion pour "amplifier" les informations non désirées et les rendre inutilisables pour l'adversaire.

Amplification de la confidentialité par discussion publique

Amplification de la confidentialité : L'amplification de la confidentialité vise à réduire cette vulnérabilité en utilisant une **fonction de hachage**, qui est une fonction mathématique permettant de transformer la clé en une version plus courte tout en préservant sa confidentialité. Nous appelons $\mathcal{F}$ la famille de fonctions de la clé X à la clé Z, et $p_{\mathcal{F}}$ une distribution de probabilité sur $\mathcal{F}$.
Une fonction de hachage deux-universelle $f : X \times Y \rightarrow Z$ est définie par :

$$\Pr Y(f(x, Y) - f(x', Y)) \leq \frac{1}{|Z|} \tag{3}$$

où f est choisie aléatoirement dans $\mathcal{F}$ selon $p\mathcal{F}$. Cela quantifie la différence entre les deux clés plus courtes générées.

Amplification de la confidentialité par discussion publique

Vérification du test :
(0) Alice et Bob ont respectivement la clé brute x, x'.
(1) Alice choisit de manière uniforme un $y \in Y$ et le transmet à Bob. Alice transmet également la fonction de hachage qu'elle choisit aléatoirement.
(2) Alice calcule la clé plus courte $z = f(x, y)$.
(3) Bob calcule $z' = f(x', y)$ qui coïncide avec z avec une probabilité de $1/|Z|$. Si les valeurs diffèrent, ils abandonnent.

Architecture globale d'un réseau QKD

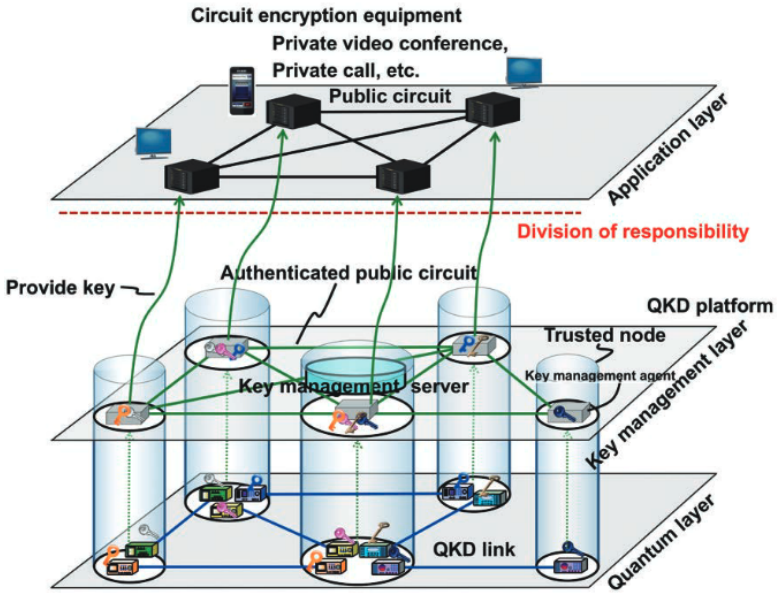
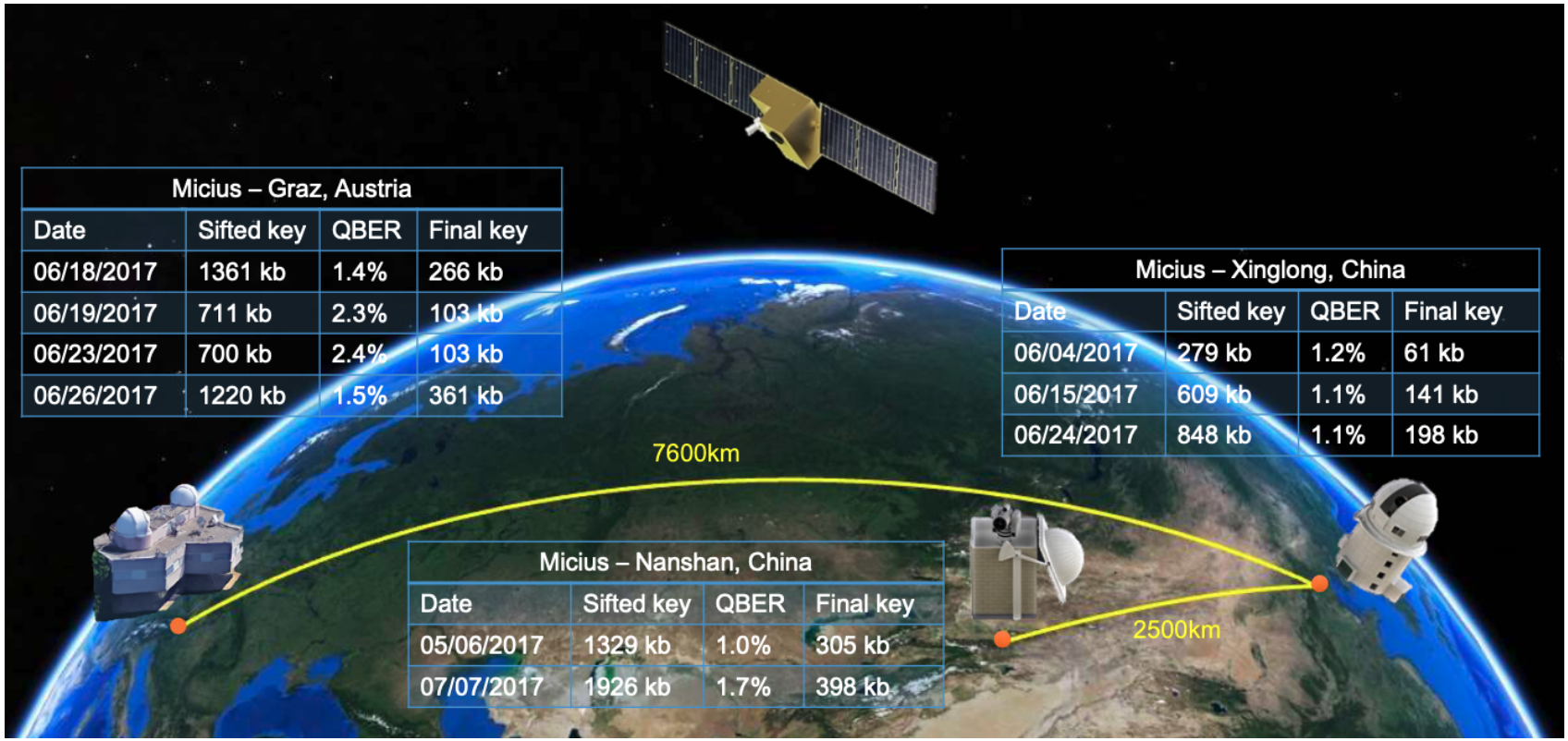


Figure 2 QKD platform overview
Quantum layer composed of QKD links from various vendors
Key management layer
Key management server: Constantly monitors overall network state and manages rerouting, etc.
Key management agent: Arranges and records cryptographic key formats and provides them according to user requests

https://www.nict.go.jp/en/data/nict-news/NICT_NEWS_1608_E.pdf

Micius satellite : prepare and measure QKD, BB84 (2017)



Micius satellite : entangled-based QKD, BBM92 (2020)

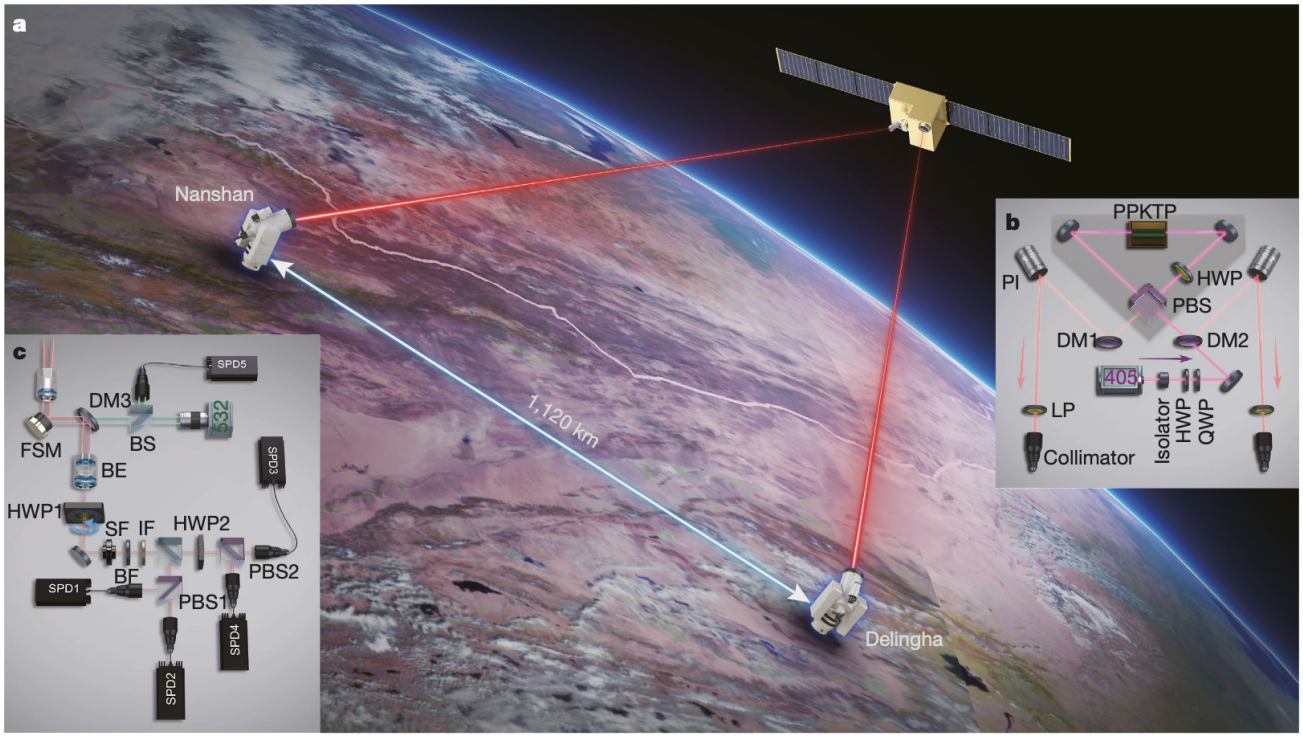
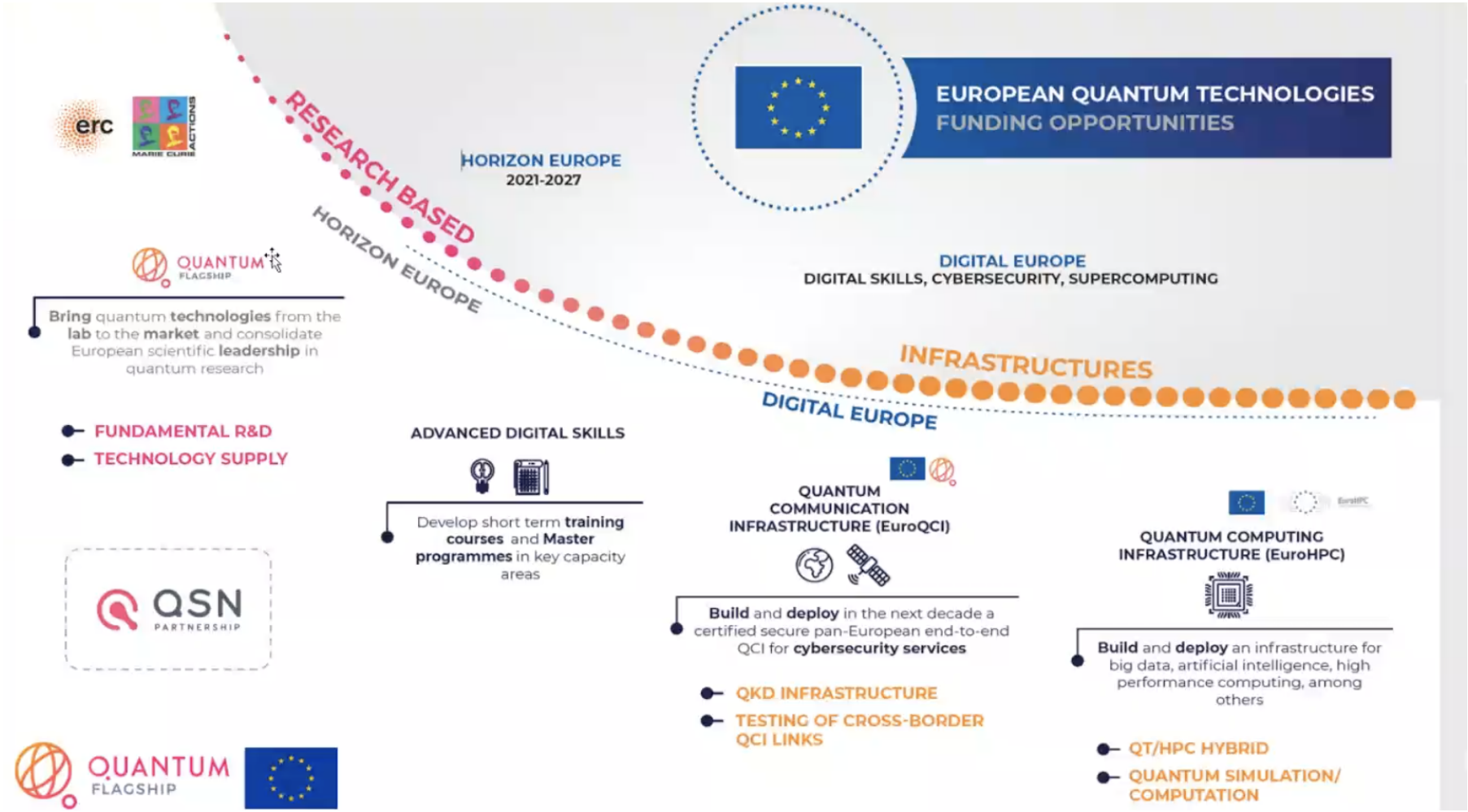


Fig. 1 | Overview of the experimental set-up of entanglement based quantum key distribution. a, An illustration of the Micius satellite and the two ground stations. Image credit: Fengyun-3C/Visible and Infrared Radiometer, with permission (2020). The satellite flies in a Sun-synchronous orbit at an altitude of 500 km. The physical distance between Nanshan and Delingha ground station is 1,120 km. **b**, The spaceborne entangled-photon source. A free space isolator is used to minimize back reflection to the 405-nm pump laser. A pair of off-axis concave mirrors is used to focus the pump laser and collimate the down-converted photon pairs. PBS, polarization beam splitter; DM, dichroic mirror; LP, long-pass edge filter; PI, piezo steering mirror; HWP, half-wave plate; QWP, quarter-wave plate; PPKTP, periodically poled $KTiOPO_4$. **c**, The follow-up optic at the optical ground station. The tracking and synchronization laser is separated from the signal photon by DM3 and detected by the single photon detector (SPD5). The spatial filter (SF), broad-bandwidth filter (BF) and interference filter (IF) are used to filter out the input light in frequency and spatial domains. BS, beam splitter; BE, beam expander; FSM, fast steering mirror.

Sommaire

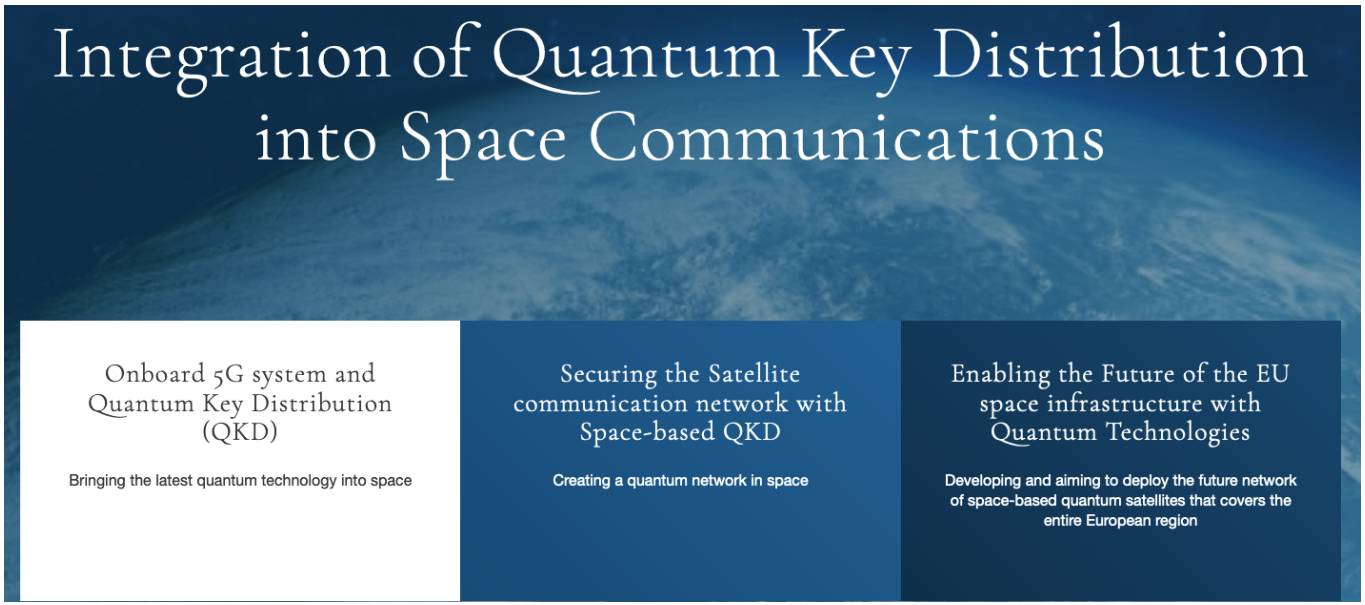
European project : EuroQCI



European project : QSNP

Communication quantique par satellite

QUDICE
QUantum Devices and subsystems for Communications in spacE



Voir également Eagle 1.

Liste non-exhaustive de partenaires

https://www.nature.com/articles/nature23655

En Italie

https://iopscience.iop.org/article/10.1088/1742-6596/2416/1/012001/pdf

Réseaux quantiques entre plusieurs villes

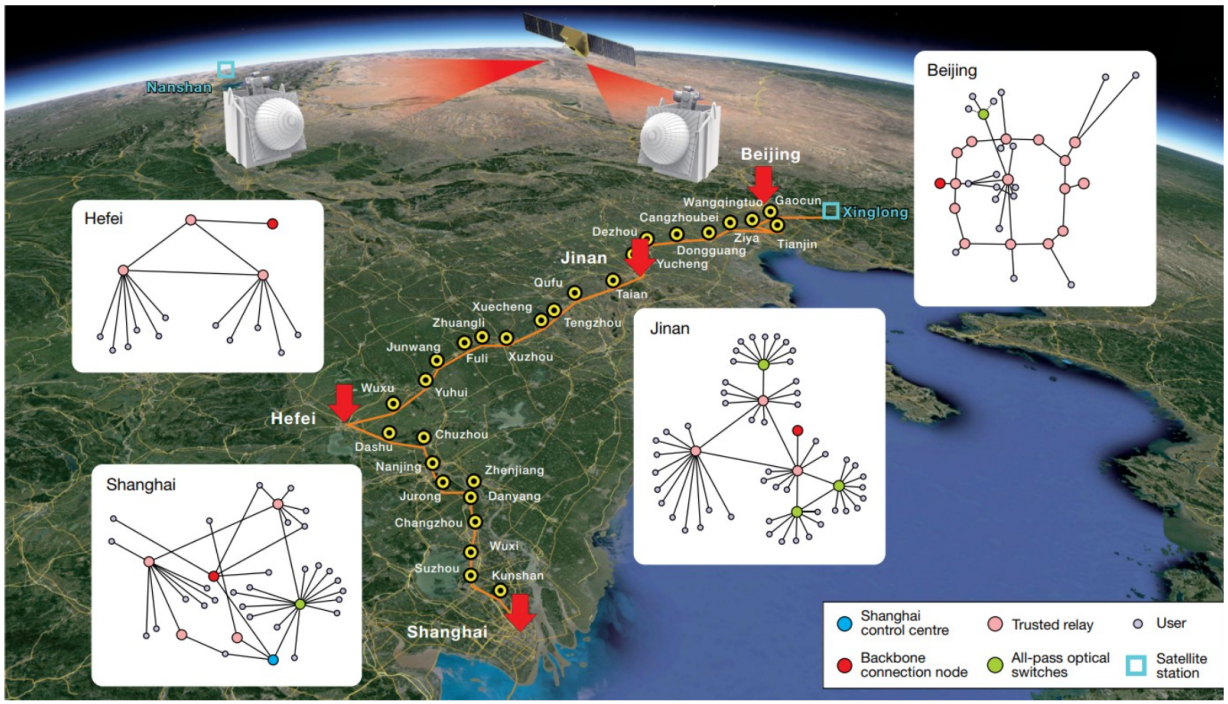
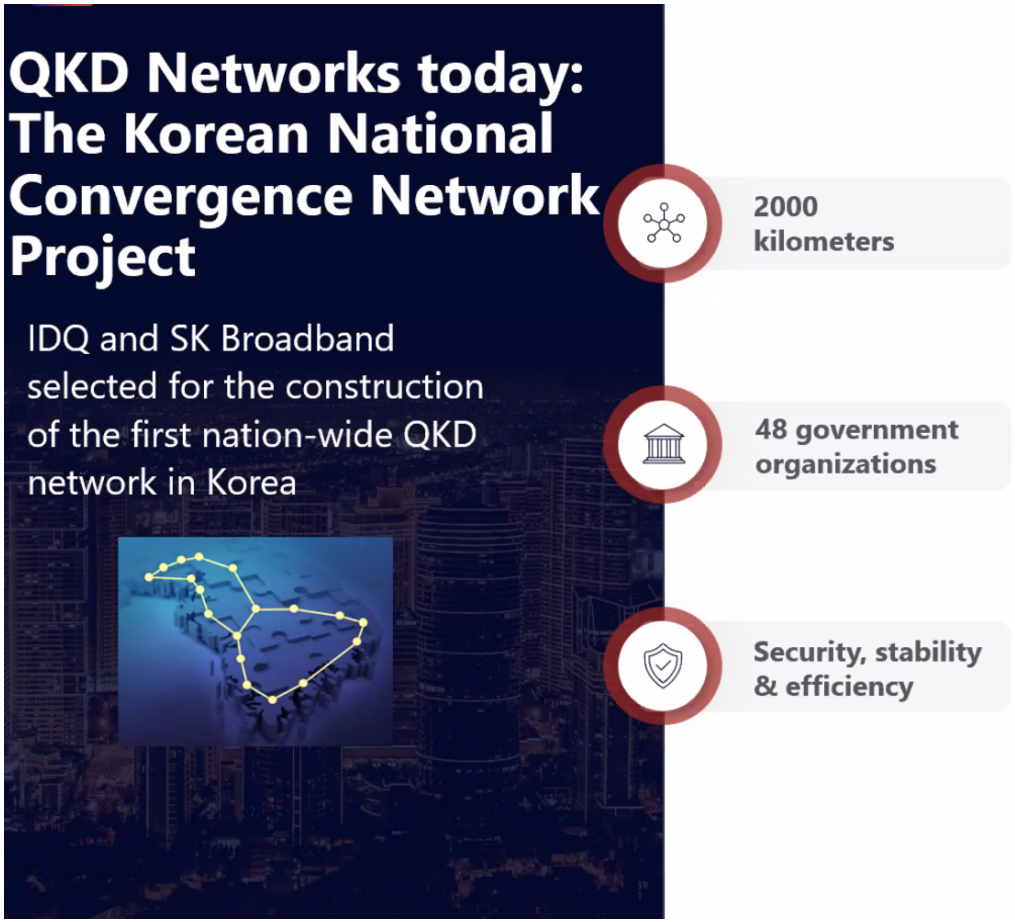
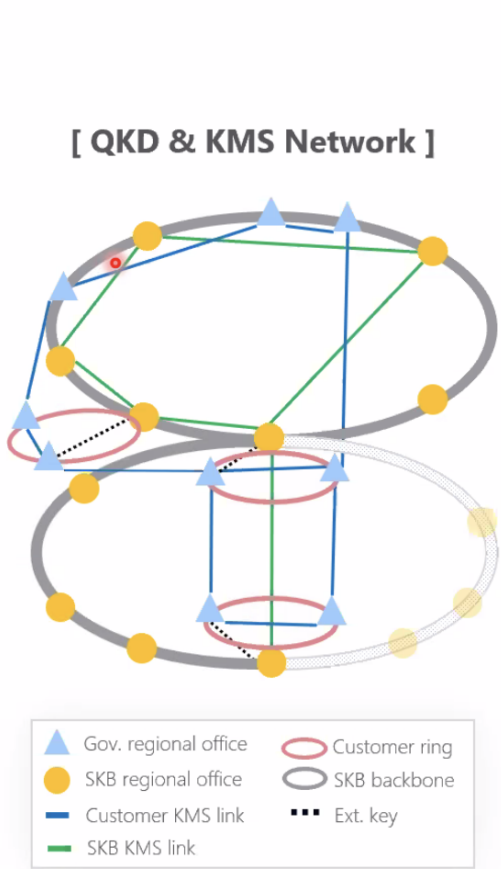


Figure 1. The network consists of four quantum metropolitan-area networks (QMANs) in Beijing, Jinan, Shanghai and Heifei, a backbone fibre link over 2,000 km (orange line) and two ground–satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. The backbone is connected by trusted relays. A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre [3].

Trusted node, integration with post-quantum solution and satellite-terrestrial link integration (QKD protocol)

En Corée du Sud





COW protocol

Réseaux quantiques 2023-2024

- **UK**

entropy
MDPI
Article
Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link
Ben Amies-King, Karolina P. Schatz, Haofan Duan, Ayan Biswas, Jack Bailey, Adrian Felvinti, Jaimes Winward, Mike Dixon, Mariella Minder, Rupesh Kumar, Sophie Albosh and Marco Lucamarini

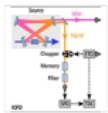
IDQ

- **Nice**

Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers
Yoann Pelet, Grégory Sauder, Mathis Cohen, Laurent Labonté, Olivier Alibart, Anthony Martin, and Sébastien Tanzilli
Phys. Rev. Applied **20**, 044006 – Published 3 October 2023

- **Barcelone**

Optica Quantum Vol. 1, Issue 2, pp. 94-102 (2023) • https://doi.org/10.1364/OPTICAQ.501848



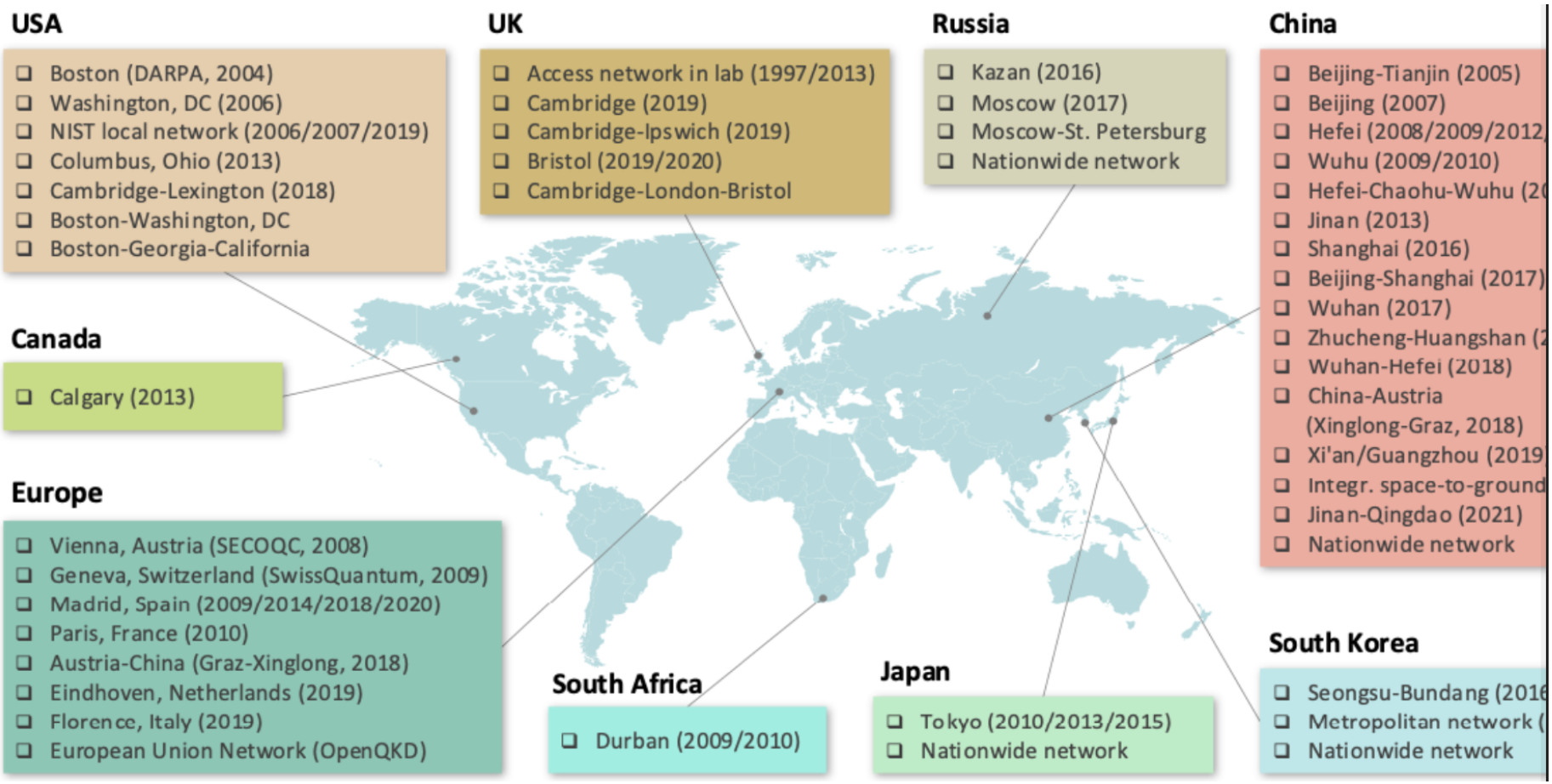
Transmission of light-matter entanglement over a metropolitan network
Jelena V. Rakonjac, Samuele Grandi, Sören Wengerowsky, Dario Lago-Rivera, Félicien Appas, and Hugues de Riedmatten
Author information • Find other works by these authors •

- **New-York**

Automated Distribution of Polarization-Entangled Photons Using Deployed New York City Fibers
Alexander N. Craddock, Anne Lazenby, Gabriel Bello Portmann, Rourke Sekelsky, Mael Flament, and Mehdi Namazi
PRX Quantum **5**, 030330 – Published 9 August 2024

- **Rio de Janeiro**

Initiatives précédentes



Sommaire

Conclusion

• Nouvelles technologies en cours de développement
• Début de réseaux quantiques (échanges de clés sécurisés) en Chine et Europe (fibre optique et satellites)
• Protocoles basés sur des "trusted nodes" : pas de mémoire quantique ni de répéteur quantique encore
• Communications quantiques signifient la connaissance de savoir si un attaquant se trouve au milieu de la ligne du bruit qu'il introduit par la mesure du système
• Dans un protocole de QKD, il y a une partie quantique (optique) et classique (post-processing).
• Les communications quantiques ne sont pas que à propos de l'échange de clés quantiques ! (digital signature, etc...)

Travaux en cours

• Hot-topics : mémoires quantiques, répéteurs quantiques (augmenter la distance sécurisé).
• Construction de nouveaux réseaux quantiques (Paris, plateau de Saclay)
• Projet européen (QSNP) ; design de nouveaux protocoles de communications quantiques, utilisation d'autres degrés de libertés, preuves de sécurités, conception de nouveau hardware (circuit intégré photonique pour la génération d'états quantique et la mesure)...

Bibliographie

- Un tutorial sur la distribution quantique de clé
https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/RobertKoenig/QKD_Tutorial.pdf
- Thèse https://www.researchgate.net/publication/251970951_On_Free_Space_Quantum_Key_Distribution_and_its_Implementation_with_a_Polarization-Entangled_Parametric_Down_Conversion_Source
- Une review
complètehttps://arxiv.org/pdf/quant-ph/0101098.pdf
- Voir chaine Youtube de Ramona Wolf pour plus de compléments

TRL : un indicateur de la maturité de la technologie