Communications sûres dans un monde quantique

Eleni Diamanti

LIP6, CNRS, Sorbonne Université

Paris Centre for Quantum Technologies

Colloque de rentrée du Collège de France

21 octobre 2022

La quête de la sécurité parfaite

Système mathématiquement indéchiffrable : le masque jetable

Sécurité parfaite si la clé est aléatoire, aussi longue que le message, et à usage unique

Les contraintes pratiques nous obligent à mettre en œuvre des versions affaiblies
→ hypothèses sur la capacité de calcul de l'adversaire

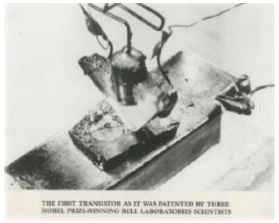
Par exemple, difficulté de factoriser des grands nombres (code RSA)

Mais ces hypothèses peuvent être invalidées par des nouvelles technologies

Peut-on s'affranchir totalement des hypothèses ?

S'appuyer sur la physique et non plus sur les mathématiques pour construire un système physiquement indéchiffrable et matériellement possible

Les révolutions quantiques



GPS

Théorie quantique de Planck — Début du 20ème siècle

Transistor — 1947

Disque dur — 1954

Laser — 1960

IRM — 1973

Comportement des électrons dans les atomes, des anomalies thermodynamiques dans les matériaux à basse température, apparition des couleurs,…

Albert Einstein (1879-1955)

Werner Heisenberg (1901-1976)

Erwin Schrödinger (1887-1961)

F. Bloch

E.M. Purcell

La première révolution quantique

Observation et manifestation macroscopique de principes quantiques

Les révolutions quantiques

“Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.”


Richard Feynman


Charles Bennett


Gilles Brassard


Artur Ekert


Serge Haroche


Alain Aspect

théorie quantique de Planck

début du 20ème siècle

fin 20ème / début 21ème

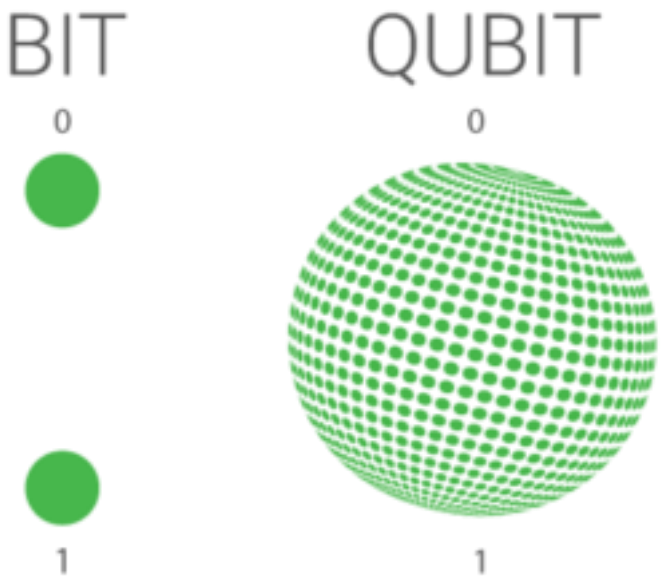
Contrôle de particules quantiques uniques
Premiers algorithmes quantiques

La deuxième révolution quantique

Manipulation active de particules quantiques uniques et interaction entre plusieurs particules pour des **applications**

La superposition

L'**information** peut être codée sur les propriétés de particules quantiques uniques
Ces particules peuvent être trouvées dans des **états de superposition**



$$\alpha|0\rangle + \beta|1\rangle$$

avec α, β nombres complexes et

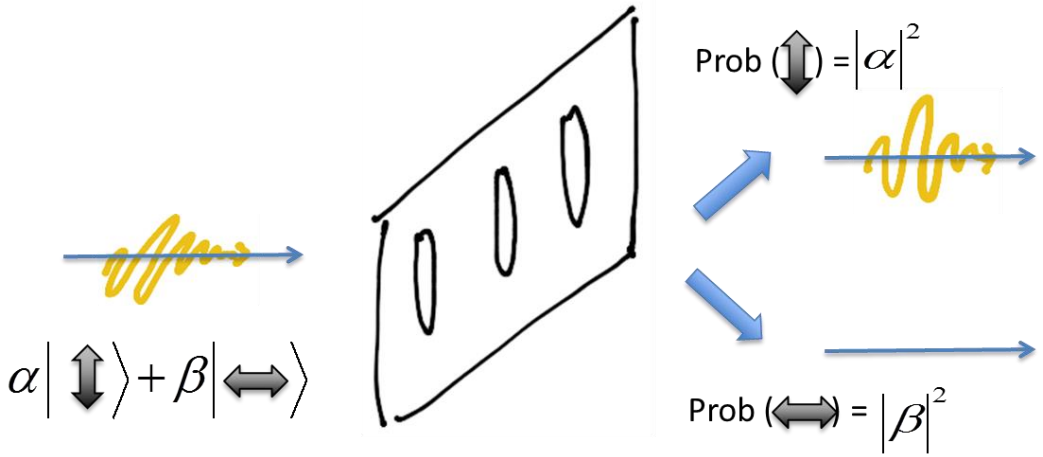
$$|\alpha|^2 + |\beta|^2 = 1$$

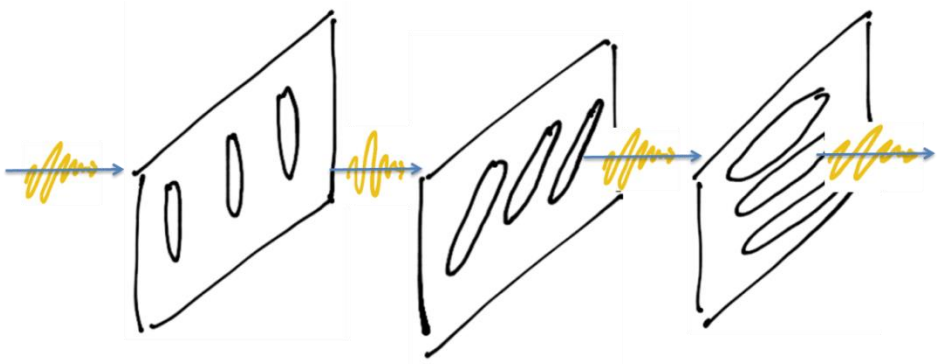
Le photon unique comme qubit

Le photon est l'aspect corpusculaire de la lumière
C'est le qubit naturel pour le transfert d'information

Théorème du non clonage
Un état quantique inconnu ne peut pas être cloné

$|\psi\rangle \rightarrow |\psi\rangle\,|\psi\rangle$ impossible



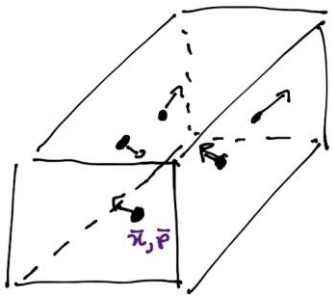


Suivant les probabilités de la mécanique quantique,
il y a une probabilité non nulle d'avoir un photon à la sortie !

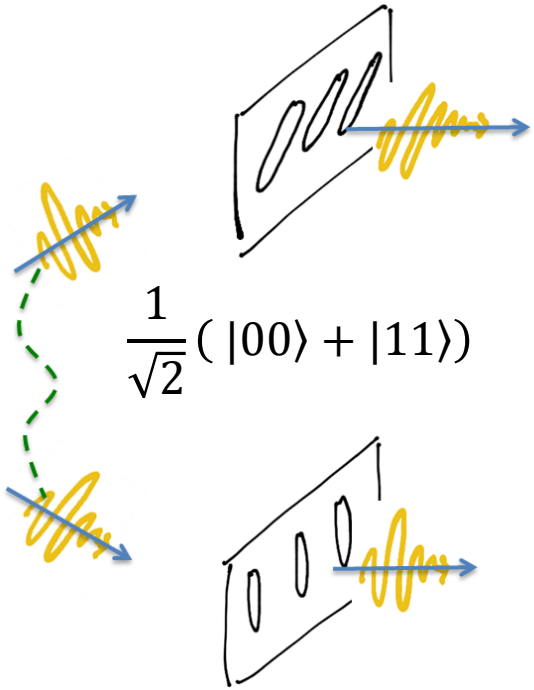
Intrication and non localité

L'information peut aussi être codée sur les propriétés de **particules intriquées**
Elles exhibent des **corrélations non locales**

En physique classique, le hasard provient de l'ignorance



Paradoxe Einstein-Podolsky-Rosen : pareil pour la mécanique quantique ?



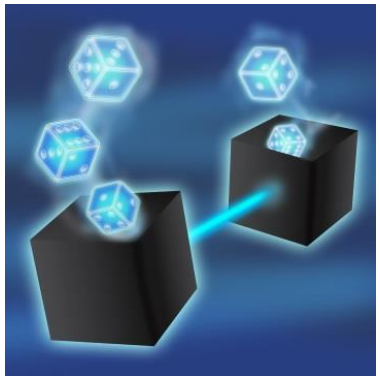
Test de l'inégalité de Bell : il n'y a pas de modèle de variables cachées locales qui explique les corrélations quantiques

Inégalité Clauser-Horne-Shimony-Holt (CHSH)

$$S = \left|E(a,b) - E(a,b') + E(a',b) + E(a',b')\right| \leq 2$$

Intrication and non localité

Les expériences d'Aspect en 1982 on confirmé les prédictions de la mécanique quantique :
l'aléa est une propriété fondamentale et la réalité est non locale



Nécessité de faire l'hypothèse d'un échantillonnage non biaisé
→ échappatoire de détection
Important dans un contexte cryptographique !

Premières expériences sans échappatoire en 2015

Les technologies quantiques

Le calcul quantique : un saut dans la puissance de calcul

“The goal in quantum computing is to choreograph things so that some paths leading to a wrong answer have positive amplitudes and others have negative amplitudes, so on the whole they cancel out and the wrong answer is not observed.” Scott Aaronson

Algorithme de Shor (1994)
Accélération exponentielle pour le problème de la factorisation

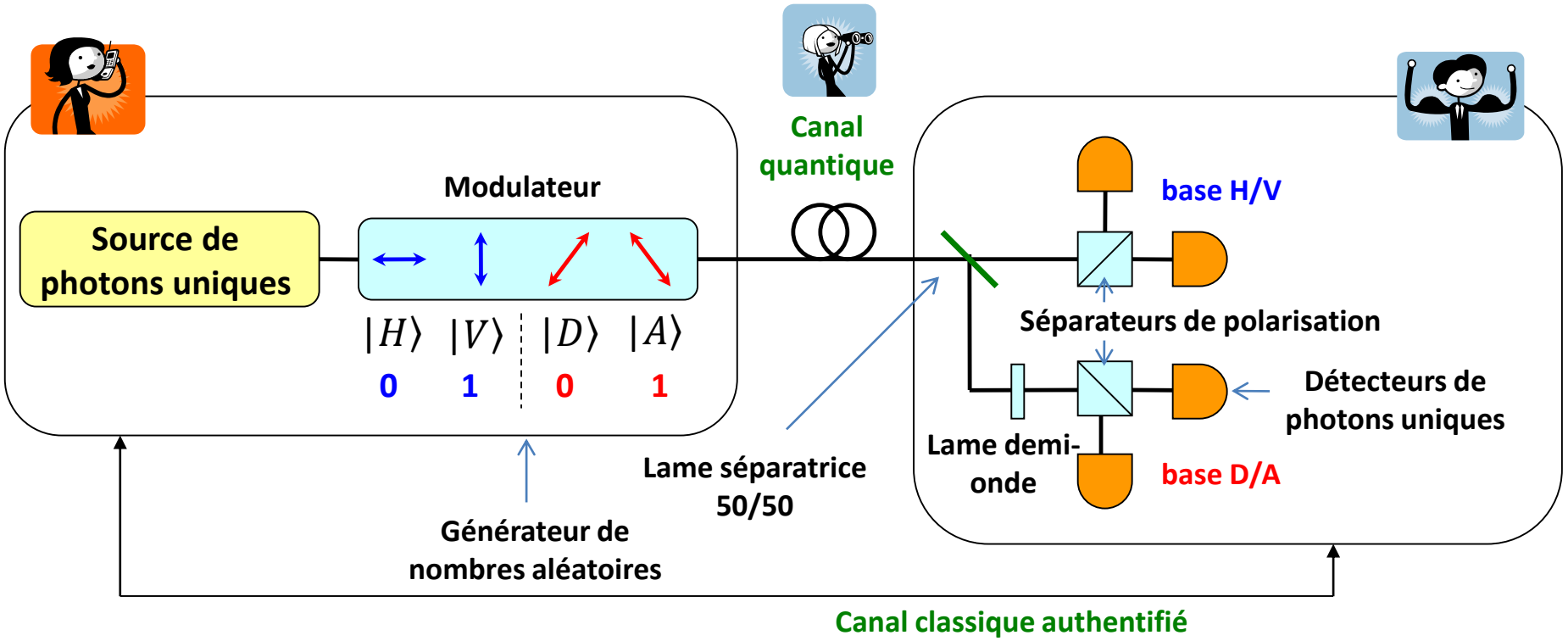
Solutions

La cryptographie post-quantique : algorithmes mathématiques considérés robustes face aux attaques quantiques

La cryptographie quantique : promesse d’une communication avec une sécurité parfaite grâce aux propriétés de la physique quantique

La distribution quantique de clés

Protocole BB84



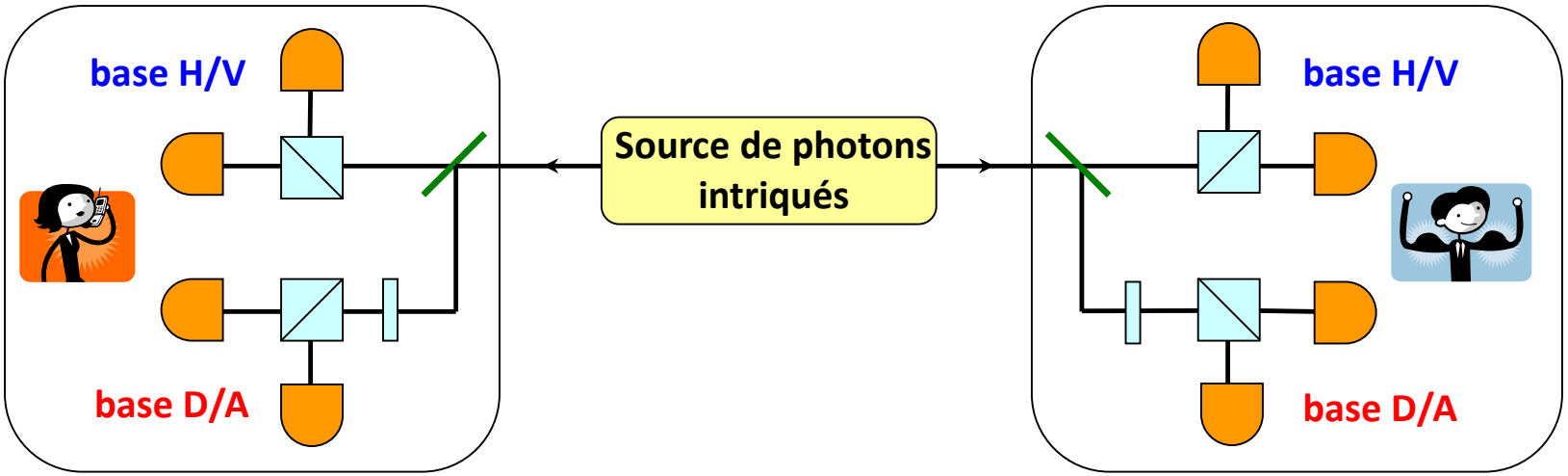
Eve ne peut pas copier les états envoyés par Alice

Elle ne peut pas observer à la fois dans les deux ensembles de direction → erreurs

Alice et Bob doivent faire confiance à leurs dispositifs

Minimiser les hypothèses

Protocoles Ekert91, BBM92



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

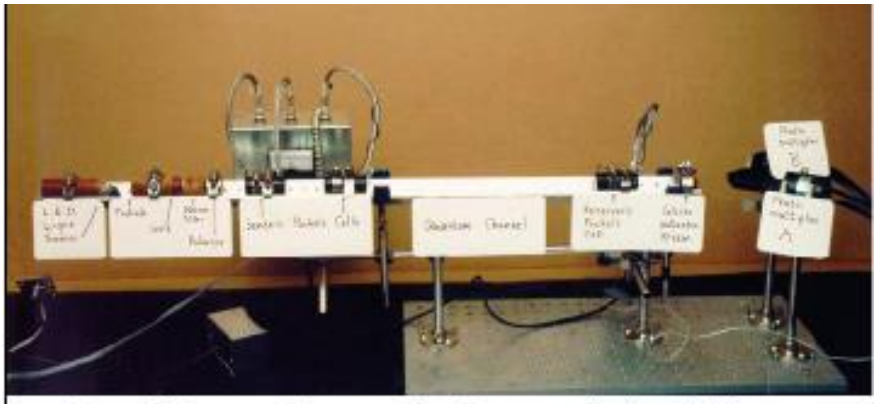
0 **1** **0** **1**

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

Une violation de l'inégalité de Bell garantit la sécurité

Hypothèses minimales sur les dispositifs : device independence

La cryptographie quantique en pratique

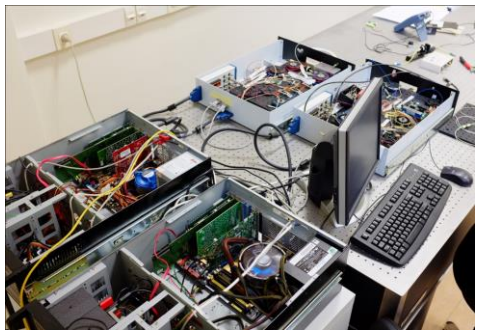


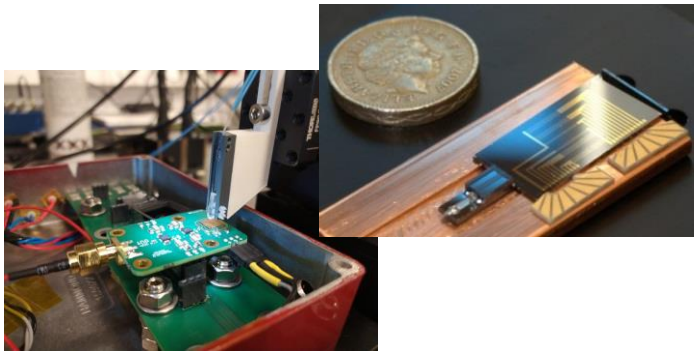
Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

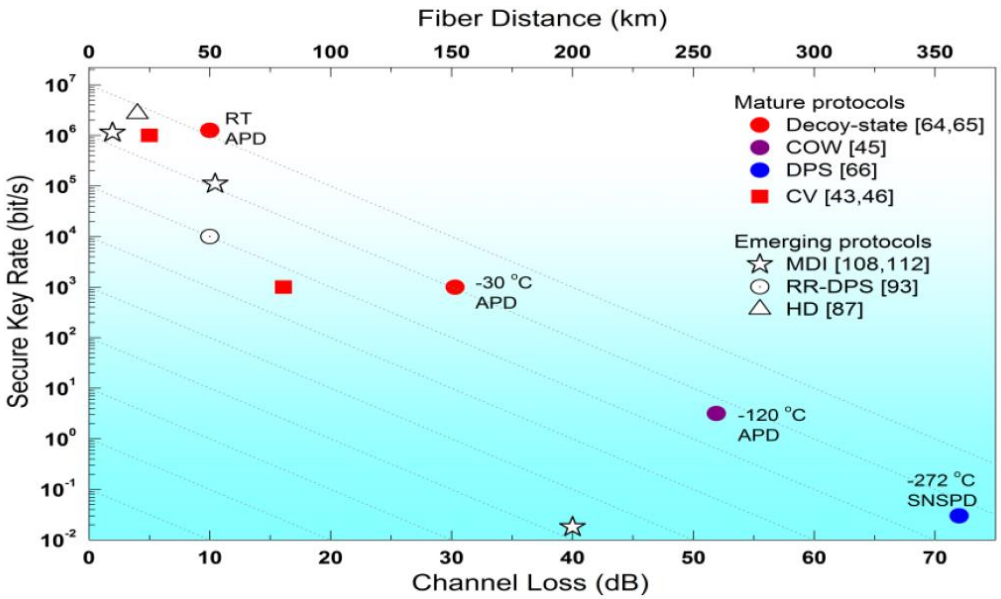
Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.







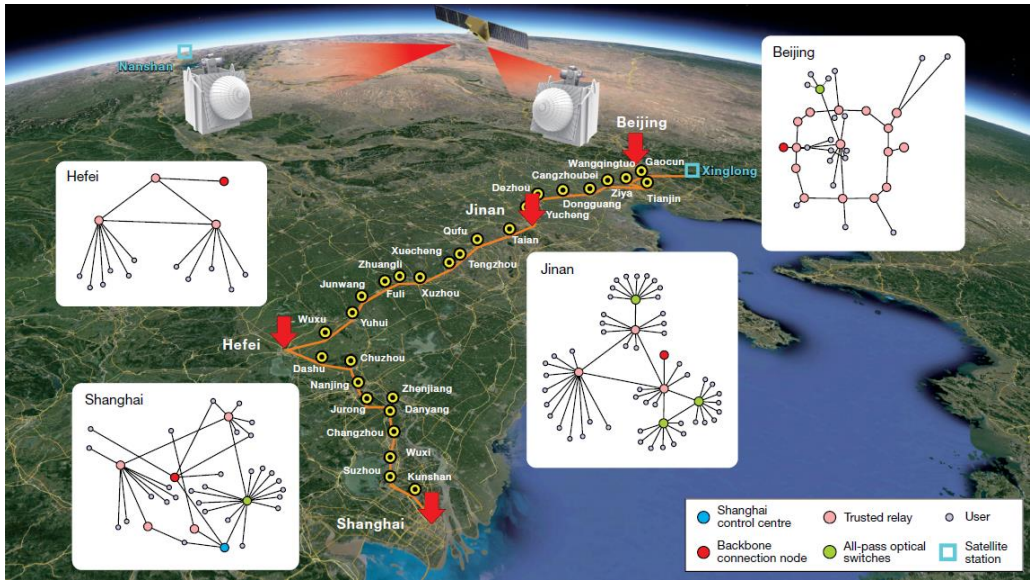
Portée maximale limitée par les pertes dans des fibres optiques

→ amplification pas possible

Réseaux de cryptographie quantique

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

Pour éviter des nœuds de confiance → répéteur quantique basé sur la téléportation quantique

Conclusion

Un système de chiffrement parfaitement indéchiffrable en pratique est sans doute une chimère

Les propriétés de la physique quantique nous permettent de minimiser les hypothèses nécessaires, s'approchant ainsi d'une sécurité parfaite

Pour une chaîne cryptographique complète (authentification, distribution de clés, chiffrement), des solutions hybrides physiques et mathématiques ont un grand intérêt pour optimiser le niveau de sécurité et les ressources