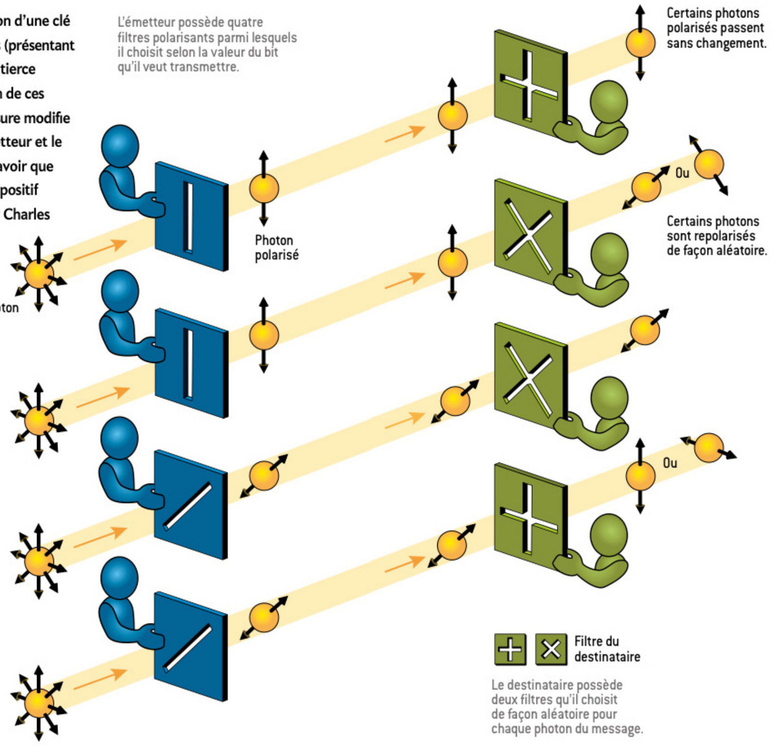
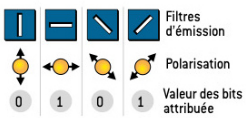
CHIFFRER SES DONNÉES GRÂCE À LA PHYSIQUE QUANTIQUE

En cryptographie quantique, la distribution d'une clé se fait grâce à un flux de photons polarisés (présentant une direction de spin particulière). Si une tierce personne tente de mesurer la polarisation de ces photons en chemin, le seul acte de la mesure modifie la polarisation de certains photons. L'émetteur et le destinataire du message pourront alors savoir que quelqu'un a tenté de lire l'échange. Le dispositif présenté ici est celui imaginé en 1984 par Charles Bennett et Gilles Brassard.



ENVOI ET RÉCEPTION DE PHOTONS POLARISÉS

L'émetteur *(en bleu)* transmet une série de photons qui passent par l'un des quatre filtres polarisants. Chaque filtre polarise le photon selon une direction, à laquelle on assigne une valeur de bit 0 ou 1 *(voir ci-dessous)*. Le destinataire *(en vert)* mesure la polarisation après le passage du photon par l'un de ses deux filtres.



DÉFINIR UNE CLÉ DE CHIFFREMENT

Le destinataire enregistre la polarisation de chaque photon reçu, puis précise publiquement quelle séquence de filtres il a utilisée. L'émetteur lui indique alors, en fonction de sa propre séquence de filtres, ceux qui n'ont *a priori* pas modifié le photon transmis. Les bits correspondants forment la clé.

1. L'émetteur polarise les photons avec ses filtres.
2. Le filtre du destinataire, choisi au hasard, transmet le photon tel quel ou le repolarise.
3. Selon les indications de l'émetteur, les bits retenus forment la clé de chiffrement.