La cryptographie quantique au Laboratoire des fibres optiques

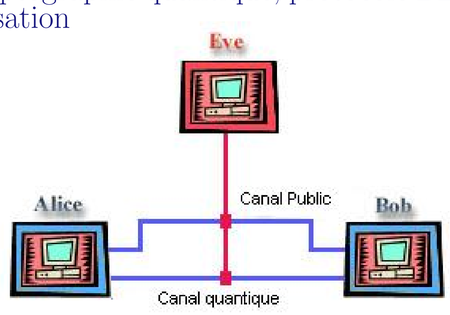
Daniel Summers-Lépine, Sylvain O'Reilly, Félix Bussières, Guido Berlin,
Nicolas Godbout, Suzanne Lacroix

Laboratoire des fibres optiques, École polytechnique de Montréal,
Centre d'optique, photonique et laser
Département de génie physique, CP 6079 succ. Centre Ville, Montréal (Québec),
H3C-3A7, Canada

Sommaire

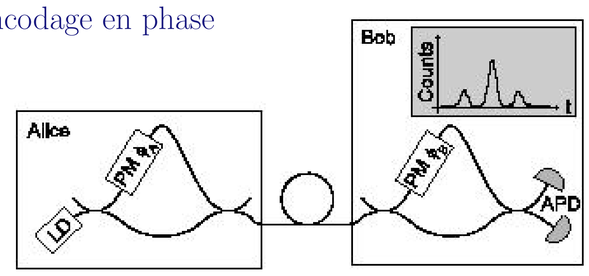
Le Laboratoire des fibres optiques travaille actuellement sur divers dispositifs pour la cryptographie quantique (CQ). On a démontré la possibilité d'utiliser le multiplexage en longueur d'onde dans le but d'élaborer un réseau optique permettant à n'importe quelle paire de participants de communiquer de façon parfaitement confidentielle. On travaille aussi sur la génération de photons intriqués et sur la stabilité d'interféromètres.

Cryptographie quantique, protocole BB84, encodage en polarisation



- Alice et Bob échangent des photons par un canal quantique
- Alice choisit la polarisation de chaque photon de façon aléatoire entre $\{|\uparrow>, |\rightarrow>\}$ et $\{|\nearrow>, |\nwarrow>\}$
- Bob mésure chaque photon sur une des deux bases, qu'il choisit aléatoirement
- Alice et Bob annoncent leurs bases sur le canal public (mais pas les résultats!!)
- Lorsque leurs bases coïncident ils ont un bit de la clé
- L'espion Eve ne peut pas agir dans le canal quantique sans rendre sa présence évidente

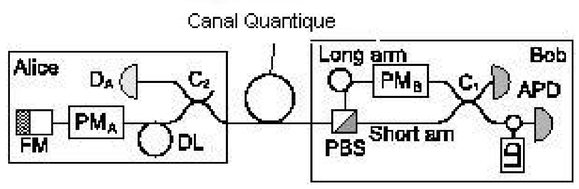
Encodage en phase



- Alice et Bob appliquent un décalage de phase choisi aléatoirement.
- Si $\Delta\phi = \pi$ ou 0 le photon va vers l'un ou l'autre détecteur.
- Si $\Delta\phi = \frac{\pi}{2}$ ou $\frac{3\pi}{2}$ alors la détection est équiprobable dans les deux détecteurs.
- Bob annonce le décalage de phase qu'il a appliqué
- Alice et Bob peuvent obtenir une clé cryptographique.
- Difficile à mantenir stable sur de longues distances

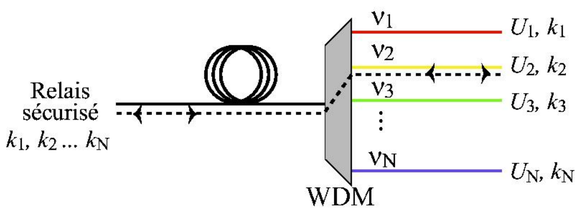
Encodage en phase

- Version auto-compensée: système Plug and Play

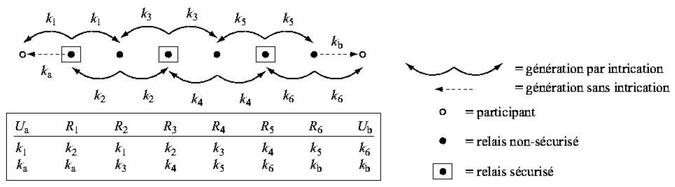


Montage Plug and Play

CQ à plusieurs usagers par multiplexage en longueur d'onde



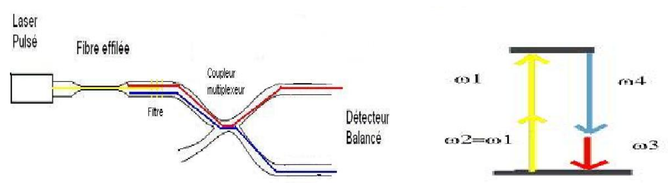
- Le multiplexage en longueur d'onde nous permet de créer un réseau en étoile.
- Un grand nombre d'utilisateurs peuvent communiquer avec une confidentialité absolue.
- Une source de photons intriqués permet de s'affranchir de la contrainte du relais sécurisé dans un réseau local.



U_a	R_1	R_2	R_3	R_4	R_5	R_6	U_b
k_1	k_2	k_1	k_2	k_3	k_4	k_5	k_6
k_a	k_a	k_3	k_4	k_5	k_6	k_b	k_b

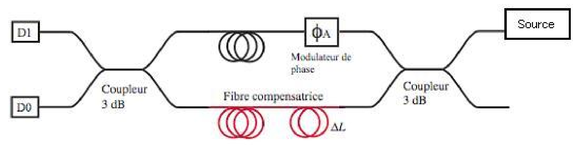
- Pour un réseau global où deux participants sont séparés par N relais, le nombre de relais sécurisés peut être reduit à $N/2$.

Source de photons intriqués accordable tout-fibre.



- Mélange à 4 ondes dans une fibre de silice
- On utilise une fibre effilée (taper) adiabatique et filtres tout-fibre.
- La pompe est pulsée pour éviter des effets non désirés (effets Brillouin) et pour avoir une haute puissance.
- On fait une mesure différentielle du bruit. Si les photons sont intriqués, le bruit doit tomber au dessous du bruit de grenaille (shot noise).

Interféromètre très stable pour encodage en phase.



- Des interféromètres très stables peuvent être utilisés pour se libérer des contraintes du montage Plug and Play, qui n'est pas inconditionnellement sécuritaire.
- On fait une compensation passive des fluctuations de température. On utilise des fibres ayant des proprietés thermo-optiques différentes pour les deux branches de l'interféromètre.
- On a $\Delta\phi = k\left[n\Delta L + (\frac{\partial n}{\partial T}\,|_1\, L_1 - \frac{\partial n}{\partial T}\,|_2\, L_2)\Delta T\right]$. Ainsi, si $\frac{L_1}{L_2} = \frac{\frac{\partial n}{\partial T}|_2}{\frac{\partial n}{\partial T}|_1}$ la dépendence en température est parfaitament compensée.
- Il est possible d'envisager une réduction de deux ordres de grandeur dans la sensibilité thermique de l'interféromètre.
- On peut l'utiliser pour encodage en phase et pour CQ avec photons intriqués.