Établissement de clé quantique BB84

Établissement de la clé

- Via un canal de communication classique publique
  - Bob envoie la chaine b'
  - Alice réponds les i tels que $b_i = b'_i$
- Le secret partagé est l'ensemble des $a_i = a'_i$ pour les i tels que $b_i = b'_i$
- Environ $n/2$ bits de clé sont produits, on peut répéter le protocole au besoin

Établissement de clé quantique BB84

Interception sur le canal quantique

- Chaque qubit envoyé est l'un de $|0\rangle, |+\rangle, |1\rangle, |-\rangle$
- Impossible d'obtenir de l'information sur des états non-orthogonaux sans perturbation
  - No-cloning theorem
- Pour les distinguer Eve doit deviner b'_i, mesurer a'_i et reconstruire $|\Psi_{a'_i b'_i}\rangle$ pour envoyer à Bob
  - Ce qubit n'est correct que lorsqu'elle devine b_i correctement

Tentative d'espionnage $\Longrightarrow$ perturbation