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

Établissement de clé quantique BB84

Détection de perturbation

- Alice et Bob peuvent sacrifier une partie de leurs bits de clé
- Alice choisi un sous-ensemble aléatoire des bons i, et révèle les a_i correspondants
  - Bob réponds OK si $a_i = a'_i$ pour tous les i révélés,
  - Bob réponds ESPION sinon (on abandonne et recommence)