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)

Établissement de clé quantique BB84

Interception sur le canal classique

- Passive
  - La chaine b ne nous apprend rien sur a
  - Les a_i sacrifiés ne nous apprennent rien sur les a_i gardés
- Active
  - Requiert un canal authentifié