Protocole BB84

Structure de la présentation

- Établissement de clé?
- Classique
  - Mise en contexte (historique) et état des lieux (en 2024)
  - RSA et Diffie-Hellman
- Quantique
  - Fonctionnement du protocole
  - Détection d’espionnage sur le canal quantique

Établissement de clé

Définition du problème

- Demande à Alice et Bob d'établir une clé secrète partagée via un canal publique
  - Sans échange / connaissance préalables
  - Sans qu'Eve (qui espionne) ne puisse découvrir le secret
- Applications
  - Chiffrement à clé privée
  - Codes d'authentification de message