Établissement de clé classique

État des lieux

- TLS 1.3 publié en 2018 (RFC 8446)
  - Utilisé par les navigateurs et serveurs web partout dans le monde
- L’une des premières étapes du protocole est un établissement de clé
- Les seules méthodes autorisées sont celles basées sur RSA ou DH

Établissement de clé quantique

Protocole BB84