Établissement de clé quantique BB84

Table des observations

- Pour chaque i, on a
  - $b_i = b'_i$, et donc $a_i = a'_i$
  - $b_i \neq b'_i$ et donc a'_i aléatoire

a_i	b_i	b_i'	a_i'
0	0	0	0
0	0	1	?
0	1	0	?
0	1	1	0
1	0	0	1
1	0	1	?
1	1	0	?
1	1	1	1

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