Établissement de clé quantique BB84

Exemple

a	0	1	0	0	0	0	1	1	0	1
b	1	0	0	0	0	1	0	0	0	1
$\|\Psi\rangle$	+	1	0	0	0	+	1	1	0	-
b'	1	1	0	1	0	0	0	1	1	1
a'	0	_	0	_	0	_	1	_	_	1

Conclusion

- Problème d'établissement de clé est important en cryptographie
- Les solutions actuelles sont
  - Imparfaites classiquement
  - Brisées quantiquement
- BB84 offre une solution quantique au problème
  - Sous la prémisse qu'on dispose d'un canal classique authentifié
  - Peut-on s'en défaire ou l'obtenir sans échange de clé préalable?
- Partage de $|\Phi^+\rangle$?