

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 $|\Phi^+\rangle$?

Merci