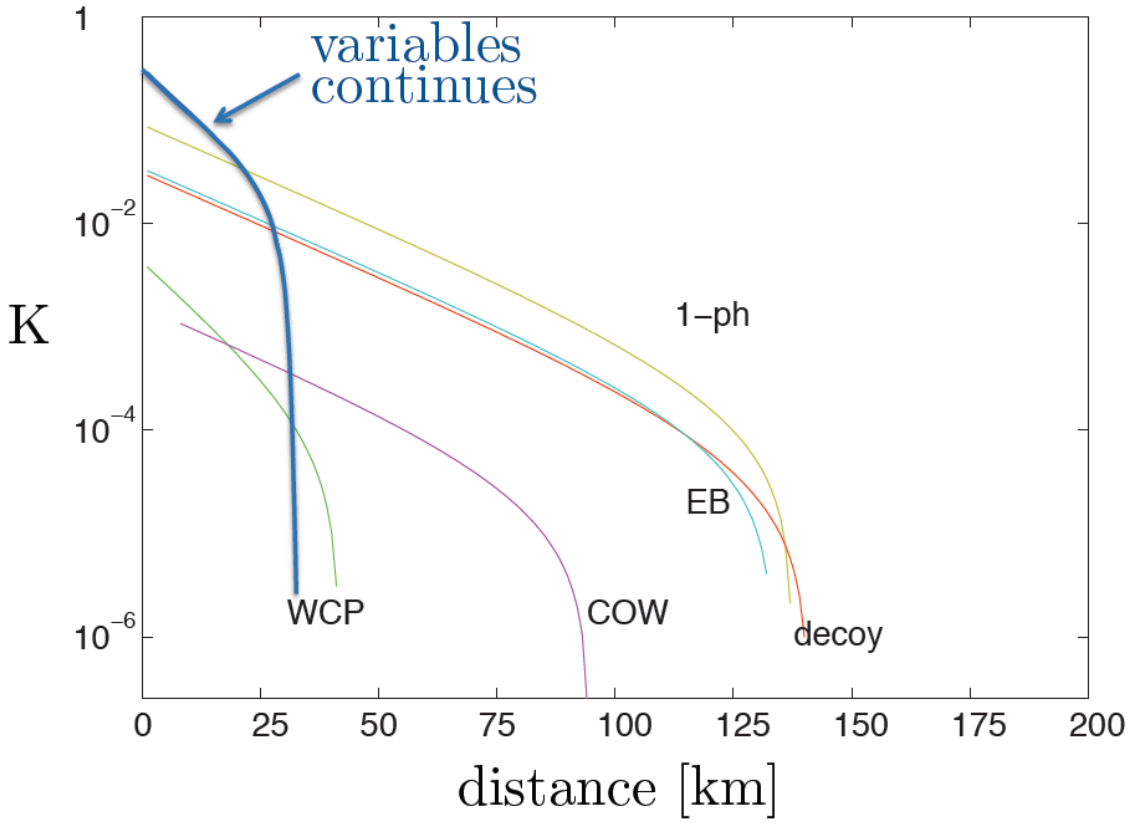
Distribution quantique de clés : Variables continues ou variables discrètes ?



V. Scarani et al, Rev. Mod. Phys. **81**, 1301 (2009)

Distribution quantique de clés : Variables continues ou variables discrètes ?

	Var. discrètes	Var. continues
Support de l'information	polarisation de photons uniques	quadratures d'états cohérents
Détection	comptage de photons	détection homodyne → interférométrie
Performances	longues distances (100-200 km)	Taux important ... à courtes distances (30 km)
Principale limitation	technologique (détecteurs)	algorithmique (réconciliation)

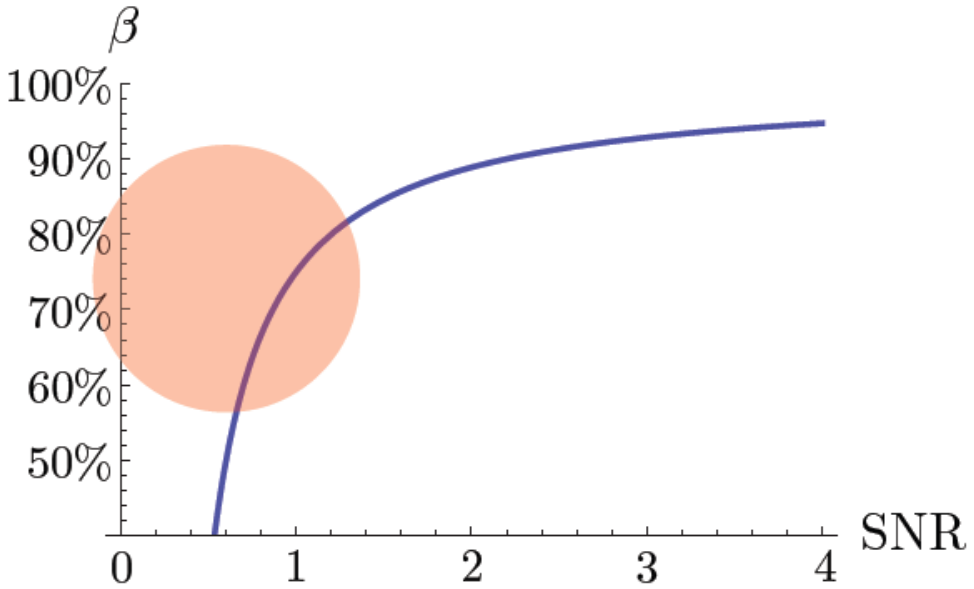
Taux secret : Le problème de la réconciliation

Taux secret : $K = \beta\, I(A;B) - I(B;E)$

β : efficacité de réconciliation

mauvaise à faible SNR pour les protocoles à modulation gaussienne

→ portée limitée à 50 km



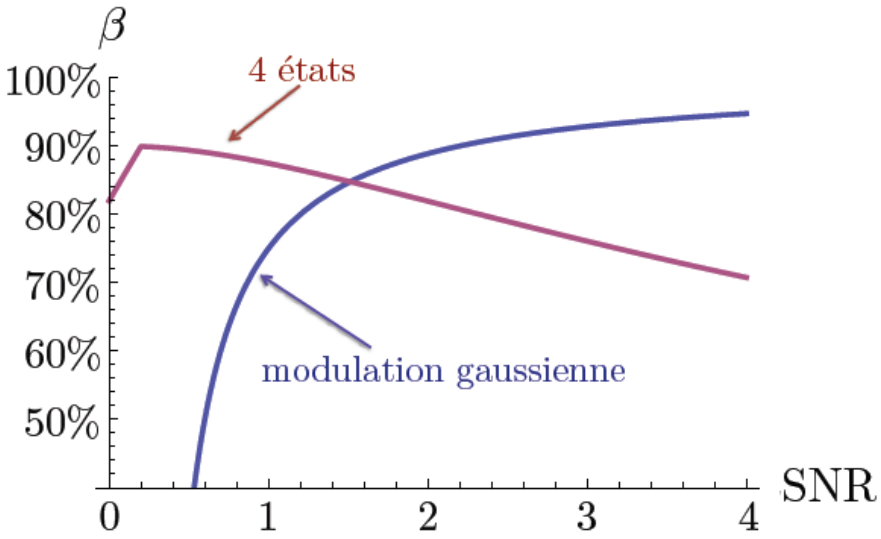
A. Leverrier, et al, Phys. Rev. A **77**, 042325 (2008)

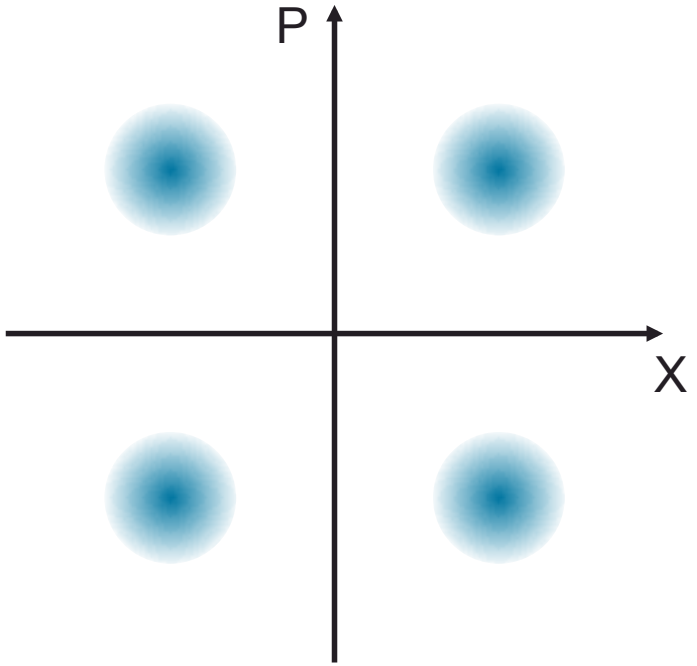
Un nouveau protocole qui résout le problème de la réconciliation

Modulation discrète chez Alice

Bob mesure l'une ou l'autre des quadratures

$$K = \beta\, I(A;B) - I(B;E)$$



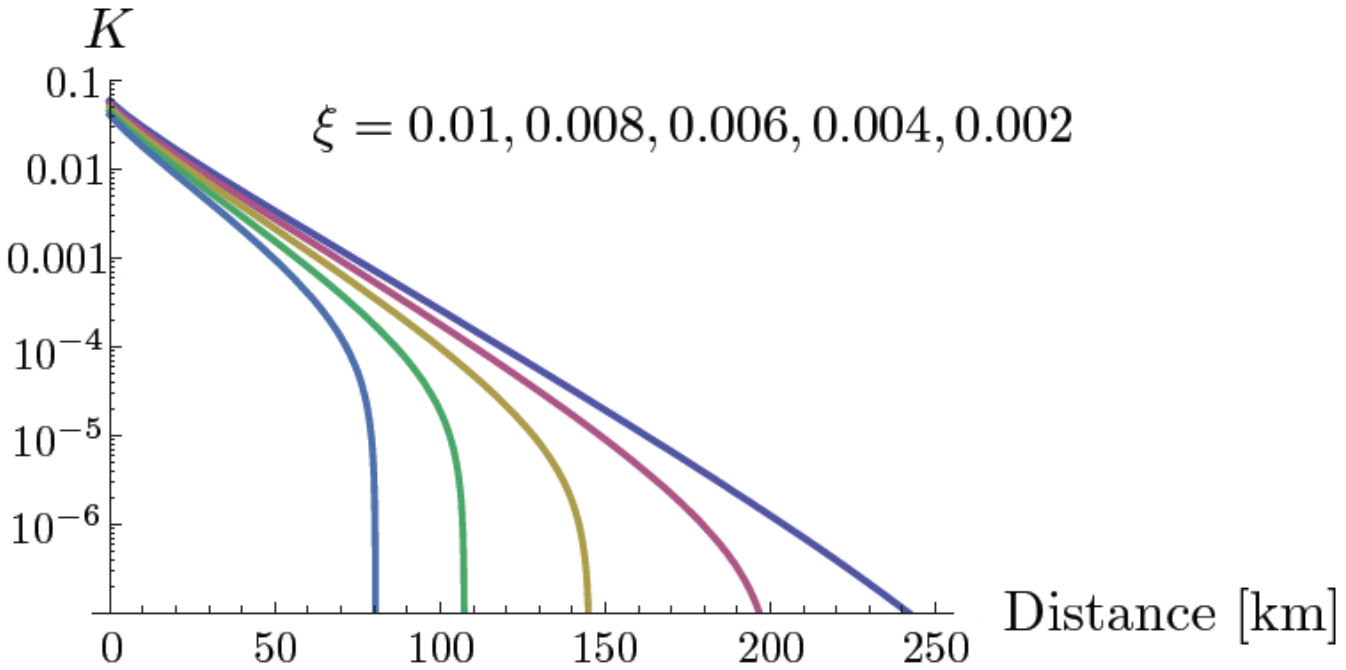


Codes correcteurs d'erreurs (LDPC) à bas rendement

β > 80% pour SNR → 0

Performances du protocole 4-états

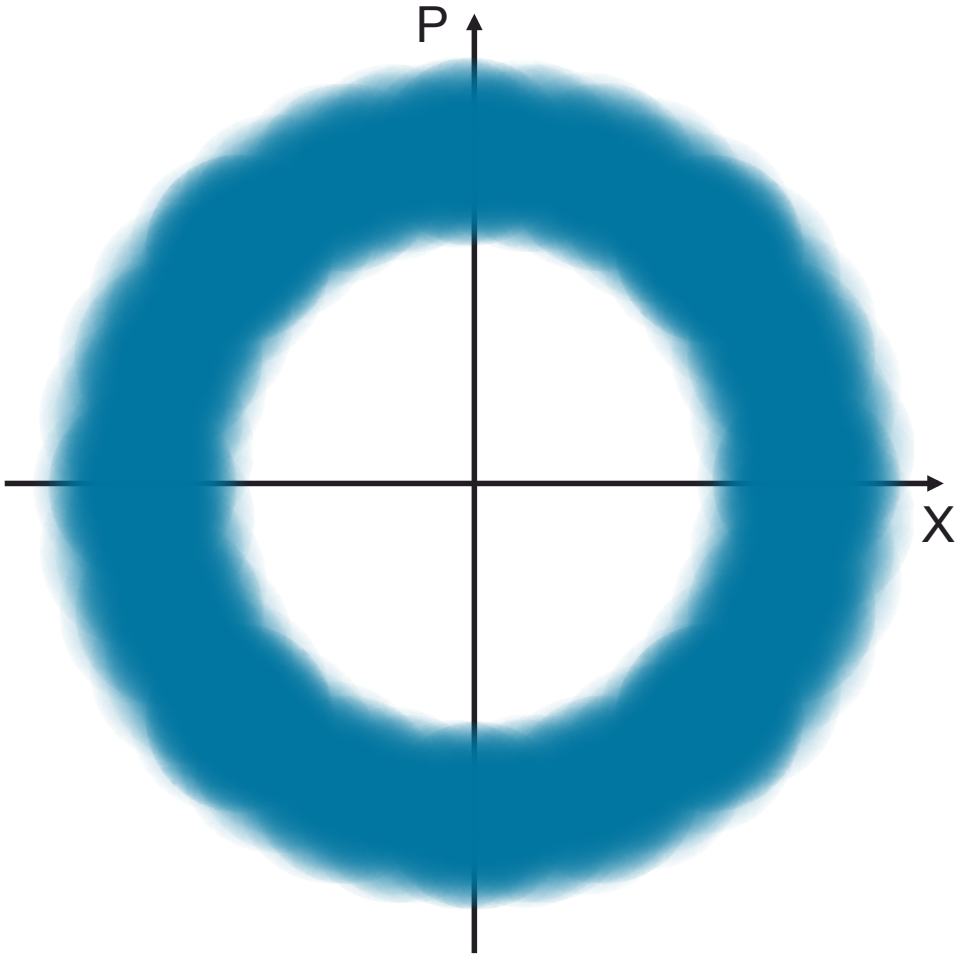
Preuves de sécurité : borner I(B;E)



A. L. & P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009)
A. L. & P. Grangier, New J. Phys (2010)

- Longues distances possibles en pratique → **brevet déposé**
- Mais résultats plus contrastés à cause des effets de taille finie
- Peut-on faire mieux ?

Protocole optimal ?
une modulation à nouveau continue



Combine :

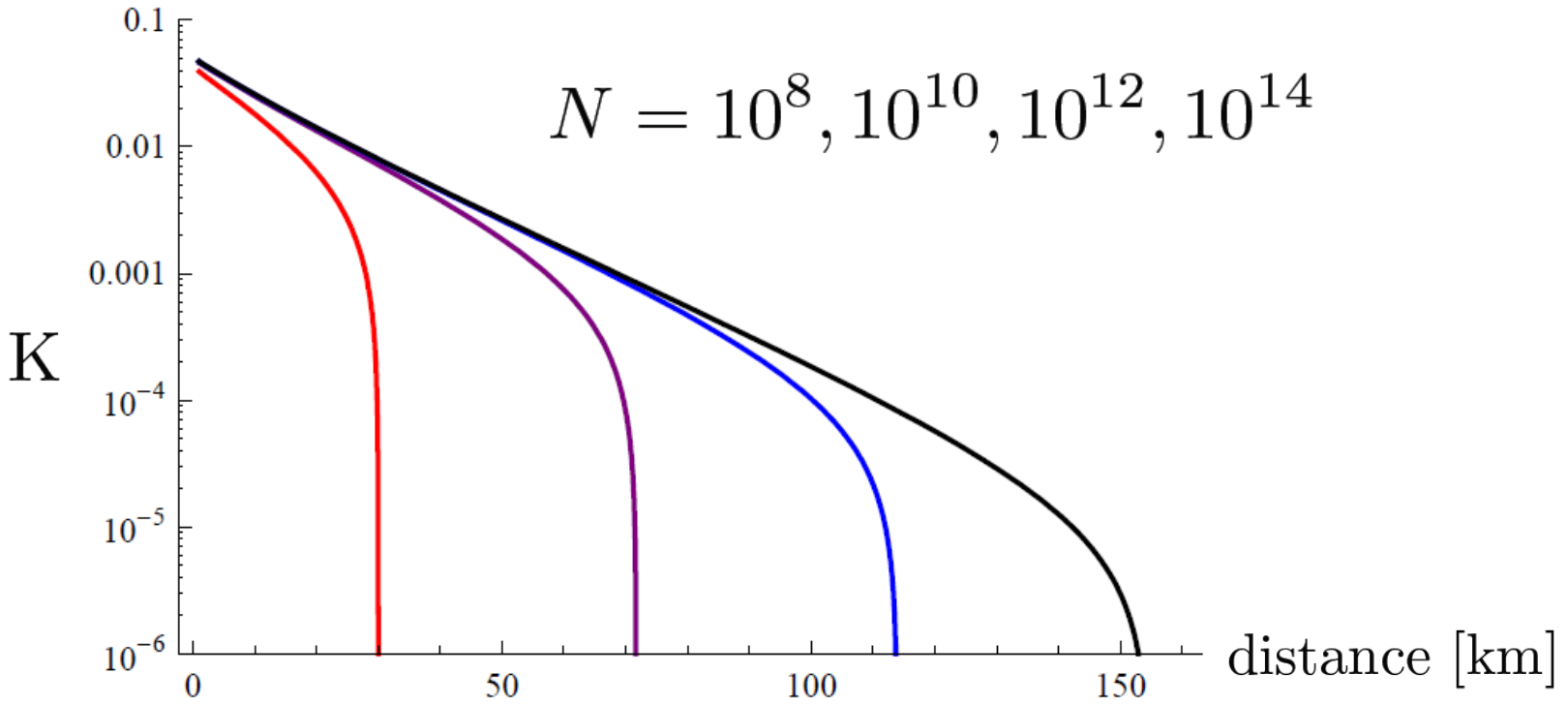
- une modulation continue … à 8 dimensions

- une détection hétérodyne

→ même efficacité de réconciliation

→ minimise les effets de taille finie
A.L., F. Grosshans, P. Grangier,
Phys. Rev. A 2010

Protocole 8-dimensions : Performances (avec effets de taille finie)



A. L. & P. Grangier, arXiv:1005.0328

- Les variables continues sont bien adaptées pour la distribution quantique de clés, même à longue distance
- Moins représentées aujourd'hui que BB84 car plus récentes
- Quid dans 5 – 10 ans ?