

Différentes classes d'attaque d'Eve envisageables

Attaques individuelles:

interaction **indiv** et mesure
indiv Eve

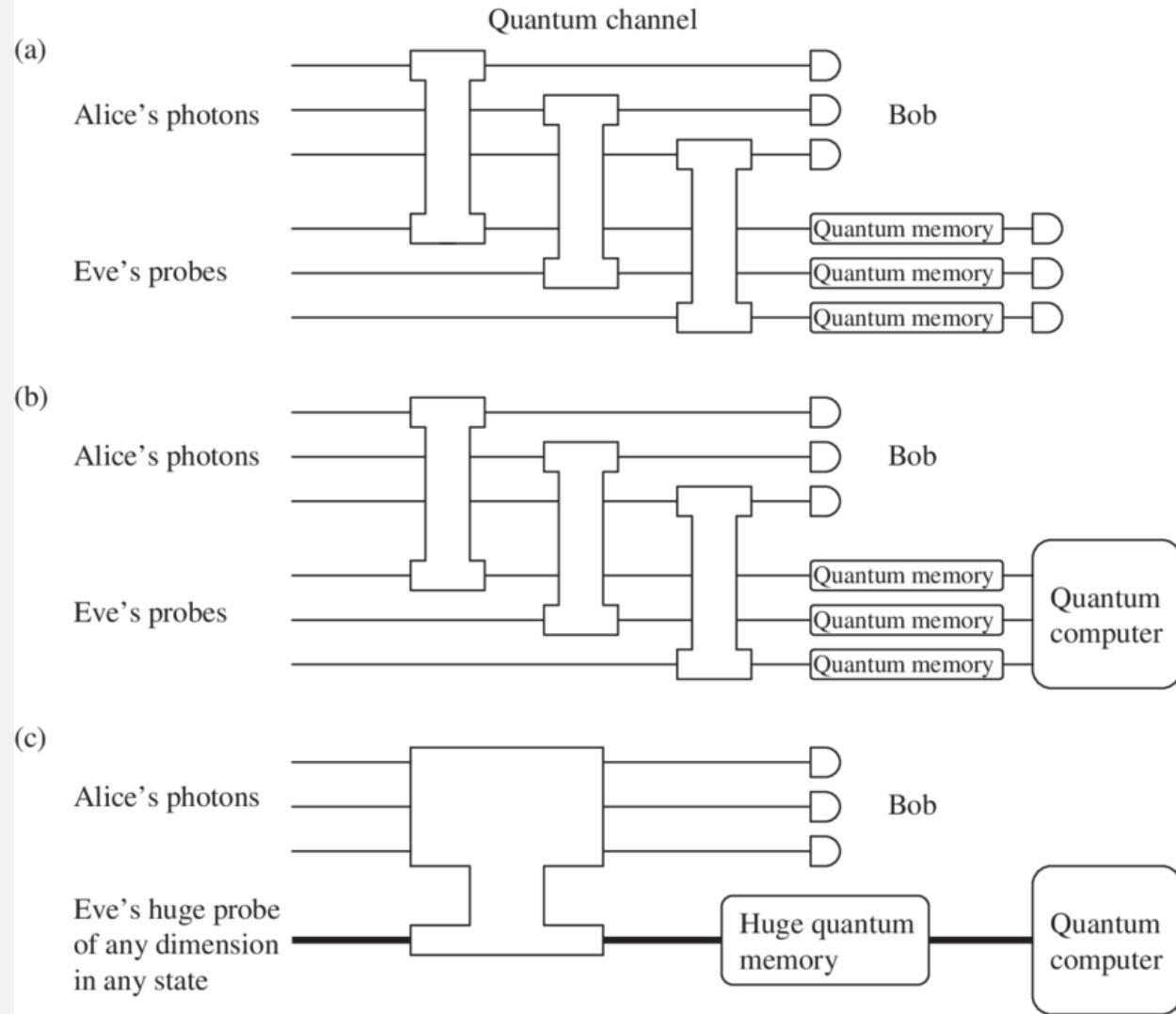
..

Attaques collectives :

interaction **indiv** et mesure
jointe Eve

Attaques cohérentes:

interaction et mesure
arbitraires Eve



Security proofs are known for the early QKD protocols, but remain an active domain of research