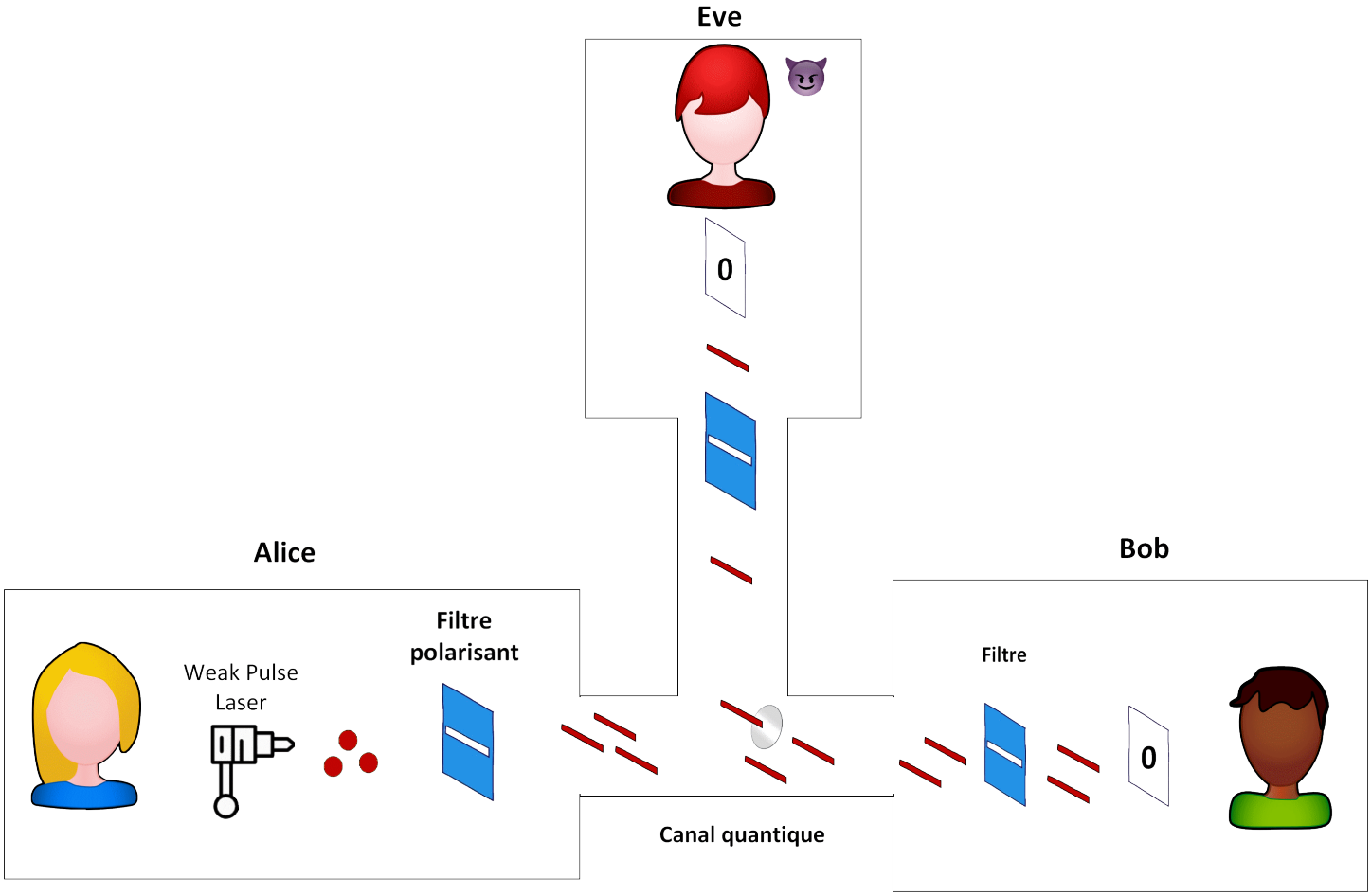
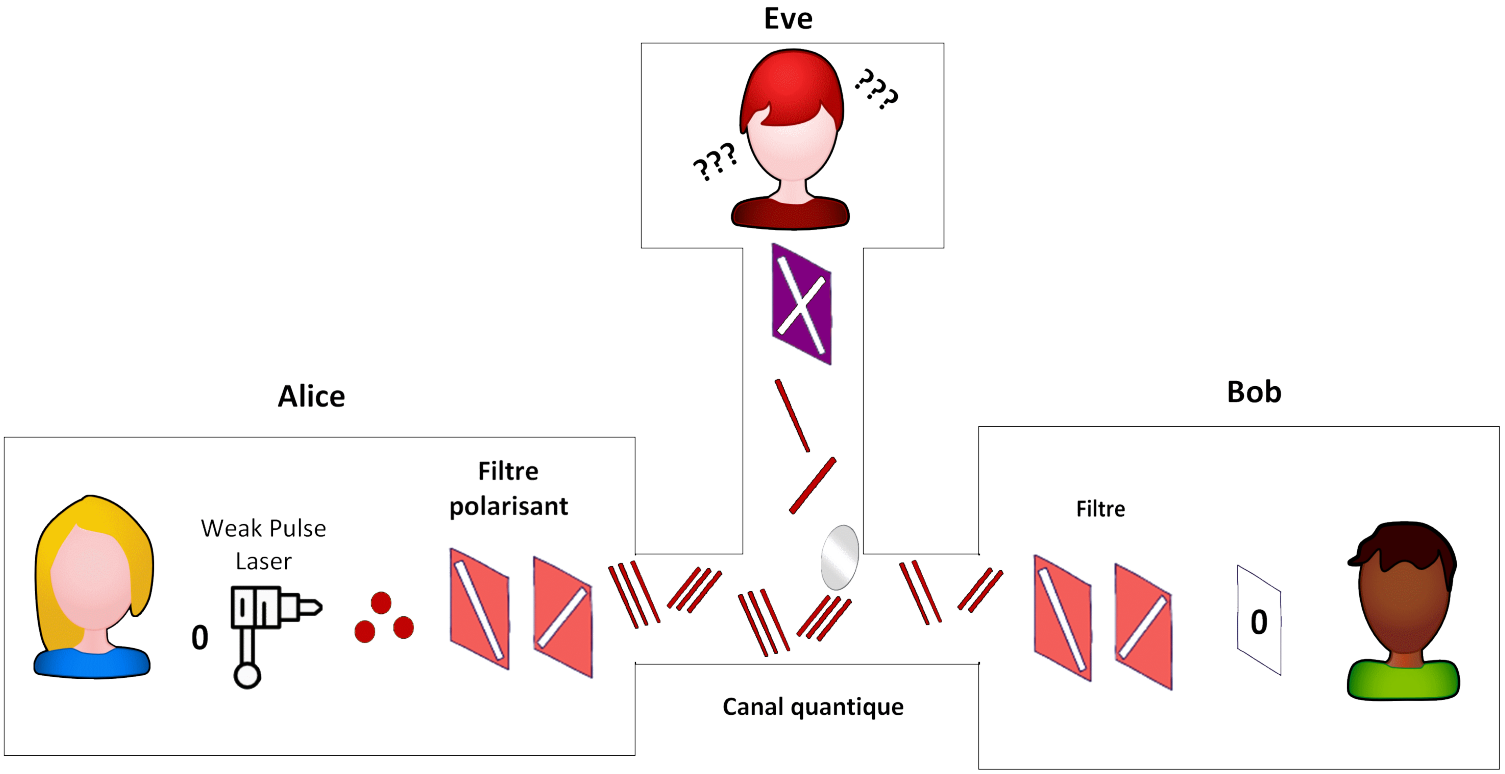
Annexe 4 – Le protocole SARG04

Il a été développé en 2004 comme son nom l'indique, et il a été créé pour contrer une attaque qui peut potentiellement être réalisée sur certains réseaux quantiques.

Dans certains cas, on ne peut pas envoyer des photons en entier, alors on utilise des lasers à faible intensité. Le souci avec des lasers, c'est qu'ils vont envoyer des bouts de photons, mais parfois en plusieurs exemplaires. Normalement, un photon ne peut pas être cloné, ça évite qu'Eve puisse copier un photon envoyé par Alice. Mais avec les lasers, Eve a juste à récupérer un exemplaire d'un morceau de photon qui transite dans le réseau, et à laisser passer les autres morceaux pour que Bob ne s'aperçoive de rien. C'est ce qu'on appelle le Photon Number Splitting Attack.



SARG04 va donc permettre d'utiliser plusieurs filtres polarisants, mais un de ces filtres est un leurre. Sur un autre canal de communication, Alice va dire à Bob quel filtre était le bon à utiliser, pour chaque qubit, et Bob pourra jeter tous les qubits reçus avec le mauvais filtre. Eve pourra toujours capturer des bouts de photons, mais elle n'aura pas connaissance du vrai filtre à mettre en place pour chacun d'eux.



Ce protocole pourra servir dans le futur mais il est arrivé un peu tôt par rapport aux capacités actuels des réseaux quantiques, parce qu'il faudrait qu'Eve possède un ordinateur quantique parmi les plus surpuissants d'aujourd'hui pour mettre en place cette captation de morceaux de photons.