Annexe 2 – Le protocole BB84

Voici le fonctionnement vulgarisé du protocole BB84. C'est un système de chiffrement symétrique, donc les deux hôtes auront la même clé. Celle-ci sera en binaire pur et simple, mais les 0 et 1 ne circulent pas à travers des bits mais des qubits, qui peuvent normalement supporter plus que 2 valeurs, mais qui sont spécifiquement réglé pour ce protocole là pour n'en coder que deux. Et ces qubits sont en fait des atomes de lumière, donc des photons, qui vont passer à travers des algorithmes.

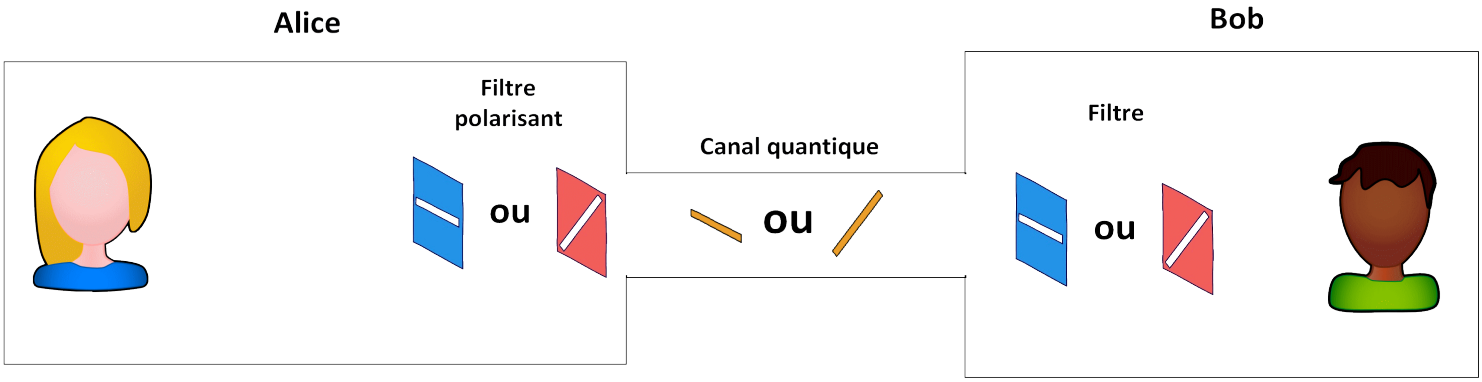
Dans un premier temps, Alice va envoyer, à travers un canal quantique, une suite de qubits sous forme de photon. Elle leur applique ensuite aléatoirement un filtre de polarisation, qu'on appelle aussi une « base », parmi 4 filtres possibles. Ces filtres sont simplement des équations qu'on applique aux photons et qui vont permettre de les transformer. On appelle cette transformation la polarisation, et ça modifie en quelque sorte la forme du photon.

Alice va donc polariser un photon dans un sens donné : Si la valeur du qubit est 0, il sera polarisé dans une base horizontale ou dévié de 45° 

; Si c'est un 1, il sera polarisé dans une base verticale ou dévié de -45° : 

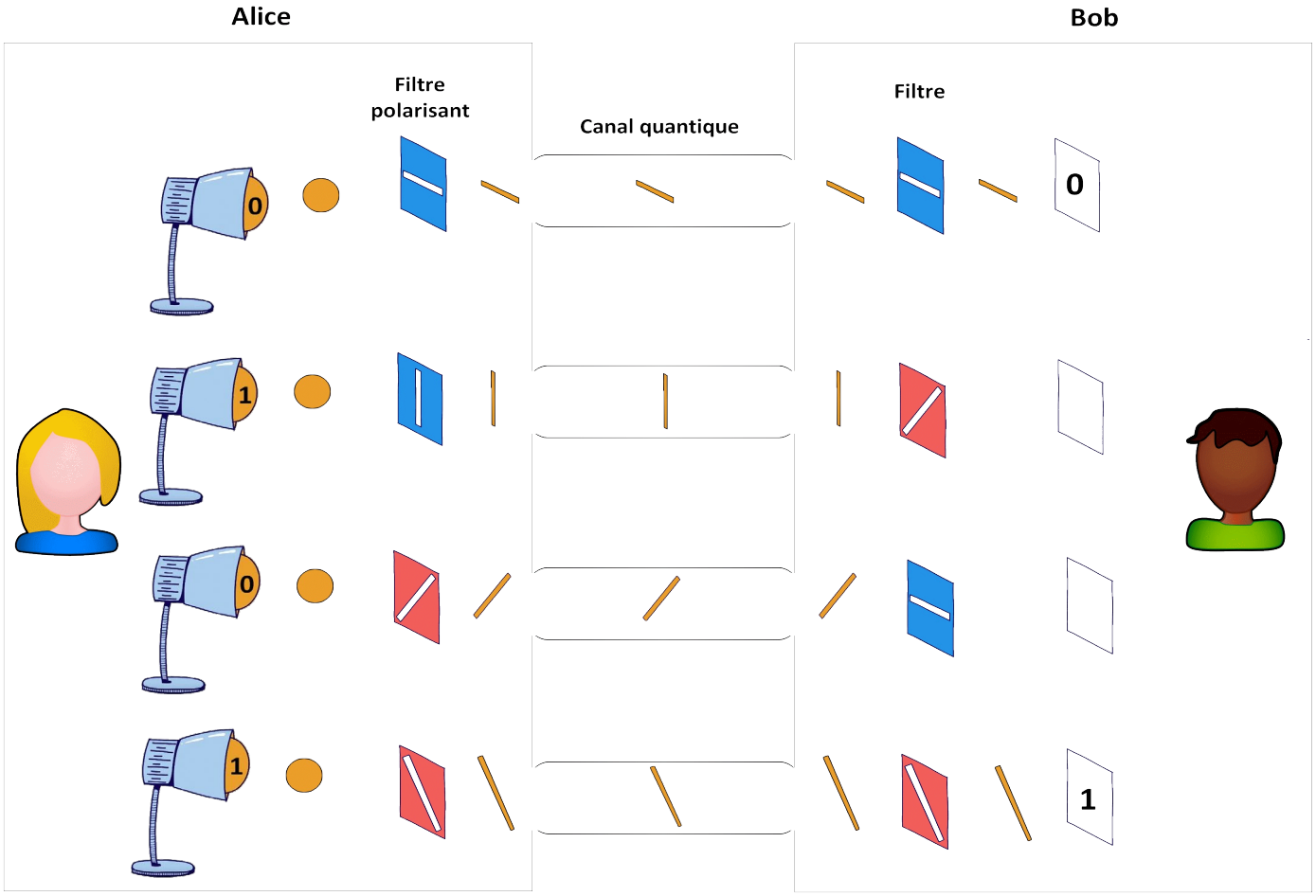
.

Chaque photon a donc une chance sur deux de circuler dans un des deux états de polarisation à travers le réseau.



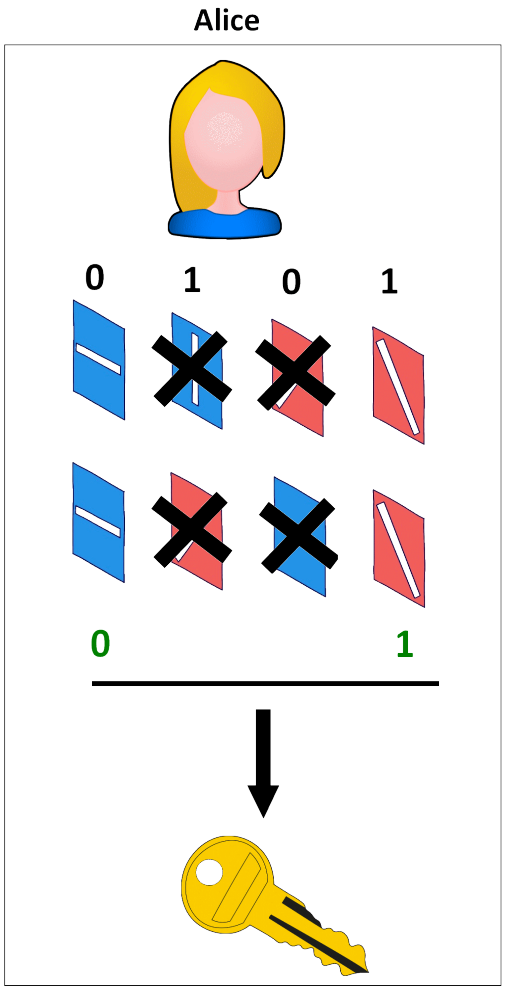
Indépendamment d'Alice, Bob va également choisir aléatoirement des filtres pour essayer de capter les photons polarisés qui circulent dans le réseau. Il utilise le même algorithme qu'Alice, donc il sait reconnaitre quand il y a un 0 ou un 1 qui va arriver. Il va donc pouvoir positionner les filtres comme il faut devant les 0 et les 1, mais il n'aura quand même qu'une chance sur deux pour les capter, étant donné qu'ils ont adopté une forme particulière.

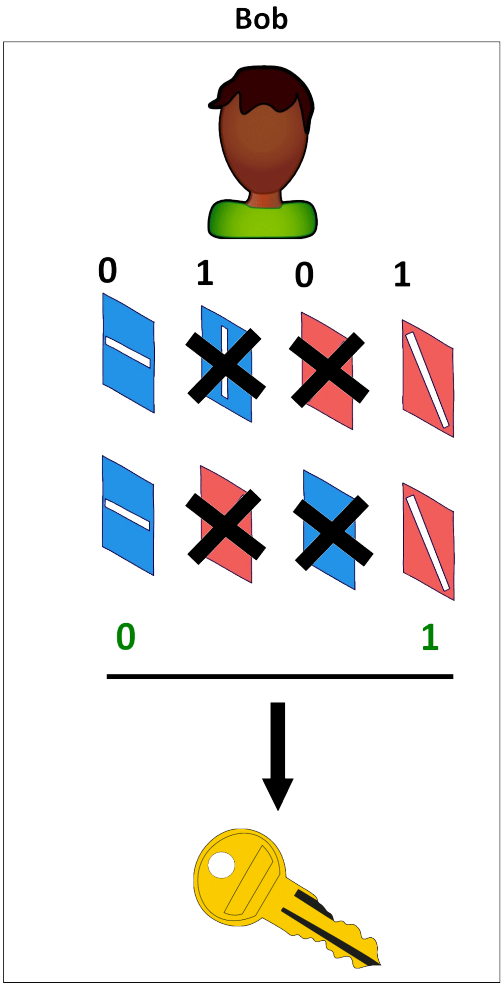
Voici ce que ça donne si on envoi 4 qubits les photons sont envoyés, ils sont polarisés, ils circulent à travers le réseau et ils arrivent chez Bob. S'il a choisi le mauvais filtre, le photon ne passera pas, ça coince littéralement, et le qubit est perdu. Si c'est bon le filtre, le photon peut passer, et la valeur du qubit est conservée pour commencer à former la clé secrète.



Une fois tous les qubits traités, Alice et Bob vont s'échanger les suites de filtres qu'ils ont chacun utilisés, et en comparant ces filtres, ils pouvoir deviner, chacun de leur côté, quel qubit a réussi à circuler ou non. Ils vont très simplement conserver les qubits qui sont passés par deux filtres identiques, et jeter les autres. Ainsi, ils vont faire le tri et former la clé secrète dans leur coin. Ils auront alors formé une clé symétrique et pourront chiffer et déchiffrer leurs futurs messages grâce à cette clé.

Ainsi, pour chaque valeur de qubit 0 ou 1, le qubit a une chance sur deux d'être détruit ou conservé. En répétant ce mécanisme, par exemple, 512 fois, vous pouvez générer une clé secrète de plus ou moins 256 qubits, en fonction des probabilités.





Sur cet exemple, les photons 0 et 1 ont pu passer car Alice et Bob ont utilisé les mêmes filtres, donc la clé secrète sera 0 1.