un résultat opposé. Cette magie peut être résumée par les quatre conditions suivantes :

$A_1 = B_1$ $\quad B_1 = A_2$
$A_2 = B_2$ $\quad B_2 \neq A_1$

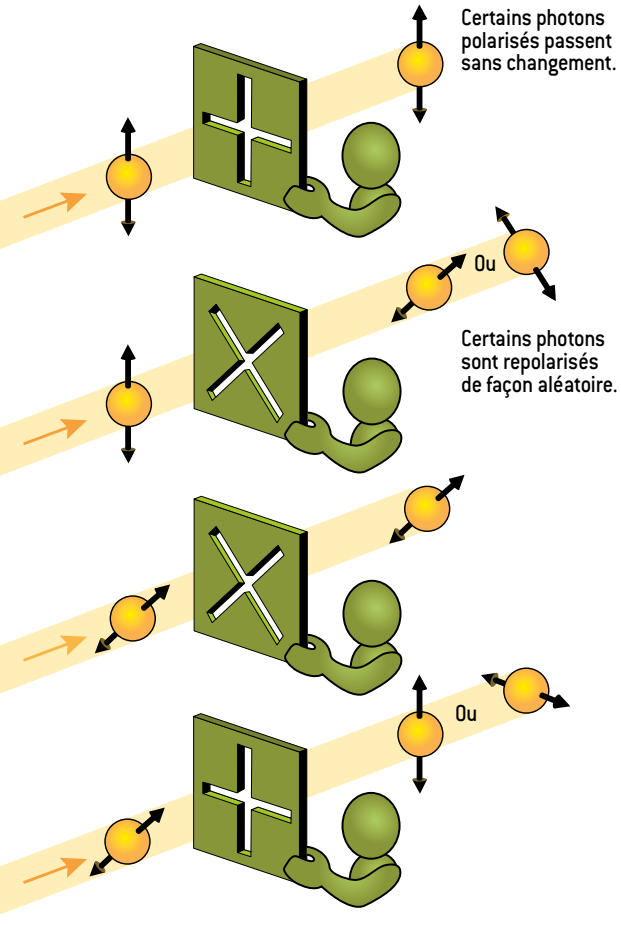
Ces conditions sont clairement contradictoires : il est impossible d'assigner à A_1, A_2, B_1 et B_2 des valeurs telles que les quatre conditions soient simultanément satisfaites. Mais il faut se rappeler qu'Alice et Bob ne peuvent lancer qu'une pièce chacun, et qu'ils ne peuvent donc tester qu'une seule des quatre conditions à la fois ; cela ne conduit à aucune contradiction.

Mais si, par exemple, Alice enfreint la règle et lance ses deux pièces A_1 et A_2 en même temps, que se passe-t-il ? Supposons qu'Alice obtienne deux faces ou deux piles ($A_1 = A_2$) ; alors Bob n'a pas d'autre choix que de lancer B_1, parce que c'est le seul lancer compatible avec les conditions des pièces magiques. De la même façon, si Alice obtient une pièce face et une pièce pile ($A_1 \neq A_2$), le seul choix qui reste à Bob est de lancer B_2.

Ainsi, lorsque Alice lance ses deux pièces, elle prive Bob de sa liberté de choisir la pièce qu'il veut tirer. Cette situation bizarre implique qu'Alice ne peut pas lancer ses deux pièces en même temps, sous peine de contradictions. Cela implique aussi que les pièces magiques ne peuvent pas être clonées. Si Ève avait une pièce Z constituant un clone de A_1, lorsque Alice lance A_2, on retrouverait des contradictions comme précédemment.

En conclusion, si les choix d'Alice et de Bob sont libres, les corrélations doivent être monogames, c'est-à-dire qu'aucune pièce tierce ne peut être corrélée à A_1, A_2, B_1 ou B_2. Cela redonne à Alice et Bob l'avantage sur Ève : ni elle, ni personne d'autre ne peut fabriquer une pièce qui correspondra toujours avec l'une quelconque des pièces détenues par Alice et Bob.

Tous les ingrédients de la distribution sécurisée des clés sont désormais en place. Concrètement, pour créer une clé de chiffrement, Alice et Bob lancent leurs pièces magiques. À chaque lancer, Alice et Bob



Le destinataire possède deux filtres qu'il choisit de façon aléatoire pour chaque photon du message.

DÉFINIR UNE CLÉ DE CHIFFREMENT

Le destinataire enregistre la polarisation de chaque photon reçu, puis précise publiquement quelle séquence de filtres il a utilisée. L'émetteur lui indique alors, en fonction de sa propre séquence de filtres, ceux qui n'ont *a priori* pas modifié le photon transmis. Les bits correspondants forment la clé.