Annexe 3 – Le protocole E91

Le protocole, décrit par Arthur Ekert en 1991, appelé E91, permet d'exploiter les particularités de l'intrication quantique pour partager une clé secrète aléatoire entre Alice et Bob en mesurant des paires de qubits intriqués.

L'intrication est un phénomène propre à la physique quantique. Lorsqu'un système est dans un état intriqué, il possède un état quantique global. Les éléments qui composent ce système ne peuvent plus être décrits indépendamment, quelle que soit la distance qui les sépare. Ils ont, par ailleurs, des propriétés physiques qui sont corrélées.

C'est grâce à ce phénomène d'intrication qu'Alice et Bob sont en mesure d'obtenir des résultats corrélés à 100% si des qbits intriqués sont mesurés dans la même base. Ils ont donc la possibilité d'obtenir une clef secrète en exploitant ces phénomènes.

De plus, les mesures des qbits effectuées dans des bases différentes peuvent permettre de déterminer si le protocole a été perturbé par un bruit ou par une attaque. C'est l'utilisation des inégalités de Bell qui permet de le calculer. Si ces inégalités sont violées, alors Alice et Bob peuvent utiliser la clé secrète générée.

Description du protocole

Etape 1 : Charlie, l'émetteur, génère deux qbit qu'ils intriquent dans l'état particulier.

$$|\psi_s\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

Il envoie ensuite à Alice et à Bob un des deux qbits.

Etape 2 :

Lorsqu'elle reçoit un qbit, Alire tire au hasard une base $a \in \{X, W, Z\}$. Elle effectue ensuite la mesure correspondante de cette base, et stocke le résultat de cette mesure.

Bob fait de même de son côté avec une base $b \in \{W, V, Z\}$

3. Alice et Bob s'échangent leurs bases respectives sur un canal classique.

4. Lorsque la base d'Alice correspond à la base de Bob, le résultat de la mesure dans cette base est placé dans le groupe *Temoin* qui servira à créer la clef.

Si la base d'Alice ne correspond pas à la base de Bob, le résultat de la mesure est placé dans le groupe *Leurre* qui servira à tester la viabilité du canal quantique.

Idem du côté de Bob.

5. Lorsque Alice dispose d'assez de mesure dans son groupe de création de clef, elle utilise les mesures stockées dans le groupe *Leurre* pour tester les inégalités de Bell.

Si les inégalités de Bell sont violées, alors Alice peut utiliser les mesures stockées dans le groupe *Temoin* pour chiffrer son message, puis l'envoyer à Bob.

Si les inégalités de Bell ne sont pas violées, alors Alice doit recréer un canal quantique entre elle et Charlie. Idem pour Bob.

6. Lorsqu'il reçoit le message chiffré, Bob peut utiliser son groupe *Temoin*, qui est identique à celui d'Alice, pour le déchiffrer.