Informatique quantique

Projet Final : Secret Sharing

1 Organisation du projet

1.1 Mise en contexte

Au cours de ce projet, nous souhaitons étudier la cryptographie quantique. La cryptographie quantique intervient dans les années 1990, lorsque Peter Shor propose un algorithme d'ordinateur quantique en temps polynomial pour la factorisation des nombres entiers. Cet algorithme aurait le pouvoir d'identifier des clés cryptographiques secrètes de manière efficace, réduisant le temps de résolution prévu pour certaines techniques cryptographiques actuelles. Les ordinateurs quantiques peuvent réaliser cette factorisation de manière exponentielle plus efficacement que les ordinateurs numériques, ce qui signifie que ces méthodes de sécurité deviendront obsolètes, et représenteront très bientôt un enjeu majeur pour les entreprises et les gouvernements.

1.2 Secret partagé en cryptographie quantique

Nous avons choisi d'introduire le concept de secret réparti en quantique. Le secret réparti est une donnée secrète que l'on souhaite partager à plusieurs destinataires. Néanmoins, ce secret ne peut être découvert que si un certain nombre de personnes mettent en commun les informations qu'ils ont reçues. On ne peut néanmoins pas savoir si une personne, un espion, essaye d'accéder à cette information. C'est pourquoi, on utilise des protocole cryptographiques quantiques. Elles permettent de sécuriser la transmission de données si un espion essaye d'obtenir des informations sur la clé permettant de coder le message.

1.3 Plan du projet

Nous souhaitons donc implémenter un algorithme qui est capable de créer une clé secrète. Cette clé sera partitionnée entre n utilisateurs (avec n un paramètre de l'algorithme). Nous souhaiterions en plus avoir en paramètre le pourcentage de restitution de la clé. En effet l'utilisateur pourra régler s'il souhaite que la clé soit décryptable avec les n clés des utilisateurs ou bien s'il faut au moins la moitié des clés pour retrouver la clé secrète.

Références

[1] Mark Hillery, Vladimir Buzek et Andre Berthiaume. *Quantum Secret Sharing*. URL : http://www.quantum.physics.sk/rcqi/mypapers/99pra1829.pdf.

[2] Dylan Liu. *Quantum Secret Sharing with Grover's Algorithm*. URL : https://crypto.stanford.edu/cs359c/17sp/projects/DylanLiu.pdf.

[3] K.P.T. Rietjens. *Quantum Secret Sharing Schemes*. URL : https://www.win.tue.nl/~henkvt/images/VerslagKarinRietjens.pdf.