EMINES TD1: Cryptographie quantique

Zaki Leghtas*

Janvier 2026

1 Exercices sur les postulats 1 et 2

1. Normaliser les états suivants: $|\psi_1\rangle = |0\rangle + |1\rangle$, $|\psi_2\rangle = |0\rangle + 3\,|1\rangle$, $|\psi_3\rangle = |0\rangle + 3i\,|1\rangle$, $|\psi_4\rangle = 4\,|0\rangle + 2i\,|1\rangle$
2. Une fois normalisés, calculer $\langle\psi_1|\psi_3\rangle$, $|\psi_1\rangle\langle\psi_3|$.
3. Algèbre de Pauli : remplissez le tableau 1.
4. Calculez les commutateurs $[\hat{X},\hat{Y}], [\hat{Y},\hat{Z}], [\hat{Z},\hat{X}]$.

$\times$	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$
$\hat{I}$				
$\hat{X}$				
$\hat{Y}$				
$\hat{Z}$				

Table 1: Algèbre de Pauli

*zaki.leghtas@ens.fr

2 Cryptographie quantique

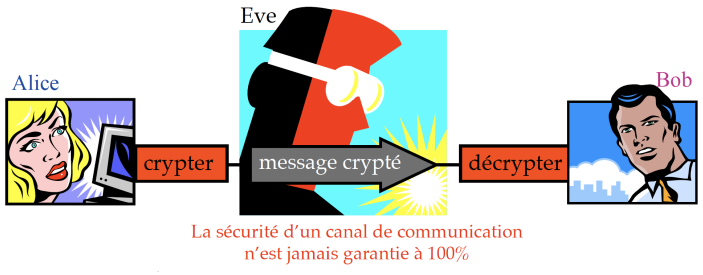

Figure 1: Alice et Bob souhaitent communiquer un message crypté par un canal accessible à l'espionne Eve.

2.1 Communication par clé secrète

Alice veut envoyer un message m à son ami Bob (e.g $m = 1010\ldots0010$). Problème: une espionne Eve accède au canal de communcation d'Alice et Bob. Ces derniers trouvent une solution: ils se mettent d'accord sur une clé secrète k (e.g $k = 0110\ldots1011$). Plutôt que d'envoyer le message m sur le canal visioné par Eve, Alice *crypte* le message, et envoie le message crypté $\bar{m}$

$$\bar{m} = m \oplus k \text{ (cryptage)},$$

où $\oplus$ correspond à l'addition modulo 2. Lorsque Bob reçoit le message crypté $\bar{m}$, il le décrypte de la façon suivante:

$$m = \bar{m} \oplus k \text{ (décryptage)}.$$

1. Démontrez l'équation qui correspond au décryptage par Bob.
2. Mettez-vous en binôme et implémentez le protocole: mettez-vous d'accord sur une clé secrète k à 10 bits. Alice choisit un message m, le crypte, envoie le message crypté $\bar{m}$ et Bob le décrypte.
3. Est-il sécure d'envoyer beaucoup de messages avec la même clé k ?

Le protocole de cryptographie par clé secrète repose sur le fait qu'Eve n'a pas accès à la clé k. Les protocoles de distribution de clés secrètes (RSA, non étudié dans ce cours) fondent leur sécurité sur des conjectures mathématiques non prouvées: la difficulté de factoriser des grands nombres entiers. Ainsi si quelqu'un dans le monde sait factoriser de grands nombres entiers, il peut décrypter la majorité des messages échangés (secrets défense, secrets bancaires, communications privés, etc).

2.2 BB84: distribution de clé quantique

En 1984, Charles Bennett (IBM, USA) et Gilles Brassard (Université de Montréal, Canada) ont inventé un protocole de distribution de clé secrète dont la sécurité est garantie par la mécanique quantique.

Plutôt que d'envoyer des bits classiques à Bob, Alice va envoyer des qubits. Pour envoyer un 0, elle envoie aléatoirement soit $|+Z\rangle$ ou $|+X\rangle$. De même, pour envoyer un 1, elle envoie aléatoirement soit $|-Z\rangle$ ou $|-X\rangle$. Lorsque Bob reçoit ces qubits, il décide de mesurer aléatoirement soit $\hat{Z}$, soit $\hat{X}$.

1. Décrire les situations où la base de mesure choisie par Bob (X/Z) coïncide ou pas avec la base de préparation d'Alice (X/Z).

Dans un premier temps, Bob dévoile à Alice ses bases de mesure, ainsi que le résultat de ses mesures. Alice et Bob comparent leurs résultats de mesure là où les bases de préparation et de mesure coïncident.

Numéro de la particule	1	2	3	4	5	6	7	8
Axe choisi par Alice (gardé secret)	z	z	x	z	z	x	x	z
Etat choisi par Alice (gardé secret)	+	−	+	−	−	−	+	−
Axe choisi par **Bob** (diffusé publiquement)	z	x	x	z	x	z	x	x
Etat mesuré par **Bob** (diffusé publiquement)								
Mesure utile ?								

Figure 2: Protocole de détection d'espionnage.

2. A titre d'exemple, remplir le tableau de la Figure. 2.

3. Décrire l'impact d'une espionne Eve qui intercepte les qubits, les mesure, et les renvoie à Bob.

4. Quelle est la probabilité qu'une espionne Eve passe inaperçue après l'échange de n qubits ?

Alice et Bob sont à présent satisfaits de l'accord entre leurs mesures et concluent que la ligne est sûre. Alice décide d'envoyer la clé secrète à Bob. Bob va cette fois-ci dévoiler ses bases de mesure mais *pas* les résultats ! Alice dévoile ensuite à Bob le numéro des qubits où les bases coïncident afin de constituer la clé secrète.

5. Remplir le tableau de la Figure. 3.

6. Quelle est la clé secrète dans cet exemple ?

Numéro de la particule	9	10	11	12	13	14	15	16
Axe choisi par Alice (gardé secret)	x	z	x	z	z	x	z	z
Etat choisi par Alice (gardé secret)	+	−	+	+	−	−	+	−
Axe choisi par Bob (diffusé publiquement)	z	z	x	x	z	z	z	x
Etat mesuré par Bob (gardé secret)								
Mesure utile ?								

Figure 3: Protocole de partage d'une clé secrète.

En pratique, Alice choisit aléatoirement quels sont les qubits de vérification de la sécurité de la ligne.