EMINES TD1: Cryptographie quantique

Zaki Leghtas*

Janvier 2026

1 Exercices sur les postulats 1 et 2

1. Normaliser les états suivants: $|\psi_1\rangle = |0\rangle + |1\rangle$, $|\psi_2\rangle = |0\rangle + 3\,|1\rangle$, $|\psi_3\rangle = |0\rangle + 3i\,|1\rangle$, $|\psi_4\rangle = 4\,|0\rangle + 2i\,|1\rangle$
   $|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|\psi_2\rangle = (|0\rangle + 3\,|1\rangle)/\sqrt{10}$, $|\psi_3\rangle = (|0\rangle + 3i\,|1\rangle)/\sqrt{10}$, $|\psi_4\rangle = (4\,|0\rangle + 2i\,|1\rangle)/\sqrt{20}$

2. Une fois normalisés, calculer $\langle\psi_1|\psi_3\rangle$, $|\psi_1\rangle\langle\psi_3|$.
   $\langle\psi_1|\psi_3\rangle = (1+3i)/\sqrt{20}$

$$|\psi_1\rangle\langle\psi_3| = \frac{1}{\sqrt{20}}(|0\rangle\langle 0| - 3i\,|0\rangle\langle 1| + |1\rangle\langle 0| - 3i\,|1\rangle\langle 1|) = \frac{1}{\sqrt{20}}\begin{pmatrix} 1 & -3i \\ 1 & -3i \end{pmatrix}$$

3. Algèbre de Pauli : remplissez le tableau 1.(Voir tableau)

4. Calculez les commutateurs $[\hat{X},\hat{Y}], [\hat{Y},\hat{Z}], [\hat{Z},\hat{X}]$.
   $[\hat{X},\hat{Y}] = 2i\hat{Z}, [\hat{Y},\hat{Z}] = 2i\hat{X}, [\hat{Z},\hat{X}] = 2i\hat{Y}$

2 Cryptographie quantique

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.

*zaki.leghtas@ens.fr

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

Table 1: Algèbre de Pauli

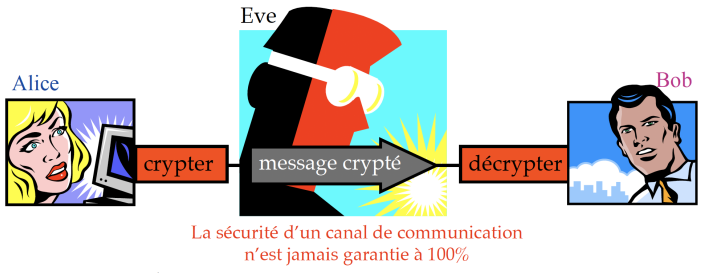

Figure 1: Alice et Bob souhaitent communiquer un message crypté par un canal accessible à l'espionne Eve.

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.
   $\bar{m} \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$

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.
Exemple: $m = 0110001010, k = 1100110101, \bar{m} = 1010111111$.

3. Est-il sécure d'envoyer beaucoup de messages avec la même clé k ?
   Non. En faisant des statistiques sur des éléments de language (présence de mots comme "à", "et", etc) ou construction de phrases (exemple: commencer un message par "bonjour"), on peut remonter au message et en déduire la clé secrète. Il est donc indisensable de régulièrement générer de nouvelles clés.

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 (que l'on note aussi $+$), elle envoie aléatoirement soit $|+Z\rangle$ ou $|+X\rangle$. De même, pour envoyer un 1 (que l'on note aussi $-$), 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).
   Si les bases conïncident, Bob va mesurer avec probabilité 1 le bit encodé par Alice. Si elle ne coïncident pas, il a seulement une chance sur deux.

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.

2. A titre d'exemple, remplir le tableau 2.(voir tableau)

3. Décrire l'impact d'une espionne Eve qui intercepte les qubits, les mesure, et les renvoie à Bob.
   Une espionne ne sait pas dans quelle base Alice encode son message, elle va donc, comme Bob, choisir aléatoire X ou Z. Lorsque (par chance pour elle), sa base de mesure coïncide avec celle d'Alice, elle passera inaperçue. Mais quand sa base ne coïncide pas, elle va projeter la particule dans un

Table 2: Protocole de détection d'espionnage

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
État choisi par Alice (gardé secret)	$+$	$-$	$+$	$-$	$-$	$-$	$+$	$-$
Axe choisi par Bob (diffusé publiquement)	z	x	x	z	x	z	x	x
État mesuré par Bob (diffusé publiquement)	$+$	$\pm$	$+$	$-$	$\pm$	$\pm$	$+$	$\pm$
Mesure utile ?	oui	non	oui	oui	non	non	oui	non

état qui n'est pas celui préparé par Alice, et ceci va affecter les mesures faites par Bob.

4. Quelle est la probabilité qu'une espionne Eve passe inaperçue après l'échange de n qubits ?
   Pour chaque qubit, il y a une proba 1/2 qu'Eve choisisse par hasard la bonne base et passe donc inaperçue. Supposant qu'elle choisisse la mauvaise base, il y a une proba 1/2 que Bob trouve quand même le même bit qu'Alice et ne s'aperçoive pas de la présence d'Eve. Il y a donc une proba $1/2 + 1/2 \times 1/2 = 3/4$ de passer inaperçue à chaque qubit, et donc $(3/4)^n$ après l'échange de n qubits. A titre d'exemple, ceci fait 10^{-4} pour $n = 32$, et 10^{-8} pour $n = 64$.

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.

Table 3: Protocole de partage d'une clé secrète

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
État choisi par Alice (gardé secret)	+	−	+	+	−	−	+	−
Axe choisi par Bob (diffusé publiquement)	z	z	x	x	z	z	z	x
État mesuré par Bob (gardé secret)	±	−	+	±	−	±	+	±
Mesure utile ?	non	oui	oui	non	oui	non	oui	non

5. Remplir le tableau 3. (voir tableau)

6. Quelle est la clé secrète dans cet exemple ?
   On garde les particules qui ont été préparées et mesurées dans la même base: 10,11,13,15. La clé secrète est donc: $-+-+$ ou en binaire: 1010.

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