Les années 1980 ont vu l'éclosion d'un nouveau domaine de la physique et de l'informatique: celui de l'information quantique, qui vise à tirer parti du potentiel de la physique quantique pour dépasser l'informatique classique dans certaines applications. Il s'agit d'un domaine de recherche très actif, très ouvert sur certains fronts, et qui a déjà acquis une certaine maturité technologique sur d'autres fronts, tels que la cryptographique quantique.

Les briques élémentaires de l'information quantique sont

1. le **bit quantique**, ou **qu-bit**, c'est-à-dire un système à deux niveaux $|0\rangle$ et $|1\rangle$ (spin $\frac{1}{2}$, état de polarisation d'un photon,...), dont l'état général est $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, avec $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, par opposition à un bit classique qui n'admet que les valeurs 0 et 1;

2. des **portes logiques quantiques**, qui sont des opérateurs linéaires unitaires agissant sur un ou plusieurs qu-bits;

3. des **opérations de mesure**, qui peuvent intervenir non seulement à la fin d'un protocole/à la sortie d'un circuit quantique pour en analyser le résultat, mais aussi à l'intérieur même d'un tel protocole/d'un tel circuit, sous la forme d'une mesure partielle qui permet de forcer la projection partielle de l'état quantique manipulé sur les états propres de certaines observables; l'exercice 1 ci-dessous illustrera ce dernier cas de figure.

Parmi les portes logiques quantiques, on distingue

- les portes à un qu-bit, par exemple la porte NOT (négation), qui à $|0\rangle$ associe $|1\rangle$ et vice versa, et dont la matrice représentative dans la "base computationnelle" $\{|0\rangle, |1\rangle\}$ est la matrice de Pauli

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

  de façon générale, une porte à un qu-bit est un opérateur linéaire unitaire $U \in U(2)$;

- les portes à deux qu-bits, dont l'exemple le plus important est la porte dite "control-NOT" ou CNOT, qui a l'action suivantes sur les éléments de la base computationnelle:

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |11\rangle \\ |11\rangle &\mapsto |10\rangle, \end{aligned}$$

  ce qui veut dire que l'état du second qu-bit est changé lorsque le premier qu-bit est dans l'état $|1\rangle$ (on parle alors d'une opération contrôlée par le premier qu-bit);

- plus généralement, les opérations à plusieurs ($n \geq 2$) qu-bits, et l'on entend souvent par là des opérations qui ne soient pas simplement des opérations séparables sous la forme $U_1 \otimes U_2 \otimes \cdots \otimes U_n$ (on appellerait un telle porte une collection d'opérations à un qu-bit).

Dans la pratique, on utilise des champs extérieurs pour effectuer des opérations à un qu-bit ou des collections d'opérations à un qu-bit (cf série 8 pour une opération susceptible d'inverser un spin 1/2), et des interactions entre qu-bits pour les opérations (non séparables) à plusieurs qu-bits.

Exercice 1 *Protocole de téléportation quantique*

Nous examinons dans cet exercice un cas d'école, celui du protocole de téléportation quantique, qui repose sur la non-localité/l'intrication d'états quantiques, mais qui met aussi en lumière les limites de cette notion de non-localité.

Dans ce protocole, Alice dispose d'un qu-bit (qu-bit 1) dans l'état

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

et elle souhaite transférer à Bob l'information quantique stockée dans ce qu-bit (les coefficients complexes α et β, qu'Alice ne connaît pas nécessairement). A cette fin, Alice et Bob se partagent aussi une paire de qu-bits dans l'état intriqué

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2}$$

Cette paire a été préparée par Alice, par Bob, ou par un troisième acteur, avant distribution à Alice et Bob d'un qu-bit chacun (qu-bits 2 et 3). L'état initial du système total à trois qu-bits est donc

$$|\Psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes \frac{|0\rangle_2 \otimes |0\rangle_3 + |1\rangle_2 \otimes |1\rangle_3}{\sqrt{2}}, \tag{3}$$

où les indices, facultatifs, ne servent qu'à rappeler l'ordre des qu-bits dans le produit tensoriel; pour simplifier l'agencement des calculs par la suite, on attribue le troisième qu-bit à Bob.

1. Alice applique à ses qu-bits une porte CNOT contrôlée par le premier qu-bit. Quel est l'état total $|\Psi_1\rangle$ après cette première opération?

2. Alice applique ensuite une porte de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4}$$

   à son premier qu-bit. Quel est alors l'état total $|\Psi_2\rangle$?

3. Alice mesure ensuite ses deux qu-bits dans la base computationnelle, ce qui veut dire qu'elle mesure l'observable "0 ou 1?" pour les deux premiers qubits, et elle note $(x, y) \in \{0, 1\}^2$ le résultat de cette mesure. Dans quel état sont les qu-bits d'Alice et le qu-bit de Bob après la mesure, pour chacun des quatre résultats (x, y) possibles ?

4. Alice envoie l'information (x, y) à Bob par un canal de communication classique (signaux de fumée, téléphonie 4G). Montrer que, sur la base de l'information (x, y) et de l'application de portes σ_x et σ_z à son qu-bit, Bob peut placer ce dernier dans l'état $|\psi\rangle$.

En suivant ce protocole, Alice et Bob transfèrent ("téléportent") donc l'état $|\psi\rangle$. Quelques questions pour réfléchir à la portée de cette notion de téléportation:

5. Y a-t-il eu téléportation de matière d'Alice vers Bob ?
6. Y a-t-il eu duplication ("clonage") de l'état $|\psi\rangle$ dans ce protocole ?
7. Y a-t-il eu transfert supraluminique d'information lors de cette téléportation ?

Exercice 2 *Protocole cryptographique BB84*

Nous nous intéressons dans cet exercice au protocole BB84 (Bennett, Brassard, 1984), connu comme le premier ou l'archétype des protocoles de cryptographie quantique. Il s'agit plus précisément d'un protocole de *distribution quantique de clé cryptographique*, qui vise à transmettre de façon totalement sécurisée une séquence de bits d'information (la clé), qui pourra ultérieurement être utilisée pour le chiffrage de communications par des moyens conventionnels (classiques). La motivation essentielle de la distribution quantique de clé (*quantum key distribution*, QKD) est que la sécurité du protocole est assurée (dans une certaine limite pratique) par les principes mêmes de la mécanique quantique, notamment l'impossibilité de cloner un état quantique arbitraire $|\psi\rangle$, ou d'en extraire de l'information sans le perturber.

Le protocole BB84 fonctionne de la manière suivante. Alice et Bob veulent se mettre d'accord sur une clé de chiffrage, et Alice est en mesure d'envoyer des qu-bits à Bob (canal de communication quantique). On supposera ici que ces qu-bits sont des spins 1/2. Alice a le choix de préparer ces qu-bits dans les états propres de $\hat{S}_z$ (ou bien de $\hat{S}_x$) pour représenter l'information classique: $0 \to |+_z\rangle$ et $1 \to |-_z\rangle$ si la base d'encodage est celle des états propres de $\hat{S}_z$ (ou bien $0 \to |+_x\rangle$ et $1 \to |-_x\rangle$ pour $\hat{S}_x$). Bob, de son côté, mesure les qu-bits selon une direction de son choix (z ou x), et traduit les résultats de mesure en bits classiques: $+\hbar/2 \to 0$ et $-\hbar/2 \to 1$.

Alice engendre deux séquences de bits aléatoires, de longueur N, par exemple

$$(a_i) = (0, 1, 1, 0, 1, 1, 0, 0, 0, \dots) \tag{5}$$

$$(b_i) = (0, 0, 1, 0, 1, 1, 1, 0, 1, \dots). \tag{6}$$

La séquence (a_i) contient une séquence de bits qu'elle veut transmettre à Bob, et la séquence (b_i) détermine la base qu'elle emploie pour l'encodage de chacun de ces bits: la base z si $b_i = 0$, et la base x si $b_i = 1$. De son côté, Bob engendre une séquence aléatoire (b'_i) de même longueur N, par exemple

$$(b'_i) = (0, 1, 0, 0, 1, 1, 0, 0, 1, \dots). \tag{7}$$

Cette séquence détermine sa base de mesure pour chaque qu-bit reçu: base z si $b'_i = 0$, et base x si $b'_i = 1$. Bob note (a'_i) la séquence de bits associée à ces résultats de mesure.

1. Construire un tableau reprenant les séquences (5), (6) et (7) ci-dessus, et indiquant pour $i = 1, .., 9$ l'état du qu-bit envoyé à Bob, la base de mesure, les résultats de mesure a'_i possibles et les probabilités associées.

Après cette étape de communication quantique, Alice et Bob rendent leurs choix de base b et b' publics, comparent ces derniers, et ne retiennent dans leurs séquences a et a' que les bits a_i et a'_i tels que $b_i = b'_i$.

2. Justifier que cette procédure leur permet de partager un séquence commune de bits en guise de clé. On pourra s'aider du tableau de la question précédente, et on supposera à ce stade qu'aucune imperfection ou intervention extérieure sur le canal quantique ne vient altérer les qu-bits à destination de Bob.

3. Pour un grand N, quelle est la longueur probable/intuitive de la clé ainsi partagée? Justifier ce résultat en montrant que la probabilité $p(N, n)$ d'avoir n coïncidences $b'_i = b_i$ suit une loi binomiale $f(N, n, \rho) = \rho^n (1-\rho)^{N-n} N!/[(N-n)!n!]$ avec $\rho = 1/2$, et en utilisant le fait que pour une telle loi binomiale la moyenne est $N\rho$ et la variance $N\rho(1-\rho)$.

On suppose dorénavant que la longueur de la séquence est $N = 4n + \delta$, avec n grand, et δ également assez grand pour que la probabilité d'une séquence commune de longueur inférieure à $2n$ soit négligeable. En l'absence d'espionnage du canal quantique, Alice et Bob peuvent donc retenir $2n$ bits de la séquence commune comme clé. Par ailleurs, le fait que les choix b et b' ne soient pas publics avant la fin de la communication quantique les prémunit aussi contre l'espionnage: si l'espionne Eve, qui n'a accès qu'au canal quantique entre Alice et Bob, désire extraire de l'information de ce canal, elle doit intercepter les qu-bits d'Alice, les mesurer dans une base qu'elle choisit sans connaître la base utilisée par Alice pour chaque qu-bit, puis préparer à destination de Bob un qu-bit qui reflète le résultat de sa mesure (elle prépare un état $|\pm\rangle$ dans la base qu'elle a utilisée pour la mesure). On suppose donc maintenant qu'Eve intervient sur le canal et mesure tous les qu-bits envoyés par Alice.

4. Quelle est la probabilité que la base b''_i choisie par Eve pour un qu-bit donné soit incompatible avec celle utilisée par Alice pour l'encodage?

5. En examinant par exemple le cas $b_1 = b'_1 = 0$, $a_1 = 0$ et $b''_1 = 1$, ainsi que les probabilités associées aux résultats possibles d'Eve puis de Bob (notés a''_1 et a_1), expliquer quel est l'impact de l'espionnage d'Eve.

Pour détecter un espionnage éventuel, Alice (ou Bob) publie un ensemble (aléatoire) correspondant à la moitié n des $2n$ bits a_i (ou a'_i) retenus après publications des bases b et b'; Bob (Alice) compare cette séquence publiée à sa séquence correspondante, et l'intervention d'Eve apparaît alors par des dissonances entre ces deux séquences. Si l'intervention d'Eve est détectée, toutes les séquences utilisées sont jetées par Alice et Bob.

6. Exprimer la probabilité que l'espionnage d'Eve passe inaperçu en fonction de n, et conclure.