Primitives cryptographiques quantiques

Omar Fawzi

30 août 2006

Introduction

L'informatique quantique se présente comme une alternative pour résoudre des problèmes difficiles de l'informatique classique. L'avancée la plus importante est sans doute l'algorithme de Shor qui permet la factorisation d'un entier en temps polynomial (alors qu'aucun algorithme classique efficace de factorisation n'est connu même si on ne sait pas si ce problème est NP complet).

Mais l'informatique quantique a des applications aussi en cryptographie, en effet il a été démontré qu'il existe un protocole quantique d'échange de clés qui est sûr de manière inconditionelle, c'est à dire sans suppositions de complexité. Pour d'autres primitives cryptographique comme la mise en gage et le tirage à pile ou face, l'informatique quantique permet d'obtenir de meilleurs résultats qu'en classique. Nous allons nous intéresser à ces problèmes. Nous allons donc commencer par une introduction à la cryptographie quantique en décrivant un protocole de distribution de clés. Ensuite nous allons étudier le problème de la mise en gage pour lequel on croyait avoir une solution quantique mais celle-ci s'est avéré fausse lorsqu'en 1995 Mayers a démontré dans [6] l'impossibilité d'une mise en gage quantique parfaitement sûre. Puis nous allons présenter les résultats existants sur le problème du tirage à pile ou face avant de donner plusieurs preuves plus ou moins complètes d'un protocole assez différent pour lequel il n'existait pas de preuve publiée.

1 Introduction à la cryptographie quantique

1.1 Qubits

En informatique quantique l'entité de base qui contient l'information est le qubit. De la même façon qu'un bit peut prendre les valeurs 0 ou 1, un qubit peut prendre des valeurs qu'on note $|0\rangle$ et $|1\rangle$, mais aussi toute combinaison linéaire à coefficients complexes de ces 2 valeurs. Ainsi un qubit s'ecrit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Mais la mesure d'un qubit ne peut donner que $|0\rangle$ et $|1\rangle$, c'est à dire qu'une mesure ne peut pas nous donner les α et β. Le sens physique de ces coefficients est que la probabilité d'obtenir $|0\rangle$ est $|\alpha|^2$, la probabilité d'obtenir $|1\rangle$ est $|\beta|^2$. On a donc nécessairement $|\alpha|^2 + |\beta|^2 = 1$.

Notons que l'on peut faire une mesure dans n'importe quelle base orthonormale de l'espace hermitien que l'on vient de definir par exemple on peut mesurer dans la base $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$. Si on $|\psi\rangle$ mesure dans la base $|\psi_1\rangle, |\psi_2\rangle$ alors on obtient $|\psi\rangle_1$ avec une probabilité qui vaut le module au carré du produit scalaire $|\langle\psi|\psi_1\rangle|^2$ et $|\psi\rangle_2$ avec une probabilité $|\langle\psi|\psi_2\rangle|^2$. Il est important de noter que lorsqu'un qubit est mesuré dans une certaine base, il prend obligatoirement l'une de valeurs de la base.

Introduisons quelques notations utilisées en informatique quantique. On peut voir les vecteurs $|\psi\rangle$ comme des matrices colonnes dans la base $|0\rangle, |1\rangle$. On note alors $\langle\psi|$ le vecteur ligne transposé et conjugué de $|\psi\rangle$. La notation $\langle\psi|\psi\rangle$ pour le produit scalaire et $|\psi\rangle\langle\psi|$ pour la projection sur $|\psi\rangle$. On note aussi pour A un opérateur linéaire $\langle\psi|A|\phi\rangle$ le produit scalaire entre $|\psi\rangle$ et $A|\phi\rangle$.

Lorsqu'on souhaite décrire un système composé, l'état global est représenté par un vecteur dans le produit tensoriel entre ces 2 espaces. Par exemple, si H_A est l'espace d'état du système A et H_B l'espace d'état du système B, alors l'espace d'état du système global est $H_A \otimes H_B$, c'est-à-dire l'espace vectoriel engendré par $(e_i \otimes f_j)_{ij}$ où (e_i) est une base de H_A et (f_j) ne base de H_B.

1.2 Distribution de clés quantiques

Nous savons que la seule méthode connue parfaitement sûre pour envoyer un message est le 'one time pad', celle-ci consiste à chiffrer un message avec une clé de la même longueur que le message. Mais le problème est qu'il faut qu'Alice et Bob se mettent d'accord sur une clé secrète. La distribution de clés quantiques permet d'effectuer cette étape de manière sûre.

Nous allons présenter l'idée de ce protocole. Mais la preuve de la sureté fait appel à la théorie quantique de l'information et sort du cadre de notre étude.

1. Alice prépare une chaine de bits a_i et tire au hasard des bits b_i
2. Alice envoie chaque bit a_i en tant que qubit dans la base b_i en considérant que la base 0 est la base $(|0\rangle, |1\rangle)$ et 1 la base $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$. Par exemple si $a_i = 1$ et $b_i = 0$, Alice envoie $|1\rangle$.
3. Bob de son côté mesure les qubits qu'il recoit dans les bases b'_i choisies de manière aléatoire.
4. Alice envoie à Bob (de manière classique) les b_i, c'est-à-dire les bases dans lesquelles il fallait mesurer et Bob donne à Alice les b'_i.
5. La clé secrète est alors constituée des a_i telles que $b_i = b'_i$.
6. Pour vérifier qu'il n'y a pas eu d'interception, Alice et Bob sacrifient certains des bits de leur clé en se les communiquant sur un canal public.

Notons d'abord qu'on suppose que Bob sait que c'est Alice qui lui envoie, et pour ceci il faut qu'il partage déjà un secret, on peut donc voir ce protocole comme un procédé d'amplification de secret. Pour comprendre pourquoi ce protocole est sûr il faut savoir qu'il est impossible de cloner un état quantique. On peut voir ceci en supposant qu'il existe une transformation U telle que

$$U|x\rangle|0\rangle = |x\rangle|x\rangle$$

mais cette transformation doit nécessairement être unitaire et donc

$$U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(U|0\rangle|0\rangle + U|1\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Mais par définition

$$U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Ce qui donne une contradiction.

Donc quelqu'un qui intercepte les qubits ne peut pas les "sauvegarder" et faire les mêmes mesures que Bob. Et si celui-ci garde les qubits d'Alice et envoie d'autres qubits à Bob, ceci sera détecté à l'étape de vérification avec une probabilité dependant du nombre de bits sacrifiés lors de cette étape.

2 Protocoles pour la mise en gage

Il y a d'autres problèmes en cryptographie pour lequels on peut espérer avoir de meilleurs résultats en utilisant des qubits par exemple celui de la mise en gage (*bit commitment*).

Définition 1 (Mise en gage)**.** Alice met en gage un bit a chez Bob, et elle peut révéler ce bit lorsqu'elle le veut. Le protocole est dit sûr lorsque:

- Bob n'a aucune information sur a
- Alice ne peut pas changer son bit à la révélation

On peut schématiser ceci en disant qu'Alice met son bit dans un coffre fort qu'elle envoie à Bob et dont elle garde la clé. On dit qu'un protocole est inconditionnellement liant si Alice ne peut pas changer son bit, et inconditionnellement camouflant si Bob ne peut rien apprendre sur a.

2.1 Un protocole classique

Il est impossible d'avoir un protocole à la fois inconditionnellement liant et camouflant mais il est possible d'avoir l'un des deux tandis que l'autre est "difficile". Par exemple on peut indiquer un protocole inconditionnellement camouflant et pour s'assurer qu'Alice ne peut pas changer son bit, on utilise des fonctions rapidement calculables mais dont l'inverse est difficile à calculer. Par exemple l'exponentiation modulo un grand nombre premier p. Ceci nous donne le protocole suivant.

Alice et Bob se mettent d'accord sur p un grand nombre premier et g un générateur de $\mathbb{Z}_p^*$. Bob choisit $c \in \mathbb{Z}_p^*$

1. Alice choisit un bit a qu'elle veut mettre en gage et un nombre $r \in \mathbb{Z}_p^*$
2. Alice calcule et envoie $g^r c^a$
3. Bob ne voit que $g^r c^a$, en déduire a est difficile
4. Dans la phase de révélation Alice envoie r et a

Ceci est un protocole sûr en pratique mais il est basé sur des suppositions de complexité, ici la difficulté du calcul du logarithme discret. En effet pour changer de bit, Alice doit calculer le logarithme discret de a puisqu'elle doit trouver r_0 et r_1 tels que $g^{r_0} c^0 = g^{r_1} c^1$ or $g^{r_0 - r_1} = a$.

2.2 Un protocole quantique

En 1984 Bennet et Brassard élaborent un protocole quantique pour la mise en gage qui ressemble à la distribution de clé. Les deux étapes du protocole sont les suivantes:

- Pour mettre le bit dans le coffre fort
  1. Alice choisit a et s bits aléatoires b_i
  2. Elle envoie tous les b_i dans la base a, on appelle 0 la base $(|0\rangle, |1\rangle)$ et 1 la base $(|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |\nwarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$
  3. Bob mesure ces qubits dans des bases aléatoires b'_i
- Pour la révelation
  1. Alice envoie a et les b_i à Bob
  2. Bob vérifie que ses mesures sont cohérentes avec ces informations c'est à dire que pour $b'_i = b$ il a bien mesuré b'_i

On pourrait croire que ce protocole est sûr, en effet Bob ne peut obtenir aucune information sur a et Alice ne peut pas changer a sans se faire detecter puisqu'elle ne connait ni les b'_i que Bob a choisies ni les résultats des mesures et donc ne peut pas changer les b_i en conséquence. Mais il s'avère que ce raisonnement est faux et qu'Alice peut changer son bit sans risquer de se faire détecter. En effet pour cela elle utilise la stratégie suivante : elle prépare des paires EPR $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et envoie le premier qubits de chaque paire et garde le deuxième. Notons ici que $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\nearrow\nearrow\rangle + |\nwarrow\nwarrow\rangle)$. La propriété interessante ici est que lorsque effectue une mesure dans l'une ou l'autre base, le qubit qu'Alice à garder devient ce même qubits. Maintenant Alice choisit le bit a qu'elle veut et envoie les b_i comme étant les résultats des mesures de ses qubits dans la base a.

2.3 Impossibilité de la mise en gage inconditionnelle

En 1993, l'article [3] donne un protocole de mise en gage et montre que ce protocole est sûr. Mais en 1996 Mayers [6] démontra que cette preuve était fausse et même qu'il est impossible d'avoir un protocole de mise en gage quantique parfaitement sûr, ce résultat a été independamment trouvé par Lo et Chau [5]. Pour présenter cette preuve nous avons besoin de la décomposition de Schmidt.

Théoreme 1 (Décomposition de Schmidt). *Soit H_A et H_B deux espaces d'état et $|\psi\rangle \in H_A \otimes H_B$. Il existe des états orthogonaux $|k_A\rangle \in H_A$ et $|k_B\rangle \in H_B$ tels que*

$$|\psi\rangle = \sum_k \lambda_k |k_A\rangle |k_B\rangle$$

où les λ_i sont des réels strictement positifs et $\sum_k \lambda_k^2 = 1$. Les λ_i sont appelés les coefficients de Schmidt.

Preuve. Nous allons nous restreindre dans cette preuve au cas où H_A et H_B sont de même dimension n. Soit $|e_i\rangle$ et $|f_i\rangle$ des bases de H_A et H_B respectivement. On écrit $|\psi\rangle = \sum_{i,j=1}^n a_{ij}|e_i\rangle|f_j\rangle$. On note alors A la matrice dont les coefficients sont a_{ij} et on effectue la décomposition en valeur singulière de cette matrice. $A = UDV$ avec U et V unitaires et D diagonale avec des coefficients positifs. On a alors

$$\begin{aligned} |\psi\rangle &= \sum_{i,j,k=1}^n u_{ik} d_{kk} v_{kj} |e_i\rangle |f_j\rangle \\ &= \sum_{k=1}^n d_{kk} |k_A\rangle |k_B\rangle \end{aligned}$$

en notant $|k_A\rangle = \sum_i u_{ik}|e_i\rangle$ et $|k_B\rangle = \sum_j v_{kj}|f_i\rangle$ et ces bases sont bien orthonormées puisque U et V sont unitaires. □

Nous avons maintenant besoin de quelques notions supplémentaires de mécanique quantique. C'est la notion de matrice densité et celle de trace partielle.

On veut pouvoir décrire un système quantique qui est dans l'état $|\psi_i\rangle$ avec une probabilité p_i. On appelle matrice densité d'un tel systeme

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Avec ce formalisme on peut encoder une distribution classique (p_x) sur des états classiques $|x\rangle$ par la matrice densité $\sum_x p_x |x\rangle\langle x|$. Notons qu'une matrice densité est une matrice symétrique positive de trace 1, ses valeurs propres sont les p_i et ses vecteurs propres sont les $|\psi_i\rangle$ si les $|\psi_i\rangle$ sont orthogonaux.

Nous voulons maintenant décrire un sous-système d'un système quantique. On suppose qu'on a 2 systèmes physiques A et B qui sont dans l'état global décrit par la matrice densité ρ^{AB}. On dit que l'opérateur densité réduit est

$$\rho^A = tr_B \rho^{AB}$$

où on définit la trace partielle par rapport à B par

$$tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = tr(|b_1\rangle\langle b_2|)|a_1\rangle\langle a_2|$$

pour les matrices densité séparées de la forme $|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|$ et on complète la définition en imposant la linéarité de la trace partielle.

Revenons à notre problème, on suppose que H_A correspond à la partie d'Alice et H_B celle de Bob. Chacun a le contrôle sur sa partie et peut y appliquer une transformation unitaire ou une mesure de son choix. Alice prépare $|\psi_{0,1}\rangle$ l'état global qui est dans $H_A \otimes H_B$ selon qu'elle veut mettre en gage 0 ou 1. Alice envoie à Bob sa partie. On peut décomposer

$$|\psi_0\rangle = \sum_i \lambda_i |e_i\rangle |f_i\rangle$$

et

$$|\psi_1\rangle = \sum_i \lambda'_i |e'_i\rangle |f'_i\rangle$$

Mais si on suppose que le protocole est sûr, Bob ne doit pas faire de différence entre $|\psi_0\rangle$ et $|\psi_1\rangle$. Donc on doit avoir $tr_A|\psi_0\rangle = tr_A|\psi_1\rangle$. Ce qui détermine les coefficients de Schmidt, on a $\lambda_i = \lambda'_i$ mais aussi $|f_i\rangle = |f'_i\rangle$ à une permutation près . En appliquant une transformation unitaire de son côté (celle qui transforme les e_i en e'_i), Alice peut donc passer de $|\psi_0\rangle$ à $|\psi_1\rangle$. Alice peut tricher sans risquer de se faire détecter.

Théoreme 2. *Il n'existe pas de protocole quantique pour la mise en gage qui soit à la fois inconditionnellement liant et inconditionnellement camouflant.*

3 Tirage à pile ou face

Une autre primitive cryptographique est le tirage à pile ou face à distance. Lors d'un communication on peut avoir besoin de nombres tirés au hasard mais sans que l'un des partis puissent les contrôler et sans avoir recours à un tiers auquel on fait confiance par exemple pour l'élection d'un leader à pile ou face, le déblocage de conflit réseau où pour des jeux équitables.

Un protocole de tirage à pile ou face peut se faire à l'aide d'un protocole de mise en gage. En effet il suffit qu'Alice mette en gage un bit a chez Bob ensuite Bob envoie un bit aléatoire b, et on prend comme bit finalement $a \oplus b$.

Mais on a vu qu'il est impossible d'avoir une mise en gage quantique parfaite, et de plus [5] fournit une preuve qu'il est aussi impossible d'avoir un tirage à pile ou face quantique parfait.

On renonce alors à avoir un tirage parfait, on accepte qu'il y ait un biais P_A, P_B, c'est à dire qu'un tricheur ne puisse influencer le résultat avec un probabilité plus grande que P_A pour Alice et P_B pour Bob. On peut définir un protocole de tirage à pile ou face comme ceci

Définition 2 (Tirage à pile ou face avec biais)**.** Un protocole de tirage à pile ou face est un protocole à la suite duquel Alice et Bob se mettent d'accord sur un bit aléatoire c. Il y a 3 issues possibles à un tel protocole : $c = 0$, $c = 1$ et *invalide* lorsqu'un des parti décide que l'autre a triché. Si Alice et Bob sont honnêtes alors $P(c = 0) = P(c = 1) = 1/2$ et $P(invalide) = 0$.

Un protocole de tirage à pile ou face avec biais (P_A, P_B) est un protocole pour lequel si Alice triche et Bob est honnête $P(c = 0) = P(c = 1) \leq 1/2 + P_A$ où c est le résultat du tirage et si Alice est honnête et Bob triche $P(c = 0) = P(c = 1) \leq 1/2 + P_B$

Remarque. On suppose toujours que pour un tricheur, se faire détecter est plus grave que d'obtenir un bit non souhaité, sinon un tricheur peut toujours invalider le protocole pour obtenir le bit qu'il veut. Ceci peut être justifié par le fait que le protocole est appliqué une seule fois.

3.1 Protocole avec biais 0.25

Le meilleur biais obtenu jusqu'à présent est 1/4. Le premier protocole qui atteint cette valeur est décrit dans [1] mais nous allons présenter un autre protocole très similaire décrit dans [4] mais dont la preuve est plus simple. Le protocole utilise des qutrits à la place des qubits, c'est à dire qu'un registre prend ses valeurs dans un espace de dimension 3 dont une base est $(|0\rangle, |1\rangle, |2\rangle)$.

On note $|\psi_a\rangle = \frac{1}{\sqrt{2}}(|aa\rangle + |22\rangle)$

1. Alice choisit un bit a au hasard et prépare l'état $|\psi_a\rangle$ et envoie le deuxieme qutrit à Bob
2. Bob renvoie un bit b aléatoire à Alice
3. Alice donne a à Bob et lui envoie sa moitié de l'état $|\psi_a\rangle$. Bob vérifie qu'il s'agit bien de l'état $|\psi_a\rangle$. Si c'est bien le cas le résultat est $c = a \oplus b$ sinon Bob décide que le résultat est *invalide*

Dans le cas où les deux acteurs sont honnêtes, a et b sont aléatoires et indépendants donc c est bien aléatoire. Si Alice et Bob trichent, il n'y a pas vraiment d'interêt à s'assurer que le protocole est sûr. On étudie donc le cas où un seul des deux triche.

Bob triche On suppose Alice honnête donc la matrice densité de l'état que reçoit Bob si $a = 0$ est

$$\rho_0 = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et si $a = 1$

$$\rho_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}$$

Nous voulons calculer la probabilté maximale de réussir à distinguer entre ces 2 matrices densité. Pour cela nous avons besoin de définir une notion de distance entre des matrices densité. La distance la plus naturelle d'abord entre 2 distributions de probabilités est la distance en variation:

$$d(p,q) = \frac{1}{2}\sum_i |p_i - q_i|$$

on a aussi

$$d(p,q) = \max_{S\subset\{1,\dots n\}} (\sum_{x\in S} p_x - \sum_{x\in S} q_x)$$

Cette distance est intéressante parce qu'on peut exprimer à l'aide de cette distance la meilleure probabilité d'erreur possible lorsqu'on essaie de distinguer entre 2 distributions. Plus précisément, si on sait qu'un certain phénomène suit une distribution soit (p_i) soit (q_i), et la probabilité qu'il suive (p_i) est $\frac{1}{2}$ et la probabilité qu'il suive (q_i) est $\frac{1}{2}$. Notre objectif est de savoir de quelle distribution il s'agit en faisant une observation de ce phénomène. Par exemple si on tire au sort on a une probabilité $\frac{1}{2}$ de se tromper sur la distribution. Essayons donc de minorer la probabilité d'erreur, c'est-à-dire la probabilité d'erreur du meilleur algorithme pour résoudre ce problème. Si A est l'ensemble sur lequel on décide que c'est la distribution p_i, c'est à dire que si on a un résultat dans A on dit qu'il s'agit de la distribution p_i, alors la probabilité d'erreur est

$$\begin{aligned}
P_{err} &= \sum_i P(\text{on observe i et on se trompe}) \\
&= \sum_i P(\text{on observe i et on décide p alors que c'est q}) + P(\text{observation i et on décide q alors que c'est p}) \\
&= \sum_{i\in A} \frac{1}{2}(p_i+q_i)\frac{q_i}{p_i+q_i} + \sum_{i\notin A} \frac{1}{2}(p_i+q_i)\frac{p_i}{p_i+q_i} \\
&= \sum_{i\in A} \frac{1}{2}q_i + \sum_{i\notin A} \frac{1}{2}p_i \\
&= \sum_{i\in A} \frac{1}{2}(q_i-p_i) + \frac{1}{2} \\
&\geq \frac{1}{2} - \frac{1}{2}d(p,q)
\end{aligned}$$

L'équivalent de cette norme pour les matrices densité est ce qu'on appelle la norme trace qui est définie par

$$\|A\|_{tr} = \frac{1}{2}tr(\sqrt{AA^*})$$

On voit que la norme trace est un cas particulier de la distance en variation en remarquant que si $\rho_p = \sum_x p_i|x\rangle\langle x|$ et $\rho_q = \sum_x q_i|x\rangle\langle x|$ alors $\|\rho_p - \rho_q\|_{tr} = d(p,q)$. Maintenant, cette norme trace est reliée à la distribution de probabilité engendrée par une certaine mesure par le théorème suivant qui est démontré par exemple dans [9] dans le chapitre 9.

Théoreme 3. *Pour toute mesure O on a*

$$|p^O_{\rho_0} - p^O_{\rho_1}|_{var} \leq \|\rho_0 - \rho_1\|_{tr}$$

oú p^O_ρ est la distribution de probabilité lorsque la mesure O est effectuée sur un système de matrice densité ρ

Donc pour toute mesure que Bob effectue il aura une probabilité d'erreur $\geq \frac{1}{2} - \frac{\|\rho_0-\rho_1\|_{tr}}{2}$ c'est-à-dire que Bob ne peut pas distinguer les 2 états avec une probabilité plus grande que

$$\frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_{tr}}{2}$$

On a

$$(\rho_0-\rho_1)(\rho_0-\rho_1)^* = \begin{pmatrix} 1/4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1/4 \end{pmatrix}$$

Donc

$$\sqrt{(\rho_0-\rho_1)(\rho_0-\rho_1)^*} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}$$

Ce qui donne

$$\|\rho_0-\rho_1\|_{tr} = \frac{1}{2} tr(\sqrt{(\rho_0-\rho_1)(\rho_0-\rho_1)^*}) = \frac{1}{2}$$

et

$$\frac{1}{2} + \frac{\|\rho_0-\rho_1\|_{tr}}{2} = \frac{3}{4}$$

Donc Bob en trichant ne peut pas imposer le résultat avec une probabilité supérieure à $\frac{3}{4}$.

De plus en mesurant dans la base $(|0\rangle, |1\rangle, |2\rangle)$ Bob obtient facilement avec probabilité $\frac{3}{4}$ le bit qu'il veut. Le biais pour Bob est donc exactement $\frac{1}{4}$.

Alice triche On suppose qu'Alice souhaite obtenir 0. Elle prépare l'état $|\psi\rangle \in H \otimes H_A \otimes H_B$ oú H est un ensemble de registres contrôlés par Alice qui lui permettent de tricher. Alice veut faire passer son bit a pour b. Elle envoie donc à Bob $a = b$. Ensuite avant de renvoyer son qutrit à Bob elle peut effectuer une transformation unitaire U_b sur les qutrits qu'elle contrôle. L'état devient donc $|\psi'_b\rangle = (U_b \otimes I_B)|\psi\rangle$ qu'on écrit sous la forme suivante en utilisant la décomposition de Schmidt en séparant H et $H_A \otimes H_B$

$$|\psi'_b\rangle = \sum_i \sqrt{p_i}|i\rangle|\phi_{ib}\rangle$$

Par orthogonalité des $|i\rangle$ on a

$$\rho = tr_H(|\psi'_b\rangle\langle\psi'_b|) = \sum_i p_i |\phi_{ib}\rangle\langle\phi_{ib}|$$

Maintenant la probabilité que Bob accepte ce qu'Alice lui envoie est

$$\begin{aligned} P(\text{Alice gagne} \mid \text{Bob envoie b}) &= \langle\psi_b|\rho|\psi_b\rangle \\ &= \sum_i p_i |\langle\psi_b|\phi_{ib}\rangle|^2 \end{aligned}$$

Ici nous allons utiliser une autre "distance" à l'aide de laquelle notre expression s'écrit simplement et qui nous permet de majorer cette probabilité à l'aide de variables connues ψ_b et σ la matrice densité de l'état que reçoit Bob au premier tour. Cette mesure est la fidélité. On définit la fidélité entre 2 matrices densité ρ et σ comme

$$F(\rho,\sigma) = \left(tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})\right)^2$$

Les propriétés de la fidélité que l'on va utiliser sont

Propriété. *1.* $F(\rho,\sigma) = F(\sigma,\rho)$

2. $0 \leq F(\rho,\sigma) \leq 1$ *et* $F(\rho,\sigma) = 1$ *si et seulement si* $\rho = \sigma$

3. Pour un système composé AB, $F(\rho,\sigma) \leq F(tr_A(\rho), tr_A(\sigma))$

La troisième propriété découle d'un théorème important (le théorème d'Uhlmann) qui caractérise la fidélité qui est démontrée dans [9]. Cette expression, un peu compliquée dans le cas général, se simplifie lorsqu'un des états est pur. En effet dans ce cas on a

$$F(\rho, |\psi\rangle\langle\psi|) = \langle\psi|\rho|\psi\rangle$$

Revenons donc à notre expression $\sum_i p_i|\langle\psi_b|\phi_{ib}\rangle|^2$, celle-ci peut se voir comme la fidélité de $|\psi\rangle\langle\psi|$ et de la matrice densité $\sigma_b = \sum_i p_i|\phi_{ib}\rangle\langle\phi_{ib}|$ et là on va pouvoir utiliser la propriété 3 de la fidélité

$$\begin{aligned} \sum_i p_i |\langle\psi_b|\phi_i b\rangle|^2 &= F(\sigma_b, |\psi_b\rangle\langle\psi_b|) \\ &\leq F(tr_A(\sigma_b), tr_A(|\psi_b\rangle\langle\psi_b|)) \\ &= F(\sigma, \rho_b) \end{aligned}$$

avec $\rho_b = tr_A(|\psi_b\rangle\langle\psi_b|) = \frac{1}{2}|b\rangle\langle b| + \frac{1}{2}|2\rangle\langle 2|$ et on rappelle que σ est la matrice densité de l'état reçu par Bob. Notons que $\sigma = tr_A(\sigma_b)$. En effet $\sigma = tr_A(|\psi\rangle)$ et $\sigma_b = tr_A(U_b \otimes I)|\psi\rangle = tr_A(|\psi\rangle)$. Pour voir qu'appliquer une transformation unitaire sur un sous-système qu'on trace n'a pas d'effet, il suffit d'écrire la décomposition de Schmidt de $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$ et on obtient $tr_A((U_A \otimes I)|\psi\rangle) = \sum_i \lambda_i |i_B\rangle\langle i_B| = tr_A(|\psi\rangle)$ puisque les $U|i_A\rangle$ restent orthogonaux.

On a maintenant

$$P(\text{Alice gagne} \mid \text{Bob envoie b}) \leq F(\sigma, \rho_b)$$

Et donc puisque Bob est honnête il envoie 0 ou 1 avec probabilité 1/2 chacun, donc

$$\begin{aligned} P(\text{Alice gagne}) &\leq \frac{1}{2}(F(\sigma,\rho_0) + F(\sigma,\rho_1)) \\ &\leq \frac{1}{2}(1 + \sqrt{F(\rho_0,\rho_1)}) \end{aligned}$$

où pour la deuxième ligne on a utilisé le lemme suivant qui est démontré dans [8] lemme 3.2

Lemme 1. *Pour toute matrice densité ρ_0, ρ_1, σ on a*

$$F(\rho_0,\sigma) + F(\rho_1,\sigma) \leq 1 + \sqrt{F(\rho_0,\rho_1)}$$

Calculons maintenant $F(\rho_0, \rho_1)$, on a

$$\sqrt{\rho_0}\rho_1\sqrt{\rho_0} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1/4 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et donc

$$tr(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}) = \frac{1}{2}$$

donc

$$P(\text{Alice gagne}) \leq \frac{3}{4}$$

De plus si Alice ne fait que renvoyer $a = b$ alors Alice gagne avec une probabilité $\frac{3}{4}$; sinon elle se fait detecter.

4 Tirage à pile ou face avec des paires EPR

Les protocoles cités sont basés sur une mise en gage, et il faut que Alice et Bob tirent vraiment un bit au hasard. On peut imaginer un autre protocole où la source du hasard soit la mesure quantique. Nous allons étudier un protocole de ce type. Le protocole :

1. Alice prépare 2 EPR paires $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et envoie à Bob le deuxième qubit de chacune d'elles.
2. Bob choisit de vérifier aléatoirement la première ou la deuxième paire. On appele v la paire à vérifier.
3. Alice envoie à Bob le premier qubit de la paire demandée. Bob vérifie qu'il s'agit bien d'une paire EPR. Sinon il décide d'annuler le protocole et le résultat est *invalide*.
4. L'autre paire est alors mesurée et donne le bit aléatoire commun b.
5. Alice envoie à Bob le bit mesuré, et Bob accepte si c'est b, le résultat du protocole est alors b et sinon *invalide*.

On voit bien que si Alice et Bob sont honnêtes $P(b = 0) = P(b = 1) = 1/2$.

Nous avons trouvé ce protocole dans une présentation [2] qui le mentionnait mais nous n'avons pas trouvé de preuve sur son biais. Nous avons donc cherché à prouver ce résultat, et nous avons montré que ni Alice ni Bob ne peuvent influencer le résultat avec un probabilité plus grande que 3/4.

4.1 Triche de Bob

On suppose d'abord Alice honnête. La seule manière pour Bob de tricher est de choisir le qubit de vérification, et pour que cela lui soit utile, il faut qu'il connaisse la valeur des qubits reçus. Il peut alors en fonction du résultat choisir ce qui l'arrange. Supposons que Bob veuille obtenir 0. Alors, si il mesure 00, 01 ou 10, il peut gagner. Donc Bob peut obtenir $P(b=0) = 3/4$. Et on voit que Bob ne peut pas faire mieux, puisqu'il ne peut pas influer sur ce que va mesurer Alice, son qubit va valoir 0 ou 1 avec probabilité $\frac{1}{2}$ chacun.

4.2 Triche d'Alice

Vu que nous n'étions pas sûrs de cette conjecture sur le biais en raison de l'absence de preuve, nous avons procédé par étape en essayant d'abord de prouver des résultats plus faibles qui semblent plus simples à analyser. Nous avons d'abord essayé d'étudier le cas où Alice ne veut pas se faire détecter, il s'est avéré qu'alors Alice doit être honnête. Ensuite nous avons démontré que le biais est $\leq \frac{\sqrt{2}}{4}$. Après cela nous avons démontré la conjecture de manière numérique en faisant certaines suppositions ce qui nous amena à trouver des méthodes pour tricher avec un probabilité 0.75. Ensuite nous avons trouvé une preuve générale qui est très courte. On note 1, 2, ... les qubits d'Alice et 1', 2' ceux de Bob.

Alice ne peut pas tricher sans risquer de se faire détecter Supposons d'abord que Alice ne veut pas se faire détecter du tout. Et montrons que alors Alice doit être honnête.

Notons $|\psi\rangle$ l'état de du système que prépare Alice au début. Par décomposition de Schmidt Alice-Bob on a

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

A l'étape 1, Alice envoie 2 qubits à Bob. On appelle ces 2 qubits $1'$ et $2'$. Lorsque Bob renvoie v, Alice applique une transformation unitaire U_v l'état devient donc $|\psi_v\rangle = \sum_i \lambda_i U_v |i_A\rangle |i_B\rangle$.

Le fait que Alice ne veut jamais se faire détecter se traduit par

$$\langle \phi^+ | tr_{11'}(|\psi_2\rangle\langle\psi_2|) |\phi^+\rangle = 1$$

et

$$\langle \phi^+ | tr_{22'}(|\psi_1\rangle\langle\psi_1|) |\phi^+\rangle = 1$$

On a alors

$$tr_{22'}(|\psi\rangle_1) = |\phi^+\rangle\langle\phi^+|$$
$$tr_{11'}(|\psi\rangle_2) = |\phi^+\rangle\langle\phi^+|$$

On utilise ensuite le lemme suivant :

Lemme 2. *Si $tr_B(|\phi\rangle\langle\phi|) = |\psi\rangle\langle\psi|$. Alors $|\phi\rangle\langle\phi| = |\psi\rangle\langle\psi| \otimes \rho_B$ ou $\rho_B = tr_A(\rho_{AB})$.*

Preuve. On écrit la décomposition de Schmidt de $|\phi\rangle$ en séparant A et B

$$|\phi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

On a alors

$$\begin{aligned} tr_B(|\phi\rangle\langle\phi|) &= \sum_{i,j} tr_B(\lambda_i\lambda_j |i_A\rangle\langle j_A| \oplus |i_B\rangle\langle j_B|) \\ &= \sum_i \lambda_i |i_A\rangle\langle i_A| \end{aligned}$$

On a donc

$$\sum_i \lambda_i^2 |i_A\rangle\langle i_A| = |\psi\rangle\langle\psi|$$

On en déduit que les λ_i sont tous nuls sauf un qui vaut 1 en remarquant par exemple que les λ_i^2 sont les valeurs propres de $\sum_i \lambda_i^2 |i_A\rangle\langle i_A|$ vu que les $|i_A\rangle$ sont orthogonaux. Donc l'état ϕ est séparé. □

On en déduit que

$$|\psi_1\rangle\langle\psi_1| = |\phi^+\rangle\langle\phi^+| \otimes \rho$$
$$|\psi_2\rangle\langle\psi_2| = \rho' \otimes |\phi^+\rangle\langle\phi^+|$$

Nous voulons maintenant revenir à la décomposition Alice-Bob, on utilise alors le lemme suivant

Lemme 3. *On a* $tr_{AB}(|\alpha\rangle_{AC} \otimes |\beta\rangle_{BD}) = tr_A(|\alpha\rangle) \otimes tr_B(|\beta\rangle)$.

Preuve. On écrit $|\alpha\rangle = \sum_i \lambda_i |i_A\rangle|i_C\rangle$ et $|\beta\rangle = \sum_i \nu_i |i_B\rangle|i_D\rangle$. On a

$$\begin{aligned} tr_B(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|) &= tr_B(|\alpha\rangle\langle\alpha| \sum_{i,j} \nu_i\nu_j |i_B\rangle\langle j_B||i_D\rangle\langle j_D|) \\ &= |\alpha\rangle\langle\alpha| \otimes \sum_i \nu_i |i_D\rangle\langle i_D| \end{aligned}$$

et donc

$$\begin{aligned} tr_{AB}(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|) &= tr_A(|\alpha\rangle\langle\alpha| \otimes \sum_i \nu_i |i_D\rangle\langle i_D|) \\ &= tr_A(\sum_{i,j} \lambda_i\lambda_j |i_A\rangle\langle j_A||i_C\rangle\langle j_C| \otimes \sum_k \nu_k |k_D\rangle\langle k_D|) \\ &= \sum_{i,j,k} \lambda_i\lambda_j\nu_k tr_A(|i_A\rangle\langle j_A| \otimes |i_C\rangle\langle j_C| \otimes |k_D\rangle\langle k_D|) \end{aligned}$$

A la dernière ligne, on a utilisé la linéarité de la trace partielle, et puisque $tr(|i_A\rangle\langle j_A|) = \delta_{ij}$, on a

$$\begin{aligned} tr_{AB}(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|) &= \sum_{i,k} \lambda_i\nu_k |i_C\rangle\langle i_C| \otimes |k_D\rangle\langle k_D| \\ &= tr_A(|\alpha\rangle) \otimes tr_B(|\beta\rangle) \end{aligned}$$

□

Et donc

$$tr_{12}(|\psi\rangle_1) = tr_1(|\phi^+\rangle) \otimes tr_2(\rho)$$

Et de même

$$tr_{12}(|\psi\rangle_2) = tr_1(\rho') \otimes tr_2(|\phi^+\rangle)$$

Mais

$$tr_{12}(|\psi\rangle_1) = tr_{12}((U_v \otimes I)|\psi\rangle) = tr_{12}(|\psi\rangle)$$

En effet, appliquer une transformation unitaire sur une partie ne change rien à la trace partielle pourvu que cette transformation n'affecte que la partie qu'on trace comme on l'a vu plus haut. On en déduit alors que

$$tr_{12}(|\psi\rangle) = \frac{1}{2} Id_{1'} \otimes \frac{1}{2} Id_{2'} = \frac{1}{4} Id_{1'2'}$$

Et puisque $tr_{12}(|\psi\rangle) = \sum_i \lambda_i |i_B\rangle\langle i_B|$, on en deduit donc que les coefficients de Schmidt $\lambda_i = 1/4$. L'état $|\psi\rangle$ s'écrit donc

$$|\psi\rangle = \frac{1}{4} \sum_{i=0}^{3} |i_A\rangle|i_B\rangle$$

De plus, quitte à changer les $|i_A\rangle$, on peut supposer que $(|i_B\rangle)$ est la base canonique. En effet on a

$$\sum_{i=0}^{3} |i_A\rangle \otimes (U|i_B\rangle) = \sum_{i=0}^{3} (U^t|i_A\rangle) \otimes |i_B\rangle$$

On en déduit donc que la

$$P(\text{Bob mesure 0}) = P(\text{Bob mesure 1}) = 1/2$$

Ici il n'y a pas de problème posé par la mesure que fait Bob lors de la vérification qui peut changer les probabilités concernant le bit contenant le résultat vu que la vérification est toujours bonne et donc la projection sur la paire EPR n'affecte pas l'état.

On a donc démontré que si Alice ne veut pas se faire détecter en train de tricher il faut qu'elle soit honnête. Cette propriété est importante si l'on accorde par exemple à un tricheur un grosse pénalité. Notons que si Bob triche, Alice ne peut pas du tout le detecter.

Méthodes de triche On peut imaginer par exemple d'essayer de tricher en séparant les deux paires $1, 1'$ et $2, 2'$ mais en ne mettant pas exactement des paires EPR. On peut donc avoir

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \otimes a'|00\rangle + b'|01\rangle + c'|10\rangle + d'|11\rangle$$

On obtient alors une probabilité de passer la vérification de

$$P(\text{passer le test}) = \frac{1}{2}(\frac{|a+d|^2}{2} + \frac{|a'+d'|^2}{2})$$

et la probabilité que le résultat soit 0 est

$$P(\text{b=0}) = \frac{1}{2}(\frac{|a+d|^2}{2}\frac{|a'|^2+|c'|^2}{2} + \frac{|a'+d'|^2}{2}\frac{|a|^2+|c|^2}{2})$$

car Alice peut envoyer 0 à la dernière étape même si elle n'a pas 0.

La contrainte qu'on a est bien sûr $|a|^2 + |b|^2 + |c|^2 + |d|^2 = |a'|^2 + |b'|^2 + |c'|^2 + |d'|^2 = 1$. On voit donc qu'on peut supposer que $b = b' = 0$ et que tous ces coefficients sont réels. On peut alors supposer aussi que $c = c' = 0$. On veut donc maximiser

$$P(\text{b=0}) = \frac{1}{8}((a+d)^2a'^2 + (a'+d')^2a^2)$$

En effectuant une résolution numérique on obtient que $P(\text{b=0}) \leq 0.728$. On pourrait croire que c'est le mieux que l'on puisse obtenir en pensant qu'intriquer les deux paires ne sert à rien. C'est ce qu'on a essayé de démontrer; mais ceci s'est averé faux lorsqu'on a trouvé une méthode qui permet à Alice d'obtenir le résultat qu'elle souhaite avec une probabilité 0.75 de réussite. On utilise ici le fait que la vérification de Bob fait une projection et peut influer sur les qubits qui donnent le bit aléatoire.

Une méthode qui permet à Alice d'obtenir $b = 0$ à 0.75 est de préparer l'état

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle|\phi^+\rangle + |\phi^+\rangle|00\rangle)$$

et d'envoyer à Bob le deuxième et le quatrième qubits ($1'$ et $2'$) ensuite pour la vérification elle lui envoie le qubit correspondant. Vu que l'état est symétrique en $1, 1'$ et $2, 2'$, on peut faire le calcul en supposant qu'on vérifie $1, 1'$. On a alors

$$\begin{aligned} P(\text{Alice passe le test}) &= \langle\psi|(|\phi^+\rangle\langle\phi^+|_{11'} \otimes I_{22'})|\psi\rangle \\ &= \frac{5}{6} \end{aligned}$$

L'état après la vérification est $\sqrt{\frac{6}{5}}\frac{1}{\sqrt{3}}(\frac{1}{\sqrt{2}}|\phi^+\rangle|\phi^+\rangle + |\phi^+\rangle|00\rangle) = |\phi^+\rangle\Big((\sqrt{\frac{2}{5}} + \sqrt{\frac{1}{10}})|00\rangle + \sqrt{\frac{1}{10}}|11\rangle\Big)$.
On a donc la probabilité de mesurer 0 sur le qubit $2'$ qui vaut $\frac{9}{10}$. Ce qui donne donc

$$P(\text{b=0}) = \frac{5}{6}\frac{9}{10} = \frac{3}{4}$$

Preuve que le biais est $\leq \frac{\sqrt{2}}{4}$ Soit $|\psi\rangle$ l'état correspondant à la communication.

Supposons que Alice veut obtenir 0, on a alors

$$P(\text{Alice gagne}) = P(\text{Alice passe le test } \textbf{et} \text{ Bob mesure 0 après vérification})$$

Or on a

$$\begin{aligned} P(\text{Alice passe le test}) &= \frac{1}{2}\langle\phi^+|tr_{22'}|\psi\rangle\langle\psi||\phi^+\rangle + \frac{1}{2}\langle\phi^+|tr_{11'}|\psi\rangle\langle\psi||\phi^+\rangle \\ &= \frac{1}{2}F(tr_{22'}|\psi\rangle\langle\psi|, |\phi^+\rangle\langle\phi^+|) + \frac{1}{2}F(tr_{11'}|\psi\rangle\langle\psi|, |\phi^+\rangle\langle\phi^+|) \\ &\leq \frac{1}{2}F(tr_{122'}|\psi\rangle\langle\psi|, \frac{1}{2}Id) + \frac{1}{2}F(tr_{121'}|\psi\rangle\langle\psi|, \frac{1}{2}Id) \end{aligned}$$

On a aussi :

$$P(\text{Alice passe le test et Bob mesure 0 après la vérification}) \leq P(\text{Bob mesure 0 sans vérification})$$

En effet on a $\langle\psi|(I_1 \otimes |0\rangle\langle 0| \otimes |\phi^+\rangle\langle\phi^+|)|\psi\rangle \leq \langle\psi|(I_1 \otimes |0\rangle\langle 0| \otimes I_{22'})|\psi\rangle$ puisque $I_{22'}$ peut se décomposer comme la somme de $|\phi^+\rangle\langle\phi^+|$ et d'autres matrices densités.

$$\begin{aligned} P(\text{Bob mesure 0 sans vérification}) &= \frac{1}{2}\langle 0|tr_{122'}|\psi\rangle\langle\psi||0\rangle + \frac{1}{2}\langle 0|tr_{121'}|\psi\rangle\langle\psi||0\rangle \\ &= \frac{1}{2}F(tr_{122'}|\psi\rangle\langle\psi|, |0\rangle\langle 0|) + \frac{1}{2}F(tr_{121'}|\psi\rangle\langle\psi|, |0\rangle\langle 0|) \end{aligned}$$

Donc

$$\begin{aligned} P(\text{Alice gagne}) &\leq \frac{1}{2}\Big(P(\text{Alice passe le test}) + P(\text{Bob mesure 0 sans vérification})\Big) \\ &\leq \frac{1}{4}\Big(F(tr_{122'}|\psi\rangle\langle\psi|, 1/2Id) \\ &\quad + F(tr_{122'}|\psi\rangle\langle\psi|, |0\rangle\langle 0|) \\ &\quad + F(tr_{121'}|\psi\rangle\langle\psi|, 1/2Id) \\ &\quad + F(tr_{121'}|\psi\rangle\langle\psi|, |0\rangle\langle 0|)\Big) \\ &\leq \frac{1}{4}(2 + 2\sqrt{F(|0\rangle\langle 0|, 1/2Id)}) \\ &= \frac{1}{2} + \frac{\sqrt{2}}{4} \\ &\simeq 0.85 \end{aligned}$$

A la troisième ligne on a utilisé le lemme 1

Analyse numérique On essaie de raisonner avec des coefficients et utiliser des outils de calcul formel pour optimiser la fonction qui donne la probabilité qu'Alice gagne. Alice prépare l'état $|\psi\rangle$ à 4 qubits. On suppose que si Bob lui demande la première paire Alice n'effectue pas de transformation et que s'il demande la deuxième, Alice applique une transformation unitaire $U = U_{12}$ à $|\psi\rangle$ avant d'envoyer la deuxième paire.

On a la probabilité qu'Alice convainc Bob avec 0 vaut

$$\begin{aligned} P &= 1/2(|\langle\psi|\phi^+00\rangle|^2 + |\langle\psi|\phi^+10\rangle|^2 + |\langle U\psi|00\phi^+\rangle|^2 + |\langle U\psi|00\phi^+\rangle|^2) \\ &= 1/2(|\langle\psi|\phi^+00\rangle|^2 + |\langle\psi|\phi^+10\rangle|^2 + |\langle\psi|U^*00\phi^+\rangle|^2 + |\langle\psi|U^*10\phi^+\rangle|^2) \end{aligned}$$

Pour alléger les notations on note U pour U^*. On veut donc calculer le maximum sur tous les $|\psi\rangle$ et tous les U possibles de cette expression. On peut donc supposer que $|\psi\rangle$ est dans l'espace engendré par ces 4 vecteurs. On peut donc écrire

$$|\psi\rangle = a|\phi^+00\rangle + b|\phi^+10\rangle + cU|00\phi^+\rangle + dU|10\phi^+\rangle$$

On va noter par la suite $|\phi\rangle_i$ ces vecteurs. On s'interesse aux relations d'orthogonalité entre ces vecteurs. On a $|\phi\rangle_{1,3}$ orthogonaux à $|\phi\rangle_{2,4}$, on peut voir ceci en écrivant ces vecteurs dans l'ordre 121'2' pour voir sur qui agit le U.

La relation qu'on a entre a, b, c et d est donc

$$a^2 + c^2 + 2\Re(ac\langle\phi_1|\phi_3\rangle) + b^2 + d^2 + 2\Re(bd\langle\phi_2|\phi_4\rangle) = 1$$

Et la quantité qu'on souhaite maximiser sous cette contrainte est

$$\begin{aligned} A &= |a + c\langle\phi_3|\phi_1\rangle|^2 + |(c + a\langle\phi_1|\phi_3\rangle)|^2 + |b + d\langle\phi_4|\phi_2\rangle|^2 + |(d + b\langle\phi_2|\phi_4\rangle)|^2 \\ &= 1 + 2\Re(ac\langle\phi_1|\phi_3\rangle) + 2\Re(bd\langle\phi_2|\phi_4\rangle) + |\langle\phi_3|\phi_1\rangle|^2(a^2 + c^2) + |\langle\phi_4|\phi_2\rangle|^2(b^2 + d^2) \end{aligned}$$

Notons aussi que $|\langle\phi_1|\phi_3\rangle| \leq 1/2$ et $|\langle\phi_2|\phi_4\rangle| \leq 1/2$. Cette optimisation est difficile même numériquement mais celle-ci se simplifie et devient faisable numériquement lorsqu'on fait des simplifications, par exemple si on suppose que $U = Id$ ou que $b = d = 0$ et on obtient 0.75. C'est en effectuant ces simplifications qu'il a été possible de trouver plusieurs techniques de triche à 0.75.

La preuve finale La preuve finale est très courte, elle utilise la notion de fidélité.

$$\begin{aligned} P(\text{b=0}) &= \frac{1}{2}\Big(F(tr_2(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{2'}|\phi^+\rangle\langle\phi^+|_{11'}) + F(tr_1((U|\psi\rangle\langle\psi|)U^*, |0\rangle\langle 0|_{1'}|\phi^+\rangle\langle\phi^+|_{22'})\Big) \\ &\leq \frac{1}{2}\Big(F(tr_{12}(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{2'} \otimes 1/2Id_{2'}) + F(tr_{12}(U|\psi\rangle\langle\psi|U^*), |0\rangle\langle 0|_{1'} \otimes 1/2Id_{2'})\Big) \\ &= \frac{1}{2}\Big(F(tr_{12}(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{2'} \otimes 1/2Id_{1'}) + F(tr_{12}(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{1'} \otimes 1/2Id_{2'})\Big) \\ &\leq \frac{1}{2}(1 + \sqrt{F(|0\rangle\langle 0|_{1'} \otimes 1/2Id_{2'}, 1/2Id_{1'} \otimes |0\rangle\langle 0|_{2'})}) \end{aligned}$$

L'inégalité de la dernière ligne est justifiée par le lemme 1 Calculons

$$\begin{aligned} \sqrt{F(|0\rangle\langle 0|_{1'} \otimes 1/2Id_{2'}, 1/2Id_{1'} \otimes |0\rangle\langle 0|_{2'})} &= tr\Big(\sqrt{(\frac{1}{\sqrt{2}}|0\rangle\langle 0|_{1'} \otimes Id_{2'})(\frac{1}{2}Id_{1'} \otimes |0\rangle\langle 0|_{2'})(\frac{1}{\sqrt{2}}|0\rangle\langle 0|_{1'} \otimes Id_{2'})}\Big) \\ &= \frac{1}{2}tr\Big(\sqrt{|0\rangle\langle 0|_{1'}|0\rangle\langle 0|_{2'}}\Big) \\ &= \frac{1}{2}tr(|00\rangle\langle 00|_{1'2'}) \\ &= \frac{1}{2} \end{aligned}$$

On a donc

$$P(\text{b=0}) \leq \frac{3}{4}$$

On a donc démontré que le protocole cité a pour biais $\frac{1}{4}$.

4.3 Version faible

On peut imaginer que Alice veut toujours obtenir le résultat 1 et Bob le résultat 0. C'est à dire qu'à l'issue du tirage on peut dire qui a gagné. C'est ce qu'on appelle le tirage à pile ou face faible. Ceci permet de faire subir une vérification à celui qui gagne et donc améliorer le biais du protocole. Les meilleurs protocoles obtiennent des biais meilleurs que ce qu'on connait pour la version forte. Par exemple jusqu'en 2005, le meilleur protocole avait un biais de $\frac{1}{\sqrt{2}} - \frac{1}{2}$, mais on ne savait pas si la borne inférieure de Kitaev s'appliquait aussi à la version faible. Ce doute prit fin lorsque Mochon publia dans [7] un protocole qui a un biais $\frac{1}{6}$ mais ce protocole n'est pas du tout évident et il fait appel à la programmation semi-définie.

Par exemple pour notre protocole utilisant des paires EPR, on ne peut rien changer pour Alice mais on peut dire que si Bob gagne, il doit renvoyer le qubit non utilisé pour qu'Alice vérifie qu'il n'a pas été mesuré. Si on suppose que Bob ne fait que des mesures de 1 ou 2 qubits alors le biais devient $\frac{1}{8}$, mais Bob peut appliquer une transformation unitaire sur ces bits et peut être d'autres puis effectuer un certain nombre de mesures à la fin, peut être qu'il est possible de tricher avec plus de $\frac{1}{8}$, l'étude reste à faire. Pour améliorer le biais d'Alice on peut faire un protocole à 3 paires. Le biais d'Alice peut se calculer de la même façon.

$$\begin{aligned} P(\text{Alice gagne}) \leq \frac{1}{3}\Big(& F(tr_{123}(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{1'} \otimes 1/4 Id_{2'3'}) \\ & + F(tr_{123}(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{2'} \otimes 1/2 Id_{1'3'}) \\ & + F(tr_{123}(|\psi\rangle\langle\psi|), |0\rangle\langle 0|_{3'} \otimes 1/4 Id_{1'2'})\Big) \end{aligned}$$

en notant ces termes a, b, c on a

$$P(\text{Alice gagne}) \leq \frac{1}{3}(\frac{a+b}{2} + \frac{a+c}{2} + \frac{b+c}{2})$$

Or par le lemme 1 on a $a + b \leq 1 + 1/4$ donc

$$P(\text{Alice gagne}) \leq \frac{1}{2} + \frac{1}{8}$$

Donc Alice a un biais de $\frac{1}{8}$.

4.4 Résultats connus

Voici un récapitulatif des résultats connus sur le sujet à ce jour sur le problème du tirage à pile ou face.

	borne inférieure	**meilleur biais connu**
normal	$\frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.207$ (Kitaev)	0.25
faible	?	$\frac{1}{6}$

Conclusion

Les problèmes reliés qui restent ouverts donc:

- Existe-t'il un protocole de tirage à pile ou face avec biais $\frac{1}{\sqrt{2}} - \frac{1}{2}$?
- Pour la version faible, peut-on avoir un biais $\leq \frac{1}{6}$?
- Comment faire pour tirer plusieurs bits, l'étude devient plus difficile vu qu'un tricheur peut intriquer les différentes exécutions d'un protocole ?

La plus grande partie du stage a donc été consacrée à l'étude de ce protocole EPR vu qu'il n'existait pas de preuve pour ce résultat. Pour cela il m'a fallu assimiler les méthodes utilisées pour ce type de raisonnement. De plus la nature un peu particulière de ce protocole a rajouté une difficulté pour bien exprimer les différentes probabilités. De sorte qu'à la fin du stage, quand j'ai revisé les premières preuves partielles que j'avais établies, je me suis rendu compte qu'il y avait des erreurs. Il resterait maintenant à appliquer ce protocole à la version faible du problème de tirage à pile ou face.

Je remercie l'équipe Algorithmique et Compléxité du LRI pour m'avoir accueilli pendant ce stage et en particulier mon maitre de stage Frédéric Magniez pour son aide tout au long du stage, ainsi que Thomas Vidick étudiant en DEA pour ses remarques utiles.

Références

[1] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences*, 2002.

[2] Andris Ambainis. Quantum bit commitment and coin flipping. *http://www.tcs.hut.fi/Research/Crypto/-minicourses/ambainis2002-3.ppt*, 2002.

[3] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. *34th Symp. on Found. of Computer Sci*, 1993.

[4] Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 2004.

[5] Hoi-Kwong Lo and H. F. Chau. Why quantum bit commitment and ideal coin tossing are impossible. *quant-ph/9711065*, 1997.

[6] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *quant-ph/9605044*, 1996.

[7] Carlos Mochon. A large family of quantum coin-flipping protocols. *Physical review*, 2005.

[8] A. Nayak and P. Shor. Bit-commitment-based quantum coin flipping. *Physical review*, 2003.

[9] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2000.