UNIVERSITÉ DU QUÉBEC À MONTRÉAL

PROTOCOLES QUANTIQUES ET RELATIVISTES DE MISE EN GAGE

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN INFORMATIQUE

PAR

HASSENE BADA

FÉVRIER 2009

REMERCIEMENTS

Je tiens tout d'abord à adresser mes vifs remerciements à mes directeurs de recherche, Gilles Brassard et Pierre Bouchard.

Merci à Gilles pour son aide et son orientation qui ont permis l'élaboration de ce travail, merci également pour la qualité de son enseignement.

Merci à Pierre Bouchard d'avoir accepté de superviser ce travail.

J'adresse également mes remerciements à mes amis, Abdeljalil et Méziane.

TABLE DES MATIÈRES

RÉSUMÉ vi

INTRODUCTION 1

CHAPITRE I
OUTILS MATHÉMATIQUES POUR LA CRYPTOGRAPHIE QUANTIQUE . 11

1.1 Espace de Hilbert 11

1.1.1 Produit scalaire 12

1.1.2 Base orthonormale 14

1.1.3 Représentation des kets, des bras et des opérateurs 14

1.1.4 Base de calcul 15

1.1.5 Produit tensoriel 15

1.1.6 Opérateurs 17

1.1.7 Relations caractéristiques d'une base orthonormée 24

CHAPITRE II
THÉORÈMES À LA BASE DE LA CRYPTOGRAPHIE QUANTIQUE 25

2.1 État 25

2.2 Qubit 25

2.2.1 États intriqués 27

2.3 Opérateur de densité 28

2.4 Trace partielle 31

2.4.1 Purification 33

2.5 Décomposition de Schmidt [68] 34

2.6 Théorème GHJW [38, 29] 35

2.7 Évolutions des systèmes quantiques 37

2.7.1 Représentation de Kraus 39

2.8 Mesure 40

2.9 Mesures généralisées 44

2.10 Réalisation d'une mesure généralisée quelconque par une transformation unitaire et une mesure projective 45

2.11 Théorème de non-clonage 48

2.12 Distance 49

2.13 Fidélité 55

2.13.1 Théorème d'Ulmann [75, 41] 56

2.14 Pseudo opérations 58

CHAPITRE III
MISE EN GAGE 63

3.1 L'impossibilité d'une mise en gage non relativiste liante et camouflante en même temps 66

3.1.1 Mise en gage classique 66

3.1.2 Mise en gage quantique 67

3.1.3 Théorème de l'impossibilité 68

3.2 Degré de lien et de camouflage 71

3.2.1 Cas général 71

3.2.2 Cas où tout le système initial provient d'Alice 78

3.2.3 Mise en gage de purification 84

3.2.4 Exemples de protocoles saturant les bornes sur $C^{\max}$ et $G^{\max}$ quand tout le système intial provient d'Alice 86

3.3 Mise en gage quantique sensible à la tricherie (cheat-sensitive) 91

CHAPITRE IV
MISE EN GAGE RELATIVISTE 96

4.1 Une mise en gage classique temporairement sécuritaire 99

4.2 Une mise en gage classique inconditionnelement sécuritaire non pratique . . 100

4.3 Une mise en gage classique inconditionnelement sécuritaire pratique 105

4.3.1 Technique de Rudich pour la mise en gage 105

4.3.2 Utilisation de la technique de Rudich pour la réalisation d'une mise en gage relativiste pratique 111

4.4 Étude de la sécurité des protocoles relativistes contre les attaques quantiques 113

CONCLUSION 120

BIBLIOGRAPHIE 122

RÉSUMÉ

Dans la vie, on peut avoir besoin de communiquer avec des parties auxquelles on ne fait pas confiance, d'où l'importance de systèmes capables de contrôler ce type de communications. Des systèmes peuvent garantir, par exemple, un ballottage secret, des ventes aux enchères secrètes, des levées d'impôt tout en conservant l'intimité, l'authentification à distance à un ordinateur, l'aide anonyme de la police dans leurs enquêtes, etc.

La cryptographie peut aider, au moins, dans quelques cas parmi ceux-ci, par la régularisation du flux d'information de telle manière qu'on n'aura plus besoin de faire confiance à l'autre partie. On fera confiance, seulement, aux systèmes cryptographiques utilisés. Une primitive, appelée mise en gage, est d'une importance suprême dans la cryptographie bipartite, où deux parties qui ne se font pas confiance essayent tout de même d'accomplir un calcul commun sur des données privées (calculer une fonction publique de leurs données secrètes). Cette primitive va être l'objet de ce mémoire. On va expliquer jusqu'à quel point on peut accomplir des taches cryptographiques de façon inconditionnellement sécuritaire, sous la seule hypothèse que la mécanique quantique et la relativité restreinte sont valides. Ce mémoire est largement basé sur les travaux de Mayers [52,53,54,55], Lo et Chau [49,50], Brassard, Crépeau, Mayers et Salvail [15], Spekkens et Rudolph [73], Hardy et Kent [35], Ishizaka [39] et Kent [43,44]. Il fait à la fois une présentation de la cryptographie quantique et une synthèse des travaux essentiels concernant les protocoles de mise en gage quantiques et relativistes.

Nous allons donc commencer par une introduction sur l'histoire de la cryptographie classique et son prolongement naturel à ses homologues, quantique et relativiste, qui permettent d'obtenir de meilleurs résultats. Ensuite, nous introduirons un certain nombre d'outils mathématiques utiles à la description de la cryptographie quantique. Nous y présenterons également les preuves de plusieurs résultats à la base de la cryptographie quantique, tels que la décomposition de Schmidt, la purification, le théorème GHJW, le théorème d'Ulmann, le théorème de non-clonage, le théorème de la représentation de Kraus, etc. Nous discuterons aussi des concepts de base de l'informatique quantique, comme la mesure projective et généralisée, l'évolution des systèmes quantiques non isolés, la trace partielle, l'opérateur de densité, etc. Nous aborderons le protocole de la mise en gage proprement dit en exposant en détail la preuve du théorème de l'impossibilité de Mayers, Lo et Chau. Nous y présentons également le travail de Rudolph et Spekkens qui ont calculé les degrés optimaux de lien et de camouflage qui peuvent être obtenus simultanément dans tout protocole de mise en gage quantique non relativiste. Il s'agit-là d'une caractéristique qu'aucun protocole classique non relativiste ne peut assurer. Un autre type de sécurité pour ce protocole est étudié aussi, c'est celui

de la mise en gage sensible à la tricherie "*cheat sensitive*" pour lequel on croyait que le protocole quantique de Hardy et Kent fonctionnait alors que Ishizaka a démontré récemment que ce n'est pas le cas. Pire, il a même remis en question toute possibilité de réaliser ce type de sécurité en ce basant sur l'utilisation du protocole du tir à pile ou face comme sous-protocole. La cryptographie relativiste fera l'objet de notre dernier chapitre. Nous commencerons par montrer comment la théorie de la relativité restreinte, et donc l'impossibilité qu'un signal puisse se déplacer à une vitesse supérieur à celle de la lumière, peut être exploitée pour construire un protocole de mise en gage temporairement sécuritaire, c'est celui de Brassard, Crépeau, Mayers et Salvail. Nous présenterons ensuite le premier protocole relativiste d'une mise en gage continuellement sécuritaire, celui de Kent, et la preuve de sa sécurité. Ce protocole ne peut malheureusement pas être implémenté, même s'il est théoriquement sûr. Nous terminerons cette étude par une description d'un deuxième protocole relativiste du même auteur, qui va remédier aux problèmes liés à l'impossibilité pratique du premier protocole. Les preuves de la sécurité de ce dernier contre les attaques classiques et quantiques du type Mayers, Lo et Chau vont être abordées.

Mots-clés : informatique quantique, mise en gage quantique, mise en gage quantique sensible à la tricherie, mise en gage relativiste.

INTRODUCTION

L'histoire de la cryptographie est déjà longue (Le plus vieux document crypté connu remonte au XVI^{e} siècle av.J.-C.). Un des premiers personnages connus pour avoir utilisé des codes mathématiques est Jules César. Son code consiste à utiliser un alphabet où chaque lettre d'un message est remplacée par la lettre qui la suit de trois positions. Une simple généralisation de cette technique est de remplacer chaque lettre par la lettre qui la suit d'un certain nombre fixé de positions dans l'alphabet. Si, par exemple, l'alphabet contient $k = 26$ lettres, alors on a 26 codes possible. En faisant une correspondance entre les caractères de notre alphabet et les valeurs $0, 1, \ldots, k-1$, le nombre i se codera avec la clef j comme $i \rightarrow (i+j) \bmod k$, pour $i = 0, 1, .., k-1$. Par exemple, si on code le mot « SECRET » à l'aide de la valeur $j = 3$, la clef de César, l'alphabet est décalé de manière à commencer à la lettre D. Ainsi, si on décale le début de l'alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ de 3 lettres, on obtient DEFGHIJKLMNOPQRSTUVWXYZABC d'où D=A, E=B, F=C, etc. Avec ce procédé, le texte en clair «SECRET» est crypté en «VHFUHW». Pour autoriser un autre utilisateur à lire le texte chiffré, on lui indique que la valeur de la clef est égale à 3.

Évidemment, ce code est extrêmement fragile, car il peut être décodé par une recherche exhaustive. Mais, cette méthode met en lumière le mécanisme de la cryptographie usuelle. Une intéressante variante du chiffrement de Jules César est lorsque les k lettres de l'alphabet sont remplacées par une de leurs $k!$ permutations possibles. La clef dans ce cas est la permutation utilisée, et le nombre de clefs est $26! > 4.10^{26}$. Bien que le déchiffrement par une recherche exhaustive soit très difficile même pour un ordinateur, cette variante peut être facilement déchiffrée par une méthode qui utilise les fréquences d'apparition des lettres dans les textes.

Claude Shannon [69, 70] a démontré que le seul système cryptographique inconditionnellement sûr, indépendamment de toute hypothèse sur la capacité de calcul de l'adversaire, est celui inventé en 1917 par Gilbert Vernam [76] et Joseph Mauborgne, ce qui exige une clef secrète aléatoire aussi longue que le message, cette clef ne devant être utilisée qu'une seule fois. Donc, dans le scénario où une personne désire envoyer un message à une autre, ils doivent partager au préalable une clef secrète aléatoire aussi longue que le message à envoyer. Deux personnes peuvent, bien entendu, établir une nouvelle clef pour chaque nouveau message à chiffrer, mais le problème est qu'elles doivent transmettre celle-ci sans que d'autres personnes en prennent connaissance. Cette clef ne peut donc pas être envoyée par un canal public qui est vulnérable à toutes sortes d'interceptions passives. Le théorème de Shannon reporte donc la sécurité de la communication sur la sécurité du partage de la clef.

C'est à ce stade qu'intervient la cryptographie quantique : elle permet à deux parties, appelées Alice et Bob, d'échanger une clef secrète, avec une sécurité garantie par les principes mêmes de la mécanique quantique; cette clef pourra ensuite être utilisée pour encrypter le «vrai» message avec une sécurité démontrée mathématiquement.

L'idée d'utiliser la mécanique quantique pour mieux accomplir des tâches cryptologiques est due à Stephen Wiesner et son article de 1970 : «congugate coding» [77] où il a montré comment le principe d'incertitude d'Heisenberg peut être considéré comme une ressource plutôt que comme une limitation, et cela en l'utilisant pour construire des billets de banque impossibles à contrefaire et aussi pour implémenter une primitive de transfert équivoque. Une décennie après (1979), Charles Bennett et Gilles Brassard sont revenus sur l'idée de Wiesner et après une série de publications, ils ont fini par publier le premier article qui donne une description complète d'un protocole quantique de distribution de clefs inconditionnellement sécuritaire [9] (c-à-d. une sécurité qui ne dépend d'aucune hypothèse à part la validité de la mécanique quantique). Ce protocole permet à Alice et Bob de produire et partager une clef secrète par la transmission de photons polarisés. Ils ont utilisé la polarisation des photons pour transmettre de l'information et non pour la stocker, ce qui est une idée plus utile et plus réaliste que celle du stockage

des photons tout en conservant leurs polarisations pendant des durées assez grandes, qui reste, jusqu'à ce jour, un problème technologiquement insurmontable.

L'impossibilité du décodage de l'information transmise par une tierce partie, appelée Ève, est assurée par le théorème *d'incertitude d'Heisenberg*. Ceci entraîne aussi le fait qu'on ne peut cloner une particule, car on ne peut jamais connaître complètement son état quantique (théorème de «non-clonage» [10, 24, 78]). Le théorème de «non-clonage» affirme qu'un état quantique inconnu ne peut être copié. On démontre en effet qu'à moins que l'on connaisse d'avance l'état du photon, il nous est impossible de reproduire cet état, c'est-à-dire d'en faire un clone. Autrement dit, le fait d'essayer d'observer un photon dont on ignore l'état le modifie sans que, par après, on puisse le remettre dans son état initial ou encore en produire un clone.

C'est en 1989 que la cryptographie quantique fit son premier pas dans le monde expérimental suite à un prototype de distribution quantique de clefs réalisé par Bennett, Bessette, Brassard, Salvail et Smolin [8]. Depuis, d'autres progrès ont suivi, tant sur les plans expérimentaux [17, 51] que théoriques.

Le champ de la cryptographie ne se limite plus à chiffrer des messages secrets depuis que Diffie et Hellman [25] ont suggéré une nouvelle direction pour celle-ci. Leur idée a ouvert la voie d'une nouvelle cryptographie ne necessitant plus d'échange de clef préalable (clef privée). Ils ont développé des systèmes cryptographiques à clefs publiques. Leur méthode utilise une clef pour chiffrer, une autre pour déchiffrer et emplois une fonction à sens unique. Cette fonction permet de calculer facilement la clef de chiffrement en connaissant la clef de déchiffrement. Par contre, l'opération réciproque est pratiquement impossible en un temps raisonnable. Un des premiers parmi ces cryptosystèmes, RSA [66], est basé sur la théorie des nombres et plus précisément la difficulté présumée de factorisation des grands entiers. Dans ces nouveaux systèmes cryptographiques, Alice et Bob peuvent communiquer secrètement même s'ils ne partagent pas de clef secrète au préalable. L'inconvénient majeur de ce type de protocoles est qu'ils reposent sur des problèmes dont la comple-xité n'est pas formellement prou-

vée ou plus précisement, qui ne l'est pas encore. C'est la raison pour laquelle on parle d'hypothèse calculatoire, une hypothèse que ces problèmes sont intrinsèquement difficiles.

Bien que la difficulté de ces problèmes ne soit pas mise en doute pour le moment, il n'existe aucune assurance qu'il en sera toujours ainsi. En fait, il existe même des preuves du contraire : par exemple, il y a quelques années, Peter Shor [71] a montré qu'avec un ordinateur quantique on peut factoriser efficacement, ce qui rend la sécurité du cryptosystème RSA liée étroitement à la technologie utilisée. Si l'ordinateur quantique voit le jour, RSA sera facilement brisé.

Si le calcul quantique exige la construction hypothétique d'un ordinateur quantique, les protocoles quantiques de la cryptographie, par contre, peuvent déjà être concrètement utilisés. Malgré cela, la famille des protocoles quantiques inconditionnellement sécuritaires est très restreinte.

Il y a d'autres problèmes en cryptographie pour lesquels on peut espérer avoir de meilleurs résultats dans le modèle quantique, par exemple ceux de la mise en gage (bit commitment) et du tir à pile ou face à distance.

Supposons qu'Alice souhaite prouver à Bob que le résultat d'un prochain match de hockey est arrangé d'avance et qu'elle connaît l'équipe qui va l'emporter, mais qu'elle ne souhaite pas la lui révéler immédiatement de peur qu'il utilise cette information dans des paris pour s'enrichir. Une solution qui s'offre à eux est d'utiliser un coffre-fort. Alice met le résultat dans le coffre-fort, conserve la clef et donne le coffre-fort à Bob. Quand les deux parties sont d'accord, Alice donne la clef à Bob, Bob ouvre le coffre-fort et lit le résultat. Ainsi, Bob ne peut lire le résultat sans la permission d'Alice, et Alice ne peut le modifier sans que Bob s'en aperçoive. Un tel protocole est appelé protocole de mise en gage. Il se compose de deux phases : 1-la phase de la mise en gage où Alice s'engage sur la valeur d'un bit; 2-la phase de la révélation, qui est facultative, où Bob vérifie la valeur du bit mis en gage. Pour qu'un protocole de mise en gage soit sécuritaire, il doit être liant, c'est-à-dire qu'après le choix du bit mis en gage, sa valeur est fixée

et Alice ne peut la modifier sans que Bob s'en aperçoive, et il doit être camouflant, c'est-à-dire que Bob ne doit rien apprendre au sujet du bit choisi. En résumé, la mise en gage s'accomplit par la transmission d'une information à Bob qui doit être suffisante pour fixer le bit et insuffisante pour que Bob découvre sa valeur. Dans le cas de notre exemple du coffre-fort, ces deux critères sont supposés présents, car Bob ne peut lire le résultat sans la permission (la clef) d'Alice, et Alice ne peut le modifier sans que Bob ne s'en aperçoive.

La mise en gage est une importante primitive dans la construction des preuves et des arguments [16, 31] sans divulgation de connaissance (zero-knowledge) et de la primitive universelle, transfert inconscient, du calcul bipartite sécurisé [46]. Dans le modèle de la cryptographie classique non relativiste où il n'y a pas de limite sur les vitesses d'interactions (on ne prend pas en considération les principes de la théorie quantique ni ceux de théorie de la relativité), il est impossible d'avoir une mise en gage inconditionnellement liante et camouflante à la fois [12], mais on peut avoir l'une des deux tandis que l'autre est «difficile à briser». Une mise en gage inconditionnellement liante et calculatoirement camouflante peut être réalisée grâce à des fonctions à sens unique [36, 62], des fonctions qu'on peut calculer efficacement, mais dont l'inverse est difficile à calculer; par contre une mise en gage inconditionnellement camouflante et calculatoirement liante peut être réalisée par des permutations à sens unique [63] ou encore n'importe quelle fonction de hachage dont les collisions sont calculatoirement trop difficiles à repérer [34]. On peut éviter l'hypothèse calculatoire dans la construction de la mise en gage par d'autres types d'hypothèses. Par exemple, il est possible d'effectuer une mise en gage à la fois inconditionnellement liante et camouflante sous l'hypothèse de l'existence d'un canal binaire symétrique dont le taux d'erreur est connu précisément [22] ou si le receveur possède un espace mémoire limité [18]. Dans le cas du calcul multipartite [7, 19, 31], une mise en gage inconditionnellement liante et camouflante peut être réalisée au moyen du modèle du secret mis en partage de façon vérifiable [26].

À ce stade, la question qui se pose est celle-ci : la mécanique quantique peut-elle sauver la primitive de mise en gage comme elle l'a déjà fait pour le protocole de

distribution de clefs? La réponse est malheureusement non.

La première tentative pour réaliser une mise en gage quantique inconditionnellement sécuritaire était implicite dès 1984 dans le travail de Bennett et Brassard [9]. Mais dans le même article [9], ils ont montré comment la mécanique quantique rend ce protocole sans valeur. Un autre protocole pour implémenter une mise en gage quantique est celui de Brassard et Crépeau [13], amélioré et généralisé par Brassard, Crépeau, Jozsa et Langlois au cas où des erreures peuvent être transmises [14]. On croyait à la sécurité de ce dernier jusqu'à ce que Mayers [52, 53], étudiant de Brassard à l'époque, démontre qu'il n'en est rien. Par la suite, Mayers [54, 55] a démontré qu'il est impossible d'avoir un protocole de mise en gage quantique inconditionnellement sécuritaire. Une version faible (moins générale) de ce résultat a été indépendamment trouvée par Lo et Chau [49] pour être généralisée ensuite par les mêmes auteurs [50]. Le point faible de tous les protocoles quantiques non relativistes, d'après Mayers, Lo et Chau, est que si Bob ne peut pas extraire toute (ou une partie de) l'information sur le bit mis en gage, Alice peut (ou peut avec une grande probabilité) changer le bit mis en gage de 0 à 1 (et l'inverse) sans être détectée.

Bien que les lois de la mécanique quantique nous ne permettent pas de réaliser une mise en gage parfaitement sécuritaire (ou même arbitrairement sécuritaire), elles nous permettent en revanche de réaliser une mise en gage quantique partiellement liante et partiellement camouflante à la fois [1, 73]. Cela veut dire que Bob ne peut pas savoir tout sur le bit mis en gage avant la révélation et qu'Alice ne peut pas révéler ce qui lui plaît sans courir le risque d'être détectée par Bob si elle triche. Une caractéristique qu'aucun protocole classique non relativiste ne peut assurer.

Un autre protocole spécifique au modèle quantique est la mise en gage quantique sensible à la tricherie (cheat sensitive) [35]. Dans ce type de protocole, Alice ne peut révéler ce qui lui plaît sans courir le risque d'être détectée avec une probabilité strictement supérieure à 0 si elle triche, et toute tentative de Bob d'extraire une information sur le bit mis en gage avant la phase de révélation l'exposera à la détection avec

une probabilité strictement supérieure à 0. Malheureusement, Satoshi Ishizaka a montré récemment dans [39] que le protocole [38] n'est pas sensible à la tricherie, ce qui pose une fois encore la question de pouvoir construire ce type de protocole.

Par opposition au cas classique, il est aussi possible, dans le cas quantique, de construire des protocoles de mise en gage parfaitement camouflants et arbitrairement liants sous l'hypothèse que la taille de la mémoire quantique du receveur est limitée [23]. Dans le cas classique [18, 26] la construction d'un protocole de mise en gage sûr, dans ce modèle, n'est possible que sous l'hypothèse que l'espace mémoire du participant malhonnête est au plus une fonction quadratique de l'espace mémoire requis par le participant honnête pour accomplir le protocole. Dans le cas quantique la situation est meilleure, car aucune mémoire quantique n'est nécessaire pour le participant honnête, et un participant malhonnête nécessite une mémoire quantique de taille égale à $\frac{n}{2}$, au moins, pour pouvoir briser le protocole (n est le nombre de qubits transmis), et aucune restriction n'est faite sur la taille de la mémoire classique des participants.

On peut également implanter un protocole de mise en gage sûr sous une hypothèse calculatoire quantique [27] : l'existence de permutations à sens unique quantiques.

Tout est bien qui finit bien, Kent [43, 44] a pu concevoir un protocole classique relativiste (protocole réalisé sous l'hypothèse de la validité de la théorie de la relativité restreinte où la vitesse d'un signal ne peut dépasser celle de la lumière) de mise en gage inconditionnellement sécuritaire et qui échappe aux attaques à la Mayers. De plus il est conjecturé sécuritaire contre toutes les attaques quantiques.

Une application très importante du protocole de la mise en gage est le protocole du tir à pile ou face à distance.

Le tir à pile ou face à distance est une autre primitive cryptographique entre Alice et Bob qui ne se font pas confiance et qui essayent, tout de même, de se mettre d'accord sur un bit uniformément aléatoire, 0 ou 1. Un scénario typique est celui introduit pour la première fois par Blum [12], où Alice et Bob sont divorcés. Ils décident de répartir

leurs biens. Malheureusement, ils n'arrivent pas à se mettre d'accord : qui doit garder la voiture. Ils décident alors de tirer au sort. Mais comme ils habitent loin l'un de l'autre, ils doivent faire cela par téléphone en dépit de leur méfiance réciproque. Tout comme la mise en gage de bit, le tir à pile ou face à distance ne peut être réalisé d'une façon inconditionnellement sécuritaire dans un modèle non relativiste, qu'il soit classique [57] ou quantique [50, 56]. Cependant, il est possible d'étudier le biais ϵ qu'un protocole pourrait garantir. Un protocole de la version dite forte du pile ou face est à biais ϵ si chacune des valeurs 0 et 1 ne peut se produire qu'avec une probabilité d'au plus $\frac{1}{2} + \epsilon$, si un des participants triche. Alors que les protocoles classiques ne peuvent garantir aucun biais inférieur à $\frac{1}{2}$, la situation en environement quantique est meilleure. En effet, Ahoronov, Ta-Shma, Vazirani et Yao, [1] ont été les premiers à avoir proposé un protocole garantissant un biais $\epsilon \leq \sqrt{2} - 1 \approx 0.414$. Un résultat plus précis dans [64, 73] montre que le biais de [1] est exactement égal à $\epsilon = \frac{1}{2\sqrt{2}}$. De plus, les protocoles d'Ambainis [2] et de Rudolph et Speckkens et [73] garantissent un biais $\epsilon = \frac{1}{4}$. Le protocole de Colbeck [16] établit lui aussi un biais $\epsilon = \frac{1}{4}$ mais, en s'appuyant sur le partage d'états intriqués. Kitaev [47] a donné une majoration du biais et, grâce à la technique d'optimisation semi-définie [42], a montré qu'il était impossible d'avoir un protocole quantique de pile ou face (version forte) avec un biais strictement inférieur à $\frac{1}{\sqrt{2}} - \frac{1}{2}$. Par ailleurs, Ambainis, Buhrman, Dodis et Röhrig [3] ont donné une preuve détaillée de la borne de Kitaev. Gutoski et Watrous [32] sont arrivés au même résultat que Kitaev sans avoir recouru à l'optimisation semi-définie.

Le scénario du couple divorcé est une version dite faible du tirage. Cette version est suffisante pour résoudre des conflits entre Alice et Bob. Par exemple, Alice parie 0 et Bob 1. Puis, ils exécutent un tir à pile ou face à distance. Le gagnant est celui qui a parié sur la bonne valeur du tirage. Ainsi, si un des deux veut tricher, l'autre sait de quel côté le premier veut biaiser la probabilité du tirage, cc qui n'était pas le cas dans la version forte (on ne s'occupe pas du cas où un joueur triche pour perdre). Pour plus de détail sur cette version, lire les articles [2, 45, 59, 60, 74].

Le tir à pile ou face sensible à la tricherie (cheat-senstive) est un autre type de sécurité qu'on peut aussi étudier dans le modèle quantique [74]. Ce type de sécurité peut être utilisé s'il y a une grande pénalité en cas de découverte de la tricherie, et s'il étudie jusqu'à quel point une des deux parties peut tricher sans aucun risque d'être détectée.

Une autre variante de la version forte est celle décrite récemment par Berlín, Brassard, Bussières et Godbout [11] montrant qu'il est aussi possible de construire un protocole de pile ou face (version forte) dans des situations pratiques réelles où il existe une possibilité de perdre l'information dans le canal quantique ou dans les appareils quantiques de stockage et de mesure.

Il est facile d'implanter un protocole de la version forte du tir à pile ou face aussi sécuritaire qu'un protocole de mise en gage existant [73]. Pour ce faire, Alice s'engage sur un bit aléatoire et Bob annonce une valeur pour ce bit à Alice. Après cela, Alice révèle la valeur du bit. La valeur du tir est 0 si Bob l'a deviné correctement, et 1 sinon. Le meilleur protocole de la version forte du pile ou face existant jusqu'à maintenant n'est qu'une application du protocole de la mise en gage [2, 73].

C'est le problème de la mise en gage qui va être étudié dans ce mémoire. On va expliquer jusqu'à quel point on peut accomplir des tâches cryptographiques de façon inconditionnellement sécuritaire, sous la seule hypothèse que la mécanique quantique et la relativité restreinte sont valides. Ce mémoire est largement basé sur les travaux de Mayers [52, 53, 54, 55], Lo et Chau [49, 50], Brassard, Crépeau, Mayers et Salvail, [65], Rudolph et Spekkens [73], Hardy et Kent [38], Ishizaka [39] et Kent [43, 44]. Il fait à la fois une présentation de la cryptographie quantique et une synthèse des travaux essentiels concernant les protocoles de mise en gage quantiques et relativistes. Dans le premier chapitre, on introduit un certain nombre d'outils mathématiques utiles à la description de la cryptographie quantique. Dans le deuxième chapitre, on présentera en détail plusieurs résultats à la base de la cryptographie quantique, tels que la décomposition de Schmidt, le théorème de la purification, le théorème GHJW, le théorème d'Ulmann, le théorème de non-clonage, le théorème de la représentation de

Kraus, etc. Nous aborderons le protocole de la mise en gage à proprement parler dans le troisième chapitre, où l'on expose en détail le théorème de l'impossibilité de Mayers, Lo et Chau. Nous y présentons également le travail de Rudolph et Spekkens qui ont calculé les degrés optimaux de lien et de camouflage qui peuvent être obtenus simultanément dans tout protocole de mise en gage quantique non relativiste. On termine ce chapitre par l'étude du problème de la mise en gage sensible à la tricherie (cheat sensitive) pour lequel on croyait que le protocole quantique de Hardy et Kent fonctionnait alors que Ishizaka a démontré récemment que ce n'est pas le cas. Pire, il a même remis en question toute possibilité de réaliser ce type de sécurité en se basant sur l'utilisation du protocole du tir à pile ou face. Enfin, la cryptographie relativiste sera l'objet du quatrième chapitre. On commencera par montrer comment la théorie de la relativité restreinte, et donc l'impossibilité qu'un signal puisse se déplacer à une vitesse supérieure à celle de la lumière, peut être exploitée pour construire un protocole de mise en gage temporairement sécuritaire, c'est celui de Brassard, Crépeau, Mayers et Salvail. Nous présenterons ensuite le premier protocole relativiste d'une mise en gage continuellement sécuritaire, celui de Kent, et la preuve de sa sécurité. Ce protocole ne peut malheureusement pas être implémenté, même s'il est théoriquement sûr. Nous terminerons cette étude par une description d'un deuxième protocole relativiste du même auteur, qui va remédier aux problèmes liés à l'impossibilité d'utilisation pratique du premier protocole. Les preuves de la sécurité de ce dernier contre les attaques classiques et quantiques du type Mayers, Lo et Chau vont être abordées.

CHAPITRE I

OUTILS MATHÉMATIQUES POUR LA CRYPTOGRAPHIE QUANTIQUE

1.1 Espace de Hilbert

Un espace de Hilbert $\mathcal{H}$ est un espace vectoriel sur les nombres complexes $\mathbb{C}$ muni d'un produit scalaire et complet pour la norme associée à ce produit scalaire. Un élément quelconque, ou vecteur, de l'espace $\mathcal{H}$ est appelé vecteur-ket, ou plus simplement ket. On le note $|\rangle$, en mettant à l'intérieur un signe distinctif permettant de caractériser le ket correspondant par rapport à tous les autres, par exemple : $|\psi\rangle$. Cette notation est dite de Dirac. Dans tout ce qui suit, on ne considère que des espaces de Hilbert de dimension finie. Si $\mathcal{H}$ est un espace de Hilbert de dimension n, on le note $\mathcal{H}^{\otimes n}$. Soit $\mathcal{H}^{\otimes n}$ un espace de Hilbert, et soit :

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ . \\ . \\ \alpha_n \end{pmatrix} \tag{1.1}$$

un ket quelconque de $\mathcal{H}^{\otimes n}$. Le conjugué hermitique de $|\psi\rangle$ est le bra $\langle\psi|$:

$$\langle\psi| = |\psi\rangle^{\dagger} = \begin{pmatrix} \alpha_1^* & \alpha_2^* & . & . & \alpha_n^* \end{pmatrix} \tag{1.2}$$

où $\dagger$ représente l'opération de transposer et de conjuguer un vecteur ou une matrice et $*$ représente l'opération de conjugaison complexe.

Remarque 1 *Dans tout ce qui suit, on ne considère que des espaces de Hilbert de dimension finie.*

1.1.1 Produit scalaire

À tout couple de deux kets $|\varphi\rangle$ et $|\psi\rangle$ pris dans cet ordre, on associe un nombre complexe, qui est leur produit scalaire et qu'on note : $\langle\varphi|\psi\rangle$. En anglais, le symbole $\langle|\rangle$ s'appelle «braket» (crochet), d'où l'origine de la dénomination bra pour la partie gauche $\langle|$, et ket pour la partie droite $|\rangle$ de ce symbole. On a les propriétés suivantes du produit scalaire :

$$\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^* \tag{1.3}$$

$$\langle\varphi|\lambda_1\psi_1 + \lambda_2\psi_2\rangle = \lambda_1 \langle\varphi|\psi_1\rangle + \lambda_2 \langle\varphi|\psi_2\rangle \tag{1.4}$$

$$\langle\lambda_1\varphi_1 + \lambda_2\varphi_2|\psi\rangle = \lambda_1^* \langle\varphi_1|\psi\rangle + \lambda_2^* \langle\varphi_2|\psi\rangle \tag{1.5}$$

$$\langle\psi|\psi\rangle \geq 0 \tag{1.6}$$

$$\langle\psi|\psi\rangle = 0 \iff |\psi\rangle = \mathbf{0} \tag{1.7}$$

$$\langle\psi|\varphi\rangle \langle\varphi|\psi\rangle = |\langle\psi|\varphi\rangle|^2 \leq \langle\psi|\psi\rangle \langle\varphi|\varphi\rangle \qquad \text{«inégalité de Schwarz»} \tag{1.8}$$

Et puisque l'espace de Hilbert est complet pour la norme associée au produit scalaire, on a :

$$|| \, |\psi\rangle \, || = \sqrt{\langle\psi|\psi\rangle}$$

Les équations (1.6), (1.7) et (1.8) donnent alors :

$$|| \, |\psi\rangle \, || \geq 0 \tag{1.9}$$

$$|| \, |\psi\rangle \, || = 0 \iff |\psi\rangle = \mathbf{0} \tag{1.10}$$

$$|\langle\psi|\varphi\rangle| \leq || \, |\psi\rangle \, || \cdot || \, |\varphi\rangle \, || \qquad \text{«inégalité de Schwarz»} \tag{1.11}$$

On a aussi :

$$||\lambda \, |\psi\rangle \, || = |\lambda| || \, |\psi\rangle \, || \quad , \lambda \in \mathbb{C}.$$

$$\forall \, |\psi\rangle \neq \mathbf{0} \wedge \forall \, |\varphi\rangle \neq \mathbf{0} \text{ on a : } |\psi\rangle \perp |\varphi\rangle \iff \langle\psi|\varphi\rangle = 0 \tag{1.12}$$

En utilisant l'inégalité de Schwarz, on peut montrer la relation :

$$|| \, |\psi\rangle \, || - || \, |\varphi\rangle \, || \leq || \, |\psi\rangle + |\varphi\rangle \, || \leq || \, |\psi\rangle \, || + || \, |\varphi\rangle \, || \tag{1.13}$$

qui sera utile dans l'étude de la sécurité du protocole relativiste de Kent [44] contre les attaques quantiques.

Voici une preuve de l'inégalité de Schwarz :

Preuve Si on écrit $|\varphi\rangle$ sous la forme

$$|\varphi\rangle = \frac{\langle\psi|\varphi\rangle}{|| \, |\psi\rangle \, ||^2} \, |\psi\rangle + \left(|\varphi\rangle - \frac{\langle\psi|\varphi\rangle}{|| \, |\psi\rangle \, ||^2} \, |\psi\rangle \right) \tag{1.14}$$

Le premier terme de droite dans (1.14) est un vecteur proportionnel à $|\psi\rangle$ et le deuxième terme est orthogonal à $|\psi\rangle$. Alors ces deux termes sont orthogonaux. Ce qui permet d'écrire :

$$|| \, |\varphi\rangle \, ||^2 = \frac{| \, \langle\psi|\varphi\rangle \, |^2}{|| \, |\psi\rangle \, ||^2} + \left|\left| |\varphi\rangle - \frac{\langle\psi|\varphi\rangle}{|| \, |\psi\rangle \, ||^2} \, |\psi\rangle \right|\right|^2 \tag{1.15}$$

En multipliant les deux membres de (1.15) par $|| \, |\psi\rangle \, ||^2$, on obtient :

$$|| \, |\psi\rangle \, ||^2 || \, |\varphi\rangle \, ||^2 = | \, \langle\psi|\varphi\rangle \, |^2 + || \, |\psi\rangle \, ||^2 \left|\left| |\varphi\rangle - \frac{\langle\psi|\varphi\rangle}{|| \, |\psi\rangle \, ||^2} \, |\psi\rangle \right|\right|^2 \tag{1.16}$$

Et puisque :

$$|| \, |\psi\rangle \, ||^2 \left|\left| |\varphi\rangle - \frac{\langle\psi|\varphi\rangle}{|| \, |\psi\rangle \, ||^2} \, |\psi\rangle \right|\right|^2 \geq 0$$

Alors :

$$|\langle\psi|\varphi\rangle| \leq || \, |\psi\rangle \, || \cdot || \, |\varphi\rangle \, ||$$

L'égalité n'aura lieu dans (1.16) que lorsque $|\psi\rangle$ et $|\varphi\rangle$ sont proportionnels.

■

Remarque 2 *À partir de maintenant, on ne considère que des vecteurs de norme égale à 1.*

1.1.2 Base orthonormale

Choisir une représentation, c'est choisir une base orthonormale dans l'espace $\mathcal{H}^{\otimes n}$. Les vecteurs et les opérateurs sont représentés dans cette base par des nombres : composantes pour les vecteurs, éléments de matrice pour les opérateurs. Un ensemble, $\{|w_i\rangle\}$, de kets est dit orthonormal si les kets de cet ensemble satisfont à la relation d'orthonormalisation :

$$\langle w_i|w_j\rangle = \delta_{ij} \tag{1.17}$$

Un ensemble,$\{|w_i\rangle\}_{i=1}^{n}$, constitue une base de $\mathcal{H}^{\otimes n}$ si tout ket $|\psi\rangle \in \mathcal{H}^{\otimes n}$ se développe d'une façon et d'une seule suivant les $|w_i\rangle$:

$$|\psi\rangle = \sum_{i=1}^{n} c_i\,|w_i\rangle \tag{1.18}$$

Si la base est orthonormale, la multiplication des deux membres de (1.18) par $\langle w_j|$ et l'utilisation de (1.17) donnent :

$$\langle w_j|\psi\rangle = c_j \tag{1.19}$$

La substitution de c_i, par sa nouvelle expression de (1.19), dans (1.18) donne :

$$|\psi\rangle = \sum_{i=1}^{n} \langle w_i|\psi\rangle\,|w_i\rangle$$

Et puisque $\langle w_i|\psi\rangle$ est un scalaire, on peut le déplacer à droite pour avoir :

$$|\psi\rangle = \sum_{i=1}^{n} |w_i\rangle\,\langle w_i|\psi\rangle \tag{1.20}$$

1.1.3 Représentation des kets, des bras et des opérateurs

Dans la base $\{|w_i\rangle\}_{i=1}^{n}$, le ket $|\psi\rangle$ est représenté par une matrice colonne :

$$\begin{pmatrix} \langle w_1|\psi\rangle \\ \langle w_2|\psi\rangle \\ . \\ . \\ \langle w_n|\psi\rangle \end{pmatrix}$$

Le bra $\langle\psi|$ est représenté dans la base $\{\langle w_i|\}_{i=1}^{n}$ par une matrice ligne :

$$\begin{pmatrix}\langle\psi|w_1\rangle & \langle\psi|w_2\rangle & . & . & \langle\psi|w_n\rangle\end{pmatrix} \tag{1.21}$$

1.1.4 Base de calcul

On appelle *base de calcul* de $\mathcal{H}^{\otimes n}$, la base :

$$|0\rangle = \begin{pmatrix}1\\0\\0\\.\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\\0\\.\\0\end{pmatrix}, ..., |n-1\rangle = \begin{pmatrix}0\\0\\0\\.\\1\end{pmatrix}$$

Tout ket $|\alpha\rangle$ peut s'exprimer dans la base de calcul :

$$|\alpha\rangle = \begin{pmatrix}\alpha_0\\\alpha_1\\.\\.\\\alpha_{n-1}\end{pmatrix} = \alpha_0|0\rangle + \alpha_1|1\rangle + ... + \alpha_{n-1}|n-1\rangle$$

1.1.5 Produit tensoriel

Soient deux espaces de Hilbert, $\mathcal{H}_1^{\otimes n}$ et $\mathcal{H}_2^{\otimes m}$. On appelle produit tensoriel de $\mathcal{H}_1^{\otimes n}$ et $\mathcal{H}_2^{\otimes m}$, l'espace $\mathcal{H}$ de dimension nm :

$$\mathcal{H}^{\otimes nm} = \mathcal{H}_1^{\otimes n} \otimes \mathcal{H}_2^{\otimes m}$$

À tout couple de kets, $|\psi_1\rangle \in \mathcal{H}_1^{\otimes n}$ et $|\psi_2\rangle \in \mathcal{H}_2^{\otimes m}$, on associe un ket $|\psi\rangle \in \mathcal{H}^{\otimes nm}$, qu'on note :

$$|\psi_1\rangle \otimes |\psi_2\rangle$$

Ou tout simplement

$$|\psi_1\rangle\,|\psi_2\rangle$$

et que l'on appelle *produit tensoriel* de $|\psi_1\rangle$ et $|\psi_2\rangle$. On a les propriétés suivantes de l'opération du produit tensoriel :

1. Linéairité par rapport à la multiplication par les nombres complexes

$$[\mu\,|\psi_1\rangle] \otimes |\psi_2\rangle = \mu\,[|\psi_1\rangle \otimes |\psi_2\rangle]\,,\ \mu \in \mathbb{C} \tag{1.22}$$

$$|\psi_1\rangle \otimes [\nu\,|\psi_2\rangle] = \nu\,[|\psi_1\rangle \otimes |\psi_2\rangle]\,, \nu \in \mathbb{C} \tag{1.23}$$

2. Distributivité par rapport à l'addition

$$|\psi\rangle \otimes [|\varphi_1\rangle + |\varphi_2\rangle] = |\psi\rangle \otimes |\varphi_1\rangle + |\psi\rangle \otimes |\varphi_2\rangle \tag{1.24}$$

$$[|\psi_1\rangle + |\psi_2\rangle] \otimes |\varphi\rangle = |\psi_1\rangle \otimes |\varphi\rangle + |\psi_2\rangle \otimes |\varphi\rangle$$

3. Si $\{|u_i\rangle\}$ et $\{|v_j\rangle\}$ sont des bases de $\mathcal{H}_1^{\otimes n}$ et de $\mathcal{H}_2^{\otimes m}$ respectivement, alors l'ensemble des kets $\{|u_i\rangle \otimes |v_j\rangle\}$ constitue une base dans $\mathcal{H}^{\otimes nm} = \mathcal{H}_1^{\otimes n} \otimes \mathcal{H}_2^{\otimes m}$(c-à-d. de dimension nm)

Exemple 1 *$|\psi\rangle$ et $|\varphi\rangle$ deux kets de $\mathcal{H}^{\otimes 2}$. Leurs produit tensoriel est un ket de $\mathcal{H}^{\otimes 4}$:*

$$|\psi\rangle \otimes |\varphi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \end{pmatrix}$$

Donc, les composantes d'un vecteur produit tensoriel sont les produits des composantes des deux vecteurs du produit. Ceci peut se traduire formellement dans la base de calcul :

Soit $|\psi\rangle \in \mathcal{H}_1^{\otimes n}$ et $|\varphi\rangle \in \mathcal{H}_2^{\otimes m}$ tels que:

$$|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i\,|i\rangle \ \text{ et } \ |\varphi\rangle = \sum_{j=0}^{m-1} \beta_j\,|j\rangle$$

alors $|\psi\rangle \otimes |\varphi\rangle \in \mathcal{H} = \mathcal{H}_1^{\otimes n} \otimes \mathcal{H}_2^{\otimes m}$ est défini comme:

$$|\psi\rangle \otimes |\varphi\rangle = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha_i \beta_j |i\rangle \otimes |j\rangle$$

Il existe dans $\mathcal{H}^{\otimes nm}$ des vecteurs qui ne sont pas des produits tensoriels d'un vecteur de $\mathcal{H}_1^{\otimes n}$ par un autre de $\mathcal{H}_2^{\otimes m}$. On peut voir ça dans l'exemple suivant.

Exemple 2 *Le ket* $|\chi\rangle \in \mathcal{H}^{\otimes 4} = \mathcal{H}_1^{\otimes 2} \otimes \mathcal{H}_2^{\otimes 2}$

$$|\chi\rangle = \frac{1}{\sqrt{2}} |0\rangle |1\rangle - \frac{1}{\sqrt{2}} |1\rangle |0\rangle \tag{1.25}$$

n'est pas un produit tensoriel d'un vecteur de $\mathcal{H}_1^{\otimes 2}$ *par un vecteur de* $\mathcal{H}_2^{\otimes 2}$. *Pour le voir, supposons par l'absurde que :*

$$\begin{aligned} |\chi\rangle &= (\alpha |0\rangle + \beta |1\rangle)(\gamma |0\rangle + \delta |1\rangle) \qquad (1.26) \\ &= \alpha\gamma |0\rangle |0\rangle + \alpha\delta |0\rangle |1\rangle + \beta\gamma |1\rangle |0\rangle + \beta\delta |1\rangle |1\rangle \end{aligned}$$

La comparaison de (1.25) et (1.26) implique :

$$\alpha\delta = \frac{1}{\sqrt{2}} \Longrightarrow \delta \neq 0$$

et

$$\left(\beta\delta = 0 \wedge \beta\gamma = \frac{1}{\sqrt{2}}\right) \Longrightarrow \delta = 0$$

d'où la contradiction.

4. On peut définir le produit scalaire dans $\mathcal{H}$ à partir des produits scalaires dans $\mathcal{H}_1$ et $\mathcal{H}_2$. Si $|\psi_1\rangle \in \mathcal{H}_1$, $|\varphi_1\rangle \in \mathcal{H}_1$, $|\psi_2\rangle \in \mathcal{H}_2$, $|\varphi_2\rangle \in \mathcal{H}_2$:

$$[\langle\psi_1| \langle\psi_2|] [|\varphi_1\rangle |\varphi_2\rangle] = \langle\psi_1|\varphi_1\rangle \langle\psi_2|\varphi_2\rangle$$

1.1.6 Opérateurs

Une application linéaire A: $\mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes m}$ fait correspondre à tout ket $|\psi\rangle \in \mathcal{H}^{\otimes n}$ un autre ket $|\psi'\rangle \in \mathcal{H}^{\otimes m}$, d'une façon linéaire :

$$|\psi'\rangle = A |\psi\rangle$$

$$A(\lambda_1 |\psi_1\rangle + \lambda_2 |\psi_2\rangle) = \lambda_1 A |\psi_1\rangle + \lambda_2 A |\psi_2\rangle$$

Un opérateur A est une application linéaire qui peut être représentée par une matrice carrée. On note l'ensemble des opérateurs agissant sur les kets de $\mathcal{H}^{\otimes n}$ par $\mathcal{L}(\mathcal{H}^{\otimes n})$. Le produit de deux opérateurs A et B, noté AB, est défini de la façon suivante:

$$(AB) |\psi\rangle = A(B |\psi\rangle)$$

On appelle élément de matrice de A entre $|\varphi\rangle$ et $|\psi\rangle$, le produit scalaire :

$$\langle\varphi| (A |\psi\rangle)$$

qu'on note

$$\langle\varphi| A |\psi\rangle$$

C'est un nombre complexe qui dépend linéairement de $|\psi\rangle$ et anti-linéairement de $|\varphi\rangle$ (car $(\lambda |\varphi\rangle)^\dagger = \lambda^* \langle\varphi|$).

Remarque 3 *Si on écrit $\langle\psi|\varphi\rangle$ dans l'ordre inverse : $|\psi\rangle \langle\varphi|$, on obtient un opérateur au lieu d'un nombre complexe. En effet, pour un ket $|\chi\rangle$ considérons :*

$$|\psi\rangle \langle\varphi|\chi\rangle$$

Puisque $\langle\varphi|\chi\rangle$ est un nombre complexe, alors $|\psi\rangle \langle\varphi|\chi\rangle$ est un ket. L'objet mathématique $|\psi\rangle \langle\varphi|$, appliqué à un ket quelconque, donne un ket : c'est donc un opérateur.

L'opérateur A est représenté dans la base $\{\langle w_i|\}_{i=1}^n$ par la matrice carrée :

$$\begin{pmatrix} A_{11} & A_{12} & ... & A_{1n} \\ A_{21} & A_{22} & ... & A_{2n} \\ . & . & ... & . \\ A_{n1} & A_{n2} & .. & A_{nn} \end{pmatrix} \text{ où } A_{ij} = \langle w_i| A |w_j\rangle$$

Le produit de Kronecker ou tensoriel de deux opérateurs A et B est :

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & ... & A_{1n}B \\ A_{21}B & A_{22}B & ... & A_{2n}B \\ & & & \\ A_{n1}B & A_{n2}B & & A_{nn}B \end{pmatrix}$$

Les propriétés du produit de Kronecker sont bien connues dans la littérature. On présente ici quelques propriétés de base du produit de Kronecker :

$$(A+B)\otimes C = A\otimes C + B\otimes C$$

$$A\otimes (B+C) = A\otimes B + A\otimes C$$

$$k(A\otimes B) = (kA)\otimes B = A\otimes (kB)\,, k\in\mathbb{C}$$

$$(A\otimes B)\otimes C = A\otimes (B\otimes C)$$

$(A\otimes B)(C\otimes D) = AC\otimes BD$ «dans la mesure où les dimensions concordent»

$$Tr(A\otimes B) = Tr\,(A)\otimes Tr\,(B)$$

Où $Tr(A) = \sum_i A_{ii}$, donc la somme des éléments de la diagonale.

$$\det(A\otimes B) = \det(A)^m \det(B)^n \text{ si } A\in\mathcal{L}(\mathcal{H}^n),\ B\in\mathcal{L}(\mathcal{H}^m)$$

$$(A\otimes B)^{-1} = A^{-1}\otimes B^{-1} \text{ «si } A \text{ et } B \text{ sont non-singuliers»}$$

$$(A\otimes B)^\dagger = A^\dagger\otimes B^\dagger$$

La conjugaison hermitique $\dagger$ a les propriétés suivantes :

$$(A^\dagger)^\dagger = A$$

$$(\lambda A)^\dagger = \lambda^* A^\dagger,\ \lambda\in\mathbb{C}$$

$$(A+B)^\dagger = A^\dagger + B^\dagger$$

$$(AB)^\dagger = B^\dagger A^\dagger$$

Définition 1 *Un opérateur A est dit*

1. *Normal si, et seulement si, $AA^\dagger = A^\dagger A$.*

2. *Hermitique si, et seulement si,* $A = A^\dagger$.

3. *Non négatif ou semi-défini positif si, et seulement si,* $\langle\psi| A |\psi\rangle \geq 0, \forall |\psi\rangle \in \mathcal{H}$.

4. *Positif ou défini positif si, et seulement si,* $\langle\psi| A |\psi\rangle > 0, \forall |\psi\rangle \in \mathcal{H}.\backslash\{\mathbf{0}\}$

5. *Unitaire si, et seulement si,* $AA^\dagger = A^\dagger A = I$.

6. *Projecteur si, et seulement si, A est hermitique et*

$$A^2 = A$$

Théorème 3 *On a les propriétés suivantes :*

1. Les opérateurs hermitiques, semi-définis positifs, définis positifs et unitaires sont normaux.

2. Un opérateur A est normal si, et seulement si, il existe une base $\{|w_i\rangle\}_{i=1}^n$ où il peut s'écrire : $A = \sum_{i=1}^{n} \lambda_i |w_i\rangle \langle w_i|, \lambda_i \in \mathbb{C}$.

3. Un opérateur A est hermitique si, et seulement si, il existe une base $\{|w_i\rangle\}_{i=1}^n$ où il peut s'écrire :

$$A = \sum_{i=1}^{n} \lambda_i |w_i\rangle \langle w_i|, \lambda_i \in \mathbb{R}. \tag{1.27}$$

4. Un opérateur A est semi-défini positif si, et seulement si, il existe une base $\{|w_i\rangle\}_{i=1}^n$ où il peut s'écrire :

$$A = \sum_{i=1}^{n} \lambda_i |w_i\rangle \langle w_i|, \lambda_i \in \mathbb{R}^+. \tag{1.28}$$

5. Un opérateur A est défini positif si, et seulement si, il existe une base $\{|w_i\rangle\}_{i=1}^n$ où il peut s'écrire :

$$A = \sum_{i=1}^{n} \lambda_i |w_i\rangle \langle w_i|, \lambda_i \in \mathbb{R}^{+*}. \tag{1.29}$$

6. Un opérateur A est unitaire si, et seulement si, il existe une base $\{|w_i\rangle\}_{i=1}^n$ où il peut s'écrire :

$$A = \sum_{i=1}^{n} \lambda_i |w_i\rangle \langle w_i|, |\lambda_i| = 1.$$

7. Un opérateur A est projecteur si, et seulement si, il existe une base $\{|w_i\rangle\}_{i=1}^{n}$ où il peut s'écrire :

$$A = \sum_{i=1}^{n} |w_i\rangle \langle w_i| . \tag{1.30}$$

Donc, si on note l'ensemble des opérateurs hermitiques, semi-définis positifs, positifs, agissant dans $\mathcal{H}^{\otimes n}$, respectivement par, $\mathsf{H}(\mathcal{H}^{\otimes n}), \mathsf{Pos}(\mathcal{H}^{\otimes n}), \mathsf{Pos}^{+}(\mathcal{H}^{\otimes n})$, on obtient :

$$\mathsf{Pos}^{+}(\mathcal{H}^{\otimes n}) \subset \mathsf{Pos}(\mathcal{H}^{\otimes n}) \subset \mathsf{H}(\mathcal{H}^{\otimes n})$$

Dans le cas des équations (1.27), (1.28), (1.29) et (1.30) on dira que l'opérateur A admet une *décomposition spectrale.* Les résultats du théorème 3 permettent d'indexer les valeurs propres d'un opérateur A agissant dans $\mathcal{H}^{\otimes n}$ qu'il soit hermitique, non négatif ou positif, en ordre décroissant :

$$\lambda_1(A) \geq \lambda_2(A) \geq ..... \geq \lambda_n(A)$$

On peut aussi les réunir dans un seul vecteur $\lambda(A)$:

$$\lambda(A) = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ . \\ \lambda_n \end{bmatrix}$$

Un opérateur semi-défini positif A est noté $A \succcurlyeq 0$. Un opérateur défini positif A est noté $A \succ 0$. L'écriture $A \succcurlyeq B$ signifie que $A - B \succcurlyeq 0$, et l'écriture $A \succ B$ que $A - B \succ 0$.

De la même manière que pour les vecteurs, on définit le produit scalaire ou le produit interne entre deux opérateurs A et B de $\mathcal{L}(\mathcal{H}^{\otimes n})$ par :

$$\langle A, B \rangle = Tr\left(A^{\dagger}B\right)$$

Si A et $B \in \mathsf{H}(\mathcal{H}^{\otimes n})$, alors :

$$\begin{aligned} \langle A, B \rangle &= Tr\left(A^{\dagger}B\right) = Tr\left(AB^{\dagger}\right) = Tr\left(\left(BA^{\dagger}\right)^{\dagger}\right) = \left(Tr\left(BA^{\dagger}\right)\right)^{*} \\ &= \left(Tr\left(A^{\dagger}B\right)\right)^{*} = \langle A, B \rangle^{*} \end{aligned}$$

Alors, le produit interne de deux opérateurs hermétiques est un réel. On a aussi les propriétés suivantes du produit interne,

Lemme 1 *Si A et $B \in \mathsf{Pos}(\mathcal{H}^{\otimes n})$ on a :*

$$\langle A, B\rangle \geq 0$$

On a aussi le corollaire suivant, qui résulte de la linéarité du produit interne :

Corollaire 1 *Si A et $B \in \mathsf{H}(\mathcal{H}^{\otimes n})$ tels que $A \succcurlyeq B$, et $C \succcurlyeq 0$, alors :*

$$\langle A, C\rangle \geq \langle B, C\rangle$$

Un autre résultat peut nous donner une idée sur la non-négativité des opérateurs et le produit tensoriel.

Corollaire 2 *Si A et $B \in \mathsf{Pos}(\mathcal{H}^{\otimes n})$, alors $A \otimes B \in \mathsf{Pos}(\mathcal{H}^{\otimes n.m})$, c-à-d.*

$$A \otimes B \succcurlyeq 0$$

Corollaire 3 *Si A et $B \in \mathsf{H}(\mathcal{H}^{\otimes n})$ tels que $A \succcurlyeq B$, et $C \succcurlyeq 0$, alors*

$$A \otimes C \succcurlyeq B \otimes C$$

Théorème 4 *Si A et B sont deux opérateurs unitaires de $\mathcal{L}(\mathcal{H}^{\otimes n})$, alors AB l'est aussi.*

Preuve

$$(AB)(AB)^\dagger = ABB^\dagger A^\dagger = AA^\dagger = I$$

$$(AB)^\dagger(AB) = B^\dagger A^\dagger AB = B^\dagger B = I$$

■

Lemme 2 *Le produit de deux opérateurs hermitiques A et B de $\mathsf{H}(\mathcal{H}^{\otimes n})$ n'est hermitique que si $[A,B] = AB - BA = 0$.*

Preuve En effet, si $A = A^\dagger$ et $B = B^\dagger$, on déduit que :

$$(AB)^\dagger = B^\dagger A^\dagger = BA$$

qui n'est égal à AB que si $[A,B] = 0$.

■

Théorème 5 *Les opérateurs unitaires préservent le produit scalaire.*

Preuve Soit A un opérateur unitaire, et soit :

$$|\psi'\rangle = A\,|\psi\rangle$$

$$|\varphi'\rangle = A\,|\varphi\rangle$$

On a :

$$\langle\varphi'|\psi'\rangle = \left\langle\varphi|A^\dagger A|\psi\right\rangle = \langle\varphi|\psi\rangle$$

■

Théorème 6 *Soit A et B deux opérateurs on a :*

$$A \text{ et } B \text{ sont unitaires} \Longrightarrow A \otimes B \text{ est unitaire}$$

$$A \text{ et } B \text{ sont hermitiques} \Longrightarrow A \otimes B \text{ est hermitique}$$

$$A \text{ et } B \text{ sont définis positifs} \Longrightarrow A \otimes B \text{ est défini positif}$$

$$A \text{ et } B \text{ sont des projecteurs} \Longrightarrow A \otimes B \text{ est projecteur}$$

1.1.7 Relations caractéristiques d'une base orthonormée

La remarque 3 de la page 18 permet d'écrire l'équation 1.20 de la manière suivante :

$$|\psi\rangle = \sum_{i=1}^{n} |w_i\rangle \langle w_i|\psi\rangle = \left(\sum_{i=1}^{n} |w_i\rangle \langle w_i|\right) |\psi\rangle$$

Donc, l'application de l'opérateur $\sum_{i=1}^{n} |w_i\rangle \langle w_i|$ sur un ket quelconque $|\psi\rangle$ redonne le même ket $|\psi\rangle$, on a alors :

$$\sum_{i=1}^{n} |w_i\rangle \langle w_i| = I_n$$

On remarque l'equivalence des quatre expressions suivantes :

$$\{|w_i\rangle\}_{i=1}^{n} \text{ est une base orthonormale}$$

$$|\psi\rangle = \sum_{i=1}^{n} \langle w_i|\psi\rangle |w_i\rangle\,, \quad \forall |\psi\rangle \in \mathcal{H}^{\otimes n}$$

$$\sum_{i=1}^{n} |w_i\rangle \langle w_i| = I_n$$

$$\langle\psi|\psi\rangle = \sum_{i=1}^{n} |\langle w_i|\psi\rangle|^2$$

CHAPITRE II

THÉORÈMES À LA BASE DE LA CRYPTOGRAPHIE QUANTIQUE

L'ordinateur classique n'emploie pas toutes les possibilités offertes par la nature. Sa mémoire est faite de bits. Chaque bit porte soit un 1 soit un 0. La machine calcule en manipulant ces bits, or dans la nature il y a une possibilité d'appliquer des transformations unitaires qui peuvent agir sur des systèmes en superposition.

2.1 État

L'état est une description de tous les aspects du système physique. En mécanique quantique, cet état est représenté par un ket $|\psi\rangle$ dans l'espace de Hilbert $\mathcal{H}$. Ce ket donne le maximum d'informations possible sur le système, dans le but de prévoir les résultats des expériences que l'on peut réaliser.

2.2 Qubit

Cela vient de quantum + bit. C'est une abstraction mathématique d'un système quantique capable de mémoriser un bit d'information. Par analogie avec un bit qui peut prendre deux valeurs, le qubit est représenté par un ket $|\psi\rangle$ dans un espace de Hilbert de dimension 2, $\mathcal{H}^{\otimes 2}$. Nous pouvons donc voir le «qubit» comme une évolution du bit logique. Dans l'article [61] les auteurs montrent qu'un qubit peut être vu comme la généralisation matricielle du bit classique. Le point de départ est l'équation de Boole :

$x^2 = x$ qui montre que les symboles logiques peuvent s'écrire sous la forme 0 ou 1. Les auteurs généralisent l'équation à une autre, qui est matricielle :

$$P^2(x) = P(x)$$

où $x \in \{0, 1\}$ est un symbole logique. Cette équation est donc l'équation d'un projecteur. La solution de cette équation est la matrice

$$P(x) = \begin{pmatrix} 1-x & 0 \\ 0 & x \end{pmatrix}$$

Le lien avec la notation de Dirac est donné par :

$$P(x) = |x\rangle \langle x|$$

où

$$|x\rangle = \begin{pmatrix} 1-x \\ x \end{pmatrix}$$

On retrouve les qubits de base $|0\rangle$ et $|1\rangle$ pour les valeurs 0 et 1 de x.

Preuve

$$\begin{aligned} |||x\rangle||^2 &= 1 \Longrightarrow (1-x)^2 + x^2 = 1 \\ &\Longrightarrow x(x-1) = 0 \Longrightarrow x = 0 \vee x = 1 \end{aligned}$$

■

Un qubit est donc un vecteur à 2 dimensions. On peut présenter un qubit sous la forme

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

où

$$|\alpha|^2 + |\beta|^2 = 1$$

et puisque dans la base de calcul :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

On peut écrire le qubit sous la forme :

$$\alpha\,|0\rangle + \beta\,|1\rangle\,,\ \text{où}\quad |\alpha|^2 + |\beta|^2 = 1$$

et on dit que $|\psi\rangle$ est en superposition des états de base $|0\rangle$ et $|1\rangle$. La force du calcul quantique vient du fait qu'il peut s'appliquer sur des états quantiques en superposition de plusieurs états de base. On appelle $\{|0\rangle, |1\rangle\}$ les états de base de $\mathcal{H}^{\otimes 2}$. Cependant, les états quantiques ne sont pas tous des qubits. On peut avoir, par exemple, un état quantique de plusieurs qubits. Donc, on doit être capable de décrire l'espace d'états correspondant. L'espace d'états pour un système composé est le produit tensoriel des espaces individuel de chaque état. Si, par exemple, on a un état de trois qubits, l'espace qui lui correspond est : $\mathcal{H}^{\otimes 2}\otimes\mathcal{H}^{\otimes 2}\otimes\mathcal{H}^{\otimes 2} = \mathcal{H}^{\otimes 2^3}$. Pour alléger l'écriture, on écrit $|10\rangle$ ou $|1\rangle\,|0\rangle$ à la place de $|1\rangle \otimes |0\rangle$. Cependant, on peut confondre l'écriture binaire "10" et l'état de base "10" (en décimal) de $\mathcal{H}^{\otimes n}$ où $n \geq 11$. A moins d'avis contraire, C'est la première écriture qui sera considérée.

2.2.1 États intriqués

Considérons les deux états à deux qubits :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|01\rangle \quad \text{et} \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

On voit que $|\psi_1\rangle$ peut être écrit sous forme de produit tensoriel

$$|\psi_1\rangle = |0\rangle\,(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle).$$

Par contre, $|\psi_2\rangle$ ne peut être factorisé ainsi (prière de relire l'exemple 2 de la page 17). l'état $|\psi_2\rangle$ est dit intriqué.

À part l'univers qui peut être considéré comme un système isolé, tous les systèmes réels ne peuvent l'être qu'à titre approximatif, et leur états ne sont souvent qu'imparfaitement déterminés. Le problème posé est comment le formalisme quantique peut-il supporter et décrire cette situation afin de faire des prédictions qui supportent au maximum ce manque d'informations ? Le formalisme des opérateurs de densité (que

nous introduisons à la prochaine section), qui generalise celui des vecteurs d'états, est un outil très efficace dans ce cas. Nous verrons dans la section suivante qu'il y a un lien intime entre les deux formalismes. Un expérimentateur (Alice) recevant le système A décrit par ρ_A et n'ayant pas accès à B (aux mains de Bob) n'a aucun moyen de savoir si A faisait partie de $A+B$ ou si c'était un système isolé préparé comme un mélange statistique.

2.3 Opérateur de densité

La notion de probabilité est généralememt utilisée lorsque l'information qu'on a sur le système est partielle. C'est le cas, par exemple, pour l'état de polarisation des photons issus d'une source de lumière non polarisée (lumière naturelle), car dans ce cas l'état de polarisation du photon est aléatoire. Cela veut dire que le photon peut avoir n'importe quel état de polarisation avec une probabilité égale. L'information partielle sur le système quantique se présente alors de la façon suivante : L'état de ce système peut être soit l'état $|\psi_1\rangle$ avec une probabilité p_1, soit l'état $|\psi_2\rangle$ avec une probabilité p_2, ..etc. On a évidement :

$$\sum_i p_i = 1$$

On dit alors qu'on a affaire à un mélange statistique. On peut représenter un mélange statitique par l'ensemble :

$$\mathcal{E} = \{(p_i, |\psi_i\rangle) : i \in \{1, ..., k\}, |\psi_i\rangle \in \mathcal{H}\}.$$

L'opérateur de densité du mélange statistique $\{(p_i, |\psi_i\rangle)\}$ est défini par :

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

On dit aussi que ρ est un opérateur de densité s'il existe un mélange statistique $\mathcal{E}$ dont il est l'opérateur de densité. Un opérateur de densité ρ de mélange statistique $\mathcal{E}$ peut être aussi un opérateur de densité pour un autre mélange statistique $\mathcal{E}' = \{(p', |\psi'\rangle)\}$. Si deux mélanges statistiques ont le même opérateur de densité, on dit qu'ils sont équivalents. Les mélanges statistiques équivalents réagissent exactement de la même façon envers les

opérations et les mesures quantiques. Ainsi, ils représentent vraiment le même état quantique. Supposons qu'on a deux parties, Alice et Bob, qui vivent respectivement dans les deux espaces $\mathcal{A}$ et $\mathcal{B}$. Si Alice et Bob partagent un état quantique $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$, alors aucun d'eux n'a le contrôle total de $|\psi\rangle$. Ainsi que nous le verrons plus loin, les mélanges statistiques peuvent être utilisés pour décrire une partie de l'état quantique quand l'autre partie de l'état n'est pas disponible.

Théorème 7 *Un opérateur ρ agissant dans $\mathcal{H}$ est un opérateur de densité si, et seulement si, ρ est positif et $Tr(\rho) = 1$.*

Preuve Si ρ est un opérateur de densité du mélange statistique $\mathcal{E} = \{(p_i, |\psi_i\rangle)\}$:

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

Donc on a

$$\begin{aligned} Tr(\rho) &= Tr\left(\sum_i p_i |\psi_i\rangle \langle\psi_i|\right) = \sum_i p_i Tr\left(|\psi_i\rangle \langle\psi_i|\right) \\ &= \sum_i p_i Tr\left(\langle\psi_i|\psi_i\rangle\right) = \sum_i p_i = 1. \end{aligned}$$

Quelque soit $|\chi\rangle$, on a

$$\langle\chi| \rho |\chi\rangle = \langle\chi| \left(\sum_i p_i |\psi_i\rangle \langle\psi_i|\right) |\chi\rangle = \sum_i p_i \langle\chi|\psi_i\rangle \langle\psi_i|\chi\rangle = \sum_i p_i |\langle\chi|\psi_i\rangle|^2 \geq 0$$

Alors, ρ est positif et $Tr(\rho) = 1$. Maintenant supposons que ρ est un opérateur positif et que $Tr(\rho) = 1$. L'opérateur de densité ρ admet, alors, une décomposition spectrale :

$$\rho = \sum_i \lambda_i |w_i\rangle \langle w_i| \text{ où } \lambda_i \geq 0.$$

On a aussi :

$$Tr(\rho) = \sum_i \lambda_i Tr\left(|w_i\rangle \langle w_i|\right) = \sum_i \lambda_i = 1 .$$

On conclut alors que ρ est un opérateur de densité pour le mélange statistique $\{(\lambda_i, |w_i\rangle)\}$.

■

Lemme 3 *Un mélange statistique d'opérateurs de densité est aussi un opérateur de densité.*

Preuve Considérons le mélange statistique d'opérateurs de densité $\{p_i, \rho_i\}$ et son opérateur de densité :

$$\rho = \sum_i p_i \rho_i.$$

Donc

$$Tr(\rho) = Tr\left(\sum_i p_i \rho_i\right) = \sum_i p_i Tr(\rho_i). = \sum_i p_i = 1.$$

Pour tout $|\chi\rangle \in \mathcal{H}$, on a

$$\langle\chi|\,\rho\,|\chi\rangle = \langle\chi|\left(\sum_i p_i \rho_i\right)|\chi\rangle = \sum_i p_i \langle\chi|\,\rho_i\,|\chi\rangle \geq 0$$

car les ρ_i sont des opérateurs positifs et $p_i \geq 0$, et le résultat suit par le théorème 7.

■

Le lemme 3 montre que l'ensemble des opérateurs de densité est convexe, c-à-d.:$\lambda \in [0,1]$, ρ_1 et ρ_2 opérateurs de densité $\Longrightarrow \lambda\rho_1 + (1-\lambda)\rho_2$ est aussi un opérateur de densité.

Lemme 4 *La trace du carré de l'opérateur de densité ρ est toujours ≤ 1 :*

$$Tr(\rho^2) \leq 1$$

Preuve Puisque ρ est positif, il existe une base orthonormale $\{|w_i\rangle\}$ où il peut s'écrire :

$$\rho = \sum_i \lambda_i |w_i\rangle \langle w_i|, \lambda_i \in \mathbb{R}^+$$

Mais le fait que $\sum_i \lambda_i = 1$ implique :

$$\lambda_i \leq 1$$

Et comme

$$\rho^2 = \sum_i \lambda_i^2 |w_i\rangle \langle w_i|$$

Alors

$$Tr(\rho^2) = \sum_i \lambda_i^2 \leq 1$$

l'égalité ne peut avoir lieu que si un seul des λ_j est non nul Ce qui donne :

$$\rho = |w_j\rangle \langle w_j|$$

Dans ce cas ρ est dit état pur (en opposition à un état mélangé).

■

2.4 Trace partielle

Définition 2 *Soit l'espace de Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, et l'opérateur de densité $\rho \in \mathsf{Pos}(\mathcal{H}^{\otimes n})$. on définit la trace partielle de ρ sur $\mathcal{H}_2$ par*

$$Tr_{\mathcal{H}_2}(\rho) = \sum_i (I_{\mathcal{H}_1} \otimes \langle i| \otimes I_{\mathcal{H}_3})\, \rho\, (I_{\mathcal{H}_1} \otimes |i\rangle \otimes I_{\mathcal{H}_3})$$

où $\{|i\rangle\}$ est une base quelconque de $\mathcal{H}_2$.

Cette définition est générale dans le sens où on peut prendre $\mathcal{H}_1 = \mathbb{C}^{\otimes 1}$et/ou $\mathcal{H}_3 = \mathbb{C}^{\otimes 1}$, et puisque le seul vecteur normé dans $\mathbb{C}^{\otimes 1}$ est égal à l'entier 1, on peut écrire $\rho = 1 \otimes \rho = \rho \otimes 1$.

Proposition 1 *La définition de la trace partielle est indépendante du choix de la base dans $\mathcal{H}_2$.*

Preuve D'aprés un résultat prouvé dans la sous-section 1.1.2, toute base $\{\langle i|\}$ dans $\mathcal{H}$ vérifie la relation de fermeture :

$$\sum_i |i\rangle \langle i| = I_{\mathcal{H}}$$

Soit l'espace de Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$. Et soit ρ un opérateur de densité. Supposons qu'on a les deux bases $\{\langle i|\}$ et $\{\langle k|\}$ de $\mathcal{H}_2$. On peut écrire alors :

$$\begin{aligned}
Tr_{\mathcal{H}_2}(\rho) &= \sum_i \left(I_{\mathcal{H}_1} \otimes \langle i| \otimes I_{\mathcal{H}_3}\right) \rho \left(I_{\mathcal{H}_1} \otimes |i\rangle \otimes I_{\mathcal{H}_3}\right) \\
&= \sum_i I_{\mathcal{H}_1} \otimes \langle i| \left(\sum_k |k\rangle \langle k|\right) \otimes I_{\mathcal{H}_3} \rho \left(I_{\mathcal{H}_1} \otimes \left(\sum_k |k\rangle \langle k|\right) |i\rangle \otimes I_{\mathcal{H}_3}\right) \\
&= \sum_{k,k'} I_{\mathcal{H}_1} \otimes \sum_i \langle i|k\rangle \langle k| \otimes I_{\mathcal{H}_3} \rho \left(I_{\mathcal{H}_1} \otimes \left(\left|k'\right\rangle \left\langle k'|i\right\rangle\right) \otimes I_{\mathcal{H}_3}\right) = \\
&= \sum_{k,k'} \left(I_{\mathcal{H}_1} \otimes \langle k| \otimes I_{\mathcal{H}_3}\right) \rho \left(I_{\mathcal{H}_1} \otimes \left|k'\right\rangle \otimes I_{\mathcal{H}_3}\right) \sum_i \delta_{i,k} \delta_{i.k'} \\
&= \sum_{k,k'} \left(I_{\mathcal{H}_1} \otimes \langle k| \otimes I_{\mathcal{H}_3}\right) \rho \left(I_{\mathcal{H}_1} \otimes \left|k'\right\rangle \otimes I_{\mathcal{H}_3}\right) \delta_{k,k'} \\
&= \sum_k \left(I_{\mathcal{H}_1} \otimes \langle k| \otimes I_{\mathcal{H}_3}\right) \rho \left(I_{\mathcal{H}_1} \otimes |k\rangle \otimes I_{\mathcal{H}_3}\right)
\end{aligned}$$

■

D'où, on peut prendre la trace partielle par rapport à n'importe quelle base dans $\mathcal{H}_2$.

Soit l'espace de Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, et soit $X \in \mathcal{L}(\mathcal{H}_2)$, on a les deux propriétés suivante :

$$1.\ Tr_{\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3}(X) = Tr_{\mathcal{H}_1 \otimes \mathcal{H}_3}(Tr_{\mathcal{H}_2}(X))$$
$$2.\ X \succcurlyeq 0 \Longrightarrow Tr_{\mathcal{H}_2}(X) \succcurlyeq 0$$

Donc, si on prend la trace partielle d'un opérateur de densité, on obtient un autre opérateur de densité.

Suposons qu'on a un état $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. Si on mesure le système B et on se débarasse du résultat, le système A, dans ce cas, est un mélange statistique dont l'état est représenté par l'opérateur de densité de $\mathrm{Pos}(\mathcal{H}_A)$:

$$\rho_A = Tr_B \left(|\psi\rangle_{AB\ AB} \langle\psi|\right)$$

Ainsi, la trace partielle est l'opération de mesurer un système et se débarasser du résultat.

Puisque la base du sous-espace à tracer est quelconque, on peut alors écrire :

$$Tr_{\mathcal{H}_2}(\rho) = Tr_{\mathcal{H}_2}(I_{\mathcal{H}_1} \otimes U_{\mathcal{H}_2} \otimes I_{\mathcal{H}_3})\rho(I_{\mathcal{H}_1} \otimes U^{\dagger}_{\mathcal{H}_2} \otimes I_{\mathcal{H}_3})$$

où $U_{\mathcal{H}_2}$ est une transformation unitaire quelconque agissante dans $\mathcal{H}_2$.

2.4.1 Purification

Etant donné un système A dont l'opérateur de densité est ρ_A, il est possible d'introduire un autre système B, de telle manière que l'état $|\psi\rangle$ du système $A+B$ soit pur et $\rho_A = Tr_B\left(|\psi\rangle_{AB\ AB}\langle\psi|\right)$. On appelle cette procédure qui permet d'exprimer l'opérateur de densité ρ_A par l'état pur $|\psi\rangle_{AB}$, une *purification*. Il n'est pas nécessaire que le système B ait un sens physique, il est plutôt un outil mathématique permettant de travailler avec des états purs au lieu des densités de matrices.

Soient les deux bases, $\{|i\rangle\}, \{|\beta\rangle\}$ des espaces d'Hilbert $\mathcal{H}_A$ et $\mathcal{H}_B$ respectivement. On peut écrire $|\psi\rangle_{AB}$ comme suit :

$$|\psi\rangle_{AB} = \sum_{i,\alpha} c_{i\alpha}\,|i\rangle_A\,|\alpha\rangle_B$$

L'opérateur de densité du système $A+B$ est :

$$\rho = |\psi\rangle_{AB\ AB}\langle\psi| = \sum_{i,\alpha}\sum_{j,\beta} c_{i\alpha}c^*_{j\beta}\,|i\rangle_A\,|\alpha\rangle_{BA}\langle j|_B\langle\beta|$$

On peut exprimer l'opérateur de densité ρ_A comme suit :

$$\rho_A = \sum_{k,l}(\rho_A)_{k,l}\,|k\rangle_{AA}\langle l|$$

On dit que $|\psi\rangle_{AB\ AB}\langle\psi|$ est une purification de ρ_A si :

$$\begin{aligned}\rho_A &= Tr_B\left(|\psi\rangle_{AB\ AB}\langle\psi|\right) = \sum_{\gamma}{}_B\langle\gamma|\left(\sum_{i,\alpha}\sum_{j,\beta} c_{i\alpha}c^*_{j\beta}\,|i\rangle_A\,|\alpha\rangle_{BA}\langle j|_B\langle\beta|\right)|\gamma\rangle_B \\ &= \sum_{\gamma}\sum_{i,j} c_{i\gamma}c^*_{j\gamma}\,|i\rangle_{AA}\langle j|\end{aligned}$$

où on a utilisé les relations ${}_B\langle\beta|\gamma\rangle_B = \delta_{\beta\gamma}$ et $\langle\gamma|\alpha\rangle_B = \delta_{\gamma\alpha}$. L'égalité entre les deux dernières expressions de ρ_A (car les indices i, j, k, l, sont muets) implique :

$$(\rho_A)_{k,l} = \sum_{\gamma} c_{k\gamma}c^*_{l\gamma}$$

Et puisqu'on connaît les éléments de matrice $(\rho_A)_{k,l}$, ce dernier système admet toujours une solution si l'espace de Hilbert du système B est suffisamment large. En fait, il suffit que $\dim \mathcal{H}_B = \dim \mathcal{H}_A$ pour que ce système admette une solution.

Si ρ_A est exprimé dans sa base diagonale $\{|i\rangle\}$ (base propre) :

$$\rho_A = \sum_i p_i \, |i\rangle_{AA} \langle i|$$

il suffit de considérer un système B ayant le même espace d'état que A. En effet, une purification de ρ_A est donnée par :

$$|\psi\rangle_{AB} = \sum_{i,i'} \sqrt{p_i} \, |i\rangle_A \, |i'\rangle_B .$$

2.5 Décomposition de Schmidt [68]

Théorème 8 *Pour tout état $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ il existe deux bases orthonormales, $\{|i\rangle_A\}$ de $\mathcal{H}_A$ et $\{|i\rangle_B\}$ de $\mathcal{H}_B$ telles que :*

$$|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} \, |i\rangle_A \, |i'\rangle_B \ , \ \lambda_i \in \mathbb{R}^+, \ \sum_i \lambda_i = 1$$

Preuve Soit $\{|i\rangle_A\}$ et $\{|l\rangle_B\}$ deux bases orthonormales de $\mathcal{H}_A$ et $\mathcal{H}_B$, respectivement. Un état $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ peut s'écrire :

$$|\psi\rangle_{AB} = \sum_{i,l} a_{il} \, |i\rangle_A \, |l\rangle_B = \sum_i |i\rangle_A \, |s_i\rangle_B$$

où

$$|s_i\rangle_B = \sum_l a_{il} \, |l\rangle_B$$

Les états $|s_i\rangle_B$ ne sont pas forcément orthonormaux. Si la base $\{|i\rangle_A\}$ est une base propre de ρ_A dans $\mathcal{H}_A$ on peut écrire :

$$\rho_A = \sum_i \lambda_i \, |i\rangle_{A \, A} \langle i| \tag{2.1}$$

où *les λ_i et $\{|i\rangle_A\}$ sont déterminés par la forme diagonale unique de ρ_A*. Mais ρ_A peut être aussi exprimé par la trace partielle :

$$\begin{aligned} \rho_A &= Tr_B(|\psi\rangle_{AB \, AB} \langle\psi|) \\ &= Tr_B \left(\sum_{i,j} |i\rangle_{A \, A} \langle j| \otimes |s_i\rangle_{B \, B} \langle s_j| \right) = \sum_{i,j} {}_B\langle s_j|s_i\rangle_B \, |i\rangle_{A \, A} \langle j| \end{aligned} \tag{2.2}$$

En comparant (2.1) avec (2.2) on trouve :

$$_B\langle s_j|s_i\rangle_B = \lambda_i \delta_{ij}$$

Ce qui prouve l'orthogonalité des $|s_i\rangle_B$. Pour avoir des vecteurs orthonormaux, on choisit l'ensemble $\{|i\rangle_B\}$ tel que :

$$|i\rangle_B = \lambda_i^{-\frac{1}{2}} |s_i\rangle_B$$

L'état $|\psi\rangle_{AB}$ devient dans ce cas :

$$|\psi\rangle_{AB} = \sum_i \lambda_i^{\frac{1}{2}} |i\rangle_A |i\rangle_B$$

■

2.6 Théorème GHJW [38, 29]

Théorème 9 *Si $|\Phi_1\rangle_{AB}$ et $|\Phi_2\rangle_{AB}$ sont deux purifications de ρ_A, alors il existe une transformation unitaire U_B dans $\mathcal{H}_B$ telle que :*

$$|\Phi_2\rangle_{AB} = (I_A \otimes U_B) |\Phi_1\rangle_{AB}$$

Preuve Un opérateur de densité ρ_A s'écrit dans sa base orthonormale propre $\{|i\rangle_A\}$:

$$\rho_A = \sum_i \lambda_i |i\rangle_{A\,A}\langle i| \ , \ \lambda_i \in \mathbb{R}^+$$

Soit les deux réalisations de ρ_A :

$$\rho_A = \sum_t \alpha_t |\phi_t\rangle_{A\,A}\langle \phi_t| \tag{2.3}$$

$$\rho_A = \sum_r \beta_r |\varphi_r\rangle_{A\,A}\langle \varphi_r| \tag{2.4}$$

De (2.3) et (2.4) on peut déduire les deux purifications $|\Phi_1\rangle_{AB}$ et $|\Phi_2\rangle_{AB}$ de ρ_A,

$$|\Phi_1\rangle_{AB} = \sum_t \alpha_t^{\frac{1}{2}} |\phi_t\rangle_A |u_t\rangle_B$$

$$|\Phi_2\rangle_{AB} = \sum_r \beta_r^{\frac{1}{2}} |\varphi_r\rangle_A |v_r\rangle_B$$

avec

$$_B\langle u_t|u_s\rangle_B = \delta_{ts}$$

$$_A\langle v_n|v_m\rangle_A = \delta_{nm}$$

Comme résultat direct de la décomposition de Schmidt on a :

$$|\Phi_1\rangle_{AB} = \sum_i \lambda_i^{\frac{1}{2}} |i\rangle_A |i\rangle_B$$

$$|\Phi_2\rangle_{AB} = \sum_i \lambda_i^{\frac{1}{2}} |i\rangle_A \left|i'\right\rangle_B$$

où

$$_A\langle i|j\rangle_A = \delta_{ij}$$

$$_B\left\langle i'|j'\right\rangle_B = \delta_{i'j'}$$

On peut toujours considérer ces deux purifications comme ayant le même nombre de termes (en complétant la somme la plus courte par des termes de probabilité nulle). Il existe alors une transformation unitaire qui agit dans B telle que :

$$|\Phi_2\rangle_{AB} = (I_A \otimes U_B) |\Phi_1\rangle_{AB}$$

où

$$\left|i'\right\rangle_B = U_B |i\rangle_B$$

On a donc

$$\begin{aligned} |\Phi_2\rangle_{AB} &= \sum_r \beta_r^{\frac{1}{2}} |\varphi_r\rangle_A |v_r\rangle_B = I_A \otimes U_B |\Phi_1\rangle_{AB} \\ &= (I_A \otimes U_B) \sum_t \alpha_t^{\frac{1}{2}} |\phi_t\rangle_A |u_t\rangle_B = \sum_t \alpha_t^{\frac{1}{2}} |\phi_t\rangle_A |w_t\rangle_B \end{aligned}$$

avec

$$|w_t\rangle_B = U_B |u_t\rangle_B$$

Ainsi les deux formes de ρ_A sont décrites par la même purification $|\Phi_1\rangle_{AB}$ dont la première correspond à une mesure (de résultats non communiqués par Bob à Alice) effectuée sur $|\Phi_1\rangle_{AB}$ de l'observable admettant comme états propres les $|u_t\rangle_B$, la seconde à une mesure sur le même état de l'observable admettant comme états propres les $|w_t\rangle_B$.

■

Donc, les diverses préparations équivalentes de l'opérateur de densité correspondent à différents types de mesures non lues dans B qui peuvent toutes être accomplies sur la même purification. Cette conclusion constitue le théorème de Gisin, Hughston, Josza et Wootters (GHJW) [38, 29].

2.7 Évolutions des systèmes quantiques

Supposons qu'on a un opérateur $\mathsf{U} \in \mathcal{L}(\mathcal{H})$ qui agit sur un système isolé décrit par l'état $|\psi\rangle$. Si $\mathcal{H}$ est de dimension finie, quelles conditions doit satisfaire U ? Si on veut qu'une telle action produise un autre état quantique, alors U doit préserver la norme :

$$||\mathsf{U}|\psi\rangle|| = 1, \forall |\psi\rangle \in \mathcal{H}$$

Cette dernière équation implique que U doit être unitaire. En fait, toute matrice unitaire est une opération valide sur l'état quantique. Maintenant, si le systeme isolé est un mélange statistique d'opérateurs de densité ρ, l'application de l'opérateur unitaire U sur ρ donne l'opérateur de densité $\mathsf{U}\rho\mathsf{U}^\dagger$, car si ρ est l'opérateur de densité du mélange statistique $\mathcal{E} = \{(p_i, |\psi_i\rangle)\}$ et si on applique U sur chaque état de $\mathcal{E}$, on obtient le mélange statistique $\mathcal{E}' = \{(p_i, \mathsf{U}|\psi_i\rangle)\}$ dont l'opérateur de densité est :

$$\rho' = \sum_i p_i(\mathsf{U}|\psi_i\rangle\langle\psi_i|\mathsf{U}^\dagger) = \mathsf{U}\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)\mathsf{U}^\dagger = \mathsf{U}\rho\mathsf{U}^\dagger$$

En fait, l'ensemble des opérations physiques que nous pouvions appliquer à un état quantique est plus large que celui des opérateurs unitaires.

Définition 3 *Soit l'ensemble de matrices :*

$$S = \{S_i : i \in \{1, ..., k\}, S_i : \mathcal{H} \to \mathcal{G}\}$$

qui satisfont

$$\sum_{i=1}^{k} S_i^\dagger S_i = I_{\mathcal{H}}.$$

On appelle opération quantique ou super-opérateur la transformation $Q_S : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{G})$ *telle que :*

$$Q_S(X) = \sum_{i=1}^{k} S_i X S_i^\dagger \quad , \quad X \in \mathcal{L}(\mathcal{H})$$

Maintenant on peut montrer que toute opération quantique préserve la trace et la positivité.

Lemme 5 *Soit un ensemble de matrices* $S = \{S_i : i \in \{1, .., k\}, S_i : \mathcal{H} \rightarrow \mathcal{G}\}$, *telle que* $\sum_{i=1}^{k} S_i^\dagger S_i = I_{\mathcal{H}}$. *On a :*

$$Tr(Q_S(X)) = Tr(X), \forall X \in \mathcal{L}(\mathcal{H})$$

Preuve

$$\begin{aligned} Tr(Q_S(X)) &= Tr\left(\sum_{i=1}^{k} S_i X S_i^\dagger\right) \\ &= \sum_{i=1}^{k} Tr(S_i X S_i^\dagger) \\ &= \sum_{i=1}^{k} Tr(S_i^\dagger S_i X) \\ &= Tr\left(\sum_{i=1}^{k} S_i^\dagger S_i X\right) \\ &= Tr(X) \end{aligned}$$

■

On démontre maintenant que toute opération quantique préseve la positivité.

Lemme 6 *Soit un ensemble de matrices* $S = \{S_i : i \in \{1, .., k\}, S_i : \mathcal{H} \rightarrow \mathcal{G}\}$, *telles que* $\sum_{i=1}^{k} S_i^\dagger S_i = I_{\mathcal{H}}$. *On a :*

$$X \text{ est positif} \Longrightarrow Q_S(X) \text{est positif}$$

Preuve Pour tout ket $|\psi\rangle \in \mathcal{G}$, on a

$$\langle\psi| Q_S(X) |\psi\rangle = \langle\psi| \left(\sum_i S_i X S_i^\dagger\right) |\psi\rangle = \sum_i \langle\psi| S_i X S_i^\dagger |\psi\rangle = \sum_i \langle\psi_i| X |\psi_i\rangle$$

où $|\psi_i\rangle = S_i^\dagger |\psi\rangle$. Et puisque X est supposé positif, alors $\langle\psi_i| X |\psi_i\rangle \geq 0$, ce qui donne $\sum_i \langle\psi_i| X |\psi_i\rangle \geq 0$.

■

Corollaire 4 *Soit un ensemble de matrices* $S = \{S_i : i \in \{1,..,k\}, S_i : \mathcal{H} \to \mathcal{G}\}$, *telles que* $\sum_{i=1}^{k} S_i^\dagger S_i = I_\mathcal{H}$. *Si* ρ *est un opérateur de densité alors* $Q_S(\rho)$ *l'est aussi.*

Preuve C'est un résultat direct des deux lemmes 5 et 6.

■

L'inverse n'est pas toujours vrai. Pour voir cela, considérons l'exemple suivant.

Exemple 10 *L'opérateur* X *défini comme suit :*

$$X = 2 |0\rangle \langle 0| - |1\rangle \langle 1|$$

n'est pas un opérateur de densité car il a une valeur propre négative. On peut definir une opération quantique Q_S *sur l'ensemble* $S = \{|0\rangle \langle 0|, |1\rangle \langle 1|\}$, *car*

$$|0\rangle \langle 0| + |1\rangle \langle 1| = I_{\mathcal{H}^{\otimes 2}}.$$

Ce qui donne :

$$Q_S(X) = \sum_{i=1}^{2} S_i X S_i^\dagger = 1 = I_{\mathcal{H}^{\otimes 1}}$$

Donc, $Q_S(X)$ *est un opérateur de densité dans* $\mathcal{L}(\mathcal{H}^{\otimes 1}) = \mathcal{L}(\mathbb{C})$, *malgré le fait que* X *ne l'est pas.*

2.7.1 Représentation de Kraus

Supposons que le système A, décrit à un instant donné par l'opérateur de densité ρ_A, est mis en contact avec le reste de l'univers E sans lui être initialement corrélé. Puisqu'on a vu qu'il est toujours possible de considérer l'état d'un système

comme étant le résultat d'une trace partielle sur un état pur appartenant à un système plus large,on peut donc décrire l'univers E par l'état pur $|0\rangle_E$ à cet instant. Supposons qu'on a un opérateur unitaire U_{AE} qui agit sur le systeme isolé décrit par l'état $\rho_A \otimes |0\rangle_{EE}\langle 0|$. Soit $\rho_A^{'}$ le nouvel opérateur de densité de A aprés l'action de U_{AE}. $\rho_A^{'}$ vérifie l'équation :

$$\begin{aligned}\rho'_A &= Tr_E\left(U_{AE}\rho_A \otimes |0\rangle_{EE}\langle 0| U_{AE}^{\dagger}\right) \\ &= \sum_i {}_E\langle i|\left(U_{AE}\rho_A \otimes |0\rangle_{EE}\langle 0| U_{AE}^{\dagger}\right)|i\rangle_E \\ &= \sum_i (S_i)_A \rho_A \left(S_i^{\dagger}\right)_A\end{aligned}$$

où $\{|i\rangle_E\}$ est une base de E et $(S_i)_A = {}_E\langle i| U_{AE}|0\rangle_E$. Les opérateurs $\{(S_i)_A\}$ représentent une opération quantique car :

$$\begin{aligned}\sum_i \left(S_i^{\dagger}\right)_A (S_i)_A &= \sum_i {}_E\langle i| U_{AE}|0\rangle_{EE}^{\dagger}\langle i| U_{AE}|0\rangle_E \\ &= \sum_i {}_E\langle 0| U_{AE}^{\dagger}|i\rangle_{EE}\langle i| U_{AE}|0\rangle_E = {}_E\langle 0| U_{AE}^{\dagger}U_{AE}|0\rangle_E \\ &= {}_E\langle 0| I_A \otimes I_E|0\rangle_E = I_A\end{aligned}$$

L'équation

$$\rho'_A = \sum_i (S_i)_A \rho_A \left(S_i^{\dagger}\right)_A$$

est connue par *la représentation de Kraus* [48].

2.8 Mesure

La mesure est une autre opération physique possible qui peut être appliquée à un état quantique. Elle représente le processus qui fait la connexion entre les mondes quantique et classique. C'est une opération irréversible qui détruit l'information quantique sur une propriété mesurable (observable) d'un système quantique et la remplace par de l'information classique. En mécanique quantique, la mesure d'une observable d'un système quantique (tel que le moment, l'énergie ou le spin) est associée à un opérateur hermitique (observable), A, dans l'espace de Hilbert. Si $|\psi\rangle$ est un vecteur propre de A avec la valeur propre λ, alors mesurer un système dont l'état est $|\psi\rangle$ donnera toujours

le résultat λ. Si l'état n'est pas un vecteur propre de A, la mesure forcera le système à donner au hasard comme résultat une des valeurs propres de l'observable A correspondant à un des vecteurs propres de A. Par exemple, un qubit $|\psi\rangle$ en superposition des états $|0\rangle$ et $|1\rangle$ peut s'écrire :

$$|\psi\rangle = \sum_{i=0}^{1} \alpha_i |i\rangle\,, \text{ où } \sum_{i=0}^{1} |\alpha_i|^2 = 1.$$

Si on mesure le qubit on aura les résultats :

$$\begin{cases} 0, \text{ avec probabilité } |\alpha_0|^2 \\ 1, \text{ avec probabilité } |\alpha_1|^2 \end{cases}$$

La somme des probabilités est égale à 1 puisque $|\psi\rangle$ est supposé normé. Il est aussi possible de mesurer une partie d'un état qui se trouve sous la forme de produit tensoriel, comme il est aussi possible d'effectuer la mesure dans des bases différentes. Supposons, par exemple, qu'on veut mesurer le sous-espace $\mathcal{K}$ de l'état quantique $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ dans la base $\{|\nu_i\rangle\}$ de $\mathcal{K}$. L'état $|\psi\rangle$ peut s'écrire :

$$|\psi\rangle = \sum_i \sqrt{\alpha_i} |\xi_i\rangle |\nu_i\rangle\,, \quad |\xi_i\rangle \in \mathcal{H}$$

où

$$\alpha_i \geq 0, \sum_i \alpha_i = 1.$$

La mesure de l'espace $\mathcal{K}$ donne le résultat $|\nu_i\rangle$ avec probabilité α_i et réduit l'état $|\psi\rangle$ à $|\xi_i\rangle |\nu_i\rangle$. On peut aussi décrire le processus de mesure grâce aux mesures projectives.

Définition 4 *Une mesure projective ou de von Neumann dans l'espace de Hilbert $\mathcal{H}$ est un ensemble de projecteurs $\{\Pi_i \in \mathcal{L}(\mathcal{H}) : i \in \{1, ..., n\}\}$ tel que :*

$$\Pi_i \Pi_j = \begin{cases} \Pi_i & si\ i = j \\ 0 & sinon \end{cases} \iff \Pi_i \Pi_j = \delta_{ij} \Pi_i \tag{2.5}$$

$$\Pi_i^\dagger = \Pi_i \tag{2.6}$$

$$\sum_{i=1}^{n} \Pi_i = I_{\mathcal{H}} \tag{2.7}$$

Si l'état du système est $|\psi\rangle \in \mathcal{H}$ juste avant la mesure, le résultat a_i est obtenu avec une probabilité égale à :

$$p(i) = \langle\psi| \Pi_i |\psi\rangle .$$

et l'état $|\psi\rangle$ devient :

$$\frac{1}{\sqrt{p(i)}} \Pi_i |\psi\rangle .$$

Dans le cas où l'état mesuré est un mélange statistique, on mesure chacun de ses états. Soit un système décrit par le mélange statistique $\mathcal{E} = \{ (q_j, |\psi_j\rangle) \}$. La probabilité que la mesure du système donne le résultat a_i est :

$$\begin{aligned} p(i) &= \sum_j q_j \langle\psi_j| \Pi_i |\psi_j\rangle \\ &= Tr(\Pi_i \rho) \end{aligned} \tag{2.8}$$

Si le résultat a_i provient de la mesure de $|\psi_k\rangle$, l'état du système juste après la mesure est :

$$\frac{\Pi_i |\psi_k\rangle}{\sqrt{\langle\psi_k| \Pi_i |\psi_k\rangle}}$$

où Π_i est le projecteur sur l'espace associé à la valeur propre a_i. Puisque le système est décrit par le mélange statistique $\mathcal{E}$, alors l'état après la mesure du résulta a_i est :

$$\rho' = \sum_k p(k|i) \frac{(\Pi_i |\psi_k\rangle \langle\psi_k| \Pi_i)}{\langle\psi_k| \Pi_i |\psi_k\rangle} \tag{2.9}$$

où $p(k|i)$ est la probabilité que le système soit dans l'état $\frac{\Pi_i|\psi_k\rangle}{\sqrt{\langle\psi_k|\Pi_i|\psi_k\rangle}}$ étant donné que le résultat mesuré est a_i. D'autre part, on a :

$$p(k,i) = p(i)p(k|i)$$

où $p(k,i)$ est la probabilité que le système soit dans l'état $\frac{\Pi_i|\psi_k\rangle}{\sqrt{\langle\psi_k|\Pi_i|\psi_k\rangle}}$ et le résultat de la mesure est a_i. De la même façon, on a :

$$p(k,i) = q_k p(i|k)$$

d'où

$$p(k|i) = \frac{p(k,i)}{p(i)} = \frac{q_k p(i|k)}{p(i)} \tag{2.10}$$

Puisque la probabilité de mesurer a_i si le système est dans l'état $|\psi_k\rangle$ est

$$p(i|k) = \langle\psi_k| \Pi_i |\psi_k\rangle ,$$

le remplacement de $p(k|i)$ et $p(i)$ par leurs expressions de (2.10) et (2.8) dans (2.9) donne :

$$\begin{aligned} \rho' &= \sum_k \frac{q_k p(i|k)}{Tr(\Pi_i \rho)} \frac{(\Pi_i |\psi_k\rangle \langle\psi_k| \Pi_i)}{\langle\psi_k| \Pi_i |\psi_k\rangle} = \sum_k \frac{q_k}{Tr(\Pi_i \rho)} (\Pi_i |\psi_k\rangle \langle\psi_k|) \Pi_i \qquad (2.11) \\ &= \frac{\Pi_i \left(\sum_k q_k |\psi_k\rangle \langle\psi_k| \right) \Pi_i}{Tr(\Pi_i \rho)} = \frac{\Pi_i \rho \Pi_i}{Tr(\Pi_i \rho)} \end{aligned}$$

Pour la mesure du sous-espace $\mathcal{K}$ de l'état $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ dans la base $\{|\nu_i\rangle\}$, on considère la mesure projective :

$$\{\Pi_i = I_{\mathcal{H}} \otimes |\nu_i\rangle \langle\nu_i|\}.$$

Ceci est en accord avec la définition de la mesure projective car les éléments de l'ensemble $\{\Pi_i = I_{\mathcal{H}} \otimes |\nu_i\rangle \langle\nu_i|\}$ vérifient les relations (2.5), (2.6) et aussi (2.7) :

$$\sum_i I_{\mathcal{H}} \otimes |\nu_i\rangle \langle\nu_i| = I_{\mathcal{H}} \otimes I_{\mathcal{K}} = I_{\mathcal{H}\otimes\mathcal{K}}$$

On peut vérifier ça avec l'exemple suivant. Si on mesure l'état :

$$|\psi\rangle = \sum_{i=0}^{1} \sqrt{\alpha_i} |\xi_i\rangle |\nu_i\rangle \in \mathcal{H} \otimes \mathcal{K}$$

Par la mesure projective $\{\Pi_i = I_{\mathcal{H}} \otimes |\nu_i\rangle \langle\nu_i|\}$, on obtient le résultat i avec probabilité

$$\begin{aligned} p_i &= Tr(\Pi_i |\psi\rangle \langle\psi|) \\ &= \sum_{j,k} \sqrt{\alpha_i \alpha_k} \langle\nu_i|\nu_j\rangle \langle\nu_k|\nu_i\rangle Tr |\xi_j\rangle \langle\xi_k| \\ &= \sqrt{\alpha_i \alpha_i} Tr |\xi_i\rangle \langle\xi_i| \\ &= \alpha_i \end{aligned}$$

et l'état après la mesure est :

$$\begin{aligned} \frac{1}{\sqrt{p_i}} \Pi_i |\psi\rangle &= \frac{1}{\sqrt{\alpha_i}} (I_{\mathcal{H}} \otimes |\nu_i\rangle \langle\nu_i|)(\sum_j \sqrt{\alpha_j} |\xi_j\rangle |\nu_j\rangle) \\ &= \frac{1}{\sqrt{\alpha_i}} \sum_j \sqrt{\alpha_j} |\xi_j\rangle |\nu_i\rangle \langle\nu_i|\nu_j\rangle \\ &= |\xi_i\rangle |\nu_i\rangle \end{aligned}$$

Ce qui est en accord avec les résultats déjà trouvés pour la mesure d'un sous-espace dans la base $\{|\nu_i\rangle\}$.

2.9 Mesures généralisées

Observer un système A comme partie d'un système plus large $A+B$ donne un éclaircissement fascinant de l'opérateur de densité, liant les idées de mesure et de décohérence (intrication avec l'environnement) à celle d'intrication. Ce point de vue permet d'étendre les mesures projectives de von Neumann à une classe plus étendue de mesures généralisées. Leurs lois de probabilité et leurs effets sur A peuvent être obtenus en les regardant comme résultat d'une mesure projective sur un système plus large $A+B$. Les mesures généralisées permettent de définir de nouvelles manipulations de l'information des systèmes ouverts. Une mesure généralisée se définit par un ensemble d'opérateurs M_i satisfaisant la relation de fermeture :

$$\sum_i M_i^\dagger M_i = I \tag{2.12}$$

mais non nécessairement la relation d'orthogonalité : $M_i^\dagger M_j \neq 0$ si $i \neq j$ en général. La mesure généralisée sur un système dans l'état $|\psi\rangle_A$ donne le résultat k avec la probabilité :

$$p_k = {}_A\langle\psi| M_k^\dagger M_k |\psi\rangle_A \tag{2.13}$$

L'équation (2.12) garantit la conservation de la probabilité totale de mesure. Si le résultat aprés la mesure est k, $|\psi\rangle_A$ devient

$$|\psi\rangle_{A|k} = \frac{M_k |\psi\rangle_A}{\sqrt{{}_A\langle\psi| M_k^\dagger M_k |\psi\rangle_A}} \tag{2.14}$$

La mesure généralisée sur un système d'opérateur de densité ρ_A donne le résultat k avec probabilité :

$$p_k = Tr\left(\rho_A M_k^\dagger M_k\right) \tag{2.15}$$

Si le résultat après la mesure est k, ρ_A devient

$$\rho_{A|k} = \frac{M_k \rho M_k^\dagger}{Tr(\rho M_k^\dagger M_k)} \tag{2.16}$$

Les équations : (2.12), (2.15) et (2.16) généralisent (2.7), (2.10) et (2.11), valables pour des mesures projectives, cas particulier de mesures généralisées correspondant à $M_k = M_k^\dagger = P_k$.

2.10 Réalisation d'une mesure généralisée quelconque par une transformation unitaire et une mesure projective

Soient $\{M_i \mid i = 1..m\}$ une mesure généralisée dans $\mathcal{H}_A$ tel que $\dim \mathcal{H}_A = n$, et $\mathcal{H}_B$ un autre espace d'Hilbert tel que $\dim \mathcal{H}_B = m$. Soient $|\psi\rangle$ un état quelconque dans $\mathcal{H}_A$, et $\{|i\rangle\}_{i=1}^m$ une base orthonormale dans $\mathcal{H}_B$. Considérons une application linéaire U_{AB} de $\mathcal{H}_A \otimes \mathcal{H}_B$ telle que sur tout état produit tensoriel $|\psi\rangle_A |0\rangle_B$:

$$U_{AB}(|\psi\rangle_A |0\rangle_B) = \sum_{i=1}^{m} (M_i |\psi\rangle_A) |i\rangle_B \tag{2.17}$$

On peut voir que U_{AB} préserve le produit scalaire dans $\mathcal{H}_A \otimes \mathcal{H}_B$. Soit $|\varphi\rangle_A$ un autre état de $\mathcal{H}_A$, on a :

$$({}_A\langle\varphi|_B \langle 0|)(|\psi\rangle_A |0\rangle_B) = ({}_A\langle\varphi|\psi\rangle_A)\,({}_B\langle 0|0\rangle_B) = {}_A\langle\varphi|\psi\rangle_A$$

Aussi :

$$\begin{aligned}
\left({}_A\langle\varphi|_B \langle 0| U_{AB}^\dagger\right)(U_{AB}(|\psi\rangle_A |0\rangle_B)) &= \left(\sum_{j=1}^{m} {}_A\langle\varphi|\,({}_B\langle j| M_j^\dagger)\right)\left(\sum_{i=1}^{m} (M_i |\psi\rangle_A)\,|i\rangle_B\right) \\
&= \sum_{i,j=1}^{m} {}_A\langle\varphi| M_j^\dagger M_i |\psi\rangle_A)_B\langle j|i\rangle_B \\
&= \sum_{i,j=1}^{m} {}_A\langle\varphi| M_j^\dagger M_i |\psi\rangle_A)\delta_{ij} \\
&= {}_A\langle\varphi| \sum_{i=1}^{m} M_i^\dagger M_i |\psi\rangle_A = {}_A\langle\varphi|\psi\rangle_A
\end{aligned}$$

La relation (2.17) définit U_{AB} sur n vecteurs de l'espace $\mathcal{H}_A \otimes \mathcal{H}_B$. Il suffit alors d'ajouter $nm - n$ vecteurs orthogonaux aux précédents et entre eux pour avoir un U_{AB} unitaire agissant dans $\mathcal{H}_A \otimes \mathcal{H}_B$ et complètement défini. Cette opération unitaire intrique en général $\mathcal{H}_A$ et $\mathcal{H}_B$. Faisons ensuite une mesure projective dans $\mathcal{H}_B$, définie par les projecteurs $P_k = |k\rangle_{BB}\langle k|$. Le résultat k est obtenu avec probabilité égale à :

$$\begin{aligned} p(k) &= \left(\left({}_A\langle\psi|_B \langle 0|\right) U^\dagger\right)\left(I_{\mathcal{H}_A} \otimes |k\rangle_B \langle k|\right)\left(U(|\psi\rangle_A |0\rangle_B)\right) \\ &= \left(\sum_{j=1}^{m} {}_A\langle\psi|_B \langle j|\, M_j^\dagger\right)\left(I_{\mathcal{H}_A} \otimes |k\rangle_B \langle k|\right)\left(\sum_{i=1}^{m}(M_i |\psi\rangle_A)\, |i\rangle_B\right) \\ &= \sum_{i,j=1}^{m}\left({}_A\langle\psi|\, M_j^\dagger\right)\left({}_B\langle j|k\rangle_{BB}\langle k|i\rangle_B\right)\left((M_i |\psi\rangle_A)\right) \\ &= \sum_{i,j=1}^{m}\left({}_A\langle\psi|\, M_j^\dagger\right)\left((M_i |\psi\rangle_A)\right)\delta_{ik}\delta_{jk} \\ &= {}_A\langle\psi|\left(M_k^\dagger M_k\right)|\psi\rangle_A \end{aligned} \tag{2.18}$$

Après une mesure von Neumann, le système $\mathcal{H}_A \otimes \mathcal{H}_B$ est projeté avec une probabilité égale à ${}_A\langle\psi|\, M_k^\dagger M_k\, |\psi\rangle_A$dans l'état :

$$\begin{aligned} |\psi'\rangle_{AB} &= \frac{I_{\mathcal{H}_A} \otimes |k\rangle_B \langle k|\left(\sum_{i=1}^{m}(M_i |\psi\rangle_A)\, |i\rangle_B\right)}{\sqrt{{}_A\langle\psi|\, M_k^\dagger M_k\, |\psi\rangle_A}} \\ &= \frac{(M_k |\psi\rangle_A)\, |k\rangle_B}{\sqrt{{}_A\langle\psi|\, M_k^\dagger M_k\, |\psi\rangle_A}} \end{aligned}$$

Une mesure projective de B donnant le résultat k, projette bel et bien A dans l'état décrit par (2.14).

Si l'état initial de $\mathcal{H}_A$ est un mélange statistique: $\{q_j, |\psi_j\rangle_A\}$, chaque état du mélange est transformé linéairement suivant (2.17) :

$$\begin{aligned} U(\sum_j q_j |\psi_j\rangle_A |0\rangle_{BA}\langle\psi_j|_A \langle 0|_B)U^\dagger &= \sum_{i,i',j}(q_j M_i |\psi_j\rangle_{AA}\langle\psi_j|\, M_{i'}^\dagger) \otimes |i\rangle_{BB}\langle i'| \\ &= \sum_{i,i'}(M_i \rho M_{i'}^\dagger) \otimes |i\rangle_{BB}\langle i'| \end{aligned}$$

Faisons une mesure de Von Neumann dans $\mathcal{H}_B$, définie par les projecteurs $P_k = |k\rangle_{BB}\langle k|$. La probabilité de mesurer k est :

$$\begin{aligned} & Tr\left(I_{\mathcal{H}_A} \otimes |k\rangle_{BB}\langle k| \sum_{i,i'}(M_i \rho M_{i'}^\dagger) \otimes |i\rangle_{BB}\langle i'|\right) \\ = \; & Tr((M_k \rho M_k^\dagger) \otimes |k\rangle_{BB}\langle k|) = Tr(M_k \rho M_k^\dagger) \end{aligned} \tag{2.19}$$

Par une mesure de von Neumann, le système $\mathcal{H}_A \otimes \mathcal{H}_B$ est projeté avec la probabilité $Tr(M_k \rho M_k^\dagger)$ dans l'état :

$$\begin{aligned} \rho' &= \frac{(I_{\mathcal{H}_A} \otimes |k\rangle_B\langle k|)\left(\sum_{i,i'}(M_i \rho M_{i'}^\dagger) \otimes |i\rangle_{BB}\langle i'|\right)(I_{\mathcal{H}_A} \otimes |k\rangle_B\langle k|)}{Tr(M_k \rho M_k^\dagger)} \\ &= \frac{(M_k \rho M_k^\dagger) \otimes |k\rangle_{BB}\langle k|}{Tr(M_k \rho M_k^\dagger)} \end{aligned} \tag{2.20}$$

Une mesure projective de B donnant le résultat k projette A dans l'état décrit par (2.16). On peut donc réaliser n'importe quelle mesure généralisée dans un système A, par une intrication unitaire de A avec B suivie d'une mesure projective de B.

La règle qui définit la probabilité dans le cas d'une mesure généralisée est

$$Tr(M_i \rho M_i^\dagger) = Tr(\rho M_i^\dagger M_i)$$

Ceci contient le terme $M_i^\dagger M_i$, qui est un opérateur positif. On peut alors définir cette probabilité par la donnée d'un ensemble $\{E_i = M_i^\dagger M_i\}$ d'opérateurs positifs telle que

$$\sum_i E_i = I$$

sans séparer explicitement les deux parties adjointes constituant chaque E_i. La probabilité de trouver le résultat i dans ce cas est

$$Tr(\rho E_i)$$

et la somme des probabilités :

$$\sum_i Tr(\rho E_i) = Tr(\rho) = 1$$

On appelle l'ensemble $\{E_i\}$ un POVM (Positive OperatorValued Measure). De la même façon qu'auparavant, on peut réaliser un POVM $\{E_i\}$ qui transforme ρ suivant la relation

$$\rho \to \sum_i \sqrt{E_i}\rho\sqrt{E_i}$$

par l'intrication unitaire de A avec B suivie d'une mesure projective de B. Dans ce cas, il suffit de profiter du fait que les E_i sont des opérateurs positifs et peuvent, alors, s'écrire :

$$E_i = \sqrt{E_i}\sqrt{E_i}$$

En posant

$$M_i = \sqrt{E_i} \text{ et donc } M_i^\dagger = \sqrt{E_i}$$

Les relations (2.19) et (2.20) deviennent respectivement :

$$\begin{aligned} & Tr\left(I_{\mathcal{H}_A} \otimes |k\rangle_{BB}\langle k| \sum_{i,i'}(M_i\rho M_i^\dagger) \otimes |i\rangle_{BB}\langle i'|\right) \\ = \; & Tr((\sqrt{E_k}\rho\sqrt{E_k}) \otimes |k\rangle_{BB}\langle k|) = Tr(\sqrt{E_k}\rho\sqrt{E_k}) \\ & \rho' = \frac{(\sqrt{E_k}\rho\sqrt{E_k}) \otimes |k\rangle_{BB}\langle k|}{Tr(\sqrt{E_k}\rho\sqrt{E_k})} \end{aligned}$$

La différence principale entre mesure généralisée (ou POVM) et mesure de von Neumann et que cette dernière donne des résultats successifs identiques (voir relation (2.5)) ce qui n'est pas nécessairement vrai pour une mesure généralisée, puisque en général on a

$$E_k E_{k'} \neq \delta_{kk'} E_k \quad \text{et} \quad M_k M_{k'} \neq \delta_{kk'} M_k$$

Un POVM $\{E_i\}$ peut être aussi réalisé par un choix convenable de système auxiliaire B et de mesure non locale sur les deux systèmes A+B initialement non intriqués. Autrement dit, on peut élargir l'espace de Hilbert au-delà de celui où les E_i sont définis et trouver dans l'espace élargi un ensemble complet de projecteurs orthogonaux $\{P_i\}$ tels que les $\{E_i\}$ correspondent à la projection des P_i dans l'espace initial (théorème de Neumark).

2.11 Théorème de non-clonage

Théorème 11 *Soient* $|\psi\rangle \in \mathcal{H}_1$ *un état quelconque et* $|\varphi\rangle \in \mathcal{H}_2$ *tel que* $\dim \mathcal{H}_1 = \dim \mathcal{H}_2$, *l'état clonant. Et soit* $|\chi\rangle \in \mathcal{H}_3$ *un état ancillaire qu'on utilise en cas de besoin. Il n'existe*

pas de transformation unitaire qui permette de cloner parfaitement $|\psi\rangle$. *C'est-à-dire, il n'existe pas de* $U : \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \longrightarrow \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ *tel que :*

$$U(|\psi\rangle |\varphi\rangle |\chi\rangle) = |\psi\rangle |\psi\rangle \left|\chi_\psi\right\rangle$$

où $\left|\chi_\psi\right\rangle$ *est un état dépendant de l'état* $|\psi\rangle$ *qu'on veut cloner.*

Preuve Soit $\{|u_i\rangle\}$ une base ortonormale de $\mathcal{H}_1$, donc on peut écrire

$$|\psi\rangle = \sum_i c_i |u_i\rangle$$

D'où

$$\begin{aligned} U(|\psi\rangle |\varphi\rangle |\chi\rangle) &= U(\sum_i c_i |u_i\rangle |\varphi\rangle |\chi\rangle) = \sum_i c_i U(|u_i\rangle |\varphi\rangle |\chi\rangle) \\ &= \sum_i c_i \left(|u_i\rangle |u_i\rangle \left|\chi_{u_i}\right\rangle\right) \end{aligned}$$

D'autre part, on a aussi

$$\begin{aligned} U(|\psi\rangle |\varphi\rangle |\chi\rangle) &= |\psi\rangle |\psi\rangle \left|\chi_\psi\right\rangle = \left(\sum_i c_i |u_i\rangle\right) \left(\sum_i c_i |u_i\rangle\right) \left|\chi_\psi\right\rangle \\ &= \sum_{i,j} c_i c_j |u_i\rangle |u_j\rangle \left|\chi_\psi\right\rangle \end{aligned}$$

Mais, en général $\sum_i c_i \left(|u_i\rangle |u_i\rangle \left|\chi_{u_i}\right\rangle\right)$ est différent de $\sum_{i,j} c_i c_j |u_i\rangle |u_j\rangle \left|\chi_\psi\right\rangle$.

■

C'est donc la linéarité de la mécanique quantique qui interdit le clonage. La preuve exposée ici n'est pas générale car on a supposé que seules les transformations unitaires sont permises, alors qu'on a vu dans la section 2.7 que l'ensemble des opérations quantiques permises est plus grand. Ce problème est étudié dans [4] où l'on montre que le théorème de non-clonage est toujours vrai.

2.12 Distance

La notion de distance est utilisée pour quantifier le degré de distinguabilité entre deux état quantiques. Dans le cas classique, si on a deux distributions de probabilité P

et Q d'un ensemble d'événements $\{1, 2, ..., n\}$:

$$P = \{p_1, ..., p_n\}$$

$$Q = \{q_1, ..., q_n\}$$

La distance entre ces deux distributions est donnée par

$$D(P, Q) = \frac{1}{2}\sum_{i=1}^{n} |p_i - q_i| \tag{2.21}$$

La présence du facteur $\frac{1}{2}$ assure que $D(P, Q) \leq 1$. On a les propriétés suivantes de cette distance :

$$D(P, P) = 0$$

$$D(P, Q) = D(Q, P)$$

$$D(P, R) \leq D(P, Q) + D(Q, R)$$

Théorème 12 *Soit deux distributions de probabilité P et Q d'un ensemble d'événements $\{1, 2, .., n\}$:*

$$P = \{p_1, ..., p_n\} \tag{2.22}$$

$$Q = \{q_1, ..., q_n\} \tag{2.23}$$

Suppsons que ces deux distributions sont équiprobables. La réalisation d'un évenement permet de distinguer les deux distributions avec probabilité égale à :

$$\frac{1}{2} + \frac{D(P, Q)}{2}$$

Preuve La réalisation de l'événement i est en faveur de P si $p_i > q_i$ et de Q si $p_i < q_i$. Puisque les deux distributions P et Q sont équiprobables, la probabilité de réalisation de l'événement i est $\frac{p_i + q_i}{2}$. Si l'événement i est effectivement réalisé, la probabilité de deviner correctement la distribution en question est :

$$\frac{\max(p_i, q_i)}{p_i + q_i} \tag{2.24}$$

On sait d'un autre coté que

$$|p_i - q_i| = \begin{cases} p_i - q_i \text{ si } p_i \geq q_i \\ q_i - p_i \text{ si } q_i \geq p_i \end{cases}$$

D'où

$$|p_i - q_i| + p_i + q_i = 2\max(p_i, q_i)$$

Et l'expression (2.24) devient

$$\frac{\max(p_i, q_i)}{p_i + q_i} = \frac{|p_i - q_i| + p_i + q_i}{2(p_i + q_i)} = \frac{|p_i - q_i|}{2(p_i + q_i)} + \frac{1}{2}$$

La probabilité de distinction est la moyenne pondérée de toutes les probabilités de conjecture correcte :

$$\begin{aligned} \sum_{i=1}^{n} (\frac{p_i + q_i}{2}) \left(\frac{|p_i - q_i|}{2(p_i + q_i)} + \frac{1}{2} \right) &= \sum_{i=1}^{n} \frac{1}{2} \frac{|p_i - q_i|}{2} + \sum_{i=1}^{n} \frac{1}{2} \frac{p_i + q_i}{2} \\ &= \frac{D(P,Q)}{2} + \frac{1}{2} \end{aligned}$$

■

Nous voyons que la différence entre deux distributions est directement proportionnelle à la distance entre elles.

Sachant que pour une matrice positive M on peut écrire :

$$M = \sum_i \lambda_i |i\rangle \langle i|$$

on définit

$$\sqrt{M} = \sum_i \sqrt{\lambda_i} |i\rangle \langle i|$$

et pour une matrice hermitique A on a :

$$|A| = \sqrt{A^\dagger A}$$

Dans le cas quantique, on définit la distance entre deux opérateurs de densité ρ et σ par :

$$D(\rho, \sigma) = \frac{1}{2} Tr|\rho - \sigma| \tag{2.25}$$

Le cas de deux opérateurs de densité ρ et σ qui commutent (il existe une base $\{|i\rangle\}$ où les deux matrices peuvent se diagonaliser en même temps) montre clairement le lien entre les deux définitions (2.21) et (2.25). On peut écrire alors :

$$\rho = \sum_i \lambda_i |i\rangle \langle i|$$

et

$$\sigma = \sum_i \gamma_i |i\rangle \langle i|$$

Si on définit les deux distributions de probabilité classique :

$$P = \{\lambda_1, ..., \lambda_n\}$$

$$Q = \{\gamma_1, ..., \gamma_n\}$$

on trouve que

$$D(\rho, \sigma) = D(P, Q)$$

Théorème 13 *([39]) Soit $\{E_i\}$ un POVM, et soient $p_i = Tr(\rho E_i)$, $q_i = Tr(\sigma E_i)$ les probabilités d'avoir l'événement i pour les deux opérateurs de densité ρ et σ respectivement. Si on définit les deux distributions de probabilité classique :*

$$P = \{p_i\}$$

$$Q = \{q_i\}$$

Alors,

$$D(\rho, \sigma) = \max_{\{E_i\}} D(P, Q)$$

Corollaire 5 *Le POVM optimal distingue entre deux opérateurs de densité ρ et σ avec une probabilité de succès égale à :*

$$\frac{D(\rho, \sigma)}{2} + \frac{1}{2} \tag{2.26}$$

Preuve C'est un résultat directe des deux théorèmes précédents.

■

Pour la preuve du théorème suivant, voir par exemple [65]

Théorème 14 *Pour tous opérateurs de densité ρ et σ de Pos($\mathcal{H}$) et sur l'ensemble des projecteurs $\{P\}$ on a :*

$$D(\rho,\sigma) = \max_P Tr(P(\rho-\sigma))$$

Proposition 2 *Pour tout opérateur hermitique ρ de H($\mathcal{H}$) et toute transformation unitaire U agissant dans $\mathcal{H}$ on a :*

$$\sqrt{U\rho U^\dagger} = U\sqrt{\rho}U^\dagger$$

Preuve Puisque ρ est hermitique, il existe une base où il est digonalisable :

$$\rho = \sum_i \lambda_i |i\rangle \langle i|, \lambda_i \in \mathbb{R}$$

Une transformation unitaire transforme deux kets orthogonaux à deux autres kets orthogonaux aussi :

$$\langle j|i\rangle = \delta_{ij} \Longrightarrow \left\langle j|U^\dagger U|i\right\rangle = \langle e_j|e_i\rangle = \delta_{ij}$$

Donc, Elle transforme une base $\{|i\rangle\}$ à une autre base $\{|e_i\rangle\}$. On peut écrire :

$$\begin{aligned}\sqrt{U\rho U^\dagger} &= \sqrt{\sum_i \lambda_i |e_i\rangle \langle e_i|} = \sum_i \sqrt{\lambda_i}|e_i\rangle\langle e_i| \\ &= \sum_i \sqrt{\lambda_i} U|i\rangle\langle i|U^\dagger = U\left(\sum_i \sqrt{\lambda_i}|i\rangle\langle i|\right)U^\dagger \\ &= U\sqrt{\rho}U^\dagger\end{aligned}$$

■

Proposition 3 *Pour tout opérateur unitaire U aggissant dans $\mathcal{H}$ et tous opérateurs de densité ρ et σ de Pos($\mathcal{H}$) on a :*

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho,\sigma)$$

Preuve

$$\begin{aligned} D(U\rho U^\dagger, U\sigma U^\dagger) &= \frac{1}{2}Tr|U\rho U^\dagger - U\sigma U^\dagger| \\ &= \frac{1}{2}Tr|U(\rho-\sigma)U^\dagger| = \frac{1}{2}Tr\sqrt{U(\rho-\sigma)^\dagger U^\dagger U(\rho-\sigma)U^\dagger} \\ &= \frac{1}{2}Tr\left(U\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}U^\dagger\right) = \frac{1}{2}Tr\left(\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right) \\ &= \frac{1}{2}Tr\,|\rho-\sigma| = D(\rho,\sigma) \end{aligned}$$

■

Pour les théorèmes suivants, voir par exemple [65].

Théorème 15 *Si Q est une opération quantique, et ρ et σ deux opérateurs de densité de Pos($\mathcal{H}$), alors :*

$$D(Q(\rho), Q(\sigma)) \leq D(\rho,\sigma)$$

Théorème 16 *Soient les deux distributions de probabilités (2.22) et (2.23), deux séries d'opérateurs de densité $\{\rho_i\}_{i=1}^n$ et $\{\sigma_i\}_{i=1}^n$ et deux opérateurs de densité ρ et σ de Pos($\mathcal{H}$), alors :*

$$D(\sum_i p_i\rho_i, \sum_i q_i\sigma_i) \leq D(Q,P) + \sum_i p_i D(\rho_i,\sigma_i)$$

On a aussi les résultats suivants :

$$D(\sum_i p_i\rho_i, \sigma) \leq \sum_i p_i D(\rho_i,\sigma)$$

Toute opération quantique Q, possède au moins un point fixe ρ :

$$Q(\rho) = \rho$$

Si Q est une opération quantique telle que

$$\forall\rho,\sigma : D(Q(\rho),Q(\sigma)) < D(\rho,\sigma)$$

alors Q possède un seul point fixe.

2.13 Fidélité

La fidélité est un outil très efficace pour calculer le degré de ressemblance entre les états. Dans le cas des deux distributions de probabilité (2.22) et (2.23), elle est définie par :

$$F(P,Q) = \sum_i \sqrt{p_i q_i} \tag{2.27}$$

On a

$$F(P,P) = \sum_i \sqrt{p_i p_i} = \sum_i p_i = 1$$

Plus deux distributions sont semblables, plus leur fidélité est grande. Dans le cas quantique [75], la fidélité entre deux opérateurs de densité ρ et σ de $\mathsf{Pos}(\mathcal{H})$ est :

$$F(\rho,\sigma) = Tr\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}} \tag{2.28}$$

Dans le cas où ces deux opérateurs de densité sont purs, $\rho = |\psi\rangle\langle\psi|$ et $\sigma = |\phi\rangle\langle\phi|$ on a :

$$\begin{aligned} F(\rho,\sigma) &= Tr\sqrt{|\psi\rangle\langle\psi|\left(|\phi\rangle\langle\phi|\right)|\psi\rangle\langle\psi|} = Tr\sqrt{|\langle\psi|\phi\rangle|^2\,|\psi\rangle\langle\psi|} \\ &= |\langle\psi|\phi\rangle| \end{aligned}$$

Si un des deux états est pur, on a :

$$\begin{aligned} F(|\psi\rangle\langle\psi|,\sigma) &= Tr\sqrt{\left(|\psi\rangle\langle\psi|\right)^{\frac{1}{2}}\sigma\left(|\psi\rangle\langle\psi|\right)^{\frac{1}{2}}} \\ &= Tr\sqrt{|\psi\rangle\langle\psi|\sigma|\psi\rangle\langle\psi|} = Tr\sqrt{\langle\psi|\sigma|\psi\rangle\,|\psi\rangle\langle\psi|} \\ &= \sqrt{\langle\psi|\sigma|\psi\rangle}Tr\sqrt{|\psi\rangle\langle\psi|} = \sqrt{\langle\psi|\sigma|\psi\rangle} \end{aligned}$$

Le cas de deux opérateurs de densité, ρ et σ de $\mathsf{Pos}(\mathcal{H})$ qui commutent montre clairement le lien entre les deux définitions (2.27) et (2.28) :

$$\begin{aligned} F(\rho,\sigma) &= Tr\sqrt{\sqrt{\sum_i \lambda_i |i\rangle\langle i|}\sum_i \gamma_i |i\rangle\langle i| \sqrt{\sum_i \lambda_i |i\rangle\langle i|}} \\ &= Tr\sqrt{\sum_i \sqrt{\lambda_i}|i\rangle\langle i| \sum_i \gamma_i |i\rangle\langle i| \sum_i \sqrt{\lambda_i}|i\rangle\langle i|} \\ &= Tr\sqrt{\sum_i \lambda_i\gamma_i |i\rangle\langle i|} = Tr\sum_i \sqrt{\lambda_i\gamma_i}|i\rangle\langle i| \\ &= \sum_i \sqrt{\lambda_i\gamma_i} = F(P,Q) \end{aligned}$$

Proposition 4 *Soient les deux opérateurs de densité ρ, σ de Pos($\mathcal{H}$), et la transformation unitaire U agissant dans $\mathcal{H}$, on a :*

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho,\sigma)$$

Preuve

$$\begin{aligned} F(U\rho U^\dagger, U\sigma U^\dagger) &= Tr\sqrt{(U\rho U^\dagger)^{\frac{1}{2}}(U\sigma U^\dagger)(U\rho U^\dagger)^{\frac{1}{2}}} \\ &= Tr\sqrt{\left(U\rho^{\frac{1}{2}}U^\dagger\right)U\sigma U^\dagger\left(U\rho^{\frac{1}{2}}U^\dagger\right)} \\ &= Tr\sqrt{U\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}U^\dagger} = Tr\left[U\left(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right)U^\dagger\right] \\ &= Tr\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}} = F(\rho,\sigma) \end{aligned}$$

■

2.13.1 Théorème d'Ulmann [75, 41]

Théorème 17 *(d'Ulmann) Soient ρ et σ deux opérateurs de densité de Pos($\mathcal{H}_A$), on a :*

$$F(\rho,\sigma) = \max_{|\psi\rangle_{AB},|\varphi\rangle_{AB}} |_{AB}\langle\varphi|\psi\rangle_{AB}| \tag{2.29}$$

où $|\psi\rangle_{AB}$ et $|\varphi\rangle_{AB}$ sont des purifications de ρ et σ respectivement et $\dim\mathcal{H}_A = \dim\mathcal{H}_B$

Ce théorème peut s'énoncer aussi des trois manières suivantes :

$$\text{Pour toute purification } |\psi\rangle_{AB} \text{ de } \rho : F(\rho,\sigma) = \max_{|\varphi\rangle_{AB}} |_{AB}\langle\varphi|\psi\rangle_{AB}| \tag{2.30}$$

$$\text{Pour toute purification } |\varphi\rangle_{AB} \text{ de } \sigma : F(\rho,\sigma) = \max_{|\psi\rangle_{AB}} |_{AB}\langle\varphi|\psi\rangle_{AB}|$$

Pour toutes purifications $|\psi\rangle_{AB}$ et $|\varphi\rangle_{AB}$ de ρ et σ respectivement, on a :

$$F(\rho,\sigma) = \max_{U_B} |_{AB}\langle\varphi|I_A \otimes U_B|\psi\rangle_{AB}| \tag{2.31}$$

La maximisation se fait sur l'ensemble des opérateurs unitaires $\{U_B\}$.

Le théorème d'Ulmann donne les corollaires suivants :

Corollaire 6 *Soient ρ et σ deux opérateurs de densité de Pos($\mathcal{H}$), on a :*

$$F(\rho,\sigma) = F(\sigma,\rho)$$

$$0 \leq F(\rho,\sigma) \leq 1$$

$$F(\rho,\sigma) = 1 \Longleftrightarrow \rho = \sigma$$

$$F(\rho,\sigma) = 0 \Longleftrightarrow \rho \perp \sigma \Longleftrightarrow \rho\sigma = \sigma\rho = 0$$

$$F(\rho_1 \otimes \sigma_1, \rho_2 \otimes \sigma_2) = F(\rho_1,\rho_2)F(\sigma_1,\sigma_2)$$

L'écriture $\rho \perp \sigma$ signifie que les supports de ces deux opérateurs de densité sont orthogonaux.

Pour les théorèmes suivants, voir par exemple [65].

Théorème 18 *(Monotonie de la fidélité) Soit Q une opération quantique, alors :*

$$F\left(Q(\rho), Q(\sigma)\right) \geq F\left(\rho,\sigma\right)$$

Théorème 19 *(concavité forte de la fidélité) Soient les deux distributions de probabilités (2.22) et (2.23), deux séries d'opérateurs de densité $\{\rho_i\}_{i=1}^n$ et $\{\sigma_i\}_{i=1}^n$ et deux opérateurs de densité ρ et σ de Pos($\mathcal{H}$), alors :*

$$F(\sum_i p_i\rho_i, \sum_i q_i\sigma_i) \geq \sum_i \sqrt{p_i q_i} F(\rho_i,\sigma_i)$$

D'une manière générale, on a aussi :

$$F(\sum_i p_i\rho_i, \sum_i p_i\sigma_i) \geq \sum_i p_i F(\rho_i, \sigma_i)$$

$$F(\sum_i p_i\rho_i, \sigma) \geq \sum_i p_i F(\rho_i, \sigma)$$

$$F(\rho, \sigma) \geq Tr(\rho\sigma)$$

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F^2(\rho,\sigma)} \quad [66] \tag{2.32}$$

$$\max_\rho (F^2(\rho,\sigma) + F^2(\rho,\omega)) = 1 + F(\sigma,\omega) \tag{2.33}$$

Dans le cas de deux états purs, on a :

$$D(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|) = \sqrt{1 - F^2(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)} \tag{2.34}$$

Si un des deux états est pur, on a :

$$1 - F^2(\rho, |\psi\rangle\langle\psi|) \leq D(\rho, |\psi\rangle\langle\psi|) \tag{2.35}$$

Si les deux états ρ et σ appartiennent à $\mathrm{Pos}(\mathcal{H}^{\otimes 2})$, on a aussi :

$$1 - F^2(\rho,\sigma) \leq D(\rho,\sigma). \tag{2.36}$$

2.14 Pseudo opérations

Pour cette section, nous donnerons la version de Bub Jeffrey [40] de la preuve de Brassard, Crépeau, Mayers et Salvail, [15]. Un protocole quantique entre Alice et Bob comporte généralement une série de transactions où ils vont s'échanger des systèmes quantiques après qu'ils leur assujettissent différentes opérations quantiques (transformations unitaires, mesure). Les opérations appliquées peuvent être choisies aléatoirement. On montre maintenant qu'il est toujours possible que Bob remplace ses opérations, sans qu'Alice ne s'aperçoive, par des intrications avec des systèmes supplémentaires (systèmes ancillaires) au lieu de suivre le protocole et faire un choix aléatoire réel pour déterminer s'il mesurera le système S, qu'il a reçu d'Alice, dans la base $X : \{|x_1\rangle, |x_2\rangle\}$ ou $Y : \{|y_1\rangle, |y_2\rangle\}$ avant de le lui retourner. On suppose que Bob n'est pas obligé de lui

divulguer le choix et les résultats de mesure avant la fin du protocole. Dans ce contexte, on peut voir que Bob peut reporter son choix et sa mesure à un moment ultérieur où le système S est chez Alice. Au lieu de suivre le protocole et mesurer le système S, supposé dans l'état $|\psi\rangle_S$, Bob peut intriquer ce dernier avec l'état initial $|d_0\rangle_D$, qui servira comme un dé pour le choix aléatoire, et $|p_0\rangle_P$, qui jouera le rôle de pointeur pour la mesure. L'intrication est réalisée via les deux transformations unitaires, U_X et U_Y agissant sur le système $S+P$ comme suit :

$$U_X\left(|x_1\rangle\,|p_0\rangle_P\right) = |x_1\rangle\,|p_1\rangle_P$$

$$U_X\left(|x_2\rangle\,|p_0\rangle_P\right) = |x_2\rangle\,|p_2\rangle_P$$

$$U_Y\left(|y_1\rangle\,|p_0\rangle_P\right) = |y_1\rangle\,|p_1\rangle_P$$

$$U_Y\left(|y_2\rangle\,|p_0\rangle_P\right) = |y_2\rangle\,|p_2\rangle_P$$

Puisque $\{|x_1\rangle, |x_2\rangle\}$ et $\{|y_1\rangle, |y_2\rangle\}$ sont des bases de S, on peut écrire $|\psi\rangle_S$ comme :

$$|\psi\rangle_S = \langle x_1|\psi\rangle_S\,|x_1\rangle + \langle x_2|\psi\rangle_S\,|x_2\rangle$$

ou encore

$$|\psi\rangle_S = \langle y_1|\psi\rangle_S\,|y_1\rangle + \langle y_2|\psi\rangle_S\,|y_2\rangle$$

ce qui permet d'écrire :

$$U_X\left(|\psi\rangle_S\,|p_0\rangle_P\right) = \langle x_1|\psi\rangle_S\,|x_1\rangle\,|p_1\rangle_P + \langle x_2|\psi\rangle_S\,|x_2\rangle\,|p_2\rangle_P$$

$$U_Y\left(|\psi\rangle_S\,|p_0\rangle_P\right) = \langle y_1|\psi\rangle_S\,|y_1\rangle\,|p_1\rangle_P + \langle y_2|\psi\rangle_S\,|y_2\rangle\,|p_2\rangle_P$$

De la même manière, Bob peut réaliser unitairement le choix aléatoire. Soit V une transformation unitaire agissant sur le système $D+S+P$ (D est un autre système ancillaire utilisé par Bob) de la manière suivante :

$$V\left(|d_X\rangle_D\,|\psi\rangle_S\,|p_0\rangle_P\right) = |d_X\rangle_D\,U_X\left(|\psi\rangle_S\,|p_0\rangle_P\right)$$

$$V\left(|d_Y\rangle_D\,|\psi\rangle_S\,|p_0\rangle_P\right) = |d_Y\rangle_D\,U_Y\left(|\psi\rangle_S\,|p_0\rangle_P\right)$$

où $\{|d_X\rangle_D, |d_Y\rangle_D\}$ est une base dans l'espace du système D. Si Bob prépare le système D dans l'état $|d_0\rangle_D = \frac{1}{\sqrt{2}}(|d_X\rangle + |d_Y\rangle)$ et applique V sur l'état $|d_0\rangle_D |\psi\rangle_S |p_0\rangle_P$, il obtient :

$$\begin{aligned} V(|d_0\rangle_D |\psi\rangle_S |p_0\rangle_P) &= \frac{1}{\sqrt{2}} V(|d_X\rangle_D |\psi\rangle_S |p_0\rangle_P) + \frac{1}{\sqrt{2}} V(|d_Y\rangle_D |\psi\rangle_S |p_0\rangle_P) \quad (2.37) \\ &= \frac{1}{\sqrt{2}} |d_X\rangle_D U_X (|\psi\rangle_S |p_0\rangle_P) + \frac{1}{\sqrt{2}} |d_Y\rangle_D U_Y (|\psi\rangle_S |p_0\rangle_P) \end{aligned}$$

Si Bob mesure réellement l'état $|\psi\rangle_S$ dans une des deux bases X ou Y qu'il choisit aléatoirement et obtient un des états $\{|x_1\rangle, |x_2\rangle, |y_1\rangle, |y_2\rangle\}$, l'état du système d'Alice, une fois que Bob lui retourne le système S après sa mesure, si elle ignore la base choisie et le résultat de la mesure de Bob, est représenté par l'opérateur de densité :

$$\frac{1}{2}(|\langle x_1|\psi\rangle_S|^2 |x_1\rangle \langle x_1| + |\langle x_2|\psi\rangle_S|^2 |x_2\rangle \langle x_2|) + \frac{1}{2}(|\langle y_1|\psi\rangle_S|^2 |y_1\rangle \langle y_1| + |\langle y_2|\psi\rangle_S|^2 |y_2\rangle \langle y_2|)$$

Mais cette matrice de densité est exactement la même que celle obtenue en traçant l'état dans (2.37). Autrement dit, l'état du système S est le même pour Alice que Bob choisisse une base et mesure réellement dans cette base ou qu'il triche en ajoutant deux ancillas et produise l'état dans (2.37). Si, à un certain moment, Bob est obligé de retourner la mesure effectuée et le résultat trouvé, à ce moment il mesure réellement le système D dans la base $\{|d_X\rangle_D, |d_Y\rangle_D\}$, et le système P dans la base $\{|p_1\rangle_P, |p_2\rangle_P\}$.

Cette stratégie de Bob ne peut être détectée par Alice car elle n'a pas accès aux systèmes ancillaires $(D + P)$ de Bob alors qu'elle ne peut savoir que son système est intriqué à celui de Bob que par une mesure de tout le système $D + S + P$.

En fait, si c'était possible pour Alice de distinguer entre les deux situations, il serait possible aussi de signaler à une vitesse supérieure à celle de la lumière :
Alice pourrais savoir instantanément si Bob a réellement mesuré ou non son ancilla en contrôlant le système S.

Il est aussi possible pour Bob d'utiliser la même stratégie s'il doit choisir à un stade du protocole entre l'application de transformations unitaires au lieu de mesures. Pour ce faire, il suffit de se débarrasser de l'ancilla P dans (2.37).

Un cas un peu moins évident où Bob restera quand même capable d'appliquer sa stratégie de tricherie, est celui où il doit effectuer une mesure ou faire un choix d'une opération parmi un ensemble d'opérations sur le système S_{i+1} et ça en fonction d'une mesure antérieure qu'il a effectuée sur le système S_i ou d'un choix d'opération parmi un ensemble d'opérations sur celui-ci. Bien sûr, si Bob est en possession de tout le système $S_i + S_{i+1}$ en même temps, il peut l'intriquer avec des ancillas réalisant chaque séquence possible d'opérations. Mais aussi dans le cas où Bob ne peut accéder au système S_{i+1} qu'après avoir retourné le système S_i, il peut toujours tricher en intriquant le système S_{i+1} avec l'ancilla qu'il a utilisée pour intriquer le système S_i. Prenons la situation suivante comme exemple : à un stade du protocole, Bob doit choisir aléatoirement entre deux mesures, X et Y, à effectuer sur le système S avant de le retourner à Alice (ici c'est la même situation exposée plus haut). Après qu'Alice reçoive S, elle lui envoie le système S'. Si Bob a mesuré S dans la base X et obtenu le résultat x_1, il doit mesurer le système S' dans la base X; si par contre c'est le résultat x_2 qu'il a obtenu il mesurera S' dans la base Y. Dans le cas où Bob mesure S dans la base Y, s'il obtient y_1 il applique la transformation unitaire U_1 sur S', et s'il obtient y_2 il lui applique U_2. Une fois appliquée l'opération requise, il retourne S' à Alice.

À première vue, on peut croire que Bob doit réellement effecteur une mesure sur le premier système S et obtenir un résultat qui va décider son action sur le système S', sous la contrainte qu'il n'a pas d'accès simultané aux deux systèmes. Toutefois, ce n'est pas le cas, et la stratégie de Bob continuera de persister. Cette fois, lorsque Bob reçoit le système S', supposé être dans l'état $|\phi\rangle$, il lui ajoute un troisième système ancillaire, soit Q, dans l'état initial $|q_0\rangle$ et applique la transformation unitaire W sur le système $D + P + S^{'} + Q$:

$$\begin{aligned}
W\left(|d_X\rangle\,|p_1\rangle\,|\phi\rangle\,|q_0\rangle\right) &= |d_X\rangle\,|p_1\rangle\,U_X\left(|\phi\rangle\,|q_0\rangle\right)\\
W\left(|d_X\rangle\,|p_2\rangle\,|\phi\rangle\,|q_0\rangle\right) &= |d_X\rangle\,|p_2\rangle\,U_Y\left(|\phi\rangle\,|q_0\rangle\right)\\
W\left(|d_Y\rangle\,|p_1\rangle\,|\phi\rangle\,|q_0\rangle\right) &= |d_Y\rangle\,|p_1\rangle\,\left(U_1\,|\phi\rangle\right)|q_0\rangle\\
W\left(|d_Y\rangle\,|p_2\rangle\,|\phi\rangle\,|q_0\rangle\right) &= |d_Y\rangle\,|p_2\rangle\,\left(U_2\,|\phi\rangle\right)|q_0\rangle
\end{aligned}$$

Un résultat important qui découle de l'analyse ci-dessus est de considérer, lors de l'étude des protocoles quantiques de mise en gage, des protocoles impliquant seulement des opérations unitaires avec une paire de mesures à la fin du protocole et aussi de ne considérer que des attaques utilisant des opérations unitaires. Cependant, tout résultat trouvé sur les bornes dans ce modèle s'applique sur le cas général où les participants peuvent appliquer les transformations de leurs choix (des mesures, des opérations quantiques, des choix aléatoires classiques ou utilisent des canaux classiques supplémentaires). En fait, cette réduction est un résultat des deux lemmes suivants, qui ont été discutés dans plusieurs travaux, voir par exemple [49, 50, 54, 55, 15].

Lemme 7 *Pour tout protocole P entre Alice et Bob, dont la composition est la plus générale (c-à-d., qui peut contenir des mesures des canaux classiques, etc.) et qui garantit un biais au maximum égal à ϵ sous la stratégie de tricherie la plus générale (c-à-d., qui peut contenir des mesures, des opérations quantiques, etc.), il existe un protocole P' qui est défini uniquement par des transformations unitaires et une paire de mesures à la fin, et qui, lui aussi, garantit le même biais ϵ sous la stratégie de tricherie la plus générale.*

Lemme 8 *Pour tout protocole P entre Alice et Bob, impliquant seulement des transformations unitaires et une paire de mesures à la fin, s'il existe une stratégie de tricherie (pouvant contenir des mesures, des opérations quantiques, etc.) qui réalise un biais ϵ, alors, il existe aussi une autre stratégie de tricherie réalisant le même biais et n'impliquant que des transformations unitaires.*

Le lemme 7 montre qu'on peut considérer seulement les protocoles où les actions honnêtes sont des transformations unitaires. Ce lemme est important pour trouver la borne inférieure du biais. Par contre, le lemme 8 indique qu'on peut chercher la stratégie optimale de tricherie parmi les stratégies utilisant seulement des transformations unitaires.

CHAPITRE III

MISE EN GAGE

La mise en gage est une primitive de cryptographie très utilisée, principalement comme élément fondamental pour construires d'autre protocoles tels que le tir à pile ou face, par exemple. Elle intervient aussi dans des preuves à divulgation nulle (zero knowledge). Son principe est simple et implique deux parties, que nous appellerons Alice et Bob. Elle s'accomplit par la transmission d'une information à Bob qui doit être suffisante pour fixer la valeur d'un bit et insuffisante pour que Bob la découvre. Pour se faire, on peut imaginer le protocole en deux étapes suivant :

Protocole 1

1. La mise en gage, à proprement parler : Alice écrit sa prédiction dans un coffre-fort, conserve la clef et donne le coffre fort à Bob.
2. Puis, la révélation : quand les deux parties sont d'accord, Alice donne la clef à Bob qui ouvre le coffre et lit la prédiction.

Ainsi Bob ne peut lire la prédiction sans l'autorisation d'Alice (le protocole est dit *camouflant*) et Alice ne peut la modifier sans que Bob s'en aperçoive (le protocole est dit *liant*).

Le protocole de la mise en gage d'un bit a déjà fait l'objet de nombreuses études, dans les cas classique comme quantique.

Définition 5 *Un* protocole quantique *est un protocole qui permet l'échange de l'information quantique en opposition à un protocole classique, qui lui ne le permet pas. On distingue aussi entre protocole relativiste, qui se fonde sur la validité de la relativité restreinte et s'appuie sur l'impossibilité qu'un signal puisse se déplacer à une vitesse supérieure à celle de la lumière et un autre non relativiste qui suppose la possibilité d'interactions instantanées.*

Définition 6 *Un protocole de mise en gage classique est* parfaitement camouflant *(idéal) s'il garantit que Bob ne puisse obtenir aucune information sur le bit d'Alice avant qu'elle ne décide de le lui révéler.*

Définition 7 *Un protocole de mise en gage classique est* parfaitement liant *si, une fois la phase d'engagement complétée, l'une des deux probabilités, de révéler 0 avec succès ou de révéler 1 avec succès, est nulle.*

Définition 8 *Un* paramètre de sécurité *dans un protocole de mise en gage est un entier positif, N, tel qu'on l'augmentant la sécurité du protocole augmente.*

Définition 9 *Un protocole classique est* arbitrairement camouflant, *ou tout simplement camouflant, si la probabilité que Bob estime correctement le bit d'Alice avant la révélation est bornée par une fonction du paramètre de sécurité N, $\epsilon(N)$ telle que* $\lim_{N\to\infty} \epsilon(N) = 0$.

Définition 10 *Un protocole classique est* arbitrairement liant, *ou tout simplement liant si, une fois la mise en gage complétée, l'une des deux probabilités, de révéler* 0 *avec succès ou de révéler* 1 *avec succès, est bornée par une fonction du paramètre de sécurité N, $\epsilon'(N)$ telle que* $\lim_{N\to\infty} \epsilon'(N) = 0$.

Dans le cas d'un protocole quantique de mise en gage, il est possible qu'Alice mette dans le coffre fort le qubit $\alpha |0\rangle_{B\,B} \langle 0| + \beta |1\rangle_{B\,B} \langle 1|$ au lieu de s'engager sur un

des deux bits 0 ou 1. Ceci est possible si elle prépare l'état intriqué

$$\sqrt{\alpha}\,|0\rangle_A\,|0\rangle_B + \sqrt{\beta}\,|1\rangle_A\,|1\rangle_B$$

et qu'elle procède à la mise en gage d'un des qubits. Maintenant, si elle décide de révéler le bit à Bob, elle mesure son qubit dans la base de calcul, et lui annonce le résultat trouvé. Bien sûr, Bob n'a aucun moyen de découvrir cette stratégie. Cette possibilité offerte à Alice, remarquée et étudiée par Brassard, Crépeau, Mayers et Salvail, [15], n'est pas avantageuse pour elle dans un protocole de mise en gage quantique isolé, mais elle peut ouvrir à Alice d'autres possibilités de tricherie si le protocole fait partie d'un système cryptographique plus large. Alors, le protocole quantique de mise en gage quantique exige des nouvelles définitions de la sécurité dans le cadre de cette possibilité, incontournable, offerte à Alice.

Définition 11 *Un protocole de mise en gage quantique est* parfaitement camouflant *s'il garantit que Bob ne puisse obtenir aucune information sur le bit d'Alice avant qu'elle ne décide de le lui révéler.*

Définition 12 *Un protocole quantique est* arbitrairement camouflant, *ou tout simplement camouflant, si la probabilité que Bob estime correctement le bit d'Alice avant la révélation est bornée par une fonction du paramètre de sécurité N, $\epsilon(N)$ telle que* $\lim_{N\to\infty} \epsilon(N) = 0$.

Définition 13 *Un protocole de mise en gage quantique est* parfaitement liant, *s'il garantit qu'Alice n'a aucune stratégie lui permettant d'agir à partir du premier point après la fin de la phase de mise en gage de manière à modifier la distribution de probabilité qu'elle a choisi dans la phase de mise en gage. Soit $p_0^{\max}$ la probabilité maximale de révéler le bit 0 avec succès, la maximisation étant faite sur toutes les staratégies qu'elle puisse appliquer après la fin de la phase de mise en gage, et soit $p_1^{\max}$ défini de la même manière, alors le protocole quantique est parfaitement liant si $p_0^{\max} + p_1^{\max} \leq 1$.*

Remarque 4 *On voit bien que cette définition ne garantit pas la condition classique de la sécurité envers Alice, qui est beaucoup plus forte, qui exigerait que l'une des deux probabilités* $p_0^{\max}$ *ou* $p_1^{\max}$ *s'annulle.*

Définition 14 *Un protocole de mise en gage quantique est* arbitrairement liant *ou tout simplement liant, si* $p_0^{\max} + p_1^{\max} \leq 1 + \epsilon(N)$ *telle que* $\lim_{N\to\infty} \epsilon(N) = 0$, *où* N *est un paramètre de sécurité.*

Définition 15 *Un protocole de mise en gage classique ou quantique est* parfaitement sûr *s'il est parfaitement camouflant et liant à la fois.*

Définition 16 *Un protocole de mise en gage classique ou quantique est* sûr *s'il est camouflant et liant à la fois.*

Définition 17 *Si la technologie ou la puissance de calcul disponible aux parties n'influence en rien la sécurité d'un protocole qui repose sur la validité d'une théorie physique, alors ce protocole est dit* inconditionnellement sûr *suivant cette théorie.*

Note 1 *Ici on ne s'intéresse qu'à la sécurité inconditionnelle des protocoles.*

3.1 L'impossibilité d'une mise en gage non relativiste liante et camouflante en même temps

3.1.1 Mise en gage classique

La sécurité d'un protocole classique non relativiste n'est que conditionnelle au mieux et s'appuie sur la difficulté non prouvée d'un problème mathématique. Un exemple d'un protocole de mise en gage d'un bit $b \in \{0, 1\}$ (donc, pas général) est un protocole défini à partir d'un couple d'ensembles (E_0, E_1) et qui contient au moins deux étapes :

Protocole 2

1. Mise en gage : Alice envoie un message $m \in E_0 \cup E_1$ à Bob.
2. Révélation : Alice envoie à Bob une preuve (m, b, x) de l'appartenance de m à E_b.

Un tel protocole est liant s'il est impossible pour Alice de trouver deux preuves de la forme $(m, 0, x_0)$ et $(m, 1, x_1)$ des appartenances respective de de $m \in E_0$ et $m \in E_1$. Un tel protocole est camouflant s'il est impossible pour Bob de prouver la non appartenance $m \notin E_{\neg b}$. Malheureusement ces deux propriétés ne peuvent être vérifiées simultanément dans le monde classique.

Proposition 5 *Le protocole de mise en gage 2 n'est pas sûr.*

Preuve Supposons que ce protocole soit liant. Alice ne peut, alors, trouver deux preuves de la forme $(m, 0, x_0)$ et $(m, 1, x_1)$. Autrement dit, deux preuves de cette forme ne peuvent exister puisqu'une Alice sans contrainte de temps pourait toujours les trouver autrement. Dans ce cas, Bob peut déduire la valeur du bit à partir du message envoyé m. Pour ce faire, il énumère tous les triplets (m', b', x') et retourne b' une fois que $m' = m$.

■

D'une manière plus générale, on a le théorème suivant.

Théorème 20 *Un protocole de mise en gage classique non relativiste parfaitement sûr est impossible.*

3.1.2 Mise en gage quantique

En 1993, Brassard, Crépeau, Jozsa et Langlois [14] proposent un protocole de mise en gage et prétendent démontrer que ce protocole est sûr. Avec deux approches

différentes faites indépendament, D. Mayers [54, 55], Lo et Chau [34, 35] ont montré que ce protocole de mise en gage quantique n'était pas sûr (Lo et Chau pensaient que le protocole de Brassard, Crépeau, Jozsa et Langlois [14] est parfaitement camouflant, mais en fait il n'est qu'arbitrairement camouflant. Leur attaque originale [49] était donc fausse! L'attaque de Mayers était, par contre, impeccable.). Pour le démontrer, ils ont exhibé une attaque sur le protocole. Mais il s'est révélé que cette attaque est en fait très générale, et fonctionne sur tout protocole parfaitement camouflant. Ensuite, les études ont porté sur des versions plus faibles de la mise en gage où le protocole n'est plus parfaitement camouflant. Dans ce cas, l'attaque reste efficace aussi.

En premier lieu, on expose le cœur de la preuve de l'impossibilité d'un protocole inconditionnellement sûr. On va voir qu'un protocole parfaitement camouflant ne peut être liant à la fois. Ensuite on expose aussi la preuve de l'impossibilité même d'un protocole arbitrairement sûr (c-à–d, liant et camouflant) et on verra que si un protocole de mise en gage quantique permet à Bob de distinguer avec une probabilité $\epsilon \to 0$, le bit mis en gage par Alice, il permet à cette dernière de changer son bit sans se faire détecter par Bob avec une probabilité supérieure $1 - \epsilon$.

3.1.3 Théorème de l'impossibilité

Les lemmes 7 et 8 de la page 62 nous permettent de voir tout protocole de mise en gage quantique d'un bit comme deux phases de calcul élaborées conjointement par Alice et Bob. Après une première phase, dite de mise en gage, le calcul s'interrompt avant de se poursuivre dans la deuxiéme phase, dite de révélation. Le calcul a comme input le bit sur lequel Alice s'engage et doit fournir l'output :

–0 si Bob est convaincu que l'input est 0.

–1 si Bob est convaincu que l'input est 1.

–*invalide* si l'un détecte que l'autre triche.

Un protocole de mise en gage spécifie la série d'actions qu'Alice doit suivre pour

s'engager sur un bit b et garantit que c'est ce bit qui va être mesuré par un Bob honnête à la fin de la phase de révélation si elle suit le protocole.

Dans un modèle quantique, on peut décrire le calcul à chaque instant par l'état de tout le système quantique à cet instant. L'évolution d'un état à un autre se fait par des opérations unitaires locales appliquées par Alice et Bob, chacun de sa part, et aussi par la communication entre eux. Selon un algorithme déterministe, Alice et Bob préparent le système $A+B$, dans l'état pur $|\psi_0\rangle_{AB} \in \mathcal{H} = \mathcal{H}_{A,0} \otimes \mathcal{H}_{B,0}$. Ensuite, ils entrent dans des tours de communications (phase de la mise en gage). Cette étape doit contenir au moins un tour de communication d'Alice vers Bob. Dans le tour i, ils appliquent conjointement l'opération unitaire $U_{A,i}(b) \otimes U_{B,i}$ à l'état du système juste avant le tour i: $|\psi(b)_{i-1}\rangle_{AB} \in \mathcal{H} = \mathcal{H}_{A,i-1} \otimes \mathcal{H}_{B,i-1}$, pour avoir :

$$|\psi(b)_i\rangle_{AB} = (U_{A,i}(b) \otimes U_{B,i}) |\psi(b)_{i-1}\rangle_{AB}$$

puis communiquent entre eux pour échanger des sous-systèmes. L'état résultant $|\psi(b)_i\rangle_{AB}$ est décomposé suivant une nouvelle répartition :$|\psi(b)_i\rangle_{AB} \in \mathcal{H} = \mathcal{H}_{A,i} \otimes \mathcal{H}_{B,i}$ entre eux, alors que la dimension de l'espace $\mathcal{H}$ restera invariante. Les états de A et B dans le tour i sont :

$$\rho_i^A(b) = Tr_{B,i}(|\psi(b)_i\rangle_{AB\ AB} \langle\psi(b)_i|)$$

$$\rho_i^B(b) = Tr_{A,i}(|\psi(b)_i\rangle_{AB\ AB} \langle\psi(b)_i|)$$

Si le protocole est parfaitement camouflant, Bob ne peut dans aucun tour $j : j \leq n$, distinguer entre les états $\rho_j^B(0)$et $\rho_j^B(1)$, où n est le nombre de tours de la phase de mise en gage. On traduit ça par :

$$\forall j \leq n, \rho_j^B(0) = \rho_j^B(1)$$

Mais dans ce cas, et d'après le théorème GHJW, Alice peut localement transformer $|\psi(0)_j\rangle_{AB}$ on $|\psi(1)_j\rangle_{AB}$ et vice versa :

$$|\psi(0)_j\rangle_{AB} = (W_{A,j} \otimes I_B) |\psi(1)_j\rangle_{AB},\ j \leq n$$

$$|\psi(1)_j\rangle_{AB} = \left(W_{A,}^{-1}{}_j \otimes I_B\right) |\psi(0)_j\rangle_{AB},\ j \leq n$$

Où les $\{W_{A,j}\}$ sont des transformations unitaires qu'Alice applique localement. Ceci prouve l'impossibilité d'un protocole inconditionnellement camouflant et liant en même temps.

Prenant maintenant le cas où les deux opérateurs de densité sont peu distinguables : $\rho_j^B(0) \approx \rho_j^B(1)$. On peut traduire ceci grâce à la notion de fidélité par :

$$F(\rho_j^B(0), \rho_j^B(1)) = 1 - \epsilon \ , \ \ \epsilon \approx 0 \ , \ j \leq n$$

Pour la purification $|\psi(0)_j\rangle_{AB}$, la relation (2.30) assure l'existence d'une purification $|\chi_j\rangle_{AB}$ de $\rho_j^B(1)$ telle que :

$$F(\rho_j^B(0), \rho_j^B(1)) = |_{AB}\langle\psi(0)_j|\chi_j\rangle_{AB}| = 1 - \epsilon$$

D'aprés le théorème GHJW, Alice peut créer localement la purification $|\chi_j\rangle_{AB}$ à partir de $|\psi(1)_j\rangle_{AB}$ (car c'est une purification du même opérateur de densité $\rho_j^B(1)$). Ainsi, si Alice commence le calcul pour $b = 1$, elle peut tricher en réalisant la purification $|\chi_j\rangle_{AB}$ et déclarant $b = 0$. Supposons que le nombre de tours de la phase de révélation est m. Dans ce cas, les états successifs de la phase de révélation sont :

$$|\chi_{n+1}\rangle_{AB}, |\chi_{n+2}\rangle_{AB} \cdots, |\chi_{n+m}\rangle_{AB}$$

et elles vérifient la relation de récurrence :

$$|\chi_{n+i}\rangle_{AB} = U_{n+i}^A \otimes U_{n+i}^B |\chi_{n+i-1}\rangle_{AB}, \ \ 1 \leq \ i \leq m$$

Et puisque

$$|_{AB}\langle\psi(0)_n|\chi_n\rangle_{AB}| = 1 - \epsilon$$

On a alors :

$$|_{AB}\langle\psi(0)_{n+m}|\chi_{n+m}\rangle_{AB}| = 1 - \epsilon$$

Soit σ^B :

$$\sigma^B = Tr_{A,n+m}(|\chi_{n+m}\rangle_{AB\ AB}\langle\chi_{n+m}|)$$

Le théorème d'Ulmann implique que

$$F(\rho^B(0)_{n+m}, \sigma^B) \geq |_{AB}\langle \psi(0)_{n+m} | \chi_{n+m} \rangle_{AB}|$$

Alors :

$$F(\rho^B(0)_{n+m}, \sigma^B) \geq 1 - \epsilon$$

Donc, d'un coté la tricherie d'Alice ne l'empêche pas de révéler 1 avec succès, si c'est ce qu'elle prefère, car elle s'est honnêtement engagée sur cette valeur. Si, par contre, elle veut révéler 0, il est au moins aussi difficile pour Bob de distinguer entre $\rho^B(0)_{n+m}$ et σ^B qu'entre $|\chi_{n+m}\rangle_{AB}$ et $|\psi(0)_{n+m}\rangle_{AB}$. Ceci prouve aussi l'impossibilité d'un protocole arbitrairement securitaire (ou tout simplement sécuritaire).

3.2 Degré de lien et de camouflage

3.2.1 Cas général

L'impossibilité d'une mise en gage parfaite nous pousse à réfléchir sur la possibilité de construire des protocoles de mise en gage moins exigeants, des protocoles de mise en gage partiellement camouflants et partiellement liants, de telle façon que si Alice est honnête, la probabilité que Bob découvre son bit est strictement inférieur à 1 et si c'est Bob qui est honnête alors Alice ne peut révéler tout le temps ce qu'elle désire sans courir le risque d'être détectée.

Note 2 *Dans ce type de sécurité, on ne se préocupe pas de la possibilité qu'Alice découvre la tricherie de Bob. Il y a d'autres types de sécurité qui s'interessent à cette situation* [35] *et qu'on étudiera dans la section 3.3.*

Dans ce qui suit, on exposera le travail de Spekkens et Rudolph [73] où ils ont calculé les degrés optimaux de lien et de camouflage qui peuvent être achevés simultanément dans tout protocole de mise en gage quantique non relativiste. Pour ce faire, ils ont introduit deux quantités, l'une mesure jusqu'à quel point, après la phase de la

mise en gage, Alice peut influencer le résultat qu'un Bob honnête peut avoir si elle suit le protocole. L'autre mesure la capacité de Bob à estimer, avant la révélation, le bit sur lequel Alice s'est engagée. On suppose que Bob n'a aucune information préalable sur le bit d'Alice et qu'Alice désire révéler 0 autant qu'elle désire révéler 1. C-à-d., la stratégie qu'elle utilise pour tricher ne favorise pas au préalable une des deux valeurs. Soit $G(S^B)$ la différence entre $P_E(S^B)$, la probabilité qu'un Bob malhonnête estime correctement le bit d'Alice quand il suit une stratégie S^B, et celle s'il est honnête et suit le protocole, c-à-d. $\frac{1}{2}$:

$$G(S^B) = P_E(S^B) - \frac{1}{2}$$

$$G(S^B) \leq \frac{1}{2}$$

De même, soit $C(S^A)$ la différence entre $P_U(S^A)$, la probabilité qu'une Alice malhonnête révèle ce qu'elle désire et passe le test de Bob, quand elle suit la stratégie S^A, et celle lorsqu'elle suit le protocole, c-à-d. $\frac{1}{2}$:

$$C(S^A) = P_U(S^A) - \frac{1}{2}$$

$$C(S^A) \leq \frac{1}{2}$$

Puisqu'un Bob malhonnête cherchera toujours la stratégie qui maximisera $G(S^B)$, on définit :

$$G^{\max} \equiv \max_{S^B} G(S^B) \tag{3.1}$$

$$0 \leq G^{\max} \leq \frac{1}{2}$$

Note 3 *Dans ce type de sécurité, Bob utilise la stratégie qui maximise sa probabilité de distinction, contrairement au cas des protocoles, dit "cheat sensitive"* [35], *où il applique des stratégies lui permettant de tricher sans qu'il coure le risque d'être découvert.*

Même chose pour Alice :

$$C^{\max} \equiv \max_{S^A} C(S^A) \tag{3.2}$$

$$0 \leq C^{\max} \leq \frac{1}{2}$$

Revenons maintenant au modèle exposé plus haut et voyons comment on peut implémenter la primitive de mise en gage. Si la phase de mise en gage contient n tours entre Alice est Bob, on peut écrire :

$$|\psi(b)_n\rangle_{AB} = U_{AB}^{gag}(b)\,|\psi_0\rangle_{AB}$$

où

$$U_{AB}^{gag}(b) = (U_{B,n} \otimes U_{A,n}(b)).....(U_{B,2} \otimes U_{A,2}(b))(U_{B,1} \otimes U_{A,1}(b))$$

représente la suite d'opérations unitaires faites par les deux parties honnêtes dans la phase de mise en gage. On voit bien que dans cette relation les opérateurs appliqués par Alice, $U_{A,j}(b)$, dependent du bit qu'elle met en gage. Ceci permet d'écrire l'opérateur de densité de Bob :

$$\rho_B^{gag}(b) = Tr_A\left(|\psi(b)_n\rangle_{ABAB}\,\langle\psi(b)_n|\right)$$

avec

$$|\psi(b)_n\rangle_{AB} \in \mathcal{H} = \mathcal{H}_{A,n} \otimes \mathcal{H}_{B,n}$$

$$\rho_B^{gag}(b) \text{ agit dans } \mathcal{H}_{B,n}$$

C'est la même chose dans la phase de révélation. Si elle contient m tours, on continue ainsi

$$|\psi(b)_{n+m}\rangle_{AB} = U_{AB}^{rev}(b)\,|\psi(b)_n\rangle_{AB}$$

où

$$U_{AB}^{rev}(b) = (U_{B,n+m} \otimes U_{A,n+m}(b))..(U_{B,n+2} \otimes U_{A,n+2}(b))(U_{B,n+1} \otimes U_{A,n+1}(b))$$

représente la suite d'opérations unitaires appliquées par les deux parties honnêtes dans la phase de révélation. L'opérateur de densité de Bob est dans ce cas :

$$\rho_B^{rev}(b) = Tr_A\left(|\psi(b)_{n+m}\rangle_{ABAB}\,\langle\psi(b)_{n+m}|\right)$$

avec

$$|\psi(b)_{n+m}\rangle_{AB} \in \mathcal{H} = \mathcal{H}_{A,n+m} \otimes \mathcal{H}_{B,n+m}$$

$$\rho_B^{rev}(b) \text{ agit dans } \mathcal{H}_{B,n+m}$$

Les états $|\psi(0)_{n+m}\rangle_{AB}$ et $|\psi(1)_{n+m}\rangle_{AB}$ sont parfaitement distinguables si les deux parties sont honnêtes. C'est à dire, si vraiment les deux parties sont honnêtes, et Alice s'engage sur le bit b, le résultat de la mesure donne b avec probabilité 1. Ceci qui implique que les deux états, $|\psi(0)_{n+m}\rangle_{AB}$ et $|\psi(1)_{n+m}\rangle_{AB}$ sont orthogonaux :

$${}_{AB}\langle\psi(1)_{n+m}|\psi(0)_{n+m}\rangle_{AB} = 0$$

La situation pour un Bob honnête est soit de mesurer le bit b révélé par Alice ou soit mesurer $\bar{b}$ alors qu'Alice a révélé b. On peut donc modéliser cette situation par une mesure projective qu'il effectue dans $\mathcal{H}_{B,n+m}$ et qui donne l'un des trois résultats de l'ensemble $\{\Pi_0, \Pi_1, \Pi_{invalide}\}$, où Π_b correspond au cas où il mesure le même bit b revélé par Alice et $\Pi_{invalide}$ correspond au cas où il mesure $\bar{b}$ alors qu'Alice a révélé b. Le cas $\Pi_{invalide}$ ne peut avoir lieu que si Alice est malhonnête. On peut supposer, dans tout protocole de mise en gage, que l'état final (après la fin de la phase de révélation), $|\psi(b)_{n+m}\rangle_{AB}$ et en la possession de Bob. Ceci permet d'écrire :

$$\Pi_b |\psi(b)_{n+m}\rangle_{AB} = |\psi(b)_{n+m}\rangle_{AB}$$

De cette relation on peut conclure que Π_b a la forme suivante :

$$\Pi_b = |\psi(b)_{n+m}\rangle_{AB\ AB}\langle\psi(b)_{n+m}| + \hat{O} \tag{3.3}$$

où

$$\hat{O}\,|\psi(b)_{n+m}\rangle_{AB} = 0 \tag{3.4}$$

La relation (3.3) implique aussi que $\hat{O}$ est positif. Pour le voir, il suffit d'écrire le projecteur Π_b dans la base de ses vecteurs propres et de ne pas oublier qu'un projecteur admet, seulement, les valeurs propres 0 et 1.

Théorème 21 *Dans tout protocole de mise en gage on a :*

$$G^{\max} \geq \frac{1}{2} D(\rho_B^{gag}(0), \rho_B^{gag}(1)) \tag{3.5}$$

$$C^{\max} \geq \frac{1}{2}F^2(\rho_B^{gag}(0), \rho_B^{gag}(1)) \tag{3.6}$$

Preuve 1- Si Bob est malhonnête il peut utiliser la stratégie S^B suivante : il suit le protocole honnêtement durant la phase de mise en gage, donc le système à la fin de cette phase est equiprobablement dans l'un des deux états $\rho_B^{gag}(0)$ ou $\rho_B^{gag}(1)$. Après ça, et avant la phase de révélation, il utilise le POVM optimal de distinction (2.26), qui estime l'état exact avec une probabilité $\frac{1}{2}D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + \frac{1}{2}$ en donnant un gain

$$G(S^B) = \frac{1}{2}D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + \frac{1}{2} - \frac{1}{2} = \frac{1}{2}D(\rho_B^{gag}(0), \rho_B^{gag}(1))$$

Puisque dans cette stratégie, Bob s'est comporté honnêtement durant la phase de mise en gage, il y a, peut être, une chance d'augmenter la probabilité d'estimation s'il exploite cette phase autrement. Toutefois, étant donné qu'il a une stratégie qui donne le gain $\frac{1}{2}D(\rho_B^{gag}(0), \rho_B^{gag}(1))$, alors le gain de la stratégie optimale vérifie :

$$G^{\max} \geq \frac{1}{2}D(\rho_B^{gag}(0), \rho_B^{gag}(1))$$

2- Si c'est Alice qui est malhonnête, elle peut utiliser la stratégie S^A suivante : Elle met en gage le bit 0 en suivant honnêtement toutes les étapes de la première phase. Après cela, si elle décide de révéler 0, elle suit honnêtement la phase de révélation. Sinon, elle applique, juste avant la phase de révélation, l'opérateur unitaire $W_{A,n}^{\max}$ déterminé par la relation :

$$\left|\langle\psi(1)_n| W_{A,n}^{\max} \otimes I_{B,n} |\psi(0)_n\rangle\right| = \max_{W_{A,n}} |\langle\psi(1)_n| W_{A,n} \otimes I_{B,n} |\psi(0)_n\rangle|$$

afin de transformer localement l'état $|\psi(0)_n\rangle$ en l'état le plus semblable possible à $|\psi(1)_n\rangle$. Si Alice suit cette stratégie et déclare 0, alors c'est exactement ce que Bob va mesurer, car dans ce cas elle a tout simplement suivi le protocole et donc elle passera le test de Bob avec probabilité $P_{U0}(S^A) = 1$. Si, par contre, Alice suit cette stratégie et déclare 1, la probabilité qu'elle passera le test de Bob est :

$$P_{U1}(S^A) = Tr\left[\Pi_1 U_{AB}^{rev}(1)\left(U_{A,n}^{\max} \otimes I_{B,n}\right)|\psi(0)_n\rangle_{AB\,AB}\langle\psi(1)_n| U_{AB}^{rev\dagger}(1)\left(U_{A,n}^{\max\,\dagger} \otimes I_{B,n}\right)\right]$$

En utilisant la relation (3.3), on obtient :

$$\begin{aligned} P_{U1}(S^A) &= {}_{AB}\langle\psi(1)_n| U_{AB}^{rev\dagger}(1) \left(U_{A,n}^{\max\,\dagger} \otimes I_{B,n}\right) \left(|\psi(1)_{n+m}\rangle_{AB\ AB}\langle\psi(1)_{n+m}| + \hat{O}\right) \\ &\quad U_{AB}^{rev}(1) \left(U_{A,n}^{\max} \otimes I_{B,n}\right) |\psi(0)_n\rangle_{AB} \\ &= \left|{}_{AB}\langle\psi(1)_{n+m}| U_{AB}^{rev}(1) \left(U_{A,n}^{\max} \otimes I_{B,n}\right) |\psi(0)_n\rangle_{AB}\right|^2 + {}_{AB}\langle\phi|\hat{O}|\phi\rangle_{AB} \end{aligned}$$

où

$$|\phi\rangle_{AB} = U_{AB}^{rev}(1) \left(U_{A,n}^{\max} \otimes I_{B,n}\right) |\psi(0)_n\rangle_{AB}$$

Et puisque

$${}_{AB}\langle\psi(1)_{n+m}| U_{AB}^{rev}(1) = \left(U_{AB}^{rev\dagger}(1) |\psi(1)_{n+m}\rangle\right)^\dagger = {}_{AB}\langle\psi(1)_n|$$

et

$${}_{AB}\langle\phi|\hat{O}|\phi\rangle_{AB} \geq 0$$

On aura alors

$$\begin{aligned} P_{U1}(S^A) &= \left|{}_{AB}\langle\psi(1)_n| \left(U_{A,n}^{\max} \otimes I_{B,n}\right) |\psi(0)_n\rangle_{AB}\right|^2 + {}_{AB}\langle\phi|\hat{O}|\phi\rangle_{AB} \qquad (3.7) \\ &\geq \left|{}_{AB}\langle\psi(1)_n| \left(U_{A,n}^{\max} \otimes I_{B,n}\right) |\psi(0)_n\rangle_{AB}\right|^2 \end{aligned}$$

Le fait que la probabilité qu'Alice révèle 0 est égale à la probabilité qu'elle révèle 1 nous permet de conclure l'expression de la probabilité qu'elle passera le test de Bob si elle utilise la stratégie S^A :

$$\begin{aligned} P_U(S^A) &= \frac{1}{2}P_{U0}(S^A) + \frac{1}{2}P_{U1}(S^A) = \frac{1}{2} + \frac{1}{2}P_{U1}(S^A) \\ &\geq \frac{1}{2} + \frac{1}{2}\left|{}_{AB}\langle\psi(1)_n| \left(U_{A,n}^{\max} \otimes I_{B,n}\right) |\psi(0)_n\rangle_{AB}\right|^2 \end{aligned}$$

L'utilisation de la relation (2.31) donne

$$P_U(S^A) \geq \frac{1}{2} + \frac{1}{2}F^2(\rho_B^{gag}(0), \rho_B^{gag}(1))$$

De la définition de $C^{\max}$ dans l'équation (3.2), on obtient :

$$C^{\max} \geq \frac{1}{2}F^2(\rho_B^{gag}(0), \rho_B^{gag}(1))$$

■

Corollaire 7 *Dans tout protocole de mise en gage on a :*

$$2G^{\max} + \sqrt{2C^{\max}} \geq 1 \tag{3.8}$$

Preuve De l'équation (2.32) on peut déduire que

$$D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + F(\rho_B^{gag}(0), \rho_B^{gag}(1)) \geq 1$$

Les équations (3.5) et (3.6) donnent respectivement :

$$2G^{\max} \geq D(\rho_B^{gag}(0), \rho_B^{gag}(1))$$

$$\sqrt{2C^{\max}} \geq F(\rho_B^{gag}(0), \rho_B^{gag}(1))$$

Ce qui nous permet d'écrire :

$$2G^{\max} + \sqrt{2C^{\max}} \geq D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + F(\rho_B^{gag}(0), \rho_B^{gag}(1)) \geq 1$$

■

Ce dernier résultat confirme l'impossibilité d'une mise en gage sûre (arbitrairement liante et arbitrairement camouflante en même temps), comme il nous montre jusqu'à quel point on peut espérer qu'un protocole peut être liant et camouflant en même temps.

Corollaire 8 *Dans tout protocole de mise en gage tel que, $G^{\max} = C^{\max}$, on a :*

$$G^{\max} = C^{\max} \geq \frac{3 - \sqrt{5}}{4} \approx 0.19098$$

Preuve Supposons qu'il existe un protocole telle que $G^{\max} = C^{\max}$. Dans ce cas, (3.8) devient :

$$2G^{\max} + \sqrt{2G^{\max}} \geq 1 \tag{3.9}$$

Puisque le membre gauche de (3.9) est une fonction croissante de $G^{\max}$, alors sa plus petite valeur est atteinte quand $G^{\max}$ est le plus petit possible :

$$2G^{\max} + \sqrt{2G^{\max}} = 1$$

Ce qui implique

$$4G^{2\max} - 6G^{\max} + 1 = 0$$

et donc

$$G^{\max} = \frac{3-\sqrt{5}}{4} \approx 0.19098$$

■

3.2.2 Cas où tout le système initial provient d'Alice

Si on suppose que tout le système utilisé dans la première phase (phase de la mise en gage) provient initialement d'Alice, on peut avoir un résultat plus fort que celui dans la relation (3.6).

Note 4 *On peut imaginer des protocoles de mise en gage qui sortent de cette catégorie. Par exemple, des protocoles où Bob transmet à Alice une partie d'un système intriqué à un autre système qu'il garde, et Alice code son bit sur ce système qu'elle a reçu de Bob, avant de le lui retourner.*

Théorème 22 *Dans tout protocole de mise en gage, si le système initial provient d'Alice, on a :*

$$G^{\max} \geq \frac{1}{2} D(\rho_B^{gag}(0), \rho_B^{gag}(1)) \tag{3.10}$$

$$C^{\max} \geq \frac{1}{2} F(\rho_B^{gag}(0), \rho_B^{gag}(1)) \tag{3.11}$$

Preuve 1- Si Bob est malhonnête, la relation (3.10) découlera directement de la relation (3.5), qui est vraie dans tout protocole de mise en gage.

2- Si c'est Alice qui est malhonnête, la relation (3.11), par contre, est plus forte que (3.6), car le seuil de $C^{\max}$ est plus élevé. On imagine une Alice malhonnête qui applique une stratégie de tricherie S^A, qui s'étend sur toutes les phases du protocole, afin de maximiser sa probabilité de succès. Dans la phase de mise en gage, elle applique

une série d'opérateurs unitaires $U'_{A,1}, U'_{A,2}, ..., U'_{A,n}$ au lieu de suivre le protocole et appliquer la série, $U_{A,1}(b), U_{A,2}(b), .., U_{A,n}(b)$, sur l'état initial $|\psi_0\rangle_A$, provenant d'elle, ce qui donne :

$$|\psi'_n\rangle_{AB} = (U_{B,n} \otimes U'_{A,n}).....(U_{B,2} \otimes U'_{A,2})(U_{B,1} \otimes U'_{A,1}) |\psi_0\rangle_A$$

Ce type de protocole donne à Alice la liberté totale du choix de l'état de tout le système $A + B$ à la fin de la phase de mise en gage, ce qui n'était pas nécessairement vrai dans le cas général, et donc, plus d'occasion pour tricher, car elle peut annuler tout effet que Bob puisse rapporter au système. Pour ce faire, elle choisit l'état qu'elle veut avoir à la fin de cette première phase, soit par exemple : $T |\psi_0\rangle_A$, et applique la série d'opérateurs unitaires :$U'_{A,1} = U^{-1}_{B,1}U^{-1}_{B,2}U^{-1}_{B,3}...U^{-1}_{B,n}T$, $U'_{A,j} = I_{A,j}$, $j \in [2, n]$ à la place de $U_{A,i}(b)$, $i \in [1, n]$. L'état résultant à la fin de la phase de mise en gage est exactement l'état voulu :

$$\begin{aligned} |\psi'_n\rangle_{AB} &= (U_{B,n} \otimes U'_{A,n}).....(U_{B,2} \otimes U'_{A,2})(U_{B,1} \otimes U'_{A,1}) |\psi_0\rangle_A \\ &= (U_{B,n} \otimes I_{A,n}).....(U_{B,2} \otimes I_{A,2})(U_{B,1} \otimes U^{-1}_{B,1}U^{-1}_{B,2}U^{-1}_{B,3}...U^{-1}_{B,n}T) |\psi_0\rangle_A \\ &= T |\psi_0\rangle_A \end{aligned}$$

Bien qu'Alice ait décidé l'état du système $A + B$ à la fin de la première phase : $|\psi\rangle_{AB,n} = T |\psi_0\rangle_A$, elle n'a plus le contrôle total sur lui quand elle décide de révéler car il appartient à $H_{A,n} \otimes H_{B,n}$. Il ne faut pas oublier que, durant la première phase, elle n'a pas encore décidé quel bit elle va révéler. Maintenant, au début de la phase de révélation, si elle décide de révéler le bit b, elle applique une transformation unitaire $U_A(b) \otimes I_{B,n}$ dépendant du bit de son choix, pour avoir, juste avant la révélation, l'état

$$(U_A(b) \otimes I_n)T |\psi_0\rangle_A$$

Sa stratégie de tricherie peut s'étendre à la phase de révélation par l'application d'une série de transformations unitaires différentes de celles prévues par le protocole, par exemple : $U'_{A,n+1}(b), U'_{A,n+2}....., U'_{n+m}(b)$ au lieu de $U_{A,n+1}(b), U_{A,n+2}....., U_{A,n+m}(b)$. Ceci donne :

$$|\psi'(b)_{n+m}\rangle_{AB} = U'^{rev}_{AB}(b)(U_A(b) \otimes I_n)T |\psi_0\rangle_A$$

où

$$U'^{rev}_{AB}(b) = (U_{B,n+m} \otimes U'_{A,n+m}(b)).....(U_{B,n+2} \otimes U'_{A,n+2}(b))(U_{B,n+1} \otimes U'_{A,n+1}(b))$$

En supposant que la probabilité qu'Alice révèle le bit 0 soit égale à la probabilité qu'elle révèle le bit 1, on peut exprimer sa probabilité de passer le test de Bob par :

$$P_U(S^A) = \frac{1}{2}P_{U_0} + \frac{1}{2}P_{U_1} \tag{3.12}$$

où

$$\begin{aligned} P_{U_b} &= Tr[\Pi_b \left|\psi'(b)_{n+m}\right\rangle_{AB\ AB} \left\langle\psi'(b)_{n+m}\right|] \\ &= Tr\left[\Pi_b U'^{rev}_{AB}(b)(U_A(b) \otimes I_n)T \left|\psi_0\right\rangle_{A\ A} \left\langle\psi_0\right| T^\dagger (U_A^\dagger(b) \otimes I_n)U'^{rev\dagger}_{AB}(b)\right] \end{aligned} \tag{3.13}$$

En substituant P_{U_b} par sa valeur de (3.13) dans (3.12) :

$$P_U(S^A) = \frac{1}{2}\sum_{b=0,1} Tr\left[\Pi_b U'^{rev}_{AB}(b)(U_A(b) \otimes I_n)T \left|\psi_0\right\rangle_{A\ A} \left\langle\psi_0\right| T^\dagger (U_A^\dagger(b) \otimes I_n)U'^{rev\dagger}_{AB}(b)\right]$$

Et puisque le but d'une Alice malhonnête est de maximiser P_U, on peut exprimer la probabilité maximale qu'elle pourra réaliser son but comme :

$$\begin{aligned} P_U^{\max} &= \frac{1}{2}\sum_{b=0,1} Tr\left[\Pi_b \max_{U'_{A,n+j}(b)} \max_{U_A(b)} U'^{rev}_{AB}(b)(U_A(b) \otimes I_n)\max_T (T \left|\psi_0\right\rangle_{A\ A} \left\langle\psi_0\right| T^\dagger)\right. \\ &\quad \left.(U_A^\dagger(b) \otimes I_n)U'^{rev\dagger}_{AB}(b)\right] \end{aligned}$$

Où $U'^{rev}_{AB}(b)$ est en fonction des $U'_{A,n+j}(b)$. C'est Alice seule qui a construit l'état $T\left|\psi_0\right\rangle_A$. Elle peut donc choisir celui qui maximise $P_U^{\max}$. Une fois la phase de mise en gage terminée, ce n'est plus la même situation, car son choix du bit à révéler se fait dans une phase où elle n'a plus le contrôle sur tout le système. Pour cette raison on peut exprimer $P_U^{\max}$ de la manière suivante :

$$\begin{aligned} P_U^{\max} &= \frac{1}{2}\max_T \sum_{b=0,1} \max_{U'_{A,n+j}(b)} \max_{U_A(b)} Tr\left[\Pi_b U'^{rev}_{AB}(b)(U_A(b) \otimes I_n)\left(T \left|\psi_0\right\rangle_{A\ A} \left\langle\psi_0\right| T^\dagger\right)\right. \\ &\quad \left.(U_A^\dagger(b) \otimes I_n)U'^{rev\dagger}_{AB}(b)\right] \end{aligned}$$

En remplaçant Π_b par sa valeur dans l'équation (3.3), et en utilisant le fait que $\hat{O}$ est positif, on obtient :

$$\begin{aligned}
P_U^{\max} &= \frac{1}{2}\max_T \sum_{b=0,1} \max_{U'_{A,n+j}(b)} \max_{U_A(b)} Tr\left[\left(|\psi(b)_{n+m}\rangle_{AB\ AB}\langle\psi(b)_{n+m}| + \hat{O}\right)\right. \\
&\quad \left. U'^{rev}_{AB}(b)(U_A(b)\otimes I_n)\left(T|\psi_0\rangle_{A\ A}\langle\psi_0|T^\dagger\right)(U_A^\dagger(b)\otimes I_n)U'^{rev\dagger}_{AB}(b)\right] \\
&= \frac{1}{2}\max_T \sum_{b=0,1} \max_{U'_{A,n+j}(b)} \max_{U_A(b)} Tr\left[\left({}_A\langle\psi_0|T^\dagger\right)(U_A^\dagger\langle b)\otimes I_n)U'^{rev\dagger}_{AB}(b)\right. \\
&\quad \left.\left(|\psi(b)_{n+m}\rangle_{AB\ AB}\langle\psi(b)_{n+m}| + \hat{O}\right)U'^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A\right] \\
&\geq \frac{1}{2}\max_T \sum_{b=0,1} \max_{U'_{A,n+j}(b)} \max_{U_A(b)} Tr\left[{}_A\langle\psi_0|T^\dagger(U_A^\dagger(b)\otimes I_n)U'^{rev\dagger}_{AB}(b)\right. \\
&\quad \left.(|\psi(b)_{n+m}\rangle_{AB\ AB}\langle\psi(b)_{n+m}|)\,U'^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A\right]
\end{aligned}$$

Si Alice utilise la série d'opérateurs $U'_{A,n+1}(b), U'_{A,n+2}.....,U'_{A,n+m}(b)$, durant la phase de révélation, au lieu de $U_{A,n+1}(b), U_{A,n+2}..,U_{A,n+m}(b)$, c'est pour augmenter la probabilité $P_U^{\max}$. Donc,

$$\begin{aligned}
P_U^{\max} &\geq \frac{1}{2}\max_T \sum_{b=0,1} \max_{U_A(b)} Tr\left[\left({}_A\langle\psi_0|T^\dagger\right)(U_A^\dagger(b)\otimes I_n)U^{rev\dagger}_{AB}(b)\right. \\
&\quad \left.(|\psi(b)_{n+m}\rangle_{AB\ AB}\langle\psi(b)_{n+m}|)\,U^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A\right]
\end{aligned}$$

Et puisque

$$\begin{aligned}
&\left[\left({}_A\langle\psi_0|T^\dagger\right)(U_A^\dagger(b)\otimes I_n)U^{rev\dagger}_{AB}(b)\,(|\psi(b)_{n+m}\rangle_{AB\ AB}\langle\psi(b)_{n+m}|)\right. \\
&\left.U^{unv}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A\right] \\
&= \left[({}_{AB}\langle\psi(b)_{n+m}|\,U^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A\ )^*\right. \\
&\left.({}_{AB}\langle\psi(b)_{n+m}|\,U^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A)\right] \\
&= \left|{}_{AB}\langle\psi(b)_{n+m}|\,U^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_{AB,n}\right|^2
\end{aligned}$$

on peut écrire alors,

$$P_U^{\max} \geq \frac{1}{2}\max_T \sum_{b=0,1} \max_{U_A(b)} \left|{}_{AB}\langle\psi(b)_{n+m}|\,U^{rev}_{AB}(b)(U_A(b)\otimes I_n)T|\psi_0\rangle_A\right|^2 \qquad (3.14)$$

On sait que

$$|\psi(b)_{n+m}\rangle_{AB} = U^{rev}_{AB}(b)\,|\psi(b)_n\rangle$$

où $|\psi(b)_n\rangle$ serait l'état du système à la fin de la phase de la mise en gage si les deux parties étaient honnêtes. La relation (3.14) devient donc :

$$P_U^{\max} \geq \frac{1}{2}\max_{T} \sum_{b=0,1} \max_{U_A(b)} \left|_{AB}\langle\psi(b)_n| (U_A(b)\otimes I_n) T |\psi_0\rangle_A\right|^2 \tag{3.15}$$

Il y a une importante différence entre cette dernière relation et la relation (3.7). Ici, Alice peut choisir l'état total du système juste après la phase de mise en gage $T|\psi_0\rangle_A$. Par contre dans la relation (3.7), cet état est un résultat de calcul commun. Une autre manière d'exprimer la relation (3.15) consiste à maximiser sur tous les états possibles $|\psi\rangle = T|\psi_0\rangle_A$ au lieu de maximiser sur toutes les transformations unitaires possible T :

$$P_U^{\max} \geq \frac{1}{2}\max_{|\psi\rangle} \sum_{b=0,1} \max_{U_A(b)} \left|_{AB}\langle\psi(b)_n| (U_A(b)\otimes I_n) |\psi\rangle\right|^2 \tag{3.16}$$

En posant :

$$\left(U_A^\dagger(b)\otimes I_B\right)|\psi(b)_n\rangle_{AB} = |\phi_b\rangle \tag{3.17}$$

la relation (3.16) peut s'écrire :

$$P_U^{\max} \geq \frac{1}{2}\max_{|\phi_b\rangle} \max_{|\psi\rangle} \sum_{b\in\{0,1\}} |\langle\phi_b|\psi\rangle|^2 \tag{3.18}$$

Il faut prendre garde que la maximisation suivant $|\phi_b\rangle$ est seulement dans $\mathcal{H}_A$. Soit $|\chi\rangle$ un vecteur propre de l'opérateur hermitien $|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|$:

$$\left(|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|\right)|\chi\rangle = \lambda|\chi\rangle \tag{3.19}$$

Par l'application du bra $\langle\chi|$ à gauche de (3.19), on obtient

$$|\langle\phi_0|\chi\rangle|^2 + |\langle\phi_1|\chi\rangle|^2 = \lambda$$

Puisque $|\psi\rangle$ est un indice muet dans la relation (3.16), l'expression à droite de cette relation n'est alors que la plus grande valeur propre de l'opérateur $|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|$. Cette valeur maximale est atteignable par la maximisation suivant $|\psi\rangle$, car c'est Alice qui a préparé cet état. L'expression de $|\phi_1\rangle$ dans la base $\{|\phi_0\rangle, |\phi_0\rangle_\perp\}$ est :

$$|\phi_1\rangle = \langle\phi_0|\phi_1\rangle|\phi_0\rangle + {}_\perp\langle\phi_0|\phi_1\rangle|\phi_0\rangle_\perp$$

Ceci nous permet d'écrire l'opérateur $|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|$ dans cette base comme suit :

$$\begin{aligned} F &= |\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1| \\ &= \begin{pmatrix} 1 + |\langle\phi_0|\phi_1\rangle|^2 & \langle\phi_0|\phi_1\rangle\langle\phi_1|\phi_0\rangle_\perp \\ {}_\perp\langle\phi_0|\phi_1\rangle\langle\phi_1|\phi_0\rangle & |{}_\perp\langle\phi_0|\phi_1\rangle|^2 \end{pmatrix} \end{aligned}$$

L'utilisation de l'équation des valeurs propres de F :

$$F|\psi\rangle = \lambda|\psi\rangle$$

implique :

$$\det[(F - \lambda I)|\psi\rangle] = 0$$

et donc :

$$\lambda^2 - 2\lambda + |{}_\perp\langle\phi_0|\phi_1\rangle|^2 = 0 \tag{3.20}$$

Les solution de l'équation (3.20) sont :

$$\lambda_1 = 1 + \sqrt{1 - |{}_\perp\langle\phi_0|\phi_1\rangle|^2} = 1 + |\langle\phi_0|\phi_1\rangle|$$

$$\lambda_2 = 1 - \sqrt{1 - |{}_\perp\langle\phi_0|\phi_1\rangle|^2} = 1 - |\langle\phi_0|\phi_1\rangle|$$

Donc,

$$\max(\lambda_1, \lambda_2) = 1 + |\langle\phi_0|\phi_1\rangle|$$

Ceci permet d'écrire (3.16) comme suit :

$$P_U^{\max} \geq \frac{1}{2}\max_{|\phi_b\rangle}\ (1 + |\langle\phi_0|\phi_1\rangle|)$$

En remplaçant $|\phi_b\rangle$ par sa valeur dans l'équation (3.17) :

$$\begin{aligned} P_U^{\max} &\geq \frac{1}{2}\max_{|\phi_0\rangle,|\phi_1\rangle} 1 + |\langle\phi_0|\phi_1\rangle| \qquad (3.21) \\ &= \frac{1}{2} + \frac{1}{2}\max_{U_A(0),U_A(1)} \left|\left\langle\psi(0)_n|(U_A(0)\otimes I_B)(U_A^\dagger(1)\otimes I_B)|\psi(1)_n\right\rangle_{AB}\right| \\ &= \frac{1}{2} + \frac{1}{2}\max_{U_A(0),U_A(1)} \left|\left\langle\psi(0)_n|(U_A(0)(U_A^\dagger(1)\otimes I_B)|\psi\langle 1)_n\right\rangle_{AB}\right| \\ &= \frac{1}{2} + \frac{1}{2}\max_{U_A} |\langle\psi(0)_n|(U_A\otimes I)|\psi(1)_n\rangle| \end{aligned}$$

Par définition de $P_U^{\max}$ et grâce à la relation (2.31), on peut écrire :

$$C^{\max} \geq \frac{1}{2} F(\rho_0, \rho_1)$$

■

Corollaire 9 *Dans tout protocole de mise en gage, si le système initial provient d'Alice, on a* $G^{\max} + C^{\max} \geq \frac{1}{2}$.

Preuve Le résultat découle directement de la relation (2.32) et du théorème 22 :

$$G^{\max} + C^{\max} \geq \frac{1}{2} F(\rho_0, \rho_1) + \frac{1}{2} D(\rho_0, \rho_1) \geq \frac{1}{2}$$

■

Corollaire 10 *Dans tout protocole de mise en gage, si le système initial provient d'Alice et* $G^{\max} = C^{\max}$, *on a* $G^{\max} = C^{\max} \geq \frac{1}{4}$

Preuve C'est un résultat direct du corollaire précédent :

$$G^{\max} = C^{\max} \Longrightarrow 2G^{\max} \geq \frac{1}{2} \Longrightarrow G^{\max} \geq \frac{1}{4}$$

■

3.2.3 Mise en gage de purification

En résumé, ce type de protocole comporte deux tours. La phase de mise en gage se déroule en un tour, où Alice prépare l'un des deux états orthogonaux, $|\psi(0)_1\rangle_{AB}$, $|\psi(1)_1\rangle_{AB}$ dans $\mathcal{H}_{A,1} \otimes \mathcal{H}_{B,2}$, et envoie le système B à Bob. La phase de révélation, comporte l'autre tour, où Alice prouve sa bonne foi à Bob en lui envoyant le système A. Bob effectue une mesure projective $\{\Pi_0, \Pi_1\}$ telle que :

$$\Pi_b = |\psi(b)_1\rangle_{AB\ AB}\langle\psi(b)_1|$$

Remarque 5 *Ce type de protocole est dit de purification, car dans la phase de révélation, une Alice honnête prouve à Bob que l'état qu'il détient, après qu'elle lui ait fourni le système A, est une purification de l'état qu'il a reçu d'elle dans la phase de mise en gage.*

La mise en gage de purification est un cas particulier du modèle exposé plus haut, où tout le système initial provenait d'Alice, elle se déroule comme suit : Dans le premier tour, dit de mise en gage, Alice prépare l'état $U_A^{gag}(b)\left|\psi_0\right\rangle_A$ et envoie à Bob le système (la partie) B. C-à-d., à la fin de la phase de mise en gage les deux parties partagent l'état $\left|\psi(b)_1\right\rangle_{AB}$:

$$\left|\psi(b)_1\right\rangle_{AB} = U_A^{gag}(b)\left|\psi_0\right\rangle_A \in \mathcal{H} = \mathcal{H}_{A,1} \otimes \mathcal{H}_{B,1}$$

À la fin de la phase de révélation, qui se déroule en un seul tour aussi, tout le système est en possession de Bob et son état est :

$$\left|\psi(b)_2\right\rangle_{AB} = U_{AB}^{rev}(b)\left|\psi(b)_1\right\rangle_{AB} = \left|\psi(b)_1\right\rangle_{AB} \in \mathcal{H} = \mathcal{H}_{B,2}$$

Ce protocole correspond dans le modèle général au cas : $n = 1, m = 1$. C-à-d.,

$$U_{AB}^{rev}(b) = I_{AB}$$

et la seule opération non triviale dans cette phase est la nouvelle répartition du système $A + B$ entre Alice et Bob.

Théorème 23 *Dans tout protocole de mise en gage de purification on a :*

$$G^{\max} = \frac{1}{2}D(\rho_B^{gag}(0), \rho_B^{gag}(1)) \tag{3.22}$$

$$C^{\max} = \frac{1}{2}F(\rho_B^{gag}(0), \rho_B^{gag}(1)) \tag{3.23}$$

Où

$$\rho_B^{gag}(b) = Tr_A\left(\left|\psi(b)_1\right\rangle_{AB\,AB}\left\langle\psi(b)_1\right|\right)$$

Preuve 1- Si Bob est malhonnête, puisque dans ce type de protocole il n'a aucun rôle dans la phase de mise en gage, alors toute tentative de tricherie de sa part, commence après qu'il aura reçu le système B d'Alice. La formule (2.26) donne alors :

$$G^{\max} = \frac{1}{2} D(\rho_B^{com}(0), \rho_B^{com}(1))$$

2- Si c'est Alice qui est malhonnête, elle ne peut tricher qu'on deux endroits. Au lieu de préparer un des deux états prévus par le protocole, $|\psi(0)_1\rangle_{AB}$ ou $|\psi(1)_1\rangle_{AB}$, elle prépare un état $|\chi\rangle_{AB}$ de son choix. Elle peut aussi appliquer une transformation unitaire locale $U(b)$ (dépendante du bit qu'elle veut révéler), au début de la phase de révélation. Le but d'Alice ici et de maximiser $P_U^{\max}$:

$$P_U^{\max} = \frac{1}{2} \max_{|\chi\rangle} \sum_b \max_{U_A(b)} |\langle \psi(b)_1 | (U_A(b) \otimes I) | \chi \rangle_{AB}|^2$$

L'utilisation de l'équation (2.31) donne :

$$P_U^{\max} = \frac{1}{2} \max_{\sigma_B} \left(F^2(\rho_B^{com}(0), \sigma_B) + F^2(\rho_B^{com}(1), \sigma_B) \right)$$

où

$$\sigma_B = Tr_A(|\chi\rangle_{AB\ AB}\langle\chi|)$$

En utilisant l'équation (2.33) et la définition de $C^{\max}$, on obtient :

$$C^{\max} = \frac{1}{2} F(\rho_B^{com}(0), \rho_B^{com}(1))$$

■

3.2.4 Exemples de protocoles saturant les bornes sur $C^{\max}$ et $G^{\max}$ quand tout le système intial provient d'Alice

Si on choisit deux opérateurs de densité tels que :

$$D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + F(\rho_B^{gag}(0), \rho_B^{gag}(1)) = 1$$

et si le protocole de mise en gage est de purification, grâce au théorème 23, le corollaire 9 donne :

$$G^{\max} + C^{\max} = \frac{1}{2} D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + \frac{1}{2} F(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \frac{1}{2}$$

L'exemple suivant sature les relations des corollaires 9 et 10.

Exemple 24 *Soient les deux opérateurs de densité* $\rho_B^{gag}(0)$, $\rho_B^{gag}(1)$ *définis par :*

$$\rho_B^{gag}(0) = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & 0 \end{pmatrix}, \rho_B^{gag}(1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

Des définitions de la fidélité et de la distance dans (2.28) et (2.25) on a :

$$D(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \lambda$$

$$F(\rho_B^{gag}(0), \rho_B^{gag}(1)) = 1 - \lambda$$

Si le protocole de mise en gage est de purification, le théorème 23 implique :

$$G^{\max} = \frac{1}{2}\lambda$$

$$C^{\max} = \frac{1}{2}(1-\lambda)$$

Pour un protocole où $G^{\max} = C^{\max}$, *on aura alors :*

$$G^{\max} = C^{\max} \Longrightarrow \frac{1}{2}\lambda = \frac{1}{2}(1-\lambda) \Longrightarrow \lambda = \frac{1}{2}$$

et donc,

$$G^{\max} = C^{\max} = \frac{1}{4}$$

Pour $\lambda = \frac{1}{2}$, *on a*

$$\rho_B^{gag}(b) = \frac{1}{2}\left|\phi_{b,0}\right\rangle\left\langle\phi_{b,0}\right| + \frac{1}{2}\left|\phi_{b,1}\right\rangle\left\langle\phi_{b,1}\right|$$

où

$$\left|\phi_{b,x}\right\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle & si\ b=0,\ x=0 \\ \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle & si\ b=0,\ x=1 \\ \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|2\right\rangle & si\ b=1,\ x=0 \\ \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|2\right\rangle & si\ b=1,\ x=1 \end{cases}$$

Donc, on peut imaginer le protocole de mise en gage suivant.

Protocole 3

1. Mise en gage : Pour s'engager sur le bit b, Alice choisit aléatoirement le nombre $x \in \{0,1\}$ et envoie l'état $|\phi_{b,x}\rangle$ à Bob.

2. Révélation : Si Alice décide de révéler le bit, elle dévoile les bits classiques b et x à Bob. Bob mesure l'état envoyé par Alice dans la phase de mise en gage dans la base $\{|\phi_{0,x}\rangle, |\phi_{1,x}\rangle\}$ et vérifie si l'état est bel et bien $|\phi_{b,x}\rangle$.

Si les opérateurs de densité $\rho_B^{gag}(0)$ et $\rho_B^{gag}(1)$ appartiennent au même espace à deux dimensions, ou si l'un d'eux est un état pur, on peut écrire, grâce aux relations (2.35) et (2.36) :

$$D(\rho,\sigma) + F^2(\rho,\sigma) \geq 1$$

L'utilisation du théorème 22 donne :

$$2G^{\max} \geq D \text{ et } 4\left(C^{\max}\right)^2 \geq F^2(\rho,\sigma)$$

D'où

$$2G^{\max} + 4\left(C^{\max}\right)^2 \geq D(\rho,\sigma) + F^2(\rho,\sigma) \geq 1$$

Dans le cas $G^{\max} = C^{\max}$, on obtient :

$$2G^{\max} + 4\left(G^{\max}\right)^2 \geq D(\rho,\sigma) + F^2(\rho,\sigma) \geq 1$$

Ceci implique :

$$2C^{\max} + 4\left(C^{\max}\right)^2 \geq D(\rho,\sigma) + F^2(\rho,\sigma) \geq 1$$

$$\begin{aligned} G^{\max} &\geq \frac{1}{4}\left(\sqrt{5}-1\right) > \frac{1}{4} \\ C^{\max} &\geq \frac{1}{4}\left(\sqrt{5}-1\right) > \frac{1}{4} \end{aligned}$$

Ceci montre l'impossibilité d'un protocole de mise en gage où le système initial provient d'Alice tel que $G^{\max} = C^{\max} = \frac{1}{4}$ si l'espace est de dimension inférieure à trois.

Les états de l'exemple suivant permettent d'avoir la valeur optimale de $G^{\max} = C^{\max}$ dans un espace à deux dimensions.

Exemple 25 *Soit un protocole de purification qui utilise les deux opérateurs de densité à deux dimensions :*

$$\rho_B^{gag}(0) = \begin{pmatrix} 1-\lambda & 0 \\ 0 & \lambda \end{pmatrix} \ , \ \rho_B^{gag}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

L'utilisation des équations (2.25) et (2.28) donne :

$$D(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \lambda$$

$$F(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \sqrt{1-\lambda}$$

Ceci implique :

$$D(\rho_B^{gag}(0), \rho_B^{gag}(1)) + F^2(\rho_B^{gag}(0), \rho_B^{gag}(1)) = 1$$

Puisque il s'agit d'une mise en gage de purification, le théorème 23 donne

$$G^{\max} = \frac{1}{2} D(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \frac{1}{2}\lambda$$

$$C^{\max} = \frac{1}{2} F(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \frac{1}{2}\sqrt{1-\lambda}$$

Pour un protocole où $G^{\max} = C^{\max}$, on obtient :

$$G^{\max} = C^{\max} \Longrightarrow \frac{1}{2}\lambda = \frac{1}{2}\sqrt{1-\lambda} \Longrightarrow \lambda = \frac{1}{2}\sqrt{5} - \frac{1}{2}$$

et donc,

$$G^{\max} = C^{\max} = \frac{1}{4}\left(\sqrt{5} - 1\right)$$

Remarque 6 *L'exemple 25 traite aussi le cas où l'un des deux états est pur puisque $\rho_B^{gag}(1) = |0\rangle\langle 0|$.*

Si les deux opérateurs de densité $\rho_B^{gag}(0)$ et $\rho_B^{gag}(1)$ représentent des états purs, l'utilisation de la relation (2.34) et du théorème 22 donne :

$$4\,(G^{\max})^2 + 4\,(C^{\max})^2 \geq D^2(\rho, \sigma) + F^2(\rho, \sigma) = 1$$

Donc

$$(G^{\max})^2 + (C^{\max})^2 \geq \frac{1}{4}$$

Si $G^{\max} = C^{\max}$,

$$\begin{aligned} G^{\max} &\geq \frac{1}{2\sqrt{2}} \\ C^{\max} &\geq \frac{1}{2\sqrt{2}} \end{aligned}$$

Les états de l'exemple suivant atteignent la valeur optimale de $G^{\max} = C^{\max}$ dans un espace à deux dimensions dans le cas d'états purs.

Exemple 26 *Soient les deux états purs :*

$$\rho_B^{gag}(0) = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\rho_B^{gag}(1) = (\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle)(\cos\alpha\,\langle 0| + \sin\alpha\,\langle 1|) = \begin{pmatrix} \cos^2\alpha & \cos\alpha\sin\alpha \\ \cos\alpha\sin\alpha & \sin^2\alpha \end{pmatrix},$$

$$0 \leq \alpha \leq \frac{\pi}{2}$$

Les équations (2.25) et (2.28) donnent

$$D(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \sin\alpha$$

$$F(\rho_B^{gag}(0), \rho_B^{gag}(1)) = \cos\alpha$$

Dans le cas d'une mise en gage de purification, le théorème 23 implique :

$$G^{\max} = \frac{1}{2}\sin\alpha$$

$$C^{\max} = \frac{1}{2}\cos\alpha$$

Dans le cas particulier où $G^{\max} = C^{\max}$, on a

$$\frac{1}{2}\sin\alpha = \frac{1}{2}\cos\alpha \Longrightarrow \alpha = \frac{\pi}{4}$$

Ceci donne

$$\begin{aligned} G^{\max} &= \frac{1}{2\sqrt{2}} \\ C^{\max} &= \frac{1}{2\sqrt{2}} \end{aligned}$$

3.3 Mise en gage quantique sensible à la tricherie (cheat-sensitive)

Dans le protocole de mise gage quantique standard, la possibilité qu'Alice détecte la tricherie de Bob n'est pas considérée. Il y a une variante du protocole de mise en gage quantique qui tente de profiter de la possibilité d'en tenir compte. Dans un tel protocole, Alice ne peut modifier la probabilité de révéler 0 ou 1, une fois la phase de mise en gage terminée, sans courir le risque d'être détectée (ce qui était le cas dans tous les protocoles considérés jusqu'à maintenant) et Bob ne peut avoir d'information sur le bit mis en gage avant la révélation sans courir le risque d'être détecté(ce qui est nouveau). Il est clair que le protocole de mise en gage quantique standard ne peut garantir ce type de sécurité, car une fois qu'Alice révèle l'état qu'elle a utilisé pour coder son bit, Bob peut lui retourner une copie de cet état, même s'il l'a mesuré avant la révélation. Dans le but d'avoir ce type de sécurité, Lucien Hardy et Adrian Kent [35] ont proposé le protocole suivant, qui a été démontré non sécuritaire, récement, par Satoshi Ishizaka [39].

Protocole 4

1. Phase (préparation) : Bob prépare l'état $|\phi^+\rangle_{CD} = \frac{1}{\sqrt{2}}(|0\rangle_C |0\rangle_D + |1\rangle_C |1\rangle_D)$, qui va être utilisé dans un jeu de pile ou face, et envoie le qubit D à Alice.

2. Phase (mise en gage) : Si Alice décide de s'engager au bit 0, elle choisit aléatoirement un des deux qubits $|0\rangle_B$ ou $|-\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B - |1\rangle_B)$ et l'envoie à Bob. Si Alice décide de s'engager au bit 1, elle choisit aléatoirement un des deux qubits $|1\rangle_B$ ou $|+\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B)$ et l'envoie à Bob.

3. Phase (Révélation) : Alice a l'option de demander à Bob qu'il lui envoie le qubit C pour qu'elle s'assure qu'il avait réellement péparé $|\phi^+\rangle_{CD}$. Cependant, elle doit alors lui révéler la valeur du bit mis en gage sans lui révéler l'état qu'elle a utilisé pour le coder. Après ça, Bob peut demander à Alice de lui retourner le qubit D si elle n'a pas utilisé cette option.

4. Phase (Pile ou face) : Si l'une des deux parties a demandé la vérification de l'état $\left|\phi^{+}\right\rangle_{CD}$ et n'a pas détecté une tricherie, alors elle perd le pile ou face. Si aucune partie n'a demandé la vérification de $\left|\phi^{+}\right\rangle_{CD}$, Bob mesure le qubit D dans la base $\{|0\rangle, |1\rangle\}$ et envoie le résultat à Alice qui doit vérifier sa conformité en mesurant le qubit C. Si le résultat est 0(1) Alice (Bob) perd le pile ou face.

5. Phase (vérification) : Si Bob gagne le pile ou face, Alice doit lui révéler le qubit B et alors Bob vérifie que c'est bon! Si Alice gagne le pile ou face, Bob doit lui retourner le qubit B et Alice vérifie que c'est bon!

Dans [35], Hardy et Kent ont montré que ce protocole garantit une probabilité non nulle de détection contre les tentatives malveillantes d'Alice. Cependant, leur démonstration en ce qui concerne la sécurité du protocole par rapport aux tentatives de Bob n'était pas correcte. Pour cela, Satoshi Ishizaka [39] a proposé la stratégie suivante, que Bob peut utiliser pour gagner de l'information sur le bit mis en gage, sans aucune possibilité de détection par Alice : Bob prépare honnêtement l'état $\left|\phi^{+}\right\rangle_{CD}$, qui va être utilisé dans le pile ou face, et envoie le qubit C à Alice. Une fois la phase de mise en gage terminée, il réalise la mesure généralisée $\{M_0, M_1 : M_0^{\dagger}M_0 + M_1^{\dagger}M_1 = I_B\}$ sur le qubit B, où :

$$M_0 = \sqrt{\frac{2}{3}}\left|\psi_0\right\rangle_{BB}\left\langle\psi_0\right| + \sqrt{\frac{1}{3}}\left|\psi_1\right\rangle_{BB}\left\langle\psi_1\right|$$

$$M_1 = \sqrt{\frac{2}{3}}\left|\psi_0\right\rangle_{BB}\left\langle\psi_0\right| + \sqrt{\frac{1}{3}}\left|\psi_1\right\rangle_{BB}\left\langle\psi_1\right|$$

et

$$\left|\psi_0\right\rangle_B = \cos\frac{\pi}{8}\left|0\right\rangle_B - \sin\frac{\pi}{8}\left|1\right\rangle_B$$

$$\left|\psi_1\right\rangle_B = \sin\frac{\pi}{8}\left|0\right\rangle_B + \cos\frac{\pi}{8}\left|1\right\rangle_B$$

Si Alice s'engage sur le bit 0, l'état du qubit B est :

$$\rho_0 = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|-\right\rangle\left\langle -\right| = \begin{pmatrix} \frac{3}{4} & \frac{-1}{4} \\ \frac{-1}{4} & \frac{1}{4} \end{pmatrix}$$

La probabilité que Bob mesure M_0 dans ce cas est :

$$p_{M_0|0} = Tr(M_0\rho_0M_0^{\dagger}) = \frac{1}{2} + \frac{\sqrt{2}}{12}$$

Si Alice s'engage sur le bit 1, l'état du qubit B est :

$$\rho_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} \end{pmatrix}$$

et la probabilité que Bob mesure M_1 cette fois est :

$$p_{M_1|1} = Tr(M_0\rho_1 M_0^\dagger) = \frac{1}{2} + \frac{\sqrt{2}}{12}$$

On démontre qu'il est toujours possible pour Bob de récupérer n'importe quel état envoyé par Alice dans la phase de mise en gage. Autrement dit, la stratégie de Bob ne dépend pas de l'état envoyé par Alice. Pour ce faire, supposons qu'Alice envoie à Bob un état $|\chi\rangle_B$. Puisque les deux états $|\psi_0\rangle, |\psi_1\rangle$ sont orthogonaux, on peut choisir comme base dans B l'ensemble : $\{|\psi_0\rangle, |\psi_1\rangle\}$. L'état $|\chi\rangle$ peut s'exprimer dans cette base par :

$$|\chi\rangle_B = \alpha|\psi_0\rangle_B + \beta|\psi_1\rangle_B$$

Si Bob mesure M_0, l'état de B devient :

$$|\Psi\rangle_B = \frac{M_0|\chi\rangle_B}{\sqrt{{}_B\langle\chi|M_0^\dagger M_0|\chi\rangle_B}} = \frac{\sqrt{\frac{2}{3}}\alpha|\psi_0\rangle_B + \sqrt{\frac{1}{3}}\beta|\psi_1\rangle_B}{\sqrt{\frac{2}{3}|\alpha|^2 + \frac{1}{3}|\beta|^2}}$$

Si Alice demande à Bob de lui envoyer le qubit D pour qu'elle puisse vérifier l'état $|\phi^+\rangle_{CD}$, vu que Bob a honnêtement préparé ce dernier, il gagne le pile ou face et sa mesure généralisée ne peut être détectée. Ensuite, Alice révèle la valeur du bit b qu'elle a mis en gage, mais cette information est inutile pour Bob. A ce stade, Bob effectue une autre mesure généralisée : $\{L_0^0, L_1^0, L_2^0 | L_0^{0\dagger}L_0^0 + L_1^{0\dagger}L_1^0 + L_2^{0\dagger}L_2^0 = I_{BD}\}$ sur l'état de BD qui dépend du résultat,M_0,trouvé dans la première mesure, et c'est cette deuxième mesure qui décidera de son action ultérieure. Les opérateurs L_i^0 sont définis comme :

$$\begin{aligned} L_0^0 &= |\psi_0\rangle_{BB}\langle\psi_0| \otimes |0\rangle_{DD}\langle 0| \\ L_1^0 &= \left(\frac{1}{\sqrt{2}}|\psi_0\rangle_{BB}\langle\psi_0| + |\psi_1\rangle_{BB}\langle\psi_1|\right) \otimes |1\rangle_{DD}\langle 1| \\ L_2^0 &= \frac{1}{\sqrt{2}}|\psi_0\rangle_{BB}\langle\psi_0| \otimes |1\rangle_{DD}\langle 1| + |\psi_1\rangle_{BB}\langle\psi_1| \otimes |0\rangle_{DD}\langle 0| \end{aligned}$$

Si Bob mesure $L_0^0(L_1^0)$, il déclare 0(1) comme résultat de la mesure du qubit D. Supposons que Bob mesure L_1^0, il perd alors le pile ou face et doit retourner le qubit B

à Alice. On vérifie aisément que dans ce cas, l'état de BC est $|\chi\rangle_B |1\rangle_C$, donc Bob récupère l'état envoyé par Alice et elle ne peut détecter la tricherie de Bob : Puisque Bob a partagé honnêtement l'état $|\phi^+\rangle_{CD}$ avec Alice, l'état du système BCD après la deuxième mesure de Bob est

$$\frac{L_1^0 \otimes I_C |\Psi\rangle_B |\phi^+\rangle_{CD}}{|L_1^0 \otimes I_C |\Psi\rangle_B |\phi^+\rangle_{CD}|} = |\chi\rangle_B |1\rangle_C |1\rangle_D$$

Cependant, si Bob mesure L_0^0 et déclare 0 comme résultat, l'état du système BCD devient :

$$\frac{L_0^0 \otimes I_C |\Psi\rangle_B |\phi^+\rangle_{CD}}{|L_0^0 \otimes I_C |\Psi\rangle_B |\phi^+\rangle_{CD}|} = |\psi_0\rangle_B |0\rangle_C |0\rangle_D$$

Cette fois aussi, Alice ne peut détecter la tricherie de Bob, car sa mesure de l'état de C donnera 0, et puisque Bob gagne le pile ou face, il n'a pas à retourner l'état de B. Dans le dernier cas, c'est à dire celui où Bob mesure L_2^0, l'état du système après la mesure est :

$$|\Phi\rangle_{BCD} = \frac{L_2^0 \otimes I_C |\Psi\rangle_B |\phi^+\rangle_{CD}}{|L_2^0 \otimes I_C |\Psi\rangle_B |\phi^+\rangle_{CD}|} = \alpha |\psi_0\rangle_B |1\rangle_C |1\rangle_D + \beta |\psi_1\rangle_B |0\rangle_C |0\rangle_D$$

Maintenant, Bob demande à Alice de lui retourner le qubit C pour le vérifier, et une fois le qubit C en sa possession, il lui applique la transformation unitaire U_{BCD}^0, telle que :

$$\begin{aligned} U_{BCD}^0 |\psi_0\rangle_B |1\rangle_C |1\rangle_D &= |\psi_0\rangle_B |0\rangle_C |0\rangle_D \\ U_{BCD}^0 |\psi_1\rangle_B |0\rangle_C |0\rangle_D &= |\psi_1\rangle_B |0\rangle_C |0\rangle_D \end{aligned}$$

L'état du système BCD devient :

$$U_{BCD}^0 |\Phi\rangle_{BCD} = \alpha |\psi_0\rangle_B |0\rangle_C |0\rangle_D + \beta |\psi_1\rangle_B |0\rangle_C |0\rangle_D = |\chi\rangle_B |0\rangle_C |0\rangle_D$$

et Bob récupère l'état $|\chi\rangle_B$ qu'il retourne à Alice et échappe à la détection.

Dans le cas où Bob mesure M_1 au lieu de M_0, il suit la même stratégie décrite plus haut, en appliquant la mesure généralisée $\{L_i^1, i = 1, 2, 3\}$ à la place de $\{L_i^0, i = 1, 2, 3\}$

et la transformation unitaire U^1_{BCD} au lieu de U^0_{BCD} telle que :

$$\begin{aligned} L^1_0 &= |\psi_1\rangle_{BB}\langle\psi_1| \otimes |0\rangle_{DD}\langle 0| \\ L^1_1 &= \left(|\psi_0\rangle_{BB}\langle\psi_0| + \frac{1}{\sqrt{2}}|\psi_0\rangle_{BB}\langle\psi_0|\right) \otimes |1\rangle_{DD}\langle 1| \\ L^1_2 &= |\psi_0\rangle_{BB}\langle\psi_0| \otimes |0\rangle_{DD}\langle 0| + \frac{1}{\sqrt{2}}|\psi_1\rangle_{BB}\langle\psi_1| \otimes |1\rangle_{DD}\langle 1| \end{aligned}$$

$$\begin{aligned} U^1_{BCD}|\psi_0\rangle_B|0\rangle_C|0\rangle_D &= |\psi_0\rangle_B|0\rangle_C|0\rangle_D \\ U^1_{BCD}|\psi_1\rangle_B|1\rangle_C|1\rangle_D &= |\psi_1\rangle_B|0\rangle_C|0\rangle_D \end{aligned}$$

On voit bien qu'on peut obtenir L^1_i à partir de L^0_i et U^1_{BCD} à partir de U^0_{BCD} en permutant $|\psi_0\rangle_B$ et $|\psi_1\rangle_B$.

CHAPITRE IV

MISE EN GAGE RELATIVISTE

La grande question maintenant est, est-ce que le théorème de l'impossibilité de Mayers-Lo-Chau est vraiment la fin de l'espoir qu'un protocole de mise en gage inconditionnellement sécuritaire puisse voir le jour? La réponse est heureusement, non! Une autre théorie physique vient encore sauver cette primitive comme la mécanique quantique l'a déjà fait pour le protocole de distribution de clefs. Kent a pu concevoir un protocole de mise en gage classique relativiste inconditionnellement sécuritaire [43, 44] et pratiquement réalisable [44] dont la sécurité repose sur le fait qu'il est impossible de signaler avec une vitesse supérieure à celle de la lumière. Ce protocole a été prouvé sécuritaire contre toute attaque classique (donc, le premier de son genre avec cette caractéristique) et il échappe aux attaques quantiques de Mayers, Chau et Lo, auquelles les protocoles non relativistes sont vulnérables. Il est aussi conjecturé sécuritaire devant toutes attaques quantiques.

Note 5 *Le protocole de distribution de clefs quantiques* [9], *contrairement à celui de la mise en gage relativiste de Kent, est démontré sécuritaire contre tous les types d'attaques* [5, 33, 72].

Avant d'entrer dans les détails du protocole de Kent, donnons tout d'abord quelques définitions utiles à la description du protocole.

Définition 18 *En relativité, un événement est une « chose » qui a lieu à un endroit*

donné dans l'espace et à un moment donné dans le temps. On peut désigner cet événement à l'aide de coordonnées spatio-temporelles (x, y, z, t) *relatives à un référentiel* R *dont l'origine* O *est à la position* $(0, 0, 0, 0)$.

Note 6 *On peut voir un message envoyé ou reçu par un observateur* A *à l'instant* t *dans la position* $M(x, y, z)$ *comme étant un événement de coordonnées spatio-temporelles* (x, y, z, t).

La relativité nous apprend qu'aucun effet, aucun signal, ne peut se propager plus vite que la lumière. Donc un événement $A(x_1, y_1, z_1, t_1)$ peut être la cause de l'événement $B(x_2, y_2, z_2, t_2)$ si la lumière qui part de A à l'instant t_1 arrive en B avant l'instant t_2; si elle arrive après t_2, B est nécessairement indépendant de A, alors, il ne peut être influencé par A; et si elle arrive à l'instant t_2, A et B sont simultanés pour un observateur placé en B, donc B ne peut pas résulter de A. Un résultat direct de cette description, est que si les deux événements $A(x_1, y_1, z_1, t_1)$ et $B(x_2, y_2, z_2, t_2)$ sont tels que :

$$\Delta = c^2(t_2 - t_1)^2 - (x_2 - x_1)^2 - (y_2 - y_1)^2 - (z_2 - z_1)^2 < 0 \qquad (4.1)$$

alors, ils sont nécessairement indépendants. La condition d'indépendance entre les deux événements A et B s'écrit donc : $\Delta < 0$.

Définition 19 *Deux événements* $A(x_1, y_1, z_1, t_1)$ *et* $B(x_2, y_2, z_2, t_2)$ *sont dits séparés par un intervalle du genre-espace si, et seulement si, leurs coordonnes spatio-temporelles vérifient l'équation (4.1).*

Définition 20 *Une région spatio-temporelle* $P(x_1, y_1, z_1, \delta, [t, t'])$ *est un ensemble d'événements* $\{(x, y, z, \tau)\}$ *tels que :*

$$(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2 \leq \delta^2 \text{ et } \tau \in [t, t']$$

Il s'agit donc d'événements se déroulant dans une région sphérique de rayon δ *et de centre* (x_1, y_1, z_1) *dans l'espace, à un instant quelconque entre* t *et* t'.

Définition 21 *Deux régions spatio-temporelles*

$$P(x_1, y_1, z_1, \delta, [t, t^{'}]) \text{ et } Q(x_2, y_2, z_2, \delta, [s, s^{'}])$$

sont dites séparées par un intervalle du genre-espace si et seulement si, pour tous événements $(x, y, z, \tau) \in P(x_1, y_1, z_1, \delta, [t, t^{'}])$ *et* $(\overline{x}, \overline{y}, \overline{z}, \varsigma) \in Q(x_2, y_2, z_2, \delta, [s, s^{'}])$ *alors :*

$$c^2(\varsigma - \tau)^2 - (\overline{x} - x)^2 - (\overline{y} - y)^2 - (\overline{z} - z)^2 < 0$$

C-à-d., les événements de la région P *sont indépendants de ceux de la région* Q*. Par conséquent, aucun événement dans la région* P *ne peut être la cause d'un autre de la région* Q*, et vise versa .*

Supposons qu'Alice et Bob ont le contrôle sur les laboratoires séparés A_1, A_2 et B_1, B_2 respectivement (ce contrôle se fait, par exemple, en plaçant des agents A_1, A_2 et B_1, B_2 au niveau des laboratoires A_1, A_2 et B_1, B_2 repectivement). On peut arranger les choses de sorte que si A_1 reçoit et répond à un message de B_1, et A_2 reçoit et répond à un message de B_2, alors Bob peut s'assurer que la réponse de A_1 est indépendante du message de B_2 et la réponse de A_2 est indépendante du message de B_1. Pour ce faire, ils doivent, tout d'abord, se mettre d'accord sur un référentiel dans l'espace-temps, soit R, pour reporter tous les événements. Puis, il suffit que les messages (donc, les événements) entre A_1 et B_1 et ceux entre A_2 et B_2 apartiennent, respectivement, à deux régions spatio-temporelles séparées par un intervalle du genre-espace, $P(x_1, y_1, z_1, \delta, [t_1, t_2])$ et $Q(x_2, y_2, z_2, \delta, [s_1, s_2])$, par rapport à R. Si cette contrainte est respectée, on est sûr que les messages entre A_1 et B_1, complétés entre t_1 et t_2, et ceux entre A_2 et B_2, complétés entre s_1 et s_2, ne peuvent influencer les uns les autres, dans un contexte où la plus grande vitesse possible est celle de la lumière.

Remarque 7 *Il aurait été possible pour nous de réaliser cette indépendance par des contraintes plus sévères dans le temps, et qui rassurent plus les participants, en exigeant la simultanéité :* $[t_1, t_2] \equiv [s_1, s_2]$*; mais il sera important pour le protocole de Kent d'être plus flexible.*

Un but purement pratique nous incite à choisir des régions P et Q largement séparées dans l'espace, telles que :

$$(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2 >> \delta^2$$

car cela permettra de garantir l'indépendance des messages pour des durées plus longues. Pour voir cela concrètement, analysons la relation (4.1). Allégeons tout d'abord l'écriture en ne considérant qu'une seule coordonnée spatiale, x, par exemple. Dans ce cas, la relation (4.1) devient :

$$\Delta = c^2(t_2 - t_1)^2 - (x_2 - x_1)^2 < 0$$

D'où

$$|t_2 - t_1| < \frac{|x_2 - x_1|}{c}$$

Suposons que $x_2 \approx x_1$. Pour avoir $\Delta < 0$ dans ce cas, il faut que ct_2 soit plus proche de ct_1 que l'est x_2 de x_1. Et donc, t_2 soit plus proche de t_1 que l'est $\frac{x_2}{c}$ de $\frac{x_1}{c}$.

4.1 Une mise en gage classique temporairement sécuritaire

Une idée permettant de construire un protocole de mise en gage classique sécuritaire (mais pas inconditionnellement sécuritaire) a été proposée par Ben-Or, Goldwasser, Kilian, et Wigderson [6]. La version relativiste (donc, inconditionnellement sécuritaire) de ce protocole est construite par Brassard, Crépeau, Mayers et Salvail, mais cette mise en gage n'était que temporairement sécuritaire [15].

Note 7 *Au long de ce chapitre, les lettres majuscules P et Q, ou plus généralement P_i et Q_i, désigneront des régions spatio-temporelles séparées par des intervalles du genre-espace. Aussi, chaque deux régions indexées Q_i, P_{i+1}, sont séparées par des intervalles du genre-espace.*

Soient les deux régions $P(x_0, y_0, z_0, \delta, [t_1, t_2])$ et $Q(x_1, y_1, z_1, \delta, [s_1, s_2])$ strictement ordonnées dans le temps : $t_1 < t_2 < s_1 < s_2$ par rapport à un référentiel R,

conventionnel entre Alice et Bob. Supposons que A_1 et B_1 échangent des messages dans P, et A_2, et B_2 le font dans Q. Dans ce cas, le protocole de [15] se déroule comme suit :

Protocole 5

1. Alice et Bob se mettent d'accord sur un grand nombre $N = 2^n$: tout le calcul se fera modulo N.
2. A_1 et A_2 fixent un nombre aléatoire m avant le protocole.
3. B_1 envoie à A_1 deux nombres différents n_0 et n_1 dans P.
4. Pour s'engager sur le bit b, A_1 lui retourne le nombre $z = m + n_b$ dans P.
5. A_2 dévoile, s'il le désire, son bit en révélant dans Q un nombre m' à B_2.
6. B_2 envoie m' à B_1. B_1 vérifie si $z - m' \in \{n_0, n_1\}$.

Ce protocole est camouflant : Puisque $z = m + n_b = \overline{m} + n_{\overline{b}}$ où $\overline{m} = m + n_b - n_{\overline{b}}$, et puisque B_1 ignore m, il ne peut pas décider s'il a eu z suite à l'addition de m à n_b, ou de $\overline{m}$ à $n_{\overline{b}}$. Et, car il y a exactement deux nombres, m et $\overline{m}$, donnant z, B_1 n'obtient aucune information sur le bit. Il est aussi temporairement liant, car A_2 ignore n_b dans Q ; supposons que A_2 veut convaincre Bob que A_1 a choisi un bit différent de bit qu'il a réellememt choisi, dans ce cas elle doit deviner une valeur $\overline{m}$ parmi $N - 1$ valeurs, et donc, la probabilité qu'elle ne sera pas détectée est égale à $\frac{1}{N-1}$ (≈ 0 pour un grand nombre N).

Bien que ce protocole soit sécuritaire, il ne peut être considéré comme un protocole réel de mise en gage, car il lui manque une très importante caractéristique : le moment de la révélation ne devrait pae être déterminé d'avance.

4.2 Une mise en gage classique inconditionnelement sécuritaire non pratique

Avant d'énoncer une variante du protocole 5 de la page 100, qui maintient l'engagement continuellement dans le temps, définissons les ingrédients de cette dernière.

D'un point de vue formel on a les contraintes suivantes

1. Alice et Bob se mettent d'accord sur un référentiel spatio-temporel R et sur des régions strictement ordonnées dans le temps par rapport à ce référentiel :

$$P_1(x_1, y_1, z_1, \delta, [t_1, t_2]), Q_1(x_2, y_2, z_2, \delta, [s_1, s_2]), ...$$
$$.., P_r(x_1, y_1, z_1, \delta, [t_i, t_{i+1}]), Q_r(x_2, y_2, z_2, \delta, [s_i, s_{i+1}]), ..$$

telles que :

$$t_1 < t_2 < s_1 < s_2 < t_3 < t_4 < s_3 < s_4 < ....t_i < t_{i+1} < s_i < s_{i+1} < ...$$

et

$$\Delta t = t_2 - t_1 = t_4 - t_3 = .. = t_{i+1} - t_i = .. = s_2 - s_1 = s_4 - s_3 = .. = s_{i+1} - s_i = ..$$

2. Prière de relire la note 7

Note 8 *Formuler les contraintes ainsi n'oblige pas les agents A_j et B_j de connaître précisément la position relative de l'un par rapport à l'autre. La position exacte des agents n'est donc pas un facteur de sécurité dans le protocole. Par contre cette formulation assure la présence des agents dans un rayon de sphère δ s'ils suivent le protocole car sinon l'éloignement abusif sera détecté.*

3. Puisque dans ce modèle toutes les régions spatio-temporelle $P_i(Q_i)$ sont situées dans la même région spaciale, alors, Alice et Bob peuvent être représentés chacun par un seul agent, dans toutes ces régions $P_i(Q_i)$, désignons-les par $A_1(A_2)$ et $B_1(B_2)$ respectivement.

4. Alice et Bob se mettent d'accord sur un grand nombre $N = 2^n$: tout le calcul se fera modulo N.

5. Le protocole nécessite que A_1 et A_2 partagent préalablement (avant leur séparation) une chaîne (donc, ordonnée) infinie de bits aléatoires, organisée comme suit: $(m_1, m_2, ..)$ telle que $m_i < N = 2^n$, car ils ne savent pas d'avance la durée du protocole (caractéristique primordiale d'un protocole de mise en gage).

6. Une condition cruciale pour la sécurité du protocole est la distance spatiale entre les laboratoires B_1 et B_2, car elle est le seul garant de l'indépendance des messages d'Alice. Bob doit donc avoir la certitude qu'il l'a estimée correctement; car ceci empêchera A_i de satisfaire le synchronisme avec B_i et d'influencer les choix de A_{3-i} en même temps. Autrement dit, c'est cette contrainte qui rend réalisabl une implantation de régions comme on l'a fait dans le point 1. On peut rassurer Bob en fusionnant les deux laboratoires B_1 et B_2 sous un seul large laboratoire B. Étendre cette idée aux laboratoires d'Alice évitera à ses agents de devoir partager préalablement une chaîne infinie de bits aléatoires ou de bâtir un canal sécurisé entre les deux laboratoires.

7. Un *tour* est défini comme étant l'ensemble des messages échangés à l'intérieur d'une région, d'où on peut le distinguer par le même nom de la région où il se déroule.

   Remarque 8 *Puisque le premier tour se déroule dans P_1, le deuxième dans Q_1, le troisième dans P_2, le quatrième dans Q_2... On conclut, alors, que le $(2i-1)^{ième}$ tour se déroule dans P_i et le $(2i)^{ième}$ tour dans Q_i. Donc, connaître le numéro du tour est équivalent à connaître la région spatio-temporelle où il se déroule. Ceux-ci seront utilisés de façon interchangeable.*

Une variante du protocole 5 permettant la prolongation (la continuité ou le maintien) dans le temps de la mise en gage a été proposée par Kent [43]. Elle se fait comme suit :

Protocole 6

1. Dans le tour P_1 (donc, le premier tour d'après notre convention dans la remarque 7), B_1 envoie à A_1 le couple de nombres (n_{01}, n_{11}) tel que $n_{01} \neq n_{11}$.Une fois reçu, si A_1 veut s'engager sur le bit b, il lui retourne le nombre $z_1 = m_1 + n_{b1}$; et la phase d'engagement termine ainsi. Tous les tours après, vont sevir à prolonger cet engagement dans le temps jusqu'à l'instant où les participants décident d'ouvrir le gage.

2. Dans le tour Q_1, B_2 envoie n couples $(n_{0,i}, n_{1,i})$, tels que $n_{0,i} \neq n_{1,i}, i \in [2..n+1]$ ($[2..n+1]$ est l'ensemble des nombres i de $\mathbb{N}$ tels que $2 \leq i \leq n+1$), à A_2 pour qu'elle s'engage sur chacun des bits constituant la forme binaire de m_1 : $m_1 = a_{n+1}a_{n-1}....a_2$ ($m_i < N = 2^n$); une fois reçu, A_2 lui retournera les n nombres $z_i = m_i + n_{a_i,i}$, tels que $i \in [2..n+1]$, pour s'engager sur chaque bit a_i d'ordre i dans l'expression binaire de m_1. Dans le tour P_2, B_2 envoie n^2 couples $(n_{0,i}, n_{1,i})$, tels que $n_{0,i} \neq n_{1,i}, i \in [n+2..n^2+n+1]$, à A_2 pour qu'elle s'engage sur chacun des bits constituant la forme binaire de chaque nombre m_k tels que $k \in [2..n+1]$ utilisé dans le tour Q_1 : $m_k = a_{nk+1}....a_{n(k-1)+2}$; une fois reçus, A_2 lui retournera les n^2 nombres $z_i = m_i + n_{a_i,i}$, tels que $i \in [n+2..n^2+n+1]$. Donc, dans le tour P_r, l'agent B_1 envoie n^{2r-2} couples $(n_{0,i}, n_{1,i})$, tels que $n_{0,i} \neq n_{1,i}, i \in [\frac{n^{2r-2}+n-2}{n-1}..\frac{n^{2r-1}-1}{n-1}]$, à A_1 qui va les utiliser pour s'engager sur chacun des bits constituant la forme binaire de chaque nombre m_k, tel que $k \in [\frac{n^{2r-3}+n-2}{n-1}..\frac{n^{2r-2}-1}{n-1}]$, utilisé dans le tour Q_{r-1}: $m_k = a_{nk+1}....a_{n(k-1)+2}$; une fois reçus, A_1 lui retournera les n^{2r-2} nombres $z_i = m_i + n_{a_i,i}$ tels que $i \in [\frac{n^{2r-2}+n-2}{n-1}..\frac{n^{2r-1}-1}{n-1}]$. Dans le tour Q_r, l'agent B_2 envoie n^{2r-1} couples $(n_{0,i}, n_{1,i})$, tels que $n_{0,i} \neq n_{1,i}, i \in [\frac{n^{2r-1}+n-2}{n-1}..\frac{n^{2r}-1}{n-1}]$, à A_2 qui va les utiliser pour s'engager sur chacun des bits constituant la forme binaire de chaque nombre m_k, tel que $k \in [\frac{n^{2r-2}+n-2}{n-1}..\frac{n^{2r-1}-1}{n-1}]$, utilisé dans le tour P_r: $m_k = a_{nk+1}....a_{n(k-1)+2}$; une fois reçus, A_2 lui retournera les n^{2r-1} nombres $z_i = m_i + n_{a_i,i}$, tels que $i \in [\frac{n^{2r-1}+n-2}{n-1}..\frac{n^{2r}-1}{n-1}]$.

3. Maintenant, si l'agent A_1 décide de révéler le bit dans le tour P_r, il doit annoncer

à B_1 l'ensemble des nombres m_k, tels que $k \in [\frac{n^{2r-3}+n-2}{n-1}..\frac{n^{2r-2}-1}{n-1}]$, utilisés par A_2 dans le tour Q_{r-1}. Et, si c'est l'agent A_2 qui va révéler dans le tour Q_r, il annonce à B_2 l'ensemble des nombres m_k, tels que $k \in [\frac{n^{2r-2}+n-2}{n-1}..\frac{n^{2r-1}-1}{n-1}]$, utilisés par A_1 dans le tour P_r. La procédure de révélation ne change pas et reste valide si les deux agents révèlent le bit en même temps. Si A_1 veut révéler dans le tour P_1 (donc, dans la région P_1), il n'a qu'à annoncer les nombres m_k, tels que $k \in [2..n+1]$, qui vont être utilisés par l'agent A_2 dans le tour Q_1. Bob peut vérifier l'honnêteté d'Alice en rassemblant toutes les donnnées chez un seul agent qui vérifiera si ces dernières peuvent correspondre à un engagement sur l'un des bits, 0 ou 1. Si c'est le cas, il accepte.

Bien que ce protocole prouve la possibilité théorique d'une mise en gage inconditionnellement sûre, il ne peut être réellement implanté. Une des raisons est le taux de communication qui croit exponentiellement avec la durée du protocole; d'aprés l'analyse précédente, dans chaque tour P_r qui correspond, d'après la remarque 7, au $(2r-1)^{\text{ième}}$ tour, si les deux agents désirent continuer le maintien du gage, ils doivent s'échanger $3n^{2r-2}$ nombres ($2n^{2r-2}$ couples $(n_{0,i}, n_{1,i})$ et n^{2r-2} nombres m_i) dans un intervalle de temps Δt. Si on pose $\lambda = (2r-1)$, ils doivent, alors, s'échanger dans le $\lambda^{\text{ème}}$ tour, $3n^{\lambda-1}$ nombres (donc, $3n^{\lambda}$ bits)dans un intervalle de temps Δt (à remarquer que cet intervalle est constant et ne dépend pas du tour). Donc, le taux de communication nécessaire pour la continuité du protocole croit exponentiellement avec le temps. Aussi, les agents A_1 et A_2 doivent préalablement partager une liste de nombres aléatoires dont la longueur croît exponentiellement avec la durée prévue du protocole : l'analyse précédente a montré que pour maintenir le gage jusqu'au tour P_r, donc le $\lambda^{\text{ième}}$ tour tel que $\lambda = (2r-1)$, les agents A_1 et A_2 utilisent au total un nombre de m_i égal à :

$$n^{2r-2} + n^{2r-3} + ... + n + 1 = \frac{n^{2r-1}-1}{n-1} = \frac{n^{\lambda}-1}{n-1}$$

Si au lieu de partager préalablement cette information, ils la génèrent aléatoirement et partagent secrètement cette liste durant le protocole (c-à-d., au fur et à mesure d'avancement du protocole), il doivent, alors, utiliser un taux de communication secrète

qui croit exponentiellement avec le temps, comme ils ont besoin de produire des nombres aléatoires avec un taux croissant exponentiellement aussi. Pour les agents de Bob, ils doivent, eux aussi, produire des couples de nombres aléatoires avec un taux croissant exponentiellement, par contre, ils n'ont pas besoin de les partager.

4.3 Une mise en gage classique inconditionnelement sécuritaire pratique

Dans un article subséquent, Kent [44] a amélioré le protocole précédent en utilisant une méthode due à Rudich [67]. Cette méthode permet à Alice (si elle est honnête) de convaincre Bob que deux gages sont du même bit sans qu'elle ait besoin de révéler le bit.

4.3.1 Technique de Rudich pour la mise en gage

Supposons qu'Alice et Bob disposent d'une boîte noire permettant à Alice de s'engager sur le bit de son choix d'une manière que Bob ne puisse avoir aucune information sur ce bit, et qu'elle lui permete aussi de révéler ce bit quand elle le désire. L'existence d'une telle boîte noire permet à Alice de s'engager sur deux bits b_1 et b_2 et de convaincre Bob (si elle est honnête) que ces deux bits sont les mêmes sans avoir besoin de les révéler. Pour ce faire, elle doit tout d'abord se mettre d'accord avec lui sur un grand nombre M, qui va servir comme paramètre de securité. Après, elle va s'engager via la boîte noire sur $2M$ bits b_1^{ij} tels que $i \in \{1,2\}$ et $j \in [1..M]$ tels que les bits b_1^{1j} sont choisis d'une manière aléatoire et indépendamment l'un par rapport à l'autre et les b_1^{2j} sont choisis de manière à satisfaire la contrainte $b_1 = b_1^{1j} \oplus b_1^{2j}$. De la même manière, elle s'engagera sur $4M$ bits, choisis indépendamment des premiers, b_2^{ij} tels que $i \in \{1,2\}$ et $j \in [1..2M]$ et telle que les bits b_2^{1j} sont choisis d'une manière aléatoire et indépendamment l'un par rapport à l'autre et les b_2^{2j} sont choisis de manière à satisfaire la contrainte $b_2 = b_2^{1j} \oplus b_2^{2j}$.

Bob vérifie l'honnêteté d'Alice comme suit. Dans une première étape, il choisit

pour chaque couple (b_1^{1j}, b_1^{2j}) tel que $j \in [1..M]$, d'une manière aléatiore, un autre couple $(b_2^{1f(j)}, b_2^{2f(j)})$ tels que $f(j) \in [1..2M]$ et demande à Alice pour chaque $j \in [1..M]$ si les deux couple sont égaux : $\left(b_1^{1j} = b_2^{1f(j)}\right)$ et $\left(b_1^{2j} = b_2^{2f(j)}\right)$, ou opposés : $\left(b_1^{1j} = \neg b_2^{1f(j)}\right)$ et $\left(b_1^{2j} = \neg b_2^{2f(j)}\right)$, car c'est seulement ces deux cas qui sont possibles si Alice s'est réellement engagée sur le même bit, $b_1 = b_2$:

$$\begin{aligned} & \left[b_1^{1j} \oplus b_1^{2j} = b_2^{1f(j)} \oplus b_2^{2f(j)}\right] \\ \Longleftrightarrow \quad & \left[\left(b_1^{1j} = b_2^{1f(j)}\right) \wedge \left(b_1^{2j} = b_2^{2f(j)}\right)\right] \vee \left[\left(b_1^{1j} = \neg b_2^{1f(j)}\right) \wedge \left(b_1^{2j} = \neg b_2^{2f(j)}\right)\right] \end{aligned} \tag{4.2}$$

Quand Bob reçoit les réponses d'Alice, il lui demande, dans une deuxième étape, de révéler pour chaque paire $\left((b_1^{1j}, b_1^{2j}), (b_2^{1f(j)}, b_2^{2f(j)})\right)$ tel que $j \in [1..M]$, l'un des couples $\left(b_1^{1j}, b_2^{1f(j)}\right)$ ou $\left(b_1^{2j}, b_2^{2f(j)}\right)$; ce choix, il le fait aléatoirement. Alice révèle les bits demandés et Bob vérifie l'exactitude de ces réponses et leurs cohérence avec ce qu'elle a prétendu concernant l'égalité des couples dans la première étape.

Si Alice passe tous les tests de Bob, il accepte qu'elle s'est réellement engagée sur deux bits égaux : $b_1 = b_2$, et par conséquent, les M couples restant (b_2^{1k}, b_2^{2k}) tels que $k \notin \{f(j) | j \in [1, M]\}$ et dont aucun bit n'a été révélé, sont presque tous, sauf avec une probabilité exponontiellement faible dans le nombre d' "d'erreurs", tels que $b = b_2^{1k} \oplus b_2^{2k}$.

Analysons, maintenant, la sécurité de la technique de Rudich pour chaque participant.

1. Même si Bob est malhonnête, c'est clair qu'il ne peut avoir aucune information sur le bit d'Alice.

2. Pour commencer l'analyse de la sécurité du protocole contre les tentatives de tricherie d'Alice donnons quelques définitions qui faciliteront cette dernière.

Définition 22 *Dans le premier engagement, Alice est dite effectivement γ-engagée sur le bit b_1 par M couples, si au moins $(1-\gamma)M$ couples de l'ensemble des M couples du premier engagement (b_1^{1j}, b_1^{2j}) où $j \in [1, M]$ sont tels que $b_1^{1j} \oplus b_1^{2j} = b_1$ et $0 < \gamma < \frac{1}{2}$; donc, au plus γM couples sont tels que $b_1^{1j} \oplus b_1^{2j} = \overline{b}_1$.*

Note 9 *Le choix de $\gamma < \frac{1}{2}$ empêche Alice d'être effectivement γ-engagé sur b et $\overline{b}$ en même temps.*

Définition 23 *Dans le deuxième engagement, Alice est dite effectivement γ-engagée sur le bit b_2 par $2M$ couples, si au moins $(2-\gamma)M$ couples de l'ensemble des $2M$ couples du deuxième engagement (b_2^{1j}, b_2^{2j}) tels que $j \in [1, 2M]$ sont tels que $b_2^{1j} \oplus b_2^{2j} = b_2$, où $0 < \gamma < \frac{1}{2}$; donc, au plus γM couples sont tels que $b_2^{1j} \oplus b_2^{2j} = \overline{b}_2$.*

Définition 24 *Alice est dite effectivement γ-engagée sur le bit b dans le protocole si elle est effectivement γ-engagée sur le bit $b_1 = b$ suivant la première définition et effectivement γ-engagée sur le bit $b_2 = b$ suivant la deuxième définition.*

Suite à ces définitions, si Alice est effectivement γ-engagée sur le bit b_1 par M couples et effectivement γ-engagée sur le bit b_2 par $2M$ couples, après les tests, elle restera toujours effectivement γ-engagée sur le bit b_2 par M couples suivant la première définition, et cela sans prendre en compte les résultats des tests en effet, dans le pire des cas, tous les M couples du deuxième engagement choisis par Bob auront la bonne forme :$b_2^{1j} \oplus b_2^{2j} = b_2$, donc, il restera au moins $(2-\gamma)M - M = (1-\gamma)M$ couples dont le ou exclusif est égal à b_2 en plus des autres γM couples dont le ou exclusif est égal à $\overline{b}_2$.

Lemme 9 *Soit $\epsilon(M)$ la probabilité maximale qu'Alice passe les tests de Bob si elle n'est pas effectivement γ-engagée dans le protocole (la maximisation est faite sur toutes les configurations possibles des bits satisfaisant la contrainte de ne pas être effectivement γ-engagée dans le protocole), dans ce cas : $\epsilon(M) \approx \exp(-CM)$ lorsque M est très grand, où C est une constante positive.*

Preuve Supposons que le nombre de couples de bits du premier engagement dont le ou exclusif est $b_1 = b$ est $(1-\gamma_1)M$, et supposons que le nombre de couples de bits du deuxième engagement dont le ou exclusif est $b_2 = b$ est $(2-2\gamma_2)M$.

Alice est effectivement γ-engagée sur le bit $b_1 = b$ dans le premier engagement, si la proposition P_1 :

$$P_1 \equiv (1 - \gamma_1) M \geq (1 - \gamma) M$$

est vraie. On peut écrire P_1 aussi :

$$P_1 \equiv \gamma_1 \leq \gamma$$

Si P_1 n'est pas vraie et si la proposition P_2 :

$$P_2 \equiv \gamma_1 M \geq (1 - \gamma) M$$

est vraie, alors Alice est effectivement γ-engagée sur le bit $b_1 = \overline{b}$ dans le premier engagement . On peut écrire P_2 aussi :

$$P_2 \equiv (1 - \gamma_1) \leq \gamma$$

Maintenant, Alice est effectivement γ-engagée sur le bit $b_2 = b$ dans le deuxième engagement si la proposition P_3 :

$$P_3 \equiv (2 - 2\gamma_2) M \geq (2 - \gamma) M$$

est vraie. On peut écrire P_3 aussi

$$P_3 \equiv 2\gamma_2 \leq \gamma$$

Si P_3 n'est pas vraie et si la proposition P_4 :

$$P_4 \equiv 2\gamma_2 M \geq (2 - \gamma) M$$

est vraie, alors Alice est effectivement γ-engagée sur le bit $b_2 = \overline{b}$ dans le deuxième engagement. On peut écrire P_4 aussi :

$$P_4 \equiv (2 - 2\gamma_2) \leq \gamma$$

Donc, Alice est effectivement γ-engagée dans le protocole (pour une certaine valeur du bit), si la proposition P :

$$P \equiv (P_1 \wedge P_3) \vee (P_2 \wedge P_4)$$

est vraie. D'où, si Alice n'est pas effectivement γ-engagée dans le protocole alors P est fausse, donc, si Alice n'est pas effectivement γ-engagée dans le protocole,

$$\neg P \equiv (\neg P_1 \vee \neg P_3) \wedge (\neg P_2 \vee \neg P_4)$$

est vraie. C-à-d., si Alice n'est pas effectivement γ-engagée dans le protocole on a :

$$[(\gamma_1 > \gamma) \vee (2\gamma_2 > \gamma)] \wedge [((1-\gamma_1) > \gamma) \vee ((2-2\gamma_2) > \gamma)]$$

Mais on a aussi :

$$(\gamma_1 > \gamma) \vee (2\gamma_2 > \gamma) \Longleftrightarrow \max(\gamma_1, 2\gamma_2) > \gamma$$

$$((1-\gamma_1) > \gamma) \vee ((2-2\gamma_2) > \gamma) \Longleftrightarrow \max(1-\gamma_1, 2-2\gamma_2) > \gamma$$

Avec ce dernier résultat, on peut conclure que si Alice n'est pas effectivement γ-engagée dans le protocole, par le choix des paramètres γ_1 et γ_2 qu'elle a fait, alors on a :

$$\max(\gamma_1, 2\gamma_2) > \gamma \text{ et } \max(1-\gamma_1, 2-2\gamma_2) > \gamma \tag{4.3}$$

Puisque, dans le deuxième engagement, le nombre de couples dont le ou exclusif est égal à b est $(2-2\gamma_2)\,M$, alors, la probabilité que Bob choisisse un de ces couples pour le test est égale à $\frac{(2-2\gamma_2)M}{2M} = 1-\gamma_2$; et puisque, dans le deuxième engagement, le nombre de couples dont le ou exclusif est égal à $\overline{b}$ est $2\gamma_2 M$, alors, la probabilité que Bob choisisse un de ces couples pour le test est égale à $\frac{2\gamma_2 M}{2M} = \gamma_2$. Étant donné que tous les couples du premier engagement subiront le test de Bob, on peut estimer (pondérer) le nombre de paires de couples possibles comme suit : $(1-\gamma_1)(1-\gamma_2)\,M$ paires de couples où ils compareront des couples de bits des deux engagements dont le ou exclusif est le même et égal à b et donc Alice passera tous les tests de Bob; $(1-\gamma_1)\,\gamma_2 M$ paires de couples où ils compareront des couples de bits des deux engagements dont le ou exclusif est égale b dans le premier engagement et égal à $\overline{b}$ dans le deuxième engagement; $\gamma_1\,(1-\gamma_2)\,M$ paires de couples où ils compareront des couples de bits des deux engagements dont le ou exclusif est égale $\overline{b}$ dans le premier engagement et égale à b dans le deuxième engagement; $\gamma_1\gamma_2 M$ paires de couples où ils compareront des couples de bits des deux engagements dont le ou exclusif est le même et égale à $\overline{b}$ et donc Alice passera tous

les tests de Bob. Une paire de couples dont le ou exclusif est différent a certainement une des formes suivantes : $((a,b),(\overline{a},b))$ ou $((a,b),(a,\overline{b}))$. On voit bien que dans le cas de la première (deuxième) paire de couples $((a,b),(\overline{a},b))\big(((a,b),(a,\overline{b}))\big)$ la probabilité que Bob demande à Alice de lui révéler le premier bit de chaque couples est égale à la probabilité qu'il lui demande de lui révéler le deuxième bit de chaque couple; donc, la probabilité qu'Alice passe le test pour une paire de couple de cette forme est égale à $\frac{1}{2}$. Puisque le nombre total de paires de couples dont le ou exclusif est différent est estimé à $(1-\gamma_1)\,\gamma_2 M + \gamma_1\,(1-\gamma_2)\,M$, alors la probabilité qu'Alice passera tous ces tests est de l'ordre de

$$\left(\frac{1}{2}\right)^{M(\gamma_1(1-\gamma_2)+\gamma_2(1-\gamma_1))} \tag{4.4}$$

On a que :

$$\max(\gamma_1, 2\gamma_2) > \gamma \Longrightarrow \max(\frac{\gamma_1}{2}, \gamma_2) > \frac{\gamma}{2} \Longrightarrow \max(\gamma_1, \gamma_2) > \frac{\gamma}{2} \tag{4.5}$$

et

$$\max(1-\gamma_1, 2-2\gamma_2) > \gamma \Longrightarrow \max(\frac{1-\gamma_1}{2}, 1-\gamma_2) > \frac{\gamma}{2} \Longrightarrow \max(1-\gamma_1, 1-\gamma_2) > \frac{\gamma}{2} \tag{4.6}$$

Et puisque :

$$(\forall x, y, \gamma; \in [0,1]) \quad : \tag{4.7}$$
$$\Big(\max(x,y) > \frac{\gamma}{2}\Big) \wedge \Big(\max(1-x, 1-y) > \frac{\gamma}{2}\Big) \implies \Big(x(1-y) + y(1-x) \geq \frac{\gamma}{2}\Big)$$

L'utilisation de la relation 4.7 et les résultats des relations (4.5) et (4.6) donne :

$$[(\max(\gamma_1, 2\gamma_2) > \gamma) \wedge (\max(1-\gamma_1, 2-2\gamma_2) > \gamma)] \tag{4.8}$$
$$\Longrightarrow \quad \Big[\gamma_1\,(1-\gamma_2) + \gamma_2\,(1-\gamma_1) \geq \frac{\gamma}{2}\Big]$$

De (4.8) et de l'expression de la probabilité qu'Alice passe le test de Bob dans (4.4) on a :

$$\left(\frac{1}{2}\right)^{M(\gamma_1(1-\gamma_2)+\gamma_2(1-\gamma_1))} \leq \left(\frac{1}{2}\right)^{\frac{M\gamma}{2}}$$

D'où, la probabilité qu'Alice passe les tests de Bob est négiligeable pour un M suffisamment grand.

■

4.3.2 Utilisation de la technique de Rudich pour la réalisation d'une mise en gage relativiste pratique

La technique de Rudich peut être combinée avec le protocole relativiste 6 de la page 103 pour détenir un protocole de mise en gage relativiste classique inconditionnellement sécuritaire et pratique. L'idée principale de ce protocole est la suivante. Alice peut s'engager, via le protocole relativiste 6, dans un tour sur le bit b_1 et dans le tour suivant, sur un bit b_2, puis utilise la technique de Rudich pour prouver à Bob que $b_1 = b_2$.

Les détails du déroulement du protocole sont comme suit. Dans la région P_1 et suivant le protocole relativiste 6, A_1 utilisera $2M$ nombres m_i pour s'engager sur chacun des $2M$ bits constituant les couples (b_1^{1j}, b_1^{2j}) tels que $j \in [1, M]$, où $b_1 = b_1^{1j} \oplus b_1^{2j}$. De sa part, A_2 s'engagera, dans la région Q_1, sur chaque bit de la forme binaire des $2M$ nombres m_i utilisés par Alice dans P_1; donc, elle s'engagera, au total, sur $2nM$ bits en utilisant $2nM$ nombres m_i. Dans la région P_2, A_1 utilisera $4M$ nombres m_i pour s'engager sur chacun des $4M$ bits constituant les couples (b_2^{1j}, b_2^{2j}) tels que $j \in [1, 2M]$, où $b_2 = b_2^{1j} \oplus b_2^{2j}$; toujours dans P_2, A_1 et B_1 utilisent la technique de Rudich pour prouver que $b_1 = b_2$; donc, A_1 révelera un bit de chaque couple (b_1^{1j}, b_1^{2j}) tels que $j \in [1, M]$ en dévoilant les n nombres m_i utilisés dans la région Q_1 pour le coder. Elle révèlera aussi un bit de chaque couple parmi les M couples choisis aléatoirement par Bob de l'ensemble des couples (b_2^{1j}, b_2^{2j}) tels que $j \in [1, 2M]$ et cela en dévoilant les nM nombres m_i qui vont être utilisés par A_2 dans Q_2 pour les coder. Dans le région Q_2, A_2 s'engagera sur chaque bit de la forme binaire des $4M$ nombres m_i utilisé par A_1 dans P_2; donc, elle s'engagera, au total, sur $4nM$ bits en utilisant $4nM$ nombres m_i. À ce stade, Bob doit vérifier les révélations d'Alice pour s'assurer si réellement $b_1 = b_2$, et pour ce faire, il doit rassembler toutes les informations fournies par A_1 dans P_2 et par A_2 dans Q_1 ou Q_2. Si tout est correct, les M bits b_1^{ij} non révélés sont écartés automatiquement du protocole; donc, tous les couples (b_1^{1j}, b_1^{2j}) tels que $j \in [1, M]$ sont écartés une fois pour toutes du protocole. Pour les $2M$ autres couples, l'affaire est un peu différente; puisque, d'après la technique de Rudich, c'est B_2 qui choisit aléatoirement les M couples parmi

les $2M$ couples qui vont subir le test (un bit pour chaque couple choisi), alors, les deux agents A_2 et B_2 peuvent déjà, dans P_2, écarter M autes couples parmi les $2M$ couples (b_2^{1j}, b_2^{2j}) tels que $j \in [1, 2M]$ et il leur reste à la fin exactement M couples (b_2^{1j}, b_2^{2j}) tels que $b_1 = b_2 = b_2^{1j} \oplus b_2^{2j}$. Mais, comme dans Q_2, l'agente A_2 ignore certainement le choix de B_1 dans P_2, l'engagement sur les $4M$ bits (via $4nM$ engagements élémentaires) est encore maintenu.

À ce stade, dans la région P_3, A_1 utilisera $4M$ nouveaux nombres m_i pour s'engager sur chacun des $4M$ bits constituant les couples (b_3^{1j}, b_3^{2j}) tels que $j \in [1, 2M]$, où $b_3 = b_3^{1j} \oplus b_3^{2j}$; toujours dans P_3, A_1 et B_1 utilisent la technique de Rudich pour prouver que $b_2 = b_3$; et ainsi de suite...

La révélation se fait de la même manière que dans le protocole 6, sauf qu'ici c'est seulement l'agent A_2 qui peut révéler le bit.

Analysons maintenant, la sécurité du protocole pour chaque participant.

1. Si Bob est malhonnête, il n'a aucun moyen lui permettant de découvrir le bit d'Alice avant la révélation, car, de son point de vue, les informations qu'il reçoit d'elle ne sont pas corrélées au bit mis en gage.

2. Pour voir la sécurité du protocole envers Alice, analysons le cas d'un seul bit. Pour qu'elle puisse révéler dans P_i avec succès un bit différent de celui sur lequel elle s'est engagée en utilisant le nombre m à n bits dans la même région P_i, elle doit deviner les n couples $(n_{0,i}, n_{1,i})$ envoyés par B_2 à A_2 dans Q_i pour coder chaque bit de la forme binaire du nombre m. L'analyse déjà faite pour le protocole 5, a montré que la probabilité de passer le test pour chaque bit de m est égale à $\frac{1}{N-1}$, donc, la probabilité qu'Alice passe le test de Bob pour tous les n bits, si elle triche en révélant un bit différent de celui sur lequel elle s'est engagée dans P_i, est égale à $\frac{1}{(N-1)^n}$. Un raisonnement similaire montre aussi, que la probabilité qu'une Alice malhonnête, révèle avec succés dans P_i un bit différent de celui sur lequel elle s'est engagée en utilisant le nombre m à n bits dans la région P_{i-1}, est égale à $\frac{1}{(N-1)^n}$.

4.4 Étude de la sécurité des protocoles relativistes contre les attaques quantiques

1. Puisque l'information que reçoit Bob d'une Alice honnête n'est pas corrélée (de son point de vue) à la valeur du bit mis en gage, alors, le fait qu'il puisse manipuler de l'information quantique, ne va pas l'aider.

2. Maintenant, examinons ce qu'une Alice malhonnête peut faire dans un cadre quantique. Dans l'article [15], Brassard, crépeau, Mayers et Salvail ont proposé l'attaque suivante contre le protocole de mise en gage temporaire 4, et qui s'étend naturellement aux deux autres protocoles relativistes de Kent [43, 44] : les agents A_1 et A_2 partagent préalablement les deux états

$$\alpha \left|0\right\rangle_{A_1} \left|0\right\rangle_{A_2} + \beta \left|1\right\rangle_{A_1} \left|1\right\rangle_{A_2}$$

et

$$\left(\frac{1}{\sqrt{2}} \left|0\right\rangle_{A_1} \left|0\right\rangle_{A_2} + \frac{1}{\sqrt{2}} \left|1\right\rangle_{A_1} \left|1\right\rangle_{A_2}\right)^n = \frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} \left|r\right\rangle_{A_1} \left|r\right\rangle_{A_2}$$

Puis, quand A_1 recoit la paire (n_{01}, n_{11}) de B_1 il appplique la transformation unitaire U telle que :

$$U\left(\frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} \left(\alpha \left|0\right\rangle_{A_1} \left|0\right\rangle_{A_2} + \beta \left|1\right\rangle_{A_1} \left|1\right\rangle_{A_2}\right) \left|r\right\rangle_{A_1} \left|r\right\rangle_{A_2} \left|0\right\rangle_C\right) \tag{4.9}$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} \left(\alpha \left|0\right\rangle_{A_1} \left|0\right\rangle_{A_2} \left|r\right\rangle_{A_1} \left|r\right\rangle_{A_2} \left|r + n_{01}\right\rangle_C + \beta \left|1\right\rangle_{A_1} \left|1\right\rangle_{A_2} \left|r\right\rangle_{A_1} \left|r\right\rangle_{A_2} \left|r + n_{11}\right\rangle_C\right)$$

Où $\left|0\right\rangle_C$ est un système ancillaire utilisé par A_1. Si on pose $r + n_{11} = k + n_{01}$, on aura $r = k + n_{01} - n_{11}$, ce qui permet d'écrire le membre droit de (4.9) comme :

$$\frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} \alpha \left|0\right\rangle_{A_1} \left|0\right\rangle_{A_2} \left|r\right\rangle_{A_1} \left|r\right\rangle_{A_2} \left|r + n_{01}\right\rangle_C \tag{4.10}$$

$$+\frac{1}{2^{\frac{n}{2}}} \sum_{k=0}^{N-1} \beta \left|1\right\rangle_{A_1} \left|1\right\rangle_{A_2} \left|k + n_{01} - n_{11}\right\rangle_{A_1} \left|k + n_{01} - n_{11}\right\rangle_{A_2} \left|k + n_{01}\right\rangle_C$$

en tenant compte que tout le calcul se fait modulo N. Puisque k est un indice muet, l'expression (4.10) devient :

$$\frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} \left(\alpha \left|0\right\rangle_{A_1} \left|0\right\rangle_{A_2} \left|r\right\rangle_{A_1} \left|r\right\rangle_{A_2} \right. \tag{4.11}$$

$$\left. +\beta \left|1\right\rangle_{A_1} \left|1\right\rangle_{A_2} \left|r + n_{01} - n_{11}\right\rangle_{A_1} \left|r + n_{01} - n_{11}\right\rangle_{A_2}\right) \left|r + n_{01}\right\rangle_C$$

À ce stade, A_1 envoie le système C a B_1. Pour la révélation maintenant, supposant que B_1 mesure le systeme C et trouve le résultat s_1, Dans ce cas, $r + n_{01} = s_1$, et l'état de l'équation (4.11) devient :

$$\begin{aligned}&\left(\alpha\left|0\right\rangle_{A_1}\left|0\right\rangle_{A_2}\left|s_1 - n_{01}\right\rangle_{A_1}\left|s_1 - n_{01}\right\rangle_{A_2}\right. \\ &\left.+\beta\left|1\right\rangle_{A_1}\left|1\right\rangle_{A_2}\left|s_1 - n_{11}\right\rangle_{A_1}\left|s_1 - n_{11}\right\rangle_{A_2}\right)\left|s_1\right\rangle_C\end{aligned} \tag{4.12}$$

Il est clair que, si A_1 et A_2 partagent l'état de l'équation (4.12), Bob ne peut en aucun cas découvrir la tricherie d'Alice; chaque agent peut révéler, quand il faut, en mesurant le système en sa possession, pour avoir 0 ou 1 avec probabilités $|\alpha|^2$ et $|\beta|^2$, respectivement, avec la valeur adéquate, $s_1 - n_{01}$ ou $s_1 - n_{11}$, pour convaincre Bob.

Cette possibilité offerte a Alice reste tout de même dans le cadre de la définition même de la sécurité des protocoles quantiques de mise en gage (revenir à la définition 13) car elle ne lui permet pas de changer la distribution initiale de probabilité ($|\alpha|^2$ et $|\beta|^2$).

Cette stratégie peut être appliquée dans le premier protocole de Kent [40], et cela en procédant de la même manière pour chaqun des deux tours successifs, tout en maintenant la superposition; on peut imaginer l'état partagé entre A_1, A_2, B_1 et B_2 après la mesure de B_2 dans le deuxième tour, qui donne, par exemple, l'état : $\left|s_2\right\rangle_{C_2} .. \left|s_{n+1}\right\rangle_{C_{n+1}}$ (cet état est obtenu après que A_2 reçoit les n couples $(n_{0,i}, n_{1,i})$ tels que $n_{0,i} \neq n_{1,i}, i \in [2, n+1]$ et applique la transformations unitaire adéquate dépendante de ces couples $(n_{0,i}, n_{1,i})$ tels que $n_{0,i} \neq n_{1,i}, i \in [2, n+1]$, puis retourne un système ancillaire $C_2 + C_3 + ...C_{n+1}$ à B_2) comme :

$$\begin{aligned}&\left[\alpha\left(\left|0\right\rangle_{A_1}\left|0\right\rangle_{A_2}\left|s_1 - n_{01}\right\rangle_{A_1}\left|s_1 - n_{01}\right\rangle_{A_2}\left|s_2 - n_{a_1 2}\right\rangle_{A_1}\left|s_2 - n_{a_1 2}\right\rangle_{A_2}\cdots\right.\right. \\ &\left.\left.. .\left|s_{n+1} - n_{a_n n+1}\right\rangle_{A_1}\left|s_{n+1} - n_{a_n n+1}\right\rangle\right)\right._{A_2} \\ &+\beta\left(\left|1\right\rangle_{A_1}\left|1\right\rangle_{A_2}\left|s_1 - n_{11}\right\rangle_{A_1}\left|s_1 - n_{11}\right\rangle_{A_2}\left|s_2 - n_{b_1 2}\right\rangle_{A_1}\left|s_2 - n_{b_1 2}\right\rangle_{A_2}\cdots\right. \\ &\left.\left. ..\left|s_{n+1} - n_{b_n n+1}\right\rangle_{A_1}\left|s_{n+1} - n_{b_n n+1}\right\rangle_{A_2}\right)\right]\left|s_1\right\rangle_{C_1}\left|s_2\right\rangle_{C_2} .. \left|s_{n+1}\right\rangle_{C_{n+1}}\end{aligned}$$

où on a supposé que les formes binaires de $s_1 - n_{01}$ et $s_1 - n_{11}$ sont :

$$\begin{aligned} s_1 - n_{01} &= a_1 a_2 .... a_n \\ s_1 - n_{11} &= b_1 b_2 .... b_n \end{aligned}$$

Note 10 *Dans le cas précédent, Alice peut révéler avec succès dans le troisième tour, et pour ce faire, les deux agents A_1 et A_2 ont dû partager préalablement, en plus de l'état $\alpha |0\rangle_{A_1} |0\rangle_{A_2} + \beta |1\rangle_{A_1} |1\rangle_{A_2}$, l'état*

$$\left[\frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} |r\rangle_{A_1} |r\rangle_{A_2} \right]^{\otimes(n+1)}$$

qui a servi comme source de nombres aléatoires. On peut conclure que si Alice compte maintenir l'engagement pour t tours, les deux agents A_1 et A_2 doivent partager, en plus de l'état $\alpha |0\rangle_{A_1} |0\rangle_{A_2} + \beta |1\rangle_{A_1} |1\rangle_{A_2}$, l'état

$$\left[\frac{1}{2^{\frac{n}{2}}} \sum_{r=0}^{N-1} |r\rangle_{A_1} |r\rangle_{A_2} \right]^{\otimes\left(\frac{n^{t-1}-1}{n-1}\right)} \quad \textit{tels que } t \geq 2$$

De la même façon, Alice peut appliquer cette technique pour le protocole amélioré de Kent [44] *en partageant les états intriqués adéquats.*

Une preuve de la sécurité temporaire, c-à-d., tour par tour, des deux protocoles de Kent [43, 44] contre les attaques quantiques, se résume dans le lemme suivant.

Lemme 10 *Si* $p_0^{j,\sup}(p_1^{j,\sup})$ *est la borne supérieure de l'ensemble des probabilités avec lesquelles Alice révèle avec succès le bit* 0 *(*1*) dans le tour* j*, sur toutes les stratégies de révélations qu'elle puisse appliquer dans ce tour. Alors* $p_0^{j,\sup} + p_1^{j,\sup} \leq 1 + \epsilon(N)$ *tels que* $\lim_{N\to\infty} \epsilon(N) = 0$ *dans le cas du premier protocole de Kent* [43] *et* $p_0^{j,\sup} + p_1^{j,\sup} \leq 1+\epsilon(N,M)$ *tels que* $\lim_{M,N\to\infty} \epsilon(N,M) = 0$ *dans le cas du deuxième protocole de Kent* [44].

Preuve Il est évident que le point essentiel pouvant donner à Alice un avantage dans ce modèle quantique est le partage de l'intrication entre ses agents A_1 et A_2. Supposons que ces agents puissent partager l'état de leurs choix (donc, celui qui leur donne le plus d'opportunité). D'après ce qu'on a vu dans le chapitre 2, il est toujours possible de considérer l'état partagé entre A_1 et A_2 comme étant un état pur, soit $|\Psi\rangle$ par exemple. Donc, on peut avoir la stratégie optimale (en supposant, que la borne maximale de la probabilité de tricherie soit réalisable) de la tricherie d'Alice dans un modèle où Alice et Bob ne partagent pas de l'intrication. Dans les protocoles de Kent [43, 44], un agent A_i révèle en envoyant à B_i une liste de nombres permetant à ce dernier de vérifier leur cohérence avec une révélation valide de l'un des deux bits, 0 ou 1. Puisqu'on a supposé que l'état paratgé entre A_1 et A_2 est pur, on peut alors considérer sa stratégie optimale de révéler 0(1) dans le tour j comme étant une mesure projective $\{P_l\}(\{Q_j\})$ de l'état $|\Psi\rangle$, où à chaque résultat possible $P_\alpha(Q_\beta)$ il lui correspond une certaine liste de nombres $\Gamma_\alpha(\Lambda_\beta)$. C-à-d., si Alice veut révéler 0(1), elle effectue la mesure $\{P_l\}(\{Q_j\})$sur l'état $|\Psi\rangle$, et si le résultat de cette mesure est $P_\alpha(Q_\beta)$, elle envoie la liste $\Gamma_\alpha(\Lambda_\beta)$ à Bob. Parmi toutes les listes possibles, il y a une qui correspond à une révélation valide de 0(1) (puisqu'elle existait dans le cas où les deux participants suivent le protocole), soit $\Gamma_0(\Lambda_1)$ cette liste. On peut écrire alors :

$$p_0^{j,\sup} = \langle\Psi| P_0 |\Psi\rangle = |P_0 |\Psi\rangle|^2 \quad \text{et} \quad p_1^{j,\sup} = \langle\Psi| Q_1 |\Psi\rangle = |Q_1 |\Psi\rangle|^2$$

On a aussi :

$$|P_0 Q_1 |\Psi\rangle| = |P_0 (I - (I - Q_1)) |\Psi\rangle| = |P_0 |\Psi\rangle - P_0 (I - Q_1) |\Psi\rangle|$$

La relation (1.13), implique :

$$|P_0 Q_1 |\Psi\rangle| = |P_0 |\Psi\rangle - P_0 (I - Q_1) |\Psi\rangle| \geq |P_0 |\Psi\rangle| - |P_0 (I - Q_1) |\Psi\rangle| \qquad (4.13)$$

On sait que, pour tout projecteur Π et tout état $|\chi\rangle$:

$$||\chi\rangle| \geq |\Pi\,|\chi\rangle|$$

donc,

$$|P_0\,(I-Q_1)\,|\psi\rangle| \leq |(I-Q_1)\,|\psi\rangle|$$

et la relation (4.13) devient :

$$|P_0Q_1\,|\psi\rangle| \geq |P_0\,|\psi\rangle| - |(I-Q_1)\,|\psi\rangle| \tag{4.14}$$

Le fait que Q_1 est un projecteur, et donc $I-Q_1$ aussi, permet d'écrire :

$$\begin{aligned} |(I-Q_1)\,|\Psi\rangle| &= \sqrt{\langle\Psi|\,(I-Q_1)\,(I-Q_1)\,|\Psi\rangle} = \sqrt{\langle\Psi|\,(I-Q_1)\,|\Psi\rangle} \\ &= \sqrt{\langle\Psi|\Psi\rangle - \langle\Psi|\,Q_1\,|\Psi\rangle} = \sqrt{1-p_1^{j,\mathrm{sup}}} \end{aligned}$$

Ceci permet d'écrire (4.14) comme :

$$|P_0Q_1\,|\psi\rangle| \geq \sqrt{p_0^{j,\mathrm{sup}}} - \sqrt{1-p_1^{j,\mathrm{sup}}} \tag{4.15}$$

Supposons, par l'absurde, que :

$$p_0^{j,\mathrm{sup}} + p_1^{j,\mathrm{sup}} - 1 > \epsilon \tag{4.16}$$

où ϵ est un nombre positif. Dans ce cas, on peut écrire :

$$p_0^{j,\mathrm{sup}} + p_1^{j,\mathrm{sup}} - 1 > 0 \Rightarrow p_0^{j,\mathrm{sup}} > 1 - p_1^{j,\mathrm{sup}} \Rightarrow \sqrt{p_0^{j,\mathrm{sup}}} - \sqrt{1-p_1^{j,\mathrm{sup}}} > 0 \tag{4.17}$$

Les relations (4.13) et (4.17) impliquent :

$$|P_0Q_1\,|\psi\rangle|^2 \geq \left(\sqrt{p_0^{j,\mathrm{sup}}} - \sqrt{1-p_1^{j,\mathrm{sup}}}\right)^2 \tag{4.18}$$

Posons,

$$\xi = p_0^{j,\mathrm{sup}} + p_1^{j,\mathrm{sup}} - 1 \tag{4.19}$$

et

$$\pi_0^{j,\mathrm{sup}} = \left(\sqrt{p_0^{j,\mathrm{sup}}} - \sqrt{1-p_1^{j,\mathrm{sup}}}\right)^2 \tag{4.20}$$

De la relation (4.18), on peut voir que l'agent A_i peut effectuer la mesure projective $\{Q_j\}$ lui permetant de révéler 1 et passer le test de Bob avec une probabilité égale à $p_1^{j,\sup}$, comme il peut révéler 0 avec une probabilité de succès supérieure ou égale à $\pi_0^{j,\sup}$ en effectuant une seconde mesure $\{P_j\}$ après la première mesure $\{Q_j\}$. Les relations (4.16) et (4.19) impliquent :

$$\xi > \epsilon \Longrightarrow p_1^{j,\sup} > \epsilon$$

Et de (4.19) et (4.20) on peut avoir :

$$\xi > \epsilon \Longrightarrow \pi_0^{j,\sup} > \left(1 - \sqrt{1-\epsilon}\right)^2$$

L'expression $\left(1 - \sqrt{1-\epsilon}\right)^2$ est strictement croissante en fonction de ϵ. Cela veut dire qu'il est possible pour A_i de révéler, en même temps, 0 avec une probabilité de succès supérieure ou égale à $\pi_0^{j,\sup}$, et 1 avec une probabilité de succès égale à $p_1^{j,\sup}$. Mais un tel résultat ne peut être vrai que si A_i connaît, avec une probabilité suffisamment grande, les differences $n_{0k} - n_{1k}$ dans les couples aléatoires (n_{0k}, n_{1k}) envoyés par $B_{\bar{i}}$ à $A_{\bar{i}}$ dans le tour $j-1$, ce qui n'est pas possible dans le cadre de la relativité restreinte, où la vitesse de tout signal ne peut surpasser celle de la lumière.

■

En adaptant le formalisme de la sous-section 3.1.3 à celui du lemme 10, on peut écrire le résultat de Mayers, Lo et Chau comme suit : dans tout protocole quantique parfaitement camouflant, on a : $p_0^{j,\sup} + p_1^{j,\sup} = 2$, et aussi, dans tout protocole quantique camouflant on a : $p_0^{j,\sup} + p_1^{j,\sup} = 2 - \epsilon(n)$ tel que $\lim_{n\to\infty} \epsilon(n) = 0$. Donc, le résultat du lemme 10 montre que le protocole de Brassard, Crépeau, Mayers et Salvail [15] échappe temporairement à l'attaque de Mayers, Lo et Chau, alors que les deux protocoles de Kent [43, 44] échappent continuellement à cette attaque.

La raison pour laquelle l'attaque de Mayers, Lo et Chau ne peut s'appliquer ici, est qu'Alice ignore totalement, lors de sa révélation, les couples fournis par Bob dans le tour précédent, et par conséquent, ne peut construire (car, elle ne peut pas avoir toutes les données nécessaires), en même temps, les transformations adéquates pour chaque

révélation.

Note 11 *Le lemme 10 ne constitue pas une preuve générale de la sécurité des protocoles de Kent contre toutes les attaques possibles, bien qu'il démontre la robustesse de ces protocoles contre l'attaque du type de Mayers, Lo et Chau, qui n'est pas l'attaque la plus générale dans le cadre quantique.*

CONCLUSION

On a commencé ce travail par l'exposition des démonstrations de plusieurs théorèmes qui ont été derrière les plus importants résultats de la cryptographie quantique, tels le théorème de purification, le théorème GHJW, le théorème de non-clonage, la décomposition de Schmidt, le théorème d'Ulmann, etc. On a aussi discuté des concepts de base de l'informatique quantique, comme la mesure projective et généralisée, l'évolution des systèmes quantiques non isolés, la trace partielle, l'opérateur de densité, etc. Ensuite, on a abordé le fameux théorème de l'impossibilité de Mayers, Lo et Chau et montré que dans tout protocole quantique non relativiste empêchant Bob d'extraire toute (ou une partie de) l'information sur le bit mis en gage, Alice peut (ou peut avec une grande probabilité) changer le bit mis en gage de 0 à 1 (et vice versa) sans être détectée. Bien que ce théorème nous interdira tout espoir de construire un protocole de mise en gage inconditionnellement sécuritaire, il n'empêche pas la réalisation d'une mise en gage quantique partiellement liante et partiellement camouflante à la fois. Il s'agit-là d'une caractéristique qu'aucun protocole classique non relativiste ne peut assurer. C'est ce que nous avons montré grâce au modèle mathématique général de Spekkens et Rudolf. On a vu une intéressante classe de protocoles de mise en gage quantique où le système initial provient d'Alice. On a vulgarisé des démarches permettant d'obtentenir une importante relation de compromis (trade-off) entre les degrés de camouflage et de lien dans cette classe de protocoles ($G^{\max} + C^{\max} \geq \frac{1}{2}$). On a exposé un protocole de purification (non-intéractif) saturant cette relation; c'est d'ailleurs ce protocole qui a permis l'implantation du meilleur protocole de la version forte du pile ou face existant jusqu'à maintenant. Un autre résultat intéressant de cette analyse est qu'un espace de dimension trois est le minimum exigé pour saturer cette relation de compromis. On étudie aussi un autre type de sécurité pour ce protocole, c'est celui de la mise en gage sensible à la tricherie (cheat sensitive) pour laquelle on croyait que le protocole quantique

de Hardy et Kent fonctionnait jusqu'à ce que, récemment, Ishizaka ait démontré que tel n'est pas le cas. Pire, il a même remis en question toute possibilité de réaliser ce type de sécurité en se basant sur l'utilisation du protocole du tir à pile ou face comme sous-protocole. On a exposé l'attaque proposée par l'auteur et on a demontré que tout état peut être récupéré par Bob sans être détecté par Alice s'il se limite à perturber le système à un certain degré; ceci pose une fois encore la question de pouvoir construire ce type de protocole. Le dernier chapitre de ce mémoire a été consacré au seul protocole de mise en gage arrivant jusqu'à maintenant d'échapper à l'attaque de Mayers, Lo et Chau. Dans les protocoles de mise en gage classiques et quantiques qu'on a souvent tenté de réaliser, il n'y a pas d'échange d'informations, pendant une durée indéterminée, entre la fin de la phase de l'engagement et le début de celle de la révélation. Kent a ajouté une troisième phase entre les deux phases précédentes, où Alice et Bob continueront, à partir de leurs sites, à s'échanger de l'information de manière régulière jusqu'à ce qu'Alice décide de révéler le bit. À ce moment, le protocole n'est pas encore terminé et Bob doit rassembler les informations de ses différents sites afin de juger la bonne foi de cette dernière. On a suivi les pas de Kent et détaillé les preuves de la sécurité de son premier protocole qui n'était malheureusement pas pratique. Toutfois il a tracé le chemin vers son deuxième protocole qui grâce à une technique inventée par Rudich (qu'on a exposé en détail) a remédié aux problèmes liés à l'impossibilité pratique du premier. On a terminé ce chapitre par la présentation de la preuve de la robustesse de ce protocole contre l'attaque quantique de Mayers, Lo et Chau. La sécurité de ce protocole contre toutes les attaques quantiques reste encore aujourd'hui une conjecture.

BIBLIOGRAPHIE

[1] D. Ahoronov, A. Ta-Shma, U.V. Vazirani et A.C. Yao, «Quantum bit escrow», in *the Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (ACM Press, New York)*, pp. 705-714, 2000, preprint *quant-ph/0004017*.

[2] A. Ambainis. «A new protocol and lower bounds for quantum coin flipping»,in *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pp. 134-142, 2001.

[3] A. Ambainis, H. Buhrman, Y. Dodis, and H. Röhrig, «Multiparty quantum coin flipping»,in *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pp. 250–259, 2004.

[4] H. Barnum, C.M. Caves, C.A. Fuchs, R. Jozsa et B. Schumacher, «Noncommuting mixed states cannot be broadcast», *Physical Review Letters*, vol. (76) : pp. 2818-2821, 1996.

[5] M. Ben-Or, «Simple security proof for quantum key distribution», Unpublished, (Voir l'exposé donné au MSRI (*Mathematical Sciences Research Institute*) durant le semestre de l'anné 2002, dédié à l'informatique quantique: http ://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html.)

[6] M. Ben-Or, S. Goldwasser, J. Kilian, et A. Wigderson, «Multi-prover interactive proofs: How to remove intractability assumptions», *Annual ACM Symposium on Theory of Computing* ,vol. (88) : pp. 113-131, 1988.

[7] M. Ben-Or, S. Goldwasser et A. Wigderson, «Completeness theorems for faulttolerant distributed computing»,in *Proc. 20th ACM Symposium on Theory of Computing*, pp. 1-10, Chicago, 1988. ACM.

[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail et J. Smolin, «Experimental quantum cryptography», *Journal of Cryptology*, vol.(5), no. (1) : pp. 3-28, 1992.

[9] C.H Bennett et G. Brassard, «Quantum cryptography: Public key distribution and coin tossing», *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp.175-179, 1984.

[10] C.H. Bennett, G. Brassard et N.D. Mermin, «Quantum cryptography without Bell's theorem», *Physical Review Letters*, vol (68) : pp. 557-559, 1996.

[11] G. Berlìn, G. Brassard, F. Bussières et N. Godbout, « Loss-tolerant quantum coin flipping », *Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM08), Sainte Luce, Martinique*, pp. 1-9, février 2008.

[12] M. Blum. «Coin flipping by telephone»,in *Allen Gersho, editor, Advances in Cryptography, Crypto 81*, pp. 11-15, Santa Barbara, California, USA, 1982. University of California, Santa Barbara.

[13] G. Brassard et C. Crépeau, «Quantum bit commitment and coin-tossing protocols», *In Advances in Cryptology: Proceedings of Crypto 90, Lecture Notes in Computer Science*, Vol. (537) : pp. 49-61. Springer-Verlag, 1991.

[14] G. Brassard, C. Crépeau, R. Jozsa et D. Langlois, «A quantum bit commitment scheme provably unbreakable by both parties»,in *29th Symposium on Foundations of Computer Science*, pp. 42-52, IEEE, 1993.

[15] G. Brassard, C. Crépeau, D. Mayers, L. Salvail, «Defeating classical bit commitments with a quantum computer», preprint *quant-ph/9806031*.

[16] G. Brassard, D. Chaum, and C. Crépeau, «Minimum disclosure proofs of knowledge», *Journal of Computer and System Sciences*, vol. (37) : pp. 156–189, 1988.

[17] J. Breguet, A. Muller et N. Gisin, «Quantum Cryptography with polarized photons in optical fibres. Experiment and practical limits», *Journal of Modern Optics*, vol. (41), no (12) : pp. 2405-2412, December 1994.

[18] C. Cachin, C. Crépeau et J. Marcil, «Oblivious transfer with a memory bounded receiver»,in, *39th Annual IEEE Symposium on Foundations of Computer Science: proceedings*, pp. 493-502. *IEEE Computer Society Press*, 1998.

[19] D. Chaum, C. Crépeau et I. Damgård, «Multiparty unconditionally secure protocols», *in symposium on Theory of computing 88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pp. 11-19, New York, NY, USA, 1988. ACM Press.

[20] B. Chor, S. Goldwasser, S. Micali et B. Awerbuch, «Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract)», *In Proc. of 26th FOCS*, pp. 383-395, *Portland, Oregon*, pp. 21-23, October 1985, IEEE.

[21] R. Colbeck, «An entanglement-based protocol for strong coin tossing with bias 1/4», *Physics Letters A*, vol.(362-5) : pp. 390-392, 2007.

[22] C. Crépeau. «Efficient cryptographic protocols based on noisy channels»,in *Walter Fumy, editor, Advances in Cryptology- EuroCrypt 97*, pp. 306-317, Berlin, 1997. *Springer-Verlag Lecture Notes in Computer Science*, vol. (1233).

[23] V. Damgård, S. Fehr, L. Salvail, et C. Schaffner, «Cryptography in the Bounded Quantum-Storage Model», in *SIAM Journal on Computing*, vol. (37), no.(6) : pp. 1865-1890, 2008.

[24] D. Dieks, «Communication by EPR devices», *Physics Letters A*, vol. (92), no (6) : pp. 271-272, 1982.

[25] W. Diffie et M. E. Hellman, «New directions in cryptography», *IEEE Transactions on Information Theory*, vol. (22), no. (6) : pp. 644-654, 1976.

[26] Y. Z. Ding, D. Harnik, A. Rosen, et R. Shaltiel, «Constant-tour oblivious transfer in the bounded storage model», in *Theory of Cryptography TCC-2004*, pp. 446-472.

[27] P. Dumais, D. Mayers, et L. Salvail, «Perfectly concealing quantum bit commitment from any quantum one-way permutation», in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2000)*, vol. (1807) of *Lecture Notes in Computer Science*, pp. 300-315, 2000.

[28] C. Fuchs et J. van de Graaf, «Cryptographic distinguishability measures for quantum mechanical states», *IEEE Transactions on Information Theory*, vol. (45): pp. 1216-1227, 1999.

[29] N. Gisin, «Stochastic quantum dynamics and relativity», *Helvetica Physica Acta*, vol. (62) : pp. 363-371, 1989.

[30] M. Goemans et D. Williamson, «Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming», *Journal of the ACM*, vol. (42): pp. 1115-1145, 1995.

[31] O. Goldreich, S. Micali, et A. Wigderson, «Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems», *Journal of the Association for Computing Machinery*, vol. (38), no. (3) : pp. 691-729, July 1991.

[32] G. Gutoski et J. Watrous, «Toward a general theory of quantum games», *Proceedings of the 39th ACM Symposium on Theory of Computing*, pp. 565-574, 2007, preprint *quant-ph/0611234v1*.

[33] D. Gottesman et H. K. Lo, «Proof of security of quantum key distribution with two-way classical communications», *IEEE. Transactions on Information Theory*, vol. (49) : pp. 457-475, 2003.

[34] S. Halevi et S. Micali, «Practical and provably-secure commitment schemes from collision-free hashing» in *Neal Koblitz, editor, Advances in Cryptology-Crypto 96*, pp. 201-215, Berlin, 1996. *Springer-Verlag. Lecture Notes in Computer Science* vol. (1109).

[35] L. Hardy et A. Kent, «Cheat sensitive quantum bit commitment», preprint, *quant-ph/9911043.*

[36] J. Hastad, R. Impagliazzo, L.A. Levin et M. Luby. «A pseudorandom generator from any one-way function», *SIAM Journal on Computing*, vol. (28), no (4) : pp..1364-1396, 1999.

[37] C.Helstrom, «Quantum detection and estimation theory», *Academic Press, New York*, 1976.

[38] L Hughston, R Jozsa et W Wootters, «A complete classification of quantum ensembles having a given density matrix», *Physical Letters A*, vol. (183) : pp. 14-18. November 1993.

[39] S. Ishizaka, «Dilemma that cannot be resolved by biased quantum coin flipping», *Physical Review Letters.* vol. (100), pp. 070501, 2008, preprint *quant-ph/0703099 v3.*

[40] B. Jeffrey, «The quantum bit commitment theorem», *Foundations of Physics*, vol. 31, no. (5): pp. 735-756, May 2001.

[41] R.Jozsa, «Fidelity for mixed quantum states», *Journal of Modern Optics*, vol. (41), no. (12) : pp. 2315 -2323,1994.

[42] R. Karp, «Reducibility among combinatorial problems», *Complexity of Computer Computations*, pp. 85–109, R. E. Miller and T. W. Thatcher (eds.), Plenum Press, New York, 1972.

[43] A. Kent, «Unconditionally secure bit commitment», *Physical Review Letters*, vol. (83) : pp. 1447-1450, 1999.

[44] A. Kent, «Secure classical bit commitment using fixed capacity communication channels», *Journal of Cryptology*, vol (18) : pp. 313-335, 2005.

[45] I. Kerenidis et A. Nayak, «Weak coin flipping with small bias», *Information Processing Letters*, vol (89), no.(3) : pp. 131-135, 2004.

[46] J. Kilian, «Founding cryptography on oblivious transfer», in *Proc. 20th ACM Symposium on Theory of Computing*, pp 20-31, Chicago, 1988. ACM.

[47] A. Kitaev, Results presented at QIP 2003 (slides and video available from MSRI). http://www.msri.org/publications/ln/msri/2002/qip/kitaev/1/index.html.

[48] K. Kraus, «States, effects, and operations: fundamental notions of quantum theory», *Lecture Notes in Physics*, vol. (190), Berlin : *Springer-Verlag*, 1983.

[49] H. K. Lo et H.F. Chau, «Is quantum bit commitment really possible?», *Physical Review Letters*, vol. (78) : pp. 3410-3413, 1997.

[50] H. K. Lo et H.F. Chau, «Why quantum bit commitment and ideal coin tossing are impossible», in *Proceedings of the Fourth Workshop on Physics and Computation (Boston: New England Complex System Institute, 1996)*, pp. 76, preprint *Quant-ph/9605026*. Revised version in *Physica D*, vol. (120): pp.177-187, 1998.

[51] C. Marand et P. D. Townsend, «Quantum key distribution over distances as long as 30 km», *Optics Letters*, 1995, vol. (20) : pp. 1695-1697, 1995.

[52] D. Mayers, presentation at the 4th Montreal Workshop on *Quantum Information Theory*, October 1995.

[53] D. Mayers, «The trouble with quantum bit commitment», preprint *quant-ph/ 9603015.*

[54] D. Mayers, «Unconditionally secure quantum bit commitment is impossible», in *Proceedings of the Fourth Workshop on Physics and Computation* (Boston: New England Complex System Institute, 1996), pp. 224-228.

[55] D. Mayers, «Unconditionally secure quantum bit commitment is impossible», *Physical Review Letters*, vol. (78): pp. 3414-3417, 1997.

[56] D. Mayers, L. Salvail et Y. Chiba-Kohno, «Unconditionally secure quantum coin-tossing», preprint *quant-ph/9904078*, 1999.

[57] E. Mendelson, «*Introducing Game Theory and Its Applications*», Chapman et Hall, CRC, 2004.

[58] C. Mochon, «Quantum weak coin-flipping with bias of 0.192», in *Proceedings of 45th Symposium on Foundations of Computer Science*, pp. 2-11, 2004.

[59] C. Mochon. «A large family of quantum weak coin-flipping protocols», *Physical Review A*, vol. (72), no (022341): pp. 1-16, 2005.

[60] C. Mochon, «Quantum weak coin flipping with arbitrarily small bias», *ArXiv: 0711.4114.*

[61] R. Muradian, D. Frias, «Revisiting boole equation in the quantum context», *ArXiv:0705.3010.*

[62] M. Naor, «Bit commitment using pseudo randomness», *Journal of Cryptology*, vol (4), no (2) :pp. 151-158, 1991.

[63] M. Naor, R. Ostrovsky, R. Venkatesan et M. Yung, «Perfect zero-knowledge arguments for NP can be based on general complexity assumptions», *E. F. Brickell, Proc. CRYPTO 92*, pp 196-214. Springer-Verlag, 1992. Lecture Notes in Computer Science, no. 740.

[64] A. Nayak et P. Shor, «Bit-commitment-based quantum coin flipping», *Physical Review A*, vol. (67): article no. 012304, 2003.

[65] M. Nielsen et I.Chuang, «*Quantum Computation and Quantum Information*», *Cambridge University Press*, 2000.

[66] R.L. Rivest, A. Shamir et L.M. Adleman, «On digital signatures and public key cryptosystems», *MIT Laboratory for Computer Science, Technical Report*, MIT/LCS/TR-212, Jan 1979, vol. (21), no. (2): pp. 120-126, Feb 1978.

[67] S. Rudich, unpublished, *circa*, 1989.

[68] E. Schmidt, *Math. Ann.*,vol. (63): pp 433, 1907.

[69] C. E. Shannon, «A mathematical theory of communication» (partie 1), *Bell System Technical Journal*, vol. (27): pp. 379-423, 1948.

[70] C. E. Shannon, «Communication theory of secrecy systems», *Bell System Technical Journal*, vol. (28): pp. 656-715, 1949.

[71] P. W. Shor. «Algorithms for quantum computation. Discrete logarithms and factoring», in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp.124-134, *IEEE Computer Society Press*, 1994.

[72] P. W. Shor et J. Preskill, «Simple proof of security of the BB84 quantum key distribution protocol», *Physical Review Letters*, vol. (85): pp. 441-444, 2000

[73] R. W. Spekkens et T. Rudolph, «Degrees of concealment and bindingness in quantum bit commitment protocols», *Physical Review A*, vol. (65), no. (012310), 2002.

[74] R. W. Spekkens et T. Rudolph, «Quantum protocol for cheat-sensitive weak coin flipping», *Physical Review Letters*, vol. (89), no. (227901), 2002.

[75] A. Uhlmann, «The "transition probability" in the state space of *-algebra.» *Reports on Mathematical Physics*, vol. (9) : pp. 273-279, 1976.

[76] G. S. Vernam, «Cypher printing telegraph system for secret wire and radio telegraphic communications», *Journal of American Institute.of Electrical Engineers*, vol. (55) : pp. 109-115, 1926.

[77] S. Wiesner, «Conjugate coding», *Sigact News*, vol. (15), no. (1) : pp. 78-88, 1983, (Manuscrit original écrit en 1970).

[78] W. Wootters et W. Zurek, «A single quantum cannot be cloned», *Nature*, vol. (299) : pp. 802-803, 1982.