Université de Montréal

Variations sur la transmission inconsciente en cryptographie quantique

par

Louis Salvail

Département d'Informatique et de Recherche Opérationnelle
Faculté des Arts et des Sciences

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de
Philosophiæ Doctor (Ph.D.)
en Informatique

Janvier 1996

Université de Montréal

Faculté des études supérieures

Cette thèse intitulée

Variations sur la transmission inconsciente en cryptographie quantique

présenté par:

Louis Salvail

a été évalué par un jury composé des personnes suivantes:

Thèse acceptée le: ____________________

Sommaire

Cette thèse s'articule autour de la primitive de transmission inconsciente en cryptographie quantique. Cette primitive permet à un envoyeur de transmettre deux chaînes de bits, q_0 et q_1, de façon à ce que le receveur puisse décider de recevoir q_c pour $c \in \{0, 1\}$ sans obtenir d'information sur q_{1-c}. À la fin de la transmission, l'envoyeur n'a pas d'information sur c. La transmission inconsciente permet la réalisation sécuritaire de l'ensemble des tâches cryptographiques à deux participants qui ne se font pas confiance. Il s'agit d'une primitive très importante qui peut être réalisée sur le canal quantique par le protocole BBCS de Bennett, Brassard, Crépeau et Skubiszewska [13].

En premier lieu, nous analysons la sécurité du protocole BBCS contre un receveur restreint à effectuer des mesures sur des photons individuels. Nous déterminons la longueur des chaînes q_0 et q_1 qui peuvent être transmises sécuritairement étant donné un facteur de sécurité n et un taux d'erreurs de transmission $p > 0$. Nous faisons aussi l'hypothèse de l'existence d'un protocole de mise en gage parfait.

En second lieu, nous nous intéressons au problème d'identification quantique. Cette tâche cryptographique permet à deux usagers, $\mathcal{A}$lice et $\mathcal{B}$ob, de vérifier qu'ils partagent un secret commun sans le dévoiler. Nous présentons un protocole simple qui, pour être sécuritaire, doit faire appel à une famille de codes correcteurs d'erreurs aux propriétés biens définies. Aucune famille de codes connue ne possède simultanément toutes les propriétés. Nous utiliserons la transmission inconsciente pour relaxer certaines contraintes sur la famille de codes recherchée. Notre solution finale est plus efficace, en terme du nombre d'appels à la transmission inconsciente, que celle déjà proposée par Fagin, Naor et Winkler [37].

Finalement, nous montrons qu'une variation du protocole de mise en gage de [21] est sécuritaire contre les attaques limitées aux mesures individuelles. Cette variation, appelée BCJL renversé, peut être utilisées comme primitive de mise en gage pour le protocole BBCS.

Mots clés: Cryptographie quantique, transmission inconsciente, identification, mise en gage.

Table des matières

Table des figures

Introduction

La cryptographie étudie les façons de réaliser des tâches interactives en protégeant l'information confidentielle des acteurs contre des participants malhonnêtes. Le scénario le plus connu est probablement celui où $\mathcal{A}$lice désire envoyer un message secret à $\mathcal{B}$ob. Un protocole qui permet la réalisation de cette tâche devra protéger $\mathcal{A}$lice contre un intrus, Eve, qui se substituerait au destinataire légitime $\mathcal{B}$ob; c'est-à-dire que, si Eve reçoit le message chiffré (le cryptogramme) à la place de $\mathcal{B}$ob, celle-ci sera dans l'incapacité d'en tirer quoi que ce soit. Il est bien connu que pour y parvenir parfaitement, $\mathcal{A}$lice et $\mathcal{B}$ob doivent au préalable partager une clef secrète aléatoire aussi longue que le message [63]. Le problème reste entier car pour échanger un message secret, $\mathcal{A}$lice et $\mathcal{B}$ob doivent s'entendre au préalable sur une clef secrète aléatoire pour chaque message à transmettre. Cette approche est impraticable dans la plupart des scénarios. Une alternative a été proposée par Diffie et Hellman [33] au milieu des années '70. L'idée consiste à remplacer la sécurité parfaite par le concept de sécurité calculatoire. C'est-à-dire que même si le cryptogramme contient toute l'information au sens de Shannon sur le message clair, Eve devra travailler pendant beaucoup trop longtemps pour cryptanalyser le cryptogramme, tandis que le receveur légitime pourra récupérer facilement le message clair. Les systèmes fonctionnant sous ce principe sont appelés cryptosystèmes à sécurité calculatoire, ils ont l'avantage de pouvoir être réalisés sans que les usagers légitimes n'aient à échanger de clefs secrètes. Cependant pour être sécuritaires, les cryptosystèmes à sécurité calculatoire doivent s'appuyer sur des hypothèses non prouvées de la théorie de la complexité du calcul. Les cryptosystèmes de Diffie et Hellman [33], de Rivest, Shamir et Adelmann [61] et tous les autres de même nature (par exemple celui de El-Gamal [34]) requièrent l'existence de *fonctions à brèche secrète* pour être réalisés sécuritairement. Ces fonctions sont faciles à évaluer mais impossibles à inverser en temps raisonnable, à moins de disposer d'une information secrète; seul le receveur légitime possède cette information, ce qui lui permet de retrouver efficacement le message clair. Cependant si $\mathbf{P} = \mathbf{NP}$, les fonctions à trappes n'existent pas et même, elles peuvent ne pas exister dans le cas contraire. Par exemple, les cryptosystèmes [33] et [61] fondent leur sécurité sur l'impossibilité pratique de factoriser des nombres composés du produit de deux grands nombres premiers. Récemment, Peter Shor [64] a montré qu'il était possible de factoriser efficacement sur l'ordinateur quantique, quoique le jour n'est pas venu où de tels ordinateurs seront en opération; en principe ces cryptosystèmes peuvent être brisés.

Dans cette thèse notre intérêt portera surtout sur les tâches cryptographiques à deux participants. Supposons qu'$\mathcal{A}$lice et $\mathcal{B}$ob, qui ne se font pas confiance, ont chacun un secret. Soit $a \in A$ et $b \in B$ les secrets d'$\mathcal{A}$lice et $\mathcal{B}$ob respectivement, le scénario est le suivant: $\mathcal{A}$lice et $\mathcal{B}$ob veulent connaître $f(a, b)$ sans dévoiler d'autre information sur a et b que ce que $f(a, b)$ divulgue. Il s'agit de la formulation générale de l'ensemble des problèmes cryptographiques à deux participants que l'on nomme *évaluation de fonctions à l'aveugle*. Par exemple, si a et b désignent les comptes en banque d'$\mathcal{A}$lice et $\mathcal{B}$ob, la fonction $f(a, b) := (a \leq b)$ permet de déterminer lequel des deux participants est le moins pauvre sans qu'ils aient à dévoiler le montant dont ils disposent. Un autre exemple, dont il sera question au chapitre 3, consiste à poser $f(a, b) := (a = b)$; cette fonction permet à $\mathcal{A}$lice de s'identifier à $\mathcal{B}$ob en vérifiant qu'ils possèdent des secrets identiques sans les dévoiler.

Le problème d'évaluation de fonctions à l'aveugle a été largement étudié notamment par [49, 24]. J. Kilian [49] a montré l'équivalence entre une solution à ce problème et l'existence d'un canal de transmission inconsciente. Ce canal a la propriété de transmettre l'information de façon équivoque. La version originale de Rabin [59] permet à $\mathcal{A}$lice de transmettre un bit $b \in \{0, 1\}$ que $\mathcal{B}$ob recevra avec probabilité $\frac{1}{2}$; de plus, $\mathcal{B}$ob est le seul à savoir s'il a récupéré b. Le canal *multiplexé* de Wiesner [69] permet à $\mathcal{A}$lice de transmettre deux messages q_0 et q_1 de façon telle que $\mathcal{B}$ob puisse choisir de recevoir q_c, pour $c \in \{0, 1\}$. À la fin de la transmission, $\mathcal{A}$lice ne possède aucune information sur c et $\mathcal{B}$ob aucune information sur q_{1-c} . Ces deux versions, et d'autres de même nature, sont tous cryptographiquement équivalentes [23, 29].

En cryptographie calculatoire, un canal de transmission inconsciente existe si et seulement si des fonctions à trappes existent [46]. Autrement dit, les fonctions à trappes sont nécessaires et suffisantes pour l'évaluation de fonctions à l'aveugle dans ce modèle.

Les principes généraux de la mécanique quantique permettent de réaliser une transmission inconsciente faible (ou transmission équivoque) en utilisant la polarisation des photons pour encoder l'information. D'une façon très superficielle, la polarisation d'un photon peut être vue comme l'angle du plan dans lequel il oscille perpendiculairement à sa direction de propagation. En général, il est impossible de mesurer exactement la polarisation des systèmes quantiques. Cependant, Il est possible de le faire si l'observateur sait que le photon est polarisé dans l'une ou l'autre de deux directions orthogonales. Autrement, une même mesure répétée sur des copies de la particule à observer ne donnerait pas nécessairement le même résultat. Le codage BB84 [6] utilise avantageusement cette propriété pour que la transmission d'un bit classique d'information soit rendue intrinsèquement équivoque.

Des tâches plus intéressantes peuvent être construites en utilisant le codage BB84 comme primitive de base pour les protocoles quantiques. Le protocole de Bennett, Brassard, Crépeau et Skubizewska [13] (que nous désignerons par la suite par BBCS) utilise justement ce codage pour réaliser une transmission inconsciente. De la même façon qu'en cryptographie basée sur la complexité du calcul, un protocole sécuritaire pour la transmission inconsciente qui soit composable permet de réaliser l'évaluation de circuits à l'aveugle dans le modèle quantique.

La transmission inconsciente est l'outil fondamental pour la réalisation des protocoles cryptographiques à deux participants. Ces protocoles sont particulièrement intéressants parce qu'ils peuvent être utilisés sur de très courtes distances. D'autre part, plus le canal quantique est long plus la transmission est difficile. Les états quantiques ont tendance à évoluer de façon imprévisible lorsqu'ils ne sont pas isolés du monde extérieur. Certaines tâches cryptographiques, comme la distribution de clefs secrètes [8], doivent pouvoir être réalisées sur de longues distances pour être utiles.

Ce n'est pas le cas pour d'autres tâches comme l'identification qui permet à $\mathcal{A}$lice de se convaincre que $\mathcal{B}$ob est bien son interlocuteur; les guichets bancaires automatisés se comportent de la même façon lorsqu'un client veut avoir accès à son compte en banque. Dans le scénario habituel, la distance entre le guichet et le client n'est que de quelques centimètres.

Nous nous intéressons principalement au protocole de transmission inconsciente BBCS. Nous analysons sa sécurité sous l'hypothèse que les mesures d'un opposant au protocole sont limitées à une classe particulière; mais cette classe est plus générale que celle déjà considérée dans [13] et [25]. Nous nous intéressons ensuite au problème d'identification sur un canal quantique et montrons comment la transmission inconsciente peut aider à sa solution. Nous terminons par l'analyse de la securité contre les mesures individuelles d'une variante du protocole de mise en gage de Brassard, Crépeau, Josza et Langlois appelé BCJL [21] (nous dénoterons le protocole de [21] par BCJL tandis que la variante que nous considérons sera dénoté BCJL *renversé*).

Plan de la thèse

Le premier chapitre est une revue des principes de la mécanique quantique nécessaires à la compréhension des chapitres subséquents. Nous y abordons les principes élémentaires de représentation des états des systèmes quantiques. Nous montrons comment représenter l'état de polarisation d'un photon à l'aide d'un espace d'Hilbert à deux dimensions. Ensuite, nous verrons comment la polarisation peut servir à coder de l'information d'une façon intrinsèquement équivoque via le codage BB84. Par la suite, nous nous intéresserons à la représentation des systèmes composés de plusieurs particules; nous verrons que ces particules peuvent être dans un état tel qu'elles semblent se parler à distance. Nous terminons ce chapitre en présentant le modèle OCPS, introduit par D. Mayers [51], pour la représentation générale des mesures admises par la mécanique quantique. Ce modèle sera utilisé au chapitre 2 pour l'analyse de la sécurité du protocole BBCS et au chapitre 4 pour celle d'une variante du protocole de mise en gage de Brassard, Crépeau, Josza et Langlois (noté BCJL).

Le chapitre 2 traite du protocole de transmission inconsciente BBCS. Nous débutons en revisant les propriétés qu'un protocole de transmission inconsciente doit avoir pour être sécuritaire. Nous voyons comment le protocole BBCS permet la transmission inconsciente en plusieurs saveurs. Nous montrons finalement, et c'est là notre contribution, que si le receveur, $\mathcal{B}$ob, est limité à faire des mesures sur des photons individuels, le protocole BBCS est sécuritaire même pour la saveur la plus générale. Nous faisons aussi l'hypothèse de l'existence d'un protocole de mise en gage parfait. Subséquemment, A. C. Yao [71] a obtenu un résultat plus général en montrant que la saveur la plus simple du protocole BBCS (dûe à [23]) est sécuritaire contre toutes les mesures permises par la mécanique quantique mais aussi sous l'hypothèse de l'existence d'un protocole parfait pour la mise en gage. Nous discutons, à la fin du chapitre, de la possibilité d'étendre notre résultat à cette classe plus générale de mesures.

Au chapitre 3, nous laissons de côté les considérations théoriques de la transmission inconsciente pour nous pencher sur un problème pratique. Nous nous intéressons à la réalisation dans le modèle quantique d'un protocole efficace pour le problème d'identification. Nous débutons en présentant un protocole simple qui ne peut pas être réalisé sécuritairement à moins qu'il existe une famille de codes aux propriétés bien définies. Puisque nous ne connaissons aucune famille de codes avec ces propriétés, nous utiliserons la transmission inconsciente quantique pour que certaines de ces propriétés ne soient plus nécessaires. La solution obtenue est plus efficace en terme du nombre de transmissions inconscientes que les autres solutions connues. Nous discuterons aussi de l'opportunité de réaliser pratiquement le protocole proposé. Nous verrons que la technologie nécessaire peut être implantée sur une carte à puces sans grandes difficultés comme décrit dans [43].

Au chapitre 4, nous analysons la sécurité contre les mesures individuelles d'une variation du protocole BCJL [21]. L'hypothèse, faite au chapitre 2, de l'existence d'un protocole parfait pour la mise en gage est donc levée. La sécurité de BBCS semble donc être garantie contre tous les attaquants qui sont limités à des mesures individuelles. Pour en obtenir la preuve formelle il faudra aussi montrer que BCJL renversé et BBCS sont composables ce qui est probablement vrai. De plus, un résultat récent de D. Mayers [53] montre qu'une mise en gage quantique parfaite est impossible. Puisque la transmission inconsciente permet d'obtenir une mise en gage, aucun protocole quantique parfait pour la transmission inconsciente qui soit sécuritaire contre les mesures cohérentes ne peut exister.

Chapitre 1

Représentation du monde quantique

1.1 Introduction

Nous présentons les concepts fondamentaux empruntés à la mécanique quantique qui sont nécessaires à la bonne compréhension de la démarche. En cryptographie quantique on encode l'information dans l'état de polarisation d'un photon comme en physique classique on représente les états d'un système par des vecteurs. En mécanique quantique, un espace d'Hilbert aux composantes complexes permet de représenter la polarisation. Les opérateurs linéaires servent à modéliser l'évolution d'un système dans le temps et les mesures qui peuvent être effectuées. Aux sections 1.2, 1.3 et 1.4 nous revisons la classe des opérateurs Hermitiens, importante dans la modélisation du processus de mesure.

Les sections 1.5, 1.6, 1.7 et 1.8 traitent du codage et du décodage de l'information quantique. Après avoir défini un observable, nous décrivons le codage BB84 et discutons de ces propriétés cryptographiques. Nous verrons ensuite que la mécanique quantique fournit un formalisme capable d'exprimer aussi bien les états purs d'un système qu'une distribution de probabilité sur ces états.

À la section 1.9, nous verrons comment les systèmes à plusieurs particules sont représentés. Nous verrons que des systèmes composés ont des propriétés étranges. Les composantes de ces systèmes peuvent être enchevêtrées et donner l'impression qu'elles communiquent entre elles instantanément peu importe la distance; observer une des composantes fixe immédiatement l'autre.

Nous terminons ce chapitre par la description des mesures généralisées sur des systèmes quantiques. Nous abordons deux modèles qui permettent d'analyser le comportement des systèmes observés lorsque les mesures sont effectuées par étapes. Le modèle MOP est celui qui est habituellement adopté en mécanique quantique et certaines limitations peuvent être évitées par l'adoption d'un modèle alternatif développé par D. Mayers. Ce modèle sera utilisé au chapitre 2 pour analyser la sécurité du protocole BBCS contre la classe des mesures faites sur des photons individuels et au chapitre 4 pour l'analyse de la sécurité d'une variation du protocole de mise en gage de Brassard, Crépeau, Josza et Skubiszewska [21] (appelé protocole BCJL).

1.2 Les opérateurs

Les opérateurs linéaires sur un espace vectoriel modélisent les mesures et l'évolution dans le temps d'un système quantique dont l'état peut être représenté par un vecteur dans cet espace.

Définition 1 *Un opérateur linéaire A sur un espace vectoriel $\mathcal{H}$ défini sur un corps $\mathcal{C}$ est une fonction $A : \mathcal{H} \rightarrow \mathcal{H}$ telle que pour tout $\mathbf{u}, \mathbf{v} \in \mathcal{H}$,*

1. $A(\mathbf{u} + \mathbf{v}) = A(\mathbf{u}) + A(\mathbf{v})$
2. $A(c\mathbf{v}) = cA(\mathbf{v})$ *pour* $c \in \mathcal{C}$.

Chaque opérateur linéaire peut être représenté par une matrice $l \times l$ d'éléments des complexes $\mathcal{C}$, où l la dimension de $\mathcal{H}$.

Une importante classe d'opérateurs en mécanique quantique est celle des opérateurs de projection. Par exemple, l'opérateur de projection P_x qui projette un vecteur $\mathbf{v} \in \mathcal{R}^2$ (la limitation aux réels sera relaxées à la section suivante) sur l'axe des x est défini par

$$P_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Si P_x est appliqué à $\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathcal{R}^2$ on a bien que

$$P_x\mathbf{v} = \begin{pmatrix} a \\ 0 \end{pmatrix}.$$

Les projections P_y et P_z, si $\mathbf{v} \in \mathcal{R}^3$, peuvent être définies de façon similaire. En général, l'opérateur P_θ qui projette tout vecteur $\mathbf{v} \in \mathcal{R}^2$ sur le rayon à angle θ avec l'axe des x est

$$P_\theta = \begin{pmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{pmatrix}.$$

Comme nous le verrons par la suite, ces opérateurs modélisent un type important de mesures largement utilisées en cryptographie quantique.

D'autres opérateurs modélisent davantage l'évolution d'un système quantique. Les opérateurs de rotation sont de ceux-là. L'opérateur R_θ fait tourner le vecteur $\mathbf{v}$ d'un angle θ, dans $\mathcal{R}^2$,

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Remarquons que le produit de deux opérateurs est aussi un opérateur; il est défini par la composition de deux opérations effectuées l'une à la suite de l'autre. Par exemple, $P_{\theta'}R_\theta\mathbf{v}$ est l'opérateur qui commence par effectuer une rotation d'un angle θ sur $\mathbf{v}$ suivi de la projection du vecteur résultant sur le rayon à angle θ' avec l'axe des x.

Définition 2 *Deux opérateurs A et B* commutent *si $AB = BA$.*

Notons en général que pour θ et θ', $P_{\theta'}$ et R_θ ne commutent pas. Cependant, $R_0 = \mathbf{I}$, l'opérateur nul représenté par la matrice identité, commute certainement avec n'importe quel autre opérateur. Dans ce cas particulier $P_{\theta'}R_0\mathbf{v} = P_{\theta'}\mathbf{I}\mathbf{v} = P_{\theta'}\mathbf{v} = \mathbf{I}P_{\theta'}\mathbf{v}$ donc $P_{\theta'}$ et R_0 commutent. En général, deux opérateurs de rotation commutent toujours.

Certains opérateurs, qui sont une généralisation des opérateurs de projection, sont caractérisés par leurs valeurs propres.

Définition 3 *Le vecteur $\mathbf{v} \neq \mathbf{0}$ est un* vecteur propre *de l'opérateur A si $A\mathbf{v} = a\mathbf{v}$ pour un scalaire a. On dit alors que le vecteur propre $\mathbf{v}$ a une* valeur propre *a.*

Un opérateur A admet une valeur propre si lorsqu'appliqué à un vecteur $\mathbf{v}$, le vecteur résultant demeure sur le même rayon que $\mathbf{v}$. Les opérateurs de rotation R_θ pour

$\theta \notin \{0, \pi\}$ n'admettent pas de valeur propre. Les opérateurs de projection P_θ, par contre, ont des valeurs propres car tous les vecteurs $\mathbf{v}$ à angle θ avec l'axe des x sont tels que $P_\theta \mathbf{v} = \mathbf{v}$. De plus, tous les vecteurs $\mathbf{v}'$ à angle $\theta' = \theta + \frac{\pi}{2}$ sont tels que $P_\theta \mathbf{v}' = 0$. L'opérateur P_θ a donc les deux valeurs propres $\{0, 1\}$. Les opérateurs qui admettent deux valeurs propres sur des rayons perpendiculaires sont symétriques.

Définition 4 *Un opérateur linéaire A sur $\mathcal{R}^2$ est symétrique si la matrice qui le représente est telle que ses éléments en-haut à droite et en-bas à gauche sont égaux.*

Remarquons que R_θ n'est pas symétrique à moins que $\theta \in \{0, \pi\}$. Les opérateurs symétriques ont la propriété d'être décomposables par des projections orthogonales.

Théorème 1 (Décomposition spectrale.) *Si A est un opérateur symétrique sur $\mathcal{R}^2$ avec valeurs propres a_1 et a_2 alors il existe deux projections orthogonales P_1 et P_2 avec*

$$A = a_1 P_1 + a_2 P_2.$$

Lorsque $a_1 \neq a_2$ la décomposition est unique. Par contre, si $a_1 = a_2$ tous les vecteurs de $\mathcal{R}^2$ sont des vecteurs propres de A. Ainsi quelle que soit la paire de projections orthogonales P_1 et P_2, on a que $A = a_1(P_1 + P_2)$.

1.3 Espaces vectoriels

Les opérateurs qui servent à modéliser les mesures sur des systèmes quantiques sont une généralisations des opérateurs symétriques. Les opérateurs *Hermitien* permettent de traiter les vecteurs d'états aux composantes complexes. Voyons comment.

En premier lieu introduisons la notation de Dirac. Soit $\mathbf{u} = (u_1, \ldots, u_n)$ et $\mathbf{v} = (v_1, \ldots, v_n)$ des vecteurs aux composantes complexes. La notation

$$|\mathbf{u}\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

est appelée le *ket* de $\mathbf{u}$.

Rappelons que pour un nombre complexe $c = a + bi$ avec $a, b \in \mathcal{R}$, c^* dénote le conjugué complexe de c défini comme $c^* = a - bi$. Si $\mathbf{u}$ est un vecteur complexe, on note

$\mathbf{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$ le vecteur dont les composantes sont les conjugués complexes de celles de $\mathbf{u}$. La notation

$$\langle \mathbf{u}| = (|u\rangle^{\mathrm{T}})^*$$

où $|u\rangle^{\mathrm{T}}$ est la transposé de $|u\rangle$, est appelée le *bra* de $\mathbf{u}$.

Le produit scalaire entre $\mathbf{u}$ et $\mathbf{v}$ est noté $\langle \mathbf{u}|\mathbf{v}\rangle$ et défini comme

$$\langle \mathbf{u}|\mathbf{v}\rangle = \sum_{i=1}^{n} u_i^* v_i$$

La norme d'un vecteur $\mathbf{u}$ est $\|\mathbf{u}\| = \langle \mathbf{u}|\mathbf{u}\rangle$ et

Définition 5 *Un vecteur* $\mathbf{u}$ *est normalisé si* $\sqrt{\langle \mathbf{u}|\mathbf{u}\rangle} = \|\mathbf{u}\| = 1$.

Rappelons la relation bien connue $\langle \mathbf{u}|\mathbf{v}\rangle = |\mathbf{u}||\mathbf{v}|\cos\theta$ où θ est l'angle entre $\mathbf{u}$ et $\mathbf{v}$. Si $\mathbf{u}$ et $\mathbf{v}$ sont normalisés on a que $\langle \mathbf{u}|\mathbf{v}\rangle = \cos\theta$. Deux vecteurs $\mathbf{u}$ et $\mathbf{v}$ sont orthogonaux si $\langle \mathbf{u}|\mathbf{v}\rangle = 0$. Pour l'opérateur de projection P_θ on a que

$$\langle \mathbf{v}|P_\theta \mathbf{v}\rangle = |P_\theta \mathbf{v}|^2 = \langle P_\theta \mathbf{v}|P_\theta \mathbf{v}\rangle = \cos^2\theta$$

où θ est l'angle entre $\mathbf{v}$ et le rayon sur lequel P_θ projette. Nous verrons à la section 1.6 que cette équation donne la probabilité d'observer le *résultat* P_θ lorsque la mesure est modélisée par des projections (les mesures de Von Neuman). Pour permettre l'interprétation probabiliste, les vecteurs d'états doivent être normalisés. Comme nous le verrons plus loin, la propriété de polarisation d'un photon s'exprime par une paire de nombres complexes.

Une autre propriété du produit scalaire est donnée par

$$\langle \mathbf{u}|\mathbf{v}\rangle = \langle \mathbf{v}|\mathbf{u}\rangle^*.$$

D'où les identités suivantes:

1. $\sqrt{\langle \mathbf{v}|\mathbf{v}\rangle} = |\mathbf{v}| \in \mathcal{R}$,
2. $\langle \mathbf{v}|P\mathbf{v}\rangle = |P\mathbf{v}|^2 = \langle P\mathbf{v}|P\mathbf{v}\rangle$.

Dans le corps des complexes, un opérateur Hermitien est l'équivalent d'un opérateur symétrique pour les réels.

Définition 6 *Un opérateur A est* Hermitien *sur $\mathcal{C}^2$ si les éléments en haut à droite et en bas à gauche de A sont conjugués l'un de l'autre.*

Comme dans le cas d'un opérateur symétrique, un opérateur Hermitien admet une décomposition spectrale.

Théorème 2 (Décomposition spectrale) *Soit A un opérateur Hermitien avec deux valeurs propres a_1 et a_2 telles que $a_1 \neq a_2$. L'opérateur peut être exprimé par*

$$A = a_1 P_1 + a_2 P_2$$

où P_1 et P_2 projettent sur les rayons orthogonaux correspondant aux vecteurs propres $\mathbf{v}_1$ et $\mathbf{v}_2$ avec valeurs propres respectives a_1 et a_2.

1.4 Projection dans un sous-espace

Au lieu de projeter sur un rayon, un opérateur de projection pourrait aussi projeter dans un sous-espace de dimension plus grande. Par exemple, si l'espace est de dimension 3, n'importe quel plan peut servir à projeter un vecteur. Pour généraliser les projections à des sous-espaces de dimension quelconque, il faut définir un produit scalaire. Pour tout $\mathbf{u}, \mathbf{v} \in \mathcal{H}$ le produit scalaire $\langle \mathbf{u} | \mathbf{v} \rangle \in \mathcal{R}$ doit avoir les propriétés suivantes:

1. $\langle \mathbf{u} | \mathbf{u} \rangle \geq 0$ et $\langle \mathbf{u} | \mathbf{u} \rangle = 0$ ssi $\mathbf{u} = \mathbf{0}$
2. $\langle \mathbf{u} | \mathbf{v} \rangle = \langle \mathbf{v} | \mathbf{u} \rangle^*$
3. $\langle \mathbf{u} | a\mathbf{v} \rangle = a \langle \mathbf{u} | \mathbf{v} \rangle$
4. $\langle \mathbf{u} | \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u} | \mathbf{v} \rangle + \langle \mathbf{u} | \mathbf{w} \rangle$.

De plus, V est un sous-espace de $\mathcal{H}$ (noté $V \subseteq \mathcal{H}$) si

1. si $\mathbf{u} \in V$ et $\mathbf{v} \in V$ alors $\mathbf{u} + \mathbf{v} \in V$.
2. si $\mathbf{u} \in V$ alors pour tout scalaire $a, a\mathbf{u} \in V$.

Définition 7 *Un opérateur A sur $\mathcal{H}$ est* Hermitien *s'il est linéaire et pour tout $\mathbf{u}, \mathbf{v} \in \mathcal{H}$,*

$$\langle \mathbf{u} | A\mathbf{v} \rangle = \langle A\mathbf{u} | \mathbf{v} \rangle.$$

L'idempotence d'un opérateur permettra de généraliser la notion de projection.

Définition 8 *A est idempotente si $AA = A$.*

Définition 9 *Un opérateur A sur un espace $\mathcal{H}$ est une projection si*

1. *A est Hermitienne*

2. *A est idempotente.*

La relation $\langle \mathbf{v} | P\mathbf{v} \rangle = \langle P\mathbf{v} | \mathbf{v} \rangle$ est observée lorsque P est une projection au sens de la définition 9.

Si A est un opérateur Hermitien sur $\mathcal{H}$ de dimension finie l, il existe des valeurs $a_1, a_2, \ldots, a_m$ avec $m \leq l$ ainsi que des projections $P_1, \ldots, P_m$ sur des espaces mutuellement orthogonaux avec

$$A = \sum_{i=1}^{m} a_i P_i.$$

Si les a_i sont tous différents alors la décomposition est unique et $\{a_1, \ldots, a_m\}$ est l'ensemble des valeurs propres de A. Il s'agit de la généralisation du théorème de décomposition spectrale pour un nombre de dimensions arbitraires.

1.5 Bases orthonormées

Un ensemble de vecteurs indépendants $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ est une base de l'espace $\mathcal{H}$ si tout vecteur $\mathbf{v} \in \mathcal{H}$ peut être exprimé comme

$$\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{v}_i$$

pour a_i des scalaires.

Définition 10 *Une base $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ est* orthonormée *si*

1. *pour tout $\mathbf{v}_i, \mathbf{v}_j \in B$ tels que $\mathbf{v}_i \neq \mathbf{v}_j, \langle \mathbf{v}_i | \mathbf{v}_j \rangle = 0$*

2. *pour tout $\mathbf{v}_i \in B, |\mathbf{v}_i| = \langle \mathbf{v}_i | \mathbf{v}_i \rangle = 1.$*

Par la suite, nous utiliserons des bases orthonormées particulières sur un espace de dimension 2. Voici quelques exemples:

- La base rectilinéaire $+ = \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\} = \{|\rightarrow\rangle, |\uparrow\rangle\}$.
- La base diagonale $\times = \{\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}\} = \{|\nearrow\rangle, |\nwarrow\rangle\}$.
- La base de Breidbart $\mathbf{b} = \{\begin{pmatrix} \cos\frac{\pi}{8} \\ \sin\frac{\pi}{8} \end{pmatrix}, \begin{pmatrix} \cos\frac{5\pi}{8} \\ \sin\frac{5\pi}{8} \end{pmatrix}\}$.
- La base circulaire $\bigcirc = \{\begin{pmatrix} \frac{-i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}\} = \{|\hookrightarrow\rangle, |\hookleftarrow\rangle\}$.

1.6 Les observables

Lorsqu'un système physique doit être mesuré pour en extraire de l'information, un opérateur Hermitien doit être défini. Un tel opérateur détermine les résutats possibles ainsi que les probabilités qu'ils se produisent étant donné le système observé.

Soit $\mathcal{H}$ l'espace d'Hilbert et le vecteur d'état normalisé $\mathbf{v}$ du système à observer Ψ. Un observable $\mathcal{O}$ est un opérateur Hermitien $\mathcal{O} : \mathcal{H} \rightarrow \mathcal{H}$. Supposons pour le moment que $\mathcal{O}$ possède des valeurs propres distinctes. Soit $P = \{p_1, p_2, \ldots, p_l\}$ l'ensemble des valeurs propres de $\mathcal{O}$ et $L = \{L_1, L_2, \ldots, L_l\}$ l'ensemble des rayons associés aux valeurs propres dans P. Puisque $\mathcal{O}$ est Hermitien, les rayons dans L sont deux à deux othogonaux. Les résultats de l'observable $\mathcal{O}$ sont en bijection avec les éléments de P et de L. Le résultat p_j est obtenu avec certitude seulement si l'état $\mathbf{v}$ de Ψ coïncide avec le rayon L_j. Si le vecteur d'état $\mathbf{v}$ ne coïncide avec aucun rayon dans L, le résultat de la mesure ne peut être prédit avec certitude. Soit P_j l'opérateur de projection sur le rayon L_j, la probabilité $p_{\mathbf{v}}(j)$ d'obtenir le résultat p_j est

$$p_{\mathbf{v}}(j) = \langle \mathbf{v} | P_j \mathbf{v} \rangle = |P_j \mathbf{v}|^2. \tag{1.1}$$

Une fois le résultat j obtenu, le système initial se retrouve dans l'état normalisé $\mathbf{u}$ qui correspond au rayon L_j (un vecteur propre associé a la valeur propre p_j). Remarquons que ce vecteur n'est pas uniquement défini. Par exemple si $\mathbf{u}$ est un état final possible, le vecteur $-\mathbf{u}$ est aussi possible. Ceci est sans conséquence car tous les vecteurs unitaires qui coïncident avec le même rayon sont indistinguables et représentent le même état physique.

1.7 Polarisation et codage de l'information

En cryptographie quantique, nous nous intéressons aux observables possibles à propos de la polarisation d'un photon. Cette quantité physique est représentée par un vecteur normalisé dans l'espace d'Hilbert de dimension 2 noté $\mathcal{H}_2$. Un observable de cette quantité est représenté par un opérateur Hermitien sur $\mathcal{H}_2$. Qu'il s'agisse de représenter la polarisation d'un photon ou le spin d'un fermion, nous pouvons interpréter géométriquement l'état d'une particule. Une paire de coordonnées complexes sur la surface d'une sphère de rayon 1 peut être représentée par deux angles $\alpha = (\phi, \theta)$ avec $\phi \in [0, \pi]$ et $\theta \in [0, \pi]$. Le vecteur d'état $\mathbf{v}_{(\phi,\theta)}$ de la polarisation d'un photon est déterminé par l'angle de latitude ϕ et l'angle de longitude θ partant du centre de la sphère jusqu'à sa surface. Pour le moment restreignons-nous à des directions de la polarisation qui peuvent être représentées par un couple de nombres réels; dans ce cas, l'angle θ suffit à la représentation.

En cryptographie quantique, on utilise la polarisation d'un photon pour transmettre un bit classique d'information via le canal quantique. Soit M_θ l'observable sur $\mathcal{H}_2$ défini pour $a_0 \neq a_1 \in \mathcal{R}$ par

$$M_\theta = a_0 P_\theta + a_1 P_{\theta+\frac{\pi}{2}}.$$

Si L_θ désigne le rayon sur lequel projette P_θ alors L_θ et $L_{\theta+\frac{\pi}{2}}$ déterminent les deux résultats possibles pour la mesure M_θ puisqu'ils définissent une bijection avec $\{a_0, a_1\}$. Si la polarisation $\mathbf{v}_\phi$ d'un photon ϕ est telle que $\mathbf{v}_\phi \in \{\theta, \theta + \frac{\pi}{2}\}$, l'observable M_θ mesurera $\mathbf{v}_\phi$ correctement. Le codage suivant permet de transmettre un bit $b \in \{0, 1\}$ par l'envoi du photon $\phi(b)$ polarisé comme

$$\mathbf{v}_{\phi(b)} = R_{\theta+b\cdot\frac{\pi}{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{1.2}$$

Pour $b = 0$, l'état de la polarisation du photon $\phi(0)$ est

$$\mathbf{v}_{\phi(0)} = R_\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (\cos\theta, \sin\theta).$$

Les probabilités d'obtenir les résultats L_θ et $L_{\theta+\frac{\pi}{2}}$ sont déterminées par l'équation 1.1,

$$\begin{aligned} p_{\mathbf{v}_{\phi(0)}}(0) &= \langle \mathbf{v}_{\phi(0)} | P_\theta \mathbf{v}_{\phi(0)} \rangle \\ &= \langle (\cos\theta, \sin\theta) | P_\theta (\cos\theta, \sin\theta) \rangle \\ &= |\mathbf{v}_{\phi(0)}|^2 \\ &= 1 \end{aligned}$$

et de la même façon,

$$p_{\mathbf{v}_{\phi(0)}}(1) = 0.$$

Par symétrie on a aussi que

$$p_{\mathbf{v}_{\phi(1)}}(0) = 0 \text{ et } p_{\mathbf{v}_{\phi(1)}}(1) = 1.$$

Ce codage n'a aucune application cryptographique puisqu'il permet à quiconque d'obtenir l'information codée à tout coup. Pour appliquer la transmission quantique à la cryptographie, il nous faut utiliser un codage équivoque qui cache une partie de l'information; le codage BB84 [6], à la base de presque tous les protocoles quantiques, est un codage équivoque. Le codage est ambigu parce qu'il ne spécifie pas uniquement l'angle θ. L'encodage d'un bit $b \in \{0, 1\}$ se fait à partir des deux angles $\theta = 0$ et $\theta = \frac{\pi}{4}$. Ainsi,

$$\mathbf{v}_{\phi(b)} = R_{\theta + b\frac{\pi}{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ pour } \begin{cases} \theta = 0 & \text{avec probabilité } \frac{1}{2} \\ \theta = \frac{\pi}{4} & \text{avec probabilité } \frac{1}{2}. \end{cases}$$

Lorsque $\theta = 0$, les deux états possibles sont

$$+ = \{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \} = \{ | \rightarrow \rangle, | \uparrow \rangle \}$$

et lorsque $\theta = \frac{\pi}{4}$,

$$\times = \{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \} = \{ | \nearrow \rangle, | \nwarrow \rangle \}.$$

Le codage BB84 est donc un choix aléatoire entre le codage 1.2 avec $\theta = 0$ et $\theta = \frac{\pi}{4}$. Pour cette raison nous dirons que l'encodage de b par un photon $\phi(b)$ dans l'état $\mathbf{v}_{\phi(b)}$ est dans la base rectilinéaire si $\theta = 0$ et diagonale si $\theta = \frac{\pi}{4}$. Notons $\mathbf{v}^{+}_{\phi(b)}$ et $\mathbf{v}^{\times}_{\phi(b)}$

l'encodage du bit b selon les bases rectilinéaire et diagonale respectivement. Voyons maintenant pourquoi le codage est équivoque.

Soit $\mathbf{v}^{+}_{\phi(b)}$ l'encodage de b dans la base rectilinéaire, la meilleure mesure pour b est M_0. De la même façon la meilleure mesure pour b encodé dans la base diagonale est $M_{\frac{\pi}{4}}$. Mais si M_0 est utilisé pour mesurer un bit b encodé dans la base diagonale, il s'agit de la pire mesure de b. Soit a_0 et a_1 les valeurs propres de M_0 qui indiquent aussi les deux résultats possibles de la mesure. La probabilité d'obtenir a_0 est donnée par l'équation 1.1,

$$\begin{aligned} p_{\mathbf{v}^{\times}_{\phi(b)}}(a_0) &= \langle \mathbf{v}^{\times}_{\phi(b)} | P_0 \mathbf{v}^{\times}_{\phi(b)} \rangle \\ &= \frac{1}{2} \\ &= p_{\mathbf{v}^{\times}_{\phi(b)}}(a_1) \end{aligned}$$

Par symétrie on a aussi que $M_{\frac{\pi}{4}}$ est la pire mesure pour b encodé dans la base rectilinéaire. Si c_0, c_1 sont les valeurs propres de $M_{\frac{\pi}{4}}$ alors on obtient que

$$p_{\mathbf{v}^{+}_{\phi(b)}}(c_0) = p_{\mathbf{v}^{+}_{\phi(b)}}(c_1) = \frac{1}{2}.$$

La classe des mesures $\{M_\theta\}_{-\pi \leq \theta \leq \pi}$ est particulièrement importante en cryptographie quantique. Lorsque le codage BB84 est utilisé, M_0 et $M_{\frac{\pi}{4}}$ sont les mesures que le receveur doit exécuter.

Définition 11 *Les opérateurs Hermitiens M_θ dans l'espace d'Hilbert à deux dimensions exprimables par $M_\theta = a_0 P_\theta + a_1 P_{\theta+\frac{\pi}{2}}$ avec $a_0 \neq a_1$ sont appelés* mesure de Von Neuman *sur cet espace. Ces mesures admettent deux résultats a_0 et a_1 correspondant à deux rayons orthogonaux.*

La mesure de Von Neumann qui maximise la probabilité d'obtenir le bon bit, peu importe que le codage soit rectilinéaire ou diagonal, est $M_{\frac{\pi}{8}}$ avec des rayons se situant à mi-chemin de ceux de M_0 et $M_{\frac{\pi}{4}}$. Cette mesure est appelée mesure de Breidbart parce que les deux rayons perpendiculaires qui représentent le résultat de la mesure sont les vecteurs de la base de Breidbart. L'équation 1.1 permet de déterminer la probabilité d'obtenir le bon bit pour la mesure de Breidbart. Soit b_0 et b_1 les valeurs propres de $M_{\frac{\pi}{8}}$, comme cette mesure est symétrique par rapport aux codages rectilinéaire et diagonal, les probabilités d'obtenir le bon bit sont les mêmes peu importe si le bit b est codé en rectilinéaire ou en diagonal. Ainsi,

$$\begin{aligned} p_{\mathbf{v}^+_{\pi(0)}}(b_0) &= \langle \mathbf{v}^+_{\pi(b)} | P_{\frac{\pi}{8}} \mathbf{v}^+_{\pi(b)} \rangle \\ &= \cos^2 \frac{\pi}{8} = p_{\mathbf{v}^+_{\pi(1)}}(b_1) = p_{\mathbf{v}^\times_{\pi(0)}}(b_0) = p_{\mathbf{v}^\times_{\pi(1)}}(b_1) \\ &\approx 0.85355. \end{aligned} \tag{1.3}$$

Peu importe le bit envoyé et la base de codage utilisée, la mesure de Breidbart donne toujours le bon bit avec probabilité $\cos^2 \frac{\pi}{8}$. Si le bit envoyé et la base utilisée sont aléatoires, le receveur maximisera la probabilité d'obtenir le bon bit en mesurant le photon reçu dans la base de Breidbart. De cette façon, le résultat de la mesure donnera toujours le bit avec probabilité environ 0.85. Noter la différence entre cette mesure et celle qui consiste à choisir de façon aléatoire entre les mesures M_0 et $M_{\frac{\pi}{4}}$. Dans ce dernier cas, si le codage coïncide avec la mesure choisie, le bit est obtenu avec certitude. Par contre, si la mauvaise mesure a été choisie, le bit obtenu est non-corrélé avec le bit envoyé. Les deux événements se produisant avec probabilité $\frac{1}{2}$, la probabilité d'obtenir le bon bit est $\frac{1}{2} + \frac{1}{4} = \frac{3}{4} < 0.85$. La géométrie de la famille $\{M_\theta\}_\theta$ implique que la probabilité d'obtenir le bon bit croît d'une façon continue pour $\theta \in [0, \frac{\pi}{8}]$ et atteint son maximum lorsque $\theta = \frac{\pi}{8}$. Il s'agit de la meilleure mesure de Von Neumann, même parmi celles qui sont représentées par des opérateurs complexes.

Le codage BB84 est fait de façon à ce que la mesure de Von Neuman qui maximise la probabilité d'obtenir le bon bit pour une base soit sans intérêt lorsque l'autre base a été utilisée. Cette propriété apparaît quand les bases possibles pour encoder le bit b font un angle $\frac{\pi}{4}$ entre elles. Soit $B_1 = \{\mathbf{b}_1, \mathbf{b}_1^\perp\}$ et $B_2 = \{\mathbf{b}_2, \mathbf{b}_2^\perp\}$ deux bases orthonormées possibles pour la transmssion d'un bit $b \in \{0,1\}$. Dans les espaces munis d'un produit scalaire, comme les espaces d'Hilbert, le codage BB84 est tel que $\forall \mathbf{b} \in B_1$ et $\forall \mathbf{b}' \in B_2$,

$$\langle \mathbf{b}' | P_b \mathbf{b}' \rangle = \cos^2 \frac{\pi}{4} = \frac{1}{2} \tag{1.4}$$

où P_b est l'opérateur de projection sur le rayon b. Cette dernière formulation a l'avantage d'être applicable aussi aux vecteurs à composantes complexes. Dans $\mathcal{R}^2$ on ne peut trouver plus de deux bases orthonormées qui simultanément observe la propriété 1.4. Mais dans $\mathcal{C}^2$ il est possible d'en trouver une troisième. La base circulaire

$\bigcirc$ satisfait l'équation 1.4 avec les bases rectilinéaires et diagonales. Le codage BB84 peut donc être étendu au choix d'une troisième base. Cependant un opérateur de rotation pour des vecteurs aux composantes complexes non nulles est nécessaire. La famille $\{R_\theta\}_\theta$ des opérateurs de rotation dans $\mathcal{R}^2$ peut être généralisée en ajoutant les opérateurs unitaires pour contenir aussi les rotations des vecteurs complexes.

Définition 12 *Un opérateur U est* unitaire *sur $\mathcal{H}$ s'il est linéaire, inversible et tel que pour tout $\mathbf{v} \in \mathcal{H}$, $|U\mathbf{v}| = |\mathbf{v}|$.*

La précédente définition formalise la notion intuitive de rotation. Celle-ci doit conserver la longueur des vecteurs qu'on y applique. De plus, s'il existe une rotation U, il doit exister une autre rotation qui permet de l'annuler. La définition 12 permet de se représenter une rotation dans un espace d'Hilbert de dimension finie quelconque. Pour le moment considérons l'espace d'Hilbert à deux dimensions exprimant l'état de polarisation linéaire d'un photon. Comme il a été mentionné au début de la présente section, les vecteurs normalisés dans $\mathcal{C}^2$ peuvent être représentés par la surface d'une sphère de rayon unitaire dans les réels. Une rotation U_α pour $\alpha = (\theta, \phi)$ appliquée au vecteur $\mathbf{v}$ le déplace d'un angle de latitude θ et d'un angle de longitude ϕ. Le codage étendu encode le bit $b \in \{0, 1\}$ par

$$\mathbf{v}_{\pi(b)} = U_{\alpha(b)} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{1.5}$$

où

$$\alpha(b) = \begin{cases} (0, b\frac{\pi}{2}) & \text{avec prob. } \frac{1}{3} \\ (0, \frac{\pi}{4} + b\frac{\pi}{2}) & \text{avec prob. } \frac{1}{3} \\ (\frac{\pi}{4}, b\frac{\pi}{2}) & \text{avec prob. } \frac{1}{3}. \end{cases}$$

Presque tous les protocoles cryptographiques utilisent le codage BB84 décrit à l'équation 1.2. Au chapitre 3 cependant, nous verrons un cas où le codage 1.5 est utile. Le protocole de camouflage quantique [21] est un autre exemple où le codage 1.5 apporte un gain d'efficacité. Par la suite, le codage BB84 référera au codage à deux bases de l'équation 1.2.

Pour faciliter la lecture, la notation suivante sera utilisée. Pour $b \in \{0, 1\}$ et $\theta \in \{0, \frac{\pi}{4}\}$, $|b\rangle_\theta$ dénote l'encodage du bit b dans la base θ. Plus précisément,

$$|b\rangle_\theta = R_{\theta + b\frac{\pi}{4}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

D'une façon équivalente nous écrirons

$$\begin{aligned}|b\rangle_{+} &= |b\rangle_{0} \text{ et}\\ |b\rangle_{\times} &= |b\rangle_{\frac{\pi}{4}}.\end{aligned}$$

1.8 États purs et états mixtes

En mécanique quantique, l'état d'un système est pur s'il peut être représenté par un vecteur normalisé dans l'espace d'Hilbert associé aux états possibles du sytème. Comme nous l'avons vu précédemment, les états $|\uparrow\rangle, |\downarrow\rangle, |\leftarrow\rangle, |\rightarrow\rangle, |\leftrightarrow\rangle$ et $|\hookrightarrow\rangle$ sont des états purs; chacun d'eux est représentés par un vecteur normalisé dans l'espace d'Hilbert à deux dimensions. Plus précisément,

Définition 13 *L'état de polarisation $|\Psi\rangle$ d'un photon est pur s'il existe une mesure de Von Neumann M_θ aux valeurs propres et résultats $\{m_0, m_1\}$ tels que pour $c \in \{0,1\}$*

$$P_\Psi(m_c) = 1 \textit{ et } P_\Psi(m_{1-c}) = 0$$

où $P_\Psi(m)$ représente la probabilité d'obtenir le résultat m lorsque le système initial est dans l'état $|\Psi\rangle$.

Ces conditions impliquent que m_0 et m_1 sont distincts et peuvent être vus comme deux valeurs propres correspondant à deux rayons orthogonaux de l'opérateur M_θ. La mesure M_θ est donc une mesure de Von Neumann dans $\mathcal{H}_2$.

Si $\mathbf{v}_1$ et $\mathbf{v}_2$ sont des états purs d'un système alors

$$\mathbf{v}_3 = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 \text{ pour } c_1, c_2 \in \mathcal{C}$$

est aussi un état pur pourvu que $|\mathbf{v}_3| = 1$. Il s'agit de prendre P_3 l'opérateur Hermitien qui mesure $\mathbf{v}_3$ comme

$$|\mathbf{v}_3\rangle\langle\mathbf{v}_3| = P_3$$

et qui projette sur le rayon induit par $\mathbf{v}_3$. La projection P_3 a deux valeurs propres m_0, m_1 telles que $\mathbf{v}_3$ est le vecteur propre associé a m_1 et tout $\mathbf{v}'$ tel que $\langle\mathbf{v}'|\mathbf{v}_3\rangle = 0$

est un vecteur propre de la valeur propre $m_0 = 0$. D'après l'équation 1.1 on a bien que

$$p_{\mathbf{v}_3}(m_1) = \langle \mathbf{v}_3 | P_3 \mathbf{v}_3 \rangle = \langle \mathbf{v}_3 | \mathbf{v}_3 \rangle = |\mathbf{v}_3| = 1$$

et

$$p_{\mathbf{v}_3}(m_0) = \langle \mathbf{v}_3 | P_3^{\perp} \mathbf{v}_3 \rangle = 0$$

où $P_3^{\perp}$ est la projection orthogonale à P_3.

Nous avons vu que les états purs d'un système peuvent être représentés par des vecteurs normalisés ou d'une façon équivalente par des projections sur les rayons associés. Nous avons aussi vu que pour les états purs $\mathbf{v}_1$ et $\mathbf{v}_2$, l'état $\mathbf{v}_3 = c_1\mathbf{v}_1 + c_2\mathbf{v}_2$ représente un état pur lorsque $|\mathbf{v}_3| = 1$, comme pour le vecteur

$$| \nearrow \rangle = \frac{1}{\sqrt{2}}(| \uparrow \rangle + | \rightarrow \rangle). \tag{1.6}$$

Un état qui est représenté par une somme normalisée de vecteurs orthogonaux est appelé une *superposition*. Le vecteur $| \nearrow \rangle$ souffre en quelque sorte d'une double personnalité. Lorsqu'il est observé par des opérateurs de projection sur les rayons $| \uparrow \rangle$ et $| \rightarrow \rangle$, il décide au moment même de la mesure de devenir $| \uparrow \rangle$ ou $| \rightarrow \rangle$ avec probabilité $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$ pour chacune des éventualités.

Il reste à voir quels peuvent être les états mixtes d'un système; on introduit donc une nouvelle classe d'opérateurs, appelés opérateurs de densité. Ces opérateurs expriment de façon plus générale les états d'un système.

1.8.1 Opérateurs de densité

Soit A un opérateur Hermitien sur un espace d'Hilbert $\mathcal{H}$.

Définition 14 *A est positif si $\forall \mathbf{v} \in \mathcal{H}, \langle \mathbf{v} | A\mathbf{v} \rangle \geq 0$.*

Si A est un opérateur positif alors A est Hermitien et A a des valeurs propres positives.

Définition 15 *La trace d'un opérateur positif A sur $\mathcal{H}$ est donnée par*

$$Tr(A) = \sum_{i=1}^{m} \langle \mathbf{v}_i | A\mathbf{v}_i \rangle$$

où $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ est une base orthonormée pour $\mathcal{H}$. Si A est exprimé par une matrice en base $\{\mathbf{v}_i\}_{i=1}^m$, la trace de A est la somme des éléments de la diagonale principale de A.

Peu importe la base orthonormée $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$, la valeur de la trace de A reste la même. La définition de la trace est indépendante de la base utilisée.

Lorsque l'opérateur Hermitien qui nous intéresse est une projection P sur un rayon, la trace de P vaut toujours 1. Ceci est facile à vérifier car en choisissant la base orthonormée $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ telle que $\mathbf{v}_1$ est un vecteur coïncidant avec le rayon sur lequel projette P on a que

$$\begin{aligned} \mathrm{Tr}(P) &= \sum_{i=1}^{l} \langle \mathbf{v}_i | P \mathbf{v}_i \rangle \\ &= \langle \mathbf{v}_1 | \mathbf{v}_1 \rangle \\ &= 1. \end{aligned}$$

En général si P est une projection sur un sous-espace de dimension m alors $\mathrm{Tr}(P) = m$. La trace a aussi les propriétés suivantes,

1. $\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$
2. $\mathrm{Tr}(cA) = c\mathrm{Tr}(A)$ pour c un scalaire
3. $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

Un opérateur de densité est défini en fonction de sa trace.

Définition 16 *Un opérateur positif D est un opérateur de densité si $Tr(D) = 1$.*

Un opérateur de projection dans un sous-espace à une dimension (sur un rayon) est donc un opérateur de densité. Lorsqu'un opérateur D peut être écrit comme $D = a_1 P_1 + a_2 P_2$ avec P_1, P_2 des projections, $a_1, a_2 \geq 0$ et $a_1 + a_2 = 1$, D est un opérateur de densité. Il s'agit de constater que

$$\begin{aligned} \mathrm{Tr}(D) &= \textstyle\sum_i \mathrm{Tr}(a_i P_i) \\ &= \textstyle\sum_i a_i \mathrm{Tr}(P_i) \quad && \text{(propriété 1)} \\ &= \textstyle\sum_i a_i && \text{(P_i est un opérateur de projection)} \\ &= 1. \end{aligned}$$

En général, si D est un opérateur de densité alors D peut s'exprimer comme

$$D = \sum_i a_i P_i$$

où P_i sont des projections. Cette décomposition n'est pas toujours unique. Par le théorème de décomposition spectrale, $\{a_i\}_i$ est l'ensemble des valeurs propres de D. Lorsque pour $i \neq j$ on a que $a_i = a_j$ la décomposition n'est pas unique. Les projections orthogonales P_i et P_j engendrent un plan L_{ij}, et pour toutes autres projections orthogonales P_i' et P_j' qui engendrent L_{ij}, on a $P_i + P_j = P_i' + P_j'$. L'opérateur peut donc être réécrit comme

$$D = a_i P_i' + a_j P_j' + \sum_{h \notin \{i,j\}} a_h P_h.$$

La non-unicité de la décomposition est importante d'un point de vue cryptographique. Nous verrons à la prochaine section que D représente l'état d'un système et la trace peut servir à déterminer la probablité d'obtenir un résultat lorsqu'on mesure ce système. Lorsque deux systèmes différents partagent une même matrice de densité, aucune mesure ne peut les distinguer.

Il faut maintenant élucider le lien entre les opérateurs de densité et les états d'un sytème quantique.

1.8.2 États mixtes

Rappelons qu'il existe une bijection entre les états purs d'un système et les projections sur les rayons dans l'espace du système. Pour $\mathbf{v}$ un vecteur normalisé d'état dans l'espace de Hilbert à deux dimensions, il existe un opérateur de projection unique $P_{\mathbf{v}} = |\mathbf{v}\rangle\langle\mathbf{v}|$ qui projette sur le rayon induit par $\mathbf{v}$. On peut tout aussi bien parler du vecteur $\mathbf{v}$ ou de l'opérateur $P_{\mathbf{v}}$ pour décrire l'état du système. Cette remarque n'est pas anodine lorsqu'on la met en perspective avec la définition d'opérateurs de densité.

Soit Q un opérateur de projection généralisée au sens de la définition 9. Nous avons que,

$$\begin{aligned} \mathrm{Tr}(QP_{\mathbf{v}}) &= \sum_i \langle \mathbf{v}_i | QP_{\mathbf{v}} \mathbf{v}_i \rangle \\ &= \mathrm{Tr}(P_{\mathbf{v}} Q) \end{aligned}$$

par la propriété 3 de la trace. Si on utilise la base orthonormée qui contient $\mathbf{v}$ comme élément, on obtient

$$\mathrm{Tr}(P_{\mathbf{v}}Q) = \sum_i \langle \mathbf{v}_i | P_{\mathbf{v}} Q \mathbf{v}_i \rangle = \langle \mathbf{v} | Q \mathbf{v} \rangle \tag{1.7}$$

car $P_{\mathbf{v}}\mathbf{v}_i = 0$ pour chaque $\mathbf{v}_i \neq \mathbf{v}$ élément de la base orthornormée qui contient $\mathbf{v}$. L'équation 1.7 n'est rien de moins que la probabilité que le vecteur $\mathbf{v}$, lorsque mesuré par l'opérateur de projection Q, donne le résultat associé au sous-espace dans lequel projette Q. On a bien que

$$p_{\mathbf{v}}(Q) = \mathrm{Tr}(P_{\mathbf{v}}Q) = \langle \mathbf{v} | Q\mathbf{v} \rangle. \tag{1.8}$$

Puisqu'un opérateur de densité peut être exprimé par $D = \sum_i a_i P_i$ avec $\sum_i a_i = 1$ et $\forall i, a_i \geq 0$, on peut interpréter la trace de D comme à l'équation 1.8. Soit Q_L un opérateur de projection dans un sous-espace L,

$$\begin{aligned} \mathrm{Tr}(DQ_L) &= \mathrm{Tr}(\sum_i a_i P_i Q_L) \\ &= \sum_i a_i \mathrm{Tr}(P_i Q_L) \\ &= \sum_i a_i p_{\mathbf{v}_i}(L). \end{aligned}$$

Puisque $p_{\mathbf{v}_i}(L)$ est une mesure de probabilité et puisque $\sum_i a_i = 1$ alors $\sum_i a_i p_{\mathbf{v}_i}(L)$ est aussi une mesure de probabilité. L'avantage d'utiliser D pour représenter l'état d'un système est qu'il est maintenant possible de spécifier un état comme une distribution de probabilité sur des états purs du système. Supposons que nous préparions un système dans l'état P_1 avec probabilité a_1 ou dans l'état P_2 avec probabilité a_2 avec $a_1 + a_2 = 1$. L'état mixte du système est

$$D = a_1 P_1 + a_2 P_2.$$

Dans le codage BB84, le système mixte correspondant à un bit uniformément distribué dans $\{0, 1\}$ encodé dans la base rectilinéaire peut être représenté par une matrice de densité ρ_+ de la façon suivante,

$$\begin{aligned} \rho_+ &= \mathrm{P}\,(\mathrm{bit} = 0)\,|\rightarrow\rangle\langle\rightarrow| + \mathrm{P}\,(\mathrm{bit} = 1)\,|\uparrow\rangle\langle\uparrow| \\ &= \frac{1}{2}|\rightarrow\rangle\langle\rightarrow| + \frac{1}{2}|\uparrow\rangle\langle\uparrow| \\ &= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \end{aligned}$$

De la même façon le système mixte pour un bit encodé dans la base diagonale correspond à la matrice de densité

$$\begin{aligned}\rho_\times &= \frac{1}{2}|\nearrow\rangle\langle\nearrow| + \frac{1}{2}|\nwarrow\rangle\langle\nwarrow| \\ &= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.\end{aligned}$$

Les deux systèmes partagent une même matrice de densité. Remarquons que l'opérateur ρ_+ n'est pas une projection car il n'est pas idempotent (i.e. $\rho_+\rho_+ = \frac{1}{2}\rho_+$). Les états ρ_+ et $\rho_\times$ ne correspondent donc pas à des états purs. De plus, la probabilité d'obtenir un résultat particulier lors d'une mesure M est seulement fonction de M et de la matrice de densité du système à observer. Il s'en suit que si deux systèmes ont une même matrice de densité ils ne peuvent pas être distingués par M.

De la même façon, on peut trouver les matrices de densité des systèmes qui correspondent à un 0 et à un 1 dans le codage BB84. Soit ρ_0 matrice de densité associée au bit 0 définie par

$$\begin{aligned}\rho_0 &= \frac{1}{2}|\rightarrow\rangle\langle\rightarrow| + \frac{1}{2}|\nearrow\rangle\langle\nearrow| \\ &= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} \\ &= \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}.\end{aligned}$$

La matrice ρ_1 associée au codage du bit 1 est

$$\begin{aligned}\rho_1 &= \frac{1}{2}|\uparrow\rangle\langle\uparrow| + \frac{1}{2}|\nwarrow\rangle\langle\nwarrow| \\ &= \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{4} & \frac{-1}{4} \\ \frac{-1}{4} & \frac{1}{4} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{4} & \frac{-1}{4} \\ \frac{-1}{4} & \frac{3}{4} \end{pmatrix}.\end{aligned}$$

Comme il fallait s'y attendre les deux matrices de densité sont distinctes. Elles représentent deux systèmes qui peuvent être distingués probabilistiquement par des mesures de Von Neumann. Par exemple, la mesure de Breidbart donne le bon bit sauf avec probabilité environ 0.15. Heureusement que ρ_0 et ρ_1 peuvent être distingués car on voit mal comment le codage BB84 pourrait autrement servir à transférer de l'information. En conclusion,

Théorème 3 *Si Ψ_1 et Ψ_2 sont deux systèmes qui partagent une même matrice de densité alors aucune mesure ne peut les distinguer. Si une source émet Ψ_1 avec probabilité p_1 et Ψ_2 avec probabilité p_2, aucune mesure du système reçu ne permet de changer la distribution a priori $\{p_1, p_2\}$ pour Ψ_1 et Ψ_2.*

En conséquence, lorsque le codage BB84 est utilisé aucun biais en faveur de la base de codage ne peut être obtenu. Le résultat de la mesure ne contient aucune information sur la base utilisée. Pour que ce soit le cas cependant, il faut que le bit soit tiré uniformément et aléatoirement dans $\{0, 1\}$.

1.9 Systèmes composés

Dans les sections précédentes nous nous sommes intéressés à la description des états de polarisation d'un photon et des mesures de cette quantité physique. Nous avons vu un codage, le codage BB84, qui permet d'encoder un bit d'une façon équivoque. Pour construire des tâches cryptographiques autour du codage BB84, plusieurs bits doivent être encodés et transmis par le canal quantique. C'est la façon d'amplifier le caractère cryptographique de la transmission équivoque d'un bit par un photon polarisé dans des bases qui ne sont pas orthogonales. Si un protocole cryptographique demande à $\mathcal{A}$lice de transmettre n bits sur le canal quantique par le codage BB84, $\mathcal{B}$ob, qui les reçoit, se trouve face à un système composé de dimension supérieure à l'espace de polarisation d'un photon. Les mesures sur ce système sont modélisées par des opérateurs Hermitiens sur l'espace du système complet à n particules. Dans le cas de l'espace qui représente la polarisation de n photons, la dimension de l'espace est 2^n. Il faut répondre à la question suivante: comment construire l'espace d'Hilbert qui contient l'état du système composé à partir de l'état des parties?

Supposons que deux systèmes quantiques Ψ_1 et Ψ_2 interagissent. Soit $\mathcal{H}^1$ et $\mathcal{H}^2$ les deux espaces d'Hilbert qui servent à représenter les états de Ψ_1 et Ψ_2 respectivement. Nous notons

$$\mathcal{H} = \mathcal{H}^1 \otimes \mathcal{H}^2$$

l'espace d'Hilbert du système composé des sous-systèmes $\mathcal{H}^1$ et $\mathcal{H}^2$. L'opération $\otimes$ désigne le produit tensoriel entre deux espaces. L'espace $\mathcal{H}$ peut être construit de façon à ce que si $v_1 = \{\mathbf{v}_i\}_i$ et $v_2 = \{\mathbf{u}_j\}_j$ sont des bases orthonormées pour $\mathcal{H}^1$ et $\mathcal{H}^2$ respectivement alors

$$v = \{\mathbf{v}_i \otimes \mathbf{u}_j\}_{i,j}$$

est une base orthonormée pour $\mathcal{H}$. En général, si $\mathbf{v} \in \mathcal{H}^1$ et $\mathbf{u} \in \mathcal{H}^2$ alors $\mathbf{v} \otimes \mathbf{u} \in \mathcal{H}$. L'opération $\otimes$ est semblable au produit cartésien entre deux ensembles. Par exemple, les deux bases

$$+ = \{|\rightarrow\rangle, |\uparrow\rangle\} \text{ et } \times = \{|\nearrow\rangle, |\nwarrow\rangle\}$$

sont deux bases orthonormées pour $\mathcal{H}_2$. L'espace $\mathcal{H}_4 = \mathcal{H}_2 \otimes \mathcal{H}_2$ forme l'espace de représentation de la polarisation d'un système composé de deux photons. Une base orthonormée pour $\mathcal{H}_4$ est obtenue en effectuant un produit cartésien entre les éléments de $+$ et de $\times$. Ainsi,

$$\begin{aligned} +\times &\triangleq \{|\rightarrow\rangle \otimes |\nearrow\rangle, |\rightarrow\rangle \otimes |\nwarrow\rangle, |\uparrow\rangle \otimes |\nearrow\rangle, |\uparrow\rangle \otimes |\nwarrow\rangle\} \\ &\triangleq \{|\rightarrow\rightarrow\rangle, |\rightarrow\nwarrow\rangle, |\uparrow\nearrow\rangle, |\uparrow\nwarrow\rangle\} \end{aligned}$$

est une base orthonormée pour $\mathcal{H}_4$. Pour obtenir explicitement le vecteur $\mathbf{u} \otimes \mathbf{v}$ pour $\mathbf{u} = (u_1, u_2)$ et $\mathbf{v} = (v_1, v_2)$ on calcule

$$(u_1, u_2) \otimes (v_1, v_2) = (u_1v_1, u_1v_2, u_2v_1, u_2v_2).$$

La description explicite de la base $+\times$ pour $\mathcal{H}_4$ est donc

$$+\times = \{(0, 0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}), (0, 0, \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}), (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0), (\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0)\}.$$

Évidemment la discussion précédente s'applique à des espace $\mathcal{H}^A$ et $\mathcal{H}^B$ arbitraires. L'espace $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ est défini de la même façon que pour $\mathcal{H}_4 = \mathcal{H}_2 \otimes \mathcal{H}_2$.

Dans l'espace $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ le produit scalaire entre $\mathbf{v} = \mathbf{v}^A \otimes \mathbf{v}^B$ et $\mathbf{u} = \mathbf{u}^A \otimes \mathbf{u}^B$ est défini de la façon suivante,

$$\langle \mathbf{v} | \mathbf{u} \rangle = \langle \mathbf{v}^A | \mathbf{u}^A \rangle \langle \mathbf{v}^B | \mathbf{u}^B \rangle.$$

Remarquons que si les vecteurs $\mathbf{v}^A$ et $\mathbf{u}^A$ sont orthogonaux alors qu'importe $\mathbf{v}^B$ et $\mathbf{u}^B$ on a que $\langle \mathbf{u}^A \otimes \mathbf{u}^B | \mathbf{v}^A \otimes \mathbf{v}^B \rangle = 0$. Dans ce cas les vecteurs $\mathbf{u}^A \otimes \mathbf{u}^B$ et $\mathbf{v}^A \otimes \mathbf{v}^B$ sont nécessairement des vecteurs orthogonaux dans $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$.

Un état pur dans $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ est un vecteur $\mathbf{v} \in \mathcal{H}$ tel que $|\mathbf{v}| = 1$. Si $\mathbf{u} \in \mathcal{H}^A$ et $\mathbf{v} \in \mathcal{H}^B$ sont des états purs, alors

$$|\mathbf{u} \otimes \mathbf{v}| = 1.$$

Le vecteur $\mathbf{u} \otimes \mathbf{v}$ représente donc un état pur dans $\mathcal{H}$. En général, si $\mathbf{u} \in \mathcal{H}^A$ et $\mathbf{v} \in \mathcal{H}^B$ sont des états purs alors $\mathbf{u} \otimes \mathbf{v}$ est un état pur de $\mathcal{H}^A \otimes \mathcal{H}^B$. Cependant, l'inverse n'est pas toujours vrai. Il y a des états purs $\mathbf{w} \in \mathcal{H}$ qui ne peuvent pas être représentés pour $\mathbf{u} \in \mathcal{H}^A$ et $\mathbf{v} \in \mathcal{H}^B$ comme

$$\mathbf{w} = \mathbf{u} \otimes \mathbf{v}.$$

L'espace $\mathcal{H}^A \otimes \mathcal{H}^B$ contient davantage d'états purs que ceux qui sont construits par $\mathbf{u} \otimes \mathbf{v}$ pour $\mathbf{u} \in \mathcal{H}^A$ et $\mathbf{v} \in \mathcal{H}^B$. Il doit y avoir des états purs $\mathbf{v} \in \mathcal{H}^A \otimes \mathcal{H}^B$ dont les composantes dans $\mathcal{H}^A$ et $\mathcal{H}^B$ représentent des états mixtes. Par exemple, dans $\mathcal{H}_4$ on peut construire un état pur qui ne peut être réduit comme un produit tensoriel d'états purs dans $\mathcal{H}_2$. La base

$$++ = \{|\rightarrow\rightarrow\rangle, |\rightarrow\uparrow\rangle, |\uparrow\rightarrow\rangle, |\uparrow\uparrow\rangle\}$$

est une base orthornormée pour $\mathcal{H}_4$. Le vecteur

$$\mathbf{v} = \frac{1}{\sqrt{2}}(|\rightarrow\rightarrow\rangle + |\uparrow\uparrow\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \tag{1.9}$$

est un état pur de $\mathcal{H}_4$ car il est obtenu par une combinaison linéaire des éléments de $++$ en plus d'être de norme $|\mathbf{v}| = 1$. Supposons que nous puissions écrire $\mathbf{v} = \mathbf{v}^A \otimes \mathbf{v}^B$ avec $\mathbf{v}^A = (x^A, y^A)$ et $\mathbf{v}^B = (x^B, y^B)$. Dans ce cas on doit avoir que

$$\begin{aligned} x^A x^B &= \frac{1}{\sqrt{2}} \\ x^A y^B &= 0 \\ y^A x^B &= 0 \\ y^A y^B &= \frac{1}{\sqrt{2}}. \end{aligned}$$

Il est impossible de satisfaire les équations précédentes car,

$$\begin{aligned} x^A x^B = \frac{1}{\sqrt{2}} &\Rightarrow x^A \neq 0 \wedge x^B \neq 0 \\ x^A y^B = 0 &\Rightarrow y^B = 0 \end{aligned}$$

ce qui rend $y^A y^B = \frac{1}{\sqrt{2}}$ impossible à satisfaire.

Les mesures possibles sur le système composé sont représentées comme à l'habitude par des opérateurs Hermitiens. L'état du système représenté par le vecteur $\mathbf{v}$ de l'exemple précédent peut être mesuré exactement en observant seulement l'état de la première particule A. L'état de la particule B est déterminé par l'état de la particule A; elles sont des copies l'une de l'autre. Supposons que nous mesurions l'état de A par l'opérateur de projection P_0. En choisissant de ne pas mesurer la seconde particule, on effectue en fait l'opérateur identité $\mathbf{I}_2$ sur celle-ci. La mesure sur le système complet est $M = P_0 \otimes \mathbf{I}_2$. Soit a_0 et a_1 les valeurs propres de P_0 coïncidant avec les rayons à des angles de 0 et $\frac{\pi}{2}$ respectivement. Lorsqu'appliqué sur $\mathbf{v}$, l'opérateur M se comporte comme suit,

$$\begin{aligned}
M\mathbf{v} &= (P_0 \otimes \mathbf{I}_2)\frac{1}{\sqrt{2}}(|\rightarrow\rightarrow\rangle + |\uparrow\uparrow\rangle) \\
&= \frac{1}{\sqrt{2}}(P_0|\rightarrow\rangle \otimes \mathbf{I}_2|\rightarrow\rangle + P_0|\uparrow\rangle \otimes \mathbf{I}_2|\uparrow\rangle) \\
&= \frac{1}{\sqrt{2}}(|\rightarrow\rangle \otimes |\rightarrow\rangle + \mathbf{0} \otimes |\uparrow\rangle) \\
&= \frac{1}{\sqrt{2}}|\rightarrow\rightarrow\rangle.
\end{aligned}$$

La probabilité $p_{\mathbf{v}}(a_0)$ que la mesure donne le résultat a_0 est $\langle \mathbf{v}|P_0 \otimes \mathbf{I}_2\mathbf{v}\rangle$ qui peut être calculée comme suit.

$$\begin{aligned}
p_{\mathbf{v}}(a_0) &= \langle \mathbf{v}|P_0 \otimes \mathbf{I}_2\mathbf{v}\rangle \\
&= \langle \mathbf{v}|\frac{1}{\sqrt{2}}|\rightarrow\rightarrow\rangle\rangle \\
&= \langle(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}})|(\frac{1}{\sqrt{2}}, 0, 0, 0)\rangle \\
&= \frac{1}{2}.
\end{aligned}$$

D'autres mesures peuvent être effectuées sur les deux particules. La mesure $M' = P_0 \otimes P_0$ est une de celle-là, elle consiste à mesurer dans la base rectilinéaire les deux particules indépendamment. Si $\mathbf{v}_0, \mathbf{v}_1$ sont les vecteurs propres normalisés de P_0 alors les vecteurs propres de $P_0 \otimes P_0$ peuvent être déterminés de la façon suivante,

$$(P_0 \otimes P_0)(\mathbf{v}_0 \otimes \mathbf{v}_1) = (P_0\mathbf{v}_0) \otimes (P_0\mathbf{v}_1)$$

$$
\begin{aligned}
&= a_0\mathbf{v}_0 \otimes a_1\mathbf{v}_1 \\
&= a_0 a_1(\mathbf{v}_0 \otimes \mathbf{v}_1)
\end{aligned}
$$

et $\mathbf{v}_0 \otimes \mathbf{v}_1$ est un vecteur propre de $P_0 \otimes P_0$. Parce que P_0 a deux vecteurs propres normalisés $\mathbf{v}_0$ et $\mathbf{v}_1$ distincts, $P_0 \otimes P_0$ a comme vecteurs propres

$$\mathbf{v}_0 \otimes \mathbf{v}_0, \mathbf{v}_0 \otimes \mathbf{v}_1, \mathbf{v}_1 \otimes \mathbf{v}_0 \text{ et } \mathbf{v}_1 \otimes \mathbf{v}_1.$$

À chacun de ceux-ci correspond un résultat possible de la mesure. On peut calculer la probabilité de chacun des résultats comme à l'équation 1.1. Soit $p_{\mathbf{v}}(j_0, j_1)$ la probabilité qu'en mesurant $\mathbf{v}$ le résultat obtenu soit celui correspondant au rayon $\mathbf{v}_{j_0} \otimes \mathbf{v}_{j_1}$ pour $j_0, j_1 \in \{0, 1\}$. On a que

$$p_{\mathbf{v}}(j_0, j_1) = \langle \mathbf{v}|P_{j_0,j_1}|\mathbf{v}\rangle$$

où $P_{j_0,j_1} = P_{j_0} \otimes P_{j_1}$ avec P_j la projection sur le rayon défini par $\mathbf{v}_j$. Un simple calcul nous donne

$$p_{\mathbf{v}}(0,0) = p_{\mathbf{v}}(1,1) = \frac{1}{2} \text{ et } p_{\mathbf{v}}(0,1) = p_{\mathbf{v}}(1,0) = 0.$$

La distribution obtenue semble indiquer que les deux particules se "parlent". Même si le résultat de la mesure sur la première particule n'est pas prédéterminé, le résultat de la seconde mesure est complètement déterminé par le première. C'est plus qu'une illusion, il existe des systèmes composés d'une paire de particules dont le comportement ne peut être expliqué par une théorie qui n'inclurait pas une corrélation instantané et à distance. Ces paires de particules sont appelées paires EPR du nom d'Einstein, Podelski et Rosen [35] qui les introduisirent pour montrer que la mécanique quantique ne respecte pas les principes de la physique classique. L'état qu'ils introduisirent est défini comme

$$|\Psi_{EPR}\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\uparrow\rangle - |\uparrow\rightarrow\rangle\right).$$

Les deux particules, lorsqu'elles sont observées dans la base rectilinéaire, montrent troujours des polarisations opposées. Cette propriété est vraie peu importe la base d'observation de la paire de particules. On dit de ce système qu'il est dans l'état *singulet*. Les statistiques associées aux mesures sur ce système ne laissent aucune place à une interprétation classique puisqu'une théorie qui expliquerait classiquement ces phénomènes doit violer l'inégalité de Bell [5], ce qui est impossible (voir chapitre 6 dans [58]). Ces phénomènes sont réels et ont été observés en laboratoire pour la première fois et de façon décisive par Alain Aspect et al. [3].

L'analyse précédente peut se traduire en termes de matrices de densité. De la même façon que pour les systèmes à une particule, les états d'un système composé peuvent être représentés par une matrice de densité. Si A est une mesure sur le système composé représenté par la matrice de densité D alors comme à l'équation 1.8 on a que

$$p_{\mathbf{v}}(a) = \mathrm{Tr}(P_a D)$$

où P_a est une projection sur le rayon déterminé par un des vecteurs propres $\mathbf{v}_a$ de A.

1.10 Mesures généralisées

Dans les sections précédentes nous avons vu comment les mesures possibles sur un photon peuvent être modélisées. Les mesures en mécanique quantique sont représentées par des opérateurs Hermitiens dans l'espace d'Hilbert qui contient la propriété à observer. La polarisation d'un photon est exprimée par un vecteur normalisé dans l'espace à deux dimensions complexes. Une mesure A donne un des résultats associés à ses valeurs propres. À chaque valeur propre est associée un ensemble de vecteurs propres dans un même sous-espace. Si $\mathcal{V}_1$ et $\mathcal{V}_2$ sont des ensembles qui contiennent chacun les vecteurs associés aux valeurs propres a_1 et a_2 respectivement alors

$$(\forall \mathbf{v}_1 \in \mathcal{V}_1)(\forall \mathbf{v}_2 \in \mathcal{V}_2)[\langle \mathbf{v}_1 | \mathbf{v}_2 \rangle = 0].$$

Les vecteurs de $\mathcal{V}_1$ sont orthogonaux à ceux dans $\mathcal{V}_2$. Par le théorème de décomposition spectrale, si A est une mesure sur l'espace d'Hilbert de dimension n alors pour $m \leq n$ et des projections $P_1, \ldots, P_m$ sur des sous-espaces orthogonaux, on peut écrire

$$A = \sum_{i=1}^{m} a_i P_i$$

où $\{a_i\}_{i=1}^{m}$ sont les valeurs propres de A.

Si pour $j \neq h$ on a que $a_j = a_h$, la décomposition spectrale de A peut être réécrite comme

$$\begin{aligned} A &= a_j(P_j + P_h) + \sum_{i \in \{1,\ldots,m\} \setminus \{j,h\}} a_i P_i \\ &= a_j P'_j + \sum_{i \in \{1,\ldots,m\} \setminus \{j,h\}} a_i P_i \end{aligned}$$

pour $P'_j = P_j + P_h$ une nouvelle projection. Ceci est facile à vérifier car

1. $P_j + P_h$ est Hermitien,

2. puisque P_j et P_h sont des projections orthogonales,

$$\begin{aligned} (P_j + P_h)^2 &= P_j + P_j P_h + P_h P_j + P_h \\ &= P_j + P_h \end{aligned}$$

   et $(P_j + P_h)$ est idempotente donc $(P_j + P_h)$ est elle-même une projection.

Lorsque $m = n$ et les valeurs propres de A sont toutes distinctes alors les projections $P_1, \ldots, P_n$ projettent sur des rayons orthogonaux. À l'opposé, si $m < n$ alors certaines projections agissent sur des sous-espaces de dimension plus grande. Un lecteur attentif remarquera que cette façon de voir les mesures est limitée lorsqu'elles s'appliquent dans l'espace de polarisation d'un seul photon. Puisqu'une mesure A sur un photon est un opérateur Hermitien sur l'espace d'Hilbert à deux dimensions, A possède au mieux deux valeurs propres distinctes. Si tel est le cas, la mesure résultante est une mesure de Von Neumann. Si A ne possède qu'une seule valeur propre, il peut être ecrit comme

$$A = a_1 P_1$$

où P_1 est une projection dans un sous-espace de dimension deux. C'est-à-dire que P_1 projette dans l'espace d'Hilbert original. Dans ce cas A est inutile, elle ne fait rien. Les mesures possibles sur un photon semblent être limitées car elles sont restreintes à des mesures de Von Neumann.

Cependant, lorsqu'une mesure B est appliquée sur une paire de photons, les possibilités semblent être multipliées. En effet, puisque B est une mesure sur un espace de dimension quatre, le nombre m de ses valeurs propres peut être $1, 2, 3$ ou 4. Lorsque

$m = 1$, la mesure est inutile et lorsque $m = 4$ la mesure est une mesure de Von Neumann ou mesure complète dans l'espace à quatre dimensions. Pour $m \in \{2, 3\}$, la mesure n'est ni inutile ni de type Von Neumann, il s'agit d'une mesure incomplète. À la section suivante, nous verrons que des mesures incomplètes qui ne sont pas inutiles peuvent aussi être effectuées sur un photon.

1.10.1 Mesures incomplètes

Entre les mesures inutiles et celles qui sont complètes, il y un éventail de mesures dont la granularité peut être plus ou moins grande. Les mesures inutiles ont un seul grain tandis que les mesures de Von Neumann ont la meilleure définition (elles ont le plus petit grain possible). La granularité d'un résultat a_i est déterminée par la dimension du sous-espace dans lequel projètte P_i lorsque la mesure est exprimée par sa décomposition spectrale. La granularité d'une mesure A est fonction du nombre de ses valeurs propres distinctes. Plus A a de valeurs propres, plus sa granularité est petite, ou dit différemment, plus sa définition est grande.

Un lecteur perspicace se demandera à quoi bon mesurer un système avec de gros grains si la mesure de Von Neumann permet d'obtenir la meilleure définition pour le même prix. La réponse dépend du contexte dans lequel la mesure est exécutée. Nous verrons qu'au centre du protocole de transmission inconsciente, une mesure à gros grains pourrait permettre à un participant malhonnête d'obtenir de l'information supplémentaire qu'une mesure de Von Neumann ne peut fournir. Ceci est dû au fait qu'un résultat à gros grains peut toujours être raffiné subséquemment de façon à obtenir après raffinement un résultat avec une définition aussi bonne que ceux obtenus par une mesure de Von Neumann. Si entre la première mesure et le raffinement, une information supplémentaire est obtenue, le résultat de la mesure qui englobe la première et la deuxième peut être plus informatif qu'une mesure de Von Neumann exécutée avant que le supplément d'information ne soit obtenu. Ceci parce que le raffinement peut être choisi en fonction du supplément d'information.

Par exemple, supposons qu'un bit $b \in \{0, 1\}$ soit encodé par $\mathcal{A}$lice en utilisant le codage BB84. Un photon π_b est transmis d'$\mathcal{A}$lice vers $\mathcal{B}$ob ce dernier ayant pour tâche de déterminer le mieux possible le bit b. Supposons qu'$\mathcal{A}$lice après avoir transmis π_b, attend un temps $t > 0$ pour annoncer ensuite la base $\theta \in \{+, \times\}$ qu'elle a utilisée pour encoder b. Envisageons deux stratégies possibles pour $\mathcal{B}$ob. La première consiste à mesurer π_b avec la mesure de Von Neumann $M_{\frac{\pi}{8}}$ au temps $t' < t$. La deuxième consiste à exécuter la mesure inutile $\mathbf{I}_2$ et d'attendre au temps t pour raffiner la mesure en exécutant M_θ pour θ la base annoncée par $\mathcal{A}$lice. Dans le premier cas, en accord avec l'équation 1.3, le bit b est obtenu avec probabilité approximativement 0.85. Dans le second cas, le bit b est déterminé avec certitude.

La mesure inutile n'est pas la seule qui puisse permettre un raffinement sur un photon. Les degrés de liberté que permettent les mesures incomplètes peuvent être obtenus en augmentant la dimension de l'espace de travail d'une mesure. Rien de plus facile, il s'agit d'ajouter un système dans un état connu $|\mathbf{z}\rangle$ résidant dans un espace d'Hilbert $\mathcal{H}$ de dimension suffisante pour obtenir la granularité voulue. Le photon π_b dans l'état $|\mathbf{v}\rangle \in \mathcal{H}_2$ et l'état $|\mathbf{z}\rangle$ du système ajouté forment un nouveau système dans l'état $|\mathbf{v}\rangle \otimes |\mathbf{z}\rangle$. L'espace d'Hilbert $\mathcal{H}'$ du système composé $|\mathbf{v}\rangle \otimes |\mathbf{z}\rangle$ est de dimension $\text{Dim}(\mathcal{H}') = \text{Dim}(\mathcal{H}_2) \times \text{Dim}(\mathcal{H})$. Une mesure complète sur le système composé est modélisée par une mesure de Von Neumann dans l'espace $\mathcal{H}'$. Une mesure incomplète est, d'autre part, modélisée par un opérateur Hermitien dont le nombre de valeurs propres distinctes est entre 1 et $\text{Dim}(\mathcal{H}')$. Les mesures généralisées sur un photon sont représentées par des opérateurs Hermitiens sur l'espace $\mathcal{H}_2 \otimes \mathcal{H}$ où $\mathcal{H}$ est l'espace où réside l'état $|\mathbf{z}\rangle$ du système qui apporte les degrés de liberté voulus. Le système dans l'état $|\mathbf{z}\rangle$ est souvent appelé système *ancillaire.*

1.10.2 Mesures cohérentes

À la section précédente nous avons montré comment des mesures incomplètes peuvent être effectuées sur un photon. Celles-ci sont les plus générales qui peuvent être appliquées sur un seul photon. L'extension des mesures incomplètes au cas où le système est composé de plusieurs particules représente les mesures les plus générales que la mécanique quantique n'autorise. Elles sont modélisées par des séquences quelconques d'opérations permises par la mécanique quantique sur le système à observer.

Les trois premières opérations ont été vues dans les sections précédentes:

1. l'exécution d'une mesure de Von Neumann,
2. l'application d'une transformation unitaire sur le système,
3. l'élargissement du système en introduisant un système ancillaire.

Ces trois premières opérations réalisent les mesures incomplètes avec la granularité voulue. À celles-ci s'ajoute une quatrième qui, en quelque sorte, inverse l'opération 3. Elle permet de ne plus considérer une partie du système à observer. À l'inverse de l'ajout d'un ancilla pour augmenter la dimension de l'espace de représentation, la trace partielle réduit l'espace de travail en ignorant une partie du système composé. L'état enchevêtré de l'équation 1.9 peut nous servir d'exemple d'application de cette opération. Nous avons vu que la matrice de densité D de l'état enchevêtré $\mathbf{v} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$ est

$$D = |\mathbf{v}\rangle\langle\mathbf{v}| = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Supposons que nous nous intéressions à seulement une des deux particules de la paire. La trace partielle permet, à partir de la matrice de densité du système composé, de retrouver l'état d'une de ces composantes sans tenir compte de l'état du reste du système. Comme nous l'avons vu précédemment, la première particule A (ou la deuxième) est représenté par la matrice de densité

$$D^A = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \mathrm{Tr}_{\mathcal{H}_2}(D). \tag{1.10}$$

Soit D une matrice de densité sur un espace $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ et soit $\{\mathbf{u}_i\}_i$ et $\{\mathbf{v}_j\}_j$ des bases orthonormées pour $\mathcal{H}^A$ et $\mathcal{H}^B$ respectivement. La trace partielle sur l'espace $\mathcal{H}^B$ du système D est une matrice de densité D^A dont chacune des entrées $i, j \in \{1, \ldots, \mathrm{Dim}(\mathcal{H}^A)\}$ est obtenue en calculant,

$$D^A_{i,j} = \sum_h \langle \mathbf{u}_i \otimes \mathbf{v}_h | D(\mathbf{u}_j \otimes \mathbf{v}_h)\rangle.$$

Il est facile de vérifier que de cette dernière équation vérifie la chaîne d'égalité représentée à l'équation 1.10 pour l'état enchevêtré $\mathbf{v} = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$. Oublier une partie d'un système est évidemment une opération que nous devrons être capable d'accomplir. Celle-ci est la quatrième et dernière opération permise par la mécanique quantique.

4. l'exécution de la trace partielle dans la but d'ignorer une partie du système considéré.

Les quatre opérations précédentes n'ont pas le caractère mathématique des mesures effectuées sur des espaces d'Hilbert fixes. Elles sont plutôt de type procédural, facile a visualiser, mais assez difficile à manipuler lorsque des situations complexes doivent être analysées. Heureusement, en vertu du théorème de Neumark [58, 57] que nous énoncerons plus loin, on peut les remplacer par un ensemble d'opérateurs Hermitiens. Un seul opérateur ne peut pas modéliser ces mesures généralisées car l'espace d'Hilbert que l'on considère peut être agrandi ou réduit par des opérations du type 3 et 4. Les opérateurs Hermitiens ne peuvent traduire ces opérations car ils opèrent sur des espaces fixes. La prochaine section explore un modèle mathématique pour représenter une séquence arbitraire des opérations permises sur un système quantique.

1.10.3 Le modèle MOP

Le modèle standard qui représente une séquence quelconque des opérations permises (1 à 4) est appelé *mesure par opérateurs positifs* noté MOP (ou POM pour *positive operator measurement*).

Une mesure généralisée qui admet m résultats possibles peut être exprimée par un ensemble $\mathcal{A} = \{A_i\}_{i=1}^m$ d'opérateurs positifs $\mathcal{H} \to \mathcal{H}$ Hermitiens aux valeurs propres positives. La mesure $\mathcal{A}$ est physiquement réalisable en autant que $\sum_{i=1}^m A_i = \mathbf{I}$, la matrice identité de l'espace d'Hilbert qui représente l'état du système à observer. Chacun des opérateurs représente un résultat possible de la mesure. Si l'état du système à observer est $|\phi\rangle$ alors la probabilité $p_\phi(k)$ d'observer le résultat $k \in \{1, \ldots, m\}$ est

$$p_\phi(k) = \langle \phi | A_k \phi \rangle.$$

Pour que le modèle MOP soit en accord avec les principes de la mécanique quantique, il faut être capable de transformer les mesures exprimées par des opérateurs positifs en une séquence d'opérations parmi les quatre qui sont permises. Le théorème de Neumark nous éclaire à ce sujet.

Théorème 4 (Neumark) *Pour tout MOP $\mathcal{A} = \{A_i\}_{i=1}^m$ sur un espace d'Hilbert $\mathcal{H}$, il y a un espace $\mathcal{Z}$ et un vecteur d'état $\mathbf{z} \in \mathcal{Z}$ tels qu'il existe une mesure de Von Neuman aux rayons $P_1, \ldots, P_m$ pour laquelle*

$$(\forall k)[A_k = Tr_{\mathcal{Z}}((\mathbf{I}_{\mathcal{H}} \otimes |\mathbf{z}\rangle\langle\mathbf{z}|)P_k)].$$

Autrement dit, si nous disposons d'un MOP $\mathcal{A}$ sur $\mathcal{H}$ alors une séquence d'opérations permises permet de simuler la même mesure. L'inverse est aussi vrai: étant donné une séquence des opérations 1 à 4, il existe une mesure MOP qui la simule. Pour plus de détails consultez [51, 58].

1.10.4 MOP et mesures de Von Neumann

Il y a une différence fondamentale entre l'interprétation que l'on peut faire du modèle MOP pour les mesures généralisées et celle que l'on peut faire pour les mesures de Von Neumann. Outre le fait que le modèle MOP est plus versatile que l'autre, une limitation dans le formalisme de ce dernier empêche une analogie poussée entre les deux modèles. Pour les mesures de Von Neumann, l'état final du système après la mesure est déterminé par le résultat lui-même. Lorsqu'une mesure de Von Neumann donne le résultat k qui correspond à la projection sur le rayon P_k, le système mesuré se retrouve, à une renormalisation près, dans l'état P_k. Ainsi, le système dans l'état $|\phi\rangle$ observé par une mesure de Von Neumann $A = \sum_{i=1}^m a_i P_i$ donne le résultat k avec probabilité

$$p_\phi(k) = \langle\phi|A\phi\rangle.$$

Une fois le résultat k obtenu, le système se retrouve dans l'état non-normalisé

$$|\phi'\rangle = P_k|\phi\rangle.$$

Une mesure MOP $\mathcal{A} = \{A_i\}_{i=1}^m$, dans les mêmes conditions, donne la formule

$$p_\phi = \langle\phi|A_k\phi\rangle$$

pour la probabilité d'obtenir le résultat k lorsque l'état $|\phi\rangle$ est mesuré. Cependant, il n'y a pas de formule explicite pour l'état final $|\phi'\rangle$ une fois le résultat k obtenu [51]. Pour l'obtenir, il faut utiliser le théorème de Neumark qui relie l'opérateur A_k à une trace partielle du système élargi par l'introduction d'un ancilla. Cette approche est moins naturelle que celle induite par le formalisme des mesures de Von Neumann.

Cette remarque devient importante lorsque la sécurité des protocoles cryptographiques entre en jeu. Le scénario habituel demande l'analyse des mesures qui sont incomplètes jusqu'à l'obtention d'une information classique supplémentaire. Le raffinement étant fonction de cette information, pouvoir obtenir l'état intermédiaire du système facilite l'analyse. Une modélisation alternative proposée par Dominic Mayers [51], permet d'obtenir les états intermédiaires d'une façon semblable au modèle de Von Neumann. La prochaine section décrit ce modèle alternatif qui sera largement utilisé par la suite.

1.11 Le modèle OCPS

Le modèle alternatif introduit par D. Mayers [51] pour représenter les mesures généralisées a la propriété de fournir l'état final du système mesuré. Lorsque cette mesure procède par raffinements successifs, les états intermédiaires peuvent eux aussi être obtenus. En ce sens, il généralise les mesures de Von Neumann pour y inclure tout ce que les opérations 1 à 4 permettent de faire. Dans ce formalisme il n'est pas nécessaire de considérer l'ajout d'un système ancillaire au système cible pour formaliser les mesures incomplètes. L'élargissement de la dimension d'un système est incluse dans le formalisme. Pour plus d'information sur l'équivalence de ce modèle avec les opérations permises ou avec le modèle MOP, consultez [51].

Au centre de ce modèle, il y a un type d'opérateurs, noté OCPS, qui conserve le produit scalaire (ou IPP pour *inner product preserving operators*).

Définition 17 *Un opérateur $U : \mathcal{H} \to \mathcal{H}'$ est OCPS si*

$$(\forall \mathbf{u}, \mathbf{v} \in \mathcal{H})[\langle \mathbf{u}|\mathbf{v}\rangle = \langle U\mathbf{u}|U\mathbf{v}\rangle]$$

où le produit scalaire doit être celui défini dans $\mathcal{H}$ à gauche de l'égalité et celui dans $\mathcal{H}'$ à droite.

Si $\mathrm{Dim}(\mathcal{H}) = n$ et $\mathrm{Dim}(\mathcal{H}') = m$, U est représenté par une matrice de dimension $n \times m$. Contrairement aux autres modèles, l'opérateur U n'est pas une fonction de l'espace des états observés dans lui-même. Lorsque $m > n$, $U|\phi\rangle$ transforme l'état $|\phi\rangle$ d'un espace $\mathcal{H}$ dans un espace plus grand $\mathcal{H}'$. Implicitement, l'introduction d'un système ancillaire est incluse dans la composition de U.

Les opérateurs OCPS lorsqu'ils sont exprimés sous la forme matricielle sont formés de colonnes orthonormées. Inversement, toute matrice dont les colonnes sont orthonormales sont des opérateurs OCPS [51]. Lorsque U est OCPS il possède toujours un inverse gauche mais pas nécessairement d'inverse droit comme dans le cas des opérateurs unitaires.

Définition 18 *Pour U une matrice $m \times n$, $U^\dagger$ dénote sa transposée conjuguée. C'est-à-dire que*

$$U^\dagger_{j,i} = (U_{i,j})^*.$$

Lorsque $U : \mathcal{H} \to \mathcal{H}'$ est OCPS, $U^\dagger$ est son inverse gauche,

$$U^\dagger U = \mathbf{I}_{\mathcal{H}}$$

où $\mathbf{I}_{\mathcal{H}}$ est l'opérateur identité dans $\mathcal{H}$.

Comme pour le modèle MOP, une mesure OCPS à m résultats est représentée par un ensemble $\mathcal{M} = \{M_i\}_{i=1}^m$ de m opérateurs $\mathcal{H} \to \mathcal{H}'$ où l'espace du système initial $\mathcal{H}$ n'est pas nécessairement égal a celui du système final $\mathcal{H}'$. Lorsque l'état $|\phi\rangle$ est mesuré, la probabilité $p_\phi(k)$ d'obtenir le résultat k est

$$p_\phi(k) = \|M_k|\phi\rangle\|^2 = |\langle\phi|M_k^\dagger M_k|\phi\rangle|^2. \tag{1.11}$$

De plus, une fois le résultat k obtenu, le nouvel état $|\phi'\rangle$ est

$$|\phi'\rangle = M_k|\phi\rangle. \tag{1.12}$$

Toute mesure OCPS $\mathcal{M} = \{M_k\}_{k=1}^m$ peut être exprimée de la façon indiquée à la prochaine définition.

Définition 19 ([51]) *Dans le modèle OCPS, une mesure $\mathcal{M} = \{M_i\}_{i=1}^m$ est physiquemet réalisable si pour chaque $k \in \{1, \ldots, m\}$ on peut poser*

$$M_k = U_k P_k U$$

pour $U : \mathcal{H} \to \mathcal{H}'$ un opérateur OCPS, une mesure de Von Neumann $A = \sum_{i=1}^m a_i P_i$ sur $\mathcal{H}'$ et $\{U_i\}_{i=1}^m$ des opérateurs OCPS tels que $U_k : \mathcal{V}_k \to \mathcal{H}'$ et $P_k U(\mathcal{H}) \subseteq \mathcal{V}_k \subseteq \mathcal{H}'$. Ici $U(\mathcal{H})$ dénote le sous-espace engendré par U lorsqu'appliqué aux éléments de $\mathcal{H}$.

Pour l'analyse des protocoles en cryptographie quantique, la matrice U nous donne à peu près tout ce dont nous avons besoin. Un opposant qui participe à un protocole cryptographique a pour but d'obtenir le plus d'information illicite possible. Pour chaque résultat k, le maximum d'information est obtenu lorsque P_k projette sur des rayons. Dans ce cas $A = \sum_i a_i P_i$ est une mesure de Von Neumann sur l'espace $\mathcal{H}'$. Dans le cas contraire, certains résultats k sont encore raffinables car P_k projette sur un sous-espace de plus d'une dimension. La mesure est donc incomplète. On peut toujours considérer que la mesure est complète auquel cas les projections $\{P_i\}_{i=1}^m$ sont orthogonales et projettent sur des sous-espaces de dimension 1 (des rayons). Dans ce cas et sans perdre de généralités $P_k U$ peut être associé à la k ième ligne de U. L'application de l'opérateur U_k est sans importance quant à l'information sur $|\phi\rangle$ que donne le résultat de la mesure. Il est toujours possible de choisir $\mathcal{H}'_k = P_k U(\mathcal{H})$ et de prendre U_k comme la matrice identité dans $\mathcal{H}'_k$. Si après avoir mesuré $|\phi\rangle$ le résultat k est obtenu, l'information sur $|\phi\rangle$ divulguée par la mesure est définie entièrement par la k ième ligne de U. Pour s'en convaincre considérons le vecteur

$$\mathbf{w} = U|\phi\rangle = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix}.$$

Puisque $|\phi\rangle$ est un état pur, sa norme vaut 1. De plus, les colonnes de U sont orthonormées ce qui implique que $\|\mathbf{w}\|^2 = \sum_{i=1}^m |w_i|^2 = 1$. Les composantes de $\mathbf{w}$ induisent une mesure de probabilité de la transition de l'état $|\phi\rangle$ vers le résultat $k \in \{1, \ldots, m\}$.

Lorsque $\mathbf{w}$ est interprété comme un vecteur d'état dans $\mathcal{H}'$, une mesure de Von Neumann sur $|\mathbf{w}\rangle$ peut toujours être considérée comme projetant sur P_k avec probabilité $|w_k|^2$. Pour une mesure de Von Neumann $A' = \sum_{i=1}^m a_i' P_i'$, le résultat k est obtenu, d'après l'équation 1.11, avec probabilité

$$\begin{aligned} p_\phi(k) &= \|P_k' U|\phi\rangle\|^2 \\ &= \|P_k'|\mathbf{w}\rangle\|^2. \end{aligned}$$

Soit $A = \sum_{i=1}^m a_i P_i$ la mesure de Von Neumann qui projette sur les rangées de U. La projection P_k pour $k \in \{1, \ldots, m\}$ est représentée par une matrice $\mathrm{Dim}(\mathcal{H}') \times \mathrm{Dim}(\mathcal{H}')$ dont le seul élément non nul est un 1 en position k de sa diagonale principale. Il existe toujours une transformation unitaire R telle que

$$P_k'|\mathbf{w}\rangle = P_k R|\mathbf{w}\rangle = P_k RU|\phi\rangle.$$

En posant $U' = RU$ on a bien que

$$p_\phi(k) = \|P_k U'|\phi\rangle\|^2 \tag{1.13}$$

pour U' un opérateur OCPS. Les lignes de U' sont donc en correspondance avec chacun des résultats possibles de la mesure. Par la suite un opérateur OCPS U qui modélise une mesure sera considéré sous la forme représentée à l'équation 1.13 avec $\{P_i\}_{i=1}^m$ les projections sur chacune des lignes de U.

Dans certains scénarios, comme ceux habituellement fournis par la cryptographie quantique, il est utile d'exprimer les colonnes U dans une base spécifique pour $\mathcal{H}$. Par exemple, une mesure à m résultats sur n bits encodés par le codage BB84 peut être représentée par un opérateur U à 2^n colonnes. Supposons que le système $|\phi\rangle$ qui encode la chaîne $b = b_1, \ldots, b_n$ ait été formé par

$$|\phi\rangle = \bigotimes_{i=1}^n |b_i\rangle_{\theta_i}$$

avec $\theta_i \in \{+, \times\}$ pour chaque $i \in \{1, \ldots, n\}$. La séquence de bases $\theta_1, \ldots, \theta_n$ est une base pour l'espace composé de n photons. Elle contient les 2^n vecteurs formés par

$$\theta = \bigotimes_{i=1}^n \theta_i$$

pour $+ = \{|\rightarrow\rangle, |\uparrow\rangle\}$ et $\times = \{|\nearrow\rangle, |\nwarrow\rangle\}$. Par l'hypothèse sur la façon dont est construit $|\phi\rangle$, on peut supposer que chacune de ses composantes est étiquetée par une chaîne dans $\{0,1\}^n$. La seule composante non nulle est celle dont l'étiquette est la chaîne b. Ce qui nous donne,

$$P_k U|\phi\rangle = U_{k,b}$$

où $U_{k,b}$ est la composante de U en rangé k et dans la colonne étiquetée par la chaîne b. La probabilité d'obtenir le résultat k lorsque $|\phi\rangle$ est mesuré est

$$p_\phi(k) = |U_{k,b}|^2.$$

L'interprétation est que chacune des entrées (k,b) de U donne l'amplitude de transition de la chaîne b encodée dans la base θ vers le résultat k. Le carré de la norme de cette amplitude est la probabilité d'obtenir le résultat k lorsque l'état $|\phi\rangle = |b\rangle_\theta$ est mesuré.

1.12 Conclusion

Dans ce chapitre nous avons passé en revue les outils nécessaires à la compréhension de la suite. Nous avons vu comment un bit d'information classique est encodé de façon équivoque dans la polarisation d'un photon. Ce codage, appelé codage BB84, est au centre de la plupart des protocoles cryptographiques quantiques dont, notamment, le protocole de transmission inconsciente BBCS [13] et de camouflage BCJL [21]. Nous avons vu que le codage BB84 a la propriété de ne donner aucune information au receveur sur la base utilisée pour transmettre un bit. Cette propriété sera utilisée au chapitre 3 comme la base d'un protocole simple d'identification quantique.

Nous avons aussi traité des modèles pour la représentation générale des mesures en mécanique quantique. Contrairement aux mesures de Von Neumann, ces modèles généraux permettent l'analyse des scénarios où l'observateur peut tirer avantage à mesurer de façon incomplète un système en attendant un supplément d'information pour compléter la mesure. C'est le cas pour le protocole BBCS où ce type de mesure peut aider un participant malhonnête à obtenir un maximum d'information illicite. Le modèle OCPS nous sera utile au chapitre 2 pour l'analyse de la sécurité du protocole

BBCS contre les mesures individuelles et au chapitre 4 pour l'analyse de sécurité d'une variante du protocole de mise en gage BCJL.

Chapitre 2

Transmission inconsciente quantique

2.1 Introduction

Ce chapitre traite du protocole de transmission inconsciente BBCS [13]. C'est autour de ce protocole qu'en grande partie cette thèse s'articule. Après avoir revu les spécifications abstraites de la transmission inconsciente, nous verrons comment le protocole BBCS la réalise. Nous reviserons la méthode utilisée pour protéger $\mathcal{A}$lice contre les mesures incomplètes de $\mathcal{B}$ob, et celles qui permettent la tolérance au bruit de transmission.

Ce chapitre fait l'analyse de la sécurité du protocole BBCS contre toutes les mesures individuelles permises par la mécanique quantique. Cette analyse s'applique au scénario général où une chaîne de $O(n)$ bits parmi deux est transmise sur un canal quantique sujet au bruit. Nous supposons qu'un protocole de mise en gage parfait est disponible. Cette supposition sera levée au chapitre 4 par la démonstration qu'un procole de mise en gage, appelé BCJL renversé, est sécuritaire contre les mesures individuelles.

Après la publication de ce résultat obtenu conjointement avec D. Mayers [54], A. C. Yao [71] a donné une preuve de la sécurité de BBCS contre toutes les mesures autorisées par les principes de la mécanique quantique aussi sous l'hypothèse que des mises en gage parfaites existent. Malheureusement un résultat récent de D. Mayers [53] montre qu'il est impossible de faire mieux car aucune mise en gage quantique parfaite ne peut exister. Le scénario étudié est celui où le canal quantique est parfait et la chaîne transmise est un bit. Nous terminerons ce chapitre par une discussion sur la possibilité de généraliser notre résultat à l'ensemble des mesures permises dans le scénario le plus général.

2.2 Tâches abstraites

Avant de présenter un protocole pour la transmission inconsciente, nous devons voir ce que cette tâche doit exactement réaliser. La définition du fonctionnement d'une tâche en terme de ses entrées et de ses sorties est appelée *tâche abstraite.* Elle ne fait aucun cas d'une réalisation particulière mais elle définit ce qu'une réalisation doit accomplir pour qu'elle soit considérée sécuritaire. La définition abstraite peut être donnée en plusieurs saveurs. Dépendant du modèle adopté, la bonne saveur est utilisée pour montrer qu'une réalisation particulière répond aux exigeances de sa définition abstraite. La saveur inconditionnelle est celle qui détermine les conditions les plus robustes et par conséquent les plus difficiles à satisfaire. La saveur statistique est en quelque sorte une variante de la saveur inconditionnelle où une déviation exponentiellement faible est tolérée. Dans ce modèle, un facteur de sécurité n apparaît, et une augmentation linéaire en n induit un rapprochement exponentiellement rapide vers la saveur inconditionnelle. Le troisième saveur est dite calculatoire. Elle est utilisée lorsque le modèle de communication sous-jacent limite la puissance de calcul des acteurs. C'est la saveur adoptée lorsqu'il n'y a pas d'hypothèses physiques sur le canal qui relie les participants. La cryptographie basée sur l'existence des fonctions à sens unique ou des fonctions à trappes est de cette nature [48]. Une fois posée l'hypothèse de l'existence de ces fonctions, aucune hypothèse supplémentaire n'est nécessaire. La cryptographie quantique étant basée sur l'existence d'un canal où transite des photons qui sont soumis aux principes généraux de la mécanique quantique, on doit s'attendre à ce que la saveur adoptée soit inconditionnelle ou statistique. De par la nature probabiliste de la mécanique quantique c'est la saveur statistique qui déterminera la formulation abstraite des tâches à réaliser.

2.2.1 Transmission inconsciente inconditionnelle

Si on veut caractériser l'information à laquelle les participants à une tâche cryptographique ont droit, il nous faut une mesure de l'information. La théorie de l'information fournit l'instrument prévilégié (et dans une certaine mesure le seul [63]) pour mesurer l'information associée à la réalisation d'événements aléatoires. L'information moyenne que le résultat d'une expérience aléatoire divulgue correspond à l'incertitude sur le résultat avant la réalisation de cette expérience. Ces deux concepts sont interchangeables.

Soit $\mathcal{D} = \{p_1, \ldots, p_n\}$ une distribution de probabilité. Notons par $X \in_{\mathcal{D}} \{e_1, e_2, \ldots, e_n\}$ une variable aléatoire qui prend la valeur e_i avec probabilité p_i. L'incertitude ou l'entropie associée à la réalisation d'un événement $X \in_{\mathcal{D}} \{e_1, e_2, \ldots, e_n\}$ est définie par

$$\mathbf{H}(X) \triangleq \mathbf{H}(p_1, \ldots, p_n) = -\sum_{i=1}^{n} p_i \lg p_i \tag{2.1}$$

où lg indique le logarithme en base 2. Le bit est l'unité de mesure de la fonction $\mathbf{H}(X)$ lorsqu'elle est définie comme à l'équation 2.1. Lorsque $\mathbf{H}(X) = \lg n$ l'incertitude est maximum. L'entropie conditionnelle, notée $\mathbf{H}(X|Y = y)$, est l'incertitude sur la variable aléatoire X étant donné la réalisation de l'événement $Y = y$. Nous définissons l'entropie conditionnelle par:

$$\mathbf{H}(X|Y = y) = -\sum_{i=1}^{n} \mathrm{P}\left(X = e_i | Y = y\right) \lg \mathrm{P}\left(X = e_i | Y = y\right).$$

De la même façon, nous notons

$$\mathbf{H}(X|Y = y, Z = z) = -\sum_{i=1}^{n} \mathrm{P}\left(X = e_i | Y = y \wedge Z = z\right) \lg \mathrm{P}\left(X = e_i | Y = y \wedge Z = z\right).$$

Si Y est une variable aléatoire à m éventualités, l'entropie conditionnelle de X étant donné Y est

$$\mathbf{H}(X|Y) = \sum_{j=1}^{m} \mathrm{P}\left(Y = y_j\right) \mathbf{H}(X|Y = y_j).$$

L'information qu'une variable aléatoire Y donne sur X est donnée par

$$\mathbf{I}(X|Y) = \mathbf{H}(X) - \mathbf{H}(X|Y).$$

L'information mesure la réduction moyenne de l'incertitude que la connaissance de Y donne sur X. Si X est une variable aléatoire de Bernoulli avec paramètre p alors nous dénoterons par $\mathbf{H}(p)$ l'incertitude $\mathbf{H}(p, 1-p)$ sur X. Pour plus de détails sur la théorie de l'information, consulter [2] ou [40].

Revenons maintenant au problème de formuler abstraitement ce que la tâche de transmission inconsciente doit accomplir. En ce sens nous reprenons la formulation de [25]. Il y a plusieurs façons de définir la tâche de transmission inconsciente. En réalité la transmission inconsciente est une tâche générique qui peut désigner l'une ou l'autre (et même davantage) de ces saveurs:

1. La transmission inconsciente d'un bit parmi deux, notée $\binom{2}{1}$–TI_1,
2. la transmission inconsciente d'un bit parmi r, notée $\binom{r}{1}$–TI_1,
3. la transmission inconsciente d'un message de m bits parmi deux, notée $\binom{2}{1}$–TI_m ou
4. toutes les variations obtenus à partir de 2 et 3.

Nous allons définir abstraitement la première primitive $\binom{2}{1}$–TI_1 qui est la plus simple et à partir de laquelle les autres peuvent être facilement définies.

Deux notions indépendantes traduisent ce qu'on entend par un protocole cryptographique sécuritaire [23]. Premièrement, il doit faire ce qu'il a à faire. Un protocole qui répond à ce critère est dit *correct.* Deuxièmement, il ne doit pas laisser filer l'information qui n'est pas prévue explicitement par la tâche abstraite. Un protocole avec cette propriété est dit *privé.* Dans le cas qui nous intéresse on peut formuler la tâche abstraite de transmission inconsciente $\binom{2}{1}$–TI_1 sous ces deux rapports.

Protocoles pour le transmission inconsciente

En général un protocole interactif entre $\mathcal{A}$lice et $\mathcal{B}$ob est spécifié par l'algorithme $\mathcal{A}$ d'$\mathcal{A}$lice et $\mathcal{B}$ de $\mathcal{B}$ob fonctionnant chacun sur une machine de Turing interactive. Un protocole pour la transmission inconsciente quantique est déterminé par les algorithmes des machines de Turing interactives $\mathcal{A}$ et $\mathcal{B}$ respectivement. Les machines $\mathcal{A}$

et $\mathcal{B}$ sont reliées par un ruban commun qui modélise un canal public entre $\mathcal{A}$lice et $\mathcal{B}$ob. Les deux acteurs peuvent lirent et écrirent sur ce ruban. Finalement, les machines $\mathcal{A}$ et $\mathcal{B}$ peuvent communiquer par un canal quantique en spécifiant l'état du photon transmis par l'envoyeur et la mesure effectuée par le receveur. Pour que les machines $\mathcal{A}$ et $\mathcal{B}$ soient probabilistes, nous supposerons aussi qu'elles ont chacune accès à une source aléatoire de bits. Les deux sources sont indépendantes.

Comme l'analyse de la sécurité des protocoles cryptographiques requiérent l'étude des comportements déviants des acteurs, le cas où les algorithmes d'$\mathcal{A}$lice et $\mathcal{B}$ob dévient par rapport aux spécifications doit être envisagé. Par la suite, nous noterons $\mathcal{A}$ et $\mathcal{B}$ les algorithmes honnêtes prescrits par les spécifications du protocole tandis que $\mathcal{A}^*$ et $\mathcal{B}^*$ noterons n'importe quels algorithmes qu'$\mathcal{A}$lice et $\mathcal{B}$ob malhonnétes pourraient exécuter. Nous noterons $\mathcal{A}$lice* une $\mathcal{A}$lice malhonnête et $\mathcal{B}$ob* un $\mathcal{B}$ob malhonnête.

Être correct

Pour être correct un protocole pour $\binom{2}{1}$–TI_1 doit accepter les entrées suivantes.

$\mathcal{A}$lice: deux bits (q_0, q_1),

$\mathcal{B}$ob: un bit de sélection c.

En fonction de ces entrées, la sortie suivante doit être obtenue:

$\mathcal{B}$ob: le bit q_c.

Un protocole $\binom{2}{1}$–TI_1 correct donne la garantie que si les participants $\mathcal{A}$lice et $\mathcal{B}$ob sont honnêtes, le protocole aura la dépendance voulue entre les entrées et les sorties.

Être privé

Ici on détermine ce qui touche davantage à la nature cryptographique de la primitive. À la façon de [25] on dénote par $V_P(H, q_0, q_1, c)$ la variable aléatoire qui détermine l'information qu'un participant P obtient suite à l'exécution sur les entrées q_0, q_1 et c. La variable H est une variable aléatoire pour l'information de P avant l'exécution du protocole. Le comportement du participant P est représenté par un programme quelconque qui peut dévier autant qu'il veut de la marche à suivre.

Pour qu'un protocole pour $\binom{2}{1}$–$\mathrm{TI}_1(q_0, q_1)(c)$ soit privé, il faut que pour tout programme $\mathcal{A}^*$ pour $\mathcal{A}$lice, aucune information sur c ne puisse être obtenue. Du point de vue de $\mathcal{B}$ob*, les entrées d'$\mathcal{A}$lice q_0 et q_1 sont des variables aléatoires. De la même façon, du point de vue d'$\mathcal{A}$lice* c peut être vue comme une variable aléatoire. Pour x un paramètre ou une variable privée spécifiée dans l'exécution d'un protocole entre $\mathcal{A}$lice et $\mathcal{B}$ob. Nous noterons $\mathbf{x}$ la variable aléatoire associée aux choix possibles de x pour une exécution du protocole. Par la suite nous adopterons aussi cette convention lorsque x est une variable quelconque définie en fonction d'expériences aléatoires.

Formellement, un protocole pour $\binom{2}{1}$–TI_1 est privé si pour tout $\mathcal{A}^*, H, q_0$ et q_1,

$$\mathbf{H}(\mathbf{c}|V_{\mathcal{A}^*}(H, q_0, q_1, c)) = \mathbf{H}(\mathbf{c}|\mathbf{H} = H, \mathbf{q}_0 = q_0, \mathbf{q}_1 = q_1).$$

Du coté de $\mathcal{B}$ob maintenant. Peu importe son programme $\mathcal{B}^*$ il doit lui être impossible d'obtenir de l'information sur q_0 et q_1 simultanément. Lorsque la transmission lui apprend la valeur du bit q_c, l'incertitude sur q_{1-c} doit demeurer ce qu'elle était avant l'exécution. Ceci doit rester vrai pour tout programme $\mathcal{B}^*$ pour $\mathcal{B}$ob*. Ainsi, un protocole pour $\binom{2}{1}$–$\mathrm{TI}_1(q_0, q_1)(c)$ est privé pour $\mathcal{A}$lice si pour tout $\mathcal{B}^*, H, c$ et $q_0, q_1 \in \{0, 1\}$, $\exists \tilde{\mathbf{c}} \in \{0, 1\}$,

$$\mathbf{H}(\mathbf{q}_{\tilde{\mathbf{c}}}|V_{\mathcal{B}^*}(H, q_0, q_1, c), \mathbf{q}_{1-\tilde{\mathbf{c}}} = q_{1-\tilde{\mathbf{c}}}) = \mathbf{H}(\mathbf{q}_{\tilde{\mathbf{c}}}|\mathbf{H} = H, \mathbf{c} = c, \mathbf{q}_{1-\tilde{\mathbf{c}}} = q_{1-\tilde{\mathbf{c}}}).$$

Autrement dit, peu importe le comportement du programme $\mathcal{B}^*$, les entrées q_0, q_1 d'$\mathcal{A}$lice et le choix c de $\mathcal{B}$ob*, il existe toujours un index $\tilde{c}$ tel que l'information sur la chaîne $q_{\tilde{c}}$ après l'exécution reste inchangée par rapport à avant l'exécution.

Pour se convaincre qu'il s'agit d'une définition adéquate pour la transmission inconsciente consulter [22].

La saveur statistique

La saveur statistique est obtenue facilement à partir de la saveur inconditionnelle. Il s'agit des mêmes conditions auxquelles nous permettons une déviation exponentiellement faible. Autrement dit, les deux saveurs de sécurité sont tellement près l'une de l'autre qu'il faudrait exécuter un protocole un nombre exponentiel de fois, en fonction d'un facteur de sécurité n, pour distinguer entre les deux saveurs. Plus précisément, un protocole de transmission inconsciente est statistiquement privé si pour $\alpha > 0$,

1. Pour tout $\mathcal{A}^*, H, q_0$ et q_1,

$$\mathbf{H}(c|V_{\mathcal{A}^*}(H, q_0, q_1, c)) \geq \mathbf{H}(c|\mathbf{H} = H, \mathbf{q}_0 = q_0, \mathbf{q}_1 = q_1) - 2^{-\alpha n} \, et$$

2. pour tout $\mathcal{B}^*, H, c$ et $q_0, q_1 \in \{0,1\}$, $\exists \tilde{c} \in \{0,1\}$,

$$\mathbf{H}(\mathbf{q}_{\tilde{c}}|V_{\mathcal{B}^*}(H, q_0, q_1, c), \mathbf{q}_{1-\tilde{c}} = q_{1-\tilde{c}}) \geq \mathbf{H}(\mathbf{q}_{\tilde{c}}|\mathbf{H} = H, \mathbf{c} = c, \mathbf{q}_{1-\tilde{c}} = q_{1-\tilde{c}}) - 2^{-\alpha n}.$$

Nous pouvons aussi définir ce qu'est un protocole statisquement correct en exigeant qu'il se comporte comme la version inconditionnelle sauf avec probabilité négligeable $2^{-\alpha n}$ pour $\alpha > 0$. Ainsi, un protocole pour la transmission inconsciente est statistiquement correct si pour les entrées:

$\mathcal{A}$lice: deux bits (q_0, q_1),

$\mathcal{B}$ob: un bit de sélection c,

la sortie suivante doit être obtenue sauf avec probabilité négligeable $2^{-\alpha n}$ pour $\alpha > 0$ en autant que n soit suffisamment grand:

$\mathcal{B}$ob: le bit q_c.

2.3 Le protocole BBCS

En premier lieu, nous présentons le protocole BBCS pour $\binom{2}{1}$–TI$_1$ sécuritaire contre les mesures de Von Neumann. Nous verrons à la section suivante que ce protocole souffre de faiblesses contre certaines attaques plus générales que celles pouvant être montées à l'aide des mesures de Von Neumann. À la section 2.5 le protocole complet sera présenté. Il consistera en l'ajout d'un test à celui présenté ici. Nous noterons par $\binom{2}{1}$–TI$_1^*$ cette version plus faible.

Le symbole Ⓒ dénote une variable aléatoire dans $\{0,1\}$ telle que

$$\mathrm{P}\left(\text{Ⓒ}=0\right)=\mathrm{P}\left(\text{Ⓒ}=1\right)=\frac{1}{2}.$$

Pour $a_0, a_1, \ldots, a_j$ une liste ordonnée d'éléments,

$$[a_0, \ldots, a_j]_k = a_k, k \in \{0, 1, \ldots, j\}$$

est la fonction qui sélectionne le k-ième élément de la liste. Le protocole 2.3.1 donne une réalisation quantique de $\binom{2}{1}$–$\mathrm{TI}_1^*(q_0, q_1)(c)$.

À l'étape 1, $\mathcal{A}$lice envoie la chaîne aléatoire $b = b_1, b_2, \ldots, b_n$ encodé par le codage BB84 avec la séquence de bases $\theta = \theta_1, \ldots, \theta_n$. $\mathcal{B}$ob détermine la séquence de bases $\widehat{\theta} = \widehat{\theta_1}, \ldots, \widehat{\theta_n}$ pour le décodage. Comme nous l'avons vu au chapitre 1, pour environ la moitié des positions $i \in \{1, 2, \ldots, n\}$(les positions pour lesquelles $\widehat{\theta}_i = \theta_i$) $\mathcal{B}$ob obtiendra le bit $\widehat{b}_i = b_i$. Lorsque $\widehat{\theta}_i \neq \theta_i$ le bit reçu $\widehat{b}_i$ est non-corrélé avec la bit b_i envoyé par $\mathcal{A}$lice, celle-ci n'a aucun moyen de déterminer les positions i pour lesquelles $\mathcal{B}$ob a obtenu le bon bit. Ceci reste vrai même après qu'elle ait vu la composition des ensembles I_0, I_1 à l'étape 3. Une fois qu'$\mathcal{A}$lice a annoncé la séquence de bases d'émission à l'étape 2, seul $\mathcal{B}$ob peut déterminer les positions des bits qui ont été bien reçus et celles où un bit non-corrélé a été obtenu. À l'étape 3, $\mathcal{B}$ob regroupe les positions i telles que $\widehat{\theta}_i = \theta_i$ et celles où $\widehat{\theta}_i \neq \theta_i$ en deux ensembles I_c et I_{1-c} respectivement. $\mathcal{B}$ob ne peut pas former deux ensembles de bits connus. Puisque $I_0 \cap I_1 = \emptyset$ et $\#I_0 = \#I_1 = \frac{n}{3}$, pour qu'à la fois I_0 et I_1 contiennent que des bits bien reçus, il faudrait que $\#\{i|\widehat{\theta}_i = \theta_i\} \geq \frac{2n}{3}$. Cet événement ne se produit qu'avec probabilité exponentiellement faible. Sauf avec probabilité négligeable, une fraction près de $\frac{1}{2}$ des bits dans I_{1-c} seront inconnus de $\mathcal{B}$ob. Ce qui est amplement suffisant pour conclure que le ou-exclusif ($\oplus$) des bits de l'ensemble I_{1-c} est inconnu de $\mathcal{B}$ob car dès qu'un bit de l'ensemble est inconnu le ou-exclusif l'est aussi. Seul le ou-exclusif des bits de l'ensemble I_c peut être déterminé par $\mathcal{B}$ob. À l'étape 4, $\mathcal{A}$lice encode les bits q_0 et q_1 qu'elle veut transmettre grâce au ou-exclusif des bits dans I_0 et I_1 respectivement et annonce q_0' et q_1'. $\mathcal{B}$ob qui peut déterminer le ou-exclusif des bits de I_c peut retrouver q_c à l'aide de q_c'. C'est ce qu'il fait à l'étape 5. Une formalisation de cette discussion montre que le protocole est correct [25] en autant que la canal quantique soit parfait.

Protocole 2.3.1 ($\binom{2}{1}$**–TI**$_1^*(q_0,q_1)(c)$**[23]**)

1: $\mathbf{FAIRE}_{i=1}^{n}$

- $\mathcal{A}$lice pige $b_i \leftarrow$ ©,
- $\mathcal{A}$lice pige $\beta_i \leftarrow$ © et détermine sa i-ième base d'émission $\theta_i \leftarrow [+,\times]_{\beta_i}$,
- $\mathcal{A}$lice transmet à $\mathcal{B}$ob le photon π_i avec polarisation $|b_i\rangle_{\theta_i}$,
- $\mathcal{B}$ob pige le bit $\widehat{\beta}_i \leftarrow$ © et mesure π_i dans la base $\widehat{\theta}_i \leftarrow [+,\times]_{\widehat{\beta}_i}$,
- $\mathcal{B}$ob pose $\widehat{b}_i \leftarrow \begin{cases} 0 & \text{si } \pi_i \text{ est observé comme } |0\rangle_{\widehat{\theta}_i} \\ 1 & \text{si } \pi_i \text{ est observé comme } |1\rangle_{\widehat{\theta}_i} \end{cases}$,

2: $\mathcal{A}$lice annonce $\theta_1,\theta_2,\ldots,\theta_n$,

3: $\mathcal{B}$ob forme deux ensembles $I_c, I_{1-c} \subseteq \{1,2,\ldots,n\}$ tels que $I_c \cap I_{1-c} = \emptyset, \#I_c = \#I_{1-c} = \frac{n}{3}$ et pour chaque $i \in I_c, \widehat{\theta}_i = \theta_i$. $\mathcal{B}$ob annonce (I_0,I_1) à $\mathcal{A}$lice,

4: $\mathcal{A}$lice calcule

$$q_0' = q_0 \oplus \bigoplus_{i\in I_0} b_i \text{ et } q_1' = q_1 \oplus \bigoplus_{i\in I_1} b_i,$$

et transmet (q_0', q_1') à $\mathcal{B}$ob,

5: $\mathcal{B}$ob calcul

$$b_c = q_c' \oplus \bigoplus_{i\in I_c} \widehat{b}_i.$$

FIG. 2.1 - *Transmission inconsciente simplifiée.*

En effet pour que le protocole soit conforme à sa spécification, il faut qu'à toutes les fois que $\widehat{\theta}_i = \theta_i$ le bon bit b_i soit décodé par $\mathcal{B}$ob. Nous verrons plus loin comment modifier le protocole pour qu'il tolère le bruit lors de la transmission sur le canal quantique. Il s'agit de la contribution principale de [13].

Les mesures de Von Neumann ne peuvent rien contre ce protocole. C'est ce que nous allons voir à la prochaine section.

2.4 BBCS contre les mesures de Von Neumann

La première étape pour l'étude de la sécurité du protocole BBCS consiste à limiter les mesures qui peuvent être faites par un opposant au protocole. Une telle approche est celle adoptée par [25]. Ce type d'hypothèses n'a pas d'influence sur l'information que peut soutirer $\mathcal{A}$lice* en participant avec un $\mathcal{B}$ob honnête. Nous supposons également que le canal quantique n'est pas sujet au bruit. La participation d'$\mathcal{A}$lice au protocole se limite à émettre des photons et fournir de l'information classique à $\mathcal{B}$ob. Elle n'effectue, pour le moment, aucune mesure.

Vérifions si le protocole $\binom{2}{1}$–TI_1^* est sécuritaire du point de vue de $\mathcal{B}$ob, à savoir si, peu importe le programme $\mathcal{A}^*$ pour $\mathcal{A}$lice malhonnête, le bit de sélection c reste secret à $\mathcal{A}$lice après l'interaction.

Théorème 5 ([25]) $\forall \mathcal{A}^*, H, q_0, q_1, c$

$$\mathbf{H}(\mathbf{c}|V_{\mathcal{A}^*}(H, q_0, q_1, c)) = \mathbf{H}(\mathbf{c}|\mathbf{H} = H, \mathbf{q}_0 = q_0, \mathbf{q}_1 = q_1).$$

Idée de la preuve. Avant l'exécution de $\binom{2}{1}$–$\mathrm{TI}_1^*(q_0, q_1)(c)$, $\mathcal{A}$lice* a $\mathbf{H}(\mathbf{c}|\mathbf{H} = H, \mathbf{q}_0 = q_0, \mathbf{q}_1 = q_1)$ bits d'incertitude sur c. Peu importe le programme $\mathcal{A}^*$, la seule information que l'exécution du protocole divulgue a $\mathcal{A}$lice* est la composition des deux ensembles (I_0, I_1). Pour toute paire (I_0, I_1) la distribution pour le bit c est la même pour $\mathcal{A}$lice* puisqu'elle dépend seulement de la concordance entre θ et $\widehat{\theta}$. Or, $\mathcal{A}$lice* n'a aucune information sur $\widehat{\theta}$. Une formalisation de cette discussion permet d'obtenir l'énoncé du théorème. Remarquons que la sécurité obtenue est inconditionnelle.

∎

C'est pour l'analyse de la sécurité du point de vue d'$\mathcal{A}$lice qu'une hypothèse sur le type de mesures possibles entre en jeu. Ici nous autorisons seulement les mesures de Von Neumann. Rappelons-nous qu'une mesure de Von Neumann sur un photon π_i est modélisée par une paire de projections orthogonales $\{P_i, P_i^{\perp}\}$. Le théorème suivant montre que limité à ces mesures, $\mathcal{B}$ob* reste impuissant à obtenir de l'information sur q_0 et q_1 simultanément. Cette fois-ci, on obtient une sécurité à saveur statistique.

Théorème 6 ([25]) $(\exists \alpha > 0)(\exists n_0)(\forall n \geq n_0)(\forall H, q_0, q_1, c)(\exists \tilde{c} \in \{0, 1\})$

$$\mathbf{H}(\mathbf{q}_{\tilde{c}} | V_{\mathcal{B}^*}(H, q_0, q_1, c), \mathbf{q_{1-\tilde{c}}} = q_{1-\tilde{c}}) \geq \mathbf{H}(\mathbf{q}_{\tilde{c}} | \mathbf{H} = H, \mathbf{c} = c, \mathbf{q}_{1-\tilde{c}} = q_{1-\tilde{c}}) - 2^{-\alpha n}.$$

Un argument géométrique peut servir à nous convaincre de la véracité du théorème 6. Au moment où $\mathcal{B}$ob* détermine sa i-ième mesure de Von Neumann $M_i = \{P_i, P_i^{\perp}\}$, la base utilisée par $\mathcal{A}$lice lui est inconnue. Soit $\vartheta_i \in \{+, \times\}$ la base pour laquelle le mesure M_i donne la moins bonne approximation, alors pour ϑ_i^c la base opposée à ϑ_i on a que

$$\langle 0|_{\vartheta_i} P_i |0\rangle_{\vartheta_i} \leq \langle 0|_{\vartheta_i^c} P_i |0\rangle_{\vartheta_i^c}$$

et

$$\langle 1|_{\vartheta_i} P_i |1\rangle_{\vartheta_i} \leq \langle 1|_{\vartheta_i^c} P_i |1\rangle_{\vartheta_i^c}.$$

Comme nous l'avons vu à la section 1.7, la meilleure mesure de Von Neumann pour déterminer le bit b_i est celle dont les projections $\{P_i, P_i^{\perp}\}$ coïncident avec l'angle de Breidbart et l'angle qui lui est orthogonal. C'est donc dire que la base ϑ_i ne peut donner le bit b_i avec probabilité meilleure que la mesure de Breidbart. La probabilité d'observer le mauvais bit $\widehat{b}_i = 1 - b_i$ lorsque l'état du photon π_i est $|b_i\rangle_{\vartheta_i}$ est

$$\frac{1}{2} \geq \mathrm{P}\left(\widehat{\mathbf{b}}_i = 1 - b_i | \theta_i = \vartheta_i\right) \geq 1 - \cos^2 \frac{\pi}{8} \geq 0.15.$$

Puisque la probabilité que la base d'émission θ_i soit la base ϑ_i est exactement $\frac{1}{2}$, environ la moitié des positions $i \in \{1, \ldots, n\}$ sont telles que

$$\frac{1}{2} \geq \mathrm{P}\left(\widehat{\mathbf{b}}_i = 1 - b_i\right) \geq 1 - \cos^2 \frac{\pi}{8}. \tag{2.2}$$

Sauf avec probabilité négligeable $2^{-\alpha n}$ pour $\alpha > 0$, un des deux ensembles $I_{\widehat{c}}$ contient au moins $\frac{n}{12}$ positions pour lesquelles l'équation 2.2 est vérifiée. Ceci parce que $\frac{n}{2}$

positions $i \in \{1, \ldots, n\}$ sont telles que $\theta_i = \vartheta_i$ et même en choisissant $\frac{n}{3}$ de ces positions comme ne faisant pas partie de $I_0 \cup I_1$, il demeure $\frac{n}{6}$ posistions pour lesquelles l'équation 2.2 est observée. Même en distribuant celles-ci également entre I_0 et I_1, $\frac{n}{12}$ bits ne sont pas mieux connus que ce que l'équation 2.2 nous indique. Par conséquent, le ou-exclusif des bits b_i pour $i \in I_{\widehat{c}}$ n'est pas approximable par $\mathcal{B}$ob* car une bonne proportion de ceux-ci sont reçus comme s'ils étaient transmis sur canal symétrique binaire avec taux d'erreur 0.15. Aucune information substantielle n'est obtenue par $\mathcal{B}$ob* au sujet du bit $q_{\widehat{c}}$. Pour une preuve formelle du théorème 6, consulter [25].

Une mesure qui brise $\binom{2}{1}$–$\mathbf{TI}_1^*$

Rien de plus facile pour $\mathcal{B}$ob* qui dispose d'un réfrigérateur d'obtenir l'information complète sur q_0 et q_1 à tout coup. Il s'agit pour lui d'exécuter une mesure semblable à celle que nous avons vue à la section 1.10.1. Aucune information sur $q_{\widehat{c}}$ ne peut être obtenue par $\mathcal{B}$ob* à condition qu'il mesure complètement les photons reçus avant qu'$\mathcal{A}$lice n'annonce la séquence de bases $\theta = \theta_1, \theta_2, \ldots, \theta_n$ (étape 4). Si au moment ou $\mathcal{B}$ob* reçoit le photon π_i il le range de façon à ne pas modifier son état, alors il peut apprendre la valeur du bit b_i. Il lui suffit de faire la mesure inutile $\mathbf{I}_2$ sur chaque photon. Par définition de la mesure inutile, ceux-ci restent intacts. Une fois qu'$\mathcal{A}$lice lui annonce sa séquence de bases θ pour chaque position i, $\mathcal{B}$ob* complète sa mesure en choisissant la mesure de Von Neumann $\{P_i, P_i^{\perp}\}$ qui projètte sur les rayons qui coïncident avec θ_i. Le tour est joué, tous les bits de la chaîne $b = b_1, \ldots, b_n$ sont maintenant connus de $\mathcal{B}$ob*. Par conséquent il apprend q_0 et q_1 à tout coup.

Pour empêcher $\mathcal{B}$ob* d'exécuter cette mesure, $\mathcal{A}$lice doit s'assurer que $\mathcal{B}$ob* a déjà mesuré les photons qu'il a reçus avant qu'elle n'annonce la séquence de bases θ. Cette vérification peut être effectuée en faisant appel à une autre primitive cryptographique appelée *mise en gage* dont nous parlons à la section suivante.

2.5 Mises en gage quantiques

Pour qu'$\mathcal{A}$lice puisse s'assurer que $\mathcal{B}$ob* a bien mesuré les photons envoyés, on doit pouvoir disposer d'une primitive qui permet à $\mathcal{B}$ob* de dissimuler le résultat de sa mesure jusqu'à ce qu'$\mathcal{A}$lice lui demande de le révéler. $\mathcal{B}$ob* ne doit pas pouvoir changer l'information camouflée une fois qu'il l'a fournie à $\mathcal{A}$lice. Une telle primitive produit un camouflage de l'information qu'elle dissimule.

Définition 20 *Une k–*mise en gage *permet à $\mathcal{B}ob$ de camoufler une chaîne de k bits de sorte que le receveur $\mathcal{A}lice$ ne puisse en prendre connaissance sans son aide. De plus, $\mathcal{B}ob$ ne peut changer la valeur de la chaîne sans être détecté par $\mathcal{A}lice$. Plus précisément, une k–mise en gage est composée de deux protocoles:* camoufle(x) *et* révèle(x) *tels que*

1. *Soit $\mathcal{V}_0$ la vue d'$\mathcal{A}lice$ sur $x \in \{0,1\}^k$ avant l'exécution de camoufle(x) avec $\mathcal{B}ob$ et soit $\mathcal{V}_{\mathcal{A}^*}(x)$ la vue sur x d'$\mathcal{A}lice^*$ après l'exécution de camoufle(x). Pour tout programme $\mathcal{A}^*$ et toute vue initiale $\mathcal{V}_0$ pour $\mathcal{A}lice^*$on a que*

$$\mathbf{H}(x|\mathcal{V}_0) \leq \mathbf{H}(x|\mathcal{V}_{\mathcal{A}^*}(x)) + 2^{-\alpha n}$$

   pour $\alpha \geq 0$ et n suffisamment grand. Une mise en gage avec cette propriété est dite camouflante.

2. *Soit $S(x) \in \{oui, non\}$ la variable aléatoire qui détermine si révèle(x) est acceptée par $\mathcal{A}lice$. Pour tout programme $\mathcal{B}^*$ de $\mathcal{B}ob^*$ exécuté dans camoufle(x), il existe $x \in \{0,1\}^k$ tel que pour chaque $x' \in \{0,1\}^k$ tel que $x' \neq x$:*

$$\mathrm{P}\left(S(x') = oui\right) \leq 2^{-\alpha n}$$

   avec $\alpha > 0$ et n suffisamment grand. Une mise en gage avec cette propriété est appelée liante.

La première condition assure $\mathcal{B}$ob qu'$\mathcal{A}$lice n'a presque pas d'information sur la chaîne $x \in \{0,1\}^k$ après l'exécution de camoufle(x). La deuxième condition assure $\mathcal{A}$lice que $\mathcal{B}$ob peut dévoiler qu'une seule valeur pour x. La vue $\mathcal{V}_0$ est, comme dans le cas de la transmission insconsciente, une variable aléatoire qui représente toute l'information dont $\mathcal{A}$lice* dispose avant le début de l'interaction avec $\mathcal{B}$ob. Après l'exécution de camoufle(x), la vue intiale $\mathcal{V}_0$ est modifiée par l'ajout du supplément d'information obtenu durant l'interaction. Cette vue *finale* est représentée par la variable aléatoire $\mathcal{V}_{\mathcal{A}^*}(x)$ qui formellement dépend aussi de $\mathcal{V}_0$.

Disposant d'un 2–camouflage, $\mathcal{A}$lice peut s'assurer que $\mathcal{B}$ob a mesuré les photons qu'elle lui a envoyés. À toute les fois qu'$\mathcal{A}$lice envoie un photon π_i, $\mathcal{B}$ob doit répondre par un 2–camouflage $c_i = (\widehat{\theta}_i, \widehat{b}_i)$ dissimulant la base de lecture utilisée ainsi que le résultat obtenu. Nous verrons comment à la prochaine section.

Le canal quantique permet la réalisation d'une primitive de camouflage sous l'hypothèse que les opposants sont limités aux mesures individuelles. En particulier, le protocole BCJL renversé (présenté plus loin) est un bon candidat pour la réalisation de cette tâche. Nous analyserons sa sécurité au chapitre 4.

La prochaine section traite d'un instrument utile à la cryptographie quantique; la théorie des codes correcteurs. Notamment, les techniques de corrections d'erreurs sont utilisées lorsque le canal quantique est sujet au bruit de transmission.

2.5.1 Codes correcteurs

Un code correcteur de longueur n sur un alphabet fini Σ, est un sous-espace de Σ^n dont chaque élément est au moins à distance fixe des autres.

Définition 21 *Soit Σ un alphabet de symboles en nombre fini et $x, y \in \Sigma^n$ deux mots quelconques. La* distance de Hamming $\Delta(x, y)$ *est le nombre de positions où x et y diffèrent. On désigne par $\Delta^*(x, y)$ l'ensemble des positions où x et y sont différents.*

Un code est défini de la façon suivante,

Définition 22 *Un $[n, k, d]$–code $C \subseteq \Sigma^n$ est tel que*

1. $\#C = \#\Sigma^k$,
2. $(\forall c, c' \in C)$ *avec* $c \neq c'$, $\Delta(c, c') \geq d$.

Le paramètre d est appelé distance minimale du code. Un $[n, k, d]$–code est un code binaire si $\Sigma = \{0, 1\}$.

On juge les performances d'un code, étant donné son taux de transmission $\frac{k}{n}$, par le nombre d'erreurs de transmission qu'il permet de corriger. Si on décode le mot bruité $\hat{c}$ par le mot de code $c \in C$ qui s'en rapproche le plus, il est possible de corriger jusqu'à $\lfloor \frac{d}{2} \rfloor$ erreurs de transmission sans jamais se tromper. Plus la distance minimale d'un code est élevée pour un taux de transmission fixe $\frac{k}{n}$ plus celui-ci est performant. Cependant, le décodage par le plus proche voisin ne peut en général être exécuté efficacement à moins que $\mathbf{P} = \mathbf{NP}$ [14]. Par contre, certaines classes de codes peuvent être décodés par le plus proche voisin d'une façon efficace. Par exemple, les codes concaténés [39], les codes de Reed-Solomon [55] et les codes à convolutions [40] sont de ceux-là.

La classe des codes linéaires est particulièrement utile en cryptographie quantique.

Définition 23 *Un $[n, k, d]$–code C est linéaire si $(\forall c, c' \in C)[c \oplus c' \in C]$.*

Un $[n, k, d]$–code linéaire sur l'alphabet Σ peut être spécifié par une matrice G de dimension $n \times k$ qu'on appelle *matrice génératrice*. La matrice G permet d'encoder un message $x \in \{0, 1\}^k$ dans le mot de code $c \in C$ par

$$c = xG.$$

Chaque code C peut être remplacé par un code équivalent C' (équivalent parce qu'il existe une bijection entre les mots du code C et ceux du code C' qui préserve les distances entre les mots) dont la matrice génératrice G est écrite sous la forme

$$G = \begin{pmatrix} \mathbf{I}_k \\ G_s \end{pmatrix}$$

pour $\mathbf{I}_k$ la matrice identité $k \times k$ et G_s une matrice $(n - k) \times k$. Lorsque G est écrite de cette façon on dit que le code est sous forme systématique. Dans ce cas,

$$xG = x_1, \ldots, x_k, s_1, s_2, \ldots, s_{n-k}.$$

Chaque mot de code contient dans ces k premières positions les symboles du message encodé. La redondance est formée par les $n - k$ derniers symboles.

Associé à la matrice G, il y a la matrice de parité H de dimension $(n - k) \times n$. Celle-ci est telle que pour chaque mot de code $c \in C$,

$$Hc = \mathbf{0}.$$

FIG. 2.2 - *Courbe de Varshamov-Gilbert*

Inversement si $Hw = \mathbf{0}$ alors $w \in C$. La matrice H^T est aussi une matrice génératrice. Le code généré par H^T est appelé code dual de C lorsque H est la matrice de parité de C.

Lorsqu'un code C est spécifié par sa matrice génératrice G, il est en général difficile de déterminer exactement sa distance minimale. Par contre, si la matrice est choisie aléatoirement, la distance minimale du code peut être estimée par la borne de Varshamov-Gilbert.

Borne et courbe de Varshamov-Gilbert

La borne de Varshamov-Gilbert traite de l'existence de codes avec distance minimale d étant donné k et n. Soit Σ un alphabet de q symboles, la borne stipule qu'il existe un $[n, k, d]$–code sur $GF(q)$ en autant que

$$\sum_{i=1}^{d-2} (q-1)^i \binom{n-1}{i} < q^{n-k}.$$

Sur $GF(2)$, des $[n, k, d]$–codes existent lorsque

$$\sum_{i=1}^{d-2} \binom{n-1}{i} < 2^{n-k}.$$

Pour $\lambda < \frac{1}{2}$ l'identité

$$\frac{2^{nh(\lambda)}}{O(\sqrt{n})} \leq \sum_{i=1}^{\lambda n} \binom{n}{i} \leq 2^{n\mathbf{H}(\lambda)}$$

est connue comme l'identité de la queue d'une binomiale [2]. On peut donc affirmer que pour $d = \lambda n$ des $[n, k, d]$–codes existent pourvu que $k < n(1 - \mathbf{H}(\lambda))$. La borne de Varshamov-Gilbert est plus utile qu'il n'y paraît. En plus de l'existence de codes avec paramètres $[n, k, d]$ la borne permet d'en trouver qui l'approche d'aussi près que l'on veut. Supposons que nous voulions un code qui permette de corriger une fraction λn ($\lambda < \frac{1}{2}$) d'erreurs de transmission. Un code linéaire aléatoire C_n spécifié par sa matrice génératrice G_n de dimension $n \times (n - k_n)$ avec $k_n < n(1 - \mathbf{H}(\lambda))$ a une distance minimale d_n qui approche , à mesure que n augmente, la borne λn. Plus précisément:

Théorème 7 ([55]) $(\forall \epsilon > 0)(\forall \lambda < \frac{1}{2}))(\exists \alpha > 0)(\forall k_n \leq n(1 - \mathbf{H}(\lambda) - \epsilon)$
$(\exists n_0(\epsilon, \lambda, \alpha))(\forall n \geq n_0(\epsilon, \lambda, \alpha))$

$$\mathrm{P}\left(\begin{pmatrix} ©_{1,1} & ©_{1,2} & \cdots & ©_{1,n} \\ ©_{2,1} & ©_{2,2} & \cdots & ©_{2,n} \\ & & \vdots & \\ ©_{k_n,1} & ©_{k_n,2} & \cdots & ©_{k_n,n} \end{pmatrix} \textit{ définit un } [n, k_n, \lambda n]\textit{–code}\right) \geq 1 - 2^{-\alpha n}.$$

Le problème de décision associé au problème du décodage d'un code aléatoire linéaire par le voisin le plus proche est **NP**–complet [14]. On sait comment obtenir des codes avec distance minimum $d_n \geq \lambda n$ mais on ne sait pas comment les décoder. Heureusement, en cryptographie quantique il arrive que nous ayons besoin d'un code sans vouloir d'algorithme de décodage efficace. Le camouflage quantique en est un exemple. D'autres situations demandent que le code utilisé permette le décodage efficace de $\frac{d_n}{2}$ erreurs. C'est le cas du protocole BBCS sur un canal imparfait. Les codes aléatoires sont inutiles pour cette tâche.

2.5.2 Camouflages BCJL

On peut maintenant voir comment un camouflage peut être réalisé sur le canal quantique. Supposons que $\mathcal{B}$ob veuille camoufler un bit $x \in \{0, 1\}$ à $\mathcal{A}$lice. Il est facile d'adapter le protocole pour camoufler une chaîne de bits plus longue. Le paramètre $p \geq 0$ est borne supérieure sur le taux d'erreurs du canal quantique. Le protocole 2.5.1 permet à $\mathcal{B}$ob de mettre en gage $x \in \{0, 1\}$ à $\mathcal{A}$lice.

Remarquons que même si le protocole permet à $\mathcal{B}$ob de camoufler un bit à $\mathcal{A}$lice, les photons transitent d'$\mathcal{A}$lice vers $\mathcal{B}$ob. À l'origine [21], les photons transitaient en sens inverse. Cette version a été la première à tomber [52] sous l'attaque générale de [53]. Même si contre cette même attaque BCJL renversé tombe aussi, nous introduisons

Protocole 2.5.1 (camoufle(x))

1: $\mathcal{A}$lice choisit une matrice booléenne G représentant la matrice génératrice d'un $[n, k, d]$–code linéaire C avec les bonnes propriétés et l'annonce à $\mathcal{B}$ob,

2: $\mathcal{B}$ob choisit un mot de code aléatoire $c \leftarrow (©_1 ... ©_k)G$ dans C et pige un $r \in \{0,1\}^n$ tel que $c \odot r = x$ puis l'annonce,

3: $\mathcal{A}$lice choisit deux chaînes aléatoires $b, b' \in_R \{0,1\}^n$,

4: $\textbf{FAIRE}_{i=1}^{n}$

- $\mathcal{A}$lice détermine sa i-ième base de transmission $\phi_i^A \leftarrow [+, \times]_{b'_i}$,
- $\mathcal{A}$lice transmet le photon π_i dans l'état de polarisation $|b_i\rangle_{\phi_i^A}$,
- $\mathcal{B}$ob mesure π_i dans la base $\phi_i^B \leftarrow [+, \times]_{c_i}$ et obtient le bit β_i,

5: $\mathcal{B}$ob annonce à $\mathcal{A}$lice $\beta = \beta_1, \ldots, \beta_n$.

FIG. 2.3 - *Camouflage BCJL renversé.*

cette variante pour deux raisons. Premièrement, dans le protocole d'identification présenté au chapitre 3, il est préférable d'utiliser BCJL-renversé. Ceci permet de mettre toute la technologie du côté d'un seul participant. De plus, au chapitre 4 nous montrons que BCJL renversé est sécuritaire contre les mesures individuelles. Puisque dans cette thèse nous nous limitons à ce type de mesures, ce protocole de mise en gage est parfait relativement à nos hypothèses.

Pour créer un camouflage, $\mathcal{B}$ob choisit un mot de code aléatoire c d'un code correcteur linéaire C de longueur n. Il pige aussi une chaîne $r \in \{0,1\}^n$ telle que $c \odot r = \oplus_{i=1}^n c_i \cdot r_i = x$. La chaîne r est annoncée publiquement à $\mathcal{A}$lice. Maintenant, $\mathcal{A}$lice transmet n photons BB84 aléatoires définis par deux chaînes de n bits b et b'. La chaîne b représente les bits qui sont transmis tandis que la chaîne b' indique les bases de transmission utilisées. Les bases d'émission sont déterminées par $\phi_i^A = [+, \times]_{b'_i}$. À l'autre bout, $\mathcal{B}$ob mesure le photon π_i dans la base $\phi_i^B = [+, \times]_{c_i}$ et obtient le bit décodé β_i.

Si le code C n'est pas trop redondant (i.e. $\frac{k}{n}$ est près de 1), l'information que donne β à propos de c devrait être insuffisante pour que l'information d'$\mathcal{A}$lice sur x soit non-négligeable.

Associé au protocole camoufle(x), le protocole révèle(x) permet à $\mathcal{A}$lice d'apprendre le contenu x du camouflage reçu. Il demande à $\mathcal{B}$ob de révéler les bases de réception en dévoilant le mot de code c en plus du bit camouflé x. $\mathcal{A}$lice vérifie ensuite que lorsque $b'_i = c_i$ le bit reçu $\beta_i = b_i$ (sauf pour une proportion tolérée δ^*) et que $x = r \odot c$.

Protocole 2.5.2 (révèle$(r, \beta, b', b, \delta^*)(c, x)$ **)**

1: $\mathcal{B}$ob révèle c et x à $\mathcal{A}$lice,

2: $\mathcal{A}$lice pose $\delta \leftarrow \frac{\#\{i \mid c_i = b'_i \wedge \beta_i \neq b_i\}}{\#\{i \mid c_i = b'_i\}}$,

3: **Si** $\delta < \delta^*$ et $x = c \odot r$ et $c \in C$ **alors** $\mathcal{A}$lice accepte **sinon** $\mathcal{A}$lice refuse.

FIG. 2.4 - *Révélation BCJL renversé.*

Imaginons comment $\mathcal{B}$ob* pourrait changer sa mise en gage en exécutant la primitive révèle$(r, \beta, b', b, \delta^*)(c, x)$. Pour pouvoir tromper $\mathcal{A}$lice, $\mathcal{B}$ob* doit être en mesure d'annoncer (c, x) et $(c', 1 - x)$ avec $c \neq c'$, de façon à ce que $\mathcal{A}$lice accepte les deux avec probabilité non négligeable. Si le code C a une distance minimale dn, c et c' seront tels que $\Delta(c, c') \geq dn$. Supposons sans perdre de généralités que l'annonce de (c, x) permet à $\mathcal{B}$ob* de passer le test de l'étape 3 du protocole de révélation avec probabilité non négligeable. Intuitivement ceci implique que β_i coïncide avec b_i lorsque i est tel que $b'_i = c_i$ (lorsque la base d'émission et la base de réception sont identiques). $\mathcal{B}$ob* n'a aucune façon de déterminer les positions i telles que $b'_i = c_i$. Ainsi, il semble qu'il n'ait d'autre choix que de mesurer la plupart du temps dans la base $[+, \times]_{c_i}$ pour presque tous les $i \in \{1, \ldots, n\}$. Comme $\Delta(c, c') \geq dn$, la mesure de $\mathcal{B}$ob* ne permettra probablement pas de mesurer correctement les bits selon c'. Plus la distance entre c et c' est grande, plus le nombre d'erreurs de mesure dans la chaîne

β sera important. Ceci n'est qu'une argumentation intuitive et ne constitue en rien une preuve de la sécurité du protocole. Nous verrons au chapitre 4 que ce protocole est sécuritaire contre les mesures individuelles.

Pour le moment nous supposons que nous disposons d'une primitive de camouflage parfaite. Dans ces conditions, voyons comment protéger le protocole 2.3.1 contre les mesures incomplètes.

2.5.3 Une Protection

Pour être convaincu que $\mathcal{B}$ob a mesuré les photons qu'il a reçus, $\mathcal{A}$lice demande à $\mathcal{B}$ob de lui fournir pour chaque photon π_i, un camouflage $c_i = (\widehat{\theta}_i, \widehat{b}_i)$ contenant la base de mesure et le bit qu'il a obtenu. $\mathcal{A}$lice peut ensuite demander à $\mathcal{B}$ob de lui révéler un sous-ensemble aléatoire des camouflages. Sur l'ensemble des camouflages révélés, $\mathcal{A}$lice vérifie que la plupart du temps lorsque $\theta_i = \widehat{\theta}_i$ le bit reçu $\widehat{b}_i = b_i$. Pour $p \geq 0$ le taux d'erreurs du canal quantique, $\mathcal{A}$lice accepte de poursuivre le protocole si le nombre de positions i pour lesquelles $\widehat{\theta}_i = \theta_i$ et $\widehat{b}_i \neq b_i$ n'est pas significativement supérieur à la fréquence attendue p.

Pour la suite, les mises en gage sont utilisées comme des boîtes noires parfaitement sécuritaires. Cette hypothèse sera levée au chapitre 4 lorsque nous montrerons que limité aux mesures individuelles, BCJL renversé est sécuritaire.

2.6 Adapter BBCS pour réaliser $\binom{2}{1}$–$\mathbf{TI}_r^*$

Le protocole 2.3.1 peut être adapté pour la tansmission inconsciente d'une chaîne de plus d'un bit par la méthode décrite dans [13]. À l'étape 4, $\mathcal{A}$lice encrypte ses bits q_0 et q_1 dans le ou-exclusif de tous les bits des ensembles I_0 et I_1 respectivement. Pour $t = \#I_0 = \#I_1$, l'encryption est obtenue par l'application de la fonction de hachage $h : \{0,1\}^t \rightarrow \{0,1\}$. Il est naturel d'étendre cette fonction au cas plus général où la sortie contient plus d'un bit. Si $\mathcal{A}$lice veut transmettre une chaîne de longueur r parmi deux, elle pourrait utiliser une fonction $h : \{0,1\}^t \rightarrow \{0,1\}^r$. Il faudra que cette fonction transforme un chaîne partiellement secrète b^{1-c} de longueur t en une autre

$h(b^{1-c})$ qui soit secrète au sens statistique. C'est-à-dire que l'information de $\mathcal{B}$ob* sur $h(b^{1-c})$ est exponentiellement faible en t. Ce processus est appelé *amplification de secret* et a été étudié par [12] et généralisé par la suite par [10]. Au centre des solutions proposées par [12, 10] il y a les classes de fonctions de hachage Universelle$_2$ de Wegman et Carter [30].

Définition 24 ([30]) *Une classe de fonctions H de $A \rightarrow B$ est Universelle$_2$ si pour chaque paire $x, x' \in A$ telle que $x \neq x'$, le nombre de fonctions $h \in H$ telles que $h(x) = h(x')$ est au plus $|H|/|B|$.*

Des classes de fonctions Universelle$_2$ sont faciles à trouver. Wegman et Carter ont défini la classe H_3 et ont démontré qu'elle est Universelle$_2$. La classe H_3 est avantageuse car il est possible de choisir $h \in_R H_3$ et d'évaluer $h(x)$ efficacement.

Définition 25 ([30]) *La classe de fonctions de hachage $H_3^{n,\lambda}$ définie par*

$$\{h : \{0,1\}^n \rightarrow \{0,1\}^{\lfloor \lambda n \rfloor} | \forall x \in \{0,1\}^n, h(x) = xH\}$$

avec H une matrice binaire de dimension $n \times \lfloor \lambda n \rfloor$.

Pour transmettre une chaîne de longueur $r = \lfloor \lambda n \rfloor$ $\mathcal{A}$lice calcule à l'étape 4,

$$q_0' = q_0 \oplus h(b^0) \text{ et } q_1' = q_1 \oplus h(b^1)$$

pour $b^0 = \biguplus_{i \in I_0} b_i$ et $b^1 = \biguplus_{i \in I_1} b_i$ et $h \in_R H^{n,\lambda}$. Le symbole $\biguplus$ indique la concaténation des éléments auxquels on applique l'opération. Les paramètres α et λ restent à être déterminés par l'analyse de la sécurité du protocole. $\mathcal{B}$ob retrouve q_c de la même façon qu'avant en calculant,

$$q_c = h^c(b^c) \oplus q_c'.$$

Nous montrerons par la suite que le protocole BBCS ainsi adapté pour transmettre des chaînes de longueur arbitraire sera sécuritaire contre les mesures individuelles.

Pour l'analyse du scénario le plus réaliste nous devons aussi supposer que le canal quantique est imparfait.

2.7 BBCS sur un canal quantique bruyant

Maintenant montrons comment réaliser la transmission inconsciente avec le protocole BBCS sur un canal quantique bruyant. La solution consiste en l'utilisation de codes concaténés pour permettre à $\mathcal{B}$ob de corriger les bits de l'ensemble I_c mais insuffisant pour la correction des bits de l'ensemble I_{1-c}. Soit $\widehat{b}^0 = \biguplus_{i\in I_0} \widehat{b}_i$ et $\widehat{b}^1 = \biguplus_{i\in I_1} \widehat{b}_i$. Les ensembles I_0 et I_1 sont ici construits de façon à ce que $t = \#I_0 = \#I_1$. En supposant que le canal quantique se comporte comme un canal symétrique binaire avec paramètre p, sauf avec probabilité exponentiellement faible $2^{-\alpha n}$ pour $\alpha > 0$, la chaîne reçue $\widehat{b}^c$ sera telle que $\Delta(b^c, \widehat{b}^c) \leq (p+\epsilon)t$ pour tout $\epsilon > 0$ et n suffisamment. Si nous diposons d'un $[m, t, 2(p+\epsilon)t]$–code C_m qui puisse être décodable efficacement, $\mathcal{B}$ob pourra récupérer b^c à partir de $\widehat{b}^c$. Pour ce faire, il s'agit de mettre C_m sous forme systématique pour qu'$\mathcal{A}$lice puisse transmettre la redondance contenu dans le mot de code qui encode le message b^c. Comme elle ne sait pas (et c'est nécessaire) lequel des deux ensembles est l'ensemble I_c, elle doit aussi transmettre la redondance pour la chaîne b^{1-c}. Le code ne doit donc pas être trop redondant ce qui pourrait permettre à $\mathcal{B}$ob* d'obtenir de l'information sur q_0 et q_1. Autrement dit, le code doit avoir une distance minimale $2(p+\epsilon)t$ mais avoir aussi un taux de transmission élevé. Il y a un lien évident entre le taux de transmission $\frac{t}{m}$ et la plus grande distance minimale possible pour un code, comme le montre la courbe de Varshamov-Gilbert. L'analyse de la sécurité du protocole BBCS doit aussi indiquer à quel taux de transmission le code doit fonctionner pour que $\mathcal{B}$ob demeure ignorant sur au moins une des deux chaînes q_0 et q_1.

En rassemblant les remarques précédentes, le protocole BBCS peut réaliser la tâche $\binom{2}{1}$–TI$_r$ sur un canal quantique bruyant. Le protocole 2.7.1 donne sa description complète. La façon de construire les ensembles I_c et I_{1-c} et un peu différente de la façon décrite au protocole 2.3.1. Ici nous voulons que

$$t = \#I_c = \#I_{1-c} = \lfloor \frac{\{i|ouvrir_i = 0\}}{2} \rfloor.$$

Il est donc possible que le nombre de positions i telles que $\widehat{\theta}_i = \theta_i$ soit moindre que t. Dans ce cas, les positions manquantes sont comblées par des positions i telles que $\widehat{\theta}_i \neq \theta_i$. Même si les bits à ces positions ne sont pas connus, le code correcteur suffira pour les retrouver car le nombre de ces positions sera, sauf avec probabilité négligeable, moindre que ϵt pour tout $\epsilon > 0$ et n assez grand. La même chose se produit lorsque le nombre de positions i telles que $\widehat{\theta}_i \neq \theta_i$. Dans ce cas, les positions manquantes sont comblées par des positions i telles que $\widehat{\theta}_i = \theta_i$.

2.8 BBCS contre les mesures individuelles

Comme il a été démontré par Crépeau [25] (théorème 5, section 2.4), $\mathcal{B}$ob est inconditionnellement protégé contre les attaques d'$\mathcal{A}$lice*. En particulier, si elle décide de déterminer malicieusement les valeurs $ouvrir_i$, elle aiderait $\mathcal{B}$ob à déterminer de l'information sur q_0 et q_1. Cependant, la sécurité contre toutes les mesures permises par la mécanique quantique n'est pas assurée du point de vue d'$\mathcal{A}$lice. Tout ce que nous pouvons dire jusqu'à maintenant, c'est que si $\mathcal{B}$ob* est limité à des mesures de Von Neumann il lui est statistiquement impossible d'obtenir de l'information sur les deux bits q_0 et q_1. Dans cette section, nous exposons le résultat d'un travail commun avec Dominic Mayers [54] qui étend la validité du théorème 6 aux mesures individuelles. Il s'agit de la classe des mesures qui s'appliquent aux photons reçus individuellement. Cette classe est plus générale que celle des mesures de Von Neumann parce qu'elle permet des mesures incomplètes jusqu'à l'annonce des bases de transmission. En fonction de la base annoncée, $\mathcal{B}$ob* peut compléter sa mesure en fonction de cette information et obtenir davantage d'information sur les bits envoyés par $\mathcal{A}$lice. Nous analysons le protocole BBCS adapté pour réaliser la tâche $\binom{2}{1}$–TI$_r$ pour $r \in O(n)$. Nous considérons un canal quantique bruyant avec paramètre $p \geq 0$. Le modèle adopté pour représenter ces mesures est le modèle OCPS.

L'analyse de sécurité du protocole BBCS qui réalise $\binom{2}{1}$–TI$_r$ contre les mesures individuelles doit permettre de déterminer,

1. Les paramètres du code concaténé qui permet à $\mathcal{B}$ob d'obtenir la chaîne b^c mais qui n'est pas suffisant pour que $\mathcal{B}$ob* obtienne la chaîne b^{1-c}.

2. Les paramètre de la classe de fonctions de hachage $H^{n,\lambda}$ pour laquelle la fonction

Protocole 2.7.1 ($\binom{2}{1}$–$\mathbf{TI}_r(q_0, q_1)(c)$)

1: $\mathcal{A}$lice et $\mathcal{B}$ob exécutent l'étape 1 du protocole $\binom{2}{1}$–TI_1^*, $\mathcal{A}$lice pose ensuite $m \leftarrow 0$ et $erreur \leftarrow 0$.

2: $\overset{n}{\underset{i=1}{\textbf{FAIRE}}}$

- $\mathcal{B}$ob et $\mathcal{A}$lice exécutent camoufle$((\widehat{\theta}_i, \widehat{b}_i))$.
- $\mathcal{A}$lice détermine $ouvrir_i \leftarrow$ ©.
- **Si** $ouvrir_i = 1$ **alors** $\mathcal{A}$lice pose $m \leftarrow m + 1$ **et**
  - $\mathcal{B}$ob et $\mathcal{A}$lice exécutent révèle$((\widehat{\theta}_i, \widehat{b}_i))$.
  - **Si** $\widehat{\theta}_i = \theta_i \wedge \widehat{b}_i \neq b_i$ **alors** $\mathcal{A}$lice pose $erreur \leftarrow erreur + 1$.

3: **Si** $\frac{erreur}{m} < \delta$ **alors** $\mathcal{A}$lice annonce $\theta_1, \theta_2, \ldots, \theta_n$ **sinon** elle refuse de continuer.

4: $\mathcal{B}$ob annonce à $\mathcal{A}$lice $I_0, I_1 \subseteq \{i | ouvrir_i = 0\}$ tels que $I_0 \cap I_1 = \emptyset$ et $t = \#I_0 = \#I_1 = \lfloor \frac{\{i | ouvrir_i = 0\}}{2} \rfloor$. L'ensemble I_c pour $c \in \{0, 1\}$ contient les positions i telles que $\widehat{\theta}_i = \theta_i$ jusqu'à concurrence de t.

5: $\mathcal{A}$lice détermine $b^0 = \biguplus_{i \in I_0} b_i$ et $b^1 = \biguplus_{i \in I_1} b_i$ et annonce la redondance $s^l, l \in \{0, 1\}$ associée au mot de code $b^l G$. G est la matrice génératrice d'un code linéaire C sous forme systématique.

6: $\mathcal{B}$ob utilise s^c pour décoder b^c à l'aide de $\widehat{b^c}$.

7: $\mathcal{A}$lice pige aléatoirement et annonce $h^0, h^1 \in H^{n,\lambda}$ et q_0', q_1' tels que

$$q_0' = q_0 \oplus h^0(b^0) \text{ et } q_1' = q_1 \oplus h^1(b^1).$$

8: $\mathcal{B}$ob calcule

$$q_c = q_c' \oplus h(b^c).$$

FIG. 2.5 - *Protocole de transmission inconsciente BBCS.*

$h \in H^{n,\lambda}$ cache presque toute l'information à $\mathcal{B}$ob* sur la chaîne

$$q_{1-c} = q'_{1-c} \oplus h(b^{1-c}).$$

La limitation aux mesures individuelles (par rapport aux mesures cohérentes) simplifie l'analyse parce que le degré de corrélation entre les résultats des mesures est faible.

2.8.1 Stratégies pour $\mathcal{B}$ob*

Dans cette section nous discutons et modélisons les stratégies possibles pour $\mathcal{B}$ob* qui veut déterminer le plus d'information possible sur les bits b_i avec $i \in \{1, \ldots, 4n\}$ transmis par $\mathcal{A}$lice[1].

Le protocole 2.8.1 donne un cadre dans lequel les stratégies possibles pour $\mathcal{B}$ob* sont inscrites. Le paramètre n est comme à l'habitude le facteur de sécurité tandis que δ est la tolérance d'$\mathcal{A}$lice quant aux erreurs de mesures qu'elle détecte lorsque les camouflages lui sont révélés. Le paramètre δ est un peu plus élevé que le taux d'erreur p du canal quantique. Si $\mathcal{A}$lice ne parvenait pas à détecter $\mathcal{B}$ob* dans le protocole 2.8.1, elle ne pourrait pas non plus le détecter dans le protocole 2.7.1 s'il exécutait la même stratégie d'attaque. Du point de vue d'$\mathcal{A}$lice, le protocole 2.8.1 est indistinguable des étapes 1 à 3 de $\binom{2}{1}$–TI_r. L'analyse se fera en deux temps. Nous montrerons en premier que lorsqu'une exécution des étapes 1 à 3 du protocole 2.7.1 est acceptée par $\mathcal{A}$lice, plusieurs bits transmis sont inconnus de $\mathcal{B}$ob*. Nous montrerons ensuite à la section 2.9 que ces bits inconnus permettent d'assurer $\mathcal{A}$lice que $\mathcal{B}$ob* ne peut obtenir d'information sur les deux chaînes q_0 et q_1 en même temps. Voyons maintenant le détail des actions permises pour $\mathcal{B}$ob* dans le protocole 2.8.1(qui modélise les attaques individuelles).

Le scénario est simple, après une phase d'initialisation $\mathcal{A}$lice transmet, à l'étape 2, $4n$ bits encodés par le codage BB84. Pour chaque photon π_i avec $i \in \{1, \ldots, 4n\}$, $\mathcal{B}$ob* exécute la mesure individuelle de son choix $\mathcal{M}_i$. En fonction du résultat, $\mathcal{B}$ob*

1. Pour simplifier la notation, le nombre de photons transmis est $4n$. Ainsi, pour appliquer l'analyse qui suit au protocole 2.7.1, $\mathcal{A}$lice transmet $4n$ photons BB84 au lieu de n.

Protocole 2.8.1 (Stratégie(δ, n))

1: $\mathcal{A}$lice pose $erreur \leftarrow 0, N \leftarrow 0$

2: $\mathbf{FAIRE}_{i=1}^{4n}$

$\mathcal{A}$lice pige $b_i \in_R \{0,1\}$ et $\theta_i \in_R \{+, \times\}$

$\mathcal{A}$lice transmet à $\mathcal{B}$ob* un photon π_i dans l'état $|b_i\rangle_{\theta_i}$

$\mathcal{B}$ob* détermine sa mesure $\mathcal{M}_i$, mesure π_i et obtient le résultat $\widehat{\theta}_i \in \{+, \times\}$ et $\widehat{b}_i \in \{0,1\}$

$\mathcal{B}$ob* transmet le 2–camouflage $C_i = (\widehat{b}_i, \widehat{\theta}_i)$ à $\mathcal{A}$lice

3: $\mathbf{FAIRE}_{i=1}^{4n}$

$\mathcal{A}$lice pige $ouvrir_i \leftarrow ©$, **si** $ouvrir_i = 1$ **alors** elle demande à $\mathcal{B}$ob* de révéler le camouflage C_i

Si $ouvrir_i = 0$ **alors** $\mathcal{A}$lice et $\mathcal{B}$ob* pose $N \leftarrow N + 1$

Sinon si $C_i = (\theta_i, 1 - b_i)$ **alors** $\mathcal{A}$lice pose $erreur \leftarrow erreur + 1$

4: **Si** $erreur \leq \delta n$ **alors** $\mathcal{A}$lice annonce les bases $\theta_1, \theta_2, \ldots, \theta_{4n}$ à $\mathcal{B}$ob **autrement** elle refuse de continuer

5: $\mathbf{FAIRE}_{i=1}^{4n}$ $\mathcal{B}$ob détermine $\mathcal{M}'_i$ et raffine sa mesure sur π_i pour obtenir le résultat final j_i.

FIG. 2.6 - *Stratégie de $\mathcal{B}$ob* contre BBCS (mesures individuelles).*

détermine $\widehat{\theta}_i$ et $\widehat{b}_i$ qu'il enferme dans un 2–camouflage $C_i = (\widehat{\theta}_i, \widehat{b}_i)$. Les résultats de cette première mesure sont étiquetés par des paires $(\widehat{\theta}_i, \widehat{b}_i)$. À l'étape 3, $\mathcal{A}$lice pige pour chaque $i \in \{1, \ldots, 4n\}$ la variable aléatoire $ouvrir_i \in \{0, 1\}$ dont la valeur détermine si le camouflage C_i lui sera révélé ou non. Lorsque $ouvrir_i = 1$, le camouflage C_i est révélé par $\mathcal{B}$ob*. Dans ce cas $\mathcal{A}$lice vérifie que si $\widehat{\theta}_i = \theta_i$ le bit camouflé $\widehat{b}_i$ vaut bien son bit envoyé b_i. Si tel n'est pas le cas, elle incrémente la variable $erreur$. À l'étape 4, $\mathcal{A}$lice compare la fréquence des erreurs détectées à son facteur de tolérance δ. Si la fréquence se situe à l'intérieur du facteur de tolérance elle annonce la séquence de bases $\theta_1, \ldots, \theta_{4n}$. Sinon, $\mathcal{B}$ob* est rejeté et $\mathcal{A}$lice refuse de continuer. À l'étape 5, $\mathcal{B}$ob* utilise la séquence de bases annoncée par $\mathcal{A}$lice pour compléter sa mesure sur chaque photon π_i.

Une stratégie pour $\mathcal{B}$ob* est pertinente si elle lui permet d'apprendre la séquence $\theta_1, \ldots, \theta_{4n}$ avec probabilité non-négligeable. Il reste à déterminer quelle quantité d'information une stratégie pertinente peut fournir à $\mathcal{B}$ob*.

2.8.2 Opérateurs OCPS pour la mesures individuelles

Nous utilisons maintenant le modèle OCPS pour représenter les mesures individuelles que $\mathcal{B}$ob* peut exécuter dans le protocole 2.8.1. Puisque chaque mesure s'applique sur des photons individuels, l'opérateur OCPS appliqué au photon π_i contient deux colonnes orthonormées car l'espace du système observé est de dimension 2. La première colonne est étiquetée 0 tandis que la deuxième porte l'étiquette 1. Le nombre de rangées peut être aussi grand que le veut $\mathcal{B}$ob*. Chacune de ces rangées représente un résultat final possible pour la mesure complète. Si $\mathcal{B}$ob* veut tirer avantage de toute la puissance des mesures individuelles permises par la mécanique quantique sur le photon π_i, il doit faire une première mesure incomplète et attendre que la base θ_i lui soit annoncée avant de la compléter. Une mesure incomplète est représentée par un sous-ensemble des rangées de l'opérateur OCPS qui modélise la mesure. La figure 2.7 représente le processus de mesure pour un photon π_i.

Chacune des rangées *à gros grains* du rectangle de gauche représente les résultats possibles pour la première mesure. À chacun des résultats partiels nous associons un

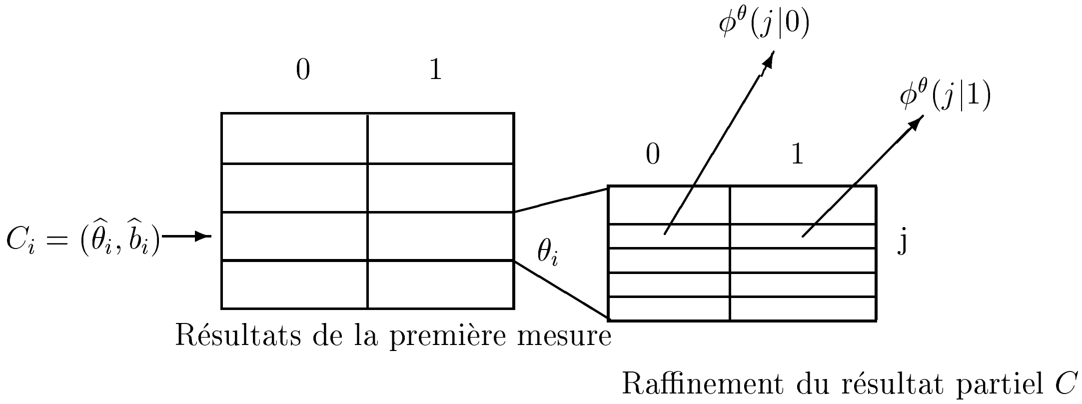

FIG. 2.7 - *Opérateur OCPS pour une mesure individuelle.*

camouflage $C_i = (\widehat{\theta}_i, \widehat{b}_i)$ pour $\widehat{\theta}_i \in \{+, \times\}$ et $\widehat{b}_i \in \{0, 1\}$. Une fois le camouflage effectué et en supposant que $ouvrir_i = 0$, $\mathcal{A}$lice annonce la base de transmission θ_i du photon π_i. Lorsque $\mathcal{B}$ob* connaît θ_i, il complète sa mesure et obtient finalement un résultat j qui correspond à une des rangées du rectangle de droite. La matrice complète de l'opérateur OCPS est composée de nombres complexes de normes entres 0 et 1 appelés amplitudes de transition. Le nombre complexe en rangée j et en colonne $b_i \in \{0, 1\}$ est noté $\phi^{\theta_i}(j|b_i)$. Soit $\mathbf{j}_i$ la variable aléatoire qui désigne le résultat final de la i–ième mesure. De la même façon définissons les variables aléatoires $\mathbf{b}_i$ pour la valeur du i–ième bit transmis et Θ_i pour celle de la i–ième base de transmission sélectionnée par $\mathcal{A}$lice. La probabilité $\mathrm{P}\left(\mathbf{j}_i = j | \mathbf{b}_i = b_i \wedge \Theta_i = \theta_i\right)$ qu'un photon π_i dont l'état de polarisation est $|b_i\rangle_{\theta_i}$ apparaisse dans l'état final j est telle que

$$\mathrm{P}\left(\mathbf{j}_i = j | \mathbf{b}_i = b_i \wedge \Theta_i = \theta_i\right) = |\phi^{\theta_i}(j|b_i)|^2. \tag{2.3}$$

La paramètre θ_i qui figure dans l'amplitude de transition $\phi^{\theta_i}(j|b_i)$ représente la base dans laquelle est exprimée l'opérateur OCPS pour la mesure du i-ième photon. Nous dirons alors que l'opérateur OCPS est exprimé dans la base θ_i. Étant donné un opérateur OCPS exprimé dans la base θ_i il est possible de l'exprimer dans la base θ'_i par un simple changement de base. Les amplitudes de transition de l'opérateur résultant sont de la forme $\phi^{\theta'_i}(j|b_i)$. Dans notre cas particulier, les deux seules bases que nous utiliserons sont celles du codage BB84. Lorsque $\theta_i \in \{+, \times\}$ nous noterons par θ_i^c l'autre base de l'ensemble.

2.8.3 Changement de base

Dans cette section nous montrons comment obtenir, étant donné un opérateur OCPS exprimé dans la base θ_i, ce même opérateur exprimé dans la base θ_i^c. Les divers états possibles du codage BB84 sont liés de la façon suivante,

$$\begin{aligned}
|0\rangle_+ &= \frac{1}{\sqrt{2}}\left(|0\rangle_\times - |1\rangle_\times\right) \\
|1\rangle_+ &= \frac{1}{\sqrt{2}}\left(|0\rangle_\times + |1\rangle_\times\right) \\
|0\rangle_\times &= \frac{1}{\sqrt{2}}\left(|0\rangle_+ + |1\rangle_+\right) \\
|1\rangle_\times &= \frac{1}{\sqrt{2}}\left(-|0\rangle_+ + |1\rangle_+\right).
\end{aligned}$$

En utilisant ces identités nous obtenons que

$$\begin{aligned}
\phi^+(j|0) &= \frac{1}{\sqrt{2}}\Big(\phi^\times(j|0) - \phi^\times(j|1)\Big) \\
\phi^+(j|1) &= \frac{1}{\sqrt{2}}\Big(\phi^\times(j|0) + \phi^\times(j|1)\Big) \\
\phi^\times(j|0) &= \frac{1}{\sqrt{2}}\Big(\phi^+(j|0) + \phi^+(j|1)\Big) \\
\phi^\times(j|1) &= \frac{1}{\sqrt{2}}\Big(-\phi^+(j|0) + \phi^+(j|1)\Big).
\end{aligned}$$

Comme nous le verrons par la suite, une borne sur la norme des amplitudes de transition qui résulte d'un changement de base est suffisante pour arriver à nos conclusions. Une rapide inspection des relations précédentes nous permet de conclure que

$$|\phi^{\theta_i}(j|b_i)| \leq \frac{1}{\sqrt{2}}\Big(|\phi^{\theta_i^c}(j|0)| + |\phi^{\theta_i^c}(j|1)|\Big). \tag{2.4}$$

Cette identité est d'une grande importance pour la suite.

2.8.4 Propriétés utiles

Nous exposons ici des parties du mécanisme qui permet de borner la quantité d'information qu'une mesure peut donner.

En premier lieu, il est bon de se rappeler que suite à la première mesure sur le photon π_i et juste avant d'apprendre la base de transmission θ_i, $\mathcal{B}$ob* n'a auncune information sur celle-ci. Ceci parce que les matrices de densité pour les états du codage BB84 dans la base rectilinéaire et ceux dans la base diagonale sont identiques (section 1.8.1).

Les états finaux $|j, \widehat{\theta}_i, \widehat{b}_i\rangle$ associés au résultat partiel $C_i = (\widehat{\theta}_i, \widehat{b}_i)$ ont chacun une amplitude $\phi^{\theta_i}(j|0)$ associée au bit 0 et $\phi^{\theta_i}(j|1)$ associée au bit 1. Comme à l'équation 2.3, nous avons que

$$\mathrm{P}\left(\mathbf{j}_i = j|\mathbf{b}_i = b_i \wedge \Theta_i = \theta_i\right) = |\phi^{\theta_i}(j|b_i)|^2.$$

En utilisant la loi de Bayes on obtient que

$$\begin{aligned}
\mathrm{P}\left(\mathbf{b}_i = b_i|\mathbf{j}_i = j \wedge \Theta_i = \theta_i\right) &= \frac{\mathrm{P}\left(\mathbf{b}_i = b_i \wedge \mathbf{j}_i = j \wedge \Theta_i = \theta_i\right)}{\mathrm{P}\left(\mathbf{j}_i = j \wedge \Theta_i = \theta_i\right)} \\
&= \frac{\mathrm{P}\left(\mathbf{j}_i = j|\mathbf{b}_i = b_i \wedge \Theta_i = \theta_i\right)\mathrm{P}\left(\mathbf{b}_i = b_i \wedge \Theta_i = \theta_i\right)}{\mathrm{P}\left(\mathbf{j}_i = j \wedge \Theta_i = \theta_i\right)} \\
&= \frac{|\phi^{\theta_i}(j|b_i)|^2}{4\mathrm{P}\left(\mathbf{j}_i = j \wedge \Theta_i = \theta_i\right)} \\
&= \frac{|\phi^{\theta_i}(j|b_i)|^2}{4\sum_{b_i\in\{0,1\}}\mathrm{P}\left(\mathbf{j}_i = j \wedge \Theta_i = \theta_i \wedge \mathbf{b}_i = b\right)} \\
&= \frac{|\phi^{\theta_i}(j|b_i)|^2}{4\left(\sum_{b\in\{0,1\}}\frac{1}{4}\mathrm{P}\left(\mathbf{j}_i = j|\Theta_i = \theta_i \wedge \mathbf{b}_i = b\right)\right)} \\
&= \frac{|\phi^{\theta_i}(j|b_i)|^2}{|\phi^{\theta_i}(j|0)|^2 + |\phi^{\theta_i}(j|1)|^2}.
\end{aligned}$$

Avec la probabilité $\mathrm{P}\left(\mathbf{b}_i = b_i|\mathbf{j}_i = j \wedge \Theta_i = \theta_i\right)$, nous pouvons caractériser l'information sur b_i que le résultat j donne à propos de b_i. Un résultat sera d'autant plus informatif que la différence

$$||\phi^{\theta_i}(j|0)|^2 - |\phi^{\theta_i}(j|1)|^2|$$

est grande.

Une grande différence entre $|\phi^{\theta_i}(j|0)|^2$ et $|\phi^{\theta_i}(j|1)|^2$ implique aussi que la différence entre les normes des amplitudes $|\phi^{\theta_i}(j|0)|$ et $|\phi^{\theta_i}(j|1)|$ est importante. Cette remarque est utile lorsque mise en perspective avec les relations pour effectuer un changement de base. Puisque

$$|\phi^{\theta_i^c}(j|b_i)| = \frac{1}{\sqrt{2}}|(|\phi^{\theta_i}(j|0)| \pm |\phi^{\theta_i}(j|1)|)|,$$

une grande différence entre $|\phi^{\theta_i}(j|0)|$ et $|\phi^{\theta_i}(j|b_i)|$ implique que

$$|\phi^{\theta_i^c}(j|b_i)| \approx |\phi^{\theta_i^c}(j|b_i)|.$$

Donc, une grande différence entre les normes des amplitudes associées à $|0\rangle_{\theta_i}$ et $|1\rangle_{\theta_i}$ se traduit par des amplitudes de transition semblables dans la base complémentaire.

Dernière remarque, considérons la portion de l'opérateur OCPS qui correspond à un résultat partiel $C_i = (\widehat{\theta}_i, \widehat{b}_i)$ (ici $\mathbf{C}_i$ est la variable aléatoire associée). Par la suite, nous Noterons $\dot{C}_i$ l'ensemble des résultats finaux j pouvant être obtenus en raffinant l'état quantique correspondant au résultat C_i. En général, on a que

$$\begin{aligned}
\mathrm{P}\left(\mathbf{C}_i = (\widehat{\theta}_i, \widehat{b}_i)|\Theta_i = \theta_i\right) &= \sum_{b\in\{0,1\}} \|\phi^{\theta_i}(C_i|b)\|^2 = \sum_{j\in\dot{C}_i} \sum_{b\in\{0,1\}} |\phi^{\theta_i}(j|b)|^2 \\
&= \sum_{j\in\dot{C}_i} \sum_{b\in\{0,1\}} |\phi^{\theta_i^c}(j|b)|^2.
\end{aligned}$$

Autrement dit, la norme des colonnes restreintes au résultat C_i est conservée peut importe la base dans laquelle l'opérateur OCPS est exprimé. Ceci est équivalent à dire qu'aucune information sur la base de transmission ne peut être obtenue avant le raffinement.

2.8.5 Résultats informatifs

Les mécanismes exposés à la section précédente sont suffisants pour conclure que $\mathcal{B}$ob* ne peut à la fois avoir beaucoup d'information sur b_i et en même temps avoir une bonne probabilité de passer le test d'$\mathcal{A}$lice lorsqu'il est appliqué sur le photon π_i. Les définitions suivantes aideront à faire le lien.

Un résultat final j est informatif lorsqu'il donne de l'information sur le bit encodé dans le photon π_i lorsque la base $\widehat{\theta}_i = \theta_i^c$. Nous noterons par $(j, \widehat{\theta}_i, \widehat{b}_i)$ le résultat j obtenu par le raffinement du résultat partiel $C_i = (\widehat{\theta}_i, \widehat{b}_i)$. Plus précisément,

Définition 26 *Un résultat* $(j, \widehat{\theta}_i, \widehat{b}_i)$ *est* ρ–informatif *pour* $\frac{1}{2} < \rho \leq 1$*, s'il existe un* $b \in \{0,1\}$ *tel que*

$$\mathrm{P}\left(\mathbf{b}_i = b|\Theta_i = \widehat{\theta}_i^c \wedge \mathbf{j}_i = j\right) = \frac{|\phi^{\widehat{\theta}_i^c}(j|b)|^2}{|\phi^{\widehat{\theta}_i^c}(j|0)|^2 + |\phi^{\widehat{\theta}_i^c}(j|1)|^2} \geq \rho.$$

Lorsqu'un résultat j est ρ–informatif, l'information sur b_i qu'il divulgue est

$$\mathbf{I}(\mathbf{b}_i|\mathbf{j}_i = j, \Theta = \widehat{\theta}_i^c) \geq 1 + \rho \lg \rho + (1-\rho)\lg(1-\rho).$$

Remarquons qu'un résultat j qui est ρ–informatif implique la relation suivante entre la norme des amplitudes de transition pour les bits 0 et 1.

$$\begin{aligned} |\phi^{\widehat{\theta}_i^c}(j|b)|^2 &\geq \rho(|\phi^{\widehat{\theta}_i^c}(j|0)|^2 + |\phi^{\widehat{\theta}_i^c}(j|1)|^2) \\ &\geq \frac{\rho}{1-\rho}|\phi^{\widehat{\theta}_i^c}(j|1-b)|^2 \text{ d'où} \\ |\phi^{\widehat{\theta}_i^c}(j|b)| &\geq \sqrt{\frac{\rho}{1-\rho}}|\phi^{\widehat{\theta}_i^c}(j|1-b)|. \end{aligned}$$

Par exemple, si j est $\frac{3}{4}$–informatif alors pour $b \in \{0,1\}$ nous avons que

$$|\phi^{\widehat{\theta}_i^c}(j|b)| \geq \sqrt{3}|\phi^{\widehat{\theta}_i^c}(j|1-b)|.$$

Il ne suffit pas de définir les résultats informatifs, il faut aussi considérer la probabilité d'en obtenir un. Un raffinement à partir du résultat partiel C_i qui a une bonne probabilité d'être informatif est dit prometteur.

Définition 27 *Un résultat partiel $C_i = (\widehat{\theta}_i, \widehat{b}_i)$, est (ρ,τ)*–prometteur *pour $0 \leq \tau \leq 1$ si pour $J = \{j \in \dot{C}_i | j \text{ est } \rho\text{–informatif}\}$ on a que*

$$\mathrm{P}(\mathbf{j}_i \in J|\mathbf{C}_i = C_i) = \frac{\mathrm{P}(\mathbf{j}_i \in J \wedge \mathbf{C}_i = C_i)}{\mathrm{P}(\mathbf{C}_i = C_i)} = \frac{\sum_{j\in J}\sum_{b\in\{0,1\}}|\phi^{\widehat{\theta}_i^c}(j|b)|^2}{\sum_{j\in \dot{C}_i}\sum_{b\in\{0,1\}}|\phi^{\widehat{\theta}_i^c}(j|b)|^2} \geq \tau.$$

Supposons que nous disposions d'un résultat partiel (ρ,τ)–prometteur, voyons ce que nous pouvons dire à propos des amplitudes de transition après un changement de base. Nous plaçons l'analyse après que le résultat de la première mesure ait été obtenu. Le camouflage de $C_i = (\widehat{\theta}_i, \widehat{b}_i)$ est fourni à $\mathcal{A}$lice. Soit $j \in J$ un résultat ρ–informatif et $b_i^* \in \{0,1\}$ tel que $|\phi^{\theta_i^c}(j|b_i^*)| \geq |\phi^{\theta_i^c}(j|1-b_i^*)|$ (en réalité b_i^* est fonction du résultat final j même si pour alléger la notation nous n'indiquerons pas clairement que tel est le cas). Remarquons que pour tout $b \in \{0,1\}$,

$$\begin{aligned} |\phi^{\theta_i}(j|b)|^2 &= |\frac{1}{\sqrt{2}}(|\phi^{\theta_i^c}(j|0)| \pm |\phi^{\theta_i^c}(j|1)|)|^2 \\ &\leq \frac{1}{2}||\phi^{\theta_i^c}(j|b_i^*)| + \sqrt{\frac{1-\rho}{\rho}}|\phi^{\theta_i^c}(j|b_i^*)||^2 \\ &\leq \frac{1}{2}|\phi^{\theta_i^c}(j|b_i^*)|^2\left(1+\sqrt{\frac{1-\rho}{\rho}}\right)^2. \end{aligned}$$

De la même façon on obtient,

$$|\phi^{\theta_i}(j|b)|^2 \geq \frac{1}{2}|\phi^{\theta_i^c}(j|b_i^*)|^2 \left(1 - \sqrt{\frac{1-\rho}{\rho}}\right)^2.$$

Quel que soit le bit $b \in \{0,1\}$, l'amplitude exprimée dans la base θ_i d'un résultat informatif en θ_i^c est coïncée entre deux valeurs voisines. Plus ρ approche 1, plus les valeurs de $|\phi^{\theta_i}(j|0)|^2$ et $|\phi^{\theta_i}(j|1)|^2$ sont près l'une de l'autre.

2.8.6 Passer le test

La probabilité de passer le test une fois le camouflage ouvert et $\widehat{\theta}_i = \theta_i$ constaté correspond à la probabilité que $\widehat{b}_i = b_i$,

$$p_t = \mathrm{P}\left(\mathbf{b}_i = \widehat{b}_i | ouvrir_i = 1 \wedge \Theta_i = \widehat{\theta}_i\right) = \frac{\|\phi^{\theta_i}(C_i|b_i)\|^2}{\|\phi^{\theta_i}(C_i|0)\|^2 + \|\phi^{\theta_i}(C_i|1)\|^2}.$$

Supposons que le résultat partiel C_i soit (ρ,τ)–prometteur.

$$\begin{aligned}
\|\phi^{\theta_i}(C_i|b_i)\|^2 &= \sum_{j\in\dot{C}_i} |\phi^{\theta_i}(j|\widehat{b}_i)|^2 \\
&= \sum_{j\in J} |\phi^{\theta_i}(j|\widehat{b}_i)|^2 + \sum_{j\in\dot{C}_i\setminus J} |\phi^{\theta_i}(j|\widehat{b}_i)|^2 \\
&\leq \sum_{j\in J} |\frac{1}{\sqrt{2}}(|\phi^{\theta_i^c}(j|0)| + |\phi^{\theta_i^c}(j|1)|)|^2 + \sum_{j\in\dot{C}_i\setminus J} |\phi^{\theta_i}(j|\widehat{b}_i)|^2 \\
&\leq \frac{1}{2}(1 - \sqrt{\frac{1-\rho}{\rho}})^2 \sum_{j\in J} |\phi^{\theta_i^c}(j|b_i^*)|^2 + \sum_{j\in\dot{C}_i\setminus J} |\phi^{\theta_i}(j|\widehat{b}_i)|^2.
\end{aligned}$$

La somme de droite peut être bornée par le fait que C_i est (ρ,τ)–prometteur de la façon suivante,

$$\begin{aligned}
\sum_{j\in\dot{C}_i\setminus J} |\phi^{\theta_i}(j|b_i)|^2 &= \frac{1}{2}\sum_{j\in\dot{C}_i\setminus J} ||\phi^{\theta_i^c}(j|0)| \pm |\phi^{\theta_i^c}(j|1)||^2 \\
&\leq \frac{1}{2}\sum_{j\in\dot{C}_i\setminus J} ||\phi^{\theta_i^c}(j|0)| + |\phi^{\theta_i^c}(j|1)||^2 \\
&\leq \sum_{j\in\dot{C}_i\setminus J} |\phi^{\theta_i^c}(j|0)|^2 + |\phi^{\theta_i^c}(j|1)|^2 \\
&\leq (1-\tau)(\|\phi^{\theta_i^c}(C_i|0)\|^2 + \|\phi^{\theta_i^c}(C_i|1)\|^2).
\end{aligned}$$

Ce qui nous donne pour p_t la borne suivante,

$$p_t = \frac{\|\phi^{\theta_i}(C_i|b_i)\|^2}{\|\phi^{\widehat{\theta}_i}(C_i|0)\|^2 + \|\phi^{\widehat{\theta}_i}(C_i|1)\|^2}$$

$$\leq \frac{\frac{1}{2}\sum_{j\in J}|\phi^{\theta_i^c}(j|b_j^*)|^2(1+\sqrt{\frac{1-\rho}{\rho}})^2+(1-\tau)(\|\phi^{\theta_i^c}(C_i|0)\|^2+\|\phi^{\theta_i^c}(C_i|1)\|^2)}{\|\phi^{\widehat{\theta}_i}(C_i|0)\|^2+\|\phi^{\widehat{\theta}_i}(C_i|1)\|^2}$$

$$\leq 1+\frac{1}{2}(1+\sqrt{\frac{1-\rho}{\rho}})^2-\tau. \tag{2.5}$$

Si pour la base annoncée $\theta_i = \widehat{\theta}_i^c$ $\mathcal{B}$ob* peut exécuter un raffinement (ρ,τ)–prometteur alors si la base annoncée avait été $\theta_i = \widehat{\theta}_i$ et si $\mathcal{A}$lice avait vérifié le camouflage, celui-ci aurait été tel que $\widehat{b}_i = b$ avec probabilité

$$p_t \leq 1+\frac{1}{2}(1+\sqrt{\frac{1-\rho}{\rho}})^2-\tau.$$

Avec probabilité plus grande que $1-p_t$ la variable *erreur* aurait été augmentée. Rappelons que suite à la première mesure, la probabilité que $\widehat{\theta}_i=\theta_i$ est exactement $\frac{1}{2}$. De plus, chaque camouflage est vérifié aussi avec probabilité exactement $\frac{1}{2}$. Donc, à chaque fois que $\mathcal{B}$ob* obtient un résultat (ρ,τ)–prometteur, la probabilité p_e qu'$\mathcal{A}$lice détecte une erreur est

$$p_e = \frac{1-p_t}{4} \geq \frac{1}{4}(\tau - \frac{1}{2}(1+\sqrt{\frac{1-\rho}{\rho}})^2). \tag{2.6}$$

2.8.7 Sécurité dans un cas simplifié

Dans cette section, nous analysons la sécurité du protocole 2.3.1 qui réalise $\binom{2}{1}$–TI$_1^*$ contre les mesures individuelles sous l'hypothèse que le canal quantique est parfait. Pour la transmission d'un bit parmi deux, nous utilisons la fonction d'amplification $h(x)=\bigoplus_{i=1}^n x_i$ pour $x\in\{0,1\}^n$.

Nous venons de voir que pour obtenir de l'information sur le bit b_i dans la base $\widehat{\theta}_i^c$, $\mathcal{B}$ob* augmente ses chances de se faire détecter. Plus sa mesure lui permet d'obtenir de l'information sur le bit plus la probabilité qu'il soit détecté est grande. Définissons l'ensemble $\mathcal{I}(\rho,\tau)\subseteq\{1,\ldots,4n\}$ des positions pour lesquelles la mesure effectuée est (ρ,τ)–prometteuse. Clairement, la cardinalité de $\mathcal{I}(\rho,\tau)$ ne doit pas être trop grande pour que $\mathcal{B}$ob* ait une probabilité non négligeable de passer l'étape 4 de **Stratégie**(δ,n) sans être rejeté. Soit $n_{\mathcal{I}}$ la cardinalité de l'ensemble $\mathcal{I}(\rho,\tau)$. Étant donné $n_{\mathcal{I}}$ on peut calculer la probabilité p_s pour $\mathcal{B}$ob* de ne pas se faire détecter étant donné la tolérance aux erreurs δ. Ainsi,

$$p_s \leq \mathrm{P}\left(\mathbf{erreur} < \delta n | \#\boldsymbol{\mathcal{I}}(\rho,\tau) = n_{\mathcal{I}}\right) \leq \sum_{j=\delta n}^{n_{\mathcal{I}}} \binom{n_{\mathcal{I}}}{j} p_e^j (1-p_e)^{n_{\mathcal{I}}-j}.$$

Comme il s'agit d'une distribution binomiale, la probabilité que le nombre de succès s'éloigne de la valeur espérée est négligeable. La valeur espérée E de la variable aléatoire *erreur* est telle que

$$E \geq n_{\mathcal{I}} \cdot p_e = n_{\mathcal{I}} \frac{1}{4}(\tau - \frac{1}{2}(1+\sqrt{\frac{1-\rho}{\rho}})^2).$$

De plus, $\mathcal{A}$lice refuse de continuer lorsque le taux d'erreurs observées est plus grand que δ. Ce taux d'erreurs est calculé sur les positions où $ouvrir_i = 1$ et $\widehat{\theta}_i = \theta_i$. Celles-ci forment environ $\frac{1}{4}$ des $4n$ photons envoyés. L'espérance du taux d'erreurs observées τ_e est

$$\tau_e = \frac{n_{\mathcal{I}} \cdot p_e}{n} = \frac{n_{\mathcal{I}}}{4n}(\tau - \frac{1}{2}(1+\sqrt{\frac{1-\rho}{\rho}})^2). \tag{2.7}$$

Exemple numérique

Pour y voir un peu plus clair, voici un exemple numérique qui permet de voir comment l'information que donne une mesure influence la probabilité qu'$\mathcal{A}$lice détecte une erreur. Supposons que $\mathcal{B}$ob* fasse $n_{\mathcal{I}}$ raffinements $(\frac{19}{20}, \frac{8}{9})$–prometteurs sur les $4n$ photons transmis par $\mathcal{A}$lice. L'espérance du taux d'erreurs observées par $\mathcal{A}$lice est

$$\tau_e = \frac{n_{\mathcal{I}}}{n} \cdot 0.0332893.$$

Pour qu'$\mathcal{A}$lice accepte de continuer, il faut que

$$\tau_e = \frac{n_{\mathcal{I}}}{n} \cdot 0.0332893 \leq \delta.$$

Ce qui implique que

$$n_{\mathcal{I}} \leq \frac{\delta n}{0.0332893}.$$

Pour que $\mathcal{B}$ob* puisse espérer passer le test avec probabilité non négligeable, le nombre de ces raffinement $(\frac{19}{20}, \frac{8}{9})$–prometteurs doit être inférieur à $\frac{\delta n}{0.0332893}$. Si $\delta = 0.01$ alors le nombre de positions qui admettent un raffinement $(\frac{19}{20}, \frac{8}{9})$–prometteurs est moindre que $0.3004n$.

Le bit inconnu

Supposons pour l'instant que la canal quantique n'est pas bruyant auquel cas l'utilisation d'un code correcteur n'est pas requise. Supposons aussi que q_0 et q_1 sont des chaînes d'un bit. Prenons comme fonction de hachage h, le ou-exclusif de tous les bits de I_0 et de I_1. Pour simplifier, nous considérons des ensembles I_0 et I_1 de cardinalité n. C'est-à-dire que sur les $4n$ photons transmis, $2n$ sont tels que $ouvrir_i = 0$ et parmi ceux-là n sont dans l'ensemble I_0 et n dans l'ensemble I_1. Cette hypothèse est valide dans le cas où un code correcteur est utilisé car même si le nombre de photons π_i mesurés dans la base $\widehat{\theta}_i = \theta_i$ est moindre que n, un $\mathcal{B}$ob honnête peut combler la différence en incluant dans son ensemble I_c des bits qu'il a mesurés en $\widehat{\theta}_i \neq \theta_i$. Sauf avec probabilité négligeable, le nombre de ces bits est moindre que ϵn pour $\epsilon > 0$ en autant que n soit assez grand, le code correcteur permettra, si sa distance minimale est suffisante, de corriger ceux-ci. Voyons combien d'information au maximum $\mathcal{B}$ob* obtient sur le bit le moins connu dans notre scécario simplifié.

Pour que $\mathcal{B}$ob* puisse obtenir de l'information sur q_0 et q_1, il doit pouvoir estimer la valeur du ou-exclusif des deux ensembles I_0 et I_1. Montrons que ceci ne peut être le cas en déterminant un ensemble $I_{\overline{c}}$ pour lequel $\mathcal{B}$ob* n'a qu'une quantité négligeble d'information sur le ou-exclusif des bits de $I_{\overline{c}}$ pour $\overline{c} \in \{0, 1\}$ tel que

$$\#(I_{\overline{c}} \cap \Delta^*(\theta, \widehat{\theta})) \geq \#(I_{1-\overline{c}} \cap \Delta^*(\theta, \widehat{\theta})).$$

Puisque $\mathrm{P}\left(\Theta_i = \widehat{\theta}_i\right) = \frac{1}{2}$, nous obtenons que sauf avec probabilité négligeable $2^{-\epsilon^2 n}$,

$$\#(I_{\overline{c}} \cap \Delta^*(\theta, \widehat{\theta})) \geq n(\frac{1}{2} - \epsilon)$$

pour tout $\epsilon > 0$ en autant que n soit suffisamment grand. Montrons maintenant que pour pouvoir obtenir une quantité non négligeable d'information sur le ou-exclusif des bits de $I_{\overline{c}}$, $\mathcal{B}$ob* doit effectuer au moins $n(\frac{1}{2} - \epsilon')$ raffinements $(\frac{19}{20}, \frac{8}{9})$–prometteurs pour tout $\epsilon' > 0$.

Lemme 1 *Pour que $\mathcal{B}ob^*$ puisse obtenir une quantité non négligeable d'information sur le ou-exclusif des bits de $I_{\overline{c}}$, il doit effectuer au moins, pour tout $\epsilon' > 0$, $n(\frac{1}{2} - \epsilon')$ raffinements $(\frac{19}{20}, \frac{8}{9})$–prometteurs.*

Preuve. Supposons que tel n'est pas le cas. Il y a donc moins de $n(\frac{1}{2} - \epsilon')$ raffinements $(\frac{19}{20}, \frac{8}{9})$–prometteurs. Rappelons qu'un raffinement sur le photon π_i est $(\frac{19}{20}, \frac{8}{9})$–prometteurs si

$$\mathrm{P}\left((\exists b \in \{0,1\})[\mathrm{P}\left(\mathbf{b}_i = b | \mathbf{j}_i = j \wedge \Theta_i = \widehat{\theta}_i^c\right) \geq \frac{19}{20}]\right) \geq \frac{8}{9},$$

la probabilité extérieure étant calculée sur les $j \in \dot{C}_i$. Sauf avec probabilité négligeable, pour tout $\epsilon > 0$

$$\#(I_{\overline{c}} \cap \Delta^*(\theta, \widehat{\theta})) \geq n(\frac{1}{2} - \epsilon),$$

le nombre $\overline{n}$ de positions $i \in I_{\overline{c}}$ pour lesquelles le raffinement sur π_i n'est pas $(\frac{19}{20}, \frac{8}{9})$–prometteurs est tel que

$$\overline{n} \geq n(\frac{1}{2} - n\epsilon) - n(\frac{1}{2} - \epsilon') = n(\epsilon' - \epsilon).$$

Soit $I'_{\overline{c}} \subseteq I_{\overline{c}}$ qui contient ces positions,

$$\begin{aligned} I'_{\overline{c}} &= \{i \in I_{\overline{c}} | \text{ Le raffinement sur } \pi_i \text{ n'est pas } (\tfrac{19}{20}, \tfrac{8}{9})\text{–prometteurs}\} \\ &= \{i \in I_{\overline{c}} | \mathrm{P}\left((\exists b \in \{0,1\})[\mathrm{P}\left(\mathbf{b}_i = b | \mathbf{j}_i = j \wedge \Theta_i = \widehat{\theta}_i^c\right) \geq \frac{19}{20}]\right) < \frac{8}{9}\} \\ &= \{i \in I_{\overline{c}} | \mathrm{P}\left((\forall b \in \{0,1\})[\mathrm{P}\left(\mathbf{b}_i = b | \mathbf{j}_i = j \wedge \Theta_i = \widehat{\theta}_i^c\right) < \frac{19}{20}]\right) \geq \frac{1}{9}\}. \end{aligned}$$

Une fois les mesures complétées, nous pouvons définir l'ensemble $I^*_{\overline{c}}$ des positions $i \in I'_{\overline{c}}$ pour lesquelles le bit b_i n'est pas connu avec probabilité meilleure que $\frac{19}{20}$. Formellement,

$$I^*_{\overline{c}} = \{i \in I'_{\overline{c}} | (\forall b \in \{0,1\})[\mathrm{P}\left(\mathbf{b}_i = b | \mathbf{j}_i = j\right) \leq \frac{19}{20}]\}.$$

Par l'indépendance entre les résultats des mesures (ici la limitation aux mesures individuelles facilite beaucoup l'analyse), sauf avec probabilité négligeable et pour $\epsilon^* > 0$,

$$\# I^*_{\overline{c}} \geq \frac{\# I'_{\overline{c}}}{9 - \epsilon^*} \geq \frac{\overline{n}}{9 - \epsilon^*} \geq \frac{n(\epsilon' - \epsilon)}{9 - \epsilon^*}.$$

Pour obtenir une quantité non négligeable d'information sur le ou-exclusif des bits de $I_{\overline{c}}$, $\mathcal{B}$ob* doit avoir de l'information sur le ou-exclusif des bits de $I^*_{\overline{c}}$. La cardinalité de $I^*_{\overline{c}}$ étant linéaire en n et chaque bit de $I^*_{\overline{c}}$ n'étant pas mieux connu que la probabilité fixe $\frac{19}{20}$, l'information sur le ou-exclusif des bits de $I^*_{\overline{c}}$ est négligeable. La probabilité p_0 que le ou-exclusif des bits de $I^*_{\overline{c}}$ soit 0 est telle que[2]

$$|p_0 - \frac{1}{2}| \leq |\frac{1}{2} - \frac{1 + (2\frac{19}{20} - 1)^{\# I^*_{\overline{c}}}}{2}| \leq 2^{-\gamma n}$$

pour $\gamma > 0$. En conclusion l'information sur la parité des bits de $I^*_{\overline{c}}$ est telle que,

$$\mathbf{I}(p_0, p_1) = 1 - \mathbf{H}(p_0, p_1) \leq 2^{-\gamma' n},$$

ce qui est négligeable.

■

Le lemme 1 stipule que $\mathcal{B}$ob* doit exécuter, pour tout $\epsilon > 0$, au moins $(\frac{1}{2} - \epsilon)n$ raffinements $(\frac{19}{20}, \frac{8}{9})$–prometteurs pour obtenir une quantité non négligeable d'information sur la parité de $I^*_{\overline{c}}$. Mais nous l'avons vu au début de cette section, $\mathcal{B}$ob* ne peut passer le test avec probabilité non négligeable s'il exécute plus de $0.3004n$ raffinements $(\frac{19}{20}, \frac{8}{9})$–prometteurs lorsque $\delta < 0.01$. Donc, sauf avec probabilité négligeable si $\mathcal{B}$ob* passe le test il n'a pas plus qu'une quantité négligeable d'information sur la parité de $I_{\overline{c}}$ et ce pour n'importe quel taux d'erreurs $p < 0.01$.

Il reste maintenant à généraliser l'argument au cas ou le canal quantique est bruyant. Dans ce scénario, $\mathcal{B}$ob* apprend de l'information supplémentaire due à l'utilisation d'un code correcteur. De plus, nous voulons permettre à $\mathcal{A}$lice de transmettre une chaîne de plus d'un bit. La prochaine section traite de ces généralisations.

2.9 Sécurité en présence de bruit

Maintenant intérressons-nous à ce qu'il advient lorsque $\mathcal{B}$ob* apprend les bits de redondance (ou bits correcteurs) du code correcteur C_n appliqué à la chaîne représentée par l'ensemble $I_{\overline{c}}$. Nous supposons que le code utilisé est linéaire. Les bits correcteurs $s(b) = s_1, \ldots, s_l$ associés à la chaîne b sont obtenus par l'application de celle-ci à la matrice génératrice G mise sous forme systématique dont on a enlevé la

2. Ceci parce que la probabilité que l expériences de Bernoulli chacune avec probabilité $1 > p > \frac{1}{2}$ de succès donnent un nombre pair de succès est $\frac{1+(2p-1)^l}{2}$.

portion prise par la matrice identité $\mathbf{I}_n$. Supposons que le code C_n généré par G est un $[n+l, n, d]$–code. Ainsi,

$$s(b) = b \cdot G \in \{0,1\}^l$$

et $(\forall b, b' \in \{0,1\}^n)[\Delta(b \uplus (b \cdot G), b' \uplus (b' \cdot G)) \geq d]$.

À la lumière de la discussion qui nous a permis de conclure que l'information sur la parité des bits de $I_{\overline{c}}$ est négligeable, nous nous intéressons au cas où l'incertitude à propos d'une sous-chaîne de $b^{\overline{c}}$ est grande suite à l'obtention des résultats de la mesure.

Définition 28 *La chaîne $\zeta \in \{0,1\}^n$ est (ρ, I)–*incertaine selon *$\mathcal{V}$ pour $\frac{1}{2} \leq \rho \leq 1$ et $I \subseteq \{1, \ldots, n\}$ si*

$$(\forall i \in I)(\forall b \in \{0,1\})[1 - \rho \leq \mathrm{P}\left(\zeta_i = b | \mathcal{V}\right) \leq \rho].$$

L'information ou la vue de $\mathcal{B}$ob* sur $b^{\overline{c}}$ suite à l'étape 4 mais avant l'étape 5 est $\mathcal{V}^4_{\mathcal{B}^*} = [H; \{j_1, \ldots, j_n\}; \{\theta_1, \ldots, \theta_n\}; I_0; I_1]$. Après l'annonce des bits correcteurs $s^0, s^1 \in \{0,1\}^l$ elle devient $\mathcal{V}^5_{\mathcal{B}^*} = [\mathcal{V}^4_{\mathcal{B}^*}; s^0; s^1]$.

Supposons que la chaîne $b^{\overline{c}}$ est (ρ, I)–incertaine selon $\mathcal{V}^4_{\mathcal{B}^*}$. Nous voulons déterminer quelle est l'incertitude résiduelle sur $b^{\overline{c}}$ une fois que les chaînes de bits correcteurs s^0 et s^1 sont obtenues (i.e. nous cherchons une borne sur $\mathbf{H}(\mathbf{b}^{\overline{c}} | \mathcal{V}^5_{\mathcal{B}^*})$). Sans perdre de généralités, supposons que

$$(\forall i \notin I)\mathrm{P}\left(\mathbf{b}_i = b_i | \mathbf{j}_i = j \wedge \Theta_i = \widehat{\theta}^c_i\right) = 1. \tag{2.8}$$

C'est-à-dire que $\mathcal{B}$ob* connaît exactement le bit b_i lorsque i n'est pas dans l'ensemble des bits incertains. Le cas réel est probablement pire auquel cas $\mathcal{B}$ob* a encore moins d'information sur la chaîne $b^{\overline{c}}$.

Définition 29 *Soit $I \subseteq \{1, \ldots, k\}$ de cardinalité r et $\beta \in \{0,1\}^k$. Le* code ponctionné *$C^{I,\beta}$ associé au $[n, k, d]$–code linéaire systématique C_n est tel que*

$$C^{I,\beta} = \{c \in C_n | (\forall i \in \{i_1, i_2, \ldots, i_{k-r}\} = \{1, \ldots, k\} \setminus I)[c_i = \beta_i]\}.$$

Il s'agit donc de l'ensemble des mots de codes de C_n pour lesquels les bits de message qui ne sont pas dans I sont fixes et correspondent à la chaîne β. Le code $C^{I,\beta}$ ainsi obtenu est un $[n, r, d]$–code linéaire. Sa matrice génératrice $G^{I,\beta}$ est facile à déterminer à partir de la matrice génératrice G du code C_n. Il s'agit simplement de la matrice G à laquelle on retire les rangées qui correspondent aux positions qui ne sont pas dans I.

Soit $b^* \in \{0,1\}^n$ la chaîne la plus probable pour $b^{\overline{c}}$ étant donné $\mathcal{V}^4_{\mathcal{B}^*}$. Puisque nous donnons gratuitement les bits $b_i^{\overline{c}}$ pour $i \notin I$, la chaîne $b^*_{[I^c]}$ est telle que $b^*_{[I^c]} = b^{\overline{c}}_{[I^c]}$. Par hypothèse que la chaîne $b^{\overline{c}}$ est (ρ, I)–incertaine selon $\mathcal{V}^4_{\mathcal{B}^*}$,

$$(\forall i \in I)[\mathrm{P}\left(\mathbf{b}_i = b_i^* | \mathcal{V}^4_{\mathcal{B}^*}\right) \leq \rho].$$

Et du point de vue de $\mathcal{B}$ob*, au mieux

$$(\forall i \in I)[\mathrm{P}\left(\mathbf{b}_i = b_i^* | \mathcal{V}^4_{\mathcal{B}^*}\right) = \rho]. \tag{2.9}$$

Lorsque les chaînes de bits correcteurs $s^0, s^1 \in \{0,1\}^l$ sont annoncées à $\mathcal{B}$ob* les candidats possibles pour $b^{\overline{c}}$ sont ceux dont la chaîne de bits correcteurs vaut $s^{\overline{c}}$ et dont les positions $i \notin I$ valent $b_i^{\overline{c}}$. On voit bien le rapport avec les codes ponctionnés; l'ensemble des candidats contient les mots $w \in \{0,1\}^n$ pour lesquels $w \uplus s^{\overline{c}}$ est un mot du code ponctionné C^{I,b^*}. Donnons toutes les chances à $\mathcal{B}$ob* de faire des ravages; donnons-lui la distance d telle que

$$\Delta(b^{\overline{c}}, b^*) = d. \tag{2.10}$$

Ici encore nous donnons à $\mathcal{B}$ob* de l'information qui ne lui est pas accessible en réalité. Nous allons montrer que même avec cette information supplémentaire, $\mathcal{B}$ob* est face à un grand nombre de candidats équiprobables.

L'ensemble des chaînes possibles pour $b^{\overline{c}}$ étant donné $\tilde{\mathcal{V}}^5_{\mathcal{B}^*}$ sont celles de l'ensemble

$$N_d^{b^*}(s^{\overline{c}}) = \{w \in \{0,1\}^n | w \uplus s^{\overline{c}} \in C^{I,b^*} \wedge \Delta(w, b^{\overline{c}}) = d\}.$$

Soit $\tilde{\mathcal{V}}^5_{\mathcal{B}^*}$ la vue de $\mathcal{B}$ob*, après l'étape 5, étant donné les coups de pouce décrits aux équations 2.8, 2.9 et 2.10. Par construction de $\tilde{\mathcal{V}}^5_{\mathcal{B}^*}$, la distribution associée aux chaînes possibles pour $b^{\overline{c}}$ est telle que

$$(\forall w \in N_d^{b^*}(s^{\overline{c}}))[\mathrm{P}\left(\mathbf{b}^c = w | \tilde{\mathcal{V}}^5_{\mathcal{B}^*}\right) = \frac{1}{\# N_d^{b^*}(s^{\overline{c}})}].$$

Ce qui nous permet de conclure que si la chaîne $b^{\overline{c}}$ est (ρ, I)–incertaine selon $\mathcal{V}^4_{\mathcal{B}^*}$, même en donnant à $\mathcal{B}$ob* les avantages suivants:

1. Les positions $i \notin I$ sont telles que le bit $b_i^{\overline{c}}$ est connu exactement de $\mathcal{B}$ob*,

2. chaque bit $i \in I$ est tel que $(\exists b \in \{0,1\})[\mathrm{P}\left(\mathbf{b}_i^{\overline{c}} = b | \mathcal{V}^4_{\mathcal{B}^*}\right) = \rho]$ et

3. $\mathcal{B}$ob* connaît exactement la distance d telle que $\Delta(b^{\overline{c}}, b^*) = d$,

le nombre de candidats équiprobables pour $b^{\overline{c}}$ est $\# N_d^{b^*}(s^{\overline{c}})$ selon $\mathcal{V}^5_{\mathcal{B}}$. Le lemme suivant, largement inspiré de [21], montre un fait important sur la cardinalité probable de $N_d^{b^*}(s^{\overline{c}})$.

Lemme 2 *Sauf avec probabilité* 2^{-t} *avec* $t > 0$*,*

$$\# N_d^{b^*}(s^{\overline{c}}) \geq \frac{\binom{r}{d}}{2^{t+l}}.$$

Preuve. En premier lieu, rappelons-nous que le code concaténé $C^{I,\beta}$ obtenu à partir de C_n, pour $r = \# I$ et $|\beta| = n - r$ est un $[r+l, r]$–code linéaire puisque C_n est lui-même un $[n+l, n]$–code linéaire. L'ensemble $N_d^{b^*}(s)$ contient les mots dont la chaîne de bits correcteurs est s et à distance exactement d de la chaîne b^* en variant seulement les positions dans I. Puisque le nombre total de mots dans $\{0,1\}^r$ à distance d de b^* est $\binom{r}{d}$, nous avons que

$$\sum_{s \in \{0,1\}^l} \# N_d^{b^*}(s) = \binom{r}{d}.$$

Soit p_{s,b^*} la probabilité d'obtenir la chaîne de bits correcteurs $\mathbf{s}^{\overline{c}} = s$, étant donné que chaque bit $b_i^{\overline{c}}$ pour $i \in I$ est tel que

$$\mathrm{P}\left(\mathbf{b}_i^{\overline{c}} = b_i^* | \mathcal{V}^4_{\mathcal{B}^*}\right) = \rho.$$

On peut écrire p_{s,b^*} comme

$$p_{s,b^*} = \frac{\# N_d^{b^*}(s)}{\binom{r}{d}}.$$

Supposons que

$$\# N_d^{b^*}(s) \leq \frac{\binom{r}{d}}{2^{t+l}}$$

pour tout $s \in S \subseteq \{0,1\}^l$. Dans ce cas pour chaque $s \in S$,

$$p_{s,b^*} \leq 2^{-t-l}.$$

La probabilité p_s que $\mathcal{B}$ob* apprenne un $s \in S$ est

$$p_s = \mathrm{P}\left(\mathbf{s}^{\overline{c}} \in S | \mathcal{V}^5_{\mathcal{B}^*}\right) \leq \#S \cdot 2^{-t-l}.$$

Puisque $\#S \subseteq \{0,1\}^l$, nous avons nécessairement

$$p_s \leq 2^{-t}.$$

En conclusion, la probabilité que $\mathcal{B}$ob* apprenne une chaîne de bits correcteurs $s \in S$ est moindre que 2^{-t}. Avec probabilité au moins $1 - 2^{-t}$, $\mathcal{B}$ob* apprendra un s tel que

$$\#N_d^{b^*}(s) \geq \frac{\binom{r}{d}}{2^{t+l}}.$$

■

La valeur de $\binom{r}{d}$ peut être bornée par l'approximation binomiale [55]:

$$\binom{r}{\gamma r} \geq \frac{2^{r\mathbf{H}(\gamma)}}{\sqrt{8r\gamma(1-\gamma)}}$$

en autant que $\gamma \leq \frac{1}{2}$. En posant $d = \gamma r$ nous obtenons par le lemme 2 que sauf avec probabilité 2^{-t},

$$\#N_d^{b^*}(s^{\overline{c}}) \geq \frac{2^{r\mathbf{H}(\gamma)-t-l}}{\sqrt{8r\gamma(1-\gamma)}}. \tag{2.11}$$

Puisque chaque bit $b_i^{\overline{c}}$ avec $i \in I$ est connu avec probabilité ρ, la valeur de d correspond au nombre de succès de r expériences de Bernoulli indépendantes avec paramètre ρ. Il est bien connnu que sous de telles conditions et pour $0 \leq \epsilon \leq \rho(1-\rho)$,

$$\mathrm{P}\left(d = \gamma r \leq (\rho - \epsilon)r\right) \leq 2^{-\epsilon^2 r}$$

pour r suffisamment grand.

En conclusion, étant donné que $b^{\overline{c}}$ est (ρ, I)–incertaine selon $\mathcal{V}^4_{\mathcal{B}^*}$, nous avons que

$$(\forall w \in \#N_d^{b^*}(s^{\overline{c}}))[\mathrm{P}\left(\mathbf{b}^{\overline{c}} = w | \tilde{\mathcal{V}}^5_{\mathcal{B}^*}\right) = \frac{1}{\#N_d^{b^*}(s^{\overline{c}})} \leq \frac{2^{r\mathbf{H}(\gamma)-t-l}}{\sqrt{8r\gamma(1-\gamma)}}] \tag{2.12}$$

sauf avec probabilité 2^{-t} pour

– $r = \#I$,

- $l = |s^{\overline{c}}|$,
- $\gamma = (\rho - \epsilon)$ pour $\epsilon > 0$.

Nous verrons à la section 2.9.2 comment choisir h^0, h^1 à l'étape 7 de façon à ce que $\mathbf{I}(h^{\overline{c}}(\mathbf{b}^{\overline{c}})|\mathcal{V}'_{\mathcal{B}^*})$ soit négligeable pour $\mathcal{V}'_{\mathcal{B}^*}$ la vue de $\mathcal{B}$ob* après l'exécution du protocole.

2.9.1 Retour à notre exemple numérique

Supposons que le taux d'erreurs estimé du canal quantique est $p < 0.0015$. Dans ce cas une tolérance $\delta = 0.0015$ fait l'affaire. D'après l'équation 2.7, le taux d'erreurs qui sera observé par $\mathcal{A}$lice est

$$\tau_e = \frac{n_{\mathcal{I}}}{n} \cdot 0.0332893$$

où $n_{\mathcal{I}}$ est le nombre de raffinement $(\frac{19}{20}, \frac{8}{9})$–prometteurs. Pour que $\mathcal{B}$ob* ait une probabilité non négligeable de passer le test, l'équation suivante doit être satisfaite:

$$n_{\mathcal{I}} \leq \frac{\delta n}{0.0332893} = 0.0450595n.$$

Le nombre de positions dans $I_{\overline{c}}$ qui ne sont pas $(\frac{19}{20}, \frac{8}{9})$–prometteurs est donc supérieur à $(1 - 0.0450595)n = 0.95494n$.

Le code correcteur C_n utilisé par $\mathcal{A}$lice et $\mathcal{B}$ob* pour corriger les bits des ensembles I_0 et I_1 doit avoir une distance minimale $d_n \geq 0.003n$. Pour être en mesure de déterminer le nombre de candidats équiprobables pour $b^{\overline{c}}$ après l'étape 5, nous devons déterminer l pour que C_n soit un $[n + l, n, 0.003n]$–code.

D'après la borne de Varshamov-Gilbert, pour qu'un tel code existe il faut que

$$n \leq (n + l)(1 - \mathbf{H}(0.003)) \leq (n + l)(1 - 0.0294641) = 0.970536(n + l).$$

Supposons que nous disposions magiquement d'un $[n+l, 0.950536(n+l), 0.003n]$–code linéaire. La longueur l de la chaîne de bits correcteurs est

$$\begin{aligned} l &= n + l - 0.970536(n + l) \\ &\leq 0.0303585n. \end{aligned}$$

Soit r la cardinalité de l'ensemble des positions qui ne sont pas connues avec probabilité plus grande que $\frac{19}{20}$. Nous utilisons maintenant l'équation 2.11 avec les paramètres suivants:

1. La valeur de r est sauf avec probabilité négligeable telle que $r \geq 0.95494 \cdot \frac{1}{9} \cdot n = 0.106104$,

2. la valeur de γ peut être telle que $\gamma = 1 - \rho = \frac{1}{20}$ de façon à ce que sauf avec probabilité négligeable $d \geq r\gamma$ pour d la distance entre b^* et $b^{\overline{c}}$.

Une fois $s^{\overline{c}}$ obtenu, le nombre de candidats équiprobables pour $b^{\overline{c}}$ est, sauf avec probabilité 2^{-t},

$$\begin{aligned} \#N_d^{b^*}(s^{\overline{c}}) &\geq \frac{2^{r\mathbf{H}(\gamma)-t-l}}{\sqrt{8r\gamma(1-\gamma)}} \\ &\geq 2^{0.030388n-0303585n-t}. \\ &\geq 2^{0.0000294678n-t}. \end{aligned}$$

En choisissant par exemple $t = 0.0000147339n$, on obtient que, sauf avec probabilité négligeable $2^{-0.0000147339n}$ en autant que $d \geq \gamma n$ et $\#I \geq r$, le nombre de candidats équiprobables sera

$$\#N_d^{b^*}(s^{\overline{c}}) \geq 2^{0.0000147339n}.$$

Pour avoir une probabilité non négligeable de passer le test, $\mathcal{B}$ob* est face à un nombre exponentiel en n de candidats équiprobables pour $b^{\overline{c}}$ suite à l'exécution de l'étape 5. La prochaine section montre que cela est suffisant pour qu'il soit possible de trouver une fonction d'amplification $h : \{0,1\}^n \rightarrow \{0,1\}^\mu$ pour $\mu \in O(n)$ telle que $h(b^{\overline{c}})$ est inconnu de $\mathcal{B}$ob*.

2.9.2 Amplification par hachage universel

Nous supposons que suite à l'obtention des résultats de ses mesures et après qu'il eut appris la chaîne de bits correcteurs s, $\mathcal{B}$ob* soit face à $2^{\sigma n}$ (i.e. $\sigma > 0$) candidats équiprobables pour $b^{\overline{c}}$. Le théorème suivant de [12] nous éclaire au sujet de l'information que $\mathcal{B}$ob* obtient sur $h(b^{\overline{c}})$ lorsque h est pigé aléatoirement dans une classe de fonctions fortement universel$_2$.

Théorème 8 ([12]) *Soit E un ensemble de candidats équiprobables pour $b^{\overline{c}}$. Soit $H \subseteq \{h : \{0,1\}^n \to \{0,1\}^\mu\}$ une classe de fonctions fortement universel$_2$. Étant donné la connaissance de E et la description de $h \in_R H$, l'information moyenne sur $h(b^{\overline{c}})$ est moindre que $lg\,(1+2^\mu/\#E)$ bits. La moyenne étant calculée sur les choix de h seulement.*

Si l'ensemble $N_d^{b^*}(s)$ de candidats équiprobables pour $b^{\overline{c}}$ est de taille $2^{\sigma n}$ alors $\mathcal{A}$lice peut transmettre par transmission inconsciente deux chaînes $q_0, q_1 \in \{0,1\}^\mu$ avec $\mu = (\sigma - \epsilon)n$. D'après le théorème 8, l'information $\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}^5_{\mathcal{B}^*}; \mathbf{h}^{\overline{c}} = h^{\overline{c}})$ pour $h^{\overline{c}} \in H$ est sauf avec probabilité négligeable telle que

$$\begin{aligned}
\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}^5_{\mathcal{B}^*}; \mathbf{h}^{\overline{c}} = h^{\overline{c}}) &\leq \mathbf{I}(h(\mathbf{b}^{\overline{c}})|\tilde{\mathcal{V}}^5_{\mathcal{B}^*}; \mathbf{h}^{\overline{c}} = h^{\overline{c}}) \\
&\leq \lg\,(1 + 2^{(\mu-\sigma)n}) \\
&\leq \lg\,(1 + 2^{-\epsilon n}) \\
&\leq 2^{-\epsilon n}/\ln 2.
\end{aligned}$$

Nous disposons maintenant de tout ce qu'il faut pour conclure à la sécurité du protocole de transmission inconsciente contre les mesures individuelles. La prochaine section fait la synthèse des relations que nous avons vu jusqu'à maintenant.

2.9.3 Synthèse

Le théorème suivant permet de déterminer les paramètres pour lesquels le protocole de transmission inconsciente $\binom{2}{1}$–TI_μ est sécuritaire contre les mesures individuelles. Comme à l'habitude, δ est le facteur de tolérance aux erreurs légèrement supérieur au taux d'erreurs du canal quantique. Le paramètre l est la longueur de la chaîne correctrice fournie par $\mathcal{A}$lice à l'étape 5. La classe $H_3^{n,\mu}$ des fonctions de hachage $h : \{0,1\}^n \to \{0,1\}^\mu$ est celle utilisée par $\mathcal{A}$lice pour amplifier son secret à l'étape 7. Pour ce faire, elle pige aléatoirement des fonctions $h^0, h^1 \in_R H_3^{n,\mu}$ et annonce leur description à $\mathcal{B}$ob*. Ici on considère que le nombre de photons BB84 transmis est $4n$.

Théorème 9 *Soit $\delta \leq 0.0006$ le facteur de tolérance d'$\mathcal{A}$lice. Soient $q_0, q_1 \in \{0,1\}^\mu$ les deux chaînes transmises par le protocole de transmission inconsciente $\binom{2}{1}$–TI_μ.*

Si $\mathcal{B}ob^*$ exécute $4n$ mesures qui lui permettent de passer le test avec probabilité non négligeable alors il existe $\overline{c} \in \{0,1\}$ tel que

$$\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}'_{\mathcal{B}^*}) \leq 2^{-0.026n+l+\mu}$$

sauf avec probabilité négligeable dans $O(2^{-0.001n})$ où $\mathcal{V}'_{\mathcal{B}^*}$ est la vue de $\mathcal{B}ob^*$ après l'exécution du protocole.

Preuve. Intéressons-nous au nombre n_I de raffinements (ρ,τ)–prometteurs pour $\rho = 0.95$ et $\tau = 0.80$. D'après l'équation 2.6, la probabilité p_e que $\mathcal{B}$ob* se fasse détecter s'il exécute un raffinement (ρ,τ)–prometteur est:

$$\begin{aligned} p_e \geq \frac{1-p_t}{4} &\geq \frac{1}{4}(\tau - \frac{1}{2}(1+\sqrt{\frac{1-\rho}{\rho}})^2) \\ &= 0.0110671. \end{aligned}$$

D'après l'équation 2.7, le taux d'erreurs moyen observé par $\mathcal{A}$lice si $\mathcal{B}$ob* effectue n_I raffinements (ρ,τ)–prometteurs est:

$$\overline{\tau}_e \geq \frac{n_I \cdot p_e}{n}$$

puisque celui-ci est calculé sur les positions $i \in \{1,\ldots,4n\}$ avec $\theta_i = \widehat{\theta}_i$ et $ouvrir_i = 1$.

Par l'indépendance entre les mesures, si n_I raffinements sont (ρ,τ)–prometteurs alors le taux d'erreurs réellement observés τ_e sera tel que $(\forall\epsilon_0 > 0)$

$$\mathrm{P}\left(\tau_e \leq \overline{\tau}_e - \epsilon_0\right) \leq 2^{-\epsilon_0^2 n}$$

par l'application de la loi des grands nombres de Bernstein [48]. Pour que $\mathcal{B}$ob* ait une probabilité non négligeable de passer le test, n_I doit être tel que

$$\frac{n_I \cdot p_e - \epsilon_0 n}{n} \leq \delta.$$

Ce qui implique pour $\epsilon_0 = 0.00001$

$$n_I \leq \frac{(\delta - \epsilon_0)n}{p_e} = \frac{(0.0006 - \epsilon_0)n}{0.0110671} = 0.0542147n.$$

Si le nombre de raffinements (ρ,τ)–prometteurs est moindre que n_I alors le nombre de raffinements $\overline{n}_I$ qui ne sont pas (ρ,τ)–prometteurs est

$$\begin{aligned} \overline{n}_I &\geq (1-n_I)n \\ &= 0.945785n. \end{aligned} \tag{2.13}$$

Soit $J_b \subseteq I_b, b \in \{0,1\}$ qui contient les positions $i \in I_b$ pour lesquelles le raffinement sur le photon π_i n'est pas (ρ,τ)–prometteurs. Soit $\overline{c} \in \{0,1\}$ tel que

$$\#J_{\overline{c}} \geq \#J_{1-\overline{c}}.$$

Par l'équation 2.13, on a que

$$\overline{n}_J = \#J_{\overline{c}} \geq \frac{\overline{n}_I}{2} = 0.4728n.$$

Encore une fois par l'indépendance entre les résultats des mesures, si au moins $\overline{n}_J$ des résultats ne sont pas (ρ,τ)–prometteurs alors sauf avec probabilité négligeable $2^{-\epsilon_1^2 n}$, pour $\epsilon_1 = 0.0001$, il existe un $I \subseteq J_{\overline{c}} \subseteq I_{\overline{c}}$ pour lequel $b^{\overline{c}}$ est (ρ, I)–incertaine selon $\mathcal{V}^4_{\mathcal{B}^*}$ avec

$$r = \#I \geq \overline{n}_J \cdot (1 - \tau - \epsilon_1) \geq 0.0944n.$$

Maintenant considérons la chaîne de bits correcteurs $s^{\overline{c}} \in \{0,1\}^l$ annoncée par $\mathcal{A}$lice. Le lemme 2 et l'équation 2.11 nous indique que sauf avec probabilité négligeable 2^{-t}, $s^{\overline{c}}$ sera telle que le nombre de candidats équiprobables $N_d^{b^*}(s^{\overline{c}})$ pour $b^{\overline{c}}$ est:

$$N_d^{b^*}(s^{\overline{c}}) \geq 2^{r\mathbf{H}(\rho)-l-t} = 2^{0.0944\mathbf{H}(0.9)n-l-t} = 2^{0.027n-l-t}.$$

En moyenne, pour $h^{\overline{c}} \in_R H_3^{n,\mu}$ l'information $\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}^5_{\mathcal{B}^*}; \mathbf{h}^{\overline{c}} = h^{\overline{c}})$ sur le résultat de la fonction $h^{\overline{c}}$ lorsqu'appliquée à $b^{\overline{c}}$ est donné par le théorème 8,

$$\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}^5_{\mathcal{B}^*}; \mathbf{h}^{\overline{c}} = h^{\overline{c}}) \quad \leq \quad 2^{-0.027n+l+t+\mu} \text{ bits.}$$

sauf avec probabilité 2^{-t} pour $N_d^{b^*}(s)$ l'ensemble des candidats équiprobables pour $b^{\overline{c}}$ comme déterminé à l'équation 2.11. Posons $t = \epsilon_0 = \epsilon_1 = 0.001n$, nous obtenons:

$$\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}'_{\mathcal{B}^*}) \leq 2^{-0.026n+l+\mu} \text{ bits.}$$

■

2.9.4 Codes correcteurs concaténés

Il est avantageux pour $\mathcal{A}$lice d'utiliser des codes concaténés. Dans [39], on montre comment ceux-ci peuvent en principe approcher la borne de Varshamov-Gilbert. Pour

n assez grand, il est possible de spécifier la proximité de la borne de Varshamov-Gilbert qu'un code concaténé peut atteindre. Ainsi pour corriger un taux d'erreurs inférieur à 0.0006 un code concaténé existe [55] avec n'importe quel

$$l \geq \frac{\mathbf{H}(0.0012)}{1 - \mathbf{H}(0.0012)} = 0.0135548.$$

Le théorème 9 peut donc être utilisé pour conclure que, sauf avec probabilité négligeable,

$$\mathbf{I}(h(\mathbf{b}^{\overline{c}})|\mathcal{V}'_{\mathcal{B}^*}) \leq 2^{-0.026n+0.014n+\mu} \leq 2^{-0.012n+\mu}.$$

Il devient donc possible de transmettre sécuritairement contre les mesures individuelles des chaînes $q_0, q_1 \in \{0,1\}^\mu$ pour $\mu < 0.013n$.

Si nous considérons que le code utilisé par $\mathcal{A}$lice est tel que la longueur de la chaîne de bits correcteurs est exactement ce qui est autorisé par la borne de Varshamov-Gilbert alors on peut représenter graphiquement l'exposant σn pour lequel, sauf avec probabilité négligeable,

$$\# N_d^{b^*}(s) \geq 2^{\sigma n}.$$

La figure 2.8 montre la valeur de l'exposant (qui détermine la longueur des chaînes pouvant être transmises) pour $\delta \in [0, \ldots, 0.0006], \tau = 0.80$ et $\rho = 0.95$. La méthode que nous avons utilisée ne permet pas de déterminer si le protocole est sécuritaire pour $\delta \geq 0.0006$, l'exposant obtenu étant négatif. Cependant, une analyse qui porterait davantage attention au choix des paramètres ρ et τ (en fonction de δ) pourrait conclure à la séucrité de BBCS pour des taux d'erreurs plus élevés. Il serait intéressant d'optimiser le résultat du théorème 9 de cette façon.

2.10 Conclusion

Après la publication du résultat précédent [54], une preuve de sécurité du protocole $\binom{2}{1}$–TI_1^* de [26] contre toutes les mesures permises par la mécanique quantique a été donnée par [71]. Pour que la transmission inconsciente puisse être utilisée dans toute sa généralité, il est important de pouvoir obtenir un résultat analogue au théorème 9 dans le cas où l'ensemble des mesures cohérentes est autorisé. C'est-à-dire qu'il doit

FIG. 2.8 - *lg_2 de la taille de $N_d^{b^*}(s)$ pour* $(\delta \in \{0, \ldots, 0.0006\}, \rho = 0.95, \tau = 0.80)$.

être possible à partir du taux d'erreurs du canal et de la longueur de la chaîne à transmettre μ, de pouvoir déterminer le nombre de photons à transmettre en plus de la fonction d'amplification à utiliser qui permettent la transmission inconsciente sécuritaire d'une chaîne de longueur μ parmi deux.

L'approche de [71] est différente de celle que nous avons adoptée ici. La sécurité du protocole $\binom{2}{1}$–TI_1^* contre les mesures cohérentes que $\mathcal{B}$ob* peut effectuer est obtenue en montrant que la matrice de densité associée aux systèmes qui sont tels que $h(b^{1-c}) = 0$ est presqu'identique à celle des systèmes qui sont tels que $h(b^{1-c}) = 1$. Notre approche n'utilise pas les matrices de densité des systèmes transmis. Nous montrons que, si $\mathcal{B}$ob* veut obtenir de l'information sur la valeur de la fonction d'amplification appliquée à la chaîne b^{1-c}, il doit effectuer une mesure qui ne lui permet pas de passer le test d'$\mathcal{A}$lice. Il est intéressant de voir comment l'approche que nous avons adoptée peut être généralisée pour tenir compte des mesures cohérentes. Le but étant de pouvoir obtenir un théorème analogue au théorème 9 pour le cas général.

Modèle OCPS et mesures cohérentes

Pour tenir compte des mesures les plus générales, l'opérateur OCPS qui modélise la mesure de $\mathcal{B}$ob* doit contenir l'ensemble de tous les états possibles pour les $N = 4n$ photons qu'$\mathcal{A}$lice envoie. Un tel opérateur contient 2^N colonnes et un nombre arbitraire de rangées. Les rangées sont regroupées par paquets représentants les résultats possibles pour la première mesure (celle-ci pouvant être incomplète). Comme pour les mesures individuelles, chacun de ces résultats partiels est étiqueté par un couple $C = (\widehat{\theta}, \widehat{b})$ représentant le contenu des camouflages à fournir pour maximiser la probabilité de passer le test. La différence ici est que $\widehat{\theta}$ est une séquence de N bases et $\widehat{b}$ est une chaîne de N bits. Une fois ce résultat obtenu, $\mathcal{A}$lice annonce la séquence de bases $\theta \in \{+, \times\}^N$ qu'elle a utilisée pour transmettre ses photons. $\mathcal{B}$ob* raffine maintenant sa mesure et obtient un résultat final $j \in \dot{C}$. L'amplitude de transition $\phi^\theta(j|b)$ est telle que $|\phi^\theta(j|b)|^2$ est la probabilité que l'état initial $|b\rangle_\theta$ produise le résultat final j. Soit $S(C, \theta) = \{b \in \{0,1\}^n | i \notin \Delta^*(\widehat{\theta}, \theta) \Rightarrow b_i = \widehat{b}_i\}$ la sphère contenant les chaînes qui ont le bit $\widehat{b}_i$ aux positions où $\theta_i = \widehat{\theta}_i$. Un résultat final informatif $j \in \dot{C}$ doit être tel que $\mathcal{D}_j^\theta = \{< b, |\phi^\theta(j|b)|^2 >\}_{b \in S(C,\theta)}$ soit une distribution loin d'être uniforme.

Changement de séquence de bases

Supposons que nous disposions de la matrice d'un opérateur OCPS exprimée dans la séquence de bases $\theta \in \{+, \times\}^n$ qui représente la mesure complète de $\mathcal{B}$ob*. Chacune des entrées de la matrice correspond à l'amplitude de transition $\phi^\theta(j|b)$ de l'état initial $|b\rangle_\theta$ vers l'état final $|j\rangle$. D'une façon analogue aux mesures individuelles, il est possible de calculer les amplitudes de transition si l'état initial était $|b\rangle_{\theta'}$ pour $\theta' \in \{+, \times\}^n$ au lieu de $|b\rangle_\theta$. La façon d'effectuer cette transformation n'est que la généralisation de celle pour le cas individuel comme représenté à l'équation 2.4. Chacune des amplitudes $\phi^\theta(j|b)$ de la rangée correspondant au résultat j pour $b \in \{0,1\}^n$ se voit transformer de la façon suivante:

$$\phi^{\theta'}(j|b) = \left(\frac{1}{\sqrt{2}}\right)^{\Delta(\theta,\theta')} \sum_{b' \in \Gamma(\theta,\theta',b)} \sigma(\theta, \theta', b')\phi^\theta(j|b')$$

pour

$$\Gamma(\theta, \theta', b) = \{b' \in \{0,1\}^n | (\forall i \in \{1, \ldots, n\})[\theta_i = \theta'_i \Rightarrow b'_i = b_i]\}$$

et

$$\sigma(\theta, \theta', b') = \prod_{i=1}^{n} \sigma_i(\theta, \theta', b')$$

avec

$$\sigma_i(\theta,\theta',b') = \begin{cases} +1 & \text{si } \theta_i = \theta'_i \\ +1 & \text{si } \theta_i = + \wedge \theta'_i = \times \wedge b'_i = 0 \\ -1 & \text{si } \theta_i = + \wedge \theta'_i = \times \wedge b'_i = 1 \\ +1 & \text{si } \theta_i = \times \wedge \theta'_i = + \wedge b'_i = 1 \\ -1 & \text{si } \theta_i = \times \wedge \theta'_i = + \wedge b'_i = 0. \end{cases}$$

Pour avoir une borne sur la norme de l'amplitude $\phi^{\theta'}(j|b)$, la fonction de signe $\sigma(\theta,\theta',b')$ n'est pas nécessaire. Comme nous l'avons vu à la section 2.8.3, l'équation suivante est une généralisation de l'équation 2.4:

$$|\phi^{\theta'}(j|b)| \leq \left(\frac{1}{\sqrt{2}}\right)^{\Delta(\theta,\theta')} \sum_{b' \in \Gamma(\theta,\theta',b)} |\phi^{\theta}(j|b')|.$$

De la même façon, si nous sommes intéressée à la norme d'une portion C d'une colonne de l'opérateur OCPS, l'équation précédente peut être exprimée de la façon suivante:

$$\|\phi^{\theta'}(C|b)\|^2 \leq 2^{-\Delta(\theta,\theta')} \sum_{j \in \dot{C}} \left(\sum_{b' \in \Gamma(\theta,\theta',b)} |\phi^{\theta}(j|b')| \right)^2. \tag{2.14}$$

Voyons maintenant comment la mesure d'un $\mathcal{B}$ob honnête peut être représentée. Nous nous servirons de ce cas pour décrire comment la généralisation aux mesures cohérentes pourrait être établie. Quelques résultats ont déjà été obtenus dans ce sens.

$\mathcal{B}$ob est honnête

Lorsque $\mathcal{B}$ob effectue des mesures honnêtes dans un contexte ou le canal quantique est parfait, chaque fois que pour une position $i \in \{1,\ldots,n\}$ on a que $\widehat{\theta}_i = \theta_i$ alors $\widehat{b}_i = b_i$. De plus, pour chaque position $i \in \{1,\ldots,n\}$ pour lesquelles $\widehat{\theta}_i \neq \theta_i$ on a que $\mathrm{P}\left(\mathbf{b}_i = \widehat{b}_i\right) = \frac{1}{2}$. La norme des amplitudes $\|\phi^{\theta}(C|b)\|$ exprimées dans la séquence $\theta \in \{+,\times\}^n$ pour $C = (\widehat{\theta},\widehat{b})$ obéie aux relations suivantes:

$$(\forall b \in S(C,\theta))[\|\phi^{\theta}(C|b)\| = \left(\frac{1}{\sqrt{2}}\right)^{\Delta(\theta,\widehat{\theta})}] \tag{2.15}$$

et

$$(\forall b \notin S(C,\theta))[\|\phi^{\theta}(C|b)\| = 0]. \tag{2.16}$$

Puisque nous faisons l'hypothèse que la mesure de $\mathcal{B}$ob est honnête, le résultat C est un résultat final correspondant à une ligne de l'opérateur OCPS qui représente la mesure. Maintenant, calculons la somme au carré des normes des amplitudes $\phi^{\theta'}(C|b)$

pour chaque $b \in S(C,\theta')$ étant donné celles exprimées dans la séquence $\theta \in \{+,\times\}^n$. D'après l'équation 2.14,

$$\sum_{b\in S(C,\theta')} \|\phi^{\theta'}(C|b)\|^2 = 2^{-\Delta(\theta,\theta')} \sum_{b\in S(C,\theta')} \left(\sum_{b'\in\Gamma(\theta,\theta',b)} |\phi^{\theta}(C|b')| \right)^2 .$$

Par la relation 2.16 on a que,

$$\sum_{b\in S(C,\theta')} \|\phi^{\theta'}(C|b)\|^2 = 2^{-\Delta(\theta,\theta')} \sum_{b\in S(C,\theta')} \left(\sum_{b'\in\Gamma(\theta,\theta',b)\cap S(C,\theta)} |\phi^{\theta}(C|b')| \right)^2 . \tag{2.17}$$

Notons par $\Delta^*(\theta,\theta',\widehat{\theta}) = \{i|\widehat{\theta}_i \neq \theta_i \wedge \theta_i \neq \theta'_i\}$ (et sa cardinalité par $\Delta(\theta,\theta',\widehat{\theta})$) l'ensemble des positions de b qui, en les faisant varier, détermine l'ensemble $\Gamma(\theta,\theta',b)\cap S(C,\theta)$. Notons aussi $\overline{\Delta}^*(\theta,\theta',\widehat{\theta}) = \Delta^*(\theta,\theta')\backslash\Delta^*(\theta,\theta',\widehat{\theta})$ (et sa cardinalité par $\overline{\Delta}(\theta,\theta',\widehat{\theta})$). Ainsi, l'équation 2.17 devient

$$\sum_{b\in S(C,\theta')} \|\phi^{\theta'}(C|b)\|^2 = 2^{-\Delta(\theta,\theta')+\Delta(\theta,\theta',\widehat{\theta})} \sum_{b\in S(C,\theta')} \sum_{b'\in\Gamma(\theta,\theta',b)\cap S(C,\theta)} |\phi^{\theta}(C|b')|^2. \tag{2.18}$$

Remarquons que l'égalité est maintenue par la relation 2.15. Il est facile de voir que l'ensemble $\Gamma(\theta,\theta',b)\cap S(C,\theta)$ a la structure suivante,

$$(\forall b' \in S(C,\theta'))[\Gamma(\theta,\theta',b')\cap S(C,\theta) = \Gamma(\theta,\theta',b)\cap S(C,\theta)] \tag{2.19}$$

À la lumière de la relation 2.19, on peut réécrire l'équation 2.18 comme

$$\sum_{b\in S(C,\theta')} \|\phi^{\theta'}(C|b)\|^2 = 2^{-\Delta(\theta,\theta')+\Delta(\theta,\theta',\widehat{\theta})+\overline{\Delta}(\theta,\theta',\widehat{\theta})} \sum_{b'\in S(C,\theta)} |\phi^{\theta}(C|b')|^2. \tag{2.20}$$

Mais comme $\Delta(\theta,\theta',\widehat{\theta}) + \overline{\Delta}(\theta,\theta',\widehat{\theta}) = \Delta(\theta,\widehat{\theta})$ on obtient

$$\sum_{b\in S(C,\theta')} \|\phi^{\theta'}(C|b)\|^2 = \sum_{b'\in S(C,\theta)} \|\phi^{\theta}(C|b')\|^2. \tag{2.21}$$

L'équation 2.21 ne nous apprend rien que nous ne savions déjà. La mesure honnête est invariante en regard de la séquence annoncée θ. Autrement dit, peu importe la séquence annoncée θ, la mesure de $\mathcal{B}$ob peut être analysée de la même façon que précédemment.

Cependant, si $\mathcal{B}$ob veut obtenir de l'information sur les bits aux positions $i \in \Delta(\widehat{\theta},\theta)$, les amplitudes associées à un résultat $j \in C$ ne doivent pas avoir les mêmes normes. Supposons que la mesure informative de $\mathcal{B}$ob* est telle que pour chaque $\theta \in \{+, \times\}^n$:

$$\sum_{b \notin S(C,\theta)} |\phi^{\theta}(j|b)| = 0.$$

Dans ces conditions:

$$\sum_{b \in S(C,\theta')} \|\phi^{\theta'}(C|b)\|^2 < \sum_{b' \in S(C,\theta)} \|\phi^{\theta}(C|b)\|^2 \tag{2.22}$$

Si en plus la séquence θ' permet aussi à $\mathcal{B}$ob d'obtenir un résultat informatif sur les bits aux positions $i \in \Delta(\widehat{\theta}, \theta')$ on obtiendrait la relation inverse

$$\sum_{b \in S(C,\theta)} \|\phi^{\theta}(C|b)\|^2 < \sum_{b' \in S(C,\theta')} \|\phi^{\theta'}(C|b')\|^2. \tag{2.23}$$

Ceci est impossible car l'opération de changement de base est symétrique. Nous pourrions conclure à l'impossibilité d'obtenir de l'information sur les bits aux positions $i \in \Delta(\theta, \widehat{\theta})$ lorsque θ est annoncée et sur les bits $i \in \Delta(\theta', \widehat{\theta})$ lorsque θ' est annoncée. La réalisation d'une mesure qui donne de l'information sur les bits b_i pour $i \in \Delta(\theta, \widehat{\theta})$ pour plus d'une séquence $\theta \in \{+, \times\}^n$ serait contradictoire avec le fait que $\mathcal{B}$ob* fasse une mesure dont la probabilité de passer le test est non négligeable. Pour que ce raisonnement puisse s'appliquer, il faut que pour $b \in S(C, \theta)$

$$\sum_{b' \in \Gamma(\theta,\theta,b) \setminus S(C,\theta)} |\phi^{\theta}(j|b)| < \epsilon(n)$$

pour $\epsilon(n)$ suffisamment petit. Si tel était le cas, l'hypothèse que C donne un résutat informatif avec bonne probabilité permet de conclure 2.22 et 2.23. Intuitivement, moins $\mathcal{A}$lice tolère d'erreurs dans les camouflages révélés, plus $\epsilon(n)$ doit être petit. À l'opposé, plus le résultat de $\mathcal{B}$ob* est informatif, plus la violation de l'égalité 2.21 est importante. La difficulté de l'exercice réside dans la difficulté de caractériser $\epsilon(n)$ d'une façon non triviale. Il serait utile d'y parvenir pour voir si l'approche que nous avons adoptée pour dériver le théorème 9 peut nous aider à traiter le cas général.

Ensuite

Maintenant que nous avons discuté de la façon dont la transmission inconsciente peut être réalisée avec l'aide d'un canal quantique, il est naturel de voir à quoi celle-ci peut bien nous servir. Le prochain chapitre discute du problème d'identification en cryptographie. Nous verrons qu'il s'agit d'un problème taillé sur mesure pour la transmission inconsciente quantique.

Chapitre 3

Identification quantique

3.1 Introduction

La majorité d'entre nous utilisons fréquemment les systèmes bancaires automatisés. Qu'il s'agisse des systèmes de guichet automatique ou de paiement direct, le consommateur a vite pris l'habitude de faire confiance aux divers mécanismes qui permettent les transactions bancaires un peu partout. Tout porte à croire que ce mode de consommation sera généralisé à l'ensemble des secteurs économiques dans un avenir rapproché. Pour effectuer ce type de transaction, on présente au consommateur un clavier sur lequel il doit entrer son numéro d'identification personnel (NIP) pour effectuer l'opération désirée. Ce type de protection cryptographique comporte des faiblesses importantes. En effet, la confiance dont les utilisateurs font preuve envers ces procédés est la plus dangereuse des attitudes à prendre. Voici deux exemples récents de fraudes contre les systèmes automatisés de transaction bancaire.

Le New-York Times [72] rapporte les faits suivants qui se sont déroulés aux États-Unis. De faux employés d'une institution bancaire installent dans un centre d'achats un faux guichet automatique identique à un guichet normal. Ce faux guichet, lorsqu'un client insère sa carte, fonctionne comme tous les autres. Il demande le NIP du client et la transaction désirée. Une fois ces informations fournies le guichet imposteur répond qu'il est hors d'usage et redonne la carte. Le client déçu reprend sa carte et s'en retourne. Après quelques jours les fraudeurs reprennent le guichet prétextant son mauvais fonctionnement. Ils peuvent ensuite récupérer les NIPs fournis par les clients dont le guichet avait pour tâche de mémoriser les NIPs et le contenu de la bande magnétique. Maintenant les fraudeurs peuvent mettre en circulation de fausses cartes leur permettant de se substituer à l'usager légitime.

À Paris, des fraudeurs ont ajouté à l'avant d'un guichet bancaire un panneau identique à celui du guichet réel. Le client insère sa carte dans la fausse fente et compose son NIP. Celle-ci demeure à l'intérieur du leurre et est plus tard récupérée par les fraudeurs qui auront tôt fait de l'utiliser à leurs fins.

Le même type d'attaque peut être utilisée pour subtiliser les mots de passe des usagers d'un réseau informatique. En effet, quoi de plus facile que d'écrire un programme qui simule l'incitateur d'accès à un réseau informatique. Le programme n'a qu'à attendre l'arrivée d'un usager crédule pour ajouter un nouveau mot de passe à son répertoire. Les usagers doivent avoir confiance dans ces systèmes pour les utiliser. Ils protègent contre la substitution en autant que personne ne puisse écouter la transmission de l'information secrète entre l'usager et le serveur. Le hic c'est que le protocole qui permet au serveur d'identifier un client demande à ce dernier de divulguer son secret. Un système d'identification ne peut être considéré sécuritaire s'il demande à l'usager de fournir son secret pour que le serveur le reconnaisse. En d'autres mots, le secret que partage le serveur et l'usager doit être utilisé pour vérifier l'authenticité des acteurs sans qu'il soit divulgué. Il faudra aussi qu'il soit court et réutilisable.

Dans le modèle calculatoire, des solutions au problème d'identification existent. Nous en ferons la revue à la prochaine section. Par la suite, nous montrerons comment la transmission quantique peut être utilisée pour obtenir un résultat similaire. Contrairement aux solutions dans le modèle calculatoire, les usagers légitimes doivent être protégés contre les attaques des fraudeurs même si ceux-ci disposent d'une puissance de calcul illimitée. Nous débuterons en présentant un protocole très simple dont la sécurité dépend de l'existence de familles de codes correcteurs avec certaines propriétés. A moins que le canal quantique ne soit *parfait* (aucune erreur de transmission), aucun code ne possède les propriétés requises. La transmission inconsciente quantique sera utilisée pour simuler un canal quantique *parfait* de façon à ce que la famille de codes recherchée existe. La solution obtenue confère aux usagers légitimes une sécurité inconditionnelle. Nous montrerons qu'en transmettant $O(n^2)$ photons $\mathcal{A}lice$ et $\mathcal{B}ob$ peuvent vérifier l'égalité de deux secrets de $O(n)$ bits de long. Qu'un fraudeur $\mathcal{P}^*$ interagisse avec $\mathcal{A}lice$ ou $\mathcal{B}ob$ il ne pourra obtenir davantage qu'une fraction exponentielle d'un bit d'information.

3.2 Le modèle calculatoire

Beaucoup de solutions au problème d'identification ont été proposées dans le cas où les acteurs ont une puissance de calcul limitée. Dans cette section nous ferons une revue sommaire des solutions déjà proposées dans le modèle calculatoire.

La première solution calculatoire est une adaptation de la solution classique suivante. $\mathcal{A}lice$ et $\mathcal{B}ob$ ont en commun une fonction aléatoire $f_\phi : \{0,1\}^n \rightarrow \{0,1\}^n$ spécifiée par la chaîne commune et secrète ϕ. À chaque fois qu'ils veulent vérifier s'ils partagent ϕ, $\mathcal{A}lice$ et $\mathcal{B}ob$ échantillonnent la fonction sur un point aléatoire $[x, f_\phi(x)]$. Puisque la fonction est aléatoire, quelqu'un qui ne connaît pas ϕ ne peut prédire avec probabilité meilleure que 2^{-n} la valeur de la fonction sur un nouveau point $[x_{n+1}, f_\phi(x_{n+1})]$ à l'aide de ceux déjà observés. Cette façon de faire est impraticable car le nombre de bits nécessaires pour décrire une fonction de n bits dans n bits est $n2^n$. Le secret ϕ devrait donc être de taille exponentielle en fonction du paramètre de sécurité n.

Pour éviter ce problème, Goldreich, Goldwasser et Micali [41] ont imaginés de remplacer la fonction aléatoire par une fonction pseudo-aléatoire.

Fonctions pseudo-aléatoires. Une classe de fonctions pseudo-aléatoires est un ensemble de fonctions qui ont les mêmes propriétés que les fonctions aléatoires par rapport à un observateur limité en temps de calcul et qui peuvent être décrites succintement. Si un individu observe des paires $[x_1, f_\phi(x_1)], [x_2, f_\phi(x_2)], \ldots, [x_n, f_\phi(x_n)]$ et ne connaît pas ϕ, il ne peut efficacement trouver une nouvelle paire $[x_{n+1}, f_\phi(x_{n+1})]$ avec probabilité sensiblement meilleure que 2^{-n}.

Une classes de fonctions pseudo-aléatoires est obtenue à partir d'un générateur pseudo-aléatoire sécuritaire de bits via la construction de [41]. À leur tour, des générateurs de bits pseudo-aléatoires peuvent être obtenus étant donné n'importe quelle fonction à sens unique [42, 45]. En résumé, sous l'hypothèse que des fonctions à sens unique existent, le protocole d'identification de [41] peut être démontré sécuritaire.

D'autres solutions dans ce modèle ont été proposées. Elles sont basés sur les preuves à divulgation nulle d'identités [38]. Ces solutions qui ont aussi le désavantage d'être valable que sous hypothèses calculatoires, sont moins efficaces que celle que nous proposons.

3.2.1 Une autre hypothèse

Le problème d'identification est étudié dans divers scénarios par Fagin, Naor et Winkler [37]. Une des solutions proposées répond à nos critères. Étant donné l'existence d'un canal de transmission inconsciente $\binom{2}{1}$–TI$_n$, ils montrent comment l'égalité entre le secret ϕ partagé par $\mathcal{A}lice$ et $\mathcal{B}ob$ peut être vérifiée. Même si dans le modèle calculatoire l'existence d'un canal de transmission inconsciente est une hypothèse plus forte que l'existence de fonctions à sens unique, cette solution offre des avantages. La transmission inconsciente peut exister sans hypothèse calculatoire. Par exemple, sous l'hypothèse que la mécanique quantique est correcte ou si un canal bruyant est accessible [26], il est possible de construire un protocole pour $\binom{2}{1}$–TI$_1$.

Le protocole final que nous présentons ici est basé sur $\binom{2}{1}$–TI$_2$. Si nous caractérisons l'efficacité d'une solution de ce type par le nombre d'appels à $\binom{2}{1}$–TI$_1$, notre solution est plus efficace. Le protocole de [37] requiert $\Theta(n^2)$ appels à $otq1$ tandis que le nôtre n'en demande que $\Theta(n)$.

3.3 Préléminaires

3.3.1 Notation et outils

Pour $b \in \{0,1\}$, la fonction de sélection est définie par

$$(x,y)_{[b]} = \begin{cases} x & \text{if } b = 0 \\ y & \text{if } b = 1 \end{cases}$$

pour x et y des scalaires. En général, si x et y sont des vecteurs à n composantes et $\vec{b} \in \{0,1\}^n$ alors $(x,y)_{[\vec{b}]}$ est la concaténation de $(x_i, y_i)_{[b_i]}$ pour chaque $i \in \{1,2,\ldots,n\}$. En particulier, $(x)_{[\vec{b}]}$ est la concaténation de x_i's pour $b_i = 1$. Par exemple: $(1001)_{[1010]} = 10$.

La prochaine définition exprime ce que nous entendons par un protocole d'identification sécuritaire. Supposons que $\phi_{(n)} \in_R \{0,1\}^n$ est le secret qu'$\mathcal{A}lice$ et $\mathcal{B}ob$ partagent. Par la suite, nous noterons par $\mathcal{B}ob^*$ (resp. $\mathcal{A}lice^*$) quelqu'un qui veut se substituer à $\mathcal{B}ob$ (resp. $\mathcal{A}lice$).

Définition 30 *Un secret $\phi \in \{\phi_{(n)}\}_{n>0}$ est* indiscernable *pour $\mathcal{P}^*$ si l'information de $\mathcal{P}^*$ à propos de ϕ peut être modélisée par un ensemble $\Phi = \{\Phi_{(n)} \subseteq \{0,1\}^n\}_{n>0}$ pour lequel il existe un $1 > \alpha > 0$ tel que pour n assez grand*

$$\frac{\#\Phi_{(n)}}{2^n} \geq 1 - 2^{-\alpha n} \quad \textit{et} \quad \mathrm{P}\left(\boldsymbol{\phi}_{(n)} \notin \Phi_{(n)}\right) < 2^{-\alpha n}$$

ainsi que pour chaque $\phi' \in \Phi_{(n)}$,

$$\mathrm{P}\left(\boldsymbol{\phi}_{(n)} = \phi' | \boldsymbol{\phi}_{(n)} \in \Phi_{(n)}\right) = \frac{1}{\#\Phi_{(n)}}.$$

L'information de Shannon donnée par $\Phi_{(n)}$ à propos de $\phi_{(n)}$ est telle que

$$\begin{aligned}
\mathbf{I}(\boldsymbol{\phi}_{(n)}|\Phi_{(n)}) &= \mathbf{H}(\boldsymbol{\phi}_{(n)}) - \mathbf{H}(\boldsymbol{\phi}_{(n)}|\Phi_{(n)}) \\
&= n - \mathbf{H}(\boldsymbol{\phi}_{(n)}|\Phi_{(n)}) \\
&= n + \sum_{\phi \in \Phi_{(n)}} \mathrm{P}\left(\boldsymbol{\phi}_{(n)} = \phi | \boldsymbol{\phi}(n) \in \Phi_{(n)}\right) \lg \mathrm{P}\left(\boldsymbol{\phi}_{(n)} = \phi | \boldsymbol{\phi}_{(n)} \in \Phi_{(n)}\right) \\
&\leq n - \lg\left((1 - 2^{-\alpha n})2^n\right) \\
&= -\lg\left(1 - 2^{-\alpha n}\right) \\
&\leq 2^{-\alpha n} \text{ pour } n \text{ suffisamment grand.}
\end{aligned}$$

Sans perdre de généralités, nous utiliserons ϕ pour noter une instance de $\phi_{(n)}$ lorsque le contexte l'autorise.

Il nous faut maintenant déterminer une définition de sécurité qui puisse permettre la caractérisation des protocoles d'identification qui soient sécuritaires. Un protocole d'identification *occulte* l'information secrète ϕ, si lorsque ϕ est indiscernable pour $\mathcal{P}^*$

avant la première exécution alors ϕ demeure indiscernable après $poly(n)$ exécutions. Cette condition doit être réalisée sauf avec probabilité négligeable. Un protocole qui aurait cette propriété devra être attaqué plus de $poly(n)$ fois, pour tout polynôme $poly(n)$, pour que le participant malhonnête puisse en retirer quoi que ce soit.

Définition 31 *Soit $\mathcal{P}^*$ un participant malhonnête pour qui ϕ est indiscernable. Pour tout polynôme $poly(n)$, pour un facteur de sécurité n et pour $\alpha > 0$, un protocole d'identification* **occulte** *l'information secrète ϕ, si un participant $\mathcal{P}^*$ qui participe $poly(n)$ fois au protocole a une probabilité plus grande que $1 - 2^{-\alpha n}$ qu'à la fin ϕ lui soit indiscernable.*

Le mot ϕ^* dénote le choix que fait $\mathcal{A}lice^*$ ou $\mathcal{B}ob^*$ pour exécuter le protocole étant donné que ϕ est indiscernable. La propriété suivante montre que si ϕ est indiscernable chacun de ses bits est statistiquement impossible à approximer.

Propriété 1 *Si $\phi \in \{0,1\}^n$ est indiscernable pour $\mathcal{P}^*$, il existe $\beta > 0$ tel que pour tout $b \in \{0,1\}$ et pour chaque position i indépendamment, $|\mathrm{P}\left(\boldsymbol{\phi}_i = b\right) - \frac{1}{2}| \leq 2^{-\beta n}$.*

Preuve. Soit Φ l'information sur ϕ pour $\mathcal{P}^*$ telle que ϕ lui est indiscernable. Supposons pour une contradiction que

$$(\exists \beta > 0)(\overset{\infty}{\exists}\, n)(\exists i)(\exists b)[\mathrm{P}\left(\boldsymbol{\phi}_i = b|\Phi\right) > \frac{1+2^{-\beta n}}{2}]$$

et ϕ est indiscernable pour $\mathcal{P}^*$. Dans ce cas, pour chaque $\beta > 0$,

$$\begin{aligned}
\mathbf{I}(\boldsymbol{\phi}|\Phi) \geq \mathbf{I}(\boldsymbol{\phi}_i|\Phi) &> 1 - \mathbf{H}(\frac{1+2^{-\beta n}}{2}) \\
&\geq \frac{1}{2}\lg\left(1+2^{-\beta n}\right) \\
&\geq 2^{-\beta n - k}
\end{aligned}$$

pour k une constante. On en conclut que ϕ n'est pas indiscernable pour $\mathcal{P}^*$, contradiction.

■

La prochaine propriété nous montre que la composition de $poly(n)$ exécutions d'un protocole qui occulte ϕ doit occulter ϕ également.

Propriété 2 *Soit $\Phi_1, \Phi_2, \ldots, \Phi_{poly(n)}$ des ensembles pour lesquels ϕ est indiscernable. Le secret ϕ est aussi indiscernable étant donné:*

$$\Phi = \bigcap_{j=1}^{poly(n)} \Phi_j.$$

Preuve. Soit $\Phi = \cap_{j=1}^{poly(n)} \Phi_j$ et soit $\alpha = \min\{\alpha_j | j \in \{1, \ldots, poly(n)\}\}$ tel que $\frac{\#\Phi_j}{2^n} \geq 1 - 2^{-\alpha_j n}$. Soit

$$n_0 = \max_{j \in \{1, \ldots, poly(n)\}} \{n_j | \; n_j \text{ est le seuil de la définition 30 pour } \Phi_j\}.$$

Nous avons que pour $n \geq n_0$,

$$\begin{aligned}
\#\Phi &\geq 2^n - \sum_{j=1}^{poly(n)} \{0,1\}^n \setminus \Phi_j \\
&\geq 2^n - 2^n \sum_j 2^{-\alpha n} \\
&= 2^n \left(1 - \sum_j 2^{-\alpha n}\right) \\
&= 2^n \left(1 - poly(n) 2^{-\alpha n}\right) \\
&\geq 2^n (1 - 2^{-\alpha' n}) \text{ pour tout } \alpha' < \alpha.
\end{aligned}$$

Ce qui montre que la première condition est vérifiée. De plus, par la construction de Φ et puisque pour tout j, ϕ est indiscernable par Φ_j, nous avons que

$$\mathrm{P}\left(\boldsymbol{\phi} = \phi | \boldsymbol{\phi} \in \Phi\right) = \frac{1}{\#\Phi}.$$

Finalement il est facile de vérifier que

$$\begin{aligned}
\mathrm{P}\left(\boldsymbol{\phi} \notin \Phi\right) &= 1 - \mathrm{P}\left(\boldsymbol{\phi} \in \Phi\right) \\
&= 1 - \prod_{j=1}^{poly(n)-1} \mathrm{P}\left(\boldsymbol{\phi} \in \Phi_j | \boldsymbol{\phi} \in \cap_{h=1}^{j-1} \Phi_h\right) \\
&\leq 1 - (1 - 2^{-\alpha n})^{poly(n)} \\
&\leq 2^{-\alpha'' n}.
\end{aligned}$$

ce qui termine la preuve que ϕ est indiscernable pour $\mathcal{P}^*$ dont l'information peut être modélisée par Φ.

■

Si un protocole d'identification occulte ϕ à $\mathcal{P}^*$ à chaque exécution, l'information divulguée par l'ensemble de ces exécutions peut être modélisée par un ensemble Φ pour lequel ϕ est indiscernable. Ceci étant vrai sauf avec probabilité négligeable. Il en résulte que l'ensemble des $poly(n)$ exécutions occultent ϕ.

3.3.2 Transmission quantique idéalisée

Jusqu'à la section 3.5, nous considérons une idéalisation de la transmission quantique. Pour le moment, seul le codage BB84 peut servir à préparer ou à mesurer un système quantique. Dans ce modèle, il n'y a que quatre façons de transmettre un photon et que deux façons de le mesurer; même pour des participants au protocole qui seraient malicieux. L'angle de polarisation d'un photon prend nécessairement l'une des valeurs $|\rightarrow\rangle, |\nearrow\rangle, |\uparrow\rangle$ ou $|\nwarrow\rangle$. À l'autre bout, le reçeveur $\mathcal{B}ob$ choisit de mesurer π_b dans la base rectilinéaire $+$ ou dans le base diagonale $\times$.

3.4 Un protocole simple

Supposons que $\mathcal{A}lice$ et $\mathcal{B}ob$ veulent vérifier sans le révéler le secret ϕ qu'ils partagent. Pour ce faire ils disposent d'un canal quantique et d'un canal public.

Soit ρ_+ et $\rho_\times$ les matrices de densité qui décrivent les systèmes associés à la transmission dans la base rectilinéaire et diagonale respectivement (voir le chapitre 1 section 1.8.2).

Puisque $\rho_+ = \rho_\times$ aucune mesure ne peut distinguer entre l'utilisation par l'envoyeur de la base $+$ et l'utilisation de la base $\times$. Cette remarque suggère d'utiliser le secret pour déterminer les bases lors de la transmission quantique. Cette propriété n'est évidemment valide que si chaque bit transmis est choisi aléatoirement. Le problème est que, si $\mathcal{A}lice$ s'identifie à $\mathcal{B}ob$ en transmettant une chaîne aléatoire, $\mathcal{B}ob$ n'a aucune façon de vérifier l'authenticité de son interlocuteur.

Pour permettre à $\mathcal{B}ob$ de reconnaître $\mathcal{A}lice$, la chaîne transmise par celle-ci pourrait être choisie aléatoirement dans un code correcteur d'erreurs. Si C_n est un (n,k)–code binaire, la proportion des chaînes valides est par définition égale à 2^{k-n}. Ainsi,

$\mathcal{A}lice$ choisit un mot de code aléatoire $c \in_R C_n$ et transmet par le canal quantique le système $|c\rangle_\phi$. $\mathcal{B}ob$ recouvre $\widehat{c}$ en mesurant $|c\rangle$ dans les bases ϕ. En autant que le canal quantique ne soit pas sujet au bruit, $\mathcal{B}ob$ obtient $\widehat{c} = c$. Pour H la matrice de parité de C_n, $\mathcal{B}ob$ peut maintenant s'assurer que $c \in C_n$ en vérifiant que $Hc = \mathbf{0}$. En réalité cependant, le canal quantique est un canal bruyant modélisé par un canal symétrique binaire avec paramètre $p > 0$. $\mathcal{B}ob$ même en connaîssant exactement ϕ, obtiendra (sauf avec probabilité négligeable) une chaîne $\widehat{c}$ telle que $\Delta(\widehat{c}, c) \leq (p+\epsilon)n$ pour tout $\epsilon > 0$ en autant que n soit suffisamment grand. Si le code C_n est décodable et de distance minimale d_n assez grande , $\mathcal{B}ob$ pourra décoder $\widehat{c}$ et recouvrer c pour vérifier si $\Delta(\widehat{c}, c) \leq (p+\epsilon)n$. Soit $c' \in C_n$ le mot de code décodé à partir de $\widehat{c}$. Nous verrons par la suite que si C_n est suffisamment épars, $\mathcal{A}lice$ doit connaître ϕ pour qu'avec bonne probabilité $\Delta(\widehat{c}, c') \leq (p+\epsilon)n$. $\mathcal{B}ob^*$, qui veut obtenir de l'information sur ϕ, doit l'obtenir à partir de la chaîne reçue $\widehat{c}$. Si le code est de dimension suffisante, $\mathcal{B}ob^*$, qui n'a pas d'information sur ϕ, pourrait ne pas en obtenir d'avantage suite à la réception de $\widehat{c}$. Le protocole 3.4 décrit cette idée d'une façon plus détaillée.

Les prochaines sections analysent la sécurité du protocole des points de vue d'$\mathcal{A}lice$ et de $\mathcal{B}ob$ étant donné une transmission quantique idéalisée.

3.4.1 $ident(\phi, \phi)$

Supposons qu'$\mathcal{A}lice$ et $\mathcal{B}ob$ partagent la même clé secrète $\phi \in \{+, \times\}^n$. Dans ces conditions, après la transmission d'un mot de code $c \in C_n$ $\mathcal{B}ob$ obtient un mot $\widehat{c} \in \{0,1\}^n$ tel qu'indépendamment pour chaque $i \in \{1, \ldots, n\}$,

$$\mathrm{P}\left(\mathbf{c}_i = \widehat{c}_i\right) = 1 - p.$$

Le nombre d'erreurs de transmission $poids(c \oplus \widehat{c})$ se comporte comme une distribution binômial avec paramètre p. Soit C_n un code correcteur de distance minimale $d_n \geq 2(p+\epsilon)n$ pour $0 < \epsilon \leq p(1-p)$. Par la loi des grands nombres de Bernstein, la probabilité que $\mathcal{B}ob$ refuse l'identité d'$\mathcal{A}lice$ est telle que

$$\mathrm{P}\left(poids(\mathbf{c} \oplus \widehat{c}) \geq (p+\epsilon)n\right) \leq \mathrm{P}\left(|poids(\mathbf{c} \oplus \widehat{c}) - pn| \geq \epsilon n\right) \leq 2e^{-n\epsilon^2}.$$

Protocole 3.4.1 ($ident(\phi)(\phi)$)

1: $\mathcal{A}lice$ and $\mathcal{B}ob$ s'entendent sur un (n, k_n, d_n)-code binaire C_n en spécifiant sa matrice génératrice G,

2: $\mathcal{A}lice$ pige un mot aléatoire $x \in_{\mathrm{R}} \{0,1\}^{k_n}$ et pose $c = xG$,

3: $\overset{n}{\underset{i=1}{\textbf{FAIRE}}}$

- $\mathcal{A}lice$ transmet à $\mathcal{B}ob$ le photon π_i dans l'état de polarisation $|c_i\rangle_{\phi_i}$ par le canal quantique,
- $\mathcal{B}ob$ mesure π_i dans la base ϕ_i,
- $\mathcal{B}ob$ pose $\widehat{c}_i = \begin{cases} 0 & \text{si } \pi_i \text{ est observé comme } |0\rangle_{\phi_i} \\ 1 & \text{si } \pi_i \text{ est observé comme } |1\rangle_{\phi_i}, \end{cases}$

4: $\mathcal{B}ob$ décode $\widehat{c}$ et obtient $c' \in C_n$

5: $\mathcal{B}ob$ accepte seulement si $\Delta(c', \widehat{c}) \leq (p + \epsilon)n$ pour $\epsilon > 0$.

FIG. 3.1 - *Protocole simple d'identification.*

La probabilité que $\mathcal{B}ob$ refuse refuse l'identité d'$\mathcal{A}lice$ honnête est donc négligeable. Si $\mathcal{A}lice$ et $\mathcal{B}ob$ partagent le même secret, le protocole se terminera par un succès sauf avec probabilité négligeable $2^{-\epsilon^2 n}$ en autant que la distance minimun $d \geq 2(p+\epsilon)n$.

3.4.2 *ident*(ϕ^*, ϕ) avec $\mathcal{A}lice^*$

Analysons le comportement du protocole *ident*(ϕ^*, ϕ) lorsqu'$\mathcal{A}lice^*$ tente de se substituer à la vraie $\mathcal{A}lice$. Nous déterminerons la distance minimale d_n du code C_n pour que la probabilité qu'$\mathcal{A}lice^*$ ne soit pas détectée soit négligeable. Pour la transmission quantique idéalisée, les comportements déviants d'$\mathcal{A}lice^*$ sont faciles à modéliser.

Sous cette hypothèse, $\mathcal{A}lice^*$ n'a de choix que pour $w \in \{0,1\}^n$ et $\phi^* \in \{+,\times\}^n$ et transmettre à $\mathcal{B}ob$ le système quantique $|w\rangle_{\phi^*}$. Supposons qu'au moment de monter l'attaque, ϕ est indicernable par $\mathcal{A}lice^*$, soit $\Phi \subseteq \{+,\times\}^n$ la modélisation de l'information sur ϕ. D'après la propriété 1, il existe $\beta > 0$ tel que pour chaque position $i \in \{1,\ldots,n\}$,

$$|\mathrm{P}\left(\boldsymbol{\phi}_i = \phi_i^* | \Phi\right) - \frac{1}{2}| \leq 2^{-\beta n}.$$

Dans ces conditions, $\mathcal{B}ob$ reçoit un mot $\widehat{w}$ tel que pour chaque position i où $\phi_i^* \neq \phi_i$ on a que $\mathrm{P}\left(\widehat{\mathbf{w}}_i \neq w_i | \boldsymbol{\phi}_i \neq \phi_i^*\right) = \frac{1}{2}$. Le lemme suivant montre qu'en choisissant un code C_n avec une *bonne* distance minimale, la probabilité que le mot de code $c_w \in C_n$ le plus près de w soit tel que $\Delta(w, c_w) \leq (p+\epsilon)n$ est négligeable. Dans ces conditions $\mathcal{B}ob$ détecte la tentative de substitution.

Lemme 3 *Soit C_n un (n,k,d)–code binaire avec $d \geq \frac{4n\mathbf{H}(p+\epsilon)}{1-\alpha}$ pour $\epsilon > 0$ et $1 > \alpha > 0$. Soit $\mathcal{A}lice^*$ pour qui ϕ est indiscernable. Peu importe la chaîne transmise $w \in \{0,1\}^n$ par $\mathcal{A}lice^*$, $\mathcal{B}ob$ obtient une chaîne $\widehat{w}$ telle que*

$$\mathrm{P}\left(\widehat{\mathbf{w}} \in S_{p+\epsilon}(\textit{Décode}(\widehat{w}))\right) \leq 2^{-\alpha' n}$$

pour $\alpha' > 0$.

Preuve. Soit $c_w = \text{Décode}(\widehat{w}) \in C_n$ un (n,k,d)–code. Chaque mot de code c_w est tel que pour tout ensemble $D \subseteq \{1,\ldots,n\}$ de $d' = \lfloor \frac{d}{2} \rfloor$ positions, toute chaîne

$w' \in X_D(c_w)$ où $X_D(c_w) = \{x \in \{0,1\}^n | (i \notin D) \Rightarrow (x_i = c_{wi})\}$ est telle que $c_w =$ Décode(w'). Soit $\Delta_D = \#\{i \in D | \phi_i^* \neq \phi_i\}$. En général,

$$\begin{aligned}
\mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w)\right) &= \mathrm{P}\left(\boldsymbol{\Delta}_D \geq \frac{d'(1-\alpha)}{2}\right) \mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w)) | \boldsymbol{\Delta}_D \geq \frac{d'(1-\alpha)}{2}\right) + \\
&\quad \mathrm{P}\left(\boldsymbol{\Delta}_D < \frac{d'(1-\alpha)}{2}\right) \mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w)) | \boldsymbol{\Delta}_D < \frac{d'(1-\alpha)}{2}\right) \\
&\leq \mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w) | \boldsymbol{\Delta}_D \geq \frac{d'(1-\alpha)}{2}\right) + \mathrm{P}\left(\boldsymbol{\Delta}_D < \frac{d'(1-\alpha)}{2}\right).
\end{aligned}$$

Par la propriété 1 et puisque ϕ est indiscernable pour $\mathcal{A}lice$, chaque $i \in D$ est tel que $\mathrm{P}\left(\boldsymbol{\phi}_i \neq \phi_i^*\right) \geq \frac{1}{2} - 2^{-\beta n}$ pour $\beta > 0$. On a donc que

$$\begin{aligned}
\mathrm{P}\left(\boldsymbol{\Delta}_D < \frac{d'(1-\alpha)}{2}\right) &\leq \sum_{j=0}^{\frac{d'(1-\alpha)}{2}} \binom{d'}{j} (\frac{1}{2} + 2^{-\beta n})^{d'} \\
&\leq (\frac{1}{2} + 2^{-\beta n})^{d'} 2^{d' \mathbf{H}(\frac{1-\alpha}{2})} \\
&\leq 2^{-d' + d'\mathbf{H}(\frac{1-\alpha}{2}) + O(1)} \\
&\leq 2^{-d'(1-\mathbf{H}(\frac{1-\alpha}{2})) + O(1)}.
\end{aligned}$$

Les bits reçus aux positions $i \in D$ avec $\phi_i^* \neq \phi_i$ sont aléatoires. Ainsi nous avons que

$$\begin{aligned}
\mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w) | \boldsymbol{\Delta}_D \geq \frac{d'(1-\alpha)}{2}\right) &\leq \sum_{j=0}^{(p+\epsilon)n} \binom{\Delta_D}{j} 2^{-\Delta_D} \\
&\leq \sum_{j=0}^{(p+\epsilon)n} \binom{n}{j} 2^{-\Delta_D} \\
&\leq 2^{-\Delta_D + n\mathbf{H}(p+\epsilon)} \\
&\leq 2^{\frac{-d'(1-\alpha)}{2} + n\mathbf{H}(p+\epsilon)}
\end{aligned}$$

En conclusion,

$$\mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w)\right) \leq 2^{-d'(1-\mathbf{H}(\frac{1-\alpha}{2})) + O(1)} + 2^{\frac{-d'(1-\alpha)}{2} + n\mathbf{H}(p+\epsilon)}.$$

Pour $\alpha > 0$ et $d' = \lfloor \frac{d}{2} \rfloor \geq \frac{2n\mathbf{H}(p+\epsilon)}{1-\alpha}$ nous avons bien que

$$\mathrm{P}\left(\hat{\mathbf{w}} \in S_{p+\epsilon}(c_w)\right) \leq 2^{-\alpha' n}$$

pour un $\alpha' > 0$ pourvu que n soit suffisamment grand.

■

3.4.3 $ident(\phi, \phi^*)$ avec $\mathcal{B}ob^*$

Analysons maintenant ce que $\mathcal{B}ob^*$ peut tirer comme information sur ϕ après l'exécution du protocole avec $\mathcal{A}lice$. De nouvelles conditions sur le code C_n seront mises en évidence. Comme dans les sections précédentes, nous considérons une transmission quantique idéalisée en plus du fait que ϕ est indiscernable pour $\mathcal{B}ob^*$.

Soit $c \in_R C_n$ le mot de code transmis par $\mathcal{A}lice$ dans la séquence de bases ϕ. $\mathcal{B}ob^*$ choisit une séquence $\phi^* \in \{+, \times\}^n$ avec laquelle il mesure c pour obtenir $\widehat{c}$. Par la propriété 1, approximativement la moitié des positions $i \in \{1, \ldots, n\}$ seront telles que $\phi_i^* = \phi_i$. À ces positions i, $\mathcal{B}ob^*$ reçoit les bits $\widehat{c}_i = c_i$. Les positions $i \in \{1, \ldots, n\}$ pour lesquelles $\phi_i^* \neq \phi_i$ sont telles que les $\widehat{c}_i$ sont non-corrélés avec les bits correspondant du mot de code c. Pour que le protocole protège le secret ϕ d'$\mathcal{A}lice$ contre $\mathcal{B}ob^*$, il faut que le code soit choisi de façon à ce que n'importe quelle moitié des bits des mots de code de C_n soit aléatoire. Si tel était le cas, les bit de c que $\mathcal{B}ob^*$ reçoit correctement sont aléatoires et ceux aux autres positions le seront également. Dans ces conditions la chaîne $\widehat{c}$ reçue par $\mathcal{B}ob^*$ est complètement aléatoire. Puisque c'est ce qui arrive pour la plupart des séquences de bases ϕ^*, $\mathcal{B}ob^*$ ne pourra déterminer d'information supplémentaire sur ϕ suite à l'exécution du protocole.

Un concept similaire a été étudié par [12],[60] (fonctions (n, j, k)) et indépendamment par [32] (fonctions t–résilientes) dans un contexte différent. La prochaine définition provient de [12].

Définition 32 ([12]) *Pour tout n, j, k tels que $n \geq j + k$, $j > 0$ et $k > 0$, une fonction $f : GF(Q)^n \rightarrow GF(Q)^j$ est (n, j, k) si, pour toute façon de fixer k symboles d'entrée, chacune des Q^j sorties peut être produite de Q^{n-j-k} façons différentes en faisant varier les $n - k$ symboles qui restent.*

Si chacun des symboles de $f(x)$ est obtenu par le calcul d'une somme dans $GF(Q)$ d'un sous-ensemble des symboles de x, nous dirons que $f(x)$ est xor-(n, j, k). Dans [12] et [32] les fonctions étudiées le sont pour le cas particulier du corps de Galois à deux éléments (i.e. $Q = 2$). Nous pouvons reformuler les définitions et théorèmes pour un corps de Galois arbitraire à Q éléments. Le théorème suivant [12], donne une façon de construire des fonctions xor-(n, j, k).

Théorème 10 ([12]) *Pour un ensemble de valeurs (n, j, k), il existe une fonction xor-(n, j, k)de $GF(Q)^n$ dans $GF(Q)^j$ si et seulement si il existe un $(n, j, k+1)$–code linéaire C_n sur $GF(Q)$.*

Si G est la matrice génératrice d'un $(n, j, k+1)$–code linéaire, alors la fonction $f(x) = Gx^T$ (où x^T est x transposé) est xor-(n, j, k). Dans la notation de [32], dire que $f(x)$ est (n, j, k) est équivalent à dire que $f^{-1}(y) = \{x | f(x) = y\}$ est un ensemble avec une projection uniforme sur n'importe quelles k positions.

Définition 33 ([32]) *Un ensemble $S \subseteq GF(Q)^n$ a une projection uniforme sur n'importe quelles k composantes si pour chaque $\omega \in \{0,1\}^n$ de poids k et toute valeur $a \in GF(Q)^k$, l'ensemble $S_{\omega,a} = \{x \in S : (x)_{[\omega]} = a\}$ est tel que $\#S_{\omega,a} = \frac{\#S}{Q^k}$.*

Le prochain théorème indique pourquoi un code C_n pourvu d'un dual avec *bonne* distance minimale permet au protocole $ident(\phi, \phi^*)$ d'être sécuritaire du point de vue d'$\mathcal{A}lice$.

Théorème 11 *Soit C_n un code linéaire tel que le dual $C_n^\perp$ de C_n a une distance minimale d'_n avec $\frac{d'_n}{n} \geq \zeta > \frac{1}{2}$. Dans ces conditions et étant donné une transmission quantique idéalisée, le protocole $ident(\phi, \phi^*)$ occulte ϕ à $\mathcal{B}ob^*$ excepté avec probabilité négligeable.*

Preuve. Par la propriété 1, excepté avec probabilité négligeable $2^{-\beta n}$ nous avons que $\Delta(\phi, \phi^*) \geq (1-\zeta)n$. En conséquence le nombre de bits de c que $\mathcal{B}ob^*$ reçoit correctement est moindre que ζn. Soit H la matrice génératrice du code $C_n^\perp$ de distance minimale $d' > \zeta n$. Par le théorème 10, la fonction Hx^T est $(n, k, \lfloor \zeta n \rfloor + 1)$. L'ensemble $H(\mathbf{0}) = \{x \in \{0,1\}^n | Hx^T = \mathbf{0}\}$ a une projection uniforme sur n'importe quelles ζn composantes et de plus $H(\mathbf{0}) = C_n$. Nous avons donc que tout ensemble de ζn positions d'un mot de code c est uniforme lorsque $c \in_R C_n$. Puisque les $(1-\zeta)n$ bits aux autres positions sont non-corrélés avec les bits de c, la chaîne $\widehat{c}$ est uniformément distribuée dans $\{0,1\}^n$. Soit Φ_0 la modélisation de l'information sur ϕ avant l'exécution courante. L'ensemble $\Phi_1 = \{\phi | \Delta(\phi^*, \phi) \geq (1-\zeta)n\}$ modélise l'information divulguée par le protocole à l'exécution courante. Remarquons que pour chaque $\phi \in \Phi_1$ on a que

$$\mathrm{P}\left(\boldsymbol{\phi} = \phi | \boldsymbol{\phi} \in \Phi_1 \wedge \hat{\boldsymbol{c}} = \hat{c}\right) = \frac{1}{\#\Phi_1}$$

et

$$\mathrm{P}\left(\boldsymbol{\phi} \notin \Phi_1\right) \leq \frac{\sum_{j=0}^{(1-\zeta)n} \binom{n}{j}}{2^n} \leq 2^{-n(1-\mathbf{H}(1-\zeta))}.$$

On en conclut que ϕ est indiscernable par Φ_1. Par la propriété 2, ϕ est aussi indiscernable par l'ensemble $\Phi = \Phi_0 \cap \Phi_1$ qui modélise l'information sur ϕ que $\mathcal{B}ob^*$ obtient après l'exécution courante étant donné Φ_0. D'une façon plus générale, si Φ_i modélise l'information sur ϕ que la $i^{\text{ième}}$ exécution divulgue et si ϕ est indiscernable par Φ_0, alors excepté avec probabilité négligeable l'ensemble

$$\Phi = \bigcap_{i=0}^{poly(n)} \Phi_i$$

modélise l'information sur ϕ que $poly(n)$ exécutions du protocole divulguent. Le secret ϕ étant indiscernable par Φ, nous obtenons que le protocole $ident(\phi, \phi^*)$ occulte ϕ du point de vue de $\mathcal{B}ob^*$.

$\blacksquare$

3.4.4 Conditions sur le choix du code

Aux sections 3.4.1,3.4.2 et 3.4.3 des contraintes sur le code C_n garantissant la sécurité du protocole $ident(\cdot, \cdot)$ ont été exhibées. Dans cette section nous en faisons la revue.

Puisque n est un facteur de sécurité qui peut être fixé arbitrairement pour refléter les besoins en sécurité d'une application particulière, nous nous intéressons à l'existence de familles de codes $\mathcal{C} = \{C_n\}_{n>0}$ indexées par le facteur de sécurité n. Les conditions sur la famille $\mathcal{C}$ qui sont jusqu'à maintenant répertoriées sont les suivantes:

1. Puisque la transmission s'exécute via le canal quantique, nous voulons que $\mathcal{C}$ soit une famille de codes binaires. De plus, pour que le théorème 11 s'applique, $\mathcal{C}$ doit être une famille de codes linéaires.

2. À l'étape 4 du protocole, $\mathcal{B}ob$ décode le mot reçu $\widehat{c}$. Nous voulons donc que $\mathcal{C}$ soit une famille de codes efficacement décodables.

3. Pour satisfaire le théorème 3, chacun des codes $C_n \in \mathcal{C}$ doit avoir une distance minimale d_n telle que $d_n \geq \frac{4n\mathbf{H}(p+\epsilon)}{1-\alpha}$.

4. Le théorème 11 implique que le dual $C_n^\perp$ de C_n a une distance minimale d'_n telle que $\frac{d'_n}{n} > \frac{1}{2}$.

L'ensemble de ces conditions est une bien mauvaise nouvelle. La moins mauvaise provient de la conjonction des contraintes 1 et 4. Celles-ci exigent que $\mathcal{C}^\perp = \{C_n^\perp\}_{n>0}$ soit une famille de codes binaires avec distance minimale $d_n > \frac{1}{2}$. Cette restriction est trop forte puisque selon la borne de Plotkin [55], un code avec distance minimale plus grande que $\frac{1}{2}$ ne peut pas contenir plus d'un nombre constant de mots. Ceci implique que le primal ne peut avoir une distance minimale plus grande qu'une constante, ce qui viole la condition 3. On peut relaxer la condition 4 pour éliminer cette contradiction en utilisant la base circulaire (voir section 1.7). Les vecteurs $|\hookrightarrow\rangle$ et $|\leftrightarrow\rangle$ sont orthogonaux et ont la propriété que $\mathrm{P}\left(\widehat{\mathbf{c}}_i = c_i | \boldsymbol{\phi}_i \neq \phi_i^*\right) = \frac{1}{2}$. Dans ce cas, le bit reçu $\widehat{c}_i$ est non-corrélé avec le bit envoyé c_i. Avec cette modification, les $\frac{2}{3}$ des bits reçus seront non-corrélés avec les bits envoyés. Dans ces conditions le théorème 11 est vérifié si la distance minimale d'_n du code dual $C_n^\perp$ est telle que $d'_n > \frac{n}{3}$. L'avantage est évident puisque des codes qui possèdent les propriétés 1,3 et 4 existent. Les codes linéaires aléatoires sont de ceux-là. D'après la borne de Varshamov-Gilbert, un $(n, 0.91n)$–code binaire aléatoire est, sauf avec probabilité négligeable, tel que sa distance minimale $d_n \geq 0.01n$. Puisque son dual est un $(n, 0.085n)$–code aléatoire, sauf avec probabilité négligeable sa distance minimale est $d'_n > \frac{n}{3}$.

Malheureusement, aucune famille connue de codes correcteurs ne respecte les quatre conditions simultanément. La familles des codes aléatoires observent les conditions 1,3 et 4 mais n'ont pas d'algorithme efficace connu pour le décodage. En fait, n'importe quel ensemble de trois conditions parmi quatre peuvent être respectées par une famille de codes. Par exemple, les codes de Reed-Solomon ont les propriétés 2,3 et 4 tandis que les codes concaténés [39] respectent les conditions 1,2 et 3. Une famille importante de codes binaires linéaires décodables sont les codes par blocs. Les mots de codes d'un code par blocs sont formés de blocs de longueur constante m formant un code correcteur interne de longueur m. À l'ensemble de ces petits codes, on ajoute un code externe qui corrige les blocs qui ont été mal décodés par le code interne. Ce type de code est inutile dans notre scénario car la distance minimale de leur dual n'est pas supérieure à m. On peut le vérifier facilement car tout code dual $C_n^{\perp}$ linéaire avec distance minimale d'_n est tel que la vue de d'_n bits de $c \in_R C_n$ donne aucune information sur les $n - d'_n$ autres bits de c. Or, un code par blocs de longueur m est tel qu'il suffit de moins de m bits pour déterminer la valeur d'un bloc.

3.4.5 Attaques passives

Même si nous disposions d'une famille $\mathcal{C}$ avec les bonnes propriétés, il y a un type de fraude qui puisse être faite contre le protocole $ident(\phi, \phi^*)$ (même étant donné une transmission quantique idéalisée). Cette fraude est d'autant plus gênante qu'elle réalise exactement ce que nous voulions éviter au départ même si $\mathcal{B}ob^*$ n'obtient pas d'information sur ϕ.

Supposons que $\mathcal{A}lice$ s'identifie à $\mathcal{B}ob^*$. Celui-ci n'a qu'à reçevoir les photons qu'$\mathcal{A}lice$ lui envoie sans les mesurer. Il les conserve sans changer leur état. Une fois la transmission quantique terminée, $\mathcal{B}ob^*$ n'a qu'à accepter aveuglément l'authenticité d'$\mathcal{A}lice$. Une fois celle-ci partie, il peut s'identifier comme étant $\mathcal{A}lice$ en transmettant ces mêmes photons. Il ne faut pas conclure que le théorème 11 est faux parce que $\mathcal{B}ob^*$ peut mener avec succès une attaque contre le protocole. Ce théorème dit seulement que $\mathcal{B}ob^*$ n'a pas d'information sur ϕ après l'interaction avec $\mathcal{A}lice$. Cependant, il est possible de frauder le système sans même connaître ϕ! Puisque le protocole présenté se base sur les propriétés d'un système physique, rien n'empêche d'entreposer ce système pour le réutiliser par la suite. Le problème peut être résolu en s'assurant qu'$\mathcal{A}lice$ sait ce qu'elle a envoyé à $\mathcal{B}ob$. Pour y parvenir, $\mathcal{B}ob$ demande à $\mathcal{A}lice$ de lui donner la parité d'un sous-ensemble aléatoire des bits du mot de code transmis. $\mathcal{B}ob$ vérifie ensuite qu'$\mathcal{A}lice$ dit vrai. Si $\mathcal{A}lice$ ne connaît pas une fraction non négligeable des bits du mot de code, la probabilité qu'elle réponde correctement est essentiellement $\frac{1}{2}$. Pour augmenter sa confiance, $\mathcal{B}ob$ n'a qu'à répéter l'expérience λn fois juste avant l'étape 5 du protocole 3.4. Entre les étapes 4 et 5, ils exécutent le sous-protocole suivant:

Protocole 3.4.2 (Vérif$(c)(c')$ **)**

1: FAIRE $\overset{\lambda n}{\underset{l=1}{}}$

- $\mathcal{B}ob$ détermine aléatoirement un ensemble de positions $X_l \subseteq \{1, \ldots, n\}$ et l'annonce à $\mathcal{A}lice$.
- $\mathcal{A}lice$ annonce
$$p_l = \bigoplus_{i \in X_l} c_i$$
- Si
$$p_l \neq \bigoplus_{i \in X_l} c'_i$$
alors $\mathcal{B}ob$ refuse l'identité d'$\mathcal{A}lice$.

Soit $\widehat{C} = \{c \uplus p_1, p_2, \ldots, p_{\lambda n} | c \in C_n\}$ le nouveau code obtenu à partir de C_n et $\{X_l\}_{l=1}^{\lambda n}$. Supposons que $\widehat{C}$ est tel que la distance minimale $\widehat{d}_n^\perp$ du dual répond à $\widehat{d}_n^\perp \geq (\frac{1}{2} + \lambda + \epsilon)n$ avec $\lambda, \epsilon > 0$. Le nombre P de positions que $\mathcal{B}ob^*$ apprend à propos de $v = c_1, c_2, \ldots, c_n, p_1, \ldots, p_{\lambda n} \in_R \widehat{C}$ est, sauf avec probabilité négligeable, tel que $P \leq \widehat{d}_n^\perp$. Dans ce cas le théorème 11 s'applique et $\mathcal{B}ob^*$ ne peut presque rien apprendre sur ϕ.

Il serait intéressant de pouvoir caractériser en général la distance minimale du code $\widehat{C}^\perp$ étant donné celle pour $C_n^\perp$. Nous ne le ferons pas ici, la solution finale que nous présentons par la suite, n'est pas sujètte à ce type d'attaque.

3.4.6 La sécurité en générale

En plus du problème que pose la recherche de familles de codes qui respectent les quatre conditions de la section 3.4.4, la modélisation idéalisée de la transmission quantique en pose de nouveaux. Les mesures réalisées par $\mathcal{B}ob^*$ sur le système $\Psi_A = |c\rangle_\phi$ peuvent être beaucoup plus complexes à modéliser que celles considérées jusqu'à maintenant. Il est facile pour $\mathcal{B}ob^*$ de mesurer Ψ_A pour rendre le théorème 11 inapplicable. $\mathcal{B}ob^*$ pourrait mesurer le photon π_i selon n'importe quelle base orthonormée, par exemple la base de Breidbart $\mathbf{b} = \{\mathbf{b_1}, \mathbf{b_1^\perp}\}$ avec $\mathbf{b_1} = (\cos 22°\frac{1}{2}, \sin 22°\frac{1}{2})$. Remarquons qu'avec une telle mesure

$$\mathrm{P}\left(\mathbf{c}_i = \widehat{c}_i | \boldsymbol{\phi}_i^* = \mathbf{b} \wedge \boldsymbol{\phi}_i = \phi_i\right) = \cos^2\left(22°\frac{1}{2}\right) \approx 0.85$$

tandis que pour tout $c \in \{0,1\}$,

$$\mathrm{P}\left(\boldsymbol{\phi}_i = + | \widehat{c}_i \wedge c_i \wedge \phi_i^* = \mathbf{b}\right) = \frac{1}{2}.$$

Il s'agit de la mesure de Von Neumann qui maximise la probabilité d'obtenir le bit c_i. Cependant, l'utlisation de la base $\mathbf{b}$ est la pire des attaques que $\mathcal{B}ob^*$ puisse monter contre $ident(\phi, \phi^*)$. Même si après la transmission $\mathcal{A}lice$ lui annonçait le bit envoyé c_i, $\mathcal{B}ob^*$ n'aurait aucune information sur la base de transmission ϕ_i. Néanmoins, si $\mathcal{B}ob^*$ choisissait ses bases de lecture entres $\mathbf{b}$ et $+$ ou entre $\mathbf{b}$ et $\times$, tout les bits reçus seraient connus avec probabilité plus grande que $\frac{1}{2}$ tout en donnant un biais sur la base d'émission lorsque le bit envoyé est connu. Dans ce cas le théorème 11 ne peut être appliqué parce qu'il suppose que $\mathrm{P}\left(\mathbf{c}_i = \widehat{c}_i | \boldsymbol{\phi}_i \neq \phi_i^*\right) = \frac{1}{2}$.

Les mesures que $\mathcal{B}ob^*$ peut effectuer ne se limitent pas aux mesures de Von Neumann. Des mesures plus subtils qui opèrent sur plusieurs photons à la fois (mesures cohérentes) pourraient aussi fournir de l'information sur le secret ϕ. La possibilité de mesurer seulement une partie d'un photon (mesures incomplètes) peut aussi donner lieu à d'autres attaques. La variété des comportements que peuvent adopter les participants malhonnêtes au protocole, rend son analyse ardue. En considérant une transmission quantique idéalisée, nous avons fait reposer la sécurité du protocole 3.4 sur une primitive cryptographique, telle que:

1. Avec probabilité moindre que $\frac{1}{2}$, $\mathcal{B}ob^*$ obtient le bon bit,

2. $\mathcal{B}ob^*$ obtient un bit non-corrélé avec le bit envoyé avec probabilité plus grande que $\frac{1}{2}$, .

Ces propriétés de la transmission quantique idéalisée ne sont pas sans rappeler celles de la transmission inconsciente. Il est naturel d'utiliser la tansmission inconsciente pour simuler une transmission quantique idéalisée et ainsi obtenir une réalisation sécuritaire du protocole 3.4. La sécurité obtenue est relative à celle de la transmission inconsciente. À la lumière du chapitre 2 et du résultat de [71], le protocole quantique de transmission inconsciente de [13] est sécuritaire contre toutes les mesures autorisées par la mécanique quantique étant donné une mise en gage parfaite. il s'agit d'un support de transmission sur lequel une modification mineure au protocole 3.4 admet une réalisation sécuritaire. À la prochaine section, nous montrerons comment utiliser la transmission inconsciente pour que des familles de codes, qui répondent aux exigeances des théorèmes 3 et 11, puissent être trouvées. Par la suite, nous montrerons comment modifier le protocole BBCS pour améliorer la complexité de communication du protocole d'identification résultant.

3.5 Le protocole final

Comme nous l'avons vu à la section précédente, aucune famille connue de codes répond aux quatres conditions de la section 3.4.4. Par contre, des familles de codes avec les propriétés 2,3 et 4 existent et sont suffisantes pour appliquer les théorèmes 3 et 11. Une solution possible consiste donc à trouver une façon de transmettre des éléments d'un corps de plus de deux éléments à la fois. C'est exactement ce que la transmission inconsciente de chaînes de longueur r (dénoté par $\binom{2}{1}$–TI$_r$) permet de faire. Nous allons modifier le protocole 3.4 pour qu'il utilise la primitive $\binom{2}{1}$–TI$_2$ au lieu de la transmission quantique idéalisée. En boni, l'utilisation de cette primitive de transmission inconsciente permet d'éléminer les problèmes dus aux erreurs de transmission.

Après avoir présenté la modification au protocole $ident(\phi, \phi^*)$ utilisant la transmission inconsciente, nous montrerons qu'il respecte les critères de sécurité élaborés aux sections précédentes. Nous montrerons ensuite comment modifier le protocole de transmission inconsciente BBCS pour réduire la complexité de communication du protocole résultant. Par la suite, nous discuterons de l'opportunité de rendre le protocole utilisable en pratique.

Protocole 3.5.1 (*identTI*(ϕ, ϕ))

1: $\mathcal{A}lice$ pige $r, s \in_{\mathrm{R}} \{00, 01, 10, 11\}^n$.

2: $\mathbf{FAIRE}_{i=1}^{n}$ $\mathcal{A}lice$ exécute $\binom{2}{1}$–$\mathrm{TI}_2(r_i, s_i)(\phi_i)$ avec $\mathcal{B}ob$ qui reçoit v_i.

3: $\mathcal{B}ob$ pige $x, y \in_{\mathrm{R}} \{00, 01, 10, 11\}^n$ et l'annonce à $\mathcal{A}lice$.

4: $\mathcal{A}lice$ pige $c \in_{\mathrm{R}} C_n$, calcule et annonce $u \leftarrow c \oplus (r \oplus x, s \oplus y)_{[\phi]}$.

5: $\mathcal{B}ob$ accepte seulement si $u \oplus v \oplus (x, y)_{[\phi]} \in C_n$.

FIG. 3.2 - *Protocole final d'identification.*

3.5.1 Description du protocole

Comme pour le protocole 3.4, $\mathcal{A}lice$ prouve à $\mathcal{B}ob$ qu'elle connaît ϕ en transmettant un mot de code aléatoire c de telle façon que $\mathcal{B}ob$ puisse le retrouver et vérifier que $c \in C_n$. À l'opposé, si $\mathcal{B}ob^*$ ne connaît pas ϕ, il reçevra une chaîne aléatoire.

Soit G une matrice aléatoire $n \times k$ sur $GF(4)$. Ici nous représentons $GF(4)$ par l'ensemble des chaînes de deux bits avec le ou-exclusif bit à bit comme opération d'addition et le produit scalaire modulo 4 pour l'opération de multiplication. La matrice G peut être choisie une seule fois et rendue publique par les autorités. Soit C_n le (n, k_n, d_n)–code linéaire sur $GF(4)$ généré par G. Soit $C_n^{\perp}$ le $(n, n-k_n, d'_n)$–code dual de C_n. Le protocole 3.5.1 utilise la transmission inconsciente $\binom{2}{1}$–TI_2 (d'une chaîne de deux bits parmi deux) pour réaliser la même idée qu'au protocole 3.4.

Les étapes 3 et 4 du protocole *idenTI*(ϕ, ϕ) ont pour but de rendre aléatoire une des deux entrées à la primitive $\binom{2}{1}$–TI_2. Ceci est nécessaire car la transmission quantique idéalisée est telle que lorsque $\phi_i \neq \phi_i^*$, $\mathcal{B}ob$ reçoit un bit aléatoire en position i. Peu importe le choix d'$\mathcal{A}lice$ pour r_i et s_i, si $\mathcal{B}ob$ pige aléatoirement x_i et y_i alors $r_i \oplus x_i$ et $s_i \oplus y_i$ sont deux éléments de $GF(4)$ aléatoires et non-corrélés. Dans ces conditions les éléments de $GF(4)$ $c_i \oplus r_i \oplus x_i$ et $c_i \oplus s_i \oplus y_i$, calculés par $\mathcal{A}lice$ à l'étape 4, sont non-corrélés. $\mathcal{A}lice$ ne peut fixer ces deux valeurs du même coup, si l'une est fixée l'autre est aléatoire.

À la lumière de l'analyse de la section précédente, on peut démontrer la sécurité du protocole $identTI(\phi, \phi^*)$.

3.5.2 $identTI(\phi, \phi)$ avec des participants honnêtes

Si $\mathcal{A}lice$ et $\mathcal{B}ob$ partagent la séquence $\phi \in \{0,1\}^n$. Nous avons que:

$$u \oplus v \oplus (x, y)_{[\phi]} = c \oplus (r \oplus x, s \oplus y)_{[\phi]} \oplus (r, s)_{[\phi]} \oplus (x, y)_{[\phi]} = c.$$

La condition de l'étape 5 du protocole étant vérifiée, $\mathcal{B}ob$ accepte l'identité d'$\mathcal{A}lice$.

3.5.3 $identTI(\phi^*, \phi)$ contre $\mathcal{A}lice^*$

Supposons qu'$\mathcal{A}lice^*$, pour qui ϕ est indiscernable, tente de s'identifer comme la vraie $\mathcal{A}lice$. Cette section spécifie les paramètres du code C_n pour lesquels $\mathcal{B}ob$ refuse l'identité d'$\mathcal{A}lice^*$ sauf avec probabilité négligeable. La preuve du prochain protocole s'apparente à celle du théorème 3.

Théorème 12 *Si C_n est un (n, k_n, d_n)–code avec $d_n \in \Omega(n)$, $\mathcal{B}ob$ refusera l'identité d'$\mathcal{A}lice^*$, pour qui ϕ est indiscernable, sauf avec probabilité $2^{-\alpha n}$ pour $1 > \alpha > 0$.*

Preuve. Puisque par hypothèse $d_n \geq 2dn$ pour $d > 0$, si $c \in C_n$ est un mot de code alors $S_{dn}(c) = \{z \in \{00, 01, 10, 11\}^n | \Delta(c, z) \leq dn\}$ est tel que pour tout $z \in S_{dn}(c)$ on a que $c = \text{Décode}(z)$. Soit $\widehat{w}$ la chaîne reçue par $\mathcal{B}ob$ où $\widehat{w} = u \oplus (r \oplus x, s \oplus y)_{[\phi]}$, soit $D \subseteq \{1, \ldots, n\}$ un ensemble quelconque de dn positions et soit $\Delta_D = \#\{i | i \in D \wedge \phi_i^* \neq \phi_i\}$. En général pour $1 > \gamma > 0$,

$$\mathrm{P}\left(\widehat{\mathbf{w}} \in C_n\right) \leq \mathrm{P}\left(\boldsymbol{\Delta}_D \leq \frac{1}{2}(1-\gamma)dn\right) + \mathrm{P}\left(\widehat{\mathbf{w}} \in C_n | \boldsymbol{\Delta}_D \geq \frac{1}{2}(1-\gamma)dn\right).$$

En premier lieu, puisque ϕ est indiscernable pour $\mathcal{A}lice^*$ et par la propriété 1, on a que

$$\mathrm{P}\left(\boldsymbol{\Delta}_D \leq \frac{1}{2}(1-\gamma)dn\right) \leq 2^{-\alpha' dn}.$$

D'autre part, en supposant que les valeurs en $i \notin D$ de $\widehat{w}$ sont telles qu'il existe un mot de code avec ces valeurs en ces positions, il n'existe qu'une façon de compléter $\widehat{w}$ en $i \in D \cap \{i | \phi_i^* \neq \phi_i\}$ pour que $\widehat{w} \in C_n$. Parce que pour $i \in D \cap \{i | \phi_i^* \neq \phi_i\}$, $\mathcal{B}\mathrm{ob}^*$

reçoit un élément de $GF(4)$ aléatoire et uniformément distribué lorsqu'il choisit x_i et y_i aléatoirement, nous avons que

$$\mathrm{P}\left(\hat{\mathbf{w}} \in C_n | \boldsymbol{\Delta}_D \geq \frac{1}{2}(1-\gamma)dn\right) \leq \left(\frac{1}{4}\right)^{\frac{1}{2}(1-\gamma)dn} \leq 2^{-\frac{(1-\gamma)}{2}d_n}.$$

Si $d_n \in \Omega(n)$ on a bien que $\mathrm{P}\left(\hat{\mathbf{w}} \in C_n\right) \leq 2^{-\alpha n}$ pour $\alpha > 0$.

■

En plus de vouloir savoir si $\mathcal{A}lice^*$ sera détectée par $\mathcal{B}ob$, nous voulons déterminer l'information sur ϕ, qu'$\mathcal{A}lice^*$ peut retirer suite à son interaction avec $\mathcal{B}ob$. Le prochain théorème montre que dans les mêmes conditions qu'au théorème 12, si ϕ est indiscernable pour $\mathcal{A}lice^*$ avant l'exécution du protocole, alors sauf avec probabilité négligeable, ϕ lui sera toujours indiscernable après l'exécution.

Théorème 13 *Si $d_n \in \Omega(n)$ alors le protocole $identTI(\phi^*, \phi)$ occulte ϕ à $\mathcal{A}lice^*$.*

Preuve. Soit $d > 0$ tel que $d_n = 2dn$ et soit $\Phi(\phi^*) = \{\phi | \Delta(\phi^*, \phi) \geq dn(1-\gamma)/2\}$ avec $0 < \gamma < 1$. On a que

1. Par le théorème 12 nous obtenons facilement que $\#\Phi(\phi^*) \geq 2^n - 2^{nh(\frac{d(1-\gamma)}{2})}$ et $\mathrm{P}\left(\boldsymbol{\phi} \in \Phi(\phi^*)\right) \geq 1 - 2^{-\alpha' dn}$.

2. Il est clair que lorsque $\mathcal{A}$lice* apprend suite à l'exécution du protocol que $\phi \in \Phi(\phi^*)$, nous avons que

$$(\forall \phi \in \Phi(\phi^*))[\mathrm{P}\left(\boldsymbol{\phi} = \phi | \boldsymbol{\phi} \in \Phi(\phi^*)\right) \geq \frac{1}{\#\Phi(\phi^*)}].$$

En conséquence ϕ est indiscernable par $\Phi(\phi^*)$. Comme au début $\mathcal{A}lice^*$ ne pouvait discerner ϕ, par la proposition 2 après $poly(n)$ exécution ϕ demeure indiscernable. Le protocole occulte donc ϕ à $\mathcal{A}lice^*$.

■

Donc $\mathcal{A}lice^*$, qui exécute le protocole $identTI(\phi^*, \phi)$ $poly(n)$ fois, à une probabilité négligeable de réussir au moins une fois à se faire passer pour $\mathcal{A}lice$. De plus, après ces $poly(n)$ exécutions $\mathcal{A}lice^*$ ne peut toujours pas discerner ϕ.

3.5.4 $ident(\phi, \phi^*)$ contre $\mathcal{B}ob^*$

Analysons maintenant ce que $\mathcal{B}ob^*$ peut tirer de son interaction avec $\mathcal{A}lice$. À la lumière du théorème 11, la distance minimale du dual de C_n permet de caractériser la sécurité du protocole contre $\mathcal{B}ob^*$.

Théorème 14 *Soit $\mathcal{B}ob^*$ pour qui ϕ est indiscernable. Excepté avec probabilité négligeable en n, le protocole $identTI(\phi, \phi^*)$ occulte ϕ à $\mathcal{B}ob^*$ qui exécute le protocole $poly(n)$ fois si le dual $C_n^\perp$ de C_n est un $(n, n-k_n, d'_n)$–code linéaire avec $d'_n \geq (\frac{1}{2}+\gamma)n$ pour $0 < \gamma < \frac{1}{2}$.*

Preuve. Pour chaque position $i \in \mathcal{I} = \{i | \phi^*_i = \phi_i\}$ $\mathcal{B}ob^*$ obtiendra la valeur c_i du mot de code $c \in C_n$ envoyé par $\mathcal{A}lice$. Puisque ϕ est indiscernable par $\mathcal{B}ob^*$ au départ, nous avons pour $\gamma > 0$ que

$$\mathrm{P}\left(\#\boldsymbol{\mathcal{I}} \geq (\frac{1}{2} + \gamma)n\right) \leq 2^{-\alpha n} \text{pour } \alpha > 0.$$

Les positions $i \in \overline{\mathcal{I}}$ sont telles que $\widehat{c}_i = (x_i, y_i)_{[1-\phi_i]} \oplus u_i \oplus v_i$ sont non-corrélées avec c_i, en autant que r et s aient été choisis aléatoirement par $\mathcal{A}lice$. Puisque la distance d'_n du dual de C_n est telle que $d'_n \geq (\frac{1}{2}+\gamma)n$, le théorème 11 s'applique et nous concluons que $identTI(\phi, \phi^*)$ occulte ϕ à $\mathcal{B}ob^*$.

■

3.5.5 Le choix du code

Maintenant que nous disposons d'un mode de transmission idéal, il existe des familles de codes qui répondent à nos exigeances. Puisque chaque symbole c_i du mot de code envoyé par $\mathcal{A}lice$ est reçu correctement par $\mathcal{B}ob$, le code C_n n'a plus à être décodable. On doit donc respecter les deux conditions suivantes:

1. La distance minimale d_n pour C_n doit être telle que $d_n \in \Omega(n)$. De cette façon, les théorèmes 12 et 13 sont vérifiés.

2. La distance minimale d'_n du code $C_n^\perp$ dual de C_n doit être telle que $d_n^\perp \geq (\frac{1}{2}+\gamma)n$. Ainsi, le théorème 14 est aussi vérifié.

Des codes linéaires dans $GF(4)$ avec ces propriétés existent. Selon la borne de Varshamov-Gilbert [55] des codes avec paramètres $(n, 0.91n, 0.02n)$ sont possibles. Les codes aléatoires de longueur n et de dimension $0.91n$ ont une distance $0.02n$ sauf avec probabilité négligeable. Le dual d'un tel code est un $(n, 0.09n)$–code aléatoire. Sauf avec probabilité négligeable, cette même borne indique que le code dual est de distance minimale $0.52n$. Cette famille répond à toutes les exigeances de sécurité du protocole $identTI(\phi, \phi^*)$.

3.6 Complexité

Cette section analyse la complexité de communication quantique et du temps de calcul du protocole $identTI(\phi, \phi)$. Nous proposons une modification au protocole BBCS permettant de ramener la complexité de communication quantique dans $O(n^2)$. Ensuite nous analysons le temps de calcul nécessaire aux participants.

Complexité de communication quantique.

Le nombre total de photons transmis est $n \times N_{TI}$ où N_{TI} est le nombre de photons transmis durant l'exécution de la primitive $\binom{2}{1}$–TI_2. Nous avons vu au chapitre 2 que $N_{TI} \in \Theta(n^2)$. La complexité de communication quantique de $identTI(\phi, \phi)$ est donc $\Theta(n^3)$. Une simple modification au protocole BBCS permet de réduire la complexité de communication quantique de $identTI(\phi, \phi)$ à $O(n^2)$. Puisqu'avec un camouflage BCJL de $O(n)$ bits de long on peut camoufler $O(n)$ bits, $\mathcal{B}ob$ peut camoufler les n bits reçus et les n bases de lecture dans un seul camouflage. Soit $\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n$ les bits reçus en mesurant les photons transmis dans la séquence de bases $\widehat{\theta}_1, \widehat{\theta}_2, \ldots, \widehat{\theta}_n$ (étape 2 du protocole BBCS). Au lieu de produire n camouflages, $\mathcal{B}ob$ exécute avec $\mathcal{A}lice$ la primitive $camoufle(\widehat{b}_1, \ldots, \widehat{b}_n, \widehat{\theta}_1, \ldots, \widehat{\theta}_n)$ qui constitue un camouflage de $2n$ bits. $\mathcal{A}lice$ tire un bit aléatoire $t \in_R \{0, 1\}$, si $t = 0$ $\mathcal{B}ob$ doit révéler le camouflage en exécutant avec $\mathcal{A}lice$ la primitive $révèle(\widehat{b}_1, \ldots, \widehat{b}_n, \widehat{\theta}_1, \ldots, \widehat{\theta}_n)$. Si $\mathcal{A}lice$ constate que $T = \#\{i | \theta_i = \widehat{\theta}_i \wedge b_i \neq \widehat{b}_i\} \leq pn$ (p est le taux d'erreurs du canal quantique), $\mathcal{A}lice$ et $\mathcal{B}ob$ recommencent l'exécution du protocole. Si $T > pn$ $\mathcal{A}lice$ refuse de continuer l'exécution du protocole. Lorsque $t = 1$, $\mathcal{A}lice$ et $\mathcal{B}ob$ continuent l'exécution du

Protocole 3.6.1 ($\binom{2}{1}$**–TI**$'_2(q_0, q_1)(c)$)

1: $\mathcal{A}lice$ et $\mathcal{B}ob$ exécutent l'étape 1 du protocole 2.3.1

2: $\mathcal{B}ob$ exécute $camoufle(\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n, \widehat{\theta}_1, \widehat{\theta}_2, \ldots, \widehat{\theta}_n)$ avec $\mathcal{A}lice$.

3: $\mathcal{A}lice$ pige un bit t aléatoire et l'annonce à $\mathcal{B}ob$.

4: Si $t = 0$ **alors**

- $\mathcal{B}ob$ exécute $révèle(\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n, \widehat{\theta}_1, \widehat{\theta}_2, \ldots, \widehat{\theta}_n)$,
- $\mathcal{A}lice$ vérifie que $\#\{i \mid \theta_i = \widehat{\theta}_i \text{ et } b_i \neq \widehat{b}_i\} < pn$ sinon elle refuse de continuer,
- $\mathcal{A}lice$ et $\mathcal{B}ob$ **recommence le protocole**.

5: $\mathcal{A}lice$ annonce les bases de transmission $\theta_1, \theta_2, \ldots, \theta_n$ à $\mathcal{B}ob$.

6: $\mathcal{B}ob$ sélectionne les ensembles aléatoires $I_0, I_1 \subset \{1, ..., n\}$ relatifs à $|I_0| = |I_1| = n/2$, $I_0 \bigcap I_1 = \emptyset$ et $\forall i \in I_0, \beta_i = \beta'_i$ ou $\forall i \in I_1, \beta_i \neq \beta'_i$, et annonce $I_c, I_{\overline{c}}$ à $\mathcal{A}lice$.

7: $\mathcal{A}lice$ et $\mathcal{B}ob$ exécutent les étapes $5, 6, 7$ et 8 du protocole 2.7.1.

FIG. 3.3 - *Protocole BBCS affaibli pour* $\binom{2}{1}$*–TI*$_2$.

protocole de transmission inconsciente normalement. Le protocole $\binom{2}{1}$–TI$'_2$ (protocole 3.6.1) décrit cette procédure. Le protocole 3.5.1 avec $\binom{2}{1}$–TI$'_2$ comme primitive de transmission inconsciente constituent notre protocole d'identification final.

Remarquons que la modification proposée affaiblie sensiblement la tâche réalisée. En effet, $\mathcal{B}ob^*$ pourrait décider de ne pas mesurer les photons reçus et ainsi avoir une probabilité $\frac{1}{2}$ (la probabilité que $t = 0$) de ne pas être détecté. Dans ce cas, il apprend les deux chaînes x_i et y_i transmises par $\mathcal{A}lice$. Cet événement ne respecte pas la description abstraite de la tâche de transmission inconsciente. La bonne nouvelle c'est que $identTI(\phi, \phi)$ est robuste par rapport à cette information supplémentaire. Si $\mathcal{B}ob^*$ veut déterminer les valeurs x_i et y_i de λn transferts avec $\lambda > 0$, la probabilité qu'il ne soit pas détecté est $2^{-\lambda n}$, en supposant que lorsque $\#T \leq pn$ un des deux symboles x_i ou y_i lui est inconnu. Si moins de d'_n positions du mot de code c ont été vues par $\mathcal{B}ob^*$, presqu'aucune information sur ϕ peut être déterminée (théorème 14). Le nombre v des positions vues par $\mathcal{B}ob^*$ est

$$v = v_H + v^*$$

où $v_H = \#\{i|\phi_i^* = \phi_i\}$ et $v^* = \#\{i|\mathcal{B}ob^* \text{ obtient de l'information sur } x_i \text{ et } y_i\}$. Lorsque ϕ est indiscernable par $\mathcal{B}ob^*$ on a que $\forall\zeta_0 > 0$

$$\mathrm{P}\left(\mathbf{v}_H \geq n(\frac{1}{2} + \zeta_0)\right) \leq 2^{-\alpha_0 n}. \tag{3.1}$$

Le test effectué par $\mathcal{A}lice$ à l'étape 3 de $\binom{2}{1}$–$\mathrm{TI'}_2$ assure que pour tout $\lambda > 0$,

$$\mathrm{P}\left(\mathbf{v}^* \geq \lambda n\right) \leq 2^{-\lambda n}. \tag{3.2}$$

De 3.1 et 3.2 on conclut que pour tout $\zeta > 0$ si n est suffisamment grand,

$$\mathrm{P}\left(\mathbf{v} \geq n(\frac{1}{2} + \zeta)\right) \leq 2^{-\alpha n} \text{ pour } \alpha > 0. \tag{3.3}$$

L'équation 3.3 et le théorème 14 impliquent que, sauf avec probabilité négligeable, ϕ est indiscernable par $\mathcal{B}ob^*$ lorsque $\binom{2}{1}$–$\mathrm{TI'}_2$ est utilisé comme primitive de transmission inconsciente dans le protocole $identTI(\phi, \phi)$. De cette façon la complexité de communication quantique est ramenée $O(n^2)$.

Complexité du temps de calcul

Le protocole $identTI(\phi, \phi)$ fonctionne en $O(n^2)$ en plus d'utiliser $O(n)$ appels à la primitive $\binom{2}{1}$–$\mathrm{TI'}_2$. Ce temps quadratique est le résultat du choix du mot de code c à l'étape 4 qui s'effectue en multipliant un vecteur aléatoire de longueur n par la matrice génératrice G de dimension $n \times k_n \in O(n^2)$. Par contre, le plus important du temps est consommé pendant les n appels à $\binom{2}{1}$–$\mathrm{TI'}_2$.

Chaque fois qu'une paire d'éléments $x_i, y_i \in GF(4)$ est envoyée par la transmission inconsciente, $\mathcal{B}ob$ doit produire un camouflage. Celui-ci demande de choisir un mot de code aléatoire s d'un code C_G [21] spécifié par sa matrice génératrice G. Cette opération demande $O(n^2)$ si la multiplication $G \cdot s^T$ est effectuée. La seule condition sur C_G nécessaire pour que le protocole de camouflage quantique de [21] soit sécuritiaire est que C_G ait une distance minimale d_G telle que $\frac{d_G}{n} \geq \beta n$ pour $\beta > 0$. Dans un article récent, Speilman [66] montre comment construire des codes avec cette propriété mais aussi avec la caractéristique qu'ils sont encodables et décodables en $O(n)$. Les codes superconcentrateurs permettent de trouver s en $O(n)$. Cependant, les bits camouflés $(r'_1, \ldots, r'_n, \beta'_1, \ldots, \beta'_n)$ sont calculés par l'application d'une fonction de hachage $h : \{0,1\}^{kn} \rightarrow \{0,1\}^{2n}$ à $s \in C_G \subseteq \{0,1\}^{kn}$. Si la fonction h est déterminée par l'opérateur linéaire $H \in \{0,1\}^{kn} \times \{0,1\}^{2n}$, le temps de calcul pour évaluer $h(s) = H \cdot s^T$ est dans $O(n^2)$. Sur l'ensemble des n transmissions le temps de calcul nécessaire est donc $O(n^3)$. $\mathcal{B}ob$ pourrait aussi précalculer $h(s)$ une fois pour les n transferts. De cette façon, le temps nécessaire est équivalent à celui de multiplier deux matrices carrées de $O(n^2)$ entrées. L'algorithme de Strassen [19] permet d'y parvenir en $O(n^{2.81})$.

Le protocole de Fagin-Naor-Winkler quantique:

Notre protocole final est plus efficace que celui de [37] lorsque nous mesurons la complexité par le nombre d'appels à $\binom{2}{1}$–TI$_2$. Le protocole $identTI(\phi, \phi)$ demande $\Theta(n)$ appels à $\binom{2}{1}$–TI$_2$ (ce qui correspond aussi à $\Theta(n)$ appels à $\binom{2}{1}$–TI$_1$), tandis que celui de [37] demande $\Theta(n)$ appels à $\binom{2}{1}$–TI$_n$. Pour obtenir la primitive $\binom{2}{1}$–TI$_n$ à partir de $\binom{2}{1}$–TI$_1$, $\Omega(n)$ appels sont nécessaires [29].

Cepandant, dans le modèle quantique, la complexité de communication des deux protocoles est semblable si le protocole de transmission inconsciente BBCS est utilisé, car sa complexité de communication est $\Theta(n^2)$ pour la transmission d'une chaîne de $O(n)$ bits parmi deux.

Par contre, il n'est pas dit, qu'en basant le protocole $identTI(\phi, \phi)$ sur un protocole de transmission inconsciente différent, le gain ne serait pas réel. Au chapitre 4, nous verrons une autre façon de transmettre l'information quantique qui pourrait nous aider à atteindre ce but.

3.6.1 Cartes à puces quantiques

Dans le scénario où un protocole d'identification servirait à identifier un client à un guichet automatisé, il est préférable que certaines composantes soient du côté du guichet. Le client doit pouvoir participer au protocole avec un minimum de ressources. Il est en général beaucoup plus facile d'émettre un photon BB84 que de le mesurer. Une diode de faible intensité et un système de polarisation pour les quatre directions BB84 sont les composantes essentielles pour la transmission. Des photodétecteurs sont nécessaires pour les mesures. Ces appareils sont physiquement plus complexes et beacuoup plus difficiles à miniaturiser que ceux pour l'émission.

Lorsqu'$\mathcal{A}lice$ exécute la transmission inconsciente vers $\mathcal{B}ob$, ce dernier doit fournir des camouflages. Heureusement le camouflage BCJL renversé permet à $\mathcal{B}ob$ de mettre en gage une chaîne de bits de façon à ce que les photons circulent d'$\mathcal{A}lice$ vers $\mathcal{B}ob$. Ainsi, la technologie nécessaire pour mesurer un photon pourrait être du côté de $\mathcal{B}ob$ (qui joue le rôle du guichet).

Il est donc possible d'envisager de mettre la technologie nécessaire à $\mathcal{A}lice$ sur une carte à puces. Verrons-nous bientôt des cartes à puces quantiques pour ce genre de tâches cryptographiques? La distance entre les acteurs pouvant être très courte, la transmission quantique peut être réalisée avec un taux d'erreur de transmission très bas. Par exemple, un taux de 0.5% a été obtenu expérimentalement sur une distance de plusieurs centaines de mètres [67, 68, 56].

3.7 Conclusion

Nous avons présenté deux protocoles d'identification basés sur le même concept, mais le premier ne peut être réalisé sécuritairement parce qu'aucune famille de codes connue n'a les propriétés requises. Est-ce que de telles familles de codes existent? La question est ouverte. En pratique cependant, les usagers peuvent être à très courte distance, le taux d'erreur peut donc être très faible. Si pour un facteur de sécurité raisonnable, le nombre d'erreurs de transmission espéré est faible, le décodage par fouille exhaustive devient possible. La famille de code n'aurait donc pas à être efficacement décodable. Sous cette condition, il existe des familles qui assurent la sécurité du protocole. Il serait donc intéressant d'analyser le comportement du protocole 3.4 contre l'ensemble des mesures permises par la mécanique quantique.

Le deuxième protocole est démontré sécuritaire étant donné l'existence d'un canal de transmission inconsciente. En terme du nombre d'appels au protocole de transmission inconsciente, le protocole présenté est plus efficace que celui de [37]. Dans le modèle quantique cependant, cet avantage disparaît car, transmettre une chaîne de $O(n)$ bits parmi deux ou un bit parmi deux, le prix est le même. Cette propriété est spécifique au modèle quantique, car la réduction classique de $\binom{2}{1}$–$\mathrm{TI}_{\alpha n}$ à $\binom{2}{1}$–TI_1 demande $\Omega(n)$ appels à $\binom{2}{1}$–TI_1 [29]. On doit donc rechercher un protocole de transmission inconsciente quantique qui peut être réalisé avec un nombre constant de photons échangés pour la transmission d'une chaîne de longueur constante parmi deux. Le protocole résultant pourra être sensiblement plus faible que la transmission inconsciente sans que la sécurité du protocole d'identification soit compromise. En effet, s'il est possible pour le receveur d'obtenir les deux bits transmis pour une certaine fraction des n transferts, en autant que cette fraction respecte les conditions vues à la section 3.6, le protocole $identTI(\cdot)(\cdot)$ demeure sécuritaire. Il est important cependant que la chaîne que $\mathcal{B}ob$ décide de lire reste inconnue d'$\mathcal{A}lice$.

Chapitre 4

Mesures individuelles et mises en gage

4.1 Introduction

Récemment Dominic Mayers [53] a montré que la mécanique quantique n'autorise pas la réalisation d'un protocole de mise en gage quantique. Les implications de ce résultat sont très importantes; les mises en gage BCJL, ou autres, peuvent être craquées par des opposants capables de manipuler des systèmes quantiques d'une façon cohérente. Puisque la transmission inconsciente permet la réalisation d'une mise en gage inconditionnellement sécuritaire, nous devons conclure aussi à l'impossibilité d'effectuer une transmission inconsciente dans le modèle quantique. Encore par voie de réduction, il semble difficile d'effectuer toute tâche intéressante entre deux participants qui ne se font pas confiance. Cependant, l'attaque générale qui doit être montée par un opposant à un protocole de mise en gage est complexe et demande une manipulation cohérente des systèmes quantiques. Au chapitre 2, nous avons montré que le protocole BBCS est sécuritaire contre les mesures individuelles si nous disposons d'un protocole de mise en gage parfait. Dans ce court chapitre, nous montrons que BCJL renversé est aussi sécuritaire contre les mesures individuelles. Ceci nous permet de conclure que la transmission inconsciente BBCS est sécuritaire contre les mesures individuelles sans autres hypothèses sur les mises en gages. Il s'agit du résultat le plus fort qui puisse être prouvé à propos de la transmission inconsciente puisque les mesures cohérentes viennent nécessairement à bout des mises en gage quantiques.

En premier lieu, nous discutons rapidement les raisons qui font que les mises en gage quantique peuvent toujours être cassées. À la section 4.3, nous analysons la sécurité de BCJL renversé contre les mesures individuelles. Nous montrons que limité à de telles mesures, le protocole est sécuritaire. La technique utilisée est semblable à celle déjà vue au chapitre 2. Les mesures de $\mathcal{B}$ob* sont modélisées par des opérateurs OCPS d'une façon semblable à l'analyse du protocole BBCS.

4.2 L'impossibilité des mises en gage

Dans cette section nous faisons une revue sommaire du résultat de Mayers [53]. Nous discutons rapidement des raisons qui interdissent la construction d'un protocole de mises en gage dans le modèle quantique.

Pour qu'un protocole de mise en gage d'un bit x soit sécuritaire, les deux conditions suivantes doivent être obsevées:

1. Le reçeveur $\mathcal{A}$lice ne doit pas avoir d'information sur le bit x après que le camouflage de x ait été fourni par l'envoyeur $\mathcal{B}$ob.

2. Une le bit x mis en gage, $\mathcal{B}$ob est dans l'impossibilité d'annoncer $1 - x$ sans se faire détecter.

Ces deux propriétés sont impossibles à observer simultanément parce qu'elles entrent en conflit avec les principes de la mécanique quantique. L'attaque de Mayers montre qu'un protocole camouflant n'est nécessairement pas liant. Dans [52], on applique l'attaque pour briser BCJL version originale. Dans [53], on montre comment l'attaque contre BCJL peut être appliquée à n'importe quel protocole de mise en gage. En particulier, BCJL renversé peut être brisé. $\mathcal{B}$ob* peut décider de son bit x au moment de la révélation.

Soit $Q =< C, R >$ un protocole de mise en gage dont C désigne la phase de camouflage et R la phase de révélation. Dans [53], on présente une façon pour $\mathcal{B}$ob* de décider du bit qu'il veut mettre en gage au moment de la révélation R dans n'importe quel protocole Q qui soit camouflant.

La stratégie de $\mathcal{B}$ob*, consiste à exécuter le protocle C pour mettre en gage $x = 0$ de toutes les façons en superposition. Pour y parvenir, il enchevêtre le système prévu dans le protocole Q avec un nouveau système $|\alpha\rangle$ dont il connaît l'état initial. Pendant l'exécution de C, il range les opérations prescrites par le protocole dans son système auxiliaire $|\alpha\rangle$. Lorsqu'une instruction de Q demande à $\mathcal{B}$ob* de faire un choix entre deux actions, il exécute ces deux actions en superposition quantique avec l'aide de son système auxiliaire. À la révélation R, $\mathcal{B}$ob* mesure son système auxiliaire pour qu'une séquence de choix soit fixée. Cette façon de faire est complètement indistinguable du comportement de $\mathcal{B}$ob honnête du point de vue d'$\mathcal{A}$lice. De plus, le fait que l'ensemble des exécutions qui permettent à $\mathcal{B}$ob de camoufler $x = 0$ ne peuvent être distinguées de celles qui lui permettent de camoufler $x = 1$, implique l'existence d'une transformation unitaire, s'appliquant seulement sur le système $|\alpha\rangle$, qui transforme une exécution de Q pour le camouflage de $x = 0$ en une exécution de Q pour le camouflage de $x = 1$ (voir aussi [50],[44]).

L'idée importante est que les systèmes quantiques permettent de faire les choix le plus tard possible. En particulier, le choix de $x = 0$ ou $x = 1$ peut être reporté à la révélation si rien de ce qui a été fait dans C ne fixe de façon irréversible la valeur de x. Pensons à BCJL renversé au moment où $\mathcal{A}$lice transmet un photon dans létat $|b\rangle_{b'}$. $\mathcal{B}$ob* doit maintenant annoncer un bit β tel que si à la révélation il annonce $c = b'$ alors $\beta = b$. Nous pourrions penser que pour que tel soit le cas, $\mathcal{B}$ob* doit choisir c avant d'annoncer β. En fait, rien n'oblige $\mathcal{B}$ob* de déterminer c avant la mesure qui donne β. Par exemple, considérons la transformation unitaire suivante qui s'applique sur le photon d'$\mathcal{A}$lice et sur un système auxiliaire dans l'état connu $|\alpha\rangle$:

$$\begin{aligned} |0\rangle \otimes |\alpha\rangle &\mapsto \frac{1}{\sqrt{2}}[|0\rangle|+\rangle + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\times\rangle] \\ |1\rangle \otimes |\alpha\rangle &\mapsto \frac{1}{\sqrt{2}}[|1\rangle|+\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|\times\rangle]. \end{aligned}$$

Après l'application de la transformation U_0^* sur $|b\rangle_{b'}$, $\mathcal{B}$ob* peut obtenir β en mesurant la première particule et obtenir plus tard c en mesurant la seconde. Entre les deux mesures, tous les choix possibles pour c sont en superposition.

C'est autour de cette possibilité que l'attaque générale de Mayers est construite. Cependant, pour monter l'attaque, $\mathcal{B}$ob* doit être en mesure de manipuler des systèmes quantiques d'une façon cohérente. La prochaine section montre que si, dans BCJL renversé, $\mathcal{B}$ob* est limité à faire des mesures individuelles, ils ne peut pas changer sa mise en gage.

4.3 Les mesures individuelles

Au chapitre 2, nous avons montré que la transmission inconsciente BBCS est sécuritaire contre les mesures individuelles si nous disposons d'un protocole parfait pour les mises en gage. L'hypothèse que seul les mesures individuelles sont permises devrait aussi être appliquée aux mises en gage qui sont nécessaires pour effectuer la transmission inconsciente. L'attaque générale contre les protocoles de mises en gage n'implique pas l'impossibilité que le protocole BCJL puisse être brisé si les opposants sont limités aux mesures individuelles. Dans cette section, nous montrons la sécurité du protocole BCJL renversé contre les mesures qui s'appliquent sur un photon à la fois. Nous verrons qu'il est possible de choisir des paramètres pour le code correcteur d'erreurs tels que BCJL renversé est sécuritaire contre ce type de mesure. La conclusion est que la transmission inconsciente est sécuritaire contre les mesures individuelles lorsque BCJL renversé est utilisé pour effectuer les mises en gage.

4.3.1 Sécurité du point de vue d'$\mathcal{A}$lice

À l'étape 4 du protocole 2.5.1, Alice transmet n photons BB84 dans l'état $|b\rangle_{\phi^A} = \bigotimes_{i=1}^{n} |b_i\rangle_{\phi_i^A}$ que $\mathcal{B}$ob* mesure possiblement d'une manière incomplète. À l'étape 5, $\mathcal{B}$ob* annonce les résultats $\beta = \beta_1, \ldots, \beta_n$ de sa première mesure sur chaque photon reçu. Associé au photon π_i, le bit annoncé β_i représente le résultat partiel de la mesure incomplète M_i. Au résultat final j on associe un bit $c_i = f(j)$ pour f une fonction déterministe de l'ensemble des résultats finaux vers $\{0, 1\}$. Le résultat de l'application $f(j)$ détermine la base c_i annoncée par $\mathcal{B}$ob* à la révélation. De la même façon qu'à la section 2.8.2, nous pouvons exprimer la mesure M_i appliquée au photon π_i par un opérateur OCPS. L'opérateur M_i est composé de deux colonnes **0** et **1** ainsi que d'un nombre arbitraire de rangées $j \in \dot{J}$. L'amplitude de transition de l'état intitial $|b_i\rangle_{b'_i}$ vers l'état final $|j\rangle$ est notée comme précédemment $\phi^{b'_i}(j|b_i)$ [1]. Un résultat partiel est un sous-ensemble de J et doit indiquer un unique $\beta_i \in \{0,1\}$ que $\mathcal{B}$ob* annonce. L'ensemble $\dot{J}$ des résultats finaux peut être partionné dans les ensembles $\dot{J}_0, \dot{J}_1 \subseteq \dot{J}$ avec $\dot{J}_0 \cap \dot{J}_1 = \emptyset$ de façon à ce que pour $\beta_i \in \{0,1\}$, J_{β_i} représente le résultat correspondant à l'annonce de β_i par $\mathcal{B}$ob*. On peut donc écrire:

$$\|\phi^{b'_i}(J_{\beta_i}|b_i)\|^2 = \sum_{j \in \dot{J}_{\beta_i}} |\phi^{b'_i}(j|b_i)|^2.$$

Puisque le résultat final correspond à l'annonce du bit c_i, seulement deux résultats sont nécessaires. C'est-à-dire que pour tout $\beta_i \in \{0,1\}$, $\dot{J}_{\beta_i} = \{j_0, j_1\}$. Si $\mathcal{B}$ob* obtient le résultat final j_{c_i}, il annonce la base $c_i \in \{0,1\}$ à $\mathcal{A}$lice. La probabilité p_E, qu'$\mathcal{A}$lice détecte une erreur pour le photon π_i une fois $\langle \beta_i, c_i \rangle$ obtenu est:

$$\begin{aligned} p_E &= \mathrm{P}\left(\mathbf{b}_i \neq \beta_i \wedge \mathbf{b}'_i = c_i\right) \\ &= \frac{1}{2}\mathrm{P}\left(\mathbf{b}_i \neq \beta_i | \mathbf{b}'_i = c_i\right) \\ &= \frac{1}{2}\frac{|\phi^{c_i}(j_{c_i}|1-\beta_i)|^2}{|\phi^{c_i}(j_{c_i}|0)|^2 + |\phi^{c_i}(j_{c_i}|1)|^2}. \end{aligned}$$

D'une façon similaire à la démarche de la section 2.8.5, un résultat final $j_{c_i} \in \dot{J}_{\beta_i}$ est *ϵ–correct* si la probabilité lorsque $\mathcal{B}$ob* annonce β_i et c_i qu'une erreur soit détectée est plus petite que $\epsilon/2$.

Définition 34 *Un résultat final $\langle \beta_i, c_i \rangle$ est ϵ–correct si*

$$p_E = \frac{1}{2}\frac{|\phi^{c_i}(j_{c_i}|1-\beta_i)|^2}{|\phi^{c_i}(j_{c_i}|0)|^2 + |\phi^{c_i}(j_{c_i}|1)|^2} \leq \frac{\epsilon}{2}.$$

Remarquons que les stratégies individuelles de $\mathcal{B}$ob* sont limitées par le fait que le résultat final j_{c_i} ne donne aucune information sur la base de transmission b'_i. Rappelons que la probabilité $p(j_{c_i})$ d'obtenir le résultat final j_{c_i} peut être exprimée comme:

$$p(j_{c_i}) = |\phi^{c_i}(j_{c_i}|0)|^2 + |\phi^{c_i}(j_{c_i}|1))|^2 = |\phi^{1-c_i}(j_{c_i}|0)|^2 + |\phi^{1-c_i}(j_{c_i}|1)|^2.$$

1. Pour alléger la notation, nous utiliserons b'_i pour désigner une base de transmission $\{+,\times\}$ où d'une façon équivalente le bit $h(b'_i)$ tel que $b'_i = \{+,\times\}_{[h(b'_i)]}$.

Un résultat partiel J_{β_i} est (ϵ, τ)-prometteur si pour au moins un $c_i \in \{0,1\}$, $\mathcal{B}$ob* peut effectuer un raffinement pour lequel la probabilité d'obtenir un j_{c_i} ϵ–correct est au moins τ. Comme au chapitre 2, nous noterons $\mathbf{j}_i$ la variable aléatoire associée au résultat final de la i–ième mesure de $\mathcal{B}$ob*. La variable aléatoire associée au i–ième résultat partiel est quant à elle noté $\mathbf{J}_i$.

Définition 35 *Un résultat partiel J_{β_i} est (ϵ, τ)–prometteur par rapport à c_i s'il existe un raffinement $\{j_{c_i}, j_{1-c_i}\}$ pour lequel j_{c_i} est ϵ–correct et*

$$\mathrm{P}\left(\mathbf{j}_i = j_{c_i} | \mathbf{J}_i = J_{\beta_i}\right) \geq \tau.$$

Il est assez clair que s'il n'existe pas de c_i pour lequel J_{β_i} est (ϵ, τ)–prometteur par rapport à c_i alors $\mathcal{A}$lice a de bonnes chances de détecter une erreur. Le lemme suivant détermine une relation entre le nombre de résultats partiels (ϵ, τ)–prometteurs et la probabilité de succès de $\mathcal{B}$ob* à la révélation.

Lemme 4 *Soit δ^* le taux d'erreurs toléré par $\mathcal{A}$lice lors de la révélation. Le nombre σn de résultats partiels (ϵ, τ)–prometteurs obtenu par $\mathcal{B}$ob avant la révélation doit respecter*

$$(1-\tau)(1-\sigma)\epsilon < \delta^*$$

pour que $\mathcal{B}$ob* ait une probabilité non-négligeable de passer le protocole révélation avec succès.

Preuve. Supposons que moins de σn des résultats partiels obtenus par $\mathcal{B}$ob* sont (ϵ, τ)–prometteurs. Soit $I \subseteq \{1, \ldots, n\}$ avec $\#I \geq (1-\sigma)n$, l'ensemble des positions $i \in I$ pous lesquelles les résultats partiels J_{β_i} sur π_i n'est pas (ϵ, τ)-prometteur. Pour chaque $i \in I$ et peu importe c_i, la probabilité p_τ d'obtenir un résultat final j_{c_i} qui n'est pas ϵ–correct est telle que $p_\tau \geq 1 - \tau$. À chaque fois qu'un tel j_{c_i} est obtenu, la probabilité p_E qu'une erreur soit détectée est telle que $p_E \geq \epsilon/2$. Sur l'ensemble des résultats partiels, la valeur espérée $\overline{\delta}$ pour δ est telle que

$$\overline{\delta} \geq \frac{(1-\tau)(1-\sigma)(\epsilon/2)n}{n/2} = (1-\sigma)(1-\tau)\epsilon.$$

De plus, la probabilité que la valeur observée de δ soit sensiblement plus petite que la valeur espérée est négligeable par une application de la loi des grands nombres de

Bernsthein. Comme $\mathcal{A}$lice accepte la révélation seulement si $\delta < \delta^*$, pour que $\mathcal{B}$ob* ait une probabilité non-négligeable que sa révélation soit acceptée, il faut que

$$\delta^* \geq (1-\sigma)(1-\tau)\epsilon.$$

■

Si $\mathcal{B}$ob* veut changer sa mise en gage, pour chaque $\tilde{c}_i \in \{0,1\}$ il doit exister un raffinement $R_{\tilde{c}_i}$ tel que J_{β_i} est (ϵ,τ)–prometteur par rapport à $\tilde{c}_i$. Montrons que ceci est impossible. Les raffinements R_0 et R_1 sont choisis en fonction du résultat partiel J_{β_i} et du bit x que $\mathcal{B}$ob* veut annoncer à la révélation. Les ensembles associés $\dot{R}_0$ et $\dot{R}_1$ contiennent les ensembles de résultats finaux qui peuvent être obtenus à partir de R_0 et R_1 respectivement. Le nombre des résultats finaux pour chacun des raffinements est sans conséquence pour la suite. Supposons que le résultat partiel J_{β_i} est (ϵ,τ)–prometteur par rapport à c_i selon le raffinement R_0. Exprimons dans la base c_i la portion de l'opérateur OCPS qui correspond au résultat partiel J_{β_i}:

$$\|\phi^{c_i}(J_{\beta_i}|b_i)\|^2 = \sum_{j\in\dot{R}_0} |\phi^{c_i}(j|b_i)|^2 = \sum_{h\in\dot{R}_1} |\phi^{c_i}(h|b_i)|^2.$$

Supposons sans perte de généralités que R_0 est (ϵ,τ)–prometteur par rapport à c_i. Soit $\dot{R}_0' \subseteq \dot{R}_0$ l'ensemble des résultats ϵ–correct par rapport au résultat partiel J_{β_i} et au raffinement R_0. Nous avons que

$$\begin{aligned}
\|\phi^{c_i}(J_{\beta_i}|\beta_i)\|^2 &= \sum_{j\in\dot{R}_0} |\phi^{c_i}(j|\beta_i)|^2 \\
&\geq \sum_{j\in\dot{R}_0'} |\phi^{c_i}(j|\beta_i)|^2 \\
&\geq \sum_{j\in\dot{R}_0'} (1-\epsilon)(|\phi^{c_i}(j|0)|^2 + |\phi^{c_i}(j|1)|^2) \\
&\geq (1-\epsilon)\sum_{j\in\dot{R}_0'} p(j) \\
&\geq (1-\epsilon)\tau(\|\phi^{c_i}(J_{\beta_i}|0)\|^2 + \|\phi^{c_i}(J_{\beta_i}|1)\|^2).
\end{aligned}$$

C'est-à-dire que

$$\frac{\|\phi^{c_i}(J_{\beta_i}|\beta_i)\|^2}{\|\phi^{c_i}(J_{\beta_i}|0)\|^2 + \|\phi^{c_i}(J_{\beta_i}|1)\|^2} \geq (1-\epsilon)\tau \tag{4.1}$$

Si R_1 est un raffinement (ϵ,τ)–prometteur par rapport à $1-c_i$, on doit aussi avoir:

$$\frac{\|\phi^{1-c_i}(J_{\beta_i}|\beta_i)\|^2}{\|\phi^{c_i}(J_{\beta_i}|0)\|^2+\|\phi^{c_i}(J_{\beta_i}|1)\|^2} \geq (1-\epsilon)\tau. \tag{4.2}$$

Mais nous savons que

$$\begin{aligned}
\|\phi^{1-c_i}(J_{\beta_i}|\beta_i)\|^2 &= \frac{1}{2}(\sum_{j\in\dot{R}_0}|\phi^{c_i}(j|\beta_i)\pm\phi^{c_i}(j|1-\beta_i)|^2) \\
&= \frac{1}{2}(\sum_{j\in\dot{R}'_0}|\phi^{c_i}(j|\beta_i)\pm\phi^{c_i}(j|1-\beta_i)|^2 \\
&\quad +\sum_{j\in\dot{R}_0-\dot{R}'_0}|\phi^{c_i}(j|\beta_i)\pm\phi^{c_i}(j|1-\beta_i)|^2).
\end{aligned}$$

Traitons séparément chacune des deux sommations. Premièrement,

$$\begin{aligned}
\sum_{j\in\dot{R}'_0}|\phi^{c_i}(j|\beta_i)\pm\phi^{c_i}(j|1-\beta_i)|^2 &\leq \sum_{j\in\dot{R}'_0}||\phi^{c_i}(j|\beta_i)|+|\phi^{c_i}(j|\beta_i)||^2 \\
&\leq (\sqrt{1-\epsilon}+\sqrt{\epsilon})^2(\sum_{j\in\dot{R}'_0}|\phi^{c_i}(j|\beta_i)|^2+|\phi^{c_i}(j|\beta_i)|^2) \\
&\leq (\sqrt{1-\epsilon}+\sqrt{\epsilon})^2\tau(\||\phi^{c_i}(J_{\beta_i}|0)\|^2+\|\phi^{c_i}(J_{\beta_i}|1)\|^2) \\
&= (\sqrt{1-\epsilon}+\sqrt{\epsilon})^2\tau \\
&\qquad (\|\phi^{1-c_i}(J_{\beta_i}|0)\|^2+\|\phi^{1-c_i}(J_{\beta_i}|1)\|^2).
\end{aligned}$$

La seconde sommation maintenant,

$$\begin{aligned}
\sum_{j\in\dot{R}_0\backslash\dot{R}'_0}|\phi^{c_i}(j|\beta_i)\pm\phi^{c_i}(j|1-\beta_i)|^2 &\leq 2(\sum_{j\in\dot{R}_0\backslash\dot{R}'_0}|\phi^{c_i}(j|\beta_i)|^2+|\phi^{c_i}(j|1-\beta_i)|^2) \\
&\leq 2(1-\tau)(\|\phi^{c_i}(J_{\beta_i}|0)\|^2+\|\phi^{c_i}(J_{\beta_i}|1)\|^2) \\
&= 2(1-\tau)(\|\phi^{1-c_i}(J_{\beta_i}|0)\|^2+\|\phi^{1-c_i}(J_{\beta_i}|1)\|^2).
\end{aligned}$$

Ce qui nous donne finalement:

$$\frac{\|\phi^{1-c_i}(J_{\beta_i}|\beta_i)\|^2}{\|\phi^{c_i}(J_{\beta_i}|0)\|^2+\|\phi^{c_i}(J_{\beta_i}|1)\|^2} \leq \frac{(\sqrt{1-\epsilon}+\sqrt{\epsilon})^2\tau}{2}+(1-\tau). \tag{4.3}$$

Pour certaine valeur de ϵ et τ l'identité 4.3 viole la relation décrite à l'équation 4.1. Par exemple, pour $\epsilon=\frac{1}{20}$ et $\tau=\frac{4}{5}$, si R_0 est un raffinement (ϵ,τ)-prometteur par rapport à $c_i=0$ alors

$$\frac{\|\phi^{1-c_i}(J_{\beta_i}|\beta_i)\|^2}{\|\phi^{1-c_i}(J_{\beta_i}|0)\|^2+\|\phi^{1-c_i}(J_{\beta_i}|1)\|^2} \leq \left(\sqrt{\frac{19}{20}}+\sqrt{\frac{1}{20}}\right)^2\frac{4}{10}+\frac{1}{5}=0.67931449.$$

Si R_1 était un raffinement (ϵ, τ)–prometteur par rapport à $1 - c_i$ nous devrions avoir par l'équation 4.2:

$$\frac{\|\phi^{1-c_i}(J_{\beta_i}|\beta_i)\|^2}{\|\phi^{1-c_i}(J_{\beta_i}|0)\|^2 + \|\phi^{1-c_i}(J_{\beta_i}|1)\|^2} \geq (1-\epsilon)\tau = 0.76,$$

ce qui contredit que R_1 est un raffinement $(\frac{1}{20}, \frac{4}{5})$–prometteur par rapport à $1 - c_i$.

Par le lemme 4, pour que $\mathcal{B}$ob* puisse révéler avec succès $c \in C$, au moins σn positions $i \in I \subseteq \{1, \ldots, n\}$ doivent être telles que J_{β_i} est (ϵ, τ)–prometteur par rapport à c_i. Soit $c' \in C$ un mot de code tel que $c' \neq c$. Par définition nous avons que $\Delta(c, c') \geq d_n$ où d_n est la distance minimum du code C. Soit $J \subseteq \{1, \ldots, n\}$ l'ensemble des positions qui sont telles que J_{β_i} est (ϵ, τ)–prometteur par rapport à c'_i. Chaque $i \in I$ tel que $c'_i \neq c_i$ ne peut être dans J pour $\epsilon = \frac{1}{20}$ et $\tau = \frac{4}{5}$ comme le montre la violation de l'inégalité présenté à l'équation 4.3. Toutes les positions $i \in I$ tels que $c_i \neq c'_i$ ne peuvent être dans J. Ce qui nous permet d'écrire

$$\#J \leq n - d_n + (1-\sigma)n.$$

Si en plus nous avons que $n - d_n + (1-\sigma)n \leq \sigma n$, la probabilité que $\mathcal{B}$ob* puisse révéler avec succès c' est négligeable. En choisissant

$$d_n > 2(1-\sigma)n \tag{4.4}$$

nous obtenons que

$$\#J < n - 2(1-\sigma) + (1-\sigma)n < \sigma n. \tag{4.5}$$

Dans ce cas et par le lemme 4, $\mathcal{B}$ob* ne peut changer sa mise en gage parce que la probabilité qu'il puisse révéler $c' \neq c$ est négligeable. Pour un choix adéquat de la distance d_n du code C, le protocole est liant. N'importe quel code avec $\frac{d_n}{n} > 0$ peut être utilisé en autant que le paramètre δ^* soit choisi en conséquence. Plus δ^* est près de 0, plus la distance minimum d_n qui satisfait l'équation 4.4 approche aussi 0 car pour que $\mathcal{B}$ob* puisse révéler avec succès c', il faut que

$$\sigma > 1 - \frac{\delta^*}{\epsilon(1-\tau)} \to 0.$$

À la prochaine section, nous montrons qu'a mesure que le taux de transmission $\frac{k}{n}$ du code C approche 1, l'information d'$\mathcal{A}$lice* sur le bit $x = c \odot r$ est négligeable. Même si $\frac{k}{n} < 1$ est très près de 1, il existe un choix pour le paramètre δ^* qui satisfasse l'équation 4.5.

Protocole 4.3.1 (ContreBCJL)

1: $\mathcal{A}$lice* transmet un photon π_i dans l'état $|\theta_i\rangle$ à $\mathcal{B}$ob.

2: $\mathcal{B}$ob choisit $c_i \in \{+, \times\}$ et mesure π_i en c_i pour obtenir le bit β_i comme résultat.

3: $\mathcal{B}$ob annonce β_i à $\mathcal{A}$lice*.

4: $\mathcal{A}$lice* obtient de l'information sur c_i en fonction de β_i et de l'état initial $|\theta_i\rangle$.

FIG. 4.1 - *Stratégie d'$\mathcal{A}$lice* contre BCJL renversé.*

4.3.2 Sécurité du point de vue de $\mathcal{B}$ob

Intéressons-nous aux comportements déviants d'$\mathcal{A}$lice*. Son but est de transmettre n photons $\pi_1, \ldots, \pi_n$ pour lesquels, une fois β annoncé par $\mathcal{B}$ob, l'information sur $c = c_1, \ldots, c_n \in C$ est maximum. Nous montrerons qu'$\mathcal{A}$lice* ne peut préparer un système tel que le nombre de candidats équiprobables pour c est petit une fois β appris. Une stratégie individuelle pour $\mathcal{A}$lice* consiste pour chaque $i \in \{1, \ldots, n\}$ à envoyer un photon π_i dans l'état

$$|\theta_i\rangle = \begin{pmatrix} \cos\theta_i \\ \sin\theta_i \end{pmatrix}.$$

Le protocole 4.3.1 décrit un cadre général dans lequel les attaques individuelles d'$\mathcal{A}$lice* contre BCJL renversé sont inscrites. Par la suite, nous noterons Θ_i la variable aléatoire pour le choix de θ_i.

En premier lieu, supposons qu'$\mathcal{A}$lice* est honnête dans sa préparation des photons qu'elle transmet à $\mathcal{B}$ob. C'est-à-dire que $|\theta_i\rangle \in \{\rightarrow, \nearrow, \uparrow, \nwarrow\}$. Une fois $\beta = \beta_1, \ldots, \beta_n$ annoncés par $\mathcal{B}$ob, $\mathcal{A}$lice* obtient de l'information sur $c = c_1, \ldots, c_n$. Si n'importe quelle chaîne $c \in \{0,1\}^n$ pouvait être utilisée par $\mathcal{B}$ob, les chaînes possibles, du point de vue d'$\mathcal{A}$lice, pour c sont celles de l'ensemble $S(b, b', \beta)$ défini comme:

$$S(b, b', \beta) = \{\hat{c} \in \{0,1\} | (\forall i \in \{1, \ldots, n\})[\beta_i \neq b_i \Rightarrow \hat{c}_i = 1 - b'_i]\}.$$

Pour chaque position i telle que $\beta_i \neq b_i$, $\mathcal{A}$lice sait que la base utilisée par $\mathcal{B}$ob est

$c_i = 1 - b'_i$. Pour chaque $\widehat{c} \in S(b, b', \beta)$ et $i \notin \Delta(\beta, b)$, on a que

$$\begin{aligned}
\mathrm{P}\left(\mathbf{c}_i = b'_i | \boldsymbol{\beta}_i = b_i\right) &= \mathrm{P}\left(\mathbf{c}_i = b'_i \wedge \boldsymbol{\beta}_i = b_i\right) / \mathrm{P}\left(\boldsymbol{\beta}_i = b_i\right) \\
&= \frac{\mathrm{P}\left(\mathbf{c}_i = b'_i \wedge \boldsymbol{\beta}_i = b_i\right)}{\frac{1}{2}(\mathrm{P}\left(\boldsymbol{\beta}_i = b_i | \mathbf{c}_i = b'_i\right) + \mathrm{P}\left(\boldsymbol{\beta} = b_i | \mathbf{c}_i \neq b'_i\right))} \\
&= \frac{4\mathrm{P}\left(\mathbf{c}_i = b'_i \wedge \boldsymbol{\beta}_i = b_i\right)}{3} \\
&= 2/3. \qquad (4.6)
\end{aligned}$$

Soit $\Delta(b, \beta, b', \widehat{c}) = \{i | \beta_i = b_i \wedge \widehat{c}_i \neq b'_i\}$. Une fois β annoncé, la probabilité $p(\widehat{c})$ que $c = \widehat{c} \in S(b, b', \beta)$ est telle que

$$p(\widehat{c}) = \left(\frac{2}{3}\right)^{\Delta(b,\beta) - \Delta(b,\beta,b',\widehat{c})} \left(\frac{1}{3}\right)^{\Delta(b,\beta,b',\widehat{c})}.$$

Il s'agit d'une distribution binômiale. Puisqu'en plus $\mathcal{A}$lice sait que $c \in C$, seul les candidats dans $S(b, \beta, b') \cap C$ sont possibles. La vue $\mathcal{V}_A$ d'$\mathcal{A}$lice sur c peut être exprimée de la façon suivante:

$$\mathcal{V}_A = \{< \widehat{c}, p(\widehat{c})/p_T >\}_{\widehat{c} \in S(b,\beta,b') \cap C}$$

pour $p_T = \sum_{\widehat{c} \in S(b,\beta,b') \cap C} p(\widehat{c})$. L'information sur c qu'$\mathcal{A}$lice honnête obtient est caractérisée par le fait que

1. Les bits de c aux positions i telles que $\beta_i \neq b_i$ sont connus et valent $1 - b'_i$. Le nombre espéré de ces positions est $n \cdot \mathrm{P}\left(\boldsymbol{\beta}_i \neq b_i\right) = n \cdot \frac{1}{2}\mathrm{P}\left(\boldsymbol{\beta}_i \neq b_i | \mathbf{c}_i \neq b'_i\right) = \frac{n}{4}$.

2. Les bits qui ne sont pas connus avec certitude sont tels que $\mathrm{P}\left(\mathbf{c}_i = b'_i | \boldsymbol{\beta}_i = b_i\right) = \frac{2}{3}$.

Nous voulons donc un code $[n, k]$–code C pour lequel $\mathbf{I}(\mathbf{x} | \mathcal{V}_A) \leq 2^{-\alpha n}$ pour $\alpha > 0$. Intuitivement, plus le taux de transmission $\frac{k}{n}$ du code C approche 1, moins β divulgue d'information sur c. Le nombre de candidats équiprobables peut être borné inférieurement par $2^{\gamma n}$ pour $\gamma > 0$. il devient alors possible d'appliquer le théorème 8 pour conclure qu'$\mathcal{A}$lice a une quantité négligeable d'information sur $c \odot r$.

Cependant, les stratégies d'$\mathcal{A}$lice* peuvent être biens différentes de la stratégie honnête et plus d'information sur c peut être obtenue en choisissant $|\theta_i\rangle$ d'une façon plus astucieuse. La situation d'$\mathcal{A}$lice* n'est pas habituelle car ses stratégies consistent

Protocole 4.3.2 (Trans(c_i) **)**

1: $\mathcal{B}$ob transmet un photon $\widehat{\pi}_i$ dans l'état:

$$|\widehat{\pi}_i\rangle = \begin{cases} |\rightarrow\rangle & \text{si } c_i = 0 \\ |\nearrow\rangle & \text{si } c_i = 1. \end{cases}$$

2: Alice choisit une mesure de Von Neumann M_{θ_i}, pour $\theta \in [0, \frac{\pi}{2}]$, dont les deux résultats possibles sont caractérisés par les projections orthogonales $\{P_{\theta_i}, P_{\theta_i}^{\perp}\}$. $\mathcal{A}$lice* mesure $\widehat{\pi}_i$ et pose

$$\widehat{\beta}_i = \begin{cases} 0 & \text{si } P_{\theta_i} \text{ est obtenu} \\ 1 & \text{si } P_{\theta_i}^{\perp} \text{ est obtenu.} \end{cases}$$

FIG. 4.2 - *Transmission équivoque de c_i.*

à choisir comment transmettre les photons et non comment les mesurer. Pour faciliter cette analyse, considérons le protocole 4.3.2 présenté à la figure 4.2.

Dans le scénario présenté au protocole 4.3.1, l'information obtenue par $\mathcal{A}$lice* sur c_i est fonction de l'état intial du système et de l'information classique β_i. Dans le deuxième scénario, l'information sur c_i est donné par une mesure de Von Neumann. Le codage des bits de c_i est intrinsèquement équivoque car les états pour un 0 et un 1 ne sont pas orthogonaux. Même si ces deux situations sont bien différentes, nous allons montrer que l'information obtenue par $\mathcal{A}$lice* sur c_i est la même dans les deux cas. Toute stratégie individuelle qui permet à $\mathcal{A}$lice* d'obtenir de l'information sur c_i dans le premier scénario peut être transformée en une autre qui donne la même information sur c_i dans le second. Dans les deux cas, nous considérons $\mathcal{B}$ob honnête.

Lemme 5 *Les protocoles 4.3.1 et 4.3.2 donnent la même information sur c_i à $\mathcal{A}$lice* peu importe sa stratégie sur des photons individuels.*

Preuve. Soit $\theta_i \in [0, \frac{\pi}{2}]$ et $\nu \in \{0, 1\}$ quelconques. Soit Θ_i la variable aléatoire qui correspond au choix de θ_i. Dans le scénario du protocole 4.3.1, nous avons que

$$\begin{aligned}
\mathrm{P}\left(\mathbf{c}_i = 0|\boldsymbol{\beta}_i = \nu \wedge \Theta_i = \theta_i\right) &= \frac{\mathrm{P}\left(\mathbf{c}_i = 0 \wedge \boldsymbol{\beta}_i = \nu|\Theta_i = \theta_i\right)}{\mathrm{P}\left(\boldsymbol{\beta}_i = \nu|\Theta_i = \theta_i\right)} \\
&= \frac{\mathrm{P}\left(\boldsymbol{\beta}_i = \nu|\mathbf{c}_i = 0 \wedge \Theta_i = \theta_i\right)\mathrm{P}\left(\mathbf{c}_i = 0|\Theta_i = \theta_i\right)}{\mathrm{P}\left(\boldsymbol{\beta}_i = \nu|\Theta_i = \theta_i\right)} \\
&= \frac{\mathrm{P}\left(\mathbf{c}_i = 0|\Theta_i = \theta_i\right)\|\{P_0, P_{\frac{\pi}{2}}\}_{[\nu]}|\theta_i\rangle\|^2}{\mathrm{P}\left(\beta_i = \nu|\Theta_i = \theta_i\right)}.
\end{aligned}$$

D'autre part, calculons cette même probabilité dans le scénario de la figure 4.3.2.

$$\begin{aligned}
\mathrm{P}\left(\mathbf{c}_i = 0|\widehat{\boldsymbol{\beta}_i} = \nu \wedge \Theta_i = \theta_i\right) &= \frac{\mathrm{P}\left(\mathbf{c}_i = 0 \wedge \widehat{\boldsymbol{\beta}_i} = \nu|\Theta_i = \theta_i\right)}{\mathrm{P}\left(\widehat{\boldsymbol{\beta}_i} = \nu|\Theta_i = \theta_i\right)} \\
&= \frac{\mathrm{P}\left(\widehat{\boldsymbol{\beta}_i} = \nu|\mathbf{c}_i = 0 \wedge \Theta_i = \theta_i\right)\mathrm{P}\left(\mathbf{c}_i = 0|\Theta_i = \theta_i\right)}{\mathrm{P}\left(\widehat{\boldsymbol{\beta}_i} = \nu|\Theta_i = \theta_i\right)} \\
&= \frac{\mathrm{P}\left(\mathbf{c}_i = 0|\Theta_i = \theta_i\right)\|\{P_{\theta_i}, P_{\theta_i}^{\perp}\}_{[\nu]}|\rightarrow\rangle\|^2}{\mathrm{P}\left(\widehat{\boldsymbol{\beta}_i} = \nu|\Theta_i = \theta_i\right)}.
\end{aligned}$$

Par symétrie, nous avons en général pour $\gamma, \zeta \in \{0, \ldots, \frac{\pi}{2}\}$ que

$$\|P_\gamma|\zeta\rangle\|^2 = \|P_\zeta|\gamma\rangle\|^2 = |\langle\gamma|\zeta\rangle|^2. \tag{4.7}$$

Ce qui nous donne:

$$\|\{P_0, P_{\frac{\pi}{2}}\}_{[\nu]}|\theta_i\rangle\|^2 = |\langle\frac{\pi \cdot \nu}{2}|\theta_i\rangle|^2$$

et

$$\|\{P_{\theta_i}, P_{\theta_i}^{\perp}\}_{[\nu]}|\rightarrow\rangle\|^2 = |\langle\theta_i + \frac{\nu \cdot \pi}{2}|\rightarrow\rangle|^2 = |\langle\frac{\pi \cdot \nu}{2}|\theta_i\rangle|^2.$$

Nous avons donc que $\mathrm{P}\left(\mathbf{c}_i = 0|\boldsymbol{\beta}_i = \nu \wedge |\theta_i\rangle\right) = \mathrm{P}\left(\mathbf{c}_i = 0|\widehat{\boldsymbol{\beta}_i} = \nu \wedge \Theta_i = \theta_i\right)$ si

$$\mathrm{P}\left(\boldsymbol{\beta}_i = \nu||\theta_i\rangle\right) = \mathrm{P}\left(\widehat{\boldsymbol{\beta}_i} = \nu|\Theta_i = \theta_i\right).$$

Vérifions que tel est bien le cas,

$$\begin{aligned}
\mathrm{P}\left(\boldsymbol{\beta}_i = \nu|\Theta_i = \theta_i\right) &= \mathrm{P}\left(\mathbf{c}_i = 0|\Theta_i = \theta_i\right)\mathrm{P}\left(\boldsymbol{\beta}_i = \nu|\mathbf{c}_i = 0 \wedge \Theta_i = \theta_i\right) \\
&\quad +\mathrm{P}\left(\mathbf{c}_i = 1|\Theta_i = \theta_i\right)\mathrm{P}\left(\boldsymbol{\beta}_i = \nu|\mathbf{c}_i = 1 \wedge \Theta_i = \theta_i\right) \\
&= \mathrm{P}\left(\mathbf{c}_i = 0|\Theta_i = \theta_i\right)\|\{P_0, P_{\frac{\pi}{2}}\}_{[\nu]}\Theta_i = \theta_i\|^2 \\
&\quad +\mathrm{P}\left(\mathbf{c}_i = 1|\Theta_i = \theta_i\right)\|\{P_{\frac{\pi}{4}}, P_{\frac{3\pi}{4}}\}_{[\nu]}|\theta_i\rangle\|^2
\end{aligned}$$

Et pour le scénario 4.3.2,

$$\begin{aligned}
\mathrm{P}\left(\widehat{\boldsymbol{\beta}}_i = \nu | \Theta_i = \theta_i\right) &= \mathrm{P}\left(\mathbf{c}_i = 0 | \Theta_i = \theta_i\right) \mathrm{P}\left(\boldsymbol{\beta}_i = \nu | \mathbf{c}_i = 0 \wedge \Theta_i = \theta_i\right) \\
&\quad + \mathrm{P}\left(\mathbf{c}_i = 1 | \Theta_i = \theta_i\right) \mathrm{P}\left(\boldsymbol{\beta}_i = \nu | \mathbf{c}_i = 1 \wedge \Theta_i = \theta_i\right) \\
&= \mathrm{P}\left(\mathbf{c}_i = 0 | \Theta_i = \theta_i\right) \| \{P_{\theta_i}, P_{\theta_i}^{\perp}\}_{[\nu]} | \rightarrow\rangle \|^2 \\
&\quad + \mathrm{P}\left(\mathbf{c}_i = 1 | \Theta_i = \theta_i\right) \| \{P_{\theta_i}, P_{\theta_i}^{\perp}\}_{[\nu]} | \nearrow\rangle \|^2
\end{aligned}$$

En utilisant l'identité 4.7 nous obtenons aussi que

$$\| \{P_{\frac{\pi}{4}}, P_{\frac{3\pi}{4}}\}_{[\nu]} |\theta_i\rangle \|^2 = \| \{P_{\theta_i}, P_{\theta_i}^{\perp}\}_{[\nu]} | \nearrow\rangle \|^2.$$

La distribution de probabilité sur c_i étant donné β_i est la même dans les deux situations peu importe la stratégie individuelle spécifiée par $\theta_i \in \{1, \ldots, \frac{\pi}{2}\}$.

■

À la lumière du chapitre 2, le second scénario peut être analysé plus facilement avec la machinerie utilisée pour l'analyse du protocole BBCS et celle utilisée pour montrer que BCJL est camouflant [21] (ce qui demeure vrai malgré l'attaque de Mayers). Le canal par lequel $\mathcal{B}$ob transmet les bits de c limite la quantité d'information par photon. Les deux états n'étant pas orthogonaux, l'information qu'il est possible de transmettre par photon est moindre que 1 bit [47]. Cependant, pour transmettre un mot aléatoire d'un $[n, k]$–code, $\frac{k}{n}$ bit d'information par photon sont nécessaires en moyenne. Soit ρ^* la matrice de densité associée à la transmission d'états dans $\{\rightarrow, \nearrow\}$ avec le maximum d'entropie (i.e. la source qui émet le plus d'information par symbole). Nous avons que

$$\begin{aligned}
\rho^* &= \frac{1}{2} | \rightarrow\rangle\langle\rightarrow | + \frac{1}{2} | \nearrow\rangle\langle\nearrow | \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \\
&= \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} \\
&= \rho_0.
\end{aligned}$$

La matrice de densité ρ^* peut être réécrite d'une façon plus intéressante. En effet,

$$\rho^* = \cos^2 \frac{\pi}{8} |\mathbf{b}_0\rangle\langle\mathbf{b}_0| + \sin^2 \frac{\pi}{8} |\mathbf{b}_0^{\perp}\rangle\langle\mathbf{b}_0^{\perp}| \tag{4.8}$$

où $\mathbf{b}_0$ est le vecteur de la base de Breidbart

$$\mathbf{b}_0 = \begin{pmatrix} \cos\frac{\pi}{8} \\ \sin\frac{\pi}{8} \end{pmatrix}$$

et $\mathbf{b}_0^\perp$ lui est orthogonal. Les deux états possibles de l'équation 4.8 sont orthogonaux ce qui nous permet de caractériser l'information moyenne maximum W que transmet chaque photon. Il s'agit de l'entropie de Von Neumann de ρ^* définie comme l'entropie de Shannon de la distribution $\{\lambda_1, \ldots, \lambda_s\}$ où chaque λ_i est une valeur propre de ρ^*. La matrice de densité ρ^* est la caractérisation de la source d'information d'entropie maximum associée à la transmission de c_i selon le codage $\{\rightarrow, \nearrow\}_{[c_i]}$. L'équation 4.8 nous indique que les valeurs propres de ρ^* sont $\cos^2\frac{\pi}{8}$ et $\sin^2\frac{\pi}{8}$. L'entropie de Von Neumann W (voir [58] page 263) associée à ρ^* est

$$W = \mathbf{H}(\cos^2\frac{\pi}{8}) \leq 0.6008761895.$$

L'information moyenne qu'un photon $\widehat{\pi}_i$ donne sur c_i est toujours moindre que W. Un tel canal ne peut transmettre plus de $W_n = nW$ bits d'information en moyenne par la transmission de n photons. D'autre part, pour transmettre un mot de code aléatoire $c \in_R C$, pour C un $[n,k]$-code, k bits d'information doivent être spécifiés. Si pour $\delta > 0$ on a que

$$k \geq (0.6008761895 + \delta)n \tag{4.9}$$

alors l'information transmise par $\mathcal{B}$ob est nécessairement insuffisante en moyenne pour retrouver de façon unique l'identité de c [62, 47]. Si le canal pouvait être modélisé par une canal symétrique binaire avec un taux d'erreurs $\cos^2\frac{\pi}{8}$, le nombre de candidats équiprobables E pour c après la réception de $\{\widehat{\pi}_i\}_{i=1}^n$ par le canal quantique serait, sauf avec probabilité négligeable $2^{-\alpha n}$, tel que

$$E \geq 2^{k - W_n - \alpha n} = 2^{n(\delta - \alpha)}$$

pour $\alpha > 0$ et k choisie comme à l'équation 4.9. On pourrait alors appliquer le théorème 8 pour conclure que l'information sur c est négligeable.

La situation réelle est plus subtile et permet à $\mathcal{A}$lice d'obtenir toute l'information sur certains c_i et moins sur d'autres. Tout ce qu'il est possible de dire c'est que l'information moyenne sur chaque c_i qu'$\mathcal{A}$lice obtient en mesurant $\widehat{\pi}_i$ est W. Pensons à la stratégie honnête qui donne le quart des bits physiques de c sans erreur et de façon à ce qu'$\mathcal{A}$lice puisse savoir lesquels. Cette information n'est certainement pas modélisable par une transmission sur un canal symétrique binaire. Cependant, certains bits c_i doivent être vus par $\mathcal{A}$lice* comme s'ils étaient transmis sur une canal symétrique binaire. Comme au chapitre 2, nous définissons de la façon suivante les résultats informatifs à propos de c_i:

Définition 36 *Un résultat $\widehat{\beta}_i$ sur le photon $\widehat{\pi}_i$ est ϵ'–informatif s'il existe $c^* \in \{0,1\}$ tel que*

$$\mathrm{P}\left(\mathbf{c}_i = c^* | \widehat{\boldsymbol{\beta}}_i = \widehat{\beta}_i\right) \geq \epsilon'.$$

Une mesure est prometteuse si elle donne un résultat informatif avec bonne probabilité.

Définition 37 *Une mesure M_i sur $\widehat{\pi}_i$ est (ϵ', τ)–prometteuse si la probabilité p_s qu'elle donne un résultat ϵ'–correct est telle que $p_s \geq \tau$.*

Remarquons que pour des couples (ϵ', τ), aucune mesure ne peut être (ϵ', τ)–prometteuse. Une mesure (ϵ', τ)-prometteuse donne au moins $R(\epsilon', \tau) \geq \tau(1 - \mathbf{H}(\epsilon'))$ bits d'information en moyenne. Puisque la quantité moyenne d'information que le canal peut transmettre est W, on doit avoir que

$$\tau(1 - \mathbf{H}(\epsilon')) \leq R(\epsilon', \tau) \leq W.$$

La probabilité $\tau(\epsilon')$ d'obtenir un résultat qui donne le bit c_i avec probabilité meilleure que ϵ' est donc telle que

$$\tau(\epsilon') \leq \frac{W}{(1 - \mathbf{H}(\epsilon'))}. \tag{4.10}$$

Puisque chaque mesure est appliquée à un seul photon, sauf avec probabilité négligeable $2^{-\alpha n}$, le nombre t des positions $i \in \overline{I} \subseteq \{1, \ldots, n\}$ pour lesquels un résultat m_i ϵ'–informatif a été obtenu est tel que $t \leq (\tau(\epsilon') - \alpha)n$. Pour les $n - t$ autres positions $i \in I$, la résultat $\widehat{\beta}_i = c_i$ avec probabilité moindre que ϵ'. Nous sommes essentiellement dans le cas traité au chapitre 2 section 2.9. Pour rendre les deux situations identiques, supposons que le code C est sous forme systématique et les k bits du message sont transmis sur le canal quantique par les photons $\widehat{\pi}_1, \ldots, \widehat{\pi}_k$ tandis que les $n-k$ bits de redondance sont annoncés en clair à $\mathcal{A}$lice*. Supposons que la chaîne annoncée est $s \in \{0,1\}^{n-k}$. Soit $\gamma \in \{0,1\}^t = c_{[\overline{I}]}$ la chaîne c aux positions dans $\overline{I}$ étant donné les résultats d'$\mathcal{A}$lice*. Peu importe la mesure, il existe un ensemble de positions $I \subseteq \{1,\ldots,k\}$ de cardinalité $k-t$ tel que les candidats pour c sont ceux de l'ensemble

$$N'_d(s) = \{w \in \{0,1\}^k | w \uplus s \in C^{I,\gamma}\}$$

où $C^{I,\beta}$ est le code ponctionné obtenu à partir de C comme indiqué à la définition 29. Pour obtenir une borne sur le nombre de candidats équiprobables, il est utile de donner une information supplémentaire à $\mathcal{A}$lice* même si cette information ne peut être obtenue par ses mesures. Pour ce faire, définissons la chaîne $\tilde{\beta}$ qui vaut $\widehat{\beta}$ aux positions qui ne sont pas ϵ'–correctes mais qui vaut c_i aux autres. La valeur de $\widehat{\beta}_i$ pour $i \in I$ est déterminée comme au protocole 4.3.2. Plus précisemment,

$$\tilde{\beta} = \begin{cases} c_i & \text{si } i \notin I \\ \widehat{\beta}_i & \text{si } i \in I. \end{cases}$$

Il s'agit de la chaîne la plus probable pour c (étant donné les résultats d'$\mathcal{A}$lice*) qui, aux positions $i \notin I$, vaut c_i. Supposons maintenant qu'$\mathcal{A}$lice* obtient magiquement la distance $d = \Delta(\tilde{\beta}, c)$ en plus de savoir avec probabilité exactement ϵ' les bits c_i aux positions $i \in I$. La situation réelle est nécessairement pire pour $\mathcal{A}$lice*. Avec cette information supplémentaire, les candidats équiprobables pour c sont

$$N_d^{\tilde{\beta}}(s) = \{w \in N'_d(s) | \Delta(\tilde{\beta}, w_{[I]}) = d\}.$$

Même si pour chaque $i \in I$ on avait que $\mathrm{P}\left(\mathbf{c}_i = c^* | \mathbf{m}_i = m_i\right) = \epsilon'$, le nombre de candidats équiprobables dans $N_d^{\tilde{\beta}}(s)$ peut être évalué en applicant le lemme 2. Ce qui nous donne que

$$\# N_d^{\tilde{\beta}}(s) \geq \frac{\binom{k-t}{d}}{2^{n-k+\alpha n}} \tag{4.11}$$

sauf avec probabilité négligeable $2^{-\alpha n}$.

On peut maintenant déterminer la valeur des constantes dans l'équation 4.11. Par l'équation 4.10, nous savons que le nombre de positions pour lesquelles le bit c_i est connu avec probabilité meilleure que $\epsilon' = \frac{19}{20}$ est

$$\tau(\frac{19}{20}) \leq \frac{\mathbf{H}(\cos^2 \frac{\pi}{8})}{1 - \mathbf{H}(\frac{19}{20})} \leq 0.8420312146.$$

On peut donc poser $t \leq 0.85k$ pour conclure que le nombre de résultats $\frac{19}{20}$–informatifs est moindre que t sauf avec probabilité négligeable. Nous avons donc que le nombre de résultats qui ne sont pas $\frac{19}{20}$–informatifs est plus grand que $0.15k$. D'autre part, la valeur espérée $\overline{d}$ pour la distance d est telle que $\overline{d} \geq 0.15k \cdot \frac{1}{20} \geq 0.007k$. La probabilité que d soit significativement moinre que $\overline{d}$ est négligeable en applicant la loi des grands nombres. Le nombre de candidats équiprobables est

$$\#N_d^{\tilde{\beta}}(s) \geq \frac{\binom{0.15k}{0.0075k}}{2^{n-k+\alpha n}}.$$

Par l'approximation standard, on obtient

$$\#N_d^{\tilde{\beta}}(s) \geq \frac{2^{\mathbf{H}(0.05)0.15k}}{2^{n-k+\alpha n}}.$$

En autant que $n - k + \alpha n < \mathbf{H}(0.05)0.15k \leq 0.042k$ le nombre de candidats équiprobables pour c est exponentiel en n. On peut alors appliquer le théorème 8 pour conclure que l'information d'$\mathcal{A}$lice* sur $c \odot r$ est négligeable. Le taux de transmission $\frac{k}{n}$ du code C doit être tel que $n - k < 0.042k$ d'où

$$\frac{k}{n} \geq 0.96. \tag{4.12}$$

Une analyse plus précise permettrait sans doutes d'améliorer sensiblement cette borne sur le taux de transmission. Ceci aurait pour avantage d'augmenter la distance minimum de C et d'augmenter le facteur de tolérance δ^* aux erreurs de lecture. L'analyse faite ici nous permet de conclure la sécurité de BCJL-renversé contre les mesures individuelles pour un facteur de tolérance δ^* très petit. En utilisant la borne de Varshamov-Gilbert, la disance minimum d_n pour un $[n, k, d_n]$–code aléatoire avec $\frac{k}{n} = 0.96$ est, pour n assez grand et sauf avec probabilité négligeable, telle que

$$d_n = 0.004n.$$

Avec la borne exprimée au lemme 4, le paramètre δ^* doit être choisi tel que

$$\delta^* > (1 - \sigma)(1 - \tau)\epsilon.$$

Pour $\epsilon = \frac{1}{20}$ et $\tau = \frac{4}{5}$ nous avons que

$$(1 - \sigma) < \frac{\delta^*}{(1 - \tau)\epsilon} < 100\delta^*.$$

En choisissant $(1-\sigma) = 100\delta^*$ Par l'équation 4.4, on obtient

$$d_n = 0.004n > 2(1-\sigma)n = 200\delta^*$$

et

$$\delta^* < 0.00002.$$

Sans aucun doute les valeurs trouvées ici peuvent être améliorées. Puisque δ^* est une borne supérieure sur le taux d'erreurs toléré sur le canal quantique, celui-ci doit être presque parfait pour satisfaire nos contraintes.

4.4 Conclusion et questions ouvertes

L'impossiblité des mises en gage est une bien mauvaise nouvelle. La cryptographie dans le modèle à deux participants est inconsistante avec les axiomes de la mécanique quantique. Il semble que nous soyons revenu à la case départ, pour être en mesure de réaliser la tâche cryptographique la plus simple, des hypothèses supplémentaires sont nécessaires. Nous avons vu que si les opposants à BCJL renversé sont limités à des mesures individuelles, ils ne peuvent rien contre le protocole. Il ne reste qu'à montrer que les preuves de sécurité contre les mesures individuelles, pour BCJL renversé et pour BBCS utilisés avec des mises en gage parfaites, peuvent être composées. Si tel était le cas, BBCS serait sécuritaire contre les mesures individuelles selon les principes de la mécanique quantique. Il s'agit d'une hypothèse physique qui ne peut être réduite à celles qui permettent les mises en gage dans le monde classique. Une analyse plus subtile qui déterminerait les paramètres optimaux pour le code correcteur et le seuil de tolérance δ^* aurait avantage à être faite. De plus, il semble bien que la limitation aux mesures individuelles ne soient nécessaire que pour l'envoyeur. La sécurité pourrait être démontrée inconditionnellement peu importe l'astuce du receveur. De la même façon, il est possible qu'un protocole de mise en gage inconditionnellement sécuritaire pour le receveur mais sécuritaire contre les mesures individuelles pour l'envoyeur existe. Il serait intéressant de vérifier que tel est bien le cas. Dans certaines situations asymétriques, des mises en gage de ce type peuvent être utiles. Le problème d'identification que nous avons étudié au chapitre 3 est de ceux-là. Un protocole qui protège contre n'importe quel guichet malhonête mais qui protège la banque contre les mesures individuelles des usagers pourrait être suffisant. La complexité de l'attaque contre les mises en gage est comparable à celle requise pour construire un ordinateur quantique. Il semble très improbable qu'un usager malhonnête réussisse à entrer un ordinateur quantique dans sa carte à puces. Il serait très intéressant d'analyser la complexité réelle de monter une attaque contre les protocoles de mises en gage. Est-ce que certains d'entre-eux sont plus difficiles à casser? Est-il possible d'en construire un pour lequel un opposant doit nécessairement utiliser une technologie excessive? Par exemple, si un opposant pour craquer un protocole de mise en gage doit absolument construire un ordinateur quantique capable d'être facilement adaptée pour factoriser, alors cet opposant est aussi dangereux contre les protocoles classiques. Les candidats connus pour être fonctions à sens unique sont tous basés sur la théorie des nombres. Être capable de factoriser efficacement permet d'inverser les fonctions candidates. Un opposant disposant d'un ordinateur quantique peut aussi inverser ces fonctions à sens unique par l'algorithme de Shor et craquer les protocoles de mises en gage obtenus à partir de ces candidats. Ces pistes de recherches devraient être empruntés pour faire la lumière sur la puissance réelle des attaques autorisées par la mécanique quantique.

Conclusion

À la fin des chapitres 2, 3 et 4 nous avons conclu et discuté des pistes de recherche associées à chacune des variations. Nous terminons par une discussion de nature plus générale sur les sujets que nous avons abordés.

Même si des hypothèses sont nécessaires pour obtenir un protocole de mise en gage, la cryptographie quantique offre des avantages par rapport à la cryptographie classique. Prenons l'exemple du protocole de distribution de clefs secrètes de [6, 8] qui réalise une tâche cryptographique impossible dans le monde classique [63]. Une question qui reste à élucider est la suivante: Est-il possible de faire mieux en cryptographie quantique qu'en cryptographie classique même dans le scénario où deux participants ne se font pas confiance? Une observation permet de penser que tel pourrait être le cas. En cryptographie classique l'existence de fonctions à sens unique ne permet pas d'obtenir automatiquement un protocole pour la transmission inconsciente [46]. Le résultat de [71] montre que des mises en gage parfaites permettent d'obtenir un protocole inconditionellement sécuritaire pour la transmission inconsciente quantique. Dans le monde classique, il y a des mises en gage si et seulement si des fonctions à sens unique existent. Donc, si des fonctions à sens unique existent, un protocole quantique pour la transmission inconsciente existe aussi. Le cryptogaphie quantique semble necessiter des hypothèses moins fortes pour réaliser la transmission inconsciente.

L'ordinateur quantique, qui permet de casser tout protocole de mise en gage quantique, est aussi une mauvaise nouvelle par la cryptographie classique. Les candidats connus pour être fonctions à sens unique, sont presque tous basés sur des problèmes de théorie des nombres comme factorisation et logarithme discret. L'algorithme de Shor [64] peut casser ces deux hypothèses en temps polynomial. Il semble que la puissance de l'ordinateur quantique soit suffisante pour interdire les mises en gage autant dans le monde classique que quantique.

Nous avons vu que limité aux mesures individuelles, la cryptographie quantique permet la réalisation de l'ensemble des tâches cryptographiques à deux participants. Cette hypothèse n'est pas équivalente à l'existence de fonctions à sens unique même si elle suppose que l'ordinateur quantique n'existe pas. Par exemple, si $\mathbf{P} = \mathbf{NP}$ des fonctions à sens unique ne peuvent pas exister, et ce, sans tenir compte de l'algorithme de Shor. L'hypothèse que les mesures sont individuelles, est une hypothèse de nature physique qui n'a pas d'équivalent dans le monde classique. Ceci suggère la recherche d'autres hypothèses sur lesquelles baser la cryptographie quantique. Pour déterminer exactement la puissance cryptographique de la mécanique quantique, la recherche d'hypothèses alternatives est essentielle. Ces hypothèses devraient être de nature physique et raisonnables. Elles devront mettre en lumière ce que la cryptographie quantique permet en comparaison avec ce qui est permis en cryptographie classique. Il est même possible que des hypothèses calculatoires plus faibles que l'existence de fonctions à sens unique permettent la réalisation de mises en gage.

Nous devrons aussi regarder comment construire des systèmes hybrides qui peuvent utiliser des hypothèses classiques minimales en plus d'un canal quantique. Il est important d'étudier les façons d'utiliser des hypothèses calculatoires en cryptographie quantique pour voir si la combinaison des deux types de cryptographie apporte un avantage significatif par rapport au cas où seul des hypothèses de calcul sont utilisées.

Bref, les nouveaux développements sont peut-être négatifs en substance mais ils motivent de nouvelles avenues de recherche.

Bibliographie

[1] R.-J. Anderson, *Why Cryptosystems Fail*, dans les actes de l'ACM Conference in Computer and Communications Security, 1993, pp. 215–227.

[2] R. Ash , *Information Theory*, John Wiley & Sons, 1965.

[3] A. Aspect, P. Grangier et G. Roger, *Experimental realization of the Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities*, Physical Review Letters, vol. 49, no. 2, 1982, pp. 91-94.

[4] D. Beaver, *Foundations of Secure Interactive Computing*, dans les actes de CRYPTO'91, Lecture Notes in Computer Science, vol. 576, Springer-Verlag, 1992, pp. 377–391.

[5] J. S. Bell, *On the Einstein Podolsky Rosen Paradox*, Physics, vol. 1, no. 1, 1964, p. 195.

[6] C.H. Bennett et G. Brassard, *Quantum Cryptography: Public key distribution and coin tossing*, dans les actes de l'IEEE International Conference on Computers, Systems, and Signal Processing, Banglore, Inde, Décembre 1984, pp. 175–179.

[7] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W. K. Wooters, *Teleporting an Unknown Quantum State via Dual Classical and EPR Channels*, Physical Review Letters, vol. 70, no.13, 1993, pp. 1895–1899.

[8] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail et J. Smolin, *Experimental Quantum Cryptography*, Journal of Cryptology, vol. 5, no. 1, 1992, pp. 3–28.

[9] C.H. Bennett, G. Brassard, S. Breidbart et S. Wiesner, *Quantum Cryptography, or Unforgeable Subway Tokens*, dans les actes de CRYPTO'82, Plenum Press, 1983, pp. 267–275.

[10] C.H. Bennett, G. Brassard, C. Crépeau et U. Maurer, *Generalized Privacy Amplification*, dans IEEE Transaction on Information Theory, vol. 41, no. 6, novembre 1995, pp. 1915–1923.

[11] C. H. Bennett, G. Brassard et N. D. Mermin, *Quantum Cryptography without Bell's Theorem*, dans Physical Review Letters, vol. 68, no. 5, 1992, pp. 557–559.

[12] C.H. Bennett, G. Brassard et J.-M. Robert, *Privacy Amplification by Public Discussion*, dans SIAM Journal on Computing, vol. 17, no. 2, 1988, pp. 210–229.

[13] C.H. Bennett, G. Brassard, C. Crépeau et M.-H. Skubiszewska, *Practical Quantum Oblivious Transfer*, dans les actes de CRYPTO'91, Lecture Notes in Computer Science, vol. 576, Springer Verlag, Berlin, 1992, pp. 351–366.

[14] E. R. Berlekamp, R. J. McEliece et H.C.A. van Tilborg, *On the Inherent Intractability of Certain Coding Problems*, IEEE Transaction on Information Theory, vol. IT-24, no. 3, 1978, pp. 384–386.

[15] A. Berthiaume, *L'ordinateur quantique: complexité et stabilisation des calculs*, thèse de doctorat, Département d'informatique et de recherche opérationelle, Université de Montréal, Québec, 1995.

[16] A. Berthiaume, R. Jozsa et D. Deutsch. *The Stabilisation of Quantum Computation*, dans les actes de PHYSCOMP'94, IEEE Computer Society Press, Dallas, 1994, pp. 60–62.

[17] G. Brassard, *On computationally Secure Authentication Tags Requiring Short Secret Shared Keys*, Advances in Cryptology: Les actes de CRYPTO'82, Plenum Press, 1983, pp. 79–86.

[18] G. Brassard, *Modern Cryptology*, Lecture Notes in Computer Science, vol. 325, Springer-Verlag, 1988.

[19] G. Brassard et P. Bratley, *Algorithmique: conception et analyse*, Masson, Les presses de l'Université de Montréal, 1987.

[20] G. Brassard, D. Chaum et C. Crépeau, *Minimum Disclosure Proofs of Knowledge*, JCSS, vol. 37, pp. 156–189.

[21] G. Brassard, C. Crépeau, R. Jozsa et D. Langlois, *A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties*, dans les actes du 34th IEEE Symposium on Foundations of Computer Science, Novembre 1993, pp. 362–371.

[22] G. Brassard, C. Crépeau et M. Sántha, *Oblivious Transfers and Intersecting Codes*, dans IEEE Transaction on Information Theory, vol. 42, no. 6, novembre 1996, pp. 1769–1780.

[23] C. Crépeau, *Correct and Private Reductions among Oblivious Transfers*, thèse de doctorat, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1990.

[24] C. Crépeau, *Verifiable Disclosure of Secret*, dans les actes de EUROCRYPT'89, Lecture Notes in Computer Science, vol. 434, Springer-Verlag, Houthalen (Belgique), 1989, pp. 150–154.

[25] C. Crépeau, *Quantum Oblivious Transfer*, dans Journal of Modern Optics, Taylor & Francis, vol. 41, no. 12, Décembre 1994, pp. 2445–2454.

[26] C. Crépeau et J. Kilian, *Achieving Oblivious Transfer Using Weakened Security Assumptions*, dans les actes du 29th IEEE Symposium on Foundations of Computer Science, Octobre 1988, pp. 42–52.

[27] C. Crépeau et L. Salvail , *Quantum Oblivious Mutual Identification*, dans les actes de EUROCRYPT'95, Lecture Notes in Computer Science, vol. 921, Springer-Verlag, Saint-Malo (France), 1995, pp. 133–146.

[28] C. Crépeau et L. Salvail , *Oblivious Verification of Common String*, CWI quaterly, vol. 8, no. 2, 1995, pp. 97–109.

[29] C. Crépeau et M. Sántha. *Efficient Reductions Among Oblivious Transfer Protocols Based on New Self-Intersecting Codes*, dans Sequences II, Methods in Communications, Security, and Computer Science, Springer-Verlag, 1991, pp. 360–368.

[30] J. L. Carter et M. N. Wegman, *Universal Classes of Hash Functions*, Journal of Computer and System Sciences, vol. 18, 1979, pp. 143–154.

[31] J. L. Carter et M. N. Wegman, *New Hash Functions and Their Use in Authentication and Set Equality*, Journal of Computer and System Sciences, vol. 22, 1981, pp. 265–279.

[32] B. Chor, O. Goldreich, J. Håstad, J. Freidman, S. Rudich et R. Smolensky, *The Bit Extraction Problem or t–resilient Functions*, dans les actes du 26th IEEE Symposium on Foundation of Computer Science, Portland, Oregon, 1985, pp. 396–407.

[33] W. Diffie et M. E. Hellman, *New Directions in Cryptography*, IEEE Transaction on Information Theory, vol. IT-22, 1976, pp. 644–654.

[34] T. El-Gamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transaction on Information Theory IT-35, vol. 31, no. 4, 1985, pp. 469–472.

[35] A. Einstein, B. Podolski et N. Rosen, *Can Quantum-Mechanical Description of Physical Reality be Considered complete?*, Physical Review, no. 47, 1935, pp. 777–780.

[36] S. Even, O. Goldreich et A. Lempel, *A Randomized Protocol for Signing Contracts*, Communications of the ACM, vol. 28, 1985, pp. 637–647.

[37] R. Fagin, M. Naor et P. Winkler, *Comparing Information without Leaking it*, dans Communications of the ACM, vol. 39, no. 5, 1994, pp. 77–85.

[38] A. Fiat et A. Shamir. *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, A. M. Odlyzko, dans les actes de CRYPTO'86, Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 186–194.

[39] G. D. Forney, *Concatenated Codes*, M.I.T. press, 1966.

[40] R.G. Gallager, *Information Theory and Reliable Communication*, Wiley and Sons inc., 1968.

[41] O. Goldreich, S. Goldwasser et S. Micali. *How to construct random functions*, dans les actes du 25th IEEE Symposium on Foundations of Computer Science, Singer Island, 1984, pp. 464–479.

[42] J. Håstad, *Pseudo-random generation under uniform assumptions*, dans les actes du 21th ACM Symposium on Theory of Computing, Mai 1990, pp. 395–440.

[43] J. Hurby, *Smart Card with Interferometric Quantum Cryptographic Device*, dans les actes de CRYPTOGRAPHY: Policy and Algorithms international conference, Lecture Notes in Computer Science, vol. 1029, Brisbane (Australie), juillet 1995, pp. 282–289.

[44] L. P. Hughston, R. Josza et W. K. Wooters, *A Complete Classification of Quantum Ensembles Having a Given Density Matrix*, Physical Review A, vol. 183, 1993, pp. 14–18.

[45] R. Impagliazzo, L.A. Levin et M. Luby, *Pseudo-Random Generation from One-Way Functions*, dans les actes du 21th ACM Symposium on Theory of Computing, Mai 1989, pp. 12–24.

[46] R. Impagliazzo et S. Rudich, *Limits on Provable Consequences of One-Way Permutation*, dans les actes du 21th ACM Symposium on Theory of Computing, 1989, pp. 44–61.

[47] R. Jozsa et B. Schumacher, *A New Proof of The Quantum Noiseless Theorem*, Journal of Modern Optics, vol. 41, no. 12, Décembre 1994, pp. 2343–2349.

[48] E. Kranakis. *Primality and Cryptography*, John Wiley and Sons, 1986.

[49] J. Kilian. *Founding Cryptography on Oblivious Transfer*, dans les actes du 20th ACM Symposium on Theory of Computing, Chicago, 1988, pp. 20–31.

[50] H.-K. Lo et H.F. Chau, *Is Quantum Bit Commitment Really Possible?*, dans `http://xxx.lanl.gov/list/quant-ph/9603004`, 1996.

[51] D. Mayers, *Quantum Transformation and Generalized Measurements*, manuscrit, 1993.

[52] D. Mayers, *The Trouble with Quantum Bit Commitment*, dans `http://xxx.lanl.gov/list/quant-ph/9603015`, 1996.

[53] D. Mayers, *Unconditionally Secure Quantum Bit Commitment is Impossible*, dans `http://xxx.lanl.gov/list/quant-ph/9605044`, 1996.

[54] D. Mayers et L. Salvail, *Quantum Oblivious Transfer is Secure Against All Individual Measurements*, dans les actes de PHYSCOMP 94, IEEE Computer Society Press, Dallas, 1994, pp. 69–77.

[55] F. J. MacWilliams et N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[56] A. Muller, N. Gisin et H. Sbinden, *Quantum Cryptography Over 23 km in Installed Under-Lake Telecom Fiber*, Europhysics Letters, vol. 33, no. 5, février 1995, pp. 335–339.

[57] Neumark, M.A., *On a representation of additive operator set functions*, C.R. Acad. Sci. URSS 41 (9), 1943, pp. 359-361.

[58] A. Peres, *Quantum Theory: Concepts ans Methods*, Fundamental Theory of Physics, Kluwer Academic Publishers, 1993.

[59] Rabin, M. O., *How to Exchange Secrets by Oblivious Transfer*, Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.

[60] J.-M. Robert, *Détection et correction d'erreur en cryptographie*, mémoire de maîtrise, Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, Québec, 1985.

[61] R. Rivest, A. Shamir et L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, MIT/LCS/TR-212, 1979.

[62] C. E. Shannon, *A Mathematical Theory of Communication (partie I)*, Bell Syst. Tech. J., vol. 27, 1948, pp. 379–423.

[63] C. E. Shannon, *Communication Theory of Secrecy System*, Bell Syst. Tech. J., vol. 28, 1949, pp. 657–715.

[64] P. W. Shor, *Algorithms for Quantum Computation: Discrete Log and Factoring*, dans les actes du 35th ACM Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, Californie, 1994, p. 124–134.

[65] D. R. Simon, *On the Power of Quantum Computation*, dans les actes du 20th Annual Symposium on Foundations of Computer Science, novembre 1994, pp. 116–123.

[66] D. Spielman, *Linear-Times Encodable and Decodable Error-Correcting Codes*, dans les actes du 27th ACM Symposium on Theory of Computing, 1995, pp. 388–397.

[67] P. D. Townsend, J. G. Rarity et P. R. Tapster, *Single Photon Interference in a 10 km Long optical Fibre Interferometer*, Electronics Letters, vol. 29, no. 7, avril 1993, pp. 634 – 635.

[68] P. D. Townsend, J. G. Rarity et P. R. Tapster, *Enhanced single photon visibility in a 10km long prototype quantum cryptography channel*, Electronics Letters, 1995.

[69] S. Wiesner, *Conjugate Coding*, manuscrit écrit *circa* 1970; susbéquemment disponible dans SIGACT News, vol. 15, no. 1, 1983, pp. 78-88.

[70] A. C. Yao, *Quantum Circuit Complexity*, dans les actes du 34th IEEE Symposium on Foundations of Computer Science, Palo Alto, Californie, novembre 1993, pp. 352–361.

[71] A. C. Yao, *Security of Quantum Protocols Against Coherent Measurements*, dans les actes du 26th Symposium on the Theory of Computing, juin 1995, pp. 67-75.

[72] *One Less Thing to Believe In: Fraud at Fake Cash Machine*, New York Times, 13 mai 1993, pp. A1 & B9.

Remerciements

Je voudrais, en premier lieu, remercier mon directeur Claude Crépeau et mon co-directeur Gilles Brassard. Le milieu d'étude qu'ils offrent est d'une très grande richesse intellectuelle où le goût du savoir est contagieux. Mes études à l'université de Montréal sont maintenant terminées, je garderai un souvenir inestimable de ces années passées avec eux et c'est avec un peu de tristesse que j'entreprends une nouvelle étape. Je leur suis reconnaissant du bagage qu'il m'ont permis d'acquérir.

Je veux remercier mes parents pour tout ce qu'ils n'ont jamais hésité à faire pour moi pendant mes longues études. Sans leur support constant, ces années n'auraient jamais été aussi belles. Ils ont été prêts à tous les compromis pour aider à la réussite de mon entreprise. Ma reconnaissance à leur égard est sans borne.

Je tiens à remercier Julie, ma compagne, pour sa patience surhumaine. Elle a enduré ma présence d'esprit partielle et ma présence physique aléatoire pendant toutes ces années.

Merci à Dominic Mayers pour m'avoir introduit à la magie quantique. Ce que j'en sais aujourd'hui, est dû au temps qu'il a investi à me l'enfoncer dans la tête à coups de marteau.

Je remercie mes partenaire de laboratoire avec qui de multiples discussions ont pu être menées. Merci à Alain, Hervé, Jeroen et Paul. Merci aussi à Charles pour ses judicieux conseils stratégiques. Un merci particulier à André, mon confrère en exil, pour sa précieuse aide lors des derniers milles.

Sans le support financier du CRSNG, FCAR et de Gilles, il aurait été impossible de passer à travers ces trois années. Je les remercie.