Mise en gage quantique avec des variables continues

Loïck Magnin

22 août 2007

1 Introduction

La mise en gage est une primitive de cryptographie très utilisée, principalement comme brique de base pour construire des protocoles plus évolués tels que le tirage à pile ou face, par exemple. Elle intervient aussi dans des preuves de *zero knowledge* mais surtout dans des applications de partage de secret, très à la mode actuellement avec la délocalisation de données sur différents serveurs.

Son principe est simple et implique deux partis, que nous appellerons Alice et Bob pour ne pas déroger à la règle traditionnelle. Alice veut envoyer un bit codé à Bob dans un premier temps et le révéler dans un second temps. Quant à Bob, il ne veut pas qu'Alice change d'avis entre les deux phases. Ce problème a déjà fait l'objet de nombreuses études, dans les cas classiques comme quantiques.

Classiquement, la sécurité du protocole n'est que conditionnelle et s'appuie sur la difficulté non prouvée d'un problème.

Un protocole quantique, BCJL a été proposé en 1993 dans [20]. Ce protocole était supposé être inconditionnellement sûr. Or, Mayers d'une part, Lo et Chau d'autre part, ont montrés ([13][15]) qu'il n'était pas possible de faire de tels protocoles quantiques en utilisant des variables discrètes.

Ces protocoles font intervenir des communications quantiques qui peuvent être à base soit de grandeurs discrètes, soit de grandeurs continues, tout comme une communication classique peut être numérique ou analogique. Les deux méthodes ont leurs avantages et leurs inconvénients. Celles à base de variables discrètes peuvent se faire en pratique sur des distances plus longues que celles à base de variables continues, en revanche ces dernières permettent des taux de transfert (théoriques comme expérimentaux) très supérieurs. Le problème de la distance est purement technologique, gageons qu'il disparaisse dans les prochaines années.

L'objet de mon étude est l'utilisation des variables continues pour effectuer une mise en gage quantique.

Les concepts de la mise en gage et l'état de l'art avant ce rapport seront énoncés dans la première partie et le formalisme pour les variables continues dans la seconde. La rencontre entre ces deux mondes s'effectuera dans la troisième partie, où le théorème d'impossibilité est étendu aux variables continues. Dans les deux dernières parties, nous nous restreindrons à l'étude d'états particuliers, les états gaussiens. Ces états sont abondamment étudiés et des protocoles de distribution de clé ont été proposés et étudiés[1]. Parmi toutes les attaques possibles, l'attaque optimale était une attaque gaussienne. Dans la dernière partie, je montrerai, qu'étonnament, il semblerait qu'il soit possible de faire de la mise en gage gaussienne, puisque l'attaque optimale n'est pas gaussienne.

[1] Mon stage de l'année dernière concernait l'étude de la sécurité d'un tel protocole

2 Mise en gage

2.1 Principe

L'image est éculée mais trop tentante pour y résister. Alice envoie son bit dans un coffre fort, mais sans lui fournir la clé dans le premier temps. Ensuite si elle décide de révéler son bit à Bob, elle la lui envoie.

La première phase est appelée **envoi**, la seconde **révélation**.

Définition 1 *Un protocole de mise en gage est dit* ***cachant*** *si Bob ne peut pas décider quel bit Alice a mis en gage, et* ***liant*** *si Alice ne peut pas modifier ce bit après la fin de la phase d'envoi.*

2.2 Impossibilité

Avec deux approches différentes faites simultanément, D. Mayers et Lo & Chau ont montré que le protocole de mise en gage quantique BCJL n'était pas inconditionnellement sûr, c'est-à-dire à la fois liant et cachant. Pour le démontrer, ils ont donné une attaque sur le protocole.

Mais il s'est révélé que cette attaque est en fait très générale, et fonctionne sur tout protocole parfaitement cachant. Ensuite les études ont portés sur des versions plus faibles de la mise en gage où le protocole n'est plus parfaitement cachant. Dans ce cas, l'attaque reste efficace :

Théorème 1 *Tout protocole de mise en gage quantique en dimension finie, s'il permet à Bob de distinguer avec une probabilité ε le bit mis en gage par Alice, permet alors à Alice de changer son bit sans se faire détecter par Bob avec une probabilité supérieure à $1-\varepsilon$.*

La preuve dans le cas général n'est pas évidente, car de nombreux cas particuliers sont à prendre en compte. Les écueils proviennent du fait qu'il peut y avoir des communications classiques lors du protocole, et qu'il peut y avoir des mesures lors de la phase d'envoi. Plusieurs auteurs ont donné de telles preuves ([18][17]). Il reste cependant quelques sceptiques qui continuent de publier des protocoles qu'ils pensent sûrs [14].

Dans [4], d'Ariano et Al. ont étudié brièvement le cas des variables continues, sous une hypothèse très forte, les états envoyés ont une énergie bornée. Sous cette hypothèse, il est très facile de se ramener au cas discret. Sans cette restriction, la question restait ouverte. Un autre travail avait été effectué sur le sujet par Jérôme Lodewyck [21], où il s'était plutôt intéressé à la transposition du protocole BCJL en variables continues, sans se soucier de sa sécurité.

3 Variables continues en mécanique quantique

Cette partie introduit le formalisme dont nous aurons besoin pour l'étude des protocoles. Celui du cas gaussien sera introduit plus tard dans la partie 5.

3.1 Bras et kets

Dans toute la suite nous utiliserons l'espace de Hilbert $\mathcal{L}_2(\mathbb{R})$.

Définition 2 (Première définition d'un ket, définition d'un bra) *Si ψ appartient à $\mathcal{L}_2(\mathbb{R})$, alors on utilise la notation ket $|\psi\rangle$. On définit le bra $\langle\psi|$ comme une forme linéaire de $\mathcal{L}_2(\mathbb{R})$ dans $\mathbb{C}$ qui a $|\phi\rangle$ associe le complexe $\int_{\mathbb{R}} \psi(x)^*\phi(x)\mathrm{d}x$ que l'on écrit alors $\langle\psi|\phi\rangle$. $\langle\psi|$ se trouve dans le dual de $\mathcal{L}_2(\mathbb{R})$.*

La relation $|\psi\rangle \mapsto \langle\psi|$ est antilinéaire :

$$\forall \alpha \in \mathbb{C} : \alpha|\psi\rangle \mapsto \alpha^* \langle\psi|$$

À chaque ket correspond un bra, l'inverse n'est pas vrai, contrairement à la dimension finie. Par exemple au bra $\langle x_0|$:

$$\langle x_0| : \phi \mapsto \int_{\mathbb{R}} \mathrm{d}x \delta(x - x_0)\phi(x) = \phi(x_0)$$

n'est associé aucun ket.

Il est cependant possible de lui associer un vecteur dans le bidual[2] de $\mathcal{L}_2(\mathbb{R})$ qui est dans ce cas la distribution $\delta(x_0 - x)$.

Nous pouvons ainsi construire des kets généralisés pour qu'à chaque bra corresponde un ket, et *vice versa*.

Définition 3 (Seconde définition d'un ket) *Un ket est un vecteur du bidual de* $\mathcal{L}_2(\mathbb{R})$.

Certains auteurs nomment ces kets, des kets généralisés. Nous n'utiliserons ici que le terme de ket par souci de légèreté, en prenant cependant soin de les distinguer lorsqu'il y en a besoin.

Définition 4 (Produit scalaire sur $\mathcal{L}_2(\mathbb{R})$) *L'application qui à* (ψ, ϕ) *associe* $\langle\psi|\phi\rangle$ *est un produit scalaire.*

Comme pour tout espace vectoriel, la notion de base est très importante car elle permet de manipuler les vecteurs de manière plus simple. Dans la section suivante, nous allons étendre la définition d'une base (au sens de l'algèbre linéaire) à celle de base de Hilbert.

3.2 Bases

Définition 5 (Base de Hilbert) *Une base de Hilbert d'un espace* $\mathcal{L}_2(\mathbb{R})$ *est une famille de kets* $|e_i\rangle, i \in \mathcal{I}$ *qui est génératrice :*

$$vect(|e_i\rangle, i \in \mathcal{I}) \quad \text{dense} \quad \text{dans} \quad \mathcal{L}_2(\mathbb{R})$$

et libre :

$$\forall \mathcal{A} \subset \mathcal{I} \quad \text{ensemble} \quad \text{fini} \quad \sum_{i \in \mathcal{A} \subset \mathcal{I}} \lambda_i |e_i\rangle = 0 \Rightarrow \forall i \in \mathcal{A}, \lambda_i = 0$$

Si $\mathcal{I}$ est un ensemble fini, alors l'espace de Hilbert est de dimension finie.
Si $\mathcal{I}$ est en bijection avec $\mathbb{N}$, alors l'espace est de dimension infinie et la base est discrète.
Si $\mathcal{I}$ est en bijection avec $\mathbb{R}$, alors l'espace est de dimension infinie et la base est continue.

Dans toute la suite, le mot **base** sera à comprendre **base de Hilbert** et non pas base au sens de l'algèbre linéaire usuelle.

Les bases orthonormées sont de loin les plus utilisées car très facilement manipulables et ayant de bonnes propriétés, comme par exemple la relation de fermeture.

[2]En dimension infinie, le bidual n'est en général pas égal au dual, nous avons la relation $\mathcal{L}_2(\mathbb{R}) \subset \mathcal{L}_2(\mathbb{R})^{**}$. Dans notre cas, l'inclusion est stricte.

3.2.1 Base discrète orthonormée

C'est une base telle que ses éléments vérifient la relation

$$\langle e_i|e_j\rangle = \delta_{ij}$$

À tout base orthonormée correspond une relation de fermeture. Dans le cas d'une base discrète, elle s'écrit ainsi :

$$\sum_{i=0}^{\infty} |e_i\rangle\langle e_i| = \mathbb{1}$$

3.2.2 Bases continues

Dans certains cas, il est commode d'utiliser des "bases" dont les éléments n'appartiennent pas à $\mathcal{L}_2(\mathbb{R})$.

Une base orthonormée continue de $\mathcal{L}_2(\mathbb{R})$ est une base de vecteurs $\{|e_\alpha\rangle, \alpha \in \mathbb{R}\}$ tel que

$$\langle e_\alpha|e_\beta\rangle = \delta(\alpha - \beta)$$

Et la relation de fermeture s'écrit :

$$\int_{\mathbb{R}} \mathrm{d}\alpha |e_\alpha\rangle\langle e_\alpha| = \mathbb{1}$$

Tout vecteur de $\mathcal{L}_2(\mathbb{R})$ peut être indifféremment décomposé sur une base discrète ou sur une base continue. Le tableau suivant résume les correspondance dans les cas $\mathcal{L}_2(\mathbb{R}) = \mathcal{L}_2(\mathbb{R})$

	Base discrète	Base continue
Orthonormalisation	$\langle e_i\|e_j\rangle = \delta_{ij}$	$\langle e_\alpha\|e_\beta\rangle = \delta(\alpha-\beta)$
Fermeture	$\sum_{i=0}^{\infty} \|e_i\rangle\langle e_i\| = \mathbb{1}$	$\int_{\mathbb{R}} \mathrm{d}\alpha \|e_\alpha\rangle\langle e_\alpha\| = \mathbb{1}$
Décomposition	$\|\psi\rangle = \sum_{i\in\mathbb{N}} \langle e_i\|\psi\rangle\|e_i\rangle$	$\|\psi\rangle = \int_{\alpha\in\mathbb{R}} \langle e_\alpha\|\psi\rangle\|e_\alpha\rangle$

3.2.3 Exemples concrets

Une base discrète est par exemple celle de Fourier c'est l'ensemble des fonctions

$$\{x \mapsto \cos(nx), n \in \mathbb{N}\} \bigcup \{x \mapsto \sin(nx), n \in \mathbb{N}^*\}$$

Une des bases continues les plus utiles est certainement la base des distribution delta de Dirac. On note $|x_0\rangle$ la distribution $x \mapsto \delta(x - x_0)$. On remarque que $|x\rangle$ n'est pas dans $\mathcal{L}_2(\mathbb{R})$ mais que $\langle x|$ est parfaitement défini, $|x\rangle$ est donc bien un ket généralisé.

$$|\psi\rangle = \int_{\mathbb{R}} \psi(x)|x\rangle \mathrm{d}x$$

De même, il est possible de définir les fonctions qui n'appartiennent pas à $\mathcal{L}_2(\mathbb{R})$ que l'on va noter $|p\rangle$ par

$$|p\rangle : x \mapsto \frac{1}{\sqrt{2\pi N_0}} e^{\imath \frac{px}{N_0}}$$

Nous avons alors les relations $\langle p_1|p_2\rangle = \delta(p_1 - p_2)$ et $\int_{\mathbb{R}} \mathrm{d}p|p\rangle\langle p| = \mathbb{1}$

Il faut faire très attention au fait que p et x ne sont pas des variables des muettes, bien qu'elles en aient l'air.

3.3 État et matrice densité

Nous allons maintenant nous intéresser à la question : qu'est-ce qu'un état physique.

Définition 6 (État pur à un seul mode) *Un état physique est représenté par un vecteur de $\mathcal{L}_2(\mathbb{R})$ auquel nous ajoutons la condition de normalisation*

$$\langle\psi|\psi\rangle = 1$$

Chaque état physique peut aussi être représenté par sa matrice densité $\hat{\rho} = |\psi\rangle\langle\psi|$ Cette matrice est hermitienne puisque

$$\hat{\rho}^\dagger = \langle\psi|^\dagger|\psi\rangle^\dagger = |\psi\rangle\langle\psi| = \hat{\rho}$$

définie positive car

$$\forall|\phi\rangle \in \mathcal{L}_2(\mathbb{R})\langle\phi|\psi\rangle\langle\psi|\phi\rangle = |\langle\psi|\phi\rangle|^2$$

La trace d'une matrice M peut être calculée par $\sum_{i\in\mathbb{N}}\langle e_i|M|e_i\rangle$ si $(|e_i\rangle)$ est une base discrète ou $\int_{\mathbb{R}} \mathrm{d}\alpha\langle e_\alpha|M|e_\alpha\rangle$ si la base est continue. Dans les deux cas, en appliquant la relation de fermeture, la trace d'une matrice densité est égale à 1.

Par oppostion aux états purs pour lesquels les densités de probabilités sont parfaitement connues, il y a les états mélangés.

Les états mélangés sont les états pour lesquels seules des informations statistiques sont connues. Un état mélangé est le mélange statistique d'états. Il est totalement caractérisé par sa matrice densité. La notation ket n'est jamais utilisé pour un état mélangé.

Définition 7 (Matrice densité dun état mélangé) *Supposons que nous ayons un état qui peut être l'état pur $|\psi_i\rangle$ avec une probabilité statistique p_i. Alors la matrice densité $\hat{\rho}$ de cet état est donnée par la formule :*

$$\hat{\rho} = \sum_{i=1}^{n} p_i|\psi_i\rangle\langle\psi_i|$$

Insistons, un état mélangé n'est pas la superposition d'états purs, c'est simplement un mélange statistique.

Théorème 2 *Un état est un état pur si et seulement si la trace de sa matrice densité est 1.*

3.4 Opérateurs

Un opérateur est une application linéaire.

L'adjoint d'un opérateur u est noté $u^\dagger$. On dit aussi que $u^\dagger$ est le conjugué méridiens[3] de u.

Nous allons considérer deux types d'opérateurs :

- Les opérateurs unitaires $u : \mathcal{L}_2(\mathbb{R}) \mapsto \mathcal{L}_2(\mathbb{R})$ tels que $uu^\dagger = u^\dagger u = \mathbb{1}$. Ils sont inversibles, et conservent le produit scalaire ($\langle u\phi|u\psi\rangle = \langle\phi|\psi\rangle$) et sont physiquement réalisables.
- Les observables $\hat{Q}$ qui sont les opérateurs hermitiques ($\hat{Q} = \hat{Q}^\dagger$) dont leurs vecteurs propres satisfont la relation de fermeture. En dimension finie cette relation est systématiquement vérifiée, ce n'est pas le cas en dimension infinie.

[3]Suivant une tradition ancestrale des physiciens, nous confondrons allègrement hermitien et hermitique

3.5 Mesure – Action des observables

Nous allons examiner le comportement des observables. Nous allons distinguer plusieurs cas suivant si le spectre de l'observable est discret (l'observable a un nombre fini des valeurs propres ou le spectre est en bijection avec $\mathbb{N}$) ou s'il est est continu (c'est-à-dire qu'il est en bijection avec $\mathbb{R}$).

3.5.1 Si le spectre de l'observable est discret

Supposons que $\hat{Q}$ ait un spectre discret de valeurs propres q_i de degré de dégénérescence d_i auxquelles sont associés les vecteurs propres $|q_i^j\rangle$ avec $1 \leq j \leq d_i$ c'est-à-dire :

$$\hat{Q}|q_i^j\rangle = q_i|q_i^j\rangle$$

Puisque $\hat{Q}$ est une observable, nous avons alors

$$\sum_{i\in\mathbb{N}}\sum_{j=0}^{d_i}|q_i^j\rangle\langle q_i^j| = \mathbb{1}$$

L'observation (ou la mesure) d'un vecteur selon une observable comporte deux aspects :

1. La mesure d'une grandeur, c'est-à-dire l'obtention d'une valeur numérique réelle qui est nécessairement une des valeurs propres de l'observable
2. La projection de l'état mesuré sur un des vecteurs propres associé à la valeur propre mesurée.

Dans le cas où nous mesurons un vecteur propre $|q_i^j\rangle$, la mesure fournit la valeur numérique q_i et l'état du système reste inchangé.

De manière générale, si nous observons l'état $|\psi\rangle = \sum_{i\in\mathbb{N}}\sum_{i=0}^{d_i} a_{ij}|q_i^j\rangle$ nous allons transformer l'état en $|q_i^j\rangle$ avec probabilité $|a_{ij}|^2$ et la valeur mesurée sera alors q_i.

Parler de la valeur moyenne observée pour un état a un sens est vaut

$$\langle q\rangle = \sum_{i\in\mathbb{N}}\sum_{i=0}^{d_i}|a_{ij}|^2 q_i$$

Remarque : cette définition est compatible avec celle d'une observable "habituelle" en calcul quantique.

3.5.2 Si le spectre de l'observable est continu

Soit $\mathcal{S}$ le spectre de l'observable. On peut écrire $\mathcal{S} = \mathcal{S}_1 \bigcup \mathcal{S}_2$ où les valeurs propres de $\mathcal{S}_1$ sont discrètement dégérées et $\mathcal{S}_2$ où elles sont continûment dégénérées.

Avec des notations "intuitives", nous pouvons écrire les relations entre les vecteurs propres

$$\langle q_s^j|q_{s'}^{j'}\rangle = \delta(s-s')\delta(j-j')$$

ce qui nous donne la relation de fermeture suivante :

$$\int_{s\in\mathcal{S}_1}\sum_{j=0}^{d_s}|q_s^j\rangle\langle q_s^j| + \int_{s\in\mathcal{S}_2}\int_{j\in\mathcal{J}_s}|q_s^j\rangle\langle q_s^j| = \mathbb{1}$$

Il est possible de décomposer tout vecteur $|\psi\rangle$ sur cette base

$$|\psi\rangle = \int_{s\in\mathcal{S}_1}\sum_{j=0}^{d_s}\psi(s,j)|q_s^j\rangle + \int_{s\in\mathcal{S}_2}\int_{j\in\mathcal{J}_s}\psi(s,j)|q_s^j\rangle \quad (1)$$

où $\psi(s,j) = \langle q_s^j|\psi\rangle$.

Pour éviter des lourdeurs d'écriture nous allons considérer dorénavant que les valeurs propres de $\hat{Q}$ sont non dégénérées, ψ devient une fonction de la seule variable s.

La valeur moyenne observée est

$$\langle q\rangle = \int_{\mathcal{S}} q_s |\psi(s)|^2 \,\mathrm{d}s$$

3.5.3 Les observables $\hat{X}$ et $\hat{P}$

Il existe deux observables $\hat{X}$ et $\hat{P}$ de spectres continus $\mathbb{R}$ non dégénérés telles que

$$\hat{X}|x\rangle = x|x\rangle \quad \text{et} \quad \hat{P}|p\rangle = p|p\rangle \tag{2}$$

Ces deux observables ne commutent pas et leur commutateur vaut $\left[\hat{X},\hat{P}\right] = 2\imath N_0$

Le passage d'une base à l'autre se fait par une transformée de Fourier :

$$\begin{aligned} |\psi\rangle &= \int_{\mathbb{R}} \mathrm{d}x\, \psi(x)|x\rangle \\ |\psi\rangle &= \int_{\mathbb{R}} \mathrm{d}p\, \psi\,[p]\,|p\rangle \end{aligned}$$

avec $\psi\,[p] = \frac{1}{4\pi N_0}\int \mathrm{d}x\, e^{\frac{\imath p x}{2N_0}}\psi(x)$

Passer la base $|p\rangle$ à la base $|x\rangle$ est un simple changement de variables. Cependant, dans de nombreux cas, il est souvent intéressant mathématiquement d'avoir l'existence simultanée des deux variables p et x ; mais il faut se souvenir que ce n'est qu'un outils mathématique.

Les valeurs moyennes $\langle x\rangle$ et $\langle p\rangle$ valent :

$$\begin{aligned} \langle x\rangle &= \int_{\mathbb{R}} x|\psi(x)|^2 \,\mathrm{d}x \\ \langle p\rangle &= \int_{\mathbb{R}} p|\psi[p]|^2 \,\mathrm{d}p \end{aligned}$$

3.6 Espace des phases

Avec le formalisme jusque là, un état physique est décrit par une fonction de $\mathbb{R}$ dans $\mathbb{C}$. Nous allons maintenant introduite l'espace des phase qui va permettre de décrire ce même état mais avec une fonction de $\mathbb{R}\times\mathbb{R}$ dans $\mathbb{R}^+$. Quel en est l'intérêt ? Pour le comprendre, faisons une analogie, retournons dans une réalité quotidienne, utilisons des objets classiques et non quantiques.

Supposons que nous voulons décrire le mouvement d'un mobile ponctuel sur une droite. Nous avons plusieurs représentations possibles. La plus intuitive, c'est de donner sa position $x = x_0$ et sa vitesse $p = p_0$. Ce mobile peut être représenté par un point de coordonnés (x_0, p_0) dans le plan (xOp). Ce plan est appelé plan de phase. Une autre méthode, moins intuitive, est de représenter l'état de ce mobile par la fonction $\psi : x \mapsto e^{-\frac{(x-x_0)^2}{2} - \imath p_0 x}$ est de dire que sa position est le centre de la gaussienne $x \mapsto |\psi(x)|^2$ qui est donc bien x_0 et que sa vitesse est le centre de la gaussienne $p \mapsto |\psi[p]|^2$ où $f[p]$ est la transformée de Fourier de ψ qui vaut p_0.

Évidement, dit comme cela, cette représentation ne semble pas avoir d'intérêt, mais pourtant, c'est bien celle que nous venons d'introduire depuis le début de la partie 3. En classique parler d'un mobile localisé avait un sens, en quantique cela n'en a pas, le mieux que l'on puisse faire, c'est de parler de la densité de probabilité de l'abscisse et de la vitesse. Toute ces informations sont contenues dans le vecteur $|\psi\rangle$.

Comme pour le mobile ponctuel à une dimension, il est possible de définir un espace des phase pour un ket :

Définition 8 (Espace des phases) *L'espace des phases est l'espace dans lequel on représente la densité de probabilité de mesurer un ket selon deux observables conjuguées.*

Dans notre cas, les variables sont x et p.

Pour pouvoir représenter un état dans le plan de phase, il faudrait représenter une nappe, ce qui n'est pas facile. La solution est d'utiliser des lignes de niveau, ou même plus simplement, une seule ligne de niveau. Si l'état est décrit par la fonction $\psi : x \mapsto e^{-\frac{(x-x_0)^2}{2} - \imath p_0 x}$ qui est une gaussienne à deux dimensions centrée en x_0, p_0 de même écart type, on le représentera dans le plan de phase xOp par un cercle de centre x_0, p_0.

L'utilisation de l'espace de phase permet souvent d'alléger les calculs et de faire des représentations visuelles de phénomènes quantiques complexes. La représentation dans l'espace des phases est équivalente à celle en utilisant uniquement les fonctions d'onde.

3.7 États à plusieurs modes

3.7.1 Définitions

Pour faire simple, le mode est aux variables continues ce que le qubit est aux variables discrètes.

Jusqu'à présent nous avons uniquement considérés des systèmes à un seul mode, c'est à dire que nous pouvons écrire sur la base $\{|x\rangle\}$. Or il est possible d'utiliser des systèmes plus complexes composés de n systèmes à 1 mode.

Le produit tensoriel de deux systèmes monomodaux est :

$$\begin{aligned} |\phi\rangle \otimes |\psi\rangle &= \int \mathrm{d}x\, \phi(x)|x\rangle \otimes \int \mathrm{d}x\, \psi(x)|x\rangle \\ &= \iint \mathrm{d}x\, \mathrm{d}y\, \phi(x)\psi(y)|x\rangle|y\rangle \end{aligned}$$

avec la condition de normalisation

$$\langle\psi|\psi\rangle \otimes \langle\phi|\phi\rangle = \iint \mathrm{d}x\, \mathrm{d}y\, \phi^*(x)\psi^*(y)\phi(x)\psi(y) = 1$$

De manière générale, pour un état pur intriqué, un système à deux modes s'écrira :

$$|\psi\rangle = \iint \mathrm{d}x\, \mathrm{d}y\, \psi(x,y)|x\rangle|y\rangle$$

avec $\iint \mathrm{d}x\, \mathrm{d}y\, \psi^*(x,y)\psi(x,y) = 1$

Cette méthode permet de construire par récurrence des états à n modes qui s'écrivent donc

$$|\psi\rangle = \int \cdots \int_{\mathbb{R}^n} \mathrm{d}x_1 \ldots \mathrm{d}x_n\, \psi(x_1, \ldots, x_n)|x_1\rangle \cdots |x_n\rangle$$

3.7.2 Trace partielle

Chaque mode est "codé" sur un système physique qui lui est propre. Ainsi deux personnes (Alice et Bob) peuvent se partager un état à n modes : Alice possède possède les n_A premiers modes et Bob les n_B suivants ($n_A + n_B = n$).

Les modes que possèdent Bob ne peuvent pas être décrit par un ket, seul un état pur le peut, c'est-à-dire l'ensemble des n modes.

Et c'est là que nous voyons l'intérêt des matrices densités. L'ensemble est décrit par la matrice densité $\hat{\rho}$, et les modes que possèdent Alice par une matrice densité partielle $\hat{\rho}^A$ que l'on calcule à partir de $\hat{\rho}$. Ce calcul est la trace partielle.

Définition 9 (Trace partielle) *La matrice densité $\hat{\rho}^A$ de l'état d'Alice est donné par la formule*

$$\hat{\rho}^A = tr_B\hat{\rho} = \left(\langle x_{n_A+1}| \cdots \langle x_n|\right) \hat{\rho} \left(|x_{n_A+1}\rangle \cdots |x_n\rangle\right)$$

Deux états purs différents peuvent avoir la même trace partielle, cela signifie qu'Alice ne peut distinguer à partir des modes qu'elle possède quel est l'état pur. Nous commençons à apercevoir l'intérêt de la trace partielle pour la mise en gage. Si deux états purs différents ont la même matrice densité partielle pour Bob, alors Bob ne pourra pas savoir lequel des deux états Alice a préparer. Dans ce cas, le protocole sera parfaitement cachant.

3.8 Fidélité

Il est nécessaire de savoir quantifier la proximité de deux états lorsque l'on connaît leurs matrice densité. Il y a plusieurs solutions pour cela. Il y a tout un choix de normes disposition (qui *a priori* ne sont pas toutes équivalentes en dimension infinie). Nous n'allons pas utiliser une norme mais la fidélité.

Définition 10 (Fidélité) *La fidélité de deux états A et B (purs ou non) décrits par les matrices densité $\hat{\rho}_A$ et $\hat{\rho}_B$ est la probabilité que pouvoir distinguer A et B en effectuant la mesure optimale.*

Nous avons alors les propriétés suivantes :
- $0 \leq F(\hat{\rho}_A, \hat{\rho}_B) \leq 1$
- $F(\hat{\rho}_A, \hat{\rho}_B) = 1$ si et seulement si $\hat{\rho}_A = \hat{\rho}_B$

4 Théorème d'impossibilité

Je ne traiter pas dans ce rapport tous les cas possibles et imaginables, j'expose uniquement le cœr de la preuve dans le cas où le protocole est cachant. Nous allons voir pourquoi il n'est pas liant.

4.1 En dimension finie

Si Alice veut mettre en gage 0, alors elle prépare un état $|\psi_0\rangle = \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij}|i\rangle|j\rangle$ et si elle veut mettre en gage 1 elle prépare un autre état $|\psi_0\rangle = \sum_{i=1}^n \sum_{j=1}^n \beta_{ij}|i\rangle|j\rangle$ où $|i\rangle\{\}$ et $|i\rangle\{\}$ sont des bases orthonormées.

calculons de deux manières la matrice densité partielle de Bob à la fin de la première phase. Commençons par le calcul direct :

$$\begin{aligned}
\hat{\rho_0}^B &= \sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij}^* \langle a_k|a_i\rangle|a_j\rangle \sum_{l=1}^n \sum_{m=1}^n \alpha_{ij}\langle b_m|\langle a_l|a_k\rangle \\
&= \alpha_{ij}^*\alpha_{im}|b_j\rangle\langle b_m|
\end{aligned}$$

La seconde méthode utilise la décomposition de Schmidt qui s'énonce dans le cas fini ainsi :

Théorème 3 *Tout état pur $|\psi\rangle = \sum_{i,j=1}^n \alpha_{ij}|i\rangle|j\rangle$ peut s'écrire*

$$|\psi\rangle = \sum_{i=1}^n \sqrt{\lambda_i}|a_i\rangle|b_i\rangle$$

où les $|a_i\rangle\{\}$ et $|a_i\rangle\{\}$ sont des bases orthonormées.

Donc $|\psi_0\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i}|a_i\rangle|b_i\rangle$.

Calculons la trace partielle à partir de cette expression :

$$tr_A|\psi_0\rangle\langle\psi_0| = \sum_{i=1}^{n} \lambda_i|i\rangle\langle i|$$

On procède de même pour $|\psi_1\rangle$ et l'égalité entre les deux méthodes donne :

$$|\psi_0\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i}|a_i\rangle|b_i\rangle$$

$$|\psi_1\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i}|a'_i\rangle|b_i\rangle$$

La transformation : $T : |a_i\rangle \mapsto |a'_i\rangle$ est un changement de base orthonormée elle est donc unitaire et

$$(T \otimes \mathbb{1})|\psi_0\rangle = |\psi_1\rangle$$

Nous pouvons maintenant déduire l'attque. Lors de la première phase Alice se comporte honnêtement comme si elle voulait mettre en gage le bit 0. Si elle veut révéler 0, alors elle continue honnêtement. En revanche, si elle veut révéler 1, elle applique la transformation T de son côté uniquement.

4.2 Dans le cas continu

Nous allons maintenant étendre le théorème d'impossibilité aux variables continues :

Théorème 4 *Il n'existe pas de protocole de mise en gage quantique inconditionnellement sûr, même en utilisant des variables continues.*

Le schéma de la preuve est identique à celui du cas fini. Il suffit de prouver le théorème de la décomposition de Schmidt dans le cas continu.

Théorème 5 *Soit un état* $|\psi\rangle = \int_{\mathbb{R}\times\mathbb{R}} \mathrm{d}x\mathrm{d}y\psi(x,y)|x\rangle|y\rangle$ *de* $\mathcal{L}_2(\mathbb{R}) \otimes \mathcal{L}_2(\mathbb{R})$. *Il existe une base orthonormée de* $\mathcal{L}_2(\mathbb{R})$ $(|\phi_i\rangle, i \in \mathbb{N})$ *et des réels positifs* λ_i *tels que*

$$|\psi\rangle = \sum_{i\in\mathbb{N}} \sqrt{\lambda_i}|\phi_i\rangle\langle\phi_i| \tag{3}$$

Bien que plusieurs fois utilisé dans des publications [22][23], la décomposition de Schmidt n'avait jamais été prouvée rigoureusement dans le cas continu. Certains auteur n'indiquent pas de référence lorsqu'ils l'utilisent, d'autres citent des articles qui ne possèdent que la preuve dans le cas fini. Il n'était d'ailleurs pas évident que l'extension aux variables continues soit valide car [12] ont publiés ce qu'ils pensait être un contre-exemple[4]. J'ai donc fait une preuve du théorème dans le cas continu.

Preuve : nous allons calculer la trace partielle de la matrice densité de deux manières différentes puis égaliser les résultats, ce qui va nous donner ce que nous souhaitons.

Calculons la trace partielle de sa matrice densité directement

$$\begin{aligned}
\hat{\rho}^A &= tr_B|\psi\rangle\langle\psi| \\
&= \int \mathrm{d}t\langle t| \int \mathrm{d}x_1\mathrm{d}y_1\psi(x_1,y_1)|x_1\rangle|y_1\rangle \int \mathrm{d}x_2\mathrm{d}y_2\psi(x_2,y_2)^*\langle x_2|\langle y_2||t\rangle \\
&= \int \mathrm{d}t \int \mathrm{d}x_1\mathrm{d}x_2|x_1\rangle\langle x_2| \int \mathrm{d}y_1\psi x_1, y_1\langle t|y_1\rangle \int \mathrm{d}y_2\psi^* x_2, y_2\langle y_2|t\rangle \\
&= \int \mathrm{d}t \int \mathrm{d}x_1\mathrm{d}x_2|x_1\rangle\langle x_2|\psi(x_1,t)\psi^*(x_2,t) \\
&= \int \mathrm{d}x_1\mathrm{d}x_2 \int \mathrm{d}t\psi(x_1,t)\psi^*(x_2,t)|x_1\rangle\langle x_2|
\end{aligned}$$

[4] Mais leur article s'est révélé faux

L'interversion des intégrales est licite puisque ψ est une fonction de carrée sommable.

On pose alors la fonction ρ^A définie ainsi : $\rho^A(x,y) = \int \mathrm{d}t \psi(x,t)\psi^*(y,t)$ ce qui permet d'écrire en renommant les variables

$$\hat{\rho}^A = \int \mathrm{d}x\mathrm{d}y \rho^A(x,y)|x\rangle\langle y|$$

et l'on remarque que $\hat{\rho}^A$ est de carré intégrable, hermitienne et définie positive. D'après le théorème de Hilbert-Schmidt pour les $\mathcal{L}_2$-noyaux hermitiens

$$\hat{\rho}^A(x,y) = \sum_{i=0}^{\infty} \lambda_i \phi_i(x)\phi_i^*(y) \tag{4}$$

où $\{|\phi_i\rangle, i \in \mathbb{N}\}$ est une base orthonormée de $\mathcal{L}_2(\mathbb{R})$ et les λ_i sont des réels positifs.

$$\begin{aligned}
\hat{\rho}^A &= \int \rho^A(x,y)|x\rangle\langle y| \\
&= \int \sum_{i=0}^{\infty} \lambda_i \phi_i(x)|x\rangle\langle y|\phi_i^*(y) \\
&= \sum_{i=0}^{\infty} \lambda_i |\phi_i\rangle\langle\phi_i|
\end{aligned}$$

En appliquant $\sum_{i=0}^{\infty} |\phi_i\rangle\langle\phi_i| \otimes \mathbb{1}$ à $|\psi\rangle$, nous obtenons :

$$\begin{aligned}
|\psi\rangle &= \sum_{i=0}^{\infty} |\phi_i\rangle \int \psi(x,y)\langle\phi_i|x\rangle \otimes |y\rangle \\
&= \sum_{i=0}^{\infty} |\phi_i\rangle \otimes \left(\int \psi(x,y)\phi_i(x)|y\rangle \right) \\
&= \sum_{i=0}^{\infty} |\phi_i\rangle \otimes |b_i\rangle
\end{aligned}$$

où les $|b_i\rangle$ n'ont aucune raison d'être orthogonaux entre eux. Il sont parfaitement définis, il suffit d'utiliser l'inégalité de Schwarz pour s'en convaincre.

Calculons $\hat{\rho}^A$ à partir de cette écriture

$$\begin{aligned}
\hat{\rho}^A &= tr_B \sum_{i,j=0}^{\infty} |\phi_i\rangle\langle\phi_i| \otimes |b_i\rangle\langle b_i| \\
&= \sum_{k=0}^{\infty} \sum_{i,j=0}^{\infty} \langle\phi_k|b_i\rangle\langle b_j|\phi_k\rangle|\phi_i\rangle\langle\phi_i| \\
&= \sum_{i,j=0}^{\infty} \langle b_j| \left(\sum_{k=0}^{\infty} |\phi_k\rangle\langle\phi_k| \right) |b_i\rangle|\phi_i\rangle\langle\phi_i| \\
&= \sum_{i,j=0}^{\infty} \langle b_j|b_i\rangle|\phi_i\rangle\langle\phi_i|
\end{aligned}$$

En comparant les résultats des deux méthodes de calcul, nous obtenons

$$\langle b_i|b_j\rangle = \sqrt{\lambda_i}\delta_{ij}$$

Ce qui prouve le théorème. □

5 Les états gaussiens

Les états gaussiens, sont des états qui jouent un rôle particulier. Il sont très étudiés en physique puisqu'ils existent naturellement[5], ils sont stables, fortement utilisés expérimentalement, et cerise sur le gâteau, une mathématisation relativement simple.

Dans cette section, nous allons introduire les concepts fondamentaux pour manipuler les états gaussiens, et nous nous intéresserons dans la section suivante aux protocoles de mise en gage n'utilisant que ces états et des transformations gaussiennes.

5.1 Matrice de covariance

La définition des états gaussiens fait intervenir les matrices de covariance.

Définition 11 *La matrice de covariance des variables $(\nu_1, \ldots, \nu_n) = \nu$ est une matrice K de taille $n \times n$ dont les coefficients sont ainsi définies :*

$$K_{ij} = E\left((\nu_i - E(\nu_i))(\nu_j - E(\nu_j))\right)$$

Les coefficients diagonaux sont en fait des variances : $E\left((\nu_i - E(\nu_i))^2\right) = var(\nu_i)$.

Les matrices de covariance sont des matrices symétriques réelles semi définies positives. De plus il est possible de prouver la réciproque.

Théorème 6 *Les matrices de covariance sont les matrices symétriques réelles semi-définies positives.*

Dans le cas où toutes les variances sont non nulles, alors la matrice est définie positive. Dans toutes la suite, c'est dans ce sens là qu'il faut comprendre la terme de matrice de covariance.

5.2 Fonction de Wigner

Les états gaussiens ont un formalisme particulièrement élégant dans l'espace des phases grâce à la fonction de Wigner. Cette fonction correspond à la distribution de probabilité, dans l'espace des phases, d'un état quantique $\hat{\rho}$.

La fonction de Wigner d'un état $\hat{\rho}$ à n modes est donnée par :

$$W_{\hat{\rho}}(\xi) = \frac{1}{(4\pi N_0)^n} \int \mathrm{d}q_1 \ldots \mathrm{d}q_n e^{\frac{\imath \sum_{i=1}^n x_i p_i}{2N_0}} \langle x_1 - \frac{q_1}{2}, \ldots, x_n - \frac{q_n}{2} | \hat{\rho} | x_1 + \frac{q_1}{2}, \ldots, x_n + \frac{q_n}{2} \rangle$$

avec $\xi = (x_1, p_1, \ldots, x_n, p_n)$.

Cette définition permet de définir la fonction d'un état pur ou mélangé.

La fonction de Wigner permet en réalité de faire une tomographie dans l'espace des phases. Pour connaître la densité de probabilité d'une variable, il suffit d'intégrer la fonction de Wigner sur toutes les autres. Par exemple la densité de probabilité de x_i d'un état pur $|\psi\rangle$ est

$$|\psi(x_i)|^2 = \int \mathrm{d}x_1 \ldots \mathrm{d}x_{i-1}\, \mathrm{d}x_{i+1} \ldots \mathrm{d}p_1 \ldots \mathrm{d}p_n\, W_{|\psi\rangle\langle\psi|}(\xi) \tag{5}$$

À partir de maintenant nous fixons $N_0 = 1$. Nous ne perdons pas en généralité car N_0 est simplement un facteur d'échelle.

[5] état d'une particule au repos, état de la lumière à la sortie d'un laser, par exemple

5.3 États gaussiens

Voici deux définitions équivalentes d'un état gaussien, pur ou mélangé :

Définition 12

$$\forall \xi, W_{\hat{\rho}}(\xi) \geq 0$$

Définition 13

$$W_{\hat{\rho}}(\xi) = \frac{1}{(2\pi)^n \sqrt{\det K}} e^{-\frac{1}{2}(\xi-\mu)K^{-1}(\xi-\mu)^\top}$$

avec K matrice de covariance et μ un vecteur de $\mathbb{R}^{2n}$.

$det(K) = 1$ pour un état pur.

Il est toujours possible, par à un changement de base astucieux de considérer uniquement les matrices K telles que $[K]_{x_i,p_j} = 0$.

Le nom "état gaussien" vient du fait de la forme quadratique dans l'exponentielle. Un état gaussien à n modes est défini par $4n^2+2n$ coefficients réels. Ceux de la matrice de covariance, qui donnent la variance des gaussiennes et ceux du vecteur μ qui sont les coordonnées du sommet de la gaussienne. On dit que la gaussienne est *centrée* en μ.

Exemple simple d'un état gaussien à un mode défini, centré en 0 et de matrice de covariance

$$K = \begin{bmatrix} \sigma_x^2 & \sigma_{xp}^2 \\ \sigma_{xp}^2 & \sigma_p^2 \end{bmatrix}$$

Nous avons donc

$$K^{-1} = \frac{1}{\sigma_x^2\sigma_p^2 - \sigma_{xp}^4} \begin{bmatrix} \sigma_p^2 & -\sigma_{xp}^2 \\ -\sigma_{xp}^2 & \sigma_x^2 \end{bmatrix}$$

Calculons la densité de probabilité de la variable x :

$$\begin{aligned} P_r(x) &= \int_{\mathbb{R}} \mathrm{d}p \, \frac{1}{2\pi\sqrt{\sigma_x^2\sigma_p^2 - \sigma_{xp}^4}} e^{-1/2\begin{bmatrix} x & p \end{bmatrix} K^{-1} \begin{bmatrix} x \\ p \end{bmatrix}} \\ &= \frac{1}{\sqrt{2\pi}\sigma_x} e^{-\frac{x^2}{2\sigma_x^2}} \end{aligned}$$

Ce résultat est donc conforme aux attentes puisque σ_x^2 est bien la variance de la variable x.

5.4 Trace partielle

La fonction de Wigner de la trace partielle sur les modes $j+1, \ldots, n$ d'un état décrit par une fonction de Wigner se calcule par intégration :

Définition 14

$$W_{Tr_{j+1,\ldots,n}(\hat{\rho})}(x_1, p_1, \ldots, x_j, p_j) = \int \mathrm{d}x_{j+1} \, \mathrm{d}p_{j+1} \, \mathrm{d}x_n \, \mathrm{d}p_n \, W_{\hat{\rho}}(\xi)$$

5.5 Fidélité

Définition 15 *Soient deux états gaussiens purs caractérisés par μ_1, K_1 et μ_2, K_2 respectivement. La fidélité de ces deux états est donnée par :*

$$\mathcal{F} = \frac{1}{\pi^n} \int \mathrm{d}\xi e^{-\frac{1}{2}\left((\xi-\mu_1)K_1^{-1}(\xi-\mu_1)^\top + (\xi-\mu_2)K_2^{-1}(\xi-\mu_2)^\top\right)}$$

Dans le cas où $\xi_1 = \xi_2$, la fidélité prend une forme particulièrement jolie :

$$\frac{2^n}{\sqrt{det(K_0^{-1} + K_1^{-1})}} \tag{6}$$

5.6 Transformations gaussiennes

Définition 16 (Transformation gaussienne) *Les transformations gaussiennes sont les applications linéaires qui transforment un état gaussien en un autre état gaussien. Elles ont l'énorme avantage d'être facilement réalisables.*

Pour les caractériser, nous avons besoin d'introduire quelques notion supplémentaires :

Définition 17 *Une matrice symplectique S de dimension $2n \times 2n$ est une matrice qui vérifie la propriété suivante :*

$$S^\top \Omega S = \Omega$$

où Ω est une matrice diagonale bloc de taille $2n \times 2n$ définie par

$$\Omega = \begin{bmatrix} 0 & 1 & & & 0 \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ 0 & & & -1 & 0 \end{bmatrix}$$

Théorème 7 *Une transformation gaussienne d'un état à n modes est décrite par une matrice symplectique de taille $2n \times 2n$. Son action sur un état (pur ou non) dont les paramètres sont (K, μ) est calculée ainsi :*

$$M : (K, \mu) \mapsto (M^\top K M, M\mu)$$

Il existe 3 transformations gaussiennes élémentaires : C-NOT$_\kappa$, diviseur de faisceaux[6] et compresseur[7]. C-NOT$_\kappa$ et le diviseur de faisceaux agissent sur deux modes. Leurs matrices sont respectivement :

$$CNOT_\kappa = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\kappa \\ \kappa & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{et} \quad R_\theta = \begin{bmatrix} \cos\theta & 0 & -\sin\theta & 0 \\ 0 & \cos\theta & 0 & -\sin\theta \\ \sin\theta & 0 & \cos\theta & 0 \\ 0 & \sin\theta & 0 & \cos\theta \end{bmatrix}$$

Le compresseur agit sur un mode et sa matrice est

$$\begin{bmatrix} s & 0 \\ 0 & 1/s \end{bmatrix}$$

5.6.1 Propriétés des matrices symplectiques

- $\det T = 1$
- $T^\top$ et T^{-1} sont aussi symplectiques
- Si T agit sur K, alors ${T^{-1}}^\top$ agit sur K^{-1}

Théorème 8 (Décomposition d'Isawa) *Toute matrice symplectique T peut se décomposer de manière unique à l'aide de ses 3 matrices :*

$$T = CNOT_\kappa \cdot S_s \cdot R_\theta$$

Une preuve de ce théorème, ainsi qu'une étude complète du groupe symplectique se trouve dans [2].

[6] Beam-splitter en anglais
[7] squeezer

5.7 Création d'une paire EPR avec des états gaussiens

À titre d'exemple, pour manipuler un peu tout ce formalisme, avant de l'utiliser dans le cas de la mise en gage, regardons comment on peut faire une paire EPR avec des états à variables continues.[8]

Considérons deux états gaussiens identiques, non corrélés de variances $N_0 = 1$, et centrés en 0. Le système est décrit par la matrice de covariance

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Comprimons le premier mode en x et le second en p par le même facteur de compression s. L'état devient :

$$\begin{bmatrix} s & 0 & 0 & 0 \\ 0 & 1/s & 0 & 0 \\ 0 & 0 & 1/s & 0 \\ 0 & 0 & 0 & s \end{bmatrix}$$

"Mélangeons" alors ces modes grâce à un diviseur de faisceau d'angle $\theta = \frac{\pi}{4}$:

$$K = \frac{1}{2} \begin{bmatrix} s+1/s & 0 & -s+1/s & 0 \\ 0 & s+1/s & 0 & s-1/s \\ -s+1/s & 0 & s+1/s & 0 \\ 0 & s-1/s & 0 & s+1/s \end{bmatrix}$$

dont l'inverse est :

$$K^{-1} = \frac{1}{2} \begin{bmatrix} s+1/s & 0 & s-1/s & 0 \\ 0 & s+1/s & 0 & -s+1/s \\ s-1/s & 0 & s+1/s & 0 \\ 0 & -s+1/s & 0 & s+1/s \end{bmatrix}$$

La fonction de Wigner de cet état vaut :

$$W(x_1, p_1, x_2, p_2) = \frac{1}{(2\pi N_0)^2} e^{-\frac{(x_1-x_2)^2}{4sN_0} - \frac{s(p_1-p_2)^2}{4N_0} - \frac{s(x_1+x_2)^2}{4N_0} - \frac{(p_1+p_2)^2}{4sN_0}}$$

Dans la limite des forts facteurs de compression $s \to 0$, la fonction de Wigner devient :

$$W(x_1, p_1, x_2, p_2) \to \delta(x_1 - x_2)\delta(p_1 + p_2)$$

6 Étude du cas gaussien

Nous allons maintenant restreindre le problème au cas gaussien. Voici le résultat que je vais montrer :

Théorème 9 *Pour tout $\varepsilon' > 0$, il existe deux états gaussiens à 2 modes $|\psi_0\rangle$ et $|\psi_1\rangle$ tels que $tr_A(|\psi_1\rangle\langle\psi_1|) = tr_B(|\psi_0\rangle\langle\psi_0|)$ et quelle que soit la transformation gaussienne $T = T_A \otimes \mathbb{1}$, $F(|T\psi_0\rangle\langle T\psi_0|, |\psi_1\rangle\langle\psi_1|) < \varepsilon'$.*

Cela montre qu'il est *presque* possible de faire un protocole de mise en gage quantique à base d'états gaussiens. Pour compléter la preuve il reste deux autre cas à étudier :

[8] D'autres résultats comme la téléportation et le codage dense ont aussi leur équivalent en continu. Pour être honnête, la paire EPR dans le papier original est présenté avec des variables continues.

– Alice prépare un état différent de $|\psi_0\rangle$ et effectue soit une transformation T_0 si elle veut envoyer 0, soit une transformation T_1 si elle veut mettre en gage 1. Cette étude ne semble pas trop difficile.
– Alice prépare un état à plus de $n > 2$ modes. Elle a de son côté $n-1$ modes et peut faire sur ces modes des transformations plus complexes que sur un mode. Cette étude est plus dure.

Les deux prochaines sous-parties sont la preuve du théorème.

6.1 Étude des états

Pour montrer ce résultat, il suffit d'exhiber de tels états. La manière dont j'ai trouvé ces deux états est détaillée en annexe 6.2. Ils sont tout deux centrés en 0 et voici l'inverse de leurs matrices de covariance :

$$K_0^{-1} = \begin{bmatrix} \frac{1}{\varepsilon} & 0 & \sqrt{\frac{1}{\varepsilon^2} - \varepsilon^2} & 0 \\ 0 & \frac{1}{\varepsilon} & 0 & 0 \\ \sqrt{\frac{1}{\varepsilon^2} - \varepsilon^2} & 0 & \frac{1}{\varepsilon} & 0 \\ 0 & 0 & 0 & \frac{1}{\varepsilon} \end{bmatrix}$$

$$K_1^{-1} = \begin{bmatrix} \frac{1}{\varepsilon^5} & 0 & 0 & 0 \\ 0 & \varepsilon^3 & 0 & \sqrt{\frac{1}{\varepsilon^2} - \varepsilon^2} \\ 0 & 0 & \varepsilon^3 & 0 \\ 0 & \sqrt{\frac{1}{\varepsilon^2} - \varepsilon^2} & 0 & \frac{1}{\varepsilon^5} \end{bmatrix}$$

Le calcul des traces partielles donne :

$$K_0^{B^{-1}} = K_0^{B^{-1}} = \begin{bmatrix} \varepsilon^3 & 0 \\ 0 & \frac{1}{\varepsilon} \end{bmatrix}$$

Il n'est pas nécessaire de vérifier que Bob peut distinguer les deux états. Il suffit de prendre $T = \mathbb{1}$ pour la transformation gaussienne. Cependant pour pouvoir comparer la "perte" de précision que provoque la meilleure attaque, c'est utile de connaître ce résultat.

$$F(\hat{\rho_0}^A, \hat{\rho_1}^A) = \frac{4\varepsilon^6}{1 + \varepsilon^4 + 2\varepsilon^8} = 4\varepsilon^6 + \mathcal{O}(\varepsilon^{10})$$

6.2 Étude des attaques

De manière générale, l'attaque est décrite par une matrice

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \lambda & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \cos\theta & \sin\theta & 0 & 0 \\ -\sin\theta & \cos\theta & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} s & 0 & 0 & 0 \\ 0 & 1/s & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

D'après la formule 6, nous allons nous intéresser au déterminant de $T^\top K_0^{-1} T + K_1^{-1}$. Alice veut maximiser la fidélité, c'est à dire minimiser ce déterminant. C'est un polynôme de degré 2 en λ qui a la forme :

$$det(T^\top K_0^{-1} T + K_1^{-1} = f_\varepsilon(\theta, s)\lambda^2 + g_\varepsilon(\theta, s)\lambda + h_\varepsilon(\theta, s)$$

Puisque la fidélité est comprise entre 0 et 1, $f_\varepsilon(\theta, s) > 0$ et ce polynôme n'a pas de racine réelle (sinon la fidélité serait infinie). Le déterminant à sa valeur minimal au "sommet" de la parabole d'abscisse $\frac{-g_\varepsilon}{2f_\varepsilon}$:

$$\lambda = \frac{\cos\theta - s\sin\theta}{\sin\theta - s\cos\theta}$$

Le déterminant est 2π-périodique. Nous l'étudions donc sur $[0, 2\pi]$. En dérivant par rapport à θ, nous ne trouvons qu'un seul minimum en

$$\theta = \arctan(1/s)$$

Nous nous sommes ramené à un seul paramètre. Nous procédons de même en dérivant par rapport à s et nous trouvons un seul minimum en

$$s = \frac{1}{2}\frac{\sqrt[4]{8+8\varepsilon^4}}{\varepsilon^3}$$

qui vaut

$$F = \frac{2\varepsilon^4\sqrt[4]{2+2\varepsilon^4}\sqrt{\sqrt{2+2\varepsilon^4}+2\varepsilon^6}}{\sqrt{1+3\varepsilon^4+3\varepsilon^8+7\varepsilon^{12}+6\varepsilon^{16}+(3\varepsilon^6+4\varepsilon^{10}+\varepsilon^{14}+2\varepsilon^{18})\sqrt{2+2\varepsilon^4}}} = 2\sqrt{2}\varepsilon^4+\mathcal{O}(\varepsilon^8)$$

Le théorème est prouvé en prenant $\varepsilon' = F$. □

Conclusion

J'ai obtenu deux résultats principaux lors de ce stage. Le premier est l'extension du théorème d'impossibilité de faire de la mise en gage quantique inconditionnellement sûr. Une étude importante reste à faire dans cette voie, c'est l'étude des protocoles ε-cachants. L'idée de base est celle-ci : peut-être qu'en permettant à Bob une faible probabilité de distinguer les états codant 0 et 1, il devient alors impossible à Alice d'effectuer une transformation efficace de son côté pour tricher. Je pense que tout comme dans le cas fini cela n'est pas possible.

Le second résultat important est celui de la partie 6. Il reste un bout de la preuve, mais j'ai bon espoir que le protocole résiste encore, c'est dans cette optique là qu'ont été choisies les matrices de covariance.

Le tirage à pile ou face est une version faible de la mise en gage. Dans le cas fini il existe un biais qui permet à un des deux joueurs de tricher. Il serait bien d'étudier ce biais dans le cas continu (s'il existe) pour voir s'il ne serait pas plus faible, et ainsi de construire un meilleur algorithme.

La principale difficulté lors de ce stage fut la modélisation de la physique. Malgré mon stage de l'année dernière, il me manquait encore une vision d'ensemble du domaine, j'ai donc du faire beaucoup de bibliographie et la formalisation ainsi présentée, et particulièrement celle des états gaussiens a nécessité un long travail car il n'est fait dans aucun papier. J'ai rencontré Frédéric Grosshans qui a travaillé au laboratoire d'optique quantique d'Orsay sur la distribution de clé, et Jérôme Lodewyck au laboratoire de physique de l'ENS Cachan qui avait fait son stage de master sur la réalisation expérimentale d'un protocole de mise en gage quantique avec des variables continues. Une autre piste est aussi à explorer de ce côté. Comme il y a une formalisation simple et de haut niveau pour les informaticiens qui étudient le calcul quantique en dimension finie, il faudrait en faire une de même qualité pour la dimension infinie.

Annexe : construction de K_0 et K_1

Dans [19], Giedke et Cirac ont montré que l'on pouvait se restreindre à certaines matrices de covariance sans perte de généralité. Nous considérons donc les matrices de covariance de la forme :

$$K_i^{-1} = \begin{bmatrix} a_i & 0 & b_i & 0 \\ 0 & \alpha_i & 0 & \beta_i \\ b_i & 0 & c_i & 0 \\ 0 & \beta_i & 0 & \gamma_i \end{bmatrix} \tag{7}$$

Après la première partie du protocole, Bob ne possède que le second mode de l'état, ce que l'on calcule en prenant la trace partielle. Nous trouvons donc

$$K_B^{-1} = \begin{bmatrix} \frac{a_i c_i - b_i^2}{a_i} & 0 \\ 0 & \frac{\alpha_i \gamma_i - \beta_i^2}{\alpha_i} \end{bmatrix} \quad \text{et} \quad \mu_B = \begin{bmatrix} x_B^i \\ p_B^i \end{bmatrix} \tag{8}$$

Supposons que le protocole soit parfaitement cachant, nous avons alors $\hat{\rho}_0^B = \hat{\rho}_1^B$ ce qui se traduit par :

$$\begin{aligned} \frac{a_0 c_0 - b_0^2}{a_0} &= \frac{a_1 c_1 - b_1^2}{a_1} \\ \frac{\alpha_0 \gamma_0 - \beta_0^2}{\alpha_0} &= \frac{\alpha_1 \gamma_1 - \beta_1^2}{\alpha_1} \end{aligned}$$

Nous allons maintenant montrer que pour qu'Alice puisse tricher parfaitement, on a $c_0 = c_1$ et $\gamma_0 = \gamma_1$.

Une attaque gaussienne d'Alice est effectuée par une matrice de la forme

$$S = \begin{bmatrix} s_x & s_{xp} \\ s_{px} & s_p \end{bmatrix} \otimes I_2 = \begin{bmatrix} s_x & s_{xp} & 0 \\ s_{px} & s_p & \\ 0 & & I_2 \end{bmatrix}$$

Nous allons considérer la matrice $T = {S^{-1}}^\top$ d'après la remarque 5.6.1.

$$T^\top K_0^{-1} T = \begin{bmatrix} t_x^2 a_0 + t_{px}^2 \alpha_0 & t_x t_{xp} a_0 + t_{px} t_p \alpha_0 & t_x b_0 & t_{xp} \beta_0 \\ t_x t_{xp} a_0 + t_{px} t_p \alpha_0 & t_{xp}^2 a_0 + t_p^2 \alpha_0 & t_{px} b_0 & t_p \beta_0 \\ t_x b_0 & t_{xp} b_0 & c_0 & 0 \\ t_{px} \beta_0 & t_p \beta_0 & 0 & \gamma_0 \end{bmatrix}$$

Cette matrice doit être égale à K_1^{-1} ce qui implique $t_{xp} = t_{px} = 0$. T est alors la matrice d'une compression sur le mode d'Alice.

Nous allons maintenant exhiber une paire de matrices qui vérifie les conditions d'un protocole parfaitement cachant et dont on ne peut pas passer de l'une à l'autre uniquement par un transformation gaussienne sur le mode d'Alice.

$\hat{\rho}_1^B = \hat{\rho}_0^B$, elles ont donc en particulier le même déterminant :

$$\frac{a_0 c_0 - b_0^2}{a_0} \frac{\alpha_0 \gamma_0 - \beta_0^2}{\alpha_0} = \frac{a_1 c_1 - b_1^2}{a_1} \frac{\alpha_1 \gamma_1 - \beta_1^2}{\alpha_1}$$

Ce qui nous donc la condition :

$$a_0 \alpha_0 = a_1 \alpha_1$$

Nous cherchons maintenant la matrice de la forme :

$$K_1^{-1} = \begin{bmatrix} v a_0 & 0 & b_1 & 0 \\ 0 & \alpha_0 / v & 0 & \beta_1 \\ b_1 & 0 & u c_0 & 0 \\ 0 & \beta_1 & 0 & \gamma_0 / u \end{bmatrix}$$

qui doit vérifier ces 4 équations :

$$\begin{aligned} \left(a_0 c_0 uv - b_1^2\right) \left(\frac{\alpha_0 \gamma_0}{uv} - \beta_1^2\right) &= \left(a_0 c_0 - b_0^2\right) \left(\alpha_0 \gamma_0 - \beta_0^2\right) \\ a_0 c_0 (u - 1) &= \frac{b_1^2}{v} - b_0^2 \\ \alpha_0 \gamma_0 (\frac{1}{u} - 1) &= v \beta_1^2 - \beta_0^2 \\ u &\neq 1 \end{aligned}$$

Des 3 premières équations, nous tirons

$$\left(b_1^2 - uvb_0^2\right)\left(\frac{\beta_0^2}{v} - u\beta_1^2\right) = \left(\frac{b_1^2}{v} - ub_0^2\right)\left(\beta_0^2 - uv\beta_1^2\right)$$

Une solution évidente de cette équation[9] est

$$b_1 = \beta_0 \quad \text{et} \quad \beta_1 = b_0$$

Les coefficients de K_1 s'expriment alors en fonction de ceux de K_0. Nous abandonnons les indices pour alléger les notations[10]

La résolution du système en u et v nous donne en plus de la solution $u = 1$ qui ne nous intéresse pas :

$$\begin{aligned} u &= \frac{\alpha\gamma}{ac}\frac{ac - b^2}{\alpha\gamma - \beta^2} \\ v &= \frac{\alpha\gamma - \beta^2}{ac - b^2} \end{aligned}$$

Nous avons donc totalement déterminé la matrice K_1 en fonction de la matrice K_0

Nous souhaitons que Bob puisse distinguer les états $\hat{\rho}_0$ et $\hat{\rho}_1$ avec la plus grande probabilité, nous voulons donc que la fidélité entre ces deux états soient la plus faible possible.

D'après l'équation 6, nous devons calculer le déterminant de $K_0^{-1} + K_1^{-1}$.

Cette équation n'est pas très jolie et longue, mais elle permet de fixer astucieusement des valeurs

$$\begin{aligned} a &= \alpha = c = \gamma \\ b &= \sqrt{a^2 - \varepsilon^2} \\ \beta &= \sqrt{a^2 - \frac{1}{\varepsilon^2}} \end{aligned}$$

Ce qui nous donne :

$$v = 1/u = \frac{1}{\varepsilon^4}$$

Il reste à déterminé a, qui ne peut pas être choisi librement. Les matrices de covariance sont définies positives, cette condition donne $a \geq \frac{1}{\varepsilon}$. J'ai choisi l'égalité afin de minimiser la fidélité.

L'idée de base qui fait tout fonctionner est assez simple : c'est la très grande valeur de v et donc le faible recouvrement des gaussienne si l'on "oublie" les modes d'Alice. Lorsqu'Alice va effectuer sur son mode une transformation, elle ne va pas modifier les valeurs des variances de x_B et p_B. Et comme la fidélité est déjà très faible ne va pas beaucoup varier. C'est pour cette raison que je pense que le nombre de modes du côté d'Alice n'a que peu d'influence, seul importe le quart inferieur droit de la matrice.

Références

[1] Communication et cryptographie quantique avec des variables continues Frédéric Grosshans *Thèse*, 2002.

[2] The Real Symplectic Groups in Quantum Mechanics and Optics Arvind B. Dutta N. Mukunda R. Simon *arXiv :quant-ph/9509002*, Septembre 1995.

[9] Il doit bien y avoir une explication physique "jolie" mais je ne la comprends pas

[10] et diminuer le temps d'écriture de ce rapport.

[3] Sending entanglement through noisy quantum channels Benjamin Schumacher *Phys. Rev. A 54, 2614 - 2628 (1996) Issue 4*, October 1996.

[4] Quantum Bit Commitment Revisited : the Possible and the Impossible Giacomo Mauro D'Ariano Dennis Kretshchmann Dirk Schlingemann Reinhard F. Werner *quant-ph/0605224*, mai 2006.

[5] Entanglement quantification and purification in continuous variable systems S. Parker S. Bose M.B. Plenio *Phys. Rev. A 61, 032305 Issue 3* , février 2000.

[6] Introduction to the basics of entanglement theory in continuous-variable systems J. Eisert M.B. Plenio *arXiv :quant-ph/031207*, décembre 2003.

[7] Fidelities for transformations of unknown quantum states Lars Bojer Madsen Klaus Molmer *arXiv :quant-ph/031207*, décembre 2003.

[8] Quantum information with continuous variables Samuel L. Braunstein Peter van Loock *Éditions Springer*, 2003.

[9] Quantum and classical fidelities for Gaussian states Hyunseok Jeong Timothy C. Ralph Warwick P. Bowen *quant-ph/0409101*, Janvier 2004.

[10] Gaussian trnasformations and distillation of entangled Gaussian states Jaromir Fiurasek *Phys. Rev. Lett. 89, 137904 Issue 13*, Septembre 2002.

[11] Classical phase-space description of continuous-variable teleportation Carlton M. Caves Krzysztof Wodkiewicz *Phys. Rev. Lett. 93*, Mai 2004

[12] Note on Schmidt Decomposition in Infinite Dimensional Hilbert Spaces Su Hu Zongwen Yu *quant-ph/0705.1694*, Mai 2007

[13] The Trouble with Quantum Bit Commitment Dominic Mayers *quant-ph/9603015*, Mars 1996

[14] QBC3 : An Unconditionally Secure Quantum Bit Commitment Protocol Horace P. Yuen *quant-ph/0702074*, Fevrier 2007.

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

[16] Defeating classical bit commitments with a quantum computer Gilles Brassard Claude Crépeau Dominic Mayers Louis Salvail *quant-ph/9806031*, juin 1998.

[17] Quantum Bit Escrow Dorit Aharonov Amnon Ta-Shma Umesh V. Vazirani Andrew C. Yao *quant-ph/0004017 - Stoc 2000*, Avril 2004.

[18] No-go theormes : Reinterpretation and Extension Minh-Dung Dang *quant-ph/0701156*, Janvier 2007.

[19] Characterization of Gaussian operations and distillation of Gaussian states Géza Giedke J. Ignacio Cirac *Phys. Rev. A 66, 032316, Issue 3*, Septembre 2002

[20] A quantum bit commitment scheme provably unbreakable by both parties, Gilles Brassard Claude Crépeau Richard Jozsa Denis Langlois ; *In IEEE Symposium on Foundations of Computer Science, pages 362–371*, 1993.

[21] Mise en gage binaire sur variables continues, Jérôme Lodewyck, *Rapport de DEA, Laboratoire d'optique quantique d'Orsay*, avril 2003.

[22] G Giedke M.M. Wolf O. Krüger R.F. Werner J.I. Cirac, *Phys. Rev. Lett. 91, 107901*, 2003.

[23] J. Eisert C. Simon M.B. Plenio, *J. Phys. A : Math. Gen. 35 ;3911-3923*, 2002.