

Université Libre de Bruxelles

Année académique 2007-2008

Faculté des Sciences Appliquées

Centre for Quantum Information and Communication

Etude des relais et répéteurs quantiques à variables continues

Mémoire de fin d'études présenté par

Laurent OLISLAGER

Directeur de mémoire :

Pr. Nicolas CERF

en vue de l'obtention du grade

d'Ingénieur Civil Physicien

Résumé

En information quantique à variables continues, l'information est codée sur les quadratures de modes du champ électromagnétique. Dans un premier temps, nous présentons les développements de l'optique quantique qui permettent un tel traitement. En particulier, le formalisme gaussien est un outil très puissant pour décrire l'évolution de certains états quantiques de la lumière. Parmi ceux-ci, les états cohérents, les états comprimés et des états bimodaux particuliers dits EPR sont autant de ressources de grande importance pour réaliser des protocoles spécifiquement quantiques.

La plupart de ces protocoles souffrent actuellement d'un inconvénient majeur : leur courte portée. Lorsqu'un état quantique parcourt une longue distance dans une ligne de transmission, il s'en trouve en effet fortement dégradé. Le but de notre travail est d'explorer différentes voies possibles pour déterminer quels sont les schémas à même de favoriser les communications quantiques à longue distance.

Nous supposons vouloir envoyer un état cohérent arbitraire dans un canal à pertes homogène. Après avoir décrit les effets d'une propagation directe, nous envisageons plusieurs schémas de transmission, dont il faut évaluer quantitativement l'efficacité par rapport au cas de référence, la simple ligne à pertes. La fidélité de l'état de sortie par rapport à l'état d'entrée constituera la grandeur à optimiser.

Nous montrons que le choix du schéma le plus performant dépend de la longueur du canal. Pour de très faibles distances, il ne semble pas pertinent d'entreprendre une quelconque action. Néanmoins, lorsque la distance augmente, l'amplification préalable du signal – au moyen de l'effet d'amplification paramétrique optique dans un cristal non linéaire – permet de réduire l'effet des pertes tout en conservant partiellement la cohérence quantique.

Un schéma plus performant consiste à utiliser ce cristal non linéaire pour créer, au milieu de la ligne de transmission, une paire EPR, dont chaque partie est envoyée vers une extrémité du canal. Le lien qui unit ces deux parties – l'intrication – permet alors de téléporter l'état quantique de l'entrée à la sortie de la ligne de transmission, sans qu'un système quantique ne transporte physiquement l'état dans le canal. La fidélité correspondant à cette opération peut être grandement supérieure aux cas étudiés auparavant.

Nous montrons finalement qu'il est possible d'améliorer la fidélité de téléportation au moyen d'une opération de soustraction de photon effectuée en sortie du cristal non linéaire, dans chaque mode d'une paire EPR. La probabilité de succès d'une telle opération est toutefois très faible, ce qui empêche de la répéter un grand nombre de fois, sous peine de faire chuter le débit de manière drastique. Un compromis doit donc être recherché.

Remerciements

En préambule à ce mémoire, je tiens bien entendu à remercier chaleureusement les personnes qui m'ont aidé, directement ou indirectement, à le réaliser.

Tout d'abord, un grand merci au professeur Nicolas Cerf pour m'avoir fait découvrir le domaine passionnant de l'information quantique et pour m'avoir ouvert les portes de son service.

Parmi les membres de QuIC, merci tout particulièrement à Evgueni Karpov pour sa gentillesse, son soutien régulier, ses précieux conseils et ses relectures attentives.

Merci beaucoup à Raul Garcia-Patron Sanchez pour avoir pris le temps de baliser mon travail avant de s'envoler vers de nouveaux horizons.

Plus largement, je vais profiter de l'occasion qui m'est offerte pour remercier toutes les personnes qui ont su éveiller puis entretenir mon goût pour les sciences. En vingt-deux ans d'apprentissage, nombreux sont les professeurs et camarades de classe à avoir joué un rôle plus qu'anecdotique, aussi ne me hasarderai-je pas à citer de nom.

Merci à Ingrid et Roland, pour avoir toujours été à mes yeux des modèles, et pour ne jamais s'être revendiqués comme tels.

Merci à Nathalie dont la présence quotidienne, au-delà d'être un enchantement, constitue le meilleur médicament anti-stress que je connaisse.

Merci à Simone, qui a toujours voulu *être là* à la fin de mes études, pour y être arrivée en pleine forme, et pour sa bonne humeur perpétuelle.

Table des matières

Introduction	1
1 Éléments d'information quantique	2
1.1 Calcul quantique	3
1.2 Cryptographie quantique	4
1.3 Intrication quantique	6
1.4 Variables continues	8
2 Éléments d'optique quantique	9
2.1 Quantification du champ électromagnétique	9
2.2 Etats de Fock	11
2.3 Etats cohérents	12
2.4 Transformations de l'optique linéaire	13
2.5 Transformations de l'optique non linéaire	15
2.6 Formalisme gaussien	17
2.7 Trace partielle	20
2.8 Mesures	21
2.9 Téléportation quantique	23
3 Propagation d'états gaussiens	27
3.1 Transmission directe	28
3.2 Modélisation du canal par tronçons	32
3.3 Transmission avec amplification	33
3.4 Transmission par téléportation	36
3.5 Conclusion	42
4 Propagation d'états non gaussiens	43
4.1 Soustraction de photon	43
4.2 Description mathématique	45
4.3 Résultats	47
Conclusion	53
Bibliographie	55

Table des figures

2.1	Représentation dans l'espace des phases, (a) de l'état vide, (b) d'un état cohérent.	13
2.2	Interaction de deux modes lumineux sur un diviseur de faisceau.	14
2.3	Représentation dans l'espace des phases d'un état comprimé, (a) à partir du vide, (b) déplacé.	16
2.4	Equivalence entre un état EPR et la combinaison sur un diviseur de faisceau équilibré de deux états comprimés dans des directions orthogonales.	19
2.5	Mesure d'une quadrature au moyen d'une détection homodyne.	22
2.6	Mesure des deux quadratures au moyen d'une détection hétérodyne.	23
2.7	Protocole de téléportation : partage d'une paire EPR, mesure jointe, communication classique et déplacement.	24
3.1	Canal de longueur L	27
3.2	Equivalence entre un canal à pertes et un canal parfait précédé d'un diviseur de faisceau.	29
3.3	Evolution de χ en fonction de T	31
3.4	Evolution de $F = 2/(2 + \chi)$ en fonction de T	31
3.5	Ligne de longueur L subdivisée en k tronçons de longueur identique.	32
3.6	Amplification à une position quelconque.	33
3.7	Evolution de $F = 2/(2 + \delta)$ en fonction de la position de l'amplificateur, avec une valeur $G = 3/2$	34
3.8	Amplification à une position optimale, en début de ligne.	34
3.9	Evolution de la fidélité F en fonction de T pour différentes valeurs du gain G , et avec $N=N_G=N_0$	35
3.10	Schéma de transmission avec une paire EPR placée à une position quelconque.	36
3.11	Variation de la fidélité en fonction de la distance, dans le cas d'un canal sans bruit ajouté, et pour $r = 1$ et $g = \sqrt{2}$	37
3.12	Valeur de r nécessaire pour atteindre une valeur $F = 2/3$ dans le cas d'un canal sans bruit ajouté et pour $g = \sqrt{2}$	38
3.13	Comparaison entre transmission avec amplification et transmission par téléportation.	39
3.14	Schéma utilisant deux paires EPR.	39
3.15	Comparaison des schémas à plusieurs EPR, en fonction de r et pour $T_L = 1/2$	40
3.16	Valeur optimale du gain de téléportation g en fonction de T , pour $r = 1$	41
3.17	Valeur optimale du gain de téléportation g en fonction de r , pour $T_L = 1/2$	41
4.1	Téléportation avec soustraction de photon.	44

4.2	Fidélité de téléportation F d'un état cohérent en fonction de T_2 , avec $\sqrt{T_{tot}} = 0,1$, $r = 0,3$ et $T = 0,95$. La signification des paramètres est précisée dans le texte.	48
4.3	Fidélité de téléportation F d'un état cohérent en fonction de T_{tot} , avec $r = 0,3$ et $T = 0,95$. (a) Transmission directe. (b) Téléportation avec une paire EPR sans soustraction de photon. (c) Téléportation avec une paire EPR avec soustraction de photon.	49
4.4	Fidélité de téléportation F d'un état cohérent en fonction de T_{tot} , avec $r = 2$ et $T = 0,95$. (a) Transmission directe. (b) Téléportation avec une paire EPR sans soustraction de photon. (c) Téléportation avec une paire EPR avec soustraction de photon.	49
4.5	Fidélité de téléportation F d'un état cohérent en fonction du paramètre de compression r de la paire EPR utilisée, avec $T_{tot} = 0,25$ et $T = 0,95$. (a) Téléportation avec une paire EPR sans soustraction de photon. (b) Téléportation avec une paire EPR avec soustraction de photon.	50
4.6	Influence du coefficient de transmission du diviseur de faisceau pour la soustraction de photon (a) sur la fidélité de téléportation F d'un état cohérent, (b) sur la probabilité de réussite de la génération de l'état. $T_{tot} = 0,25$ et $r = 0,3$	50
4.7	Téléportation avec quatre soustractions de photon.	51
4.8	Amélioration de la fidélité suite à quatre soustractions de photons, à faible valeur de r	51
4.9	Comparaison du taux de réussite pour deux et pour quatre soustractions de photons, en fonction de r	52

Introduction

L'information est physique. Ce constat ouvre à deux interprétations. D'une part, il peut être considéré comme une limitation. L'information perd son statut de concept mathématique abstrait ; soumise aux lois de la physique, elle devient la proie des imperfections et des dégradations propres au monde réel. D'autre part, il peut être exploité comme une ressource. Ce nouveau point de vue est à la base d'une branche de la physique relativement récente qui s'est appelée l'information quantique.

Dans le premier chapitre de ce mémoire, nous décrivons en guise d'introduction les grands principes, les différentes voies et quelques réalisations de cette théorie. Très diversifiée, elle mène à des considérations théorico-philosophiques comme à des applications très concrètes ; ainsi de la cryptographie quantique ou encore de la téléportation quantique qui, contrairement à ce que l'on pourrait penser, est d'ores et déjà réalisée expérimentalement.

Pour exploiter les propriétés quantiques, on choisit souvent de coder l'information sous forme lumineuse. Plus particulièrement, nous étudions le cas d'un codage utilisant les quadratures de modes du champ électromagnétique. Dans le deuxième chapitre, nous présentons les développements d'optique quantique et établissons le formalisme mathématique permettant une telle description. Nous terminons par la description du protocole de téléportation quantique à variables optiques continues.

Si bon nombre de protocoles de l'information quantique sont maîtrisés tant théoriquement qu'expérimentalement, un de leurs inconvénients majeurs est leur courte portée. Dans le troisième chapitre, nous constatons qu'un état quantique parcourant une distance de quelques kilomètres dans un canal à pertes subit une forte dégradation. Pour remédier à cette situation, nous envisageons plusieurs schémas de *relais quantiques* et les optimisons. Nous observons que le protocole de téléportation quantique peut contribuer à améliorer la transmission.

Le quatrième chapitre étudie une amélioration de la communication dans une ligne à pertes basée sur le protocole de téléportation quantique, à l'aide de la production d'états non gaussiens de la lumière. En particulier, nous évaluons l'impact de soustractions de photons sur la qualité de la téléportation. La particularité de notre travail est de prendre en compte les pertes de la ligne de transmission pour optimiser le schéma envisagé.

Nous concluons en tirant les enseignements apportés par nos calculs et précisons quelles sont les pistes les plus prometteuses sur la voie d'une communication quantique à longue distance.

Chapitre 1

Eléments d'information quantique

Classical ideas such as realism and locality do not form the basis for explaining how the universe works. [Ili07]

Pour ne pas surcharger l'introduction, nous avons choisi de rédiger un chapitre autonome sur l'information quantique. Nous énonçons les principales découvertes et les idées essentielles qui les sous-tendent. Pour une revue plus détaillée et exhaustive, on pourra consulter les désormais nombreux ouvrages et articles qui traitent de ce domaine, notamment [NC00], livre de référence reconnu.

La naissance de l'information quantique a nécessité la maturation préalable de ses deux géniteurs : l'avènement de la théorie de l'information, dont les bases furent jetées par l'article fondateur de C. Shannon en 1948 [Sha48], et celui de la mécanique quantique. La théorie de l'information quantique résulte d'une prise de conscience d'une possible exploitation des propriétés quantiques dans une approche informationnelle.

Dans la deuxième moitié du vingtième siècle, l'information a pris une place prépondérante dans la société grâce aux avancées technologiques basées sur un traitement binaire de l'information. L'information, stockée et transportée sous diverses formes (électrique, optique...), est dès lors interprétée comme une collection de *bits* de valeurs "1" ou "0". Le passage de l'analogique au numérique, et donc d'un ensemble continu de valeurs à un ensemble discret, a constitué une amélioration considérable des capacités des systèmes d'information, ouvrant la voie au développement d'outils performants tels que les codes correcteurs d'erreur.

C'est donc tout naturellement que le concept fondateur de l'information quantique est une généralisation du bit, que l'on appelle *bit quantique* ou *qubit* : [NC00]

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (1.1)$$

avec $\alpha, \beta \in \mathbb{C}$, et $|\alpha|^2 + |\beta|^2 = 1$. Un qubit est un système physique à deux niveaux, dont l'état $|\psi\rangle$ appartient à un espace de Hilbert à deux dimensions, que l'on développe sur une base orthonormée $\{|0\rangle, |1\rangle\}$. On associe aux vecteurs de base le sens classique de bits de valeurs "0" et "1". Dans le cas où α (respectivement β) est nul, le qubit est interprété comme un bit de valeur "1" (respectivement "0").

De nombreuses méthodes ont été explorées pour réaliser physiquement de tels états, en encodant l'information sur divers objets quantiques. On peut coder l'information *via* le niveau – fondamental ou excité – d'un atome, le spin – up ou down – d'un électron, la polarisation d'un photon unique... Dans ce dernier cas, il est possible d'utiliser la base linéaire (auquel cas le 0 correspond à une polarisation horizontale et le 1 à une polarisation verticale) ou la base circulaire (une polarisation gauche s'interprète comme un 0 et une polarisation droite comme un 1).

1.1 Calcul quantique

Le concept de qubit porte en soi le développement d'une discipline appelée *calcul quantique*, qui repose sur le principe de superposition propre aux systèmes quantiques. Traditionnellement, un protocole informatique est une suite de portes logiques qui associent une valeur de sortie à une valeur d'entrée donnée.

Un ordinateur quantique exploite quant à lui le parallélisme quantique en faisant correspondre à une *superposition* d'états d'entrée une *superposition* d'états de sortie. Un protocole quantique, basé sur des portes logiques quantiques¹ équivalentes aux portes logiques classiques, doit alors se charger de sélectionner la sortie désirée.

On conçoit aisément qu'une telle propriété peut mener à des gains de temps considérables. L'avènement d'un tel ordinateur obligerait à repenser toute la théorie de la complexité algorithmique : certains problèmes réputés difficiles, c'est-à-dire n'ayant pas d'algorithme de résolution efficace, peuvent devenir faciles à résoudre à l'aide d'un algorithme quantique.

L'exemple le plus emblématique est l'*algorithme de Shor* [Sho94] : en 1994, ce dernier a démontré théoriquement l'existence d'un protocole quantique permettant de factoriser de grands nombres – problème pour l'heure complexe – en un temps polynomial².

Toutefois, la réalisation d'un hypothétique ordinateur quantique se heurte à de grandes difficultés technologiques. Il faut pouvoir produire, stocker et manipuler de façon sûre des qubits dans des circuits physiques. Il faut isoler parfaitement l'ordinateur quantique pour éviter toute interférence avec le monde extérieur et donc toute décohérence. Il faut assurer une conservation de l'information, la mécanique quantique étant réversible...

De nombreuses recherches, exploitant différentes voies, sont actuellement en cours ; elles n'aboutiront vraisemblablement pas avant un horizon relativement lointain.

¹Citons les portes Hadamard et controlled-NOT. Voir par exemple [NC00].

²A une famille de fonctions $\{f_n\}$, où f_n a une entrée de n bits, est associée une famille de circuits $\{C_n\}$ qui réalisent ces fonctions. On dit que cette famille est de "taille polynomiale" si elle ne grandit pas plus vite qu'une puissance de n : $\text{taille}(C_n) \leq \text{polynôme}(n)$. On définit alors P comme l'ensemble des problèmes de décision résolus par des circuits de taille polynomiale, c'est-à-dire en un "temps polynomial". Ces problèmes sont dits faciles à résoudre, au contraire des autres [Pre98].

1.2 Cryptographie quantique

La théorie de l'information quantique a donné lieu à des réalisations bien plus proches d'une possible exploitation scientifique voire commerciale. Ainsi de la *cryptographie quantique*, qui exploite les limitations intrinsèques – imposées par les lois de la mécanique quantique – sur la connaissance et la manipulation d'états quantiques.

Le *principe d'incertitude de Heisenberg* stipule que si deux observables \hat{A} et \hat{B} ne commutent pas, on ne peut connaître simultanément leurs valeurs propres avec une précision arbitraire :

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}|\langle[\hat{A}, \hat{B}]\rangle|, \quad (1.2)$$

où $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ est le commutateur de \hat{A} et \hat{B} . Le symbole Δ représente quant à lui la déviation standard, ou écart quadratique moyen, d'un opérateur \hat{O} . Il est défini à partir de la moyenne des carrés des écarts des mesures par rapport à leur moyenne et vaut

$$\Delta\hat{O} = \left(\langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2 \right)^{1/2}. \quad (1.3)$$

Rappelons que la moyenne d'un opérateur \hat{O} est définie comme

$$\langle\hat{O}\rangle = \text{Tr}[\rho\hat{O}], \quad (1.4)$$

où Tr est l'opération de Trace, et où ρ est la *matrice densité* de l'état considéré. En mécanique quantique, le formalisme de la matrice densité permet de définir des *mélanges statistiques* qui, contrairement aux *états purs*, ne peuvent être caractérisés par un vecteur d'état unique $|\psi\rangle$. Si, à un instant donné t , un système physique a des probabilités p_j de se trouver dans des états quantiques $|\psi_j\rangle$, sa matrice densité s'écrit [Bay05]

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|. \quad (1.5)$$

Nous notons la matrice densité ρ – et non $\hat{\rho}$ – mais il s'agit d'un opérateur.

Le *théorème de non-clonage* interdit toute duplication parfaite d'un état quantique inconnu.

Le postulat sur la *réduction du paquet d'onde* montre qu'en mesurant une grandeur physique d'un système quantique, on perturbe l'état du système.

La première personne à avoir pensé à exploiter ces limitations semble être Stephen Wiesner, de l'université de Columbia : au début des années 1970, il a émis l'idée de coder des billets de banque dont l'infalsifiabilité serait garantie par le principe d'incertitude. En incorporant une série aléatoire de spins 1/2 sur chaque billet, on assure l'incapacité d'un faussaire de reproduire la liste sans erreur. Cette proposition, irréalisable en pratique, n'a suscité à l'époque presque aucun intérêt³.

Cependant, Wiesner inspira Charles H. Bennett et Gilles Brassard ; en 1984, ils publièrent

³Son manuscrit de 1970 ne fut finalement publié qu'en 1983 [Wie83].

un protocole de distribution de clé secrète, désormais célèbre, et qui fut appelé le *protocole BB84*. Etant donné son importance historique, nous nous y attardons quelque peu ci-dessous, après avoir décrit le problème à résoudre.

Selon les conventions adoptées en cryptographie, la situation est la suivante : Alice (A) désire envoyer un message à Bob (B) sans qu'une espionne, appelée Eve (E), puisse le déchiffrer. On suppose que E peut intercepter le message de A , le manipuler de toutes les façons que le permettent les lois de la physique, et le réenvoyer vers B . Si A se contente d'envoyer son message à B sous la forme d'une suite de bits, il suffit à E de lire la liste, la copier et la réenvoyer vers B : elle connaît alors le contenu du message, sans que ni A ni B ne se rendent compte qu'ils ont été espionnés.

Pour éviter cela, A doit coder son message de telle sorte que, même si E parvient à l'intercepter, elle ne puisse le déchiffrer. Les spécialistes de la cryptographie, science millénaire [Sin99], ont longtemps cherché le "code parfait", à même de ne jamais être percé à jour. La solution consiste à utiliser le *chiffre de Vernam* : A génère une clé secrète K , liste de bits aléatoires aussi longue que son message clair M , et envoie le message chiffré $C = \text{XOR}(M, K)$. Par exemple,

$$\begin{aligned} M & : 0001101111010001, \\ K & : 1010100111110111, \\ C & : 1011001000100110. \end{aligned}$$

Le message chiffré C revêt le caractère aléatoire de la clé K . Seule la connaissance de K permet de reconstituer le message, à l'aide de l'opération $M = \text{XOR}(C, K)$. Si B veut lire le message de A , il doit donc disposer de la clé K . Le problème se réduit ainsi à un problème de *distribution de clé*, qui ne doit pas être connue de E . Le transfert de clé sécurisé, voire de "main à main", provoque des contraintes importantes.

Un protocole d'un genre totalement nouveau, le *RSA* [RSA78], est alors apparu ; il repose sur le principe d'une clé asymétrique, c'est-à-dire qui n'est pas identique pour le chiffage et pour le déchiffage. Toute personne désirant envoyer un message à B dispose de la partie publique de sa clé, qui permet de chiffrer ; B , grâce à la partie privée de sa clé, est le seul à même de pouvoir déchiffrer le message. La sécurité de la transmission repose sur le fait que déterminer la clé privée de B à partir de sa clé publique n'est pas réalisable en un temps polynomial, car l'opération nécessite la factorisation de grands nombres. Toutefois, aucune preuve rigoureuse de cette impossibilité n'a pu être apportée ; au contraire, nous avons vu qu'un ordinateur quantique serait à même de réaliser cette opération.

Si le calcul quantique peut apporter un "poison" cryptographique, l'information quantique apporte, au préalable, le "remède". En effet, le protocole BB84 permet à A et B de partager un chiffre de Vernam, tout en garantissant la sécurité de la transmission, non par un quelconque argument de temps calculatoire, mais *par les lois de la physique*. Voici la procédure à suivre :

- A encode ses valeurs au moyen de qubits photoniques, à savoir l'état de polarisation de photons individuels. La particularité est qu'elle choisit aléatoirement de les coder au moyen de la base linéaire ou de la base circulaire, deux bases non orthogonales. Elle les envoie sur un canal quantique à B .

- Pour connaître la clé secrète, E doit intercepter les qubits, les mesurer et les réenvoyer (le théorème de non-clonage implique qu'elle ne peut pas en faire de copie sans les mesurer). Cependant, on ne peut pas déterminer en même temps la polarisation d'un photon dans les bases linéaire et circulaire. Ne pouvant connaître la base de codage utilisée par A , elle en choisit une au hasard. Une fois sur deux, elle se trompe. Dans ce cas, elle obtient un résultat tout à fait aléatoire. Globalement, un quart de ses bits sont donc faux.
- B mesure les qubits reçus de la même façon. Lorsqu'il a reçu tous les qubits, A révèle pour chacun d'eux quelle base elle a utilisé pour coder. Si B n'a pas utilisé la même, le bit est rejeté – la moitié des bits environ le seront. Le reste est utilisé comme chiffre inviolable pour un futur message, qui peut être envoyé sur un canal classique.
- E semble *a priori* pouvoir disposer d'une certaine quantité d'information. Mais en mesurant un état, en vertu des postulats de la mécanique quantique, elle le *transforme*. En analysant un sous-échantillon de leur liste commune, A et B ne devraient constater aucune erreur. Si ce n'est pas le cas, ils peuvent détecter la présence de E et recommencer la procédure. En pratique, en imputant toute erreur (qui peut être due à un défaut de transmission) à la présence de E , on peut, jusqu'à un certain niveau de bruit, prouver la sécurité de la transmission – en supposant des attaques d'espionnage optimales. Une procédure d'*amplification de confidentialité* permet de réduire à néant la connaissance d'un éventuel espion.

Le premier prototype de distribution quantique de clé secrète [BBB⁺92] a fonctionné sur une distance de 32 centimètres en 1989. D'autres démonstrations expérimentales ont ensuite été établies sur de plus grandes distances de fibres optiques [MBG93]. D'autres protocoles ont été proposés et mis en pratique, par exemple [Eke91], qui utilise une autre propriété spécifiquement quantique, et réellement fascinante, appelée *intrication*.

1.3 Intrication quantique

Si l'on groupe deux bits classiques, on obtient quatre états possibles : 00, 01, 10 et 11. Considérons à présent un système de deux qubits. La paire de qubits peut être développée sur une base de référence constituée de quatre vecteurs. Elle est une *superposition* de ces quatre états :

$$|\psi\rangle = \alpha_{00}|0, 0\rangle + \alpha_{01}|0, 1\rangle + \alpha_{10}|1, 0\rangle + \alpha_{11}|1, 1\rangle, \quad (1.6)$$

avec $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. Deux qubits initialement indépendants peuvent former un état à deux qubits en interagissant dans une porte logique. Des exemples importants d'états à deux qubits, appelés *états de Bell* ou *états EPR*, sont : [NC00]

$$|\beta_{0,0}\rangle = \frac{|0, 0\rangle + |1, 1\rangle}{\sqrt{2}} \quad (1.7)$$

$$|\beta_{0,1}\rangle = \frac{|0, 1\rangle + |1, 0\rangle}{\sqrt{2}} \quad (1.8)$$

$$|\beta_{1,0}\rangle = \frac{|0, 0\rangle - |1, 1\rangle}{\sqrt{2}} \quad (1.9)$$

$$|\beta_{1,1}\rangle = \frac{|0, 1\rangle - |1, 0\rangle}{\sqrt{2}} \quad (1.10)$$

Considérons, à titre d'exemple, le premier de ces états. Si nous effectuons une mesure – selon la base de référence $\{|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle\}$ – du premier qubit, on obtient le résultat :

- “0” avec une probabilité $1/2$. Dans ce cas l'état post-mesure est transformé en un nouvel état, $|0,0\rangle$. Une mesure sur le second qubit donnerait alors pour résultat “0” avec une probabilité unitaire.
- “1” avec une probabilité $1/2$. Dans ce cas l'état post-mesure est transformé en un nouvel état, $|1,1\rangle$. Une mesure sur le second qubit donnerait alors pour résultat “1” avec une probabilité unitaire.

Les résultats de mesures sur les deux parties du système sont donc parfaitement corrélés ! Ces corrélations demeurent même si les deux qubits sont physiquement très éloignés, voire même si, dans une certaine mesure, ils ont subi des interactions avec l'environnement⁴. Ce constat frappant est à la base du *paradoxe EPR*, du nom d'Einstein, Podolsky et Rosen, qui doutaient de la réalité d'une telle propriété [EPR35]. Selon eux, la mécanique quantique ne pouvait constituer une théorie achevée; afin de préserver les principes de causalité et de *réalisme local* (toute l'information d'un objet est “écrite dessus”), il fallait considérer des *variables cachées*. Ces dernières seraient des paramètres physiques non pris en compte par les postulats de la mécanique quantique et qui assureraient une évolution dynamique *déterministe* d'un état quantique.

L'intrication – ou enchevêtrement – quantique a donné lieu à de vives controverses scientifiques voire philosophiques. Une contribution importante a été apportée dans les années 1970 par John Bell : à condition de violer les fameuses *inégalités de Bell*, des objets physiques peuvent effectivement avoir des corrélations plus fortes que ce qui pourrait être atteint classiquement [Bel64]. Ces inégalités ont depuis été violées expérimentalement [Asp76] [ADR82]. S'il apparaît ainsi que la Nature ne se comporte pas comme Einstein le pensait, le débat quant à la pertinence des mesures expérimentales continue et de nouvelles expériences, potentiellement à même de lever le doute, sont proposées actuellement [GPFC05].

L'existence de l'intrication quantique n'est toutefois plus mise en cause. Des états seront dits intriqués s'ils satisfont un critère d'inséparabilité : on ne peut écrire le vecteur d'état $|\psi\rangle$ comme un produit de vecteurs d'états individuels $|\phi\rangle_1|\phi\rangle_2\dots|\phi\rangle_n$, où n est le nombre de parties de l'état intriqué, qui peut être supérieur à deux. Utiliser ce critère est toutefois impossible en pratique pour vérifier la présence ou l'absence d'intrication. Dès lors, plusieurs outils théoriques sont nés pour tenter de la caractériser et de la quantifier. La violation du principe de réalisme local constitue une condition nécessaire et suffisante pour que deux états purs soient intriqués : cela se traduit par un *rang de Schmidt* supérieur à 1, ou encore par une *entropie partielle de von Neumann* supérieure à 0. La définition de ces grandeurs peut être trouvée dans [BvL05]. On y énonce également d'autres critères, dans le cas de mélanges statistiques et/ou d'intrication multi-partite. De manière générale, les états intriqués sont ceux qui ne peuvent être préparés à l'aide des seules opérations locales et communications classiques (LOCC en anglais).

On constate que l'étude de l'information quantique a permis de mieux comprendre la

⁴Dans ce cas il se produit toutefois un phénomène de décohérence; c'est ce qui empêche des états macroscopiques d'être intriqués.

mécanique quantique elle-même, qui permet un traitement de l'information au-delà des limites du monde classique. De nombreuses recherches en information quantique sont actuellement tournées vers l'étude et la production expérimentale d'intrication, ressource essentielle dans diverses applications, comme le *codage dense*⁵ ou la *téléportation quantique*. Nous verrons qu'elle est un moyen indispensable vers la communication quantique à longue distance, qui nous intéresse plus particulièrement dans le cadre de ce travail.

1.4 Variables continues

La lumière, facilement manipulable et aux propriétés bien connues, s'est vite avérée être l'instrument de prédilection de la théorie de l'information quantique. Comme nous l'avons vu, la notion de qubit, très puissante conceptuellement, implique de travailler avec des variables optiques *discrètes*. Cette approche a un inconvénient majeur : la difficulté expérimentale de manipuler de telles variables. La production, la mise en interaction, le stockage et la mesure⁶ de photons individuels sont difficiles à réaliser.

L'histoire des sciences est fortement corrélée à l'histoire de la technologie⁷. Une autre voie a alors été empruntée. Il s'agissait dorénavant de coder l'information au moyen de variables *continues* – qui “vivent” dans un espace de Hilbert de dimension infinie. Cette approche s'est avérée fructueuse, permettant de reproduire les concepts théoriques et résultats expérimentaux obtenus en variables discrètes, et ouvrant la voie à de nouvelles recherches.

Les variables utilisées sont des quadratures de modes du champ lumineux⁸. On peut décrire cette approche au moyen de l'optique quantique ; le chapitre suivant s'y attelle.

⁵Si Alice et Bob se partagent un état intriqué, il leur est possible de se transmettre par après l'équivalent de *deux* bits au moyen d'*un* seul qubit.

⁶Ce point est particulièrement limitatif. Il faut disposer de photodiodes à avalanche capables de détecter des photons individuels. Du fait du processus de collection des charges, ces détecteurs ont de plus une bande passante limitée.

⁷On entend par là qu'une proposition théorique, souvent inspirée de l'expérience, doit pouvoir être vérifiée expérimentalement puis, pour être exploitée, doit se prêter aux manipulations expérimentales.

⁸Pour observer les effets quantiques, on utilise des impulsions cohérentes de faible intensité. A l'opposé du cas discret, une technique de mesure performante est disponible, comme nous le verrons à la section 2.8.

Chapitre 2

Eléments d'optique quantique

Every word or concept, clear as it may seem to be, has only a limited range of applicability. (W. Heisenberg)

L'optique quantique est un vaste domaine de la physique ; les phénomènes qu'elle décrit ne se limitent aucunement à l'information quantique. En nous contentant de reproduire les résultats directement utiles à notre travail, nous effectuons une description nécessairement limitative. La littérature abonde de développements plus complets ; pour plus de détails, on peut par exemple consulter [MSI90] [SZ97] [Man07].

2.1 Quantification du champ électromagnétique

Les équations de Maxwell, en établissant un lien entre les champs électrique \mathbf{E} et magnétique \mathbf{H} , constituent une description appropriée d'un champ électromagnétique classique. Dans le vide, en l'absence de charges libres, elles s'écrivent :

$$\nabla \times \mathbf{E} = -\epsilon_0 \frac{\partial \mathbf{H}}{\partial t}, \quad \nabla \cdot \mathbf{E} = 0, \quad (2.1)$$

$$\nabla \times \mathbf{H} = \mu_0 \frac{\partial \mathbf{E}}{\partial t}, \quad \nabla \cdot \mathbf{H} = 0, \quad (2.2)$$

où ϵ_0 et μ_0 sont respectivement la permittivité et la perméabilité du vide. Il s'ensuit que \mathbf{E} satisfait l'équation d'onde

$$\Delta \mathbf{E} - \frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2} = 0. \quad (2.3)$$

Cette équation a pour solution générale un ensemble d'ondes planes se propageant à la vitesse de la lumière $c \equiv (\epsilon_0 \mu_0)^{-1/2}$:

$$\mathbf{E}(\mathbf{r}, t) = \sum_{\mathbf{k}} E_{\mathbf{k}} \mathbf{e}_{\mathbf{k}}^{(\lambda)} \left[\frac{a_{\mathbf{k},\lambda}}{\sqrt{2}} e^{i(\mathbf{k}\mathbf{r} - \omega_{\mathbf{k}}t)} + \frac{a_{\mathbf{k},\lambda}^*}{\sqrt{2}} e^{-i(\mathbf{k}\mathbf{r} - \omega_{\mathbf{k}}t)} \right] \quad (2.4)$$

$$= \sum_{\mathbf{k}} E_{\mathbf{k}} \mathbf{e}_{\mathbf{k}}^{(\lambda)} [x_{\mathbf{k},\lambda} \cos(\mathbf{k}\mathbf{r} - \omega_{\mathbf{k}}t) + p_{\mathbf{k},\lambda} \sin(\mathbf{k}\mathbf{r} - \omega_{\mathbf{k}}t)], \quad (2.5)$$

où

$$E_{\mathbf{k}} = \sqrt{\frac{\hbar \omega_{\mathbf{k}}}{\epsilon_0}} \quad (2.6)$$

contient les facteurs dimensionnels¹. La somme porte sur tous les modes \mathbf{k} , auxquels correspondent les pulsations $\omega_{\mathbf{k}}$ et les vecteurs de polarisation $\mathbf{e}_{\mathbf{k}}^{(\lambda)}$. Les constantes complexes adimensionnelles $a_{\mathbf{k},\lambda}$, $a_{\mathbf{k},\lambda}^*$, $x_{\mathbf{k},\lambda}$ et $p_{\mathbf{k},\lambda}$ sont liées entre elles par les relations :

$$x_{\mathbf{k},\lambda} = \frac{a_{\mathbf{k},\lambda} + a_{\mathbf{k},\lambda}^*}{\sqrt{2}}, \quad p_{\mathbf{k},\lambda} = i \frac{a_{\mathbf{k},\lambda}^* - a_{\mathbf{k},\lambda}}{\sqrt{2}}, \quad (2.7)$$

$$a_{\mathbf{k},\lambda} = \frac{x_{\mathbf{k},\lambda} + ip_{\mathbf{k},\lambda}}{\sqrt{2}}, \quad a_{\mathbf{k},\lambda}^* = \frac{x_{\mathbf{k},\lambda} - ip_{\mathbf{k},\lambda}}{\sqrt{2}}. \quad (2.8)$$

En substituant une solution modale dans l'équation (2.3), celle-ci peut s'écrire, pour tout mode \mathbf{k} , avec la définition $k^2 \equiv \omega^2/c^2$:

$$\Delta \mathbf{E}_{\mathbf{k}} + k^2 \mathbf{E}_{\mathbf{k}} = 0. \quad (2.9)$$

Chaque mode du champ électromagnétique vérifie donc une équation de Helmholtz, semblable à celle d'un oscillateur harmonique. Les constantes x et p sont donc formellement identiques à la position et l'impulsion qui décrivent le mouvement d'un oscillateur harmonique. En particulier, l'évolution au cours du temps des coordonnées (x, p) dans un *espace des phases* traduit l'évolution du système.

Cette constatation implique que le champ électromagnétique peut être décrit de manière quantique en procédant à une quantification semblable à celle de l'oscillateur harmonique, opération bien connue en mécanique quantique [Bay05]. Dans le formalisme dit de la seconde quantification², les constantes $a_{\mathbf{k},\lambda}$, $a_{\mathbf{k},\lambda}^*$, $x_{\mathbf{k},\lambda}$ et $p_{\mathbf{k},\lambda}$ deviennent les *opérateurs* d'annihilation $\hat{a}_{\mathbf{k},\lambda}$, de création $\hat{a}_{\mathbf{k},\lambda}^\dagger$, et de quadrature $\hat{x}_{\mathbf{k},\lambda}$ et $\hat{p}_{\mathbf{k},\lambda}$. Par correspondance avec le cas classique, les relations suivantes sont vérifiées³ :

$$\hat{x} = \frac{\hat{a} + \hat{a}^\dagger}{\sqrt{2}}, \quad \hat{p} = i \frac{\hat{a}^\dagger - \hat{a}}{\sqrt{2}}, \quad (2.10)$$

$$\hat{a} = \frac{\hat{x} + i\hat{p}}{\sqrt{2}}, \quad \hat{a}^\dagger = \frac{\hat{x} - i\hat{p}}{\sqrt{2}}. \quad (2.11)$$

Les opérateurs d'annihilation et de création vérifient les relations de commutation bosoniques :

$$[\hat{a}_{\mathbf{k},\lambda}, \hat{a}_{\mathbf{k}',\lambda'}^\dagger] = \delta_{\mathbf{k}\mathbf{k}'} \delta_{\lambda\lambda'}, \quad (2.12)$$

$$[\hat{a}_{\mathbf{k},\lambda}, \hat{a}_{\mathbf{k},\lambda}] = 0, \quad (2.13)$$

$$[\hat{a}_{\mathbf{k},\lambda}^\dagger, \hat{a}_{\mathbf{k},\lambda}^\dagger] = 0. \quad (2.14)$$

Les opérateurs de quadrature vérifient quant à eux la relation de commutation :

$$[\hat{x}, \hat{p}] = \frac{i}{2} ([\hat{a}, \hat{a}^\dagger] - [\hat{a}^\dagger, \hat{a}]) = i. \quad (2.15)$$

¹Dans la suite de ce travail, nous utilisons un système d'unités tel que $\hbar = 1$. Nous travaillerons en termes de fréquences ω des photons plutôt qu'en termes de leurs énergies $\hbar\omega$.

²Après avoir quantifié les niveaux d'énergie de la *matière*, on quantifie le champ de *lumière*, ce qui permet une description purement quantique de l'interaction lumière-matière.

³Pour la clarté des notations, nous omettons désormais les indices \mathbf{k} et λ lorsque nous décrivons un seul mode \mathbf{k} du champ électromagnétique.

Comme on peut le vérifier aisément avec (2.10), les opérateurs de quadrature, au contraire des opérateurs d'annihilation et de création, sont hermitiques. Par ailleurs, leurs états propres forment une base. Ce sont donc des observables. Toutefois, une mesure conjointe des valeurs propres x et p ne peut fournir une précision arbitraire. Les opérateurs \hat{x} et \hat{p} sont *canoniquement conjugués*⁴ et vérifient la relation d'incertitude (1.2),

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{1}{2} |\langle [\hat{x}, \hat{p}] \rangle| = \frac{1}{2}. \quad (2.16)$$

Les opérateurs de quadrature, qui jouent le rôle d'opérateurs de position et d'impulsion, obéissent à une relation d'incertitude analogue.

2.2 Etats de Fock

Le champ électromagnétique *quantifié* correspond à un ensemble d'oscillateurs harmoniques quantifiés. A chaque mode \mathbf{k} , il correspond donc un Hamiltonien⁵ :

$$\hat{H} = \omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right). \quad (2.17)$$

Par analogie avec l'oscillateur harmonique, nous définissons l'opérateur compteur $\hat{n} = \hat{a}^\dagger \hat{a}$ et notons ses états propres $|n\rangle$, de valeurs propres $n \in \mathbb{N}$:

$$\hat{a}^\dagger \hat{a} |n\rangle = n |n\rangle. \quad (2.18)$$

Ces états sont également états propres de l'Hamiltonien (2.17) :

$$\hat{H} |n\rangle = E_n |n\rangle, \quad \text{avec} \quad E_n = \omega(n + 1/2). \quad (2.19)$$

Les états $|n\rangle$ sont appelés *états de Fock* ou encore *états nombres* : on les interprète habituellement comme correspondant à la présence de n photons dans le mode correspondant. Remarquons que pour un état de Fock $|n\rangle$, l'égalité suivante est satisfaite :

$$\Delta\hat{x}\Delta\hat{p} = n + \frac{1}{2}. \quad (2.20)$$

L'*état vide* $|0\rangle$, défini tel que $\hat{n}|0\rangle = 0$, est d'énergie minimale et sature l'inégalité de Heisenberg, tandis que le "disque d'incertitude" des quadratures augmente avec le nombre de photons.

En utilisant $[\hat{a}, \hat{a}^\dagger] = 1$ et la définition de l'opérateur compteur, on montre facilement que les opérateurs d'annihilation et de création permettent respectivement d'enlever ou d'ajouter un photon au mode considéré :

$$\hat{a} |n\rangle = \sqrt{n} |n-1\rangle, \quad (2.21)$$

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle. \quad (2.22)$$

En appliquant de façon répétée \hat{a}^\dagger sur $|0\rangle$, on obtient l'expression d'un état de Fock quelconque en fonction de l'état vide,

$$|n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle. \quad (2.23)$$

⁴Deux opérateurs sont dits canoniquement conjugués si leur commutateur vaut $i\hbar = i$.

⁵Comme précisé au paragraphe précédent, nous sous-entendons les indices \mathbf{k} et posons $\hbar = 1$.

Les états de Fock sont orthogonaux et forment une base de l'ensemble des états. Un *état pur* peut s'écrire

$$|\psi\rangle = \sum_n c_n |n\rangle, \quad (2.24)$$

tandis qu'un *mélange statistique* peut être décrit par l'opérateur densité

$$\rho = \sum_{n,m} \rho_{n,m} |n\rangle\langle m|. \quad (2.25)$$

Pour traiter le cas d'un champ multimode, il suffit de définir une base $|n_{\mathbf{k}}\rangle$, produit tensoriel des bases $|n\rangle$ de chaque mode.

2.3 États cohérents

Les états de Fock correspondent à une vision *discrète* du champ électromagnétique : des photons sont ajoutés un à un à partir du vide quantique. L'obtention de tels états est toutefois difficile expérimentalement dès que $n > 2$. À l'inverse, les *états cohérents*, qui correspondent à une description *continue* du champ électromagnétique, sont ceux générés par un laser. Ils sont définis comme les vecteurs propres de l'opérateur d'annihilation \hat{a} :

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \quad (2.26)$$

où les valeurs propres α sont complexes, \hat{a} n'étant pas hermitique. Chaque état cohérent a un développement unique sur la base des états de Fock :

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (2.27)$$

En corollaire, le nombre de photons n'est pas déterminé dans un état cohérent⁶. La probabilité qu'un champ préparé dans un état cohérent $|\alpha\rangle$ contienne n photons suit une loi de Poisson :

$$p(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}. \quad (2.28)$$

Un état cohérent peut être vu comme l'état vide auquel on applique un *opérateur de déplacement* $D(\alpha)$:

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0\rangle = D(\alpha)|0\rangle. \quad (2.29)$$

Dans l'espace des phases, cet opérateur de déplacement a pour effet de déplacer les valeurs moyennes de \hat{x} et \hat{p} , qui sont nulles dans le cas du vide, d'une valeur respective $d_x = \sqrt{2}\Re\alpha$ et $d_p = \sqrt{2}\Im\alpha$. Cette translation n'affecte en rien les variances des quadratures, qui sont toujours égales l'une à l'autre, et saturent l'inégalité de Heisenberg :

$$\Delta\hat{x}\Delta\hat{p} = (\Delta\hat{x})^2 = (\Delta\hat{p})^2 = \frac{1}{2}. \quad (2.30)$$

Pour cette raison, les états cohérents sont souvent appelés *états quasi-classiques*. Ces propriétés sont illustrées sur la figure 2.1 – la visualisation en termes d'*espace des phases* est empruntée au monde classique.

⁶Par contre, la phase peut être définie, tandis qu'elle est parfaitement aléatoire pour un état de Fock. On peut voir la dualité des descriptions discrète–continue sous l'angle de la dualité amplitude–phase des descriptions de la lumière.

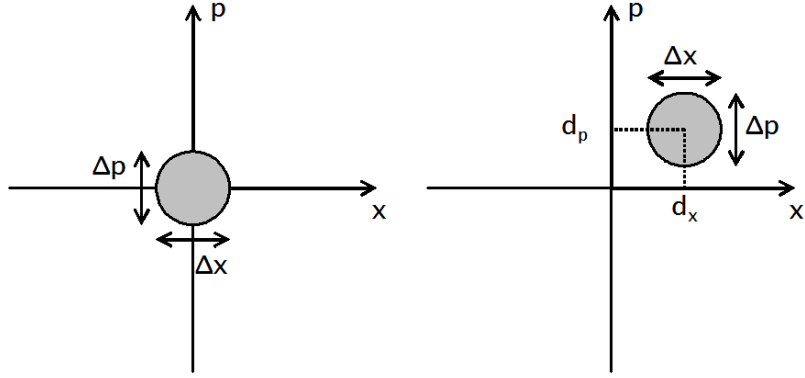


FIG. 2.1 – Représentation dans l’espace des phases, (a) de l’état vide, (b) d’un état cohérent.

Signalons enfin que les états cohérents satisfont une relation de fermeture, mais ne sont pas parfaitement orthogonaux. $|\alpha\rangle$ et $|\beta\rangle$ ne deviennent orthogonaux que s’ils sont infiniment “éloignés” :

$$|\langle\beta|\alpha\rangle|^2 = e^{-|\alpha-\beta|^2}. \quad (2.31)$$

2.4 Transformations de l’optique linéaire

Expérimentalement, il est intéressant de manipuler les états cohérents dont nous disposons en sortie d’un laser. Nous allons décrire quelques transformations possibles et leur associer une représentation mathématique. Tant qu’aucune mesure n’est réalisée, l’évolution du système est réversible et chaque transformation sera représentée par une matrice unitaire⁷.

L’évolution au cours du temps d’un système est régie par l’Hamiltonien de ce système. Dans la représentation de Schrödinger, l’Hamiltonien transforme les vecteurs d’état sur lesquels il agit. Dans la représentation de Heisenberg, l’Hamiltonien transforme les opérateurs avec lesquels il ne commute pas. En adoptant cette vision, nous pouvons déterminer la transformation des opérateurs de quadrature soumis à un Hamiltonien. On utilise pour ce faire l’équation d’évolution en représentation de Heisenberg : pour un opérateur \hat{O} ne dépendant pas explicitement du temps,

$$\frac{d\hat{O}}{dt} = \frac{1}{i}[\hat{O}, \hat{H}]. \quad (2.32)$$

En résolvant une simple équation différentielle, on obtient la transformation des quadratures \hat{x} et \hat{p} , pour un Hamiltonien donné, qui dépend d’elles⁸, et qui s’exerce pendant un temps Δt donné.

La première transformation à considérer est un simple *déphasage*. Si un faisceau lumineux parcourt un chemin optique plus long qu’un faisceau de référence (par exemple au

⁷L’inverse d’une matrice unitaire est la matrice adjointe, égale à la matrice transposée dans le cas d’éléments réels.

⁸La forme de l’Hamiltonien est dérivable intuitivement en fonction des opérateurs \hat{a} et \hat{a}^\dagger . La forme correspondante en fonction de \hat{x} et \hat{p} est dérivable à l’aide des équations (2.11) et (2.15).

moyen d'un matériau transparent dont l'indice de réfraction est supérieur à celui du vide), il accumule une phase additionnelle $\theta = \omega\Delta t$ proportionnelle au temps d'interaction. Dans l'espace des phases, cela correspond à une simple rotation des quadratures⁹ :

$$\begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}_{out} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}_{in} = S_{PS} \begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}_{in}, \quad (2.33)$$

où PS est noté pour *phase shift*. Cette transformation est la conséquence de l'équation du mouvement de Heisenberg (2.32) pour un Hamiltonien $\hat{H} = \omega\hat{a}^\dagger\hat{a} = \frac{\omega}{2}[\hat{x}^2 + \hat{p}^2 - 1]$.

Considérons à présent la transformation conjointe de *deux* modes du champ lumineux. Un *diviseur de faisceau* est une lame de verre partiellement réfléchissante : il transmet une partie du signal incident et réfléchit le reste.

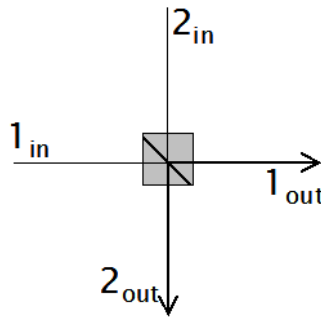


FIG. 2.2 – Interaction de deux modes lumineux sur un diviseur de faisceau.

En envoyant un mode de lumière à chaque entrée d'un diviseur de faisceau (figure 2.2), on applique un Hamiltonien d'interaction qui annihile des photons dans le mode 1 pour les créer dans le mode 2, et inversement :

$$H = \omega(\hat{a}_2^\dagger\hat{a}_1 + \hat{a}_1^\dagger\hat{a}_2). \quad (2.34)$$

En réécrivant H en fonction des opérateurs de quadrature et en utilisant (2.32), on constate que l'on recueille sur chaque sortie une combinaison linéaire des modes d'entrée telle que¹⁰ :

$$\begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \end{pmatrix}_{out} = \begin{pmatrix} t & 0 & r & 0 \\ 0 & t & 0 & r \\ -r & 0 & t & 0 \\ 0 & -r & 0 & t \end{pmatrix} \begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \end{pmatrix}_{in} = S_{BS} \begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \end{pmatrix}_{in}, \quad (2.35)$$

où BS est noté pour *beamsplitter*. Les coefficients t et r sont fonctions du temps d'interaction : $t = \cos(\omega\Delta t)$ et $r = \sin(\omega\Delta t)$.

Les faisceaux interagissent tout en conservant le nombre total de photons. Cette dernière propriété est justifiée par le fait que, technologiquement, les lames de verre utilisées

⁹Comme la phase absolue d'un faisceau individuel n'a aucun sens physique, cette transformation nous révèle que les rôles des quadratures peuvent être intervertis à loisir, ou que l'on peut en considérer des combinaisons linéaires.

¹⁰La position des signes négatifs résulte d'une convention arbitraire. On peut les placer sur les coefficients de réflexion des deux premières lignes.

présentent de très faibles pertes ($< 0,25\%$). Dans notre modèle, elle se traduit par la relation :

$$t^2 + r^2 = 1 \quad \Leftrightarrow \quad T + R = 1, \quad (2.36)$$

où nous avons défini $T = t^2$ et $R = r^2$. Une fraction T de la lumière incidente est transmise et une fraction R est réfléchi : T et R sont appelés respectivement coefficient de transmission et coefficient de réflexion. Dans le cas où $T = R = 1/2$, le diviseur de faisceau est dit équilibré et :

$$\begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \end{pmatrix}_{out} = \frac{1}{\sqrt{2}} \begin{pmatrix} x_1 + x_2 \\ p_1 + p_2 \\ x_2 - x_1 \\ p_2 - p_1 \end{pmatrix}_{in}. \quad (2.37)$$

La transformation réalisée par un diviseur de faisceau est facilement réalisable et d'une grande importance expérimentale et théorique. Nous l'utiliserons tout au long de ce travail.

2.5 Transformations de l'optique non linéaire

Les transformations autorisées par l'optique linéaire correspondent toujours à des rotations dans l'espace des phases engendré par les quadratures impliquées, et préservent le caractère quasi-classique des états produits par le laser. Des propriétés spécifiquement quantiques peuvent être introduites par des non-linéarités optiques du second ordre¹¹.

Divers effets peuvent se produire lorsqu'un champ incident interagit avec un cristal $\chi^{(2)}$ [Man07]. Le plus emblématique d'entre eux est certainement la génération de seconde harmonique (SHG) : des photons de fréquence ω sont combinés en des photons de fréquence double. Le processus inverse, l'amplification paramétrique optique (OPA), convertit un photon de fréquence 2ω en deux photons de fréquence ω .¹² Si ces deux photons sont générés sur le même mode, l'OPA est dit dégénéré (DOPA) ; s'ils sont émis sur deux modes indépendants, l'OPA est non dégénéré (NOPA). Dans les deux cas, ce processus est une source d'états extrêmement importants pour l'information quantique.

Traitons tout d'abord le cas d'un DOPA, pour lequel les paires de photons sont créées dans le même mode. L'Hamiltonien qui y correspond contient donc un terme en $\hat{a}^{\dagger 2}$, ainsi qu'un terme en \hat{a}^2 pour assurer l'hermiticité :

$$\hat{H} \propto i(\hat{a}^2 - \hat{a}^{\dagger 2}). \quad (2.38)$$

La grandeur de proportionnalité dépend de la force de l'interaction non linéaire, donc de $\chi^{(2)}$. L'équation du mouvement de Heisenberg fournit alors la transformation :

$$\begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}_{out} = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^r \end{pmatrix} \begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}_{in} = S_{DOPA} \begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}_{in}, \quad (2.39)$$

¹¹Les effets non linéaires d'ordre supérieur sont beaucoup moins prononcés et donc difficilement exploitables. Toutefois, dans les cristaux à symétrie d'inversion, les non-linéarités du deuxième ordre s'annulent et celles du troisième ordre sont alors dominantes [NVT06].

¹²SHG et OPA sont des cas particuliers de SFG (sum frequency generation) et DFG (difference frequency generation), respectivement. Cela correspond à un échange d'énergie entre deux modes appelés *signal* et *idler* (*complémentaire*), de fréquences ω_s et ω_i , et un mode appelé *pump* (*pompe*), de fréquence $\omega_p = \omega_s + \omega_i$. Un photon à la fréquence ω_p peut être converti en deux photons de fréquences ω_s et ω_i ou inversement.

où r , proportionnel à la force et au temps d'interaction, est le *facteur de compression*.

Les fluctuations de l'une des quadratures sont comprimées tandis que les fluctuations de l'autre quadrature sont amplifiées : l'état produit, appelé *état comprimé*, a des propriétés purement quantiques. La compression d'une quadrature se fait au détriment de l'autre, de telle sorte que la relation d'incertitude de Heisenberg est toujours vérifiée :

$$\Delta x \Delta p = \frac{1}{2} e^{-2r} e^{2r} = \frac{1}{2} \neq (\Delta x)^2 \neq (\Delta p)^2 \quad (2.40)$$

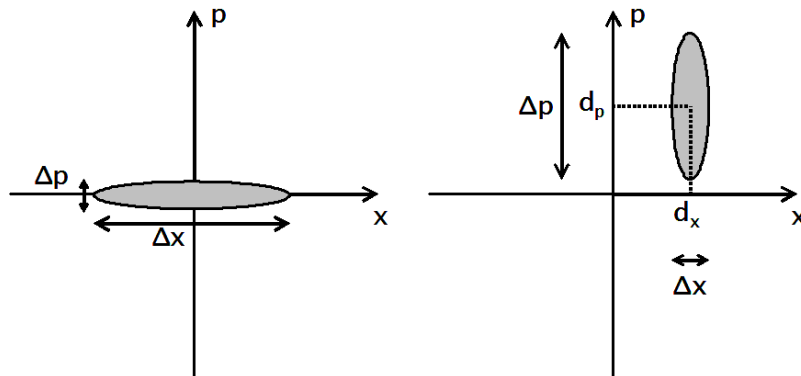


FIG. 2.3 – Représentation dans l'espace des phases d'un état comprimé, (a) à partir du vide, (b) déplacé.

Une représentation schématique est donnée à la figure 2.3. Elle illustre le fait qu'un état comprimé peut être obtenu soit à partir du vide soit à partir d'un état cohérent quelconque. Les rôles des quadratures comprimées et anti-comprimées peuvent être inversés à loisir au moyen d'un terme de phase. On peut également effectuer la compression selon une direction arbitraire θ . Dans tous les cas, cette opération revient à appliquer un *opérateur de compression* $\hat{S}(r, \theta)$ sur $|0\rangle$ ou $|\alpha\rangle$, avec

$$\hat{S}(r, \theta) = \exp\left(\frac{r}{2} (\hat{a}^2 e^{-i\theta} - \hat{a}^{\dagger 2} e^{i\theta})\right). \quad (2.41)$$

La lettre S est utilisée pour symboliser l'opération de *squeezing* – compression, en anglais. L'état du vide comprimé à un mode s'écrit ainsi en base de Fock

$$S(r)|0\rangle = \frac{1}{\cosh r} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh r^n |2n\rangle. \quad (2.42)$$

La série ne contient que des états nombres pairs, les photons étant créés par paires.

Intéressons-nous à présent au cas non dénégéré (NOPA). L'Hamiltonien correspondant s'écrit

$$\hat{H} \propto i(\hat{a}_1 \hat{a}_2 - \hat{a}_1^\dagger \hat{a}_2^\dagger). \quad (2.43)$$

Cette fois la transformation affecte deux modes du champ électromagnétique. Avec (2.32), on peut écrire :

$$\begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \hat{x}_2 \\ \hat{p}_2 \end{pmatrix}_{out} = \begin{pmatrix} \cosh r & 0 & \sinh r & 0 \\ 0 & \cosh r & 0 & -\sinh r \\ \sinh r & 0 & \cosh r & 0 \\ 0 & -\sinh r & 0 & \cosh r \end{pmatrix} \begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \hat{x}_2 \\ \hat{p}_2 \end{pmatrix}_{in} = S_{NOPA} \begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \hat{x}_2 \\ \hat{p}_2 \end{pmatrix}_{in}. \quad (2.44)$$

En base de Fock, l'état du vide comprimé à deux modes s'écrit

$$S(r)|0, 0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} (\tanh r)^n |n, n\rangle \quad (2.45)$$

$$= \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n, n\rangle, \quad (2.46)$$

avec $\lambda = \tanh r$. Les deux modes portent le même nombre de photons.

Si le facteur de compression r (ou λ) est nul ($\cosh r = 1$ et $\sinh r = 0$), l'expression (2.44) montre qu'il n'y a aucun échange d'énergie entre les modes. Par contre, en présence d'un effet non linéaire, il y a interaction. Dans la limite des grands facteurs de compression, pour $r \rightarrow \infty$, on a $\hat{x}_1 = \hat{x}_2$ et $\hat{p}_1 = -\hat{p}_2$. Il y a donc corrélation parfaite entre les quadratures des deux modes : l'état produit est un état EPR.

Formellement, l'état comprimé à deux modes n'est un état EPR que dans la limite d'un facteur de compression infini. A énergie finie, r est limité à des valeurs finies : l'état comprimé à deux modes n'est alors pas un état EPR parfait¹³. Pour disposer de sources d'intrication les plus performantes possibles, des efforts technologiques sont entrepris. Actuellement, plusieurs équipes sont à même de fournir des valeurs de facteurs de compression de l'ordre de 3 dB en régime continu et de 10 dB en régime impulsionnel. La relation

$$r[\text{dB}] = 20 \log_{10}(e^r) = \frac{20}{\ln 10} \times r \quad (2.47)$$

montre qu'une valeur de r de 3 dB (respectivement 10 dB) correspond à $r \approx 0,35$ (respectivement $r \approx 1,15$). Les effets non linéaires sont une ressource essentielle pour produire des états aux propriétés spécifiquement quantiques et de l'intrication.

2.6 Formalisme gaussien

On peut efficacement caractériser un état quantique à n modes, de matrice densité ρ , à l'aide de la *fonction de Wigner*. Définie en fonction des vecteurs propres des quadratures ($\hat{x}|x\rangle = x|x\rangle$), elle s'écrit, dans notre système d'unités,

$$W(x, p) = \frac{1}{(2\pi)^n} \int_{\mathbb{R}^n} \langle x - y | \rho | x + y \rangle e^{iyp} d^n y, \quad x, p \in \mathbb{R}^n. \quad (2.48)$$

La fonction de Wigner jouit de propriétés agréables, comme la linéarité et la normalisation à une valeur unité. Intégrée sur x (respectivement p), elle fournit la distribution marginale correcte de p (respectivement x). Ce n'est toutefois pas une densité de probabilité classique, car elle peut revêtir des caractéristiques particulières : par exemple, elle prend parfois des valeurs négatives – trace claire du caractère quantique d'un état. C'est une fonction dite de quasi-probabilité.

Nous allons nous intéresser à une classe d'états particuliers, les *états gaussiens*, qui ont une fonction de Wigner gaussienne :

$$W(r) = \frac{1}{\pi^n \sqrt{\det \gamma}} e^{-(r-d)^T \gamma^{-1} (r-d)}. \quad (2.49)$$

¹³Selon une pratique courante nous l'appellerons néanmoins ainsi.

Dans cette expression, nous avons groupé les quadratures de l'état à n modes en un vecteur

$$r = (r_1, \dots, r_{2n})^T = (x_1, p_1, x_2, p_2, \dots, x_n, p_n)^T, \quad (2.50)$$

nous utilisons le vecteur des moyennes

$$d = \text{Tr}[\rho \hat{r}] = \langle \hat{r} \rangle, \quad (2.51)$$

et nous définissons la matrice de covariance, symétrique et de taille $2n \times 2n$, dont les coefficients s'écrivent

$$\gamma_{ij} = \text{Tr}[\rho \{(\hat{r}_i - d_i), (\hat{r}_j - d_j)\}], \quad (2.52)$$

où $\{\hat{A}, \hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$ désigne l'anti-commutateur de deux opérateurs.

Les états gaussiens appartiennent à un espace de Hilbert de dimension infinie mais sont entièrement caractérisés par leurs premier et deuxième moments. Cette description aisée en fait une classe d'états privilégiée. A titre d'exemple, un état monomode de valeur moyenne nulle est décrit par une matrice de covariance

$$\gamma = \begin{pmatrix} \langle 2x^2 \rangle & \langle xp + px \rangle \\ \langle xp + px \rangle & \langle 2p^2 \rangle \end{pmatrix}. \quad (2.53)$$

Dans le cas d'états gaussiens à plusieurs modes, il est toujours possible par des opérations locales de se ramener à un choix de base où les quadratures en x et p sont découplées [Our07]. Dans le cas d'un système à deux modes dont les quadratures sont de valeurs moyennes nulles, la matrice de covariance devient alors

$$\gamma = \begin{pmatrix} \langle 2x_1^2 \rangle & 0 & \langle x_1x_2 + x_2x_1 \rangle & 0 \\ 0 & \langle 2p_1^2 \rangle & 0 & \langle p_1p_2 + p_2p_1 \rangle \\ \langle x_1x_2 + x_2x_1 \rangle & 0 & \langle 2x_2^2 \rangle & 0 \\ 0 & \langle p_1p_2 + p_2p_1 \rangle & 0 & \langle 2p_2^2 \rangle \end{pmatrix}. \quad (2.54)$$

Outre l'avantage d'une description mathématique simple, les états gaussiens s'avèrent être une classe très générale d'états : ils représentent la quasi-totalité des états manipulés en optique quantique. En particulier, les états cohérents, les états comprimés et les états EPR sont des états gaussiens. L'état du vide et les états cohérents ont une matrice de covariance $\gamma = \mathbb{I}$ et un vecteur déplacement $d = (d_x, d_p)$, nul dans le cas du vide. Les états comprimés à un mode ont une matrice de covariance qui s'écrit

$$\gamma = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}, \quad (2.55)$$

tandis que la matrice de covariance des états comprimés à deux modes est

$$\gamma = \begin{pmatrix} \cosh 2r \mathbb{I} & \sinh 2r \sigma_z \\ \sinh 2r \sigma_z & \cosh 2r \mathbb{I} \end{pmatrix}, \quad (2.56)$$

où la matrice identité \mathbb{I} et la matrice de Pauli σ_z s'écrivent

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.57)$$

La présence d'éléments non diagonaux non nuls dans une matrice de covariance multi-mode est le signe de corrélations.

Que la grande majorité des états manipulés en optique quantique soient des états gaussiens s'explique par deux réalités expérimentales. Premièrement, les états cohérents fournis par les lasers sont gaussiens. Deuxièmement, les transformations qu'ils subissent sont principalement des *transformations gaussiennes* : elles préservent le caractère gaussien des états gaussiens. Les transformations étudiées jusqu'à présent constituent des éléments de cette classe. Elles sont représentées par une matrice S dite *symplectique*, c'est-à-dire qui vérifie la relation

$$S\sigma S^T = \sigma \quad (2.58)$$

pour toute matrice σ de taille $2n \times 2n$, bloc-diagonale et anti-symétrique, de la forme

$$\sigma = \bigoplus_{j=1}^n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (2.59)$$

Le groupe des matrices symplectiques est constitué des matrices correspondant aux transformations passives (par exemple S_{PS} et S_{BS}) et de celles correspondant aux transformations actives (par exemple S_{DOPA} et S_{NOPA}). Ces dernières modifient le nombre de photons contenus dans le système.

Une matrice symplectique S agit sur un état de vecteur \hat{r} et de matrice de covariance γ de telle sorte que :

$$\hat{r}_{out} = S \hat{r}_{in} \quad \text{et} \quad \gamma_{out} = S \gamma_{in} S^T. \quad (2.60)$$

En guise d'illustration, nous pouvons voir un état EPR, produit comme nous l'avons vu par pompage optique d'un milieu non linéaire, comme équivalent à l'état à deux modes émergent d'un diviseur de faisceau équilibré où l'on a fait interagir deux états comprimés dans des directions orthogonales, comme schématisé sur la figure 2.4.

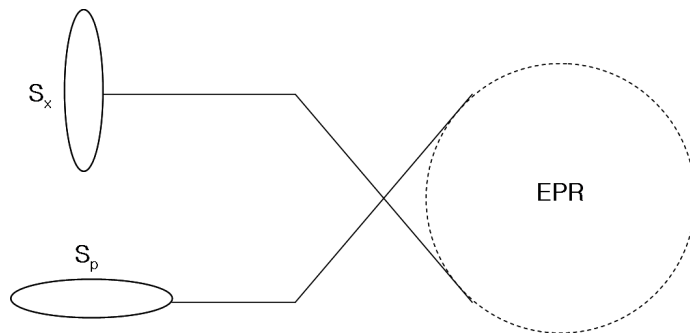


FIG. 2.4 – Equivalence entre un état EPR et la combinaison sur un diviseur de faisceau équilibré de deux états comprimés dans des directions orthogonales.

Soit donc $\hat{r}_1 = (e^r x_1^{(0)}, e^{-r} p_1^{(0)})^T$ et $\hat{r}_2 = (e^{-r} x_2^{(0)}, e^r p_2^{(0)})^T$. Après passage dans un diviseur de faisceau équilibré, les opérateurs de quadrature de l'état du vide comprimé à deux modes peuvent s'écrire comme

$$\begin{pmatrix} \hat{r}_1 \\ \hat{r}_2 \end{pmatrix}_{out} = \begin{pmatrix} \sqrt{T} \mathbb{I} & \sqrt{1-T} \mathbb{I} \\ -\sqrt{1-T} \mathbb{I} & \sqrt{T} \mathbb{I} \end{pmatrix} \begin{pmatrix} \hat{r}_1 \\ \hat{r}_2 \end{pmatrix}_{in}, \quad (2.61)$$

en utilisant la transformation (2.35). Le diviseur de faisceau étant équilibré, on obtient :

$$\begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \hat{x}_2 \\ \hat{p}_2 \end{pmatrix}_{out} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^r x_1^{(0)} + e^{-r} x_2^{(0)} \\ e^{-r} p_1^{(0)} + e^{+r} p_2^{(0)} \\ e^{+r} x_1^{(0)} - e^{-r} x_2^{(0)} \\ e^{-r} p_1^{(0)} - e^{+r} p_2^{(0)} \end{pmatrix} \quad (2.62)$$

Sachant que $\langle x_1^{(0)2} \rangle = \langle p_1^{(0)2} \rangle = \langle x_2^{(0)2} \rangle = \langle p_2^{(0)2} \rangle = 1/2$, en prenant la moyenne du carré des expressions ci-dessus, on obtient

$$\langle x_1^2 \rangle = \langle p_1^2 \rangle = \langle x_2^2 \rangle = \langle p_2^2 \rangle = \frac{1}{4}(e^{2r} + e^{-2r}) = \frac{\cosh(2r)}{2}, \quad (2.63)$$

$$\langle x_1 x_2 \rangle = -\langle p_1 p_2 \rangle = \frac{1}{4}(e^{2r} - e^{-2r}) = \frac{\sinh(2r)}{2}. \quad (2.64)$$

En utilisant directement la formule (2.60), on peut également montrer que la matrice de covariance obtenue est bien celle d'un état EPR :

$$\gamma_{EPR} = \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}. \quad (2.65)$$

Selon la définition (2.52), l'élément $V_{q_i q_j}$ (où $q = x$ ou p et $1 \leq i, j \leq n$) d'une matrice de covariance à n modes est en effet le *double* de l'expression $\langle q_i q_j \rangle$. La variance du vide prend donc une valeur unitaire :

$$N_0 \equiv V_{q^{(0)}} = 2 \langle q^{(0)2} \rangle = 1, \quad (2.66)$$

où nous écrivons $V_{q_i^2} \equiv V_{q_i}$. La convention $N_0 = 1$ est baptisée *shot noise unit*, du nom du bruit de grenaille que l'on prend pour référence. Comme l'état du vide sature l'inégalité de Heisenberg, tout état aura une variance $N \geq N_0$.

2.7 Trace partielle

De façon générale, un état gaussien bimode est décrit par une matrice de covariance

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix}, \quad (2.67)$$

où C est non nulle en présence de corrélations. Il est possible de traiter séparément l'état individuel A (ou B) au moyen d'une opération de *trace partielle*. En termes de vecteur déplacement et matrice de covariance, l'opération $\text{Tr}_B[\rho_{AB}]$ s'écrit :

$$d_{AB} = (d_A, d_B)^T \rightarrow d_A \quad , \quad \gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix} \rightarrow \gamma_A. \quad (2.68)$$

Par exemple, si l'on effectue cette opération sur un état EPR,

$$\gamma_{EPR} = \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix} \quad (2.69)$$

$$= \begin{pmatrix} V & 0 & \sqrt{V^2-1} & 0 \\ 0 & V & 0 & -\sqrt{V^2-1} \\ \sqrt{V^2-1} & 0 & V & 0 \\ 0 & -\sqrt{V^2-1} & 0 & V \end{pmatrix} \rightarrow \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}, \quad (2.70)$$

on obtient un état thermique de variance $V = \cosh(2r) = 2n + 1$. L'état EPR est un état particulier seulement si l'on regarde ses propriétés *globales*.

Cette opération n'est plus unitaire car elle correspond à une perte d'information. Pour décrire les opérations irréversibles, on utilise un *map gaussien* plus général, basé sur l'utilisation de deux matrices X et Y , et tel que

$$d_{out} = X d_{in} \quad , \quad \gamma_{out} = X \gamma_{in} X^T + Y. \quad (2.71)$$

Pour illustrer cette notion, considérons l'exemple important de l'*amplification* d'un signal, à l'aide d'effets non linéaires. Cette opération est décrite quantiquement par l'interaction du mode *signal* avec un mode complémentaire *idler*, qui est initialement dans l'état vide. L'interaction se fait au moyen d'un NOPA dont nous rappelons ci-dessous l'effet, défini en (2.44) :

$$\begin{pmatrix} r_{signal} \\ r_{idler} \end{pmatrix}_{out} = \begin{pmatrix} \sqrt{G} \mathbb{I} & \sqrt{G-1} \sigma_z \\ \sqrt{G-1} \sigma_z & \sqrt{G} \mathbb{I} \end{pmatrix} \begin{pmatrix} r_{signal}^{(0)} \\ r_{idler}^{(0)} \end{pmatrix}_{in}, \quad (2.72)$$

où $r = (x, p)^T$. Le gain de l'amplificateur est $G = \cosh^2 r$, r désignant cette fois le facteur de compression. L'opération bimodale est unitaire. Toutefois, en pratique, le mode *idler* n'est pas utilisé. Si l'on ne considère que le mode *signal*, celui-ci est certes amplifié, mais il est aussi "bruté" à cause de l'interaction avec le mode complémentaire. Dans le formalisme gaussien généralisé, cela est décrit par les expressions (2.71), avec $X = \sqrt{G} \mathbb{I}$ et $Y = (G - 1) \mathbb{I}$.

Une amplification s'accompagne toujours de bruit quantique : cette constatation fondamentale montre toute la difficulté des communications quantiques à longue distance, car on ne peut pas amplifier un signal sans en payer le prix. Nous verrons au chapitre suivant que les pertes dans un canal correspondent à une situation similaire.

2.8 Mesures

Si l'évolution d'un système quantique isolé est réversible et correspond à des interactions unitaires dans l'espace des états, ce n'est en revanche plus le cas lorsque ce système interagit avec l'environnement.

Par exemple, l'interaction avec un appareil de mesure se traduit par des projections dans l'espace de Hilbert. Nous utiliserons cette notion dans le chapitre 4.

Les quadratures d'un mode de lumière sont des observables et sont donc mesurables. Toutefois, dans le domaine optique, le champ oscille à des fréquences de l'ordre de 500 THz , ce qui rend sa mesure directe impossible. Ci-dessous nous décrivons une technique de mesure basée sur l'interférence, appelée *détection homodyne* équilibrée [SZ97]. Le principe est illustré à la figure 2.5.

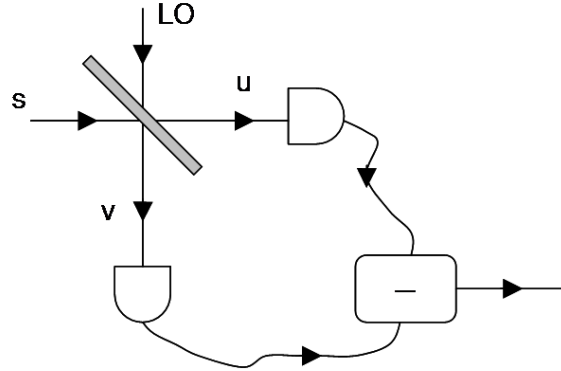


FIG. 2.5 – Mesure d'une quadrature au moyen d'une détection homodyne.

Supposons donc que l'on veuille mesurer une quadrature d'un état quantique préparé dans le mode *signal*, de quadratures \hat{x}_s et \hat{p}_s . Pour ce faire, on le fait interférer à travers un diviseur de faisceau équilibré avec le champ d'un oscillateur local, de quadratures \hat{x}_{LO} et \hat{p}_{LO} . Les modes de sortie s'écrivent :

$$\begin{pmatrix} \hat{x}_u \\ \hat{p}_u \\ \hat{x}_v \\ \hat{p}_v \end{pmatrix}_{out} = \frac{1}{\sqrt{2}} \begin{pmatrix} \hat{x}_s + \hat{x}_{LO} \\ \hat{p}_s + \hat{p}_{LO} \\ \hat{x}_s - \hat{x}_{LO} \\ \hat{p}_s - \hat{p}_{LO} \end{pmatrix}. \quad (2.73)$$

Leurs intensités sont mesurées à l'aide de deux photodiodes. Elles sont proportionnelles au nombre moyen de photons présents dans le faisceau :

$$I_{u,v} \propto \hat{N}_{u,v} = \frac{1}{2} (\hat{x}_{u,v}^2 + \hat{p}_{u,v}^2 - 1). \quad (2.74)$$

Le champ de l'oscillateur local est d'intensité élevée. On peut donc négliger ses fluctuations quantiques et remplacer les opérateurs de quadratures par des grandeurs réelles : $(\hat{x}_{LO}, \hat{p}_{LO}) \rightarrow (X_{LO}, P_{LO})$. Le champ (classique) vaut alors

$$E_{LO} = |E_{LO}| e^{i\omega t} = |X_{LO} + iP_{LO}| e^{i\omega t}. \quad (2.75)$$

De plus, on peut choisir la phase de l'oscillateur local comme référence : $(X_{LO}, P_{LO}) \rightarrow (X_{LO}, 0)$. Sous ces conditions, on peut estimer la valeur d'une quadrature du champ *signal* en effectuant la soustraction des deux photocourants mesurés,

$$\Delta I = I_u - I_v \propto X_{LO} \hat{x}_s. \quad (2.76)$$

Le facteur X_{LO} , racine carrée de l'intensité de l'oscillateur local classique, peut être mesuré. Il permet d'amplifier les variations quantiques du champ *signal* pour qu'elles soient mesurables macroscopiquement.

Dans ce cas-ci, le résultat ΔI nous permet de déduire la valeur de x . Pour déterminer p , il aurait suffi de tourner la phase de l'oscillateur local de nonante degrés. On peut de la même façon déterminer une quadrature x_θ arbitrairement orientée.

Il est possible de mesurer les deux quadratures simultanément, au moyen d'une *détection hétérodyne*. Comme le montre la figure 2.6, il faut alors scinder le faisceau d'entrée sur un diviseur de faisceau, et effectuer une détection homodyne sur chaque sortie. Comme \hat{x} et \hat{p} sont des variables canoniquement conjuguées, une détection hétérodyne ne peut pas fournir une précision arbitraire.

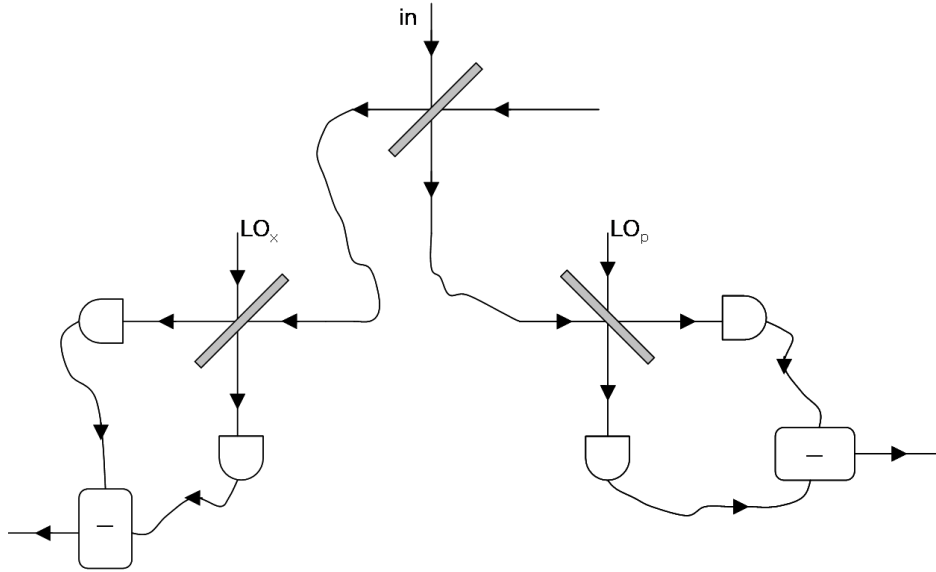


FIG. 2.6 – Mesure des deux quadratures au moyen d'une détection hétérodyne.

La mesure de quadratures est un élément essentiel du protocole de téléportation quantique abordé dans la section suivante.

2.9 Téléportation quantique

Il est possible de *téléporter* un état quantique inconnu d'un système physique à un autre. Le théorème de non-clonage présenté à la section 1.3 montre qu'une telle opération n'est pas triviale. Pour que l'on puisse parler de téléportation quantique, trois critères sont généralement retenus : [BvL05]

- Un état quantique “inconnu” entre dans la station envoyeuse pour la téléportation.
- Un état téléporté émerge de la station receveuse pour évaluation ou exploitation.
- Le *degré de fidélité* entre l'état d'entrée et l'état téléporté est plus grand que ce qui pourrait être réalisé si la station envoyeuse et la station receveuse étaient liées par un canal classique.

En utilisant des techniques classiques, on ne peut créer qu'une pâle copie d'un état donné. Un protocole utilisant une ressource typiquement quantique, l'intrication, permet d'améliorer ce résultat. Nous décrivons ci-dessous la version *variables continues*, similaire à celle en *variables discrètes* présentée notamment dans [NC00], et qui a également été réalisée expérimentalement. L'ensemble de la procédure est schématisé à la figure 2.7.

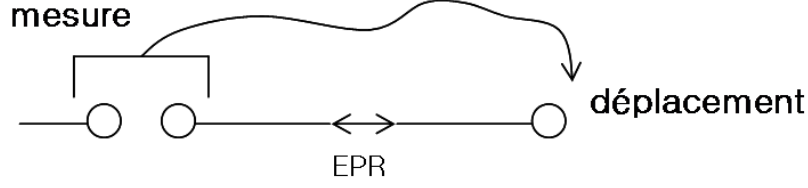


FIG. 2.7 – Protocole de téléportation : partage d’une paire EPR, mesure jointe, communication classique et déplacement.

La situation est la suivante : Alice dispose d’un état inconnu $|\psi\rangle$ et souhaite le transmettre à Bob. Pour ce faire, Alice et Bob peuvent se partager les modes 1 et 2 d’une paire EPR :

$$\begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \hat{x}_2 \\ \hat{p}_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{+r} x_1^{(0)} + e^{-r} x_2^{(0)} \\ e^{-r} p_1^{(0)} + e^{+r} p_2^{(0)} \\ e^{+r} x_1^{(0)} - e^{-r} x_2^{(0)} \\ e^{-r} p_1^{(0)} - e^{+r} p_2^{(0)} \end{pmatrix} \quad (2.77)$$

Pour effectuer la téléportation, Alice effectue une mesure jointe, ou *mesure de Bell* : à l’aide d’un diviseur de faisceau équilibré, elle combine son mode avec le mode “in” à téléporter. Les états u et v de sortie sont :

$$\begin{pmatrix} \hat{x}_u \\ \hat{p}_u \\ \hat{x}_v \\ \hat{p}_v \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} x_{in} - x_1 \\ p_{in} - p_1 \\ x_{in} + x_1 \\ p_{in} + p_1 \end{pmatrix} \quad (2.78)$$

Alice transmet alors les valeurs x_u et p_v à Bob, qui déplace¹⁴ son mode de la paire EPR pour fournir l’état téléporté,

$$x_{tel} = x_2 + g x_u \quad (2.79)$$

$$= \frac{g}{\sqrt{2}} x_{in} - \frac{g - \sqrt{2}}{2} e^{+r} x_1^{(0)} - \frac{g + \sqrt{2}}{2} e^{-r} x_2^{(0)}, \quad (2.80)$$

$$p_{tel} = p_2 + g p_v \quad (2.81)$$

$$= \frac{g}{\sqrt{2}} p_{in} + \frac{g - \sqrt{2}}{2} e^{+r} p_2^{(0)} + \frac{g + \sqrt{2}}{2} e^{-r} p_1^{(0)}, \quad (2.82)$$

$$(2.83)$$

g étant le gain du déplacement appliqué. Le fait d’utiliser x_u et p_v , et non x_v et p_u , n’est pas anodin. Pour $g = \sqrt{2}$,

$$x_{tel} = x_{in} - \sqrt{2} e^{-r} x_2^{(0)}, \quad (2.84)$$

$$p_{tel} = p_{in} + \sqrt{2} e^{-r} p_1^{(0)}, \quad (2.85)$$

et la téléportation sera parfaitement réalisée si le facteur de compression de la paire EPR est infini. Cette situation étant irréalisable en pratique, on quantifie “l’écart” entre l’état

¹⁴On montre aisément avec l’expression (2.35) que l’opération de déplacement $D(\alpha)$ évoquée à la section 2.3 est réalisée en combinant dans un diviseur de faisceau de transmittance $T \approx 1$ un signal avec un champ local cohérent de forte intensité $I = \alpha/(1 - T)$.

d'entrée et l'état téléporté à l'aide des variances

$$\langle x_{tel}^2 \rangle = \langle x_{in}^2 \rangle + 2e^{-2r} \langle x_2^{(0)2} \rangle \rightarrow V_{x_{tel}} = V_{x_{in}} + 2e^{-2r} N_0 \equiv V_{x_{in}} + \delta, \quad (2.86)$$

$$\langle p_{tel}^2 \rangle = \langle p_{in}^2 \rangle + 2e^{-2r} \langle p_1^{(0)2} \rangle \rightarrow V_{p_{tel}} = V_{p_{in}} + 2e^{-2r} N_0 \equiv V_{p_{in}} + \delta, \quad (2.87)$$

où l'on a défini $\delta = V_{x_{tel}} - V_{x_{in}} = V_{p_{tel}} - V_{p_{in}}$. L'état téléporté est une reproduction d'autant plus fidèle de l'état d'entrée que la source d'intrication s'approche d'un état EPR parfait : $\delta = 2e^{-2r} N_0 \rightarrow 0$ pour $r \rightarrow \infty$. A l'opposé, pour $r = 0$, chacune des quadratures téléportées a deux unités additionnelles de bruit du vide par rapport aux quadratures originales. Ces deux unités sont appelées les “*quduties*” : c'est le prix à payer pour téléporter un état en l'absence d'intrication [BvL05].

Pour quantifier le fait que nous disposons d'une source d'intrication imparfaite ($0 < r < \infty$), nous utilisons la notion de fidélité. La fidélité entre un état de matrice densité σ et un état de matrice densité ρ s'écrit :

$$F = \text{Tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}. \quad (2.88)$$

Dans le cas où σ est un état pur $|\psi\rangle$, F devient :

$$F = \text{Tr} [|\psi\rangle\langle\psi| \rho] = (2\pi)^n \int_{\mathbb{R}^{2n}} W_{|\psi\rangle\langle\psi|}(r) W_{\rho}(r) d^{2n}r. \quad (2.89)$$

Dans le cas d'états gaussiens, dont l'un est pur, F s'écrit encore :

$$F = \frac{C}{\sqrt{\det(\gamma_{in} + \gamma_{out})}}. \quad (2.90)$$

La constante C vaut 2 pour un état d'entrée cohérent ($\gamma_{in} = \mathbb{I}$), car elle est définie de telle sorte que la fidélité vaut 1 si l'état de sortie est le même que l'état d'entrée. Si la différence entre les variances de l'état d'entrée et de l'état de sortie vaut δ , F devient :

$$F = \frac{2}{2 + \delta}. \quad (2.91)$$

Dans le cadre du protocole de téléportation présenté ci-dessus, la fidélité entre l'état d'entrée et l'état téléporté est :

$$F = \frac{1}{1 + e^{-2r}}. \quad (2.92)$$

La fidélité est une grandeur variant entre 0 et 1. Entre ces deux bornes, présentons deux valeurs particulières :

- Pour $\delta = 2$, on obtient la valeur $F = 1/2$. C'est la fidélité maximale obtenue en effectuant une téléportation en l'absence d'intrication ($r = 0$). Cette limite distingue fondamentalement les domaines classique et quantique.
- Pour $\delta = 1$ (la variance de l'état de sortie est doublée par rapport à celle de l'état d'entrée cohérent), on obtient la valeur $F = 2/3$. Cette borne revêt une grande importance dans certains protocoles de cryptographie quantique. Au-delà d'une telle valeur, on est en effet assuré – grâce au théorème de non-clonage quantique – qu'aucune copie de meilleure qualité n'a pu être produite. Dans le cadre du protocole de téléportation quantique, la valeur $F = 2/3$ est atteinte pour $r = \ln 2/2 \approx 0,35$.

Comme nous l'avons signalé, la présence d'intrication permet en théorie d'obtenir une fidélité de valeur unitaire. A cause des imperfections des corrélations EPR¹⁵, cette borne n'est jamais atteinte. Une autre source d'imperfection doit également être prise en compte : il se produit une perte partielle des corrélations EPR lors d'une transmission séparée dans un canal à pertes, au contact de l'environnement. Nous reviendrons sur ces aspects dans le prochain chapitre.

¹⁵Il s'agit du prix à payer pour travailler avec des variables continues : les états sont plus aisés à manipuler, les protocoles sont inconditionnels, mais nous ne disposons pas d'une source d'intrication parfaite, r étant fini.

Chapitre 3

Propagation d'états gaussiens

Make everything as simple as possible, but not simpler. (A. Einstein)

Le but de notre travail est d'établir des *schémas de transmission* les plus *efficaces* possibles. Dans un premier temps, il est nécessaire de définir, d'une part la ligne de transmission, et d'autre part ce que l'on entend par le terme *efficacité*, afin de pouvoir comparer les performances des schémas envisagés.

Comme représenté à la figure 3.1, nous considérons un canal quantique de longueur L , dans lequel des états quantiques peuvent se propager d'une entrée *in* à une sortie *out*. Ce peut être par exemple une fibre optique.

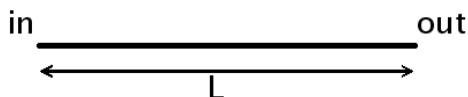


FIG. 3.1 – Canal de longueur L .

Nous supposons vouloir envoyer un état cohérent de l'entrée vers la sortie. Comme nous l'avons vu, les états cohérents sont les états produits en sortie d'un laser et sont par conséquent très utilisés en information quantique. Des protocoles de cryptographie quantique sont par exemple basés sur la modulation d'états cohérents. Par ailleurs, un état cohérent est gaussien, ce qui permet un traitement mathématique simple. Il est entièrement caractérisé par ses valeurs moyennes d_x et d_p (que nous supposons quelconques) et sa matrice de covariance $\gamma = \mathbb{I}$.

L'objectif est d'obtenir en sortie du canal une reproduction la plus *fidèle* possible de l'état envoyé. La transmission sera considérée comme parfaite si les moyenne et variance des quadratures sont identiques en entrée et en sortie : idéalement, l'état de sortie est centré au même endroit de l'espace des phases et sature toujours l'inégalité de Heisenberg, de telle sorte que ses fluctuations quantiques sont minimales.

Dans la première section, nous décrivons l'effet des pertes et du bruit d'un canal dans le cas d'une transmission directe. Nous formalisons ensuite l'évolution des paramètres du

canal en fonction de la distance. Cela nous permettra de traiter des schémas de répétition de l'information scindant la ligne en différents tronçons. La première amélioration envisagée est l'amplification du signal. Nous utilisons ensuite l'intrication quantique de paires EPR pour téléporter l'état à transmettre, cette opération ayant un impact fondamental sur la transmission.

3.1 Transmission directe

Considérons un premier schéma de transmission où l'état cohérent est envoyé directement de l'entrée à la sortie du canal. Celui-ci présente des pertes intrinsèques, que nous supposons réparties de façon homogène et notons :

$$T_L = e^{-\alpha L}, \quad (3.1)$$

où $\alpha [m^{-1}]$ est le *coefficient d'atténuation*. Ces pertes de puissance par unité de longueur sont aisément converties en décibels :

$$\begin{aligned} \alpha [dB km^{-1}] &= -\frac{10}{1km} \times \log_{10} \frac{P(z = 1000m)}{P(z = 0)} = 10000 \times \log_{10} e \times \alpha [m^{-1}] \\ &= 4343 \alpha [m^{-1}] = 4,343 \alpha [km^{-1}]. \end{aligned}$$

Typiquement, pour des fibres optiques standard aux longueurs d'onde télécom, α est de l'ordre de $0,2 dB/km$, soit $0,046 km^{-1}$. Le paramètre adimensionnel T , qui varie entre 0 et 1, sera utilisé préférentiellement pour effectuer des variations ou des comparaisons dans nos développements ultérieurs¹. Le tableau ci-dessous permettra de garder à l'esprit les ordres de grandeur des distances correspondant à une valeur donnée de T ou αL , dans le cas d'une fibre télécom standard. Retenons par exemple la valeur de $L = \ln(2)/\alpha$ pour $T = 1/2$.

T	αL	$L [km]$
1	0	0
0,9	0,105	2,288
0,8	0,223	4,846
0,7	0,357	7,745
0,6	0,511	11,092
0,5	0,693	15,051
0,4	0,916	19,897
0,3	1,204	26,144
0,2	1,609	34,949
0,1	2,303	50,000
0	∞	∞

TAB. 3.1 – Tableau de correspondance entre T , αL et L , pour une valeur $\alpha = 0,2 dB/km$.

Classiquement, les pertes se traduisent par une décroissance exponentielle de l'intensité du faisceau transmis. Du point de vue quantique, les pertes elles-mêmes doivent être considérées comme un *bruit* : lors de sa transmission, le signal est "mêlé" avec l'état

¹Ce qui a le petit inconvénient d'obliger à lire de droite à gauche les graphiques tracés en fonction de T , si l'on veut les lire dans le sens d'une distance parcourue croissante.



FIG. 3.2 – Equivalence entre un canal à pertes et un canal parfait précédé d'un diviseur de faisceau.

du vide. Un canal à pertes sera ainsi modélisé par un canal parfait de longueur L coupé par un diviseur de faisceau de transmittivité² T_L , comme illustré à la figure 3.2.

Les deux entrées de ce diviseur de faisceau contiennent d'une part le signal, de quadratures³ x_{in} et p_{in} , et d'autre part le vide, de quadratures⁴ x_E et p_E . La transformation (2.35) du diviseur de faisceau affecte les quadratures d'entrée de telle sorte que

$$x_{out} = \sqrt{T_L} x_{in} + \sqrt{1 - T_L} x_E, \quad (3.2)$$

$$p_{out} = \sqrt{T_L} p_{in} + \sqrt{1 - T_L} p_E. \quad (3.3)$$

De façon similaire que lors d'une amplification (section 2.7), le mode auxiliaire n'est pas considéré en sortie, mais affecte le signal. La transformation devient dès lors irréversible et peut être décrite dans le cadre du formalisme gaussien généralisé, avec $X = \sqrt{T_L}\mathbb{I}$ et $Y = (1 - T_L)\mathbb{I}$ dans les expressions (2.71).

Les quadratures du vide ayant des valeurs moyennes nulles, on a :

$$\langle x_{out} \rangle = \sqrt{T_L} \langle x_{in} \rangle, \quad (3.4)$$

$$\langle p_{out} \rangle = \sqrt{T_L} \langle p_{in} \rangle. \quad (3.5)$$

Pour compenser l'atténuation – d'un facteur $\sqrt{T_L} < 1$ – et égaler les valeurs moyennes, il est nécessaire d'effectuer un *upscaling* en multipliant⁵ les résultats obtenus par $1/\sqrt{T_L}$. L'introduction de ce facteur d'échelle n'est pas sans conséquence pour les variances des quadratures :

$$V_{x_{out}} = T_L V_{x_{in}} + (1 - T_L) V_{x_E} \rightarrow V_{x_{out}} = V_{x_{in}} + \frac{1 - T_L}{T_L} V_{x_E} \quad (3.6)$$

$$V_{p_{out}} = T_L V_{p_{in}} + (1 - T_L) V_{p_E} \rightarrow V_{p_{out}} = V_{p_{in}} + \frac{1 - T_L}{T_L} V_{p_E} \quad (3.7)$$

En sortie, les variances des quadratures de l'état sont augmentées d'un terme χ_L , le bruit ramené à l'entrée d'un canal quantique de longueur L :

$$\chi_L = V_{x_{out}} - V_{x_{in}} = V_{p_{out}} - V_{p_{in}} = \frac{1 - T_L}{T_L} N_0, \quad (3.8)$$

²Ce qui justifie l'utilisation de la lettre T pour symboliser les pertes.

³Dans la suite de ce travail, les *opérateurs* de quadrature \hat{x} et \hat{p} seront notés x et p sans risque de confusion.

⁴L'indice E est placé pour *Eve*, suivant les conventions adoptées en cryptographie, selon lesquelles tout bruit est imputé à un espion potentiel.

⁵Remarquons qu'il s'agit d'une opération purement mathématique, qui ne correspond à aucune amplification physiquement réalisée, qui inévitablement ajouterait du bruit.

où nous avons écrit $V_{x_E} = V_{p_E} = N_0 = 1$, la variance du vide. Cette valeur N_0 est multipliée par une expression doublement dépendante de T_L .

Premièrement, le facteur $1 - T_L$ traduit l'influence de l'interaction du signal avec l'environnement, qui est d'autant plus importante que la distance de propagation est grande.

Deuxièmement, le facteur $1/T_L$ provient du fait que, l'atténuation du signal augmentant avec la distance, la variance du vide prend une valeur relative d'autant plus grande. L'*upscaling*, ou mise à l'échelle, traduit cet effet. C'est pour cette raison que l'on utilise l'expression de bruit "ramené à l'entrée".

La situation que nous avons traitée ci-dessus est celle d'un canal sans *bruit ajouté*. Il est possible d'étendre aisément cette description au cas d'un canal *avec* bruit ajouté⁶. Si nous considérons que le bruit est gaussien, de valeur moyenne nulle et symétrique en x et p , les développements effectués restent valables, à ceci près que l'état interagissant avec le signal n'est plus le vide mais un état thermique de variance supérieure : $V_{x_E} = V_{p_E} = N \geq N_0$.

Le coefficient $\chi_L \equiv (1 - T_L)/(T_L)N$ représente toujours la valeur du bruit ramenée à l'entrée. Nous pouvons décomposer son expression sous la forme d'une somme, le premier terme correspondant au bruit du vide, le second au bruit ajouté :

$$\chi_L = \frac{1 - T_L}{T_L} + \epsilon_L, \quad (3.9)$$

avec, par définition :

$$\epsilon_L = \frac{1 - T_L}{T_L}(N - 1) \quad \Leftrightarrow \quad N = 1 + \frac{T_L}{1 - T_L}\epsilon_L. \quad (3.10)$$

En pratique, ϵ est un terme correctif de petite valeur : l'écart entre N et N_0 est de l'ordre de 1% de N_0 . Nous pouvons donc considérer en bonne approximation que N a une valeur unitaire. Dans nos futurs développements, nous vérifions que de légères variations ne modifient pas les conclusions qualitatives que l'on peut en tirer.

La figure 3.3 représente l'évolution de χ en fonction de T pour un canal sans bruit ajouté⁷. La transmission est évidemment parfaite pour une longueur arbitrairement petite ($T \rightarrow 1$) tandis qu'elle devient très mauvaise pour $L \rightarrow \infty$ ($T \rightarrow 0$). Nous pouvons remarquer que pour $T = 1/2$, $\chi = 1$: à cette position intermédiaire, la variance d'un état cohérent est doublée entre l'entrée et la sortie.

La figure 3.4 représente le schéma équivalent en termes de fidélité entre l'état cohérent d'entrée et l'état de sortie⁸. Elle vaut $2/3$ pour $T = 1/2$ et passe sous le seuil de $1/2$ pour $T < 1/3$, comme on peut le vérifier avec la formule (2.91) dans le cas où $\delta = (1 - T)/T$.

⁶Remarquons que nous supposons un bruit optique purement dû au canal. Les systèmes d'émission et de détection sont considérés comme parfaitement efficaces et parfaitement couplés à la ligne de transmission.

⁷Un graphique tout à fait équivalent est obtenu pour un canal avec bruit ajouté ; χ sera simplement multiplié par le facteur $N > 1$ correspondant. Cet effet n'est toutefois pas visible sur la figure pour les valeurs courantes de bruit ajouté.

⁸Les valeurs moyennes sont artificiellement égalées par l'*upscaling*.

Nous constatons que lors de communications quantiques dans des lignes de transmission, les états quantiques sont soumis à des couplages avec l'environnement. Leur évolution temporelle dépend de l'interaction subie avec, soit le vide, soit un état thermique de variance supérieure. Ils subissent ainsi non seulement des pertes, mais également de la décohérence. Cette description est un bon modèle de transmission de la lumière dans des fibres optiques⁹ [CLP07]. Il est donc indispensable de modifier le schéma de transmission pour tenter d'améliorer la portée des communications quantiques.

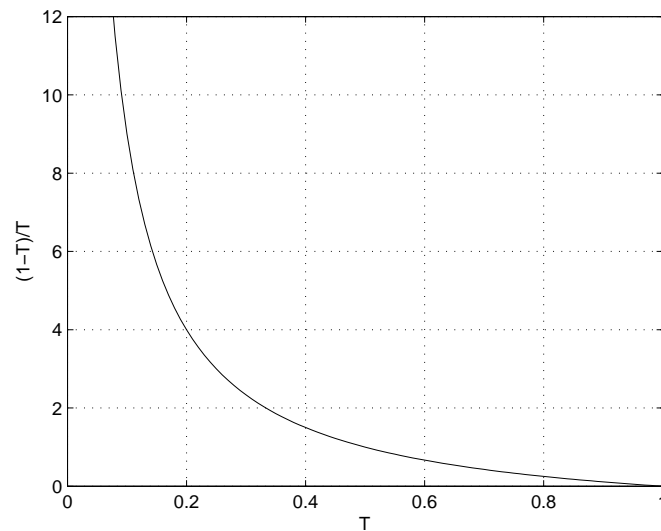


FIG. 3.3 – Evolution de χ en fonction de T .

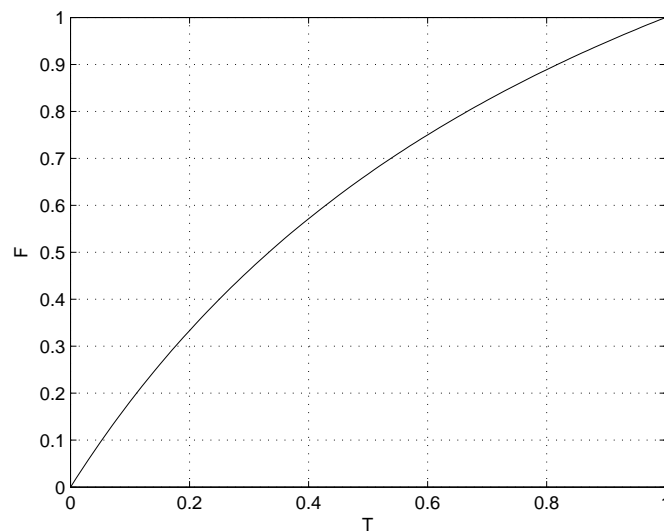


FIG. 3.4 – Evolution de $F = 2/(2 + \chi)$ en fonction de T .

⁹Plus largement, toute évolution temporelle peut être vue comme l'action d'un canal.

3.2 Modélisation du canal par tronçons

Supposons que la ligne de transmission de longueur L est subdivisée en k tronçons de longueur $L/k \equiv l$, comme le montre la figure 3.5.

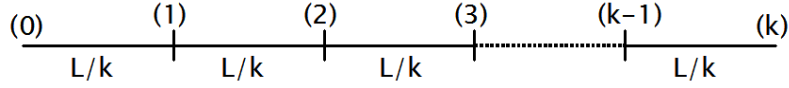


FIG. 3.5 – Ligne de longueur L subdivisée en k tronçons de longueur identique.

Etudions la propagation d'un état "de proche en proche", tronçon par tronçon, jusqu'au bout du canal. Considérons la quadrature x , le cas de la quadrature p étant identique¹⁰ :

$$\begin{aligned}
 x_1 &= \sqrt{T_l} x_0 + \sqrt{1 - T_l} x_{E_1} = t_l x_0 + r_l x_{E_1} \\
 x_2 &= \sqrt{T_l} x_1 + \sqrt{1 - T_l} x_{E_2} = t_l x_1 + r_l x_{E_2} = t_l^2 x_0 + r_l t_l x_{E_1} + r_l x_{E_2} \\
 x_3 &= \sqrt{T_l} x_2 + \sqrt{1 - T_l} x_{E_3} = t_l x_2 + r_l x_{E_3} = t_l^3 x_0 + r_l t_l^2 x_{E_1} + r_l t_l x_{E_2} + r_l x_{E_3} \\
 &\dots \\
 x_k &= \sqrt{T_l} x_{k-1} + \sqrt{1 - T_l} x_{E_k} = t_l x_{k-1} + r_l x_{E_k} \\
 &= t_l^k x_0 + r_l t_l^{k-1} x_{E_1} + r_l t_l^{k-2} x_{E_2} + \dots + r_l t_l^2 x_{E_{k-2}} + r_l t_l x_{E_{k-1}} + r_l x_{E_k},
 \end{aligned}$$

où $T_l + R_l = t_l^2 + r_l^2 = 1$. On a donc :

$$\langle x_k^2 \rangle = T_l^k \langle x_0^2 \rangle + R_l T_l^{k-1} \langle x_{E_1}^2 \rangle + \dots + R_l \langle x_{E_k}^2 \rangle + \sum_{i \neq j} C_{ij} \langle x_{E_i} x_{E_j} \rangle. \quad (3.11)$$

La subdivision du canal est artificielle : aucune opération n'y est associée. L'expression ci-dessus doit donc correspondre à

$$\langle x_k^2 \rangle = T_L \langle x_0^2 \rangle + (1 - T_L) \langle x_E^2 \rangle, \quad (3.12)$$

où $\langle x_E^2 \rangle = N/2$ correspond à l'ensemble du canal.

L'égalité des deux expressions ne peut être obtenue qu'en formulant que $T_L = T_l^k = T_{L/k}^k$. De plus, pour éliminer les termes croisés, le bruit de chaque tronçon doit être indépendant des autres. En outre, la variance du bruit est identique quel que soit le tronçon ou sa longueur. On a donc $\langle x_{E_i} x_{E_j} \rangle = \delta_{ij} N/2$, où δ_{ij} est le symbole de Kronecker. Sous ces conditions, on peut en effet écrire :

$$\langle x_k^2 \rangle = T_L \langle x_0^2 \rangle + (1 - T_l) (T_l^{k-1} + T_l^{k-2} + \dots + T_l^2 + T_l + 1) \langle x_E^2 \rangle \quad (3.13)$$

$$= T_L \langle x_0^2 \rangle + (1 - T_L) \langle x_E^2 \rangle, \quad (3.14)$$

avec $\sum_{n=0}^{k-1} T^n = \frac{1-T^k}{1-T}$ pour $|T| < 1$. Nous avons donc confirmé les comportements attendus :

$$N_{L/k} = N_L = N \quad ; \quad T_{L/k} = e^{-\alpha L/k} = T_L^{1/k}. \quad (3.15)$$

¹⁰Comme dans la suite de ce chapitre.

3.3 Transmission avec amplification

Pour lutter contre les pertes induites par la propagation, nous pouvons envisager d'amplifier le signal à transmettre le long du canal de longueur L . Etudions le cas représenté à la figure 3.6 : le signal se propage sur une distance L_1 (premier paramètre à optimiser) où il subit des pertes $T_{L_1} = e^{-\alpha L_1}$; il est ensuite amplifié par un amplificateur de gain G tel que $1 \leq G < \infty$ (second paramètre à optimiser) ; enfin, il parcourt une distance $L_2 = L - L_1$, qui en toute généralité est différente de L_1 .

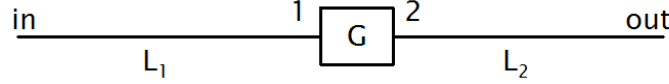


FIG. 3.6 – Amplification à une position quelconque.

On peut écrire :

$$x_1 = \sqrt{T_{L_1}} x_{in} + \sqrt{1 - T_{L_1}} x_{E_1}, \quad (3.16)$$

$$x_2 = \sqrt{G} x_1 + \sqrt{G - 1} x_{E_G}, \quad (3.17)$$

$$x_{out} = \sqrt{T_{L_2}} x_2 + \sqrt{1 - T_{L_2}} x_{E_2}. \quad (3.18)$$

Comme nous l'avons vu, les processus de perte et d'amplification peuvent être décrits au moyen des expressions (2.71), avec respectivement $X = \sqrt{T}\mathbb{I}$ et $Y = (1 - T)\mathbb{I}$ et $X = \sqrt{G}\mathbb{I}$ et $Y = (G - 1)\mathbb{I}$. Donc, en accord avec les expressions ci-dessus,

$$\langle x_1 \rangle = \sqrt{T_{L_1}} \langle x_{in} \rangle, \quad (3.19)$$

$$\langle x_2 \rangle = \sqrt{G} \langle x_1 \rangle, \quad (3.20)$$

$$\langle x_{out} \rangle = \sqrt{T_{L_2}} \langle x_2 \rangle, \quad (3.21)$$

et

$$V_{x_1} = T_{L_1} V_{x_{in}} + (1 - T_{L_1}) N, \quad (3.22)$$

$$V_{x_2} = G V_{x_1} + (G - 1) N_G, \quad (3.23)$$

$$V_{x_{out}} = T_{L_2} V_{x_2} + (1 - T_{L_2}) N. \quad (3.24)$$

Pour évaluer les valeurs moyennes en entrée et en sortie, nous devons effectuer une mise à l'échelle en multipliant l'expression de x_{out} par le facteur $1/\sqrt{GT_{L_1}T_{L_2}} = 1/\sqrt{GT_L}$. La variance $V_{x_{out}}$ sera ainsi multipliée par le facteur $1/(GT)$. Finalement, $\delta = V_{x_{out}} - V_{x_{in}}$ a pour expression :

$$\delta = \frac{1}{T_{L_1}} \left(N \left(1 - T_{L_1} + \frac{1 - T_{L_2}}{G T_{L_2}} \right) + N_G \frac{G - 1}{G} \right). \quad (3.25)$$

Tant la transmission que l'amplification contribuent à l'écart entre les variances δ . Pour une longueur L et un gain G donnés, nous désirons déterminer la position idéale de l'amplificateur. Exprimons donc δ en fonction du seul paramètre T_{L_1} , sachant que $T_{L_2} = T_L/T_{L_1}$:

$$\delta = \frac{1}{T_{L_1}} \frac{G - 1}{G} (N_G + N) + N \left(\frac{1}{T_L G} - 1 \right). \quad (3.26)$$

Comme $G \geq 1$, le facteur $1/T_{L_1}$ multiplie une expression qui contribue à augmenter la variance de l'état de sortie. Pour minimiser δ , il importe donc – comme on peut le visualiser sur la figure 3.7 – de maximiser T_{L_1} , soit de poser $T_{L_1} = 1$, ce qui correspond à $L_1 = 0$.

La différence de variances devient alors :

$$\delta = N_G \frac{G-1}{G} + N \frac{1-T}{T G}. \quad (3.27)$$

On peut aisément se convaincre qu'amplifier en début de ligne est en effet le cas idéal : on y amplifie alors uniquement le signal et pas le bruit. La situation d'amplification optimisée est représentée sur la figure 3.8.

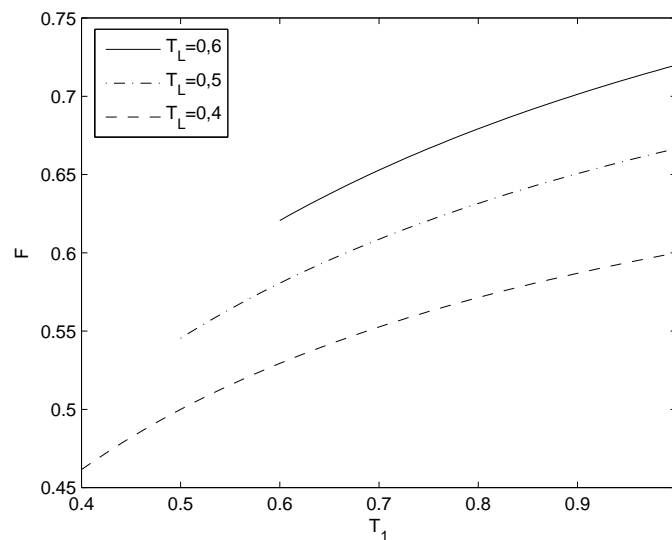


FIG. 3.7 – Evolution de $F = 2/(2 + \delta)$ en fonction de la position de l'amplificateur, avec une valeur $G = 3/2$.

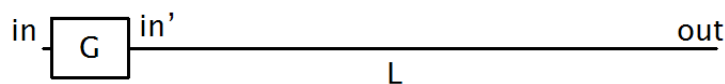


FIG. 3.8 – Amplification à une position optimale, en début de ligne.

Connaître la position idéale de l'amplificateur ne signifie aucunement qu'amplifier est préférable au cas direct, l'amplification elle-même ajoutant du bruit. Afin de connaître le gain optimal, comparons l'expression de δ pour deux gains différents, G_1 et G_2 , avec par hypothèse $1 \leq G_1 < G_2 < \infty$:

$$\begin{aligned} \delta_{G_1} - \delta_{G_2} &= N_G \frac{G_1 - 1}{G_1} + N \frac{1 - T}{T G_1} - N_G \frac{G_2 - 1}{G_2} - N \frac{1 - T}{T G_2} \\ &= \left(\frac{1}{G_1} - \frac{1}{G_2} \right) \left(\frac{1 - T}{T} N - N_G \right). \end{aligned} \quad (3.28)$$

Pour que l'augmentation de gain (de G_1 à G_2) soit favorable, il faut que $\delta_{G_1} - \delta_{G_2}$ soit positif. Le premier facteur du membre de droite étant positif, le deuxième facteur fournit

la condition :

$$T < \frac{N}{N_G + N}. \quad (3.29)$$

Dans le cas d'un bruit ajouté nul, tant au niveau de la propagation que de l'amplification, cette condition devient :

$$T < \frac{1}{2} \Leftrightarrow L > \frac{\ln 2}{\alpha}. \quad (3.30)$$

Dans le cas de *courtes* (au sens de l'inégalité ci-dessus) distances, le gain optimal est le plus petit possible, soit $G = 1$, pour lequel on retrouve avec (3.27) l'expression $\delta = N(1 - T)/T = \chi$. En pratique, aucune amplification n'est effectuée : l'optimum est la transmission directe.

Dans le cas de *longues* distances, au contraire, il convient d'amplifier le signal avec un gain G le plus grand possible. Les valeurs de $G = \cosh^2(r)$ accessibles expérimentalement sont cependant limitées à $G_{max} \approx 3$ pour $r_{max} \approx 1$. Il est important de noter dans le cadre des communications quantiques à longue distance que l'amplification doit se faire *préalablement* à la transmission.

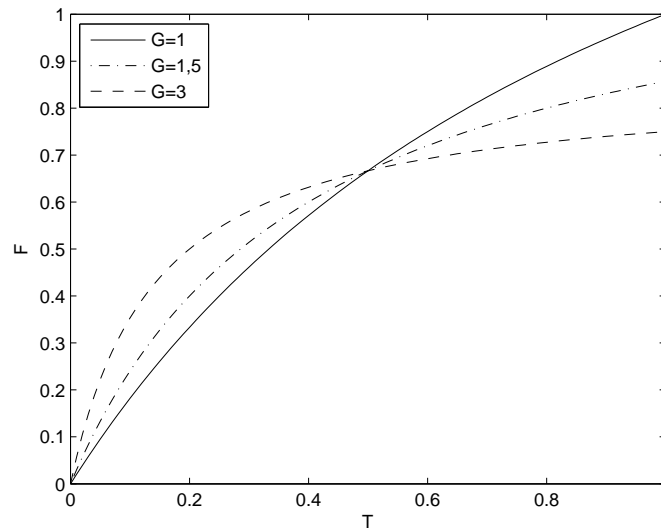


FIG. 3.9 – Evolution de la fidélité F en fonction de T pour différentes valeurs du gain G , et avec $N=N_G=N_0$.

La figure 3.9 résume les considérations énoncées. L'amplification détériore la transmission à courtes distances mais l'améliore à longues distances, lorsque la condition (3.29) est vérifiée. Plus le bruit du canal augmente – par rapport à celui provoqué par l'amplification – plus vite l'amplification devient favorable. Si le canal est très fortement bruité ($N \gg N_G$), l'amplification est presque toujours favorable. On peut alors choisir un gain G permettant d'égaliser, pour une distance donnée, les valeurs moyennes entre l'état d'entrée et l'état de sortie ($G = 1/T$) tout en diminuant la variance relative.

L'utilisation d'amplification a donc tendance à "aplatir" la courbe de fidélité en fonction de la distance. Dans la limite irréaliste $G \rightarrow \infty$, δ prend la valeur de $N_G \approx 1$ pour toute distance : la variance est doublée entre l'entrée et la sortie. Une amplification de

gain limité permet, aux longues distances – au sens de l'inégalité (3.29) – de se rapprocher de la valeur seuil $F = 2/3$ mais jamais de passer au dessus.

3.4 Transmission par téléportation

Nous avons vu dans la section 2.9 que l'intrication de paires EPR pouvait être utilisée pour *téléporter* un état quantique. Il est possible d'exploiter cette propriété dans le cadre d'une transmission dans un canal à pertes. Soit donc la situation représentée sur la figure 3.10. Le signal à transmettre sur une distance totale $L = L_0 + L_1 + L_2$ parcourt physiquement une distance L_0 . Son état est alors mesuré avec la moitié A d'une paire EPR (qui a parcouru une distance L_1). Le résultat de la mesure permet à B d'appliquer un déplacement sur sa moitié de la paire EPR (qui a parcouru une distance L_2) pour reproduire l'état en sortie. Remarquons que les opérations de mesure et de déplacement ne sont pas représentées sur la figure.

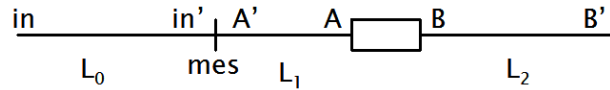


FIG. 3.10 – Schéma de transmission avec une paire EPR placée à une position quelconque.

Selon l'expression (2.92), l'état téléporté est une reproduction d'autant plus *fidèle* de l'état d'entrée que le facteur de compression de la paire EPR est grand. Dans la limite d'un *squeezing* infini, la téléportation est parfaite. Il faut néanmoins nuancer cette dernière affirmation. Dans le cas que nous étudions, la propagation des états dans le canal – et donc leur interaction avec l'environnement – induit une décorrélation partielle entre les deux parties de la paire EPR. Même à *squeezing* infini, elles ne seront plus des intermédiaires parfaitement “transparents” pour la téléportation.

Les pertes du canal s'appliquent aux différents états :

$$x_{in'} = \sqrt{T_{L_0}} x_{in} + \sqrt{1 - T_{L_0}} x_{E_0}, \quad (3.31)$$

$$x_{A'} = \sqrt{T_{L_1}} x_A + \sqrt{1 - T_{L_1}} x_{E_1}, \quad (3.32)$$

$$x_{B'} = \sqrt{T_{L_2}} x_B + \sqrt{1 - T_{L_2}} x_{E_2}. \quad (3.33)$$

L'état de sortie sera donné par :

$$x_{out} = x_{B'} + x_{mix} \quad (3.34)$$

$$= x_{B'} + \frac{g}{\sqrt{2}}(x_{in'} - x_{A'}) \quad (3.35)$$

$$= \sqrt{T_{L_2}} x_B + \sqrt{1 - T_{L_2}} x_{E_2} + \frac{g}{\sqrt{2}} \left(\sqrt{T_{L_0}} x_{in} + \sqrt{1 - T_{L_0}} x_{E_0} - \sqrt{T_{L_1}} x_A - \sqrt{1 - T_{L_1}} x_{E_1} \right) \quad (3.36)$$

Soit, après une mise à l'échelle adéquate – une multiplication par $\sqrt{2/(g^2 T_{L_0})}$:

$$x_{out} = x_{in} + \frac{\sqrt{2}}{g} \left(\sqrt{\frac{T_{L_2}}{T_{L_0}}} x_B + \sqrt{\frac{1 - T_{L_2}}{T_{L_0}}} x_{E_2} \right) + \sqrt{\frac{1 - T_{L_0}}{T_{L_0}}} x_{E_0} - \sqrt{\frac{T_{L_1}}{T_{L_0}}} x_A - \sqrt{\frac{1 - T_{L_1}}{T_{L_0}}} x_{E_1} \quad (3.37)$$

La différence de variances entre la sortie et l'entrée est donc :

$$\begin{aligned} \delta &= \frac{1}{T_{L_0}} \left(\cosh(2r) \left(T_{L_1} + T_{L_2} \frac{2}{g^2} \right) - \sinh(2r) \left(2\sqrt{T_{L_1} T_{L_2}} \frac{\sqrt{2}}{g} \right) \right) \\ &\quad + \frac{N}{T_{L_0}} \left(1 - T_{L_0} + 1 - T_{L_1} + (1 - T_{L_2}) \frac{2}{g^2} \right) \end{aligned} \quad (3.38)$$

Pour minimiser cette expression, il importe de bien choisir les longueurs de propagation L_0 , L_1 et L_2 . On remarque qu'il est préférable de fixer $T_{L_0} = 1$ et donc $L_0 = 0$, et de symétriser les pertes en prenant $T_{L_1} = T_{L_2} = T_{L/2} = T_L^{1/2}$. De cette façon, l'état d'entrée est fixe et la paire EPR est au milieu du canal. On a alors $x_{in'} = x_{in}$, et donc

$$x_{out} = x_{B'} + \frac{g}{\sqrt{2}}(x_{in} - x_{A'}). \quad (3.39)$$

Après un *upscaling* de valeur $\sqrt{2}/g$, on peut écrire :

$$\delta = V_{x'_A} + \frac{2}{g^2} V_{x'_B} - 2 \frac{\sqrt{2}}{g} V_{x'_A x'_B} \quad (3.40)$$

$$= \left(T_L^{1/2} \cosh(2r) + N(1 - T_L^{1/2}) \right) \left(1 + \frac{2}{g^2} \right) - 2 \frac{\sqrt{2}}{g} T_L^{1/2} \sinh(2r), \quad (3.41)$$

où r est le paramètre de compression de la paire EPR. Si l'on choisit le gain de téléportation supposé optimal $g = \sqrt{2}$, et sachant que $\cosh(2r) - \sinh(2r) = \exp(-2r)$, on trouve

$$\delta_L = 2 \left(T_L^{1/2} e^{-2r} + N \left(1 - T_L^{1/2} \right) \right). \quad (3.42)$$

La fidélité équivalente $F = 2/(2 + \delta)$ est représentée à la figure 3.11.

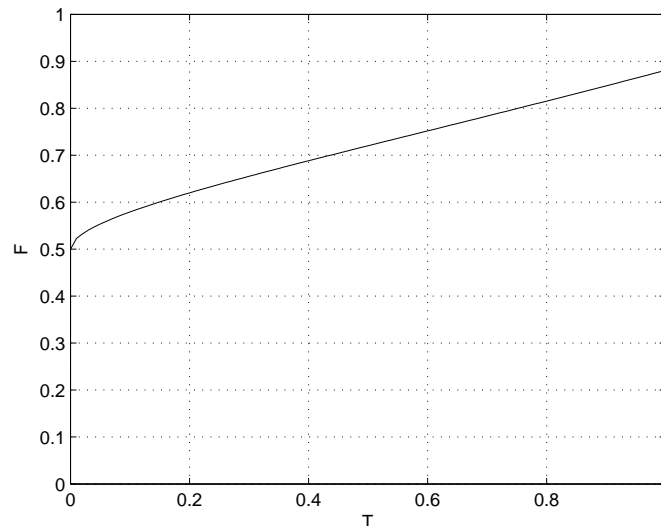


FIG. 3.11 – Variation de la fidélité en fonction de la distance, dans le cas d'un canal sans bruit ajouté, et pour $r = 1$ et $g = \sqrt{2}$.

Dès que la longueur du canal augmente, elle devient nettement moins grande que la valeur donnée en (2.92), qui n'est valable que pour $T_L = 1$. Le facteur de compression

effectif de la paire EPR diminue lors de la propagation dans le canal.

Supposons que l'on désire atteindre une fidélité F aussi grande – malgré la propagation – que celle obtenue, avec un facteur r donné, par la formule (2.92). Pour contrebalancer l'effet de décohérence dû à la propagation dans le canal, il faut créer la paire EPR avec une valeur $r^* > r$. La comparaison des formules (2.92) et (3.42) nous fournit la valeur nécessaire

$$r^* = \frac{1}{2} \ln \left(\frac{T_L^{1/2}}{\exp(-2r) - N(1 - T_L^{1/2})} \right). \quad (3.43)$$

Pour un r donné, le dénominateur de cette expression s'annule pour une valeur T_{seuil} . A cette valeur, r^* doit prendre une valeur infinie pour remplir la condition. Sous cette valeur, il n'est donc plus possible de contrebalancer l'effet du canal même à *squeezing* infini.

A titre d'exemple, sur la figure 3.12, nous représentons en fonction de la transmittance du canal la valeur de r nécessaire pour atteindre une fidélité de $2/3$, soit $\delta = 1$. A distance nulle, la valeur de r nécessaire est de $\ln(2)/2$. A *squeezing* infini, on sait que $\delta \rightarrow 2(1 - T_L^{1/2})$. Cette grandeur vaut 1 pour $T_L = 1/4$. Sous cette valeur de seuil, il n'est plus possible, même à *squeezing* infini, de remplir la condition $F = 2/3$. Ainsi, pour $T_L \rightarrow 0$, F tend au mieux (c'est-à-dire à *squeezing* infini) vers la valeur $1/2$.

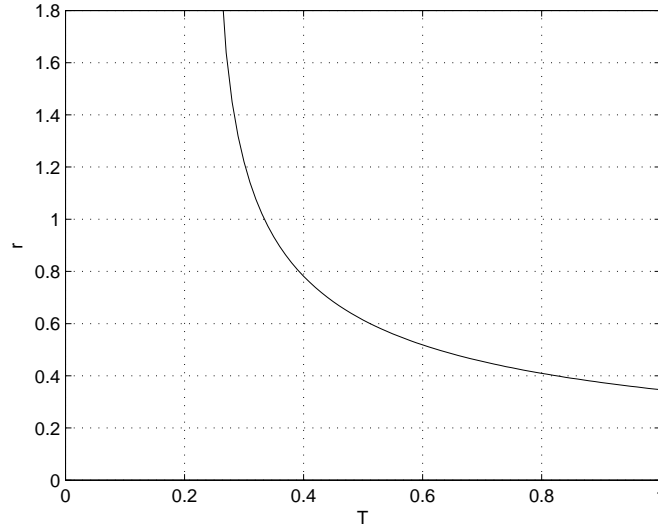


FIG. 3.12 – Valeur de r nécessaire pour atteindre une valeur $F = 2/3$ dans le cas d'un canal sans bruit ajouté et pour $g = \sqrt{2}$.

Ces limitations ne doivent pas nous empêcher de remarquer que l'utilisation d'intrication est un formidable outil pour les communications quantiques. Pour évaluer la pertinence d'utiliser ce schéma, nous confrontons ses performances aux autres schémas. Aux faibles distances, le schéma de transmission direct reste préférable. En effet, la paire EPR a un *squeezing* fini et, en vertu de l'équation (2.92), la fidélité n'est pas unitaire même pour $T \rightarrow 1$. Cependant, lorsque la distance augmente, nous avons vu que la propagation du signal le dégrade très fortement. Il devient alors favorable d'utiliser le schéma basé sur la téléportation : les deux parties de la paire EPR sont de plus en plus dégradées,

mais l'effet est bien moins prononcé que la dégradation du signal lui-même s'il est véhiculé physiquement dans le canal.

La figure 3.13 compare les performances du schéma basé sur l'intrication à celui basé sur une amplification. À *squeezing* équivalent, la téléportation donne de meilleurs résultats aux grandes distances. De plus, l'état à transmettre ne voyageant pas physiquement dans le canal, la valeur moyenne est automatiquement préservée – dans un cas pratique d'amplification, le gain G doit être réglé à $1/T$ pour restaurer la valeur moyenne. Pour des valeurs de r modérées et à relativement faibles distances, le schéma d'amplification peut néanmoins être préférable à celui basé sur la téléportation – en raison de sa plus grande facilité de mise en oeuvre – mais dans ce cas le schéma direct est souvent plus performant.

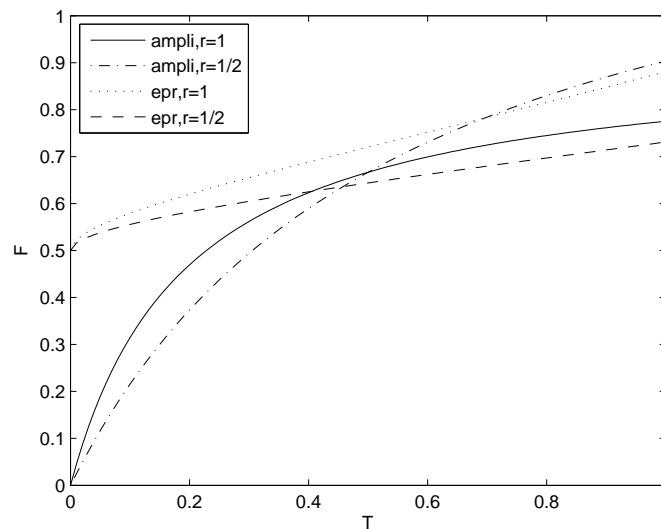


FIG. 3.13 – Comparaison entre transmission avec amplification et transmission par téléportation.

Il apparaît donc que les paires EPR sont un élément essentiel pour les communications quantiques à longues distances. Etant donné les résultats encourageants observés en utilisant une paire EPR, nous sommes tentés de répéter ce schéma en plaçant plusieurs paires EPR le long de la ligne de transmission, comme autant de *relais quantiques*. La figure 3.14 représente le cas de deux paires EPR.

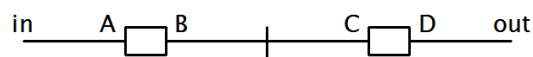


FIG. 3.14 – Schéma utilisant deux paires EPR.

Le processus consiste à utiliser l'échange d'intrication (*entanglement swapping*). Il s'agit d'une double téléportation : les parties B et C des paires EPR se propagent vers le milieu du canal ; le résultat de leur mesure sert au déplacement de la partie D qui s'est propagée vers la sortie. L'état de sortie est déplacé à nouveau, en fonction du résultat de la mesure entre la partie A et l'état d'entrée.

Considérons immédiatement un cas "équilibré", pour lequel l'état in est fixe, et chaque

mode des paires EPR parcourt une longueur $L/4$:

$$\begin{aligned}\delta &= V_{x_{A'}} + \frac{g_2^2}{g_1^2} (V_{x_{B'}} + V_{x_{C'}}) + \frac{2}{g_1^2} V_{x_{D'}} \\ &= -2 \frac{g_2}{g_1} V_{x_{A'} x_{B'}} - 2 \frac{\sqrt{2} g_2}{g_1^2} V_{x_{C'} x_{D'}},\end{aligned}\quad (3.44)$$

où g_2 est le gain de téléportation utilisé après la mesure de x_B et x_C , et où g_1 est le gain de téléportation utilisé après la mesure de x_A et x_{in} . Si $g_1 = g_2 = \sqrt{2}$, on peut écrire :

$$\delta = 4 T_L^{1/4} e^{-2r} + 4 N (1 - T_L^{1/4}).\quad (3.45)$$

Ce résultat est facilement généralisable au cas où l'on utilise k paires EPR :

$$\delta = 2 k T_L^{1/2k} e^{-2r} + 2 k N (1 - T_L^{1/2k}).\quad (3.46)$$

La figure 3.15 compare la valeur de l'expression $F = 2/(2 + \delta)$ pour différents nombres de paires EPR utilisées. Elle est tracée en fonction de r et pour une valeur de $T = 1/2$, mais son allure est similaire pour toute valeur de T .

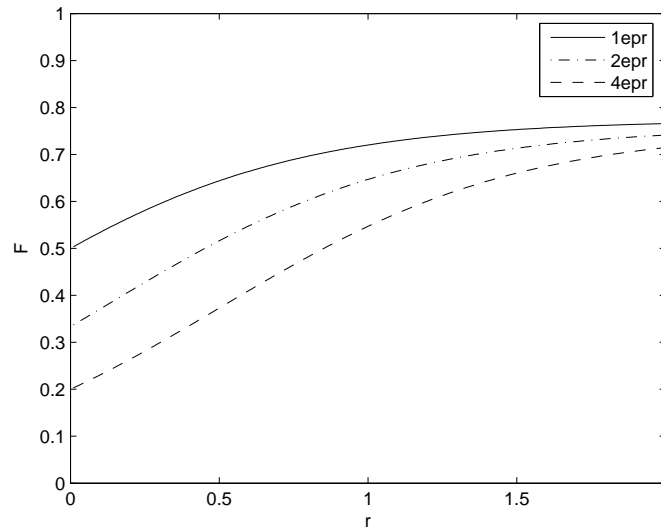


FIG. 3.15 – Comparaison des schémas à plusieurs EPR, en fonction de r et pour $T_L = 1/2$.

Plus le nombre de paires EPR utilisées est grand, moins bon est le résultat ! Le fait d'effectuer plusieurs téléportations séquentielles, à facteur de compression fini, contribue à augmenter la variance de l'état téléporté. Les paires EPR interagissent avec l'environnement sur une longueur moindre (cf. le facteur $1 - T_L^{1/2k}$) mais cela ne compense pas le fait que, lorsque nous scindons la ligne en $2k$ différents tronçons, la variance N du bruit du canal vient s'ajouter autant de fois (cf. le facteur $2kN$).

Avant de conclure, revenons sur l'expression (3.41). En la dérivant par rapport à g et en égalant la dérivée à zéro, on peut trouver le gain optimal

$$g_{optimal} = \frac{2 \left(T_L^{1/2} \cosh(2r) + N \left(1 - T_L^{1/2} \right) \right)}{\sqrt{2} T_L^{1/2} \sinh(2r)}.\quad (3.47)$$

On retrouve bien $g = \sqrt{2}$ pour $T = 1$ et $r = \infty$, mais en toute généralité l'expression est dépendante de r et de T . La figure 3.16 représente la variation du gain optimal en fonction de T et la figure 3.17 représente sa variation en fonction de r .

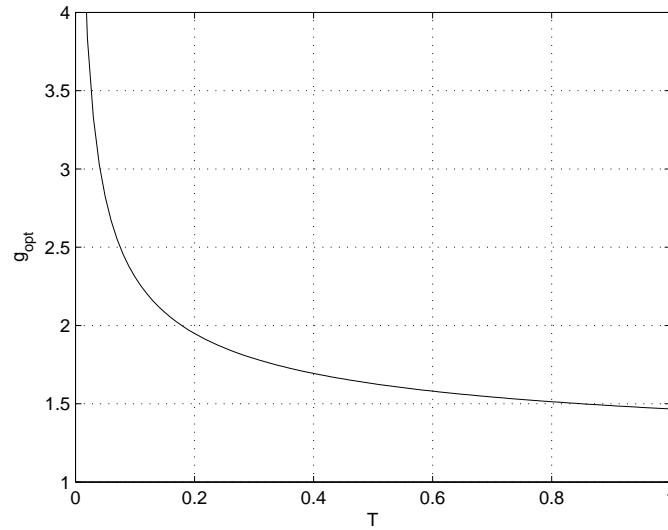


FIG. 3.16 – Valeur optimale du gain de téléportation g en fonction de T , pour $r = 1$.

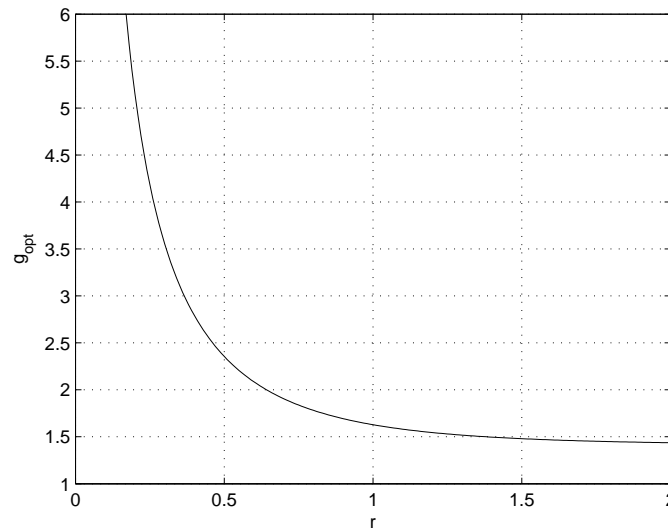


FIG. 3.17 – Valeur optimale du gain de téléportation g en fonction de r , pour $T_L = 1/2$.

On remarque que lorsque le taux de compression est faible, ou que la longueur du canal augmente¹¹, le gain optimal est fortement différent de celui envisagé dans le protocole standard de téléportation. Bien entendu, il faut noter que l'utilisation d'un gain différent de $\sqrt{2}$ ne conserve pas la valeur moyenne.

Compte tenu de cette observation, il peut être intéressant de dériver une relation similaire dans le cas de deux paires EPR. En supposant que le gain g_1 de la téléportation

¹¹Ce qui revient, comme nous l'avons vu, à une diminution du facteur de compression effectif.

impliquant A et in est fixé à une valeur arbitraire ($\sqrt{2}$), on peut écrire le gain optimal g_2 à partir de l'expression (3.44) :

$$g_{optimal} = \frac{W' (g_1 + 2\sqrt{2})}{2V'}, \quad (3.48)$$

où nous avons posé $W' = T_L^{1/4} \sinh(2r)$ et $V' = T_L^{1/4} \cosh(2r) + (1 - T_L^{1/4})$.

On peut constater en utilisant le gain optimal une amélioration – faible¹² – de la fidélité. Cependant, dans le cadre d'un réseau de communications quantiques, le fait que le gain de téléportation à utiliser dépende de la distance de transmission et du facteur de compression est quelque peu limitatif.

3.5 Conclusion

Le schéma de transmission optimal apparaît fortement dépendant, d'une part de la distance, et d'autre part du taux de compression que l'on peut réaliser. A faibles distances, la transmission directe est la plus indiquée. Lorsque la distance et/ou le bruit augmente, il peut devenir intéressant d'amplifier le signal avant sa transmission.

Enfin, le meilleur schéma pour les communications quantiques à longue distance semble être l'utilisation d'un “relais” quantique, à savoir un milieu $\chi^{(2)}$ placé au centre¹³ de la ligne de transmission et fournissant des paires EPR (suffisamment corrélées) susceptibles de téléporter un état cohérent désiré de l'entrée à la sortie. Dans ce cas, la fidélité de téléportation F tend vers une valeur finie pour $L \rightarrow \infty$, même pour un facteur de compression de valeur finie. Si considérer une distance infinie est une vue de l'esprit, cela montre néanmoins tout l'intérêt de ce schéma.

L'utilisation de plusieurs relais est par contre défavorable par rapport à l'utilisation d'une seule paire EPR. Cette conclusion, opposée au cas discret (voir par exemple [CGDR05]), semble quelque peu surprenante et limitative. Des améliorations du protocole standard de téléportation sont néanmoins possibles ; nous en montrons un exemple au prochain chapitre.

¹²Cette amélioration n'est pas à même de rendre le schéma à plusieurs paires EPR plus performant que le schéma à une seule paire EPR.

¹³Cette précision est importante. Si les deux parties de la paire EPR ne parcourent pas la même distance, la téléportation peut devenir très mauvaise. Cela est notamment le cas si une partie de la ligne présente un défaut, auquel cas notre hypothèse d'homogénéité tombe. On peut alors avoir $T_1 \neq T_2$ malgré $L_1 = L_2$: la “distance” effective est modifiée.

Chapitre 4

Propagation d'états non gaussiens

Once you find you can't walk as far and as fast as you were able, life becomes more complicated. (R. Sheckley)

Les transformations d'états que nous avons décrites au chapitre 2 étaient des transformations *gaussiennes*. Récemment, des résultats théoriques et expérimentaux ont montré l'intérêt d'utiliser des transformations qui ne préservent pas le caractère gaussien d'un état (par exemple [ESP02]). Ainsi, la téléportation d'un état cohérent peut être améliorée si elle utilise des états non gaussiens [OPB03]. Etant donné le rôle de la téléportation dans le cadre des communications quantiques à longue distance, ce constat nous intéresse tout particulièrement.

Les opérations non gaussiennes ont toutefois l'inconvénient d'être difficilement accessibles expérimentalement. Nous utiliserons l'une d'entre elles, la *soustraction de photon*, qui est réalisable dans l'état actuel de la technologie. Cette opération produit un état spécifiquement quantique, au contraire d'une simple atténuation pour laquelle des photons sont enlevés de façon statistiquement homogène. Des travaux récents ont utilisé ce type d'états pour proposer des démonstrations des inégalités de Bell [GPFC05].

4.1 Soustraction de photon

Considérons un mode de lumière duquel on souhaite extraire un et un seul photon. Pour ce faire, on fait passer le faisceau à travers une lame partiellement réfléchissante de transmittance $T \approx 1$. Dans l'approximation $T \rightarrow 1$, presque tout le faisceau est transmis et la fraction déviée $R = \epsilon$ ne contient le plus souvent aucun photon. De temps en temps, elle en contiendra un et un seul – la probabilité que plus d'un photon soit dévié est beaucoup plus faible.

Pour détecter l'occurrence d'un tel événement, on place sur le mode de sortie auxiliaire (à l'entrée duquel se trouve l'état du vide) un photodétecteur à même de détecter un photon unique. Lorsque le photodétecteur “clique”, l'état de sortie sur le mode signal est bien l'état d'entrée duquel on a soustrait un photon.

De tels détecteurs sont technologiquement accessibles actuellement. S'ils distinguent la présence d'un photon, ils ne sont cependant pas capables de discriminer le nombre de photons. Les photodétecteurs réels souffrent en outre de diverses imperfections : [Our07]

- Leur efficacité est limitée : un photon incident peut ne pas être détecté. Pour modéliser cette situation, on peut considérer un photodétecteur idéal précédé d'un diviseur de faisceau de transmittance η , l'efficacité quantique de la photodiode à avalanche.
- A l'opposé, le détecteur peut émettre un signal sans qu'aucun photon ne lui parvienne (*dark counts*). Cet inconvénient est limité en pratique par la synchronisation du détecteur sur une horloge : il n'est activé que durant le laps de temps où un événement est attendu.

Dans notre étude, les photodétecteurs seront considérés comme parfaits. Notre but est en effet d'explorer les différents cas où l'utilisation d'un tel dispositif s'avère être *a priori* favorable. Nous mettons l'accent sur l'amélioration de la portée des communications quantiques. La nouveauté de notre approche consistera à étudier l'effet des pertes tant sur les états gaussiens (*avant* la soustraction) que sur les états non gaussiens (*après* la soustraction). Le schéma de téléportation envisagé est représenté à la figure 4.1. Il s'agit du schéma de base où une paire EPR placée au centre du canal est la source d'intrication nécessaire pour effectuer une téléportation. Il faut noter que ce sont les modes A et B de la paire EPR qui circulent dans le canal. Selon le protocole de téléportation, on effectue une mesure jointe entre l'état *in* et le mode A , l'état *out* est obtenu après déplacement du mode B .

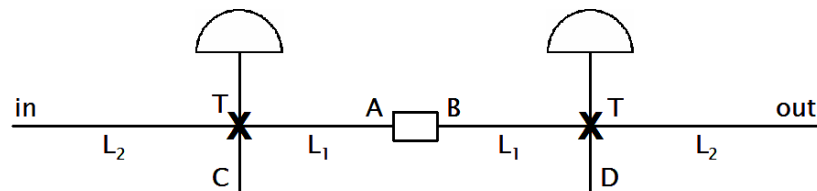


FIG. 4.1 – Téléportation avec soustraction de photon.

Chaque mode de la paire EPR parcourt une distance L_1 , subit une soustraction de photon, puis parcourt une distance L_2 . Pour évaluer la pertinence d'un tel schéma, nous utiliserons les mêmes critères qu'au chapitre 3 : les modes de la paire EPR doivent servir à téléporter au mieux un état cohérent de l'entrée du canal vers la sortie.

Le premier objectif de ce chapitre est d'optimiser la position de la soustraction de photon. Cette dernière permet-elle une décorrélation moins grande des modes de la paire EPR si elle se produit au début de la propagation ($L_1 = 0$) ou en fin de propagation ($L_2 = 0$) ?

Dans un deuxième temps, nous comparons les résultats trouvés au schéma direct et au schéma de téléportation sans soustraction de photon, à même distance de propagation totale $L_{tot} = 2(L_1 + L_2)$, soit $T_{tot} = (T_1 T_2)^2$, et quantifions l'amélioration éventuelle.

Cependant, nous ne disposons pas encore des outils mathématiques nécessaires au traitement d'une opération non gaussienne telle que la soustraction de photon. Le développement

nécessaire est l'objet de la prochaine section. Etant donné la lourdeur des expressions formelles obtenues lorsque nous les explicitons, nous les traiterons numériquement.

4.2 Description mathématique

Un photodétecteur, lorsqu'il réalise une mesure, effectue une projection dans l'espace de Hilbert. Comme il ne peut pas discriminer le nombre de photons, cette projection s'effectue soit sur le vide (s'il n'y a pas de "clic"), soit sur le reste de l'espace de Hilbert (en cas de "clic"). Les projecteurs correspondants s'écrivent :

$$\Pi_0 = |0\rangle\langle 0| \quad ; \quad \Pi_1 = \mathbb{I} - |0\rangle\langle 0|, \quad (4.1)$$

où \mathbb{I} représente l'identité. Pour traiter ces projections, nous utilisons le formalisme de Wigner, dans lequel un opérateur P est associé à une fonction de Wigner W_P :

$$W_{\Pi_0}(r) = \frac{1}{\pi} e^{-x^2 - p^2} \quad ; \quad W_{\Pi_1}(r) = \frac{1}{2\pi} - \frac{1}{\pi} e^{-x^2 - p^2}. \quad (4.2)$$

La soustraction de photon n'est pas une opération gaussienne, la fonction de Wigner W_{Π_1} n'est donc pas gaussienne, mais elle est néanmoins la *différence* de gaussiennes. Bien que l'état créé ne soit pas gaussien, il pourra toujours s'exprimer sous la forme d'une *combinaison linéaire* d'états gaussiens¹. Tout le formalisme développé pour les états gaussiens reste donc valable, et nous pouvons effectuer les développements ci-dessous (voir [GPS07]).

Comme nous effectuons une projection dans les modes C et D puis que nous regardons en sortie uniquement les états A et B (voir figure 4.1), l'opération s'écrit :

$$\rho_{AB} = \text{Tr}_{CD} [\rho_{ABCD} (\mathbb{I}_{AB} \otimes (\mathbb{I}_C - |0\rangle\langle 0|_C) \otimes (\mathbb{I}_D - |0\rangle\langle 0|_D))] \quad (4.3)$$

$$= \text{Tr}_{CD} [\rho_{ABCD} (\mathbb{I}_{ABCD} - \mathbb{I}_{ABC}|0\rangle\langle 0|_D - \mathbb{I}_{ABD}|0\rangle\langle 0|_C + \mathbb{I}_{AB}|0\rangle\langle 0|_{CD})]. \quad (4.4)$$

Nous allons traiter cette équation terme à terme, en utilisant le formalisme de Wigner. Nous savons que, pour un état à n modes,

$$\text{Tr}[XY] = (2\pi)^n \int W_X(r) W_Y(r) d^{2n}r. \quad (4.5)$$

Nous aurons donc à effectuer des intégrales gaussiennes, de type

$$\int e^{-r^T \Gamma r} d^n r = \frac{\pi^n}{\sqrt{\det \Gamma}}, \quad (4.6)$$

où n est le nombre de modes sur lequel on intègre, et où Γ est l'inverse de la matrice de covariance de l'état considéré pour la soustraction de photon : $\Gamma = \gamma^{-1}$.

Le premier terme de (4.4) donne donc :

$$\begin{aligned} \text{Tr}_{CD} [\rho_{ABCD} \mathbb{I}_{ABCD}] &= (2\pi)^4 \int_{CD} W_{ABCD} W_{\mathbb{I}_{ABCD}} dr_{CD} \\ &= \int_{CD} W_{ABCD} dr_{CD} \\ &= \frac{1}{\pi^4} \frac{1}{\sqrt{\det \gamma}} \int_{CD} e^{-r^T \gamma^{-1} r} dr_{CD} \\ &= \frac{\sqrt{\det \Gamma}}{\pi^4} \int_{CD} e^{-r^T \Gamma r} dr_{CD} \equiv \text{Int}. \end{aligned} \quad (4.7)$$

¹Cette combinaison linéaire aura 2^p termes, où p est le nombre de soustractions de photon.

avec $\Gamma = \gamma^{-1}$ que nous écrivons sous la forme, en respectant la séparation $AB - CD$:

$$\Gamma = \begin{pmatrix} \Gamma_{AB} & \sigma \\ \sigma^T & \Gamma_{CD} \end{pmatrix}. \quad (4.8)$$

L'expression ci-dessus s'écrit donc :

$$\begin{aligned} \text{Int} &= \frac{\sqrt{\det \Gamma}}{\pi^4} \int_{CD} e^{-[r_{AB}^T \Gamma_{AB} r_{AB} + r_{AB}^T \sigma r_{CD} + r_{CD}^T \sigma^T r_{AB} + r_{CD}^T \Gamma_{CD} r_{CD}]} dr_{CD} \\ &= \frac{\sqrt{\det \Gamma}}{\pi^4} \int_{CD} e^{-[r_{CD}^T + r_{AB}^T \sigma \Gamma_{CD}^{-1}] \Gamma_{CD} [r_{CD} + \Gamma_{CD}^{-1} \sigma^T r_{AB}] + r_{AB}^T \sigma \Gamma_{CD}^{-1} \sigma^T r_{AB} - r_{AB}^T \Gamma_{AB} r_{AB}} dr_{CD} \\ &= \frac{\sqrt{\det \Gamma}}{\pi^4} \int_{CD} e^{-\tilde{r}_{CD}^T \Gamma_{CD} \tilde{r}_{CD}} dr_{CD} e^{-r_{AB}^T (\Gamma_{AB} - \sigma \Gamma_{CD}^{-1} \sigma^T) r_{AB}}, \end{aligned} \quad (4.9)$$

avec $\tilde{r}_{CD} = r_{CD} + \Gamma_{CD}^{-1} \sigma^T r_{AB}$ qui constitue un vecteur r_{CD} translaté, ce qui ne change rien à la valeur de l'intégrale. On a donc :

$$\text{Tr}_{CD} [\rho_{ABCD} \mathbb{I}_{ABCD}] = \frac{1}{\pi^2} \frac{\sqrt{\det \Gamma}}{\sqrt{\det \Gamma_{CD}}} e^{-r_{AB}^T \Gamma_1 r_{AB}}, \quad (4.10)$$

avec $\Gamma_1 = \Gamma_{AB} - \sigma \Gamma_{CD}^{-1} \sigma^T$.

Le deuxième terme de (4.4) s'écrit quant à lui :

$$\begin{aligned} \text{Tr}_{CD} [\rho_{ABCD} \mathbb{I}_{ABC} |0\rangle \langle 0|_D] &= (2\pi)^4 \int_{CD} W_{ABCD} W_{\mathbb{I}_{ABC}} W_{|0\rangle \langle 0|_D} dr_{CD} \\ &= 2\pi \int_{CD} \frac{\sqrt{\det \Gamma}}{\pi^4} e^{-r^T \Gamma r} \frac{1}{\pi} e^{-r_C^T \mathbb{I} r_C} \\ &= \frac{2\sqrt{\det \Gamma}}{\pi^4} \int_{CD} e^{-r^T \Gamma' r}, \end{aligned} \quad (4.11)$$

où

$$\Gamma' = \begin{pmatrix} \Gamma_{AB} & \sigma \\ \sigma^T & \Gamma_{CD_2} \end{pmatrix}, \quad (4.12)$$

avec $\Gamma_{CD_2} = \Gamma_{CD} + \mathbb{I}_C \otimes \mathbb{O}_D$, \mathbb{O} étant une matrice nulle. On peut donc écrire :

$$\text{Tr}_{CD} [\rho_{ABCD} \mathbb{I}_{ABC} |0\rangle \langle 0|_D] = \frac{2}{\pi^2} \frac{\sqrt{\det \Gamma}}{\sqrt{\det \Gamma_{CD_2}}} e^{-r_{AB}^T \Gamma_2 r_{AB}}, \quad (4.13)$$

où $\Gamma_2 = \Gamma_{AB} - \sigma \Gamma_{CD_2}^{-1} \sigma^T$.

Grâce à la symétrie du problème, le troisième terme de (4.4) est similaire :

$$\text{Tr}_{CD} [\rho_{ABCD} \mathbb{I}_{ABD} |0\rangle \langle 0|_C] = \frac{2}{\pi^2} \frac{\sqrt{\det \Gamma}}{\sqrt{\det \Gamma_{CD_3}}} e^{-r_{AB}^T \Gamma_3 r_{AB}}, \quad (4.14)$$

où $\Gamma_3 = \Gamma_{AB} - \sigma \Gamma_{CD_3}^{-1} \sigma^T$ et $\Gamma_{CD_3} = \Gamma_{CD} + \mathbb{O}_C \otimes \mathbb{I}_D$.

Enfin, le dernier terme de (4.4) est :

$$Tr_{CD} [\rho_{ABCD} \mathbb{I}_{AB} |0\rangle\langle 0|_{CD}] = (2\pi)^4 \int_{CD} W_{ABCD} W_{\mathbb{I}_{AB}} W_{|0\rangle\langle 0|_{CD}} dr_{CD} \quad (4.15)$$

$$= \frac{4}{\pi^2} \frac{\sqrt{\det \Gamma}}{\sqrt{\det \Gamma_{CD_4}}} e^{-r_{AB}^T \Gamma_4 r_{AB}}, \quad (4.16)$$

où $\Gamma_4 = \Gamma_{AB} - \sigma \Gamma_{CD_4}^{-1} \sigma^T$ et $\Gamma_{CD_4} = \Gamma_{CD} + \mathbb{I}_C \otimes \mathbb{I}_D$.

La fonction de Wigner globale est ainsi la combinaison linéaire de quatre fonctions de Wigner :

$$W_{AB}^{out} = \sum_{j=1}^4 C_j W^{(j)}, \quad (4.17)$$

où les coefficients sont donnés par les expressions respectives des fonctions de Wigner individuelles :

$$C_j = \frac{q_j}{\pi^2} \frac{\sqrt{\det \Gamma}}{\sqrt{\det \Gamma_{CD_j}}} \times \frac{\pi^2}{\sqrt{\det \Gamma_{AB_j}}}, \quad (4.18)$$

avec $q_1 = 1$, $q_2 = q_3 = -2$ et $q_4 = 4$. Il est important de noter que la soustraction de photon est un événement relativement improbable. Les fonctions de Wigner des états créés *conditionnellement* à la réussite de la soustraction de photon sont donc renormalisées en tenant compte de la probabilité P_G de générer l'état,

$$P_G = \sqrt{\det \Gamma} \sum_{j=1}^4 \frac{q_j}{\sqrt{\det \Gamma_{AB_j} \det \Gamma_{CD_j}}}. \quad (4.19)$$

Les expressions que nous avons dérivées vont nous permettre de calculer les matrices de covariance correspondantes *après* les soustractions de photon, d'évaluer leur évolution ultérieure suite à la transmission sur une longueur L_2 , et de les utiliser pour téléporter un état cohérent. La fidélité étant en effet linéaire en les fonctions de Wigner, nous aurons

$$F = \sum_{j=1}^4 C_j F^{(j)}, \quad (4.20)$$

les fidélités "individuelles" pouvant être calculées à l'aide des formules pour les états gaussiens (voir section 2.9).

4.3 Résultats

Les paramètres ajustables du schéma de transmission présenté à la figure 4.1 sont :

- La longueur du canal $L_{tot} = 2(L_1 + L_2)$, c'est-à-dire $T_{tot} = (T_1 T_2)^2$;
- Pour une longueur fixée, la position de la soustraction de photon, c'est-à-dire la valeur de T_1 , qui fixe la valeur de T_2 , ou inversement ;

- La valeur réelle de $T \approx 1$ du coefficient de transmission du diviseur de faisceau utilisé pour effectuer la soustraction de photon ;
- Le paramètre de compression r de la paire EPR.

Pour des valeurs de T_{tot} , T et r fixées, nous pouvons déterminer la position idéale de la soustraction de photon en faisant varier T_1 et T_2 . La figure 4.2 présente le degré de fidélité observé en fonction de T_2 – les valeurs des autres paramètres sont arbitraires et n’influent pas sur l’aspect qualitatif de la courbe. On observe que la fidélité croît de façon monotone lorsque T_2 diminue. Elle est maximale pour $T_2 = T^{1/2}$, c’est-à-dire lorsque $T_1 = 1$: la soustraction de photon doit se faire au *début* de la transmission, à la sortie du milieu non linéaire où la paire EPR est créée. La soustraction de photon ayant pour objectif de renforcer les corrélations entre les parties de la paire EPR, il semble effectivement logique de l’effectuer le plus tôt possible sur le schéma de transmission. Pour l’évaluation des performances du schéma optimisé, nous posons donc dans la suite $L_1 = 0 \Leftrightarrow T_1 = 1$.

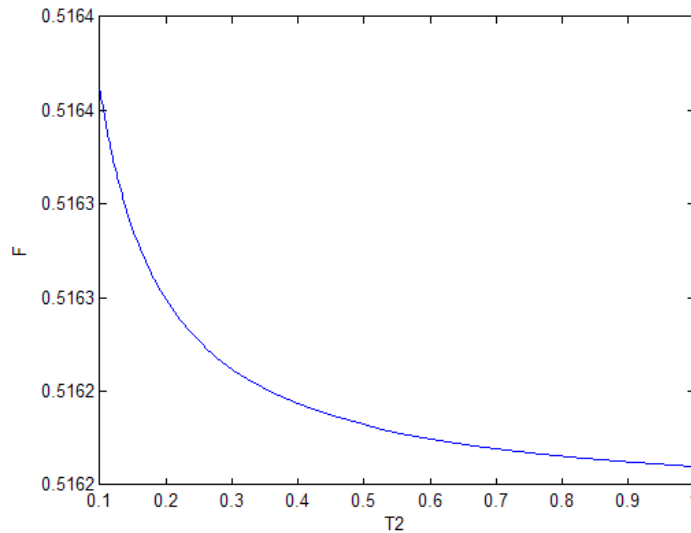


FIG. 4.2 – Fidélité de téléportation F d’un état cohérent en fonction de T_2 , avec $\sqrt{T_{tot}} = 0,1$, $r = 0,3$ et $T = 0,95$. La signification des paramètres est précisée dans le texte.

La figure 4.3 représente la variation de F en fonction de $T_{tot} = e^{-\alpha L_{tot}}$. L’effet escompté est bien présent : pour toutes les gammes de longueur de canal, la fidélité est améliorée par rapport au cas de téléportation sans soustraction de photon. A faibles distances toutefois, le fait que la source EPR ait un facteur de compression r fini rend le cas direct plus avantageux.

Le même graphique est tracé sur la figure 4.4, à ceci près que le paramètre r est plus grand. Cette fois, la soustraction de photon n’est plus favorable !

Le paramètre de compression joue donc un rôle pour déterminer si la soustraction de photon est utile, comme on peut le voir sur la figure 4.5. Si la fidélité augmente avec r , elle n’augmente pas aussi vite si l’on effectue une soustraction de photon. La soustraction permet ainsi de renforcer les corrélations EPR dans le cas de *squeezings* relativement faibles. Par contre, si la paire EPR est fortement corrélée, lui appliquer une soustraction de photon va au contraire dégrader ces corrélations.

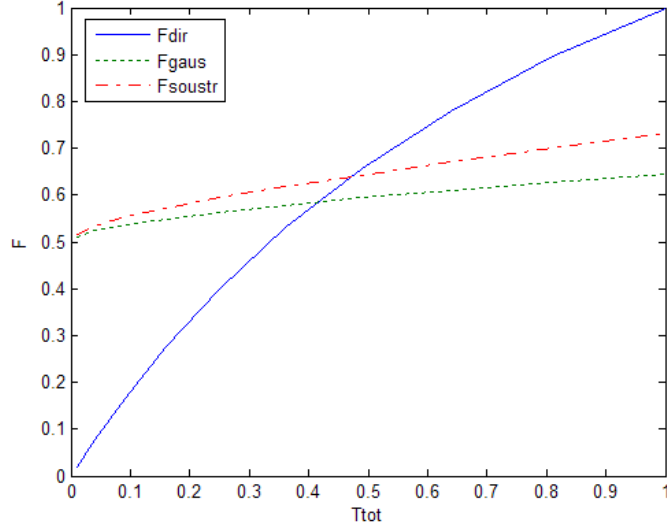


FIG. 4.3 – Fidélité de téléportation F d'un état cohérent en fonction de T_{tot} , avec $r = 0,3$ et $T = 0,95$. (a) Transmission directe. (b) Téléportation avec une paire EPR sans soustraction de photon. (c) Téléportation avec une paire EPR avec soustraction de photon.

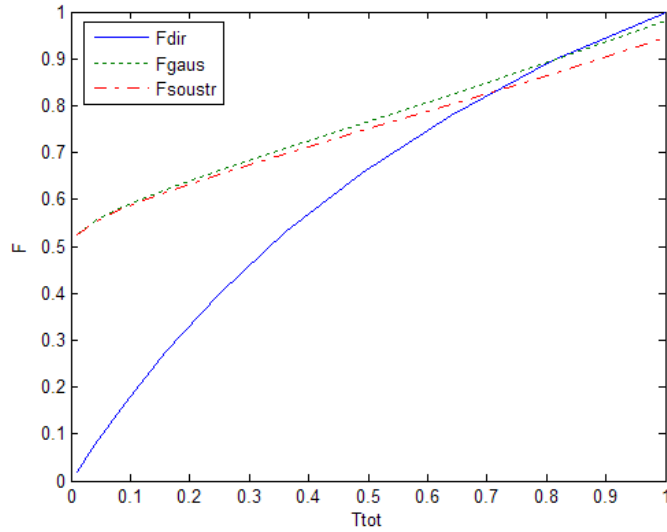


FIG. 4.4 – Fidélité de téléportation F d'un état cohérent en fonction de T_{tot} , avec $r = 2$ et $T = 0,95$. (a) Transmission directe. (b) Téléportation avec une paire EPR sans soustraction de photon. (c) Téléportation avec une paire EPR avec soustraction de photon.

Enfin, comme on peut le voir sur la figure 4.6, le coefficient de transmission T doit quant à lui être le plus grand possible pour maximiser la fidélité, qui est approximativement linéaire en T . En effet, lorsque $T \rightarrow 1$, un “clic” simultané des deux photodétecteurs signale avec une probabilité presque unitaire la soustraction d'un photon sur chaque mode de la paire EPR. Si T diminue, on dévie une plus grande fraction du faisceau, et l'on ne peut plus garantir que l'opération visée s'est effectivement déroulée.

La même figure montre cependant qu'il est nécessaire de procéder à un compromis entre la qualité de l'état *conditionnellement* créé et la probabilité de réussite de génération

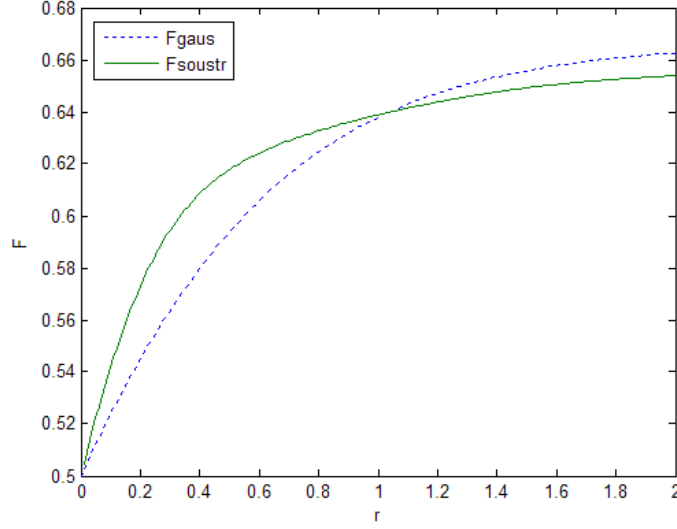


FIG. 4.5 – Fidélité de téléportation F d'un état cohérent en fonction du paramètre de compression r de la paire EPR utilisée, avec $T_{tot} = 0,25$ et $T = 0,95$. (a) Téléportation avec une paire EPR sans soustraction de photon. (b) Téléportation avec une paire EPR avec soustraction de photon.

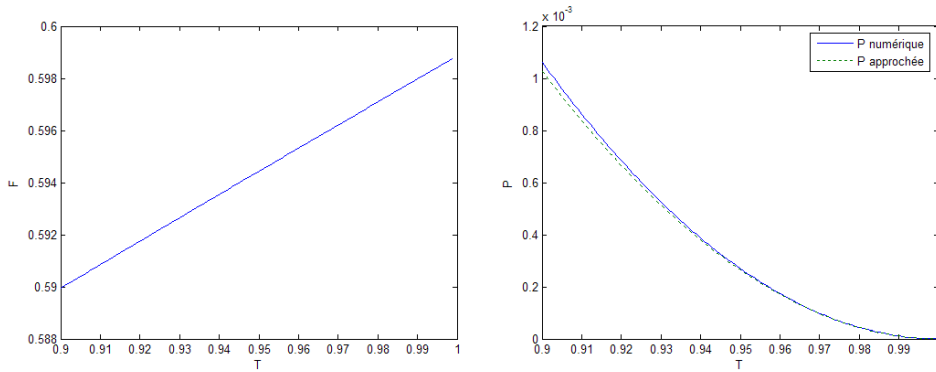


FIG. 4.6 – Influence du coefficient de transmission du diviseur de faisceau pour la soustraction de photon (a) sur la fidélité de téléportation F d'un état cohérent, (b) sur la probabilité de réussite de la génération de l'état. $T_{tot} = 0,25$ et $r = 0,3$.

de cet état. Si T est trop faible, on risque de soustraire plus d'un photon, mais si T est trop élevé, la soustraction de photon devient hautement improbable. Dans la limite $T = 1$, la probabilité devient nulle.

Il est possible de calculer de manière approchée la probabilité de soustraire un photon dans le mode A et dans le mode B . En représentation de Schrödinger, dans la limite $T \rightarrow 1$, la soustraction d'un photon revient à appliquer l'opérateur d'annihilation sur l'état considéré. L'état EPR s'écrit en base de Fock :

$$|\psi\rangle = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle_A \otimes |n\rangle_B, \quad (4.21)$$

où $\lambda = \tanh(r)$. Annihiler un photon dans les modes A et B revient à appliquer $\hat{a}_A \otimes \hat{a}_B$ sur cet état. On peut montrer [GPS07] que la probabilité de réussite s'écrit :

$$p = (1 - T)^2 \lambda^2 (1 - \lambda^2) \frac{1 + T^2 \lambda^2}{(1 - T^2 \lambda^2)^3}. \quad (4.22)$$

Cette expression est comparée à notre résultat numérique sur la figure 4.6 (b). Un très bon accord est présent aux valeurs proches de $T = 1$; lorsque l'on s'éloigne du domaine de validité de l'approximation, l'expression (4.22) sous-évalue quelque peu la probabilité de réussite, qui s'accroît d'autant plus que T diminue.

La soustraction de photon permettant une amélioration de la fidélité lorsqu'un *squeezing* limité est disponible, on peut envisager de répéter cette opération, comme le montre la figure 4.7. Les calculs nécessitent alors de traiter une combinaison linéaire de seize fonctions de Wigner et donc seize matrices de covariance.



FIG. 4.7 – Téléportation avec quatre soustractions de photon.

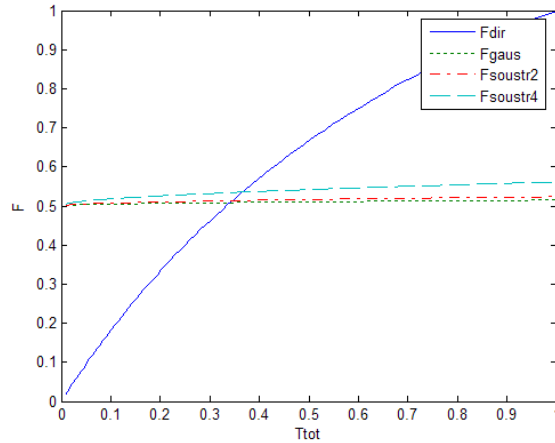


FIG. 4.8 – Amélioration de la fidélité suite à quatre soustractions de photons, à faible valeur de r .

La figure 4.8 montre les résultats de la simulation numérique effectuée. On constate un nouveau gain en fidélité.

Toutefois, nos considérations quant à la probabilité de réussite d'un tel événement peuvent s'étendre à ce cas, qui nécessite cette fois quatre "clics" simultanés et est donc hautement improbable. Une formule théorique approchée [GPS07] donne :

$$p = 4T^2(1 - T)^4 \lambda^4 (1 - \lambda^2) \frac{1 + 4T^4 \lambda^2 + T^8 \lambda^4}{(1 - T^4 \lambda^2)^5}. \quad (4.23)$$

La valeur de cette expression et les valeurs obtenues numériquement sont représentées sur la figure 4.9. On constate effectivement que la probabilité de réussite diminue drastiquement lorsque le nombre de soustractions augmente. On constate le même phénomène si l'on utilise deux paires EPR et que l'on soustrait un photon de chacun des quatre modes.

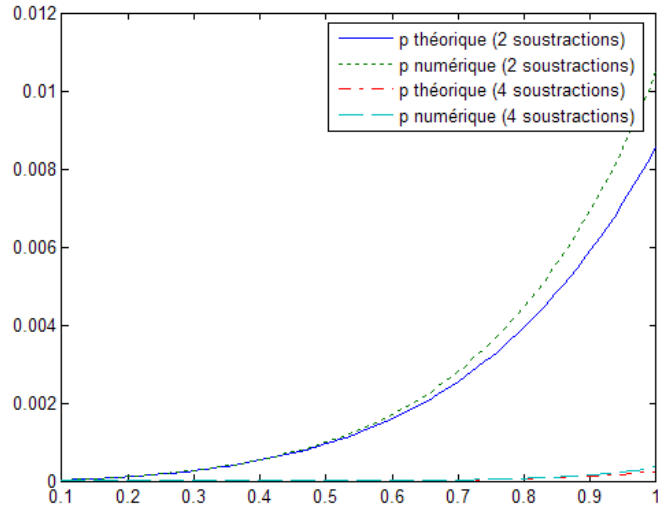


FIG. 4.9 – Comparaison du taux de réussite pour deux et pour quatre soustractions de photons, en fonction de r .

La soustraction de photon s'avère donc être une opération utile dans le cadre des communications quantiques à longue distance. Elle permet d'atteindre une valeur de fidélité donnée à plus grande distance. Toutefois, chaque soustraction est un événement relativement improbable. Il est donc peu réaliste d'envisager un schéma de transmission combinant un grand nombre de soustractions de photons : le débit du canal s'en trouverait fortement réduit.

Conclusion

Le but de notre travail était d’explorer les voies possibles pour établir des communications quantiques à longue distance. Les variables optiques continues, grâce à leurs avantages expérimentaux, sont un choix privilégié. Néanmoins, nous avons pu remarquer que “chaque avantage a son prix”.

Premièrement, en information quantique à variables continues – à l’inverse de l’information quantique à photons uniques (variables discrètes) – les pertes du canal sont à considérer comme du bruit : le signal, mélangé avec le bruit du vide, subit une très forte dégradation.

Une amplification préalable, bien qu’elle soit elle-même entachée de bruit, permet d’améliorer la transmission pour de longues distances. Le protocole de téléportation quantique est plus favorable encore ; il est possible de l’optimiser compte tenu des pertes et de la décohérence du canal. Cependant, de telles opérations nécessitent l’exploitation de cristaux non linéaires. Si cette technique est actuellement maîtrisée en laboratoire, les effets en termes d’intrication sont quantitativement limités. Un futur réseau de communications quantiques se devrait d’intégrer de tels éléments.

L’utilisation d’états quantiques non gaussiens de la lumière apporte un supplément de qualité à la transmission. Des opérations de soustraction de photon entraînent cependant un coût prohibitif pour le débit de la transmission (même en négligeant tout défaut expérimental) : statistiquement, une même opération doit être répétée un grand nombre de fois avant d’être effectivement réalisée.

Notre travail a montré toute la pertinence d’utiliser le protocole de téléportation comme moyen pour les communications quantiques à longue distance. Produire et répartir de l’intrication le long de la ligne de transmission quantique semble donc être le défi principal à relever pour le moyen terme. Les recherches en ce sens sont prometteuses.

A plus long terme, la présence de *répéteurs* quantiques, dotés, à l’opposé des relais, d’une mémoire quantique, pourrait révolutionner le domaine. Ils permettraient en effet de stocker un certain laps de temps des états quantiques au sein de la ligne de transmission, pour en faire usage au moment opportun – ce qui ne nécessite plus d’attendre la réalisation hautement improbable d’événements simultanés. L’intrication pourrait alors être répartie tout au long d’un canal pendant un laps de temps non négligeable.

Bibliographie

- [ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental tests of bell's inequalities using time-varying analysers. *Physical Review Letters*, 49, 1982.
- [Asp76] A. Aspect. Proposed experiment to test the non-separability of quantum mechanics. *Physical Review D*, 14, 1976.
- [Bay05] D. Baye. *Mécanique quantique. Première partie : Notions de base*. Presses Universitaires de Bruxelles, Bruxelles, 2005.
- [BBB⁺92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1), 1992.
- [Bel64] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1, 1964.
- [BvL05] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77, 2005.
- [Cav82] C. M. Caves. Quantum limits on noise in linear amplifiers. *Physical Review D*, 26(8), 1982.
- [CGDR05] D. Collins, N. Gisin, and H. De Riedmatten. Quantum relays for long distance quantum cryptography. *Journal of Modern Optics*, 52 (5), 2005.
- [CLP07] N.J. Cerf, G. Leuchs, and E. S. Polzik. *Quantum information with continuous variables of atoms and light*. Imperial College Press, London, 2007.
- [Eke91] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6), 1991.
- [EPR35] A. Einstein, R. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 4 (7), 1935.
- [ESP02] J. Eisert, S. Scheel, and M. B. Plenio. Distilling gaussian states with gaussian operations is impossible. *Physical Review Letters*, 89(13), 2002.
- [GG02] F. Grosshans and Ph. Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5), 2002.
- [GPFC05] R. Garcia-Patron, J. Fiurasek, and N. J. Cerf. Loophole-free test of quantum nonlocality using high-efficiency homodyne detectors. *Physical Review A*, 71(022105), 2005.
- [GPS07] R. Garcia-Patron Sanchez. *Quantum information with optical continuous variables. From Bell tests to key distribution*. PhD thesis, Université Libre de Bruxelles, 2007.
- [Ili07] N. Ilic. The ekert protocol. *Journal of Phy334*, 2007.
- [Lan99] M. Langlois. *Cryptographie quantique - solution au problème de distribution de clefs secrètes*. Université d'Ottawa, 1999.

- [Man07] P. Mandel. *Introduction à l'optique non-linéaire et à l'optique quantique. Notes de cours*. Université Libre de Bruxelles, 2007.
- [MBG93] A. Muller, J. Breguet, and N. Gisin. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. *Europhysics Letters*, 23(6), 1993.
- [MSI90] M. Meystre and M. Sargent III. *Elements of Quantum Optics*. Springer-Verlag, Berlin, third edition, 1990.
- [NC00] M.A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- [NVT06] K. Neyts, I. Veretennicoff, and P. Tassin. *Optical materials*. Vrije Universiteit Brussel, Bruxelles, 2006.
- [OPB03] S. Olivares, M. G. A. Paris, and R. Bonifacio. Teleportation improvement by inconclusive photon subtraction. *Phys. Rev. A*, 67(032314), 2003.
- [Our07] A. Ourjountsev. *Etude théorique et expérimentale de superpositions quantiques cohérentes et d'états intriqués non-gaussiens de la lumière*. PhD thesis, Université Paris-Sud XI, 2007.
- [Pre98] J. Preskill. *Physics 219 : Quantum computation*. 1998. <http://www.theory.caltech.edu/people/preskill/ph219/>.
- [RSA78] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communication of the ACM*, 21 (2), 1978.
- [Sha48] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27, 1948.
- [Sho94] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.
- [Sin99] S. Singh. *The Code Book*. Fourth Estate Ltd, 1999.
- [SZ97] M.O. Scully and M.S. Zubairy. *Quantum Optics*. Cambridge University Press, Cambridge, 1997.
- [TW92] P. Tombesi and D. F. Walls. *Quantum Measurements in Optics*. Plenum Press, New York, 1992.
- [Wen04] J. Wenger. *Dispositifs impulsions pour la communication quantique à variables continues*. PhD thesis, Université Paris XI, 2004.
- [Wie83] S. Wiesner. Conjugate coding. *Sigact News*, 15(1), 1983.