Dispositifs impulsionnels pour la communication quantique à variables continues

Jérôme Wenger

N° d'ordre : 7591

LABORATOIRE CHARLES FABRY
DE L'INSTITUT D'OPTIQUE
CNRS UMR 8501

UNIVERSITÉ PARIS XI
U.F.R. SCIENTIFIQUE D'ORSAY

THÈSE

Spécialité : Lasers et Matière

présentée pour obtenir
le grade de Docteur en Sciences
de l'Université Paris XI Orsay

par

Jérôme WENGER

Sujet :

DISPOSITIFS IMPULSIONNELS POUR LA COMMUNICATION QUANTIQUE À VARIABLES CONTINUES

Soutenue le 09 septembre 2004 devant la Commission d'examen :

M.	Alain ASPECT	Président
M.	Nicolas CERF	Examinateur
M.	Juan-Ariel LEVENSON	Rapporteur
M.	Jean-François ROCH	Rapporteur
Mme	Rosa TUALLE-BROURI	Examinatrice
M.	Philippe GRANGIER	Directeur de thèse

Résumé

L'objectif central de cette thèse est d'exploiter les propriétés quantiques du champ électromagnétique pour développer de nouveaux dispositifs de communication. L'étude porte sur les composantes de quadrature (variables quantiques continues) d'un mode impulsionnel du champ lumineux.

Une démonstration expérimentale de cryptographie quantique avec des états cohérents a été réalisée. Le dispositif se base sur des impulsions modulées en amplitude et en phase et comportant en moyenne une centaine de photons. Pour chaque impulsion lumineuse, une détection homodyne résolue en temps permet de mesurer une composante de quadrature particulière avec une forte efficacité. Une clé secrète a ainsi été transmise à un débit de 1.7 Mbits/s en l'absence de pertes et 75 kbits/s pour une transmission présentant des pertes de 3.1 dB, ce qui ouvre la voie pour des applications de cryptographie quantique à hauts débits.

Afin d'étudier l'utilisation de spécificités quantiques, nous avons développé une source impulsionnelle d'états comprimés et d'états intriqués. Cette source utilise des conversions non-linéaires d'impulsions ultrabrèves intervenant dans un cristal mince de niobate de potassium. Suivant la configuration, la réduction du bruit en quadrature est de 2.7 dB sous le niveau de bruit quantique standard, ou les corrélations entre les quadratures des faisceaux intriqués sont de 2.5 dB. Grâce à ce dispositif, nous avons mis en œuvre la première expérience de "dégaussification", pour transformer des impulsions de vide comprimé en des états non-gaussiens. Ce protocole est directement lié à la distillation de l'intrication de variables continues, qui permet d'améliorer la portée des dispositifs de cryptographie.

Enfin, des schémas sont étudiés pour réaliser des tests complets des inégalités de Bell avec des variables continues mesurées par des détections homodynes.

Mots Clés

Information quantique – communication quantique – cryptographie quantique – variables continues – détection homodyne impulsionnelle – impulsions femtosecondes – amplification paramétrique – états comprimés – états non-gaussiens – intrication quantique – inégalités de Bell

Aux co-auteurs des articles publiés lors de cette thèse :

Philippe, Rosa, Frédéric, Nicolas, Jaromir, Raoul, Mohammad, Alexei et Gilles.

Ce manuscrit reflète les travaux que nous avons menés en commun. Cependant, tout ce que nous avons appris ensemble ne représente que peu de chose par rapport à ce que vous m'avez enseigné. Que ce document soit alors aussi l'expression de mes plus chaleureux remerciements et le témoin d'une amitié fidèle.

Table des matières

Introduction : information quantique avec des variables continues

Suivant l'observation de Moore, la vitesse des microprocesseurs double tous les 18 mois. Les composants électroniques élémentaires deviennent ainsi plus petits, et ne comporteront bientôt plus que quelques atomes. A cette échelle, les effets quantiques deviendront alors importants. Il faut donc *comprendre* les lois qui régissent les objets quantiques.

Suivant l'observation d'Einstein, la mécanique quantique prédit des corrélations qui dépassent celles offertes par un système classique, et vont même à l'encontre du sens commun. La physique quantique propose ainsi des ressources nouvelles. Il faut donc *exploiter* les lois qui régissent les objets quantiques.

Suivant l'observation de Murphy, toute expérience qui pourrait rater va aller de travers. Les systèmes quantiques, fragiles par nature, sont délicats à manipuler. Il faut donc *maîtriser* les lois qui régissent les objets quantiques.

Le projet de recherche du groupe d'Optique Quantique de l'Institut d'Optique s'inscrit dans le triple objectif de compréhension, maîtrise et exploitation de certains objets quantiques, dans le but de développer de nouveaux systèmes de communication et de traitement de l'information. En particulier, ce travail de thèse est consacré aux communications quantiques avec les composantes de quadrature d'un mode du champ électromagnétique.

Vers une technologie quantique

La découverte et la formalisation de l'électromagnétisme au XIX^{e} siècle ont profondément affecté les développements technologiques du XX^{e} siècle. Une aventure similaire va peut-être se produire pour la mécanique quantique, découverte et formalisée au début du XX^{e} siècle, et dont les applications pourraient avoir une influence notable sur la technologie du XXI^{e} siècle. Bien que les lasers et les semiconducteurs soient déjà des objets courants liés à la physique quantique, ils peuvent se représenter suivant un modèle semi-classique et n'exploitent pas toutes les possibilités du monde quantique. La physique quantique offre des applications encore plus décisives : depuis les deux dernières décennies, de nombreuses études théoriques et expérimentales ont démontré que les effets quantiques peuvent être exploités pour réaliser de nouvelles opérations de communication ou de calcul, qui dans certains cas sont impossibles à réaliser avec des systèmes classiques [1, 2].

Nous vivons actuellement les prémices de la *seconde révolution quantique* [5]. La première révolution quantique est intervenue au début du XX^{e} siècle, et nous donne de nouvelles règles pour comprendre les phénomènes physiques. La seconde révolution quantique tire parti de ces règles pour développer des applications nouvelles de traitement de l'information. Parmi ces applications, la plus médiatique est la téléportation quantique [158], la plus proche d'une réalisation

commerciale est la cryptographie quantique [43]. Comme pour toute révolution, des événements fondateurs initient son émergence. Premièrement, grâce aux développements technologiques récents, il est maintenant possible de manipuler des objets quantiques individuels. Deuxièmement, grâce aux développements conceptuels récents, il est reconnu que l'information est enregistrée, transmise et manipulée par des systèmes matériels qui obéissent aux lois de la physique. La convergence de ces deux points a donné naissance au concept de l'*information quantique*, c'est-à-dire l'exploitation des possibilités offertes par la physique quantique pour traiter l'information de manière plus efficace qu'avec des systèmes classiques.

La première considération du principe d'incertitude d'Heisenberg comme une ressource plutôt que comme une limitation semble avoir été proposée par Wiesner en 1969 [42]. Son idée est de proposer des billets de banque infalsifiables à base de spin 1/2 : chaque billet comporte une série de spins quantiques stockés sur le billet, dont l'orientation est différente pour chaque billet et n'est connue que de la banque seule. D'après le principe d'incertitude, tout faux-monnayeur qui essaierait de dupliquer le billet induira nécessairement des erreurs dans l'orientation des spins. Comme la banque connaît l'orientation initialement portée par le billet, elle peut en vérifier parfaitement l'authenticité. L'idée de Wiesner – dont l'application est fortement limitée par les temps de stockage des spins 1/2 – a dans un premier temps été refusée par toutes les revues scientifiques avant d'être finalement publiée en 1983. Cette date est révélatrice : au début des années 1980, l'utilisation des ordinateurs se développe, l'information est considérée comme une quantité physique, mesurable en bits. Toutes les conditions sont présentes pour que la physique quantique rejoigne la théorie de l'information.

L'idée de codage de Wiesner se retrouve dans le protocole de transmission d'une clé secrète avec des états quantiques proposé Bennett et Brassard en 1984 [43]. L'échange se fait en envoyant des photons uniques, dont la polarisation particulière code pour une valeur de bit. Suivant le principe d'incertitude d'Heisenberg, une tentative d'espionnage du photon induira nécessairement des perturbations, et pourra donc être décelée par les partenaires autorisés. Ce principe permet ainsi de garantir la sécurité du transfert à partir des lois de la physique. Le protocole de Bennett et Brassard a été mis en œuvre pour la première fois en 1992, et a donné lieu depuis à de nombreux développements, dont des systèmes disponibles commercialement [40]. Aujourd'hui connu sous le nom de *cryptographie quantique*, c'est un domaine pluridisciplinaire en pleine expansion, à l'intersection de la physique, de l'informatique et de la théorie de l'information. Dans une plus large mesure, l'utilisation des propriétés quantiques pour réaliser de nouveaux systèmes d'échange d'information forme le domaine de la *communication quantique*, dans lequel s'inscrit assez largement ce travail de thèse.

L'information quantique est également constituée d'une branche consacrée à l'étude de nouveaux algorithmes basés sur les principes de la physique quantique. Initié par une idée de Feynman en 1982, ce domaine, le *calcul quantique*, a explosé dans les années 1990 après l'introduction par Shor d'un algorithme quantique de factorisation qui permet une amélioration exponentielle par rapport aux algorithmes classiques existants [1]. Dans un ordinateur exploitant des algorithmes quantiques, l'information est généralement codée sur des bits quantiques, ou *qubits*, qui sont régis par la physique quantique. Contrairement aux bits classiques qui ne peuvent prendre que la valeur binaire 0 ou 1, les qubits peuvent se trouver dans une superposition d'états codant pour 0 ou 1. Cette particularité permet de placer l'ordinateur quantique dans une superposition de tous les états d'un ordinateur classique contenant le même nombre de bits. Les algorithmes quantiques exploitent alors ce parallélisme pour effectuer certaines opérations plus efficacement que des systèmes classiques. Même si la réalisation expérimentale d'un ordinateur quantique se heurte à de nombreuses difficultés techniques, le calcul quantique est néanmoins un domaine de recherche fructueux, propice à l'émergence d'idées innovantes.

Utilisation des variables quantiques continues

Les possibilités d'applications pratiques des systèmes quantiques ont amené de nombreux protocoles de traitement de l'information quantique [1, 2]. Parmi les résultats les plus marquants, nous pouvons citer par exemple la distribution de clé quantique, la téléportation quantique ou l'algorithme de factorisation quantique. Pour la plupart, ces concepts ont été initialement formulés pour des systèmes quantiques à deux états ou *qubits*, comme le spin 1/2, l'atome à deux niveaux d'énergie ou la polarisation d'un photon unique. Ces états simples sont représentés dans un espace de Hilbert de dimension 2, mais présentent toutes les particularités quantiques : superposition d'états, intrication... Comme le nombre de valeurs possibles prises lors de mesures est fini, on parle alors de *variables quantiques discrètes*.

Récemment, une attention soutenue a été apportée à une autre approche, fondée sur l'utilisation de *variables quantiques continues*, comme par exemple les composantes de quadrature d'un mode du champ électromagnétique ou les composantes de spin d'un ensemble atomique. Les variables continues peuvent prendre une infinité de valeurs, et définissent un espace de Hilbert de dimension infinie, beaucoup plus riche qu'un espace de dimension 2. Par exemple, comme nous le verrons au cours de cette thèse, chaque valeur prise par une variable continue peut transmettre plusieurs bits d'information, alors qu'une variable discrète à deux niveaux ne fournit au mieux qu'un bit par valeur échangée. De plus, les variables continues présentent de nombreux avantages expérimentaux intrinsèques, en étant plus simples à produire et à manipuler que des qubits. En effet, une limite technique majeure est imposée aux qubits par leurs systèmes de détection, qui doivent être sensibles à un quantum individuel. Or ces systèmes sont généralement lents, chers et d'une efficacité limitée, ce qui restreint leurs applications pour des procédures de communication à haut débit. A l'opposé, les variables continues peuvent être mesurées par des détections interférométriques, qui emploient des photodiodes usuelles, rapides et efficaces.

L'étude expérimentale des variables continues a débuté à partir de 1985 avec les mesures de réduction des fluctuations quantiques et la production d'états comprimés [105, 106, 107]. L'intrication quantique entre les composantes de quadrature a ensuite été considérée théoriquement [133] et expérimentalement [143, 144]. Les variables continues sont également au cœur des mesures quantiques non-destructives [21, 22]. La première utilisation des variables continues pour la communication quantique a été implicitement proposée dans le protocole de cryptographie à base de deux états quantiques non-orthogonaux développé par Bennett en 1992 [46]. Une autre date également retenue pour indiquer les débuts de l'information quantique avec des variables continues est l'extension du protocole de téléportation par Vaidman en 1994 [159, 158]. La première expérience de traitement de l'information quantique avec des variables continues a consisté en une version légèrement différente de ce protocole de téléportation et a été réalisée par l'équipe de Jeff Kimble en 1998 [146]. Depuis, de nombreux travaux théoriques et expérimentaux ont été menés dans le domaine des variables continues, comme nous le verrons au cours des références présentées dans ce manuscrit.

Contexte scientifique en début de thèse

Ce travail de thèse a été débuté au cours du mois d'avril 2001. A ce moment, de nombreux protocoles de traitement de l'information quantique, initialement formulés pour les variables discrètes, ont été étendus au cas des variables continues : téléportation [159, 146], codage dense [162], clonage [80, 81, 82]. L'utilisation des variables continues pour la communication et le calcul quantique a ainsi pris son essor. La caractérisation et l'exploitation de l'intrication quantique font l'objet de nombreuses études [134, 135]. Par ailleurs, des méthodes ont été proposées pour

effectuer des codes quantiques correcteurs d'erreurs [191, 65] ainsi que des opérations de calcul quantique avec des variables continues [161, 3]. La cryptographie quantique fait également l'objet de nombreuses propositions théoriques de protocoles au cours de l'année écoulée [61, 62, 63, 64].

D'un point de vue fondamental, diverses questions restent sans réponses. En cryptographie quantique, il est plus ou moins admis qu'il est nécessaire d'utiliser des spécificités quantiques comme la compression des fluctuations ou l'intrication, mais aucune étude ne donne les bornes minimales des effets quantiques à atteindre. Dans le cadre de la manipulation de l'intrication, Duan et ses collaborateurs proposent une méthode de purification de l'intrication portée par des variables continues gaussiennes [125], mais la mise en œuvre de ce dispositif est une expérience particulièrement délicate. Ceci soulève la question de l'existence de protocoles simples de distillation de l'intrication de variables continues. Dans une plus large mesure, les limites des possibilités de manipulation des états gaussiens par des opérations gaussiennes locales sont inconnues. Enfin (et surtout) le domaine des variables continues manque fortement de réalisations expérimentales : système de cryptographie quantique, production d'états intriqués, manipulation des composantes de spin d'ensembles atomiques... Ce travail de thèse intervient sur le point particulier de l'exploitation des composantes de quadrature pour réaliser le premier système complet de cryptographie quantique avec des variables continues et pour monter une source impulsionnelle polyvalente d'états quantiques comprimés ou intriqués.

Plan et guide de lecture

Ce manuscrit est composé de trois parties, qui regroupent entre trois et cinq chapitres. La première partie introduit les moyens théoriques et expérimentaux qui seront utilisés pour manipuler les variables continues au cours de cette thèse. Un premier chapitre consacré à l'information classique sert de préliminaire à l'exploitation des variables continues dans le cadre de l'information quantique. Nous passons ensuite au domaine quantique avec le second chapitre, qui rappelle brièvement les principaux outils de l'optique quantique pour les variables continues. Enfin le troisième chapitre donne les différents aspects théoriques et expérimentaux de la mesure des variables continues avec une détection homodyne résolue en temps.

La seconde partie traite du système de cryptographie quantique avec des impulsions cohérentes qui a été développé par notre groupe de recherche. Le chapitre 4 présente les protocoles théoriques de cryptographie quantique avec des états cohérents, qui avaient déjà été étudiés lors du travail de thèse de Frédéric Grosshans [71]. Ces protocoles sont ensuite mis en œuvre expérimentalement, ce qui donne lieu au chapitre 5. Enfin, pour clore la partie consacrée à la cryptographie quantique, le chapitre 6 discute le lien entre l'intrication et les protocoles avec des états cohérents.

La troisième et dernière partie quitte l'utilisation des états quasi-classiques pour se concentrer sur la génération et la caractérisation d'états spécifiquement quantiques du champ lumineux. Le chapitre 7 propose une source d'états comprimés par amplification paramétrique d'impulsions femtosecondes individuelles. Ces états comprimés sont ensuite caractérisés lors du chapitre 8 par une méthode originale qui ne fait pas intervenir de référence de phase. Le chapitre 9 décrit une procédure pour transformer des états comprimés en des états non-gaussiens, qui ouvrent des perspectives expérimentales nouvelles pour le traitement de l'information quantique. Nous délaissons ensuite la classe des états monomodes pour considérer les états quantiques à deux modes. Le chapitre 10 présente un dispositif de génération d'états impulsionnels intriqués en quadratures. Enfin, l'utilisation des variables continues pour des tests inconditionnels des inégalités de Bell est discutée lors du chapitre 11.

Afin de simplifier la lecture de ce document, une brève introduction de une à deux pages en tête de chaque chapitre replace le sujet abordé dans son contexte de recherche, tandis qu'une rapide conclusion en fin de chaque chapitre résume les principaux résultats obtenus. Par ailleurs, les formules essentielles apparaissent sur un fond gris. Les principales données techniques sont résumées dans des tableaux récapitulatifs présentés dans les chapitres concernés. Enfin, les références bibliographiques sont triées par domaine spécifique d'application. Les chapitres 1, 2, 4, 6 et 11 sont essentiellement théoriques. Les chapitres 3, 5, 7, 8, 9 et 10 sont à dominante expérimentale.

Partie I

Moyens théoriques et expérimentaux pour l'exploitation des variables continues

Chapitre 1

Information classique avec des variables continues

Sommaire

Le projet général de cette thèse s'inscrit dans la conception et la réalisation de nouveaux protocoles de traitement de l'information à partir de la manipulation des propriétés quantiques du champ lumineux. Avant d'aborder le domaine de l'information quantique proprement dite, il est utile de rappeler les concepts et les résultats majeurs de la théorie classique de l'information. Ces résultats caractérisent les limites classiques des protocoles de communication et nous guideront ainsi naturellement dans nos choix de dispositifs expérimentaux et de protocoles quantiques de traitement de l'information. C'est donc avec une arrière-pensée d'utilisateur que nous abordons cette théorie classique, en vue d'une transposition dans le domaine quantique.

Les fondements de la théorie de l'information telle que nous la connaissons aujourd'hui ont été posés par Claude Shannon dans un article devenu une référence célèbre [6] toujours d'actualité. Son intuition majeure est d'identifier un processus de communication comme un processus fondamentalement *aléatoire* où une source (communément nommée Alice) envoie un message inconnu à un récepteur (appelé Bob) à travers un canal physique qui est le siège d'inévitables perturbations. Si banale qu'elle puisse nous paraître maintenant, l'identification de ce schéma était une condition nécessaire à l'élaboration de la théorie de l'information, et dans une plus large mesure, à la conception de l'information en tant que grandeur physique au sens propre.

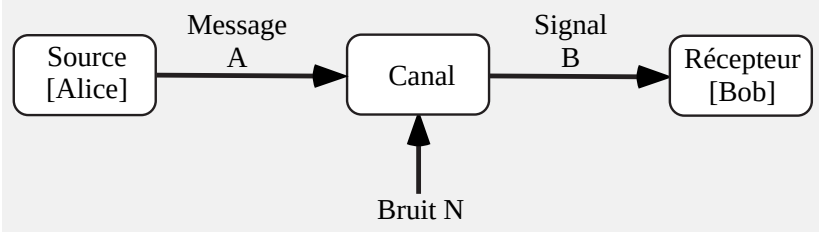

Figure 1.1: *Paradigme de Shannon : schéma fondamental d'une transmission.*

En vue d'introduire la théorie de Shannon avec des variables continues, il est préférable de commencer par en manipuler les concepts dans le cas plus intuitif des variables discrètes, puis de passer aux spécificités des variables continues. Nous verrons ensuite comment exploiter pratiquement cette théorie pour extraire le maximum d'information binaire à partir de variables continues. L'ensemble de ces particularités constitue un guide précieux pour la conceptions des expériences décrites plus avant dans ce manuscrit.

1.1 Introduction par les variables discrètes

Pour introduire la mesure quantitative et la communication de l'information, il est pratique de considérer une source discrète et finie. Les messages émis par une telle source sont des suites de symboles issus d'un ensemble fini qui constitue l'alphabet de la source. Nous pouvons déjà préciser d'autres caractéristiques de cette source : du point de vue du destinataire, les signaux émis sont nécessairement aléatoires (s'ils étaient parfaitement déterministes, le problème de la communication ne se poserait pas). Par ailleurs, la source réalisant une succession d'événement répétitifs, nous supposerons par la suite que la distribution de probabilité des messages est invariante dans le temps, ce qui nous amène à considérer le cas d'un système stationnaire et ergodique. Ces remarques ont conduit Shannon à traiter une source d'information comme le siège d'événements aléatoires formant le message et à définir la quantité d'information de ce message comme une mesure de son imprévisibilité [6]. Une analogie avec la thermodynamique conduit alors à introduire l'*entropie* d'une variable statistique.

1.1.1 Mesure de l'information : entropie de Shannon

Définition de l'entropie

Si le nombre de messages à considérer est fini, alors n'importe qu'elle fonction monotone de ce nombre peut être considérée comme une mesure de l'information véhiculée par chacun des messages. Cette information apportée étant directement liée au caractère *imprévisible* du message, la mesure quantitative de l'information devra donc être reliée à l'*inattendu*. Ainsi, un événement certain apportera une quantité d'information nulle alors qu'un ensemble d'événements d'égales probabilités apportera une quantité d'information maximale. Par ailleurs, notre intuition de deux événements indépendants nous amène à concevoir leur quantité d'information mutuelle comme la somme de leurs quantités d'information individuelles. Ces critères conduisent alors naturellement vers une quantification de l'information basée sur la fonction logarithme.

Considérant une source stationnaire discrète émettant des lettres d'un alphabet mutuellement indépendantes $X \in \{x_i\}_{i=1,..,n}$ avec des probabilités associées $\Pr(x_i) = Prob(X = x_i)$, Shannon

a introduit la mesure de la quantité d'information de la variable X par la notion d'*entropie* de X, définie par [6] :

$$H(X) = -\sum_{i=1}^{n} \Pr(x_i) \log_2 \Pr(x_i) \tag{1.1}$$

La base des logarithmes détermine l'unité d'information. Conformément au choix de Shannon, la base est prise ici égale à 2. L'unité d'entropie s'exprime alors en *b*inary un*it* : *bit* qui caractérise le choix entre deux possibilités [1] (pour éviter toute confusion avec les bits électroniques *b*inary dig*it*, certains textes utilisent la dénomination *shannon* pour l'unité binaire d'information).

L'entropie $H(X)$ peut ici se concevoir comme une moyenne de l'*imprévisibilité* de chaque événement x_i, que l'on définit comme $\log_2[1/\Pr(x_i)]$. Cette mesure de la quantité d'information est très dissociée du sens commun que l'on donne à l'information : véracité, pertinence, affectivité... La théorie de Shannon est ainsi à concevoir comme un ensemble purement technique, où la notion d'information est totalement différente de la teneur sémantique associée au message propre.

Le théorème fondamental de codage de source [6, 7, 8] assure qu'il est possible d'éliminer toute redondance d'une source par un codage adéquat des messages émis. Pour un message codé dépourvu de redondance, l'entropie par symbole est alors le nombre de bits nécessaires à la spécification de chaque symbole du message, ce qui s'exprime par la relation :

$$H = \lim_{L \to \infty} \frac{\log_2 m(L)}{L} \tag{1.2}$$

où $m(L)$ est le nombre de messages possibles de longueur L, et $\log_2 m(L)$ le nombre de bits nécessaires pour spécifier complètement le message. Dans le cas d'une source émettant des symboles uniformément répartis suivant la norme ASCII (alphabet de 128 éléments), chaque symbole envoyé représentera donc 7 bits d'information.

Enfin, il est possible d'étendre le formalisme de l'entropie de l'information au cas à plusieurs variables. L'entropie conjointe de deux variables A et B d'éléments a_i, b_j s'exprime par :

$$H(A,B) = -\sum_{i=1}^{n_a} \sum_{j=1}^{n_b} \Pr(a_i, b_j) \log_2 \Pr(a_i, b_j) \tag{1.3}$$

De façon analogue, on peut définir des entropies conditionnelles :

$$H(B|A) = -\sum_{i=1}^{n_a} \sum_{j=1}^{n_b} \Pr(a_i, b_j) \log_2 \Pr(b_j|a_i) \tag{1.4}$$

Cette dernière grandeur quantifie l'incertitude résiduelle sur B quand on connaît A, ce qui est représenté sur la figure 1.2.

Propriétés de l'entropie

Avant d'aborder le sujet de l'échange d'information entre deux parties, quelques propriétés fondamentales de l'entropie comme mesure de l'information sont rappelées ci-après [7, 8] :

[1] Plus précisément, l'entropie éq.(1.1) définit une entropie par symbole émis. On peut exprimer un débit d'entropie (exprimé en bits/s) en multipliant $H(X)$ par la cadence d'émission des symboles.

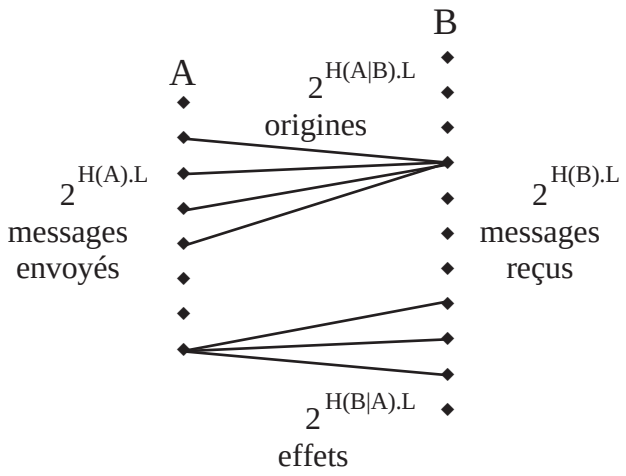

Figure 1.2: *Relations entre les messages à la source (A) et au récepteur (B), pour des blocs de longueur L symboles transitant au travers d'un canal bruité. Seuls les messages les plus probables sont représentés (ou du moins ceux qui se réduisent à cet ensemble via un codage optimal adéquat).*

- A une constante multiplicative près (changement d'échelle), la définition (1.1) de l'entropie est unique.
- L'entropie d'une variable discrète est positive ou nulle, $H(X) \geq 0$. Elle s'annule si un des événement est certain (probabilité associée égale à 1).
- $H(A, B) \leq H(A) + H(B)$ avec égalité si et seulement si les variables A et B sont indépendantes.
- $H(A, B) = H(A) + H(B|A) = H(B) + H(A|B)$
- La connaissance d'une variable supplémentaire ne peut pas augmenter l'entropie : $H(B|A) \leq H(B)$
- L'entropie ne peut que croître si on ajoute un nouveau système : $H(B) \leq H(B, A)$
- L'entropie est maximale lorsque tous les événements sont équiprobables.

A titre d'exemple, l'entropie d'une variable aléatoire binaire valant 0 avec la probabilité p et 1 avec la probabilité $1 - p$ s'exprime par $H(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$. Cette fonction est représentée en fonction de la valeur de p sur la figure 1.3. L'entropie est nulle lorsqu'un des événements est sûr ($p = 0$ ou 1) et maximale lorsque les événements sont équiprobables ($p = 1/2$). Dans ce cas, l'entropie vaut un choix parmi deux possibilités, soit une unité binaire ou 1 bit.

1.1.2 Transfert d'information : information mutuelle et capacité d'un canal

Une autre mesure de l'information, différente de l'entropie d'une variable, consiste en la quantité d'information que la connaissance d'un signal en sortie d'un canal (bruité) de communication

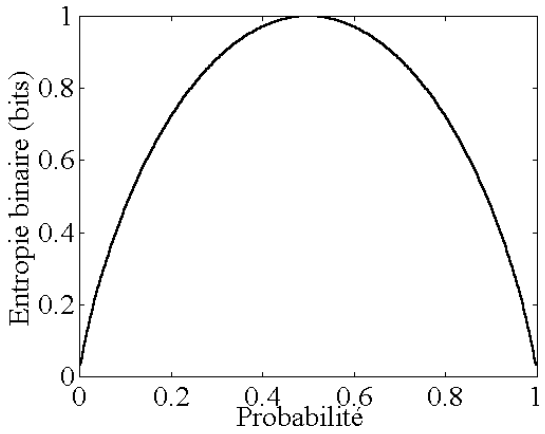

Figure 1.3: *Entropie d'une variable binaire en fonction de la probabilité de l'événement "0".*

apporte sur le message émis à l'entrée. On s'intéresse alors non plus à l'indétermination mais à la connaissance utile échangée.

D'une façon plus générale, on introduit la notion d'*information mutuelle moyenne* I_{AB} pour un couple de variables, qui caractérise l'information que la donnée de l'une apporte sur l'autre. Exprimée en bits par symbole, l'information mutuelle caractérise le débit d'information utile aux deux parties.

$$\begin{aligned} I_{AB} &= H(A) - H(A|B) && \text{(1.5a)} \\ &= H(B) - H(B|A) && \text{(1.5b)} \\ &= H(A) + H(B) - H(A,B) && \text{(1.5c)} \end{aligned}$$

La première ligne s'interprète comme l'information émise $H(A)$ diminuée de l'indétermination quant au symbole émis lorsque le symbole reçu est connu $H(A|B)$, qui est la quantité d'information supplémentaire à fournir pour corriger le message reçu. Symétriquement, la seconde ligne s'interprète comme l'information reçue moins l'incertitude sur le symbole reçu quand le symbole émis est donné. Enfin, la troisième ligne se conçoit comme la somme des informations de chaque partie, moins l'indétermination commune : en un sens, il s'agit du nombre de bits utiles communs aux deux stations.

Pour transmettre efficacement un signal à travers un canal, encore faut-il que ce canal soit adapté au débit d'information envoyée et qu'il ne rajoute pas trop de bruit. D'une manière analogue à l'entropie, la capacité $\mathcal{C}$ d'un canal discret est définie par :

$$\mathcal{C} = \lim_{L\to\infty} \frac{\log_2 m_c(L)}{L} \tag{1.6}$$

où $m_c(L)$ est le nombre de messages possibles de longueur en symboles L transitant à travers le canal et compatibles avec ses contraintes techniques. En l'absence de bruit, la capacité est alors la quantité d'information maximale que chacun des symboles peut apporter en sortie.

En présence de bruit, la capacité d'un canal est donnée par le taux maximal de transfert d'information sans distorsion irrémédiable du signal. Le maximum s'entend par rapport au seul paramètre extérieur variable, c'est-à-dire par rapport à toutes les distributions de sources stationnaires et ergodiques d'alphabet fixé :

$$\mathcal{C} = \max_{A}\{I_{AB}\} \tag{1.7}$$

Le théorème fondamental de codage de canal [6, 7, 8] assure qu'il est possible, en utilisant un codage approprié, de transmettre un message à travers un canal bruité avec une qualité de restitution arbitrairement élevée, du moment que l'entropie de la source $H(A)$ est inférieure à la capacité du canal $\mathcal{C}$. De la même manière qu'en électronique où le transfert de puissance est maximum lorsque les impédances de la source et de la charge sont adaptées, en théorie des communications, le transfert d'information est optimal lorsque l'entropie de la source est adaptée à la capacité du canal. Mais si la théorie de Shannon affirme qu'un tel taux de transfert est atteignable, elle ne fournit malheureusement pas de codage explicite pour atteindre un tel niveau. Par la suite, nous considérerons que la distribution de la source est connue et fixée et que le canal de transmission est adapté à la source, c'est-à-dire qu'il n'introduit pas de déformation non-corrigeable au signal. Dans ce cas, le paramètre pertinent pour la transmission est l'information mutuelle I_{AB} effectivement obtenue.

Nous venons de définir les grandeurs permettant de quantifier l'information moyenne d'une variable discrète et l'information transmise entre deux parties. Le cas de la source discrète émettant des symboles (lettres) issus d'un alphabet fini a permis d'introduire simplement une certaine intuition de l'information en tant que grandeur physique. Pour bien comprendre les choix qui ont motivé notre équipe vers des protocoles de communication à base de variables continues, voyons maintenant les avantages spécifiques de telles variables dans le cadre de la théorie classique de l'information.

1.2 Application aux variables continues

1.2.1 Passage aux variables continues

La quantité d'information, ou d'imprévu, associée au choix d'une variable parmi un continuum de valeurs possibles ne peut pas se définir de manière immédiatement analogue au cas discret : dans le cas d'une telle analogie, cette quantité d'information serait infinie vu qu'elle correspondrait à la réalisation d'un événement de probabilité nulle.

Cependant, on peut formellement introduire des quantités appelées *entropies différentielles* et définies à partir des densités de probabilité $\Pr_A$ d'une variable A [6, 7, 8].

$$H_d(A) = -\int Pr_A(a)\, \log_2 Pr_A(a)\, da \tag{1.8}$$

$$H_d(A,B) = -\iint \Pr_{A,B}(a,b)\, \log_2 \Pr_{A,B}(a,b)\, da\, db \tag{1.9}$$

$$H_d(A|B) = -\iint \Pr_{A,B}(a,b)\, \log_2 \Pr_{A|B}(a|b)\, da\, db \tag{1.10}$$

Pour l'information mutuelle moyenne, la généralisation au cas continu se fait sans grande difficulté mathématique. De plus, avec les définitions ci-dessus des entropies différentielles, l'information mutuelle s'exprime par :

$$\begin{aligned} I_{AB} &= H_d(A) - H_d(A|B) \\ &= H_d(B) - H_d(B|A) \\ &= H_d(A) + H_d(B) - H_d(A,B) \end{aligned} \tag{1.11}$$

où une simple substitution des entropies par des entropies différentielles a été effectuée par rapport au cas discret (1.5).

Avec ces définitions, les entropies différentielles possèdent globalement les mêmes propriétés que les entropies des variables discrètes. Ainsi, les formules suivantes sont (toujours) valables :

$$\begin{aligned} H_d(A,B) &= H_d(A) + H_d(B|A) = H_d(B) + H_d(A|B) && (1.12)\\ H_d(A) &\leq H_d(A,B) && (1.13)\\ H_d(A|B) &\leq H_d(A) && (1.14) \end{aligned}$$

Par contre, deux différences essentielles sont à noter quand on passe aux variables continues. La première est que les entropies différentielles sont définies *à une constante additive près*, relativement à un certain choix d'échelle. L'entropie différentielle ne possède donc plus de sens intrinsèque comme mesure de l'imprévisibilité, par contre, la différence de ces entropies (l'information mutuelle) conserve toute sa portée physique. La seconde particularité est qu'alors une entropie différentielle peut tout à fait être négative. Une entropie différentielle nulle ne renseigne en rien sur le caractère certain de la variable associée.

1.2.2 Cas des distributions gaussiennes

Dans le même article qui pose les fondements de la théorie de l'information [6], Claude Shannon a démontré deux résultats majeurs pour le cas des variables continues suivant une distribution de probabilité gaussienne :

1. *A variance fixée, la forme de distribution de probabilité qui maximise l'entropie est une distribution gaussienne.*
2. *L'entropie différentielle d'une variable gaussienne de variance $\langle X^2 \rangle$ est donnée par :*

$$H_d(X) = \frac{1}{2}\log_2\left(\frac{\langle X^2\rangle}{N_0}\right) \qquad (1.15)$$

où N_0 est une constante correspondant au choix d'échelle effectué. Le premier point indique explicitement le type de distribution à choisir expérimentalement comme modulation pour rendre maximal le taux de transfert d'information. Le deuxième point sera un résultat essentiel pour caractériser le taux de transfert d'un canal additif à bruit gaussien.

1.2.3 Canaux additifs gaussiens : théorème de Shannon

Les canaux de transmission les plus importants dans la pratique pour les variables continues sont des canaux où un bruit blanc gaussien N s'additionne au message émis A pour former le signal détecté B. Le bruit est considéré comme statistiquement indépendant du message. De plus, on introduit un facteur de gain G entre l'entrée et la sortie du canal et on considère enfin que le message A suit une distribution gaussienne, de telle sorte que toutes les distributions suivent des lois gaussiennes et maximisent ainsi l'entropie.

$$B = \sqrt{G}\,A + N \qquad (1.16)$$

Comme le bruit N et le message A sont indépendants, l'entropie mutuelle devient alors :

$$H_d(A,B) = H_d(A,N) = H_d(A) + H_d(N) \qquad (1.17)$$

D'après (1.11c), il en résulte que le taux d'information utile échangée s'exprime par la différence de l'entropie du signal détecté et de l'entropie du bruit.

$$I_{AB} = H_d(B) - H_d(N) \qquad (1.18)$$

Le signal et le bruit étant gaussiens, l'information mutuelle s'exprime uniquement en fonction des variances des distributions d'après la formule (1.15) :

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{\langle B^2\rangle}{\langle N^2\rangle}\right) \tag{1.19}$$

A ce niveau, il est utile de faire une analogie entre le canal de communication et un système électronique pour introduire le bruit équivalent ramené en entrée $N_{in} = N/\sqrt{G}$:

$$B = \sqrt{G}\,(A + N_{in}) \tag{1.20}$$

Dans cette notation, l'équation (1.19) se réécrit en ce qui est généralement appelé le *théorème de Shannon* :

$$\boxed{I_{AB} = \frac{1}{2}\log_2\left(1 + \frac{\langle A^2\rangle}{\langle N_{in}^2\rangle}\right)} \tag{1.21}$$

Le rapport des variances de modulation signal et du bruit équivalent en entrée $\langle A^2\rangle/\langle N_{in}^2\rangle$ est fréquemment appelé le *rapport signal à bruit* pour un transfert par canal additif gaussien. Il faut prendre garde au fait que le rapport signal à bruit utilisé ici ne caractérise pas le rapport des signaux physiques mesurés en sortie de canal, mais le rapport de leurs variances. Ceci provient directement du fait que l'entropie d'une variable gaussienne dépend uniquement de sa variance, et non pas de sa moyenne linéaire.

Un exemple numérique de tracé de l'information mutuelle en fonction du gain de la ligne est donné sur la figure 1.4, en considérant un canal additif gaussien. Cet exemple met en évidence l'opportunité majeure de transmettre plusieurs bits pour un seul symbole en exploitant les propriétés des variables continues. Ainsi pour un gain unité et un rapport signal à bruit $\langle A^2\rangle/\langle N_{in}^2\rangle = 15$, le taux de transfert d'information atteint le niveau de 2 bits par symbole échangé.

Autres formulations utiles

On peut par exemple utiliser la variance conditionnelle de B sachant A :

$$V_{B|A} = \langle B^2\rangle - \frac{\langle AB\rangle^2}{\langle A^2\rangle} = \langle N^2\rangle \tag{1.22}$$

D'après (1.19), le théorème de Shannon devient alors :

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{\langle B^2\rangle}{V_{B|A}}\right) \tag{1.23}$$

Pour des variables gaussiennes (éventuellement centrées), il est pratique d'introduire le coefficient de corrélation ρ_{AB} entre les variables A et B.

$$\rho_{AB} = \frac{\langle AB\rangle}{\sqrt{\langle A^2\rangle\langle B^2\rangle}} \tag{1.24}$$

Ce coefficient de corrélation est relié à la variance conditionnelle $V_{B|A}$ par :

$$V_{B|A} = \langle B^2\rangle\,(1 - \rho_{AB}^2) \tag{1.25}$$

Le théorème de Shannon (1.21) s'écrit alors :

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{1}{1-\rho_{AB}^2}\right) \tag{1.26}$$

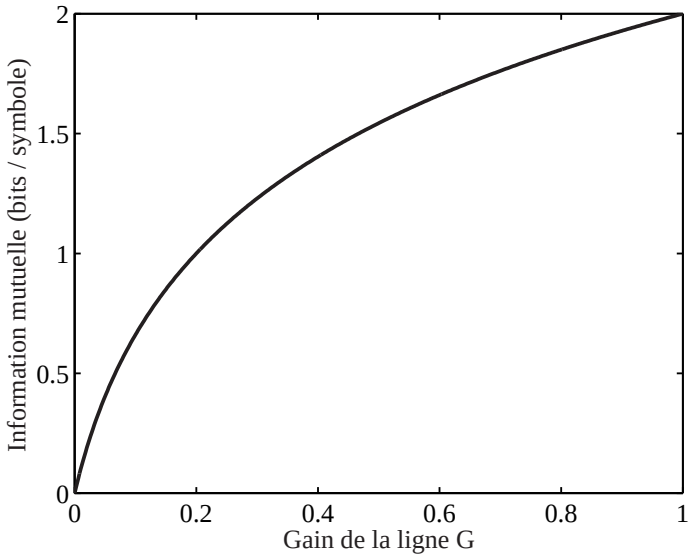

Figure 1.4: *Information mutuelle moyenne en bits par symbole entre la source et le récepteur d'un canal additif en fonction du gain effectif de la ligne G pour une modulation gaussienne de variance* $\langle A^2 \rangle = 15$ *et un bruit additif gaussien de variance constante* $\langle N^2 \rangle = 1$ *(au niveau du récepteur).*

1.3 Extraction pratique d'une information : réconciliation par tranches

1.3.1 Contexte dans le cadre de l'exploitation des variables continues

Si la théorie de l'information énoncée par Shannon apporte d'impressionnants résultats et fixe les limites du possible en terme de communication, elle n'offre cependant pas de méthode pratique pour atteindre de tels taux de codage et de transfert. Quel processus de codage appliquer pour éviter toute redondance à la source ? Comment extraire l'information utile I_{AB} d'un signal bruité ? On ne peut cependant réfuter les apports indéniables de cette théorie de l'information, ne serait-ce que pour les domaines de recherche nouveaux qu'elle a ouverts. Par exemple, l'utilisation des "turbo-codes" [53, 60] apporte une perspective d'atteindre les taux limites fixés par le théorème de Shannon (1.21).

Dans le cas spécifique des variables continues, nous avons vu tout l'intérêt d'utiliser des variables gaussiennes afin de maximiser les taux de communication. Pour de telles variables, la formule de Shannon (1.21) donne alors le taux maximal de transfert. Une question judicieuse est de savoir comment extraire pratiquement cette information à partir des variables corrélées partagées par la source et le destinataire. Ceci soulève d'autres problèmes : comment corriger les erreurs introduites par le bruit du canal ? Comment obtenir toute l'information contenue dans les variables comme l'indique Shannon ?

Pour l'extraction pratique d'information binaire à partir de variables gaussiennes continues, nous avons utilisé dans cette thèse le protocole de "réconciliation par tranches" (*sliced reconciliation*) développé par Gilles Van Assche, Jean Cardinal et Nicolas Cerf [56]. L'invention de ce protocole d'extraction d'information a constitué une percée majeure, en particulier dans le domaine de la cryptographie quantique avec des variables continues, où il fut une condition

préalable nécessaire pour la validation des protocoles pratiques de cryptographie à base d'états cohérents proposés par Frédéric Grosshans et Philippe Grangier [70, 73, 74, 75]. Ce dispositif a été employé en particulier pour notre expérience de cryptographie quantique avec des états cohérents décrite au chapitre 5.

Le principe de ce protocole d'extraction est rapidement décrit ci-dessous. Sa mise en œuvre pratique dans le cadre d'une expérience réelle de cryptographie quantique sera décrite plus spécifiquement dans le chapitre 5, mais surtout dans la thèse de Gilles Van Assche qui a conçu et réalisé la programmation informatique de cette procédure. Néanmoins, dans un soucis de clarté et pour assurer une bonne compréhension de nos protocoles théoriques de cryptographie quantique à base de variables continues (chapitre 4), je souhaite aborder dès maintenant le problème essentiel de l'extraction binaire à partir de variables gaussiennes continues.

1.3.2 Principe de la procédure

Supposons que deux parties, Alice et Bob, aient échangé des données suivant une modulation continue. Pour maximiser le taux de transfert selon Shannon, Alice a choisi d'utiliser une modulation gaussienne. En sortie du canal additif de bruit gaussien, Bob dispose d'une variable continue gaussienne B, corrélée au signal A envoyé par Alice. Deux étapes sont alors nécessaires pour extraire une information utile :

1. Obtenir des bits discrets à partir de données continues.

2. Corriger les erreurs introduites par le bruit du canal.

Ces deux étapes ont été imbriquées dans le protocole de réconciliation par tranches [56] pour extraire une chaîne de bits commune à Alice et Bob.

Le principe de base d'une réconciliation par tranches est qu'Alice convertisse ses données gaussiennes en une chaîne de bits, pendant que Bob fait progressivement de même, tout en échangeant des informations avec Alice pour corriger ses erreurs et en se servant des informations dont il dispose déjà.

Pour extraire une information binaire, la distribution de probabilité gaussienne d'Alice est découpée en 2^N intervalles où N est le nombre de bits à extraire pour chaque symbole. Les bits discrets associés à une valeur particulière A_j de la variable continue sont alors la représentation binaire du numéro de la tranche à laquelle la valeur A_j appartient, ordonnés du bit le moins significatif (LSB) au bit de poids fort (MSB). Par exemple dans la figure 1.5, on associerait à une valeur continue tombant dans le troisième intervalle à partir de la gauche le mot binaire "0 1 0". Cette opération de binarisation est appelée par ses inventeurs "découpage en tranches" [56], la première tranche étant constituée du bit de poids faible alors que la dernière tranche est formée du bit de poids fort. Le nombre d'intervalles à choisir est bien sûr lié au rapport signal à bruit au niveau de Bob et est optimisé numériquement suivant le nombre de bits qu'il est possible d'extraire au maximum selon la formule de Shannon. Il en va également de même pour la position des intervalles de cette binarisation. Typiquement, on choisit généralement d'extraire environ 5 bits par symbole, soit un découpage de la distribution de probabilité en $2^5 = 32$ intervalles.

Du fait du bruit du canal, les bits de la tranche d'Alice diffèrent de ceux de la tranche de Bob. Pour corriger ces erreurs au niveau de chaque chaîne de bits, Alice et Bob utilisent un protocole de réconciliation de chaîne binaire de type *Cascade* [52, 57]. L'innovation majeure vient ici du fait qu'Alice et Bob effectuent cette réconciliation séquentiellement pour chaque tranche ou niveau de binarisation. Pour chaque estimation de la tranche suivante, Bob se sert des informations dont il dispose sur sa variable continue, mais il utilise également toutes les informations issues

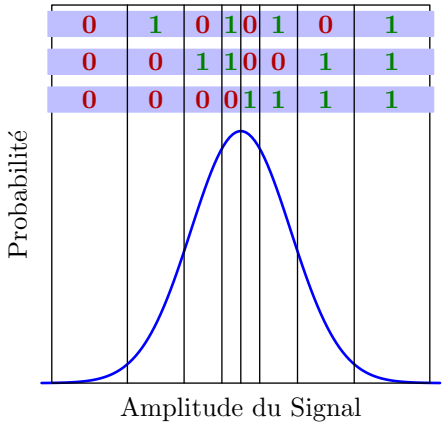

Figure 1.5: *Procédure de discrétisation appliquée au protocole de réconciliation par tranches. Ici la distribution gaussienne a été découpée en 2^3 intervalles. A chaque intervalle est associé un mot représentant en binaire le numéro de l'intervalle. L'ordre des différentes tranches est présenté de haut en bas suivant la succession utilisé par l'algorithme, en partant des bits de poids faible vers les bits les plus significatifs.*

des tranches précédentes. Ainsi, pour construire la n-ième tranche, il utilisera les $n-1$ tranches préalablement corrigées. Ceci lui donne un avantage certain sur sa précision, et minimise les erreurs qu'il pourrait introduire lors du n-ième découpage. Numériquement, il a été montré qu'il est préférable de partir de la chaîne de bits de poids faible (soit un niveau de détail fin) pour aller ensuite vers les tranches de poids forts (soit un niveau de détails plus grossiers) [56].

Cette procédure de correction d'erreur séquentielle confère une excellente efficacité intrinsèque à cet algorithme. Associée à une procédure de correction (réconciliation) réelle, comme *Cascade*, cette méthode permet d'extraire environ 80 à 85% de la limite de Shannon. Par ailleurs, il a été démontré que cet algorithme peut devenir optimal et tendre vers la limite de Shannon lorsque la dimension du découpage par tranches augmente [56]. Enfin, d'autres protocoles de correction binaires nouveaux pourraient améliorer l'efficacité globale de ce dispositif [58].

Il est intéressant de reprendre l'exemple numérique de la figure 1.4 dans le cas d'un rapport signal à bruit de $\langle A^2\rangle/\langle N_{in}^2\rangle = 15$ et d'un découpage de la distribution gaussienne en 5 tranches. Le tableau ci-dessous donne la probabilité d'erreur de Bob en fonction du numéro de la tranche, en allant du bit le moins significatif au bit de poids fort [2].

Tranche	**Taux d'erreur**
1	0,482
2	0,459
3	0,184
4	$8{,}1\ 10^{-3}$
5	$1{,}1\ 10^{-7}$

Pour les deux premières tranches, qui correspondent à un niveau de détail fin, la probabilité d'erreur de Bob est de l'ordre de 50% et les chaînes de bits d'Alice et Bob sont à peu près complètement décorrélées avant correction [3]. Cependant, grâce à la connaissance des tranches

[2] Je remercie Gilles Van Assche de m'avoir fourni les données numériques citées ici.

[3] La correction des tranches de poids faible n'apporte qu'une quantité d'information finale négligeable, compte tenu des forts taux d'erreur. Dans la pratique, ce tranches sont alors simplement annoncées publiquement par

précédentes, Bob peut affiner son découpage des tranches ultérieures, ce qui se traduit par une diminution progressive de son taux d'erreur, alors même que l'information est plus facile à obtenir (bits de poids fort). Le résultat final est la production de 4.60 bits par symbole alors que la correction d'erreur consomme 2.75 bits, soit un taux net final de 1.85 bits réconciliés. Ce dernier chiffre est à comparer au taux maximum de 2 bits extractibles suivant la formule de Shannon pour un rapport signal à bruit de 15, soit une efficacité ici de 92.5%.

1.4 Conclusion

Ce chapitre intervient en quelque sorte comme un préliminaire classique à l'utilisation des variables quantiques continues pour réaliser des protocoles de communication quantique. La théorie de l'information de Shannon met en évidence des propriétés spécifiques des variables continues pour guider nos choix de protocoles quantiques.

- Grâce au protocole de réconciliation par tranche des variables continues, il est possible d'accéder à l'information de Shannon et de transmettre plusieurs bits par symbole.
- Dans le cas d'un canal gaussien, l'utilisation de modulations gaussiennes rend le taux de transfert d'information maximal.
- Le paramètre pertinent pour quantifier un transfert d'information avec des variables continues gaussiennes n'est pas le rapport du signal mesuré au bruit mesuré, mais le rapport des variances de ces signaux.

Enfin, pour échanger des informations, il est absolument nécessaire de résoudre temporellement chaque symbole échangé. Toutes ces constatations nous guident donc naturellement vers la conception de systèmes de communication quantique à base de variables quantiques continues, utilisant des modulations gaussiennes et fonctionnant en régime impulsionnel pour assurer la résolution temporelle. Deux systèmes répondant à ce cahier des charges ont été développés au cours de cette thèse. Le premier est un dispositif de cryptographie quantique à base d'impulsions cohérentes (partie II.), le second est un ensemble de génération d'états quantiques particuliers servant comme ressource de base pour de futurs protocoles de communication quantique (partie III.). Avant d'aborder de tels dispositifs, il est nécessaire de passer au domaine quantique et d'introduire les variables quantiques continues utilisées au cours de cette thèse.

Alice sans une correction qui consommerait plus de bits qu'elle n'en produirait. Ces tranches sont néanmoins utiles pour la suite de l'algorithme de correction séquentielle des tranches de niveau plus élevé, où Bob se sert de l'information des tranches précédentes pour améliorer son estimation du découpage de la tranche en cours.

Chapitre 2

Outils de l'optique quantique avec des variables continues

Sommaire

L'objectif majeur de l'optique quantique actuelle est d'exploiter les particularités quantiques de la lumière pour réaliser des nouvelles tâches de traitement de l'information. En particulier, l'attention de la communauté scientifique s'est portée vers des tâches impossibles à effectuer avec des systèmes basés exclusivement sur la physique classique [1, 2, 3] : téléportation quantique, cryptographie quantique... Dans ce domaine, nous nous intéressons plus particulièrement à l'exploitation des variables quantiques continues plutôt qu'aux variables discrètes. En effet, comme nous l'avons indiqué dans l'introduction ainsi qu'au chapitre précédent, les variables

continues offrent certains avantages sur la variables discrètes, notamment de plus forts débits d'information.

Avant de parler explicitement de communication quantique, ce chapitre introduit brièvement les différents outils apportés par l'optique quantique dans le cadre de la manipulation des variables quantiques continues. Une première section définit les opérateurs quantiques de quadrature qui sont les variables continues utilisées au cours de cette thèse. La section suivante présente différentes méthodes de représentation des états quantiques. Ces techniques seront ensuite appliquées pour décrire quelques états quantiques particulièrement intéressants. Enfin la dernière section traite des opérations de manipulation de base de nos variables continues. La question de la mesure des variables continues fera quant à elle l'objet du prochain chapitre, qui sera entièrement consacré à ce sujet.

Pour l'essentiel, ce chapitre est plus conçu comme un catalogue de définitions et de méthodes que comme une présentation rigoureuse et complète des variables continues. Les résultats ne seront donc pas redémontrés mais offrent plutôt le point de vue naïf d'un opticien utilisateur. Le lecteur intéressé pourra se référer aux nombreux ouvrages de références en optique quantique présentés dans la bibliographie, ma préférence personnelle allant aux références [15, 13, 17].

2.1 Quadratures du champ électromagnétique quantique

2.1.1 Composantes de quadrature d'un champ monomode classique

Pour décrire l'aspect ondulatoire de la lumière, la théorie de l'optique quantique repose partiellement sur le formalisme classique de description d'une radiation lumineuse. Quelques brefs rappels et notations sont énoncés ci-dessous dans le cadre de l'optique ondulatoire classique, notamment en vue d'introduire de façon heuristique la quantification du champ et d'établir des correspondances entre description quantique et formalisme classique.

A grande distance de la source de rayonnement, le champ électrique transverse solution des équations de Maxwell dans le vide peut se décomposer sur la base des ondes planes monochromatiques, où chaque mode $\overrightarrow{E}_{cl,m}$ peut être conçu comme la modélisation dans l'espace $\overrightarrow{r}$ et le temps t d'un faisceau lumineux issu d'une source monomode continue de fréquence ω_m, de vecteur polarisation $\overrightarrow{\varepsilon_m}$ et de direction de propagation $\overrightarrow{k_m}$ [15].

$$\begin{aligned} \overrightarrow{\mathbf{E}}_{\perp,cl}(\overrightarrow{r},t) &= \sum_m \overrightarrow{E}_{cl,m}(\overrightarrow{r},t) \\ &= \sum_m \imath\,\mathcal{E}_m\,\overrightarrow{\varepsilon_m}\left(\alpha_m e^{\imath(\overrightarrow{k_m}\overrightarrow{r}-\omega_m t)} - \alpha_m^* e^{-\imath(\overrightarrow{k_m}\overrightarrow{r}-\omega_m t)}\right) \end{aligned} \tag{2.1}$$

où α_m est un nombre sans unité quantifiant l'amplitude du champ monomode $\overrightarrow{E}_{cl,m}$ et $\mathcal{E}_m$ est homogène à un champ électrique. On introduit ici $\mathcal{E}_m$ de telle sorte qu'un champ défini par $\alpha_m = 1$ et localisé dans un volume V ait une énergie $\hbar\omega_m$, soit $\mathcal{E}_m = \sqrt{\hbar\omega_m/(2\epsilon_0 V)}$ en volts par mètre.

En précisant que l'amplitude complexe généralisée α_m se décompose en $\alpha_m = |\alpha_m|\, e^{\imath\varphi_m}$, chaque composante d'onde plane se met alors sous la forme générale d'un champ sinusoïdal décrit par $|\alpha_m|$ et φ_m [15] :

$$\overrightarrow{E}_{cl,m}(\overrightarrow{r},t) = -2\,\mathcal{E}_m\,\overrightarrow{\varepsilon_m}\,|\alpha_m|\,\sin(\overrightarrow{k_m}\overrightarrow{r} - \omega_m t + \varphi_m) \tag{2.2}$$

Ce champ oscillant peut se représenter dans un plan complexe par un vecteur de Fresnel d'amplitude normalisée $|\alpha_m|$ et d'angle polaire ou phase relative φ_m (voir figure 2.1). Dans une telle représentation, la dépendance temporelle est alors passée sous silence, ce qui revient à définir le vecteur de Fresnel comme figé au sein d'un référentiel tournant à la fréquence optique ω_m.

Au lieu de ses coordonnées polaires $(|\alpha_m|, \varphi_m)$, le champ monomode classique peut aussi être exprimé en fonction de ses coordonnées cartésiennes $(\overline{X}_m, \overline{P}_m)$. Les projections du vecteur de Fresnel sur les axes définissent ainsi les *composantes de quadrature classiques* du champ électrique :

$$\overline{X}_m = 2\sqrt{N_0}\,|\alpha_m|\cos\varphi_m \tag{2.3a}$$

$$\overline{P}_m = 2\sqrt{N_0}\,|\alpha_m|\sin\varphi_m \tag{2.3b}$$

où N_0 est une constante de dimensionnement, fonction du choix des unités. En développant le terme en sinus dans l'équation (2.2), on peut directement exprimer le champ classique en fonction de ses composantes de quadrature :

$$\overrightarrow{E}_{cl,m}(\overrightarrow{r},t) = -\frac{\mathcal{E}_m}{\sqrt{N_0}}\overrightarrow{\varepsilon_m}\left(\overline{X}_m\sin(\overrightarrow{k_m}\overrightarrow{r}-\omega_m t)+\overline{P}_m\cos(\overrightarrow{k_m}\overrightarrow{r}-\omega_m t)\right) \tag{2.4}$$

Un tel mode du champ électromagnétique est donc parfaitement déterminé par la donnée d'un nombre *fini* de paramètres : son amplitude, sa phase relative, sa fréquence optique, sa direction de propagation et sa polarisation. Dans le cas plus réel d'un mode gaussien, il faudrait encore préciser la dépendance spatiale par le diamètre et la position du waist.

Cependant, une telle source de lumière parfaitement constante ne peut pas exister. D'une part, elle serait en contradiction avec les propriétés statistiques d'un faisceau lumineux réel et d'autre part, elle irait à l'encontre de la mécanique quantique. Ce détour par l'optique ondulatoire classique sera néanmoins fructueux, ne serait-ce que pour introduire par analogie les composantes de quadratures quantiques du champ lumineux, qui sont les variables continues étudiées lors de cette thèse.

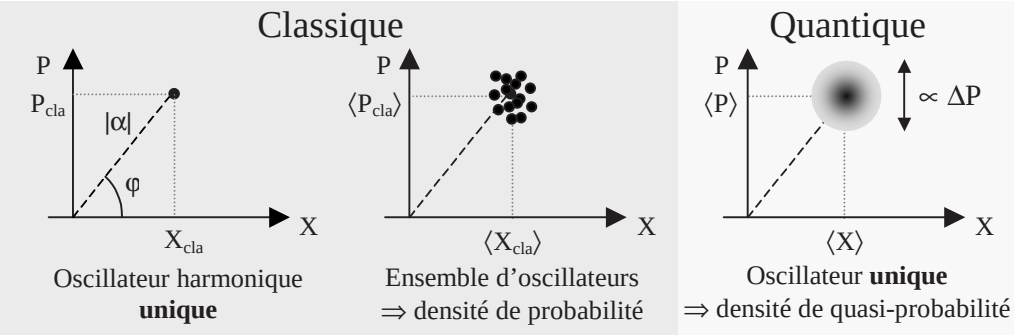

Figure 2.1: *L'état d'un oscillateur classique peut être décrit à tout moment par la donnée d'un point dans l'espace des phases (X, P). Toujours dans le cadre de la physique classique, on peut représenter l'état d'un ensemble de nombreux oscillateurs par une densité de probabilité. En mécanique quantique, aucun état ne peut être totalement spécifié, il faut recourir à une description par une densité de quasi-probabilité associée même à un état quantique unique.*

2.1.2 Quantification du champ et opérateurs quadratures

Champ quantique

Partant des équations de Maxwell dans le vide, la formule (2.1) exprime le champ transverse classique comme une superposition linéaire de différents modes oscillateurs harmoniques $\alpha_m\, e^{-\imath\omega_m t}$ indépendants les uns des autres. Ce résultat est plus qu'un outil mathématique commode, il nous permet de définir la notion de mode du champ électromagnétique et guidera la quantification du champ.

Par analogie formelle avec la quantification d'un oscillateur harmonique matériel, les modes oscillants du champ électromagnétique sont quantifiés en remplaçant les nombres quantiques α_m, α_m^* par des opérateurs *annihilation* $\hat{a}_m$ et *création de photon* $\hat{a}_m^\dagger$ [12, 9, 15, 14] :

$$\begin{array}{rcl} \alpha_m & \rightarrow & \hat{a}_m \\ \alpha_m^* & \rightarrow & \hat{a}_m^\dagger \end{array} \tag{2.5}$$

Cette quantification est complétée en postulant les relations de commutation :

$$\begin{array}{rcl} [\hat{a}_m, \hat{a}_n^\dagger] & = & \delta_{m,n} \\ [\hat{a}_m, \hat{a}_n] & = & [\hat{a}_m^\dagger, \hat{a}_n^\dagger] = 0 \end{array} \tag{2.6}$$

et en associant à la quantité $\alpha_m\alpha_m^*$ l'opérateur symétrisé $(\hat{a}_m^\dagger\hat{a}_m + \hat{a}_m\hat{a}_m^\dagger)/2$.

Opérateurs composantes de quadrature

De façon similaire à (2.1), l'*opérateur* champ électrique monomode s'écrit alors :

$$\hat{E}_m(\overrightarrow{r}, t) = \imath\, \mathcal{E}_m\, \overrightarrow{\varepsilon_m} \left(\hat{a}_m e^{\imath(\overrightarrow{k_m}\overrightarrow{r} - \omega_m t)} - \hat{a}_m^\dagger e^{-\imath(\overrightarrow{k_m}\overrightarrow{r} - \omega_m t)} \right) \tag{2.7}$$

Cette expression se réécrit suivant la forme (2.4) pour faire apparaître les opérateurs composantes de quadrature introduits par analogie avec les composantes de quadrature d'un champ classique :

$$\hat{E}_m(\overrightarrow{r}, t) = -\frac{\mathcal{E}_m}{\sqrt{N_0}}\, \overrightarrow{\varepsilon_m} \left(\hat{X}_m \sin(\overrightarrow{k_m}\overrightarrow{r} - \omega_m t) + \hat{P}_m \cos(\overrightarrow{k_m}\overrightarrow{r} - \omega_m t) \right) \tag{2.8}$$

En prenant comme définitions pour les *opérateurs composantes de quadrature* [1] :

$$\boxed{\begin{array}{c} \hat{X} = \sqrt{N_0}\, (\, \hat{a} + \hat{a}^\dagger \,) \\ \hat{P} = \sqrt{N_0}\, \dfrac{(\, \hat{a} - \hat{a}^\dagger \,)}{\imath} \end{array}} \tag{2.9}$$

où N_0 est une constante réelle positive dépendant des variables considérées et du système d'unités choisi. Les observables associées à ces opérateurs peuvent prendre une infinité de valeurs possibles réparties dans un continuum, on parle alors de *variables continues*.

Il est également pratique de donner une expression des opérateurs $\hat{a}$ et $\hat{a}^\dagger$ à partir des composantes de quadrature dans ce système de notations.

$$\hat{a} = \frac{\hat{X} + \imath\hat{P}}{2\sqrt{N_0}} \qquad\qquad \hat{a}^\dagger = \frac{\hat{X} - \imath\hat{P}}{2\sqrt{N_0}} \tag{2.10}$$

[1] Afin d'alléger les notations en l'absence d'ambiguïté, la notation $\hat{}$ pour désigner les opérateurs ne sera plus mentionnée dans les autres chapitres de ce manuscrit.

Compte tenu de la relation de commutation imposée $[\hat{a}, \hat{a}^\dagger] = 1$, les opérateurs composantes de quadrature ne commutent pas et vérifient la relation :

$$\boxed{[\hat{X}, \hat{P}] = 2\imath N_0} \tag{2.11}$$

Du fait de cette non-commutation, il n'est pas possible selon le principe d'Heisenberg de connaître simultanément et avec une précision absolue les observables conjuguées X et P associées à un même état quantique. Toutes les caractéristiques d'un état quantique ne peuvent être spécifiées simultanément. La relation d'incertitude d'Heisenberg formalise cette affirmation en l'inégalité :

$$\boxed{\Delta X \, \Delta P \geq N_0} \tag{2.12}$$

où $\Delta\cdot$ désigne l'écart-type de la mesure associée à l'observable. En particulier pour un état cohérent, les variances associées à X et P sont égales et valent N_0. Pour cette raison, on désigne souvent N_0 par le *niveau de bruit quantique standard* (appelé également selon le contexte bruit de photon, bruit de grenaille, shot noise…).

Le choix de la valeur de N_0 est fonction de la convenance des différents auteurs et varie couramment d'une référence à l'autre. Pour les expérimentateurs, le bruit quantique N_0 sert de référence pour les mesures, d'où la convention $N_0 = 1$ fréquemment posée. Néanmoins ce choix qui impose alors $\hbar = 2$ ne recueille généralement pas les suffrages des théoriciens qui lui préfèrent $\hbar = 1$, soit $N_0 = 1/2$… Ne voulant pas prendre parti dans ce débat, et conformément à la notation introduite dans la thèse de Frédéric Grosshans [71], nous conserverons la notation explicite N_0 pour éviter toute confusion.

Remarques :

- Du fait de l'analogie entre un oscillateur mécanique et un mode du champ électromagnétique, les quadratures X et P sont souvent désignées comme la position et l'impulsion d'un oscillateur électromagnétique. Bien sûr, il ne s'agit que d'une analogie : les composantes de quadrature n'ont rien à voir avec la "position" ou "l'impulsion" d'un photon.

- L'hamiltonien de l'oscillateur harmonique $\hat{H}$ s'écrit alors sous la forme suivante et fait apparaître l'opérateur nombre de photons $\hat{N} = \hat{a}^\dagger \hat{a}$ [9].

$$\hat{H} = \frac{\hbar\omega}{4N_0}\left(\hat{X}^2 + \hat{P}^2\right) = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2}) \tag{2.13}$$

- En applicant un déphasage $\hat{a} \rightarrow \hat{a}e^{-\imath\theta}$, on peut définir des opérateurs composantes de quadratures généralisées :

$$\begin{aligned} \hat{X}_\theta &= \hat{X}\cos\theta + \hat{P}\sin\theta \\ \hat{P}_\theta &= -\hat{X}\sin\theta + \hat{P}\cos\theta \end{aligned} \tag{2.14}$$

  Les nouveaux opérateurs $(\hat{X}_\theta, \hat{P}_\theta)$ vérifient la même relation de commutation que $(\hat{X}, \hat{P})$ et possèdent donc les mêmes propriétés quantiques.

- De la même manière que l'on définissait les composantes de quadratures classiques indépendamment du temps dans un repère tournant à la fréquence optique, les opérateurs quadratures quantiques se définissent dans un espace des phases dont les axes tournent à cette même fréquence. On omettra donc de préciser la dépendance temporelle en $\omega_m t$ pour employer un choix d'observables "fixes" définies à partir d'une référence externe de phase (oscillateur local) ou par un choix adéquat de l'origine des temps.

Autres variables continues

De nombreuses autres caractéristiques d'un mode du champ électromagnétique varient de façon continue et pourraient servir de variables continues pour les procédures de communication quantique : phase relative, polarisation, temps d'arrivée d'une impulsion... Généralement, il s'agit plutôt de "fausses" variables continues : les quantités citées codent dans un espace de dimension finie, ce qui en fait dès lors des variables discrètes. Pour l'essentiel, elles sont utilisées dans des protocoles mettant en œuvre des photons uniques ou des impulsions très atténuées, se limitant à un nombre restreint de réalisations possibles (fréquemment au nombre de 4 dans des protocoles de cryptographie quantique de type BB84).

Il faut cependant citer l'exception de la polarisation d'un faisceau brillant, où les composantes du vecteur de Stokes peuvent définir un "vrai" ensemble de variables continues. Dans le cas d'une composante intense fortement polarisée, les opérateurs de Stokes suivent une relation de commutation équivalente à (2.11). Des dispositifs exploitant ces variables continues en polarisation sont actuellement en cours de développement parallèlement à l'utilisation des quadratures du champ lumineux, et promettent des applications fructueuses. On peut citer pour référence les travaux des groupes de Gerd Leuchs [148, 199], Elisabeth Giacobino [200, 201], Ping Koy Lam [198] et Eugene Polzik [197].

2.1.3 Modes spatio-temporels

Si nous souhaitons décrire des impulsions lumineuses de durée finie se propageant dans le vide, la description monochromatique ci-dessus ne présente plus une approximation satisfaisante. En effet, une localisation dans l'espace des temps se traduit directement par une relation de transformée de Fourier en une certaine étendue dans l'espace des fréquences. Nous devrons alors considérer des modes spatio-temporels définissant une impulsion, en quelque sorte délocalisés dans l'espace fréquentiel, mais localisés dans l'espace spatial et temporel [34, 36].

L'opérateur $\hat{E}(t)$ définissant le champ signal en fonction du temps est la transformée de Fourier de l'opérateur $\hat{a}^\dagger_\omega$ [37] :

$$\hat{E}(t) = \int \hat{a}^\dagger_\omega \, e^{\imath\omega t} \, d\omega \tag{2.15}$$

Pour décrire la création d'un photon dans le mode de l'impulsion, il est alors naturel de considérer l'opérateur défini par [37, 36, 34] :

$$\hat{A}^\dagger = \int f(t) \, \hat{E}^\dagger(t) \, dt = \int \widetilde{f}(\omega) \, \hat{a}^\dagger_\omega \, d\omega \tag{2.16}$$

avec f une fonction normée telle que $\int |f(\omega)|^2 d\omega = 1$ ($\widetilde{f}$ désigne la transformée de Fourier de f). La définition la plus utile pour f est de la prendre égale à l'enveloppe temporelle du paquet d'onde, normalisée par un facteur d'échelle. Dans ce cas, $\widetilde{f}$ désigne l'enveloppe spectrale de l'impulsion.

Le nouvel opérateur de création $\hat{A}^\dagger$ obéit alors à la même relation de commutation et possède les mêmes propriétés qu'un opérateur monomode continu $\hat{a}^\dagger$:

$$[\hat{A}, \hat{A}^\dagger] = 1 \tag{2.17}$$

Suivant la démarche de quantification du champ monomode continu, il est intéressant de considérer les états propres $|N\rangle$ de l'opérateur nombre de photons dans l'impulsion $\hat{A}^\dagger\hat{A}$. Ces

états vérifient les relations habituelles de création et d'annihilation pour des modes continus et décrivent une base orthonormale complète pour la décomposition de tous les paquets d'ondes :

$$\begin{aligned} \hat{A}^\dagger |N\rangle &= \sqrt{N+1}\,|N+1\rangle \\ \hat{A}\,|N\rangle &= \sqrt{N}\,|N-1\rangle \end{aligned} \tag{2.18}$$

Les opérateurs $\hat{A}, \hat{A}^\dagger$ peuvent donc être considérés comme des équivalents parfaits aux opérateurs monomodes continus $\hat{a}, \hat{a}^\dagger$ dans le cadre de la description d'un mode "impulsion lumineuse". En particulier, on peut reprendre la démarche présentée dans la section précédente et définir des opérateurs composantes de quadrature de façon similaire à (2.9).

Dans la suite de cette thèse, nous travaillerons avec des impulsions lumineuses quasiment limitées par Fourier. Afin de se conformer aux notations communément utilisées dans la littérature et de permettre une lecture plus intuitive, les opérateurs création et annihilation de photon dans un mode impulsionnel seront notés par $\hat{a}, \hat{a}^\dagger$, étant entendu que les modes considérés sont des modes impulsionnels définis par (2.16) et non plus des modes continus.

Cette partie a permis de définir la notion d'opérateurs composantes de quadrature d'un mode lumineux au sens large. Ces quadratures nous serviront dans la suite de cette thèse comme variables continues pour le développement de protocoles de communication quantique. Un deuxième ingrédient fondamental pour ces protocoles est la manipulation d'états quantiques particuliers, qui fera l'objet du reste de ce chapitre.

2.2 Représentation des états quantiques

2.2.1 Matrice densité

Le premier postulat de la mécanique quantique [9] est de décrire complètement l'état d'un système physique par un vecteur d'état $|\psi\rangle$ appartenant à un espace de Hilbert. Un système parfaitement préparé et qui peut se représenter par un vecteur $|\psi\rangle$ unique dans l'espace de Hilbert sera appelé un état pur. Afin de décrire une classe plus large d'objets quantiques, il faut prendre en compte des imperfections lors de la génération des états quantiques qui peuvent préparer une superposition statistique de différents états purs $|\psi_n\rangle$ avec des probabilités associées p_n. Un tel système ne peut plus être défini par un seul état pur, il faut recourir à la description en terme d'opérateur densité $\hat{\rho}$ [17, 18] :

$$\boxed{\hat{\rho} = \sum_n p_n\,|\psi_n\rangle\langle\psi_n|} \tag{2.19}$$

où les vecteurs d'états purs et les probabilités sont normalisées de telle sorte que $\mathrm{Tr}(\hat{\rho}) = 1$. La représentation de $\hat{\rho}$ dans une base donnée est appelée *matrice densité*. Pour des états impurs, cette représentation n'est cependant pas unique et dépend de la base choisie.

La matrice densité permet de prédire la valeur moyenne de la mesure de n'importe quel observable $\hat{O}$ appliquée à cet état quantique :

$$\langle\hat{O}\rangle = \mathrm{Tr}(\,\hat{\rho}\,\hat{O}\,) \tag{2.20}$$

La matrice densité contient donc toutes les informations concernant le système étudié et constitue la description la plus générale d'un état quantique. En ce sens, la connaissance d'un état quantique est ici identifiée à la capacité de prédire toute les informations statistiques de toutes

les quantités physiques observables [17]. En particulier, on peut quantifier le degré de mélange de l'état considéré en plusieurs états purs. On définit pour cela la notion de pureté $\mathcal{P}$ de l'état par :

$$\mathcal{P} = \mathrm{Tr}(\hat{\rho}^2) \tag{2.21}$$

2.2.2 Fonction de Wigner

Un système quantique ne pouvant être décrit de façon parfaitement déterministe, il est tentant de modéliser l'état quantique par une sorte de distribution de probabilité dans l'espace des phases, voisine de celle dessinée sur la figure 2.1. Une représentation très utilisée est la fonction de Wigner, introduite pour la première fois par E. Wigner dans son article de 1932 [24]. Avec les notations N_0, cette fonction se définit à partir de l'opérateur densité par [71] :

$$W(x,p) = \frac{1}{4\pi N_0} \int \langle x - \frac{q}{2} | \, \hat{\rho} \, | x + \frac{q}{2} \rangle \, e^{\imath \frac{pq}{2N_0}} \, dq \tag{2.22}$$

où $|x\rangle$ désigne un état propre de l'opérateur quadrature $\hat{X}$.

La propriété la plus essentielle de la fonction de Wigner ainsi définie est qu'elle se comporte *comme* une densité de probabilité conjointe pour des mesures de X et P, sans jamais mentionner de mesure simultanée des quadratures. Par exemple, la distribution de probabilité $\Pr(x)$ associée à l'observable X correspond à la distribution marginale en X de la fonction de Wigner, comme on pouvait l'espérer pour une distribution de probabilité classique [25, 17, 18] :

$$\Pr(x) = \int_{-\infty}^{+\infty} W(x,p) dp \tag{2.23}$$

De façon plus générale pour n'importe quelle composante de quadrature définie par une rotation d'angle θ :

$$\boxed{\Pr(x,\theta) = \langle X | \hat{U}_\theta \, \hat{\rho} \, \hat{U}_\theta^\dagger | X \rangle = \int_{-\infty}^{+\infty} W(x\cos\theta - p\sin\theta, x\sin\theta + p\cos\theta) dp} \tag{2.24}$$

où $\hat{U}_\theta = \exp(-\imath\theta \hat{a}^\dagger \hat{a})$ est l'opérateur rotation d'angle θ dans l'espace des phases.

Si la fonction de Wigner présente de nombreuses similitudes avec une distribution classique de probabilités, une différence importante induite par la mécanique quantique est d'autoriser des valeurs négatives pour certains états quantiques. Cette négativité peut se concevoir comme une conséquence du fait que la probabilité de transition entre deux états orthogonaux est nulle, ce qui implique que le recouvrement des deux fonctions de Wigner correspondantes doit s'annuler. Or ce dernier point n'est possible que si une des fonctions prend des valeurs négatives. La négativité de la fonction de Wigner constitue donc une signature de l'aspect spécifiquement quantique d'un état. Des états présentant des fonctions de Wigner prenant des valeurs négatives sont par exemple le photon unique (présenté à la section suivante), ou le vide comprimé conditionné (qui fera l'objet d'une étude théorique et expérimentale lors du chapitre 9). Pour la distinguer d'une distribution de probabilité classique, on qualifie alors la fonction de Wigner de distribution de *quasi*-probabilité.

Du fait de sa relation (2.22) avec la matrice densité, la fonction de Wigner contient toutes les informations concernant un état quantique. De même que l'opérateur densité (2.20), elle peut être utilisée pour calculer la valeur moyenne d'une observable quelconque [17, 18] :

$$\langle \hat{O} \rangle = 4\pi N_0 \iint W(x,p) \, W_{\hat{O}}(x,p) \, dx \, dp \tag{2.25}$$

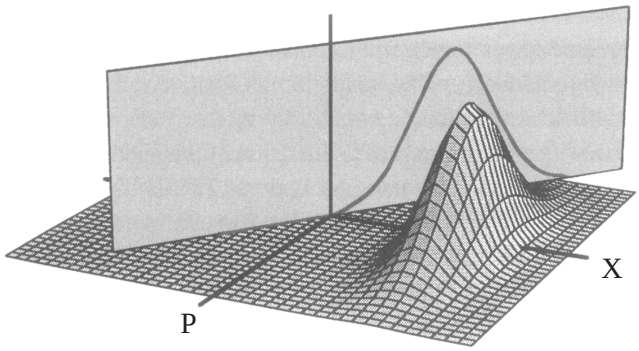

Figure 2.2: *Principe de la tomographie quantique, d'après la référence [17].*

où $W_{\hat{O}}(x,p)$ est la "fonction de Wigner" associée à l'opérateur $\hat{O}$ en remplaçant $\hat{\rho}$ par $\hat{O}$ dans (2.22). Tout résultat d'une mesure sur le système peut ainsi être considéré comme un filtrage adéquat de la fonction de Wigner. « Tout ce que nous pouvons voir, ce sont les ombres des états quantiques, dans un sens très proche de la fameuse parabole de la caverne de Platon » écrit Ulf Leonhardt dans son excellent ouvrage [17].

Si nous ne pouvons voir que les ombres des états quantiques, il devrait cependant être possible de reconstruire un modèle de l'état à partir de la connaissance de plusieurs ombres, enregistrées sous différents points de vue. Cette démarche repose sur une analogie avec la technique de tomographie médicale, qui dresse une cartographie tridimensionnelle d'un organe à partir de mesures d'absorption de rayons X pour différents angles de visée. Dans le domaine de l'optique quantique, la méthode de tomographie est transposée pour reconstruire la fonction de Wigner de l'état à partir des différentes projections qui sont les distributions de probabilité pour des composantes de quadratures quantiques, mesurées avec un système de détection homodyne. Pour accéder mathématiquement à la fonction de Wigner à partir des distributions de probabilités $\Pr(x,\theta)$, il suffit en principe d'inverser la relation (2.24). Cette opération est connue sous le nom de transformée de Radon inverse [17, 29] et fera l'objet d'une étude spécifique lors de la caractérisation des états comprimés présentée au chapitre 7. Il existe également d'autres méthodes numériques pour la tomographie quantique. On peut citer pour référence les méthodes de "quantum state sampling" [17] et de "maximum likelihood" [32].

Enfin, il est possible de définir de nombreuses autres distributions de quasi-probabilités pour représenter l'état quantique. Parmi elles, on peut citer la fonction P ou fonction de Glauber-Sudarshan et la fonction Q ou fonction de Husimi [18, 17]. La fonction P correspond à l'ordre normal $(\hat{a}^\dagger\,\hat{a})$ des opérateurs création et annihilation et peut présenter des points singuliers pour des états non-classiques. Inversement, la fonction Q correspond à l'ordre anti-normal des opérateurs et varie faiblement suivant l'état quantique. Enfin, la fonction de Wigner correspond à un arrangement symétrique des opérateurs. Cette dernière peut prendre des valeurs négatives, mais ne présente pas de singularités, ce qui fait généralement préférer la fonction de Wigner comme représentation de l'état.

2.2.3 Matrice de covariance des états gaussiens

Les états gaussiens, définis par le fait que leur fonction de Wigner associée est gaussienne, forment une classe importante des états de l'espace de Hilbert. D'une part, ce sont les états les plus simples à produire expérimentalement (le vide est gaussien) et d'autre part, leurs fonctions

de Wigner sont en tous points définies positives et on peut alors pousser plus loin l'analogie avec une vraie distribution de probabilité pour exploiter tous les théorèmes statistiques.

Partant du résultat de statistique classique qu'une distribution gaussienne est parfaitement connue par ses moments d'ordre un (sa moyenne) et d'ordre deux (sa variance), un état quantique gaussien quelconque est parfaitement connu par la donnée des valeurs moyennes et des variances des différentes composantes de quadrature de ses modes. Pour un état à n modes, on définit par commodité le vecteur $r = (X_1, P_1, X_2, P_2, \ldots, X_n, P_n)$. L'état gaussien est alors parfaitement déterminé par le vecteur des valeurs moyennes $(\langle r_i \rangle)_{i=1,2n}$ et par la *matrice de covariance* γ [13, 123] :

$$\gamma_{i,j} = \frac{1}{2N_0} \left(\langle \delta r_i \delta r_j \rangle + \langle \delta r_j \delta r_i \rangle \right) \tag{2.26}$$

avec $\delta r_i = r_i - \langle r_i \rangle$. Dans le cas particulier d'un état monomode de valeur moyenne nulle, la matrice de covariance s'écrit explicitement :

$$\gamma = \frac{1}{N_0} \begin{pmatrix} \langle X^2 \rangle & \frac{1}{2}\langle XP + PX \rangle \\ \frac{1}{2}\langle XP + PX \rangle & \langle P^2 \rangle \end{pmatrix} \tag{2.27}$$

La donnée de cette matrice permet de connaître différentes grandeurs physiques pertinentes. La réduction maximale de bruit quantique (*squeezing*), i.e. la plus faible variance en quadrature mesurable V_{min} est déterminée par la plus petite valeur propre de la matrice de covariance, ce qui s'exprime en fonction de la trace et du déterminant de γ par [123] :

$$V_{min} = \frac{N_0}{2} \left[\mathrm{Tr}(\gamma) - \sqrt{\mathrm{Tr}^2(\gamma) - 4\det(\gamma)} \right] \tag{2.28}$$

Par ailleurs, la pureté $\mathcal{P} = \mathrm{Tr}(\hat{\rho}^2)$ pour un mélange statistique vaut :

$$\mathcal{P} = \frac{1}{\sqrt{\det(\gamma)}} \tag{2.29}$$

Enfin, 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 [134]. Dans le cas d'un système à deux modes dont les quadratures sont de valeurs moyennes nulles, la matrice de covariance devient alors :

$$\gamma = \frac{1}{N_0} \begin{pmatrix} \langle {X_1}^2 \rangle & 0 & \frac{1}{2}\langle X_1X_2 + X_2X_1 \rangle & 0 \\ 0 & \langle {P_1}^2 \rangle & 0 & \frac{1}{2}\langle P_1P_2 + P_2P_1 \rangle \\ \frac{1}{2}\langle X_1X_2 + X_2X_1 \rangle & 0 & \langle {X_2}^2 \rangle & 0 \\ 0 & \frac{1}{2}\langle P_1P_2 + P_2P_1 \rangle & 0 & \langle {P_2}^2 \rangle \end{pmatrix} \tag{2.30}$$

La détermination expérimentale de la matrice de covariance d'un vide comprimé avec et sans mesures homodynes fera l'objet du chapitre 8. L'étude d'un faisceau intriqué à deux modes sera présentée au chapitre 10. Afin de donner une vision plus intuitive des représentations des états quantiques, la partie suivante se concentre sur les propriétés de quelques états quantiques particuliers.

2.3 Zoologie quantique : exemples d'états particuliers

Dans cette section, nous rappelons brièvement les définitions et propriétés de différents états quantiques utiles pour les applications en communication quantique. Conformément à nos notations précédentes et au travail de Frédéric Grosshans [71], les formules ci-dessous sont présentées dans la notation normalisée de N_0 pour la variance du bruit de photon.

Le premier de ces états est l'état de quadrature $|x\rangle$, définit comme l'état propre de l'opérateur $\hat{X}$ avec la valeur propre x. L'ensemble de ces états forme une base orthogonale complète de l'espace de Hilbert. Néanmoins, comme ces états ne sont visiblement pas normalisables, ils n'ont pas de réalité physique propre et apparaissent davantage comme une commodité mathématique pour définir la fonction d'onde d'un état $\psi(x) = \langle x|\psi\rangle$. A l'opposé, la fonction d'onde $\psi(x)$ possède bien une réalité physique : son module carré représente la distribution de probabilité en x de l'état, qui est mesurée avec une détection homodyne.

2.3.1 Etat fondamental du champ : vide

L'état fondamental $|0\rangle$ de l'oscillateur harmonique est défini par l'annulation de l'opérateur annihilation :

$$\hat{a}|0\rangle = 0 \tag{2.31}$$

Cette équation implique que le nombre moyen de photons dans cet état est nul, $\langle\hat{N}\rangle = 0$. Pour cette raison, l'état $|0\rangle$ est appelé l'état *vide*.

L'énergie moyenne de l'oscillateur harmonique définie par l'hamiltonien (2.13) est alors minimale, d'où l'appellation d'état fondamental du champ. Cette énergie vaut alors :

$$\langle 0|\hat{H}|0\rangle = \frac{\hbar\omega}{2} \tag{2.32}$$

Dans ce système de notation, l'énergie d'un mode vide n'est pas nulle et vaut l'énergie d'un demi-photon ! Ce résultat est à relier au fait que si la valeur moyenne du champ est nulle, le champ présente néanmoins des fluctuations statistiques non nulles, conformément au principe d'Heisenberg. Si on considère l'ensemble des modes vides de l'espace, l'énergie contenue dans le vide diverge vers l'infini, ce qui pose le problème critique de la normalisation de la théorie quantique des champs. Cependant, nos mesures expérimentales de l'énergie électromagnétique ne permettent d'accéder qu'à une différence d'énergie à partir de l'énergie du vide. La valeur du niveau de référence n'aura donc pas d'influence dans nos expériences.

Plutôt que de considérer le mode vide sous ses aspects énergétiques, on peut s'intéresser aux moments statistiques de son champ électromagnétique :

$$\langle X\rangle = 0 \tag{2.33}$$

$$\Delta X^2 = \langle X^2\rangle = N_0 \neq 0 \tag{2.34}$$

Comme on pouvait s'y attendre, la moyenne du champ électrique dans le vide est nulle. Par contre, même dans le vide, les composantes de quadratures fluctuent avec une variance N_0 non nulle. Ces fluctuations sont des aspects spécifiquement quantiques du champ et sont absolument nécessaires à la théorie quantique, sans quoi la relation fondamentale d'incertitude de Heisenberg serait violée. On peut d'ailleurs noter que pour l'état vide, les variances sont symétriques et minimales au sens de la relation d'Heisenberg : $\Delta X^2 = \Delta P^2 = N_0$.

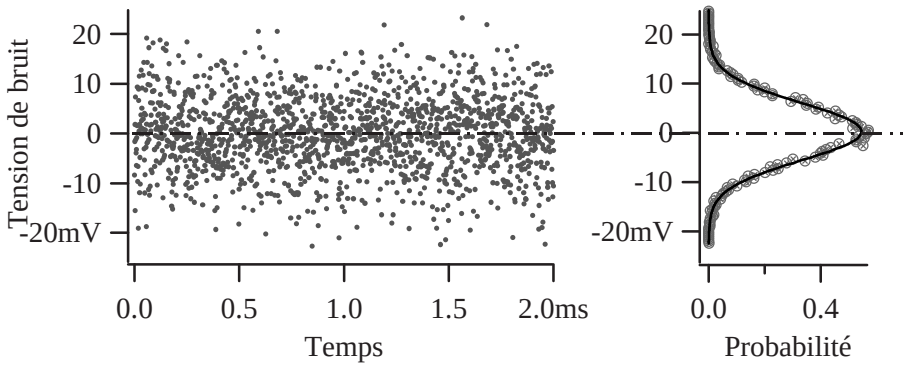

Figure 2.3: *Mesure expérimentale d'une quadrature du vide avec une détection homodyne.*

Une équation différentielle vérifiée par la fonction d'onde du vide s'obtient en réécrivant la formule (2.31) avec (2.10) et $\hat{P} = \imath \frac{\partial}{\partial x}$ [9]. La fonction d'onde en X du vide s'écrit alors :

$$\psi_0(x) = \frac{1}{(2\pi N_0)^{\frac{1}{4}}} e^{-\frac{x^2}{4N_0}} \tag{2.35}$$

Ce qui permet de calculer la fonction de Wigner associée [18, 17] :

$$W_0(x,p) = \frac{1}{2\pi N_0} e^{-\frac{x^2+p^2}{2N_0}} \tag{2.36}$$

On remarquera que ces fonctions sont des gaussiennes. L'état vide est un exemple fondamental d'état gaussien.

2.3.2 Etats nombres : base de Fock

Les états nombres ou états de Fock $|n\rangle$ sont les états pour lesquels le nombre de photons dans le mode est parfaitement défini [13, 15] :

$$\hat{a}^\dagger \hat{a} |n\rangle = n|n\rangle \tag{2.37}$$

Cette définition en tant qu'états propres de l'opérateur nombre de photons impose alors des relations décrites par (2.18) où l'opérateur $\hat{a}^\dagger$ intervient pour la création d'un photon. On peut alors définir n'importe quel état $|n\rangle$ comme une excitation obtenue à partir du vide :

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}} |0\rangle \tag{2.38}$$

De cette définition découle alors l'orthonormalité des états de Fock et le fait qu'ils forment une base complète de l'espace de Hilbert. Cette propriété constitue l'intérêt essentiel des états de Fock pour représenter n'importe quel autre état quantique. En effet, ces états sont difficiles à produire expérimentalement au-delà de $n = 2$ et apportent donc plutôt une commodité de représentation et de calcul.

L'expression de la fonction d'onde de l'état de Fock $|n\rangle$ est donnée par l'expression [18, 17] :

$$\psi_n(x,\theta) = \frac{H_n\left(\frac{x}{\sqrt{2N_0}}\right)}{(2\pi N_0)^{\frac{1}{4}}\sqrt{2^n n!}}\ e^{-\frac{x^2}{4N_0}}\ e^{-\imath n\theta} \tag{2.39}$$

où H_n désigne le n-ième polynôme de Hermite défini par :

$$H_0(x) = 1 \ ; \ H_1(x) = 2x \ ; \ H_2(x) = 4x^2 - 2 \ ; \ \frac{dH_n}{dx} = 2n\, H_{n-1}(x) \tag{2.40}$$

La fonction de Wigner associée à l'état $|n\rangle$ s'écrit [18, 71] :

$$W_n(x,p) = \frac{(-1)^n}{2\pi N_0} e^{-\frac{x^2+p^2}{2N_0}} L_n\left(\frac{x^2+p^2}{N_0}\right) \tag{2.41}$$

où L_n désigne le n-ième polynôme de Laguerre défini par :

$$L_n(x) = \sum_{k=0}^{n} C_n^k \frac{(-x)^k}{k!} \tag{2.42}$$

Cette expression montre que pour n impair, la fonction de Wigner W_n est négative à l'origine, ce qui est une signature flagrante de l'aspect spécifiquement quantique des états de Fock.

2.3.3 Etats cohérents dits quasi-classiques

Afin de modéliser un champ monomode dépourvu de bruit technique, on cherche un état quantique dont la valeur du champ en amplitude et phase est définie au mieux compte tenu de la relation d'Heisenberg. Cet état servira alors pour modéliser intuitivement le champ issu d'un laser monomode opérant largement au-dessus du seuil. L'expression du champ électromagnétique quantifié (2.7) conduit à définir cet état quasi-classique $|\alpha\rangle$ comme la valeur propre de l'opérateur $\hat{a}$.

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{2.43}$$

Cette définition permet immédiatement de calculer les valeurs moyennes et les variances des composantes de quadratures :

$$\langle X\rangle = 2\sqrt{N_0}\, Re(\alpha) \tag{2.44}$$
$$\langle P\rangle = 2\sqrt{N_0}\, Im(\alpha) \tag{2.45}$$
$$\Delta X^2 = \Delta P^2 = N_0 \ \ (= constante) \tag{2.46}$$

Ce qui justifie a posteriori la définition (2.43) : l'état cohérent $|\alpha\rangle$ possède des fluctuations en quadratures minimales indépendantes de l'amplitude et est centré sur la valeur α attendue pour un champ classique. En particulier, l'état vide $|0\rangle$ est aussi un état cohérent. Cette similitude peut être poussée plus loin en démontrant que tout état cohérent est un état vide déplacé dans l'espace des phases [13, 15].

En se servant des états de Fock comme base de l'espace de Hilbert, un état cohérent peut se décomposer selon [13, 15] :

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.47}$$

Cette équation montre en particulier que le nombre de photon d'un état cohérent suit une distribution de Poisson de moyenne $|\alpha|^2$ et d'écart-type $|\alpha|$. On retrouve alors la célèbre formule de Schottky du bruit de photon ou *shot noise* : l'écart-type du bruit de détection est proportionnel à la racine carrée du nombre moyen de photons.

Compte tenu de la relation de déplacement entre un état cohérent et le vide, on peut déduire la fonction d'onde d'un état cohérent $|\alpha\rangle$ [18, 17] :

$$\psi_\alpha(x) = \frac{1}{(2\pi N_0)^{\frac{1}{4}}} e^{-\frac{(x-\langle x\rangle)^2}{4N_0}} e^{+\imath\frac{\langle P\rangle p}{2N_0} - \imath\frac{\langle X\rangle\langle P\rangle}{4N_0}} \tag{2.48}$$

A un terme de phase près, la fonction d'onde correspond à celle d'un vide déplacé. La densité de probabilité associée est alors exactement celle d'un état vide centré sur les valeurs moyennes des quadratures. Cette relation permet d'exprimer la fonction de Wigner associée de façon très intuitive :

$$W_\alpha(x,p) = W_0(x - \langle X\rangle, p - \langle P\rangle) \tag{2.49}$$

Les états cohérents sont donc eux aussi des états gaussiens.

Une dernière propriété importante est que les états cohérents ne sont pas orthogonaux entre eux :

$$\langle\beta|\alpha\rangle = \exp(-|\beta - \alpha|^2) \tag{2.50}$$

Cette propriété sera essentielle pour l'étude des protocoles de cryptographie quantique présentée au chapitre 4.

2.3.4 Etats comprimés

Les états cohérents ont la particularité de ne pas posséder davantage de fluctuations statistiques que l'état vide, et de minimiser la relation d'incertitude d'Heisenberg. Dans son esthétique démonstration de 1932 [10], Wolfgang Pauli démontra que les fonctions d'ondes minimisant la relation d'incertitude d'Heisenberg étaient nécessairement des gaussiennes. La relation d'Heisenberg (2.12) ne spécifiant que le produit des variances, il est possible d'imaginer des états quantiques tels que la variance d'une quadrature soit inférieure au niveau de bruit quantique standard N_0. Le prix à payer pour cette réduction de bruit est une augmentation du bruit de la quadrature conjuguée, de sorte à conserver un niveau minimal de la relation d'Heisenberg. On appelle ces états des *états comprimés*, tels que :

$$\Delta X^2 = s\, N_0 \qquad\qquad \Delta P^2 = \frac{1}{s}\, N_0. \tag{2.51}$$

où s est un facteur de compression, pris par convention inférieur à 1. Les expériences basées sur la génération d'états comprimés par amplification paramétrique utilisent également la notion de paramètre de compression r tel que $s = e^{-2r}$. Le paramètre r est alors directement lié à la nonlinéarité effective de l'interaction.

Lorsque les valeurs moyennes des quadratures sont nulles, l'état comprimé est centré sur l'origine de l'espace des phases et on parle alors de *vide comprimé*. Il est intéressant de noter que la valeur moyenne du nombre de photons dans un état vide comprimé est non nulle et vaut $\langle\hat{N}\rangle = \sinh^2 r$. Cet effet peut se comprendre comme une conséquence de l'émission spontanée dans le milieu non-linéaire. Une autre propriété intéressante démontre [13] que tout état comprimé se déduit d'un vide comprimé par l'application d'un opérateur de déplacement.

Du fait de leurs relations entre les distributions de bruit des quadratures, les états comprimés présentent des particularités spécifiquement quantiques. Par exemple, le vide comprimé de facteur de compression $s = e^{-2r}$ peut se décomposer sur la base des états de Fock selon [17] :

$$|\Psi_s\rangle = \frac{1}{\sqrt{\cosh(r)}} \sum_{k=0}^{\infty} \left[C_{2k}^k \left(\frac{1}{2}\tanh(r)\right)^{2k} \right]^{1/2} |2k\rangle \tag{2.52}$$

Cette relation montre que les seuls termes présents dans la décomposition sont les termes pairs en nombre de photons, ce qui est une conséquence physique du fait que les photons sont émis par paires lors du processus d'interaction paramétrique à l'origine de la compression des fluctuations. Cette particularité quantique sera essentielle à la conception d'une source d'états non-gaussiens présentée en détails au chapitre 9.

D'un point de vue élémentaire, notre intuition conçoit le vide comprimé comme un état vide dont les échelles des axes de quadratures auraient été étirées ou comprimées. Cette intuition se retrouve de manière plus formelle dans l'expression de la fonction d'onde du vide comprimé donnée ici à un terme de phase près [18, 17] :

$$\psi_s(x) = \frac{1}{s^{\frac{1}{4}}}\,\psi_0(\frac{x}{\sqrt{s}}) \tag{2.53}$$

Il en va de même pour la fonction de Wigner associée :

$$W_s(x,p) = W_0(\frac{x}{\sqrt{s}}, \sqrt{s}\,p) \tag{2.54}$$

2.3.5 Etats intriqués en quadratures

Jusqu'à présent, nous n'avons considéré que des états monomodes. Une des richesses de la mécanique quantique est de manipuler des états à plusieurs composantes spatiales qui ne peuvent se réduire à un simple produit tensoriel d'états indépendants. En particulier, certains états ont la spécificité de présenter des corrélations au niveau des distributions quantiques entre leurs composantes.

Dans leur célèbre expérience de pensée proposée en 1935 [132], Einstein, Podolsky et Rosen prédisent l'existence de corrélations quantiques entre deux objets décrits par leurs opérateurs "position" et "impulsion" (X_A, P_A) et (X_B, P_B), qui vérifient la relation de commutation (2.11). Leur intuition est de remarquer qu'alors les opérateurs $X_A - X_B$ et $P_A + P_B$ commutent : $[X_A - X_B, P_A + P_B] = 0$. Selon le principe de Heisenberg, cette relation autorise la connaissance parfaite des quantités $(X_A - X_B)$ et $(P_A + P_B)$. Ainsi, des états bi-modes peuvent exister dans le cas particulier où les opérateurs X_A et X_B sont parfaitement corrélés alors que P_A et P_B sont parfaitement anti-corrélés [2]. De tels états sont alors appelés *états intriqués* ou *états EPR*.

La génération expérimentale de tels états est possible dans le cadre de l'optique quantique, par couplage de deux vides comprimés déphasés sur une lame semiréfléchissante [146] ou bien par amplification paramétrique non-dégénérée [143]. La qualité des corrélations expérimentales est cependant évidemment limitée, ne serait-ce que par couplage de l'état avec l'environnement. Il faut donc décrire l'état par le degré fini des corrélations entre composantes. Suivant la méthode choisie pour générer ces états, différentes notations sont utilisées : par la variance V de l'état thermique vu par chaque composante, par le facteur de compression s ou par le paramètre d'interaction nonlinéaire r. Ces notations sont résumées dans le tableau 2.1. L'utilisation de la variance V est plus appliquée au cas de la cryptographie quantique, le facteur de compression s est davantage utilisé dans les expériences générant l'intrication par un mélange de deux vides comprimés tandis que le paramètre de nonlinéarité r est adapté aux techniques de génération par amplification paramétrique.

En fin de compte, l'expression la plus intuitive est celle présentée par Grosshans et Grangier dans [70]. Dans une expression inspirée des notations en traitement du signal, la quadrature

[2] L'interprétation initiale de ces corrélations par Einstein, Podolsky et Rosen en tant que remise en cause fondamentale de la mécanique quantique sera discutée au chapitre 10 traitant de la génération d'états intriqués.

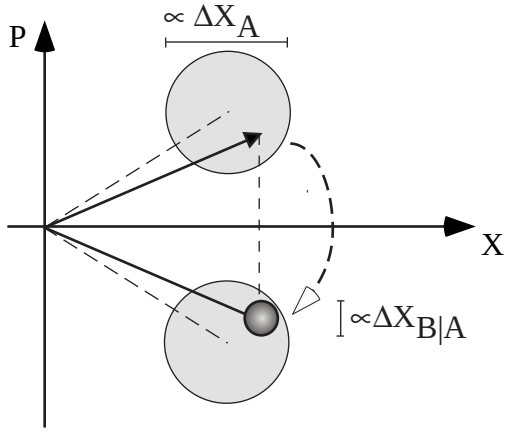

Figure 2.4: *Représentation d'un état EPR dans le diagramme de Fresnel. La mesure d'une composante fournit une information conditionnelle sur l'autre où l'incertitude est donnée par l'écart-type conditionnel* $\Delta X_{B|A} = \sqrt{V_{X_B|X_A}}$.

$\langle X_A^2 \rangle = \langle X_B^2 \rangle$	$V\, N_0$	$\frac{1}{2}\left(\frac{1}{s} + s\right)\, N_0$	$\cosh(2r)\, N_0$
$\langle (X_A - X_B)^2 \rangle$	$2(V - \sqrt{V^2-1})\, N_0$	$2s\, N_0$	$2e^{-2r}\, N_0$
$\langle X_A X_B \rangle$	$\sqrt{V^2-1}\, N_0$	$\frac{1}{2}\left(\frac{1}{s} - s\right)\, N_0$	$\sinh(2r)\, N_0$
$V_{X_B\|X_A}$	$N_0 \,/\, V$	$2N_0 \,/\, \left(s + \frac{1}{s}\right)$	$N_0 \,/\, \cosh(2r)$

Tableau 2.1: *Différents systèmes de notations pour décrire un état intriqué en quadratures à deux composantes A et B, avec pour conventions* $V > 1$, $s < 1$ *et* $r > 0$. *Les expressions pour la quadrature P sont identiques, à un signe négatif près dû aux anti-corrélations.*

reçue X_B s'exprime en une partie corrélée à X_A (le signal atténué par le gain de la ligne), plus un terme de fluctuations indépendantes (le bruit) :

$$X_B = g\, X_A + B \tag{2.55}$$

avec B indépendant de X_A, $\langle B X_A \rangle = 0$ et

$$g = \tanh 2r = \frac{1 - s^2}{1 + s^2} \tag{2.56}$$

$$\langle B^2 \rangle = \frac{N_0}{\cosh 2r} = \frac{2s}{1 + s^2}\, N_0 \tag{2.57}$$

Les corrélations quantiques que possèdent ces états intriqués constituent une ressource physique fondamentale pour l'exploitation de protocoles de communicaton quantique. L'influence particulière de l'intrication en cryptographie quantique sera abordée au chapitre 6, tandis que la génération expérimentale d'états intriqués en quadrature fera l'objet du chapitre 10.

2.3.6 Chats de Schrödinger

Si la mécanique quantique prédit l'existence d'états du champ électromagnétique, elle autorise également toute superposition linéaire de tels états. Suite au fameux "paradoxe" de l'(in)existence de superposition macroscopique d'états quantiques, la communauté de l'optique quantique désigne une superposition linéaire de deux états cohérents par le nom de *chat de Schrödinger*. Nous nous limiterons par la suite à l'étude de la superposition $|\alpha\rangle + |-\alpha\rangle$ avec α réel et dans le cas où les deux états cohérents sont suffisamment distincts, i.e. $\langle -\alpha|\alpha\rangle = e^{-4\alpha^2} \ll 1$ ce qui impose $\alpha > 2$. Dans ce cas, l'état *chat de Schrödinger* s'écrit :

$$|\psi\rangle \simeq \frac{1}{\sqrt{2}} \left(|\alpha\rangle + |-\alpha\rangle\right). \tag{2.58}$$

Les gaussiennes ne se recouvrant presque pas, la distribution de probabilité en X associée correspond à la moyenne des distribution de probabilité des deux états [202] :

$$|\psi(x)|^2 \simeq \frac{1}{2} \left(|\langle x|\alpha\rangle|^2 + |\langle x| - \alpha\rangle|^2\right) \tag{2.59}$$

La distribution suivant la quadrature X ne se distingue donc pas d'un mélange statistique classique de l'état $|\alpha\rangle$ et de l'état $|-\alpha\rangle$ avec des probabilités 1/2.

La particularité quantique de ces états apparaît en quadrature P, où les fonctions d'ondes de chaque état cohérent sont quasiment identiques à un facteur de phase près. Les termes de phase vont alors interférer dans la superposition quantique, avec pour conséquence l'apparition de franges d'interférences. La distribution de probabilité en P s'écrit alors comme une gaussienne modulée par un cosinus [202, 71] :

$$|\psi(p)|^2 = \sqrt{\frac{2}{\pi\, N_0}}\, e^{-\frac{p^2}{2N_0}}\, \cos^2 \frac{\alpha\, p}{\sqrt{N_0}}. \tag{2.60}$$

Cette distribution gaussienne modulée diffère fondamentalement d'un simple mélange statistique qui prédirait une gaussienne simple. Cependant, tout couplage avec l'environnement (décohérence) aura pour effet de brouiller la visibilité des franges d'interférence et ramènera au cas d'un mélange statistique.

Le terme d'interférence se retrouve dans la fonction de Wigner de l'état [71, 17] :

$$W_{chat,\alpha}(x,p) = \frac{1}{2} W_{\alpha}(x,p) + \frac{1}{2} W_{-\alpha}(x,p) + 2\, W_{interf}(x,p) \tag{2.61}$$

où W_{interf} décrit un terme d'interférence prenant des valeurs négatives :

$$W_{interf}(x,p) = \frac{1}{4\pi\, N_0}\, e^{-\frac{x^2+p^2}{2N_0}}\, \cos \frac{2\alpha p}{\sqrt{N_0}}. \tag{2.62}$$

L'étude d'états du type "chats de Schrödinger" nous a conduit à proposer un nouveau schéma théorique de test des inégalités de Bell avec des variables continues et une détection homodyne. Ce schéma sera détaillé dans le chapitre 11.

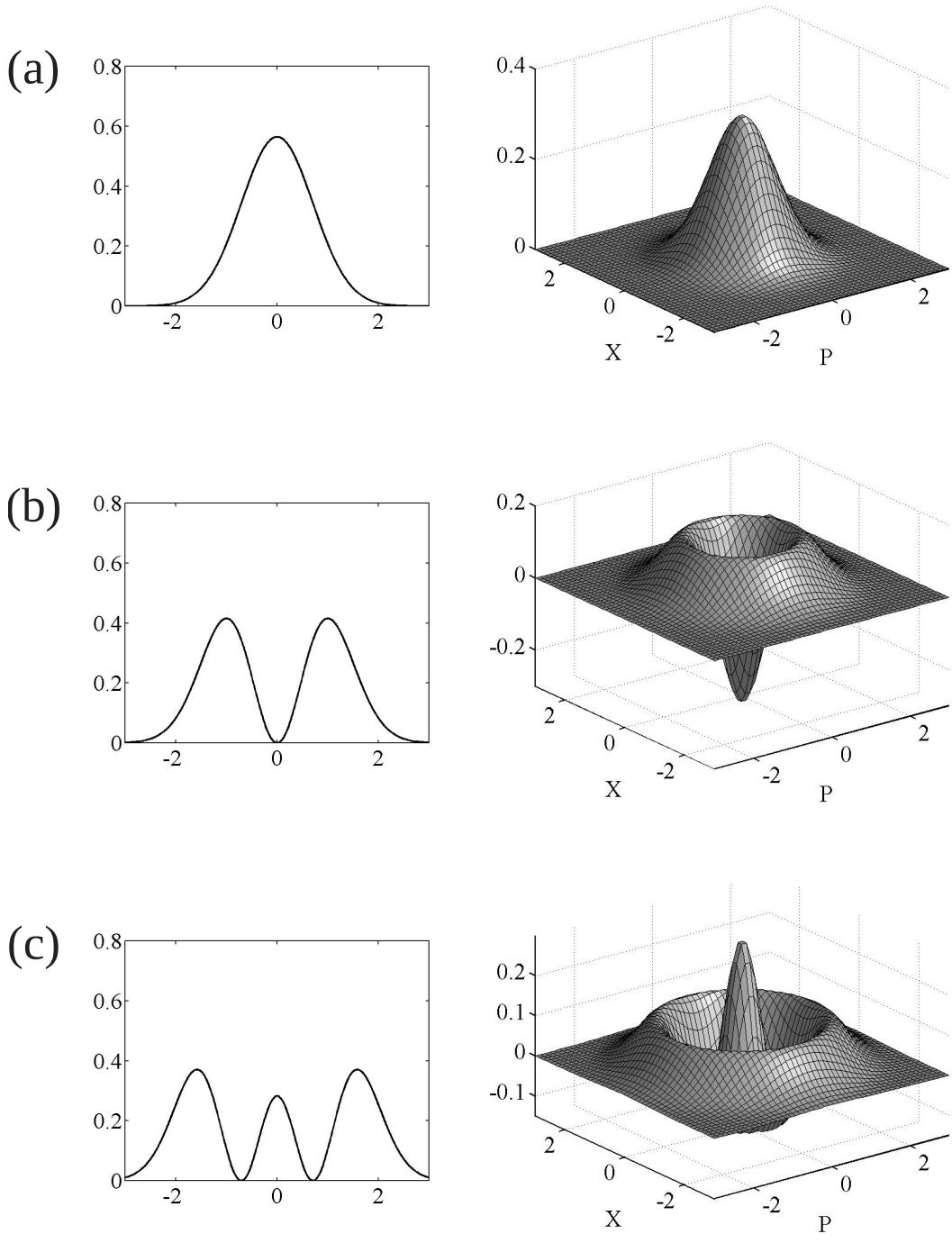

Figure 2.5: *Densité de probabilité pour une quadrature arbitraire et fonction de Wigner de différents états quantiques. (a) Vide* $|0\rangle$*, (b) Photon unique* $|1\rangle$*, (c) Etat de Fock* $|2\rangle$*. Les tracés ont été effectués avec la notation* $N_0 = 1/2$*.*

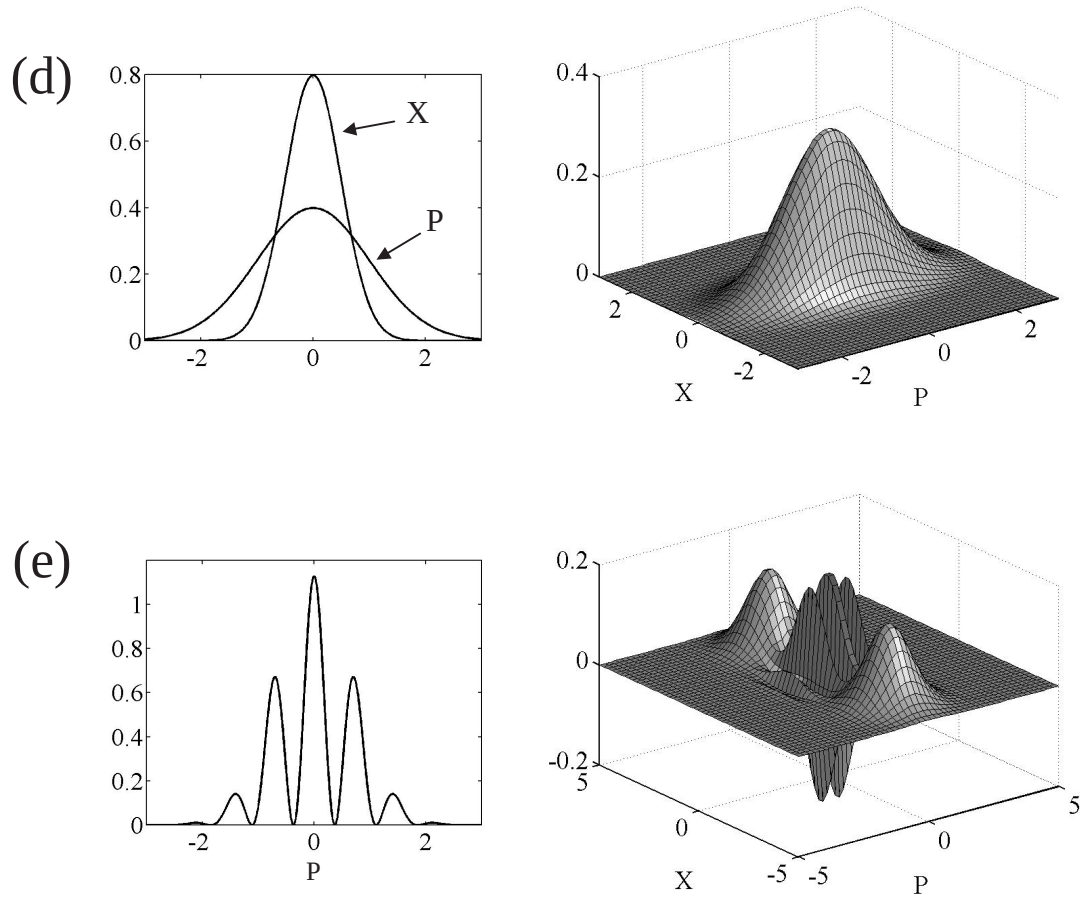

Figure 2.6: *(d) Vide comprimé de compression* $s = 0.5$*, (e) Chat de Schrödinger* $\alpha = 3$.

2.4 Manipulation des composantes de quadrature

Les états quantiques décrits précédemment seront utilisés tout au long de cette thèse, de la cryptographie quantique aux tests des inégalités de Bell. Afin de présenter les manipulations les plus usuelles de ces états, cette section décrit quelques composants optiques de base pour l'optique quantique avec des variables continues : la lame partiellement réfléchissante et les amplificateurs dépendants et indépendants de la phase.

2.4.1 Combinaison : lame partiellement réfléchissante

Comparée à d'autres branches de la physique, la photonique quantique se distingue par la simplicité de ses montages : une table optique, un laser monomode, quelques composants optiques de base et un thésard suffisent généralement aux expériences de ce domaine. Parmi ces composants optiques de base, la lame partiellement réfléchissante – au demeurant très simple

– permet déjà de mettre en évidence différents effets de la nature quantique de la lumière : interférences à un photon [19], corrélations bi-photoniques [20], génération d'états intriqués en variables discrètes [2] ou avec des variables continues [146]...

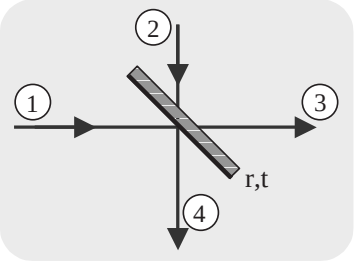

Figure 2.7: *Modèle d'une lame semi-réfléchissante sans pertes.*

Considérons une lame partiellement réfléchissante représentée sur la figure 2.7. Nous supposerons que cette lame n'absorbe pas la lumière et n'induit aucun déphasage particulier. De la sorte, deux modes incidents $\hat{a}_1, \hat{a}_2$ interfèrent sur la lame pour produire deux modes émergents $\hat{a}_3, \hat{a}_4$. Dans cette description, la lame est toujours considérée comme un élément à quatre ports : deux entrées et deux sorties. Même si un seul faisceau physique est présent en entrée, le formalisme de l'optique quantique considère que le second port d'entrée est occupé par un mode *vide* incident introduit dans la section 2.3.1.

Nous nous restreignons ici au cas de transformations unitaires à coefficients réels. Une analogie avec l'électromagnétisme classique nous conduit à exprimer la relation de passage à travers la lame par :

$$\begin{aligned} \hat{a}_3 &= t\hat{a}_1 + r\hat{a}_2 \\ \hat{a}_4 &= -r\hat{a}_1 + t\hat{a}_2 \end{aligned} \tag{2.63}$$

où r et t désignent les coefficients de réflexion et de transmission en amplitude de la lame, liés par la conservation de l'énergie $r^2 + t^2 = 1$. Un calcul rigoureux [14] basé sur l'expression de l'interaction entre le champ lumineux et les atomes de la lame permet de justifier ces relations (2.63). Les relations de transformation appliquées aux quadratures X, P se déduisent alors automatiquement, et permettent de vérifier que la relation de commutation (2.11) est toujours vérifiée pour les modes sortants.

En représentation de Schrödinger, la fonction d'onde à deux modes sortant se déduit par une rotation dans l'espace des phases de la fonction d'onde entrant [17] :

$$\psi(x_1, x_2) \Rrightarrow \psi(tx_3 - rx_4, rx_3 + tx_4) \tag{2.64}$$

Cette expression fournit une vision nouvelle de l'intrication émergeant de l'interférence sur une lame semi-réfléchissante de deux vides comprimés déphasés de $\pi/2$:

$$\begin{aligned} \psi(x_1, x_2) &\propto \exp(-\frac{x_1^2}{4sN_0}) \exp(-\frac{x_2^2}{4N_0/s}) \\ \Rrightarrow \psi(x_3, x_4) &\propto \exp(-\frac{(x_3 - x_4)^2}{8sN_0}) \exp(-\frac{(x_3 + x_4)^2}{8N_0/s}) \end{aligned} \tag{2.65}$$

Cela met en évidence les corrélations entre les quadratures des faisceaux EPR émergents.

La décomposition sur la base des états de Fock offre une perspective différente. L'action générale d'une lame sur un état de type $|n_1, n_2\rangle$ donne une formule complexe que l'on peut trouver par exemple dans l'équation (4.42) de la référence [17]. Un cas particulier de cette formule utile pour cette thèse consiste en le cas ou l'un des ports est occupé par un état de Fock $|n\rangle$ alors que l'autre mode est vide. On a alors la transformation suivante qui exprime la répartition binomiale des photons entre chaque sortie :

$$|n, 0\rangle \Rrightarrow \sum_{k=0}^{n} \sqrt{C_n^k}\, t^k\, r^{n-k}\, |k, n-k\rangle \tag{2.66}$$

Les photons ne sont pas scindés en fractions; le cas $n = 1, r = t = 1/\sqrt{2}$ donne en sortie l'état maximalement intriqué $(|0,1\rangle + |1,0\rangle)/\sqrt{2}$, ce qui ouvre les perspectives d'utilisation d'une lame pour mettre en évidence la dualité onde-corpuscule de la lumière et pour servir de source d'intrication. La formule (2.66) sera particulièrement utile dans les chapitres 9 et 11.

L'application la plus utile et la plus commune de la lame réfléchissante avec des variables continues est de modéliser l'effet de pertes par atténuation. L'absorption, les réflexions parasites, les problèmes de recouvrement de faisceaux sont décrits par un modèle de pertes très simple basé sur une lame partiellement réfléchissante de facteur de transmission en intensité η [17]. Cette formulation est également très intéressante pour comprendre la philosophie de la manipulation des variables continues, des mesures quantiques non-destructives à la cryptographie quantique.

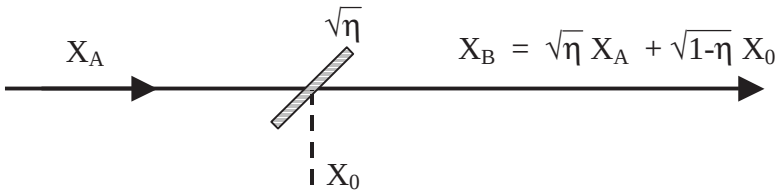

Figure 2.8: *Modélisation des pertes d'un canal quantique par une lame de transmission en intensité η.*

Considérons un signal X_A envoyé à travers un canal quantique de transmission η où les pertes sont modélisées par une lame (voir figure 2.8). La seconde entrée de la lame est occupée par un mode vide X_0 qui va s'ajouter en sortie sur le signal et diminuer le rapport signal à bruit. L'effet des pertes sur la quadrature en sortie X_B s'exprime alors par :

$$X_B = \sqrt{\eta}\, X_A + \sqrt{1-\eta}\, X_0 \tag{2.67}$$

Cette équation fait apparaître le canal quantique comme un *canal de communication à bruit additif gaussien* similaire à celui présenté dans la section 1.2.3 traitant de la théorie classique de l'information. Il est utile d'introduire un *bruit équivalent en entrée* B_{eq} tel que :

$$X_B = \sqrt{\eta}\,(X_A + B_{eq}) \tag{2.68}$$

$$B_{eq} = \sqrt{\frac{1-\eta}{\eta}} X_0 \tag{2.69}$$

ce qui fait apparaître un bruit gaussien centré de variance $\langle B_{eq}^2 \rangle = (1-\eta)/\eta\, N_0$ additionné au signal. Ce point de vue sera généralisé à un bruit quelconque dans la présentation de cryptographie quantique au chapitre 4.

2.4.2 Amplification indépendante de la phase

On peut chercher à étendre les formules de manipulation des quadratures pour une lame partiellement réfléchissante au cas d'un coefficient de transmission supérieur à un, c'est-à-dire à une amplification de gain supérieur à l'unité. L'étude des limites imposées par la physique quantique à l'amplification a été menée par Carlton Caves [79] dans le cas des amplificateurs linéaires. Dans cette section, nous cherchons à décrire un amplificateur monomode dont le champ en sortie dépend linéairement du champ d'entrée, sans effet de discrimination entre les quadratures, i.e. indépendamment de la phase relative du champ entrant.

L'amplification étant linéaire, l'opérateur annihilation en sortie $\hat{a}_{out}$ doit alors s'écrire comme une superposition linéaire des opérateurs $\hat{a}_{in}, \hat{a}_{in}^\dagger$ du champ entrant, plus un terme $\hat{a}_{bruit}^\dagger$ qui introduit du bruit d'émission spontanée de photons intervenant lors de l'amplification. Comme on impose le choix d'une amplification indépendante de la phase, $\hat{a}_{out}$ ne doit pas dépendre de $\hat{a}_{in}^\dagger$, ce qui donne in fine [79] :

$$\hat{a}_{out} = \sqrt{G}\,\hat{a}_{in} + \hat{a}_{bruit}^\dagger \tag{2.70}$$

où G désigne le gain en intensité, considéré comme réel. La physique quantique imposant une transformation unitaire, le terme de bruit $\hat{a}_{bruit}^\dagger$ doit commuter avec $\hat{a}_{in}$, ce qui nous permet de calculer le commutateur $[\hat{a}_{out}, \hat{a}_{out}^\dagger]$:

$$[\hat{a}_{out}, \hat{a}_{out}^\dagger] = 1 = G + [\hat{a}_{bruit}, \hat{a}_{bruit}^\dagger] \tag{2.71}$$

Compte tenu de la relation d'incertitude d'Heisenberg, ce commutateur fixe une limite fondamentale au bruit ajouté lors d'une amplification indépendante de la phase :

$$\Delta\hat{a}_{bruit}^2 \geq \frac{1}{2}|[\hat{a}_{bruit}, \hat{a}_{bruit}^\dagger]| = \frac{1}{2}(G-1) \tag{2.72}$$

Il n'est donc pas possible de concevoir un amplificateur quantique de gain strictement supérieur à 1 et indépendant de la phase (i.e. insensible en quadrature) qui soit dénué de tout bruit ajouté. Dès lors qu'il y a amplification, il existe nécessairement un bruit d'émission spontanée.

La limite de Caves est atteinte dans le cas d'un amplificateur paramétrique non-dégénéré, décrit par l'hamiltonien d'interaction entre deux modes $\hat{a}_1, \hat{a}_2$ [13] :

$$\hat{H}_{nd} = \imath\hbar\chi\,(\hat{a}_1^\dagger\hat{a}_2^\dagger - \hat{a}_1\hat{a}_2) \tag{2.73}$$

où χ est une constante de couplage nonlinéaire proportionnelle à la susceptibilité quadratique du milieu et à l'intensité de la pompe. Les équations d'évolution d'Heisenberg s'écrivent alors :

$$\begin{aligned} \frac{d\hat{a}_1}{dt} &= \frac{1}{\imath\hbar}\,[\hat{a}_1, \hat{H}_{nd}] = \chi\,\hat{a}_2^\dagger \\ \frac{d\hat{a}_2}{dt} &= \frac{1}{\imath\hbar}\,[\hat{a}_2, \hat{H}_{nd}] = \chi\,\hat{a}_1^\dagger \end{aligned} \tag{2.74}$$

Ces équations permettent de décrire les modes en sortie de l'amplificateur en fonction des modes en entrée :

$$\begin{aligned} \hat{a}_{out,1} &= \hat{a}_{in,1}\cosh r + \hat{a}_{in,2}^\dagger \sinh r \\ \hat{a}_{out,2} &= \hat{a}_{in,2}\cosh r + \hat{a}_{in,1}^\dagger \sinh r \end{aligned} \tag{2.75}$$

où on a posé $r = \chi\tau$ avec τ le temps caractéristique de l'interaction. Ces équations montrent que le gain de l'amplification paramétrique quantique correspond au gain classique attendu :

$$G = \cosh^2 r \tag{2.76}$$

On peut enfin exprimer les relations entre les quadratures des modes de sortie 1 et 2, en écrivant explicitement le terme de gain de l'amplification :

$$\begin{aligned} X_{out,1} &= \sqrt{G}\, X_{in,1} + \sqrt{G-1}\, X_{in,2} \\ P_{out,1} &= \sqrt{G}\, P_{in,1} - \sqrt{G-1}\, P_{in,2} \\ X_{out,2} &= \sqrt{G}\, X_{in,2} + \sqrt{G-1}\, X_{in,1} \\ P_{out,2} &= \sqrt{G}\, P_{in,2} - \sqrt{G-1}\, P_{in,1} \end{aligned} \tag{2.77}$$

Dans le cas d'un amplificateur où le mode 2 entrant est vide, il est facile de voir que cet amplificateur non-dégénéré atteint la limite prévue par Caves en identifiant :

$$\hat{a}_{bruit} = \sinh(r)\, \hat{a}_{in,2} = \sqrt{G-1}\, \hat{a}_{in,2} \tag{2.78}$$

Un tel amplificateur est un élément essentiel pour l'information quantique, où il intervient notamment dans les actions de clonage quantique avec des variables continues [82, 3] ou dans la génération d'états intriqués en quadratures [143]. Son implication dans les stratégies d'espionnage quantique sera étudiée au chapitre 4, tandis que la réalisation expérimentale d'un tel amplificateur fera l'objet du chapitre 10.

2.4.3 Amplification sélective en quadratures

S'il n'est pas possible de concevoir un amplificateur sans bruit et indépendant de la phase, nous allons voir qu'en relâchant la contrainte sur la phase il est possible de réaliser un amplificateur qui n'ajoute aucun bruit supplémentaire.

La démarche a été effectuée par Caves dans le même article [79], où l'amplification dépendante en quadrature s'écrit maintenant :

$$\begin{aligned} X_{out} &= \sqrt{G_X}\, X_{in} + X_{bruit} \\ P_{out} &= \sqrt{G_P}\, P_{in} + P_{bruit} \end{aligned} \tag{2.79}$$

En imposant toujours une transformation unitaire et en calculant le commutateur $[X_{out}, P_{out}]$, on montre que le bruit ajouté doit vérifier la relation d'Heisenberg [79] :

$$\Delta X_{bruit} \Delta P_{bruit} \geq (\sqrt{G_X G_P} - 1)\, N_0 \tag{2.80}$$

En choisissant alors $G_X = 1/G_P$, le terme de droite dans l'inégalité ci-dessus s'annule et il est alors théoriquement possible de supprimer toutes les fluctuations de bruit.

Une telle amplification est réalisée par un amplificateur optique dégénéré. La description de cet amplificateur se fait très simplement en considérant le cas non-dégénéré de la section précédente et en remplaçant $\hat{a}_1, \hat{a}_2$ par un seul mode $\hat{a}_{in}$ [13]. L'opérateur annihilation en sortie de l'amplificateur s'écrit :

$$\hat{a}_{out} = \hat{a}_{in} \cosh r + \hat{a}_{in}^{\dagger} \sinh r \tag{2.81}$$

où à nouveau r est un terme d'interaction non-linéaire, proportionnel à la susceptibilité en second ordre du milieu, à l'intensité pompe et au temps d'interaction. On remarquera en particulier que l'expression (2.81) ne comporte aucun terme de bruit ajouté, mais est sensible à la phase. On en déduit immédiatement l'expression pour les quadratures en sortie :

$$X_{out} = e^{+r}\, X_{in} \qquad\qquad P_{out} = e^{-r}\, P_{in} \tag{2.82}$$

L'amplification est bien réalisée sans bruit supplémentaire et est sensible en phase : la quadrature X est amplifiée tandis que la quadrature P est déamplifiée.

En particulier, on peut remarquer ici que si le mode incident est un mode vide, alors les variances du mode en sortie sont de la forme :

$$\langle X^2 \rangle = e^{+2r} N_0 \qquad \langle P^2 \rangle = e^{-2r} N_0 \tag{2.83}$$

ce qui constitue la signature d'un vide comprimé. L'amplificateur dégénéré sera donc une source de compression des fluctuations quantiques au même titre que l'amplificateur non-dégénéré est une source de corrélations quantiques. Cette technique d'amplification paramétrique dépendante de la phase sera utilisée expérimentalement pour générer des états comprimés, et est détaillée au chapitre 7.

2.5 Conclusion

Les différents outils de l'optique quantique présentés au cours de ce chapitre sont essentiels aux protocoles de traitement de l'information quantique avec des variables continues [3, 1], pour la représentation des ressources quantiques comme pour la manipulation des composantes de quadrature.

L'utilisation des états quantiques de référence présentés se fera tout au long de cette thèse. La mesure du vide est à la base de la calibration de notre système de détection homodyne, les états cohérents serviront à l'expérience de cryptographie quantique, les états comprimés et intriqués seront générés et caractérisés expérimentalement pour fournir les ressources nécessaires à de futures mises en œuvre de protocoles de communication quantique. Enfin, les superpositions quantiques d'états cohérents seront utiles pour envisager des tests des inégalités de Bell avec des variables continues.

Un point essentiel pour la manipulation des variables continues a été volontairement passé sous silence au cours de ce chapitre : comment mesurer expérimentalement une composante de quadrature ? Cette quantité étant dépendante du champ électromagnétique, il n'est pas possible de la mesurer avec une simple photodiode sensible à l'intensité moyenne du champ, mais il faut recourir à un système interférométrique plus complexe appelé *détection homodyne*. La description théorique et expérimentale d'une telle détection sera l'objet essentiel du chapitre suivant.

Chapitre 3

Réalisation d'une détection homodyne impulsionnelle

Sommaire

Introduction au principe de la mesure homodyne

Les variables continues que nous souhaitons utiliser étant proportionnelles au champ électrique, il n'est pas possible d'utiliser un système de détection de type photodiode basé sur une mesure d'un terme quadratique au champ lumineux, comme l'intensité crête ou le nombre de photons. Par ailleurs, la fréquence d'oscillation du champ optique ($\backsimeq$ 100 THz) est trop élevée pour envisager une mesure électronique directe de ce champ. Pour accéder au champ signal, il est alors nécessaire de considérer une mesure de battement relatif par rapport à un champ de référence. Lorsque cette référence est parfaitement synchrone au champ signal, un des termes de battement se trouve au voisinage de la fréquence nulle, ce qui est alors aisément mesuré électroniquement.

Ce principe, identique à celui d'une détection électronique synchrone, est illustré sur la figure 3.1. Le terme utile de battements est obtenu par interférences optiques entre le champ signal et un champ intense de référence, appelé oscillateur local. Le faisceau signal est mélangé avec l'oscillateur local sur une lame semi-réfléchissante, puis l'intensité de chaque voie est mesurée avec une photodiode de haute efficacité quantique. Pour supprimer les intensités moyennes mesurées par chaque photodiode qui n'apportent aucune information utile, les photocourants sont soustraits pour ne conserver que les termes croisés d'interférence signal-oscillateur local. Le signal utile en sortie est alors directement proportionnel à la composante du champ entrant en phase avec l'oscillateur local. Ce signal est de plus amplifié d'un facteur fixé par l'intensité de l'oscillateur local. Enfin, la fréquence de sortie est dans une gamme accessible aux composants électroniques. Le champ de référence étant parfaitement synchrone au champ signal, on parle alors d'un système de *détection homodyne*, par opposition à la détection hétérodyne où les champs signal et oscillateur local sont légèrement décalés en fréquence.

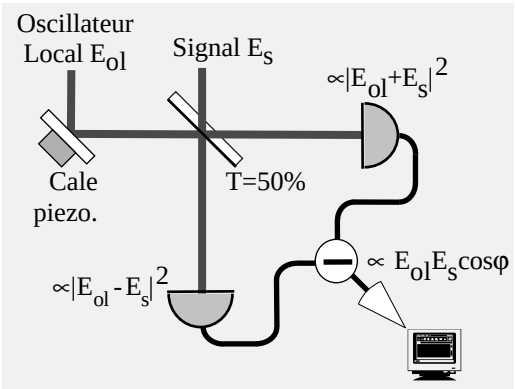

Figure 3.1: *Schéma de principe d'une détection homodyne parfaite.*

Particularités de nos expériences : résolution temporelle

Depuis la proposition théorique de Yuen et Chan en 1983 [33], le système de détection homodyne a été utilisé avec succès dans différentes applications de l'optique quantique ou du traitement quantique de l'information : mesure des états comprimés du champ [105, 106], tomographie quantique [30, 27, 28], téléportation quantique [146], cryptographie quantique [73].

La grande majorité des mesures est effectuée dans le domaine fréquentiel, même pour des expériences employant des impulsions lumineuses [106]. Ce choix de domaine résulte en partie du fait que la réalisation d'une détection homodyne y est plus simple techniquement. En effet, l'utilisation d'un analyseur de spectre permet de n'étudier qu'une bande spectrale étroite à une fréquence de l'ordre de quelques MHz et ainsi de filtrer efficacement tous les bruits techniques présents à des fréquences inférieures. Cette technique souffre cependant de certaines limitations pour une utilisation en traitement quantique de l'information : l'échange de symboles portant des informations nécessite obligatoirement de prendre en compte l'aspect temporel du message, donc d'utiliser une détection qui soit résolue en temps. Par ailleurs, une détection dans le domaine fréquentiel ne fournit généralement des informations que dans une bande latérale particulière. En régime impulsionnel, elle nécessite une moyenne sur plusieurs impulsions individuelles.

La technique de détection homodyne résolue en temps que nous avons développée permet une application plus prometteuse pour la communication quantique. Pour chaque impulsion lu-

mineuse incidente, l'électronique rapide de la détection échantillonne en temps réel une valeur de la quadrature du champ signal en phase avec l'oscillateur local. On peut alors directement décoder l'information portée sur les propriétés quantiques de chaque impulsion et accéder à la distribution statistique en quadrature en répétant ces mesures de nombreuses fois. Il est alors facile d'analyser ces transferts en terme d'information de Shannon (chapitre 1) ou bien de reconstruire la fonction de Wigner de l'état (chapitre 2). De plus, ce système peut fonctionner à des cadences élevées (de l'ordre du MHz), ce qui permet d'atteindre des débits d'informations élevés en cryptographie quantique [73], ou d'acquérir suffisamment de points en un temps raisonnablement court pour éviter des dérives expérimentales en tomographie quantique [128].

L'inconvénient majeur d'une détection homodyne impulsionnelle est la difficulté de sa réalisation expérimentale. D'une part, la bande passante de l'électronique doit être suffisamment large pour permettre une mesure résolue en temps et d'autre part, la mesure d'une composante de quadrature ne doit pas être noyée sous un bruit à basse fréquence. L'équilibrage entre les voies doit alors être le plus parfaitement réalisé et l'électronique doit afficher un très bas bruit sur l'ensemble de la plage spectrale utile.

Des systèmes de détection homodyne impulsionnelle résolue en temps ont été développés au préalable par les équipes de Michael Raymer [26] et de Stefan Schiller [35, 30] pour des applications en tomographie quantique. Notre groupe a été le premier à utiliser expérimentalement un tel système pour échanger une clé secrète [73]. Cette réalisation a été rendue possible par les travaux de Frédéric Grosshans, Jiangrui Gao, Rosa Tualle-Brouri et André Villing qui ont largement participé à la conception du premier prototype à amplification de tension. Le second prototype à amplification de charge a été réalisé grâce aux contributions de Rosa Tualle-Brouri, Jérôme Lodewyck, Alexeï Ourjoumtsev et André Villing.

Ce chapitre est entièrement dédié à l'étude d'une détection homodyne résolue en temps, des aspects théoriques (sections 3.1 et 3.2) à la réalisation expérimentale (sections 3.3 à 3.6). Nous aborderons ainsi la modélisation théorique d'une détection homodyne, l'influence des imperfections, et la discussion de la réalisation des deux prototypes utilisés.

3.1 Aspects théoriques

Dans cette section, nous ne considérerons que le cas d'une détection idéale, décrite sur la figure 3.1 : les deux voies sont parfaitement équilibrées, la visibilité des franges d'interférences est maximale. L'étude de l'influence de diverses sources d'imperfections expérimentales sera effectuée dans la section 3.2.

3.1.1 Point de vue classique

L'optique ondulatoire classique offre une compréhension partielle mais rapide du fonctionnement d'une détection homodyne. En notation indépendante du temps, le champ oscillateur local se compose d'une amplitude $|\mathcal{E}_{ol}|$ et d'une phase ϕ_{ol} :

$$\mathcal{E}_{ol} = |\mathcal{E}_{ol}|e^{\imath\phi_{ol}} \tag{3.1}$$

On introduit de plus l'intensité du champ en prenant la convention $I_{ol} = |\mathcal{E}_{ol}|^2$.

Par rapport à la phase de l'oscillateur local, le champ signal (normalisé) de même fréquence se décompose en ses composantes de quadratures suivant la notation complexe :

$$\mathcal{E}_s = \frac{1}{2\sqrt{N_0}}(X_{s,\phi_{ol}} + \imath P_{s,\phi_{ol}})e^{\imath\phi_{ol}} \tag{3.2}$$

où le terme en $1/2\sqrt{N_0}$ est introduit de sorte à avoir les mêmes conventions pour les quadratures que (2.9) et (2.44), et la normalisation en $\mathcal{E}_m$ est ici passée sous silence. Les photocourants I_+ et I_- détectés sur chaque voie sont sensibles aux interférences entre le champ signal et l'oscillateur local.

$$\begin{aligned} I_\pm = \frac{1}{2}\left|\mathcal{E}_{ol} \pm \mathcal{E}_s\right|^2 &= \frac{1}{2}\left(\left|\mathcal{E}_{ol}\right| \pm \frac{1}{2\sqrt{N_0}} X_{s,\phi_{ol}}\right)^2 + \frac{P^2_{s,\phi_{ol}}}{8N_0} \\ &= \frac{1}{2} I_{ol} + \frac{1}{2} I_s \pm \frac{1}{2\sqrt{N_0}} \left|\mathcal{E}_{ol}\right| X_{s,\phi_{ol}} \end{aligned} \tag{3.3}$$

La différence des photocourants permet de s'affranchir des intensités moyennes pour ne conserver que les termes croisés d'interférence :

$$\delta I = I_+ - I_- = \sqrt{\frac{I_{ol}}{N_0}}\, X_{s,\phi_{ol}} \tag{3.4}$$

Cette expression montre alors que la différence des photocourants est proportionnelle à la composante de quadrature signal en phase avec l'oscillateur local. En faisant varier la phase ϕ_{ol}, il est alors possible de mesurer n'importe quelle quadrature signal souhaitée.

L'équation (3.4) exprime de plus que la quadrature signal utile est amplifiée par l'amplitude de l'oscillateur local $\sqrt{I_{ol}}$. Ce dispositif permet donc de détecter des valeurs extrêmement faibles du champ signal tout en assurant un niveau suffisant pour dépasser le courant d'obscurité des photodiodes polarisées. On peut ainsi employer des photodiodes d'efficacité quantique élevée pour étudier des champs comportant moins d'un photon en moyenne.

3.1.2 Modélisation quantique

Le modèle de la mesure homodyne classique (3.4) n'explique pas la présence du bruit de photon (ou bruit Schottky) lorsqu'aucun faisceau n'est envoyé sur la voie signal. Pour expliquer l'origine de ce phénomène, il nous faut recourir à une description quantique du processus de photodétection, soit en introduisant une répartition aléatoire des temps d'arrivée des quanta d'énergie lumineuse, soit en considérant la présence d'un mode vide quantique du champ électromagnétique signal.

Dans un formalisme quantique, d'après les définitions du chapitre 2, chaque voie de la détection homodyne est décrite par un opérateur annihilation monomode $\hat{a}_\pm$:

$$\hat{a}_\pm = \frac{1}{\sqrt{2}}(\hat{a}_{ol} \pm \hat{a}_s) = \frac{1}{\sqrt{2}}(|\mathcal{E}_{ol}|e^{\imath\phi_{ol}} \pm \hat{a}_s) \tag{3.5}$$

Dans cette dernière équation, nous avons fait la supposition que l'amplitude de l'oscillateur local est très grande devant le champ signal, de sorte à pouvoir négliger dans un premier temps les fluctuations de l'oscillateur local et considérer ce mode comme un champ parfait purement classique (l'influence de cette hypothèse sera discutée explicitement dans la section 3.2.4). Les photocourants détectés sur chaque voie sont alors proportionnels à l'opérateur nombre de photon :

$$\hat{I}_\pm = \hat{a}^\dagger_\pm \hat{a}_\pm = \frac{1}{2}|\mathcal{E}_{ol}|^2 + \frac{1}{2}\hat{a}^\dagger_s \hat{a}_s \pm \frac{1}{2}|\mathcal{E}_{ol}|(e^{-\imath\phi_{ol}}\hat{a}_s + e^{+\imath\phi_{ol}}\hat{a}^\dagger_s) \tag{3.6}$$

La différence des photocourants permet à nouveau de s'affranchir des intensités moyennes pour ne conserver que les termes croisés d'interférence :

$$\boxed{\delta\hat{I} = |\mathcal{E}_{ol}|(e^{-\imath\phi_{ol}}\hat{a}_s + e^{+\imath\phi_{ol}}\hat{a}^\dagger_s) = \sqrt{\frac{I_{ol}}{N_0}}\, X_{s,\phi_{ol}}} \tag{3.7}$$

où la quadrature en phase avec l'oscillateur local $X_{s,\phi_{ol}}$ est définie d'après les équations (2.14) et (2.9). On retrouve alors les résultats du traitement classique : la soustraction des photocourants est proportionnelle à la quadrature signal en phase avec l'oscillateur local, multipliée par l'amplitude du champ oscillateur local. Ce résultat permet aussi d'étendre l'interprétation classique : l'oscillateur intervient comme une direction de projection privilégiée de l'espace des phases, non seulement pour la valeur moyenne des quadratures mais également pour tous les moments statistiques d'ordres supérieurs. En prenant plusieurs phases différentes de référence, on peut acquérir suffisamment de mesures pour accéder à la distribution de probabilité associée à chaque quadrature $\Pr(x,\theta)$. Connaissant ces distributions, il est alors possible de modéliser l'état quantique sans aucune hypothèse a priori, en reconstruisant la fonction de Wigner associée ou la matrice densité (voir la section 2.2).

Ce traitement met également en évidence des effets spécifiquement quantiques, comme par exemple le bruit de photon lorsque le signal entrant est dans un mode vide. Dans ce cas $\langle X_s^2\rangle = N_0$, et on retrouve la formule de Schottky du bruit de photon $\langle \delta\hat{I}^2\rangle \propto I_{ol}$, la variance du bruit des photocourants est proportionnelle à l'intensité du flux lumineux incident. Une interprétation de ce résultat est que tous les bruits techniques (classiques) corrélés au niveau de chaque photodiode sont parfaitement soustraits, et il ne reste alors que les fluctuations quantiques. Ceci constitue alors une manière simple et efficace de mesurer la référence de bruit standard N_0 et de vérifier l'équilibrage des voies : la voie signal étant masquée, la variance de bruit mesurée doit croître *linéairement* avec l'intensité incidente, alors qu'un bruit classique de photodétection introduirait une dépendance quadratique de la variance avec l'intensité.

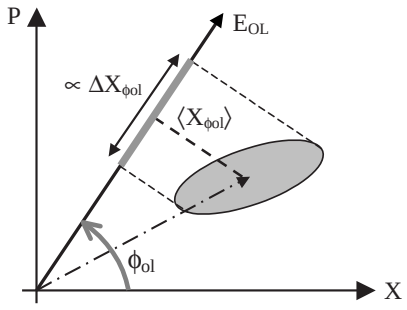

Figure 3.2: *Action intuitive d'une détection homodyne dans l'espace des phases.*

3.2 Influence des imperfections

Si la détection homodyne parfaite est un puissant outil d'investigation des propriétés quantiques des états lumineux, toute mise en œuvre expérimentale sera inévitablement confrontée à diverses sources d'imperfections : déséquilibre des voies, transmissions des optiques différentes de 1, rendements quantiques limités des photodiodes, mauvaise adaptation des modes... L'influence de ces imperfections sera détaillée dans cette section où nous reprenons enfin le calcul de la détection homodyne en tenant compte du bruit présent sur la faisceau oscillateur local.

3.2.1 Déséquilibre

Tout déséquilibre de l'intensité entre les voies peut facilement se modéliser par une lame séparatrice non parfaitement semi-réfléchissante. On est amené à introduire les coefficients de

réflectivité R et de transmission T en intensité de la lame :

$$T = \frac{1}{2} + \varepsilon \qquad\qquad R = \frac{1}{2} - \varepsilon. \tag{3.8}$$

avec $\varepsilon \ll 1/2$. Un calcul classique fournit dans ce cas les valeurs des photocourants détectés :

$$\begin{aligned} I_+ &= |\sqrt{T}\,\mathcal{E}_{ol} + \sqrt{R}\,\mathcal{E}_s|^2 = \frac{1}{2}(I_{ol} + I_s) + \varepsilon\,(I_{ol} - I_s) + 2\sqrt{\frac{1}{4} - \varepsilon^2}\,|\mathcal{E}_{ol}\mathcal{E}_s|\cos\phi_{ol} \\ I_- &= |\sqrt{R}\,\mathcal{E}_{ol} - \sqrt{T}\,\mathcal{E}_s|^2 = \frac{1}{2}(I_{ol} + I_s) - \varepsilon\,(I_{ol} - I_s) - 2\sqrt{\frac{1}{4} - \varepsilon^2}\,|\mathcal{E}_{ol}\mathcal{E}_s|\cos\phi_{ol} \end{aligned} \tag{3.9}$$

En négligeant le terme en ε^2 devant $1/4$, ainsi que le terme I_s dans $(I_{ol} - I_s)$, la différence des photocourants s'écrit alors :

$$\delta I = 2|\mathcal{E}_{ol}||\mathcal{E}_s|\cos\phi_{ol} + 2\varepsilon I_{ol} \tag{3.10}$$

Le premier terme dans le membre de droite est notre signal utile proportionnel au champ du signal, le second terme est un bruit classique ajouté par le déséquilibre de la détection, dont la variance varie quadratiquement avec la puissance de l'oscillateur local. Tout déséquilibre de la détection entraîne un écart par rapport à la mesure du bruit de photon et une dépendance alors quadratique de la variance détectée en fonction de l'intensité de l'oscillateur local.

Dans le cadre d'une détection homodyne résolue en fréquence d'un faisceau continu, la composante constante en $2\varepsilon I_{ol}$ est généralement filtrée par un filtre passe-haut en entrée de l'analyseur de spectre, qui permet de s'affranchir des bruits techniques. Il n'en va pas de même pour une détection homodyne résolue en temps, où toutes les composantes spectrales doivent être prises en compte, du quasi-continu à (au moins) la cadence de répétition des impulsions. Il n'est alors pas possible de filtrer le bruit classique et l'équilibrage doit être le plus parfait possible.

La formule (3.10) permet de quantifier la précision de l'équilibrage ε. Cette équation se réécrit en exprimant la quantité amplifiée par l'oscillateur local :

$$\delta I = \sqrt{\frac{I_{ol}}{N_0}}\,(X_s + 2\varepsilon\sqrt{I_{ol}N_0}) \tag{3.11}$$

Pour mesurer les fluctuations du vide où X_s prend des valeurs typiques de l'ordre de $\sqrt{N_0}$, il faut alors garantir un équilibrage $\varepsilon \ll 1/(2\sqrt{I_{ol}})$. Pour un oscillateur local comportant 10^8 photons par impulsion, l'équilibrage entre les voies devra être réalisé à mieux de 5×10^{-5} près. Cette contrainte devra obligatoirement être prise en compte dans le dimensionnement pratique de notre système de détection.

3.2.2 Pertes optiques

Nous allons montrer dans cette section que les différentes pertes par atténuation dans la détection peuvent se traduire par une lame partiellement réfléchissante placée en amont de la détection, qui atténue le signal incident tout en ajoutant des fluctuations du vide.

Nous partons de la modélisation des pertes décrite sur la figure 3.3(a), en supposant que la détection est équilibrée de telle sorte à avoir les mêmes pertes sur les deux bras. Chaque mode détecté s'écrit alors :

$$\hat{a}_\pm = \sqrt{\frac{\eta}{2}}\,(\hat{a}_{ol} \pm \hat{a}_s) + \sqrt{1-\eta}\,\hat{a}_{0,\pm} \tag{3.12}$$

où $\hat{a}_{0,\pm}$ désigne un mode vide entrant sur la voie + ou − de quadratures $X_{0,\pm}$. On peut alors calculer les photocourants détectés par chaque voie ainsi que la soustraction de ces photocourants.

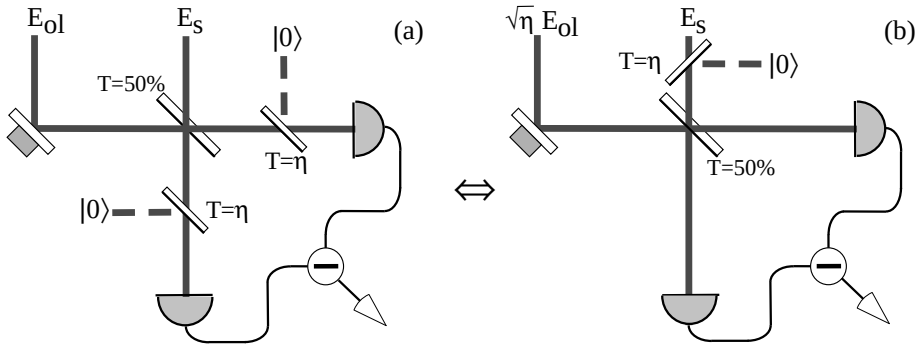

Figure 3.3: *(a) et (b) : modélisations équivalentes d'une détection d'efficacité limitée η.*

En ne gardant que les termes proportionnels au champ de l'oscillateur local, la différence des photocourants s'écrit :

$$\delta\hat{I} = \eta\sqrt{\frac{I_{ol}}{N_0}}\,X_{s,\phi_{ol}} + \sqrt{\frac{\eta(1-\eta)}{2}}\,\sqrt{\frac{I_{ol}}{N_0}}\,(X_{0,+} + X_{0,-}) \tag{3.13}$$

Les bruits entrant sur les voies + et − étant indépendants, on peut formellement remplacer la somme normalisée des modes vides $(X_{0,+} + X_{0,-})/\sqrt{2}$ par un mode vide unique X_0 de moyenne nulle et de même variance N_0. L'équation (3.13) se réécrit alors en :

$$\delta\hat{I} = \sqrt{\frac{\eta I_{ol}}{N_0}}\,\left(\sqrt{\eta}\,X_{s,\phi_{ol}} + \sqrt{1-\eta}\,X_0\right) \tag{3.14}$$

Ce qui justifie a posteriori la modélisation de la figure 3.3(b) où une lame de transmission en intensité η modifie le signal en amont de la détection. Il est à noter que les pertes affectent également le faisceau oscillateur local, qui peut être formellement considéré comme ayant une intensité effective ηI_{ol}.

3.2.3 Adaptation des modes

Un mauvais recouvrement des modes spatio-temporels du signal et de l'oscillateur local va à nouveau se traduire par une efficacité équivalente, dont les effets sont modélisés par une lame partiellement réfléchissante placée en amont de la détection. Parce que l'oscillateur local intervient comme une sorte "d'amplificateur optique", il constitue le paramètre déterminant le choix du mode spatio-temporel observé. Par le phénomène d'interférences, l'oscillateur local sélectionne exclusivement le mode spatio-temporel qui lui est adapté, et permet ainsi d'isoler un mode "signal visible" du reste de l'univers. Nous donnons ici un calcul intuitif de l'efficacité d'adaptation des modes en décomposant le mode signal en un mode parallèle parfaitement adapté et en modes orthogonaux qui n'interfèrent pas. Un traitement plus complet est donné dans [36].

Dans un modèle simple, deux points de vue peuvent être développés, soit en décomposant le mode du signal (figure 3.4(a)), soit en décomposant le mode de l'oscillateur local (figure 3.4(b)). Les deux points de vue fournissent bien sûr le même résultat. Cependant, la décomposition (a) du mode signal donne des calculs plus allégés. Ce mode se décompose alors en un mode identique à celui de l'oscillateur local $\hat{a}_{s,//}$ et en différents modes orthogonaux $\hat{a}_{s,\perp,i}$ avec une répartition

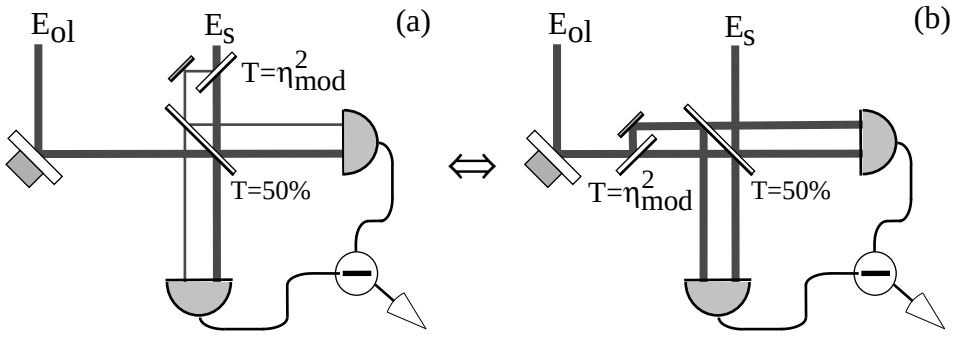

Figure 3.4: *(a) et (b) : modélisations équivalentes d'une détection où les modes ne sont pas parfaitement adaptés. Les modes vides entrant ne sont pas représentés.*

η_{mod} et de probabilités associées p_i (telles que $\sum {p_i}^2 = 1$) :

$$\hat{a}_s = \eta_{mod}\,\hat{a}_{s,//} + \sqrt{1-\eta_{mod}^2}\,\left(\sum_i p_i\,\hat{a}_{s,\perp,i}\right) \tag{3.15}$$

Seul le mode parallèle interfère avec l'oscillateur local. Pour ce dernier , les interférences avec les modes $\hat{a}_{s,\perp,i}$ équivalent à des interférences avec un mode vide. Une mauvaise adaptation de modes peut donc formellement se représenter comme l'action d'une lame séparatrice : seule une fraction η_{mod} du signal est transmise, tandis que des fluctuations du vides sont introduites à hauteur de $\sqrt{1-\eta_{mod}^2}$. Précisons enfin que les interférences des modes $\hat{a}_{s,\perp}$ avec des modes vides entrant du côté de l'oscillateur local sont négligées. Avec ce modèle, la différence des photocourants mesurés par chaque voie de la détection s'écrit :

$$\delta\hat{I} = \sqrt{\frac{I_{ol}}{N_0}}\,\left(\sqrt{\eta_{mod}^2}\,X_{s,\phi_{ol}} + \sqrt{1-\eta_{mod}^2}\,X_0\right) \tag{3.16}$$

où X_0 désigne la quadrature du mode vide adapté entrant par l'autre voie de la lame sur le faisceau signal. La différence essentielle entre une inadaptation de modes et des pertes est que dans le cas des pertes l'intensité de l'oscillateur local est diminuée alors qu'elle est inchangée dans le cas de l'adaptation des modes.

Compte tenu de notre modèle de lame fictive et à la vue de l'équation (3.16), pourquoi définir la transmission en intensité de la lame comme η_{mod}^2, ce qui est peut intuitif et peut prêter à confusion ? Le choix de cette notation provient du lien entre η_{mod} et la visibilité des franges d'interférence. En prenant comme champ signal un champ classique de même intensité que l'oscillateur local et qui se décompose au travers de la lame comme indiqué sur la figure 3.4(a), les interférences classiques entre les champs s'écrivent avec $I_s = I_{ol}$:

$$I_\pm = \frac{1}{2}\,(I_{ol} + I_s \pm 2\eta_{mod}|\mathcal{E}_{ol}||\mathcal{E}_s|\cos\varphi) = I_{ol}\,(1 \pm \eta_{mod}\,\cos\varphi) \tag{3.17}$$

La visibilité des franges d'interférences mesurée classiquement sur un bras de la détection fournit directement le paramètre d'adaptation des modes η_{mod}. C'est donc le paramètre utile expérimentalement pour caractériser la qualité du recouvrement des champs. Expérimentalement, la détermination du paramètre η_{mod} utilisera toujours cette méthode de mesure de la visibilité des franges d'interférences classiques, lorsque les faisceaux ont la même intensité.

3.2.4 Excès de bruit de l'oscillateur local

On se propose ici de dériver un calcul quantique sans négliger *a priori* le bruit présent sur le faisceau oscillateur local. Nous introduisons pour cela des notations linéarisées pour le mode de l'oscillateur local, qui se décompose en une composante classique constante $|\mathcal{E}_{ol}|e^{\imath\phi_{ol}}$ plus une composante quantique fluctuante de moyenne nulle $\delta\hat{E}_{ol}$, ce qui revient à considérer l'état de l'oscillateur local comme un état thermique déplacé :

$$\hat{a}_{ol} = |\mathcal{E}_{ol}|e^{\imath\phi_{ol}} + \delta\hat{E}_{ol} \tag{3.18}$$

Les photocourants détectés sur chaque voie s'écrivent alors :

$$\begin{aligned}
\hat{I}_{\pm} = \hat{a}_{\pm}^{\dagger}\hat{a}_{\pm} &= \frac{1}{2}(|\mathcal{E}_{ol}|e^{-\imath\phi_{ol}} + \delta\hat{E}_{ol}^{\dagger} \pm \hat{a}_s^{\dagger})(|\mathcal{E}_{ol}|e^{+\imath\phi_{ol}} + \delta\hat{E}_{ol} \pm \hat{a}_s) && (3.19)\\
&= \frac{1}{2}[|\mathcal{E}_{ol}|^2 + \delta\hat{E}_{ol}^{\dagger}\delta\hat{E}_{ol} + \hat{a}_s^{\dagger}\hat{a} + |\mathcal{E}_{ol}|(e^{-\imath\phi_{ol}}\delta\hat{E}_{ol} + e^{+\imath\phi_{ol}}\delta\hat{E}_{ol}^{\dagger}) && (3.20)\\
&\quad \pm|\mathcal{E}_{ol}|(e^{-\imath\phi_{ol}}\hat{a}_s + e^{+\imath\phi_{ol}}\hat{a}_s^{\dagger}) \pm (\delta\hat{E}_{ol}^{\dagger}\hat{a}_s + \hat{a}_s^{\dagger}\delta\hat{E}_{ol})]
\end{aligned}$$

Lors de la soustraction des photocourants, les intensités moyennes et les termes de la forme $|\mathcal{E}_{ol}|\delta\hat{E}_{ol}$ disparaissent. Par ailleurs, on suppose que le champ signal et les fluctuations $\delta\hat{E}_{ol}$ sont faibles devant l'amplitude de l'oscillateur local, de sorte à pouvoir négliger le terme en $\delta\hat{E}_{ol}^{\dagger}\hat{a}_s$. Dans ce cas, on retrouve pour l'expression de la soustraction des photocourants la formule (3.7) où les fluctuations de l'oscillateur local avaient été négligées. Dans le cadre des fluctuations de l'oscillateur local linéarisables selon (3.18), le bruit de l'oscillateur local n'intervient pas sur le courant en sortie de la détection homodyne.

3.2.5 Conclusion : modèle d'une détection homodyne imparfaite

Une fois la détection équilibrée et limitée au bruit de photon (i.e. sans bruit technique ajouté), les imperfections ont alors trois origines distinctes : la transmission des optiques η_{opt} différente de 100%, l'efficacité quantique limitée η_{phot} des photodétecteurs et enfin une adaptation des modes imparfaite de paramètre η_{mod}. En regroupant formellement tous les termes de modes vides introduits par les imperfections en un mode vide unique $X_{0,imperf}$ équivalent, le signal mesuré en sortie de la détection s'écrit d'après les équations (3.14) et (3.16) :

$$\delta\hat{I} = \sqrt{\frac{\eta_{opt}\eta_{phot}I_{ol}}{N_0}}\left(\sqrt{\eta_{opt}\eta_{phot}\eta_{mod}^2}X_{s,\phi_{ol}} + \sqrt{1-\eta_{opt}\eta_{phot}\eta_{mod}^2}X_{0,imperf}\right) \tag{3.21}$$

Ce qui permet d'identifier le terme d'efficacité globale η_{hom} de la détection homodyne :

$$\boxed{\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2} \tag{3.22}$$

Cette efficacité, qui vaut typiquement 75% expérimentalement, illustre la qualité et l'intérêt d'une détection homodyne pour la mesure d'effets quantiques. Les différentes sources d'imperfections expérimentales seront quantifiées plus précisément dans la suite de ce chapitre. Mais avant cela, passons à la réalisation pratique d'une telle détection.

3.3 Dimensionnement général de la détection

Nous souhaitons utiliser une détection homodyne résolue en temps pour étudier les effets quantiques d'impulsions lumineuses. Ces impulsions seront générées soit par un laser femtoseconde (durée des impulsions : 150 fs) à la cadence de 800kHz, soit par une diode laser modulée (durée des impulsions : 120 ns) à la même cadence de 800 kHz. L'utilisation des impulsions femtoseconde se fera pour la génération d'états non-classiques (partie III), l'application des impulsions nanoseconde sera présentée dans le cadre de l'expérience de cryptographie quantique (II). Pour la description suivante des détections homodynes employées, la source laser sera simplement considérée comme étant une source d'impulsions à la cadence de 800kHz et de durée nettement plus courte que le temps caractéristique de la réponse impulsionnelle de l'électronique de détection. Avant d'aborder la réalisation détaillée des deux prototypes, cette section présente différents points communs entre nos systèmes : spécifications, montage optoélectronique, procédure de réglage, acquisition numérique et calibration.

3.3.1 Cahier des charges

Comme nous l'avons déjà mentionné dans l'introduction de ce chapitre, la mise en œuvre d'une détection homodyne résolue en temps constitue un des défis expérimentaux majeurs de l'exploitation des variables continues. Une détection impulsionnelle satisfaisante doit répondre à l'ensemble des points suivants :

- Large bande passante.
- Excellente réjection entre les voies.
- Très bas niveau de bruit de l'électronique.

Le besoin de résolution temporelle et d'une cadence de répétition élevée impose nécessairement une bande passante étendue, du quasi-continu à plus de la cadence de répétition des impulsions. Notre source laser émettant des impulsions à un taux de 800kHz, il a fallu concevoir un système électronique de bande supérieure au MHz. Pour accéder au niveau du bruit de photon de la détection avec une puissance d'oscillateur local aussi faible que $\mathcal{N}_{ol} = 10^6$ photons par impulsions, soit 0.2 pJ/impulsion à 850nm, il faut obtenir un équilibrage supérieur à $\sqrt{\mathcal{N}_{ol}} / \mathcal{N}_{ol} = 10^{-3}$. Ce critère fixe une borne supérieure à la puissance lumineuse et à la quantité de signal utile. Par ailleurs, le bruit de l'électronique employée doit être très inférieur au signal utile qui est essentiellement le bruit de photon de l'oscillateur local. Pour une puissance d'oscillateur local de $\mathcal{N}_{ol} = 10^6$ photons par impulsions, le bruit de photon intégré sur l'ensemble de la bande passante vaut typiquement $\sqrt{\mathcal{N}_{ol}} = 1000$ photons par impulsion. Il faut donc utiliser des composants de bruit très inférieur à ce niveau, tout en assurant une puissance lumineuse suffisante pour avoir un bon rapport signal à bruit. La plage utile en puissance lumineuse d'oscillateur local doit donc répondre à un compromis en offrant suffisamment de puissance pour émerger du bruit électronique tout en assurant une qualité d'équilibrage satisfaisante.

3.3.2 Montage optoélectronique

Pour assurer la qualité de l'équilibrage, les deux voies de la détection doivent être les plus identiques possible : intensité lumineuse, dimension des faisceaux focalisés, longueur des chemins optiques, position des points de focalisation sur les photodiodes, sensibilité et capacité parasite des photodiodes ... Nous avons donc retenu un montage optique offrant le plus de paramètres de réglages possibles :

- Chaque bras optique est équipé d'un ensemble {lame demi-onde + cube polariseur}. Ces ensembles identiques permettent un équilibrage fin de la puissance lumineuse, en complément de la lame semi-réfléchissante.
- Les longueurs de chemin optique sur chaque bras de la détection sont contrôlés à quelques millimètres près. Le choix d'éléments identiques sur chaque voie permet alors d'assurer simplement la même dimension des faisceaux optiques en amont de la focalisation.
- Chaque lentille de focalisation est positionnée sur une platine de translation. On peut ainsi optimiser indépendamment la dimension de la tache de focalisation.
- Chaque bras comporte au moins deux miroirs réglables afin d'ajuster la position du faisceau selon la dépendance spatiale en sensibilité de la photodiode. Un centrage soigneux permet également de supprimer les effets de fluctuations spatiales du faisceau.

De plus, le montage électronique des photodiodes (Hamamatsu S3883 ou Centronix BPX65) suit les principes suivants :

- Ces photodiodes silicium ont été choisies pour leur rendement quantique élevé, leur temps de réponse court, leur faible niveau de courant d'obscurité et de bruit équivalent NEP.
- Les photodiodes ont été triées pour offrir des caractéristiques optoélectroniques voisines. Chacune est de plus polarisée par une tension ajustable séparément, de sorte à équilibrer les capacités parasites.
- La soustraction des photocourants est réalisée par une application de la loi des nœuds directement en sortie des photodiodes, sans passer par des amplificateurs intermédiaires.
- Les photodiodes sont placées le plus près possible l'une de l'autre pour réduire tout effet induit par un rayonnement parasite.

Le montage optique complet de la détection homodyne est détaillé suivant les applications dans les chapitres 5 ou 7. Le montage électronique utilisé est discuté selon le prototype aux sections 3.4 et 3.5 de ce chapitre.

Procédure de réglage

La liste suivante détaille une proposition de différentes étapes pour achever l'équilibrage de la détection :

1. Au commencement du montage, ajuster la lame séparatrice en incidence pour égaliser au mieux l'intensité des deux voies.
2. Assurer le centrage des points de focalisation sur les photodiodes en observant chaque voie à l'aide d'une caméra CCD (pour obtenir un signal utilisable, il est préférable que les photodiodes soient décapsulées).
3. Egaliser grossièrement les flux avec un puissancemètre en tournant les lames demi-onde placées en amont des cubes polariseurs.
4. Egaliser grossièrement les tensions de polarisation des photodiodes.
5. Ajuster le délai électronique et la synchronisation de la carte sur un maximum de la réponse de la détection (une des voies est masquée pour ce réglage).

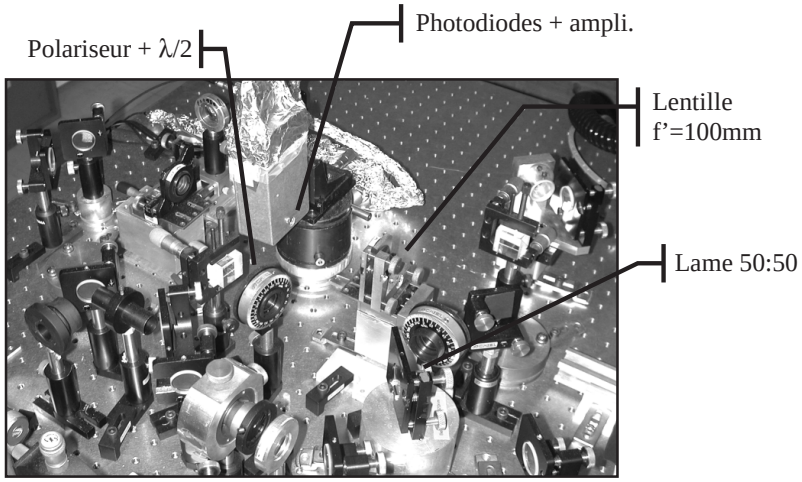

Figure 3.5: *Photographie du montage expérimental.*

6. A l'oscilloscope, visualiser le signal en sortie de la détection et équilibrer les voies en retouchant à l'ajustement des lames demi-onde.

7. Vérifier le centrage du point de focalisation sur la photodiode en retouchant à l'ajustement des miroirs pour maximiser le signal observé à l'oscilloscope sur chaque voie.

8. Parfaire l'équilibrage en retouchant aux tensions de polarisation des photodiodes.

9. Ajuster la focalisation sur les photodiodes en translatant longitudinalement chaque lentille. On peut également faire varier la dimension de la tache de focalisation en translatant simultanément les deux lentilles.

10. Au besoin, retoucher aux réglages de la source laser pour diminuer tout excès de bruit technique (température de la diode laser, réglages de l'électronique du cavity dumper du laser femtoseconde).

Efficacité globale

Comme exposé à la section 3.2.5, l'efficacité globale d'une détection homodyne est le produit de la transmission des optiques η_{opt}, de l'efficacité quantique des photodiodes η_{phot} et du carré de la visibilité des franges d'interférences entre le faisceau signal et l'oscillateur local η^2_{mod}. Suivant les montages, la transmission de l'ensemble des bras de la détection η_{opt} s'échelonne entre 92% et 94%. Les photodiodes ont été privées de leur capsule protectrice et triées pour présenter une efficacité quantique la plus élevée possible. Pour les photodiodes BPX65 utilisées avec la diode laser à 780nm, $\eta_{phot} = 92\%$ tandis que pour les photodiodes S3883 utilisées avec le laser femtoseconde à 850nm $\eta_{phot} = 94.5\%$. Le facteur d'adaptation du mode signal à l'oscillateur local η_{mod} constitue la source prépondérante d'inefficacité dans la détection homodyne. L'utilisation de fibres optiques monomodes dans l'expérience de cryptographie quantique [73] a permis d'obtenir une visibilité jusqu'à $\eta_{mod} = 99\%$, tandis que dans le cas de l'utilisation de notre source femtoseconde, les imperfections du mode spatial n'ont permis d'atteindre au mieux

qu'une visibilité $\eta_{mod} = 93.5\%$ [111] . Le tableau ci-dessous reprend les valeurs typiques pour le calcul de l'efficacité globale de la détection homodyne correspondant à différentes expériences :

Efficacité	**Tomographie du vide**	**Cryptographie cohérente [73]**	**Etats non-gaussiens [128]**
η_{opt}	93%	92%	94%
η_{phot}	94.5%	92%	94.5%
η_{mod}	100%	98%	92%
Total	88%	81%	75%

Acquisition numérique

Pour garantir la résolution temporelle, les signaux en sortie de la chaîne d'amplificateurs de la détection homodyne sont numériquement échantillonnés par une carte d'acquisition rapide *National Instruments* PCI-6111E. Cette carte permet d'acquérir jusqu'à 5 millions de points par seconde, ce qui convient amplement à notre cadence de répétition de 800kHz, tout en introduisant un bruit négligeable (écart-type dû à la carte seule = 0.1 mV à comparer au bruit électronique total = 2mV). En utilisant un gain interne de 50, l'échantillonnage est effectué sur 12 bits dans la plage ±200 mV qui nous servira de référence pour concevoir les étages d'amplification de l'électronique. Enfin, grâce au travail de Frédéric Grosshans, la synchronisation est directement effectuée sur un signal externe provenant du laser, sans passer par l'horloge interne de la carte. Les données sont ensuite récupérées et traitées sous le logiciel *Igor* de la société *Wavemetrics*.

Données techniques pour la carte NiDAQ PCI-6111E	
Entrées analogiques	2 entrées; Résolution 12 bits dans ±10V; Max échantillonnage 5MHz; Impédance 1MΩ + 100 pF; Gain entre 1 et 50; Précision avec un gain de 50 = 0.05mV.
Sorties analogiques	2 sorties; Résolution 16 bits dans ±10V; Max émission 4MHz (1 sortie) ou 2.5MHz (2 sorties); Impédance 50Ω.
Trigger	Entrée PFI7, seuil TTL, impédance 10kΩ.

3.3.3 Procédure de calibration

Afin de vérifier l'équilibrage de la détection et de garantir une limitation au bruit de photon, une procédure de calibration a été mise en œuvre. Cette technique consiste à mesurer la tension en sortie de la détection pour différentes puissances d'oscillateur local, lorsque la voie du signal optique est masquée (vide incident). Si l'équilibrage est réalisé, la mesure fournit le bruit de photon associé à la puissance d'oscillateur local : la variance de bruit augmente donc linéairement avec cette puissance. Par contre, si l'équilibrage est imparfait, un bruit classique s'ajoute et comme nous l'avons vu à la section 3.2.1, la variance de bruit suit une dépendance quadratique avec la puissance de l'oscillateur local.

La même procédure permet d'accéder directement à la calibration quantitative du gain de la détection. En notant R le facteur de conversion de la détection en volts par électrons, la tension en sortie de la détection s'écrit alors :

$$V_{out} = R\,\delta I \tag{3.23}$$

En appliquant l'équation (3.21) au cas du signal vide (variance N_0, adaptation parfaite $\eta_{mod} = 1$) et en tenant compte explicitement des pertes optiques et des inefficacités des photodiodes, la variance de la tension mesurée en sortie de détection équilibrée vaut :

$$\Delta V_{out}^2 = R^2 \, \eta_{opt} \, \eta_{phot} \, \mathcal{N}_{ol} \tag{3.24}$$

où $\mathcal{N}_{ol}$ est le nombre de photons par impulsion de l'oscillateur local. La mesure de la pente de la variance ΔV_{out}^2 en fonction de $\mathcal{N}_{ol}$ permet alors de connaître le gain R, si on a de plus mesuré séparément la transmission des optiques η_{opt} et le rendement quantique des photodiodes η_{phot}.

L'intérêt de cette procédure de calibration est de reposer exclusivement sur la mesure impulsionnelle du bruit de photon, avec des signaux suffisamment faibles pour être dans la plage de linéarité des amplificateurs et en utilisant l'électronique d'acquisition de la carte. Une autre technique possible serait de caractériser le gain de la chaîne en mesurant la réponse de chacune des photodiodes à une impulsion lumineuse donnée, l'autre photodiode tant masquée. On collecterait ainsi un signal suffisant pour une mesure directe à l'oscilloscope, qui fournit également le gain total de la chaîne. Cette méthode a été utilisée comme vérification supplémentaire, mais comme elle ne fonctionne pas exactement dans les mêmes conditions que les mesures quantiques impulsionnelles, la première procédure de calibration lui sera préférée.

3.4 Prototype I : amplificateur de tension

Principe

Le premier prototype de détection homodyne résolue en temps que nous avons réalisé repose sur l'utilisation d'un amplificateur de tension de très bas niveau de bruit *OEI* AH0013, précédemment employé dans notre groupe pour des expériences de mesures quantiques non-destructives [21, 22] et de réduction de bruit des diodes laser [23]. Le schéma électronique de l'ensemble de la détection est présenté sur la figure 3.6. L'amplificateur bas bruit étant opéré en tension, la différence des photocourants qui constitue notre signal est convertie en tension au passage d'une résistance de 4.7 kΩ, puis cette tension est amplifiée une première fois d'un facteur 10 par l'amplificateur *OEI* AH0013 avant d'être à nouveau amplifiée d'un facteur 10 par un second étage d'amplification *Minicircuits* MAR-3SM. Le signal en sortie du deuxième étage est alors dirigé vers l'entrée de la carte *National Instruments* décrite précédemment.

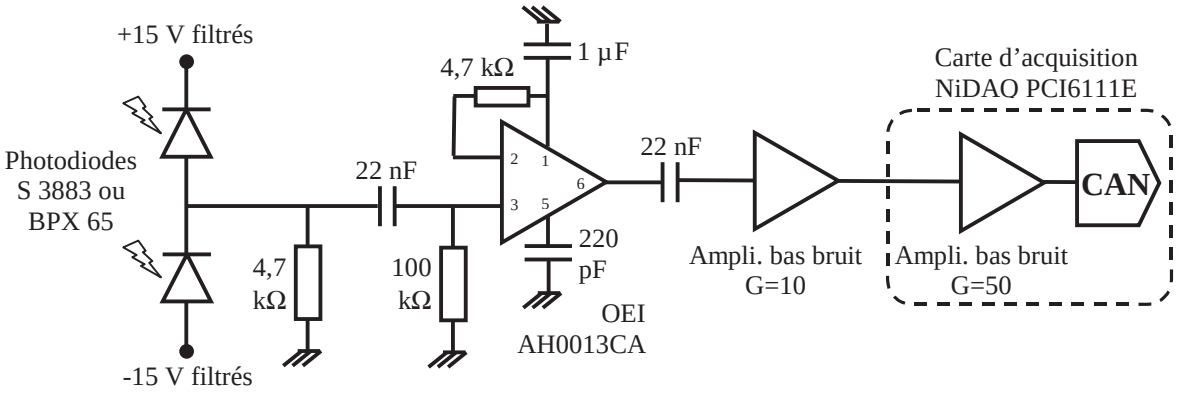

Figure 3.6: *Schéma électronique de la détection à amplification de tension*

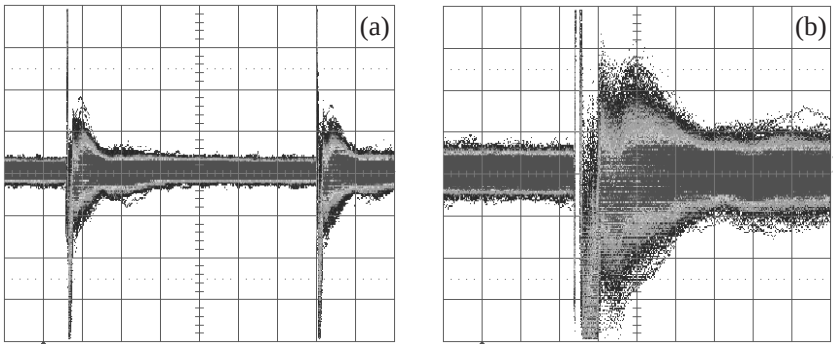

Figure 3.7: *Mesure de bruit à l'oscilloscope pour la détection à amplification de tension. Puissance OL 36 μW, bruit de photon 7.09 mV, bruit électronique 2.13 mV. Echelles : (a) H : 0.2μs/div, V : 20mV/div; (b) H : 50ns/div, V : 10mV/div. (La différence de capacité d'entrée et la persistence à l'oscilloscope tendent à augmenter la hauteur crête-crête du bruit). L'acquisition de la carte est déclenchée sur le maximum de l'impulsion de bruit. Les pics de tension proviennent d'un léger retard entre les réponses temporelles de chaque photodiode, imputable à une faible différence de capacité de l'ordre du pF.*

Le choix de la résistance de charge de 4.7 kΩ a été effectué empiriquement en testant différentes valeurs de résistance. Ce choix doit nécessairement répondre à un compromis. La résistance doit être la plus élevée possible afin de mesurer un signal intense et de garantir un bon rapport entre le signal et le bruit thermique de la résistance. Cette résistance doit aussi ne pas être trop forte, pour ne pas diminuer la bande passante de la détection et conserver la résolution temporelle à 800 kHz.

Calibration

En reprenant la procédure de calibration décrite à la sous-partie 3.3.3, on trace la courbe 3.8, ce qui permet de vérifier la réalisation de l'équilibrage et la limite de la détection au niveau du bruit de photon jusqu'à des puissances d'oscillateur local de $5.3\,10^8$ photons par impulsion, soit une puissance moyenne d'environ 100 μW à 800kHz (l'équilibrage est jugé satisfaisant lorsque la détection ne présente pas d'excès de bruit supérieur à 3% par rapport au bruit de photon attendu). La réjection maximale en variance est introduite par le rapport de la variance de bruit (de photon) sur le signal incident au carré, conformément aux références [35, 34] :

$$10\log\left(\left[\frac{\sqrt{\mathcal{N}_{ol,max}}}{\mathcal{N}_{ol,max}}\right]^2\right) = -10\log\mathcal{N}_{ol,max} \tag{3.25}$$

où $\mathcal{N}_{ol,max}$ est le nombre maximum de photons par impulsion d'oscillateur local pour lequel le critère d'équilibrage est réalisé. Dans le cas de la détection à amplification de tension $\mathcal{N}_{ol,max} = 5.3\,10^8$ photons/impulsion et la réjection maximale vaut alors 87.2 dB. La pente de la courbe 3.8 permet également selon (3.24) de caractériser le gain total de la détection en microvolts par électron :

$$\boxed{R_{Dét1} = 0.54 \pm 0.01\ \mu V/e} \tag{3.26}$$

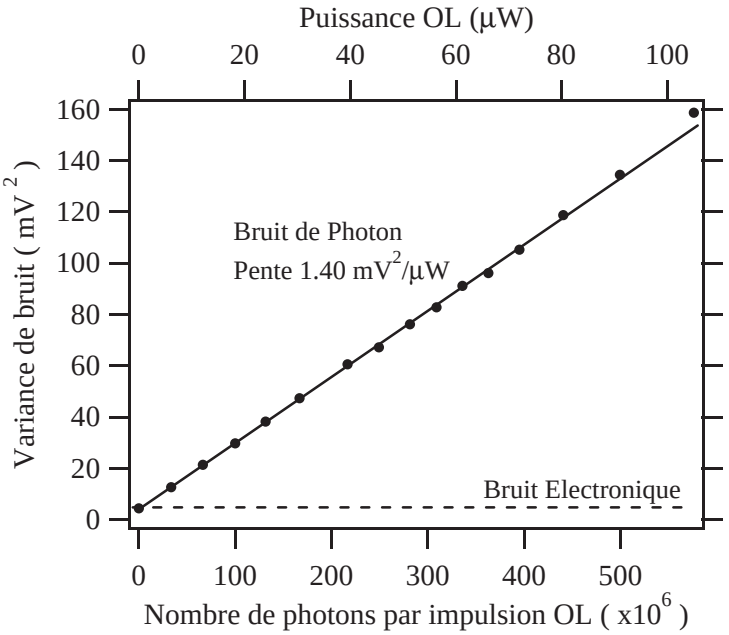

Figure 3.8: *Variance de bruit de la détection à amplification de tension en fonction de la puissance de l'oscillateur local.*

Données techniques pour la détection à amplification de tension	
Photodiodes BPX65	Centronix / Siemens; Silicium λ_{peak} 850nm; surface 1mm^2; efficacité quantique mesurée à 780nm 92%, efficacité quantique mesurée à 850nm 94%; courant d'obscurité 1nA, NEP $3.3\,10^{-14}W/\sqrt{\text{Hz}}$; Capacité à 20V 2.5pF
Photodiodes S3883	Hamamatsu; Silicium λ_{peak} 840nm; surface 1.7mm^2; efficacité quantique mesurée à 850nm 94.5%; courant d'obscurité 0.05nA, NEP $6.7\,10^{-15}W/\sqrt{\text{Hz}}$; Capacité à 20V 6pF.
Ampli. de tension	OEI AH0013. Gain en tension $\times$10 à 800kHz; Bande passante max 100MHz; Bruit $2\text{nV}/\sqrt{\text{Hz}}$; slew-rate $400\text{V}/\mu\text{s}$; polarisation +15V.
Second étage	Minicircuits MAR-3SM Gain en tension $\times$10 à 800kHz; Bande passante max 2GHz; polarisation +15V.
Détection complète	Gain 0.54 μV/e; Bande passante 6.5MHz;
Réjection	Equilibrage $P_{ol} = 5.3\,10^8$ photons/impulsion à 800kHz, soit une puissance moy. de 100 μW; Réjection 87.2 dB.
Bruit élec.	Ecart-type 2.1mV, soit 3900 électrons RMS par impulsion.
Signal / bruit	Pour $P_{ol} = 36\mu$W, bruit de photon 7.1mV, bruit élec. 2.1mV; rapport signal à bruit en variance 11.4 (10.6dB)

Bruit électronique

La valeur typique de l'écart-type de bruit électronique de la détection à amplification de tension est de 2.1 mV mesurés avec la carte d'acquisition, soit 3900 électrons de bruit équivalent en

entrée (d'après la notation introduite dans [35]). Plusieurs sources de bruit contribuent à ce bruit électronique, mais l'origine prédominante du bruit est le bruit thermique de la résistance de charge de 4.7 kΩ. L'écart-type de bruit thermique de la résistance (en courant) est donné par la formule de Johnson-Nyquist : $\sigma I_R = \sqrt{4k_B T \Delta f / R_L}$. Pour la largeur spectrale utilisée $\Delta f = 6.5 MHz$, on obtient pour $R_L = 4.7$ kΩ, $\sigma I_R \backsimeq 4.8$ nA soit en sortie de la chaîne amplificatrice $\sigma V_{R,out} \backsimeq 100\, R_L\, \sigma I_R \backsimeq 2.2$ mV, ce qui correspond sensiblement au bruit électronique mesuré. Parmi les autres sources (négligeables) de bruit, on peut citer le courant d'obscurité des photodiodes (0.05 nA pour les S3883) ou la puissance de bruit équivalente NEP (S3883 : $NEP = 6.7\,10^{-15} W/\sqrt{\text{Hz}}$ soit un courant de bruit au niveau des photodiodes de 0.01 nA pour une plage de 6.5 MHz). Le bruit de l'amplificateur *OEI* est de 2 nV/$\sqrt{\text{Hz}}$, soit en sortie de la détection un bruit de 50 μV.

3.5 Prototype II : amplificateur de charge

Principe

Pour réduire le niveau de bruit électronique de notre détection homodyne à amplification de tension, il est tentant de retirer la source principale de bruit, c'est-à-dire la résistance de charge en sortie des photodiodes. Sans cette résistance, les charges ne sont cependant pas converties en tension, et il faut alors utiliser un premier étage amplificateur de charges. Cet étage est réalisé par un amplificateur *Amptek* A250 spécifiquement conçu pour l'amplification bas bruit de très faibles courants. Le schéma de principe de ce système de détection s'inspire largement du travail de Hauke Hansen et de ses collaborateurs à l'université de Constance [35, 34, 30].

Le schéma électronique utilisé pour le second prototype de détection homodyne, à base d'amplification de charge, est présenté sur la figure 3.9. La différence de photocourants en sortie des photodiodes est collectée par un condensateur de capacité 470 pF nettement plus grande que la capacité des photodiodes *Hamamatsu* S3883 (6 pF). Pour éviter une saturation du condensateur dans le cas d'un mauvais équilibrage, le condensateur est mis à la masse à travers une résistance de forte résistivité (10 MΩ). La différence des photocourants est ensuite amplifiée d'un gain de 0.16μV/e par un premier étage formé de l'amplificateur *Amptek* A250 associé à un transistor FET 2SK152. En sortie de ce premier étage, le signal suit la cadence des impulsions avec des sauts de tension de temps de montée 6 ns et avec une décroissance lente de temps caractéristique 300 μs (voir la figure 3.10(a)). Cette décroissance lente est réduite par un étage dérivateur à une durée plus courte de 100 ns. Ces impulsions sont ensuite amplifiées d'un facteur 40 par un amplificateur opérationnel *Maxim* MAX4107 (voir les figures 3.10(b) et (c)).

Calibration

De la même manière que pour la détection précédente, on trace la courbe 3.12 de la variance de bruit en fonction de la puissance de l'oscillateur local. L'équilibrage pour la détection à amplification de charge est réalisé avec un excès de bruit de moins de 3% jusqu'à des puissances d'oscillateur local de $2.1\,10^8$ photons par impulsion, soit une puissance moyenne d'environ 40 μW à 800kHz. La réjection maximale en variance vaut alors 83.2 dB. La pente de la courbe 3.12 permet enfin d'accéder au gain total de la détection en microvolts par électron :

$$\boxed{R_{Dét2} = 2.24 \pm 0.04\ \mu V/e} \tag{3.27}$$

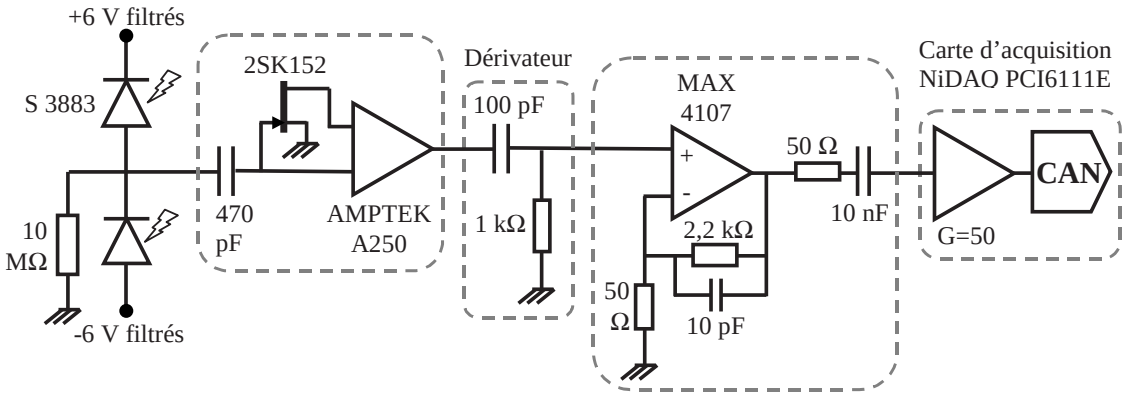

Figure 3.9: *Schéma électronique de la détection à amplification de charge*

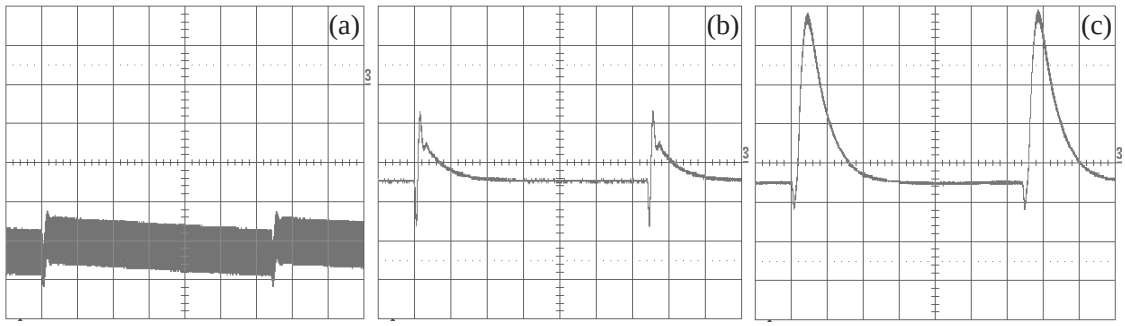

Figure 3.10: *Réponse de la détection à amplification de charge à un déséquilibre des voies. (a) sortie de l'amplificateur de charge, H : 0,2 µs/div, V : 200 mV/div; (b) sortie du dérivateur, H : 0,2 µs/div, V : 50 mV/div; (c) sortie du second amplificateur, H : 0,2 µs/div, V : 500 mV/div.*

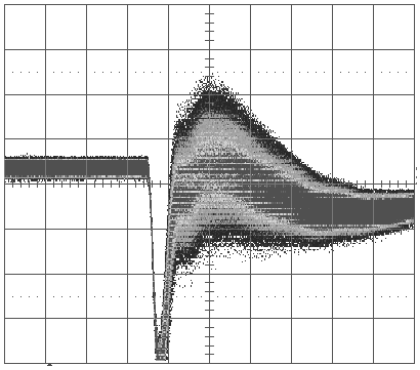

Figure 3.11: *Bruit à l'oscilloscope pour la détection à amplification de charge. Puissance OL 36 µW, bruit de photon 31 mV, bruit électronique 1.9 mV. Echelle H : 50ns/div, V : 50mV/div.*

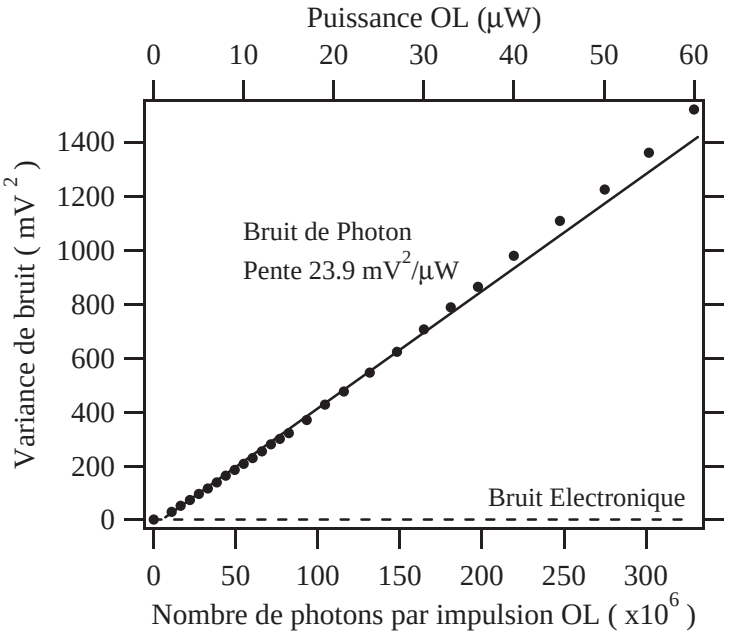

Figure 3.12: *Variance de bruit de la détection à amplification de charge en fonction de la puissance de l'oscillateur local.*

Données techniques pour la détection à amplification de charge	
Photodiodes S3883	Hamamatsu; Silicium λ_{peak} 840nm; surface 1.7mm^2; efficacité quantique mesurée à 850nm 94.5%; courant d'obscurité 0.05nA, NEP $6.7\,10^{-15} W/\sqrt{\text{Hz}}$; Capacité à 6V 6pF.
Ampli. de charge	Amptek A250 avec FET 2SK152; Gain 0.16μV/e; Bruit $\backsimeq$200e RMS; temps de montée 6ns, temps de descente 300μs; impédance de sortie 100Ω; polarisation $\pm$6V.
Second étage	Maxim MAX4107; Gain en tension $\backsimeq$40; Bruit $0.75\text{nV}/\sqrt{\text{Hz}}$; temps de montée/descente $<$ 6ns; slew-rate 500V/μs; polarisation $\pm$5V.
Détection complète	Gain 2.24 μV/e; Bande passante 10MHz;
Réjection	Equilibrage $P_{ol} = 2.1\,10^8$ photons/impulsion à 800kHz, soit une puissance moyenne de 40 μW; Réjection 83.2 dB.
Bruit élec.	Ecart-type 1.9mV, soit 850 électrons RMS par impulsion.
Signal / bruit	Pour $P_{ol} = 36\mu$W, bruit de photon 31mV, bruit élec. 1.9mV; rapport signal à bruit en variance 266 (24.3dB)

Bruit électronique

La meilleure valeur obtenue de l'écart-type de bruit électronique pour la détection à amplification de charge est de 1.9 mV, soit 850 électrons de bruit équivalent en entrée par impulsion. A nouveau, le bruit intrinsèque des photodiodes est négligeable (quelques picoampères, à comparer aux nanoampères du bruit de photon), de même que le bruit introduit par l'étage MAX4107.

Suivant la documentation du constructeur, l'amplificateur de charge *Amptek* associé au transistor 2SK152 devrait idéalement présenter un bruit de l'ordre de 200 électrons RMS pour notre bande passante d'environ 10 MHz. La seconde source importante de bruit est le bruit thermique de la résistance de 10 MΩ de mise à la terre. Ce courant de bruit vaut $\sigma I_R = \sqrt{4k_B T \Delta f / R_L} = 0.3$ nA, et correspond à une charge équivalente de bruit d'environ 200 électrons par réponse impulsionnelle. La différence entre ces bruits théoriques et le niveau de bruit expérimental peut s'expliquer par des effets de rayonnements parasites induits ainsi que par une modélisation théorique trop simplifiée.

3.6 Conclusion

Grâce aux interférences optiques avec un champ intense de référence, le système de détection homodyne permet de mesurer efficacement un champ incident très faible et d'accéder au domaine des fluctuations quantiques. Avec une électronique rapide garantissant une résolution temporelle, la détection homodyne impulsionnelle permet simplement d'accéder à une mesure de la quadrature en phase avec le champ de référence *pour chaque impulsion incidente*. Ceci permet en particulier une utilisation pour des protocoles de communication quantique, mais est également applicable à d'autres domaines de l'optique, comme par exemple la microscopie de haute sensibilité.

La principale difficulté d'un tel système réside dans l'équilibrage fin entre les voies. Nous sommes parvenus à dépasser ces difficultés techniques pour réaliser une détection résolue en temps fonctionnant à une cadence de 800kHz, équilibrée au-delà de 200 millions de photons par impulsion d'oscillateur local et présentant un rapport signal à bruit de 10 à 20 dB. Cette détection constitue l'élément clé de notre dispositif expérimental pour la mise en œuvre de protocoles de communication quantique avec des variables continues.

Partie II

Système de cryptographie quantique avec des impulsions cohérentes

Chapitre 4

Protocoles théoriques de cryptographie quantique avec des états cohérents

Sommaire

Introduction à la cryptographie quantique

La cryptographie quantique utilise les propriétés quantiques de la lumière pour protéger efficacement la transmission d'un message secret. En tentant d'obtenir des informations sur un signal envoyé au travers d'un canal quantique adéquat, un espion introduira nécessairement des perturbations sur le message quantique, perturbations qui pourront ensuite être décelées par le destinataire officiel. Il est alors possible de savoir si la ligne de transmission a été espionnée, et quelle quantité d'information a pu être obtenue par l'espion. Si les partenaires officiels (traditionnellement appelés Alice et Bob) possèdent davantage d'information que l'espion (désigné par le nom d'Eve), des procédés d'algorithmique classique permettent alors de supprimer toute connaissance que l'espion a pu obtenir pour ne conserver qu'un message utile parfaitement secret entre Alice et Bob.

Deux points sont essentiels pour la cryptographie quantique. Le premier est que l'information quantique ne peux pas être parfaitement copiée, au contraire de l'information classique (théorème

de non-clonage quantique [78]). S'il est possible de copier imparfaitement un état quantique, la physique quantique fixe cependant des limites strictes à la qualité des copies d'après le principe d'incertitude d'Heisenberg. Le second point essentiel est que le signal secret qu'échangent Alice et Bob au travers du canal quantique ne contient pas d'information pertinente en lui-même, mais est une succession de chiffres binaires servant a posteriori de clé pour encoder le message réel, suivant un système de cryptographie à clé secrète ou code de Vernam (*one-time pad*) [2, 39].

Dans un tel système à code de Vernam, le message utile est chiffré grâce à une clé secrète connue exclusivement par Alice et Bob, puis ce message codé est ouvertement transmis par un canal public au destinataire. Seul ce dernier peut décrypter le message, puisqu'il est le seul à connaître la clé adéquate. Si la clé est d'entropie supérieure ou égale à l'entropie du message et si elle n'est utilisée qu'une seule fois, Shannon a démontré explicitement que le code de Vernam est alors parfaitement sûr [41]. Tout le problème réside dans la transmission de cette clé aléatoire secrète, qui doit être aussi longue que le message et changée à chaque nouvelle transmission. C'est à ce niveau qu'intervient la cryptographie quantique, plus précisément appelée *distribution quantique de clé secrète*. L'avantage décisif d'un dispositif de cryptographie quantique est que la sécurité repose sur des principes physiques et peut être rigoureusement prouvée, au contraire des protocoles de cryptographie classique (RSA, DES, AES...) qui reposent tous sur des conjectures mathématiques et sur des limitations technologiques supposées des capacités de l'espionnage. Un deuxième avantage décisif pour la cryptographie quantique est que l'espionnage peut être non seulement décelé, mais également quantifié, en fixant une limite supérieure à la quantité d'information dont dispose au mieux un espion potentiel d'après les lois de la physique quantique.

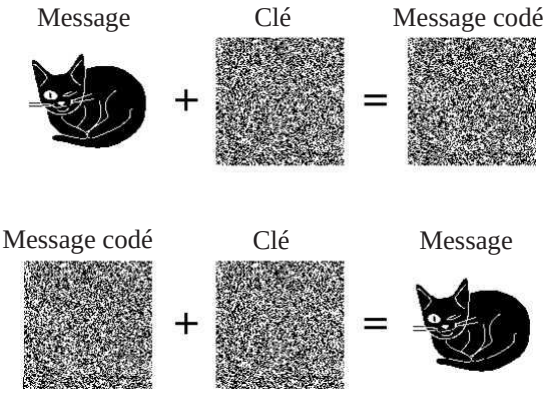

Figure 4.1: *Application bidimensionnelle du code de Vernam (one-time-pad) pour les processus de codage (haut) et de décodage (bas), d'après Gilles Van Assche.*

Variables discrètes et variables continues

Depuis la première proposition explicite de cryptographie quantique par Bennett et Brassard en 1984 [43], l'essentiel des protocoles de cryptographie quantique existants repose sur l'utilisation de variables discrètes codées sur des photons uniques (d'unicité plus ou moins approximative). Ces protocoles ont connu de rapides et brillants développements théoriques et expérimentaux, fixant les limites actuelles à des transmissions jusqu'à 101 km dans une fibre optique et 23.5 km en espace libre, avec des taux nets de transfert allant de quelques dizaines à quelques milliers de bits secrets par seconde (pour une vue d'ensemble de ce domaine, voir la référence [40]).

L'utilisation de photons uniques n'est cependant pas indispensable à la cryptographie quantique. Une condition minimale pour la sécurité quantique est de disposer de deux états non-orthogonaux, donc non parfaitement discernables lors de mesures [46]. L'utilisation des variables quantiques continues offre une alternative intéressante à l'exploitation des variables discrètes, qui sont basées sur des techniques de comptage de photons. En effet, les variables continues permettent d'envisager l'utilisation d'états quantiques intenses comportant un grand nombre de photons, plus simples à produire et à mesurer que des photons uniques. Un second avantage inhérent aux variables continues est que cette technique permet d'atteindre de hauts niveaux de débits, en transmettant plusieurs bits secrets par impulsions à une cadence de répétition élevée.

Entre la première proposition de Tim Ralph en 1999 et le début de nos travaux en juillet 2001, de nombreux protocoles théoriques exploitant les variables continues ont été proposés [61, 62, 63, 64, 65, 66, 67, 68, 69]. Tous possèdent la particularité de reposer sur des états spécifiquement quantiques de la lumière : états intriqués ou états comprimés. Frédéric Grosshans et Philippe Grangier ont cependant démontré dans [70] que l'utilisation de tels états spécifiquement quantiques n'est pas indispensable, et qu'un niveau de sécurité équivalent peut être atteint tout en utilisant des états quasi-classiques du champ lumineux.

Ce chapitre se concentre sur les procédés de transfert de clés secrètes par échange d'états cohérents, utilisés lors de l'expérience de cryptographie quantique présentée au chapitre 5. Le cas le plus général utilisant des états comprimés ou des états intriqués sera abordé lors du chapitre 6. L'étude théorique de ces différents protocoles a été essentiellement menée par Frédéric Grosshans lors de ses travaux de thèse [71]. Le chapitre présent a pour vocation essentielle de présenter succinctement les résultats majeurs obtenus par Frédéric Grosshans et Philippe Grangier, à qui reviennent tous les mérites de l'invention de ces protocoles. De nombreux détails supplémentaires se trouveront dans le manuscrit [71] ainsi que dans les articles [70, 73, 74, 75].

Plusieurs résultats majeurs pour la cryptographie quantique avec des états cohérents seront démontrés au cours de ce chapitre :

- Il est possible de concevoir un protocole de cryptographie quantique sûr avec des états quasi-classiques.
- De hauts débits de transfert peuvent être atteints avec des variables continues.
- Une clé secrète peut être théoriquement échangée à travers un canal de transmission arbitrairement faible grâce au processus de réconciliation inverse.

4.1 Présentation générale des protocoles

4.1.1 Transfert quantique de clé secrète avec des états cohérents

Le principe général de nos protocoles à états cohérents [70, 73] repose sur l'échange quantique de données variant continûment suivant des distributions gaussiennes, puis sur le traitement classique de ces données pour en extraire une clé secrète binaire.

Dans une première étape, Alice choisit deux nombres $\overline{X}_A, \overline{P}_A$ dans une distribution gaussienne de variance $V_A N_0$ ($V_A \gg 1$) puis elle envoie à Bob l'état cohérent de quadratures centrées sur $(\overline{X}_A, \overline{P}_A)$. Au niveau d'Alice, ceci revient à envoyer des impulsions cohérentes modulées dans l'espace des phases suivant une distribution gaussienne classique bidimensionnelle de variance $V_A N_0$ (voir la figure 4.2). Du côté de la réception, Bob choisit aléatoirement pour chaque impulsion d'effectuer une mesure homodyne soit de la quadrature X, soit de la quadrature P. Après un grand nombre d'échange d'états cohérents, Bob informe ensuite publiquement Alice de

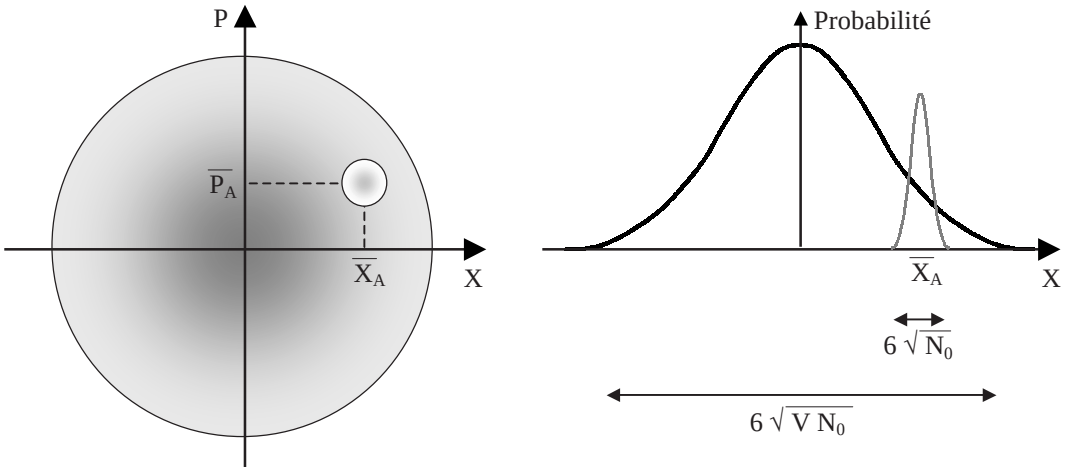

Figure 4.2: *Modulation d'Alice pour un protocole à états cohérents. $V = V_A + 1$ désigne la variance totale de la modulation d'Alice (incluant le bruit de photon des états cohérents émis), prise en unités de bruit quantique standard.*

son choix de direction de mesure pour chaque impulsion, de telle sorte qu'Alice puisse sélectionner l'information en quadrature qu'elle partage avec Bob et négliger le reste. A la fin de cette étape, Alice et Bob (et l'espion potentiel Eve) disposent d'un ensemble de variables continues corrélées qui suivent des distributions gaussiennes. Ces valeurs sont appelées "éléments de clé".

Un traitement classique de l'information commune aux partenaires est alors nécessaire pour extraire une clé parfaitement secrète. Dans une deuxième étape, Alice et Bob comparent publiquement un sous-ensemble de leurs valeurs respectives choisies aléatoirement. Ils obtiennent ainsi une évaluation représentative de la transmission de la ligne et du taux d'erreur induit par le canal quantique. A partir des corrélations entre les valeurs révélées, Alice et Bob peuvent déduire la quantité d'information qu'ils partagent $I_{AB} = I_{BA}$. Ils peuvent également déceler d'après la quantité de perturbation introduite si le canal quantique a été espionné. Enfin, grâce au formalisme quantique développé ci-après, Alice et Bob peuvent fixer une limite supérieure à la quantité d'information espionnée. L'information dont dispose Eve sur le valeurs d'Alice est notée I_{AE}, celle commune à Eve et Bob est I_{BE}. En cryptographie classique, le théorème de Csiszar-Körner [50] repris par Maurer [51], stipule qu'il est possible d'extraire une clé secrète de dimension $\mathcal{S}$ à la condition suffisante :

$$\boxed{\mathcal{S} > \max(I_{AB} - I_{AE}, I_{BA} - I_{BE})} \tag{4.1}$$

Cette possibilité d'extraction de clé secrète repose exclusivement sur une communication classique authentifiée et uni-directionnelle entre Alice et Bob. Connaissant les estimations de I_{AB}, I_{AE} et I_{BE}, Alice et Bob peuvent calculer la quantité $\max(I_{AB} - I_{AE}, I_{BA} - I_{BE})$. Si cette valeur est négative, l'espion dispose de trop d'information pour qu'une communication sûre soit possible. Alice et Bob arrêtent alors l'échange. Par contre, si les partenaires disposent d'un avantage sur l'espion, il peuvent extraire une clé binaire secrète des variables continues.

Dans une troisième étape appelée "réconciliation", Alice et Bob utilisent des algorithmes classiques pour extraire une chaîne binaire commune à partir de leurs éléments de clé, tout en révélant le moins d'information possible à un espion potentiel. Cette étape a été adaptée au cas des variables gaussiennes continues par l'équipe de Nicolas Cerf [56] dans une procédure appelée

"réconciliation par tranches" qui combine l'extraction de données binaires et la correction des erreurs présentes dans ces données. Cette procédure a été décrite à la section 1.3 du chapitre 1 et sera discutée dans le cas de la cryptographie à la sous-section suivante. Elle permet notamment d'extraire quasiment toute l'information utile des éléments de clé pour accéder à la quantité d'information mutuelle selon la formule de Shannon.

Pour obtenir une clé finale connue d'eux seuls, Alice et Bob doivent supprimer toute information résiduelle que conserverait l'espion sur la clé. Cette quatrième et dernière étape est effectuée par un processus classique appelé "amplification de confidentialité" [54], qui réalise des opérations binaires entre les éléments des chaînes d'Alice et Bob. Eve n'a alors pas d'autre choix que d'effectuer les mêmes opérations, mais puisqu'elle dispose de moins d'information, ses incertitudes sur les valeurs des bits vont se propager à l'ensemble des bits de clé pour supprimer en fin de compte toute l'information dont elle disposait. L'amplification de confidentialité est efficacement réalisée par des algorithmes classiques, au prix d'une clé finale de dimension réduite. Cette opération étant néanmoins relativement consommatrice en nombre de bits, il faut disposer au préalable d'une borne stricte à la quantité d'information espionnée I_{AE} ou I_{BE}, ce qui constitue un point crucial de notre étude.

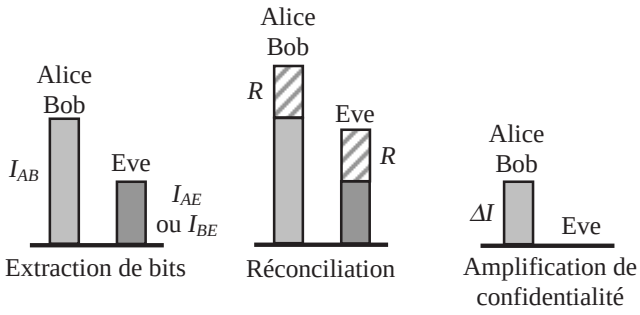

Figure 4.3: *Représentation intuitive de l'évolution des informations lors de la cryptographie quantique. Après l'extraction de bits, Alice et Bob partagent des informations, mais ces données présentent des erreurs. La réconciliation fournit l'information $\mathcal{R}$ pour corriger les erreurs entre Alice et Bob. Eve, qui espionne toutes les communications, obtient elle aussi sensiblement la même quantité d'information supplémentaire. Enfin, l'amplification de confidentialité permet de supprimer toute la connaissance d'Eve pour ne conserver qu'une clé plus courte, mais parfaitement secrète.*

Les protocoles présentés dans ce chapitre supposent que les canaux de transfert d'information soient authentifiés, c'est-à-dire qu'Alice soit sûre de parler à Bob et non pas à un espion qui se ferait passer pour Bob. Cette vérification est efficacement réalisée par des protocoles classiques spécifiques à partir d'une courte clé secrète au préalable connue par Alice et Bob. Il faut bien distinguer la différence entre une attaque globale (ici interdite) des canaux quantiques et classiques où l'espion se fait respectivement passer pour un des partenaires autorisés, et une attaque de type "*intercept-resend*" (prise en compte dans nos calculs) où l'espion se place sur le canal quantique entre Alice et Bob, mesure les impulsions d'Alice et renvoie d'autres états à Bob.

Par ailleurs, du fait de la résolution temporelle impulsion par impulsion du protocole, il est très simple de caractériser ces échanges en terme d'information de Shannon. Le choix d'une modulation gaussienne est en partie alors dictée par le fait qu'une loi gaussienne maximise l'entropie de Shannon à variance fixée et permet ainsi un débit maximum d'information.

4.1.2 Comment réconcilier Alice et Bob ?

Deux options sont principalement utilisées pour effectuer la correction d'erreurs ou réconciliation, suivant que la procédure utilise les bits d'Alice (réconciliation directe) ou ceux de Bob (réconciliation inverse) pour former la clé finale.

Réconciliation directe

Dans une procédure de réconciliation directe, Alice envoie des données de correction à Bob, qui corrige ses erreurs pour avoir les mêmes valeurs qu'Alice. Alice fait une estimation de la quantité d'information $\mathcal{R}$ qu'elle doit révéler à partir de sa connaissance des corrélations Alice-Bob. Si le processus a été parfait, Alice et Bob disposent après corrections de $I_{AB} + \mathcal{R}$ bits d'information commune, tandis que Eve en connaît $I_{AE} + \mathcal{R}$. Un protocole à réconciliation directe permet un échange de clé secrète à la condition $I_{AB} - I_{AE} > 0$. Ce processus est appelé "réconciliation directe", car Bob reconstitue la clé initialement choisie par Alice. Le flux d'information de correction suit ici la même direction que l'information quantique.

La réconciliation directe est relativement intuitive, et a été utilisée dans les premières propositions de cryptographie quantique avec des variables continues [70]. Cependant, cette technique ne fonctionne plus dès lors que la transmission du canal quantique est inférieure à 50% (pertes > 3 dB). Dans ce cas, l'espion pourrait théoriquement accéder à plus de la moitié du faisceau émis par Alice et donc extraire davantage d'information que Bob ($I_{AE} > I_{AB}$), ce qui interdit toute communication sécurisée comme nous le démontrerons à la section 4.2.

Réconciliation inverse

Dans une procédure de réconciliation inverse, le flux d'information de correction est inversé par rapport à la direction du flux d'information quantique. Dans ce cas, Bob envoie des données de correction à Alice, qui modifie ses valeurs pour obtenir les mêmes que Bob. D'une certaine manière, Alice va copier les erreurs mesurées par Bob. Les éléments de la clé finale seront donc différents de ceux initialement choisis par Alice. Ceci est absolument sans importance, la clé finale ne contient pas d'information pratique mais sert uniquement à coder le message. Seul importe qu'à la fin du processus Alice et Bob disposent d'une chaîne de bits commune et connue d'eux seuls. Bob effectue donc une estimation de la quantité d'information $\mathcal{R}$ à révéler. Si le processus a été parfait, Alice et Bob disposent après corrections de $I_{BA} + \mathcal{R}$ bits d'information commune, tandis que Eve en connaît $I_{BE} + \mathcal{R}$. Un protocole à réconciliation inverse parfait conserve la quantité $I_{BA} - I_{BE}$ et permet un échange secret à la condition $I_{BA} - I_{BE} > 0$.

L'inversion de la direction de la réconciliation confère toujours un avantage à Alice et Bob sur un espion potentiel, ce qui autorise en théorie des transmissions pour des pertes arbitrairement élevées. Une explication intuitive de cette affirmation réside dans le fait qu'il est toujours plus difficile à un espion de connaître le bruit mesuré par Bob que d'estimer la modulation d'Alice. Nous examinerons ce point plus spécifiquement à la section 4.3, après une première étude des protocoles à réconciliation directe.

4.2 Protocoles directs

Dans un premier temps, nous nous limitons au cas des attaques individuelles et gaussiennes de l'espion : l'espion possède toute liberté pour effectuer des opérations quantiques gaussiennes sur chaque état pris individuellement [70, 73]. Le cas plus général des attaques quelconques sur un ensemble de plusieurs états sera abordé dans la partie 4.3.4.

4.2.1 Echange d'états quantiques et transfert d'information

Le canal quantique gaussien peut être modélisé par les relations suivantes, analogues de celles utilisées dans le cadre des mesures quantiques non destructives [21, 22] :

$$X_B = \sqrt{G_X}\,(\,\overline{X}_A + \delta X_A + N_{X,B}\,) \qquad\qquad P_B = \sqrt{G_P}\,(\,\overline{P}_A + \delta P_A + N_{P,B}\,) \tag{4.2}$$

où $G_{X,P}$ est la transmission de la ligne pour les quadratures X ou P. $\overline{X}_A$,$\overline{P}_A$ sont les valeurs classiques de modulation [1] choisies par Alice suivant une loi gaussienne centrée de variance $\langle \overline{X}_A{}^2 \rangle = \langle \overline{P}_A{}^2 \rangle = V_A\, N_0$. Lors de l'envoi d'un état cohérent centré sur $(\overline{X}_A, \overline{P}_A)$, le bruit de photon N_0 est pris en compte par des termes de fluctuations quantiques en sortie de la source $\delta X_A, \delta P_A$ de valeur moyenne nulle et de variance égale au bruit quantique : $\langle \delta X_A{}^2 \rangle = \langle \delta P_A{}^2 \rangle = N_0$. L'état cohérent modulé en sortie de la source d'Alice est ainsi donné par le couple d'opérateurs $(\overline{X}_A + \delta X_A, \overline{P}_A + \delta P_A)$. Enfin, le bruit équivalent en entrée pour les quadratures détectées rajouté par le canal est noté par les variables quantiques $N_{X,B}$, $N_{P,B}$. Ce bruit additif est supposé gaussien de moyenne nulle et de variances respectives notées $\langle N_{X,B}{}^2 \rangle = \chi_{X,B}\, N_0$, $\langle N_{P,B}{}^2 \rangle = \chi_{P,B}\, N_0$. Les perturbations induites par la ligne étant indépendantes de la source d'Alice, le bruit ajouté en ligne est donc non corrélé au signal : $\langle (\overline{X}_A + \delta X_A) N_{X,B} \rangle = \langle (\overline{P}_A + \delta P_A) N_{P,B} \rangle = 0$.

Comme la modulation d'Alice est symétrique et comme Bob effectue un choix aléatoire de mesure entre les quadratures X et P, la meilleure attaque d'Eve devra nécessairement conserver la symétrie entre les quadratures. On peut donc considérer simplement le cas parfaitement symétrique, soit $G_X = G_P = G$ et $\chi_{X,B} = \chi_{P,B} = \chi_B$. Les déviations expérimentales à cette symétrie devront néanmoins être prises en compte par des estimations statistiques.

Dans ces conditions, la variance mesurée au niveau de Bob s'écrit :

$$V_B\, N_0 = G\,(V_A + 1 + \chi_B)\, N_0 = G\,(V + \chi_B)\, N_0 \tag{4.3}$$

en posant dans la dernière égalité $V = V_A + 1$ la variance totale de la modulation en sortie d'Alice prise en unité de bruit de photon. D'après le théorème de Shannon (1.21), l'information mutuelle entre Alice et Bob s'écrit alors (les répartitions en quadrature sont symétriques) :

$$\begin{aligned} I_{AB} = I_{BA} &= \frac{1}{2}\log_2\left(1 + \frac{\langle \overline{X}_A{}^2 \rangle}{\langle (\delta X_A + N_{X,B})^2 \rangle}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{V_A}{1+\chi_B}\right) \end{aligned} \tag{4.4}$$

Cette formule montre que des taux de transferts à plus d'un bit par symbole ($I_{AB} > 1$) sont facilement atteignables avec des variables continues. Associée à une cadence de répétition de symboles élevée, cette propriété permet d'atteindre de hauts débits de transmission avec des états cohérents, comme nous le démontrerons expérimentalement au chapitre 5.

Si la théorie de l'information de Shannon indique qu'Alice et Bob partagent une quantité d'information I_{AB}, cette théorie n'indique cependant pas de méthode explicite pour atteindre ce niveau d'information. Grâce à la procédure de réconciliation par tranches décrite dans [56] ainsi qu'à la section 1.3, nos protocoles peuvent atteindre sensiblement l'information de Shannon I_{AB}. Cette procédure est absolument indispensable à la mise en œuvre de nos protocoles.

[1] Au cours de ce manuscrit, la barre verticale sur les variables désigne des termes classiques, pouvant être parfaitement déterminés. Cela permet de distinguer ces variables des quadratures quantiques affectées par la relation d'incertitude d'Heisenberg.

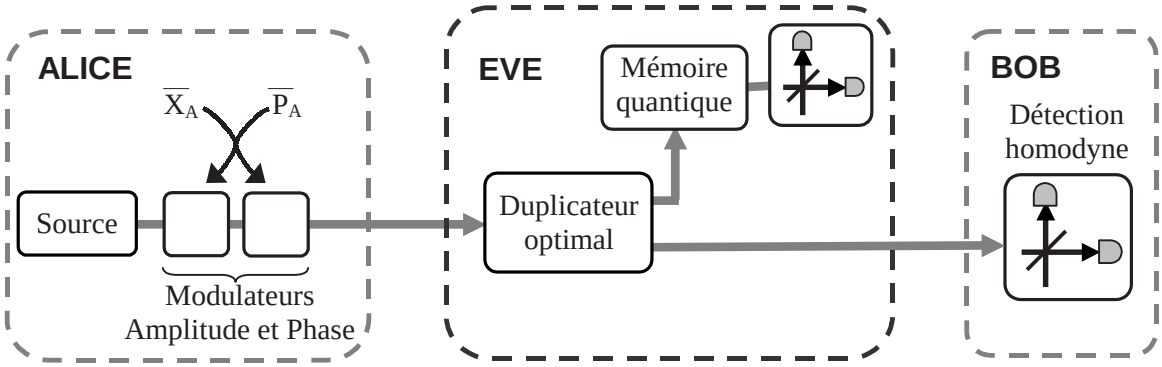

Figure 4.4: *Schéma de cryptographie à protocole direct et espionnage optimal dans le cadre d'une attaque gaussienne individuelle.*

4.2.2 Stratégies d'espionnage individuel optimales

Pour espionner la ligne, Eve doit interagir avec le faisceau d'Alice pour obtenir une partie du signal, dans une problématique similaire à celle des cloneuses quantiques [80, 81, 82, 83]. Le schéma d'une attaque individuelle optimale dans le cas d'une réconciliation directe est présenté sur la figure 4.4. Cette interaction est décrite par l'opération la plus générale de duplication du faisceau où le champ détecté par Bob est décrit par les équations (4.2) et celui collecté par Eve s'écrit de façon analogue :

$$X_E = \sqrt{H_X}\,(\,\overline{X}_A + \delta X_A + N_{X,E}\,) \qquad\qquad P_E = \sqrt{H_P}\,(\,\overline{P}_A + \delta P_A + N_{P,E}\,) \tag{4.5}$$

En tenant toujours compte de la symétrie du protocole, on fixe $H_X = H_P = H$. Les bruits équivalents ajoutés du côté d'Eve sont de variance $\langle {N_{X,E}}^2 \rangle = \langle {N_{P,E}}^2 \rangle = \chi_E\, N_0$ et sont toujours indépendants de la modulation d'Alice.

Les quadratures des faisceaux distincts d'Alice, Bob et Eve vérifient les relations de commutation :

$$[\delta X_A,\, \delta P_A] = [X_B,\, P_B] = [X_E,\, P_E] = 2\,\imath\, N_0 \tag{4.6}$$

$$[X_B,\, P_E] = [X_E,\, P_B] = 0 \tag{4.7}$$

La relation (4.7) associée à la modélisation du canal quantique (4.2) et (4.5) permet de déduire le commutateur des bruits équivalents [83] :

$$[N_{X,B},\, N_{P,E}] = [N_{P,B},\, N_{X,E}] = -2\,\imath\, N_0 \tag{4.8}$$

Ces relations de commutations entre les modes de Bob et d'Eve fournissent les inégalités d'Heisenberg croisées pour les variances des bruits équivalents :

$$\langle {N_{X,B}}^2 \rangle \langle {N_{P,E}}^2 \rangle \geq N_0^2 \qquad\qquad \langle {N_{P,B}}^2 \rangle \langle {N_{X,E}}^2 \rangle \geq N_0^2 \tag{4.9}$$

Dans les notations du cas symétrique, ces relations s'écrivent alors simplement :

$$\chi_B\, \chi_E \geq 1 \tag{4.10}$$

Ces relations interdisent alors à Bob et Eve de conspirer pour mesurer conjointement l'état d'Alice avec une précision meilleure que celle autorisée par le principe d'incertitude d'Heisenberg, ce qui est à la base du théorème de non-clonage quantique [78].

Dans le cadre de la cryptographie quantique, Alice et Bob doivent supposer que l'espion effectue l'action la plus forte autorisée par la physique quantique. Seule la théorie quantique fixe la limite à la qualité de l'espionnage. Compte tenu de l'estimation du canal quantique effectuée par Alice et Bob et de la valeur mesurée du bruit ajouté χ_B, l'espionnage à considérer est celui qui sature la relation (4.10), soit $\chi_E = 1/\chi_B$. Cette équation indique que plus l'action d'Eve est forte et sa précision bonne, et plus le bruit ajouté du côté de Bob sera important.

La mécanique quantique permet alors de quantifier la qualité maximale des mesures de l'espion, compte tenu des perturbations introduites. Cette précision de mesure d'Eve se traduit également dans une borne maximale sur l'information mutuelle entre Alice et Eve selon :

$$I_{AE} = \frac{1}{2}\log_2\left(1 + \frac{V_A}{1 + \frac{1}{\chi_B}}\right) \tag{4.11}$$

4.2.3 Sécurité et taux de transfert secret : cas direct

D'après le théorème de Csiszar-Körner [50, 51] exprimé par la relation (4.1), il est théoriquement possible d'extraire une clé secrète de taille $\mathcal{S}$ supérieure ou égale à la différence des informations mutuelles $I_{AB} - I_{AE}$. Une condition suffisante pour que la cryptographie quantique à réconciliation directe soit possible est alors donnée par $I_{AB} - I_{AE} > 0$. En pratique, cette limite (pourtant une borne inférieure !) est difficile à atteindre, essentiellement parce qu'il est difficile de concevoir des algorithmes permettant d'atteindre la quantité d'information de Shannon.

La quantité pertinente pour quantifier le taux de transfert secret en réconciliation directe est alors donnée par la différence des informations mutuelles $\underrightarrow{\Delta I}$:

$$\boxed{\underrightarrow{\Delta I} = I_{AB} - I_{AE} = \frac{1}{2}\log_2\left(\frac{V + \chi_B}{\chi_B V + 1}\right)} \tag{4.12}$$

Cette quantité est positive si Bob dispose de davantage d'information sur Alice qu'Eve, ce qui est vérifié à la condition :

$$\boxed{\textit{Sécurité protocole direct } \Leftrightarrow \chi_B < 1} \tag{4.13}$$

Il est ainsi possible de transmettre une clé secrète sans utiliser des états spécifiquement quantiques, comme des états comprimés ou des états intriqués. La sécurité des protocoles à états cohérents est basée sur les propriétés du clonage quantique, et non pas sur les particularités de ces états.

Il est très intéressant de dissocier dans le bruit ajouté la partie provenant de la contribution des pertes optiques à celle d'un bruit supplémentaire. Dans le cas des pertes seules d'un canal de transmission G, le bruit équivalent en entrée est de variance $(1 - G)/G$ d'après (2.69). La variance totale de bruit χ_B se décompose alors selon :

$$\chi_B = \frac{1 - G}{G} + \varepsilon \tag{4.14}$$

où ε désigne la variance d'un bruit supplémentaire non lié aux pertes seules. La condition de sécurité (4.13) se réécrit alors :

$$\varepsilon < 2 - \frac{1}{G} \tag{4.15}$$

Dans le meilleur des cas, lorsque le bruit supplémentaire est nul $\varepsilon = 0$, la condition de sécurité (4.13) est alors équivalente à une transmission $G > 50\%$, soit des pertes inférieures à 3 dB. Une

condition nécessaire à la sécurité d'un protocole à réconciliation directe est alors de travailler avec une transmission de plus de 50%. Par ailleurs, aux forts taux de transmission $G \to 1$, le protocole de réconciliation directe est robuste à un excès de bruit jusqu'à $\varepsilon \backsimeq 1$.

$$\textit{Conditions suffisantes à un protocole direct} \ : \ G > \frac{1}{2} \ \textit{et} \ \varepsilon < 2 - \frac{1}{G} < 1 \tag{4.16}$$

Les protocoles à réconciliation directe sont donc relativement robustes à un excès de bruit, mais ils ne fonctionnent de manière satisfaisante que pour de fortes valeurs de transmission G. Afin d'étendre le domaine d'application de la cryptographie quantique avec des états cohérents, il convient d'inverser le sens du flux d'information de correction et d'utiliser un protocole de réconciliation inverse. Dans ce cas, Alice et Bob possèdent un avantage sur un espion potentiel pour toute valeur de transmission, ce qui autorise dans ce cas des transmissions en théorie pour des pertes arbitrairement élevées comme nous allons le montrer à la section suivante.

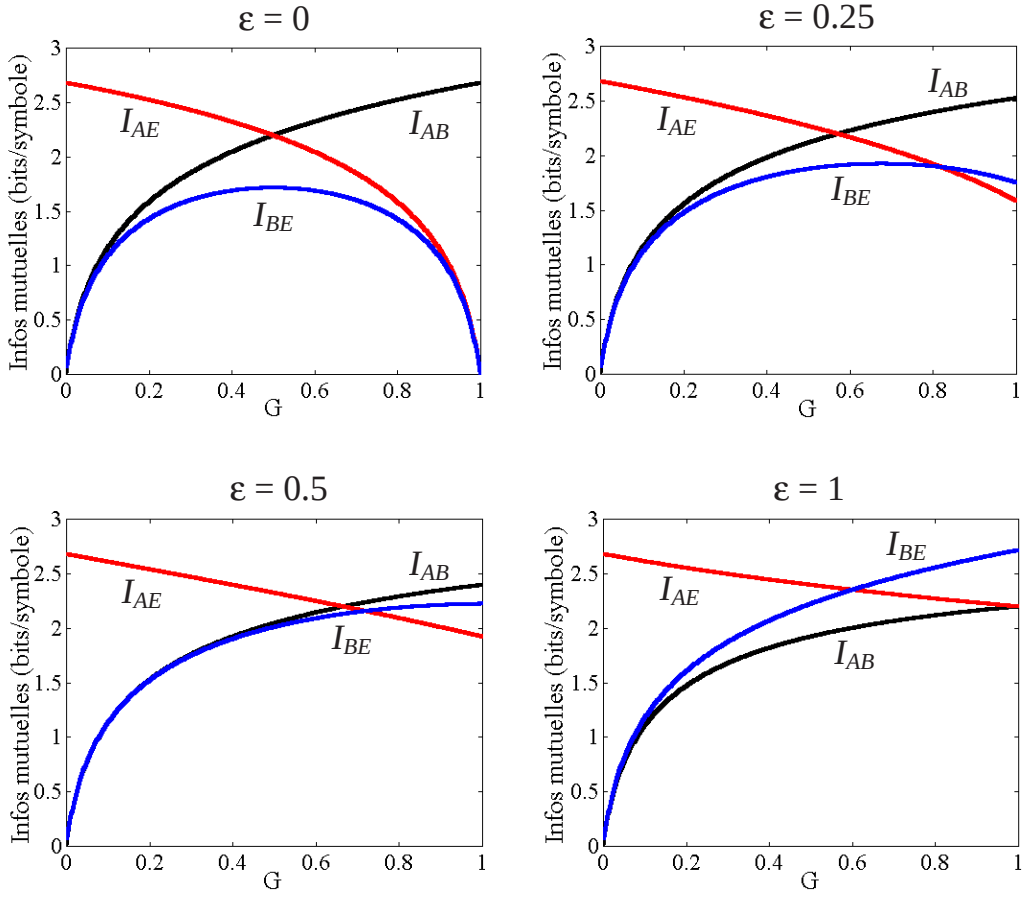

Figure 4.5: *Informations mutuelles I_{AB}, I_{AE} et I_{BE} en fonction de la transmission G de la ligne pour une variance de modulation $V_A = 40$ et différents niveaux ε de bruit ajouté. La cryptographie à protocole direct est possible si $I_{AB} > I_{AE}$, celle à protocole inverse s'applique lorsque $I_{AB} > I_{BE}$.*

4.3 Protocoles inverses

4.3.1 Limites de la quantité d'information espionnée

Il existe plusieurs moyens théoriques pour échanger des clés secrètes au-delà du seuil de 3 dB de pertes. Par exemple, il est possible d'utiliser un processus de postsélection [72] pour ne conserver que les valeurs où Bob possède un avantage sur Eve. Dans le cadre de l'utilisation de faisceaux intriqués, l'intrication peut être améliorée par des protocoles de purification [125]. La procédure à base de réconciliation inverse que nous avons proposée dans [73, 75] possède l'avantage d'être beaucoup plus simple à mettre en œuvre et de ne pas nécessiter l'utilisation d'une procédure de postsélection. En effet, la réconciliation inverse met l'accent sur les valeurs mesurées par Bob, qui sont toujours plus difficiles à déterminer pour un espion que les valeurs de la modulation d'Alice. Cet avantage décisif confère alors aux partenaires la possibilité de transmettre théoriquement une clé secrète pour toute valeur de la transmission de la ligne.

Les protocoles inverses suivent exactement le schéma général énoncé dans la section 4.1. La seule différence intervient au niveau de l'application d'une réconciliation inverse, où Bob envoie des données de correction à Alice. Ainsi, le canal quantique entre Alice et Bob est toujours décrit par les formules de la section 4.2.1.

Le point délicat dans un protocole inverse est de fixer une borne à la quantité d'information espionnée. Cette quantité est ici donnée par l'information I_{BE} dont dispose Eve sur les valeurs de Bob. D'une manière générale en réconciliation inverse, Alice et Eve doivent estimer les valeurs mesurées par Bob. On peut par exemple s'intéresser à l'estimateur d'Alice sur les mesures de Bob en X. Cet estimateur est de la forme $\alpha\,\overline{X}_A$, où α est un paramètre qui caractérise l'estimation d'Alice sur Bob et $\overline{X}_A$ la valeur (classique) de la modulation connue d'Alice. L'erreur commise sera alors donnée par :

$$X_{B|A,\alpha} = X_B - \alpha\,\overline{X}_A \tag{4.17}$$

Le meilleur estimateur d'Alice sera celui qui minimise la variance $\langle {X_{B|A,\alpha}}^2 \rangle$ en fonction de α, ce qui est atteint pour le paramètre $\alpha = \langle \overline{X}_A X_B \rangle / \langle {\overline{X}_A}^2 \rangle$. Pour ce meilleur paramètre, l'erreur d'Alice sur les mesures de Bob s'écrit alors :

$$X_{B|A,min} = X_B - \frac{\langle \overline{X}_A X_B \rangle}{\langle {\overline{X}_A}^2 \rangle}\,\overline{X}_A \tag{4.18}$$

On retrouve également une formule bien connue de la variance conditionnelle :

$$V_{X_B|\overline{X}_A} = \min_{\alpha}(\langle {X_{B|A,\alpha}}^2 \rangle) = \langle {X_B}^2 \rangle - \frac{\langle \overline{X}_A X_B \rangle^2}{\langle {\overline{X}_A}^2 \rangle} \tag{4.19}$$

De la même manière, l'erreur résiduelle d'Eve sur les mesures de Bob en P s'écrit :

$$P_{B|E,min} = P_B - \frac{\langle P_B P_E \rangle}{\langle {P_E}^2 \rangle}\,P_E \tag{4.20}$$

Comme les opérateurs (X_B, P_E) et $(P_B, \overline{X}_A)$ commutent, on peut directement écrire le commutateur :

$$[X_{B|A,min}, P_{B|E,min}] = [X_B, P_B] = 2\,\imath\,N_0 \tag{4.21}$$

Les variances conditionnelles doivent donc suivre une relation d'incertitude de Heisenberg, ce qui limite la qualité de l'espionnage d'Eve :

$$V_{X_B|\overline{X}_A}\,V_{P_B|P_E} \geq {N_0}^2 \qquad\qquad V_{P_B|\overline{P}_A}\,V_{X_B|X_E} \geq {N_0}^2 \tag{4.22}$$

Pour les protocoles à états cohérents, on pourra simplement retenir le cas symétrique :

$$V_{B|A}\, V_{B|E} \geq {N_0}^2 \tag{4.23}$$

A nouveau, ces relations signifient qu'Alice et Eve ne peuvent pas connaître le faisceau de Bob mieux que ne l'autorise le principe d'incertitude d'Heisenberg. Connaissant les corrélations entre leurs valeurs (étape 2 du protocole général), Alice et Bob peuvent borner leur variance conditionnelle mutuelle et ainsi fixer une limite à la connaissance d'Eve.

Dans le cas d'un protocole symétrique à états cohérents, les formules (4.2) et (4.19), permettent de calculer directement la variance conditionnelle d'Alice sur les mesures de Bob :

$$V_{B|A,coh} = G\,(1+\chi_B)\,N_0 \tag{4.24}$$

Pour limiter la variance conditionnelle d'Eve, on pourrait utiliser cette valeur de $V_{B|A}$ injectée dans la relation d'Heisenberg croisée (4.23). Comme nous allons le voir, cette valeur ne donne cependant pas la limite optimale de la variance conditionnelle d'Eve. Les corrélation entre les sorties de la machine d'espionnage d'Eve ne dépendent que de la matrice densité ρ_A du champ entrant (X_A, P_A) et non pas de la manière dont ce champ a été produit, c'est-à-dire qu'il soit issu d'une source d'états cohérents ou d'états spécifiquement quantiques comme des états intriqués. Les inégalités (4.22) doivent donc être vérifiées pour toutes les valeurs physiquement autorisées de $V_{X_B|\overline{X}_A}, V_{P_B|\overline{P}_A}$ étant donnée la matrice densité ρ_A, indépendamment de la source effectivement utilisée par Alice. Ainsi, les valeurs de $V_{X_B|\overline{X}_A}, V_{P_B|\overline{P}_A}$ qui doivent être injectées dans les inégalités (4.22) sont les variances conditionnelles minimales qu'Alice *pourrait* atteindre connaissant ρ_A. Ces variances minimales sont atteintes lorsqu'Alice utilise l'intrication maximale compatible avec ρ_A, ce qui fournit comme nous le démontrerons au chapitre 6 :

$$V_{B|A,min} = V_{X_B|\overline{X}_A,min} = V_{P_B|\overline{P}_A,min} = G\,(\frac{1}{V}+\chi_B)\,N_0 \tag{4.25}$$

On obtient alors la meilleure borne sur la variance conditionnelle d'Eve :

$$V_{B|E} \geq \frac{N_0}{G\,(\frac{1}{V}+\chi_B)} = V_{B|E,opt} \tag{4.26}$$

Cette borne inférieure est directement connectée à l'intrication, même si Alice n'utilise pas d'états intriqués. L'argument essentiel est qu'elle *aurait* pu utiliser de tels états, sans que Bob ou Eve aient des moyens physiques de le savoir. La sécurité des protocoles à états cohérents apparaît donc intimement liée à l'intrication quantique, même si aucune intrication n'est physiquement présente. Ce lien entre sécurité et intrication a motivé une étude plus poussée qui fera l'objet du chapitre 6 et qui a été publiée dans [75]. Un dispositif d'espionnage permettant d'atteindre la limite (4.26) est présenté sur la figure 4.6. Ce système est appelé une *cloneuse intricante* et a été détaillé dans la thèse de Frédéric Grosshans [71].

4.3.2 Sécurité et taux de transfert secret : cas inverse

Pour garantir la sécurité d'un protocole de réconciliation inverse à états cohérents, nous supposerons que l'espionnage d'Eve peut atteindre la limite (4.26) fixée par la physique quantique. En réconciliation inverse, l'information mutuelle au sens de Shannon entre Alice et Bob est la même qu'en réconciliation directe, mais elle est plus efficacement écrite en fonction des variances conditionnelles d'après la formule (1.23) pour des canaux additifs gaussiens :

$$I_{BA} = \frac{1}{2}\log_2\left(\frac{\langle {X_B}^2\rangle}{V_{B|A,coh}}\right) = \frac{1}{2}\log_2\left(\frac{V+\chi_B}{1+\chi_B}\right) = I_{AB} \tag{4.27}$$

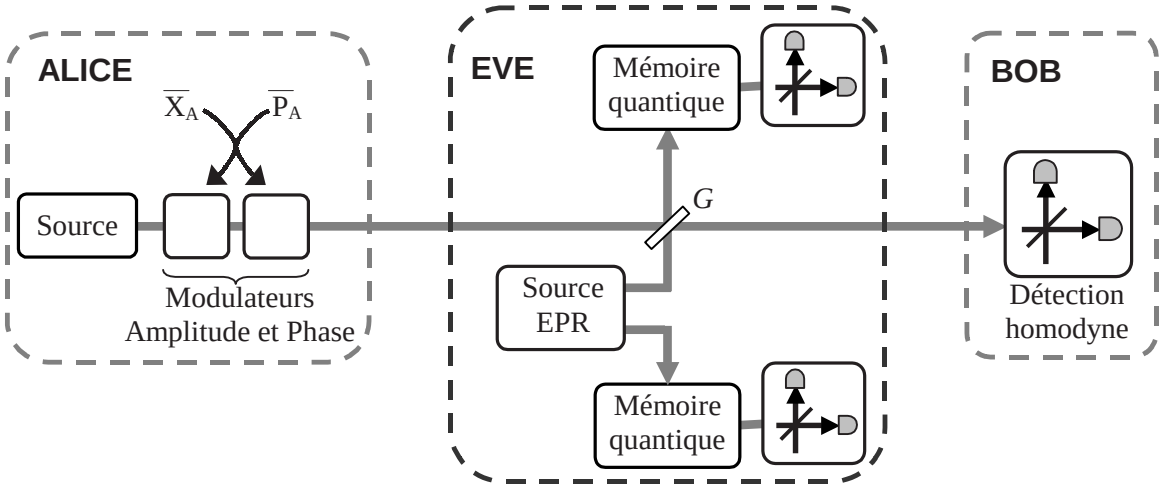

Figure 4.6: *Schéma de cryptographie à protocole inverse et attaque optimale par une cloneuse intricante. Toutes les pertes de la ligne sont concentrées dans la lame de transmission G, les éléments utilisés par Eve sont supposés dépourvus de toute limitation d'ordre technique.*

L'information espionnée par Eve s'écrit suivant la borne (4.26) :

$$I_{BE} = \frac{1}{2}\log_2\left(\frac{\langle {X_B}^2\rangle}{V_{B|E,opt}}\right) = \frac{1}{2}\log_2\left(G^2\,(V+\chi_B)\,(\frac{1}{V}+\chi_B)\right) \tag{4.28}$$

Enfin, d'après le théorème de Csiszar-Körner (4.1), le taux de transfert secret est donné par la quantité :

$$\boxed{\underleftarrow{\Delta I} = I_{BA} - I_{BE} = -\frac{1}{2}\log_2\left(G^2\,(1+\chi_B)\,(\frac{1}{V}+\chi_B)\right)} \tag{4.29}$$

La sécurité est garantie si $\underleftarrow{\Delta I} > 0$, c'est-à-dire si le bruit entre Bob et Alice est plus faible que le bruit d'Eve.

$$\boxed{\begin{aligned} \textit{Sécurité protocole inverse} \;&\Leftrightarrow\; V_{B|A,coh} < V_{B|E,opt} \qquad (4.30)\\ &\Leftrightarrow\; G^2\,(1+\chi_B)\,(\frac{1}{V}+\chi_B) < 1 \qquad (4.31)\end{aligned}}$$

Contrairement aux protocoles directs, cette condition peut être vérifiée pour toute valeur de la transmission G de la ligne, comme le montre la figure 4.5. Il est donc possible en théorie de transmettre une clé secrète quelle que soit l'atténuation du canal. Pour démontrer clairement cette affirmation, on peut reprendre la décomposition (4.14) du bruit ajouté χ_B en une partie liée aux pertes $(1-G)/G$ et un bruit ajouté ε. La condition de sécurité (4.31) s'écrit alors :

$$\varepsilon < \frac{V-1}{2V}\underbrace{-\frac{1}{G}+\sqrt{\frac{1}{G^2}+\frac{1}{4}\left(1-\frac{1}{V}\right)^2}}_{\geq 0} \tag{4.32}$$

La condition $\varepsilon < \frac{V-1}{2V}$ apparaît alors comme une condition suffisante pour vérifier cette inégalité, quelle que soit la valeur de G. Tant que l'excès de bruit ne sera pas trop important, une clé

secrète pourra être échangée.

$$\textit{Condition suffisante à un protocole inverse} \ : \ \forall\, G,\ \ \varepsilon < \frac{V-1}{2V} \backsimeq \frac{1}{2} \tag{4.33}$$

Si les protocoles inverses fonctionnent en théorie pour toute valeur de transmission, ils sont par contre moins robustes à un excès de bruit que les protocoles directs, qui sous certaines conditions peuvent tolérer jusqu'à $\varepsilon < 1$. Suivant la qualité du canal quantique, les protocoles directs peuvent être préférés lorsque les pertes optiques sont faibles. Un avantage de nos protocoles est qu'Alice et Bob peuvent décider du sens de la réconciliation à utiliser au cours du processus, une fois que la qualité effective de l'échange a été caractérisée.

4.3.3 Comparaison avec le protocole discret BB84

Dans le domaine de la cryptographie quantique avec des variables discrètes, le taux de transfert est limité par le temps de relaxation des détecteurs de photons uniques, dont les processus sont délicats à maîtriser aux forts taux de comptage. A l'opposé, une détection homodyne peut raisonnablement fonctionner à des cadences de répétitions de quelques dizaines de MHz. De plus, la grande dynamique de modulation dans l'espace des phases pour les variables continues permet de coder plusieurs bits secrets par impulsion, ce qui est impossible avec des protocoles discrets. Il en résulte donc que les protocoles à états cohérents permettent simplement d'atteindre de très hauts débits de transmission secrète pour des lignes à faibles pertes.

Dans le cas des fortes pertes $G \ll 1$, le taux de transmission d'un protocole inverse à états cohérents devient $\underleftarrow{\Delta I} \backsimeq \frac{1}{2\ln 2}\, G$ pour de fortes modulations sans bruit ajouté. Ce taux est alors voisin du taux obtenu pour un protocole de type BB84 valant $\frac{1}{2}\, G\, \overline{n}$ où $\overline{n}$ est le nombre moyen de photons émis par impulsion ($\overline{n} = 1$ pour une source parfaite de photons uniques et $\overline{n} \backsimeq 0.1$ pour une impulsion laser atténuée). Si on considère une distance réaliste de transmission de 67.1 km avec 14.3 dB de pertes [40], associée à une modulation raisonnable $V = 50$, le protocole inverse à états cohérents donnerait un taux de transfert secret de 0.027 bit par symbole. Le taux pour un protocole BB84 avec une source de photon unique parfaite serait de 0.019 bit par symbole, voire un ordre de grandeur plus faible avec une source laser atténuée. Avec une détection homodyne fonctionnant à une cadence de 1MHz, la cadence de transfert serait théoriquement de l'ordre de 30 kbits secrets par seconde. Bien que nos systèmes expérimentaux soient loin d'atteindre ces valeurs, cette comparaison démontre toutefois clairement les possibilités des protocoles à états cohérents.

4.3.4 Preuves de sécurité inconditionnelle

Au commencement de nos études en juillet 2001, le seul protocole connu inconditionnellement sûr était le protocole de Gottesman et Preskill [65], qui utilise la technique des codes correcteurs quantiques pour relier le domaine des variables continues aux protocoles de purification de qubits. Ce protocole nécessite cependant l'utilisation d'états comprimés de facteur de compression d'au moins 2.5 dB et est limité à des pertes inférieures à 1.6 dB.

Entre cette publication et novembre 2003, peu d'études de sécurité inconditionnelle ont été menées, les protocoles se restreignant au cas des attaques gaussiennes individuelles (qui font déjà intervenir des dispositifs extrêmement élaborés comme des mémoires quantiques, des sources parfaites...). Une avancée majeure dans les preuves inconditionnelles de sécurité a alors été apportée par Frédéric Grosshans et Nicolas Cerf dans [76]. En utilisant une forme entropique de la relation d'incertitude d'Heisenberg, ils ont démontré que les protocoles inverses à états cohérents

sont sûrs contre des attaques non-gaussiennes et cohérentes sur un nombre d'impulsions fixé et inférieur à la taille de la clé. De plus, il a été prouvé dans cette même publication que l'attaque optimale contre ces protocoles est une attaque gaussienne individuelle, telle que considérée dans ce chapitre. Dès lors, le canal est un canal additif gaussien et donc la modulation optimale pour Alice est une gaussienne d'après la théorie de Shannon.

Une autre étude menée en parallèle par Sofyan Iblisdir, Gilles Van Assche et Nicolas Cerf [77], propose un lien avec les codes correcteurs quantiques pour démontrer de façon inconditionnelle la sécurité et s'affranchir de la limite sur la taille de l'attaque cohérente dans [76]. Jusqu'à présent, cette preuve s'applique à des protocoles directs, le cas des protocoles inverses est en cours d'étude.

4.4 Conclusion

La cryptographie quantique offre une technologie de transmission de message secret où la sécurité est fondée sur des lois physiques et l'espionnage est quantifiable. L'utilisation d'états cohérents, techniquement plus simples à produire et à mesurer que des photons uniques, ouvre des perspectives prometteuses pour transmettre une clé secrète avec de forts débits, en principe pour des distances arbitrairement élevées. Ces résultats innovants appellent deux questions essentielles qui feront l'objet des deux prochains chapitres. D'une part, qu'en est-il de la réalisation physique de tels protocoles ? Quels sont leurs taux atteignables, leurs limites techniques ? D'autre part, la sécurité quantique des protocoles inverses à états cohérents apparaît intimement liée à l'intrication, même si aucune intrication n'est effectivement utilisée dans le montage. Comment expliquer ce lien ?

Chapitre 5

Démonstration expérimentale de cryptographie quantique à états cohérents

Sommaire

Présentation de l'expérience

Suivant les propositions théoriques de notre équipe pour la cryptographie quantique avec des états cohérents [70, 73], l'utilisation des variables quantiques continues offre une alternative intéressante aux protocoles basés sur l'exploitation de photons uniques [40]. En effet, l'usage

d'impulsions cohérentes comportant un grand nombre de photons ouvre des perspectives particulièrement prometteuses en terme de débit de clé et de simplicité de réalisation. Afin de valider ces propositions et d'en évaluer les paramètres caractéristiques, nous avons réalisé une démonstration expérimentale du principe de distribution de clé quantique avec des variables continues.

Des états cohérents sont modulés suivant une distribution gaussienne avant d'être échangés puis mesurés avec une détection homodyne résolue en temps limitée au bruit de photon. Les données sont ensuite traitées pour aboutir à une extraction pratique de clé secrète suivant l'ensemble des étapes nécessaires : extraction de chaînes binaires, correction d'erreurs (réconciliation directe ou inverse) et suppression de la connaissance de l'espion (amplification de confidentialité). Notre système a ainsi généré une clé secrète à un débit de 1.7 Mbits/s en l'absence de pertes et 75 kbits/s pour une transmission présentant 3.1 dB de pertes. Cet ensemble constitue le premier dispositif *complet* et *sûr* de cryptographie quantique avec des variables continues [73].

Notre schéma possède plusieurs spécificités essentielles qui le distinguent des autres protocoles à variables continues (voir la référence [70] pour une présentation rapide de ce domaine). Premièrement, aucune particularité quantique comme l'intrication ou la compression des fluctuations quantiques n'est physiquement requise pour notre dispositif. Deuxièmement, la partie optique de ce système est entièrement continue : des variables quantiques continues sont modulées suivant une distribution gaussienne avant d'être mesurées avec une détection homodyne. Un protocole particulièrement efficace d'extraction de bits [56] permet l'exploitation de quasiment toute l'information de Shannon contenue dans ces mesures. Troisièmement, notre système de détection homodyne est résolu en temps et non pas en fréquence. Il est ainsi directement sensible à la distribution statistique des quadratures du champ signal et permet une exploitation simple des débits d'information. Enfin, grâce à l'inversion du sens de la correction des erreurs, ce système est théoriquement sûr quelle que soit la transmission du canal.

Conception du dispositif optique

Le schéma optique de l'expérience est relativement simple : Alice envoie à Bob à travers un canal quantique authentifié des états cohérents modulés continûment suivant une distribution gaussienne dans l'espace des phases. Par ailleurs, elle transmet un faisceau de référence (considéré comme classique et public) servant d'oscillateur local pour la détection homodyne ainsi que divers signaux classiques de synchronisation. Bob choisit alors aléatoirement de mesurer la quadrature X ou la quadrature P de chaque impulsion incidente. Il vient ensuite une seconde étape purement algorithmique où Alice et Bob échangent classiquement et publiquement certaines informations pour évaluer la qualité du transfert et extraire une clé parfaitement secrète.

Une réalisation expérimentale complète doit vérifier strictement le cahier des charges suivant :

- *Source* : états cohérents monomodes sans excès de bruit à cadence régulière.
- *Modulation* : arbitraire en amplitude et phase pour chaque impulsion suivant une distribution gaussienne en (X, P).
- *Canal* : authentifié, permettant la synchronisation entre les partenaires, la qualité du canal (G et χ_B) doit être testée sur un échantillon représentatif des impulsions échangées.
- *Détection* : résolue en temps pour chaque impulsion, limitée au bruit de photon, choix aléatoire de la quadrature mesurée, fort rapport signal à bruit, faible bruit électronique, excellente efficacité globale.
- *Réconciliation* : directe ou inverse par communication uni-directionnelle.

Notre dispositif expérimental ne valide cependant pas l'ensemble de ces points. Comme nous le verrons dans ce chapitre, la modulation en phase est déterministe, les nombres (pseudo) aléatoires ne sont pas de qualité cryptographique, le canal n'a pas été authentifié (Alice et Bob partagent le même ordinateur), la réconciliation uni-directionnelle a été approximée... Si notre système ne permet donc pas un échange de clé secrète au sens strict, il fournit cependant des données physiques qui suivent la même répartition statistique que pour un transfert réel. L'ensemble des paramètres utiles pour la caractérisation de nos protocoles pourra ainsi être évalué expérimentalement. Notre philosophie pour le développement de cette expérience sera donc de réaliser une démonstration de principe pertinente plutôt que de concevoir un réel système de cryptographie.

Ce chapitre détaille le dispositif expérimental décrit dans [73]. Les résultats concernant l'évaluation effective de l'espionnage et l'extraction de clé [1] sont ensuite présentés avant d'aborder enfin les perspectives pratiques offertes par ce dispositif en terme de réalisations futures.

5.1 Dispositif expérimental détaillé

Données techniques pour l'expérience de cryptographie cohérente	
Diode laser	Spectra Physics SDL 5412, λ 780nm, Cavité étendue en montage Littrow avec un réseau Jobin-Yvon 1200 traits/mm, seuil 36mA, largeur spectrale <40MHz, Puissance utile 40mW pour 100mA.
Modulateur Acousto-optique	A-A OptoElectronic Modèle AA.ST.110, caractéristiques avec une focalisation de 150mm : efficacité 30%, durée impulsion FWHM 120ns, cadence 800kHz.
Fibre optique	Thorlabs FS-PM-4611-HT, monomode à 780nm, maintien de polarisation (pol. mesurée en sortie 1:200), longueur 40cm, couplage 15% (pas de connecteurs).
Modulateur Electro-optique	United Technologies Photonics, λ 780nm, tension demi-onde $V_\pi = 2.5V$, bande passante 2GHz, efficacité couplage 15% (pas de connecteurs), extinction mesurée DC $\backsim$ 4% (14dB), à 800kHz $\backsim$ 1%, puissance max < 30dBm.
Cale piezo-électrique	Saint Gobain Quartz, tension demi-onde $V_\pi = 95V$, bande passante alimentation HT 700 Hz.
Puissance signal	$\backsim$ 250 photons/impulsion au maximum de la modulation soit 50pW moyens à 800kHz. Modulation typ. $V_A = 43$.
Puissance OL	$1.3\,10^8$ photons/impulsion soit 26.5μW moyens à 800kHz.
Détection homodyne	Modèle à amplificateur de tension, efficacité globale $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2 = 79\%$ ou 83% avec $\eta_{opt} = 92\%$, $\eta_{phot} = 92\%$, $\eta_{mod} = 96.5\%$ ou 99% suivant l'expérience; bruit de photon 4.23mV, bruit électronique 2.14mV, SNR en variance modulation / bruit total 27.

[1] L'extraction de bits, la correction d'erreurs et l'amplification de confidentialité ont été réalisées par Gilles Van Assche et Nicolas Cerf de l'Université Libre de Bruxelles avec qui nous avons collaboré pour ce projet.

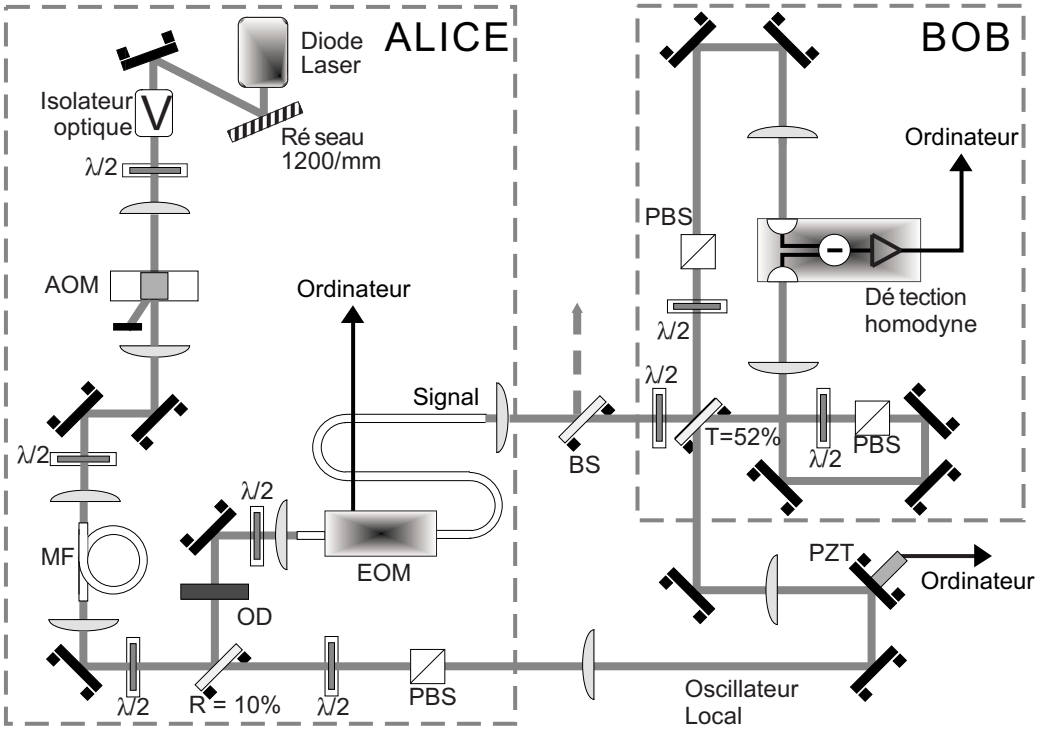

Figure 5.1: *Dispositif expérimental complet. AOM : modulateur acousto-optique, MF : fibre optique monomode à maintien de polarisation, EOM : modulateur électro-optique d'amplitude, OD : densité optique, BS : lame séparatrice simulant les pertes de transmission.*

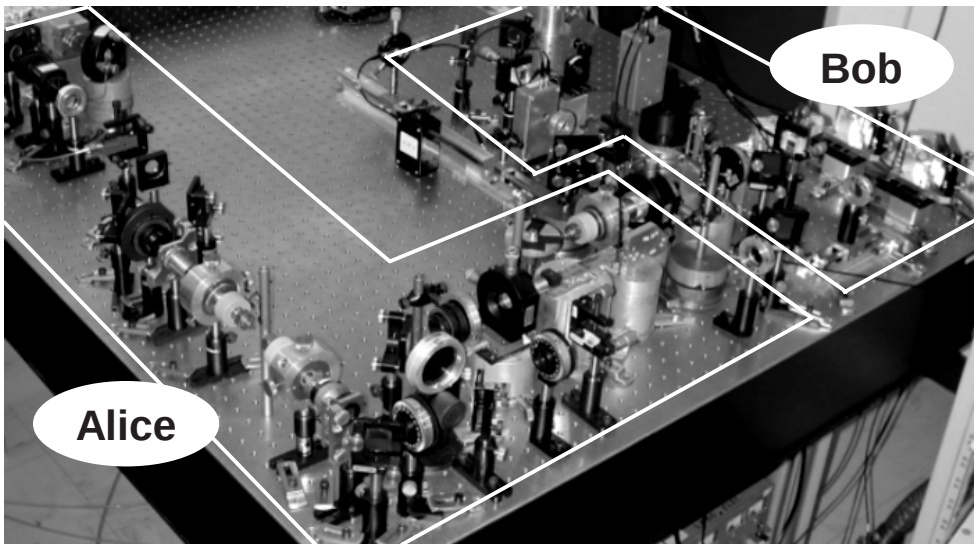

Figure 5.2: *Photographie du montage expérimental. Alice et Bob ne sont distants que de 7cm, mais des éloignements arbitraires peuvent être simulés en induisant des pertes grâce à la lame BS de transmission variable.*

5.1.1 Source d'impulsions cohérentes

Le dispositif expérimental présenté sur la figure 5.1 utilise comme source une diode laser continue émettant à 780nm. Pour générer des impulsions lumineuses de durée 120ns (largeur totale à mi-hauteur FWHM) à la cadence de 800kHz, le faisceau continu est modulé en puissance par un modulateur acousto-optique. Afin de réduire l'excès de bruit de la diode, un réseau optique réalise une cavité optique étendue en configuration de Littrow. Enfin, une fibre optique monomode à maintien de polarisation permet un filtrage spatial efficace du faisceau. Une forte atténuation optique du faisceau signal avant l'étage de modulation permet enfin de rendre négligeable l'excès de bruit introduit par la diode laser et ainsi de disposer d'une source cohérente d'impulsions au niveau du bruit de photon. Les caractéristiques techniques des différents éléments sont résumées dans le tableau page précédente.

5.1.2 Modulation en amplitude

Caractéristique du modulateur

La distribution gaussienne des états cohérents dans l'espace des phases est générée en modulant à la fois l'amplitude et la phase des impulsions lumineuses. Dans notre mise en œuvre expérimentale, l'amplitude de chaque impulsion est arbitrairement modulée à la cadence de 800kHz par un modulateur d'amplitude électro-optique[2] formant un interféromètre de Mach-Zehnder intégré en niobate de lithium $LiNbO_3$. La transmission en amplitude de cet appareil pour la quadrature X en phase avec l'oscillateur local est présentée sur la figure 5.3(c) en fonction de la tension de commande. L'utilisation d'une technologie d'optique intégrée permet notamment de travailler avec une faible tension demi-onde ($V_\pi = 2.5\,V$) et une large bande passante de modulation (jusqu'à 2 GHz).

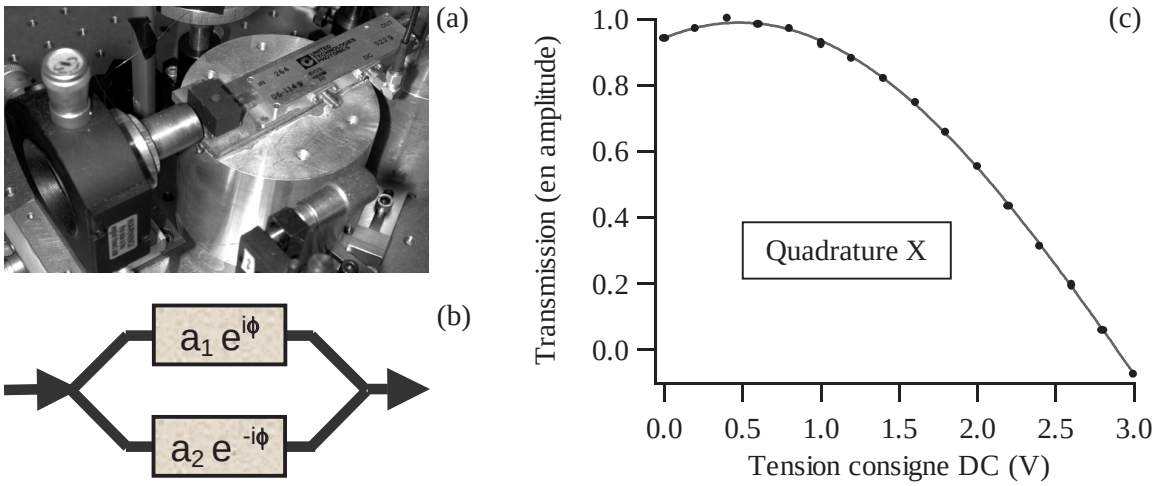

Figure 5.3: *(a) Photographie et (b) modèle simple du modulateur électro-optique d'amplitude (a_i désigne la transmission en amplitude de chaque voie). (c) Transmission expérimentale en amplitude du modulateur pour la quadrature X en phase avec l'oscillateur local, en fonction de la tension de consigne, la courbe est une interpolation suivant un modèle sinusoïdal.*

[2]Je remercie vivement la société Thalès TRT et M. Thierry Debuisschert pour le prêt de cet appareil.

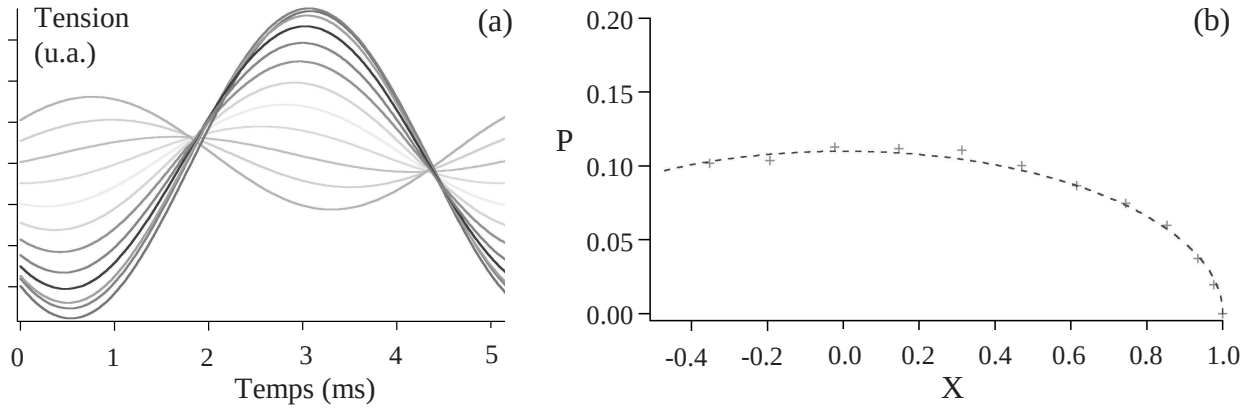

Figure 5.4: *Caractéristique du modulateur d'amplitude mesurée dans l'espace des phases. (a) Champs moyens transmis par le modulateur et mesurés par la détection homodyne pour différents échelons de tension en consigne du modulateur de 0 à 3V alors que la phase de l'oscillateur local est balayée linéairement. Il apparaît que l'extinction est non-négligeable, de même que le déphasage induit entre les niveaux de transmission. (b) Caractéristique déduite dans l'espace* (X, P)*, la courbe en tirets indique une simulation théorique (suivant le schéma 5.3) considérant que chaque bras de l'interféromètre formant le modulateur induit la même phase en valeur absolue.*

La caractéristique transmission-tension tracée sur la figure 5.3(c) est à considérer avec certaines précautions. Cette courbe est obtenue d'après une mesure à la détection homodyne : la quantité mesurée résulte donc de la projection du champ signal sur la direction de l'oscillateur local. En particulier, la figure 5.3(c) n'indique donc pas forcément que l'extinction en sortie du modulateur peut être parfaitement nulle. Afin d'obtenir une caractéristique complète du modulateur dans l'espace des phases, nous avons appliqué différents échelons de tension en consigne et mesuré simultanément le champ signal à la détection homodyne lorsque la phase de l'oscillateur local est balayée linéairement. Les résultats expérimentaux sont présentés sur la figure 5.4. Il apparaît alors que l'extinction est de 11% en amplitude, ce qui se traduit par une caractéristique non-linéaire dans l'espace des phases (figure 5.4(b)). Cet effet peut assez simplement s'expliquer par un déséquilibre entre les voies de l'interféromètre formant le modulateur comme le montre le modèle tracé en tirets sur la figure 5.4(b) ($a_2 \neq a_1$ où a_i désigne la transmission en amplitude de la voie i). D'après nos mesures d'extinction, en posant que la transmission maximale vaut $a_1 + a_2 = 1$ et la transmission minimale $a_1 - a_2 = 0.11$, on obtient $a_1 \approx 0.55$ et $a_2 \approx 0.45$.

Avec le modèle de la figure 5.3(b), le champ transmis par le modulateur d'amplitude est proportionnel à la transmission complexe de l'élément, qui s'exprime par :

$$a_1\, e^{\imath\,\phi} + a_2\, e^{-\imath\,\phi} = (a_1 + a_2)\cos\phi + \imath(a_1 - a_2)\sin\phi \tag{5.1}$$

Si Alice applique de plus un déphasage θ, la quadrature directement mesurée par Bob s'écrit alors (voir la figure 5.5) :

$$X_{B,mes} = X_{A,max}\left[(a_1 + a_2)\cos\phi\cos\theta - (a_1 - a_2)\sin\phi\sin\theta\right] \tag{5.2}$$

où $X_{A,max}$ désigne la valeur maximale de la modulation d'Alice. Cette équation contient le terme de modulation parfaite en $(a_1 + a_2)\cos\phi\cos\theta$, plus un terme traduisant la mauvaise extinction

du modulateur d'amplitude. Il devient alors possible de décomposer le champ transmis en un champ utile modulé suivant la quadrature X avec une extinction parfaite et un champ parasite déphasé de $\pi/2$. Pour une preuve de cryptographie parfaite, il faudrait supprimer ce champ en superposant au niveau d'Alice un champ supplémentaire dont les interférences annuleraient les effets du champ parasite. Une autre solution serait d'utiliser un meilleur modulateur (dans le cas d'un prototype complet à 1.55μm, des modulateurs d'extinction supérieure à 30 dB sont commercialement disponibles).

Dans notre expérience, qui est simplement vouée à être une démonstration du principe de cryptographie quantique avec des états cohérents, nous avons choisi de corriger les effets de cette mauvaise extinction lors d'un traitement a posteriori des données de Bob. Pour supprimer parfaitement les effets du champ parasite, il faudrait connaître à la fois l'amplitude et la phase choisie par Alice (ce qui revient à disposer des quantités θ et ϕ dans l'équation (5.2)). Cependant, si on choisit cette option de correction, le transfert d'information perd alors tout son sens : pour traiter ses données, Bob doit être informé parfaitement des valeurs de modulation d'Alice ! Nous avons décidé de mettre en œuvre une correction qui soit davantage dans l'esprit d'un échange de données. Dans notre dispositif, le champ parasite maximal $(a_1 - a_2)\sin\theta$ est soustrait des données mesurées, ce qui revient à translater la caractéristique du modulateur suivant l'axe P pour obtenir une extinction parfaite (figure 5.4). Cette opération est possible car comme nous le verrons à la section suivante, la phase θ n'est pas modulée aléatoirement, mais est déterministe dans notre expérience. Bob peut ainsi connaître simplement le champ parasite en $-(a_1-a_2)\sin\theta$ à soustraire de ses mesures. Les données effectives de Bob correspondent alors à :

$$X_{B,corr} = X_{A,max}\left[(a_1+a_2)\cos\phi\cos\theta - (a_1-a_2)\sin\theta(\sin\phi - 1)\right] \tag{5.3}$$

Cette équation contient le terme de modulation parfaite en $(a_1 + a_2)\cos\phi\cos\theta$, plus un terme de correction pour tenir compte de la non-linéarité de la réponse du modulateur d'amplitude. Cette non-linéarité résiduelle après corrections sera également prise en compte dans les calculs des données d'Alice.

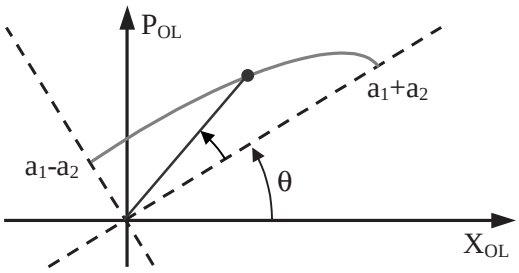

Figure 5.5: *Modèle utilisé pour le calcul de la quadrature mesurée par Bob. Le point indique la valeur de transmission choisie par Alice. La caractérisation du modulateur électro-optique fournit* $a_1 + a_2 = 1$ *et* $a_1 - a_2 = 0.11$.

Génération d'une modulation gaussienne

Pour la génération de la modulation gaussienne de variance $V_A\,N_0$, nous avons choisi de fixer la valeur de la variance par le nombre de photons maximal $\mathcal{N}_s$ du faisceau d'Alice (calibré d'après une mesure avec une photodiode). Ce choix permet d'utiliser l'ensemble de la plage

disponible du modulateur, dont la transmission varie entre 0 et 1. L'écart-type de la modulation en transmission vaut donc $\sigma_{\mathrm{T}} = 1/3$ (pour une distribution gaussienne, l'écart-type est pris égal au tiers de la valeur maximale admise, soit une transmission de 1 dans notre cas). Le lien entre V_A et le nombre de photons $\mathcal{N}_s$ est alors donné par $V_A = 2\,\mathcal{N}_s\,\sigma_{\mathrm{T}}^2 = 2/9\,\mathcal{N}_s$.

Quelle distribution de probabilité en amplitude r et phase θ choisir pour obtenir une modulation gaussienne en (X, P) ? Ce calcul a été effectué par Frédéric Grosshans dans [71] et sera brièvement repris ici. Nous posons l'amplitude r comme la transmission en champ du modulateur : $0 < r < 1$. Le point de départ consiste à identifier les densités de probabilité suivant [203] :

$$\mathcal{P}_{X,P}\,dX\,dP = \frac{1}{2\pi\sigma^2} e^{-\frac{X^2+P^2}{2\sigma^2}}\,dX\,dP = \mathcal{P}_{r,\theta}\,dr\,d\theta \tag{5.4}$$

où $\sigma = 1/3$ est l'écart-type de la distribution gaussienne pour la transmission en amplitude, choisie de telle sorte que 3σ soit égal à une transmission unité. Avec $dX\,dP = r\,dr\,d\theta$, une identification dans (5.7) fournit :

$$\mathcal{P}_r\,dr = \frac{r}{\sigma^2} e^{-\frac{r^2}{2\sigma^2}}\,dr = -d\left\{e^{-\frac{r^2}{2\sigma^2}}\right\} \tag{5.5}$$

$$\mathcal{P}_\theta\,d\theta = \frac{d\theta}{2\pi} \tag{5.6}$$

Ce qui donne explicitement la forme de la modulation en amplitude r à choisir et prouve comme on pouvait s'y attendre que la distribution en phase à appliquer est une loi uniforme sur $[0, 2\pi]$.

Pour passer d'une variable (pseudo-) aléatoire y, générée par l'ordinateur et uniformément répartie dans l'intervalle $[0, 1]$, à la variable r définie suivant la distribution (5.5), il faut à nouveau appliquer une relation du type :

$$|\mathcal{P}_y\,dy| = |\mathcal{P}_r\,dr| \tag{5.7}$$

Puisque la variable y est uniforme sur $[0, 1]$, $\mathcal{P}_y = 1$ d'où :

$$dy = d\left\{e^{-\frac{r^2}{2\sigma^2}}\right\} \qquad \Leftrightarrow \qquad y = e^{-\frac{r^2}{2\sigma^2}} \tag{5.8}$$

Avec le modèle du modulateur électro-optique, le lien entre la tension V à appliquer et la transmission en amplitude s'écrit :

$$r = \sin\left(\frac{\pi}{2}\,\frac{V_{min} - V}{V_\pi}\right) = \sigma\sqrt{-2\ln y} \tag{5.9}$$

où V_{min} est la tension d'annulation de la transmission et V_π la tension demi-onde du modulateur. Pour obtenir une modulation gaussienne entre 0 et 1 de la transmission, la tension à appliquer au modulateur s'écrit finalement à partir de la variable pseudo-aléatoire y fournie par l'ordinateur :

$$V = V_{min} - \frac{2}{\pi}\,V_\pi\,\arcsin(\sigma\sqrt{-2\ln y}) \tag{5.10}$$

Pour éviter une divergence dans cette formule lorsque y tend vers zéro, il faut tronquer la distribution de cette variable à $[y_{min}, 1]$. y_{min} est obtenu lorsque l'amplitude normalisée r transmise par le modulateur vaut 1, soit avec notre choix $\sigma = 1/3$: $y_{min} = \exp(-1/2\sigma^2) = e^{-4.5} \approx 0.011$.

Effets du codage discret

La tension de commande appliquée au modulateur élecro-optique est générée par la carte d'acquisition (*National Instruments* PCI 6111E) connectée à un ordinateur. Cette tension prend uniquement des valeurs discrètes, bien que nos propositions théoriques de protocoles supposent une distribution continue. Cependant, cette contrainte expérimentale peut ne pas être gênante si le nombre de niveaux de discrétisation codés par la carte est très grand devant le nombre de niveaux requis pour masquer le "quadrillage" de la distribution sous le bruit de photon. Dans ce cas, la distribution discrète est suffisamment dense par rapport au bruit quantique pour que l'espion ne puisse discerner les différents niveaux.

Un calcul très simple permet de quantifier l'influence des niveaux discrets de la tension fournie par la carte (une autre approche est développée dans [71]). Suivant la direction de la modulation d'amplitude, la quadrature envoyée par Alice s'écrit :

$$X_A = X_{A,max} \sin\left(\frac{\pi}{2}\frac{V_{min}-V}{V_\pi}\right) = 3\sqrt{V_A\,N_0}\,\sin\left(\frac{\pi}{2}\frac{V_{min}-V}{V_\pi}\right) \tag{5.11}$$

L'influence d'une faible variation de tension sur la transmission du modulateur est plus critique dans la portion où la transmission varie linéairement par rapport à la tension de commande, c'est-à-dire au voisinage du minimum d'amplitude transmise $V \approx V_{min}$. L'écart maximum en quadrature entre deux niveaux de tension séparés de δV vaut alors :

$$\delta X_r = X_A(V_{min}) - X_A(V_{min}-\delta V) \approx 3\,\sqrt{V_A\,N_0}\,\frac{\pi}{2}\,\frac{\delta V}{V_\pi} \tag{5.12}$$

Pour que les niveaux discrets générés par la carte soient noyés sous le bruit quantique, il faut $\delta X_r \ll \sqrt{N_0}$. Avec nos conditions expérimentales, $V_A \backsimeq 40$, $V_\pi = 2.5$ V, le critère $\delta X_r = 0.05\sqrt{N_0}$ impose une résolution en tension de $\delta V = 4$ mV, soit environ 12 bits dans la plage $\pm$10V de notre carte. Les sorties de notre carte étant codées sur 16 bits, nous pouvons donc très raisonnablement considérer que la modulation en amplitude est continue et que les effets de la discrétisation sont négligeables.

5.1.3 Modulation de phase

La société *Thalès* a pu nous prêter un modulateur intégré d'amplitude à 780 nm. Il s'agit d'un système datant d'une dizaine d'années et qui n'était plus disponible commercialement dans cette gamme de longueurs d'ondes au moment de notre expérience. Malheureusement, nous n'avons pas pu trouver de modulateur de phase fonctionnant à la longueur d'onde de 780 nm pour adresser arbitrairement la phase à la cadence nominale de 800 kHz. En effet, l'essentiel de la branche des modulateurs intégrés se concentre sur la fenêtre télécom 1.3-1.5 μm (depuis lors, de nouveaux modulateurs intégrés sont apparus sur le marché pour les longueurs d'onde 810 ou 1064 nm, commercialisés par la société *Linos*). En conséquence, la phase expérimentale des données d'Alice n'est pas modulée mais balayée continûment entre 0 et 2π par une cale piezo-électrique [3]. Les données sont ensuite permutées aléatoirement par un traitement informatique de sorte à obtenir exactement la même structure de données que pour une expérience réelle de cryptographie. Aucune clé secrète ne peut être rigoureusement transmise avec une telle variation déterministe de la phase, mais l'expérience permet de valider en conditions réelles les

[3] Sur le montage expérimental, cette cale piezo-électrique est commune à Alice et Bob qui l'utilisent alternativement pour moduler les données ou recaler la référence de phase entre les transferts.

caractéristiques du dispositif optique ainsi que le fonctionnement des algorithmes d'extraction de clé.

De même que pour la modulation d'amplitude, les effets du codage discret de la tension de commande doivent être évalués pour la modulation en phase, afin d'assurer que cette modulation peut raisonnablement être considérée comme continue. La modulation en phase étant uniforme sur $[0, 2\pi]$, deux points de phase adjacents sont séparés de la phase $\delta\theta = 2\pi/2^{n_\theta}$ où n_θ est le nombre de bits du codage en phase. L'écart maximal en quadrature entre deux points adjacents pour la modulation de phase s'écrit alors :

$$\delta X_\theta = X_{A,max}\,\delta\theta = 3\sqrt{V_A\,N_0}\,\frac{2\pi}{2^{n_\theta}} \tag{5.13}$$

A nouveau, la condition $\delta X_\theta \ll \sqrt{N_0}$ doit être vérifiée pour que les niveaux discrets de phase générés par la carte soient noyés sous le bruit quantique. Avec nos conditions expérimentales, $V_A \backsimeq 40$, le critère $\delta X_\theta = 0.05\sqrt{N_0}$ impose un codage de la phase sur $n_\theta = 11.2$ bits. Comme notre générateur de haute tension associé à la cale piezo-électrique n'utilise qu'une gamme de 4 V de la plage ± 10 V de la tension en sortie de carte, le codage au niveau de la sortie de la carte doit comporter 13.5 bits. Le codage en phase est donc plus critique que celui en amplitude, mais comme nous utilisons des sorties codées sur 16 bits, les effets de la discrétisation ne seront pas un problème expérimental.

5.1.4 Stabilisation de la phase

L'information secrète étant codée sur les quadratures du champ électromagnétique, notre système de détection interférométrique nécessite un faisceau de référence de phase (fourni par l'oscillateur local OL). Ainsi, l'ensemble du montage de la figure 5.1 peut être considéré comme un seul interféromètre de Mach-Zehnder dont chaque bras mesure plus d'un mètre de long. Pour garantir la qualité interférométrique de l'échange, aucune fluctuation incontrôlée de phase ne devrait perturber la phase relative entre l'impulsion signal d'Alice et l'impulsion OL correspondante. Expérimentalement, cette phase relative ne peut cependant pas être parfaitement maîtrisée, ce qui se traduit par des fluctuations ajoutées sur les mesures de Bob. Deux types de bruits de phase d'origines distinctes interviennent : des perturbations lentes (de l'ordre du Hz) d'origine mécanique ou thermique (modification de l'indice de l'air) et des perturbations rapides (de l'ordre de la centaine de Hz) d'origine acoustique. Les fluctuations lentes seront contrôlées et corrigées par un asservissement numérique et une rétroaction sur la cale piezo-électrique de l'oscillateur local. Les fluctuations rapides de phase seront atténuées par un choix approprié des puissances optiques des faisceaux. Ce problème de stabilité de la phase relative conduit alors à une limite supérieure de la puissance signal, afin de limiter l'influence de ces fluctuations sur le signal de sortie.

Fluctuations lentes de phase et asservissement

L'utilisation des entrées et sorties de la carte d'acquisition numérique, couplée à un ordinateur et à une cale piezo-électrique permet de concevoir simplement une boucle d'asservissement numérique des fluctuations lentes de la carte (le temps de réponse de l'alimentation haute tension de la cale et le temps d'échange de données entre la carte *NiDAQ* et le logiciel *Igor* limitent la vitesse de l'asservissement à des corrections de fluctuations de l'ordre de quelques Hz). Le principe retenu pour l'asservissement est le suivant : pour toute la durée de la mesure et la correction de la phase, Alice envoie la puissance maximale pour le faisceau signal. Bob cherche

alors à fixer la phase de l'oscillateur local pour annuler le signal d'interférence mesuré à la détection homodyne. Ceci s'effectue en 10 étapes identiques où une mesure de la tension moyenne sur 2000 impulsions en sortie de détection fournit le signal de correction à appliquer sur la cale piezo-électrique pour annuler les interférences. Le choix d'un nombre fixe de 10 itérations permet une précision dans la mesure de la phase de 0.7 mV (bruit de photon de 4.2 mV) ainsi qu'une convergence à la fin d'une durée fixe. Enfin, un déphasage supplémentaire de $\pi/2$ induit par la cale piezo-électrique permet de recaler la quadrature mesurée par Bob avec la direction X de la modulation d'Alice.

Fluctuations rapides de phase et choix de la modulation

Une première série d'expériences avait été effectuée avec une puissance moyenne signal de 1 nW (soit environ 5000 photons/impulsion à 800kHz) et une puissance OL de 10 μW. La variance de modulation est alors de l'ordre de $1000\,N_0$, ce qui devrait permettre un taux de transfert I_{AB} en l'absence de pertes et de bruit ajouté de l'ordre de 5 bits par impulsion. Cependant, pour cette puissance signal relativement "intense", des différences de phase relative aussi faibles que $\lambda/250$ viennent entacher le signal en sortie de la détection homodyne. Une étude du spectre de bruit révèle alors la présence de différentes fréquences particulières entre 200 et 300 Hz, ce qui indique que des vibrations acoustiques sont à l'origine des incertitudes de phase. Ces fluctuations se traduisent par une incertitude supplémentaire d'un écart-type de 5 mV sur une mesure moyenne de la phase, lorsque l'écart-type du bruit de photon correspondant est de 4.2 mV. Cette incertitude, qui devrait être très inférieure au bruit de photon, ne permet donc pas pour cette configuration un échange adéquat de données.

Afin de limiter l'influence des perturbations de phase, la puissance signal a été réduite à 250 photons par impulsion, tout en conservant une puissance OL de 10 μW, soit $1.3\,10^8$ photons par impulsion. Cette réduction de la puissance signal permet une diminution de la visibilité des franges d'interférences parasites sur chaque voie de la détection, ce qui atténue l'effet des perturbations rapides de phase, mais n'a pas d'influence sur l'efficacité de la détection homodyne. Pour ces puissances optiques, la précision de mesure moyenne de la phase est de 0.7 mV, à comparer au bruit de photon de 4.2 mV. Le prix à payer pour s'être quasiment débarrassé des fluctuations rapides de phase est une variance de modulation réduite, mais qui atteint tout de même la valeur de $43\,N_0$. Cette variance apparaît encore tout à fait acceptable pour la transmission d'information avec $I_{AB} = 2.7$ bits/impulsion en l'absence de pertes et une détection parfaite. [4]

Grâce à un choix adéquat des puissances optiques et à un asservissement actif des fluctuations lentes de la phase, le signal moyen en sortie de la détection homodyne est stable à mieux de 1% pour des durées supérieures à 0.1s, soit des ensembles de 80 000 impulsions, ce qui nous permet dès lors d'envisager des transferts de blocs de quelques dizaines de milliers de symboles.

5.1.5 Structure des données et synchronisation

Le traitement informatique utilisé pour l'amplification de confidentialité [73] est optimisé pour des blocs de données de 36 800 ou 55 200 bits. Expérimentalement, nous avons choisi

[4] Du fait des perturbations rapides de la phase, le meilleur choix pour la variance de modulation V_A n'est pas forcément la valeur la plus élevée possible évitant la saturation de la détection homodyne. Un autre argument dans ce sens est de remarquer que l'information mutuelle $I_{AB} = 1/2\log_2(1+V_A)$ en l'absence de pertes augmente relativement lentement par rapport à V_A au-delà de $V_A = 30$. Enfin, comme nous le verrons dans la section sur les taux de transfert expérimentaux, il peut être avantageux de travailler avec des variances de modulation réduites pour optimiser l'extraction de bits secrets compte tenu de l'efficacité limitée de nos algorithmes de réconciliation.

d'organiser les transferts de données par blocs de 60 000 points, ce qui permet de conserver quelques valeurs supplémentaires pour évaluer la qualité du canal de transmission. La durée utile d'un transfert de 60 000 impulsions à 800kHz est de 75 ms, ce qui permet de garantir une stabilité satisfaisante de la phase relative entre les faisceaux. Entre chaque bloc de données, des séquences d'impulsions sont envoyées pour recaler la phase relative suivant l'asservissement décrit précédemment, puis une autre séquence permet la synchronisation des partenaires. Dans notre expérience, un bloc de données de 60 000 points est envoyé toutes les 1.6 secondes, soit un rapport cyclique de l'ordre de 5%. Ce rapport cyclique n'a pas été conçu pour être le plus efficace possible et est clairement sous-optimisé pour cette expérience, mais il devrait pouvoir être amélioré simplement lors de prototypes futurs.

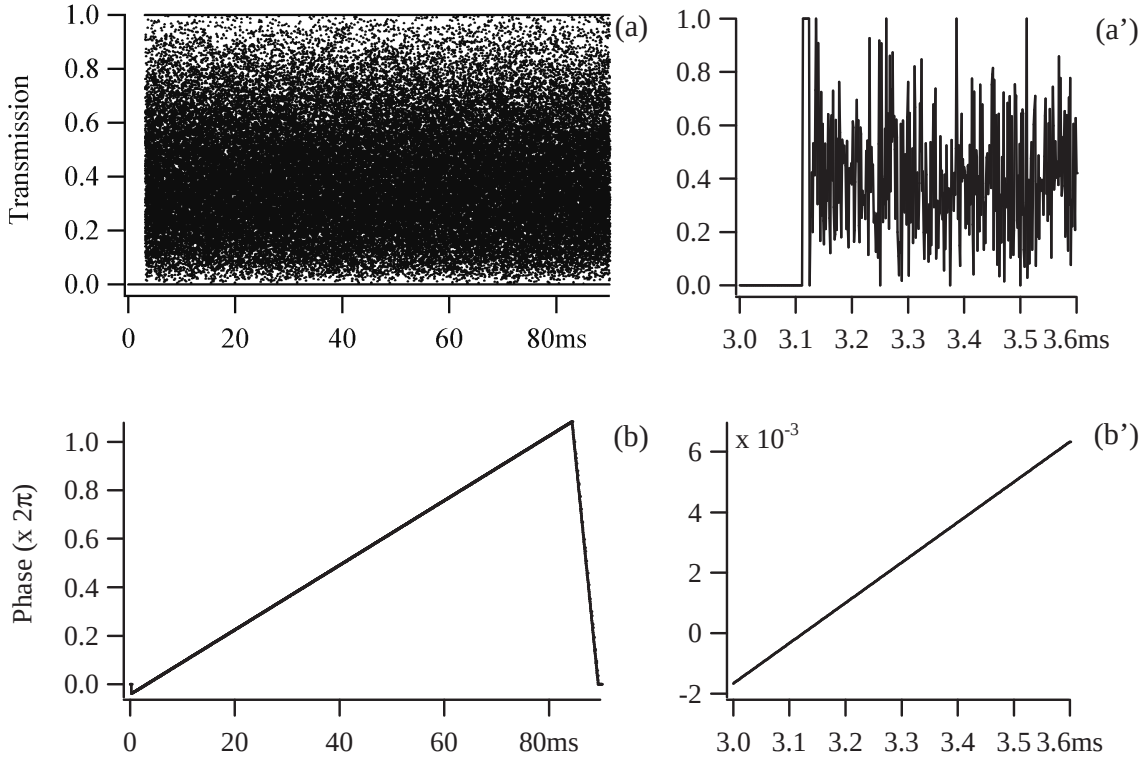

Figure 5.6: *Modulations expérimentales pour un bloc de 60 000 points. (a) transmission (calculée) en quadrature du modulateur, (b) phase (en unités de 2π) appliquée par la cale piezoélectrique. (a') et (b') sont des agrandissements des courbes (a) et (b) au début du transfert.*

La figure 5.6 présente les modulations expérimentales en transmission et en phase pour un bloc de données. Au cours d'un transfert, ces signaux sont envoyés dès que l'asservissement de correction des dérives de phase a bouclé un cycle d'itérations. Avant l'envoi des données proprement dites, un sous-bloc de 2500 impulsions permet de signaler le début du transfert. Ce bloc se compose de la manière suivante : pour les 2490 premiers points, la transmission du modulateur est mise au minimum, puis elle est fixée au maximum pour les 10 derniers points. Le récepteur peut alors facilement détecter le front montant dans l'amplitude, et savoir alors que le transfert débute 10 impulsions plus tard (pour notre démonstration de principe où Alice et Bob partagent le même ordinateur, nous n'avons besoin que de cette synchronisation simple du début du transfert).

En plus des données utiles pour le transfert de clé, Alice envoie une impulsion à la transmission minimale du modulateur toutes les 100 impulsions signal à partir de la première impulsion. Ceci permet à Bob de connaître précisément la valeur correspondante du champ parasite du modulateur électro-optique. Une interpolation sur ces données fournit ensuite les valeurs à soustraire aux données brutes du transfert pour corriger la mauvaise extinction du modulateur. Enfin, Alice envoie également une impulsion à la transmission maximale du modulateur toutes les 100 impulsions signal à partir de la dixième impulsion, ce qui permet a posteriori de connaître précisément la phase envoyée et de sélectionner exclusivement la plage $[0, 2\pi]$.

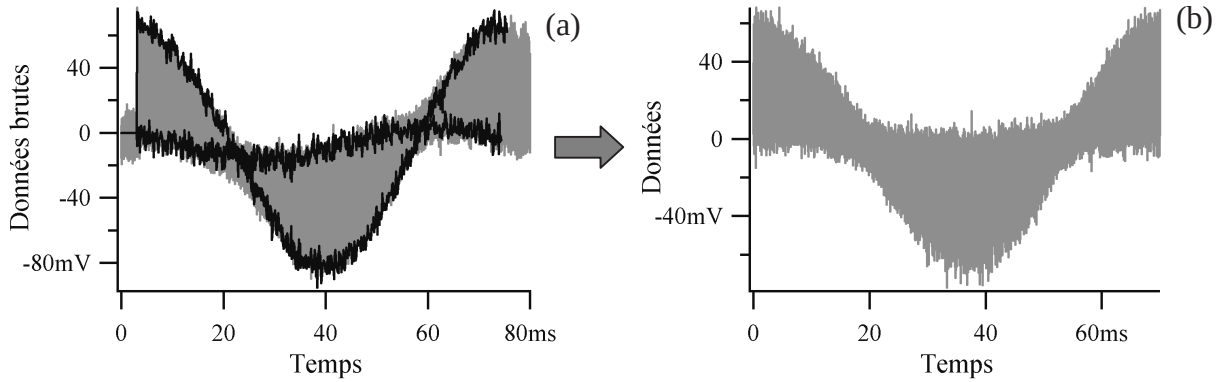

Figure 5.7: *(a) Exemple de données brutes (gris) mesurées en sortie de la détection homodyne avant traitement. (b) Données corrigées après synchronisation et suppression du champ parasite. Les courbes noires désignent les points au maximum et au minimum de transmission du modulateur, utilisés pour sélectionner la plage* $[0, 2\pi]$ *et pour soustraire le champ parasite introduit par le modulateur électro-optique.*

5.1.6 Détection homodyne impulsionnelle

Notre expérience utilise le premier prototype de détection homodyne résolue en temps, fonctionnant sur le principe d'un premier étage amplificateur de tension, décrit dans la section 3.4. Cette détection est limitée au bruit de photon jusqu'à des puissances oscillateur local de 500 millions de photons par impulsion, mais nous n'utiliserons qu'une puissance OL de 130 millions de photons par impulsion, pour des impulsions signal contenant jusqu'à 250 photons. Suivant les réglages expérimentaux, l'efficacité globale de la détection η_{hom} vaut typiquement 79%. Cette efficacité s'exprime suivant les résultats de la section 3.2.5 comme $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2$ avec la transmission des optiques de la détection $\eta_{opt} = 92\%$, l'efficacité quantique des photodiodes (*Centronix* BPX65) $\eta_{phot} = 92\%$, et l'efficacité d'adaptation des modes (visibilité des franges d'interférence) $\eta_{mod} = 96.5\%$. Au niveau de la quadrature détectée en entrée de la détection homodyne, ces inefficacités se traduisent par un bruit ajouté de variance $\chi_{hom}\,N_0$ suivant le résultat (5.19) : $\chi_{hom} = (1 - \eta_{hom})/\eta_{hom}$. Pour notre dispositif expérimental, on obtient $\chi_{hom} = 0.27$.

En plus du bruit de photon et du bruit équivalent virtuellement introduit par les pertes, la détection homodyne présente également un bruit électronique non-négligeable. Pour notre puissance OL de $1.3\,10^8$ photons/impulsion, l'écart-type du bruit de photon détecté est de 4.23mV alors que l'écart-type du bruit électronique est de 2.14mV. Le bruit électronique apparaît alors comme un bruit additif sur les valeurs mesurées en sortie avec une variance de $(2.14/4.23)^2 = 0.26\,N_0$. Si de plus on considère les bruits en entrée de la détection homodyne, donc tenant

compte de l'efficacité limitée η_{hom} de la détection, la variance de bruit électronique à considérer d'après (5.19) est $\chi_{elec}\,N_0 = 0.26/\eta_{hom}\,N_0 = 0.33\,N_0$.

Le bruit total ajouté par la détection vaut $(\chi_{hom} + \chi_{elec})\,N_0$ auquel il faut encore additionner une unité N_0 pour le bruit de photon du faisceau d'Alice. Avec une variance de modulation de $V_A = 43$, le rapport signal à bruit (en variances selon Shannon) en l'absence bruit ajouté en ligne est $SNR = V_A/(1 + \chi_{hom} + \chi_{elec}) = 27$, ce qui permet en théorie d'atteindre le débit $I_{AB} = 1/2\,\log_2(1 + SNR) = 2.4$ bits par impulsion.

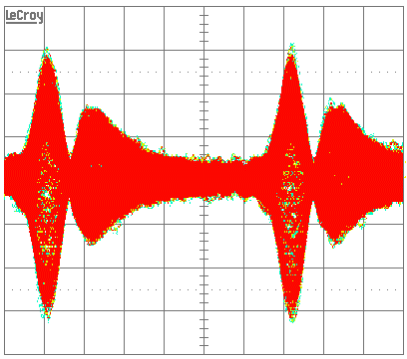

Figure 5.8: *Observation à l'oscilloscope du signal en sortie de la détection pour des impulsions signal d'amplitude maximale et modulées en phase. La persistence de l'oscilloscope est utilisée pour superposer de nombreuses réponses (temps de persistence 5 s). Puissance OL* $9.7\,10^7$ *photons/impulsion, puissance signal 80 photons/impulsion, échelles H : 0.2µs/div, V : 20mV/div.*

Après cette description détaillée du dispositif expérimental de cryptographie quantique avec des états cohérents, la section suivante aborde les échanges physiques de clés, ainsi que les résultats obtenus pour l'extraction finale de l'information binaire. En particulier, l'influence précise des bruits de la détection homodyne de Bob dans l'évaluation de l'espionnage sera présentée dans la section 5.2.3.

5.2 Discussion des résultats expérimentaux

5.2.1 Echange quantique de données

Le canal quantique complet, incluant la détection imparfaite de Bob, peut être modélisé par le schéma présenté sur la figure 5.9. Par la suite, nous n'écrivons les relations que pour la quadrature X, étant entendu que les relations sont identiques pour la quadrature P. Le canal de transmission proprement dit entre Alice et Bob est caractérisé par sa transmission (en intensité) G et sa variance de bruit équivalent en entrée χ_{ligne} comme nous l'avons vu au chapitre précédent. La quadrature en sortie de ce canal est notée X_{ligne} et s'exprime selon (4.2) :

$$X_{ligne} = \sqrt{G}\,(\,\overline{X}_A + \delta X_A + B_{ligne}\,) \tag{5.14}$$

L'état cohérent modulé en sortie de la source d'Alice est donné par $\overline{X}_A + \delta X_A$ où $\overline{X}_A$ est la valeur classique de modulation parfaitement connue d'Alice et δX_A désigne les fluctuations quantiques du faisceau. Le bruit équivalent en entrée rajouté par le canal est noté par B_{ligne}, de variance $\langle {B_{ligne}}^2 \rangle = \chi_{ligne}\,N_0$.

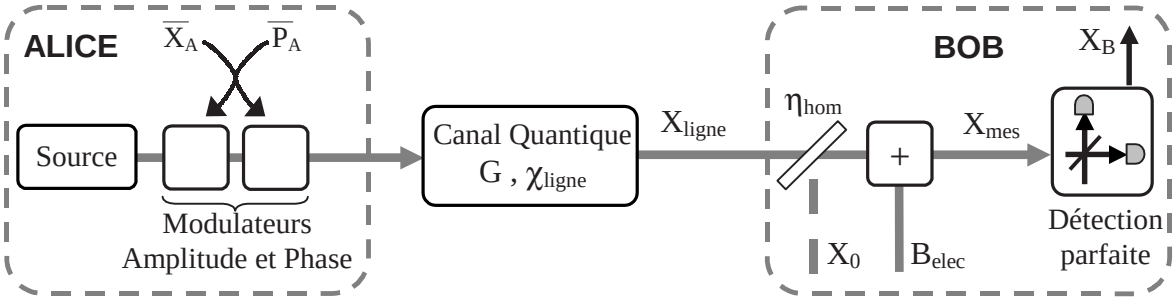

Figure 5.9: *Modèle de la transmission quantique et notations dans le cas d'une prise en compte "réaliste" du bruit de la détection homodyne de Bob (voir la discussion section 5.2.3).*

Pour tenir compte des imperfections de la détection homodyne, les différentes pertes sont modélisées par une lame de transmission égale à l'efficacité globale de la détection η_{hom}. De plus, un bruit supplémentaire B_{elec} non lié à une atténuation tient compte du bruit électronique de la détection. La variance de ce bruit, exprimée en unités de bruit de photon, est égale au rapport de la variance mesurée du bruit électronique sur la variance mesurée du bruit de photon. La quadrature mesurée par la détection homodyne peut alors s'exprimer selon :

$$X_{mes} = \sqrt{\eta_{hom}}\, X_{ligne} + \sqrt{1-\eta_{hom}}\, X_0 + B_{elec} \tag{5.15}$$

Enfin, Bob déduit son estimation de la quadrature reçue en sortie de la ligne en corrigeant ses mesures de l'atténuation $\sqrt{\eta_{hom}}$:

$$X_B = \frac{X_{mes}}{\sqrt{\eta_{hom}}} = \sqrt{G}\,(\,\overline{X}_A + \delta X_A + B_{ligne}\,) + \sqrt{\frac{1-\eta_{hom}}{\eta_{hom}}}\, X_0 + \frac{1}{\sqrt{\eta_{hom}}}\, B_{elec} \tag{5.16}$$

La variance des données X_B de Bob vaut alors, en unités de N_0 :

$$V_B = \frac{\langle {X_B}^2 \rangle}{N_0} = G\,(\,V_A + 1 + \chi_{ligne}\,) + \frac{1-\eta_{hom}}{\eta_{hom}} + \frac{\langle {B_{elec}}^2 \rangle}{\eta_{hom}} \tag{5.17}$$

Ce qui peut se réécrire sous la forme condensée :

$$V_B = G\,(\,V + \chi_{ligne}\,) + \chi_{hom} + \chi_{elec} = G\,(\,V + \chi_{tot}\,) \tag{5.18}$$

Avec $V = V_A + 1$ la variance totale de la modulation d'Alice et les bruits χ_{hom}, χ_{elec} ajoutés par la détection homodyne

$$\chi_{hom} = \frac{1-\eta_{hom}}{\eta_{hom}} \qquad\qquad \chi_{elec} = \frac{\langle {B_{elec}}^2 \rangle}{\eta_{hom}} \tag{5.19}$$

Finalement, le bruit équivalent total de la transmission χ_{tot} s'exprime par :

$$\chi_{tot} = \chi_{ligne} + \frac{\chi_{hom} + \chi_{elec}}{G} \tag{5.20}$$

Ces différentes définitions du bruit ajouté seront utiles suivant les hypothèses de la prise en compte par l'espion des bruits de la détection de Bob (voir la discussion section 5.2.3).

Les figures 5.10 et 5.11 présentent les données X_B et $\overline{X}_A$ ainsi définies, pour un bloc de données de 60 000 impulsions correspondant à une transmission de $G = 100\%$. Pour ce transfert, la variance des données d'Alice vaut $V_A = 40.7$, celle des données de Bob vaut $V_B = 42.3$. La différence entre V_B et V_A est liée au bruit de photon (une unité N_0) ainsi qu'aux différents autres bruits : bruit ajouté en ligne, pertes de la détection homodyne, bruit électronique. D'après (5.18) pour une transmission de 100%, on attendrait $V_B = V_A+1+\chi_{hom}+\chi_{elec} = 40.7+1+0.27+0.33 = 42.3$, ce qui correspond bien à la variance mesurée et indique que $\chi_{ligne} = 0$, comme on pouvait l'espérer pour une ligne sans pertes.

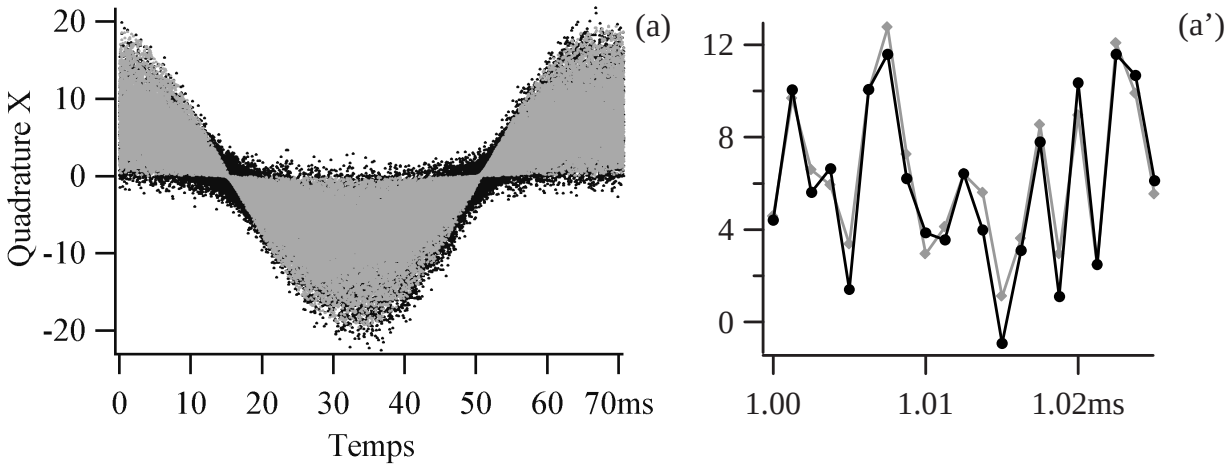

Figure 5.10: *(a) Quadrature mesurée X_B par Bob (noir) et quadrature envoyée $\overline{X}_A$ par Alice (gris) en fonction du temps pour un bloc de 60 000 points à la cadence de 800kHz. La transmission du canal est de 100% et la variance de modulation vaut $V_A = 40.7$. (a') est un agrandissement de (a) montrant un échantillon des données de Bob (noir) par rapport à celles d'Alice (gris).*

5.2.2 Estimation des paramètres de la ligne

Une fois l'échange quantique effectué, une première étape vers l'extraction d'une clé secrète binaire est d'estimer les paramètres G et χ_{ligne} du canal quantique. Lors d'un échange cryptographique réel, cette estimation s'effectue en révélant publiquement un sous-ensemble de données statitistiquement représentatif et choisi aléatoirement (donc inconnu d'Eve lors de l'espionnage). Alice et Bob peuvent alors comparer leurs résultats pour estimer les paramètres utiles. Bien sûr, les données ainsi révélées sont ensuite supprimées et n'interviennent plus pour l'extraction d'une clé secrète. Pour notre démonstration de principe, l'intégralité des 60 000 impulsions transmises est utilisée pour évaluer les paramètres G et χ_{ligne} (l'efficacité et le bruit de la détection homodyne sont par ailleurs calibrés avant et après chaque transfert).

L'évaluation des caractéristiques du canal utilise le coefficient de corrélation ρ^2 entre les données d'Alice et Bob.

$$\rho^2 = \frac{\langle \overline{X}_A X_B \rangle}{\sqrt{\langle \overline{X}_A{}^2 \rangle \langle X_B{}^2 \rangle}} = G\,\frac{V_A}{V_B} = \frac{V_A}{V_A + 1 + \chi_{tot}} \tag{5.21}$$

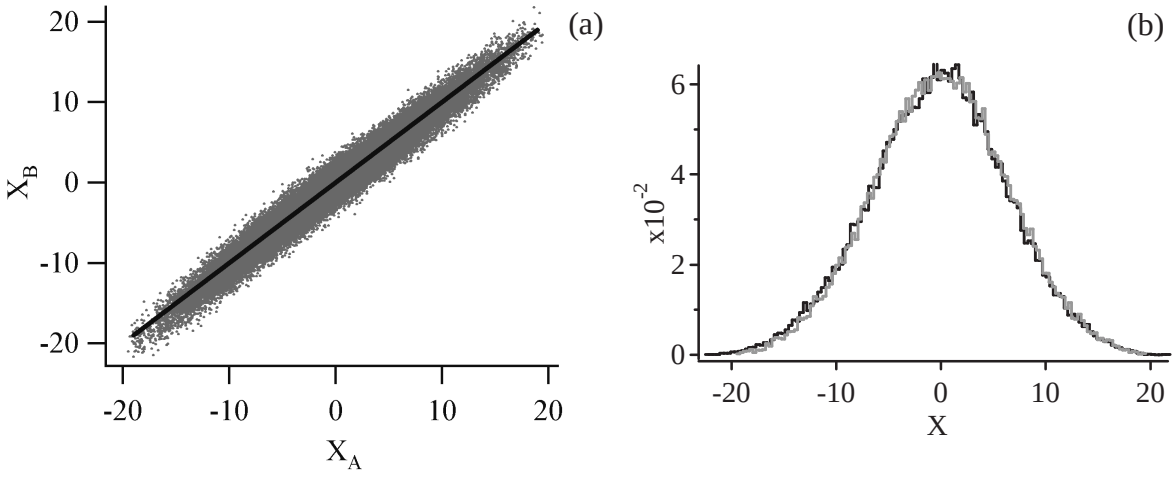

Figure 5.11: *(a) Quadrature mesurée X_B par Bob en fonction de la quadrature envoyée $\overline{X}_A$ par Alice pour un bloc de 60 000 points. La transmission du canal est de 100% et la variance de modulation vaut $V_A = 40.7$. La courbe en trait plein représente la droite de pente unité attendue. (b) Histogrammes des données d'Alice (gris) et de Bob (noir). La variance des données d'Alice vaut $V_A = 40.7$, celle des données de Bob vaut $V_B = 42.3$.*

Ce coefficient permet d'exprimer l'ensemble des caractéristiques selon :

$$G = \rho^2 \frac{V_B}{V_A} \tag{5.22}$$

$$\chi_{tot} = V_A \frac{1-\rho^2}{\rho^2} - 1 \tag{5.23}$$

$$I_{AB} = -\frac{1}{2}\log_2(1-\rho^2) \tag{5.24}$$

Les seuls paramètres nécessaires en plus du coefficient de corrélation sont les variances V_A et V_B des distributions d'Alice et Bob. Une propriété essentielle qui nous a fait préférer l'utilisation du coefficient ρ^2 est qu'il est indépendant du gain G et permet de s'affranchir ainsi de l'incertitude sur la calibration de la transmission.

Plus spécifiquement, pour évaluer le gain de la transmission lors de notre expérience, nous utilisons un faisceau intense à la place du faisceau signal d'Alice et mesurons directement au puissancemètre la transmission de la lame BS qui simule les pertes de la ligne entre Alice et Bob. La formule (5.22) est ensuite utilisée pour vérifier la calibration de la variance d'Alice, qui avait été effectuée avant le transfert par une mesure directe de la puissance maximale du signal émis (photodiode silicium calibrée avec une résistance de charge de 10 MΩ).

Afin d'estimer le bruit ajouté par la ligne, nous calibrons précisément les paramètres η_{hom} et χ_{elec} avant chaque transfert. Ceci nous permet de calculer le bruit total ajouté par la détection homodyne, et connaissant de plus le coefficient de corrélation ρ^2 entre Alice et Bob, les formules (5.23) et (5.20) permettent d'accéder au bruit ajouté par la ligne χ_{ligne}. En modifiant la transmission de la lame BS simulant les pertes de la transmission, nous avons mesuré ce coefficient de bruit ajouté par la ligne en fonction de la transmission de la lame G. Nos résultats expérimentaux sont présentés sur la figure 5.12, et suivent raisonnablement la prédiction théorique $\chi_{ligne} = (1-G)/G$, notre expérience ne faisant intervenir qu'un bruit additif provenant de pertes pures (l'excès de bruit en ligne ε_{ligne} est nul dans ce cas).

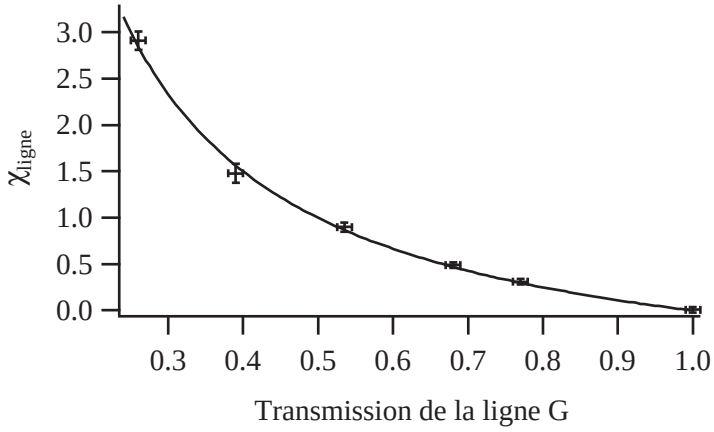

Figure 5.12: *Variance expérimentale χ_{ligne} du bruit équivalent en entrée en fonction de la transmission du canal G. La courbe en trait plein indique la prédiction théorique $(1-G)/G$.*

5.2.3 Caractérisation de l'espionnage

Les bruits ajoutés par la détection homodyne χ_{hom} et χ_{elec} sont clairement pris en compte dans le calcul (5.24) de l'information mutuelle I_{AB} entre Alice et Bob, que l'on peut par ailleurs exprimer selon :

$$I_{AB} = I_{BA} = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_{tot}}\right) = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_{ligne}+\frac{\chi_{hom}+\chi_{elec}}{G}}\right) \tag{5.25}$$

La question est plus délicate en ce qui concerne l'influence des bruits ajoutés par la détection de Bob sur l'évaluation de l'espionnage. Un premier point de vue – extrême – serait de considérer que tous les bruits dans le système de détection de Bob peuvent être contrôlés par Eve, qui peut intriquer librement ses faisceaux avec la détection de Bob. Ce point de vue constitue l'approche que nous qualifions de *paranoïaque*. Le paramètre pertinent pour évaluer l'action de l'espion dans les formules (4.10) et (4.26) est alors le bruit total χ_{tot} comprenant le bruit ajouté par la ligne ainsi que celui provenant de la détection homodyne. Le gain effectif à considérer est alors le produit $G\,\eta_{hom}$. L'information espionnée en réconciliation directe $I_{AE,par}$ ou inverse $I_{BE,par}$ dans la prise en compte "paranoïaque" du bruit de la détection s'écrit :

$$I_{AE,par} = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\frac{1}{\chi_{tot}}}\right) \tag{5.26}$$

$$I_{BE,par} = \frac{1}{2}\log_2\left(\frac{\eta_{hom}\,V_B}{\frac{1}{\eta_{hom}\,G\,(\chi_{tot}+1/V)}}\right) = \frac{1}{2}\log_2\left(G^2\,{\eta_{hom}}^2\,(V+\chi_{tot})\,(\frac{1}{V}+\chi_{tot})\right) \tag{5.27}$$

Dans une deuxième approche, appelée *réaliste*, nous pouvons considérer que puisque les bruits χ_{hom} et χ_{elec} proviennent de la détection homodyne de Bob, ces bruits ne peuvent pas contribuer à la connaissance d'Eve qui n'a pas accès à cette détection. La quantité pertinente pour quantifier l'espionnage est alors uniquement le bruit χ_{ligne} ajouté par la ligne de transmission, c'est à dire quand les états quantiques sont dans le domaine d'Eve. L'évaluation de l'information espionnée sur les données d'Alice (réconciliation directe) prend donc uniquement en compte χ_{ligne} pour

borner χ_E :

$$I_{AE,real} = \frac{1}{2}\log_2\left(1 + \frac{V_A}{1+\frac{1}{\chi_{ligne}}}\right) \tag{5.28}$$

Dans le cadre de la réconciliation directe, il découle de la définition de la variance conditionnelle que :

$$\begin{aligned} V_{B|E,real} &= V_{B|E,ligne} + \chi_{hom} + \chi_{elec} \\ &= \frac{1}{G(\chi_{ligne}+1/V)} + \chi_{hom} + \chi_{elec} \end{aligned} \tag{5.29}$$

car les bruits ajoutés par la détection homodyne sont des bruits indépendants. L'information espionnée sur les données de Bob (réconciliation inverse) s'exprime alors selon :

$$I_{BE,real} = \frac{1}{2}\log_2\left(\frac{V_B}{\frac{1}{G(\chi_{ligne}+1/V)} + \chi_{hom} + \chi_{elec}}\right) \tag{5.30}$$

Il faut préciser ici que cette prise en compte "réaliste" des bruits ne limite en rien les actions d'espionnage sur la ligne. Eve peut mettre en œuvre toutes les attaques compatibles avec l'évaluation de χ_{ligne} : duplicateur quantique optimal, mémoire quantique, source EPR parfaite...

Les informations mutuelles entre les partenaires sont représentées sur la figure 5.13 pour les paramètres expérimentaux réels et suivant les deux points de vue de prise en compte des bruits de la détection homodyne. On peut noter que même dans l'hypothèse "paranoïaque", notre système permet tout de même une extraction de clé secrète en réconciliation inverse pour les fortes transmissions. Par la suite, nous considérerons exclusivement l'approche "réaliste" où le bruit de la détection homodyne n'est pas contrôlé par Eve.

5.2.4 Extraction d'une clé secrète

Pour extraire une clé secrète binaire des données continues échangées, il faut utiliser un traitement informatique assez élaboré, réalisé par Gilles Van Assche, Kim-Chi Nguyen et Nicolas Cerf de l'Université Libre de Bruxelles avec qui nous avons collaboré pour la réalisation d'un dispositif complet de cryptographie quantique à impulsions cohérentes [73]. Ce traitement se décompose en deux étapes principales : la correction des erreurs (réconciliation directe ou inverse) et le filtrage de l'information espionnée (amplification de confidentialité).

Réconciliation par tranches

Le principe de l'extraction de données binaires et de la correction des erreurs repose sur l'utilisation d'un algorithme de "réconciliation par tranches" introduit par Gilles Van Assche, Jean Cardinal et Nicolas Cerf dans [56] et qui a été présenté dans la section 1.3.

Pour l'extraction de bits dans le cadre de notre expérience, cet algorithme décompose la distribution des données continues en $2^5 = 32$ intervalles et associe à chaque donnée continue un mot binaire de 5 bits correspondant au numéro de l'intervalle dans lequel se trouve la valeur continue. Le nombre d'intervalles ainsi que la largeur de chaque intervalle ont été optimisés numériquement compte tenu de nos rapports signal à bruit expérimentaux.

Du fait des pertes optiques, de l'espionnage et des bruits de la détection, différentes erreurs sont présentes dans ces chaînes binaires. Pour corriger ces erreurs suivant l'algorithme de réconciliation binaire *Cascade* [52, 57], notre traitement n'utilise pas la totalité des bits en une

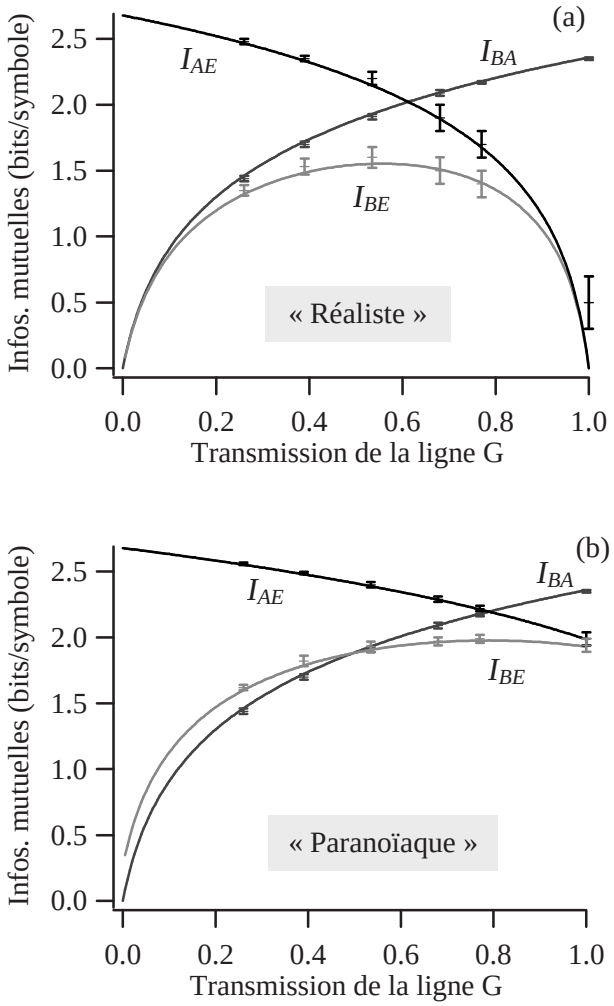

Figure 5.13: *Informations mutuelles I_{BA}, I_{BE} et I_{AE} en fonction de la transmission G du canal évaluées pour $V \approx 40$ et avec les bruits expérimentaux χ_{hom} et χ_{elec} réels pris en compte selon les hypothèses d'espionnage "réaliste" (a) ou "paranoïaque" (b). L'information mutuelle I_{BA} entre Alice et Bob est bien sûr inchangée suivant les hypothèses d'espionnage. La cryptographie par réconciliation directe fournit une clé secrète si $I_{AB} > I_{AE}$, la réconciliation inverse opère pour $I_{BA} > I_{BE}$.*

seule opération, mais discrimine entre les bits de poids différents. Plus précisément, on forme des ensembles de bits ("tranches") de niveaux successifs suivant le poids du bit au sein de chaque mot binaire. La première tranche contient tous les bits de poids faible des différentes impulsions, et ainsi de suite jusqu'à la cinquième tranche constituée des bits de poids forts. L'intérêt de cette procédure est de corriger successivement les différentes tranches, ce qui permet d'utiliser l'information déjà obtenue sur les tranches précédentes pour affiner l'estimation de la tranche suivante et extraire le maximum d'information au sens de Shannon.

Parmi les cinq ensembles de bits dont nous disposons, les deux premiers (de poids faibles, donc de fort taux d'erreur) sont simplement révélés, et ne servent qu'à améliorer la précision des estimations suivantes. Ces deux tranches sont ensuite supprimées et ne participent pas à

l'élaboration de la clé finale. Les trois tranches suivantes (de poids forts) sont ensuite corrigées séquentiellement en utilisant la procédure *Cascade*. Afin d'éviter qu'Eve utilise l'information échangée au cours de la procédure de réconciliation pour améliorer ses connaissances, Alice et Bob cryptent toutes leurs communications classiques avec un code de Vernam (*one-time-pad*) en utilisant une fraction des bits secrets préalablement échangés. Les blocs de parités échangés au cours de la procédure sont codés avec la même clé secrète par Alice et Bob [59], ce qui renseigne Eve sur la position des erreurs, mais ne l'informe pas de la valeur de ces erreurs. Eve peut toutefois obtenir une information supplémentaire en couplant sa connaissance des données avec la position des erreurs. Dans la procédure actuelle, cette quantité d'information est numériquement calculée et majorée en supposant une attaque par une cloneuse intriquante [73]. Cette information est ensuite supprimée lors de l'amplification de confidentialité.

Amplification de confidentialité

Afin de filtrer la connaissance de l'espion sur les éléments de clé, les bits réconciliés sont traités par une classe des fonctions de hachage [54], ce qui a pour effet de répartir les incertitudes d'Eve à l'ensemble des bits de clé finale dont elle n'aura aucune information. Dans notre cas, les bits corrigés sont considérés comme les coefficients d'un polynôme $r(x)$ dans le corps fini $GF(2^{110503})/p$ des polynômes à coefficients binaires modulo le polynôme premier $p(x) = x^{110503} + x^{519} + 1$. Le fait que cette opération soit connue et puisse être mise en œuvre efficacement a motivé notre choix [5]. Les bits secrets sont obtenus en multipliant le polynôme r par un polynôme arbitrairement choisi dans $GF(2^{110503})/p$ et publiquement annoncé. La clé finale est alors formée des coefficients binaires de la multiplication polynomiale, dont on ne conserve qu'un nombre déterminé par la borne sur l'information espionnée. Afin d'obtenir une taille de clé et une qualité de secret satisfaisantes, il est absolument crucial pour cette étape d'avoir une estimation aussi précise que possible de la quantité maximale d'information espionnée et des pertes d'information lors de la réconciliation. Enfin, le coût du codage de Vernam lors de la réconciliation est soustrait de la taille de la clé finale.

5.2.5 Taux de transferts expérimentaux

D'après le théorème de Csiszar et Körner [50, 51], la taille minimale $\mathcal{S}$ de la clé finale qu'il est possible d'extraire est donnée par $\mathcal{S} > \max(I_{AB} - I_{AE}, I_{BA} - I_{BE})$. Dans une mise en œuvre pratique, ce théorème n'est toutefois vrai que dans la mesure où les différentes parties parviennent à extraire suffisamment d'information de leur corrélations pour atteindre le taux d'information mutuelle au sens de Shannon. Si nous supposons que l'espion possède une capacité de calcul illimitée et peut atteindre les taux théoriques I_{AE} et I_{BE}, il n'en va pas de même pour la capacité de calcul de réconciliation entre Alice et Bob : des écarts inévitables de nos algorithmes réels à la limite de Shannon réduisent le taux d'information réconciliée I_{rec} entre Alice et Bob. Avec nos données expérimentales ($V \approx 40$, $\chi_{hom} + \chi_{elec} \approx 0.6$), l'efficacité des protocoles η_{rec} de réconciliation se situe autour de 85% pour le domaine des faibles atténuations du canal puis diminue entre 80% et 75% pour des atténuations plus fortes. Ceci permet d'extraire expérimentalement une information réconciliée I_{rec} égale à η_{rec} de la limite de Shannon I_{BA}. Le taux de transfert effectif de clé secrète est alors diminué pour valoir $\max(I_{rec} - I_{AE}, I_{rec} - I_{BE})$ et la portée effective de nos échanges est réduite. Pour une certaine transmission G_{min} telle que $I_{rec}(G_{min}) < I_{BE}(G_{min})$, Alice et Bob ne peuvent plus exploiter simplement leur avantage

[5] Le degré 110503 du polynôme permet de traiter 110503 bits à la fois, soit 3 tranches de 36800 impulsions ou 2 tranches de 55200 impulsions, ce qui a dirigé la structure des données optiques échangées.

V_A	G	Pertes (dB)	I_{BA} (bit)	I_{BE} ($\%I_{BA}$)	I_{rec} ($\%I_{BA}$)	Taux Réc. Inverse idéal (kbit/s)	Inverse effectif (kbit/s)	Taux Réc. Directe idéal (kbit/s)	Directe effectif (kbit/s)
40.7	1	0	2.39	0	88	1 920	1 690	1 910	1 660
37.6	0.79	1.0	2.17	58	85	730	470	540	270
31.3	0.68	1.7	1.93	67	79	510	185	190	–
26	0.49	3.1	1.66	72	78	370	75	0	–
42.7	0.26	5.9	1.48	93	71	85	–	0	–

Tableau 5.1: *Paramètres caractéristiques de l'échange de clé obtenus pour différentes valeurs de la transmission G du canal. Les différentes valeurs de la variance de la modulation d'Alice $V_A = V - 1$ sont dues à des ajustements expérimentaux différents. L'information I_{BA} est exprimée en bits par impulsion. I_{rec} est la quantité d'information obtenue par Alice et Bob avec nos algorithmes réels de réconciliation, exprimée en pourcentage de I_{AB}. Les taux idéaux seraient atteints par une réconciliation parfaite fournissant $I_{BA} - I_{BE}$ en réconciliation inverse et $I_{AB} - I_{AE}$ en direct, alors que les taux effectifs sont ceux obtenus avec notre procédure réelle (le bruit ajouté par la détection de Bob est considéré suivant l'approche "réaliste" où Eve ne contrôle pas ce bruit). Les débits d'information sont tous exprimés pour des blocs de 60 000 impulsions à 800kHz et ne prennent pas en compte le rapport cyclique (5%) de notre dispositif expérimental, ni la durée du traitement classique des données.*

quantique en réconciliation inverse, tandis que notre dispositif expérimental ne fournit plus de clé secrète.

Le tableau 5.1 présente les différents résultats de taux de transfert pour la réconciliation directe et inverse en fonction de la transmission G de la ligne. Les taux idéaux correspondent à la limite de Shannon, tandis que les taux effectifs prennent en compte notre efficacité limitée de réconciliation. Dans le cas des transmissions sans pertes avec une modulation $V \approx 40$, notre dispositif atteint le taux net de clé secrète de 1.7 Mbits/s, à comparer à une limite théorique attendue de 1.9 Mbits/s.

Avec une modulation $V \approx 40$ et une réconciliation inverse, la transmission minimale G_{min} pour extraire expérimentalement une clé secrète se situe autour de 55%. Cette transmission est alors principalement limitée par notre efficacité de réconciliation $\eta_{rec} = 80\%$. Afin d'améliorer la portée expérimentale, il est avantageux de diminuer la variance de modulation, ce qui atténue les informations mutuelles I_{BA} et I_{BE}, mais augmente le quotient I_{BA}/I_{BE} (voir la courbe 5.14). L'information à filtrer lors de l'amplification de confidentialité est donc plus faible, ce qui permet d'atteindre expérimentalement la portée de $G = 49\%$ (3.1 dB) pour $V = 27$ avec un débit de 75 kbits/s. Ceci démontre que la réconciliation inverse avec des états cohérents peut fonctionner au-dessus de la limite théorique de 3 dB des protocoles à réconciliation directe.

Une amélioration de l'efficacité de réconciliation η_{rec} se traduirait immédiatement par une augmentation de la portée de notre système. Par ailleurs, nous pourrions également limiter les possibilités d'attaques de l'espionnage : dans les deux approches "réaliste" et "paranoïaque", nous supposons toujours que l'espion dispose de dispositifs quantiques parfaits et que sa capacité de calcul est infinie. Si ces hypothèses étaient quelque peu relâchées, la portée de notre dispositif pourrait être étendue au-delà de la limite actuelle. Cependant, cette démarche n'a pas été poursuivie car nous considérons qu'il n'est pas dans le principe de la cryptographie quantique de poser des limites technologiques aux actions d'espionnage. [6]

[6] Même si on considère la prise en compte "paranoïaque" des bruits de la détection homodyne, le taux de secret

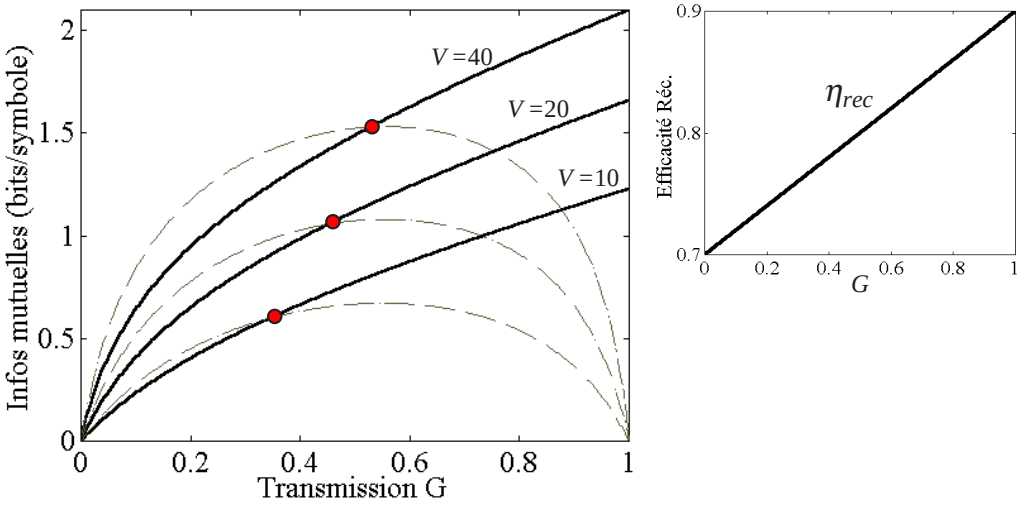

Figure 5.14: *Informations $I_{rec} = \eta_{rec} I_{BA}$ (trait plein) et I_{BE} (tirets) en fonction de la transmission G et de la variance de modulation V avec les bruits $\chi_{hom} = 0.27$ et $\chi_{elec} = 0.33$ pris en compte de façon "réaliste" et dans le cas d'un bruit du canal $\chi_{ligne} = (1-G)/G$. L'efficacité de réconciliation η_{rec} est supposée varier linéairement entre 70% pour les faibles transmissions et 90% pour les fortes transmissions (courbe de droite), ce qui est confirmé par le tableau 5.1. De plus, l'approximation simple considère que η_{rec} est indépendante de V pour $10 < V < 40$. Les points indiquent la portée maximale effective où $I_{rec} = I_{BE}$. Cette portée augmente lorsque V diminue car le ratio I_{BA}/I_{BE} devient alors plus avantageux, bien que la quantité d'information nette soit plus faible.*

5.2.6 Conclusions sur notre démonstration expérimentale

Une démonstration expérimentale *complète* du principe de distribution de clé quantique avec des états cohérents a été réalisée, incluant l'échange d'états quantiques et l'extraction algorithmique d'une clé secrète. Notre système a ainsi généré une clé secrète à un débit de 1.7 Mbits/s en l'absence de pertes et 75 kbits/s pour une transmission présentant 3.1 dB de pertes, soit dans un cas où l'espion dispose virtuellement de plus de 50% du faisceau signal. Cet ensemble constitue le premier dispositif complet et sûr de cryptographie quantique avec des variables continues [73].

De très hauts débits d'information sont ainsi atteignables tant que l'atténuation du canal de transmission n'est pas trop grande. Dans le domaine des fortes pertes, la portée de notre protocole est pour le moment limitée par l'efficacité de nos algorithmes de réconciliation, mais ses performances intrinsèques demeurent élevées par rapport aux protocoles à photons uniques [40]. A ce sujet, il faut garder à l'esprit que le domaine de la cryptographie quantique avec des variables discrètes bénéficie de progrès notables et d'un recul acquis au cours de dix années de développement depuis la première démonstration par Bennett et Brassard en 1992, alors qu'en comparaison notre première démonstration expérimentale avec des variables continues n'a été effectuée qu'en 2002.

Les limitations actuelles étant essentiellement de nature technologique (absence de modulateurs efficaces à 780nm, programmation de la réconciliation,...), de nombreuses améliorations restent possibles, tant sur le point du dispositif optique (cadence augmentée, réduction du bruit

effectif en réconciliation inverse pour une ligne sans pertes reste non-nul et vaut 195 kbits/s (le taux idéal serait de 420 kbits/s), ce qui atteste de la robustesse et du niveau de sécurité de notre système.

électronique, amélioration de l'efficacité homodyne...) que des logiciels de réconciliation (réconciliation multi-dimensionnelle [56], utilisation de turbo-codes [53, 60], nouveaux algorithmes de réconciliation binaire [58]...). La voie apparaît donc ouverte pour des protocoles simples et efficaces de cryptographie quantique à hauts débits, dont nous détaillons certaines perspectives à la section suivante.

5.3 Perspectives pratiques

5.3.1 Distances et débits atteignables

Afin d'être plus quantitatif sur les perspectives à court terme de ce dispositif, quelques éléments pratiques peuvent être avancés dans l'estimation des débits et des portées maximales atteignables de manière réaliste. Concernant le domaine des fortes transmissions ($G \approx 100\%$), il est raisonnable de concevoir une détection homodyne fonctionnant à une cadence de quelques MHz. A titre d'exemple, nous prenons 5 MHz, ce qui correspond à la vitesse maximale de la carte d'acquisition. Avec une modulation $V = 100$, notre détection homodyne à amplification de charge réalisant $\chi_{hom} = 0.25$ ($\eta_{hom} = 80\%$) et $\chi_{elec} = 0.01$, une efficacité de réconciliation $\eta_{rec} = 95\%$ aux fortes transmissions, on obtient pour $G = 1$ et dans le cas d'une absence de bruit ajouté ($\varepsilon = 0$) un taux secret net $\underleftarrow{\Delta I} = 3$ bits/impulsion, soit un débit secret net de 15 Mbits/s. Si on intègre de plus un faible bruit ajouté lors de l'échange $\varepsilon = 0.1$, le taux de secret aux fortes transmissions demeure à $\underleftarrow{\Delta I} = 1.3$ bits/impulsion, soit un débit de 6.5 Mbits/s.

Concernant la distance maximale atteignable de façon réaliste avec nos protocoles, notre dispositif a déjà obtenu le résultat d'échanger une clé secrète pour une transmission $G = 0.49$ soit des pertes de 3.1 dB, que l'on associe à une distance atteignable de l'ordre de 15 km lors d'une transmission par fibre optique (étendue au domaine 1.55 μm avec des pertes standard de 0.2 dB/km). En améliorant sensiblement le dispositif tel que décrit dans le paragraphe précédent (débit 5 MHz, bruit $\chi_{hom} = 0.25$, $\chi_{elec} = 0.01$) et en optimisant la variance de modulation à $V = 15$, ce système atteindrait la transmission de $G = 0.32$ (pertes 5 dB ou distance de 25 km) avec un taux de transfert de $\underleftarrow{\Delta I} = 0.05$ bits/impulsion, soit un débit appréciable de 250 kbits/s. L'efficacité de réconciliation requise pour ce niveau est $\eta_{rec} = 85\%$, ce qui semble encore tout à fait raisonnable.

5.3.2 Prototype complet

L'essentiel des limitations du dispositif optique actuel provient de l'absence de modulateurs d'amplitude et de phase adéquats à 780 nm. Afin d'éviter de plus une forte atténuation lors d'une propagation fibrée, il est judicieux de concevoir un système opérant aux longueurs d'ondes télécom (1540-1580 nm) où la technologie commercialement disponible est plus appropriée. Par ailleurs, du fait des problèmes de stabilisation de la phase, il n'est pas réaliste de transmettre séparément le faisceau oscillateur local et le faisceau signal. Une possibilité serait alors de transmettre dans la même fibre optique les impulsions signal et oscillateur local décalées temporellement d'une durée relativement faible (typiquement 5 ns pour un modulateur au GHz et des impulsions de durée 1 ns). La figure 5.15 donne un schéma de principe d'un dispositif optique de ce type. Les impulsions suivent alors sensiblement le même chemin optique et toute perturbation de phase de fréquence inférieure à la centaine de MHz n'affectera pas la phase relative. Pour faire interférer l'impulsion signal avec l'impulsion oscillateur local correspondante, il faut séparer à nouveau les impulsions afin de compenser le retard introduit. Cette opération doit impérativement conserver la phase relative, mais comme la démodulation est effectuée au sein

de l'unité réceptrice et ne fait intervenir que des bras d'interféromètre de quelques mètres (1.5 m pour un décalage de 5 ns), la conservation de la phase relative devrait être plus simple à réaliser expérimentalement. Ce dispositif demeure cependant une réalisation technologique d'envergure et se heurte à de nombreux autres problèmes comme le maintien de la polarisation ou les pertes d'insertion dans le démodulateur.

Dans le cadre du projet européen *SECOQC* (*SEcure COmmunication based on Quantum Cryptography*), un partenariat avec la société *Thalès* est actuellement en cours afin de réaliser un prototype complet de cryptographie quantique avec des états cohérents opérant à la longueur d'onde télécom 1.55 μm. Notre équipe a ainsi l'opportunité de collaborer spécifiquement avec Mrs. Thierry Debuisschert (*Thalès TRT*) et Jérôme Lodewyck (*Thalès TRT / LCFIO*).

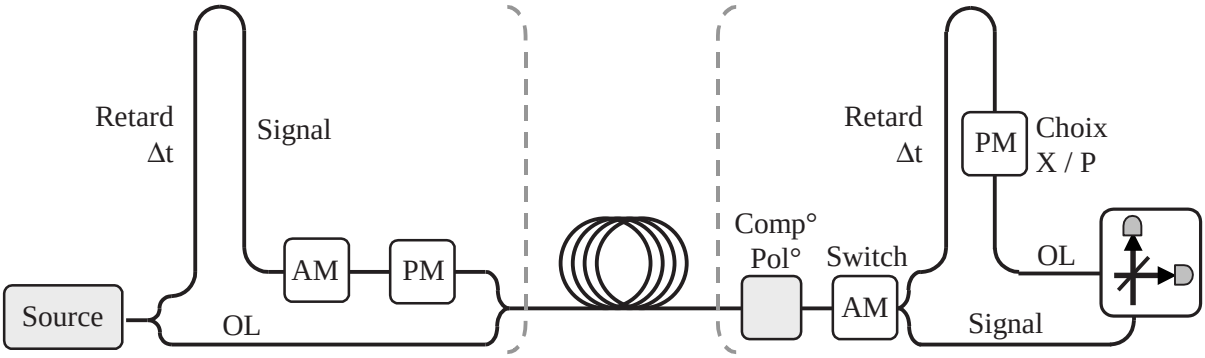

Figure 5.15: *Esquisse de prototype de cryptographie quantique avec des impulsions cohérentes. Pour ce dispositif, les impulsions signal et oscillateur local sont décalées temporellement de* $\Delta t \approx$ *quelques ns. AM : modulateur d'amplitude, PM : modulateur de phase.*

5.3.3 Que faire avec des bits parfaitement secrets ?

Cette question quelque peu iconoclaste a été soulevée par Gilles Brassard [204]. Si la très large majorité des protocoles de cryptographie quantique conçoit le transfert de clé secrète pour une utilisation ultérieure avec un code de Vernam (*one-time-pad*), cette application n'est peut-être pas forcément la plus adéquate. En effet, bien que depuis la démonstration de Shannon [41], le code de Vernam est connu pour être parfaitement sûr (lorsque la clé binaire aléatoire est aussi longue que le message et utilisée une seule fois), ce code est également connu pour souffrir d'un débit lent et d'une forte consommation de bits secrets.

Une autre possibilité [204] – non inconditionnellement sûre – serait d'utiliser les bits secrets pour effectuer un cryptage à clé privée de type AES [39] sur 128 bits et d'utiliser des techniques standard d'expansion de clé. Ce dispositif permet alors de hauts débits de cryptage. De plus, si le canal quantique fonctionne en parallèle, il est tout à fait possible de changer de nombreuses fois par seconde les 128 bits secrets de la base AES, ce qui fournirait déjà un niveau de sécurité inégalé pour ces débits.

Chapitre 6

Influence de l'intrication en cryptographie quantique avec des variables continues

Sommaire

Nous avons démontré qu'il était possible de concevoir des protocoles de cryptographie quantique avec des états quasi-classiques (chapitre 4). Ces protocoles peuvent être simplement mis en œuvre en modulant une source laser impulsionnelle et en effectuant des mesures homodynes résolues en temps (chapitre 5). Même si aucun état intriqué n'est expérimentalement utilisé, le phénomène d'intrication quantique joue cependant un rôle essentiel dans l'analyse de la sécurité d'un protocole inverse à états cohérents. L'argument majeur dans la démonstration de sécurité est que l'espionnage d'Eve doit vérifier la relation d'Heisenberg pour toute valeur de corrélations physiquement autorisées par le champ émis par Alice, indépendamment de la technique effectivement utilisée. Ainsi, la borne supérieure sur l'information espionnée repose sur l'intrication qu'Alice et Bob *auraient* pu utiliser étant données les propriétés de leurs dispositifs quantiques, et non pas sur l'intrication effectivement utilisée.

L'objectif de ce chapitre est de discuter l'influence précise de l'intrication pour la transmission d'une clé secrète. Après la présentation détaillée et comparée d'un protocole à états intriqués (sections 6.1 et 6.2), il est démontré dans la section 6.3 que les protocoles directs et inverses de cryptographie quantique à états cohérents (sans intrication) sont équivalents à des protocoles

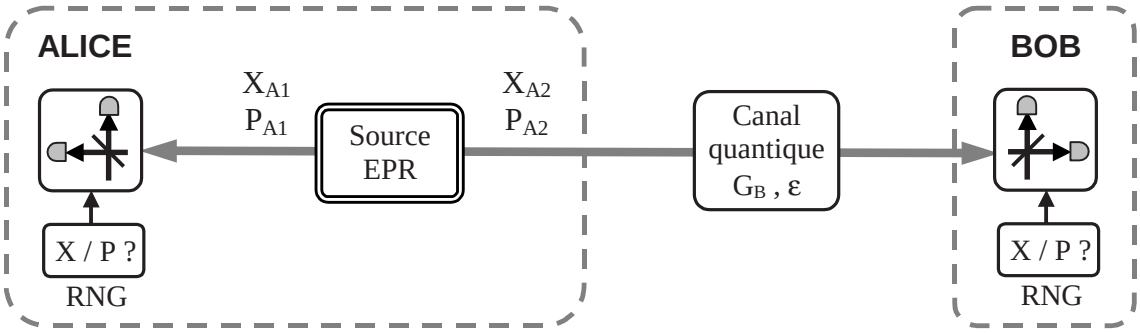

Figure 6.1: *Protocole simple à états intriqués. Un générateur de nombres aléatoires binaires (RNG : random number generator) permet d'effectuer le choix de la quadrature de mesure pour chaque impulsion incidente sur la détection homodyne.*

utilisant des états intriqués. Enfin, les critères de sécurité de nos protocoles sont comparés aux conditions de séparabilité de l'intrication pour des variables continues. La sécurité d'un protocole de cryptographie apparaît alors comme reliée à la capacité du canal à transmettre de l'intrication quantique, et non pas à l'intrication effectivement transmise [1].

6.1 Premier protocole à états EPR

Dans un protocole simple utilisant des états intriqués tel que présenté sur la figure 6.1, Alice dispose d'une source d'états EPR à deux modes dont les quadratures (X_{A1}, P_{A1}) et (X_{A2}, P_{A2}) sont de valeurs moyennes nulles. Pour chaque impulsion, Alice choisit aléatoirement de mesurer la quadrature X ou P du faisceau $A1$ tandis que le faisceau $A2$ est envoyé à Bob au travers d'un canal quantique de gain G et de bruit ajouté $\chi_B = (1-G)/G + \varepsilon$. De son côté, Bob effectue également une mesure homodyne après un choix aléatoire de la quadrature à mesurer. A la fin de l'échange d'états quantiques, Alice et Bob annoncent publiquement la direction de mesure qu'ils avaient choisie pour chaque impulsion, ce qui leur permet de supprimer les mesures où leurs directions diffèrent pour ne conserver que les mesures corrélées. Nécessairement, à ce niveau, Alice et Bob perdent environ la moitié des impulsions échangées. Ceci diminue d'un facteur 2 le débit de clé secrète mais simplifie l'analyse de la sécurité. La suite du protocole se poursuit alors comme pour le protocole à états cohérents : estimation publique des paramètres G et χ_B de la ligne, réconciliation par tranches et amplification de confidentialité.

Pour mettre ce protocole en équation, nous utilisons la représentation des états EPR par un paramètre V tel que décrit dans le tableau 2.1 de la section 2.3.5. On a alors :

$$\langle {X_{A1}}^2 \rangle = \langle {P_{A1}}^2 \rangle = \langle {X_{A2}}^2 \rangle = \langle {P_{A2}}^2 \rangle = V\, N_0 \tag{6.1}$$

$$\langle X_{A1}\, X_{A2} \rangle = \sqrt{V^2-1}\, N_0 \qquad \langle P_{A1}\, P_{A2} \rangle = -\sqrt{V^2-1}\, N_0 \tag{6.2}$$

$$V_{X_{A2}|X_{A1}} = V_{P_{A2}|P_{A1}} = \frac{N_0}{V} \tag{6.3}$$

[1] Ce travail a donné lieu à la publication [75] et a été mené postérieurement aux propositions théoriques de cryptographie avec des états cohérents [70, 74] ainsi qu'à leur réalisation expérimentale [73]. L'équivalence entre un protocole à états cohérent et un protocole utilisant de l'intrication a constitué un prérequis essentiel pour la preuve de sécurité inconditionnelle de la cryptographie inverse à états cohérents [76].

Une interprétation générale de cette source est de considérer qu'en mesurant une quadrature X_θ du mode $A1$, Alice projette le faisceau $A2$ sur un état comprimé en X_θ de variance $s\,N_0 = V_{A2|A1} = N_0/V$. L'utilisation de faisceaux intriqués garantit une compression $s = 1/V$ maximale étant donnée la modulation. On peut également relever que l'utilisation d'états intriqués assure par la même occasion la modulation du faisceau suivant une distribution gaussienne de variance V. Alice n'a alors pas besoin d'utiliser des modulateurs d'amplitude et de phase. De même, la valeur aléatoire de la modulation est directement effectuée au niveau quantique sans nécessiter une source externe classique de nombres aléatoires, qui constitue toujours un point délicat à réaliser en cryptographie.

Par exemple, une des quadratures du faisceau reçu par Bob s'écrit :

$$X_B = \sqrt{G}\,(\,X_{A2} + N_{X,B}\,) \tag{6.4}$$

où $N_{X,B}$ est un terme de bruit indépendant équivalent en entrée de variance $\chi_B\,N_0$. Ce protocole étant symétrique par rapport aux quadratures X et P, le meilleur espionnage sera lui aussi nécessairement symétrique, et on considère alors que le bruit ajouté est de même variance sur les quadratures X et P. La variance des mesures de quadratures de Bob s'écrit comme dans le cas des états cohérents :

$$\langle {X_B}^2 \rangle = V_B\,N_0 = G\,(V + \chi_B)\,N_0 \tag{6.5}$$

Dans le cas présent des états intriqués, la variance conditionnelle d'Alice sur les mesures de Bob vaut :

$$\begin{aligned} V_{B|A,EPR} = V_{X_B|X_{A1}} = V_{P_B|P_{A1}} &= \langle {X_B}^2 \rangle - \frac{\langle X_{A1}\,X_B \rangle^2}{\langle {X_{A1}}^2 \rangle} && \text{(6.6a)} \\ &= G\,(V + \chi_B)\,N_0 - G_B\,\frac{V^2 - 1}{V}\,N_0 && \text{(6.6b)} \\ &= G\,(\frac{1}{V} + \chi_B)\,N_0 && \text{(6.6c)} \end{aligned}$$

L'équation (6.6c) indique la valeur minimale de la variance conditionnelle d'Alice sur Bob étant donnée la matrice densité ρ_A de l'état transmis à Bob et la variance totale de modulation V [75]. Dans le cas de la réconciliation inverse, c'est cette valeur qui doit être utilisée pour borner l'espionnage d'Eve en saturant la relation d'Heisenberg (4.22), même si aucune intrication n'est physiquement exploitée dans le montage.

6.2 Sécurité du protocole à états EPR

6.2.1 Informations mutuelles

Pour analyser la sécurité d'un protocole à états intriqués, nous reprenons la démarche introduite au chapitre 4 et exprimons les différentes informations mutuelles entre Alice, Bob et Eve. Il faut tenir compte ici que du fait du choix aléatoire de mesure par Alice et Bob, seuls 50% des impulsions sont mesurées pour la même quadrature et seront utilisées dans l'élaboration d'une

clé secrète.

$$I_{AB,EPR} = I_{BA,EPR} = \frac{1}{2}\frac{1}{2}\log_2\left(\frac{\langle {X_B}^2\rangle}{V_{B|A,EPR}}\right) = \frac{1}{4}\log_2\left(\frac{V+\chi_B}{\frac{1}{V}+\chi_B}\right) \quad (6.7)$$

$$I_{AE,EPR} = \frac{1}{2}\frac{1}{2}\log_2\left(\frac{V+\frac{1}{\chi_B}}{\frac{1}{V}+\frac{1}{\chi_B}}\right) = \frac{1}{4}\log_2\left(\frac{\chi_B V+1}{\frac{\chi_B}{V}+1}\right) \quad (6.8)$$

$$I_{BE,EPR} = \frac{1}{2}\frac{1}{2}\log_2\left(\frac{\langle {X_B}^2\rangle}{V_{B|E,opt}}\right) = \frac{1}{4}\log_2\left(G^2\,(V+\chi_B)(\frac{1}{V}+\chi_B)\right) \quad (6.9)$$

On peut remarquer à ce niveau que la variance conditionnelle optimale d'Eve sur les données de Bob est la même avec des états EPR qu'avec des états cohérents. Ceci provient du fait que l'on considère toujours un espionnage maximal selon la physique autorisée par la relation d'Heisenberg (4.22), indépendamment de la nature physique exacte des états employés.

6.2.2 Réconciliation directe

Un protocole de réconciliation directe est sûr si $I_{AB} > I_{AE}$ [50] et le taux de transfert secret vaut au moins :

$$\underrightarrow{\Delta I}_{EPR} = I_{AB,EPR} - I_{AE,EPR} = \frac{1}{2}\log_2\left(\frac{V+\chi_B}{\chi_B\,V+1}\right) = \underrightarrow{\Delta I}_{coh} \quad (6.10)$$

On retrouve ici le taux de transfert $\underrightarrow{\Delta I}_{coh}$ obtenu pour les protocoles directs à états cohérents. La condition de sécurité est alors la même : $\chi_B < 1$, ce qui n'est possible que pour des transmissions supérieures à 50%.

D'une manière générale, on peut montrer que le taux de transfert en réconciliation directe ne dépend pas du facteur de compression utilisé [70, 71]. Il faut cependant noter que l'on considère seulement des protocoles simples à états EPR, où Alice et Bob ne s'accordent pas sur le choix de quadrature une impulsion sur deux en moyenne. Si Alice et Bob pouvaient s'accorder de manière déterministe et secrète sur la quadrature à mesurer, le taux de transfert serait alors doublé dans le cas d'un protocole EPR (théoriquement, il suffirait que Bob puisse disposer d'une mémoire quantique parfaite identique à celles utilisées par Eve pour attendre qu'Alice révèle sa direction de mesure). On pourrait imaginer qu'Alice et Bob se servent d'une clé secrète aléatoire préétablie entre eux pour déterminer leur choix de mesure. Dans ce cas, le taux de transfert secret vaudrait $2\underrightarrow{\Delta I}_{coh} - 1$ pour tenir compte du bit de codage de la direction de mesure consommé par chaque impulsion.

Une autre possibilité serait de faire varier la répartition entre les mesures de quadratures pour privilégier une certaine direction : Alice et Bob mesurent par exemple aléatoirement la quadrature X avec une probabilité ξ ($\approx 90\%$)et la quadrature P avec une probabilité $1-\xi$. Dans ce cas, Alice et Bob s'accordent sur le choix de quadrature mesurée à hauteur d'une portion $\xi^2 + (1-\xi)^2$ des impulsions échangées. Le taux de transfert avec des états EPR serait alors de $2\left[\xi^2 + (1-\xi)^2\right]\underrightarrow{\Delta I}_{coh}$. Le point délicat dans l'analyse de la sécurité est qu'alors il n'est pas immédiat de prouver que la meilleure attaque d'Eve est une attaque symétrique. Par ailleurs, Eve pourrait également modifier la statistique de la répartition entre les quadratures.

6.2.3 Réconciliation inverse

Le taux de transfert secret en réconciliation inverse est donné par :

$$\underleftarrow{\Delta I}_{EPR} = I_{BA,EPR} - I_{BE,EPR} = -\frac{1}{2}\log_2\left(G\,(\chi_B + \frac{1}{V})\right) \quad (6.11)$$

Ce terme est positif et le protocole est sûr à la condition $G(\chi_B + 1/V) < 1$, ce qui est possible pour toute valeur de la transmission de la ligne et s'écrit en fonction du bruit ajouté ε :

$$\textit{Sécurité protocole EPR inverse} \Leftrightarrow \varepsilon < \frac{V-1}{V} \approx 1 \tag{6.12}$$

Un protocole inverse à états EPR est donc plus robuste à un excès de bruit qu'un protocole à états cohérents qui ne peut tolérer que $\varepsilon < (V-1)/2V \approx 1/2$.

On peut comparer le taux de transfert avec des états EPR au cas des états cohérents :

$$\underleftarrow{\Delta} I_{coh} = -\frac{1}{2}\log_2\left(G^2\,(1+\chi_B)\,(\frac{1}{V}+\chi_B)\right) \tag{6.13a}$$

$$= \underleftarrow{\Delta} I_{EPR} - \frac{1}{2}\log_2\left(G\,(1+\chi_B)\right) \tag{6.13b}$$

$$= \underleftarrow{\Delta} I_{EPR} - \frac{1}{2}\log_2\left(1+G\,\varepsilon\right) \tag{6.13c}$$

D'une manière générale on a alors :

$$\underleftarrow{\Delta} I_{coh} \leq \underleftarrow{\Delta} I_{EPR} \tag{6.14}$$

avec égalité si l'excès de bruit ε est nul. Dans un cas où tout le bruit ajouté provient exclusivement des pertes, l'utilisation de l'intrication n'améliore donc pas le taux de transfert secret pour ce type de protocole.

Même si les protocoles simples à états intriqués présentent des taux de transfert sensiblement identiques à un protocole à états cohérents, ils offrent néanmoins certains avantages spécifiques, liés à l'utilisation physique de l'intrication. Les quantités d'information espionnées I_{AE} et I_{BE} sont plus faibles dans le cas EPR que dans le cas des états cohérents. La procédure d'amplification de confidentialité est donc plus simple et plus robuste à mettre en œuvre. De plus, le dispositif expérimental à états intriqués est aussi dispensé d'une source aléatoire externe de modulation continue. Ceci constitue une particularité importante pour un système de cryptographie, où la qualité des sources classiques de nombres aléatoires est toujours un point délicat. Enfin, un avantage quantique spécifique des protocoles EPR est qu'il est possible d'envisager l'utilisation de protocoles de distillation de l'intrication pour augmenter la portée de distribution pratique.

Nous introduisons maintenant un second protocole à états EPR, dont l'étude apporte un éclairage nouveau sur l'influence de l'intrication dans la sécurité quantique.

6.3 Intrication virtuelle et états cohérents

Une autre possibilité pour Alice d'utiliser des états intriqués est de mesurer simultanément les quadratures X_{A1} et P_{A1} de son faisceau (voir la figure 6.2). Une telle mesure simultanée peut se faire par exemple en divisant le faisceau sur une lame séparatrice de réflectivité 50% puis en effectuant une mesure homodyne de chaque bras. Ces mesures sont alors notées $\overline{X}_A$ et $\overline{P}_A$ et suivent une distribution gaussienne de variance $\langle \overline{X}_A{}^2 \rangle = \langle \overline{P}_A{}^2 \rangle = \frac{V+1}{2} N_0$.

Par rapport à l'autre faisceau (X_{A2}, P_{A2}) en sortie de la source, les mesures d'Alice fournissent les informations :

$$\langle \overline{X}_A\, X_{A2} \rangle = -\langle \overline{P}_A\, P_{A2} \rangle = \sqrt{\frac{V^2-1}{2}}\, N_0 \tag{6.15}$$

$$V_{X_{A2}|\overline{X}_A} = V_{P_{A2}|\overline{P}_A} = V\, N_0 - \frac{(V^2-1)/2}{(V+1)/2}\, N_0 = N_0 \tag{6.16}$$

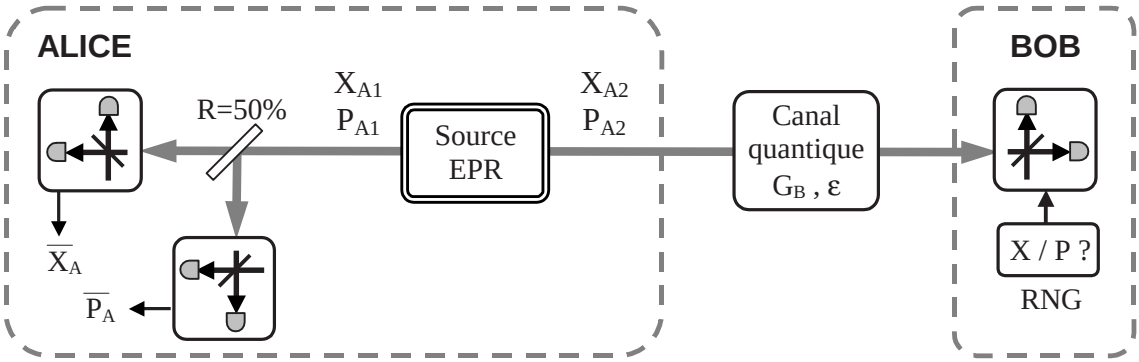

Figure 6.2: *Protocole symétrique à états intriqués : Alice divise son faisceau EPR en deux parties qu'elle mesure avec une détection homodyne, ce qui fournit les résultats* $(\overline{X}_A, \overline{P}_A)$ *pour chaque impulsion.*

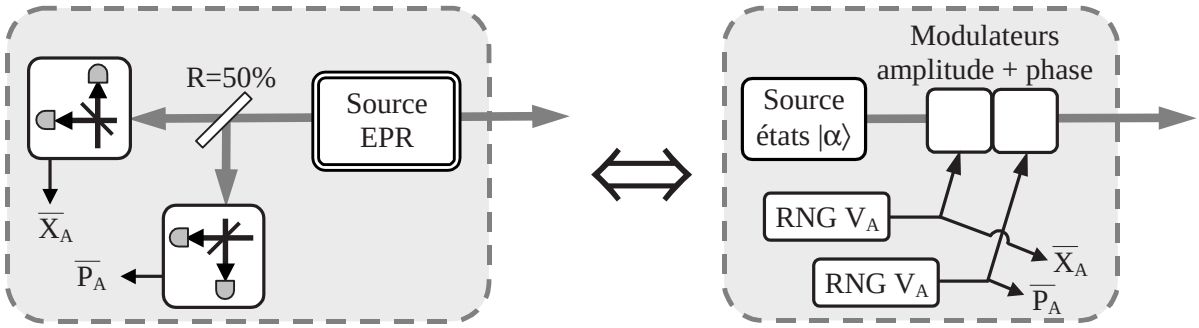

Figure 6.3: *Sources équivalentes pour la cryptographie quantique(avec ou sans intrication réelle). RNG* V_A *désigne un générateur parfait de nombre aléatoire suivant une distribution gaussienne de variance* V_A*.*

En d'autres termes, la mesure simultanée d'Alice projette l'état $A2$ en un état cohérent. Les valeurs moyennes des quadratures sont proportionnelles aux résultats d'Alice $(\overline{X}_A, \overline{P}_A)$ et avec une incertitude fixée au bruit de photon N_0, comme si Alice avait préparé un état cohérent modulé suivant une distribution gaussienne (voir la figure 6.3).

Par rapport aux mesures de Bob (X_B, P_B), Alice dispose des corrélations :

$$\langle \overline{X}_A \, X_B \rangle = -\langle \overline{P}_A \, P_B \rangle = \sqrt{\frac{G}{2}} \sqrt{V^2 - 1} \, N_0 \tag{6.17}$$

$$\begin{aligned} V_{B|A,EPR} = V_{X_B|\overline{X}_A} = V_{P_B|\overline{P}_A} &= G\,(V + \chi_B)\,N_0 - G\,\frac{V^2-1}{V+1}\,N_0 \\ &= G\,(1 + \chi_B)\,N_0 \\ &= V_{B|A,coh} \end{aligned} \tag{6.18}$$

Dans le cas présent, Alice ne possède ainsi pas davantage d'information sur la mesure de Bob que dans le cas d'un état cohérent modulé.

Supposons que l'ensemble de la source d'Alice soit placé dans une boîte noire. Les seuls éléments émergeant de cette boîte sont le faisceau (X_{A2}, P_{A2}) et les valeurs $\overline{X}_A$ et $\overline{P}_A$. Cette boîte noire n'est alors pas distinguable d'une autre boîte noire, représentée sur la figure 6.3, où les nombres $\overline{X}_A$ et $\overline{P}_A$ sont choisis par un générateur aléatoire gaussien de variance adéquate et le faisceau émergent (X_{A2}, P_{A2}) est issu d'une source d'états cohérents modulés.

Nous appelons cette possibilité l'*intrication virtuelle* [75] : même si Alice n'utilise pas effectivement d'intrication pour générer ses états cohérents modulés, il existe un dispositif absolument équivalent (la boîte noire présentée sur la figure 6.3) qui utilise l'intrication quantique. Cette affirmation s'appuie sur le fait que la sortie de tout appareil physique, y compris le système d'espionnage d'Eve, ne peut dépendre que de la matrice densité de ses entrées (ici le faisceau émis par Alice) et non pas de la manière dont ces entrées ont été préparées. La sécurité d'un protocole de cryptographie apparaît alors comme reliée à la capacité du canal à transmettre de l'intrication quantique, et non pas à l'intrication effectivement transmise, comme nous allons le souligner plus précisément à la section suivante.

6.4 Critères de sécurité et de séparabilité

6.4.1 Séparabilité d'une intrication en quadratures

Si le canal quantique entre Alice et Bob est de trop mauvaise qualité, l'*intrication virtuelle* entre (X_{A1}, P_{A1}) et (X_B, P_B) sera détruite. Le seuil à partir duquel cet effet intervient peut être calculé en utilisant le critère de séparabilité de Duan et Simon pour les variables continues d'un état gaussien à deux modes [134, 135]. D'après l'équation (17) de la référence [134], le critère pour que l'état entre Alice et Bob présente toujours de l'intrication virtuelle s'écrit :

$$(\langle {X_{A1}}^2 \rangle - N_0)\,(\langle {X_B}^2 \rangle - N_0) < \langle X_{A1}\, X_B \rangle^2 \tag{6.19}$$

avec

$$\langle {X_{A1}}^2 \rangle = V\, N_0 \tag{6.20a}$$

$$\langle {X_B}^2 \rangle = G\,(V + \frac{1-G}{G} + \varepsilon)\, N_0 \tag{6.20b}$$

$$\langle X_{A1}\, X_B \rangle = \sqrt{G}\,\sqrt{V^2-1}\, N_0 \tag{6.20c}$$

Dans notre cas, le critère (6.19) devient :

$$G(V-1)(V-1+\varepsilon) < G(V-1)(V+1) \tag{6.21}$$

Ce qui se formalise en le résultat :

$$Non - séparabilité\ \ Duan - Simon \Leftrightarrow \varepsilon < 2 \tag{6.22}$$

L'intrication virtuelle est donc présente dès que la modulation et la transmission de la ligne sont non-nulles ($V > 1$ et $G > 0$), à la seule condition que l'excès de bruit ajouté par le canal ne dépasse pas le seuil de deux fois le niveau de bruit de photon N_0.

6.4.2 Comparaison aux critères de sécurité

Le tableau 6.1 résume les différents critères de sécurité pour nos protocoles de cryptographie en fonction de l'excès de bruit ε de la ligne. Pour les protocoles directs, à états cohérents ou

intriqués, le critère de sécurité impose $\varepsilon < 1$ de telle sorte que la condition d'intrication virtuelle (6.22) est toujours vérifiée. Pour les protocoles inverses, la condition de sécurité requiert $\varepsilon < 1/2$ pour les états cohérents et $\varepsilon < 1$ pour les états EPR, et ainsi la condition de non-séparabilité $\varepsilon < 2$ est également toujours vérifiée. Ces résultats sont présentés sur la figure 6.4, où la condition d'intrication est comparée à nos seuils de sécurité. Il apparaît alors clairement que les zones de sécurité des différents protocoles directs et inverses sont nettement à l'intérieur de la zone d'intrication, où le canal quantique peut distribuer de l'intrication utile.

Protocole	**Direct**	**Inverse**
Etats cohérents	$\varepsilon < 2 - \frac{1}{G}$	$\varepsilon < \frac{V-1}{2V} \approx \frac{1}{2}$
Etats intriqués	$\varepsilon < 2 - \frac{1}{G}$	$\varepsilon < \frac{V-1}{V} \approx 1$

Tableau 6.1: *Conditions de sécurité des protocoles de cryptographie quantique à variables continues [70, 73] pour un canal de gain G et de bruit équivalent en entrée $\chi_B = (1-G)/G + \varepsilon$, où ε désigne l'excès de bruit non-lié aux pertes.*

Le seuil de non-séparabilité $\varepsilon = 2$ correspond physiquement au cas d'un espionnage de type *intercept-resend* [63] où Eve divise le faisceau $A2$ provenant d'Alice en deux parties pour effectuer une mesure simultanée des quadratures X et P et ré-émettre un faisceau cohérent centré sur le résultat de ses mesures. Eve doit alors supporter le coût d'un bruit en entrée d'une fois le bruit de photon N_0 ("taxe quantique" selon [146]) pour la mesure simultanée de X et P, puis une deuxième "taxe quantique" N_0 au niveau de la ré-émission de l'état cohérent. Le bruit ajouté du côté de Bob (en plus du bruit de photon) sera alors de $2\,N_0$, soit $\varepsilon = 2$ [63]. En d'autres termes, au niveau où l'état conjoint d'Alice et Bob devient séparable ($\varepsilon = 2$), il existe une attaque explicite d'espionnage, ce qui interdit l'existence de tout protocole sûr de cryptographie.

La région entre la condition de non-séparabilité et la limite de sécurité des protocoles EPR connus, $1 < \varepsilon < 2$ correspond à une région où le canal quantique peut toujours transmettre de l'intrication, mais où les protocoles connus ne sont plus sûrs. L'existence même de protocoles sûrs opérant dans cette région reste pour le moment une question ouverte. La différence entre nos conditions de sécurité et la condition d'intrication semble indiquer que nos protocoles n'utilisent pas efficacement toutes les ressources d'intrication disponible. En principe, des procédures basées sur la purification quantique de l'intrication [1], ou sur la distillation classique de l'avantage (*advantage distillation* [55]) permettent d'exploiter l'intrication jusqu'à ses limites ultimes, mais ces procédures soit sont très difficiles à mettre en œuvre expérimentalement (purification quantique), soit proposent des débits de clé secrète extrêmement bas (distillation classique). Une seconde question ouverte est de déterminer l'origine de la différence entre les seuils de sécurité et d'intrication. Est-ce que cet effet provient des observables de mesure limitées, de la procédure d'extraction de bits ou bien d'un autre phénomène ?

Enfin, nous pouvons également nous intéresser à un autre critère caractérisant l'intrication, énoncé par Reid et Drummond [133]. Ce critère, plus restrictif que celui de Duan-Simon (6.19), caractérise la violation du "paradoxe" Einstein-Podolsky-Rosen (voir le chapitre 10) :

$$V_{X_B|X_{A1}}\, V_{P_B|P_{A1}} < {N_0}^2 \tag{6.23}$$

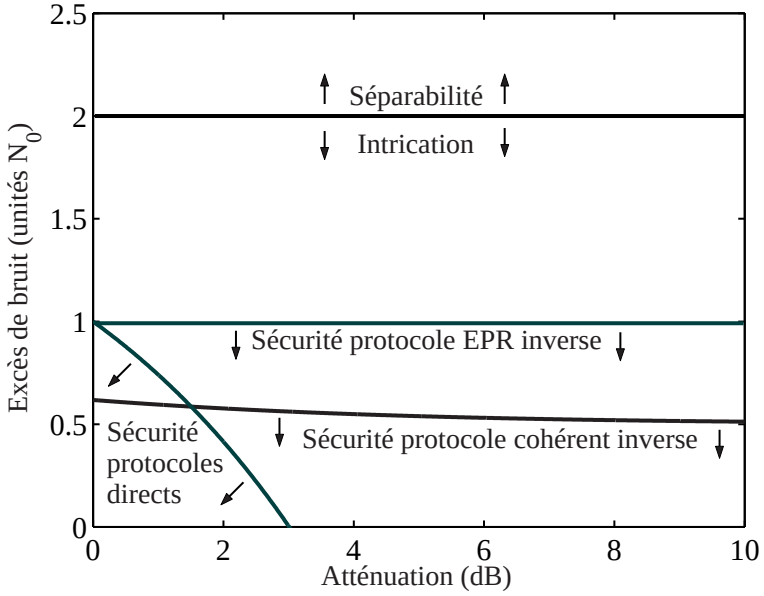

Figure 6.4: *Excès de bruit ε en fonction de l'atténuation de la ligne $-10\log_{10} G$, dans le cas des fortes modulations ($V \gg 1$).*

Pour le cas du protocole à intrication réelle vu à la section 6.1, on a $V_{X_B|X_{A1}} = V_{P_B|P_{A1}} = G(\chi_B + 1/V)N_0$ et le critère de Reid-Drummond devient :

$$G\,(\frac{1-G}{G} + \varepsilon + \frac{1}{V}) < 1 \tag{6.24}$$

soit

$$\varepsilon < \frac{V-1}{V} \tag{6.25}$$

ce qui correspond exactement à la limite de sécurité de nos protocoles inverses à états intriqués.

Pour le cas des protocoles à intrication virtuelle, $V_{X_B|X_{A1}} = V_{P_B|P_{A1}} = G(\chi_B + 1)N_0$. Le critère de Reid-Drummond (6.23) s'écrit alors $1 + G\varepsilon < 1$, ce qui trivialement ne peut pas être vérifié pour G et $\varepsilon \geq 0$. Ce résultat était tout à fait prévisible : dans le cas de l'intrication virtuelle, Alice et Bob ne possèdent pas davantage d'information que dans le cas où Alice utilise des états cohérents déplacés, qui ne présentent aucune intrication physique et ne peuvent prétendre violer le paradoxe EPR (6.23). Cependant, même si le protocole à intrication virtuelle ne vérifie pas la condition d'intrication de Reid-Drummond, ce protocole peut tout de même être sûr si $\varepsilon < 1/2$. Les conditions de sécurité suivent donc une intrication virtuelle qui pourrait être présente, mais n'est pas réellement utilisée...

6.5 Conclusion

Nous avons démontré dans ce chapitre le résultat qu'un protocole à états cohérents pouvait être considéré comme complètement équivalent à un protocole utilisant des états intriqués. Par ailleurs, les conditions de sécurité de nos protocoles à états cohérents sont nettement dans le domaine de la non-séparabilité de l'intrication au sens de Duan et Simon. Ces résultats ont

offert une nouvelle compréhension du lien entre la sécurité quantique et l'usage de l'intrication, et ont contribué aux preuves ultérieures de sécurité inconditionnelle de nos protocoles [76, 77].

L'équivalence dans le domaine des variables continues entre un protocole à états cohérents et un protocole à états intriqués n'est pas sans rappeler l'analogie présentée dans [45] pour les variables discrètes entre le protocole sans intrication BB84 [43] et le protocole EPR proposé par Ekert [44]. L'étude du lien entre la sécurité et l'intrication a été poussée plus loin par Acin et ses collaborateurs [49], qui démontrent une équivalence complète dans le cas des variables quantiques discrètes entre l'intrication de deux qubits et la sécurité d'un protocole de distribution de clé : une clé secrète peut être échangée de manière sûre au travers d'un canal quantique si et seulement si ce canal permet la distribution de l'intrication.

Si dans le domaine des variables continues nos preuves de sécurité ne possèdent pas encore ce recul, il serait cependant faux de conclure de cette étude que l'utilisation réelle de faisceaux EPR ne présente aucun intérêt pour la cryptographie quantique. Comme nous l'avons vu lors de la réalisation expérimentale des protocoles à états cohérents (chapitre 5), l'usage des variables continues avec des états cohérents ne permet pas d'envisager des portées de transmission plus grandes que celles des protocoles à photons uniques. Du fait de l'absorption exponentielle dans une fibre optique, les protocoles actuels atteignent une limite en distance de transmission entre 10 et 100km. Au-delà de cette distance, les bits secrets sont noyés dans diverses erreurs, qui vont des coups d'obscurité des détecteurs à un traitement imparfait des données. Pour dépasser ces distances et améliorer la situation actuelle, un défi expérimental majeur serait de mettre en œuvre des procédures de distillation de l'intrication pour réaliser un répéteur quantique [160]. De façon ultime, les bits secrets seraient simplement téléportés dans la station réceptrice avec laquelle un partage d'intrication quantique aurait été préalablement effectué [158]. Pour toutes ces propositions de distribution de clé à longue distance, l'utilisation réelle de l'intrication et des états EPR apparaît comme un prérequis essentiel : sans intrication, aucune distillation quantique n'est évidemment envisageable. Cet état de fait nous a donc conduit à développer un dispositif expérimental de génération d'états spécifiquement quantiques, en vue de futures applications pour des protocoles de communication quantique à longue distance. La description de ce dispositif et de ses applications fera l'objet de la prochaine partie de cette thèse.

Partie III

Source impulsionnelle d'états non-classiques : dispositif et applications

Chapitre 7

Génération d'états comprimés par amplification paramétrique

Sommaire

Dans le domaine très actif du traitement de l'information quantique avec des variables continues [3], la génération et la détection d'états spécifiquement quantiques est un sujet d'un intérêt considérable. Les états comprimés ou intriqués peuvent être directement utilisés comme une ressource quantique pour des protocoles de cryptographie (voir les références citées dans [70]). Ils servent ainsi à améliorer la robustesse des protocoles par rapport à l'utilisation d'états cohérents, ou à atteindre des portées de transfert plus longues (distillation de l'intrication et répéteurs quantiques [160]). Par ailleurs, la combinaison de deux vides comprimés sur une lame semi-réfléchissante génère un état bi-mode maximalement intriqué, nécessaire pour effectuer certaines tâches de l'information quantique comme la téléportation quantique [146] ou le codage dense [162]. Enfin, la compression des fluctuations quantiques apparaît comme une ressource essentielle pour effectuer des opérations de calcul quantique avec des variables continues [161].

Depuis la première expérience de génération d'états comprimés par Slusher et ses collaborateurs en 1985 [105], de nombreux phénomènes physiques ont été exploités pour réduire certaines fluctuations quantiques sous le niveau du bruit de photon : mélange à quatre ondes, amplification

et oscillation paramétrique, génération de second harmonique, effet Kerr, stabilisation de courant des diodes laser... (Voir les références [16, 15, 14] pour une vue d'ensemble des expériences de génération d'états comprimés). Parmi ces différentes possibilités, l'amplification paramétrique d'impulsions ultrabrèves lors d'un simple passage dans un cristal non-linéaire apparaît comme un dispositif simple et efficace, grâce à l'association de cristaux de coefficients non-linéaires élevés avec les fortes puissances crêtes et les possibilités de mise en forme des impulsions ultrabrèves [106, 107, 108, 109, 110, 26]. Avec cette technique, la forte compression obtenue est de 5.8 dB sous le bruit quantique standard en utilisant un oscillateur local correctement adapté [108].

Comme nous l'avons vu à la section 2.4.3, un amplificateur paramétrique dégénéré monomode permet une amplification sélective en quadratures sans bruit ajouté. Les quadratures de l'état en sortie de l'amplificateur s'expriment en fonction des quadratures d'entrée selon [13] :

$$X_{out} = e^{+r}\, X_{in} \qquad\qquad P_{out} = e^{-r}\, P_{in} \tag{7.1}$$

où r est un facteur de gain. Ce paramètre est une fonction linéaire de l'amplitude crête de l'onde pompe, du coefficient de non-linéarité du second ordre $\chi^{(2)}$ et de la longueur d'interaction non-linéaire. Si l'état en entrée de l'amplificateur (X_{in}, P_{in}) est un état cohérent ou un état vide, les variances des quadratures en sortie valent alors :

$$V_{X,out} = e^{+2r}\, N_0 \qquad\qquad V_{P,out} = e^{-2r}\, N_0 \tag{7.2}$$

Ces équations sont la signature d'un état comprimé, de fluctuations réduites en quadrature P.

Nous avons utilisé expérimentalement le phénomène d'amplification paramétrique dégénérée pour produire des états comprimés [111] : des impulsions de 150 fs sont amplifiées paramétriquement lors d'un simple passage au travers d'un cristal mince (100 μm) de niobate de potassium ($KNbO_3$) avec une déamplification significative de l'ordre de -3 dB. Les quadratures des états comprimés sont ensuite échantillonnées par notre détection homodyne résolue en temps, démontrant une réduction des fluctuations mesurée à -1.87 dB sous le bruit quantique standard.

A notre connaissance, notre expérience est la première à utiliser des cristaux de $KNbO_3$ de très faibles épaisseurs (100 μm) pour réaliser des conversions non-linéaires du second ordre d'impulsions ultrabrèves : génération de second harmonique et amplification paramétrique. Ces cristaux très minces permettent une large plage d'accord de phase et évitent les conditions de forte dispersion de vitesse de groupe, qui limitaient l'utilisation de cristaux épais de $KNbO_3$ [97, 98]. Même pour les très courtes longueurs d'interaction utilisées ici, le niobate de potassium offre un gain paramétrique important, grâce à la forte non-linéarité du cristal (environ 12 pm/V) et à un accord de phase non-critique.

Un deuxième aspect essentiel de notre expérience est que tout le traitement est effectué dans le domaine temporel, et non dans le domaine fréquentiel, comme c'est généralement le cas même pour des expériences de génération d'états comprimés impulsionnels [106]. Pour chaque impulsion incidente, notre détection homodyne résolue en temps échantillonne la composante de quadrature en phase avec l'oscillateur local. Nos mesures permettent donc d'accéder directement à la distribution statistique des quadratures étudiées. Ceci permet alors une analyse claire et simple des transferts d'information impliqués dans des protocoles de communication quantique [73, 70]. Des systèmes de détection similaires avaient déjà été réalisés avec des impulsions picosecondes [26, 35], mais notre dispositif est le premier opérant dans le domaine femtoseconde.

Ce chapitre détaille les différents aspects expérimentaux de notre dispositif de génération impulsionnelle d'états comprimés, présenté à la figure 7.1. Nous décrivons ainsi successivement la source d'impulsions femtosecondes, les effets non-linéaires dans le cadre de l'optique classique (génération de second harmonique et amplification paramétrique dégénérée), puis la mesure homodyne d'un état vide comprimé.

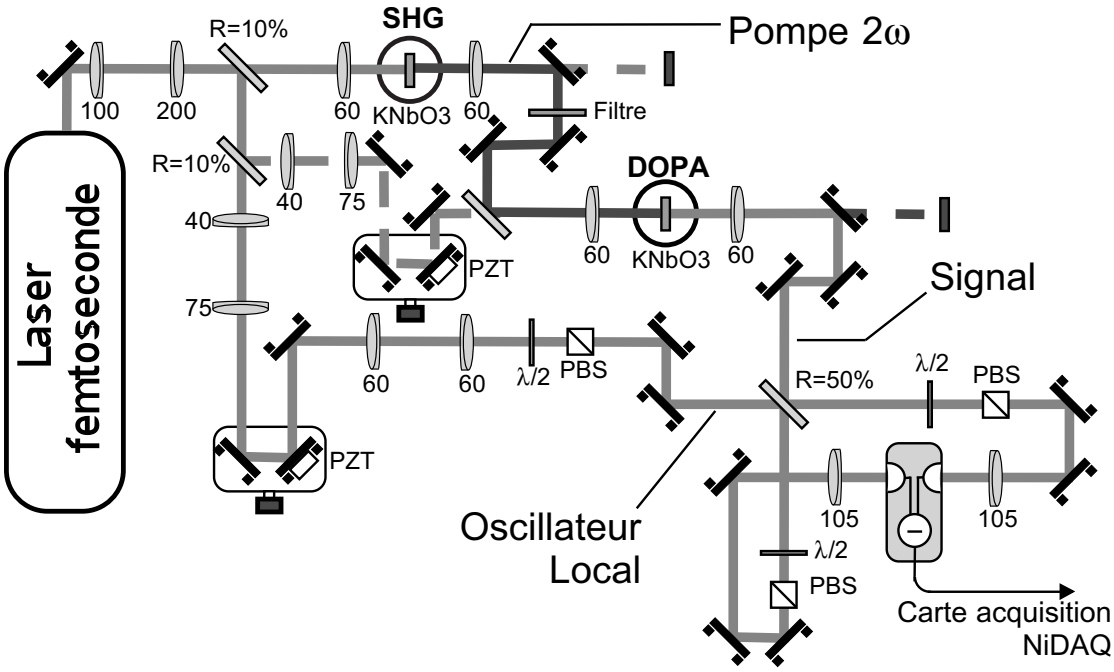

Figure 7.1: *Dispositif expérimental complet pour la génération d'états comprimés. Les focales des optiques sont indiquées en millimètres.*

7.1 Source laser femtoseconde

Pour la génération impulsionnelle d'états comprimés ou d'états intriqués du champ lumineux par amplification paramétrique, la source laser initiale doit être choisie avec précautions et valider différents critères :

- De fortes puissances crêtes afin d'obtenir des effets non-linéaires significatifs. Ce critère se traduit par le besoin d'impulsions de durées ultrabrèves et d'énergies par impulsion importantes ($>$ 10 nJ/impulsion).
- Une cadence de répétition suffisamment élevée ($>$ 100 kHz) pour acquérir rapidement des données en évitant les dérives expérimentales et atteindre de hauts débits de transmission. Par ailleurs, la cadence de répétition des impulsions ne doit pas dépasser les capacités de résolution temporelle de notre système de détection homodyne (de l'ordre du MHz).
- Une bonne qualité de mode spatial pour obtenir une adaptation de modes correcte entre le faisceau signal et l'oscillateur local de la détection.
- Des enveloppes temporelles et spectrales en bonne approximation limitées par Fourier, de manière à pouvoir considérer simplement les impulsions comme monomodes du point de vue de l'optique quantique.

De la sorte, nos critères rejoignent certaines expériences de spectroscopie ultrarapide, comme les expériences pompe-sonde ou d'écho de photon, dans le besoin d'une source d'impulsions de fortes énergies et de cadence intermédiaire (de l'ordre du MHz). Nos expériences ne peuvent utiliser ni les oscillateurs femtosecondes standard (de cadence $\sim$ 100 MHz trop élevée et

d'énergie < 10 nJ/impulsion trop faible), ni les amplificateurs régénératifs commerciaux (de cadence ~ 10 kHz trop lente).

Le quatrième point (qualité spectrale et temporelle des modes) fixe de plus une borne inférieure à la durée des impulsions que nous pouvons envisager utiliser : pour les impulsions de durée inférieure à 100 fs, il n'est pas possible en première approximation de négliger l'étalement temporel et le glissement de fréquence (*chirp*) qui apparaissent lors de la traversée d'un milieu dispersif, même pour des épaisseurs de quelques millimètres comme le montre la figure 7.2. La durée de 150 fs apparaît alors comme un compromis acceptable pour une largeur temporelle suffisamment faible permettant d'obtenir une puissance crête intense tout en demeurant relativement robuste à la dispersion lors de la traversée d'un milieu matériel.

La source finalement retenue est un laser commercial *Tiger-CD* de la société *Time-Bandwidth Products*, dont nous détaillons les principales caractéristiques dans cette section.

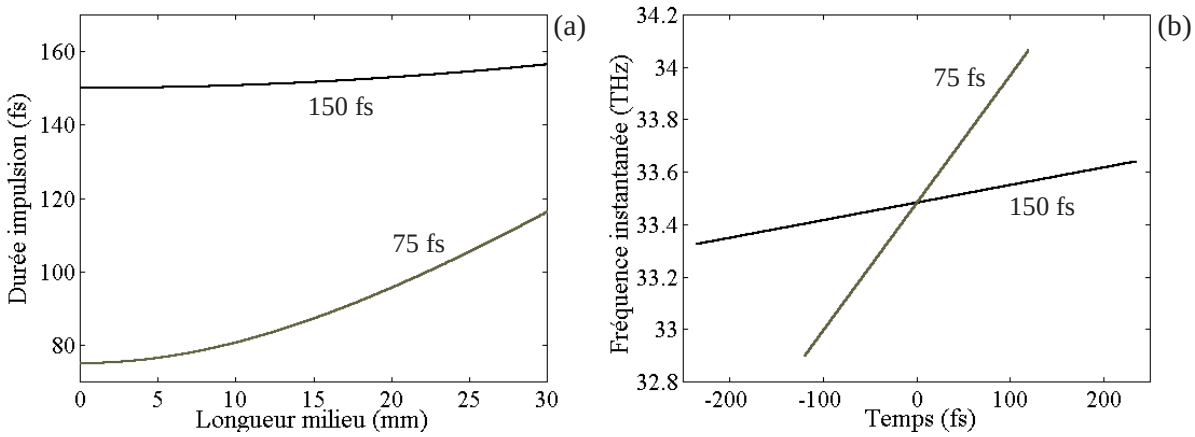

Figure 7.2: *Propagations comparées à travers un milieu dispersif (verre BK7) d'impulsions gaussiennes de largeurs 75 et 150 fs (FWHM) à 850 nm. (a) Etalement de la largeur temporelle de l'impulsion en fonction de l'épaisseur du milieu traversé. (b) Fréquence instantanée en fonction du temps pour une traversée de 30 mm de BK7. La dépendance linéaire de la fréquence correspond au* chirp *(glissement de fréquence) de l'impulsion. Les calculs correspondants proviennent des références [84, 85].*

7.1.1 Caractéristiques du laser femtoseconde *Tiger-CD*

On énonce généralement trois conditions essentielles qui doivent être vérifiées par une source laser délivrant des impulsions ultrabrèves [84]. La première est de disposer d'un milieu amplificateur de grande largeur spectrale, de manière à ce que le spectre des impulsions puisse être étendu pour produire une allure temporelle (transformée de Fourier du spectre) de durée ultrabrève. La deuxième condition nécessaire est de compenser la dispersion de vitesse de groupe introduite par les différents éléments optiques de la cavité. Enfin, la dernière condition est de synchroniser les différents modes en phase pour garantir une somme cohérente des modes conduisant à un fonctionnement impulsionnel.

Le laser femtoseconde *Tiger-CD* que nous utilisons vérifie bien entendu ces trois conditions pour émettre des impulsions de durée totale à mi-hauteur 150 fs (FWHM) centrées à 846 nm, quasiment limitées par Fourier, avec une énergie jusqu'à 75 nJ et à la cadence de 780 kHz.

Données techniques pour le laser Tiger-CD / Time-Bandwitdh Products	
Puissance	Typique : moyenne 40mW, énergie 50nJ/impulsion à 780kHz, puissance crête 300kW; Max : moyenne 60mW, énergie 75nJ/impulsion à 780kHz, puissance crête 450kW
Temps-Fréquence	Durée $\Delta t_{FWHM} = 150$fs, largeur spectrale $\Delta\lambda_{FWHM} = 5.5$nm à 846nm, $\Delta t_{FWHM}.\Delta\nu_{FWHM} = 0.35$
Laser pompe	*Melles Griot* 58 GLS 309. Puissance 3.1W à 532nm, $M^2 \approx 4$, polarisation linéaire verticale 1:100, diamètre 0.25mm, divergence totale 12mrad, stabilité pointé 40μrad, bruit rms 3%
Mode-Locking	Technologie SESAM (absorbant saturable semiconducteur en cavité)
Cavity Dumper	Cellule de Bragg *Neos* N13389, électronique associée *Neos* N64389-SYN, fréquence 371MHz, facteur de division 100
Divers	Fréquence intra-cavité 78.2MHz, divergence totale 1.6mrad, bruit rms en amplitude $< 3\%$, polarisation verticale "s" utilisée pour le montage

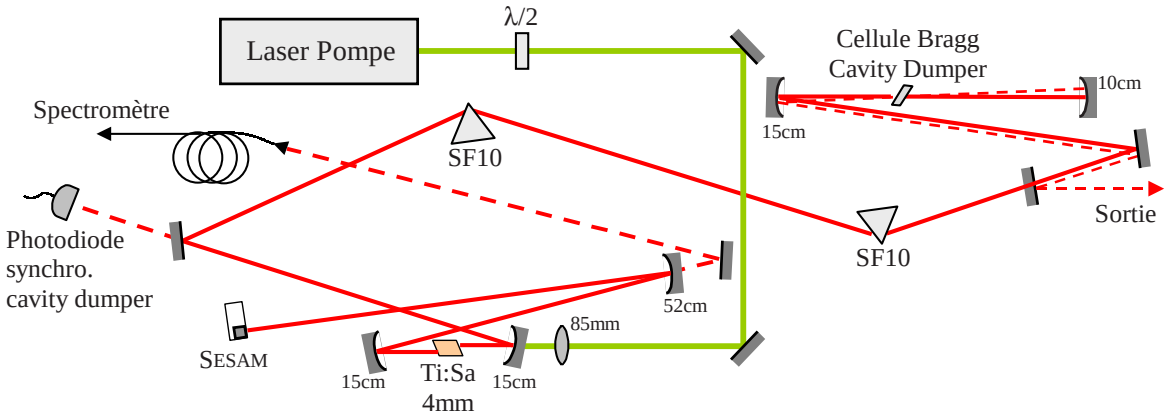

Figure 7.3: *Cavité du laser femtoseconde* Tiger-CD.

Pour satisfaire la première condition de milieu amplificateur à large bande spectrale, le laser *Tiger-CD* utilise un cristal de saphir dopé au titane Ti:Al_2O_3 dont la bande de gain s'étend de 0.7 à 1 μm, permettant d'atteindre des impulsions de durée de l'ordre de 10 fs. Ce matériau se distingue de plus par une grande densité de stockage d'énergie et d'excellentes propriétés thermiques qui en font le matériau le plus généralement utilisé pour concevoir des oscillateurs femtosecondes. La compensation de la dispersion de vitesse de groupe (seconde condition) est effectuée de façon standard par un ensemble de prismes [84] dont le matériau et la distance sont optimisés pour retarder les grandes longueurs d'onde qui se propagent le plus rapidement dans le reste de la cavité. Enfin, pour verrouiller les modes en une phase commune, notre système utilise les propriétés d'un absorbant saturable à semiconducteur.

Si la vérification des trois conditions ci-dessus est nécessaire pour générer des impulsions ultrabrèves, elle n'est cependant pas suffisante pour satisfaire notre cahier des charges d'impulsions intenses à une cadence intermédiaire de l'ordre du MHz. L'ensemble {cristal titane:saphir, prismes,

SESAM} constitue un oscillateur femtoseconde de base, délivrant des impulsions d'énergie de l'ordre de quelques nanojoules par impulsion à la cadence d'aller-retour de l'impulsion au sein de la cavité, soit 78 MHz. Pour augmenter l'énergie des impulsions émises tout en diminuant la cadence d'émission, le laser utilise une cellule de Bragg en tant que déflecteur optique (*cavity dumper*). Lorsqu'aucun signal n'est envoyé sur la cellule, le faisceau intra-cavité n'est pas dévié et aucune impulsion (en dehors des pertes) ne sort de la cavité. L'impulsion peut alors être amplifiée au cours d'un nombre fixé d'allers-retours (de l'ordre de 100) jusqu'à ce qu'un signal externe commande la déflection du faisceau et la sortie d'une impulsion. L'énergie par impulsion extraite peut cette fois s'élever jusqu'à 75 nJ à la cadence de 780 kHz. Cette technique de "cavity dumper" sera détaillée dans la section 7.1.3, après une discussion du blocage des modes en phase présentée à la section suivante.

7.1.2 Verrouillage des modes en phase : SESAM

Pour obtenir des impulsions de 150 fs limitées par Fourier, la largeur spectrale doit être de l'ordre de 5.5 nm à 850 nm, soit $\Delta\nu = 2.3$ THz. L'intervalle spectral libre entre les modes pour notre cavité étant de 78 MHz, notre génération d'impulsions ultrabrèves requiert de synchroniser en phase environ $2.3\,10^{12}\,/78\,10^{6} \approx 30\,000$ modes. Ce verrouillage en phase est obtenu en introduisant un absorbant saturable dans la cavité dont les oscillations naturelles sont continuellement amplifiées pour aboutir à la génération d'un train d'impulsions lumineuses stables après un certain temps de construction.

Ce phénomène de verrouillage des modes est plus simple à expliquer dans le domaine temporel [84]. Rappelons que l'absorbant saturable est un élément dont les pertes diminuent lorsque l'intensité incidente augmente. Lorsque le faisceau de pompe est envoyé sur le milieu amplificateur, différents modes de la cavité commencent à osciller avec des phases respectives aléatoires, ce qui donne naissance à des pics d'intensité. Alors que la puissance intra-cavité augmente, le pic de puissance le plus intense commence à saturer le milieu absorbant. Ce pic subit alors moins de pertes que les autres maxima locaux, ce qui le favorise dans la compétition pour le gain au sein du milieu amplificateur. Si les conditions sont favorables, les autres pics sont éliminés et une seule impulsion se propage à travers la cavité.

L'association de l'absorbant saturable et du milieu amplificateur permet ensuite de stabiliser la structure temporelle et spectrale de l'impulsion : lorsque l'impulsion arrive sur l'absorbant saturable, son front avant – d'intensité faible – subit de fortes pertes, mais pas son maximum d'intensité qui sature l'absorbant. Le front arrière bénéficie alors de la "transparence" induite par le maximum lors du temps caractéristique de relaxation de l'absorbant saturable (voir la figure 7.4). L'impulsion de durée réduite arrive ensuite sur le milieu amplificateur. Le front avant de l'impulsion est fortement amplifié, mais pas le front arrière qui est affecté par la saturation du gain induite par l'amplification du font avant, ce qui a pour effet de diminuer davantage la durée de l'impulsion. L'impulsion atteint sa structure finale stable lorsqu'elle revient identique à elle-même après un aller-retour dans la cavité. Si la dispersion de vitesse de groupe est correctement compensée, la durée de l'impulsion est typiquement limitée par la largeur spectrale de l'absorbant saturable qui est l'élément le plus critique intra-cavité.

Les absorbants saturables les plus utilisés dans le passé étaient les colorants organiques. Bien qu'ils puissent présenter certains avantages pour des applications de laboratoire, ces éléments souffrent de courtes durées de dégradation et d'une manipulation délicate. Pour des dispositifs tout-solide, il est maintenant possible de réaliser des semiconducteurs de large bande d'absorption et de paramètres contrôlables (temps de relaxation, intensité de saturation...). Ces semiconducteurs peuvent être intégrés dans une structure de miroirs en configuration de Fabry-

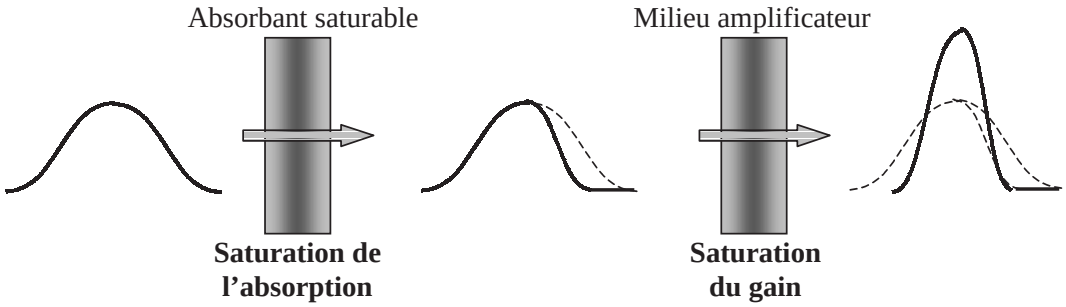

Figure 7.4: *Illustration de la propagation d'une impulsion brève dans un ensemble* {*absorbant saturable + milieu amplificateur* }.

Perot à anti-résonance, de sorte à obtenir un élément dont la réflectivité augmente lorsque la puissance incidente augmente [89]. Ce système est appelé *SEmiconductor Saturable Absorber Mirrors* (SESAM), ou *Antiresonant Fabry-Perot Saturable Absorber* (A-FPSA). L'anti-résonance de la structure Fabry-Perot permet de réaliser un élément de faibles pertes, de forte intensité de saturation et niveau d'endommagement faible.

Cette technique de verrouillage de modes, appelée *soliton-like mode-locking*, ne nécessite pas de processus supplémentaire au démarrage et est très différente du blocage de modes par lentille de Kerr (*Kerr-lens mode-locking*) où le fonctionnement impulsionnel est privilégié par l'association d'un filtre spatial et d'une focalisation induite par effet Kerr pour les fortes intensités [84]. On peut toutefois remarquer que l'effet Kerr intervient tout de même dans la cavité, même s'il ne constitue pas le processus majeur de blocage de modes. La référence [89] présente une vue d'ensemble sur les différentes techniques passives de synchronisation des modes en phase. Le traitement théorique complet de la génération d'impulsions ultrabrèves avec un absorbant saturable est effectué dans [90].

7.1.3 Extraction des impulsions : Cavity dumper

Pour extraire l'énergie à une cadence définie, un déflecteur optique (*cavity dumper*) est placé à l'intérieur de la cavité. La déflection peut être réalisée soit par un élément acousto-optique (cellule de Bragg), soit par un modulateur électro-optique (cellule de Pockels). Si ces deux méthodes s'appliquent en principe à un oscillateur femtoseconde, la méthode acousto-optique est en général préférée, du fait des courtes longueurs et de la faible dispersion des cellules de Bragg utilisées. La première réalisation d'un laser avec cavity dumper a été présentée par Ramaswamy *et al* en 1993 [87] pour produire des impulsions de 50 fs et d'énergie 100 nJ à diverses cadences (jusqu'à 950kHz). Cette équipe a ainsi démontré la possibilité d'un fonctionnement femtoseconde stable, malgré les fortes perturbations de la cavité introduites par le processus de déflection. Avec un verrouillage de modes par effet Kerr, une durée d'impulsion aussi courte que 10 fs a pu être obtenue [88].

Le cavity dumper utilisé au sein du laser *Tiger-CD* repose sur une cellule de Bragg positionnée au centre de courbure du miroir de fin de cavité dans une structure dite à double passage [87]. Ce déflecteur est le seul coupleur utile de sortie de cavité, tous les autres miroirs sont de forte réflectivité afin de minimiser les pertes. Pour décrire le processus de déflection optique, l'impulsion intra-cavité est représentée par $E(t) = E_0 \cos(\omega t)$ où E_0 désigne l'enveloppe temporelle de l'impulsion et ω la pulsation optique de la porteuse. Après un premier passage dans

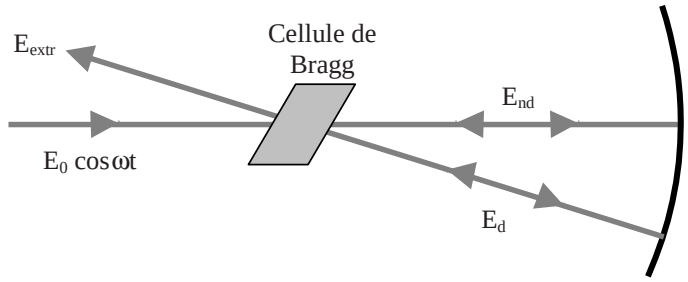

Figure 7.5: *Modèle de cavity dumper à double passage*

la cellule de Bragg, l'impulsion est scindée suivant l'efficacité de déviation η en une partie non-déviée E_{nd} et une partie déviée E_d décalée en fréquence de la pulsation Ω de l'onde RF appliquée à la cellule (voir la figure 7.5) :

$$E_d = \sqrt{\eta}\, E_0\, \cos(\omega t + \Omega t + \phi) \qquad\qquad E_{nd} = \sqrt{1-\eta}\, E_0\, \cos(\omega t) \tag{7.3}$$

où ϕ désigne la phase (ajustable) de l'onde RF. Après réflexion sur le miroir sphérique de fin de cavité, les impulsions sont refocalisées dans la cellule de Bragg et à nouveau déviées. Si l'ajustement interférométrique des miroirs et de la cellule est correct, le champ total sortant contient alors les contributions de la partie déviée au deuxième passage du champ E_{nd} et de la partie non déviée du champ E_d :

$$\begin{aligned} E_{extr} &= \sqrt{1-\eta}\,\sqrt{\eta}\, E_0\, \cos(\omega t + \Omega t + \phi) + \sqrt{\eta}\,\sqrt{1-\eta}\, E_0\, \cos(\omega t - \Omega t - \phi) \\ &= 2\sqrt{\eta(1-\eta)}\, E_0\, \cos(\omega t)\, \cos(\Omega t + \phi) \end{aligned} \tag{7.4}$$

Grâce aux interférences des voies, l'intensité extraite est proportionnelle à :

$$I_{extr} \propto \eta\,(1-\eta)\,|E_0|^2\, \cos^2(\Omega t + \phi) \tag{7.5}$$

Le maximum d'énergie peut alors être extrait avec une efficacité de diffraction limitée à $\eta = 50\%$ et une phase RF nulle $\phi = 0$ (cette phase est contrôlable depuis le boîtier électronique du modulateur). Pour réaliser l'ensemble de ce réglage interférométrique, une monture spéciale a été dessinée pour la cellule de Bragg [91].

Outre la forte efficacité d'extraction de puissance, la configuration à double passage offre aussi la propriété essentielle de pouvoir supprimer la déviation des impulsions précédant et suivant l'impulsion de commande RF. En effet, l'enveloppe du signal RF (temps de montée et de descente de l'ordre de 7 ns) est du même ordre de grandeur que le temps d'aller-retour dans la cavité (13 ns) ce qui empêche la sélection par le signal RF d'une seule impulsion lumineuse et nous oblige à prendre en compte l'impulsion optique précédant et suivant l'impulsion déviée. L'astuce ici est de remarquer que si la fréquence $\nu_{RF} = \Omega/2\pi$ de l'onde RF est convenablement choisie telle que $\nu_{RF} = (n + 0.5)/2\ \nu_{cav}$ où ν_{cav} est la cadence de répétition intra-cavité et n un entier, alors le terme en cosinus dans (7.5) s'annule pour l'impulsion précédant ou suivant l'impulsion signal.

Dans notre système laser, une photodiode rapide permet de synchroniser l'onde RF avec la fréquence intra-cavité ν_{cav}. Des multiplicateurs de fréquence génèrent une onde RF de fréquence 9.5/2 fois plus grande que ν_{cav}, soit 371 MHz, ce qui permet de supprimer efficacement les fractions déviées des impulsions précédant et suivant l'impulsion signal. Le choix de la cadence de répétition est optimisé en fonction de l'électronique de commande et de la puissance RF

disponible pour obtenir les impulsions de plus haute énergie. Un facteur de division égal à 100 est retenu entre la fréquence intra-cavité de 78 MHz et la cadence d'émission des impulsions à 780 kHz. Enfin, pour une extraction optimale, la position de l'enveloppe et la phase de l'onde RF appliquée au modulateur sont contrôlables par le boîtier d'électronique *Neos*.

L'énergie maximale disponible est limitée par différentes instabilités intervenant lorsque de fortes puissances intra-cavité saturent l'effet introduit par le SESAM. Plusieurs impulsions peuvent alors coexister au sein de la cavité, ce qui diminue de manière importante l'énergie utile par impulsion. Pour éviter la naissance d'impulsions multiples, la puissance intra-cavité est volontairement limitée sous le seuil critique en introduisant des pertes lors de la conception de la cavité, et en choisissant une puissance de pompe adéquate.

7.1.4 Caractérisation des impulsions

Cette section fait un rapide bilan des mesures de caractérisation des impulsions laser : énergie, puissance, durée et largeur spectrale. Le profil temporel de la puissance lumineuse est supposé suivre une dépendance en sécante hyperbolique carrée $\mathrm{sech}^2(.) = 1/\cosh^2(.)$, ce qui nous permet de présenter quelques formules utiles sur ces fonctions.

Energie et puissance

La dépendance de la puissance en fonction du temps s'écrit :

$$\mathcal{P}(t) = \mathcal{P}_{crête}\ \mathrm{sech}^2\left(2\ln(1+\sqrt{2})\,\frac{t}{\Delta t_{FWHM}}\right) \tag{7.6}$$

Si nous ne disposons pas de détecteurs optoélectroniques suffisamment rapides pour suivre cette évolution directement à l'échelle de la femtoseconde, il est cependant facile de mesurer avec un puissancemètre la puissance moyenne $\mathcal{P}_{moy}$. Indépendamment du profil temporel ou de la longueur d'onde, la puissance moyenne permet d'accéder à l'énergie par impulsion $\mathcal{E}$ selon :

$$\mathcal{P}_{moy} = \mathrm{C}\int_{impulsion}\mathcal{P}(t)dt = \mathcal{E}\,\mathrm{C} \tag{7.7}$$

où C = 780 kHz est la cadence de répétition des impulsions. A partir du profil (7.6), on peut également accéder à la puissance crête de l'impulsion :

$$\mathcal{P}_{crête} = \mathcal{P}_{moy}\,\frac{1}{\mathrm{C}\,\Delta t_{FWHM}}\,\ln(1+\sqrt{2}) \tag{7.8}$$

(dans le cas d'un profil gaussien, le terme correcteur en logarithme est remplacé par $\sqrt{4\ln 2/\pi}$).

Profil temporel

Pour mesurer la largeur temporelle totale à mi-hauteur Δt_{FWHM} d'une impulsion, on utilise un dispositif standard autocorrélateur d'intensité en montage non-colinéaire [84, 85] avec un cristal non-linéaire de BBO de longueur 0.5mm de sorte à minimiser la dispersion introduite lors du doublage de fréquence. L'impossibilité de mesurer les moments d'ordre supérieurs à deux de la puissance lumineuse nous oblige à faire une hypothèse sur l'allure temporelle des impulsions afin de déduire la largeur des impulsions à partir de la largeur $\Delta t_{FWHM,autocorr}$ de la fonction d'autocorrélation d'intensité. D'après [84], les largeurs temporelles du profil et de l'autocorrélation d'intensité sont reliées par $\Delta t_{FWHM} = \Delta t_{FWHM,autocorr}\,/\,K$ où $K = 1.543$

pour une sécante hyperbolique carrée (ou $K = 1.414$ pour une gaussienne). La mesure présentée sur la figure 7.6 de l'autocorrélation d'intensité des impulsions d'une largeur totale à mi-hauteur de 7.4 μs permet d'accéder à une largeur d'autocorrélation $\Delta t_{FWHM,autocorr} = 240$ fs avec une calibration de 32 fs/μs. On en déduit alors une largeur $\Delta t_{FWHM} \approx 150$ fs.

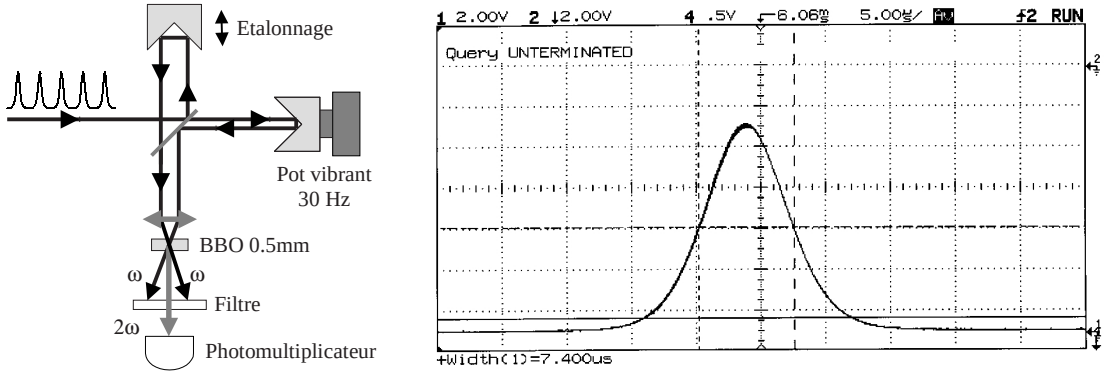

Figure 7.6: *Montage autocorrélateur et courbe expérimentale d'autocorrélation d'intensité.*

Spectre

Nous utilisons un spectromètre CCD intégré *CVI Spectral Products* SM240-USB-FC de résolution inférieure au nanomètre pour visualiser le spectre des impulsions lumineuses. A partir d'une mesure de largeur spectrale $\Delta\lambda_{FWHM,mes} = 6$ nm et connaissant la résolution du spectromètre, nous pouvons évaluer la largeur réelle des impulsions à $\Delta\lambda_{FWHM} \approx 5.5$ nm (produit de convolution par la caractéristique du spectromètre). Cette largeur permet de calculer alors le produit $\Delta t_{FWHM}.\Delta\nu_{FWHM} = 0.35$ pour nos valeurs expérimentales. D'après les propriétés de la transformée de Fourier, les largeurs temporelles et spectrales sont liées par la relation croisée $\Delta t_{FWHM}.\Delta\nu_{FWHM} \geq \mathcal{K}$ avec $\mathcal{K} = 0.315$ pour une sécante hyperbolique carrée et $\mathcal{K} = 0.441$ pour une gaussienne [84]. Notre valeur expérimentale de 0.35, relativement peu éloignée de la limite 0.315, confirme notre hypothèse de départ d'un profil en sech^2, et indique que le profil de l'impulsion est quasiment limité par Fourier, ce qui nous autorise à considérer simplement les impulsions lumineuses comme des objets quantiques monomodes (le profil spatial est lui aussi raisonnablement proche d'une allure gaussienne).

Grâce à cette source femtoseconde particulière, nous disposons d'impulsions intenses à une cadence intermédiaire, ce qui nous permet de concevoir des dispositifs simples d'optique non-linéaire pour générer des états quantiques impulsionnels particuliers. Pour des détails supplémentaires concernant notre système et les modifications apportées, on pourra se référer à la note interne [92].

7.2 Optique non-linéaire impulsionnelle

Les interactions non-linéaires permettent de manipuler les propriétés quantiques des impulsions lumineuses. Dans ce sens, elles seront notre outil de base pour la génération d'états quantiques particuliers. Quatre processus non-linéaires sont employés dans nos expériences :

- **Génération de second harmonique** pour convertir les impulsions émises par le laser à 846 nm vers 423 nm et servir de pompe pour les processus paramétriques.

- **Amplification paramétrique dégénérée** pour introduire une amplification dépendante de la phase (sensible en quadratures) à partir d'un faisceau sonde.
- **Amplification paramétrique non-dégénérée** pour introduire une amplification indépendante en phase d'un faisceau sonde et dupliquer l'état quantique. Ce phénomène fera l'objet du chapitre 10.
- **Fluorescence paramétrique** lorsqu'aucun faisceau sonde n'est présent (émission spontanée et/ou stimulée par le vide). Le choix du mode de l'oscillateur local permet de sélectionner l'état quantique observé, entre un vide comprimé (amplification dégénérée) ou un état vide intriqué (amplification non-dégénérée).

7.2.1 Choix des cristaux non-linéaires

Pour nos applications d'optique quantique, il est absolument crucial de conserver l'aspect monomode des impulsions : profils temporels et spectraux limités par Fourier et mode spatial TEM_{00}. Il faut donc concevoir les applications non-linéaires de sorte à déformer le moins possible les propriétés modales des impulsions, tout en assurant de forts effets. Le type de cristal non-linéaire employé ainsi que les longueurs utilisées devront donc satisfaire aux critères d'un fort coefficient de non-linéarité $\chi^{(2)}$, de faible décalage de direction de propagation entre les faisceaux (*walk-off*), de faible désaccord de vitesse de groupe (GVM : *Group Velocity Mismatch*) et de dispersion de vitesse de groupe négligeable (GVD : *Group Velocity Dispersion*) [1]. Enfin, la taille de la tache de focalisation devra être optimisée suivant un compromis entre une focalisation suffisamment forte pour obtenir des effets intenses et suffisamment faible pour éviter tout phénomène parasite venant déformer les propriétés modales de l'impulsion (absorption, échauffement du milieu...).

Suivant un choix couramment effectué pour des expériences d'optique non-linéaire avec des impulsions femtosecondes [84], nous avons débuté nos expériences en considérant des cristaux de β-barium borate (BBO). Ce cristal présente l'avantage d'avoir un coefficient non-linéaire $d_{eff} = 1.36$ pm/V important à 850 nm et un coefficient de désaccord de vitesse de groupe acceptable de 190 fs/mm à 850 nm. Nous pourrions ainsi utiliser des longueurs de 0.5 à 0.8 mm pour nos applications. Malheureusement, la biréfringence intrinsèque du BBO impose un décalage de 3.8° entre le faisceau fondamental (846 nm) et le faisceau converti de second harmonique (423 nm). Pour des faisceaux focalisés de 30 μm de diamètre, ce décalage, ou *walk-off*, sera un facteur critique dès que la longueur d'interaction dépasse quelques centaines de micromètres. Afin de conserver les qualités spatiales et temporelles du mode fondamental, il serait nécessaire d'utiliser des taches de focalisation plus grandes que 30 μm ainsi que les longueurs de cristal de l'ordre de 0.1 à 0.2 mm, ce qui n'est pas compatible avec nos besoins d'effets non-linéaires intenses.

Nous avons finalement choisi d'utiliser des cristaux minces de niobate de potassium ($KNbO_3$), proposés par la société *FEE GmbH*. Ce cristal offre l'avantage d'un accord de phase non-critique (à 90 degrés ou NCPM : *Non Critical Phase Matching*) accordable en température. Ainsi le problème du *walk-off* ne se pose pas : l'onde fondamentale et de second harmonique possèdent des directions de propagation et des vecteurs de Poynting colinéaires. De plus, le niobate de potassium offre un coefficient non-linéaire $d_{eff} \approx 12$ pm/V qui en fait un des cristaux de plus forte non-linéarité connus à ce jour [96]. L'inconvénient majeur de ce cristal réside dans le fort

[1] La GVM correspond à l'étalement de l'impulsion de second harmonique du fait du décalage temporel entre la fraction doublée en entrée du cristal et celle doublée en sortie, les impulsions bleues et rouges ne se propageant pas à la même vitesse. La GVD correspond à l'étalement intrinsèque de l'impulsion lors de la traversée d'un milieu dispersif.

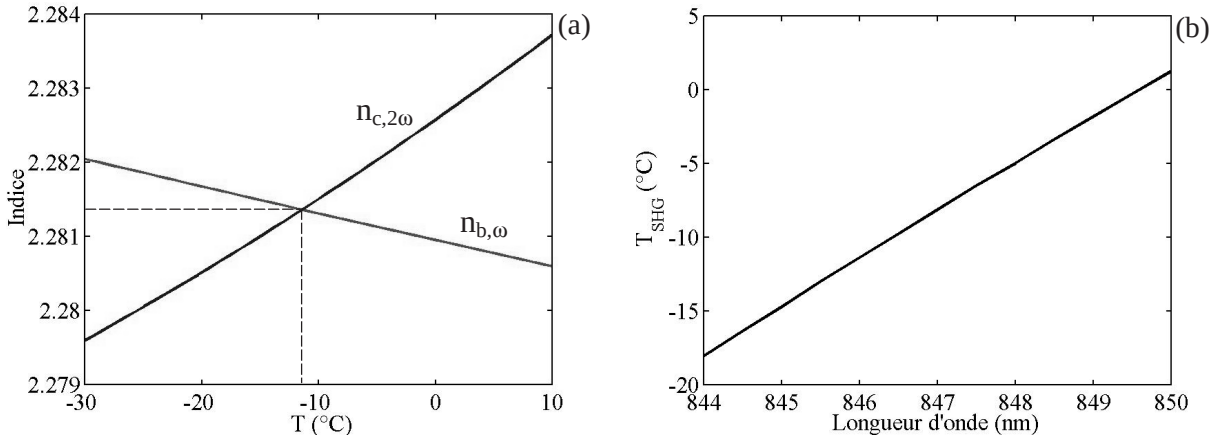

Figure 7.7: *(a) Indices de réfraction du $KNbO_3$ pour le fondamental (axe cristallographique b) et le second harmonique (axe c) en fonction de la température pour 846 nm d'après les équations de [96]. (b) Température optimale d'accord de phase non-critique en fonction de la longueur d'onde.*

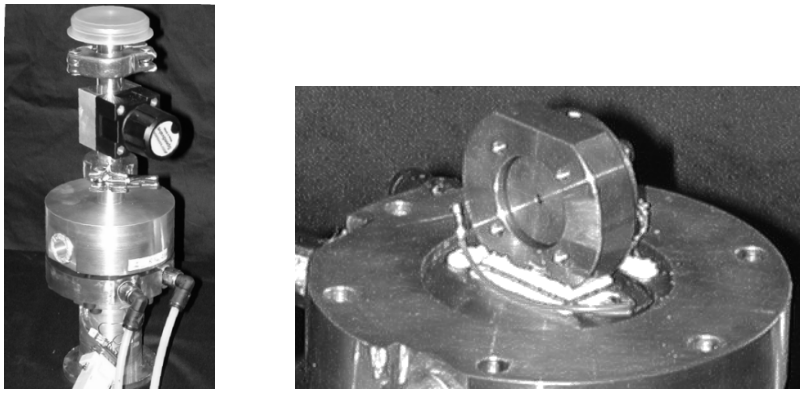

Figure 7.8: *Enceinte à vide réfrigérante pour le cristal de $KNbO_3$.*

désaccord de vitesses de groupe, évalué par le paramètre $\mathcal{D} = 1/v_{g,2\omega} - 1/v_{g,\omega}$ où $v_{g,.}$ désigne la vitesse de groupe de l'onde. Si la condition d'accord de phase garantit l'égalité des vitesse de phase, elle n'assure en rien l'égalité des vitesses de groupe dans un milieu dispersif comme le $KNbO_3$ dont le désaccord $\mathcal{D}$ est de l'ordre de 1.2 ps/mm [96]. Avec des impulsions de 150 fs, il n'est donc possible de tolérer que des distances au plus de 0.1 mm. Obtenir des cristaux de $KNbO_3$ aussi minces avec des surfaces de qualité optique est une tâche très délicate, mais la société *FEE* a su dépasser ces difficultés pour nous proposer des cristaux de 100 μm d'épaisseur, taillés suivant l'axe a et traités anti-reflets à 850 et 425 nm.

Pour le $KNbO_3$, l'accord de phase non-critique de type I (*ooe*) est obtenu à température ambiante pour la longueur d'onde de 860 nm. L'accordabilité de notre source laser ne nous permettant pas d'atteindre cette valeur, nous avons exploité la dépendance de l'indice de réfraction du $KNbO_3$ en fonction de la température pour obtenir un accord de phase non-critique pour de plus basses longueurs d'ondes. Les courbes 7.7 présentent les prédictions théoriques d'après les expressions des indices de réfraction de la référence [96]. Pour obtenir les conditions d'accord de

phase à 846 nm, la température doit être abaissée autour de -12°C. Nous avons alors conçu une monture spéciale permettant d'abaisser la température du cristal : le refroidissement est obtenu par un élément Peltier, lui-même refroidi par une circulation d'eau. Le cristal et sa monture sont placés dans une enceinte à vide (pression interne typique 10^{-2} mbar) afin d'éviter tout phénomène de condensation et de garantir une isolation thermique adéquate. La température minimale atteignable avec ce dispositif est de -30°C, limitée par l'écart de température maximal entre les faces de l'élément Peltier (50°C). Ceci nous a permis d'optimiser l'accord de phase selon la plus forte efficacité de génération de second harmonique à 846 nm pour une température mesurée de -14°C, qui correspond sensiblement aux prévisions théoriques de la figure 7.7.

$\lambda = 850nm$	**$KNbO_3$**	**BBO**
Type	*FEE GmbH*, $a-cut$, NCPM type I (ooe) à 850 nm, 5.0x4.7x0.1 mm^3, AR 850-425nm	*Castech*, $\theta = 28.5°$, $\varphi = 0°$, type I (ooe) à 850 nm, 5x5x0.5 mm^3 AR 820-410nm
Nonlinéarité	$d_{eff} \approx 12$ pm/V	$d_{eff} \approx 1.36$ pm/V
Indice de réfraction	$n_{b,\omega} = n_{c,2\omega} = 2.281$	$n_{o,\omega} = n_{e,2\omega} = 1.660$
Walk-off	0° (NCPM)	3.8°
GVM	1.2 ps/mm	190 fs/mm
Dispersion	0.38 $fs^2/\mu m$	0.035 $fs^2/\mu m$
Seuil de dommage	2 GW/cm^2	20 GW/cm^2
Absorption	< 0.002 cm^{-1}	< 0.005 cm^{-1}

7.2.2 Génération de second harmonique

La génération de nouveaux états quantiques par amplification paramétrique nécessite une onde pompe à fréquence double. Le premier effet non-linéaire que nous allons chercher à obtenir sera donc la génération de second harmonique par doublage de fréquence d'une impulsion fondamentale. Comme nous allons le voir, ce phénomène peut être obtenu très simplement lors d'un simple passage dans un cristal de $KNbO_3$ grâce aux très fortes puissances crêtes disponibles.

Les impulsions femtosecondes sont focalisées dans un cristal de $KNbO_3$, refroidi pour garantir le meilleur accord de phase et exalter le signal de génération de second harmonique. Différentes optiques (voir la figure 7.1) mettent en forme le faisceau fondamental pour obtenir un waist à l'intérieur du cristal d'environ $w_0 \approx 16$ μm. Cette configuration assure un paramètre confocal $2z_R = 2\pi n w_0^2/\lambda_\omega \approx 4$ mm, grand devant la longueur $L = 0.1$ mm du cristal. Ainsi, nous pouvons considérer le front d'onde comme plan au niveau du doublage et négliger les effets de la diffraction du faisceau gaussien [93, 94]. Cette configuration permet alors d'utiliser les formules théoriques de l'efficacité de conversion obtenues dans l'hypothèse d'une onde plane, en prenant en compte le mode spatial gaussien dans la dépendance entre la puissance crête et l'intensité : $\mathcal{P}_{crête} = (\pi w_0^2/2)\,\mathcal{I}_{crête}$.

Dans les hypothèses d'un mode spatial gaussien de waist w_0, d'un front d'onde plan et de parfait accord de phase non-critique, l'efficacité de conversion théorique de second harmonique s'écrit, en tenant compte de la déplétion du fondamental [94, 95] :

$$\eta_{SHG} = \tanh^2\left(\frac{L}{L_{NL}}\right) \qquad\qquad L_{NL} = \sqrt{\frac{w_0^2\, n^3\, \varepsilon_0\, c\, \lambda_\omega^2}{16\,\pi\, d_{eff}^2\, \mathcal{P}_{crête}}} \tag{7.9}$$

où $n = 2.281$ est l'indice de réfraction du milieu et $d_{eff} = 12$ pm/V le coefficient de non-linéarité. Pour une évaluation de l'efficacité de doublage attendue, on peut appliquer cette formule dans notre configuration, $w_0 = 16$ μm, $\lambda_\omega = 846$ nm, $\mathcal{P}_{crête} = 300$ kW, $L = 0.1$ mm, ce qui aboutit à une longueur d'interaction non-linéaire $L_{NL} \approx 50$ μm et une efficacité $\eta_{SHG} \approx 90\%$. Cette valeur importante atteste des fortes capacités de notre montage, même en simple passage avec un cristal aussi mince que 100 μm.

Cette prévision théorique est à comparer à la plus forte efficacité de conversion obtenue expérimentalement de 32% (corrigée des pertes), avec une efficacité typique de 28% (selon les réglages du laser), obtenues pour un waist au sein du cristal de 16 μm. Pour nos puissances disponibles, cette configuration spatiale apparaît comme un optimum : bien que la formule (7.9) prédise une augmentation quadratique de l'efficacité η_{SHG} lorsque la taille du waist w_0 est diminuée, nous avons observé expérimentalement que l'efficacité de doublage aux fortes puissances diminue lors de plus fortes focalisations. Les mesures de rendement de conversion en fonction de la puissance incidente et de la focalisation sont présentées sur la figure 7.9(a). Aux faibles puissances incidentes, l'efficacité de conversion augmente linéairement avec la puissance de pompe, comme indiqué par le modèle (7.9). Par contre, pour de fortes puissances, l'efficacité de conversion décroît lorsque le faisceau est trop focalisé, et l'on observe un minimum de l'efficacité lorsqu'on déplace le point de focalisation par rapport au centre du cristal (voir la figure 7.9(b)). Ces effets apparaissent lorsque l'intensité infrarouge dans le cristal dépasse une certaine intensité seuil, qui est de l'ordre de 0.1 GW/cm^2 pour notre expérience.

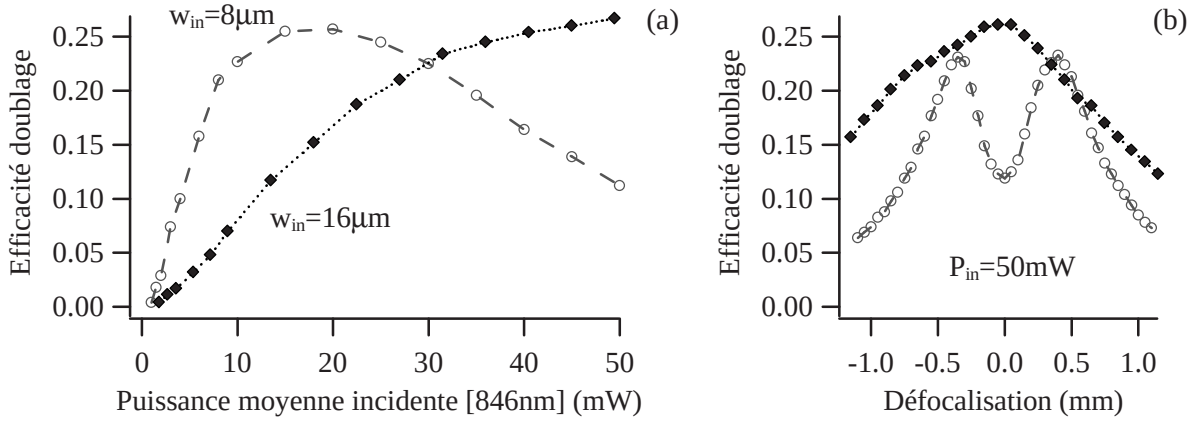

Figure 7.9: *(a) Efficacité de conversion de second harmonique mesurée en fonction de la puissance moyenne du fondamental pour deux configurations de focalisation : waist au niveau du cristal de 8 μm (cercles) et de 16 μm (losanges). (b) Efficacité de conversion lorsque la position du waist est décalée par rapport au centre du cristal (défocalisation) pour une puissance moyenne en entrée de 50 mW, correspondant à une intensité de 0.1 GW/cm^2 pour un waist de 16 μm (losanges) et 0.4 GW/cm^2 pour un waist de 8 μm (cercles).*

Alors qu'elles étudiaient des cristaux de $KNbO_3$ épais de 3 mm et 10 mm, d'autres équipes ont également observé une décroissance de l'efficacité de conversion aux fortes puissances lorsque la focalisation est forte [97, 98]. Ces équipes expliquent ce phénomène par une forte absorption du faisceau fondamental associée à une absorption de l'infrarouge induite par l'onde bleue [99]. Notre dispositif expérimental est cependant relativement différent de ces études : d'une part, nous étudions des cristaux minces (0.1 mm), ce qui minimise les effets de l'absorption, et d'autre part, même dans les cas des focalisations les plus fortes, le paramètre confocal donné par la

distance de Rayleigh est toujours supérieur à la longueur du cristal.

Pour comprendre l'origine du phénomène qui limite l'efficacité de conversion de notre montage, d'autres expériences complémentaires ont été réalisées. En particulier, nous avons modulé l'intensité du faisceau fondamental avec un hacheur mécanique et observé l'allure temporelle de la puissance bleue en fonction des conditions de focalisation. Pour des conditions telles que l'efficacité de conversion présente un creux en fonction de la position du waist (forte focalisation et forte puissance incidente), il apparaît une décroissance de la puissance doublée en fonction du temps d'exposition du cristal au faisceau rouge (voir la figure 7.10). Le temps caractéristique de cet effet est de l'ordre de 100 μs, mais notre modulateur ne permettant au mieux qu'un temps de montée de 20 μs, aucune mesure précise de ce temps caractéristique n'a pu être effectuée. Il est à noter que la décroissance disparaît de même que le creux en fonction de la focalisation lorsque l'intensité rouge au niveau du cristal est baissée en dessous du seuil critique de 0.1 GW/cm^2.

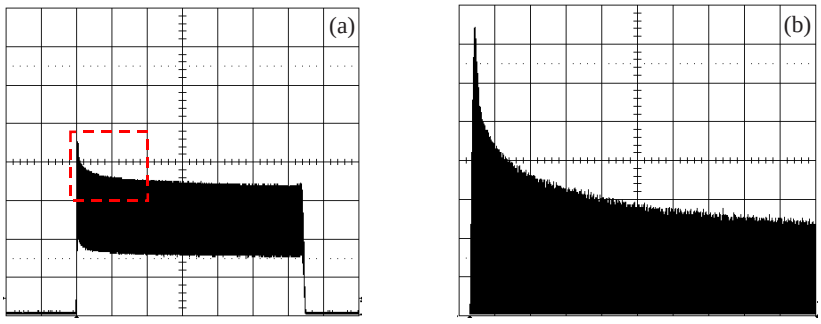

Figure 7.10: *(a) Observation du flux lumineux bleu avec une photodiode rapide lorsque l'intensité rouge incidente est modulée mécaniquement (fréquence 150 Hz) pour une focalisation au centre du cristal et une intensité crête de 0.4 GW/cm^2. La décroissance observée disparaît lorsque le faisceau rouge est défocalisé par rapport au centre du cristal. Echelles : H : 0.5ms/div, V : 1.0V/div. (b) agrandissement de (a). Echelles : H : 0.1ms/div, V : 200mV/div.*

Ces expériences nous permettent de dresser un rapide bilan des phénomènes parasites et de leur influence sur la conversion de fréquence : BLIIRA, effet photoréfractif, effet thermique local et absorption à deux photons.

BLIIRA

L'absorption de l'infrarouge induite par l'onde bleue (BLIIRA : *Blue Light Induced InfraRed Absorption*) dans le niobate de potassium a pour la première fois été étudiée dans la référence [99] dans le cadre de cristaux épais (10 mm) utilisés comme oscillateurs paramétriques optiques continus (OPO-CW). Pour notre expérience, l'influence de cet effet est amoindri par la très faible épaisseur de cristal utilisée et le passage unique. D'autre part, aucune absorption de l'infrarouge induite par le bleu n'a pu être mise en évidence lors de l'amplification paramétrique d'une sonde infrarouge avec un cristal similaire de $KNbO_3$. Tout porte donc à conclure que l'effet observé est induit par l'infrarouge et non pas par le faisceau bleu.

Effet photoréfractif

Le $KNbO_3$ est également connu et utilisé pour ses fortes propriétés photoréfractives [100]. Des porteurs de charge mobiles, générés par l'absorption à deux photons ou la photoionisation,

sont collectés dans de nouvelles régions du cristal, ce qui induit un champ électrique local et une modification d'indice de réfraction par effet photoélectrique. La modification de l'indice de réfraction altère l'accord de phase et limite l'efficacité de conversion non-linéaire. Précisons qu'un tel effet n'interviendrait pas à l'échelle de temps d'une impulsion, mais se construirait progressivement.

Différents indices tendent à montrer que ce phénomène intervient peu dans notre montage : le temps caractéristique observé sur la figure 7.10 est inchangé alors que la puissance du fondamental ou du second harmonique est modifiée. De plus, ce temps (100 μs) est court devant les échelles typiques des effets photoréfractifs (de l'ordre de la milliseconde dans le $KNbO_3$ [100]). Enfin, nous avons éclairé le cristal en continu avec une puissance de 2 W à 532 nm, focalisée sur un waist de l'ordre de 50 μm dans le cristal, de sorte à obtenir une répartition uniforme des porteurs de charges. Cette expérience n'a absolument pas modifié nos observations sur l'efficacité de doublage.

Effet thermique local

Une autre source potentielle de dommage optique est l'endommagement par avalanche (*avalanche breakdown*) [93] : un petit nombre d'électrons libres initialement présents dans le matériau (ou générés par excitation multiphotonique) sont accélérés lors de l'interaction avec l'impulsion laser. Ces électrons peuvent ensuite ioniser par collision d'autres atomes dans le cristal, produisant ainsi d'autres électrons libres qui vont également être accélérés pour produire en cascade d'autres collisions. Une partie de l'énergie est dissipée lors de chaque collision, ce qui induit un échauffement local du cristal à l'endroit de l'interaction avec le faisceau lumineux. Le $KNbO_3$ ayant une forte dépendance de l'indice de réfraction en fonction de la température (figure 7.7), une élévation locale (non-uniforme) de la température aura pour effet de modifier l'indice de réfraction et d'altérer l'accord de phase.

D'après le modèle de la référence [93], l'intensité seuil de cet effet est de l'ordre de la dizaine de GW/cm^2, alors que nous observons un seuil de 0.1 GW/cm^2. Néanmoins, ce phénomène pourrait expliquer partiellement nos observations (voir le modèle simple ci-dessous). En particulier, le temps calculé de diffusion thermique d'une impulsion dans le $KNbO_3$ est de l'ordre de 30 μs [156], ce qui correspond aux observations de la figure 7.10.

Absorption multiphotonique

Dans le cadre de l'absorption multiphotonique, le système subit une transition d'un état fondamental vers un état excité par une absorption simultanée de deux ou de plusieurs photons. Puis le système revient dans l'état fondamental par une désexcitation non-radiative. Le niveau excité peut tout à fait ne pas correspondre à un niveau d'énergie réel, tandis que d'autres niveaux d'impuretés peuvent intervenir dans le processus. Cet effet n'a pour l'instant été que peu étudié avec du $KNbO_3$, et toujours dans le cas d'un cristal épais placé en cavité optique [101].

Nous avons mesuré simultanément la transmission de l'infrarouge et le rendement de conversion de second harmonique selon deux conditions de focalisation. Un modèle très simple est proposé pour représenter nos mesures (voir la figure 7.11) en incluant un terme pour l'absorption à deux photons et un terme pour l'altération de la condition d'accord de phase due à un échauffement du cristal. La puissance du second harmonique en sortie du cristal est arbitrairement posée :

$$\mathcal{P}_{2\omega} = \eta_{SHG}\, T_{\mathrm{TPA}}\, \mathcal{P}_{\omega 0} \tag{7.10}$$

où η_{SHG} est le rendement de conversion, T_{TPA} est la transmission selon les processus multiphotoniques de l'onde infrarouge, $\mathcal{P}_{\omega 0}$ désigne la puissance infrarouge incidente sur le cristal. Pour une absorption multiphotonique faible, T_{TPA} s'exprime au premier ordre selon [94, 95] :

$$T_{\mathrm{TPA}} = 1 - \alpha_1 \frac{\mathcal{P}_{\omega 0}}{\mathcal{A}} \tag{7.11}$$

où α_1 est une constante et $\mathcal{A}$ désigne l'aire du faisceau focalisé. Le rendement de conversion inclut une dépendance linéaire selon l'intensité infrarouge, plus un terme correctif quadratique (α_2 et α_3 sont d'autres constantes) :

$$\eta_{SHG} = \alpha_2 \frac{\mathcal{P}_{\omega 0}}{\mathcal{A}} \left(1 - \alpha_3 \frac{\mathcal{P}_{\omega 0}}{\mathcal{A}}\right) \tag{7.12}$$

Enfin, dans une première approximation de la déplétion du fondamental, nous posons la puissance d'infrarouge transmise comme la portion restante après doublage de la puissance $T_{\mathrm{TPA}}\,\mathcal{P}_{\omega 0}$:

$$\mathcal{P}_{\omega} = (1 - \eta_{SHG})\, T_{\mathrm{TPA}}\, \mathcal{P}_{\omega 0} \tag{7.13}$$

Les paramètres α_i sont ensuite librement ajustés pour interpoler simultanément les courbes mesurées de transmission infrarouge et d'efficacité de conversion suivant la variable $\mathcal{A}$. Nos résultats sont présentés sur la figure 7.11. Même si ce modèle est bien sûr extrêmement basique et qu'aucune évaluation des paramètres α_i n'a été reliée à des grandeurs expérimentales, la concordance correcte du modèle avec les mesures de la figure 7.11 semble confirmer l'hypothèse d'effets conjoints d'une absorption multiphotonique et d'une altération de l'accord de phase pour expliquer l'origine des limites expérimentales dans la génération de second harmonique.

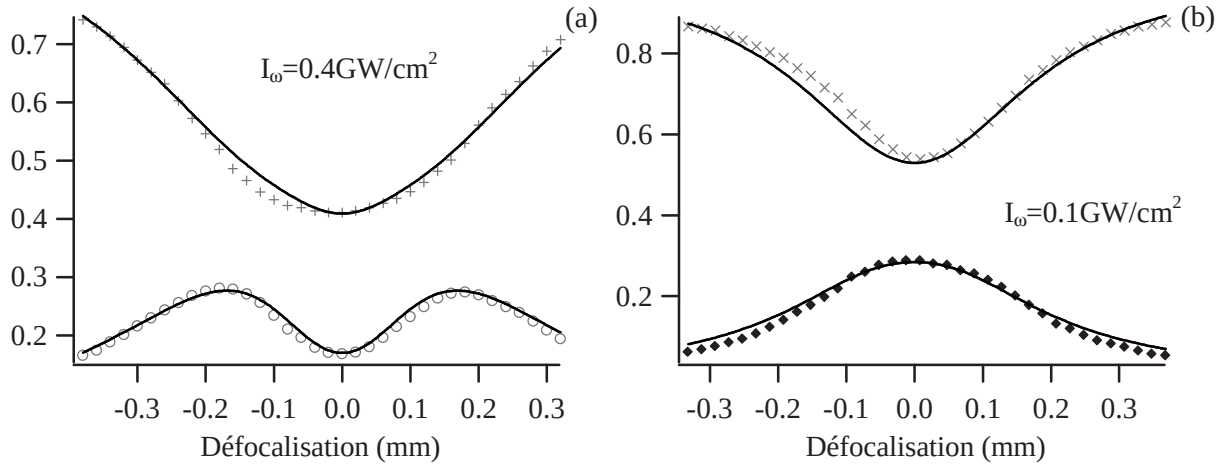

Figure 7.11: *Transmission infrarouge (courbes du haut) et efficacité de conversion (bas) lorsque la position du waist est décalée par rapport au centre du cristal (défocalisation) pour une intensité de 0.4 GW/cm^2 (a) et 0.1 GW/cm^2 (b). Le paramètre confocal $2z_R$ est identique pour ces mesures et vaut 1 mm. Les courbes sont les résultats du modèle présenté dans le texte et sont obtenues avec les mêmes paramètres α_i pour la transmission et pour l'efficacité de doublage.*

Optique non-linéaire impulsionnelle – $KNbO_3$ 0.1mm	
Génération de second harmonique (SHG)	Puissance incidente 40mW, efficacité typique 28%, efficacité max 32%, puissance bleue typique disponible 5mW, puissance bleue max 9mW (pompe *Verdi*)
Amplification paramétrique (OPA)	Déamplification/Amplification typique 0.50 / 2.50, max 0.40/2.65 (pompe 5mW)

7.2.3 Amplification paramétrique

L'amplification paramétrique permet de transférer de l'énergie du faisceau pompe vers la sonde ou réciproquement, et sera notre outil de base pour générer des états comprimés du champ lumineux (section 2.4.3). Mais avant de passer au domaine des fluctuations quantiques, nous étudions le signal de l'amplification paramétrique classique d'un faisceau sonde relativement intense. Ce faisceau est une faible fraction (1%) du faisceau fondamental, prélevée avant le doublage. Pour l'amplification paramétrique, nous utilisons un cristal mince de $KNbO_3$ (0.1 mm, NCPM en température), dans une configuration de type I dégénérée, et pour un simple passage des impulsions pompe et sonde.

Cette étape est d'une importance cruciale car l'interaction entre la pompe et la sonde fournit un signal (macroscopique) représentatif des modes quantiques que nous souhaitons produire. Ce signal permet d'ajuster l'alignement et l'adaptation du mode de l'oscillateur local pour la détection homodyne.

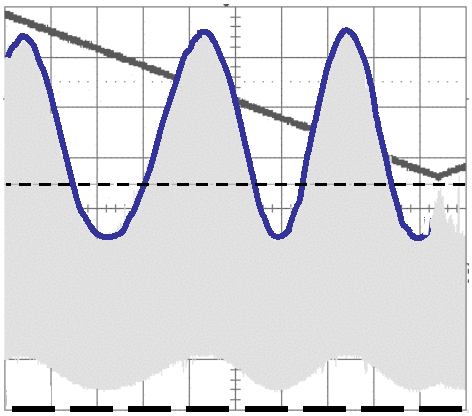

Figure 7.12: *Puissance du faisceau sonde après amplification paramétrique lorsque la phase de la pompe est balayée linéairement. La courbe en sinusoïde indique le signal utile produit par la photodiode rapide. La droite en tirets larges indique le niveau de référence (masse), celle en tirets étroits indique le niveau de puissance sonde en l'absence d'onde pompe. La tension en triangle (fond) correspond à la commande de la modulation de phase. Pour ces courbes, les gains paramétriques mesurés sont 0.76 et 1.64.*

Lors d'une expérience d'amplification paramétrique dégénérée, la phase relative entre la pompe et la sonde détermine le facteur de gain [93, 94]. Remarquons qu'une estimation théorique chiffrée de ces gains nécessiterait une connaissance précise du recouvrement entre le mode pompe

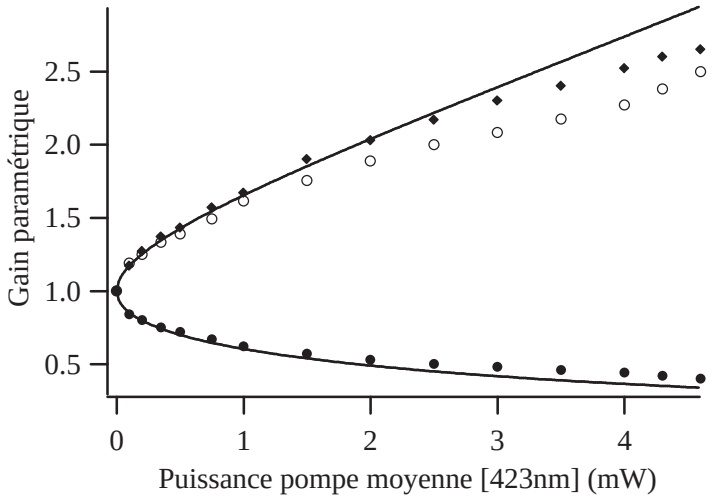

Figure 7.13: *Gain paramétrique en fonction de la puissance de pompe moyenne à 423 nm. Les disques et losanges pleins correspondent à la déamplification et à l'amplification. Les cercles marquent l'inverse du gain de déamplification. Les courbes solides sont des interpolations selon le modèle des ondes planes, obtenues pour des puissances de pompe inférieures à 0.5 mW.*

et le mode sonde, ainsi que la donnée des caractéristiques du mode spatio-temporel de la pompe, ce qui est délicat à estimer dans le cadre de nos expériences. Les gains paramétriques sont mesurés par une détection directe sur une photodiode de la puissance moyenne de la sonde amplifiée. Un exemple typique de la tension de photodétection observée à l'oscilloscope est présentée sur la figure 7.12, alors que la phase relative pompe-sonde est balayée linéairement. Le meilleur gain de déamplification mesuré est de 0.40 (-4.0 dB) correspondant à une amplification de 2.65 (+4.2 dB).

La figure 7.13 présente les gains paramétriques classiques en fonction de la puissance de la pompe, ainsi qu'une interpolation basée sur le modèle gain = $\exp(\pm\alpha\sqrt{\mathcal{P}_{2\omega}})$ dans le cadre de l'hypothèse des ondes planes. Ici, α est une constante dimensionnée proportionnelle au coefficient de non-linéarité effective et à la longueur du cristal. Ce paramètre est estimé suivant une interpolation des points expérimentaux pour des puissances moyennes de pompe inférieures à 0.5 mW. $\mathcal{P}_{2\omega}$ désigne la puissance moyenne de la pompe de second harmonique. Comme on pouvait le prévoir, le modèle théorique s'écarte des points expérimentaux pour de fortes puissances de pompe : la théorie des ondes planes ne peut pas modéliser la focalisation de faisceaux gaussiens ou l'utilisation d'impulsions ultracourtes. Un modèle plus raffiné nécessiterait une prise en compte de ces différents effets ainsi que des recouvrements limités des modes de la pompe et de la sonde.

La différence entre l'amplification et l'inverse de la déamplification apparaît également plus importante aux fortes puissances de pompe, où le phénomène de diffraction induite par le gain (GID : *Gain-Induced Diffraction*) est connu pour altérer la déamplification [102, 103, 104]. A cause de la dépendance spatiale gaussienne de l'intensité de pompe, la portion du faisceau sonde proche de l'axe de propagation est plus amplifiée que les portions aux bords, ce qui déforme le front d'onde, dégrade l'accorde de phase et limite le gain paramétrique. Comme on peut le voir sur la modélisation de la figure 7.14(a), le mode déamplifié est plus sensible à cet effet que le mode amplifié, ce qui explique que la diffraction induite par le gain affecte en premier lieu le

gain de déamplification.

Expérimentalement, nous avons optimisé le recouvrement entre la pompe et la sonde pour obtenir la meilleure déamplification (la configuration optique est présentée sur le schéma 7.1). La meilleure configuration est obtenue dans notre cas lorsque le waist de la sonde w_{sonde} est $\sqrt{2}$ fois plus petit que le waist pompe w_{pompe} à l'intérieur du cristal. Cette configuration est alors très différente du cas généralement étudié en théorie $w_{sonde} = \sqrt{2}\, w_{pompe}$ qui garantit le parfait accord des fronts d'ondes lors de la propagation [102, 103, 104]. Si cette dernière condition est théoriquement optimale avec des faisceaux gaussiens très focalisés, la sonde est nettement plus étendue que la pompe et une large portion spatiale de la sonde se propage dans une région "non-pompée" (figure 7.14(a)), ce qui dégrade la déamplification. L'optimisation expérimentale $w_{sonde} \simeq w_{pompe}/\sqrt{2}$ apparaît comme un compromis entre de faibles désaccords des fronts d'ondes et le recouvrement spatial des faisceaux. Un argument de plus en ce sens est qu'avec notre configuration optique, le paramètre confocal $2z_R$ est toujours grand devant la longueur du cristal. Les fronts d'ondes au niveau du cristal sont alors quasiment plans, ce qui permet de tolérer une certaine différence entre les fronts pompe et sonde.

La figure 7.15 présente les gains paramétriques mesurés lorsque la puissance pompe est fixée et le waist sonde est augmenté par rapport au waist pompe. On observe effectivement que le gain paramétrique diminue lorsque la dimension transverse de la sonde est augmentée. Cet effet est une conséquence directe du mauvais recouvrement spatial entre la pompe et la sonde. Pour de plus faibles waists sondes que ceux présentés sur la figure 7.15, le gain paramétrique est dégradé, tandis que la différence de courbure des fronts d'ondes ne peut plus être négligée. Nos mesures sont confrontées à un modèle simple selon [102] dans la limite de fronts d'ondes plans et en prenant en compte une répartition spatiale gaussienne. Le gain paramétrique s'exprime simplement selon :

$$G_{\mathrm{OPA}} = \frac{\int [E_{sonde}(r)\, exp(\pm \alpha E_{pompe}(r))]^2\, r\, dr}{\int [E_{sonde}(r)]^2\, r\, dr} \tag{7.14}$$

où $E_{sonde}(r)$ et $E_{pompe}(r)$ représentent les répartitions transverses gaussiennes, et α est une constante de gain fixée.

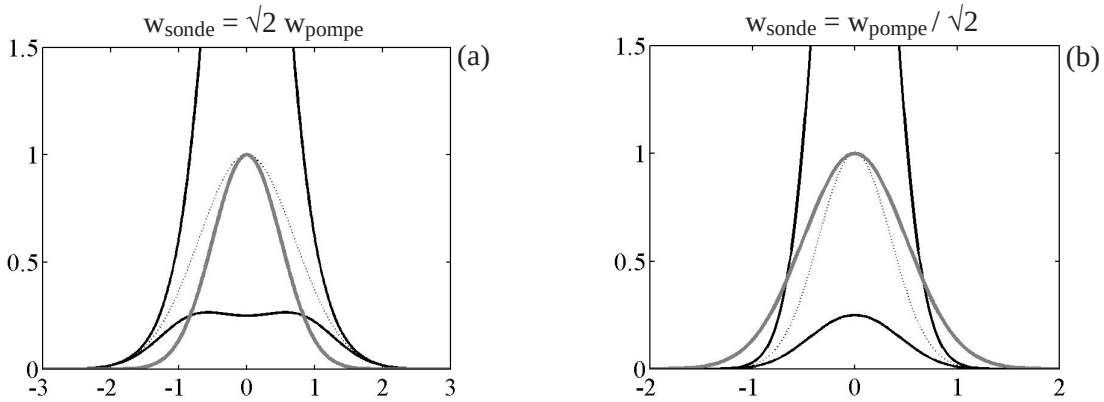

Figure 7.14: *Allure spatiale des modes sondes amplifiés et déamplifiés (noir). La courbe en pointillés indique le mode sonde en entrée du cristal et est à comparer au mode de la pompe (gris). Dans les cas (a) et (b), le gain paramétrique est fixé à 4 pour faire clairement apparaître les effets de déformation du mode déamplifié. Le cas (b) correspond sensiblement à notre configuration expérimentale (la courbure des fronts d'onde est négligée dans ce calcul).*

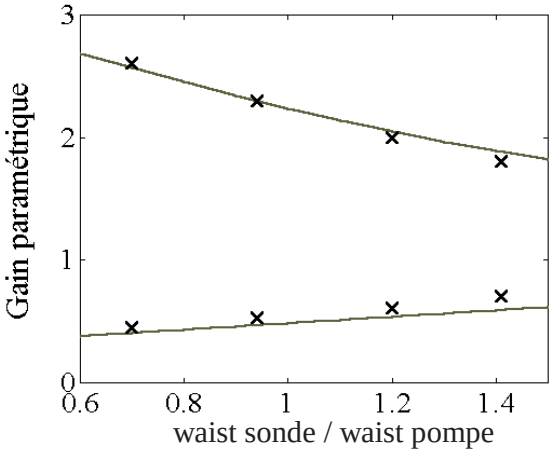

Figure 7.15: *Gain paramétrique en fonction du rapport waist sonde / waist pompe. Les croix indiquent nos mesures expérimentales tandis que les lignes sont un ajustement des points expérimentaux suivant le modèle (7.14).*

7.3 Génération de vide comprimé impulsionnel

7.3.1 Mesures homodynes individuelles

Lorsqu'aucun faisceau sonde n'est injecté dans l'amplificateur paramétrique, le processus non-linéaire jusqu'alors stimulé devient une émission spontanée de fluorescence paramétrique dans toute la plage d'accord de phase accessible (largeur spectrale ≈ 150 nm, acceptance angulaire $\approx 10°$). Cette émission fortement multimode peut heureusement être restreinte à l'étude d'un cas monomode : seul le mode signal adapté au faisceau oscillateur local sera détecté par la détection homodyne. L'oscillateur local intervient comme un filtre optique pour ne sélectionner que le mode spatio-temporel qui nous intéresse, en l'occurrence le mode vide comprimé issu de l'amplification paramétrique dégénérée d'un mode vide incident [111]. Pour obtenir un bon recouvrement de modes entre l'oscillateur local et le mode vide comprimé, le faisceau sonde (macroscopique) est réglé pour obtenir la meilleure déamplification paramétrique, puis ce faisceau sonde est ajusté pour interférer avec l'oscillateur local. Le visibilité des franges d'interférences obtenues fournit immédiatement l'efficacité d'adaptation des modes (voir le chapitre 3).

Notre système de détection homodyne impulsionnelle permet de mesurer la quadrature de l'impulsion vide comprimé en phase avec l'oscillateur local, ce qui offre un accès direct à la distribution statistique des quadratures signal dans le domaine temporel. La figure 7.16 présente le résultat de ces mesures de bruit en quadrature ainsi que la variance correspondante alors que la phase de l'oscillateur local est balayée linéairement. Pour certaines valeur de la phase relative, la variance de bruit mesurée passe sous le niveau de bruit quantique standard (SNL : *Shot Noise Level* $= N_0$), ce qui est la signature d'un faisceau comprimé. Les distributions de probabilité mesurées et théoriques correspondant aux quadratures comprimées et anti-comprimées sont représentées sur la figure 7.17.

Pour notre meilleur résultat, la variance mesurée de la quadrature comprimée (sans correction des pertes) est à -1.87 ± 0.06 dB sous le bruit quantique standard ($= 0.65\, N_0$), alors que la variance de la quadrature anti-comprimée se situe 3.32 ± 0.04 dB au-dessus du SNL ($= 2.15\, N_0$). Ces résultats s'accordent correctement avec les prédictions -1.92 ± 0.06 dB et $+3.32 \pm 0.06$ dB,

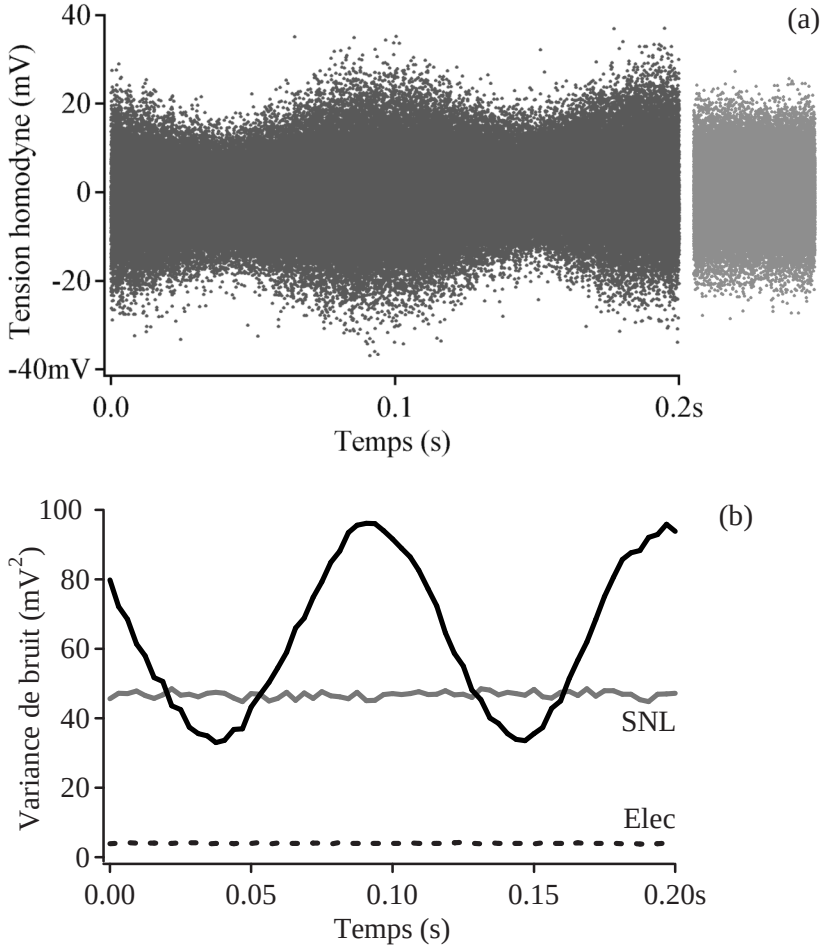

Figure 7.16: *(a) Mesures homodynes des quadratures du vide comprimé dans le domaine temporel alors que la phase de l'oscillateur local est balayée linéairement (la répartition du bruit correspondant au bruit de photon est représentée à droite à la même échelle en gris clair). (b) Variance correspondante tracée sur une échelle linéaire et calculée d'après des blocs de 2500 points expérimentaux de la figure (a). La puissance OL est de* 1.6×10^8 *photons/impulsion, bruit de photon 6.54 mV, bruit électronique 2.01 mV, bruit minimum mesuré 5.29 mV* ($0.65N_0$)*, bruit maximum 9.59 mV* ($2.15N_0$)*.*

obtenues d'après les mesures des gains paramétriques classiques du faisceau sonde (0.53 ± 0.01 et 2.51 ± 0.05) associées avec l'évaluation de l'efficacité globale de détection η_{hom}, d'après la formule (2.67). La procédure de mesure de cette efficacité globale est bien établie depuis les expériences de réduction des fluctuations quantiques [105, 106]. Elle peut également être vérifiée par une comparaison croisée entre le gain paramétrique et la réduction de bruit. D'après la formule (3.22), l'efficacité globale de détection s'exprime par $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2 = 0.76 \pm 0.01$ où la transmission optique $\eta_{opt} = 0.92$, l'efficacité quantique des photodiodes $\eta_{phot} = 0.945$ et l'adaptation des modes $\eta_{mod} = 0.935$ sont mesurées indépendamment. Si l'effet des pertes est virtuellement corrigé de nos mesures, les niveaux de bruit du vide comprimé en sortie du cristal sont alors de -2.68 dB et de $+4.0$ dB (0.54 et $2.51\,N_0$).

Ce résultat de compression des fluctuations quantiques est particulier dans le sens où, comme

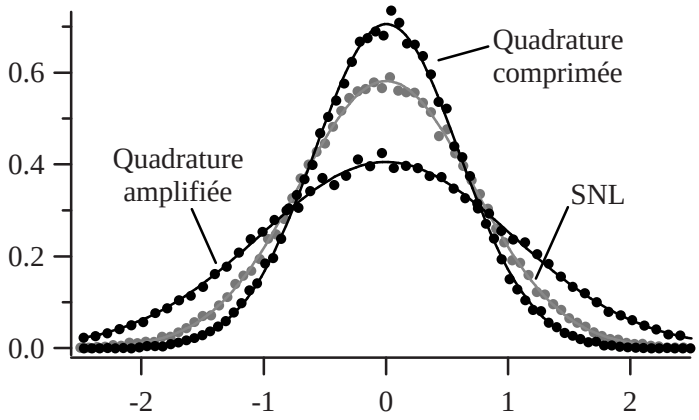

Figure 7.17: *Distributions de probabilité mesurées et normalisées pour les quadratures comprimées et anti-comprimées, avec la convention $N_0 = 1/2$. La variance de la quadrature comprimée est -1.87 dB sous le bruit quantique standard (SNL) alors que celle de la quadrature anti-comprimée est à +3.32 dB au-dessus du SNL.*

dans la référence [26], aucun analyseur de spectre n'est utilisé pour observer la réduction des fluctuation sur une plage étroite de fréquences mais qu'au contraire, la réduction de bruit est mesurée selon la répartition statistique de chaque impulsion sur l'ensemble des fréquences accessibles à notre détection homodyne.

7.3.2 Tomographie quantique du vide comprimé

Pour caractériser complètement le vide comprimé produit, nous avons mis en œuvre une procédure standard de tomographie quantique pour reconstruire la fonction de Wigner associée à l'état [17, 18, 29]. Pour les états comprimés, une telle démarche a déjà fait l'objet de différentes études par le passé [26, 27, 28]. Nous présenterons au chapitre suivant une méthode originale de caractérisation du vide comprimé, tandis que les techniques de tomographie quantique employées ici avec des états comprimés seront réutilisées au chapitre 9 dans le cadre des états non-gaussiens.

Reconstruction numérique de la fonction de Wigner par transformée de Radon inverse

Les distributions de probabilité en quadrature s'obtiennent par des projections de la fonction de Wigner suivant la direction de la quadrature choisie (section 2.2.2). Inversement, il est possible de reconstruire la fonction de Wigner associée à l'état étudié à partir des différentes distributions de probabilité en quadrature, ce qui constitue un des sujets majeurs du domaine de la tomographie quantique. Mathématiquement, il suffit d'inverser la relation (2.24) qui donne la distribution de probabilité $\Pr(x,\theta)$ pour la quadrature X_θ en fonction de la fonction de Wigner $W(x,p)$ de l'état. Cette opération nécessite cependant certaines précautions de calcul numérique [17], alors que la fonction de Wigner s'exprime à partir de $\Pr(x,\theta)$ par :

$$\begin{aligned} W(x,p) &= \frac{1}{4\pi^2 N_0}\int_0^{\pi}\int_{-\infty}^{+\infty} \Pr(q,\theta)\, K(x\cos\theta + p\sin\theta - q)\, dq\, d\theta \\ &= \frac{1}{4\pi^2 N_0}\int_0^{\pi} [\Pr(\theta) * K(x\cos\theta + p\sin\theta)]\, d\theta \end{aligned} \tag{7.15}$$

où $*$ désigne le produit de convolution classique et $K(q)$ est la fonction (*kernel*) définie par :

$$K(q) = \frac{1}{4\,N_0} \int_{-\infty}^{+\infty} |\varepsilon| \exp(\imath \frac{\varepsilon q}{2\,N_0})\, d\varepsilon \tag{7.16}$$

La formule (7.15) est connue sous le nom de *transformée de Radon inverse* et est la procédure de reconstruction de la fonction de Wigner la plus communément employée. Une mise en œuvre numérique réelle nécessite cependant un certain filtrage pour régulariser la fonction K et éviter des oscillations rapides sur la fonction de Wigner. Ce filtrage s'obtient en choisissant convenablement la fréquence de coupure k_c dans la définition régularisée de K [17] :

$$\begin{aligned} K(q) &= \frac{1}{4\,N_0} \int_{-k_c}^{+k_c} |\varepsilon| \exp(\imath \frac{\varepsilon q}{2\,N_0})\, d\varepsilon & (7.17)\\ &= \frac{2N_0}{q^2} \left[\cos(\frac{k_c q}{2N_0}) + \frac{k_c q}{2N_0} \sin(\frac{k_c q}{2N_0}) - 1\right] & (7.18) \end{aligned}$$

Au voisinage de $q = 0$ (lorsque $|k_c q| < 0.2\,N_0$), cette expression est développée en puissances de q pour éviter une divergence à l'origine.

L'algorithme de reconstruction de la fonction de Wigner par la transformation de Radon fonctionne de la manière suivante : étant donnée la fréquence de coupure k_c, la fonction K est calculée pour l'espace de points utiles avant d'être enregistrée. La fonction de Wigner s'obtient ensuite par des convolutions numériques des distributions de probabilités mesurées $\Pr(x, \theta)$ avec la fonction K suivant la formule (7.15), en approximant l'intégration sur la phase par une somme suivant les différentes références de phase disponibles après les mesures.

Ce paragraphe n'est qu'un bref résumé d'introduction au problème de la reconstruction expérimentale de la fonction de Wigner d'un état. Une autre méthode numérique, dite par "maximum de vraisemblance", sera décrite au chapitre 9. De nombreuses autres informations peuvent se trouver dans les références [17, 18, 29].

Mise en œuvre expérimentale

Une procédure automatisée permet d'acquérir les statistiques homodynes correspondant à 6 références de phase, réparties entre 0 et $5\pi/6$ (une propriété générale de la fonction de Wigner est d'être une fonction réelle définie par $\Pr(x, \theta)$ pour $\theta \in [0, \pi]$ [18]). Pour éviter des dérives expérimentales, la détection acquiert des ensembles de 50 000 impulsions correspondant à une phase particulière avant de lancer une procédure de recalage de phase décrite à la section 9.2.2 du chapitre 9. Pour chacune des 6 références de phase, les 50 000 mesures homodynes sont ensuite réparties en 90 canaux ce qui permet de construire les histogrammes présentés sur la figure 7.18.

La fonction de Wigner du vide comprimé est reconstruite à partir de la transformation de Radon inverse appliquée aux distributions de probabilité symétrisées $[\Pr(x, \theta) + \Pr(-x, \theta)]/2$ sans aucune correction de l'efficacité limitée η_{hom} de la détection homodyne (voir la figure 7.18). L'utilisation des distributions de probabilité symétrisées permet d'éviter des déformations de la fonction de Wigner reconstruite, qui seraient dues à un bruit statistique dans chaque canal des histogrammes de mesure. Notre programme de reconstruction numérique a été entièrement réalisé en langage C par Rosa Tualle-Brouri sur la base de la transformée de Radon inverse.

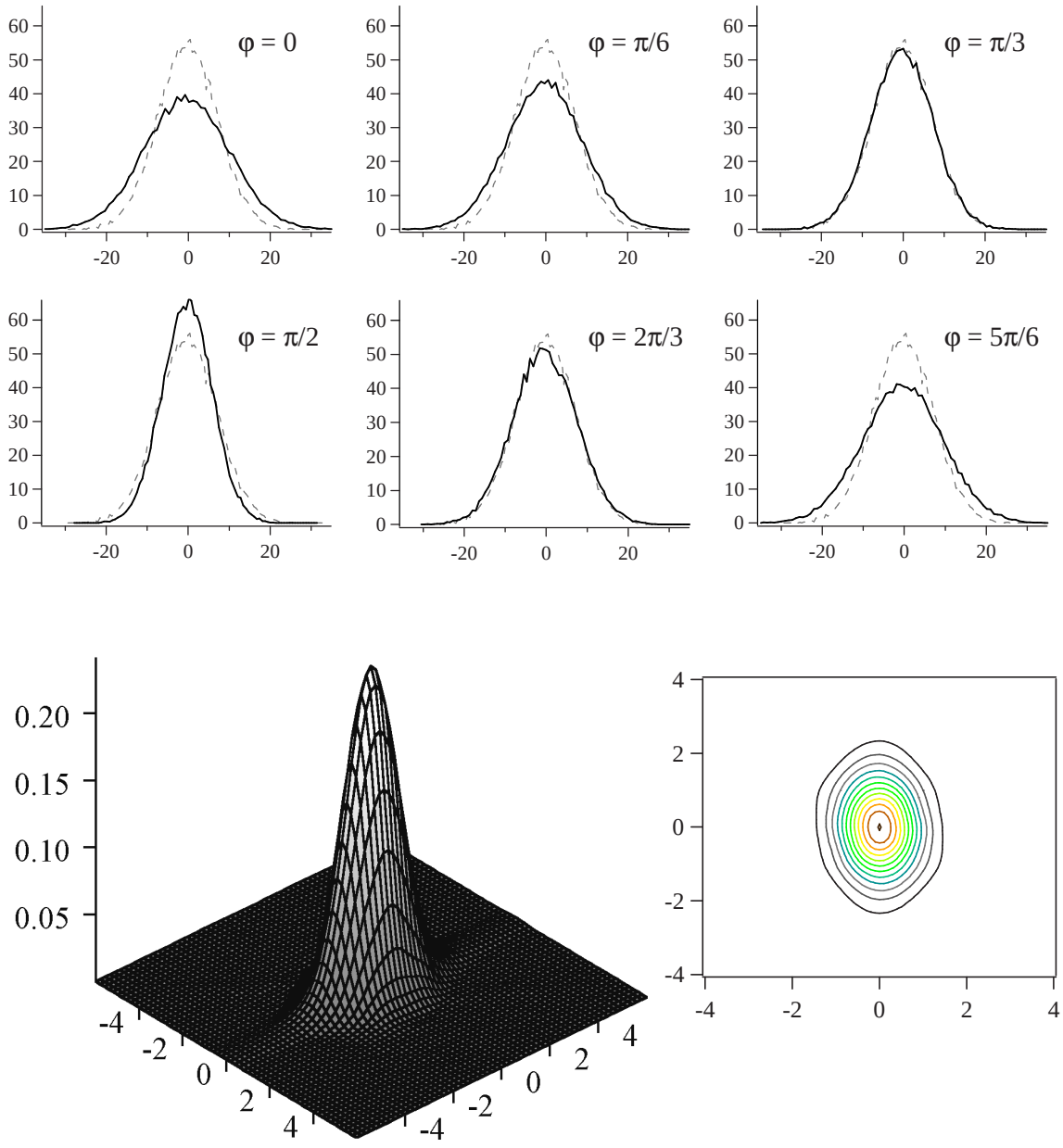

Figure 7.18: *Tomographie quantique d'un état vide comprimé. Les courbes du haut représentent les histogrammes des données brutes pour les 6 phases de référence utilisées lors de la reconstruction de la fonction de Wigner du vide comprimé. L'histogramme gaussien en gris correspond à la référence du bruit quantique standard pour la convention $N_0 = 1/2$. La variance de la quadrature comprimée (phase $\varphi = \pi/2$) est 1.75 dB sous le niveau de bruit quantique standard, tandis que la variance de la quadrature amplifiée (phase $\varphi = 0$) présente un excès de bruit de 3.1 dB. Le graphe en trois dimensions du bas représente la fonction de Wigner reconstruite à partir des données expérimentales non-corrigées par transformée de Radon inverse (efficacité homodyne $\eta_{hom} = 0.75$). L'équidistance entre les courbes de niveaux (à droite) est de 0.02. La troncature numérique dans le calcul de la transformée de Radon inverse est fixée à $k_c = 8$.*

7.4 Conclusion

Des états comprimés impulsionnels ont été simplement et efficacement générés en utilisant des conversions non-linéaires d'impulsions ultrabrèves dans des cristaux minces de niobate de potassium, permettant d'atteindre une réduction du bruit en quadrature de 2.7 dB sous le niveau de bruit quantique standard. Compte tenu de notre efficacité de mesure, ceci fournit une réduction mesurée de 1.9 dB. Les processus non-linéaires intervenant lors de ce processus ont été étudiés avec une attention particulière aux phénomènes limitant notre montage (absorption multiphotonique et échauffement thermique pour la génération de second harmonique et diffraction induite par le gain pour l'amplification paramétrique).

Associé à notre détection homodyne impulsionnelle, ce dispositif fournit tous les éléments pour des applications futures de traitement quantique de l'information utilisant des états comprimés, et sera notre montage de base en vue de la caractérisation des états comprimés par comptage de photons (chapitre 8) et de la génération d'états non-gaussiens (chapitre 9).

Chapitre 8

Caractérisation du vide comprimé par comptage de photons

Sommaire

Toute application utilisant des états comprimés de la lumière dans des protocoles de communication ou de calcul quantique devra nécessairement faire face au problème de la caractérisation de ces états. Un état quantique peut être complètement décrit par sa fonction de Wigner, que l'on peut reconstruire expérimentalement grâce à des procédures de tomographie quantique (voir la section 7.3.2 et les références [17, 27, 29]). D'une autre manière, on peut rappeler qu'un état gaussien est parfaitement déterminé par les moments d'ordre un et deux pour ses composantes de quadrature [18]. Une autre description complète d'un état gaussien est alors donnée par les moyennes des quadratures X et P et la matrice de covariance γ de l'état (introduite à la section 2.2.3). Il est ensuite possible de calculer différents autres paramètres caractéristiques, comme la réduction maximale du bruit quantique observable [116] ou la pureté de l'état [121, 122].

Pour déterminer la matrice de covariance d'un état gaussien, la technique généralement utilisée consiste à effectuer des mesures homodynes des quadratures, ce qui n'est qu'une autre manière d'effectuer une tomographie quantique de l'état. Jaromir Fiurášek et Nicolas Cerf ont récemment proposé une méthode alternative pour obtenir la matrice de covariance d'un état gaussien sans recourir à une détection homodyne [123], ou plus précisément sans aucun faisceau oscillateur local intense pour servir de référence de phase. Le schéma proposé repose exclusivement sur des techniques de comptage non-discriminantes en nombres de photons, utilisant des lames partiellement réfléchissantes et des détecteurs de photon uniques comme les photodiodes à avalanche.

Pour caractériser un état gaussien quelconque, le dispositif de Fiurášek et Cerf nécessite des mesures conjointes sur deux copies de l'état quantique. Cependant, cette méthode peut heureusement se réduire à des mesures sur une seule copie si on sait a priori que les valeurs moyennes des quadratures sont nulles, c'est-à-dire que l'état quantique est centré sur l'origine de l'espace des phases. Ainsi, dans le cas des états vides comprimés, une caractérisation complète peut être obtenue simplement à partir de techniques de comptage de photons sur une seule copie, et sans nécessiter de stabilité interférométrique. Les seules hypothèses requises sont que l'état caractérisé soit gaussien et centré sur l'origine de l'espace des phase.

Lors d'une collaboration avec Jaromir Fiurášek et Nicolas Cerf, nous avons expérimentalement mis en œuvre cette proposition théorique et discuté de sa faisabilité et de sa pertinence pour caractériser des états vides comprimés produits par le dispositif présenté au chapitre précédent [124]. La section 8.1 rappelle brièvement le principe théorique de la méthode de caractérisation par comptage de photons présentée dans [123]. Pour valider les résultats de cette technique, nous avons utilisé deux méthodes de référence, basées sur des mesures classiques du gain paramétrique et sur des mesures homodynes. L'exploitation de ces références sera abordée à la section 8.2 avant de discuter en détail nos résultats expérimentaux (section 8.3). Enfin, des simulations numériques (section 8.4) permettent d'illustrer l'utilisation de la méthode de comptage avec des conditions différentes de celles imposées par l'expérience.

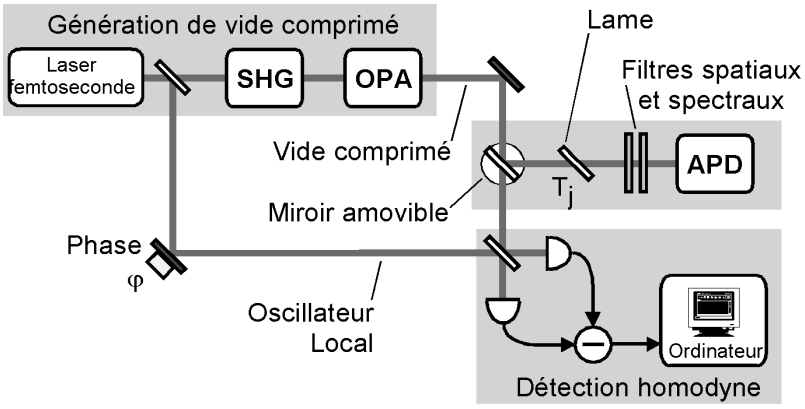

Figure 8.1: *Schéma de principe de l'expérience de génération et de caractérisation du vide comprimé impulsionnel.*

8.1 Méthode de caractérisation par comptage de photons

Les résultats théoriques exposés dans cette section reprennent pour l'essentiel ceux énoncés par Fiurášek et Cerf dans la description de leur nouvelle méthode de caractérisation [123, 124]. Tout au plus un nouvel éclairage est donné dans la direction d'une mise en œuvre expérimentale. Ces calculs se focalisent sur le cas d'un état vide gaussien issu d'un mélange statistique (i.e. de pureté $\mathcal{P} = Tr(\hat{\rho}^2)$ a priori différente de un). Un traitement complet de la méthode de caractérisation par comptage pour des états gaussiens quelconques est présenté dans [123].

8.1.1 Représentation du vide comprimé général par sa matrice de covariance

Un état gaussien général (a priori non pur), dont les quadratures sont de valeurs moyennes nulles, est théoriquement déterminé parfaitement par la donnée de sa matrice de covariance associée γ qui comprend les moments d'ordre deux des variables conjuguées X et P. Suivant la définition présentée à la section 2.2.3, γ est définie avec notre normalisation N_0 du bruit quantique :

$$\gamma = \frac{1}{N_0} \begin{pmatrix} \langle X^2 \rangle & \frac{1}{2}\langle XP + PX \rangle \\ \frac{1}{2}\langle XP + PX \rangle & \langle P^2 \rangle \end{pmatrix} \tag{8.1}$$

Afin de déterminer la réduction maximale du bruit quantique observable et le degré de pureté de l'état, il faut simplement mesurer les deux quantités invariantes de γ par changement de référentiel, à savoir sa trace $\mathrm{Tr}(\gamma)$ et son déterminant $\det(\gamma)$. La réduction maximale de bruit (*squeezing*), i.e. la plus petite variance en quadrature mesurable $V_{\min}$ pour un état, est déterminée par la plus petite valeur propre de la matrice de covariance. Ceci s'exprime en fonction de la trace et du déterminant de γ par [123] :

$$V_{\min} = \frac{N_0}{2}\left[Tr(\gamma) - \sqrt{Tr^2(\gamma) - 4\det(\gamma)}\right] \tag{8.2}$$

Par ailleurs, la pureté $\mathcal{P} = Tr(\hat{\rho}^2)$ pour un mélange statistique vaut [122] :

$$\mathcal{P} = \frac{1}{\sqrt{\det(\gamma)}} \tag{8.3}$$

8.1.2 Estimation par double comptage

Le principe de base de la caractérisation par comptage est illustré sur la figure 8.1. Le vide comprimé impulsionnel, produit par amplification paramétrique dégénérée [111], est envoyé sur une lame partiellement réfléchissante de transmission variable T avant d'être mesuré par une photodiode à avalanche (APD : *Avalanche PhotoDiode*). Ce dernier élément permet de discriminer entre la présence ou l'absence d'au moins un photon dans l'impulsion, fournissant un clic ou une absence de clic. La caractérisation par comptage repose sur des mesures de la probabilité de non-comptage de photon (non-clic) pour différentes valeurs de la transmission de la lame. En théorie, deux transmission T_1 et T_2 suffisent pour déterminer la matrice de covariance γ, ce que nous appelons la méthode par "double comptage". Dans le cadre d'une expérience réelle entachée d'incertitudes et de bruits, il peut être avantageux d'effectuer un plus grand nombre de mesures pour différentes valeurs de transmission, ce qui constitue la méthode par "maximum de vraisemblance".

L'action de la photodiode à avalanche d'efficacité limitée η_{apd} peut être modélisée par une lame de transmission η_{apd} suivie d'un détecteur idéal effectuant une mesure dichotomique décrite par les projecteurs $\Pi_0 = |0\rangle\langle 0|$ (absence de clic) et $\Pi_1 = 1 - \Pi_0$ (un clic).

Pour un état de matrice densité $\hat{\rho}$, la probabilité de non-clic est donnée par $P = \langle 0|\hat{\rho}|0\rangle$. Afin de relier cette probabilité à la matrice de covariance γ, il est utile d'exploiter la fonction Q de Husimi associée à l'état, qui est une autre description de l'opérateur densité $\hat{\rho}$ dans l'espace des phases. Pour un état gaussien centré sur l'origine de l'espace des phases, la fonction Q s'exprime par [18] :

$$Q(x,p) = \frac{1}{2\pi N_0}\langle\alpha|\hat{\rho}|\alpha\rangle = \frac{1}{\pi N_0\sqrt{\det(\gamma+I)}}\exp\left[-\frac{1}{N_0}\, r^T(\gamma+I)^{-1}r\right] \tag{8.4}$$

où $r = (x,p)$, $\alpha = (x+\imath p)/(2\sqrt{N_0})$ et I est la matrice identité. Avec cette définition, il est immédiat de voir que la probabilité de projection de l'état $\hat{\rho}$ sur le vide s'écrit :

$$P = 2\pi N_0\, Q(0) = \frac{2}{\sqrt{\det(\gamma+I)}} \tag{8.5}$$

(pour le cas d'un mode vide simple, $\det(\gamma+I) = 4$ et la probabilité de non-clic vaut 1).

La procédure de caractérisation fonctionne en effectuant plusieurs mesures de la probabilité de non-clic P_j pour différentes valeurs de la transmission de la lame T_j. La matrice de covariance γ_j de l'état après passage au travers de la lame s'écrit $\gamma_j = T_j\gamma + (1-T_j)I$, où γ est la matrice de covariance de l'état initial. En introduisant γ_j dans l'équation (8.5), on obtient après quelques calculs :

$$\frac{4}{P_j^2} = (\eta_{\text{apd}}T_j)^2\,\det(\gamma) + \eta_{\text{apd}}T_j(2-\eta_{\text{apd}}T_j)\,\mathrm{Tr}(\gamma) + (2-\eta_{\text{apd}}T_j)^2 \tag{8.6}$$

Ceci montre que P_j dépend de la transmission totale $\eta_{\text{apd}}T_j$, de la trace et du déterminant de la matrice de covariance γ de l'état initial. On peut remarquer de plus que $4/P_j^2$ est une fonction *linéaire* des deux inconnues $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$. Deux mesures de P_j pour deux transmission T_j différentes suffisent selon (8.6) pour constituer un système de deux équations d'inconnues $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$. Ce système peut alors facilement s'inverser pour fournir les estimations de $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$:

$$\mathrm{Tr}(\gamma) = \frac{2}{\eta_{\text{apd}}(T_2-T_1)}\left(\frac{T_2}{T_1P_1^2} - \frac{T_1}{T_2P_2^2}\right) + 2 - \frac{2}{\eta_{\text{apd}}T_1} - \frac{2}{\eta_{\text{apd}}T_2} \tag{8.7}$$

$$\det(\gamma) = \frac{2}{\eta_{\text{apd}}(T_1-T_2)}\left(\frac{2-\eta_{\text{apd}}T_2}{\eta_{\text{apd}}T_1P_1^2} - \frac{2-\eta_{\text{apd}}T_1}{\eta_{\text{apd}}T_2P_2^2}\right) + \frac{(2-\eta_{\text{apd}}T_1)(2-\eta_{\text{apd}}T_2)}{\eta_{\text{apd}}^2T_1T_2} \tag{8.8}$$

Ensuite, connaissant la trace et le déterminant de γ, on peut estimer les propriétés de réduction de bruit de l'état ainsi que sa pureté par les équations (8.2) et (8.3).

8.1.3 Estimation par le maximum de vraisemblance

La méthode ci-dessus, basée sur des mesures pour seulement deux valeurs de transmission, n'est pas forcément la plus avantageuse ou la plus précise lorsqu'il s'agit de caractériser une expérience réelle présentant d'inévitables bruits et incertitudes supplémentaires. Une procédure plus réaliste consiste à effectuer des mesures pour des valeurs de transmission T_j aussi nombreuses que possible, puis d'essayer d'extraire le maximum d'information (en terme de précision) de ces multiples mesures. Pour améliorer la précision sur l'estimation à partir de plusieurs mesures, une possibilité est de mettre en œuvre une procédure dite par maximum de vraisemblance (à ce sujet, voir par exemple les références [118, 119, 120]). Le principe de cette méthode est de fournir

les paramètres variables $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$ les plus à même de produire les données expérimentales mesurées.

Dans le cas général de l'application de la méthode par maximum de vraisemblance, on cherche à estimer un paramètre Υ à partir d'une série de n mesures de la variable x. La forme de la densité de probabilité $p(x|\Upsilon)$ de x conditionnée par Υ est connue, mais pas la valeur de Υ. On introduit alors la densité conjointe de probabilité conditionnée pour l'ensemble des mesures :

$$\mathcal{L}(\Upsilon) = \prod_{j=1}^{n} p(x_j|\Upsilon) \tag{8.9}$$

Cette fonction de Υ est appelée la fonction de vraisemblance des données. Le meilleur estimateur selon la méthode de maximum de vraisemblance est donné par la valeur du paramètre Υ qui maximise la fonction $\mathcal{L}$ [118, 119, 120].

Dans notre cas, la fonction de vraisemblance des données s'écrit :

$$\mathcal{L}\left(\mathrm{Tr}(\gamma), \det(\gamma)\right) = \prod_{j=1}^{n} P_j^{N_{\mathrm{rep}}-C_j}(1-P_j)^{C_j} \tag{8.10}$$

Ici C_j désigne le nombre de clics de photodétection par seconde mesurés pour la transmission T_j, N_{rep} est la cadence de répétition des impulsions, n le nombre de transmissions différentes utilisées. La probabilité de non-clic P_j est reliée à $\mathrm{Tr}(\gamma)$, $\det(\gamma)$ et T_j par la formule (8.6). Nous devons aussi prendre en compte certaines contraintes additionnelles sur les valeurs que peuvent prendre les paramètres $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$. Le fait que la matrice de covariance γ soit définie positive et doive satisfaire la relation d'incertitude d'Heisenberg $\det(\gamma) \geq 1$ impose les contraintes :

$$1 \leq \det(\gamma) \leq \left(\frac{\mathrm{Tr}(\gamma)}{2}\right)^2 \tag{8.11}$$

Avant d'exposer les résultats de ces méthodes originales de caractérisation d'un vide comprimé, nous présentons d'autres techniques utilisées comme références pour estimer la fiabilité de la méthode de comptage.

8.2 Autres méthodes : classique et homodyne

Pour prendre en compte un état le plus général possible (i.e. de pureté a priori différente de un), nous devons affiner le modèle de base de l'amplificateur paramétrique monomode pour exploiter au mieux les informations fournies par les mesures classiques de gains paramétriques et les mesures homodynes.

8.2.1 Modèle général de l'amplificateur paramétrique monomode

Si on reprend les résultats de l'étude du vide comprimé présentée au chapitre 7, il apparaît que l'inverse du gain de déamplification n'est pas égal au gain d'amplification,. Dans ce cas, l'état produit n'est pas pur mais correspond à un mélange statistique. Pour prendre en considération cette particularité, il faut améliorer le modèle simple de l'amplificateur paramétrique dégénéré (section 2.4.3) qui prédit une amplification e^{+2r} et une déamplification e^{-2r}.

De la manière la plus générale, un état gaussien monomode – dont les quadratures sont de valeurs moyennes nulles – s'exprime comme le résultat de l'action d'un opérateur de compression sur un état thermique gaussien [122, 117]. Traduit en termes de dispositifs d'optique quantique,

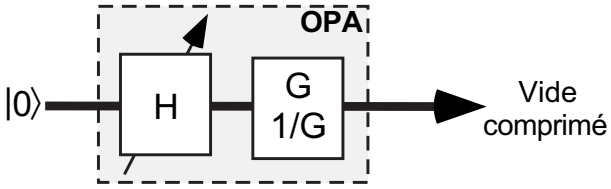

Figure 8.2: *Modèle général d'une source paramétrique monomode d'état vide comprimé. H est le gain d'un amplificateur non-dégénéré indépendant en phase, G et $1/G$ sont les gains paramétriques d'amplification et de déamplification d'un amplificateur dégénéré sensible en phase.*

ce théorème signifie que la source la plus générale d'états vides comprimés monomodes est réalisée par l'association de deux amplificateurs linéaires simples, telle que décrite à la figure 8.2 : un amplificateur indépendant de la phase de gain H, suivi d'un amplificateur sensible en quadratures de gains $G > 1$ (amplification) et $1/G$ (déamplification). Si on considère que notre état vide comprimé expérimental est généré par une boîte noire, cette boîte peut être complètement décrite par les paramètres H et G ou de manière équivalente par la donnée de $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$. [1]

Les composantes conjuguées de quadratures en sortie de l'amplificateur paramétrique total s'expriment par :

$$X_{\mathrm{out}} = \frac{1}{\sqrt{G}}\left(\sqrt{H}X_{\mathrm{vac}} + \sqrt{H-1}X_{\mathrm{aux}}\right) \tag{8.12a}$$

$$P_{\mathrm{out}} = \sqrt{G}\left(\sqrt{H}P_{\mathrm{vac}} - \sqrt{H-1}P_{\mathrm{aux}}\right) \tag{8.12b}$$

où nous posons X_{out} comme la quadrature comprimée. X_{vac} et X_{aux} sont respectivement les modes vide et auxiliaire incidents. Les variances des quadratures comprimées et amplifiées en sortie de l'amplificateur valent :

$$V_{\min} = \frac{(2H-1)}{G}N_0 \tag{8.13}$$

$$V_{\max} = (2H-1)\,G\,N_0 \tag{8.14}$$

Ceci permet d'obtenir la trace et le déterminant de la matrice de covariance par :

$$\mathrm{Tr}(\gamma) = \frac{V_{\min}+V_{\max}}{N_0} = (2H-1)\left(G+\frac{1}{G}\right) \tag{8.15}$$

$$\det(\gamma) = \frac{V_{\min}V_{\max}}{N_0^2} = (2H-1)^2 \tag{8.16}$$

Inversement, la trace et le déterminant de γ fournissent les variances minimales et maximales :

$$V_{\mathrm{max,min}} = \frac{N_0}{2}\left[\mathrm{Tr}(\gamma) \pm \sqrt{\mathrm{Tr}^2(\gamma) - 4\det(\gamma)}\right] \tag{8.17}$$

[1] Ce modèle d'association de deux amplificateurs est le modèle *monomode* le plus général pour décrire notre système physique [122, 117]. Cependant, ce modèle n'est pas unique : par exemple, on pourrait très bien inverser la position des amplificateurs G et H. Les équations seraient alors légèrement différentes, mais les résultats seraient similaires. Nous avons préféré la modélisation décrite sur la figure 8.2, qui est celle la plus communément utilisée dans la littérature. Un autre modèle très simple pour expliquer des gains paramétriques différents consisterait à décomposer le faisceau sonde en deux modes qui suivent chacun une amplification spécifique. Néanmoins, ce modèle *multimode* ne sera pas considéré plus avant et nous nous restreignons pour le moment à notre dispositif monomode général.

Finalement, la pureté $\mathcal{P} = \mathrm{Tr}[\hat{\rho}^2]$ d'un mélange statistique gaussien monomode est directement liée au nombre de photons moyen correspondant au bruit thermique $\overline{n} = H - 1$ [122] :

$$\mathcal{P} = \frac{1}{2\,\overline{n}+1} = \frac{1}{2H-1} \tag{8.18}$$

Avec ce modèle général de source monomode de vide comprimé, nous disposons de trois couples de paramètres équivalents pour caractériser l'état gaussien : $(\mathrm{Tr}(\gamma), \det(\gamma))$, (G, H) et $(V_{\min}, V_{\max})$. Si les formules ci-dessus nous permettent facilement de passer d'une représentation à une autre, chaque ensemble est néanmoins relié à une technique de mesure préférentielle : $(\mathrm{Tr}(\gamma), \det(\gamma))$ est donné par le comptage de photons, (G, H) par la mesure des gains paramétriques classiques et $(V_{\min}, V_{\max})$ par une mesure homodyne.

8.2.2 Méthode "classique"

Une première mesure de base pour caractériser l'amplificateur dégénéré est d'observer les gains paramétriques classiques pour un faisceau sonde macroscopique. Une telle démarche est simplement mise en œuvre comme à la section 7.2.3 par une mesure directe sur une photodiode de la puissance moyenne de la sonde lorsque la phase relative pompe-sonde est balayée. L'ajustement de cette phase relative permet d'accorder le gain paramétrique classique du minimum de gain de déamplification (en intensité) $\mathcal{G}_{\min}$ au gain maximum d'amplification $\mathcal{G}_{\max}$. La mesure des gains $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$ fournit une estimation sur les paramètres G et H caractéristiques de notre modèle d'amplificateur paramétrique :

$$G = \sqrt{\mathcal{G}_{\max}/\mathcal{G}_{\min}} \tag{8.19}$$

$$H = \sqrt{\mathcal{G}_{\max}\mathcal{G}_{\min}} \tag{8.20}$$

Avec ces valeurs, il est ensuite possible de calculer la trace et le déterminant de γ d'après les formules (8.15) et (8.16) ou bien la pureté de l'état d'après (8.18). Nous appelons "méthode classique" cette technique de caractérisation par une mesure des gains paramétriques classiques. Une limite fondamentale à la qualité de cette estimation pour représenter le vide comprimé quantique est posée par l'adaptation de modes limitée entre le faisceau pompe et le faisceau sonde. Néanmoins, pour les puissances et les configurations utilisées, la bonne concordance entre les niveaux de compression obtenus d'après les mesures homodynes et les mesures classiques lors de la section 7.3 nous permettent d'être confiants dans cette technique. Par ailleurs, nous pourrons comparer les résultats de cette caractérisation "classique" à ceux fournis par des mesures homodynes.

8.2.3 Méthode "homodyne"

D'après les principes de la tomographie quantique [17], une caractérisation complète du vide comprimé peut être obtenue par des mesures homodynes des composantes de quadratures conjuguées. La détection homodyne résolue en temps que nous avions déjà utilisée lors de l'étude des chapitres précédents nous permet de distinguer entre la quadrature la plus comprimée et la quadrature amplifiée pour en mesurer ensuite les variances $V_{\mathrm{hom,min}}$ et $V_{\mathrm{hom,max}}$. Suivant la démarche instaurée à la section 7.3, les pertes et les imperfections de la détection homodyne peuvent être modélisées par une lame de transmission $\eta_{\mathrm{hom}} = 0.76 \pm 0.01$ correspondant à l'efficacité globale de notre détection. Compte tenu de cette efficacité, on peut virtuellement

corriger l'influence des pertes pour estimer les variances des quadratures comprimées et amplifiées produites par la source paramétrique(en entrée de la détection homodyne) :

$$\begin{aligned} V_{\min} &= [\,V_{\mathrm{hom,min}} - (1-\eta_{\mathrm{hom}})N_0\,]/\eta_{\mathrm{hom}} \\ V_{\max} &= [\,V_{\mathrm{hom,max}} - (1-\eta_{\mathrm{hom}})N_0\,]/\eta_{\mathrm{hom}} \end{aligned} \tag{8.21}$$

D'après les relations de la section 8.2.1, ces mesures permettent la caractérisation complète de la matrice de covariance de l'état $(\mathrm{Tr}(\gamma), \det(\gamma))$ ou des paramètres de l'amplificateur paramétrique (G, H). Cette technique constitue la méthode de caractérisation dite "homodyne", et sera utilisée comme référence pour valider la nouvelle méthode par comptage.

8.3 Caractérisations expérimentales

8.3.1 Dispositif expérimental

Nous reprenons le dispositif de génération de vide comprimé impulsionnel introduit au chapitre précédent [111]. Le principe général du montage de validation de la caractérisation de l'état par comptage est présenté sur la figure 8.1. Une fois produit par amplification paramétrique dégénérée, le vide comprimé peut être dirigé vers deux modules de détection différents grâce à un miroir amovible.

- *Détection homodyne impulsionnelle* : chaque impulsion incidente interfère avec une impulsion intense correspondant à l'oscillateur local. L'électronique rapide de détection permet une mesure de quadrature résolue pour chaque impulsion incidente (chapitre 3).

- *Compteur de photons* : le vide comprimé est envoyé sur une lame de transmission T variable. Ce faisceau est ensuite filtré spatialement par deux trous dans des plans conjugués par Fourier, puis par un filtre spectral de largeur 3 nm centré à la longueur d'onde du fondamental 846 nm. La présentation détaillée de ce montage de filtrage sera discutée au chapitre 9. Enfin, le faisceau est détecté par une photodiode à avalanche silicium standard (EG&G SPCM-AQ-131). Le filtrage est rendu nécessaire par la très large plage d'émission de fluorescence paramétrique de notre montage (largeur spectrale $\approx$ 150 nm, acceptance angulaire $\approx 10°$) et par le fait que la photodiode à avalanche – contrairement à la détection homodyne – est sensible à des photons dans tous les modes spatio-temporels incidents. Le dispositif de filtrage est alors crucial pour s'assurer que seul le mode vide comprimé qui nous intéresse est détecté par la photodiode.

Un dernier module de détection différent utilise un faisceau sonde intense et une photodiode pour mesurer les gains paramétriques classiques.

8.3.2 Mesures de référence

Les résultats des déductions obtenues à partir des mesures "classiques" et "homodynes" sont présentés sur les figures 8.3, 8.4 et 8.5 pour différentes puissances de pompe. Comme on peut le remarquer en particulier sur la figure 8.3(b), pour de fortes puissances de pompe, les résultats des mesures homodynes et classiques ne se recouvrent plus au sein de leur barres d'erreurs respectives. La raison principale de cet effet est que notre "boîte noire" amplificateur paramétrique est simplement un modèle monomode et souffre de limitations fondamentales. En effet, aux fortes puissances de pompe, la physique impliquée entre dans un régime multimode du fait notamment de la diffraction induite par le gain [102].

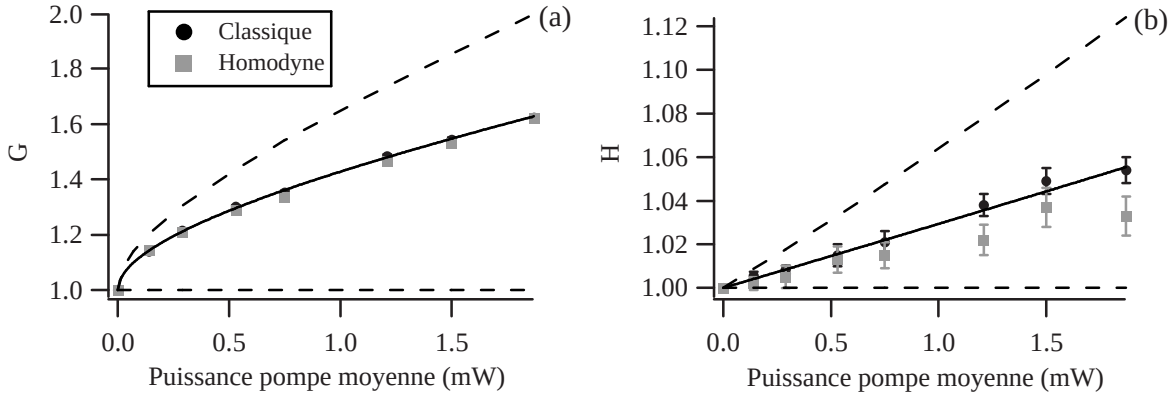

Figure 8.3: *Gains paramétriques G et H en fonction de la puissance moyenne de pompe à 425 nm. Les mesures "classiques" (disques noirs) corespondent aux mesures de l'amplification d'une sonde classique. Les mesures "homodynes" (carrés gris) sont estimées d'après les mesures homodynes de variances $V_{\min}$ et $V_{\max}$. La courbe en trait plein est une interpolation des mesures "classiques" d'après la théorie des ondes planes : $G = \exp(2\alpha\sqrt{P_{pompe}})$, $H = \cosh^2(\beta\sqrt{P_{pompe}})$. Les bornes obtenues à partir de la méthode de comptage de photons sont indiquées par les courbes en pointillés (voir la discussion section 8.3.5).*

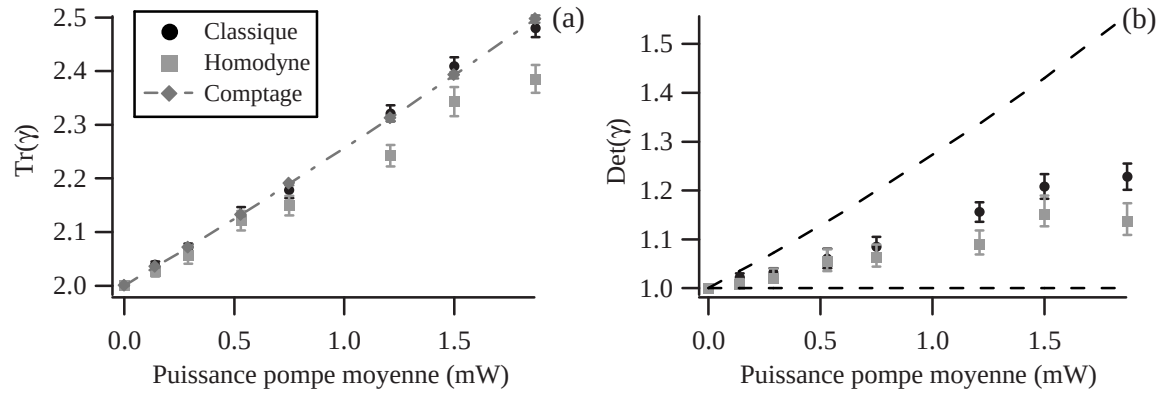

Figure 8.4: *Trace* $\mathrm{Tr}(\gamma)$ *et déterminant* $\det(\gamma)$ *en fonction de la puissance moyenne de pompe avec les notations de la figure 8.3. Pour faciliter la lecture de la figure (a), les résultats expérimentaux sur l'estimation de la trace par la méthode de comptage (losanges) sont reliés par une ligne en trait-point.*

8.3.3 Efficacité de détection par comptage

Un point essentiel pour la caractérisation d'un vide comprimé par les nouvelles méthodes de comptage est d'estimer aussi précisément que possible l'efficacité globale de détection η_{apd} de la voie photodiode à avalanche. Cette efficacité globale inclut plusieurs termes : les transmissions des optiques et des différents filtres (spatiaux et spectraux) ainsi que l'efficacité quantique de la photodiode à avalanche silicium. Une première estimation peut donc être effectuée en tenant compte des transmissions des filtres mesurées avec un faisceau sonde intense. Les filtres spatiaux et spectraux transmettent respectivement 16% et 17% du faisceau sonde, tandis que l'efficacité

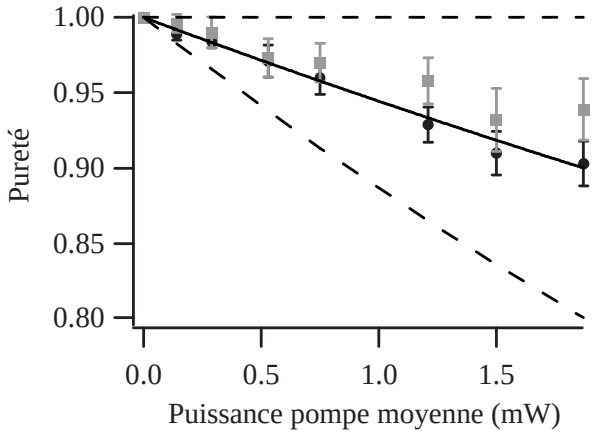

Figure 8.5: *Pureté $\mathcal{P}$ de l'état en fonction de la puissance moyenne de pompe. Les notations sont les mêmes que sur la figure 8.3.*

quantique de la photodiode à avalanche est estimée autour de 50% (donnée constructeur), ce qui fournit une valeur d'efficacité globale $\eta_{\text{apd}} \approx 1.4\%$. Cependant, en l'absence de mesure précise de l'efficacité quantique de la photodiode à avalanche, nous ne pouvons pas donner une estimation précise de η_{apd}.

Pour obtenir une estimation plus fiable de η_{apd}, nous exploitons les mesures de taux de comptage de photons dans le cadre de la caractérisation du vide comprimé. Lorsque la transmission de la lame supplémentaire est fixée à $T = 1$, un modèle simple permet de montrer que le nombre d'événements de photodétection par seconde C_{clics} est directement relié à η_{apd} dans la limite des faibles taux de comptage. Pour cela, nous utilisons le modèle général de l'amplificateur paramétrique de la figure 8.2. D'après les formules des amplificateurs paramétriques présentées au chapitre 2, l'opérateur création de photon dans le mode de sortie s'écrit :

$$\hat{a}_{\text{out}} = \sqrt{H}\,(\hat{a}_{\text{vac}}\,\cosh r + \hat{a}^{\dagger}_{\text{vac}}\,\sinh r) + \sqrt{H-1}\,(\hat{a}^{\dagger}_{\text{aux}}\,\cosh r + \hat{a}_{\text{aux}}\,\sinh r) \tag{8.22}$$

où r désigne le facteur de compression donné par $G = \exp(2r)$. Les modes $\hat{a}_{\text{vac}}$ et $\hat{a}_{\text{aux}}$ sont respectivement les modes vide et auxiliaire entrant dans le dispositif de la figure 8.2, conformément aux équations (8.12). L'expression de l'opérateur $\hat{a}_{\text{out}}$ permet de calculer ensuite le nombre d'événements de photodétection par seconde C_{clics}, lorsque la transmission de la lame supplémentaire est fixée à $T = 1$. Compte tenu de l'efficacité de détection η_{apd}, et dans la limite des faibles taux de comptage, on obtient :

$$\begin{aligned} C_{\text{clics}} &= \eta_{\text{apd}}\,N_{\text{rep}}\,[\,H\,\sinh^2(r) + (H-1)\,\cosh^2(r)\,] \\ &= \frac{1}{2}\,\eta_{\text{apd}}\,N_{\text{rep}}\,[\,(\,H-1/2\,)(\,G+1/G\,)-1\,] \end{aligned} \tag{8.23}$$

où $N_{\text{rep}} = 780.4$ kHz est la cadence de répétition des impulsions. Pour obtenir une estimation précise de η_{apd}, la mesure de C_{clics} est répétée pour différentes puissances de pompe et toujours avec $T = 1$. Les dépendances de G et H en fonction de la puissance de pompe sont prises en compte par le modèle des ondes planes $G = \exp(2\alpha\sqrt{P_{pompe}})$ et $H = \cosh^2(\beta\sqrt{P_{pompe}})$, où les coefficients α et β sont obtenus d'après les mesures par la méthode "classique", présentées sur la figure 8.3. L'équation (8.23) permet alors grâce à une interpolation des points expérimentaux de la figure 8.6 une estimation $\eta_{\text{apd}} = 0.84 \times 10^{-2} \pm 0.02 \times 10^{-2}$. Le décalage entre cette valeur et la

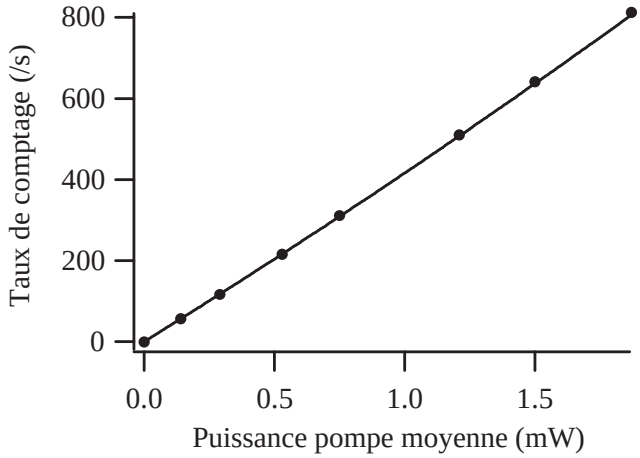

Figure 8.6: *Nombre d'événements de photodétection par seconde en fonction de la puissance de pompe moyenne pour la transmission maximale de la lame $T = 1$. La ligne en trait plein est le résultat du modèle de l'équation (8.23), d'où on extrait l'estimation de l'efficacité globale de détection de la voie photodiode à avalanche $\eta_{\mathrm{apd}} = 0.84 \times 10^{-2} \pm 0.02 \times 10^{-2}$.*

précédente estimation grossière de η_{apd} peut s'expliquer par de faibles différences entre le mode vide comprimé et le mode de la sonde réglée pour le maximum de déamplification classique.

8.3.4 Estimation par double comptage

Dans notre expérience, nous avons utilisé entre 4 et 6 valeurs différentes pour la transmission de la lame T_j. Pour chaque transmission, 100 mesures du nombre de d'événements de photodétection par seconde C_j sont effectuées afin d'obtenir une bonne précision statistique sur la moyenne. Grâce à un filtrage et un fenêtrage temporel adéquat de la détection, le nombre de coups d'obscurité par seconde a été maintenu à un niveau raisonnablement faible (environ 20 coups/s) et a été soustrait des données expérimentales.

Comme nous l'avons vu à la section 8.1.2, deux mesures de la probabilité de non-clic pour deux valeurs différentes T_1 et T_2 de la transmission de la lame sont suffisantes en théorie pour obtenir les valeurs de $\mathrm{Tr}(\gamma)$ et $\det(\gamma)$ d'après les équations (8.7) et (8.8). Avec nos données expérimentales, la formule (8.7) fournit une valeur satisfaisante de $\mathrm{Tr}(\gamma)$, qui est proche des valeurs obtenues par les mesures classiques et homodynes. Cependant, la formule (8.8) n'offre aucune estimation correcte du déterminant $\det(\gamma)$ avec des valeurs typiquement de 1.2 ± 0.6.

L'incertitude étendue sur la valeur du déterminant est une conséquence de la faible efficacité de détection η_{apd} employée. Dans notre configuration expérimentale, les incertitudes de mesures possèdent une forte influence sur la précision de l'estimation du déterminant, alors que la trace est moins sensible. A titre d'exemple, si on étudie les effets d'une incertitude sur P_1, on trouve :

$$\frac{d\,\mathrm{Tr}(\gamma)}{dP_1} = \frac{4}{\eta_{\mathrm{apd}} P_1^3} \qquad \frac{d\det(\gamma)}{dP_1} = \frac{-16}{\eta_{\mathrm{apd}}^2 P_1^3} \tag{8.24}$$

Ceci montre que pour notre dispositif expérimental le déterminant est environ 400 fois plus sensible à de faibles incertitudes sur P_1 que la trace. Des conclusions identiques peuvent être tirées concernant les incertitudes sur P_2, T_1, T_2 ou η_{apd} (l'écart-type de l'incertitude relative sur C_j vaut typiquement 1%, celui sur T_j 0.5% et celui sur η_{apd} 1%).

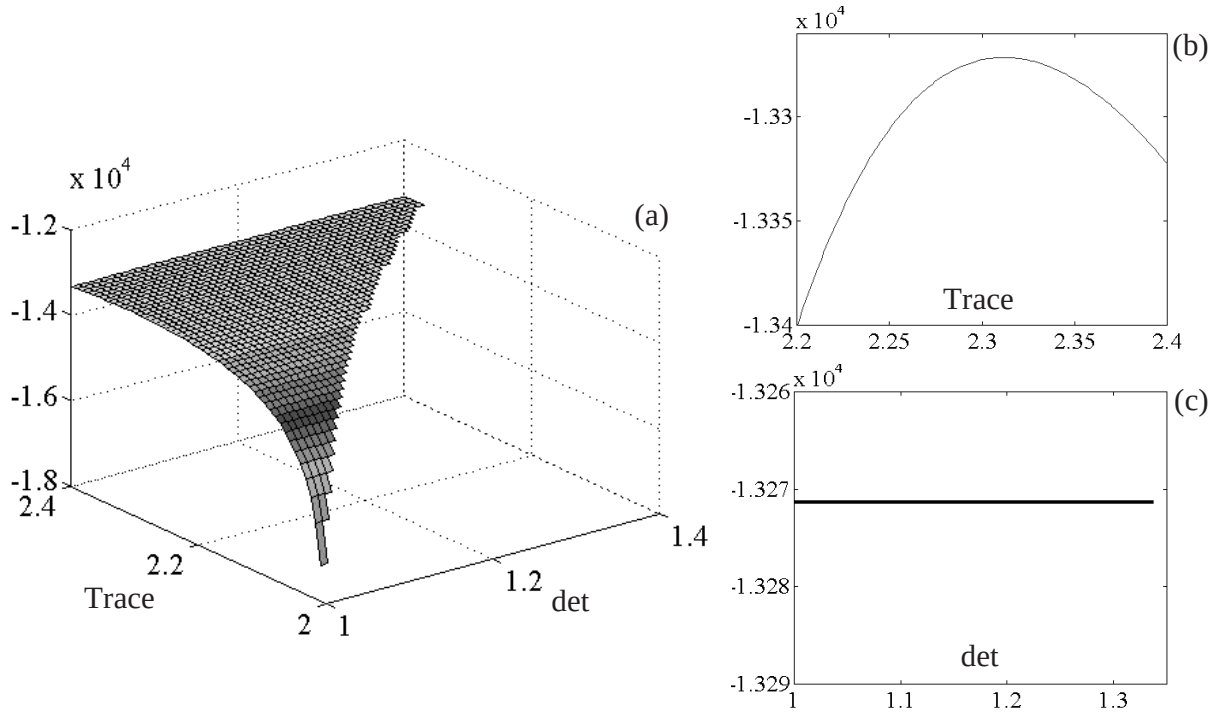

Figure 8.7: *(a) Fonction de vraisemblance des données obtenues pour une puissance de pompe moyenne de 1.21 mW, en fonction des paramètres libres trace et déterminant. (b) Coupe en fonction de la trace pour* $\det = 1.1$. *(c) Coupe en fonction du déterminant pour la trace optimale* $\mathrm{Tr} = 2.316$ *qui maximise* $\mathcal{L}$. *Pour ce réglage expérimental, la méthode "classique" fournit les résultats* $\mathrm{Tr}(\gamma) = 2.321$ *et* $\det(\gamma) = 1.156$.

8.3.5 Estimation par le maximum de vraisemblance

Pour gagner en précision sur l'estimation du déterminant en exploitant l'ensemble de nos mesures, nous avons mis en œuvre une méthode par maximum de vraisemblance telle que présentée dans la section 8.1.3. Le logarithme de la fonction de vraisemblance $\mathcal{L}$ donnée par l'équation (8.10) est calculé à partir des données expérimentales C_j, de l'estimation de l'efficacité η_{apd} et des transmissions T_j mesurées par le facteur de transmission d'un faisceau sonde intense. Le maximum global de $\log(\mathcal{L})$ est ensuite recherché par un tri numérique entre les valeurs.

Les résultats expérimentaux sur l'estimation de $\mathrm{Tr}(\gamma)$ pour différentes puissances de pompes sont représentées sur la figure 8.4(a) et correspondent largement avec les valeurs obtenues par la méthode "classique". Il est à noter que des trois techniques de mesure mises en œuvre, la méthode de comptage associée à une estimation par le maximum de vraisemblance fournit la plus faible incertitude sur la valeur estimée de $\mathrm{Tr}(\gamma)$, ce qui n'a rien d'étonnant vu le nombre de mesures effectuées et la précision statistique obtenue ainsi.

Malheureusement, compte tenu de la faible efficacité globale de détection η_{apd}, la fonction de vraisemblance est quasiment une fonction constante du déterminant $\det(\gamma)$ dans la région autorisée par les contraintes (8.11) (voir la figure 8.7). En conséquence, aucune estimation précise du déterminant de la matrice de covariance n'a pu être obtenue à partir de nos données expérimentales, la maximisation de la fonction de vraisemblance retournant essentiellement une

valeur variable entre les bornes 1 et $(\mathrm{Tr}(\gamma)/2)^2$. La technique de comptage appliquée à notre dispositif ne permet de ne donner que des bornes sur les gains paramétriques H et G à partir de la seule connaissance de la trace $\mathrm{Tr}(\gamma)$:

$$1 \leq G \leq \left[\frac{\mathrm{Tr}(\gamma)+\sqrt{\mathrm{Tr}(\gamma)^2-4}}{\mathrm{Tr}(\gamma)-\sqrt{\mathrm{Tr}(\gamma)^2-4}}\right]^{1/2} \tag{8.25}$$

$$1 \leq H \leq \frac{\mathrm{Tr}(\gamma)+2}{4} \tag{8.26}$$

Les courbes en tirets sur les figures 8.3, 8.4(b) et 8.5 expriment le fait qu'aucune estimation du déterminant meilleure que celle autorisée par (8.11) sachant la valeur de $\mathrm{Tr}(\gamma)$ n'a pu être obtenue.

8.3.6 Discussion

Nous avons également essayé d'autres méthodes d'estimations numériques pour obtenir une valeur du déterminant – comme une inversion de moindres carrés ou des méthodes par récurrence – mais aucune de ces techniques n'a pu offrir une estimation correcte. Une meilleure compréhension de la difficulté intrinsèque d'estimer précisément $\det(\gamma)$ peut être obtenue en réécrivant la formule (8.6) suivant les termes de transmission :

$$\frac{4}{P_j^2} = [\det(\gamma) - \mathrm{Tr}(\gamma) + 1]\ (\eta_{\mathrm{apd}}\, T_j)^2 \ + \ 2\ [\mathrm{Tr}(\gamma) - 2]\ \eta_{\mathrm{apd}}\, T_j \ + \ 4 \tag{8.27}$$

Cette formule fait apparaître que le déterminant est directement relié à la dépendance quadratique de P_j^{-2} par rapport à la transmission globale, alors que la trace peut être obtenue par le coefficient de dépendance linéaire de P_j^{-2}. La difficulté fondamentale de l'estimation de $\det(\gamma)$ résulte du fait que l'information pertinente pour le déterminant est présente dans des termes en $(\eta_{\mathrm{apd}}\, T)^2$, qui sont très faibles pour nos données expérimentales compte tenu de l'efficacité de détection η_{apd}.

On pourrait alors essayer d'augmenter l'efficacité de détection, en diminuant les restrictions des filtrages spatiaux et spectraux. Cependant, cette démarche ne nous semble pas réaliste d'un point de vue expérimental pour plusieurs raisons. Premièrement, si les filtres sont moins efficaces, la physique associée aux mesures sera dans un régime clairement multimode, ce qui dépasse le cadre de notre modèle [2]. Deuxièmement, nous perdrions ainsi toute possibilité de vérifier la concordance des résultats fournis par la technique de comptage avec les autres méthodes classiques et homodynes. Enfin, même dans le cas d'une absence de filtre spatial et d'un filtre spectral de 10 nm de large, l'efficacité de détection expérimentale demeurera faible (de l'ordre de 15% en raison de l'efficacité quantique de la photodiode à avalanche et de la réflectivité du réseau de diffraction utilisé comme filtre spectral). D'après nos simulations numériques, cette valeur améliorée d'efficacité ne nous permet pas d'affiner beaucoup notre estimation sur $\det(\gamma)$, comme nous allons le voir à la section suivante.

[2] En principe, la méthode de comptage permet de vérifier si une description monomode est appropriée ou non. Si un seul mode est détecté, P^{-2} est un polynôme d'ordre deux en $(\eta_{\mathrm{apd}}\, T)$ d'après l'équation (8.27). Plus généralement, on peut montrer que si le détecteur mesure N modes, alors P^{-2} devient un polynôme d'ordre $2N$ en $(\eta_{\mathrm{apd}}\, T)$ [123]. Cependant, pour déterminer expérimentalement le degré du polynôme P^{-2} en fonction de la transmission, il faut obtenir une très haute précision dans la mesure de P et de fortes valeurs de η_{apd}, ce qui n'est pas le cas de notre montage.

8.4 Simulations numériques

Si nos valeurs expérimentales d'efficacité de détection ne permettent pas une caractérisation complète du vide comprimé par la méthode de comptage, il est alors très important d'estimer quelle est l'efficacité minimale à atteindre. Nous avons simulé les résultats expérimentaux pour différentes valeurs de η_{apd}, les autres paramètres étant choisis en concordance avec notre dispositif. La trace et le déterminant de la matrice de covariance sont ensuite estimés par l'application de la méthode de maximum de vraisemblance à partir de nos données expérimentales simulées. Les mesures sont supposées être effectuées pour quatre valeurs de transmission $T_1 = 1$, $T_2 = 0.75$, $T_3 = 0.5$ et $T_4 = 0.25$, avec pour chaque valeur 100 mesures du nombre d'événements de photodétection par seconde. Nous utilisons enfin les valeurs $\det(\gamma)_{\text{exp}} = 1.156$ et $\text{Tr}(\gamma)_{\text{exp}} = 2.321$ comme un exemple typique (correspondant à une puissance de pompe moyenne de 1.21 mW). Cette simulation numérique a été mise en œuvre par Jaromir Fiurášek avec qui nous avons collaboré lors de cette étude.

Pour caractériser l'erreur de notre estimation comparée à la valeur expérimentale réelle, nous introduisons les quantités :

$$\begin{aligned} {\sigma_{\text{det}}}^2 &= \langle\, |\det(\gamma)_{\text{est}} - \det(\gamma)_{\text{exp}}|^2 \,\rangle \\ {\sigma_{\text{Tr}}}^2 &= \langle\, |\text{Tr}(\gamma)_{\text{est}} - \text{Tr}(\gamma)_{\text{exp}}|^2 \,\rangle \end{aligned} \tag{8.28}$$

Ces estimateurs d'erreur sont obtenus par des moyennes statistiques sur 1000 expériences simulées.

Pour isoler l'influence intrinsèque des faibles valeurs d'efficacité η_{apd} des incertitudes statistiques de mesure sur T_j et η_{apd}, nous avons d'abord considéré que ces paramètres sont connus précisément et que les fluctuations statistiques de C_j (de l'ordre de 1%) sont les seules sources d'erreurs. L'estimateur d'erreur σ_{det} correspondant à cette hypothèse est représenté par des disques sur la figure 8.8. Cette quantité décroît rapidement lorsque η_{apd} augmente, pour atteindre une estimation fiable de $\det(\gamma)$ avec $\sigma_{\text{det}} < 10^{-2}$ lorsque $\eta_{\text{apd}} > 15\%$. Dans le cadre d'une expérience réelle, les incertitudes supplémentaires sur T_j et η_{apd} vont induire une plus grande erreur sur l'estimation de $\det(\gamma)$. En prenant une incertitude relative de 0.5% pour T_j et de 1% pour η_{apd}, nos calculs prédisent un estimateur d'erreur σ_{det} nettement plus important (carrés gris sur la figure 8.8). Pour atteindre une estimation fiable de $\det(\gamma)$ avec $\sigma_{\text{det}} \approx 2 \times 10^{-2}$, il faut dans ce cas $\eta_{\text{apd}} > 50\%$.

Enfin, ces simulations numériques confirment la bonne précision de l'estimation de la trace $\text{Tr}(\gamma)$: nous avons pu obtenir $\sigma_{\text{Tr}} < 10^{-2}$ pour η_{apd} aussi faible que 1% et avec les incertitudes expérimentales réelles prises en compte.

8.5 Conclusion

Nous avons mis en œuvre une technique originale de caractérisation complète d'un état vide comprimé par la matrice de covariance associée. Cette technique est basée sur des méthodes de comptage de photons et ne nécessite pas de stabilité interférométrique ou de référence de phase. Notre dispositif expérimental a pu déterminer avec précision la trace de la matrice de covariance associée à l'état, mais malheureusement une efficacité de détection trop faible nous a empêché d'estimer précisément le déterminant. Si la trace peut être déterminée correctement avec une efficacité de détection de l'ordre du pourcent, il faut une efficacité nettement plus importante pour estimer le déterminant, typiquement de l'ordre de 50%.

En principe, différentes voies d'amélioration sont possibles. La première serait de reprendre la conception de la source paramétrique pour générer un état comprimé monomode, ce qui

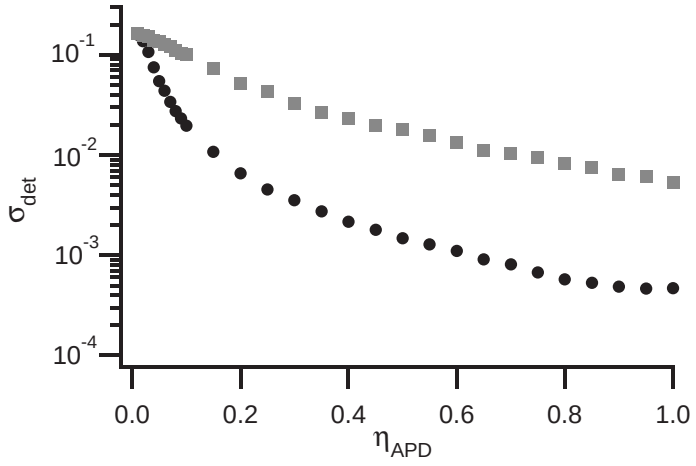

Figure 8.8: *Erreur sur l'estimation* $\sigma_{\rm det}$ *du déterminant* $\det(\gamma)$ *en fonction de l'efficacité de détection* $\eta_{\rm apd}$ *dans le cas où les paramètres* T_j *et* $\eta_{\rm apd}$ *sont parfaitement connus (disques) ou entachés d'une incertitude de 0.5% sur* T_j *et 1% sur* $\eta_{\rm apd}$ *(carrés).*

peut être avoisiné sous certaines conditions d'accord de phase et de focalisation dans un cristal non-linéaire. Une deuxième direction serait d'améliorer la transmission des filtres spatiaux et spectraux, par exemple en utilisant des filtres multidiélectriques de meilleure transmission qu'un réseau de diffraction classique. L'ensemble de ces techniques expérimentales améliorées pourra dans l'avenir offrir des perspectives d'exploitation nouvelles pour des applications en communication ou en calcul quantique avec des variables continues.

Chapitre 9

Source d'états quantiques non-gaussiens

Sommaire

Le dispositif de transfert de clé secrète avec des états cohérents introduit au chapitre 5 présente l'intérêt d'atteindre de très hauts débits de transmission dans le domaine où les pertes du canal sont faibles, tout en ne nécessitant que des techniques relativement simples de manipulation de champs lumineux cohérents [73]. Pour une atténuation du canal de l'ordre de quelques dB, les protocoles à états cohérents offrent ainsi un fort potentiel de développement par rapport aux protocoles à photons uniques [40]. Par contre, dans le domaine où les pertes lors de la transmission sont importantes, les protocoles à états cohérents ne permettent pas dans leur réalisation actuelle d'envisager des portées supérieures à quelques dizaines de kilomètres (voir la discussion à la section 5.3.1). Dans le cas de l'utilisation de variables discrètes portées par des photons uniques, la distance maximale atteinte en pratique est de l'ordre de la centaine de kilomètres [40], ce qui constitue actuellement le record de portée de la cryptographie quantique. Au-delà de cette distance, les données secrètes sont noyées dans des erreurs de diverses origines, dues par exemple aux coups d'obscurité des détecteurs ou aux imperfections des algorithmes de traitement des données.

Afin d'améliorer cette portée maximale, un défi technologique majeur pour la cryptographie quantique à variables continues ou discrètes est de mettre en œuvre des dispositifs permettant de propager l'information quantique sur de longues distances : les *répéteurs quantiques* [160, 1, 2]. En principe, ces éléments compensent les pertes en ligne sans ajout de bruit, ce qui les distingue des amplificateurs classiques utilisés pour les télécommunications optiques. Les propositions actuelles de tels systèmes sont toutes basées sur l'exploitation de l'intrication quantique partagée entre deux parties à grande distance. De façon ultime, cette intrication permet de téléporter ensuite l'information de l'émetteur au récepteur [158, 159]. La condition indispensable pour une transmission quantique à grande distance est alors de disposer d'une ressource d'intrication de qualité satisfaisante, ce qui impose de corriger par des actions locales les perturbations ayant affecté le transfert. Une telle action d'amélioration de l'intrication quantique par des opérations locales est appelée *distillation de l'intrication*. Ce processus joue aussi un rôle crucial dans les preuves inconditionnelles de sécurité en cryptographie quantique [65, 77].

Pour des systèmes de dimension finie, des états d'intrication faible peuvent être transformés en des états plus intriqués par des dispositifs physiques agissant localement, au prix d'une réduction du nombre de systèmes quantiques préparés [47]. De manière surprenante, la transposition de ce résultat dans le domaine des variables continues n'est pas simple et pose des problèmes fondamentaux sur les possibilités de manipulation des variables continues. Il a été prouvé récemment que des états gaussiens (qui sont les états utilisés par presque tous les protocoles de communication quantique à variables continues) ne peuvent pas être distillés vers des états de plus forte intrication par des opérations gaussiennes seules [163, 164]. Pour distiller l'intrication de variables continues gaussiennes, il faut impérativement sortir du domaine gaussien, quitte à y revenir par des opérations ultérieures [127]. Avec des opérations non-gaussiennes, la référence [125] propose une méthode pour distiller l'intrication d'états gaussiens, mais les états après transformation ne sont plus gaussiens. De plus, la mise en œuvre pratique de cette proposition constitue un défi technologique considérable.

Une approche originale de la distillation de l'intrication portée par des états gaussiens a été présentée dans [127]. Ce protocole permet de distiller en sortie des états gaussiens de degré d'intrication arbitraire, et ne nécessite que des éléments optiques passifs et des photodétecteurs distinguant entre la présence et l'absence de photons. Au sein de la procédure proposée, une première étape appelée "dégaussification" transforme des états EPR en états non-gaussiens. Ces états sont ensuite distillés par des opérations linéaires et des photodétections vers d'autres états de plus forte intrication, tout en étant ramenés vers des états gaussiens par une méthode de "gaussification". Le principe de base pour cette procédure est de combiner des états sur des lames semi-réfléchissantes, et de mesurer le champ dans l'un des ports de sortie de la lame avec une photodiode à avalanche. La présence ou l'absence d'un photon sur la voie mesurée conditionne la sélection de l'autre voie, qui est distillée par ce processus.

Les limites des méthodes gaussiennes de manipulation de l'information quantique [163, 164] et le protocole de distillation de l'intrication [127] nous encouragent à nous intéresser aux états quantiques non-gaussiens et à leur exploitation. Par ailleurs, l'utilisation d'une préparation d'état conditionnelle par addition ou soustraction de photon [138, 139, 140] est une méthode connue pour ses possibilités de génération d'états quantiques spécifiques : états sub-Poissoniens [112, 113, 114], non-gaussiens [126] ou chats de Schrödinger [131, 129].

Nous avons ainsi mis en œuvre une procédure de "dégaussification", qui transforme des états vides comprimés en états monomodes non-gaussiens [128]. Le principe de cette procédure est présenté sur la figure 9.1 : un faisceau vide comprimé est envoyé sur une lame de faible réflectivité, dont la voie réfléchie est dirigée sur une photodiode à avalanche. La détection d'un photon par cet élément conditionne alors la projection de l'état transmis sur un état non-gaussien, caractérisé

ensuite par notre détection homodyne résolue en temps. Comme dans [127], ce protocole est basé sur une post-sélection commandée par un événement de photodétection et n'utilise que des éléments linéaires simples. De plus, l'extension de ce dispositif à une paire de faisceaux EPR intriqués constituerait la première étape de la procédure de distillation de l'intrication proposée dans [127].

Ce chapitre détaille notre procédure de dégaussification monomode [128], des aspects théoriques (section 9.1) à l'exploitation des données expérimentales (sections 9.2 et 9.3) avant d'aborder quelques applications pour la manipulation de l'information quantique (section 9.4).

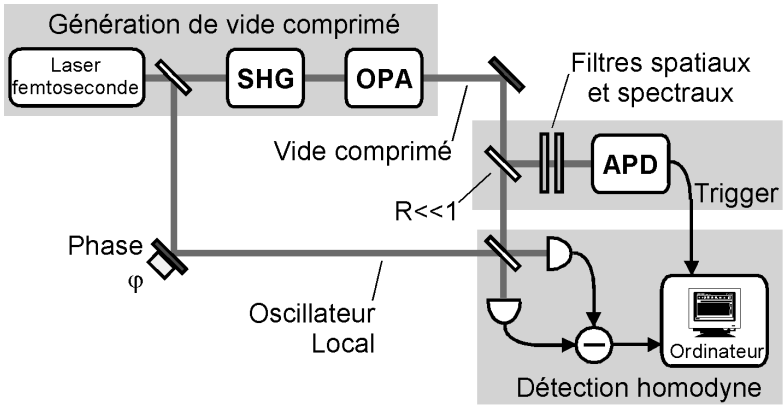

Figure 9.1: *Schéma de principe de la source d'états non-gaussiens impulsionnels.*

Figure 9.2: *Photographie du montage complet montrant les éléments de détection homodyne (1), de conditionnement (2) et de source du vide comprimé (3).*

9.1 Procédure théorique de dégaussification

Pour générer un état non-gaussien, notre procédure de dégaussification fonctionne en deux étapes : passage de l'impulsion vide comprimé sur une lame de faible réflectivité, puis conditionnement par un événement de photodétection sur la voie réfléchie. Pour aborder les aspects théoriques de cette procédure, nous proposons d'abord un calcul simple dans le cas d'un état pur (faible réflectivité de la lame), avant de présenter les résultats généraux plus proches de la réalité expérimentale.

9.1.1 Principe de conditionnement

Le vide comprimé pur, produit par fluorescence paramétrique dégénérée, ne comporte que des termes pairs en nombre de photons, ce qui résulte de l'annihilation d'un photon bleu pour la génération d'une paire de photons rouges lors du processus paramétrique. La décomposition du vide comprimé sur la base des états de Fock s'écrit [17] :

$$|\Psi_s\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{m=0}^{\infty} \left[C_{2m}^{m} \left(\frac{1}{2} \tanh r \right)^{2m} \right]^{1/2} |2m\rangle \;=\; \sum_{m=0}^{\infty} \alpha_{2m} \, |2m\rangle \tag{9.1}$$

où r est le facteur de compression défini par $V_{\min} = e^{-2r} N_0$. Avec nos valeurs typiques $r = 0.43$, on obtient $\alpha_0 = 0.96$, $\alpha_2 = 0.27$ et $\alpha_4 = 0.10$. Ceci indique déjà que les termes d'ordre supérieurs à 2 dans la décomposition de Fock ne seront pas négligeables pour nos degrés de compression des fluctuations quantiques. L'état vide comprimé produit dans notre expérience diffère donc d'une production aléatoire d'une paire de photons paramétrique, présentée par exemple dans [30].

L'état $|\Psi_s\rangle$ est envoyé sur une lame partiellement réfléchissante de réflectivité (en intensité) R et de transmission $T = 1 - R$. L'autre port d'entrée de la lame est dans un mode vide. Les photons incidents sont alors répartis entre chaque sortie suivant une distribution binomiale, ce qui induit la création d'un état intriqué à deux modes entre les voies de sortie de la lame. D'après la formule (2.66) de la section 2.4.1, l'état à deux modes $|\Psi'_s\rangle$ en sortie de la lame s'écrit :

$$|\Psi'_s\rangle = \sum_{m=0}^{\infty} \sum_{k=0}^{2m} \alpha_{2m} \sqrt{C_{2m}^{k}} \, \sqrt{R}^{\,k} \, \sqrt{T}^{\,2m-k} \, |k\rangle_1 \, |2m-k\rangle_2 \tag{9.2}$$

où $|\,.\rangle_1$ désigne l'état réfléchi envoyé vers la photodiode à avalanche et $|\,.\rangle_2$ est l'état transmis envoyé vers la détection homodyne.

Dans le cas où la réflectivité de la lame R est très faible, on peut dans un premier temps négliger les termes d'ordre supérieur à 1 en nombre de photons dans la voie réfléchie (le calcul général fait l'objet de la section suivante). L'état sur la voie homodyne après conditionnement d'un événement de photodétection sur la voie APD s'obtient en appliquant le projecteur $|1\rangle_1\langle 1|_1$ sur l'état $|\Psi'_s\rangle$, ce qui fournit l'état après conditionnement sur un click (les effets des pertes de la voie APD ne sont pas considérés ici) :

$$|\Psi_{\text{cond}}\rangle \;=\; \mathcal{N} \sum_{m=1}^{\infty} \alpha_{2m} \sqrt{C_{2m}^{1}} \, \sqrt{R} \, \sqrt{T}^{\,2m-1} \, |2m-1\rangle_2 \tag{9.3}$$

$$\;=\; \sqrt{2RT}\,\mathcal{N} \left[\alpha_2 \, |1\rangle_2 + \sqrt{2}\, T \, \alpha_4 \, |3\rangle_2 + \ldots \right] \tag{9.4}$$

où $\mathcal{N}$ est un facteur de normalisation défini par (9.8) tel que la norme de $|\Psi_{\text{cond}}\rangle$ soit égale à 1.

La formule (9.3) montre que l'état conditionné $|\Psi_{\rm cond}\rangle$ ne contient que des termes *impairs* dans sa décomposition sur la base de Fock. D'une manière intuitive, l'opération de conditionnement / dégaussification peut s'imaginer comme une soustraction de photon à l'état vide comprimé : le terme de vide $\alpha_0 |0\rangle$ disparaît, la présence d'un photon dans la voie réfléchie garantit en première approximation l'existence d'un terme impair en nombre de photons dans la voie transmise.

La fonction d'onde d'un état de Fock de nombre impair étant nulle à l'origine, il en résulte que la fonction d'onde associée à $|\Psi_{\rm cond}\rangle$ sera (en théorie) également nulle à l'origine. Ceci constitue une signature flagrante de l'aspect non-gaussien de l'état. De façon similaire, la fonction de Wigner associée à l'état de Fock $|n\rangle$ vaut à l'origine de l'espace des phases $W_{|n\rangle}(0,0) = (-1)^n/(2\pi N_0)$. D'après la propriété de linéarité des fonctions de Wigner, nous obtenons pour l'état conditionné :

$$W_{\rm cond}(0,0) = \frac{-1}{2\pi N_0} |\langle \Psi_{\rm cond} \mid \Psi_{\rm cond}\rangle|^2 = \frac{-1}{2\pi N_0} \tag{9.5}$$

qui est négatif et vaut ≈ -0.32 pour $N_0 = 1/2$. Le conditionnement par un click sur la voie réfléchie est donc une procédure simple pour générer un état fortement non-classique.

L'état conditionné donné par la formule (9.3) s'écrit explicitement [1] :

$$|\Psi_{\rm cond}\rangle = \frac{2\mathcal{N}\sqrt{R}}{\sqrt{\cosh r}} \sum_{p=0}^{\infty} \frac{\sqrt{(2p+1)!}}{p!} \left(\frac{1}{2}\tanh r\right)^{p+1} \sqrt{1-R}^{\,2p+1} \mid 2p+1\rangle_2 \tag{9.6}$$

$$= \frac{1}{\sqrt{\cosh^3 \zeta}} \sum_{p=0}^{\infty} \frac{\sqrt{(2p+1)!}}{p!} \left(\frac{1}{2}\tanh \zeta\right)^{p} \mid 2p+1\rangle_2 \tag{9.7}$$

avec

$$\mathcal{N} = \sqrt{\frac{\cosh^3 r}{\sinh^2 r \, \cosh^3 \zeta \; R(1-R)}} \quad \text{et} \quad \tanh \zeta = (1-R)\, \tanh r \tag{9.8}$$

Dans l'hypothèse où la réflectivité de la lame est très faible ($R \ll 1$) et ou un seul photon est réfléchi, l'état après conditionnement $|\Psi_{\rm cond}\rangle$ est un état pur, ce qui simplifie nettement les calculs utilisant cet état pour des procédures d'exploitation de l'information quantique. Cependant, notre expérience utilise une lame de réflectivité $R = 11.5\%$ et ne satisfait donc pas la condition $R \ll 1$. L'état conditionné n'est ainsi pas projeté vers un état pur, mais un mélange statistique d'états. De plus, en vue d'un traitement complet du dispositif expérimental, il faut incorporer dans notre calcul les effets des différentes pertes par transmission ou inefficacités du dispositif, ce qui est pris en compte à la section suivante.

9.1.2 Calcul général

Pour tenir compte d'une valeur arbitraire de la réflectivité R, la sommation dans la formule (9.2) du vide comprimé après passage à travers la lame est réagencée suivant le nombre de photons réfléchis. Nous tronquerons le nombre de photons pris en compte dans la décomposition du vide comprimé à $2N = 10$, ce qui est largement suffisant pour nos degrés de compression

[1] Le seul point non immédiat du calcul est le développement mathématique :

$$\cosh^3 r = \sum_{k=0}^{\infty} \frac{(2k+1)!}{2^{2k}\,(k!)^2} \,(\tanh r)^{2k}$$

(avec $2N = 10$, on peut raisonnablement décrire des facteurs de compression jusqu'à $r \simeq 0.55$). L'état en sortie de lame se réécrit :

$$|\Psi'_s\rangle = \sum_{k=0}^{2N} \sum_{m=\lceil k/2 \rceil}^{N} \alpha_{2m} \sqrt{C_{2m}^k}\, \sqrt{R}^{\,k}\, \sqrt{T}^{\,2m-k}\, |k\rangle_1\, |2m-k\rangle_2 \tag{9.9}$$

Dans le cas d'une détection parfaite monomode, le conditionnement (dégaussification) s'effectue simplement en appliquant le projecteur $\Pi_1 = 1 - |0\rangle_1\langle 0|_1$ à l'état $|\Psi'_s\rangle$, ce qui revient à ne conserver que les termes du développement ci-dessus pour lesquels k (nombre de photons réfléchis) est non nul. La densité de probabilité pour une mesure de quadrature $\Pr_{\text{cond}}(x)$ doit enfin tenir compte de la cohérence quantique entre les états pour lesquels le nombre de photons réfléchis est le même, ce qui est une opération de trace partielle sur les états de même paramètre k :

$$\Pr_{\text{cond}}(x) = \sum_{k=1}^{2N} \left| \sum_{m=\lceil k/2 \rceil}^{N} \alpha_{2m} \sqrt{C_{2m}^k}\, \sqrt{R}^{\,k}\, \sqrt{T}^{\,2m-k}\, \psi_{2m-k}(x) \right|^2 \tag{9.10}$$

où $\psi_n(x)$ est la fonction d'onde en quadrature x de l'état de Fock $|n\rangle$ (voir la section 2.3.2).

Nous avons de plus incorporé les effets des inefficacités de la détection homodyne en rajoutant une lame de transmission η_{hom}, qui modifie l'état suivant la formule (2.66) de la section 2.4.1. Les pertes sur la voie réfléchie (vers la photodiode à avalanche) sont également prises en compte comme au chapitre 8 par une efficacité globale de détection η_{apd} (ces pertes n'affectent pas directement l'état transmis, mais modifient la répartition des événements où deux photons sont détectés sur la voie APD et aucun sur la voie homodyne). Enfin, le bruit électronique de la détection homodyne peut se modéliser par une convolution de la densité de probabilité théorique par une gaussienne de largeur égale au bruit électronique normalisé au bruit de photon. Ces effets sont simples à prendre en compte dans le calcul, mais leur écriture est lourde et ne sera donc pas présentée ici.

La figure 9.3 présente les résultats de ce modèle pour différentes valeurs de la réflectivité R et dans le cas d'une détection parfaite. Dans le cas où $R \to 0$, la densité de probabilité en quadrature tend effectivement à s'annuler à l'origine, ce qui lui confère une allure fortement non-gaussienne. On peut de plus remarquer que cet aspect est relativement robuste vis-à-vis des pertes pour la quadrature amplifiée, comme le montre la figure 9.4 [2].

Remarques :

Notre procédure de dégaussification peut être comparée à l'expérience de mesure homodyne d'un photon unique présentée dans la référence [30], où les auteurs exploitent une paire de photons paramétriques. Un des photons est dirigé vers une photodiode à avalanche qui sert à déclencher la détection homodyne de l'autre photon. Idéalement, cette expérience mesure la densité de probabilité en quadrature d'un photon unique. Si cette expérience présente certaines analogies avec notre dispositif, ses données homodynes conditionnées sont indépendantes de la phase, alors que nos prédictions (figure 9.3) et nos mesures (figure 9.7) mettent en évidence des statistiques non-gaussiennes *dépendantes* de la phase. Cet effet ne peut pas s'expliquer simplement par une mesure conditionnée d'un photon unique : elle nécessite la prise en compte de termes d'ordre élevé dans la décomposition du vide comprimé sur la base de Fock (au-delà de

[2] L'effet d'une atténuation par une lame de transmission η_{hom} peut se comprendre comme une convolution de la fonction de Wigner de l'état par la fonction de Wigner (gaussienne) du vide. Ainsi, la quadrature comprimée est la plus sensible aux inefficacités du montage de détection.

la production paramétrique d'une paire de photons). Ces termes jouent ainsi un rôle essentiel dans la modélisation de l'état produit par dégaussification, en induisant une dépendance en phase dans nos mesures. Compte tenu du paramètre de compression r relativement important, notre expérience s'apparente plutôt à la génération conditionnelle d'un photon unique *comprimé*, comme nous le verrons explicitement à la section 9.4.

Par ailleurs, lorsque la réflectivité R de la lame n'est pas très faible devant 1, les termes comportant plus d'un photon réfléchi ne peuvent plus être négligés, tandis que le creux au centre de la distribution de probabilité prend une valeur non-nulle (voir la figure 9.3). Ceci n'est pas une imperfection expérimentale à proprement parler, mais correspond à une caractéristique intrinsèque de l'état conditionné pour des valeurs plus importantes de R : dès que deux photons ont été réfléchis sur la voie APD, la décomposition (9.9) fait intervenir des termes pairs en nombre de photons, qui rajoutent une composante positive à l'origine de l'espace des phases.

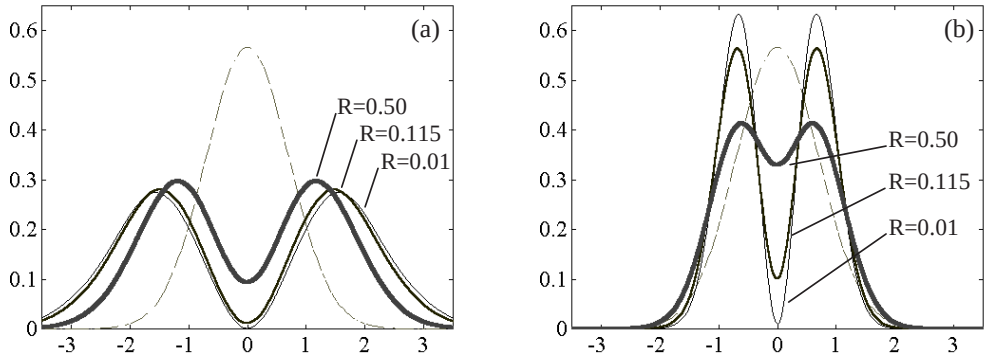

Figure 9.3: *Densité de probabilité théorique des données conditionnées pour la quadrature amplifiée (a) et la quadrature comprimée (b) pour différentes valeur de la réflectivité R de la lame (avec la convention $N_0 = 1/2$). La courbe en tirets indique le mode vide de référence. Le paramètre de compression des fluctuations est $r = 0.43$ et correspond à la valeur expérimentale. La détection est supposée parfaite et monomode : $\eta_{hom} = 1$.*

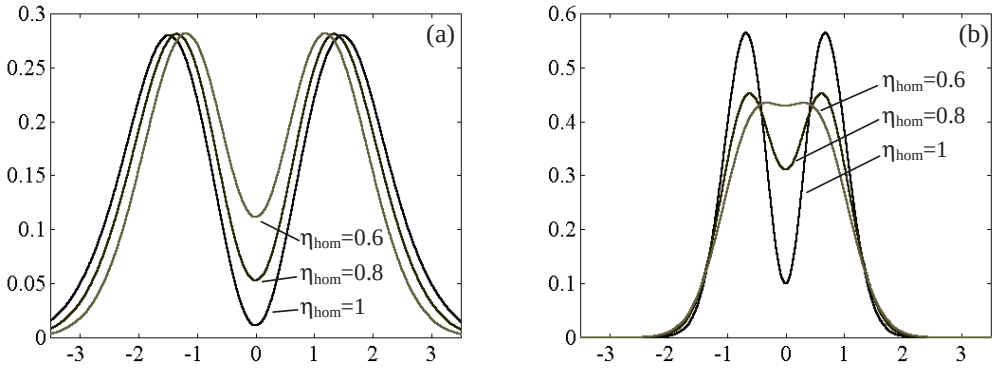

Figure 9.4: *Densité de probabilité théorique des données conditionnées pour la quadrature amplifiée (a) et la quadrature comprimée (b) pour différentes valeur de l'efficacité η_{hom} de la détection homodyne, avec la compression $r = 0.43$, la réflectivité $R = 0.115$ et la convention $N_0 = 1/2$.*

9.2 Dispositif expérimental de conditionnement

La mise en œuvre de notre protocole de dégaussification monomode exploite le montage de génération de vide comprimé impulsionnel présenté au chapitre 7. Grâce aux conversions non-linéaires intenses d'impulsions femtosecondes dans des cristaux minces de $KNbO_3$, des paramètres de compression des fluctuations significatifs ($\backsimeq 3$ dB) peuvent être obtenus. Une faible fraction ($R = 11.5\%$) du faisceau vide comprimé est alors prélevée par une lame pour être dirigée vers des filtres spatiaux et spectraux, avant d'être détectée par une photodiode à avalanche en mode de comptage de photon (figure 9.5). Le reste du faisceau comprimé est quant à lui mesuré par le système de détection homodyne impulsionnelle (résolue en temps) présentée au chapitre 3. Les histogrammes expérimentaux et les distributions de probabilités normalisées présentés dans ce chapitre sont directement obtenus à partir des mesures de quadratures pour chaque impulsion incidente.

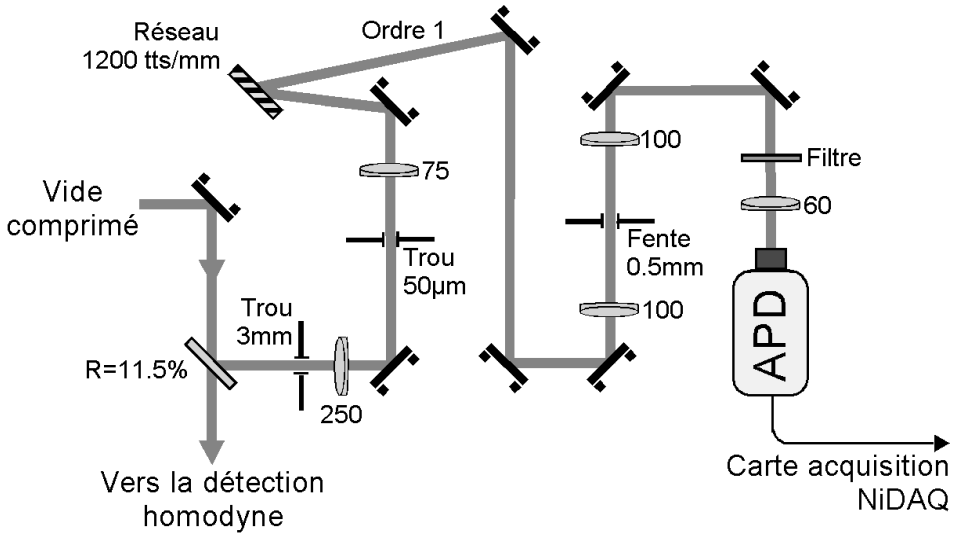

Figure 9.5: *Dispositif expérimental pour le conditionnement : lame partiellement réfléchissante, filtres et photodiode à avalanche. Les focales des optiques sont données en millimètres. Le reste du montage de génération et de caractérisation d'états non-gaussiens est présenté sur la figure 7.1. Le trajet du faisceau lumineux permet de positionner de nombreux caches et tubes afin d'éviter toute lumière parasite incidente sur la photodiode.*

9.2.1 Montage optique

Le premier choix crucial pour la qualité des données observées est la valeur du coefficient de réflexion R de la lame. D'après l'étude théorique de la figure 9.3, plus ce facteur est faible et plus le creux dans la distribution est marqué. Mais un faible R signifie également un faible nombre d'événements de photodétection par seconde, donc un temps d'acquisition plus long et une influence plus marquée des dérives expérimentales. Le choix du coefficient R répond donc à un compromis entre une valeur suffisamment faible pour obtenir un effet notable dans la distribution de probabilité mesurée, et une valeur suffisamment élevée pour acquérir un nombre conséquent de points en un temps raisonnable et minimiser l'influence des coups d'obscurité de la photodiode à avalanche. Nous avons retenu $R = 11.5\%$ qui présente un effet théorique net

(voir la figure 9.3). Ce paramètre fournit avec $r = 0.43$ et $\eta_{\text{apd}} \approx 1.4\%$ un taux de comptage attendu $\eta_{\text{apd}}\, R\, \sinh^2 r\, \text{C} \approx 250$ coups/s pour une cadence C = 780 kHz, ce qui est confortable par rapport aux coups d'obscurité de 8/s mesurés après échantillonnage temporel par la carte d'acquisition à 780 kHz (le taux de comptage moyen mesuré corrigé des coups d'obscurité est de 280 coups/s).

Un filtrage spatial et spectral est ensuite nécessaire du fait de la très large plage d'émission de fluorescence paramétrique de notre dispositif (largeur spectrale ≈ 150 nm, acceptance angulaire $\approx 10°$). En effet, la photodiode à avalanche – contrairement à la détection homodyne – est sensible à des photons dans tous les modes spatio-temporels incidents, et pas seulement dans le mode vide comprimé qui nous intéresse.

Le filtrage spatial s'effectue par deux trous placés dans des plans conjugués, transformés de Fourier l'un de l'autre par une lentille de focale 250 mm. Les diamètres des trous (respectivement 3 mm et 50 μm) ont été optimisés suivant un calcul numérique pour fournir la meilleure transmission du mode TEM_{00}, tout en assurant un filtrage efficace des modes TEM_{01} ou TEM_{10}, ce qui permet d'obtenir une transmission de 17% de la sonde (référence du mode TEM_{00}) pour une transmission estimée inférieure à 0.5% des modes parasites (la transmission des modes d'ordre supérieur est alors totalement négligeable).

Le filtrage spectral est simplement obtenu par un réseau de diffraction et une fente réglable permettant de sélectionner une plage de largeur 3 nm centrée sur la longueur d'onde du laser. Un deuxième filtre (verre teinté) permet de supprimer toute trace de la pompe bleue qui subsisterait suite à un recouvrement de spectre lors de la diffraction par le réseau. Le tableau ci-dessous présente différentes caractéristiques techniques des éléments utilisés pour le filtrage.

Données techniques pour le montage de conditionnement	
Lame	Coefficient de réflexion en intensité $R = 11.5\%$, transmission $T = 88.5\%$
Filtrage spatial	Ensemble de deux trous dans des espaces conjugués. Trou 1 : diamètre 3mm, transmission 58%; Trou 2 : diamètre 50μm, transmission 30%; Transmission totale sonde (TEM_{00}) 17%, transmission estimée mode TEM_{01} $\approx 0.5\%$
Filtrage spectral	Réseau *Jobin-Yvon* 1200 traits/mm, dispersion angulaire 1.4mrad/nm, focalisation 100mm, dispersion au plan focal 7nm/mm, fente largeur 0.5mm soit $\approx$ 3nm centré à 846nm. Efficacité réseau 37%, transmission fente 53%, filtre coloré anti-repliement de spectre transmission 92% (850nm), transmission totale filtre spectral 3nm 17%
Photodiode à avalanche	*PerkinElmer* (EG&G) SPCM-AQR-13, efficacité quantique $\approx$ 50% à 850nm, diamètre 175μm, coups d'obscurité intrinsèque 200/s, coups d'obscurité effectif montage 8/s, temps mort 50ns, probabilité afterpulse $<$0.3% ($<$0.01% à 800kHz), sortie TTL largeur 30ns, polarisation 5V.
Efficacité totale	$\eta_{\text{apd}} = 0.17{*}0.17{*}0.50 \approx 1.4\%$ estimée d'après le faisceau sonde.

9.2.2 Acquisition numérique

La carte numérique *National Instruments* PCI-6111E permet une acquisition simultanée des signaux de la détection homodyne et de la photodiode à avalanche. Les clics de photodétection sont ensuite utilisés pour post-sélectionner les mesures homodynes, ce qui fournit nos statistiques non-gaussiennes grâce à certaines précautions expérimentales détaillées dans cette section.

Une ligne à retard électronique permet la synchronisation entre l'acquisition de la carte et le front avant du signal issu de la photodiode à avalanche lorsqu'une impulsion lumineuse est présente. Cette synchronisation a été réglée grâce à un faisceau sonde très atténué (de l'ordre de 100 photons par impulsion) remplaçant les impulsions du vide comprimé. En utilisant un tel fenêtrage temporel à la cadence exacte des impulsions lumineuses, l'influence des coups d'obscurité de la photodiode à avalanche (alimentée en continu) peut être réduite à moins d'une dizaine de mauvais déclenchements par seconde, alors que le signal est au-dessus de 250 coups/s. Ces coups parasites résiduels tendent néanmoins à dégrader la statistique observée après conditionnement : un faux déclenchement correspond à une mesure du vide comprimé – gaussien – à la détection homodyne, ce qui tend à rajouter une composante gaussienne à la statistique observée (cette influence sera discutée plus en détails à la section 9.3.2).

Pour garantir la mesure homodyne de la même composante de quadrature et compenser les inévitables fluctuations lentes de la phase relative entre le signal et l'oscillateur local, un asservissement numérique voisin de celui utilisé lors de l'expérience de cryptographie quantique est mis en œuvre. Le principe retenu est d'effectuer de manière itérative des mesures homodynes par blocs de 15 000 points et d'ajuster pas à pas la phase de l'oscillateur local par la commande d'une cale piezo-électrique en maximisant la variance calculée pour les mesures homodynes. La procédure est stoppée lorsque la variance mesurée est proche de la variance de consigne plus ou moins un seuil fixé par l'utilisateur. Ceci permet de repérer efficacement la direction de la quadrature amplifiée. Une dizaine d'itérations suffit en pratique pour garantir une précision de l'asservissement à quelques pourcents. Connaissant la calibration de la cale piezo-électrique, il est alors possible d'imposer une phase relative arbitraire en appliquant une tension déterminée à la cale. Les mesures sont alors stables à quelques pourcents pendant une durée de 0.4s, ce qui permet de traiter une acquisition de plus de 300 000 impulsions avant de relancer le programme d'asservissement.

La valeur moyenne de la tension homodyne devrait en théorie toujours être centrée sur zéro, mais des fluctuations lentes de l'équilibrage des voies de la détection homodyne fait légèrement dévier cette tension moyenne de ± 3 mV autour de zéro. L'échelle de temps de ces fluctuations est de l'ordre de la minute. Comme nos mesures des fluctuations en quadratures du vide comprimé présentées au chapitre 7 s'effectuent sur 50 000 impulsions (soit une durée de 62 ms), ce bruit sur l'équilibrage n'affecte pas nos mesures. Par contre, pour les données conditionnées où le nombre de coups par seconde est faible ($\approx$ 300 cps/s), les fluctuations sur l'équilibrage devient non-négligeable. Les déviations induites sont malheureusement suffisantes pour altérer l'allure non-gaussienne des statistiques mesurées. Notre hypothèse est que les fluctuations de l'équilibrage proviennent essentiellement d'un bruit (d'origine mécanique) dans la direction de pointé du faisceau oscillateur local, ce qui se traduit par une légère différence de la réponse de chaque photodiode. Pour compenser ce défaut d'équilibrage, un traitement numérique après acquisition (lors du conditionnement des données) permet de soustraire à la tension sélectionnée la valeur moyenne *locale* de la tension homodyne, prise dans un ensemble de ± 7500 points autour du point conditionné. Cette procédure permet de garantir une valeur moyenne nulle dont les écarts n'excèdent pas 0.5 mV, alors que l'écart-type du bruit quantique standard est de 7 mV.

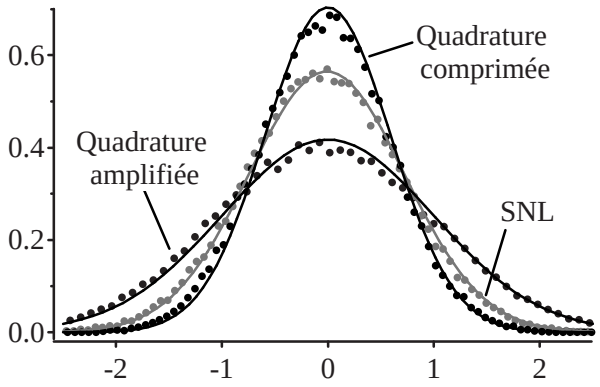

Figure 9.6: *Distributions de probabilité normalisées pour les données non-conditionnées issues de la détection homodyne impulsionnelle (avec la normalisation $N_0 = 1/2$). La variance de la quadrature comprimée est 1.75 dB sous le niveau de bruit quantique standard (SNL, correspondant à la mesure du mode signal vide), tandis que la variance de la quadrature amplifiée excède le SNL de 3.1 dB. Les courbes en traits pleins sont une modélisation monomode avec $r = 0.43$, $R = 0.115$ et $\eta_{hom} = 0.75$.*

9.3 Caractérisation d'états non-gaussiens

9.3.1 Distributions de probabilité en quadrature

Le dispositif expérimental décrit précédemment permet d'obtenir la répartition statistique des données (conditionnées ou non) pour une quadrature particulière. La figure 9.6 présente les distributions de probabilité normalisées pour les données non-conditionnées (gaussiennes) correspondant à la quadrature amplifiée et la quadrature comprimée. Les données brutes, sans correction des pertes ou des inefficacités, fournissent une variance de la quadrature comprimée de $0.67\,N_0$ (-1.75 dB), alors que la variance de la quadrature amplifiée est de $2.04\,N_0$ (+3.1 dB). Ces valeurs correspondent sensiblement aux prévisions théoriques de $0.67\,N_0$ et $2.06\,N_0$, obtenues à partir des gains paramétriques classiques (0.50 et 2.60 mesurés par un faisceau sonde) et de l'efficacité de détection totale $\eta_{hom}(1-R) = 0.66$. Cette valeur tient compte de l'efficacité intrinsèque de la détection homodyne $\eta_{hom} = 0.75$ (voir la discussion à la section 9.3.2) et de la transmission $1 - R = 0.885$ de la lame.

Comme nous l'avons déjà remarqué et discuté au cours des chapitres 7 et 8, les gains d'amplification et de déamplification ne sont pas inverses l'un de l'autre, essentiellement à cause de la diffraction induite par le gain qui déforme le front d'onde déamplifié aux fortes puissances de pompe (voir la discussion et les références à la section 7.2.3). Cette différence de gains signifie dans un premier temps que l'état vide comprimé n'est pas à proprement parler un état pur. On pourrait alors être tenté d'appliquer le modèle général de l'amplificateur paramétrique *monomode* introduit à la section 8.2.1. Si ce modèle offre une représentation correcte pour des puissances de pompe modérées, il n'est plus très satisfaisant aux fortes puissances utilisées pour la dégaussification : les valeurs de variances en quadrature prédites sont en désaccord net avec les valeurs mesurées. La physique de notre expérience se situe alors dans un régime fondamentalement multimode, tandis qu'un modèle détaillé des effets mesurés devrait prendre en compte ces aspects multimodes. L'étude de tels effets sort cependant du cadre que nous avons fixé pour notre expérience, à savoir la mise en place de procédés impulsionnels simples de manipulation

de l'information quantique.

Pour représenter nos résultats, nous avons donc choisi d'utiliser le modèle *monomode* présenté au début de ce chapitre, en utilisant le paramètre de compression des fluctuations r qui modélise au mieux les distributions en quadrature mesurées, suivant un gain monomode $\exp(\pm 2r)$ et une efficacité totale $\eta_{hom}(1-R)$. L'interpolation des données homodynes fournit $r = 0.43$, ce qui permet une modélisation assez satisfaisante des mesures d'après les courbes de la figure 9.6. Comme les effets multimodes demeurent ainsi raisonnablement faibles dans nos conditions expérimentales, nous utiliserons par la suite cet unique paramètre monomode r pour décrire l'amplification *et* la déamplification.

La figure 9.7 montre les distributions des données post-sélectionnées par la procédure de dégaussification, faisant apparaître un creux net au centre de la distribution correspondant à la quadrature amplifiée. L'état généré est clairement non-gaussien et présente une forte dépendance en phase des quadratures. Comme nous l'avons vu à la section 9.1, cet effet ne peut s'expliquer que par une prise en considération des termes d'ordres supérieurs dans la génération de photons, au-delà de la production d'une paire paramétrique. La dépendance des statistiques par rapport à la phase de l'oscillateur local est donc reliée aux fortes valeurs de compression des fluctuations quantiques observées. Les courbes théoriques en traits pleins présentées sur la figure 9.7 proviennent du modèle monomode simple introduit à la section 9.1.2, et sont en bon accord avec les données expérimentales. Ce calcul théorique prend en compte le gain paramétrique monomode r obtenu à partir des mesures de réduction du bruit quantique ainsi que diverses sources d'imperfections expérimentales (pertes optiques, mauvaise adaptation de modes, bruit électronique, coups d'obscurité et pureté modale imparfaite), que nous détaillons à la section suivante.

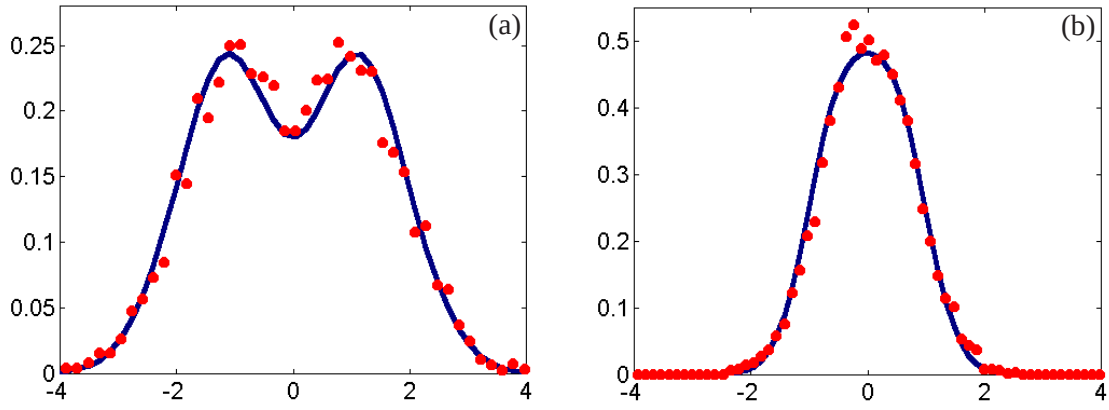

Figure 9.7: *Distributions de probabilité normalisées ($N_0 = 1/2$) pour les données conditionnées correspondant à la quadrature amplifiée (a) et à la quadrature comprimée (b). Les points sont nos données expérimentales tandis que les courbes correspondent au modèle de calcul présenté avec $r = 0.43$, $R = 0.115$, $\eta_{hom} = 0.75$ et $\xi = 0.7$.*

9.3.2 Influence des imperfections expérimentales

Pour caractériser les imperfections expérimentales, il faut remarquer que la détection homodyne et la photodiode à avalanche possèdent des comportements très différents. La détection homodyne n'est sensible qu'au mode incident défini par le mode de l'oscillateur local, tandis que

des photons dans d'autres modes ne seront pas détectés. Inversement, la photodiode à avalanche n'est pas sensible à des modes vides, mais détecte des photons dans n'importe quel mode incident. En conséquence, deux paramètres devront être utilisés pour représenter les différentes imperfections : un paramètre d'*efficacité homodyne* η_{hom} qui mesure l'adaptation entre le mode signal utile et le mode détecté [36, 111], et un paramètre de *pureté modale* ξ qui caractérise la fraction des événements de photodétection qui correspondent au mode signal (vide comprimé) souhaité [38].

Dans une approche simple, l'efficacité homodyne limitée pourra être représentée par une lame de transmission η_{hom} placée en amont de la détection homodyne comme au chapitre 3, ce qui a pour effet d'introduire une composante dans un mode vide (voir la figure 9.8). Par contre, la pureté modale ξ ne peut pas se modéliser par une autre lame partiellement réfléchissante, car une mauvaise pureté modale correspond à de faux déclenchements de la photodiode à avalanche pour lesquels le vide comprimé est toujours mesuré à la détection homodyne. Une faible valeur de ξ traduit en fait une mauvaise opération de post-sélection des données homodynes, reliée physiquement à un filtrage modal imparfait en amont de la photodiode à avalanche. Pour décrire la distribution de probabilité mesurée après post-sélection $\mathrm{Pr}_{\mathrm{ps}}$, nous utilisons donc le modèle suivant :

$$\mathrm{Pr}_{\mathrm{ps}} = \xi \, \mathrm{Pr}_{\mathrm{cond}} + (1 - \xi) \, \mathrm{Pr}_{\mathrm{non-cond}} \tag{9.11}$$

où $\mathrm{Pr}_{\mathrm{cond}}$ est la distribution de probabilité conditionnée réelle et $\mathrm{Pr}_{\mathrm{non-cond}}$ la distribution des données non-conditionnées (i.e. correspondant au vide comprimé gaussien). Ces deux quantités dépendent des valeurs de r, η_{hom} et R.

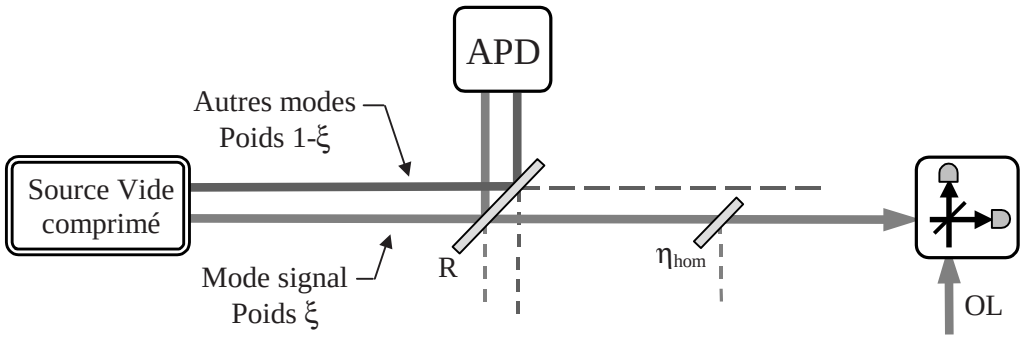

Figure 9.8: *Modèle des imperfections expérimentales : efficacité homodyne η_{hom} et pureté modale ξ. La photodiode à avalanche déclenche sur un photon dans n'importe quel mode incident, tandis que la détection homodyne n'est sensible qu'au mode incident (couplé au vide) adapté à l'oscillateur local.*

On peut alors facilement déterminer les valeurs de η_{hom} et ξ qui font correspondre notre modèle aux données mesurées. La procédure pour déterminer l'efficacité de la détection homodyne η_{hom} est la même que celle employée pour des expériences de compression des fluctuations quantiques [106, 111], et peut être vérifiée en comparant les gains paramétriques classiques mesurés avec le niveau de réduction expérimental de bruit quantique. Comme dans l'expérience du chapitre 7, l'efficacité globale de la détection homodyne s'exprime par $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2 = 0.75$ où la transmission optique $\eta_{opt} = 0.94$, l'efficacité quantique des photodiodes $\eta_{phot} = 0.945$ et l'adaptation des modes $\eta_{mod} = 0.92$ sont mesurées indépendamment.

La procédure pour déterminer ξ est moins habituelle, et revient à déterminer la quantité de photons parasites qui passent au travers des différents filtres et induisent de faux déclenchements

de la photodiode à avalanche. Les coups d'obscurité sont en partie responsables d'une mauvaise pureté ξ : le nombre moyen de coups d'obscurité est de 8/s à comparer à un taux de comptage total de 290/s, soit un paramètre de pureté uniquement dû aux coups d'obscurité de $(290 - 8)/290 \approx 0.97$. Une évaluation simple de la pureté totale ξ s'obtient en comparant le taux de comptage total effectivement mesuré au taux de comptage attendu compte tenu de la compression mesurée des fluctuations r et des conditions expérimentales R et η_{apd}. Malheureusement, en l'absence de mesure précise de la transmission effective η_{apd} des filtres de la voie APD pour le vide comprimé (voir la discussion à la section 8.3.3), nous ne pouvons donner qu'une estimation grossière $0.6 < \xi < 0.8$. La compression des fluctuations r étant indépendamment déterminée par les mesures homodynes non-conditionnées, l'estimation du paramètre ξ est directement faite en interpolant les données de la figure 9.7 suivant le modèle de l'équation (9.11). On obtient alors $\xi = 0.7$, en bon accord avec les estimations issues des taux de comptage.

9.3.3 Tomographie quantique de l'état non-gaussien

Pour caractériser complètement l'état produit par dégaussification, nous avons mis en œuvre une procédure standard de reconstruction de la fonction de Wigner associée à l'état par tomographie quantique [17, 18, 29]. Deux méthodes numériques de reconstruction ont été utilisées : la technique par transformée de Radon inverse, présentée au chapitre 7, et une technique itérative de maximum de vraisemblance [32], dont nous indiquons ici le principe. La technique par maximum de vraisemblance présente l'intérêt d'être moins sensible aux bruits expérimentaux que la transformée de Radon. De plus, cette méthode permet de corriger les effets des inefficacités de mesure. Cependant, elle nécessite de limiter a priori la dimension de la matrice densité et le nombre maximum de photons présents dans l'état mesuré. Suivant une approche différente, la méthode par transformée de Radon inverse permet de présenter l'état effectivement déduit des mesures, sans hypothèse a priori sur la forme de l'état (hormis une troncature numérique simple pour garantir la convergence du calcul, voir la section 7.3.2).

Dans un premier temps, nous présentons les résultats de nos mesures et leur utilisation directe dans une procédure par transformée de Radon inverse. Ces résultats sont ensuite discutés avant d'introduire la méthode par maximum de vraisemblance pour corriger les inefficacités de la détection homodyne.

Mise en œuvre expérimentale et résultats des mesures

Nous avons mis en place une procédure automatisée pour acquérir les statistiques homodynes conditionnées pour 6 références de phase, réparties entre 0 et $5\pi/6$, comme pour l'expérience de tomographie du vide comprimé décrite au chapitre 7. Pour éviter des dérives expérimentales, l'acquisition traite des blocs de 200 000 impulsions correspondant à une phase particulière avant de lancer la procédure d'asservissement et de recalage de phase décrite à la section 9.2.2. Chaque bloc numéro j de 200 000 impulsions est fixé à une phase $j\pi/6 \mod(6)$, de sorte à traiter alternativement au cours du temps les différentes phases de référence. Pour acquérir suffisamment de données conditionnées, la procédure est répétée pour 480 acquisitions de 200 000 impulsions, en une durée totale de 3 heures (toutes les 20 minutes, une recalibration manuelle est effectuée : gain paramétrique classique, adaptation des modes, filtrage spatial, équilibrage de la détection homodyne...). Il en résulte environ 5000 points conditionnés pour chacune des 6 références de phase, ce qui permet de construire les histogrammes sur 40 canaux présentés sur la figure 9.7 et 9.9.

La fonction de Wigner de l'état conditionné, présentée sur la figure 9.10, est reconstrui-

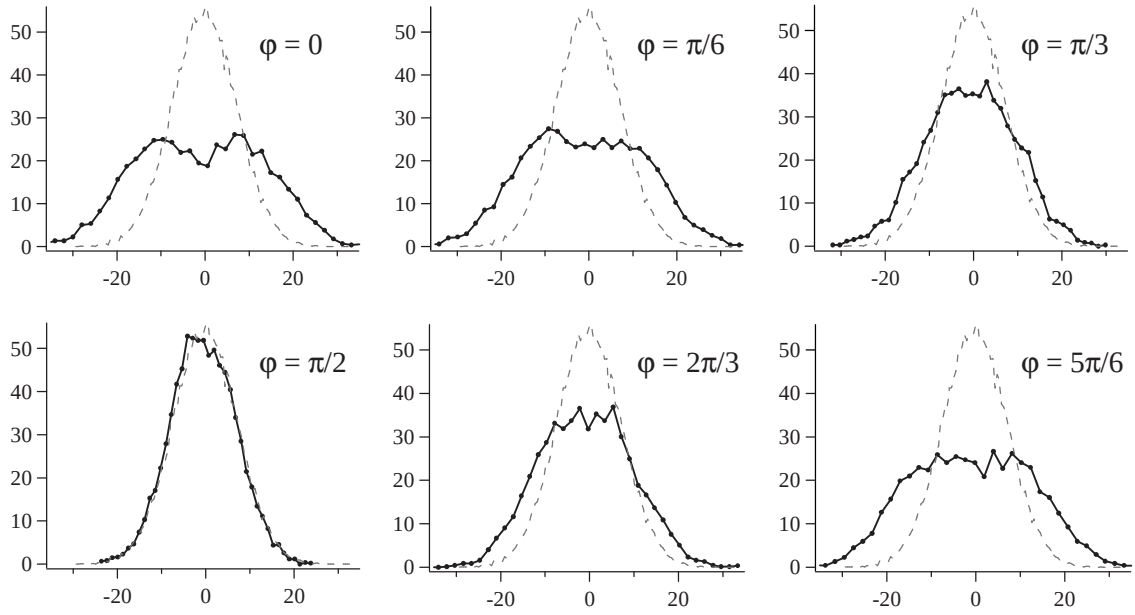

Figure 9.9: *Histogrammes des données homodynes brutes conditionnées utilisées pour la reconstruction de la fonction de Wigner associée à l'état dégaussifié. Chaque histogramme est issu d'un ensemble de 5000 points répartis en 40 canaux. L'histogramme gaussien en gris correspond à la référence du bruit quantique standard.*

te à partir de la transformation de Radon inverse appliquée aux distributions de probabilité symétrisées $[\Pr(x,\theta) + \Pr(-x,\theta)]/2$, sans aucune correction de l'efficacité limitée η_{hom} de la détection homodyne (l'algorithme de reconstruction par maximum de vraisemblance donne un résultat sensiblement identique). Comme pour la tomographie du vide comprimé, l'utilisation des distributions de probabilité symétrisées permet d'éviter des déformations de la fonction de Wigner, qui seraient dues à un bruit statistique dans chaque canal des histogrammes de mesure.

La fonction de Wigner reconstruite expérimentalement présente un creux net à l'origine de l'espace des phases $W_{\exp}(0,0) = 0.067$ alors que le maximum est à 0.12 (des vues en coupe sont présentées sur la figure 9.12). La fonction de Wigner théorique de l'état pour notre degré de compression $r = 0.43$ et notre valeur de réflectivité $R = 0.115$ est également présentée sur la figure 9.10, dans le cas d'une détection homodyne parfaite et monomode $\eta_{hom} = \xi = 1$. La valeur théorique à l'origine est clairement négative $W_{\text{th}}(0,0) = -0.26$ (figure 9.11), ce qui atteste de l'aspect spécifiquement quantique de l'état préparé par la procédure (idéale) de dégaussification.

Comment observer une fonction de Wigner négative ?

Comme dans l'expérience de tomographie de photons uniques à l'université de Constance [30, 34], les conditions pour observer des valeurs négatives de la fonction de Wigner sont très délicates à remplir expérimentalement. Dans le cas de la dégaussification du vide comprimé monomode, la négativité de la fonction de Wigner est liée à la présence d'un méplat sur la distribution de probabilité des mesures pour la quadrature comprimée (indépendamment des autres paramètres expérimentaux). Nous n'avons pas démontré rigoureusement ce résultat, mais il ressort clairement de nos diverses simulations numériques en faisant varier tous les paramètres expérimentaux.

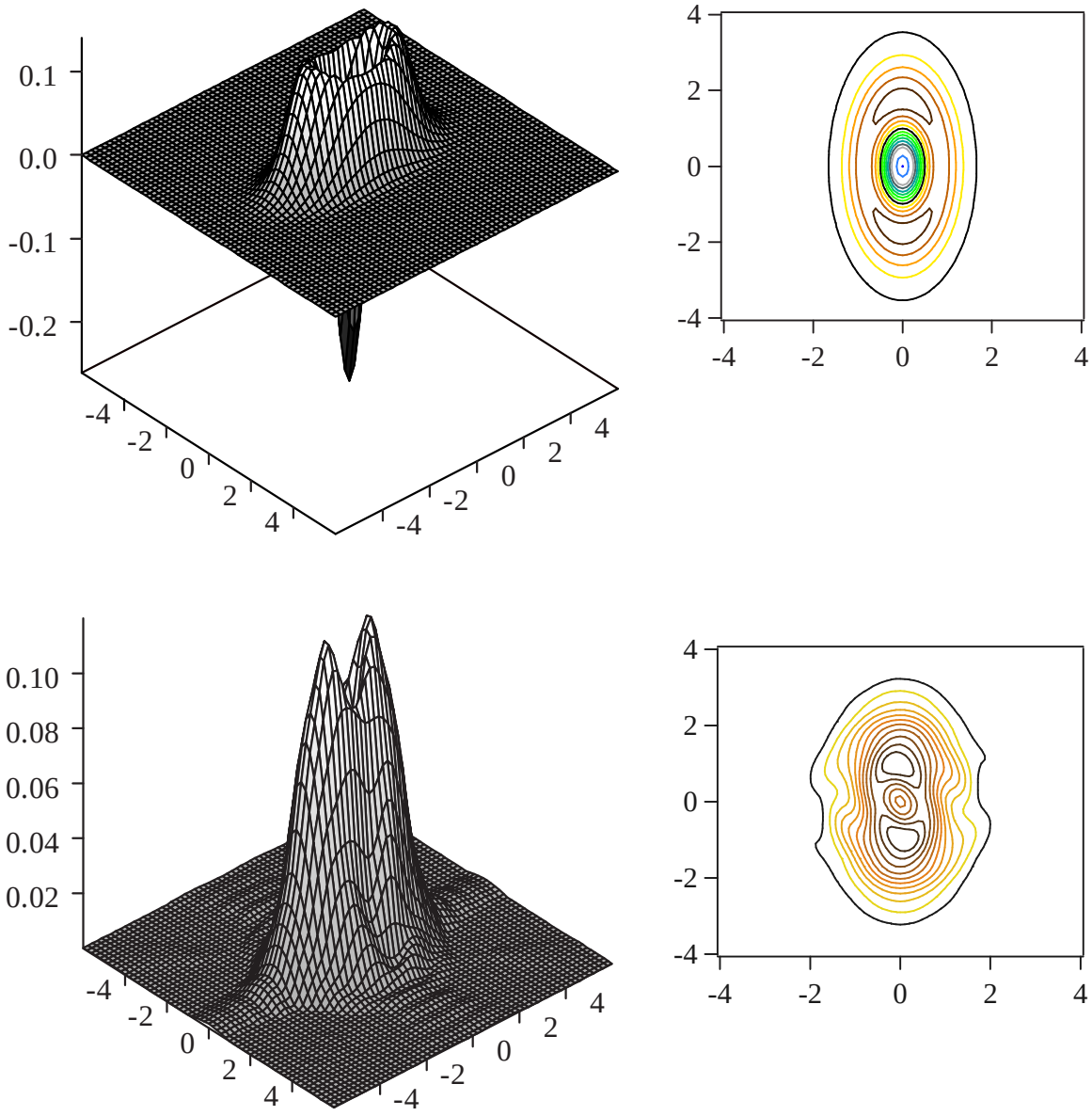

Figure 9.10: *(Haut) Fonction de Wigner théorique de l'état produit par la procédure de dégaussification, avec* $r = 0.43$, $R = 0.115$ *et en supposant une détection monomode parfaite* ($\eta_{hom} = \xi = 1$). *La convention pour la définition des quadratures est* $N_0 = 1/2$. *Les courbes de niveaux correspondantes (droite) sont équidistantes de 0.03. (Bas) Fonction de Wigner expérimentale des données non-corrigées* ($\eta_{hom} = 0.75$, $\xi = 0.7$). *Cette fonction est reconstruite par transformée de Radon inverse. L'équidistance entre les courbes de niveaux est de 0.01. Les fonctions de Wigner représentées prennent les valeurs à l'origine :* $W_{\rm th}(0,0) = -0.26$ *et* $W_{\rm exp}(0,0) = 0.067$. *La troncature numérique dans le calcul de la transformée de Radon inverse est fixée à* $k_c = 8$.

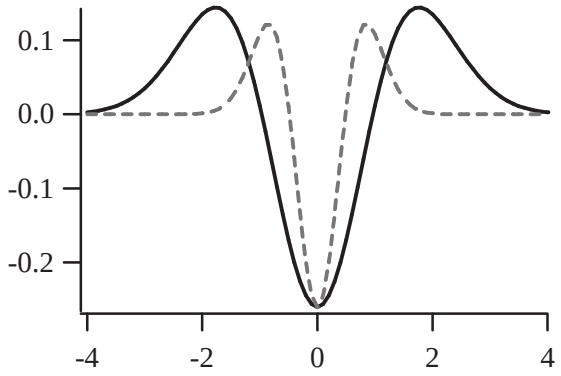

Figure 9.11: *Coupe de la fonction de Wigner théorique de l'état conditionné avec une détection parfaite monomode (présentée figure 9.10) suivant les axes principaux des quadratures.*

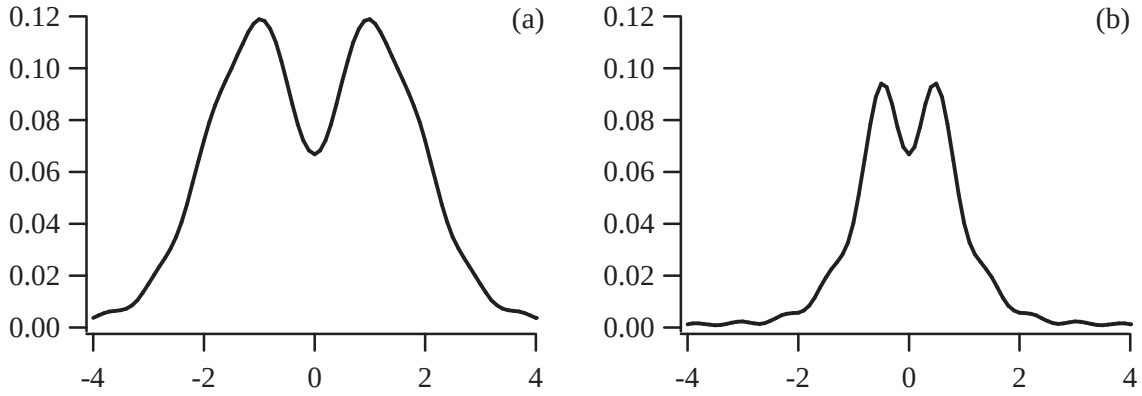

Figure 9.12: *Coupe de la fonction de Wigner reconstruite par transformée de Radon de l'état expérimentalement dégaussifié sans correction des pertes ($\eta_{hom} = 0.75$, $\xi = 0.7$, voir la figure 9.10) suivant la quadrature amplifiée (a) ou comprimée (b).*

Etant données nos conditions $r = 0.43$, $R = 0.115$ et $\eta_{hom} = 0.75$, la pureté modale pour obtenir une fonction de Wigner négative est d'au moins $\xi > 0.85$, ce qui n'est malheureusement pas accessible expérimentalement en conservant un taux de comptage APD au-dessus de quelques dizaines de coups par seconde. Inversement, avec les paramètres $r = 0.43$, $R = 0.115$ et la pureté expérimentale $\xi = 0.7$, la condition de négativité porte sur l'efficacité de la détection homodyne et devient : $\eta_{hom} > 0.85$. Ceci nécessiterait une adaptation de modes de plus de 98%, qui semble peu réalisable compte tenu du dispositif actuel. En modifiant l'ensemble des paramètres expérimentaux (baisse du degré de compression r et de la réflectivité de la lame R, amélioration du filtrage APD, de l'adaptation des modes et de la stabilisation du montage), il devrait être possible de mesurer expérimentalement une fonction de Wigner négative. La borne minimale des paramètres tolérables est fixée par le taux d'événements de photodétection par seconde, qui doit être assez grand pour éliminer les effets des diverses fluctuations et dérives, et coups d'obscurité parasites.

Reconstruction numérique de la fonction de Wigner par maximum de vraisemblance

Avec les paramètres $r = 0.43$, $R = 0.115$, $\xi = 0.7$ et une détection homodyne parfaite ($\eta_{hom} = 1$), la fonction de Wigner théorique de l'état préparé après la lame prend une valeur négative à l'origine, $W_{\mathrm{th,corr}}(0,0) \approx -0.06$. Notre expérience de conditionnement génèrerait donc un état en amont de la détection homodyne avec une fonction de Wigner négative, mais l'efficacité limitée de la détection ne permettrait pas d'observer cette particularité. Pour vérifier expérimentalement ce résultat à partir de nos mesures, nous avons mis en œuvre une procédure de reconstruction de la fonction de Wigner par maximum de vraisemblance, qui permet de corriger virtuellement l'effet de l'efficacité limitée de la détection homodyne, tant que les pertes ne sont pas trop importantes ($\eta_{hom} > 50\%$, ce qui est le cas ici) [32, 29].

Le principe général de la méthode de maximum de vraisemblance, introduite au chapitre 8, est de fournir les paramètres les plus à même de décrire les différentes mesures réalisées. Dans le cadre de la tomographie quantique, cette technique s'applique en cherchant parmi tous les états physiques possibles la matrice densité qui maximise la probabilité d'obtenir les données mesurées expérimentalement. La référence [32] présente une procédure itérative particulièrement simple pour appliquer une reconstruction par maximum de vraisemblance qui sera mise en œuvre ici. La fonction de vraisemblance $\mathcal{L}$ de la matrice densité ρ s'écrit :

$$\mathcal{L}(\rho) = \prod_{j=1}^{N} \mathrm{Pr}_j{}^{f_j} \tag{9.12}$$

où N indique le nombre de mesures, f_j est la nombre d'occurrences expérimentales du résultat j, et Pr_j désigne la probabilité d'obtenir théoriquement le résultat j pour l'état ρ. On peut alors obtenir la matrice densité ρ en maximisant la fonction de vraisemblance $\mathcal{L}$ à partir des données expérimentales f_j.

Pour trouver la meilleure matrice densité ρ, Lvovsky introduit l'opérateur suivant [32, 31] :

$$\hat{R}(\rho) = \sum_j \frac{f_j}{\mathrm{Pr}_j} \hat{\Pi}_j \tag{9.13}$$

où $\hat{\Pi}_j$ désigne l'opérateur projection sur le résultat j. Notons qu'alors on peut écrire $\mathrm{Pr}_j = \mathrm{Tr}(\hat{\Pi}_j \rho)$. La clé de l'algorithme [31, 32] est d'observer que pour la matrice densité ρ_0 qui maximise la fonction de vraisemblance (9.12), f_j est proportionnel à Pr_j et alors $\hat{R}(\rho_0) \propto \hat{1}$. ρ_0 est donc stable sous l'action de $\hat{R}$:

$$\hat{R}(\rho_0)\, \rho_0\, \hat{R}(\rho_0) \propto \rho_0 \tag{9.14}$$

La procédure itérative par maximum de vraisemblance fonctionne alors de la manière suivante : étant donné un choix de départ pour ρ (la matrice identité dans notre cas), l'opérateur $\hat{R}$ est appliqué de manière répétitive :

$$\rho^{(k+1)} = \mathcal{N}\left[\, \hat{R}(\rho^{(k)})\, \rho^{(k)}\, \hat{R}(\rho^{(k)}) \,\right] \tag{9.15}$$

où $\mathcal{N}$ est une normalisation pour obtenir une trace unité. A chaque étape, la vraisemblance de la matrice $\rho^{(k)}$ sera augmentée, alors que cette matrice tend asymptotiquement vers ρ_0. Cette procédure permet donc d'accéder de manière approximative à la matrice densité ρ_0 qui maximise la fonction de vraisemblance. Il est ensuite possible de calculer la fonction de Wigner correspondant à cette matrice densité en appliquant l'algorithme décrit à la section 5.2.6 de la référence [17].

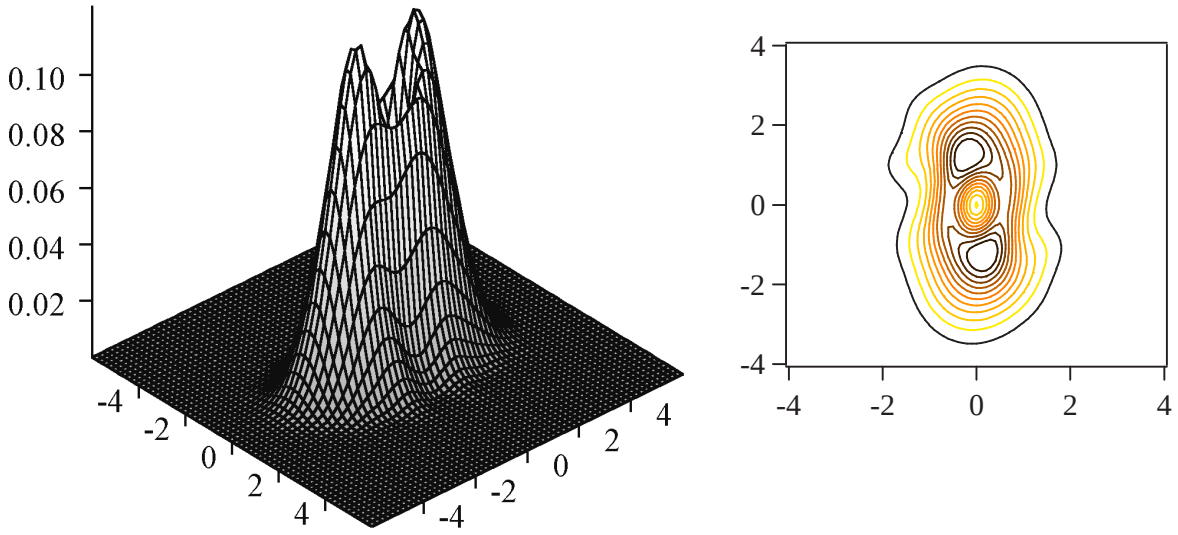

Figure 9.13: *Fonction de Wigner reconstruite par maximum de vraisemblance après correction des pertes de la détection homodyne ($\eta_{hom} = 0.75$) et du bruit électronique ($0.08\,N_0$). Cette fonction prend la valeur à l'origine $W_{\mathrm{exp,corr}}(0,0) \approx +0.01$. L'équidistance entre les courbes de niveaux (à droite) est de 0.01 .*

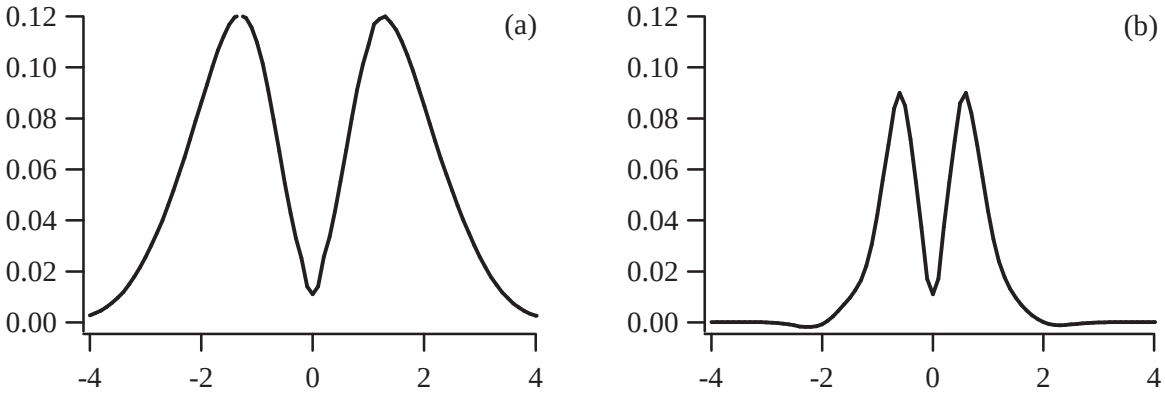

Figure 9.14: *Coupe de la fonction de Wigner reconstruite par maximum de vraisemblance avec correction des pertes de la détection homodyne et du bruit électronique (correspondant à la figure 9.13). (a) indique une coupe suivant la quadrature amplifiée tandis que (b) correspond à la quadrature comprimée.*

Pour modéliser l'action des pertes introduite par la détection homodyne sur une matrice densité arbitraire ρ_{in}, nous utilisons la *transformation de Bernoulli généralisée* [17]. Cette opération fournit la matrice densité réduite sur une sortie de la lame par rapport à la matrice densité entrante (une trace partielle a été effectuée sur l'autre mode de sortie de la lame) :

$$\langle m|\hat{\rho}_{out}|n\rangle = \sum_{k=0}^{\infty} \sqrt{b_n^{n+k}\, b_m^{m+k}}\, \langle m+k|\hat{\rho}_{in}|n+k\rangle \tag{9.16}$$

où b_n^{n+k} est la distribution binomiale :

$$b_n^{n+k} = C_{n+k}^n \, \eta_{hom}^n \, (1-\eta_{hom})^k = \frac{(n+k)!}{n!\,k!} \, \eta_{hom}^n \, (1-\eta_{hom})^k \tag{9.17}$$

Grâce à la procédure itérative et à cette relation pour prendre en compte les pertes, il est possible de corriger les effets des pertes introduites par la détection homodyne sur les données expérimentales. Notre programme de reconstruction numérique a été réalisé en langage C par Rosa Tualle-Brouri sur la base de ces principes. Dans notre mise en œuvre, nous utilisons les données expérimentales présentées sur la figure 9.9 réparties en 40 canaux pour fournir les nombres d'occurrences f_j. 4150 itérations de l'étape (9.15) sont ensuite nécessaires pour faire converger la matrice densité ρ vers l'état qui maximise au mieux la fonction de vraisemblance des données expérimentales.

La fonction de Wigner corrigée des imperfections de la détection homodyne est présentée sur les figures 9.13 et 9.14. Malheureusement, nous ne retrouvons pas le résultat théorique qui prédisait une valeur négative de la fonction de Wigner à l'origine $W_{\mathrm{th,corr}}(0,0) \approx -0.06$, mais nous obtenons la valeur $W_{\mathrm{exp,corr}}(0,0) \approx +0.01$. Des perturbations supplémentaires entachent encore nos données mesurées, comme des fluctuations rapides de phase ou des imprécisions de pointé des phases de référence.

9.4 Applications potentielles

9.4.1 Distillation de l'intrication des variables gaussiennes continues

Comme nous l'avons déjà évoqué au début de ce chapitre, les preuves d'impossibilité de distillation de l'intrication par des opérations gaussiennes [163, 164] nous incitent à considérer la manipulation d'états non-gaussiens. Une procédure prometteuse pour distiller l'intrication d'états gaussiens (de type paire EPR) a été proposée dans [127]. Ce protocole permet de sortir du domaine gaussien, de purifier l'intrication et de revenir enfin (de façon approximative) vers des états gaussiens.

La cellule de base pour cette procédure itérative est présentée sur la figure 9.15. Elle permet de combiner des états intriqués sur des lames semi-réfléchissantes et de mesurer un des ports de sortie de la lame avec une photodiode à avalanche. Suivant l'opération souhaitée, la sélection des états en sortie est conditionnée sur une double photodétection ou une double absence de clics. La

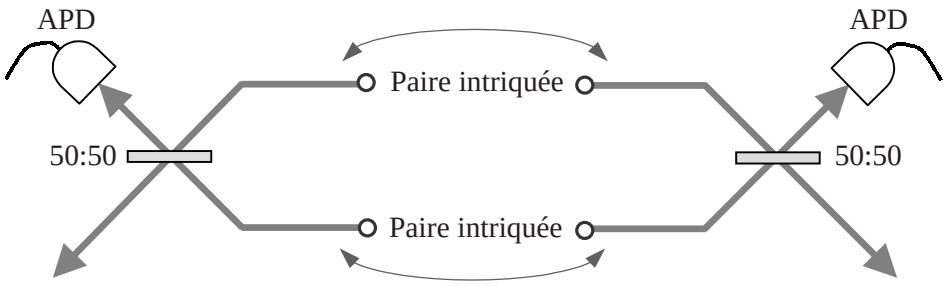

Figure 9.15: *Dispositif élémentaire pour le protocole [127]. Le conditionnement des détecteurs sur deux photodétections simultanées permet la dégaussification. La sélection sur une double absence de clic (pour des états non-gaussiens) permet la distillation et la regaussification.*

présence simultanée de deux événements de détection rend l'état en sortie non-gaussien et constitue la phase préparatoire de projection. Lors d'itérations successives, ces états non-gaussiens sont injectés dans des cellules du type de la figure 9.15. La double absence de photodétection induit alors une distillation de l'intrication et une regaussification de l'état en sortie [127].

Dans ce contexte, notre dégaussification du vide comprimé s'inscrit dans le principe de l'étape préparatoire de ce protocole de distillation de l'intrication pour les variables continues, dont aucune réalisation expérimentale n'a été présentée à ce jour. En particulier, l'étude de nos conditions et imperfections expérimentales s'étend facilement au cas d'une paire intriquée EPR.

9.4.2 Augmentation des ressources en intrication

Une des manières les plus simples de générer de l'intrication en quadratures est d'envoyer un état vide comprimé sur une face d'une lame partiellement réfléchissante, l'autre entrée étant vide. Les deux modes des sorties de la lame présentent alors des corrélations non-locales entre leurs composantes de quadrature, ce qui peut se quantifier en terme d'intrication quantique par l'entropie de Von Neumann [1, 141], définie par $E = -\mathrm{Tr}(\rho_A \log_2 \rho_A)$ où ρ_A désigne la matrice densité réduite pour une des sorties de la lame. Nous avons calculé cette quantité pour mesurer l'intrication produite par une lame parfaitement semi-réfléchisssante pour différents états en entrée :

1. Vide comprimé sur une seule voie (l'autre entrée est vide).

2. Vides comprimés déphasés de $\pi/2$ sur les deux entrées.

3. Etat dégaussifié pur (cas de la section 9.1.1) sur une seule voie (l'autre entrée est vide).

Dans la configuration où des états parfaitement purs sont considérés, l'entropie de Von Neumann est la seule mesure pertinente de l'intrication quantique pour des variables continues. Cette quantité est directement calculée numériquement à partir de la décomposition de Fock des états et de la formule (9.16) de l'action d'une lame réfléchissante. Les résultats des calculs d'entropie sont présentés sur la figure 9.16. Il apparaît clairement que pour de faibles valeurs de paramètres de compression r, l'état conditionné produit une intrication de l'ordre de 1 ebit, qui est nettement supérieure à l'intrication produite par un ou même deux vides comprimés [3]. Cet effet peut facilement se comprendre à la limite où $r \to 0$: les faisceaux comprimés sont globalement dans un état vide $|0,0\rangle$ qui n'offre aucune intrication en sortie de lame alors que l'état conditionné s'apparente à un photon unique, ce qui fournit l'état de Bell en sortie $(|0,1\rangle + |1,0\rangle)/\sqrt{2}$ contenant une intrication de 1 ebit.

L'amélioration de l'intrication quantique par la procédure de dégaussification est à mettre en parallèle avec l'exploitation en variables discrètes d'une source de photon unique basée sur le conditionnement d'une paire paramétrique de photons [2]. Par ailleurs, l'utilisation de lames faiblement réfléchissantes et de photodiodes à avalanche pour post-sélectionner des événements est connue pour augmenter la fidélité de téléportation quantique pour des variables continues [138, 139, 140]. Cette idée sera l'élément clé pour notre proposition récente de test *faisable* des inégalités de Bell avec des variables continues et des détections homodynes [188].

[3] Ce résultat peut paraître surprenant dans la mesure où l'association de deux vides comprimés déphasés de $\pi/2$ est connue pour maximiser l'intrication EPR [142]. Cependant, cette propriété des états comprimés ne s'applique que dans le cas d'une classe d'états de même énergie fixée, ce qui n'est clairement pas le cas dans notre comparaison.

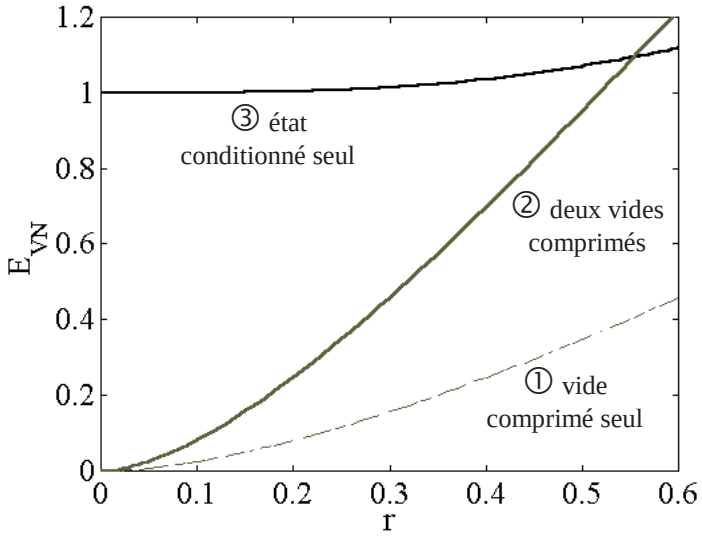

Figure 9.16: *Entropie de Von Neumann en fonction du paramètre de compression r, exprimée en unités d'ebits (les logarithmes sont pris en base 2) pour différents états en entrée d'une lame séparatrice* 50 : 50. *L'entropie de Von Neumann quantifie l'intrication présente entre les deux faisceaux émergents. Pour ce calcul, nous avons pris $R = 0.02$ pour la génération de l'état dégaussifié, afin de pouvoir considérer l'état après conditionnement comme un état pur.*

9.4.3 Génération de chats de Schrödinger

Depuis l'énoncé par Erwin Schrödinger du fameux paradoxe du chat en 1935, de nombreux travaux expérimentaux ont tenté de mettre en évidence une superposition quantique d'états d'un système mésoscopique. Dans le domaine particulier de l'optique quantique, un état "chat de Schrödinger" potentiel est formé d'une superposition de deux états cohérents déphasés de π, dont nous avons abordé certaines propriétés fondamentales à la section 2.3.6. D'une part, ces états sont particulièrement intéressants pour étudier les fondements théoriques de la mécanique quantique. D'autre part, les potentialités intrinsèques des chats de Schrödinger en font des ressources spécifiques pour effectuer certaines tâches de traitement de l'information quantique, comme la correction d'erreurs ou le calcul quantique [130], ce qui leur vaut un intérêt accru au cours de ces dernières années.

La génération et la manipulation d'un chat quantique est une tâche extrêmement délicate compte tenu de la technologie actuelle. S'il est bien connu qu'une interaction non-linéaire de type Kerr peut générer simplement un tel état [202], les nonlinéarités requises dépassent nettement celles disponibles actuellement. Par ailleurs, la nécessité de disposer d'un champ lumineux se *propageant* dans une superposition d'état limite la portée d'expériences de type électrodynamique quantique en cavité [195] pour des applications en communication quantique. Récemment, les études [131, 129] ont montré l'intérêt des mesures conditionnelles (du type de celle que nous avons développé expérimentalement) pour la production de chats quantiques, grâce notamment aux effets quantiques importants créés par l'opération de soustraction de photon.

Dans ce contexte, il est intéressant de considérer l'état produit par dégaussification par rapport à un chat de Schrödinger. Pour choisir le chat particulier que nous souhaitons étudier, une propriété intéressante de la superposition $|\alpha\rangle - |-\alpha\rangle$ est qu'elle ne comporte que des termes *impairs* dans sa décomposition de Fock, ce qui n'est pas sans rappeler l'expression (9.7) de l'état

produit après dégaussification dans le cas où $R \to 0$:

$$|\text{chat}_-\rangle = \frac{1}{\sqrt{2(1-e^{-2\alpha^2})}} \left(|\alpha\rangle - |-\alpha\rangle\right) \tag{9.18}$$

$$= \frac{e^{-\alpha^2/2}}{\sqrt{2(1-e^{-2\alpha^2})}} \sum_{n=0}^{\infty} \frac{\alpha^n - (-\alpha)^n}{\sqrt{n!}} |n\rangle \tag{9.19}$$

$$= \frac{\sqrt{2}\, e^{-\alpha^2/2}}{\sqrt{1-e^{-2\alpha^2}}} \sum_{p=0}^{\infty} \frac{\alpha^{2p+1}}{\sqrt{(2p+1)!}} |2p+1\rangle \tag{9.20}$$

Avec cette décomposition et l'expression (9.7) dans le cas d'un état pur après dégaussification, il est facile de calculer le recouvrement entre ces états, exprimé par la fidélité $\mathcal{F}$:

$$\mathcal{F} = |\langle \text{chat}_-|\Psi_{\text{cond}}\rangle|^2 = \frac{2\,\alpha^2\, e^{-\alpha^2}}{(1-e^{-2\alpha^2})\,\cosh^3\zeta} \left[\sum_{p=0}^{\infty} \frac{1}{p!} \left(\frac{\alpha^2}{2}\,\tanh\zeta\right)^p\right]^2 \tag{9.21}$$

$$= \frac{2\,\alpha^2}{(1-e^{-2\alpha^2})\,\cosh^3\zeta}\, \exp[\alpha^2\,(\tanh\zeta - 1)] \tag{9.22}$$

où $\tanh\zeta = (1-R)\,\tanh r$. Cette fonction est tracée sur la figure 9.17 en fonction de l'amplitude α du chat quantique pour notre paramètre expérimental $r = 0.43$ (ces calculs supposent un état dégaussifié pur, généré avec $R = 0.01$). Il apparaît alors que l'état conditionné correspond avec une fidélité de plus de 99% au chat $|\alpha\rangle - |-\alpha\rangle$ avec $\alpha = 1.16$. Précisons que des fidélités encore meilleures peuvent être obtenues pour des compressions r plus faibles (typiquement $\mathcal{F} > 0.997$ pour $r = 0.30$, $\alpha = 0.95$).

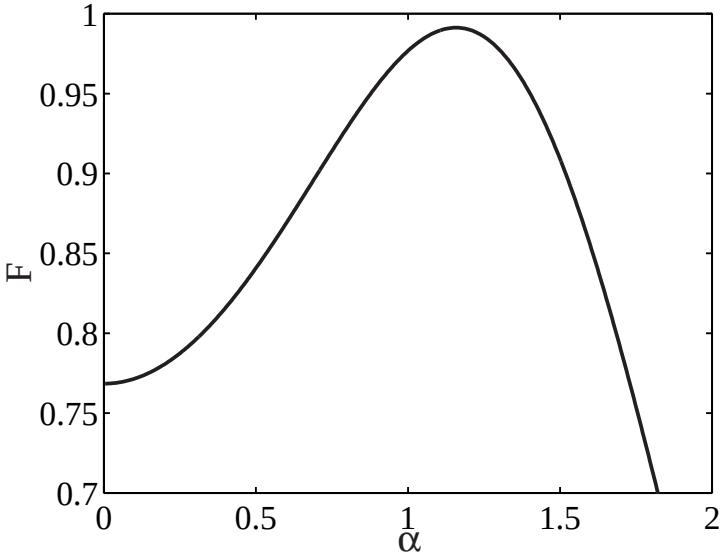

Figure 9.17: *Fidélité* $\mathcal{F} = |\langle \text{chat}_-|\Psi_{\text{cond}}\rangle|^2$ *entre un chat impair et l'état pur après dégaussification du vide comprimé de paramètre* $r = 0.43$*, dans la configuration monomode pure et* $R = 0.01$*, tracée en fonction de l'amplitude* α *du chat.*

Pour qu'une superposition linéaire d'états de la forme $|\alpha\rangle - |-\alpha\rangle$ soit un candidat au titre de chat de Schrödinger, il faut que les deux états cohérents puissent être distingués macroscopiquement par le résultat d'une mesure (par exemple une mesure homodyne). Cette condition impose une séparation dans l'espace de Hilbert $\langle -\alpha|\alpha\rangle \ll 1$, soit une amplitude α supérieure à 2. Le chat $\alpha = 1.16$ approximé par l'état conditionné avec $r = 0.43$ ne satisfait pas vraiment cette condition de séparation dans l'espace des phases, mais notre procédure ne demeure pas moins une technique simple et efficace en théorie pour générer de faibles "chatons" de Schrödinger. L'intérêt de cette procédure est de ne pas nécessiter d'interaction Kerr importante ou de détecteurs permettant de résoudre le nombre de photons. Des facteurs de compression modérés et des éléments optiques standards suffisent à notre dispositif. Enfin, les chatons $\alpha \approx 1.2$ peuvent ensuite être utilisés pour produire un chat de plus grande amplitude ($\alpha > 2$) avec une excellente fidélité ($\mathcal{F} > 99\%$) par le processus d'amplification conditionnelle proposé dans [131], qui lui aussi semble expérimentalement réalisable avec la technologie actuelle.

Dans une autre optique, si on s'intéresse aux états connus pouvant approcher l'état produit par notre procédure de dégaussification, la fonction de Wigner de l'état conditionné parfait (figure 9.10) n'est pas sans rappeler celle du photon unique auquel on aurait appliqué un opérateur de compression / dilatation de quadratures. Pour calculer la fidélité entre l'état conditionné et un photon unique comprimé, nous utilisons la décomposition de Fock de l'opérateur de compression $\hat{S}(r)$ appliqué à un photon unique [14, 131] :

$$\hat{S}(r)|1\rangle = \sum_{n=0}^{\infty} \frac{(\tanh r)^n}{\sqrt{\cosh^3 r}} \frac{\sqrt{(2n+1)!}}{2^n\, n!} |2n+1\rangle \tag{9.23}$$

Cette expression ne fait apparaître que des termes impairs dans la décomposition de Fock. Si on compare l'équation (9.23) à la formule (9.7), l'expression de l'état conditionné est mathématiquement identique à celle du photon unique comprimé en faisant l'identification entre le paramètre de compression réelle r et la compression formelle ζ :

$$|\Psi_{\text{cond}}\rangle \equiv \hat{S}(\zeta)|1\rangle \tag{9.24}$$

avec $\tanh\zeta = (1-R)\,\tanh r$. Lorsque $R \to 0$, $\zeta \approx r$ et l'état dégaussifié correspond formellement au photon unique comprimé $\hat{S}(r)|1\rangle$. Ce résultat peut se retrouver par un calcul de fidélité montrant que $\mathcal{F} \to 1$ lorsque $R \to 0$:

$$\mathcal{F} = |\langle\Psi_{\text{cond}}|\hat{S}(r)|1\rangle|^2 = \left[1 - \frac{R^2}{R + \frac{1}{\sinh^2 r}}\right]^{\frac{3}{2}} \tag{9.25}$$

Par la même occasion, nous retrouvons ici qu'un chat de Schrödinger impair d'amplitude α faible peut s'approximer par un photon unique comprimé (ce parallèle a été explicitement étudié dans la référence [131]).

9.5 Conclusion

Nous avons décrit la première observation expérimentale d'un protocole de "dégaussification" qui transforme des impulsions femtosecondes individuelles de vide comprimé en des états clairement non-gaussiens [128]. Cette procédure se base exclusivement sur des éléments optiques linéaires (incluant la compression des fluctuations quantiques) et une photodétection non-discriminante en nombre de photons. Les statistiques observées présentent des structures non-gaussiennes dépendantes en phase, ce qui ne peut s'expliquer que par l'effet de "soustraction

de photon" de la procédure de conditionnement et par des termes d'ordres supérieurs dans la production de photons (au-delà d'une simple paire paramétrique).

Cette procédure offre des perspectives prometteuses, tant pour l'exploitation de l'intrication portée par des variables continues, que pour la manipulation d'états spécifiquement quantiques, permettant l'étude des processus fondamentaux en physique quantique.

Chapitre 10

Génération d'états impulsionnels intriqués en quadratures

Sommaire

Dans leur célèbre article publié en 1935 [132], Einstein Podolsky et Rosen (EPR) considèrent un état quantique composé de deux modes définis respectivement par leurs opérateurs (X_A, P_A) et (X_B, P_B). Si chacun de ces couples obéit à la relation de commutation $[X_j, P_j] = 2\imath N_0$, le commutateur $[X_A - X_B, P_A + P_B]$ est quant à lui nul. Cela autorise d'après la relation d'Heisenberg l'existence d'états à deux modes dont les opérateurs X_A et X_B sont parfaitement corrélés alors que les opérateurs P_A et P_B sont parfaitement anti-corrélés. De tels états sont appelés des états intriqués ou états EPR. Pour ces états particuliers, Einstein et ses collaborateurs imaginent l'expérience de pensée suivante : l'observable X est mesurée pour le mode A, ce qui permet aussitôt de déduire avec certitude la valeur physique d'une mesure $X_B = X_A$ de l'autre mode. Selon l'interprétation EPR, si A peut prédire le résultat à distance d'une mesure en B, alors un "élément de réalité" [132] doit être associé à la quantité X_B. Inversement, l'observable P peut également être précisément mesurée en A. Ceci fournit simultanément la valeur $P_B = -P_A$ pour une mesure sur le mode B, qui est à relier selon EPR à un autre "élément de réalité"

caractérisant P_B. Sans interagir avec le mode B, il est ainsi possible de déterminer les deux "éléments de réalité" distincts caractérisant parfaitement X_B et P_B. Or ceci est en contradiction directe avec le principe d'incertitude d'Heisenberg et la non-commutation des observables. Ce raisonnement constitue ce qui est désormais connu sous le nom de *paradoxe EPR*.

Selon Einstein, Podolsky et Rosen, l'existence d'états intriqués et l'expérience de pensée ci-dessus mettent en question la mécanique quantique en tant que théorie *complète* de description des phénomènes physiques. Le point clé de leur raisonnement est qu'ils conçoivent les phénomènes physiques dans une hypothèse réaliste et locale, c'est-à-dire que les mesures faites à un endroit ne peuvent influencer les résultats en un autre endroit, et que les propriétés physiques possèdent des valeurs indépendamment de l'observation. Cette publication a depuis suscité de nombreux et fructueux débats, des échanges avec Niels Bohr aux tests expérimentaux des inégalités de Bell, qui seront abordés au chapitre 11.

Si cette interrogation est d'une importance capitale pour la compréhension des fondements de la physique quantique, une autre lecture de l'article EPR [132] offre une application tout aussi essentielle pour l'information quantique : l'exploitation des corrélations quantiques d'états intriqués. L'aspect important des états EPR est qu'ils peuvent offrir des corrélations plus fortes qu'aucun système classique. L'intrication a depuis été reconnue comme une *ressource* physique essentielle pour effectuer des tâches nouvelles de traitement de l'information quantique ou pour améliorer l'efficacité de certains autres protocoles [141, 1, 3]. Parmi ces applications pour les variables continues, on peut donner quelques références pour la téléportation quantique [158, 146, 150], le codage dense [162, 153], certains protocoles spécifiques de cryptographie quantique [62, 63, 64, 67, 69, 70], les répéteurs quantiques [160, 127] ou le calcul quantique [161, 3].

Dans le domaine spécifique des recherches entreprises lors de ce travail de thèse, le rôle de l'intrication quantique dans les protocoles de cryptographie avec des états cohérents a été discuté au chapitre 6, où il est démontré que nos protocoles à états cohérents exploitent une intrication quantique "virtuelle" pour garantir la sécurité du transfert. Nous avons de plus introduit un protocole spécifique exploitant des états EPR qui dans certaines conditions peut s'avérer plus avantageux et plus robuste que les protocoles à états cohérents. Par ailleurs, comme nous l'avons souligné dans l'introduction du chapitre 9, l'utilisation réelle de l'intrication est une condition indispensable pour mettre en œuvre des procédures de distillation quantique afin d'améliorer la portée des protocoles actuels de cryptographie quantique. Il est donc très intéressant de poursuivre notre développement de ressources de base pour le traitement de l'information quantique avec des variables continues en y adjoignant un dispositif de production d'états EPR [157].

Forts de nos expériences dans la génération d'états comprimés et d'états non-gaussiens monomodes (chapitres 7 et 9), nous reprenons le montage expérimental pour produire des faisceaux intriqués en quadratures à partir de l'amplification paramétrique non dégénérée d'impulsions femtosecondes. Comme pour toute ressource, une caractérisation de l'intrication expérimentale est nécessaire pour pouvoir exploiter tout son potentiel. Après une brève description de la manipulation de l'intrication en quadratures à la section 10.1, le dispositif d'amplification paramétrique classique non dégénérée est décrit lors de la section 10.2, avant d'aborder la caractérisation expérimentale d'états impulsionnels intriqués (section 10.3).

10.1 Retour sur l'intrication avec des variables continues

Quelques précisions sont apportées sur l'intrication quantique entre les composantes de quadrature d'un état EPR à deux modes, en s'appuyant sur trois aspects : production, caractérisation et quantification.

10.1.1 Production de l'intrication

Plusieurs techniques différentes ont été développées au cours de ces dernières années pour produire des faisceaux intriqués en quadratures. Parmi les expériences ayant été menées, deux classes particulières émergent : l'amplification paramétrique non-dégénérée et le couplage sur une lame semi-réfléchissante de deux vides comprimés déphasés de $\pi/2$. L'amplification paramétrique a été utilisée pour la première expérience de production de faisceaux EPR en 1992 [143, 144]. Le couplage de deux vides comprimés a constitué la source nécessaire d'intrication pour la première réalisation de la téléportation quantique avec des variables continues en 1998 [146].

Si ces deux techniques de production d'états EPR sont théoriquement équivalentes et fournissent la même intrication pour des couplages non-linéaires identiques, elles ont été développées séparément suivant les types de cristaux et de configurations employés. L'amplification non-dégénérée utilise des effets non-linéaires du second ordre (processus $\chi^{(2)}$), généralement dans un cristal de KTP en accord de phase de type II placé en cavité optique, formant ainsi un oscillateur paramétrique optique (OPO) [143, 144, 147, 149, 154, 155]. Suivant une autre approche, la combinaison de deux vides comprimés déphasés permet d'utiliser l'ensemble des techniques de production des états comprimés : oscillation paramétrique dégénérée [150, 151, 152, 153], effet Kerr dans des fibres optiques [148, 199]... Pour ces différentes expériences, les corrélations en quadratures mesurées sont typiquement de l'ordre de 4 dB en dessous du niveau de bruit quantique standard, mais la possibilité d'utiliser des sources d'états fortement comprimés permet d'atteindre des corrélations de plus de 7 dB [115]. Citons enfin la possibilité de produire des faisceaux intriqués en quadrature par l'interaction entre un champ cohérent et un nuage froid d'atomes de Cesium placés dans une cavité de forte finesse [200, 201].

La quasi-totalité des références citées ci-dessus utilise des cavités optiques pour exalter les interactions non-linéaires et produire des effets quantiques intenses. L'inconvénient de cette technique est qu'elle implique de fait l'usage de faisceaux continus, qui ne permettent pas des échanges simples de symboles temporels pour des protocoles de communication. A notre connaissance, seules les références [148, 199] ont mis en œuvre une source impulsionnelle d'états intriqués avec des variables continues en utilisant l'effet Kerr dans des fibres optiques. Une autre constatation intéressante est que si l'amplification paramétrique non-dégénérée en simple passage est une méthode bien connue pour produire des états EPR [13, 14], cette technique n'a pas encore été présentée expérimentalement dans le cadre spécifique des variables continues, notamment du fait des faibles effets non-linéaires généralement disponibles.

Dans ce contexte, nous nous proposons d'exploiter les possibilités de notre montage d'optique non-linéaire impulsionnelle présenté au chapitre 7 : forte puissance crête des impulsions, coefficient non-linéaire élevé du $KNbO_3$, large plage d'accord de phase et résolution temporelle de la détection homodyne impulsionnelle. Plutôt que de dupliquer les optiques pour générer deux vides comprimés, nous choisissons d'utiliser un seul cristal de niobate de potassium dans une configuration spatialement non-dégénérée pour obtenir la génération d'états EPR. Cette disposition offre trois avantages particuliers [157] :

- *Une production simple d'intrication* : les faisceaux émergeant du cristal sont directement intriqués sans aucune autre action supplémentaire (ce qui n'est pas le cas de la combinaison de deux vides comprimés dont la phase relative doit être correctement contrôlée).

- *Des effets non-linéaires intenses* grâce au cristal de $KNbO_3$ permettant comme nous allons le voir par la suite des corrélation de l'ordre de 3 dB.

- *Une structure impulsionnelle complète* de la source à la détection homodyne, fournissant l'ensemble des éléments pour des protocoles de communication quantique avec des états

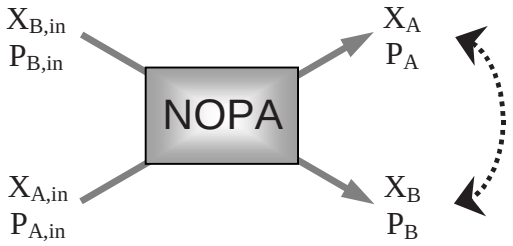

Figure 10.1: *Notations employées pour décrire les modes entrant et sortant d'un amplificateur paramétrique en configuration non-dégénérée.*

EPR. En particulier, l'analyse des transferts d'information au sens de Shannon est alors simple et claire [73, 70].

Avant d'aborder d'autres points sur la manipulation de l'intrication avec des variables continues, nous présentons d'abord quelques rappels et notations sur la génération d'états intriqués. Un amplificateur paramétrique en configuration non-dégénérée réalise une amplification indépendante de la phase et a été présentée à la section 2.4.2. Les quadratures (X_A, P_A) et (X_B, P_B) des modes de sortie s'expriment en fonction des modes d'entrée $(X_{A,in}, P_{A,in})$, $(X_{B,in}, P_{B,in})$ [79, 13] :

$$\begin{aligned} X_A &= \sqrt{G}\, X_{A,in} + \sqrt{G-1}\, X_{B,in} && \text{(10.1a)} \\ P_A &= \sqrt{G}\, P_{A,in} - \sqrt{G-1}\, P_{B,in} \\ X_B &= \sqrt{G}\, X_{B,in} + \sqrt{G-1}\, X_{A,in} && \text{(10.1b)} \\ P_B &= \sqrt{G}\, P_{B,in} - \sqrt{G-1}\, P_{A,in} \end{aligned}$$

où $G = \cosh^2 r$ est le gain paramétrique, et r le facteur de compression, fonction de la non-linéarité effective du cristal et de la puissance de pompe (dans ces notations, $\sqrt{G} = \cosh r$ et $\sqrt{G-1} = \sinh r$). Il est à noter que l'on retrouve des formules similaires dans le cas de la combinaison de deux vides comprimés déphasés sur une lame semiréfléchissante, en définissant la variance comprimée $s = e^{-2r}$.

Par la suite, nous nous restreindrons au cas où les modes entrants sont indépendants et sont dans l'état vide. L'état à deux modes A et B alors généré par l'amplificateur est appelé *vide comprimé à deux modes*. Il est facile de montrer que les modes de sortie sont corrélés en exprimant leurs termes croisés ou les variances conditionnelles des mesures d'une quadrature connaissant l'autre :

$$\langle X_A\, X_B \rangle = -\langle P_A\, P_B \rangle = 2\sqrt{G\,(G-1)}\, N_0 = \sinh 2r\, N_0 \qquad (10.2)$$

$$\langle (X_A - X_B)^2 \rangle = \langle (P_A + P_B)^2 \rangle = 2\,(\sqrt{G} - \sqrt{G-1})^2\, N_0 = 2\, e^{-2r}\, N_0 \qquad (10.3)$$

$$V_{X_B|X_A} = V_{P_B|P_A} = \frac{1}{2G-1}\, N_0 = \frac{1}{\cosh 2r}\, N_0 \quad < \; N_0 \qquad (10.4)$$

Pour des effets non-linéaires infinis $r \to \infty$, les corrélations entre quadratures deviennent parfaites (par exemple $\langle (X_A - X_B)^2 \rangle \to 0$ et $V_{X_B|X_A} \to 0$), ce qui réalise l'état initialement prévu par Einstein, Podolsky et Rosen [132].

L'état produit est un état gaussien dont les quadratures sont de valeurs moyennes nulles. Il peut alors être complètement représenté par sa matrice de covariance, définie à la section 2.2.3. D'après la référence [134], 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, comme par exemple la base (X_A, P_A, X_B, P_B) :

$$\gamma = \frac{1}{N_0} \begin{pmatrix} \langle {X_A}^2 \rangle & 0 & \frac{1}{2}\langle X_A X_B + X_B X_A \rangle & 0 \\ 0 & \langle {P_A}^2 \rangle & 0 & \frac{1}{2}\langle P_A P_B + P_B P_A \rangle \\ \frac{1}{2}\langle X_A X_B + X_B X_A \rangle & 0 & \langle {X_B}^2 \rangle & 0 \\ 0 & \frac{1}{2}\langle P_A P_B + P_B P_A \rangle & 0 & \langle {P_B}^2 \rangle \end{pmatrix} \tag{10.5}$$

Une caractérisation complète de l'état EPR ne nécessite donc que la mesure de 6 termes (4 si les modes sont symétriques) pour définir la matrice de covariance ci-dessus. Dans le cas d'un état pur, l'expression de la matrice γ est encore plus simple, et ne fait intervenir que le paramètre de compression r :

$$\gamma = \frac{1}{N_0} \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix} \tag{10.6}$$

Par ailleurs, il est également utile suivant les applications de connaître la décomposition sur la base de Fock d'un tel état pur :

$$|\Psi\rangle_{AB} = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n \, |n\rangle_A \, |n\rangle_B \tag{10.7}$$

où $\lambda = \tanh r$. Les nombres de photons mesurés dans les modes A et B sont toujours égaux, ce qui est une conséquence du processus paramétrique non-dégénéré où l'annihilation d'un photon pompe produit exactement un photon dans le mode A et un photon dans le mode B.

Si la donnée de la matrice de covariance ou de la matrice densité indique des corrélations entre les quadratures, elle ne précise pas immédiatement si l'état est séparable ou non, ni quelle est la force de l'intrication. Différents paramètres sont alors introduits pour caractériser et quantifier l'intrication [141, 3].

10.1.2 Caractérisation de l'intrication

Critère de non-séparabilité de Duan-Simon

Dans le domaine des variables continues, Duan et Simon ont indépendamment formulé une condition suffisante pour qu'un état à deux modes A,B soit non-séparable [134, 135] :

$$\mathcal{I}_{\mathrm{DS}} = \frac{1}{2}\left[\Delta^2(X_A - X_B) + \Delta^2(P_A + P_B)\right] < 2\,N_0 \tag{10.8}$$

où $\Delta^2(.)$ indique la variance de l'opérateur entre parenthèses. (Pour un état gaussien symétrique entre les modes A et B, la vérification de ce critère devient une condition nécessaire et suffisante de non-séparabilité).

Dans le cas de l'état EPR pur, le calcul de la quantité $\mathcal{I}_{\mathrm{DS}}$ fournit immédiatement $\mathcal{I}_{\mathrm{DS}} = 2\,e^{-2r}\,N_0$, ce qui est inférieur à $2N_0$ dès que $r > 0$. Ainsi tout état EPR généré par amplification

paramétrique parfaite est intriqué (non-séparable) indépendamment de la force de l'interaction non-linéaire. On peut de plus remarquer que la vérification du critère de Duan-Simon est d'autant meilleure que la compression r est grande, ce qui suggère d'utiliser également ce critère comme une quantification de l'intrication entre les modes. Cependant, nous verrons plus loin dans cette section qu'il existe d'autres manières pertinentes de quantifier l'intrication.

Critère de Reid-EPR

Les corrélations dans le faisceau intriqué en quadratures ont conduit Einstein et ses collaborateurs à formuler le "paradoxe EPR". Dans le cas de ressources physiques limitées, la condition pour l'existence de corrélations EPR s'écrit sous la forme du critère de Reid-EPR en fonction des variances conditionnelles des quadratures [133] :

$$\mathcal{I}_{\mathrm{EPR}} = V_{X_B|X_A}\, V_{P_B|P_A} < {N_0}^2 \tag{10.9}$$

Cette forme reprend la démonstration du "paradoxe EPR" et suggère une "pseudo"-violation de l'inégalité d'Heisenberg [1]. La vérification de ce critère est une condition suffisante (mais non nécessaire) pour que les modes en jeu soient non-séparables. De plus, il a été démontré que la présence de corrélations EPR satisfaisant (10.9) implique nécessairement la vérification du critère de non-séparabilité de Duan-Simon (10.8) [136]. La condition de Reid-EPR apparaît donc comme un critère plus strict d'intrication que celui de Duan-Simon. La présence de pertes souligne en particulier la différence entre ces deux derniers critères : alors que la condition de Duan-Simon peut être vérifiée pour des pertes arbitraires, la condition de Reid-EPR nécessite des pertes inférieures à 50% [152].

Pour l'état EPR introduit à la section précédente, on obtient $\mathcal{I}_{\mathrm{EPR}} = {N_0}^2/\cosh^2 2r$, ce qui est inférieur à ${N_0}^2$ dès que $r > 0$. Ainsi tout état EPR généré par amplification paramétrique parfaite présente des corrélations au sens EPR et est nécessairement intriqué. Comme pour le critère de Duan-Simon, la vérification de la condition Reid-EPR est d'autant plus forte que la compression r est grande. Ainsi ce critère a lui aussi été utilisé comme expression de la qualité de l'intrication, depuis la première source expérimentale d'états intriqués en quadratures présentée par Ou et ses collaborateurs [143] avec $\mathcal{I}_{\mathrm{EPR}} = 0.70\,{N_0}^2$.

Fidélité de téléportation quantique

A proprement parler, la fidélité d'un protocole de téléportation quantique à variables continues n'est pas un critère pour caractériser ou pour quantifier l'intrication de faisceaux EPR. Cependant, elle constitue le paramètre pertinent pour valider le succès d'une expérience de téléportation où la qualité de l'intrication disponible est fondamentale. Son interprétation physique étant relativement simple [83], la fidélité est ainsi une donnée intéressante pour qualifier une source de faisceaux intriqués.

La fidélité d'un processus de téléportation quantique est définie comme le recouvrement de l'état en sortie avec l'état en entrée. Pour un protocole de téléportation idéale d'un état cohérent, de gain égal à l'unité et exploitant l'intrication des faisceaux A et B, la fidélité s'exprime par [150, 71] :

$$\mathcal{F} = |\langle\psi_{in}|\hat{\rho}_{out}|\psi_{in}\rangle| = \frac{1}{\sqrt{\left(1+\frac{\Delta^2(X_A-X_B)}{2\,N_0}\right)\left(1+\frac{\Delta^2(P_A+P_B)}{2\,N_0}\right)}} \tag{10.10}$$

[1] La condition dans l'expression des variances conditionnelles dans (10.9) n'étant pas la même, le principe d'incertitude d'Heisenberg n'est pas mis en contradiction. On peut facilement vérifier par exemple que $V_{X_B|X_A}\, V_{P_B|X_A} \geq N_0^2$ pour l'état EPR introduit à la section 10.1.1.

La limite $\mathcal{F} = 1/2$ correspond au meilleur résultat qu'il est possible d'obtenir en utilisant l'optique classique. D'après [146], pour vérifier $\mathcal{F} > 1/2$, il faut nécessairement utiliser de l'intrication quantique. Le critère $\mathcal{F} > 1/2$ apparaît alors comme une autre condition nécessaire pour que l'état de modes A, B soit non-séparable, ce qui se réécrit en :

$$\mathcal{I}_{\rm Fid} = \frac{1}{\mathcal{F}} = \sqrt{\left(1 + \frac{\Delta^2(X_A - X_B)}{2\,N_0}\right)\left(1 + \frac{\Delta^2(P_A + P_B)}{2\,N_0}\right)} < 2 \tag{10.11}$$

Pour des états symétriques en X et P, on retrouve alors la condition de Duan-Simon. Dans le cas d'un vide comprimé à deux modes pur tel que défini à la section 10.1.1, on obtient $\mathcal{F} = 1/(1+e^{-2r})$, ce qui est supérieur à $1/2$ dès que $r > 0$ et atteste de l'intrication de l'état considéré.

Précisons enfin que pour garantir que l'état téléporté constitue la meilleure copie possible de l'état initial, il faut vérifier $\mathcal{F} > 2/3$ [83], soit au moins $r > 0.35$ pour une téléportation idéale.

10.1.3 Quantification de l'intrication

Les critères de Duan-Simon et de Reid-EPR et la fidélité d'une téléportation idéale permettent de caractériser la non-séparabilité de l'état. Toutes ces quantités, et dans une certaine mesure les corrélations $\langle X_A\, X_B\rangle$ et $\langle P_A\, P_B\rangle$, peuvent ensuite être utilisées pour apprécier et comparer la qualité de l'intrication quantique, en indiquant des corrélations plus ou moins fortes. Cependant, pour constituer une mesure correcte de l'intrication, une grandeur physique doit vérifier certains critères précis, présentés par exemple dans [141]. Malheureusement, les critères de Duan-Simon et de Reid-EPR ne vérifient pas ces conditions. Ils ne sont donc pas à proprement parler des mesures complètes de l'intrication.

Pour formuler une mesure quantifiant l'intrication, il faut distinguer deux cas, suivant que l'état est pur ou non. Dans le cas d'un état pur, on définit l'*entropie de Von Neumann* $E_{\rm VN} = -{\rm Tr}(\rho_A \log \rho_A)$, où $\rho_A = {\rm Tr}_B(\rho_{AB})$ est la matrice densité réduite vue par A. Cette quantité est alors la seule mesure propre de l'intrication [141, 1, 3]. Par contre, dans le cas d'un mélange statistique d'états, il n'existe pas de définition unique d'une mesure correcte de l'intrication, ce qui a donné lieu à l'introduction de diverses définitions (voir par exemple les références citées dans [141]). En particulier, nous retiendrons l'*entropie de formation* $E_{\rm F}$ [137], qui représente le nombre de paires de qubits intriquées pures nécessaires pour préparer les corrélations observées. Giedke et ses collaborateurs [142] ont calculé explicitement cette entropie pour le cas d'états gaussiens symétriques, de matrice de covariance s'exprimant par :

$$\gamma = \begin{pmatrix} V & 0 & K_x & 0 \\ 0 & V & 0 & -K_p \\ K_x & 0 & V & 0 \\ 0 & -K_p & 0 & V \end{pmatrix} \tag{10.12}$$

L'entropie de formation de l'état décrit par γ vaut alors [142] :

$$E_{\rm F} = f\left(\sqrt{(V - K_x)(V - K_p)}\right) \tag{10.13}$$

avec $f(x) = c_+(x)\log c_+(x) - c_-(x)\log c_-(x)$ et $c_\pm(x) = [x^{-1/2} \pm x^{1/2}]^2/4$. Pour un état EPR symétrique, cette entropie est directement reliée au paramètre de Duan-Simon défini par l'équation (10.8) [201] :

$$E_{\rm F} = f\left(\frac{\mathcal{I}_{\rm DS}}{2\,N_0}\right) \tag{10.14}$$

Pour conclure cette section, nous pouvons calculer l'entropie de Von Neumann dans le cas d'un vide comprimé à deux modes pur, défini à la section 10.1.1. D'après la formule (10.15) la matrice densité réduite ρ_A vue depuis le mode A s'écrit :

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = (1-\lambda^2)\sum_{n=0}^{\infty} \lambda^{2n} \, |n\rangle\langle n|_A \tag{10.15}$$

Ce qui permet de calculer explicitement l'entropie de Von Neumann :

$$\begin{aligned} E_{\mathrm{VN}} = -\mathrm{Tr}(\rho_A \log \rho_A) &= \frac{\lambda^2}{1-\lambda^2} \log \lambda^2 + \log(1-\lambda^2) \\ &= \cosh^2 r \, \log \cosh^2 r - \sinh^2 r \, \log \sinh^2 r \end{aligned} \tag{10.16}$$

où on a posé $\lambda = \tanh r$ avec r le paramètre de compression [2]. On peut de plus remarquer que l'entropie de Von Neumann et l'entropie de formation fournissent le même résultat dans le cas d'un état pur.

Munis de ce formalisme technique pour l'exploitation de l'intrication avec des variables continues, nous pouvons désormais aborder le dispositif expérimental d'amplification classique non dégénérée qui permet la génération d'états intriqués en quadratures, caractérisés à la section 10.3.

10.2 Amplification paramétrique classique en configuration non-dégénérée

10.2.1 Mise en œuvre expérimentale

Grâce aux fortes puissances crêtes des impulsions femtosecondes et aux nonlinéarités élevées de nos cristaux de $KNbO_3$, l'amplification paramétrique non-dégénérée en simple passage peut être utilisée en régime impulsionnel pour produire des états d'intrication élevée en quadratures. Avant d'aborder le domaine des corrélations quantiques, nous considérons l'amplification non-dégénérée classique d'un faisceau sonde à la longueur d'onde du fondamental. D'après les formules (10.1), le gain attendu classiquement est $G = \cosh^2 r$ et est indépendant de la phase relative entre la pompe et la sonde. Pour lever la dégénérescence, nous nous plaçons dans une configuration non-colinéaire : pompe et sonde suivent des directions de propagation décalées angulairement au niveau du cristal (voir la figure 10.2). Les modes "signal" et "complémentaire" (*idler*) générés par le système sont alors symétriques par rapport à l'axe de la pompe. De plus, l'accord de phase est pris de type I dégénéré spectralement (signal et complémentaire ont la même polarisation et la même fréquence optique).

Le premier point est de vérifier que l'accord de phase peut effectivement être obtenu dans cette configuration pour nos cristaux niobate de potassium, taillés suivant l'axe a et refroidis en température (les propriétés détaillées des cristaux sont présentées au chapitre 7). L'épaisseur du cristal étant très faible par rapport à la distance de Rayleigh des faisceaux focalisés (100 μm à comparer à environ 1 mm), il n'y aura pas de problème de recouvrement spatial entre les faisceaux

[2] Le choix de la base des logarithme est laissée à l'appréciation de l'utilisateur. Par analogie avec les variables discrètes, la base 2 est souvent choisie, auquel cas l'entropie de Von Neumann s'exprime en "ebits", de telle sorte que l'état $1/\sqrt{2}\,(|01\rangle + |10\rangle)$ présente une intrication de 1 ebit. Pour des variables continues, il est plus cohérent d'utiliser la base naturelle des logarithmes népériens, et dans ce cas E_{VN} s'exprime en "enats" [3] (1 enat $= 1/\ln 2$ ebit).

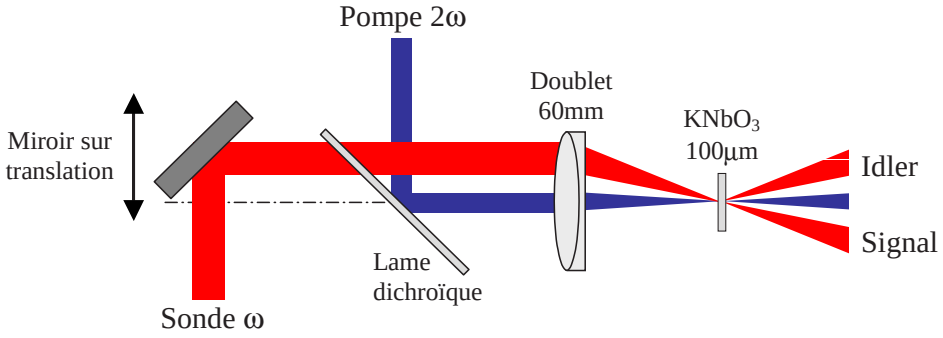

Figure 10.2: *Schéma du montage d'amplification paramétrique en configuration non-colinéaire. Pour la disposition expérimentale produisant la plus forte amplification, les diamètres des faisceaux sonde et pompe en entrée de focalisation sont respectivement de 5.5 mm et 2.5 mm, et leur séparation est de l'ordre de 4 mm.*

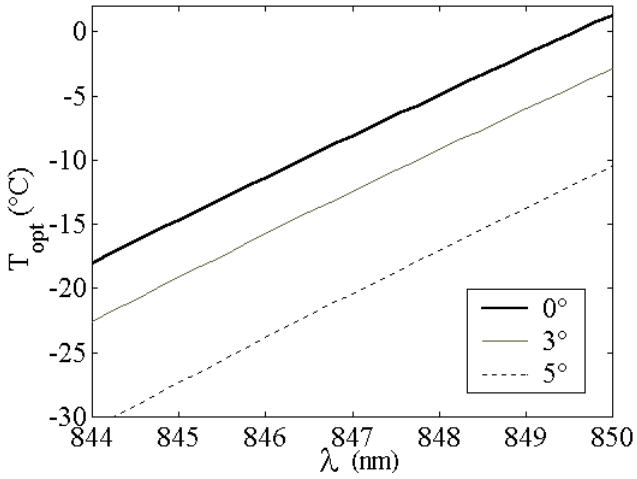

Figure 10.3: *Température optimale d'accord de phase non-colinéaire dégénéré en fréquence, pour un cristal de $KNbO_3$ taillé suivant l'axe a, en fonction de la longueur d'onde du fondamental et de l'angle de décalage horizontal pris en dehors du cristal entre les axes de la sonde ω et de la pompe 2ω. La sonde polarisée s est décalée horizontalement dans le plan p (dans ce cas, la polarisation de la sonde correspond toujours à l'axe cristallographique b). La propagation de la pompe est prise normale à la surface du cristal (cas de la figure 10.2).*

dans la zone d'interaction. De plus, nous pourrons raisonnablement prendre l'approximation des ondes planes au niveau de la focalisation dans le cristal.

Pour un angle θ entre la sonde et la pompe, la condition d'accord de phase (conservation des vecteurs d'ondes) s'écrit $n_\omega(\theta, T)\cos\theta + n_\omega(-\theta, T)\cos\theta = 2\, n_{2\omega}(0, T)$ où nous avons pris l'incidence de la pompe normale à la surface du cristal. Compte tenu de la symétrie axiale de notre système (accord de phase colinéaire non-critique), cette condition se simplifie en $n_\omega(\theta, T)\cos\theta = n_{2\omega}(0, T)$. La sonde étant polarisée verticalement, il est intéressant de considérer un décalage angulaire θ dans le plan horizontal. Dans ce cas, la polarisation de la sonde demeure toujours verticale et correspond quel que soit l'angle de décalage θ à l'axe cristallo-

graphique b : $n_\omega(\theta, T) = n_{b,\omega}(T)$. Pour cette configuration, la condition d'accord de phase s'exprime simplement $n_{b,\omega}(T)\cos\theta = n_{2\omega}(0, T)$, ce qui permet de rechercher alors la meilleure température vérifiant cette condition compte tenu du décalage θ au sein du cristal. Les résultats de nos calculs sont présentés sur la figure 10.3 en fonction du décalage angulaire et de la longueur d'onde du fondamental. Les expressions des indices proviennent de la référence [96]. Il apparaît que les effets d'un décalage de 3 à 5° peuvent facilement être compensés par un refroidissement supplémentaire du cristal de 5 à 10°C. Expérimentalement, nous travaillerons avec des faisceaux décalés d'environ 4° en dehors du cristal, ce qui se traduit du fait de la réfraction par $\theta \approx 2°$ à l'intérieur du cristal. Ce décalage angulaire est largement à l'intérieur de la plage de température accessible par nos systèmes de refroidissement, et l'accord de phase en configuration non-linéaire est donc possible.

Le décalage angulaire entre la sonde et la pompe est obtenu en translatant horizontalement un miroir du chemin sonde, ce qui permet une translation réglable de la sonde par rapport à la pompe, tout en conservant des directions de propagation identiques en amont de la focalisation. Le décalage transverse est ensuite transformé en un décalage angulaire par le doublet de focalisation (voir la figure 10.2).

10.2.2 Mesure du gain paramétrique classique

La puissance moyenne du faisceau sonde après interaction non-linéaire est directement mesurée par une photodiode. L'amplification paramétrique indépendante de la phase est atteinte lorsque le décalage angulaire est choisi de telle sorte qu'il n'y ait plus aucun recouvrement entre les vecteurs d'ondes de la pompe et de la sonde. Ceci impose une séparation nette entre les modes spatiaux des faisceaux en amont de la focalisation, comme l'indique la figure 10.2. En plus de ce critère, les dimensions des modes transverses des faisceaux ont été optimisées pour fournir le meilleur gain paramétrique. Empiriquement, on retrouve en régime non-colinéaire la configuration optimale obtenue pour l'amplification dégénérée : aucune modification du faisceau pompe et un grandissement d'environ 2 sur le faisceau sonde en amont de la focalisation (voir le montage total sur la figure 10.6). Le meilleur gain mesuré en configuration non-colinéaire est de $G = 1.24$, ce qui est cohérent avec nos précédents résultats sur l'amplification dégénérée ($G = 1.24$ donne formellement $r = 0.47$, soit $e^{-2r} = 0.39$ et $e^{+2r} = 2.56$).

La figure 10.4 présente les mesures du gain paramétrique classique en fonction de la puissance de pompe, ainsi qu'une interpolation basée sur le modèle gain $= \cosh^2(\alpha\sqrt{\mathcal{P}_{2\omega}})$ dans le cadre de l'hypothèse des ondes planes. Ici, α est une constante dimensionnée proportionnelle au coefficient de non-linéarité effective et à la longueur du cristal tandis que $\mathcal{P}_{2\omega}$ désigne la puissance moyenne de la pompe de second harmonique. Remarquons enfin que le gain mesuré est indépendant de la puissance sonde, comme il se doit pour une amplification paramétrique sans déplétion de la pompe.

10.3 Caractérisation expérimentale d'états impulsionnels intriqués

10.3.1 Dispositif de caractérisation de l'intrication

La technique la plus simple et la plus claire pour caractériser deux modes intriqués est d'effectuer des mesures homodynes simultanées de chaque mode. Les données peuvent ensuite être comparées et traitées pour extraire les différents coefficients de corrélations entre les quadratures. Ces corrélations permettent enfin de caractériser et de quantifier l'intrication quantique comme nous l'avons indiqué à la section 10.1. Cette expérience étant actuellement dans une phase

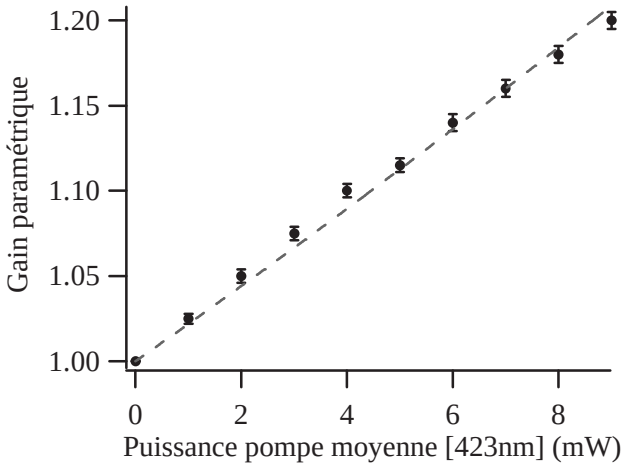

Figure 10.4: *Gain paramétrique en configuration hors d'axe en fonction de la puissance de pompe moyenne. Les disques sont les résultats des mesures de la puissance moyenne de la sonde amplifiée, la courbe est une interpolation selon le modèle des ondes planes.*

de démarrage, nous n'avons pas pu mettre en œuvre deux détections homodynes synchronisées pour l'instant.

Pour caractériser l'intrication entre les quadratures des modes A et B, nous avons alors choisi de recombiner ces modes sur une lame semiréfléchissante. Le principe de ce dispositif est schématisé sur la figure 10.5. De la même manière que la combinaison sur une lame de deux vides comprimés déphasés génère un état de type EPR, inversement, la combinaison de deux modes EPR intriqués sur une lame fournit deux vides comprimés déphasés. Pour formuler plus rigoureusement le résultat de notre dispositif de caractérisation, nous pouvons reprendre les expressions (10.1) pour donner les composantes de quadrature $(X_{s,1}, P_{s,1})$ d'un mode émergeant de la lame. Compte tenu du déphasage θ imposé entre les faisceaux EPR, le mode recombiné vaut :

$$\begin{aligned} X_{s,1} &= \frac{1}{\sqrt{2}}\left(X_A + \cos\theta X_B + \sin\theta P_B\right) \qquad (10.17a)\\ &= \frac{1}{\sqrt{2}}\big(\left[\cosh r + \cos\theta \sinh r\right] X_{A,in} + \left[\sinh r + \cos\theta \cosh r\right] X_{B,in} \\ &\qquad - \sin\theta \sinh r\, P_{A,in} + \sin\theta \cosh r\, P_{B,in}\big) \end{aligned}$$

$$\begin{aligned} P_{s,1} &= \frac{1}{\sqrt{2}}\left(P_A - \sin\theta X_B + \cos\theta P_B\right) \qquad (10.17b)\\ &= \frac{1}{\sqrt{2}}\big(\left[\cosh r - \cos\theta \sinh r\right] P_{A,in} + \left[-\sinh r + \cos\theta \cosh r\right] P_{B,in} \\ &\qquad - \sin\theta \sinh r\, X_{A,in} - \sin\theta \cosh r\, X_{B,in}\big) \end{aligned}$$

Il est alors facile de constater que le faisceau $(X_{s,1}, P_{s,1})$ est comprimé suivant la quadrature $\sin(\frac{\theta}{2})\, X_{s,1} + \cos(\frac{\theta}{2})\, P_{s,1}$ et anti-comprimé suivant la quadrature $\cos(\frac{\theta}{2})\, X_{s,1} - \sin(\frac{\theta}{2})\, P_{s,1}$. Vu dans l'espace des phases, le déphasage θ lors de la recombinaison fait tourner l'axe de l'ellipse d'un angle $\theta/2$, mais sans en modifier l'ellipticité traduisant la compression des fluctuations.

En particulier, lorsque les modes EPR sont en phase lors de la recombinaison ($\theta = 0$), les

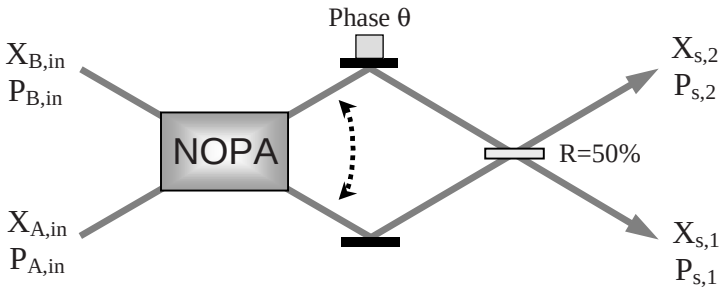

Figure 10.5: *Principe du dispositif de caractérisation de l'intrication en recombinant les faisceaux EPR.*

quadratures $(X_{s,1}, P_{s,1})$ s'expriment par :

$$X_{s,1} = \frac{1}{\sqrt{2}}(X_A + X_B) = \frac{e^r}{\sqrt{2}}(X_{A,in} + X_{B,in}) \tag{10.18a}$$

$$P_{s,1} = \frac{1}{\sqrt{2}}(P_A + P_B) = \frac{e^{-r}}{\sqrt{2}}(P_{A,in} + P_{B,in}) \tag{10.18b}$$

L'état en sortie de la lame est alors un état vide comprimé suivant la quadrature $P_{s,1}$, dont les variances des quadratures valent $\langle {X_{s,1}}^2 \rangle = e^{2r} N_0$ et $\langle {P_{s,1}}^2 \rangle = e^{-2r} N_0$. Ainsi, la présence de réduction des fluctuations sur le mode recombiné témoigne des corrélations quantiques entre les modes incidents. On peut de plus remarquer que la mesure pour $\theta = 0$ fournit directement la quantité $\Delta^2(P_A + P_B)$ nécessaire au critère de non-séparabilité de Duan-Simon (10.8).

Ces expressions peuvent être reprises pour la configuration $\theta = \pi$, auquel cas le vide est comprimé suivant la quadrature $X_{s,1}$:

$$X_{s,1} = \frac{1}{\sqrt{2}}(X_A - X_B) = \frac{e^{-r}}{\sqrt{2}}(X_{A,in} - X_{B,in}) \tag{10.19a}$$

$$P_{s,1} = \frac{1}{\sqrt{2}}(P_A - P_B) = \frac{e^{r}}{\sqrt{2}}(P_{A,in} - P_{B,in}) \tag{10.19b}$$

En mesurant la quadrature $X_{s,1}$ pour $\theta = \pi$, on peut alors accéder avec le même dispositif au deuxième terme $\Delta^2(X_A - X_B)$ du critère de Duan-Simon. Ainsi, en recombinant les deux faisceaux intriqués sur une lame semi-réfléchissante et en contrôlant leur phase relative θ, on peut accéder à tous les paramètres nécessaires pour exprimer la quantité de Duan-Simon $\mathcal{I}_{\mathrm{DS}}$, ce qui suffit à caractériser l'intrication quantique. Outre le fait de ne nécessiter qu'une seule détection homodyne, le montage de la figure 10.5 présente également l'avantage de mesurer *directement* les différents termes du paramètre $\mathcal{I}_{\mathrm{DS}}$. Ceci permet alors de caractériser la non-séparabilité de l'état, mais aussi de quantifier l'intrication par l'entropie de formation et la formule (10.14).

Enfin, une dernière configuration particulière s'obtient lorsque $\theta = \pi/2$, auquel cas le mode recombiné devient :

$$\begin{aligned} X_{s,1} &= \frac{1}{\sqrt{2}}(\cosh r\, X_{A,in} + \sinh r\, X_{B,in} - \sinh r\, P_{A,in} + \cosh r\, P_{B,in}) \\ P_{s,1} &= \frac{1}{\sqrt{2}}(\cosh r\, P_{A,in} - \sinh r\, P_{B,in} - \sinh r\, X_{A,in} + \cosh r\, X_{B,in}) \end{aligned} \tag{10.20}$$

Ces équations sont bien caractéristiques d'un état comprimé suivant la quadrature $(X_{s,1} + P_{s,1})/\sqrt{2}$.

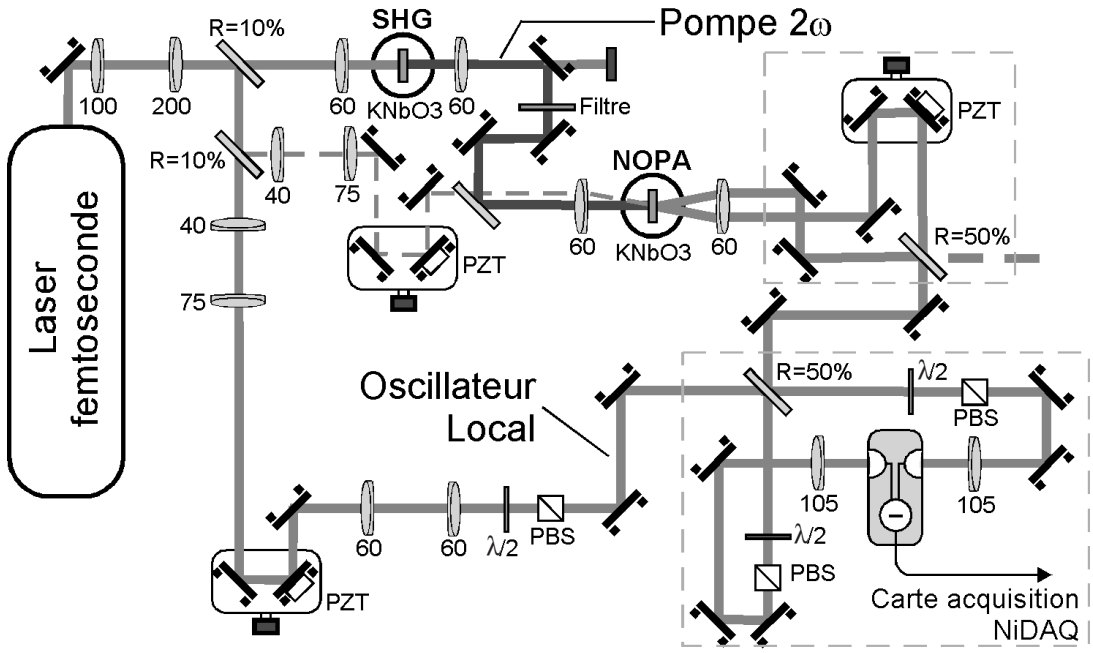

Figure 10.6: *Dispositif expérimental complet pour la génération d'états intriqués. Les focales des optiques sont indiquées en millimètres. Le faisceau sonde (tirets) est optionnel et sert à l'alignement des éléments.*

10.3.2 Montage optique détaillé

L'ensemble des différentes possibilités de recombinaison des états EPR pourra être étudié avec le montage expérimental présenté sur la figure 10.6, où on remarquera en particulier l'élément de recombinaison interférométrique des faisceaux EPR et la détection homodyne (cadres rectangulaires).

En l'absence de faisceau sonde, l'amplificateur paramétrique fonctionne en régime d'émission spontanée, exactement comme dans la configuration pour produire des impulsions dans l'état vide comprimé, présentée au chapitre 7. La seule différence entre les montages de fluorescence paramétrique tient dans le réglage de l'oscillateur local, qui sert de filtre pour sélectionner le mode spatio-temporel du signal. En configuration dégénérée, l'oscillateur local permet ainsi des mesures homodynes du vide comprimé. Dans un montage non-dégénéré comme indiqué sur la figure 10.6, l'oscillateur local sélectionne le mode issu de la recombinaison des faisceaux EPR. Pour obtenir un bon recouvrement entre les modes, le faisceau intense de la sonde est réglé pour fournir la meilleure amplification indépendante de la phase, puis les modes "signal" et "complémentaire" issus de l'amplificateur sont recombinés sur une lame semiréfléchissante. Le faisceau résultant de l'interférence entre ces modes est ensuite ajusté par rapport à l'oscillateur local de la détection homodyne.

Une première cale piezo-électrique permet de régler la phase θ lors de l'interférence des faiceaux EPR. Une seconde cale, placée sur le faisceau oscillateur local, permet de choisir la phase φ de la quadrature mesurée à la détection homodyne. Pour la caractérisation des états intriqués, la phase θ est incrémentée par paliers successifs, avec au total 20 paliers répartis sur l'intervalle $[0, \pi]$. Pour chaque palier de la phase de recombinaison, la phase φ de l'oscillateur local est balayée rapidement entre 0 et 2π, de sorte à effectuer une tomographie de l'état correspondant

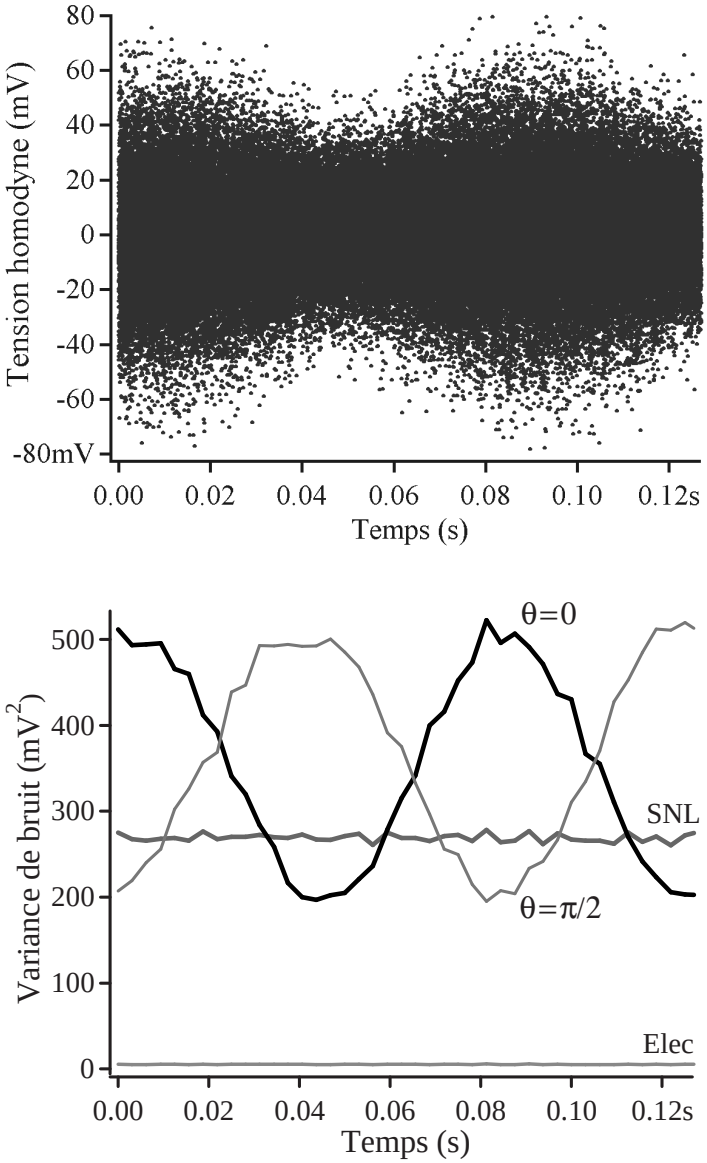

Figure 10.7: *(a) Mesures homodynes du faisceau issu de la recombinaison en phase des états EPR ($\theta = 0$), alors que la phase de l'oscillateur local est balayée linéairement. (b) Variance correspondante tracée sur une échelle linéaire et calculée d'après des blocs de 2500 points expérimentaux de la figure (a), pour des phases de recombinaison $\theta = 0$ et $\theta = \pi$. La variance minimale du bruit mesuré est de $0.70\,N_0$, la variance maximale vaut $1.96\,N_0$.*

(la durée d'un tel balayage est de 250 ms, ce qui correspond à la mesure de 195 000 impulsions).

10.3.3 Mesures homodynes impulsionnelles

La figure 10.7 présente les résultats des mesures homodynes impulsionnelles, tandis que la phase de l'oscillateur local est balayée linéairement. Les données affichées sur la figure 10.7(a) sont directement issues du signal en sortie de la détection homodyne, lorsque les faisceaux sont

recombinés en phase ($\theta = 0$). Ces données correspondent à la mesure pour chaque impulsion incidente de la quadrature signal en phase avec l'oscillateur local. La figure 10.7(b) présente les variances des quadratures mesurées, calculées pour des blocs de 2500 impulsions, et correspondant aux phases de recombinaison $\theta = 0$ et $\theta = \pi$.

Comme attendu pour les faisceaux comprimés produits lors de la recombinaison des états EPR, nous observons effectivement des oscillations périodiques de la variance de bruit. Pour une certaine phase de l'oscillateur local, cette variance mesurée passe sous le niveau de bruit quantique standard (SNL), ce qui est la signature d'un état comprimé. La meilleure réduction des fluctuations quantiques obtenue est de $0.70\,N_0$ (-1.55 dB), à quoi correspond une variance de la quadrature amplifiée de $1.96\,N_0$ (+2.92 dB).

Cette expérience a été répétée à de nombreuses reprises pour différentes phases θ de recombinaison des faisceaux EPR. Ceci nous a permis de vérifier la symétrie des états comprimés produits : la réduction de bruit traduisant les corrélations quantiques entre les quadratures est identique pour $\theta = 0$, $\theta = \pi$ et diverses autres phases (compte tenu d'incertitudes statistiques raisonnables inférieures à $0.01\,N_0$). En conséquence, nous pouvons admettre que les correlations entre les quadratures des états EPR sont identiques : $\Delta^2(X_A - X_B) = \Delta^2(P_A + P_B)$.

10.3.4 Caractérisation et quantification de l'intrication

Pour caractériser et quantifier l'intrication produite par notre expérience, il est alors logique de corriger l'effet des pertes introduites par la détection homodyne d'après les formules (8.21). Nous pouvons ainsi déduire la réduction des fluctuations quantiques et donc les corrélations EPR en amont de la détection. Comme pour les expériences de génération de vide comprimé ou d'état non-gaussien, nous évaluons l'efficacité globale de la détection homodyne par $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2 = 68\%$ avec la transmission optique $\eta_{opt} = 93\%$, l'efficacité quantique des photodiodes $\eta_{phot} = 94.5\%$ et l'adaptation des modes $\eta_{mod} = 88\%$ (toutes ces quantités sont mesurées indépendamment, l'adaptation des modes est obtenue à partir des franges d'interférences avec un faisceau sonde d'alignement).

Compte tenu de cette évaluation de l'efficacité homodyne η_{hom}, les mesures corrigées fournissent une réduction des fluctuations quantiques de $\Delta^2(X_A - X_B)/2 = \Delta^2(P_A + P_B)/2 = 0.56\,N_0$ (-2.52 dB). Cette valeur peut être directement utilisée pour évaluer le paramètre de Duan-Simon (10.8) : $\mathcal{I}_{\rm DS} = \frac{1}{2}\left[\Delta^2(X_A - X_B) + \Delta^2(P_A + P_B)\right] = 1.12\,N_0$. Cette quantité est clairement sous le seuil de séparabilité ($< 2\,N_0$), ce qui atteste de l'intrication quantique produite. Ces données permettent également de calculer directement la fidélité $\mathcal{F} = 0.64$ d'une expérience de téléportation idéale suivant l'équation (10.10). Pour ces états gaussiens, l'intrication peut ensuite être quantifiée grâce à l'entropie de formation donnée par l'équation (10.14), ce qui fournit pour notre expérience une intrication de $E_{\rm F} = 0.44$ ebit .

Le critère de Reid-EPR, donné par l'équation (10.9), est quant à lui plus délicat à évaluer, car il ne peut pas s'exprimer simplement par nos mesures du faisceau en sortie de l'interféromètre de recombinaison. Pour estimer ce paramètre sans ambiguïté, il nous faudrait utiliser deux détections homodynes pour caractériser simultanément chaque faisceau EPR.

10.3.5 Caractérisation de la matrice de covariance

Théoriquement, un état gaussien général est entièrement caractérisé par les valeurs moyennes de ses composantes de quadratures et par sa matrice de covariance γ, qui contient les moments d'ordre deux des quadratures. Pour un état général à deux modes, la matrice de covariance contient 16 termes. Cependant, dans notre cas, les états EPR générés par l'amplificateur

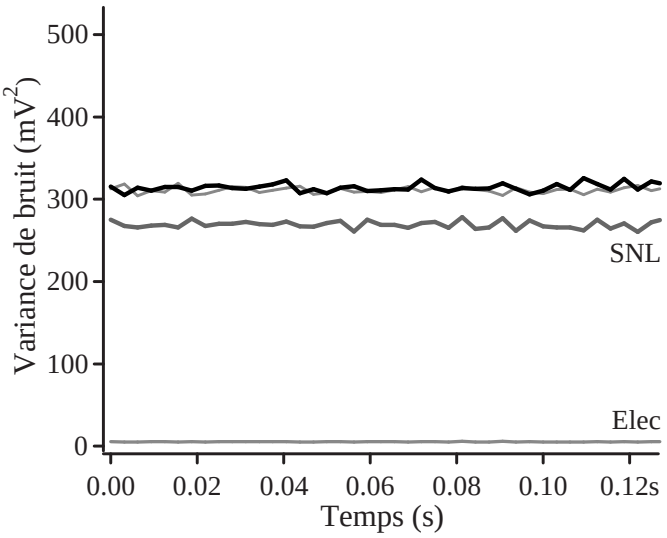

Figure 10.8: *Variance du bruit de quadrature d'un faisceau intriqué (courbe sombre), mesurée en aval de la lame de recombinaison avec la détection homodyne impulsionnelle, alors que la phase de l'oscillateur local est balayée linéairement et que l'autre faisceau intriqué est bloqué en amont de la lame* $50-50$*. La seconde courbe en gris clair au-dessus du SNL correspond au cas inverse où le premier faisceau EPR est bloqué, et le second est caractérisé par la détection homodyne.*

paramétrique sont produits et manipulés de manière symétrique. Ce point a été expressément vérifié sur notre expérience, comme nous le discutons dans la section précédente. En conséquence, la matrice de covariance de nos états EPR peut se réduire à la forme donnée par l'équation (10.12), avec $V\,N_0 = \Delta^2 X_A = \Delta^2 P_A = \Delta^2 X_B = \Delta^2 P_B$ et $K_x\,N_0 = K_p\,N_0 = \frac{1}{2}\langle X_A X_B + X_B X_A\rangle = -\frac{1}{2}\langle P_A P_B + P_B P_A\rangle$. Ceci signifie que pour la définition des quadratures suivant les axes les plus intriqués, il n'y a pas de corrélations entre les quadratures. Précisons également que pour des états gaussiens, il existe toujours une procédure théorique pour réduire la matrice de covariance suivant la forme (10.12) en utilisant des opérations unitaires locales [134].

En bloquant un des faisceaux intriqués en amont de la séparatrice $50-50$, nous pouvons accéder aux termes diagonaux de la matrice de covariance (compte tenu de la transmission de 50% de la lame et de l'efficacité η_{hom} de la détection homodyne). Les résultats de nos mesures impulsionnelles de bruit sont tracés sur la figure 10.8, lorsque la phase de l'oscillateur local est balayée linéairement. Pour chacun des faisceaux intriqués, nous avons mesuré une variance de $1.17 \pm 0.01\,N_0$. En corrigeant l'effets des pertes homodynes $\eta_{hom} = 68\%$ et de la transmission de la lame de recombinaison, nous pouvons alors obtenir $V\,N_0 = \Delta^2 X_A = \Delta^2 P_A = \Delta^2 X_B = \Delta^2 P_B = 1.50\,N_0$.

Les termes non-diagonaux de la matrice de covariance γ (10.12) s'obtiennent en constatant que grâce à nos mesures de réduction de bruit nous pouvons obtenir :

$$\begin{aligned} \frac{1}{2}\,\Delta^2(X_A - X_B) &= \frac{1}{2}\left(\Delta^2 X_A + \Delta^2 X_B - \langle X_A X_B + X_B X_A\rangle\right) \\ &= (V - K_x)\,N_0 \end{aligned} \tag{10.21}$$

Avec $V = 1.50$ et $\Delta^2(X_A - X_B)/2 = 0.56\,N_0$, nous obtenons directement $K_x = K_p = 0.94$. Ainsi

la matrice de covariance reconstruite pour les états EPR s'exprime par :

$$\gamma = \begin{pmatrix} 1.50 & (0) & 0.94 & (0) \\ (0) & 1.50 & (0) & -0.94 \\ 0.94 & (0) & 1.50 & (0) \\ (0) & -0.94 & (0) & 1.50 \end{pmatrix} \tag{10.22}$$

Les valeurs qui ont été fixées à zéro suite à des considérations de symétrie sont indiquées par des parenthèses. Une procédure similaire d'expression de la matrice de covariance d'états intriqués a déjà été mise en œuvre par Bowen et ses collaborateurs [152], mais dans le cas de faisceaux continus mesurés aux fréquences de 3.5 ou 6.5 MHz à l'aide d'un analyseur de spectre. Le schéma proposé ici possède cependant la particularité de fonctionner entièrement en régime impulsionnel.

10.4 Conclusion

Grâce aux possibilités d'interactions non-linéaires des impulsions ultrabrèves dans des cristaux minces de $KNbO_3$, des états intriqués en quadratures ont été simplement et efficacement générés lors d'un simple passage d'une impulsion dans un cristal en configuration d'amplification non-dégénérée. Nous avons ainsi pu mettre en évidence des corrélations entre les quadratures de $\Delta^2(X_A - X_B)/2 = 0.56\,N_0$ (-2.5 dB) [157]. En recombinant les deux faisceaux intriqués sur une lame semiréfléchissante, il est possible d'évaluer directement la non-séparabilité de l'état grâce au critère de Duan-Simon, ce qui fournit $\mathcal{I}_{\rm DS} = 1.12\,N_0$ ($< 2\,N_0$). Enfin, le même dispositif de caractérisation peut également quantifier directement l'intrication par l'entropie de formation. Expérimentalement, une quantité de $E_{\rm F} = 0.44$ ebit est disponible physiquement pour chaque paire d'impulsions intriquées.

Une particularité de notre dispositif est d'être entièrement impulsionnel, de la production des états intriqués à la détection homodyne. Auparavant, seul le groupe de Gerd Leuchs à l'université d'Erlangen avait mis en œuvre des états EPR impulsionnels [148, 199], mais le système de détection était basé sur un analyseur de spectre, donc non résolu en temps. Notre dispositif fournit quant à lui tous les éléments de base pour des applications futures de traitement de l'information quantique portée par des états EPR. En particulier, l'analyse des transferts d'informations au sens de Shannon est alors très simple, et permet des applications immédiates pour la cryptographie quantique avec des états EPR [73].

Outre ses possibilités pour l'information quantique, l'intrication de variables continues est également un domaine prometteur pour les tests des inégalités de Bell. En particulier, nous étudions en détails une proposition récente de Jaromir Fiurášek, Raoul Garcia-Patron Sanchez et Nicolas Cerf pour un dispositif expérimental faisable permettant un test *inconditionnel* des inégalités de Bell [188]. Ce système est basé sur une source d'états EPR impulsionnels décrits ici, sur des opérations de conditionnement présentées au chapitre 9 et sur des détections homodynes résolues en temps. Les différentes possibilités des variables continues pour la validation de la physique quantique feront l'objet du chapitre suivant.

Chapitre 11

Test des inégalités de Bell avec des variables continues

Sommaire

Validations expérimentales de la physique quantique

L'intrication quantique est un des aspects les plus surprenants de la physique quantique. Ses conséquences sont tellement différentes du sens commun qu'elles ont conduit Einstein, Podolsky et Rosen à affirmer en 1935 que la mécanique quantique est incomplète [132]. Leur argument se base sur le fait que toute théorie physique doit être à la fois "locale" et "réaliste", c'est-à-dire que les mesures faites en un endroit A ne peuvent influencer les résultats de mesures en un endroit B différent (hypothèse de localité) et que les propriétés physiques possèdent des valeurs définies, qui existent indépendamment de l'observation (hypothèse de réalisme). Les conséquences déroutantes de l'intrication quantique par rapport à nos intuitions sont discutées par exemple dans la référence [165].

Pour quantifier le débat entre la mécanique quantique et les théories à variables supplémentaires cachées, John Bell introduit en 1964 un ensemble d'inégalités devant être vérifiées par toute théorie locale et réaliste, alors que la mécanique quantique prévoit une violation de ces inégalités [166, 167, 168]. Ces inégalités ont dès lors permis de transposer le débat du domaine de l'épistémologie à la physique expérimentale [173]. Ainsi, au début des années 1980, les expériences menées par Alain Aspect, Jean Dalibard, Philippe Grangier et Gérard Roger [170, 171, 172] ont vérifié de manière très claire les prévisions de la mécanique quantique. Si ces résultats convainquent l'immense majorité des physiciens que la nature ne peut être à la fois "locale" et "réaliste", il faut néanmoins reconnaître que deux points faibles ou "échappatoires" (*loopholes*) affectent le dispositif expérimental. Ces points faibles sont un problème expérimental majeur car ils empêchent l'exclusion de toutes les théories à variables cachées (voir par exemple la référence [174]). Les tests effectués ne permettent donc pas de valider complètement et définitivement la mécanique quantique face aux autres théories.

Le premier de ces points faibles, appelé "échappatoire de localité", intervient dès que la séparation entre les systèmes de détection n'est pas suffisante pour rejeter toute possibilité d'échange d'information de vitesse inférieure à la vitesse de la lumière durant la mesure [169, 175]. La seconde faiblesse, ou "échappatoire d'efficacité de détection", apparaît lorsque l'efficacité des systèmes de détection n'est pas suffisamment élevée, de telle sorte que les événements mesurés pourraient ne pas être représentatifs de la statistique de l'ensemble [176, 177]. En 1982, Alain Aspect et ses collaborateurs [172] ont réalisé une première expérience de test des inégalités de Bell avec des analyseurs qui varient rapidement par rapport au temps de vol des photons intriqués. Ceci permet de séparer les détecteurs par des intervalles de genre espace et de clore l'échappatoire de localité. Cette expérience a depuis été reprise en 1998 par Anton Zeilinger et son équipe [178] qui utilisent une séparation des détecteurs de près de 400 m et des analyseurs rapides. Ces expériences ont permis de valider les prédictions de la physique quantique par rapport à l'échappatoire de localité, mais l'efficacité des détecteurs employés n'était malheureusement pas suffisante pour fermer la deuxième échappatoire. En 2001, David Wineland et son équipe ont mesuré les corrélations quantiques entre deux ions de Beryllium [179] avec une efficacité de détection de près de 80%, suffisante pour clore l'échappatoire d'efficacité de détection, mais dans le même temps, la séparation des deux ions (environ 8 μm) est trop faible pour éviter l'échappatoire de localité.

Dans ce contexte, un défi expérimental majeur est de concevoir et de réaliser une expérience permettant de fermer simultanément les deux échappatoires pour permettre un test complet des théories réalistes locales.

Utilisation des variables continues

Une expérience de test des inégalités de Bell implique typiquement deux systèmes de détection A et B qui effectuent des mesures simultanées sur deux sous-parties d'un état quantique intriqué. L'optique quantique offre un domaine d'expérimentation intéressant, les photons pouvant être transportés à grande distance tout en n'interagissant que très peu avec leur environnement, ce qui permet des séparations entre les systèmes suffisantes pour fermer l'échappatoire de localité. Par ailleurs, l'utilisation des détections homodynes de fortes efficacités est une alternative prometteuse par rapport aux dispositifs standards de comptage de photons, afin d'éviter l'échappatoire d'efficacité de détection. L'exploitation des variables quantiques continues présente donc toutes les particularités requises pour une validation logique complète de la physique quantique.

Malheureusement, les états EPR intriqués en quadratures ne peuvent pas être des candidats potentiels pour tester les inégalités de Bell : leur fonction de Wigner étant positive et gaussienne [1],

[1] Le théorème de Hudson-Piquet [18] précise que la seule fonction de Wigner qui soit partout positive est une

elle fournit directement la distribution de probabilité des variables cachées supplémentaires pour des mesures homodynes. Une violation d'une inégalité de Bell avec des détections homodynes ne peut être obtenue que pour des états quantiques non-gaussiens de fonctions de Wigner négatives.

Au moment où nous débutions nos études dans le domaine précis de l'utilisation des variables continues avec des détections homodynes, quelques propositions théoriques avaient été faites dans ce sens [183, 184, 185]. Cependant, pour ces dispositifs, la violation maximale prédite n'est que de quelques pourcents, ce qui est loin de la plus grande violation atteignable : $2\sqrt{2}$ par rapport à 2 (soit 41%) pour l'inégalité dite de Clauser-Horne-Shimony-Holt (CHSH) [167] ou de $(1+\sqrt{2})/2$ par rapport à 1 (soit 21%) pour l'inégalité de Clauser-Horne (CH) [168]. Dans la première proposition de test des inégalités de Bell avec des détections homodynes [183, 184], Gilchrist utilise un état défini par :

$$|\Psi_{\mathrm{C}}\rangle \propto \int_0^{2\pi} |r_0 e^{\imath\phi}\rangle_A |r_0 e^{-\imath\phi}\rangle_B \, d\phi \tag{11.1}$$

où $|r_0 e^{\imath\phi}\rangle$ est un état cohérent d'amplitude r_0 et de phase ϕ. Cet état induit une violation de 1.015 (> 1) de l'inégalité CH lors de mesures homodynes.

Munro considère quant à lui un état de nombres de photons corrélés [185] :

$$|\Psi_{\mathrm{M}}\rangle = \sum_{n=0}^{10} c_n |n\rangle|n\rangle \tag{11.2}$$

Les coefficients c_n sont optimisés suivant un calcul numérique pour fournir la plus grande violation de Bell lors de mesures homodynes. Avec un choix spécifique pour les dix coefficients utilisés c_n (qui sont non-négligeables jusqu'à $n = 7$), l'inégalité CHSH est violée de 2.076 (> 2) et l'inégalité CH de 1.019 (> 1). Cependant, cet état optimal paraît relativement irréalisable, tant sa décomposition de Fock est particulière. Aucune méthode n'est actuellement envisagée pour le générer expérimentalement.

Suivant une approche différente, Auberson et ses collaborateurs introduisent des inégalités de Bell dans l'espace des phases [186] et proposent un état permettant une violation maximale de $2\sqrt{2}$ (> 2). Cet état possède la fonction d'onde suivante :

$$\Psi_{\mathrm{A}}(x_A, x_B) = \frac{1}{2\sqrt{2}} \left[1 + e^{i\frac{\pi}{4}} \,\mathsf{sgn}(x_A)\,\mathsf{sgn}(x_B)\right] \, f(|x_A|)\, f(|x_B|) \tag{11.3}$$

où $f(x)$ est une forme régularisée de $\frac{1}{\sqrt{x}}$ de norme $\int_{-\infty}^{+\infty} f(x)^2\, dx = 1$. Le principal problème avec cette fonction d'onde se situe dans ses singularités mathématiques et ses sauts de phase. En conséquence, cet état nécessite des régularisations importantes avant de pouvoir être considéré comme un état physique acceptable.

Suite à ces différentes propositions, nous avons cherché à déterminer un état physique "simple" (réalisable) induisant une violation significative des inégalités de Bell. Plus précisément, nous avons examiné les deux questions suivantes :

1. Quels sont les états *physiques* permettant une violation maximale d'une inégalité de Bell lors de mesures homodynes ?

2. Quel dispositif peut-on concevoir en vue d'un test expérimental avec des variables continues ?

---

fonction gaussienne.

La réponse que nous apportons à la première question est présentée à la section 11.2 et discutée à la section 11.3, après un nouvel éclairage sur les inégalités de Bell dans le cadre des variables continues (section 11.1). Nous analysons enfin explicitement un dispositif expérimental *faisable* pour une validation logique complète de la physique quantique avec des détections homodynes de fortes efficacités (section 11.4).

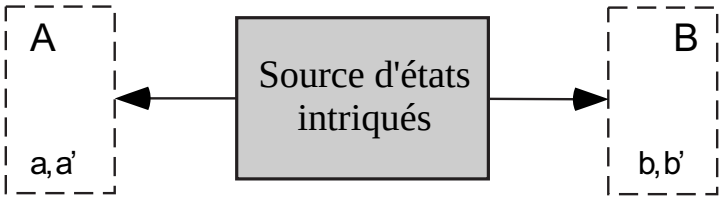

Figure 11.1: *Schéma général d'une expérience de test des inégalités de Bell. La source génère des états quantiques corrélés qui sont dirigés vers les systèmes de détection A et B, de paramètres ajustables a ou a′ et b ou b′. Chaque mesure fournit un résultat individuel noté "+" ou "-".*

11.1 Inégalités de Bell et variables continues

11.1.1 Retour sur les inégalités de Bell

Le schéma général d'une expérience de test des inégalités de Bell est présenté à la figure 11.1. Un état intriqué à deux modes est analysé par deux détecteurs A et B fournissant tous deux pour chaque mesure individuelle le résultat "+" ou "-". Dans le cadre des variables continues, ces systèmes de mesure seront des détections homodynes de fortes efficacités pour verrouiller l'échappatoire d'efficacité de détection. Chaque détecteur possède un paramètre ajustable entre les valeurs (a, a') et (b, b'). Pour les détections homodynes, ces paramètres sont les phases de référence respectives des oscillateurs locaux des éléments A et B. De plus, les systèmes d'analyse sont supposés suffisamment éloignés pour éviter toute communication de vitesse inférieure à celle de la lumière, ce qui permet de fermer simultanément l'échappatoire de localité.

Une remarque judicieuse est d'observer que chaque détection homodyne fournit un résultat variant continûment. La manière dont nous déduisons un résultat binaire ("+" ou "-") d'une mesure homodyne continue sera détaillée à la section suivante. Pour le moment, nous admettons qu'un processus algorithmique adéquat permet d'obtenir un chiffre binaire à partir d'une mesure de variable continue (par exemple, conserver le bit de signe du résultat de mesure).

Pour qu'une expérience de test de la physique quantique face aux théories réalistes et locales soit recevable, il suffit qu'elle induise une violation d'une certaine inégalité de Bell dans une configuration expérimentale particulière [173]. Nous avons choisi d'étudier l'inégalité de Clauser-Horne-Shimony-Holt (CHSH) [167], qui est celle la plus fréquemment utilisée en optique quantique. Dans notre approche de test avec des variables continues, il faut préciser qu'aucune opération de post-sélection des données n'est effectuée : toutes les mesures, correspondant à toutes les impulsions signal sont utilisées. Aucune hypothèse supplémentaire n'est alors nécessaire pour interpréter notre dispositif [167]. Dans ces conditions, l'inégalité CHSH, qui doit être vérifiée par toute théorie (classique) locale et réaliste, s'écrit :

$$S = |E(a', b') + E(a', b) + E(a, b') - E(a, b)| \quad \leq 2 \tag{11.4}$$

où $E(a,b)$ est la fonction de corrélation des mesures. Cette dernière est définie par :

$$E(a,b) = P_{++}(a,b) + P_{--}(a,b) - P_{+-}(a,b) - P_{-+}(a,b) \tag{11.5}$$

où $P_{++}(a,b)$ est la probabilité conjointe qu'un résultat "+" soit obtenu en A et en B, conditionnellement aux ajustements a et b.

Ayant choisi l'inégalité de Bell-CHSH et un dispositif expérimental de mesure (détections homodynes et binarisation de toutes les données), il nous reste à choisir la forme de l'état quantique particulier à étudier. Nous avons retenu une superposition de deux fonctions d'onde à deux modes :

$$\boxed{|\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|ff\rangle + e^{\imath\theta}|gg\rangle\Big)} \tag{11.6}$$

avec $\theta \in [0, 2\pi]$ et en supposant que f est une fonction réelle, *paire* et normalisée à 1, tandis que g est supposée réelle, *impaire* et normalisée à 1. Ce type d'état est voisin de celui étudié par l'équipe d'Auberson [186], mais les fonctions f et g que nous utiliserons dans la section 11.2 ainsi que la binarisation des variables continues seront très différentes.

11.1.2 Binarisation des mesures

Pour exploiter les inégalités de Bell classiques (CHSH, CH ...), il faut disposer de données binaires, et donc convertir les résultats continus des mesures homodynes en chaînes de bits. Ainsi, chaque mesure de quadrature doit être classifiée selon "+" ou "-". Pour cette procédure, la binarisation la plus couramment utilisée consiste en un découpage "positif-négatif" suivant le signe de la mesure [184, 185, 186]. Le choix du découpage est ici totalement arbitraire, du moment que toutes les mesures sont classées. Pour l'état décrit par (11.6), nous choisissons d'introduire un autre découpage appelé découpage par tranches (*Root Binning*) qui est basé sur les racines des fonctions f et g. Le résultat "+" est assigné aux mesures x pour lesquelles $f(x)$ et $g(x)$ possèdent le même signe, tandis que la valeur "-" concerne les mesures pour lesquelles $f(x)$ et $g(x)$ sont de signes opposés. Ce découpage est bien sûr connu par avance des expérimentateurs en A et B.

En termes mathématiques, nous introduisons les domaines D^+ et D^- comme les unions des intervalles où $f(x)$ et $g(x)$ possèdent respectivement un signe identique ou opposé :

$$D^+ = \{\ x\ \in\ \mathbb{R}\ |\ f(x)\ g(x)\ \geq\ 0\} \tag{11.7a}$$
$$D^- = \{\ x\ \in\ \mathbb{R}\ |\ f(x)\ g(x)\ <\ 0\} \tag{11.7b}$$

Comme les fonctions sont réelles, normalisées à 1 et de parités différentes, le produit $f\,g$ est une fonction impaire et on a nécessairement les propriétés suivantes :

$$\int_{D^+} f(x)^2\,dx = \int_{D^-} f(x)^2\,dx = \int_{D^+} g(x)^2\,dx = \int_{D^-} g(x)^2\,dx = \frac{1}{2} \tag{11.8}$$

$$\int_{D^+} f(x)\,g(x)\,dx = -\int_{D^-} f(x)\,g(x)\,dx \tag{11.9}$$

L'intérêt de ce découpage est que l'inégalité de Bell CHSH (11.4) prend alors une forme particulièrement simple du fait des parités imposées pour les fonctions f et g. Pour exprimer la quantité S, nous allons calculer les différentes fonctions de corrélations E dans (11.4) lorsque des mesures des quadratures X ou P sont effectuées. Dans un premier temps, nous considérons par

exemple qu'une mesure de la quadrature X a été effectuée des deux côtés A et B. La densité de probabilité conjointe pour les mesures de quadratures s'écrit :

$$\begin{aligned} \Pr(x_A, x_B) &= |\langle x_A|\langle x_B|\Psi\rangle|^2 \\ &= \frac{1}{2}\left[f(x_A)^2\, f(x_B)^2 + g(x_A)^2\, g(x_B)^2 + 2\,\cos\theta\, f(x_A)\, g(x_A)\, f(x_B)\, g(x_B)\right] \end{aligned} \tag{11.10}$$

Cette équation permet d'exprimer les probabilités binaires nécessaires pour calculer $E(x_A, x_B)$ selon :

$$P_{i\,j}(x_A, x_B) = \int_{D^i}\int_{D^j} \Pr(x_A, x_B)\, dx_A\, dx_B \tag{11.11}$$

où $i, j \in \{+, -\}$. Grâce à la propriété (11.8), on obtient :

$$P_{i\,j}(x_A, x_B) = \frac{1}{4} + \cos\theta \int_{D^i} f(x_A)\, g(x_A)\, dx_A \int_{D^j} f(x_B)\, g(x_B)\, dx_B \tag{11.12}$$

Il est ici utile d'introduire la quantité V :

$$V = \int_{D^+} f(x)g(x)dx - \int_{D^-} f(x)g(x)dx = \int_{-\infty}^{+\infty} |f(x)g(x)|dx \tag{11.13}$$

Compte tenu de (11.9) et de la définition des domaines D^+,D^-, nous pouvons exprimer les probabilités binaires [2] :

$$P_{++}(x_A, x_B) = P_{--}(x_A, x_B) = \frac{1}{4} + \frac{V^2}{4}\cos\theta \tag{11.14a}$$

$$P_{+-}(x_A, x_B) = P_{-+}(x_A, x_B) = \frac{1}{4} - \frac{V^2}{4}\cos\theta \tag{11.14b}$$

L'expression de la fonction de corrélation $E(x_A, x_B)$ est alors très simple :

$$E(x_A, x_B) = P_{++} + P_{--} - P_{+-} - P_{-+} = V^2\cos\theta \tag{11.15}$$

Un découpage similaire peut être appliqué pour les quadratures P. Comme nous supposons que $f(x)$ est une fonction réelle et paire, sa transformée de Fourier $\tilde{f}(p)$ est également réelle et paire. Dans le cas de la fonction g réelle et impaire, sa transformée de Fourier est imaginaire pure $\imath\tilde{h}(p)$ et $\tilde{h}(p)$ est une fonction réelle et impaire. En utilisant ces propriétés et en prenant garde au facteur $\imath$ supplémentaire, le même raisonnement que précédemment s'applique pour $\tilde{f}$, $\tilde{h}$ que pour f, g. Nous introduisons la quantité W :

$$W = \int_{\widetilde{D}^+} \tilde{f}(p)\tilde{h}(p)dp - \int_{\widetilde{D}^-} \tilde{f}(p)\tilde{h}(p)dp = \int_{-\infty}^{+\infty} |\tilde{f}(p)\tilde{h}(p)|dp \tag{11.16}$$

Les probabilités pour des mesures conjointes de la quadrature P en A et B s'expriment alors par :

$$P_{++}(p_A, p_B) = P_{--}(p_A, p_B) = \frac{1}{4} - \frac{W^2}{4}\cos\theta \tag{11.17a}$$

$$P_{+-}(p_A, p_B) = P_{-+}(p_A, p_B) = \frac{1}{4} + \frac{W^2}{4}\cos\theta \tag{11.17b}$$

[2] On peut par ailleurs vérifier $P_+ = P_- = 1/2$: l'indéterminisme est parfait pour les mesures de chaque station.

La fonction de corrélation associée s'écrit :

$$E(p_A, p_B) = -W^2 \cos\theta \tag{11.18}$$

Enfin, de manière équivalente pour des mesures de quadratures différentes :

$$P_{++}(x_A, p_B) = P_{--}(x_A, p_B) = P_{++}(p_A, x_B) = P_{--}(p_A, x_B) = \frac{1}{4} - \frac{VW}{4}\sin\theta \tag{11.19a}$$

$$P_{+-}(x_A, p_B) = P_{-+}(x_A, p_B) = P_{+-}(p_A, x_B) = P_{-+}(p_A, x_B) = \frac{1}{4} + \frac{VW}{4}\sin\theta \tag{11.19b}$$

$$E(x_A, p_B) = E(p_A, x_B) = -V\,W\,\sin\theta \tag{11.20}$$

En combinant les équations (11.15), (11.18) et (11.20), l'inégalité de Bell CHSH (11.4) se réécrit :

$$S = |\cos\theta(V^2 + W^2) - 2\sin\theta V\,W| \leq 2 \tag{11.21}$$

Le maximum de S en fonction de la phase θ est obtenu pour $\tan\theta_{\rm m} = -2VW/(V^2+W^2)$, avec $\theta_{\rm m} \to -\pi/4$ lorsque $V, W \to 1$. Pour la phase optimale $\theta_{\rm m}$, l'inégalité CHSH prend finalement la forme simple suivante :

$$\boxed{S = |\sqrt{W^4 + V^4 + 6\,V^2\,W^2}| \leq 2} \tag{11.22}$$

En conséquence, la validation de la physique quantique face aux théories locales et réalistes peut se réduire à trouver des fonctions f et g convenables dont les intégrales V, W violent l'inégalité (11.22) [3]. En comparaison avec la binarisation "positive-négative", notre décomposition par tranches offre l'avantage de présenter deux paramètres variables V et W au lieu d'un seul [186]. Ceci permet notamment de trouver des états physiques présentant une violation de l'inégalité CHSH en évitant les pathologies mathématiques présentes dans [186], comme nous allons le voir à la section suivante.

11.2 Choix des états quantiques

Pour obtenir une violation de l'inégalité CHSH avec des mesures homodynes et une binarisation par tranches, il suffit de choisir de manière adéquate les fonctions f et g définissant l'état à deux modes (11.6). Nous proposons ici une famille complète d'états *physiques* qui induisent une violation maximale de l'inégalité CHSH, montrant qu'il est possible d'atteindre ce seuil avec des variables continues sans avoir recours à des fonctions d'ondes présentant de fortes singularités.

11.2.1 Tests avec des états simples

Pour commencer notre recherche des fonctions f et g, le plus intuitif est de considérer un état $|\Psi\rangle$ de la forme :

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + e^{\imath\theta_{\rm m}}|11\rangle\Big) \tag{11.23}$$

où la fonction d'onde (paire) ψ_0 associée à l'état vide $|0\rangle$ joue le rôle de f, tandis que g est prise égale à la fonction d'onde (impaire) ψ_1 associée au photon unique $|1\rangle$. Dans ce cas, la

[3] Un cas particulièrement intéressant intervient lorsque les distributions f et g sont des fonctions propres de la transformée de Fourier, auquel cas $V = W$ et l'équation (11.22) devient $S = 2\sqrt{2}\,V^2$. Si de plus les fonctions possèdent le recouvrement optimum pour obtenir $V = 1$, la violation de l'inégalité CHSH sera maximale avec $S = 2\sqrt{2}$ [181].

binarisation par tranches équivaut à un découpage simple "positif-négatif". Les fonctions sont ici des opérateurs propres de le transformée de Fourier, ce qui permet de calculer $V = W \approx 0.80$. Ce recouvrement n'est malheureusement pas suffisant pour obtenir une violation de l'inégalité CHSH, alors que la formule (11.22) donne $S \approx 1.80 < 2$. De la même manière, aucune violation d'une inégalité de Bell n'a pu être obtenue avec des états du type :

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + e^{i\theta_{\mathrm{m}}}|nn\rangle\right) \tag{11.24}$$

avec n entier [4].

Parmi les états usuels en optique quantique de fonction de Wigner négative, on peut s'intéresser au cas d'un état "chat de Schrödinger", formé d'une superposition de deux états cohérents d'amplitudes a et $-a$. Nous considérons donc un chat pair pour f et un chat impair pour g [5] :

$$f_2(x) \propto e^{-(x+a)^2/2} + e^{-(x-a)^2/2} \tag{11.25a}$$
$$g_2(x) \propto -e^{-(x+a)^2/2} + e^{-(x-a)^2/2} \tag{11.25b}$$

Avec ces définitions, nous obtenons un excellent recouvrement en x : $V = 1$, mais le recouvrement des fonctions d'onde pour la quadrature P est moins bon : $W \approx 0.64$ pour $a \to \infty$, de sorte que $S \approx 1.90 < 2$. L'état (11.6) formé de chats de Schrödinger simples ne permet donc pas d'obtenir une violation de l'inégalité CHSH (Gilchrist [183, 184] étudie également des chats de Schrödinger, mais sans obtenir de violation d'inégalités de Bell).

11.2.2 Chats de Schrödinger à 4 pattes

Si des états "simples" ne permettent pas d'obtenir une violation de l'inégalité (11.22), nous pouvons – du moins en théorie – manipuler des états quantiques plus exotiques, mais qui conservent toutefois leur sens d'états physiques. La question principale qui nous motive ici est de déterminer les limites des possibilités de test des inégalités de Bell en mesurant des composantes continues de quadrature. Au lieu de chats de Schrödinger pouvant être vivants ou morts, nous considérons des chats dans une superposition de quatre états physiologiques différents ("chats à 4 pattes") :

$$f_4(x) \propto -e^{-(x+3a)^2/2} + e^{-(x+a)^2/2} + e^{-(x-a)^2/2} - e^{-(x-3a)^2/2} \tag{11.26a}$$
$$g_4(x) \propto -e^{-(x+3a)^2/2} - e^{-(x+a)^2/2} + e^{-(x-a)^2/2} + e^{-(x-3a)^2/2} \tag{11.26b}$$

Ces fonctions d'ondes ainsi que leurs transformées de Fourier sont tracées sur la figure 11.2. Pour ces définitions, chaque pic dans la représentation X est distant de ses voisins de $\alpha = 2a$. Cette configuration permet un meilleur recouvrement des fonctions $\tilde{f}$ et $\tilde{h}$ et donc une plus forte valeur du paramètre S. La meilleure violation apparaît lorsque l'amplitude a tend vers l'infini, auquel cas $V = 1$ et $W \approx \frac{8}{3\pi}$. Ceci fournit $S \approx 2.417 > 2$, soit une violation de près de 21% de l'inégalité CHSH. La condition $a \to \infty$ n'est en fait pas contraignante : une amplitude limitée à $a = 5$ est suffisante numériquement pour obtenir $S \approx 2.417$. Une telle violation constitue une

[4] Le raisonnement mené à la section 11.1 s'applique également pour un état du type $|\Psi\rangle = 1/\sqrt{2}\left(|fg\rangle + e^{i\theta}|gf\rangle\right)$, ce qui permet d'exclure de notre étude des états $1/\sqrt{2}\left(|01\rangle + e^{i\theta}|10\rangle\right)$.

[5] Le choix de la normalisation N_0 n'a que peu d'influence ici. Pour alléger les notations, nous donnons les valeurs numériques pour la convention $N_0 = 1/2$, les autres conventions s'en déduisant par un simple changement d'échelle.

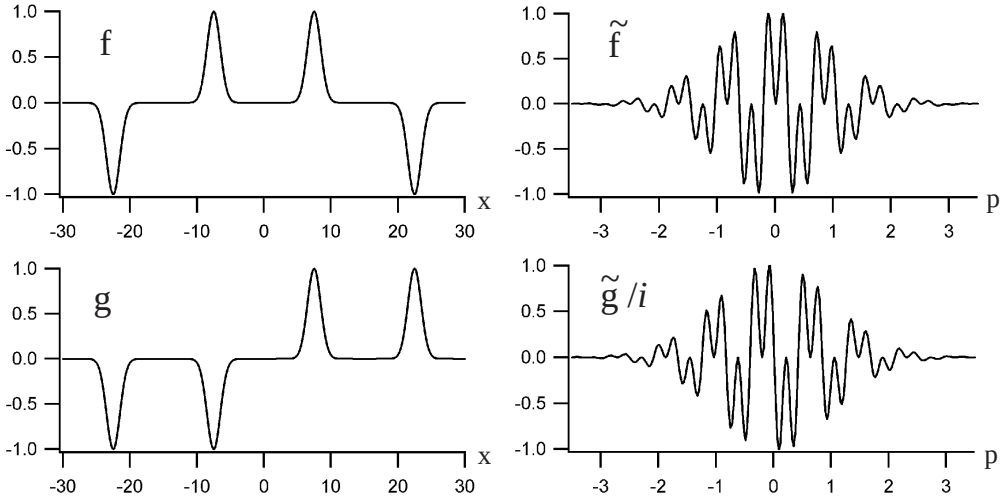

Figure 11.2: *Fonctions d'ondes f_4 et g_4 pour un chat à 4 pattes défini par les équations (11.26) pour la quadrature X (gauche) et la quadrature P (droite), avec $\alpha = 15$ et la convention $N_0 = 1/2$. Les axes verticaux sont en unités arbitraires. La violation obtenue pour l'état (11.6) défini avec ces fonctions est de $S = 2.417$.*

nette amélioration par rapport au meilleur résultat précédent obtenu par Munro avec $S = 2.076$ [185], alors que notre état ne présente aucune singularité mathématique. Cependant, la violation obtenue ici demeure éloignée de la valeur maximale $S = 2\sqrt{2}$ autorisée par la physique quantique [181].

11.2.3 Généralisation : chats de Schrödinger à N pattes

Les résultats obtenus avec les chats à deux et à quatre pattes suggèrent qu'une manière d'augmenter la violation calculée est de considérer un nombre de pattes plus important. Nous généralisons le choix des fonctions chats f et g au cas de N pattes, pour un certain écartement d'amplitude α entre les pics :

$$f_N(x) \propto \sum_{j=-\frac{N}{2}}^{\frac{N}{2}-1} \cos\left(\frac{\pi}{4}[2j+1]\right) e^{-\frac{1}{2}\left(x-[j+\frac{1}{2}]\alpha\right)^2} \tag{11.27a}$$

$$g_N(x) \propto \sum_{j=-\frac{N}{2}}^{\frac{N}{2}-1} \sin\left(\frac{\pi}{4}[2j+1]\right) e^{-\frac{1}{2}\left(x-[j+\frac{1}{2}]\alpha\right)^2} \tag{11.27b}$$

Avec ces définitions, le signe est alterné tous les deux pics, ce qui permet de meilleurs recouvrements V et W. La figure 11.3 présente les résultats du calcul numérique de la violation S en fonction du nombre total de pics N. Dès que $N \geq 4$, l'inégalité CHSH est violée suivant une proportion qui augmente avec N.

Pour comprendre cet effet, nous considérons la limite $N \to \infty$, en définissant les distributions suivantes, présentées sur la figure 11.4 (le terme sinusoïdal sert à donner le signe adéquat aux

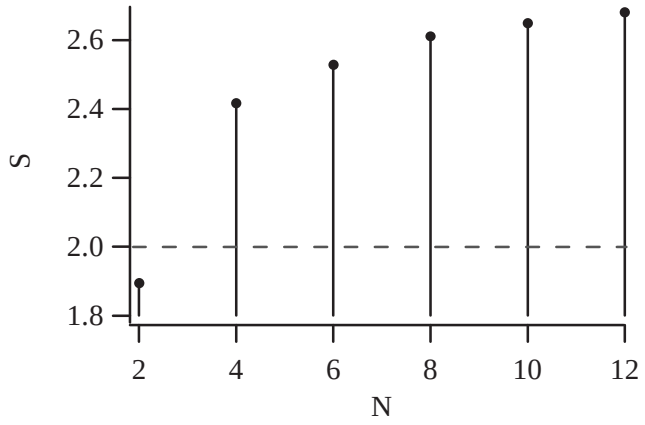

Figure 11.3: *Violation S calculée pour des états chats de Schrödinger à N pattes définis par les équations (11.6) et (11.27), et pour un écartement en amplitude de* $\alpha = 15$*, chaque pic ayant la même hauteur.*

différents pics) :

$$f_{\infty,\alpha}(x) \propto \sum_{j=-\infty}^{+\infty} \delta(x - \alpha[j+1/2]) \ \cos\left(\frac{\pi x}{2\alpha}\right) \tag{11.28a}$$

$$g_{\infty,\alpha}(x) \propto \sum_{j=-\infty}^{+\infty} \delta(x - \alpha[j+1/2]) \ \sin\left(\frac{\pi x}{2\alpha}\right) \tag{11.28b}$$

Les fonctions ci-dessus sont le produit d'un peigne de Dirac de période α par une sinusoïde de période 4α. Leurs transformées de Fourier seront alors des peignes de Dirac de période $2\pi/\alpha$, convolués par des pics de Dirac introduisant des translations de $\pm 2\pi/(4\alpha)$, comme l'indique la figure 11.4. Pour notre définition particulière de l'alternance des signes des pics, il est alors facile de montrer que ces fonctions sont à un facteur d'échelle près identiques à leurs transformées de Fourier (dans le cas particulier d'une amplitude $\alpha = \sqrt{\pi}$, elles en sont rigoureusement des fonctions propres). Le recouvrement de f_∞, g_∞ ainsi que de $\tilde{f}_\infty$, $\tilde{h}_\infty$ étant optimum, les intégrales V et W valent 1, ce qui permet d'atteindre la violation maximale $S = 2\sqrt{2}$ d'après (11.22). Bien que ces états ne soient pas normalisables, et donc ne représentent pas des fonctions d'ondes physiques, les distributions f_N et g_N définies par (11.27) peuvent néanmoins se comprendre comme des régularisations de f_∞ et g_∞ en prenant des gaussiennes de largeur finie à la place des pics de Dirac et en tronquant le nombre de pics. Ceci indique clairement que pour nos définitions $S \to 2\sqrt{2}$ lorsque $N \to \infty$.

Une autre régularisation des fonctions peignes (11.28) consiste à élargir chaque pic de Dirac en une gaussienne de largeur s, et à imposer une enveloppe gaussienne de largeur $1/s$ pour les amplitudes des pics :

$$f_{\infty,\alpha,s}(x) \propto G_{1/s}(x)\,[f_{\infty,\alpha} * G_s](x) \tag{11.29a}$$

$$g_{\infty,\alpha,s}(x) \propto G_{1/s}(x)\,[g_{\infty,\alpha} * G_s](x) \tag{11.29b}$$

où $G_s(x) = \exp(-\frac{x^2}{2s^2})$ est une gaussienne de largeur $s < 1$ (de transformée de Fourier gaussienne de largeur $1/s$), et $*$ désigne le produit de convolution. Ces fonctions sont dès lors normalisables,

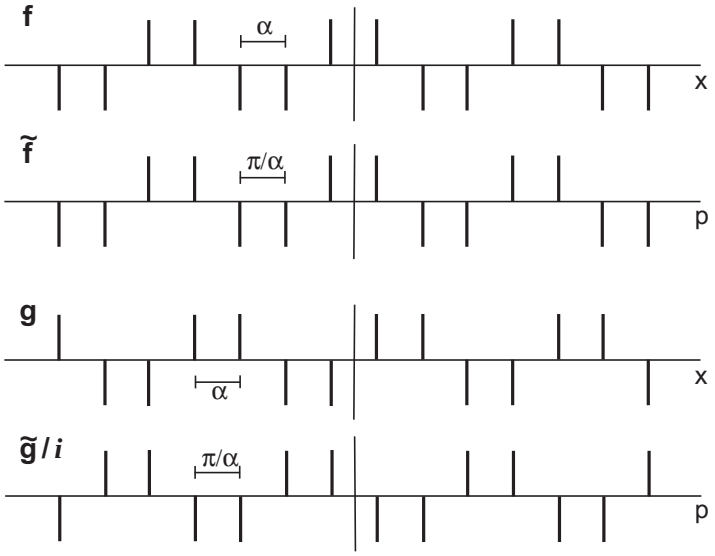

Figure 11.4: *Distributions généralisées f_∞ et g_∞ dans les espaces position et impulsion. Les segments représentent des pics de Dirac. La violation obtenue pour l'état (11.6) défini avec ces fonctions est de $S = 2\sqrt{2}$*

et représentent donc un état physique selon la définition (11.6). Si le recouvrement des fonctions d'ondes en X est optimal $V = 1$, il faut vérifier la condition $W > 0.68$ du recouvrement des fonctions d'ondes en P pour obtenir une violation de l'inégalité CHSH (11.22). Cette condition sur W impose de choisir convenablement l'amplitude α des états. Les transformées de Fourier des fonctions (11.29) s'écrivent alors :

$$\widetilde{f}_{\infty,\alpha,s}(p) \quad \propto \quad G_s * [f_{\infty,\pi/\alpha}\, G_{1/s}](p) \tag{11.30a}$$

$$\widetilde{h}_{\infty,\alpha,s}(p) \quad \propto \quad G_s * [g_{\infty,\pi/\alpha}\, G_{1/s}](p) \tag{11.30b}$$

Pour $s \ll 1$, la multiplication et la convolution dans les équations ci-dessus sont quasiment associatives, auquel cas les approximations $\widetilde{f}_{\infty,\alpha,s}(p) \approx f_{\infty,\pi/\alpha,s}(p)$ et $\widetilde{h}_{\infty,\alpha,s}(p) \approx -g_{\infty,\pi/\alpha,s}(p)$ sont valables. En particulier, on retrouve que pour l'amplitude spécifique $\alpha = \sqrt{\pi}$ les fonctions f et g sont approximativement des fonctions propres de la transformée de Fourier, ce qui permet d'atteindre $W \approx 1$ et une violation maximale $S \approx 2\sqrt{2}$. Par ailleurs, la violation S présente une symétrie $S(\alpha) = S(\frac{\pi}{\alpha})$ autour de son maximum $\alpha = \sqrt{\pi}$.

Grâce à l'enveloppe gaussienne dans (11.29), les fonctions peignes $f_{\infty,\alpha}$ et $g_{\infty,\alpha}$ peuvent être tronquées à une nombre fini N de pics sans affecter significativement les allures numériques des fonctions d'ondes. Pour cela, il faut satisfaire la condition suivante sur N, α et s, qui traduit le fait que l'amplitude des derniers pics doit être plus petite qu'un paramètre ε :

$$N > \frac{2\sqrt{2|\ln \varepsilon|}}{\alpha s} \tag{11.31}$$

Avec les conditions typiques $\varepsilon = 0.01$, $\alpha = \sqrt{\pi}$ et $s = 0.3$, la condition ci-dessus fixe le nombre de pics minimum à $N = 12$. En d'autres termes, pour cette configuration avec $N \geq 12$, les fonctions (11.29) sont une bonne régularisation numérique des peignes (11.28), tout en conservant leurs propriétés de forte violation S. Ce résultat théorique est confirmé par un calcul numérique

fournissant $S \approx 2\sqrt{2}$ avec une erreur relative de 0.01% pour les conditions $\alpha = \sqrt{\pi}$, $s = 0.3$ et $N = 12$. Les fonctions d'ondes correspondantes, tracées sur la figure 11.5, donnent explicitement un état *physique* offrant une violation maximale de l'inégalité CHSH lors des mesures homodynes.

Indépendamment de la condition (11.31) sur le nombre N de pics dans les fonctions régularisées (11.29), nous pouvons choisir de limiter arbitrairement ce nombre à une valeur finie, étant donnés les paramètres α et s. Cependant, alors que les fonctions tronquées à N ne peuvent plus être considérées comme des régularisations immédiates de $f_{\infty,\alpha}$ et $g_{\infty,\alpha}$, la meilleure amplitude α va différer de $\sqrt{\pi}$ tandis que la violation optimale S sera légèrement plus faible. Les résultats de calculs numériques pour $s = 0.3$ fixé et N variant de 4 à 12 sont présentés dans le tableau 11.1, montrant la quantité S ainsi que l'amplitude optimale α_{opt} de violation. Grâce à la régularisation gaussienne (11.29), les résultats sont ici considérablement améliorés par rapport au cas de la figure 11.3 où tous les pics possèdent la même amplitude, avec par exemple $S = 2.764$ pour $N = 4$ au lieu de $S < 2.417$ pour les fonctions f_4, g_4.

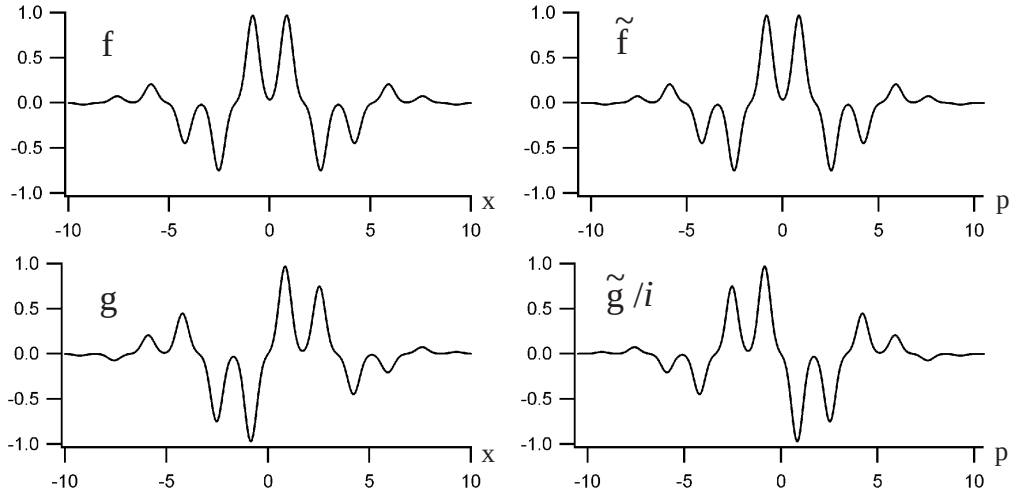

Figure 11.5: *Fonctions d'ondes f et g pour un chat à 12 pattes et une enveloppe gaussienne défini par les équations (11.29) pour la quadrature X (gauche) et la quadrature P (droite), avec $\alpha = \sqrt{\pi}$ et $s = 0.3$. Les axes verticaux sont en unités arbitraires. La violation obtenue pour l'état (11.6) défini avec ces fonctions est de $S \approx 2\sqrt{2}$*

N	4	6	8	10	12
α_{opt}	2.6	2.3	2	1.8	1.8
S	2.764	2.823	2.826	2.828	2.828

Tableau 11.1: *S en fonction du nombre de pics N pour les définitions (11.29) des fonctions d'ondes normalisées, avec un paramètre $s = 0.3$ et pour une amplitude α_{opt} optimisée numériquement.*

11.2.4 D'autres possibilités d'états

Il est particulièrement intéressant d'étudier la décomposition des états $|f\rangle$ et $|g\rangle$ sur la base de Fock $|n\rangle$. Partant des chats de Schrödinger à N pattes d'enveloppe gaussienne (11.29) avec

$\alpha = \sqrt{\pi}$, $s = 0.4$ et N satisfaisant la condition (11.31), nous avons obtenu en prenant en compte les termes jusqu'au 14^e ordre :

$$|f\rangle = \sqrt{0.459}\,|0\rangle - \sqrt{0.491}\,|4\rangle - \sqrt{0.008}\,|8\rangle - \sqrt{0.042}\,|12\rangle \quad (11.32a)$$

$$|g\rangle = \sqrt{0.729}\,|1\rangle + \sqrt{0.155}\,|5\rangle - \sqrt{0.107}\,|9\rangle - \sqrt{0.009}\,|13\rangle \quad (11.32b)$$

Ces états permettent d'atteindre une violation de $S = 2.81$. Il apparaît que l'état $|f\rangle$ ne contient que des termes $n \equiv 0\ (mod\ 4)$ tandis que $n \equiv 1\ (mod\ 4)$ pour $|g\rangle$. Ceci s'explique par le fait que $\langle p|n\rangle = (-i)^n \langle x|n\rangle_{x=p}$ et $(-i)^4 = 1$, de telle sorte que des états $\sum_k c_k |n_0 + 4k\rangle$ sont des états propres de la transformée de Fourier, ce qui est exactement une des propriétés recherchées pour les états $|f\rangle$ et $|g\rangle$. Grâce à cet éclairage nouveau, nous avons pu obtenir une violation de $S = 2.68$ pour

$$|f\rangle = \sqrt{0.585}\,|0\rangle - \sqrt{0.415}\,|4\rangle \qquad |g\rangle = \sqrt{0.848}\,|1\rangle + \sqrt{0.152}\,|5\rangle \quad (11.33)$$

et $S = 2.3$ pour

$$|f\rangle = \sqrt{0.67}\,|0\rangle - \sqrt{0.33}\,|4\rangle \qquad |g\rangle = |1\rangle \quad (11.34)$$

Ces états sont relativement simples, et ont motivé l'étude [196] de Jaromir Fiurášek et ses collaborateurs pour concevoir un processus de génération conditionnelle de tels états. Il est à noter que ce dispositif se généralise au cas d'états intriqués de la forme (11.6) dont les états $|f\rangle$ et $|g\rangle$ possèdent des décompositions arbitraires dans la base de Fock.

11.3 Discussions

Cette section détaille différents points ayant trait aux états chats de Schrödinger intriqués introduits à la section précédente : méthode de préparation, influence des pertes et tests d'autres inégalités de Bell (le lecteur peu intéressé par ces détails assez techniques pourra avantageusement passer à la section 11.4).

11.3.1 Préparation conditionnelle des chats intriqués à N pattes

La génération de chats de Schrödinger à N pattes est une tâche particulièrement délicate. Nous proposons ici une méthode de préparation des états définis par les équations (11.27). Compte tenu de la fragilité expérimentale de tels états face au phénomène de décohérence, notre démarche n'est pas de proposer une expérience faisable, mais d'attester de l'aspect physique de nos états en proposant explicitement une procédure de génération. Nous nous concentrerons donc sur la génération de chats intriqués, sans considérer la faisabilité du dispositif à plus ou moins long terme.

Les états utilisés présentent de fortes analogies avec les *encoded states* introduits par Gottesman et Preskill [191] pour effectuer des codes quantiques correcteurs d'erreurs. Récemment, Travaglione et Milburn ont présenté une procédure pour générer de manière non-déterministe de tels états [192]. En s'inspirant de ces études, nous proposons un protocole de génération de l'état $|g_N\rangle$ à N pattes défini par (11.27), puis une technique pour produire l'état complet (11.6).

Génération de l'état $|g_N\rangle$

La procédure débute avec le mode signal dans l'état vide $|0\rangle$ et un qubit auxiliaire $|0\rangle_{aux}$ (si on souhaite utiliser un paramètre de compression $s \neq 1$, il suffit de débuter cette procédure avec

un vide comprimé à la place du vide signal). Une étape de préparation consiste à appliquer l'opérateur :

$$H_{aux}\ e^{-\imath\,\alpha\,\hat{p}\,\sigma_{z,aux}}\ H_{aux} \tag{11.35}$$

où $\hat{p}$ est l'opérateur impulsion appliqué à l'état signal ($\hat{D}(\alpha) = e^{-\imath\alpha\hat{p}}$ est l'opérateur déplacement suivant X de l'amplitude α). H_{aux} et $\sigma_{z,aux}$ sont respectivement les opérateurs de Hadamard et de Pauli appliqués au qubit auxiliaire, définis par :

$$H_{aux} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \sigma_{z,aux} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{11.36}$$

L'opérateur de préparation permet de générer une superposition d'états cohérents déplacés conditionnellement par rapport à la valeur du qubit :

$$H_{aux}\ e^{-\imath\,\alpha\,\hat{p}\,\sigma_{z,aux}}\ H_{aux}\,|0\rangle|0\rangle_{aux} \propto (|-\alpha\rangle + |\alpha\rangle)\ |0\rangle_{aux} + (-|-\alpha\rangle + |\alpha\rangle)\ |1\rangle_{aux} \tag{11.37}$$

Le qubit est alors dans l'état fondamental ou dans l'état excité avec une probabilité $1/2$. S'il est projeté dans l'état $|1\rangle_{aux}$, alors le mode signal se trouve dans $|\Upsilon_1\rangle \propto -|-\alpha\rangle + |\alpha\rangle$, qui sera utilisé pour la suite de la procédure. Si par contre le qubit est mesuré dans l'état $|0\rangle_{aux}$, la procédure est arrêtée et recommencée depuis le départ.

Pour la suite de la préparation, le qubit est transformé en $|0\rangle_{aux}$ (*bit-flip*), puis la séquence suivante est appliquée à l'état :

$$H_{aux}\ e^{-\imath\,2\alpha\,\hat{p}\,\sigma_{z,aux}}\ H_{aux} \tag{11.38}$$

La mesure du qubit dans l'état $|0\rangle_{aux}$ résulte en une projection de l'état signal dans $|\Upsilon_2\rangle \propto -|-3\alpha\rangle + |-\alpha\rangle - |\alpha\rangle + |3\alpha\rangle$. pour générer un nombre plus important de pics, la procédure suivante est itérée, étant donné $|\Upsilon_{n-1}\rangle$ et le qubit dans l'état $|0\rangle_{aux}$:

1. Appliquer la séquence $H_{aux}\ e^{-\imath 2^{n-1}\alpha\hat{p}\sigma_{z,aux}}\ H_{aux}$.
2. Mesurer le qubit.
3. Si le qubit est dans $|0\rangle_{aux}$, la procédure a généré $|\Upsilon_n\rangle$.
4. Sinon, la procédure est annulée et reprise au début.

Une fois que le nombre de pics est considéré comme satisfaisant, l'itération ci-dessus est arrêtée. La dernière étape pour produire $|g_N\rangle$ consiste à "dupliquer" les pics, ce qui est effectué par l'opérateur :

$$H_{aux}\ e^{-\imath\,\frac{\alpha}{2}\,\hat{p}\,\sigma_{z,aux}}\ H_{aux} \tag{11.39}$$

Si le qubit est ensuite dans l'état $|0\rangle_{aux}$, alors cette procédure a produit l'état $|g_N\rangle$ défini par l'équation (11.27), avec un nombre de pics $N = 2^{n+1}$. Cet état est produit de manière probabiliste, avec une chance de réussite théorique de $1/2^{n+1}$ (dans la dernière section de la référence [192], les auteurs considèrent la question de la mise en œuvre physique d'une telle procédure en utilisant des pièges à ions. Nous ne détaillerons pas davantage cet aspect).

Production de l'état $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|ff\rangle + e^{i\theta}|gg\rangle\right)$

La figure 11.6 présente une vue globale de la procédure de génération de l'état complet $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|ff\rangle + e^{i\theta}|gg\rangle\right)$. Le bloc Γ correspond à la méthode de production de l'état $|g_N\rangle$ que nous venons d'aborder. Notre processus est basé sur une porte CNOT qui intrique deux qubits

($|\psi\rangle_{aux} = \frac{1}{\sqrt{2}}(|11\rangle_{aux} + e^{i\theta}|00\rangle_{aux})$) [1, 2]. Chaque qubit est ensuite associé avec un état $|g_N\rangle$ à travers l'opérateur :

$$\Lambda = e^{\frac{\imath\pi}{4}\left(\frac{\hat{x}}{\alpha/2}-1\right)(1-\sigma_{z,aux})} \tag{11.40}$$

où $\hat{x}$ est l'opérateur position pour le mode de l'état $|g_N\rangle$ et $\sigma_{z,aux}$ est la matrice de Pauli appliquée au qubit. Si le qubit est à zéro, l'état $|g_N\rangle$ est inchangé. Si le qubit est à un, pour $\alpha \gg 1$, le signe d'un pic sur deux est changé, ce qui transforme l'état $|g_N\rangle$ en $|f_N\rangle$. Une fois que l'opérateur Λ a été appliqué, l'état global est :

$$e^{i\theta}\ |g_N\ g_N\ 0\ 0\rangle + |f_N\ f_N\ 1\ 1\rangle \tag{11.41}$$

Afin de décomposer les états chats des qubits, chaque qubit passe par une porte de Hadamard avant une mesure conditionnelle. Si les deux qubits sont mesurés dans l'état fondamental, le système des chats est projeté sur l'état attendu :

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|f_N f_N\rangle + e^{i\theta}|g_N g_N\rangle\right) \tag{11.42}$$

Un tel processus génère des états chats de Schrödinger à N pattes de même amplitude décrits par les équations (11.27). Le cas (11.29) d'une enveloppe gaussienne est plus délicat à produire, chaque pic devant être d'une amplitude différente, ce qui nécessite un filtrage particulier dans l'espace des phases. Bien que cette procédure paraisse totalement irréalisable avec la technologie actuelle, le but de notre démarche est de donner explicitement une procédure physique qui montre les états comme les produits de l'action de certains hamiltoniens de couplage, et non comme des fonctions mathématiques pures issues de l'espace de Hilbert.

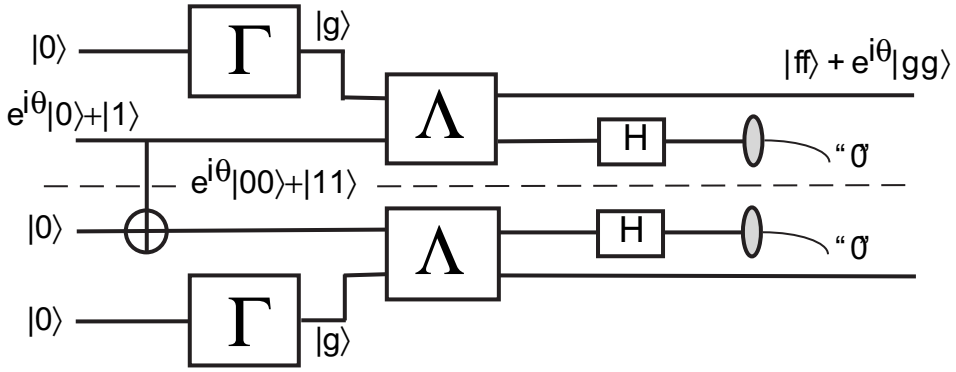

Figure 11.6: *Schéma théorique de génération de l'état* $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|ff\rangle + e^{i\theta}|gg\rangle\right)$ *avec* f *et* g *définies par les équations (11.27).* Γ *permet la génération de l'état* $|g_N\rangle$*.* Λ *transforme* $|g_N\rangle$ *en* $|f_N\rangle$ *conditionnellement au qubit auxiliaire.*

11.3.2 Influence des pertes

Nous nous proposons d'étudier l'influence des inefficacités des détecteurs A et B sur la violation mesurée de l'inégalité de Bell CHSH. Chaque station est supposée posséder la même efficacité globale de détection η_{hom} (<1), représentée par une lame de transmission η_{hom} suivie d'une détection idéale. Pour modéliser l'action des pertes sur une matrice densité arbitraire, nous

utilisons la formule (4.58) de la référence [17], appelée *transformation de Bernoulli généralisée*. Cette formule exprime la matrice densité réduite en sortie de la lame par rapport à la matrice densité entrante (une trace partielle a été effectuée sur l'autre mode de sortie de la lame) :

$$\langle m|\hat{\rho}_{out}|n\rangle = \sum_{k=0}^{\infty} \sqrt{b_n^{n+k}\, b_m^{m+k}}\, \langle m+k|\hat{\rho}_{in}|n+k\rangle \tag{11.43}$$

où b_n^{n+k} est la distribution binomiale :

$$b_n^{n+k} = C_{n+k}^n\, \eta_{hom}^n\, (1-\eta_{hom})^k = \frac{(n+k)!}{n!\,k!}\, \eta_{hom}^n\, (1-\eta_{hom})^k \tag{11.44}$$

Comme nous l'avons vu à la section 11.2.4, l'état $|f\rangle$ défini par (11.29) ne contient que des termes pairs (modulo 4) dans sa décomposition de Fock, tandis que $|g\rangle$ ne comporte que des termes impairs. D'après la formule ci-dessus, les densités de probabilité en X associées à f et g demeurent des fonctions paires, même après passage au travers de la lame (somme de carrés de fonctions paires ou impaires). Or d'après les résultats de la section 11.1, seuls les termes croisés (impairs) en $|f\rangle\langle g|$ interviennent dans l'expression de la corrélation $E = P_{++} + P_{--} - P_{+-} - P_{-+}$. Tous les termes pairs associés aux matrices densités $|f\rangle\langle f|$ et $|g\rangle\langle g|$ n'interviennent donc pas dans le calcul.

Pour exprimer la corrélation $E(x_A, x_B)$, nous nous intéressons simplement à la quantité suivante qui exprime l'influence des termes croisés $|f\rangle\langle g|$ après passage au travers de la lame :

$$\begin{aligned} O(x) &= \langle x| \left(\sum_{m,n} \sum_{k=0}^{\infty} \sqrt{b_n^{n+k}\, b_m^{m+k}}\, [\langle m+k|f\rangle\langle g|n+k\rangle]\, |m\rangle\langle n| \right) |x\rangle \\ &= \sum_{m,n} \sum_{k=0}^{\infty} \sqrt{b_n^{n+k}\, b_m^{m+k}}\, f_{m+k}\, g_{n+k}\, \varphi_m(x)\, \varphi_n(x) \end{aligned} \tag{11.45}$$

Comme les coefficients f_{m+k} et g_{n+k} sont nuls sauf si $m+k \equiv 0\ (mod\ 4)$ et $n+k \equiv 1\ (mod\ 4)$, il en résulte que $O(x)$ est une fonction impaire.

Nous reprenons alors le raisonnement poursuivi à la section 11.1, en redéfinissant les domaines D^+ et D^- compte tenu de l'efficacité limitée η_{hom} :

$$D^+ = \{\ x\ \in\ \mathbb{R}\ |\ O(x)\ \geq\ 0\} \tag{11.46a}$$

$$D^- = \{\ x\ \in\ \mathbb{R}\ |\ O(x)\ <\ 0\} \tag{11.46b}$$

Pour ce découpage par tranches, la corrélation en (x_A, x_B) devient $E(x_A, x_B) = V'^2 \cos\theta$ avec un nouveau coefficient de recouvrement :

$$V' = \int_{-\infty}^{+\infty} |O(x)|\, dx \tag{11.47}$$

Par ailleurs, l'action d'une lame partiellement réfléchissante n'altère pas l'aspect de fonction propre de la transformée de Fourier d'un état :

$$\begin{aligned} \widetilde{O}(p) &= \sum_{m,n} \sum_{k=0}^{\infty} \sqrt{b_n^{n+k}\, b_m^{m+k}}\, f_{m+k}\, g_{n+k}\, \langle p|m\rangle\langle n|p\rangle \\ &= \sum_{m,n} \sum_{k=0}^{\infty} \sqrt{b_n^{n+k}\, b_m^{m+k}}\, f_{m+k}\, g_{n+k}\, (-\imath)^m (\imath)^n \langle x|m\rangle\langle n|x\rangle \\ &= \imath\, O(x) \end{aligned} \tag{11.48}$$

avec $x = p$, $m + k \equiv 0 \ (mod\ 4)$ et $n + k \equiv 1 \ (mod\ 4)$. Donc si les fonctions f et g sont auto-transformées de Fourier et vérifient $W = V$, alors même après passage au travers des lames, on aura encore $W' = V'$. La violation s'exprime alors par $S = 2\sqrt{2}\,V'^2$ où V' est donné par la formule (11.47).

La figure 11.7 présente la violation S en fonction des efficacités η_{hom} des détections homodynes pour le cas des chats à $N = 12$ pics avec une enveloppe gaussienne produisant la violation maximale $S \approx 2\sqrt{2}$, et définis par les équations (11.6) et (11.29). Pour ces états d'allure très particulière, la violation reste relativement robuste aux pertes en permettant $S > 2$ pour des efficacités $\eta_{hom} > 73\%$.

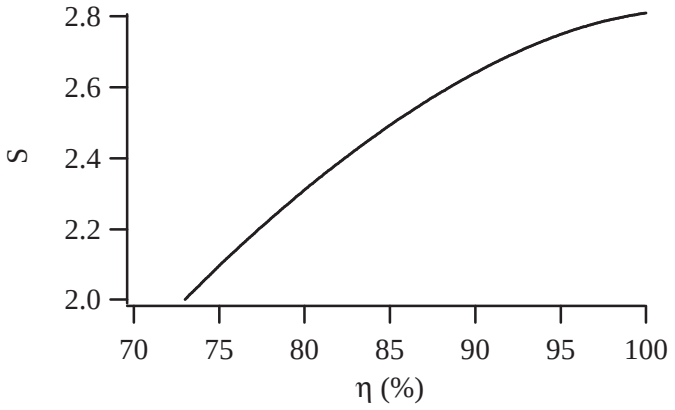

Figure 11.7: *Violation S de l'inégalité CHSH en fonction de l'efficacité limitée η_{hom} des détecteurs, pour un état défini par (11.6) et (11.29), avec $\alpha = \sqrt{\pi}$, $s = 0.4$ et $N = 12$.*

11.3.3 D'autres inégalités de Bell

Parmi les autres inégalités de Bell existant dans la littérature, la plus connue est l'inégalité de Clauser-Horne (CH) donnée par [168] :

$$S_{\mathrm{CH}} = \left| \frac{P_{++}(x_A, x_B) + P_{++}(x_A, p_B) + P_{++}(p_A, x_B) - P_{++}(p_A, p_B)}{P_{+}(p_A) + P_{+}(p_B)} \right| \leq 1 \tag{11.49}$$

Pour cette inégalité, la violation maximale autorisée par la mécanique quantique est de $S_{\mathrm{CH}} = (1 + \sqrt{2})/2$ [181]. Compte tenu de nos expressions des probabilités P_{++} obtenues à la section 11.1, le paramètre S_{CH} devient dans le cas de l'état (11.6) :

$$\begin{aligned} S_{\mathrm{CH}} &= \left| \frac{1}{2} + \frac{V^2}{4}\cos\theta + \frac{W^2}{4}\cos\theta - \frac{V\,W}{2}\sin\theta \right| \\ &= \frac{1}{4}\left| 2 + \left[(V^2 + W^2)\cos\theta - 2\,V\,W\,\sin\theta \right] \right| \end{aligned} \tag{11.50}$$

On retrouve dans cette expression la même quantité à maximiser par rapport à la variable θ que dans le cas de l'inégalité CHSH. Pour la phase optimale θ_{m}, l'équation (11.50) devient :

$$S_{\mathrm{CH}} = \frac{1}{4}\left(2 + \sqrt{V^4 + W^4 + 6\,V^2\,W^2} \right) = \frac{1}{4}\left(2 + S_{\mathrm{CHSH}} \right) \tag{11.51}$$

Dans notre cas particulier, cette dernière égalité fait apparaître qu'une violation de l'inégalité CHSH ($S_{\mathrm{CHSH}} > 2$) induit directement une violation de l'inégalité CH ($S_{\mathrm{CH}} > 1$). De plus,

une violation maximale de l'inégalité CHSH ou CH se traduit immédiatement par une violation maximale de l'autre ($S_{\mathrm{CHSH}} = 2\sqrt{2}$ est ici équivalent à $S_{\mathrm{CH}} = (1+\sqrt{2})/2$). Notre famille d'états chats de Schrödinger peut donc être étudiée de façon parfaitement équivalente par rapport à l'inégalité CHSH ou CH, et présente des comportements similaires.

D'autres formes intéressantes des inégalités de Bell utilisent le formalisme de la théorie de l'information posé par Shannon [6]. La première inégalité de Bell informationnelle a été introduite par Braunstein et Caves [193] qui exploitent une propriété des entropies de Shannon conditionnelles. Cette inégalité, qui doit être validée par toute théorie locale et réaliste, s'écrit :

$$S_{\mathrm{BC}} = H(p_A|x_B) + H(x_B|x_A) + H(x_A|p_B) - H(p_A|p_B) \geq 0 \tag{11.52}$$

où $H(x_B|x_A)$ est l'entropie conditionnelle de Shannon telle que définie par l'équation (1.4). Cette inégalité est généralisée par Cerf et Adami en utilisant les informations mutuelles de Shannon entre les chaînes de données [194] :

$$S_{\mathrm{CA}} = I(x_A, x_B) + I(p_A, x_B) + I(x_A, p_B) - I(p_A, p_B) \leq 2 \tag{11.53}$$

D'après les expressions des probabilités présentées à la section 11.1, il est facile de calculer le paramètre de test S_{BC} et de montrer que dans notre cas ces deux inégalités sont parfaitement équivalentes. Malheureusement, avec l'état défini par (11.6) et (11.29), il n'a pas été possible d'exhiber une violation des inégalités informationnelles ci-dessus en utilisant des détections homodynes et des découpages par tranches. En fait, notre dispositif fournit la borne minimale prévue par la physique classique lorsque $V \to 1$ et $W \to 1$. D'une manière similaire, Munro n'a pas pu obtenir de violation d'une inégalité informationnelle avec l'état qu'il considère [185]. Le processus de binarisation supprime une grande partie de l'information contenue dans les mesures continues, ce qui est peut-être à l'origine de l'absence de violation observée pour les inégalités informationnelles. Cet effet ne remet cependant pas en cause notre étude, la violation d'*une* inégalité de Bell dans *une* configuration particulière étant suffisante pour valider la physique quantique face aux théories à variables cachées.

11.4 Vers une expérience de test inconditionnel

Si les états chats de Schrödinger intriqués prouvent la possibilité de violation maximale des inégalités de Bell avec des variables continues mesurées par des détections homodynes [187], la mise en œuvre d'une telle expérience nécessite des outils (Hamiltoniens de couplage, portes logiques...) qui ne sont pas accessibles avec la technologie actuelle. La réalisation expérimentale d'un test complet d'une inégalité de Bell (sans échappatoires conceptuelles) demeure donc un problème ouvert.

Dans cette section, nous analysons en détails un dispositif optique faisable pour effectuer un test de Bell sans échappatoire avec des détections homodynes de fortes efficacités [188]. Ce schéma a été initialement présenté par Jaromir Fiurášek, Raoul Garcia-Patron Sanchez et Nicolas Cerf, avec qui nous collaborons actuellement sur ce sujet. Le principe de base est de produire un état non-gaussien à deux modes par un processus de dégaussification similaire à celui introduit au chapitre 9, en utilisant une paire de faisceaux EPR, des lames partiellement réfléchissantes et des détecteurs de photons uniques. Ce dispositif permet d'atteindre une violation de l'inégalité CHSH de plus de 1% avec une intrication de 6 dB et une efficacité homodyne de 95%. Les calculs correspondants ont été réalisés par Jaromir Fiurášek, Raoul Garcia-Patron Sanchez et Nicolas Cerf, et seront brièvement décrits à la section 11.4.1. Nous aborderons ensuite en détails la mise en œuvre expérimentale de ce protocole (section 11.4.2) [6].

[6] Indépendamment de notre étude, le groupe de recherche de Carmichael a très récemment proposé un dispositif

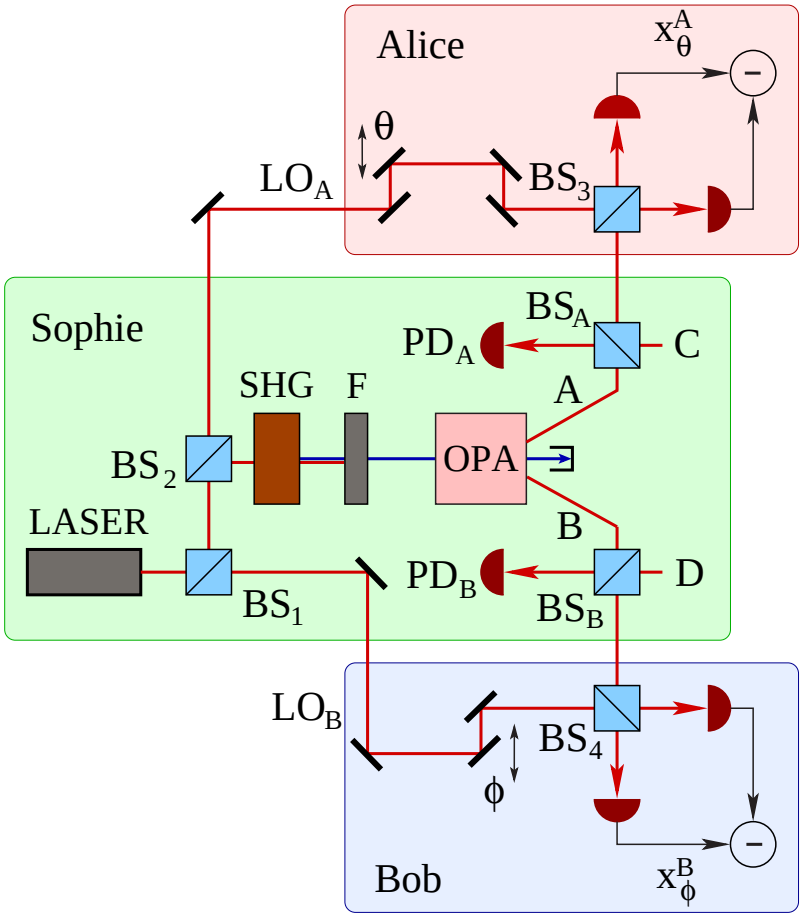

Figure 11.8: *Schéma du dispositif expérimental impulsionnel de test inconditionnel. Des photons sont soustraits des modes A et B par des lames BS_A et BS_B et des détecteurs de photons uniques PD_A et PD_B. Chaque détection homodyne (Alice, Bob) effectue une mesure résolue en temps d'une quadrature choisie indépendamment et aléatoirement entre deux possibilités.*

11.4.1 Principe du dispositif de test

Le dispositif simple présenté sur la figure 11.8 suffit à prédire une violation de l'inégalité de Bell CHSH. Ce schéma repose sur une source impulsionnelle de vide comprimé à deux modes, présentée au chapitre 10, générant l'état :

$$|\psi_{\text{in}}\rangle_{AB} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n,n\rangle_{AB} \tag{11.54}$$

où $\lambda = \tanh r$ avec r le paramètre de compression des fluctuations quantiques. Si l'état EPR (11.54) produit par fluorescence paramétrique n'est pas directement utilisable pour un test de Bell, un ensemble de lames et de photodiodes à avalanche permet de rendre facilement cet état non-gaussien. Dès lors, cet état est un candidat potentiel pour un test de la physique quantique face aux théories locales et réalistes.

de test similaire avec lequel il obtient des résultats identiques aux nôtres [189].

L'idée de base pour rendre l'état EPR non-gaussien est de soustraire un photon de chaque mode [138, 139, 140, 128], en utilisant deux lames partiellement réfléchissantes BS_A et BS_B, de réflectivité (en intensité) $R \ll 1$ et de transmission $T = 1 - R$. Le mode réfléchi par chaque lame est dirigé vers une série de filtres spatiaux et spectraux avant d'être détecté par une photodiode à avalanche en mode de comptage de photon PD_A ou PD_B. La procédure conditionnelle de dégaussification réussit lorsque deux événements de photodétection sont obtenus simultanément sur les photodiodes PD_A et PD_B. Comme dans le cas monomode du chapitre 9, l'effet de dégaussification peut facilement se comprendre à la limite des fortes transmissions des lames $T \to 1$. Dans ce cas, la cause la plus probable d'un événement de photodétection est liée à la réflexion d'un photon unique sur la lame. L'état conditionné est alors très proche d'un état pur [139] :

$$|\psi_{\mathrm{out}}\rangle_{AB} \quad \propto \quad \hat{a}_A \hat{a}_B |\psi_{\mathrm{in}}\rangle_{AB} \quad \propto \quad \sum_{n=0}^{\infty} (n+1)(T\lambda)^n |n,n\rangle_{AB} \tag{11.55}$$

La contribution des différents termes est donc modifiée, et en particulier la contribution du vide est réduite, ce qui augmente l'aspect non-classique de l'état.

Dans le principe de l'expérience proposée ici, Alice et Bob mesurent respectivement les quadratures $x_A^\theta = \cos\theta\, x_A + \sin\theta\, p_A$ et $x_B^\phi = \cos\phi\, x_B + \sin\phi\, p_B$ avec un choix entre deux phases de référence θ_1, θ_2 et ϕ_1, ϕ_2. Les données continues sont ensuite binarisées suivant un découpage simple "positif-négatif" afin de calculer le paramètre S pour l'inégalité de Bell CHSH (11.4).

Avant d'évaluer la valeur prédite par la physique quantique pour le paramètre S, nous devons clarifier le fait que le formalisme des inégalités de Bell s'applique bien à cette source conditionnelle. L'idée principale développée ici est de *pré*-sélectionner les données plutôt que de les *post*-sélectionner. Considérons trois partenaires : Alice et Bob, qui effectuent les mesures homodynes, et Sophie, qui contrôle la source (voir la figure 11.8). L'ensemble de l'analyse des données doit être effectué en régime impulsionnel, Sophie envoyant des impulsions (signal et oscillateur local) de cadence déterminée à Alice et Bob. Pour chaque impulsion, Sophie enregistre les clics de photodétection, tandis qu'Alice et Bob effectuent une mesure homodyne résolue en temps. Après un grand nombre d'impulsions échangées, seules les mesures ayant été initiées par un double clic des photodétecteurs de Sophie sont retenues. Aucune sélection n'est effectuée à partir des données d'Alice ou Bob, c'est le signal d'initialisation de Sophie qui commande. Ceci place donc notre expérience dans le formalisme des détecteurs "*event-ready*" selon John Bell [166]. Les données marquées par Sophie servent ensuite à calculer les corrélations nécessaires au paramètre S de l'inégalité CHSH.

Dans une approche réaliste et locale, des variables cachées supplémentaires μ affectent chaque impulsion et déterminent le résultat des mesures homodynes. Le point essentiel est que les systèmes d'Alice et Bob, ainsi que les détecteurs de photons de Sophie, sont tous séparés par des intervalles de genre espace, ce qui interdit toute communication entre eux [169]. En conséquence, la distribution de probabilité des variables cachées $\Pr(\mu)$ doit être indépendante des paramètres $\{\theta_{1,2},\ \phi_{1,2}\}$ choisis par Alice et Bob ainsi que des résultats s_A, s_B de leurs mesures. Cette indépendance permet alors d'écrire :

$$E(\theta_j, \phi_k) = \int \Pr(\mu)\, s_A(\theta_j, \mu)\, s_B(\phi_k, \mu)\, d\mu \tag{11.56}$$

A partir de cette relation, il est alors facile de retrouver l'inégalité CHSH $S \leq 2$ par la démonstration habituelle [167]. Ainsi, la seule hypothèse pour appliquer l'inégalité CHSH au dispositif de la figure 11.8 est le réalisme local, qui est justement le point crucial pour valider la physique quantique.

Pour l'évaluation du paramètre S selon le formalisme quantique, les détecteurs sont représentés par des détecteurs idéaux précédés de lames de transmissions respectives η_{hom} pour les détection homodynes et η pour les compteurs de photons. Il est alors possible d'exprimer la fonction de Wigner de l'état conditionné, et d'en déduire ensuite par projection les densités de probabilité des mesures en quadratures d'Alice et Bob. Le coefficient de corrélation E (et le paramètre S) peuvent ensuite être obtenus par une intégration des densités de probabilité. De plus amples détails sur ces calculs effectués par J. Fiurášek, R. Garcia-Patron Sanchez et N. Cerf sont donnés dans les références [188] et [190].

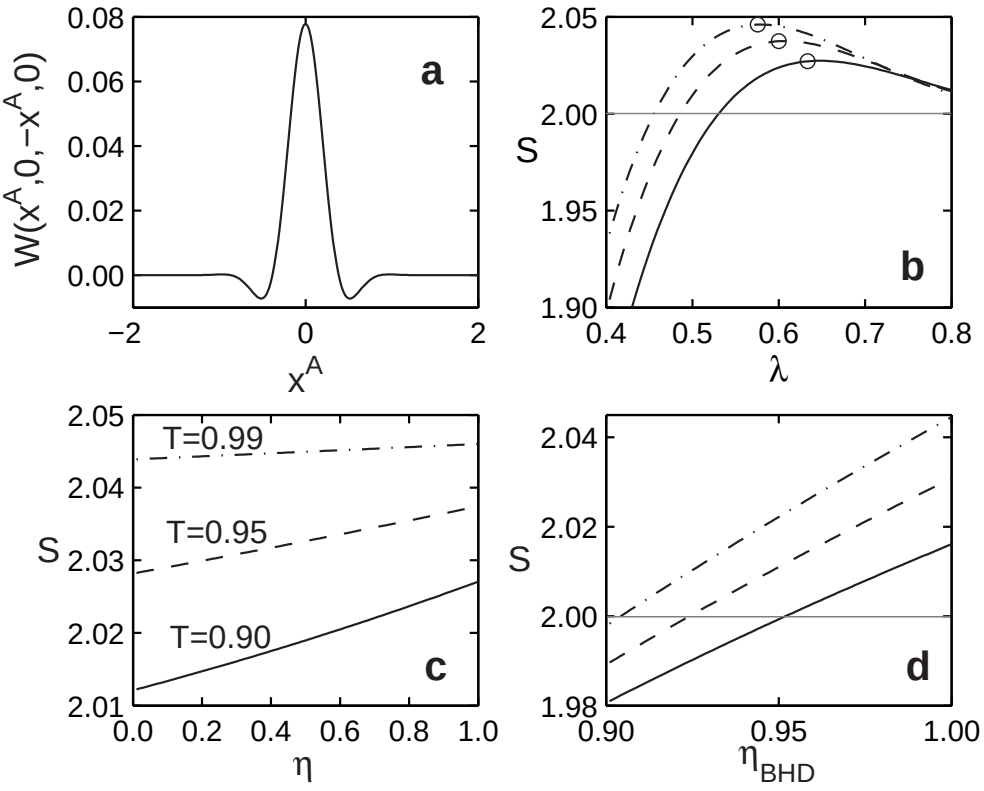

Figure 11.9: *(a) Coupe de la fonction de Wigner de l'état conditionné avec $\lambda = 0.5$, $T = 0.95$, et $\eta = 30\%$ pour la ligne $x_B = -x_A$, $p_A = p_B = 0$. (b) Paramètre de Bell S en fonction de la compression λ du faisceau EPR initial, pour des détections parfaites ($\eta = \eta_{hom} = 100\%$), avec $T = 0.9$ (trait plein), $T = 0.95$ (tirets), and $T = 0.99$ (tirets-points). Les cercles indiquent les points pour lesquels $T\lambda = 0.57$. (c) Paramètre de Bell S en fonction de l'efficacité η des compteurs de photons pour $\lambda T = 0.57$, $\eta_{hom} = 100\%$ et les mêmes transmissions qu'en (b). (d) Paramètre de Bell S en fonction de l'efficacité η_{hom} des détections homodynes pour $\lambda T = 0.57$, $\eta = 30\%$ et les mêmes transmissions qu'en (b).*

Les résultats du calcul quantique font apparaître les choix de phases optimales : $\theta_1 = 0$, $\theta_2 = \pi/2$, $\phi_1 = -\pi/4$, $\phi_2 = \pi/4$. Pour ces dispositions, la figure 11.9(a) montre que la fonction de Wigner associée à l'état conditionné est négative dans certaines régions de l'espace des phases, ce qui est une condition nécessaire pour obtenir une violation d'une inégalité de Bell avec des détections homodynes. La figure 11.9(b) montre la violation $S \geq 2$ en fonction du paramètre de compression λ, ce qui fait notamment apparaître une compression optimale $\lambda_{\rm opt}$ pour laquelle

la violation est maximale [7]. Avec notre dispositif, il est donc possible de prévoir une violation de l'inégalité CHSH. Le meilleur paramètre de Bell obtenu prédit $S \approx 2.046$, ce qui représente une violation d'environ 2.3%. Pour atteindre cette valeur, il faut une compression $\lambda \approx 0.57$, soit environ 5.6 dB, et une transmission des lames $T \approx 0.99$ aussi élevée que possible. La figure 11.9(c) montre que le paramètre de Bell S dépend relativement peu de l'efficacité η des détecteurs de photons uniques, une violation pouvant être obtenue alors même que $\eta < 10\%$. Par contre, la violation est nettement plus sensible à l'efficacité des détections homodynes η_{hom} qui doit être supérieure à 90% (voir la figure 11.9(d)).

11.4.2 Paramètres expérimentaux

Plusieurs points spécifiques doivent être pris en compte lors de la mise en œuvre expérimentale du schéma décrit à la figure 11.8. Pour le dimensionnement pratique de cette expérience future, nous nous basons sur la réalisation du protocole de dégaussification monomode présenté au chapitre 9.

Afin de verrouiller l'échappatoire de localité, les éléments d'Alice, Bob et Sophie doivent être séparés par des intervalles de genre espace. Les choix des phases de référence pour les détections homodynes doivent être effectués aléatoirement après que l'impulsion signal ait quitté la source, ce qui impose une séparation temporelle claire entre les impulsions (typiquement 1.25 μs avec notre source) ainsi qu'une modulation de phase rapide (de l'ordre de 100 ns) et aléatoire. Associée à une distance de propagation d'environ 50 m (temps de vol 150 ns), ce point devrait pouvoir être assez simplement validé avec la technologie actuelle.

Comme pour notre expérience de dégaussification monomode, le choix de la transmission T des lames de conditionnement BS_A et BS_B est crucial et répond à un compromis entre un fort taux de comptage ($T \ll 1$) et une violation plus importante (S est maximale lorsque $T \to 1$). Au premier ordre, la probabilité de succès de la préparation peut être estimée comme la probabilité d'une réflexion d'un photon sur les deux lames : $P \approx \eta^2 R^2$, qui diminue fortement lorsque $T \to 1$. Le choix optimal de la transmission T nécessitera donc une prise en considération des incertitudes statistiques des données et de la quantité de mesures à effectuer pour obtenir une violation statistiquement significative.

Paramètres techniques pour le test inconditionnel de l'inégalité CHSH	
Compression	$\lambda = 0.6$, $r = 0.69$ (-6 dB).
Transmission lames	$T = 95\%$.
Photodiode APD	Efficacité totale $\eta = 30\%$, coups d'obscurité $< 0.1/s$.
Détection homodyne	Efficacité $\eta_{hom} > 95\%$ (transmission 99%, rendement quantique photodiode 99%, adaptation de modes 98.5%), bruit électronique -20 dB.
Taux de comptage	Probabilité succès conditionnement $P \approx \eta^2 R^2 \approx 2.3 \times 10^{-4}$, cadence 800 kHz, taux effectif 200/s.
Violation CHSH	$S \approx 2.02$ soit environ 1%.

Nous pouvons alors donner un ensemble de paramètre expérimentaux qui devraient être atteints pour une violation inconditionnelle de l'inégalité CHSH (voir le tableau ci-dessus). Avec ces paramètres, la violation est de $S \approx 2.02$, soit environ 1%. Soulignons que pour que ce chiffre

[7] Un calcul simple fournit la relation $\lambda_{\mathrm{opt}} T \approx 0.57$, ce qui est assez correctement vérifié par les simulations numériques de la figure 11.9(b)

soit significatif, la violation doit être nettement supérieure à la précision des mesures, donnée par l'écart-type statistique δS de la violation, ce qui impose une contrainte supplémentaire sur la fiabilité de nos résultats : $\delta S \ll 0.02$ (avec une valeur de l'ordre de $\delta S = 0.004$, on observerait alors une violation de 5 écarts-types, ce qui constitue un résultat satisfaisant [170]). Avec une cadence de répétition de l'ordre de 1 MHz et une probabilité de préparation réussie de $P \approx 2.3 \times 10^{-4}$, le taux de production de données sera de quelques centaines par seconde, ce qui permet d'acquérir des données statistiquement représentatives en un temps raisonnablement court (moins d'une heure, en incluant des périodes de recalibration de la phase). Par ailleurs, les bruits électroniques doivent être maintenus aux niveaux les plus faibles. Les effets des coups d'obscurité des photodiodes à avalanche peuvent être réduits à une valeur négligeable en ne polarisant les photodiodes que dans la fenêtre temporelle d'arrivée d'une impulsion lumineuse. Pour permettre la violation indiquée, le bruit électronique de la détection homodyne doit être de 15 à 20 dB sous le bruit quantique, ce qui est atteignable avec des détections homodynes à amplificateur de charges.

Obtenir l'ensemble de ces paramètres simultanément constitue indiscutablement un défi expérimental majeur. Cependant, ces différents chiffres ont déjà été atteints séparément lors d'expériences passées. Il nous semble donc qu'un créneau expérimental est désormais ouvert pour des tests inconditionnels des inégalités de Bell avec des mesures homodynes.

11.5 Conclusion

Dans le cadre du débat entre la physique quantique et les théories réalistes et locales, nous proposons d'exploiter les composantes continues de quadrature d'impulsions lumineuses, mesurées par des détections homodynes résolues en temps. Dans ce domaine spécifique, nous prouvons dans un premier temps qu'il est possible d'obtenir une violation maximale d'une inégalité de Bell en exploitant de telles mesures homodynes avec des fonctions d'ondes physiques. Pour cela, nous introduisons explicitement une famille complète d'états quantiques induisant une violation arbitrairement proche de la violation maximale autorisée par la physique quantique, ce qui constitue une avancée notable par rapport aux précédents travaux de ce domaine [183, 184, 185, 186].

Dans un second temps, nous analysons un dispositif optique *faisable*, proposé par Jaromir Fiurášek, Raoul Garcia-Patron Sanchez et Nicolas Cerf, pour effectuer un test logique complet (inconditionnel) de la physique quantique face aux théories réalistes et locales. Nous donnons explicitement les paramètres caractéristiques d'une telle expérience future basée sur la dégaussification conditionnelle des deux modes d'un faisceau EPR intriqué. Les variables quantiques continues offrent ainsi une ouverture expérimentale sérieuse pour un test complet des inégalités de Bell.

Au-delà des applications immédiates des inégalités de Bell pour valider les fondements de la physique contemporaine, la violation de ces inégalités offre des perspectives intéressantes dans les protocoles de communication quantique. Par exemple, la violation d'une inégalité de Bell est une condition pour la sécurité d'un protocole de distribution de clé secrète avec des variables discrètes [44, 48]. D'une manière plus générale, Brukner et ses collaborateurs ont prouvé que la violation d'une inégalité de Bell est une condition nécessaire et suffisante pour l'existence d'un protocole quantique (basé sur les états violant l'inégalité) qui soit plus efficace qu'un protocole classique équivalent [182]. La violation d'une inégalité de Bell ouvre donc des possibilités d'applications au-delà de l'observation de non-localité ou de non-réalisme.

Conclusion générale et perspectives

Au cours de ces dernières années, les variables quantiques continues sont apparues comme une alternative intéressante aux variables quantiques discrètes, incarnées par les "qubits". Les variables quantiques continues présentent différents avantages. D'un point du vue classique, la manipulation de l'information portée par une variable continue présente l'avantage de comporter plusieurs bits d'information par symbole échangé, ce qui permet d'atteindre des hauts débits de transfert d'information. D'un point de vue quantique, les variables continues s'avèrent plus simples à produire et à manipuler que des photons uniques qui représentent généralement les qubits.

L'objectif majeur de ce travail de thèse est de mettre en œuvre de nouveaux dispositifs de traitement de l'information, qui tirent parti des particularités quantiques de la lumière portées par des variables continues. En guise de conclusion générale, nous présentons un rapide bilan des résultats principaux obtenus au cours de cette thèse. La manière dont s'inscrivent ces résultats dans le contexte de recherche actuel est ensuite discutée. Enfin, ce manuscrit s'achève sur différentes perspectives d'applications offertes par notre dispositif d'exploitation des variables quantiques continues.

Résultats et impacts

Mesure des variables continues

Notre équipe exploite les composantes de quadrature d'un mode du champ électromagnétique, qui forment un couple de variables quantiques continues conjuguées. Ces composantes de quadrature obéissent ainsi au principe d'incertitude d'Heisenberg, et sont donc un sujet d'étude intéressant pour la manipulation de l'information quantique : toutes les spécificités quantiques se retrouvent sur ce couple de variables qui ne peuvent pas être parfaitement déterminées simultanément.

La détection des composantes de quadrature repose sur des techniques de détection cohérente, basée sur un effet d'interférence avec un champ intense. Grâce à une électronique rapide garantissant la résolution temporelle de chaque impulsion optique incidente, nous avons mis en œuvre une détection homodyne permettant de mesurer directement une composante de quadrature pour chaque impulsion signal. La principale difficulté de ce système réside dans l'équilibrage fin entre les voies, qui doit garantir typiquement une réjection de l'ordre de 10^{-4}. Grâce à un dispositif opto-électronique soigné, nous avons réalisé une détection homodyne résolue en temps, fonctionnant à une cadence de 800kHz et limitée au bruit de photon pour des puissances de plus de 200 millions de photons par impulsion d'oscillateur local.

Cette détection permet d'accéder à l'évolution temporelle des quadratures signal, ce qui est indispensable pour tout protocole de transfert d'information. Elle constitue l'élément clé de notre dispositif de communication quantique avec des variables continues. A l'heure actuelle,

seuls deux systèmes équivalents ont été réalisés [26, 35], mais ces détections étaient employées dans un contexte de tomographie quantique et n'intervenaient pas dans une visée d'exploitation de l'information quantique. Notre équipe est donc la première à utiliser une détection homodyne impulsionnelle pour la communication quantique. Cette expertise sera un élément crucial pour l'avenir des protocoles de transfert de l'information quantique portée par des variables continues.

Cryptographie quantique avec des états cohérents

Nous avons réalisé une démonstration expérimentale *complète* du principe de distribution de clé quantique avec des états cohérents, de l'échange d'états quantiques à l'extraction informatique d'une clé secrète [73]. Le premier intérêt de cette expérience est de prouver qu'il est possible de transmettre une clé secrète avec des états quasi-classiques. La sécurité quantique est alors liée aux lois quantiques du clonage et de la copie, mais n'est pas conditionnée à la présence réelle d'états non-classiques. Le second apport de cette réalisation est d'estimer physiquement les paramètres caractéristiques d'un tel protocole à états cohérents. Notre système a généré une clé secrète à un débit de 1.7 Mbits/s en l'absence de pertes et 75 kbits/s pour une transmission présentant 3.1 dB de pertes. De très hauts débits d'information sont ainsi atteignables tant que l'atténuation du canal de transmission n'est pas trop grande. Dans le domaine des fortes pertes, la portée de notre protocole est pour le moment limitée par l'efficacité de nos algorithmes de réconciliation.

De nombreuses améliorations du dispositif sont encore envisageables, tant sur le point du dispositif optique que des logiciels de traitement des données. Cette démonstration ouvre donc la voie pour des protocoles efficaces de cryptographie quantique à hauts débits. En particulier, un partenariat avec la société *Thalès* est actuellement développé afin de réaliser un prototype complet avec des états cohérents opérant dans le domaine des longueurs d'ondes télécoms. Ce prototype s'inscrit dans le cadre du projet européen *SECOQC* (*SEcure COmmunication based on Quantum Cryptography*), qui vise à doter l'Union Européenne d'un réseau global de communications sécurisées à l'échelle de 4 ans. Regroupant 41 unités de 12 pays européens, le projet *SECOQC* entend amorcer une ère nouvelle dans la sécurité des réseaux informatiques.

Source impulsionnelle d'états non-classiques

En complément de l'expérience de cryptographie quantique avec des états cohérents, nous souhaitons étudier l'utilisation d'états spécifiquement quantiques du champ lumineux pour des applications de traitement de l'information quantique. En effet, l'exploitation de l'intrication quantique ou des fluctuations quantiques réduites peut permettre d'améliorer la portée et la robustesse des protocoles de communication quantique. Dans ce but, une première étape est de disposer d'une source impulsionnelle d'états comprimés et d'états intriqués en quadrature.

Pour produire simplement et efficacement des états comprimés, notre équipe utilise l'amplification paramétrique dégénérée mise en œuvre lors d'un simple passage d'impulsions ultrabrèves dans un cristal mince de niobate de potassium. La réduction du bruit en quadrature est alors de 2.7 dB sous le niveau de bruit quantique standard [111], ce qui constitue un effet appréciable. Différentes techniques de caractérisation des états vides comprimés ont été mises en œuvre expérimentalement. En particulier, nous avons discuté la réalisation d'une méthode originale, basée sur des mesures de taux de comptage de photons et ne nécessitant pas de référence de phase [124].

Nous avons ensuite utilisé cette source d'états comprimés pour réaliser la première démonstration expérimentale d'un protocole de "dégaussification", qui transforme des impulsions de

vide comprimé en des états clairement non-gaussiens [128]. Notre procédure se base exclusivement sur des éléments optiques linéaires et une photodétection non-discriminante en nombre de photons. La "dégaussification" et la "regaussification" d'états quantiques offrent des perspectives prometteuses pour la manipulation des variables continues. En particulier, elles sont la clé pour des protocoles de distillation de l'intrication de variables gaussiennes continues [127], nécessaires à l'amélioration de la portée des dispositifs de cryptographie quantique.

Avec le même dispositif expérimental, nous avons également produit des impulsions intriquées en quadratures, montrant des corrélations de $\Delta^2(X_A - X_B)/2 = 0.56\,N_0$ (-2.5 dB) [157]. En recombinant les deux faisceaux intriqués sur une lame, la non-séparabilité de l'état a été directement évaluée grâce au critère de Duan-Simon, et fournit $\mathcal{I}_{\rm DS} = 1.12\,N_0$ ($< 2\,N_0$). Ce montage entièrement impulsionnel demeure très particulier dans le domaine des variables continues : auparavant, seul le groupe de Gerd Leuchs avait généré des états EPR impulsionnels en utilisant l'effet Kerr dans une fibre optique [148, 199] .

Associée à notre détection homodyne impulsionnelle, cette source d'états non-classiques fournit tous les éléments de base pour des applications futures de traitement de l'information quantique portée par des états EPR ou des états comprimés. En particulier, l'analyse des transferts d'information au sens de Shannon est alors très simple, et permet des applications immédiates pour la cryptographie quantique [73, 75].

Test complet de la physique quantique avec des variables continues

En dehors de ses possibilités pour l'information quantique, l'intrication de variables continues est également un domaine prometteur pour les tests des inégalités de Bell, grâce aux grandes séparations accessibles entre les systèmes d'analyse et aux fortes efficacités intrinsèques des détections homodynes. En effet, ces deux dernières spécificités permettent d'envisager des tests *complets* (*loophole-free*) de la physique quantique face aux théories réalistes et locales.

Nous donnons explicitement une famille d'états quantiques *physiques* induisant une violation des inégalités de Bell arbitrairement proche de la valeur maximale autorisée par la physique quantique [187, 190]. Ce résultat est obtenu pour des mesures homodynes, et constitue une avancée notable par rapport aux précédents travaux de ce domaine.

En parallèle de cette étude, nous étudions en détails une proposition récente de Jaromir Fiurášek, Raoul Garcia-Patron Sanchez et Nicolas Cerf, pour un dispositif expérimental *faisable* permettant un test *inconditionnel* des inégalités de Bell [188]. Cette expérience se base sur la dégaussification conditionnelle des deux modes d'un faisceau EPR intriqué et sur des mesures homodynes de fortes efficacités. En particulier, nous discutons les différents paramètres caractéristiques de cette expérience. Les variables quantiques continues offrent ainsi une ouverture expérimentale sérieuse pour un test complet des inégalités de Bell.

Contexte scientifique en fin de thèse

Entre 1998 et 2003, différentes avancées expérimentales majeures ont mis en évidence toute la richesse de la manipulation de l'information quantique portée par des variables continues : téléportation d'un état cohérent [146], génération d'états intriqués impulsionnels [148], intrication entre des ensembles atomiques séparés [197] et distribution quantique d'une clé secrète avec des états cohérents [73]. En plus de ces réalisations, de nombreuses études ont été menées dans le domaine du clonage quantique, de la caractérisation de l'intrication et de la manipulation d'états gaussiens. Si ces investigations prouvent la richesse du concept des variables quantiques conti-

nues, des recherches plus approfondies doivent néanmoins être encore menées pour aboutir à une véritable application technologique de ces variables quantiques continues.

Pour développer la cryptographie quantique à grande distance, un défi majeur est de concevoir et réaliser un système de "répéteur quantique" pour améliorer la portée des dispositifs actuels au-delà de quelques dizaines de kilomètres. Ceci nécessite des études poussées de la distillation et de la purification de l'intrication quantique, et amène vers des opérations non-gaussiennes pour les variables continues. En particulier, la manipulation d'états non-gaussiens intriqués en quadratures apparaît comme un domaine très prometteur, et qui reste encore à défricher. Un autre projet essentiel pour l'exploitation à grande distance des variables continues est de développer des "mémoires quantiques", vraisemblablement basées sur des techniques de manipulation du spin collectif d'ensembles atomiques. Précisons enfin que la maîtrise de ces différentes techniques ouvrira également la voie vers des algorithmes de calcul quantique avec des variables continues.

Ce travail de thèse intervient donc dans une première étape de développement de l'information quantique avec des variables continues. Dans ce domaine pluridisciplinaire en plein essor, les prochaines années seront décisives pour le mûrissement et l'affirmation des procédures quantiques utilisant les variables continues. Témoin de l'intérêt croissant pour les variables quantiques continues et de la vivacité de ce domaine, la série de colloques *CVQIP* (*Continuous Variable Quantum Information Processing*) attire annuellement depuis 2002 près de 40 experts européens.

Afin d'être plus spécifique sur les perspectives ouvertes par notre dispositif expérimental, la prochaine section présente différents développements possibles, classés par domaine d'application.

Perspectives de recherche

Communication quantique

Notre dispositif expérimental actuel permet de mettre en œuvre très simplement un protocole de distribution de clé secrète basé sur des états EPR impulsionnels envisagé dans [70, 75]. Pour cela, il suffit de disposer de deux détections homodynes résolues en temps sur chaque faisceau EPR, puis de traiter les données continues échangées suivant la démarche présentée au chapitre 5. L'utilisation de faisceaux EPR apporte certains avantages par rapport aux états cohérents, notamment une plus grande robustesse à un excès de bruit dans le cadre d'une réconciliation inverse (voir le chapitre 6). La réalisation de ces protocoles n'a encore jamais été présentée.

Un autre avantage apporté par la cryptographie avec des états intriqués est de rendre envisageable la distillation de l'intrication. Pour cette application, notre dispositif de "dégaussification", étendu à un état EPR à deux modes, constitue la première étape du protocole de distillation quantique présenté dans [127]. Le même montage permet également une augmentation des ressources en intrication avec des états non-gaussiens [138].

Ces différentes applications nécessitent toutes de disposer de corrélations quantiques les plus élevées possibles. Il est donc essentiel de chercher à augmenter les effets des interactions non-linéaires. Plusieurs approches sont possibles, de la modification des cristaux (dispositifs à quasi-accord de phase pour des impulsions femtosecondes) à l'amélioration des caractéristiques de la source laser (modification de la cavité, utilisation d'un amplificateur multi-passage).

La sécurité de nos protocoles de cryptographie quantique se fonde sur les limites fondamentales imposées par la physique à la qualité des actions quantiques de copie ou de clonage d'un état. Dans un contexte de manipulation de l'information quantique, l'étude expérimentale de ces limites est donc un sujet particulièrement attractif. La référence [82] donne explicitement un dispositif optimal pour le clonage d'un état cohérent, mais ce montage n'a pas encore été mis en œuvre expérimentalement. La principale difficulté de cette proposition, représentée à la

figure 11.10, est de nécessiter un gain paramétrique important de $G = 2$ (alors que le meilleur gain obtenu avec notre dispositif est de $G = 1.24$). D'après différentes estimations basées sur notre dispositif expérimental, pour atteindre un gain paramétrique de 2, il faudrait disposer d'une puissance de pompe moyenne d'environ 20 mW à 425 nm, soit une puissance moyenne de fondamental en sortie du laser de l'ordre de 100 mW (ce qui équivaut à une énergie de 130 nJ par impulsion à 780 kHz). Un tel niveau de puissance nécessite donc un développement supplémentaire de notre source, mais offre des perspectives inédites de manipulation de l'information quantique.

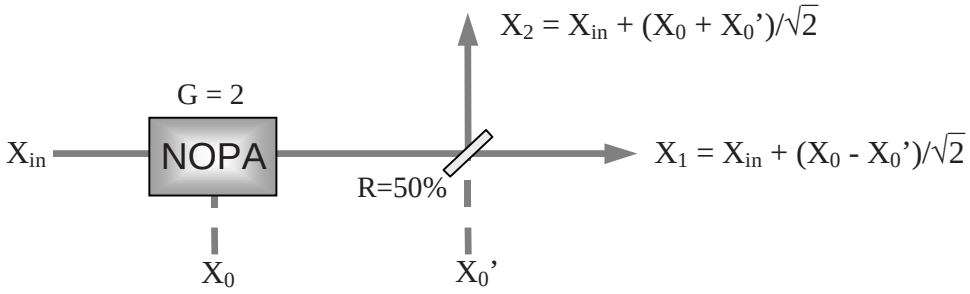

Figure 11.10: *Schéma d'un dispositif de clonage optimal d'un état cohérent. L'une des quadratures de l'état en entrée est notée X_{in}. X_0 et X_0' désignent respectivement les modes vides entrant dans l'amplificateur indépendant de la phase et dans la lame semiréfléchissante.*

Calcul quantique

Si l'essentiel des efforts de recherche se concentre actuellement sur la communication quantique, les variables continues offrent cependant un domaine d'étude particulièrement intéressant pour des systèmes de calcul quantique. Par exemple, Gottesman et Preskill proposent un code quantique correcteur d'erreurs basé sur l'utilisation de faisceaux comprimés [65]. Ce domaine fait également l'objet de différentes études menées par Braunstein et Lloyd [3].

Une porte logique particulière pour le calcul quantique avec des variables continues est la porte C-NOT, qui effectue les opérations suivantes [3] :

$$\begin{array}{ccc} |x\rangle & \Longrightarrow & |x\rangle \\ |y\rangle & & |x+y\rangle \end{array}$$

En modifiant légèrement le dispositif d'amplification paramétrique non-dégénérée dans une configuration qui s'inspire des mesures quantiques non-destructives, il est possible de réaliser cette porte C-NOT pour des variables continues (voir la figure 11.11). Le gain paramétrique requis est de $G = 1.25$, ce qui est relativement accessible à notre montage. A l'heure actuelle, aucune démonstration expérimentale de calcul quantique avec des variables continues n'a encore été proposée.

Physique fondamentale

Notre montage expérimental présente actuellement tous les éléments pour un test inconditionnel des inégalités de Bell selon [188] : source paramétrique impulsionnelle, ensemble de conditionnement, détection homodyne résolue en temps. Cependant, aucun de ces éléments

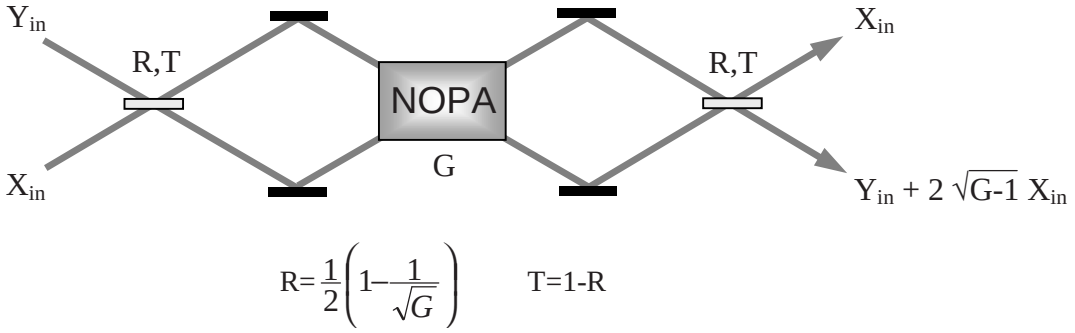

Figure 11.11: *Proposition de porte C-NOT avec des variables continues. Dans le cas où $G = 1.25$, les quadratures des modes en sortie sont X_{in} et $X_{in}+Y_{in}$, ce qui réalise une porte C-NOT d'après [3].*

n'atteint les paramètres requis pour observer expérimentalement une violation des inégalités de Bell : corrélation de 6 dB, efficacité homodyne de 95%... Obtenir l'ensemble de ces paramètres simultanément constitue un défi expérimental majeur, mais permet une validation définitive de la physique quantique. Par ailleurs, le même dispositif de test offre de nombreuses opportunités de traitement de l'information quantique portée par des variables continues.

Par ailleurs, comme nous l'avons suggéré au chapitre 9, notre procédure de "dégaussification" du vide comprimé génère un état voisin d'un "chaton" de Schrödinger. Ces états peuvent ensuite être utilisés dans une procédure d'amplification pour produire un chat de plus forte amplitude avec une excellente fidélité [131]. L'état final sera alors un "vrai" chat de Schrödinger, c'est-à-dire une superposition de deux états cohérents dont la fonction d'onde présente deux pics séparés macroscopiquement. Cette étude permet de mettre en évidence des processus fondamentaux de la physique quantique, et offre aussi des perspectives nouvelles pour le traitement de l'information quantique [130].

Ce travail de thèse s'inscrit dans les programmes suivants :

- *IST/FET/QIPC QUICOV (QUantum Information with COntinuous Variables)*
- *IST/IP SECOQC (SEcure COmmunication based on Quantum Cryptography)*
- *IST/FET/STREP COVAQUIAL (COntinuous VAriable QUantum Information with Atoms and Light)*
- *ACI Photonique (Ministère de la Recherche) : Production et manipulation d'états quantiques de la lumière produits par fluorescence et amplification paramétrique en régime femtoseconde.*
- *ASTRE (Département de l'Essonne) : Information quantique en régime femtoseconde.*

Bibliographie

Généralités sur l'information quantique

[1] M.A. Nielsen et I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge (2000).

[2] D. Bouwmeester, A. Ekert et A. Zeilinger (Eds.), *The physics of quantum information*, Springer, Berlin (2000).

[3] S.L. Braunstein et A.K. Pati, *Quantum Information with Continuous Variables*, Kluwer Academic, Dordrecht, (2003).

[4] C.H. Bennett et D.P. DiVincenzo, Quantum information and computation, *Nature* **404**, 247 (2000).

[5] J.P. Dowling et G.J. Milburn, Quantum technology : the second quantum revolution, arXiv quant-ph/0206091 (2002); voir aussi "Une nouvelle révolution quantique", Chapitre 5 de l'ouvrage collectif *Demain, la physique*, Editions Odile Jacob (2004).

Théorie classique de l'information

[6] C.E. Shannon, A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 623-656 (1948).

[7] T.M. Cover et J.A. Thomas, *Elements of Information Theory*, Wiley, New York (1991).

[8] G. Battail, *Théorie de l'information – Application aux techniques de communication*, Masson, Paris (1997).

Ouvrages de référence en optique quantique

[9] C. Cohen-Tannoudji, B. Diu et F. Laloë, *Mécanique quantique, tome I*, Hermann, Paris (1977).

[10] W. Pauli, *General principles of quantum mechanics*, Springer, Berlin (1980).

[11] R. Loudon, *The quantum theory of light, second edition*, Oxford Science Publications, Oxford (1983).

[12] C. Cohen-Tannoudji, J. Dupont-Roc et G. Grynberg, *Processus d'interaction entre photons et atomes*, InterEditions, Paris (1988).

[13] D.F. Walls et G.J. Milburn, *Quantum Optics*, Springer, Berlin (1994).

[14] L. Mandel et E. Wolf, *Optical coherence and quantum optics*, Cambridge University Press, Cambridge (1995).

[15] G. Grynberg, A. Aspect et C. Fabre, *Introduction aux lasers et à l'optique non-linéaire*, Ellipses, Paris (1997).

[16] H.A. Bachor, *A guide to experiments in quantum optics*, Wiley-VCH, Weinheim (1998).

[17] U. Leonhardt, *Measuring the quantum state of light*, Cambridge University Press, Cambridge, (1997).

[18] W.P. Schleich, *Quantum optics in phase space*, Wiley-VCH, Weinheim (2001).

Articles de référence en optique quantique

[19] A. Aspect, P. Grangier et G. Roger, Experimental evidence for a photon anticorrelation effect on a beamsplitter : a new light on single-photon interferences, *Europhys. Lett.* **1**, 173 (1986).

[20] C. Hong, Z. Ou et L. Mandel, Measurement of sub-picosecond time intervals between two photons by interference, *Phys. Rev. Lett.* **59**, 2044 (1987).

[21] J.-F. Roch, K. Vigneron, P. Grelu, A. Sinatra, J.-P. Poizat et P. Grangier, Quantum non-demolition measurements using cold trapped atoms, *Phys. Rev. Lett.* **78**, 634 (1997).

[22] P. Grangier, J.-A. Levenson et J.-P. Poizat, Quantum non-demolition measurements in optics, *Nature* **396**, 537 (1998).

[23] J.-P. Poizat, *Bruit quantique des diodes laser*, Habilitation à diriger des recherches, Université Paris XI, décembre 1999.

Tomographie quantique et fonction de Wigner

[24] E.P. Wigner, On the quantum correction for thermodynamic equilibrium, *Phys Rev.* **40**, 749 (1932).

[25] J. Bertrand et P. Bertrand, A tomogarphic approach to Wigner's function, *Found. Phys.* **17** 397 (1987).

[26] D.T. Smithey, M. Beck, M.G. Raymer et A. Faridani, Measurements of the Wigner Distribution and the density matrix of a light mode using optical homodyne tomography, *Phys. Rev. Lett.* **70**, 1244 (1993).

[27] G. Breitenbach, S. Schiller et J. Mlynek, Measurements of the quantum states of squeezed light, *Nature* **387**, 471 (1997).

[28] T. Coudreau, *Réduction du bruit et tomographie quantique d'un faisceau laser interagissant avec des atomes froids : théorie et expériences*, Thèse, Université Paris 6 (1997).

[29] D.-G. Welsch, W. Vogel, et T. Opatrný, *Homodyne Detection and Quantum-State Reconstruction*, Vol. 39 de Progress in Optics, édité par E. Wolf, Elsevier, Amsterdam (1999).

[30] A.I. Lvovsky, H. Hansen, T. Aichele, O. Benson, J. Mlynek et S. Schiller, Quantum state reconstruction of the single-photon Fock state, *Phys. Rev. Lett.* **87**, 050402 (2001).

[31] J. Rehacek, Z. Hradil, M. Jesek, Iterative algorithm for reconstruction of entangled states, *Phys. Rev. A* **63**, 040303 (2001).

[32] A.I. Lvovsky, Iterative maximum-likelihood reconstruction in quantum homodyne tomography, arXiv quant-ph/0311097 (2003).

Détection homodyne impulsionnelle

[33] H.P. Yuen et V.W.S. Chan, Noise in homodyne and heterodyne detection,*Opt. Lett.* **8**, 177 (1983).

[34] H. Hansen, *Generation and characterization of new quantum states of the light field*, Thèse, Universität Konstanz, Allemagne (2000).

[35] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A.I. Lvovsky, J. Mlynek et S. Schiller, An ultrasensitive pulsed balanced homodyne detector : application to time-domain quantum measurements, *Opt. Lett.* **26**, 1430 (2001).

[36] F. Grosshans et P. Grangier, Effective quantum efficiency in the pulsed homodyne detection of a n-photon state, *Eur. Phys. J. D* **14**, 119 (2001).

[37] Z.Y. Ou, Parametric down-conversion with coherent pulse pumping and quantum interference between independent fields, *Quant. Semiclass. Opt.* **9**, 599 (1997).

[38] T. Aichele, A.I. Lvovsky et S. Schiller, Optical mode characterization of single photon prepared by means of conditional measurements on a biphoton state, *Eur. Phys. J. D.* **18**, 237 (2002).

Généralités sur la cryptographie quantique

[39] L'art du secret, Dossier *Pour la Science* **36**, juillet/octobre 2002.

[40] N. Gisin, G. Ribordy, W. Tittel et H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

[41] C.E. Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J.* **28**, 656 (1949).

[42] S. Wiesner, Conjugate coding, *Sigact News* **15** 78 (1983).

[43] C.H. Bennett et G. Brassard, Quantum cryptography : public-key distribution and coin tossing, dans *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175 (1984).

[44] A.K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).

[45] C.H. Bennett, G. Brassard et N.D. Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**, 557 (1992).

[46] C.H. Bennett, Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).

[47] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin et W.K. Wooters, Mixed state entanglement and quantum error correction, *Phys. Rev. A* **54**, 3824 (1996).

[48] V. Scarani et N. Gisin, Quantum communication between N partners and Bell's inequalities, *Phys. Rev. Lett.* **87**, 117901 (2001).

[49] A. Acin, N. Gisin et L. Masanes, Equivalence between two-qubit entanglement and secure key distribution, *Phys. Rev. Lett.* **91**, 167901 (2003).

Procédures classiques de réconciliation et d'amplification de confidentialité

[50] I. Csiszár et J. Körner, Broadcast channel with confidential messages. *IEEE Trans. Inform. Theory* **24**, 339 (1978).

[51] U.M. Maurer, Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory* **39**, 733 (1993).

[52] G. Brassard et L. Salvail, Secret-key reconciliation by public discussion. *Advances in Cryptology - Eurocrypt'93* Lecture Notes in Computer Science (ed. Helleseth, T.) 411 (Springer, New York, 1993).

[53] C. Berrou, A. Glavieux et P. Thitimajshima, Near Shannon limit error correcting, coding and decoding : Turbo-Codes, *Proceedings of ICC'93*, 1064, Genève, Suisse, 23-26 mai 1993.

[54] C.H. Bennett, G. Brassard, C. Crépeau et U.M. Maurer, Generalized privacy amplification. *IEEE Trans. Inform. Theory* **41**, 1915 (1995).

[55] N. Gisin et S. Wolf, Quantum cryptography on noisy channels : quantum versus classical key-agreement protocols, *Phys. Rev. Lett.* **83**, 4200 (1999).

[56] G. Van Assche, J. Cardinal et N.J. Cerf, Reconciliation of a quantum-distributed Gaussian key, *IEEE Trans. Inform. Theory* **50**, 394 (2003). Voir aussi arXiv cs.CR/0107030 (2001).

[57] K. Nguyen, *Extension des Protocoles de Réconciliation en Cryptographie Quantique*, Thèse, Univ. Libre de Bruxelles (2002).

[58] W.T. Buttler, S.K. Lamoreaux, J.R. Torgerson, G.H. Nickel et C.G. Peterson, Fast, efficient error reconciliation for quantum cryptography, arXiv quant-ph/0203096 (2002).

[59] H.K. Lo, Method for decoupling error correction from privacy amplification, arXiv quant-ph/ 0201030 (2002).

[60] K.-C. Nguyen, G. Van Assche et N.J. Cerf, Side-Information Coding with Turbo Codes and its application to quantum key distribution, arXiv cs.IT/0406001 (2004), accepté dans *2004 International Symposium on Information Theory and its Applications, ISITA2004.*

Cryptographie quantique avec des variables continues

[61] M. Hillery, Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000).

[62] T.C. Ralph, Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303(R) (2000).

[63] T.C. Ralph, Security of continuous-variable quantum cryptography. *Phys. Rev. A* **62**, 062306 (2000).

[64] M.D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A* **62**, 062308 (2000).

[65] D. Gottesman et J. Preskill, Secure quantum key distribution using squeezed states. *Phys. Rev. A* **63**, 022309 (2001).

[66] N.J. Cerf, M. Lévy et G. Van Assche, Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).

[67] K. Bencheikh, T. Symul, A. Jankovic et J.A. Levenson, Quantum key distribution with continuous variables. *J. Mod. Optics* **48**, 1903 (2001).

[68] N.J. Cerf, S. Iblisdir et G. Van Assche, Cloning and cryptography with quantum continuous variables. *Eur. Phys. J. D* **18**, 211 (2002).

[69] C. Silberhorn, N. Korolkova, et G. Leuchs, Quantum key distribution with bright entangled beams. *Phys. Rev. Lett.* **88**, 167902 (2002).

Cryptographie quantique avec des états cohérents

[70] F. Grosshans et Ph. Grangier, Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).

[71] F. Grosshans, *Communication et cryptographie quantiques avec des variables continues*, Thèse, Université Paris-Sud 11 (2002).

[72] Ch. Silberhorn, T.C. Ralph, N. Lütkenhaus et G. Leuchs, Continuous variable quantum cryptography beating the 3 dB loss limit. *Phys. Rev. Lett.* **89**, 167901 (2002).

[73] **F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf et Ph. Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature* 421, 238 (2003).**

[74] F. Grosshans et Ph. Grangier, Reverse reconciliation protocols for quantum cryptography with continuous variables. E-print arXiv:quant-ph/0204127. *Proc. 6th Int. Conf. on Quantum Communications, Measurement, and Computing*, (Rinton Press, Princeton, 2003).

[75] **F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri et Ph. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables *Quant. Inf. Comput.* 3, 535 (2003), voir aussi arXiv quant-ph/0306141.**

[76] F. Grosshans et N.J. Cerf, Security of continuous-variable quantum cryptography against non-gaussian attacks, *Phys. Rev. Lett.* **92**, 047905 (2004).

[77] S. Iblisdir, G. Van Assche et N.J. Cerf, Security of quantum key distribution with coherent states and homodyne detection, arXiv quant-ph/0312018 (2003).

Clonage quantique

[78] W.K. Wooters et W.H. Zurek, A single quantum state cannot be cloned, *Nature* **299**, 802 (1982).

[79] C.M. Caves, Quantum limits on noise in linear amplifiers, *Phys. Rev. D* **26** 1817 (1982).

[80] N.J. Cerf, A. Ipe et X. Rottenberg, Cloning of continuous variables, *Phys. Rev. Lett.* **85**, 1754 (2000).

[81] N.J. Cerf et S. Iblisdir, Optimal N-to-M cloning of conjugate quantum variables. *Phys. Rev. A* **62**, 040301(R) (2000).

[82] S.L. Braunstein, N.J. Cerf, S. Iblisdir, P. Van Loock et S. Massar, Optimal cloning of coherent states with a linear amplifier and beamsplitters, *Phys. Rev. Lett.* **86** 4938 (2001).

[83] F. Grosshans et P. Grangier, Quantum cloning and teleportation criteria for continuous quantum variables, *Phys. Rev. A* **64**, 010301(R) (2001).

Impulsions laser femtosecondes

[84] C. Rullière (Ed.), *Femtosecond laser pulses*, Springer, Berlin (1998).

[85] M. Joffre, *Propagation linéaire et non-linéaire d'une impulsion ultrabrève*, cours de l'ENSTA (1998).

[86] J.M. Hopkins et W. Sibbett, Lasers à impulsions ultracourtes, *Pour la Science* **277**, 86 (2000).

[87] M. Ramaswamy, M. Ulman, J. Paye et J.G. Fujimoto, Cavity-dumped femtosecond Kerr-lens mode-locked Ti:Al_2O_3 laser, *Opt. Lett.* **18**, 1822 (1993).

[88] M.S. Pshenichnikov, W.P. De Boeij et D.A. Wiesma, Generation of 13fs, 5MW pulses from a cavity-dumped Ti:sapphire laser, *Opt. Lett.* **19**, 572 (1994).

[89] U. Keller, Ultrafast all-solid-state laser technology, *Appl. Phys. B* **58**, 347 (1994).

[90] F.X. Kärtner et U. Keller, Stabilization of solitonlike pulses with a slow saturable absorber, *Opt. Lett.* **20**, 16 (1995).

[91] S. Schneider, A. Stockmann et W. Schüsslbauer, Self-starting mode-locked cavity-dumped femtosecond Ti:sapphire laser employing a semiconductor saturable absorber mirror, *Opt. Exp.* **6**, 220 (2000).

[92] J. Wenger, Carnet d'utilisation du laser *Tiger-CD*, note interne LCFIO (2004).

Optique non-linéaire impulsionnelle

[93] R.W. Boyd, *Nonlinear optics*, 2e édition, Academic Press, San Diego (2003).

[94] Y.R. Shen, *Principles of nonlinear optics*, Wiley Classics Library, New York (1983).

[95] R.L. Sutherland, *Handbook of nonlinear optics*, Marcel Dekker Inc., New York (1995).

[96] V.G Dmitriev, G.G. Gurzadyan et D.N. Nikogosyan, *Handbook of nonlinear optical crystals*, 3e édition, Springer, Berlin (1999).

[97] A.M. Weiner, A.M. Kan'an et D.E. Leaird, High efficiency blue generation by frequency doubling of femtosecond pulses in a thick nonlinear crystal, *Opt. Lett.* **23**, 1441 (1998).

[98] Y.Q. Li, D. Guzun et M. Xiao, Quantum noise measurements in high efficiency single pass second harmonic generation with femtosecond pulses, *Opt. Lett.* **24**, 987 (1999).

[99] H. Mabuchi, E.S. Polzik et H.J. Kimble, Blue-light-induced infrared absorption in $KNbO_3$, *J. Opt. Soc. Am. B* **11**, 2023 (1994).

[100] R.G. Reeves, M.G. Jani, B. Jassemnejad, R.C. Powell, G.J. Mizell et W. Fay, Photorefractive properties of $KNbO_3$, *Phys. Rev. B* **43**, 71 (1991).

[101] A.D. Ludlow, H.M. Nelson, et S.D. Bergeson, Two-photon absorption in potassium niobate, *J. Opt. Soc. Am. B* **18**, 1813 (2001).

[102] A. Laporta et R.E. Slusher, Squeezing limits at high parametric gain, *Phys. Rev. A* **44**, 2013 (1991).

[103] R.R. Tucci, Diffraction and squeezed light, *Int. J. Mod. Phys. B* **7** 4403, (1993).

[104] K.G. Koprulu et O. Aytur, Analysis of Gaussian-beam degenerate optical parametric amplifiers for the generation of quadrature-squeezed light, *Phys. Rev. A* **60**, 4122 (1999).

Génération d'états comprimés

[105] R.E. Slusher, L.W. Hollberg, B. Yurke, J.C. Mertz et J.F. Valley, Observation of squeezed states generated by four wave mixing in an optical cavity, *Phys. Rev. Lett.* **55**, 2409 (1985).

[106] R.E. Slusher, P. Grangier, A. LaPorta, B. Yurke et M.J. Potasek, Pulsed squeezed light, *Phys. Rev. Lett.* **59**, 2566 (1987).

[107] P. Kumar, O. Aytur et J. Huang, Squeezed light generation with an incoherent pump, *Phys. Rev. Lett.* **64**, 1015 (1990).

[108] C. Kim et P. Kumar, Quadrature-squeezed light detection using a self-generated matched local oscillator, *Phys. Rev. Lett.* **73**, 1605 (1994).

[109] M.E. Anderson, M. Beck, M.G. Raymer et J.D. Bierlein, Quadrature squeezing with ultrashort pulses in nonlinear optical waveguides, *Opt. Lett.* **20**, 620 (1995).

[110] E.M. Daly, A.S. Bell, E. Riis et A.I. Ferguson, Generation of picosecond squeezed pulses using an all-solid-state cw mode-locked source, *Phys. Rev. A* **57**, 3127 (1998).

[111] **J. Wenger, R. Tualle-Brouri et P. Grangier, Pulsed homodyne measurements of femtosecond squeezed pulses generated by single-pass parametric deamplification, *Opt. Lett.* 29, 1267 (2004).**

[112] J. Fiurášek, Conditional generation of sub-Poissonian light from two-mode squeezed vacum via balanced homodyne detection on idler mode, *Phys. Rev. A* **64**, 053817 (2001).

[113] J. Laurat, T. Coudreau, N. Treps, A. Maître et C. Fabre, Conditional preparation of a quantum state in the continuous variables regime : generation of a sub-Poissonian state from twin beams, *Phys. Rev. Lett.* **91**, 213601 (2003).

[114] J. Laurat, T. Coudreau, N. Treps, A. Maître et C. Fabre, Conditional preparation of a quantum state in the continuous variables regime : theoretical study, *Phys. Rev. A* **69**, 033808 (2004).

[115] K. Schneider, M. Lang, J. Mlynek et S. Schiller, Generation of strongly squeezed continuous-wave light at 1064 nm, *Optics Express* **2**, 59 (1998).

Caractérisation d'états gaussiens

[116] R. Simon, N. Mukunda et B. Dutta, Quantum noise matrix for multimode systems: U(n) invariance, squeezing and normal forms, *Phys. Rev. A* **49**, 1567 (1994).

[117] G. Adam, Density matrix elements and moments for generalized Gaussian state fields, *J. Mod. Opt.* **42**, 1311 (1995).

[118] Z. Hradil, Quantum state estimation, *Phys. Rev. A* **55**, R1561 (1997).

[119] G.M. D'Ariano, M.G.A. Paris et M. Sacchi, Parameter estimation in quantum optics, *Phys. Rev. A* **62**,023815 (2000).

[120] J. Řeháček, Z. Hradil et M. Ježek, Iterative algorithm for reconstruction of entangled states, *Phys. Rev. A* **63**, 040303 (2001).

[121] M.S. Kim, J. Lee et W.J. Munro, Experimentally realizable characterization of continuous-variable Gaussian state, *Phys. Rev. A* **66**, 030301 (2002).

[122] M.G.A. Paris, F. Illuminati, A. Serafini et S. De Siena, Purity of Gaussian states: Measurement schemes and time evolution in noisy channels, *Phys. Rev. A* **68**, 012314 (2003).

[123] J. Fiurášek et N.J. Cerf, How to measure squeezing and entanglement of gaussian states without homodyning, *Phys. Rev. Lett.* **93**, 063601 (2004).

[124] **J. Wenger, J. Fiurášek, R. Tualle-Brouri, N.J. Cerf et P. Grangier, Pulsed squeezed vacuum characterization without homodyning, arXiv quant-ph/0403234, accepté pour publication dans *Phys. Rev. A* (2004).**

Etats non-gaussiens et applications

[125] L.M. Duan, G. Giedke, J.I. Cirac et P. Zoller, Entanglement purification of Gaussian continuous variables quantum states, *Phys. Rev. Lett.* **84**, 4002 (2000).

[126] M.G.A. Paris, M. Cola et R. Bonifacio, Quantum state engineering assisted by entanglement, *Phys. Rev. A* **67**, 042104 (2003).

[127] D.E. Browne, J. Eisert, S. Scheel et M.B. Plenio, Driving non-Gaussian to Gaussian states with linear optics, *Phys. Rev. A* **67**, 062320 (2003). Voir aussi quant-ph/0307106.

[128] **J. Wenger, R. Tualle-Brouri et P. Grangier, Non-gaussian statistics from individual pulses of squeezed light, *Phys. Rev. Lett.* 92, 153601 (2004).**

[129] M. Dakna, J. Clausen, L. Knöll et D.G. Welsch, Generating and monitoring Schrödinger cats in conditional measurements on a beam splitter, arXiv quant-ph/9805048 (1998).

[130] A. Gilchrist, K. Naemoto, W.J. Munro, T.C. Ralph, S. Glancy, S.L. Braunstein et G.J. Milburn, Schrödinger cats and their power for quantum information processing, *J. Opt. B: Quant. Semiclass. Opt.* **6**, S828 (2004).

[131] A.P. Lund, H. Jeong, T.C. Ralph et M.S. Kim, Conditional production of Schrödinger cats with inefficient photon detection, *Phys. Rev. A* **70**, 020101(R) (2004).

Intrication en quadratures : théorie

[132] A. Einstein, B. Poldolsky et N. Rosen, Can quantum mechanical description of physical reality be considered complete ?, *Phys. Rev.* **47**, 777 (1935).

[133] M.D. Reid, Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification, *Phys. Rev. A* **40**, 913 (1989).

[134] L.M. Duan, G. Giedke, J.I. Cirac et P. Zoller, Inseparability criterion for continuous variable systems, *Phys. Rev. Lett.* **84**, 2722 (2000).

[135] R. Simon, Peres-Horodecki separability criterion for continuous variable systems, *Phys. Rev. Lett.* **84**, 2726 (2000).

[136] M.D. Reid, The Einstein-Podolsky-Rosen paradox and entanglement : signatures of EPR correlations for continuous variables, arXiv quant-ph/0112038 (2001).

[137] W.K. Wooters, Entanglement of formation and concurrence, *Quantum. Inf. Comput.* **1**, 27 (2001).

[138] T. Opatrný, G. Kurizki et D.-G. Welsch, Improvement on teleportation of continuous variables by photon subtraction via conditional measurement, *Phys. Rev. A* **61**, 032302 (2000).

[139] P.T. Cochrane, T.C. Ralph et G.J. Milburn, Teleportation improvement by conditional measurements on the two-mode squeezed vacuum, *Phys. Rev. A* **65**, 062306 (2002).

[140] S. Olivares, M.G.A. Paris et R. Bonifacio, Teleportation improvement by inconclusive photon subtraction, *Phys. Rev. A* **67**, 032314 (2003).

[141] J. Eisert et M.B. Plenio, Introduction to the basics of entanglement theory in continuous-variable systems, *Int. J. Quant. Inf.* **1**, 479 (2003).

[142] G. Giedke, M.M. Wolf, O. Krüger, R.F. Werner et J.I. Cirac, Entanglement of Formation for symmetric Gaussian states, *Phys. Rev. Lett.* **91**, 107901 (2003).

Intrication en quadratures : expériences

[143] Z.Y. Ou, S.F. Pereira, H.J. Kimble et K.C. Peng, Realization of the Einstein-Podolsky-Rosen paradox for continuous variables, *Phys. Rev. Lett.* **68**, 3663 (1992).

[144] Z.Y. Ou, S.F. Pereira et H.J. Kimble, Realization of the Einstein-Podolsky-Rosen paradox for continuous variables in nondegenerate parametric amplification, *Appl. Phys. B* **55**, 265 (1992).

[145] K. Bencheikh, J.A. Levenson, P. Grangier et O. Lopez, Quantum nondemolition demonstration via repeated backaction evading measurements, *Phys. Rev. Lett.* **75**, 3422 (1995).

[146] A. Furusawa, J. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble et E. Polzik, Unconditionnal quantum teleportation, *Science* **282**, 706 (1998).

[147] Y.Zhang, H. Wang, X. Li, J. Jing, C. Xie et K. Peng, Experimental generation of bright two-mode quadrature squeezed light from a narrow-band nondegenerate optical parametric amplifier, *Phys. Rev. A* **62**, 023813 (2000).

[148] C. Silberhorn, P.K. Lam, O. Weiss, F. Konig, N. Korolkova et G. Leuchs, Generation of continuous variable Einstein-Podolsky-Rosen entanglement via the Kerr nonlinearity in an optical fibre, *Phys. Rev. Lett* **86**, 4267 (2001).

[149] C. Schori, J.L. Sørensen et E.S. Polzik, Narrow-band frequency tunable light source of continuous quadrature entanglement, *Phys. Rev. A* **66**, 033802 (2002).

[150] W.P. Bowen, N. Treps, B.C. Buchler, R. Schnabel, T.C. Ralph, T. Symul et P.K. Lam, Unity gain and non-unity gain quantum teleportation, *IEEE J. of Quant. Elect.* **9**, 1519 (2003).

[151] W.P. Bowen, R. Schnabel, P.K. Lam et T.C. Ralph, Experimental investigation of criteria for continuous-variable entanglement, *Phys. Rev. Lett.* **90**, 043601 (2004).

[152] W.P. Bowen, R. Schnabel, P.K. Lam et T.C. Ralph, Experimental characterization of continuous-variable entanglement, *Phys. Rev. A* **69**, 012304 (2004).

[153] J. Mizuno, K. Wakui, A. Furusawa et M. Sasaki, Experimental demonstration of quantum dense coding using entanglement of a two-mode squeezed vacuum state, arXiv quant-ph/0402040 (2004).

[154] L. Longchambon, J. Laurat, T. Coudreau et C. Fabre, Non-linear and quantum optics of a type II OPO containing a birefingent element Part 2 : bright entangled beams generation, *Eur. Phys. J. D* **30**, 279 et 287 (2004).

[155] J. Laurat, T. Coudreau, G. Keller, N. Treps et C. Fabre, Compact soucre of EPR entanglement and squeezing at very low noise frequencies, arXiv quant-ph/0403224 (2004).

[156] A. Ourjoumtsev, Génération et caractérisation d'impulsions laser intriquées en quadrature en régime femtoseconde, Rapport de stage de DEA de Physique Quantique, Paris (2004).

[157] **J. Wenger, A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Time-reslved homodyne characterization of individual quadrature-entangled pulses, soumis à *J. Opt. B: Quant. Semiclass. Opt.* (2004).**

Manipulation de l'information quantique avec des variables continues

[158] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W.K. Wooters, Teleporting an unknow quantum state via dual classical and Einstein Podolsky Rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).

[159] L. Vaidman, Teleportation of quantum states, *Phys. Rev. A* **49**, 1473 (1994).

[160] H.J. Briegel, W. Dur, J.I. Cirac et P. Zoller, Quantum repeaters : the role of imperfect local operations in quantum communication, *Phys. Rev. Lett.* **81**, 5932 (1998).

[161] S. Lloyd et S.L. Braunstein, Quantum computation over continuous variables, *Phys. Rev. Lett.* **82**, 1784 (1999).

[162] S.L. Braunstein et H.J. Kimble, Dense coding for continuous variables, *Phys. Rev. A* **61**, 042302 (2000).

[163] J. Eisert, S. Scheel et M.B. Plenio, Distilling Gaussian states with Gaussian operations is impossible, *Phys. Rev. Lett.* **89**, 137903 (2002).

[164] G. Giedke et J.I. Cirac, Characterization of Gaussian operations and distillation of Gaussian states, *Phys. Rev. A* **66**, 032316 (2002).

Introduction aux tests des inégalités de Bell

[165] N.D. Mermin, Is the Moon there when nobody looks ? Reality and the quantum theory, *Physics today*, avril 1985, 38 (1985).

[166] J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, 1988.

[167] J. F. Clauser, M. A. Horne, A. Shimony et R. A. Holt, Proposed experiment to test local hidden variable theories, *Phys. Rev. Lett.* **23**, 880 (1969).

[168] J. F. Clauser et M. A. Horne, Experimental consequences of objective local theories, *Phys. Rev. D* **10**, 526 (1974).

[169] A. Aspect, Proposed experiment to test the nonseparability of quantum mechanics, *Phys. Rev. D* **14**, 1944 (1976).

[170] A. Aspect, P. Grangier, et G. Roger, Experimental Tests of Realistic Local Theories via Bell's Theorem, *Phys. Rev. Lett.* **47**, 460 (1981).

[171] A. Aspect, P. Grangier, et G. Roger, Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities, *Phys. Rev . Lett.* **49**, 91 (1982).

[172] A. Aspect, J. Dalibard, et G. Roger, Experimental Test of Bell's Inequalities Using Time- Varying Analyzers, *Phys. Rev. Lett.* **49**, 1804 (1982).

[173] A. Aspect, Bell's theorem : the naive view of an experimentalist, arXiv quant-ph/0402001 (2004).

[174] A.G. Valdenebro, Assumptions underlying Bell's inequalities, *Eur. Phys. J.* **23**, 1 (2002).

[175] E. Santos, Critical analysis of the empirical tests of local hidden-variable theories, *Phys. Rev. A* **46**, 3646 (1992).

[176] Philip M. Pearle, Hidden-Variable Example Based upon Data Rejection, *Phys. Rev. D* **2**, 1418 (1970).

[177] N. Gisin et B. Gisin, A local hidden variable model of quantum correlation exploiting the detection loophole, *Phys. Lett. A* **260**, 323 (1999).

[178] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter et A. Zeilinger, Violation of Bell's Inequality under Strict Einstein Locality Conditions, *Phys. Rev. Lett.* **81**, 5039 (1998).

[179] M.A. Rowe, D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe et D.J. Wineland, Experimental violation of a Bell's inequality with efficient detection. *Nature* **409**, 791 (2001).

[180] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden et N. Gisin, Experimental demonstration of quantum correlations over more than 10 km, *Phys. Rev. A* **57**, 3229 (1998).

[181] B.S. Cirel′son, Quantum generalizations of Bell's inequality, *Lett. Math. Phys.* **4**, 93 (1980).

[182] C. Brukner, M. Zukowsky, J.W. Pan et A. Zeilinger, Violation of Bell's inequality : criterion for quantum communication complexity advantage, arXiv quant-ph/0210114 (2002).

Tests des inégalités de Bell avec des variables continues

[183] A. Gilchrist, P. Deuar et M. D. Reid, Contradiction of quantum mechanics with local hidden variables for quadrature phase amplitude measurements, *Phys. Rev. Lett.* **80**, 3169 (1998).

[184] A. Gilchrist, P. Deuar et M. D. Reid, Contradiction of quantum mechanics with local hidden variables for quadrature phase amplitude measurements on pair coherent states and squeezed macroscopic superpositions of coherent states, *Phys. Rev. A* **60**, 4259 (1999).

[185] W. J. Munro, Optimal states for Bell inequality violations using quadrature-phase homodyne measurements, *Phys. Rev. A* **59**, 4197 (1999).

[186] G. Auberson, G. Mahoux, S.M. Roy et V. Singh, Bell inequalities in phase space and their violation in quantum mechanics, arXiv quant-ph/0205157. Voir aussi arXiv quant-ph/0205185 (2002).

[187] **J. Wenger, M. Hafezi, F. Grosshans, R. Tualle-Brouri et P. Grangier, Maximal violation of Bell inequalities using continuous-variable measurements, *Phys. Rev. A* 67, 012105 (2003).**

[188] **R. Garcia-Patron Sanchez, J. Fiurášek, N.J. Cerf, J. Wenger, R. Tualle-Brouri et P. Grangier, Proposal for a loophole-free Bell test using homodyne detection, accepté pour publication dans *Phys. Rev. Lett.* (2004). Voir aussi arXiv quant-ph/0403191.**

[189] H. Nha et H.J. Carmichael, Proposed test of quantum nonlocality for continuous variables, *Phys. Rev. Lett.* **93**, 020401 (2004).

[190] R. Garcia-Patron Sanchez, J. Fiurášek, et N.J. Cerf, Loophole-free test of quantum non-locality using high-efficiency homodyne detectors, arXiv quant-ph/0407181 (2004).

[191] D. Gottesman, A. Kitaev et J. Preskill, Encoding a qubit in an oscillator, *Phys. Rev. A* **64**, 012310 (2001).

[192] B. C. Travaglione et G. J. Milburn, Preparing encoded states in an oscillator, *Phys. Rev. A* **66**, 052322 (2002).

[193] S. L. Braunstein et C. M. Caves, Information-theoretic Bell inequalities, *Phys. Rev. Lett.* **61**, 662 (1988).

[194] N. J. Cerf et C. Adami, Entropic Bell inequalities, *Phys. Rev. A* **55**, 3371 (1997).

[195] M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J.-M. Raimond et S. Haroche, Observing the progressive decoherence of the "meter" in a quantum measurement, *Phys. Rev. Lett.* **77**, 4887 (1996).

[196] J. Fiurášek, S. Massar et N.J. Cerf, Conditional generation of arbitrary multimode entangled states of light with linear optics, *Phys. Rev. A* **68**, 042325 (2003).

Variables continues en polarisation

[197] B. Julsgaard, A. Kozhekin et E.S. Polzik, Experimental long-lived entanglement of two macroscopic objects, *Nature* **413**, 400 (2001).

[198] W.P. Bowen, N. Treps, R. Schnabel et P.K. Lam, Experimental demonstration of continuous variable polarization entanglement, *Phys. Rev. Lett* **89**, 253601 (2002).

[199] O. Glöckl, J. Heersink, N. Korolkova, G. Leuchs et S. Lorenz, A pulsed source of continuous variable polarization entanglement, *J. Opt. B: Quant. Semiclass. Opt.* **5**, S492 (2003).

[200] V. Josse, A. Dantan, L. Vernac, A. Bramati, M. Pinard et E. Giacobino, Polarization squeezing with cold atoms, *Phys. Rev. Lett* **91**, 103601 (2003).

[201] V. Josse, A. Dantan, A. Bramati, M. Pinard et E. Giacobino, Continuous variable entanglement using cold atoms, *Phys. Rev. Lett* **92**, 123601 (2004).

Divers

[202] J.-L. Basdevant et J. Dalibard, Mécanique quantique - recueil de problèmes, Ecole Polytechnique, Palaiseau (2002). Voir le problème 4 proposé par Philippe Grangier.

[203] W.H. Press, S.A. Teutolsky et W.T. Vetterling, *Numerical Recipes in C. The art of scientific computing*, Cambridge University Press, Cambridge, (1992).

[204] G. Brassard, communication personnelle (2004).