Dispositifs pour la cryptographie quantique

Rosa Tualle-Brouri

▶ **To cite this version:**

Rosa Tualle-Brouri. Dispositifs pour la cryptographie quantique. Physique Atomique [physics.atom-ph]. Université Paris Sud - Paris XI, 2006. tel-00369277

HAL Id: tel-00369277
https://theses.hal.science/tel-00369277

Submitted on 18 Mar 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

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

Mémoire pour l'obtention du diplôme
d'Habilitation à Diriger des Recherches

par

Rosa TUALLE-BROURI

Sujet :

DISPOSITIFS POUR LA CRYPTOGRAPHIE QUANTIQUE

Soutenue le 21 septembre 2006 devant le jury:

M.	Jean-Michel LOURTIOZ	Président
M.	Pierre GLORIEUX	Rapporteur
M.	Juan-Ariel LEVENSON	Rapporteur
M.	Jean-François ROCH	Rapporteur
M.	Nicolas CERF	
M.	Philippe GRANGIER	

Table des matières

Présentation du manuscrit

Ce mémoire couvre l'ensemble de mes activités de recherche au laboratoire Charles Fabry, dans le groupe d'optique quantique dirigé par Philippe Grangier. Ces activités entrent dans le cadre de l'information quantique, discipline au carrefour de la théorie de l'information et de la mécanique quantique. Nous nous sommes ainsi attachés à synthétiser et à étudier différents états quantiques de la lumière, avec pour objectif la mise au point de protocoles de cryptographie quantique. Il existe en effet un intérêt croissant pour ces protocoles, avec de nombreux investissements dans ce domaine.

J'ai ainsi consacré mes deux années post-doctorales à la conception d'une source de photons uniques déclenchée, qui nous a permis de réaliser dès 2002 la première expérience de cryptographie quantique utilisant ce type de source. Parallèlement à cette activité, j'ai également travaillé à la réalisation d'un dispositif de cryptographie à variables continues, proposé par Frédéric Grosshans et Philippe Grangier, qui s'est révélé être très performant. L'information est ici codée sur les quadratures d'une impulsion lumineuse: par rapport à d'autres expériences sur les variables continues, où un analyseur de spectre sélectionnant une bande de fréquence étroite est généralement utilisé, notre dispositif se distingue en ce que l'on mesure ici une quadrature associée à une impulsion lumineuse unique.

Le succès de ces expériences utilisant les variables continues en régime impulsionnel nous a incité à aller plus loin dans leur étude en adaptant les outils de l'optique quantique, pour la génération d'états comprimés ou d'états intriqués, à ce régime impulsionnel. Nous avons ainsi initié une série d'expériences utilisant le niobate de potassium comme amplificateur paramétrique optique. Si ce travail a pour objectif la mise au point de techniques permettant d'augmenter la portée des protocoles de cryptographie à variables continues, nous avons montré qu'il pouvait également permettre une violation sans échappatoire des inégalités de Bell.

Le manuscrit est organisé en quatre chapitres de la manière suivante :

Chapitre 1: Cryptographie et Théorie de l'information

Il m'a semblé indispensable d'inclure un chapitre d'introduction présentant les différentes techniques de la théorie de l'information que nous avons été amenés à utiliser. Les différents concepts permettant de quantifier l'information seront ainsi présentés, et notamment le concept d'information mutuelle, qui détermine la quantité maximale d'information pouvant être transmise par un canal bruité. Les techniques de correction d'erreurs, qui permettent d'approcher cette limite, seront abordées, ainsi que la notion d'amplification de confidentialité, essentielle pour l'extraction d'une clé secrète. L'analyse de la sécurité du protocole à variables discrètes BB84 sera discutée dans le cas des attaques dites "individuelles". Le problème de la sécurité inconditionnelle de ce protocole sera également évoqué.

Chapitre 2: Réalisation d'une source de photons uniques déclenchée

La sécurité du protocole BB84, présenté au chapitre 1, est notamment liée à l'émission de photons uniques. Disposer d'une source déclenchée de photons uniques pourrait donc permettre d'améliorer sensiblement les performances d'un dispositif de cryptographie basé sur ce protocole. Nous commencerons par montrer qu'il est possible de réaliser un tel dispositif en excitant un centre émetteur par une impulsion lumineuse suffisamment courte et suffisamment intense.

Le centre émetteur que nous avons sélectionné pour notre expérience est un défaut du cristal de diamant: le centre NV (Nitrogen-Vacancy). Ses propriétés photo-physiques, et notamment sa photo-stabilité, en font un candidat de choix pour la réalisation d'une source performante et fiable. Nous avons développé un dispositif de microscopie confocale afin d'exciter un centre unique et d'en collecter la lumière de fluorescence. Des mesures d'autocorrélation nous ont permis, par l'observation du phénomène de dégroupement de photons, de nous assurer de l'unicité du centre émetteur et d'en déterminer les paramètres photo-physiques.

L'étape suivante a consisté en la réalisation d'une source laser impulsionnelle, utilisée pour l'excitation du centre émetteur. Nous avons ainsi obtenu l'émission d'un train de photons uniques, utilisable en cryptographie quantique.

Le protocole BB84 peut être mis en œuvre en codant chaque bit d'information sur l'état de polarisation d'un photon unique. Deux bases de polarisations doivent alors être utilisées (on pourra par exemple utiliser une base de polarisations linéaires et une base de polarisations circulaires). La mise en œuvre de ce protocole sera présentée, ainsi que les performances que nous avons pu obtenir.

Ce travail a fait l'objet de la thèse d'Alexios Beveratos, soutenue le 20 décembre 2002.

Articles annexés au chapitre:

[2.1] R. Brouri, A. Beveratos, J. P. Poizat, P. Grangier, Single photon generation by pulsed excitation of a single dipole, *Phys. Rev. A* **62**, 063814 (2000).

[2.2] R. Brouri, A. Beveratos, J.-Ph. Poizat et P. Grangier, Photon antibunching in the fluorescence of individual color centers in diamond, *Opt. Lett.* **25**, 1294 (2000).

[2.3] A.Beveratos, R.Brouri, J.P. Poizat et P.Grangier, Bunching and antibunching from single NV color centers in diamond, *QCM&C 3 Proceedings (Kluver Academic/Plenum Publisher).*

[2.4] A.Beveratos, R.Brouri, T.Gagoin, J.P. Poizat et P.Grangier, Nonclassical radiation from diamond nanocrystals, *Phys. Rev. A* **64**, 061802 (2001).

[2.5] A.Beveratos, S.Kühn, R.Brouri, T.Gagoin, J.P. Poizat et P.Grangier, Room temperature stable single photon source, *EPJ D* **18**, 191 (2002).

[2.6] A.Beveratos, R.Brouri, T.Gacoin, A.Villing, H.P.Poizat et P.Grangier, Single photon quantum cryptography, *Phys. Rev. Lett.* **89**, 187901 (2002).

[2.7] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle et P. Grangier, Experimental open air quantum key distribution with a single photon source, *New J. Phys* **6**, 92 (2004).

Chapitre 3: Cryptographie avec des variables continues

Ce chapitre est introduit par quelques rappels d'optique quantique, notamment sur la notion de quadratures, qui sont des observables à spectre continu. La possibilité de coder de

l'information en utilisant ces observables, c'est-à-dire sur des variables continues, avait déjà fait l'objet de plusieurs tentatives d'exploitation, mais nous avons franchi une étape importante en montrant qu'il était possible de coder une information secrète en utilisant simplement des impulsions cohérentes. Ce protocole sera exposé avec une analyse de sécurité, ainsi qu'un exemple d'attaque individuelle optimale.

La principale difficulté du dispositif expérimental a consisté en la réalisation d'une détection homodyne capable de fonctionner en régime impulsionnel à la limite du bruit quantique. Un tel dispositif, dédié à la mesure des quadratures, doit en effet combiner haute sensibilité, large bande passante et fort taux de réjection. Au final, nous avons atteint des performances très élevées, avec notamment un débit de plus de 2 bits secrets par impulsion en utilisant un canal de transmission sans pertes.

L'analyse de sécurité sera ensuite rediscutée, notamment en ce qui concerne la sécurité inconditionnelle de ce protocole. Nous concluerons sur les possibilités d'amélioration et les perspectives de ce travail, qui a fait l'objet de la thèse de Frédéric Grosshans, soutenue le 12 décembre 2002, ainsi que d'une partie de celle de Jérôme Wenger.

Articles annexés au chapitre:

[3.1] 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).

[3.2] 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).

Chapitre 4: Génération et tomographie d'états non-gaussiens en régime impulsionnel

Pour aller plus loin dans la cryptographie à variables continues, il nous faut pouvoir produire et manipuler des états quantiques plus complexes que les états cohérents. Ainsi, c'est en utilisant un cristal de niobate de potassium comme amplificateur paramétrique optique que nous avons pu générer, en régime impulsionnel, un état comprimé. Cette expérience, dont la description fait l'objet d'une importante première partie, est en fait le premier pas vers la préparation conditionnelle d'états non-gaussiens, pour laquelle le régime impulsionnel est crucial. Nous avons également réussi, par amplification paramétrique non dégénérée, à produire des paires d'impulsions intriquées en quadrature.

Tous ces savoirs-faire sont nécessaires pour réaliser des opérations telles que la purification d'intrication, par lesquelles la portée des protocoles à variables continues pourrait être considérablement augmentée. Mais nous verrons qu'en combinant impulsions intriquées et préparation conditionnelle, il est également possible d'envisager une violation sans échappatoire des inégalités de Bell.

Ce travail a fait l'objet de la thèse de Jérôme Wenger, soutenue le 9 septembre 2004.

Articles annexés au chapitre:

[4.1] 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).

[4.2] J. Wenger, J. Fiurášek, R. Tualle-Brouri, N.J. Cerf et P. Grangier, Pulsed squeezed vacuum characterization without homodyning, *Phys. Rev. A* **70** 053812 (2004).

[4.3] J. Wenger, R. Tualle-Brouri et P. Grangier, Non-gaussian statistics from individual pulses of squeezed light, *Phys. Rev. Lett.* **92**, 153601 (2004).

[4.4] J. Wenger, A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Time-resolved homodyne characterization of individual quadrature-entangled pulses, *Eur. Phys. J. D* **32** 391-396 (2005).

[4.5] 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).

[4.6] 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, *Phys. Rev. Lett.* **93** 130409 (2004).

Chapitre 1

Cryptographie et théorie de l'information

Sommaire

Avec l'explosion des télécommunications la cryptographie prend une importance tout à fait particulière, notamment dans les domaines bancaire et militaire. Nous savons depuis 1984, et l'article fondateur de C.H. Bennett et G. Brassard[17], que l'on peut tirer profit des propriétés quantiques de la lumière pour mettre au point des systèmes de cryptographie extrêmement sûrs. Si cette idée a depuis débouché sur des démonstrateurs commerciaux, elle a également ouvert une voie de recherche actuellement en pleine effervescence. De nombreux progrès, tant en optique quantique qu'en théorie de l'information, sont en effet encore attendus pour augmenter significativement la portée et le débit de ces systèmes. Cet objectif est l'élément fédérateur de mes activités de recherche depuis mon entrée dans le groupe d'Optique Quantique en 1998, avec le développement d'une source de photons uniques (chapitre 2), d'un système de cryptographie à variable continue (chapitre 3), mais aussi avec la synthèse d'états quantiques non-gaussiens

(chapitre 4), qui ouvre la possibilité de concevoir des répéteurs quantiques. J'ai choisi de consacrer un chapitre complet à l'introduction de ce manuscrit afin de présenter succinctement différents concepts de la théorie de l'information, qui ne sont pas directement l'objet des recherches de notre groupe, mais qui leur sont indissociablement liés.

1.1 Introduction

1.1.1 La problématique de la cryptographie

Nous reprendrons tout au long de ce manuscrit les conventions usuelles, à savoir qu'Alice cherche à envoyer un message confidentiel au dénommé Bob, l'espion Eve ne devant rien connaître du contenu de ce message. Trouver un système de codage inviolable n'est pas en soi une grande difficulté puisqu'il existe des solutions très simples, comme par exemple le code de Vernam:

Alice veut envoyer un message binaire M de longueur n. M est en fait un élément de $\mathbb{F}_2^n$, espace vectoriel de dimension n sur le corps binaire $\mathbb{F}_2$ (ou $\mathbb{Z}/2\mathbb{Z}$ en notation française). Rappelons que l'addition et la multiplication dans ce corps correspondent respectivement aux opérations booléennes 'ou exclusif' et 'et'. Si Alice et Bob s'accordent sur une clé secrète K de même taille que le message, choisie aléatoirement dans $\mathbb{F}_2^n$ avec une distribution uniforme, Alice pourra envoyer $C = M + K$, l'opération de décodage consistant simplement à calculer $C + K$. Ce système de codage est parfaitement sûr puisque quel que soit le message Y susceptible d'être envoyé par Alice, ce message aurait pu être codé par la clé $K_Y = C + Y$; la connaissance de C n'apporte donc aucune information à l'espion. Cette clé ne peut cependant être utilisée qu'une seule fois, puisque si M et M' sont codés par cette méthode, on aura une information sur la somme de ces messages par $C + C' = M + M'$. Ce système de codage permet donc d'envoyer un message de longueur n de façon parfaitement confidentielle, à condition d'avoir au préalable envoyé une clé de même longueur et de façon tout aussi confidentielle.

Ce problème de transmission de clé est un problème récurrent en cryptographie: Alice et Bob doivent se rencontrer au préalable pour s'accorder sur leurs clés secrètes, avant toute télétransmission. Cette difficulté est astucieusement contournée par le système de codage à clé publique RSA, inventé en 1977 par R.Rivest, A.Shamir et L.Adleman[146], qui est maintenant largement utilisé pour la sécurisation des transmissions informatiques. La clé de codage est ici différente de la clé de décodage, et il existe une réelle difficulté mathématique pour extraire la clé de décodage de la clé de codage, liée à la décomposition en facteurs premiers des très grands nombres. Il suffit donc pour Bob de distribuer publiquement la clé de codage, étant le seul à pouvoir lire les messages codés par cette clé. Ce type de codage n'est cependant jamais à l'abri d'une avancée théorique ou technologique; il suffit de rappeler que l'un des premiers algorithmes proposés pour exploiter le potentiel d'un ordinateur quantique est l'algorithme de Shor[151], qui permet justement de factoriser un nombre m en moins de $(\ln m)^3$ opérations. Et l'ordinateur quantique n'est plus aujourd'hui considéré comme un objectif inaccessible. Les avancées récentes dans ce domaine[129, 33] laissent entrevoir une issue au terme d'une trentaine d'années. Il faut réaliser que ceci pose un important problème car les secrets, militaires ou industriels, qui sont échangés aujourd'hui, ne seront pas forcément périmés à cette échéance. Si l'ordinateur quantique reste du domaine de la recherche fondamentale, à relativement long terme, la nécessité de nouveaux protocoles de cryptographie est quant à elle d'une brûlante actualité.

L'idée de la cryptographie quantique est d'utiliser les propriétés quantique de la lumière pour transmettre une clé secrète. Il existe de nombreuses façon de coder de l'information dans un système quantique[72]. On peut par exemple convenir arbitrairement qu'un photon polarisé linéairement selon une certaine direction codera le bit 0, tandis qu'un photon polarisé selon la direction

orthogonale représentera le bit 1. Mais le système peut également se trouver dans n'importe quelle superposition linéaire de ces deux états, amenant à la notion de "qubit"; c'est cette propriété qui permet potentiellement à l'ordinateur quantique de réaliser des calculs massivement parallèles. L'intérêt fondamental de cette notion en cryptographie réside dans le théorème de non-clonage[56, 180, 12, 129], qui stipule que si $\{|\psi_i\rangle\}$ est l'ensemble des états possibles d'un système quantique, il est impossible de dupliquer l'état de ce système si la famille $\{|\psi_i\rangle\}$ n'est pas orthogonale. Donc, si l'on complète les deux états de polarisation linéaire du photon ci-dessus par la possibilité de coder le bit d'information sur une autre base des états de polarisation (en convenant par exemple qu'une polarisation circulaire gauche correspond au bit 0 tandis qu'une polarisation circulaire droite correspond au bit 1), il sera impossible pour un espion de dupliquer cette famille d'états, et donc d'écouter la ligne sans perturber l'information transmise. Voici qui mène au protocole proposé par Bennett et Brassard en 1984, dit protocole $BB84$[17] :

- Alice envoie à Bob une suite binaire aléatoire, chaque bit étant codé sur l'état de polarisation d'un photon, selon l'une des deux bases rectiligne ou circulaire choisie de manière aléatoire.
- Bob mesure l'état de polarisation de chaque photon émis selon l'une de ces deux bases, choisie de manière également aléatoire.
- Alice et Bob révèlent ensuite publiquement les bases de polarisation choisies, et rejètent les données correspondant à des bases différentes.
- Alice et Bob révèlent publiquement une partie de leurs données afin d'estimer le taux d'erreur e de Bob, directement lié à une éventuelle activité d'espionnage.

S'il est avéré que la ligne n'a pas été écoutée, la clé ainsi échangée pourra ensuite être utilisée pour coder un message, en utilisant par exemple le code de Vernam. Ce protocole de cryptographie est schématisé sur la figure 1.1. Si Eve décide par exemple de mesurer l'état de polarisation du photon émis par Alice selon l'une des deux bases possibles, puis de renvoyer à Bob un autre photon polarisé selon le résultat de la mesure, on peut facilement montrer qu'elle va introduire un taux d'erreur $e = 25\%$, et se faire ainsi facilement repérer.

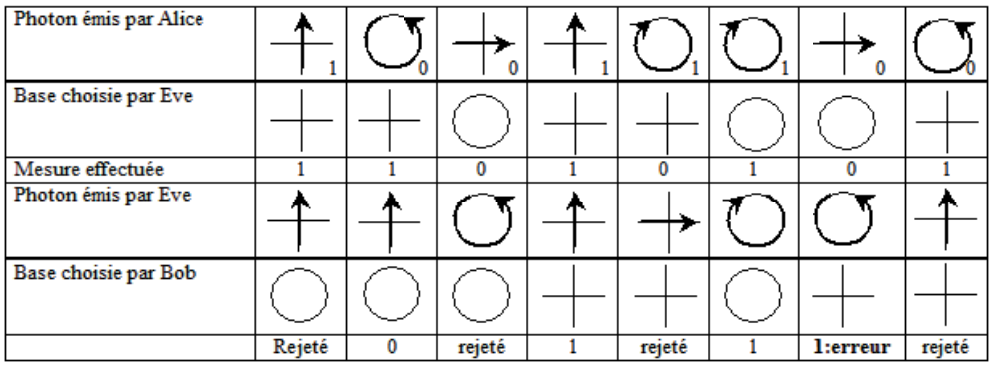

Figure 1.1: *Protocole de cryptographie $BB84$. Eve applique une stratégie d'interception-émission et introduit 25% d'erreur.*

S'assurer de la sécurité de ce protocole n'est cependant pas aussi simple. L'espion peut en effet, comme nous allons le voir maintenant, appliquer des stratégies plus subtiles que cette stratégie dite "d'interception-émission".

1.1.2 Cryptographie quantique et sécurité

L'objectif de la cryptographie quantique est donc la mise à disposition d'un protocole inconditionnellement sûr : la sécurité du protocole doit être garantie quel que soit le niveau de développement technologique de l'espion. Ce dernier peut notamment disposer de mémoires quantiques, et plus généralement d'ordinateurs quantiques d'une puissance arbitrairement grande. On pourra toutefois supposer inviolables les locaux d'Alice et Bob, ainsi que leurs dispositifs d'émission et de réception, la problématique dépassant dans le cas contraire le cadre de la simple cryptographie.

Voyons pour fixer les idées un exemple d'attaque du protocole $BB84$, tiré de l'article de revue de N. Gisin et ses collaborateurs [72]. Une stratégie assez générale consiste à intriquer des systèmes auxiliaires avec les différents qbits transmis (figure 1.2). L'espion dispose d'un système auxiliaire, initialement dans l'état $|a\rangle_i$, qu'il va faire interagir avec le i^{ime} qbit $|\psi\rangle_i$ émis par Alice. Cette interaction pourra être modélisée par une transformation unitaire U, sachant que toute transformation unitaire sur des qubits peut être simulée par un ordinateur quantique. En sortie, un photon dans l'état $|\psi_{out}\rangle_i$ est envoyé à Bob à travers un canal sans pertes, tandis que le système auxiliaire est conservé dans une mémoire quantique pour une mesure ultérieure.

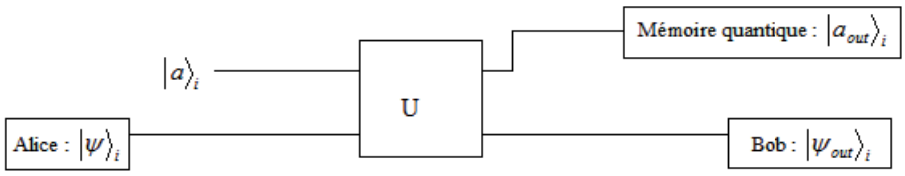

Figure 1.2: *Exemple d'attaque sur la transmission du bit quantique i.*

Etant donnée la symétrie du protocole $BB84$ entre les bases de polarisation linéaire $(|H\rangle, |V\rangle)$ et circulaire $(|+\rangle, |-\rangle)$, on s'intéressera à une attaque possédant cette symétrie. On peut alors montrer[72] que la transformation U va agir sur la base $|H\rangle, |V\rangle$ de la façon suivante:

$$\begin{aligned} \text{si } |\psi\rangle = |H\rangle, \quad & U|H,a\rangle = \sqrt{F}|H,\phi_H\rangle + \sqrt{D}|V,\theta_H\rangle \\ \text{si } |\psi\rangle = |V\rangle, \quad & U|V,a\rangle = \sqrt{F}|V,\phi_V\rangle + \sqrt{D}|H,\theta_V\rangle \end{aligned} \tag{1.1}$$

tous ces états étant normalisés, les espaces engendrés par $(|\phi_H\rangle, |\phi_V\rangle)$ et $(|\theta_H\rangle, |\theta_V\rangle)$ étant orthogonaux, avec $\langle\phi_H|\phi_V\rangle$ réel, que l'on posera égal à $\cos x$, et avec $\langle\theta_H|\theta_V\rangle = \cos y$. U étant unitaire, on a également $D + F = 1$. Ce faisant, Eve introduit des erreurs sur les données de Bob avec un taux d'erreur D.

L'attaque est symétrique, et U doit agir de façon analogue à (1.1) sur l'autre base du protocole $BB84$: $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$, avec des états $|\phi_\pm\rangle$ et $|\theta_\pm\rangle$ du système auxiliaire qui vérifient des propriétés analogues à $|\phi_{H,V}\rangle$ et $|\theta_{H,V}\rangle$, soit entre autres $\|\theta_+\|^2 = 1$. En exprimant $|\theta_+\rangle$ en fonction de $|\phi_{H,V}\rangle$ et $|\theta_{H,V}\rangle$, et en calculant le carré de sa norme, on obtient:

$$D = \frac{1 - \cos x}{2 - \cos x + \cos y} \tag{1.2}$$

On prendra par la suite $x = y$ pour simplifier les calculs (mais ce cas se trouve être optimal pour Eve).

Le système auxiliaire est donc ensuite conservé dans une mémoire quantique, jusqu'à ce que Bob révèle publiquement la base de polarisation choisie. S'il s'agit de la base $|H\rangle, |V\rangle$ (mais

on aura une procédure analogue pour l'autre base), Eve va d'abord effectuer une mesure pour savoir si son système auxiliaire se trouve dans l'espace $(|\phi_H\rangle, |\phi_V\rangle)$ ou dans $(|\theta_H\rangle, |\theta_V\rangle)$; ces deux espaces étant orthogonaux, une telle mesure ne soulève pas de difficulté fondamentale. Une autre mesure devra ensuite être effectuée pour déterminer l'état dans lequel se trouve ce système. Par exemple, si le système auxiliaire se trouve dans l'espace $(|\phi_H\rangle, |\phi_V\rangle)$, Eve va effectuer une mesure dont les vecteurs propres $|u_H\rangle$ et $|u_V\rangle$ forment une base orthogonale optimisée pour trouver le bon résultat[72, 137] (voir figure 1.3).

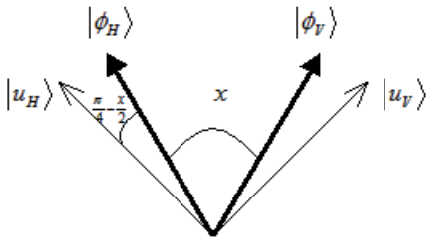

Figure 1.3: *Mesure optimale de deux états non orthogonaux.*

La probabilité pour Eve de trouver le bon résultat sera donc :

$$p_{E,opt} = \cos^2(\frac{\pi}{4} - \frac{x}{2}) = \frac{1}{2}(1 + \sin x) = \frac{1}{2}(1 + \sqrt{4D - 4D^2}) \tag{1.3}$$

Dans la stratégie d'interception-émission, la probabilité pour Eve de trouver le bon résultat était de 75% pour un taux d'erreurs introduites de 25%. Ici, on atteindra la même performance pour un taux d'erreur de $6,7\%$!

Par ailleurs, la fiabilité du protocole $BB84$ repose sur l'utilisation de photons uniques, et nous aurons l'occasion de revenir sur le fait qu'il n'existe pas de sources de photons uniques parfaites: un certain nombre d'impulsions émises contiendront deux photons ou plus. Eve peut appliquer une stratégie particulière lorsque plusieurs photons sont émis, en détectant cet événement par une mesure non destructive et en prélevant l'un des photons; elle peut dans ce cas espionner sans introduire aucune erreur.

Ainsi, malgré son apparente simplicité, il est difficile d'analyser la sûreté réelle apportée par ce protocole, et cette tâche exige de nombreuses notions de théorie de l'information. Les protocoles à variables continues que je développerai au chapitre 3 sont quant à eux absolument indissociables de cette théorie, et c'est la raison pour laquelle je propose d'en exposer succinctement les bases dans ce chapitre.

Mais pour mettre en perspective la difficulté réelle de la sécurité inconditionnelle, il faut signaler que la stratégie d'attaque qui vient d'être exposée est loin d'exploiter toutes les possibilités offertes par la mécanique quantique. En effet, Eve se contente ici d'une "attaque individuelle": elle effectue séparément des mesures sur ses systèmes auxiliaires, qui correspondent chacun à un qubit particulier émis par Alice; la stratégie appliquée à la suite de ses mesures entre dans le cadre du traitement classique de l'information. On aurait pu imaginer un cadre plus général, où Eve applique un traitement quantique (une transformation unitaire) à l'ensemble des systèmes auxiliaires mémorisés avant d'effectuer ses mesures: elle réaliserait ainsi ce que l'on désigne par "attaque collective". Plus général encore Eve pourrait, lorsqu'elle reçoit le i^{ime} qubit $|\psi\rangle_i$ émis par Alice, utiliser les systèmes auxiliaires précédemment mémorisés pour le calcul quantique de $|\psi_{out}\rangle_i$. Cette dernière attaque n'a pas de dénomination particulière, car on lui préfère l'attaque

la plus générale, l'"attaque cohérente", dans laquelle tous les qbits émis par Alice sont simultanément attaqués par Eve. Personne n'a montré la pertinence de telles attaques, mais leur existence est en soi une menace, suscitant une intense activité de recherche sur laquelle nous reviendrons au 1.3.4.

1.2 La théorie de l'information

1.2.1 L'entropie, mesure de l'information

La plupart des concepts de la théorie de l'information se trouvent dans l'article fondateur de C. Shannon[149]. Le premier d'entre eux est le concept d'entropie comme mesure de l'information. Considérons un message M choisi aléatoirement dans un ensemble fini $\mathbf{M}$ avec une distribution de probabilité p; on définit l'entropie par:

$$H(M) = -\sum_{m\in\mathbf{M}} p(M=m)\log_2 p(M=m) \tag{1.4}$$

Cette quantité est évidemment positive, et elle est maximale lorsque tous les messages sont équiprobables. Elle vaut dans ce cas $H(M) = \log_2 |\mathbf{M}|$, la notation $|\mathbf{M}|$ désignant le cardinal de $\mathbf{M}$. Cette dernière expression est particulièrement simple à interpréter, puisqu'il s'agit du nombre de bits nécessaires pour énumérer tous les messages de $\mathbf{M}$ (le choix de la base 2 pour le logarithme définit l'unité de H comme étant le bit d'information).

Pour comprendre plus précisément la signification de l'entropie, considérons maintenant les messages constitués de n symboles indépendants, tirés d'un alphabet $\mathbf{A}$: $\mathbf{M} = \mathbf{A}^n$. La probabilité pour que la lettre $A = a$ soit utilisée est $p(a)$, et l'on peut définir l'entropie $H(A)$ d'après (1.4). Les symboles étant indépendants, on montre facilement que $H(M) = nH(A)$. Les messages ainsi émis contiendront, aux fluctuations statistiques près, $n_a \approx np(a)$ occurrences de la lettre a. On dit qu'un tel message est typique, et l'on notera $\overline{\mathbf{M}}$ l'ensemble de ces messages. La probabilité d'avoir un message atypique, c'est-à-dire s'éloignant significativement des fluctuations statistiques, est asymptotiquement nulle aux grands n. Si un message m contient n_a occurrences de la lettre a, sa probabilité est simplement

$$p(M=m) = \prod_{a\in\mathbf{A}} p(a)^{n_a} \tag{1.5}$$

et cette probabilité devient, lorsque $n_a = np(a)$:

$$p(M=m) = 2^{-nH(A)} \tag{1.6}$$

La probabilité $p(M=m)$ d'une suite typique va bien sûr fluctuer autour de cette valeur, mais on montre[149, 14] que $n^{-1}\log_2 p(M=m)$ est asymptotiquement proche de $-H(A)$ aux grands n.

Pour résumer on peut, pour toutes constantes positives η et ϵ, et pour n suffisamment grand, définir $\overline{\mathbf{M}}$ tel que[149, 14]:

$$\begin{aligned} \forall m \in \overline{\mathbf{M}}, |n^{-1}\log_2 p(M=m) + H(A)| < \eta \\ p(M \notin \overline{\mathbf{M}}) < \epsilon \end{aligned} \tag{1.7}$$

Les messages typiques sont donc en un certain sens équiprobables, même si l'on a en toute rigueur pour tout $m \in \overline{\mathbf{M}}$:

$$2^{-n[H(A)+\eta]} < p(M=m) < 2^{-n[H(A)-\eta]} \tag{1.8}$$

On peut facilement en déduire une estimation du nombre de messages typiques; la probabilité d'avoir un message typique $p(M \in \overline{\mathbf{M}}) = \sum_{m\in\overline{\mathbf{M}}} p(M=m)$ étant comprise entre $1-\epsilon$ et 1, on déduit en effet directement de (1.5) que:

$$(1-\epsilon)2^{n[H(A)-\eta]} < |\overline{\mathbf{M}}| < 2^{n[H(A)+\eta]} \tag{1.9}$$

d'où l'on tire :

$$\lim_{n\to\infty} n^{-1}\log_2|\overline{\mathbf{M}}| = H(A) = n^{-1}H(M) \tag{1.10}$$

Il est donc possible d'énumérer tous les messages typiques en utilisant (pour n suffisamment grand) en moyenne $H(A)$ bits par symbole. Ce point permet donc d'interpréter $H(A)$ comme étant le nombre de bits d'information contenus dans le symbole A, cette assertion n'ayant de sens qu'à travers l'emploi d'un grand nombre de symboles.

1.2.2 La transmission de l'information

Voyons maintenant comment quantifier l'information transmise à travers un canal bruité. Considérons comme précédemment l'envoi et la détection de n caractères: la source (Alice) émet un message X consitué de n caractères A appartenant à un alphabet $\mathbf{A}$ ($X \in \mathbf{X} = \mathbf{A}^n$); le détecteur (Bob) reçoit des caractères B d'un alphabet $\mathbf{B}$, constituant le message $Y \in \mathbf{Y} = \mathbf{B}^n$. Les 2 alphabets $\mathbf{A}$ et $\mathbf{B}$ sont généralement identiques, et s'ils sont de plus munis d'une addition on pourra définir l'erreur $E = Y - X$ commise par Bob.

Nous supposerons que les caractères émis par la source sont indépendants, et que la ligne de transmission est "sans mémoire", c'est-à-dire que les caractères reçus sont également indépendants. La transmission est alors complètement décrite par la probabilité conjointe $p(a,b)$. Cette distribution permet sans équivoque de définir l'entropie conjointe $H(A,B)$. Les caractères étant indépendants, on a $H(X,Y) = nH(A,B)$. Comme nous l'avons vu à la section précédente, $H(A,B)$ représente le nombre moyen de bits par symbole nécessaire pour dénombrer les couples (X,Y) typiques. Comme $H(B)$ bits par symbole sont nécessaires pour dénombrer les messages Y typiques, Bob doit disposer d'au moins $H(A|B)$ bits par symboles supplémentaires pour déterminer le message X, où $H(A|B)$ est l'entropie conditionnelle de A sachant B, définie par:

$$H(A|B) = H(A,B) - H(B) \tag{1.11}$$

On parle également pour $H(A|B)$ d'ambiguité, puisqu'il s'agit de l'information minimale qui manque à Bob pour corriger ses erreurs et connaître parfaitement le message d'Alice. Cela signifie que l'information maximale que Bob a sur les données d'Alice est:

$$I(A;B) = H(A) - H(A|B) = H(A) + H(B) - H(A,B) = H(B) - H(B|A) \tag{1.12}$$

$I(A;B)$ est l'information mutuelle. On peut facilement se convaicre que cette quantité est positive, puisque l'ambiguité $H(A|B)$ ne saurait être supérieure à $H(A)$. Elle est de plus symétrique

par rapport à A et B; elle représente en fait la quantité maximale d'information partagée par Alice et Bob à l'issue de la transmission par le canal bruité, et c'est la raison pour laquelle on parle d'information mutuelle. Cette symétrie a une conséquence très importante en cryptographie:

On peut en effet considérer que Bob a une ambiguïté sur le message envoyé par Alice, et que cette dernière doit envoyer au moins $nH(A|B)$ bits d'information pour lever cette ambiguïté. Ceci est le principe de la réconciliation mono-directionnelle, schématisé sur la figure 1.4, qui est très proche de la notion de codage de canal initialement introduite par C. Shannon[149]. Mais on peut également considérer qu'Alice à une ambiguïté sur le message reçu par Bob, qui devra envoyer au moins $nH(B|A)$ bits d'information pour lever cette ambiguïté, suivant le principe décrit sur la figure 1.5; on parle dans ce cas de réconciliation inverse, et nous aurons l'occasion de revenir sur son intérêt. Dans les deux cas Alice et Bob partageront un même message après la phase de réconciliation, qui sera selon le cas le message envoyé par Alice ou le message reçu par Bob.

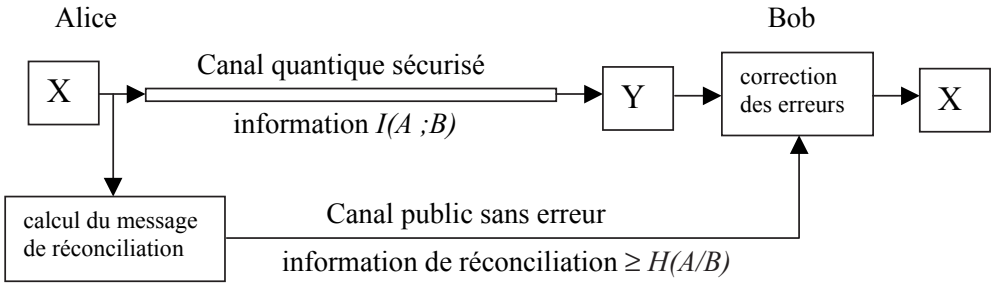

Figure 1.4: *Schéma de principe de la réconciliation mono-directionnelle. Alice envoie des données supplémentaires par un canal public sans erreur.*

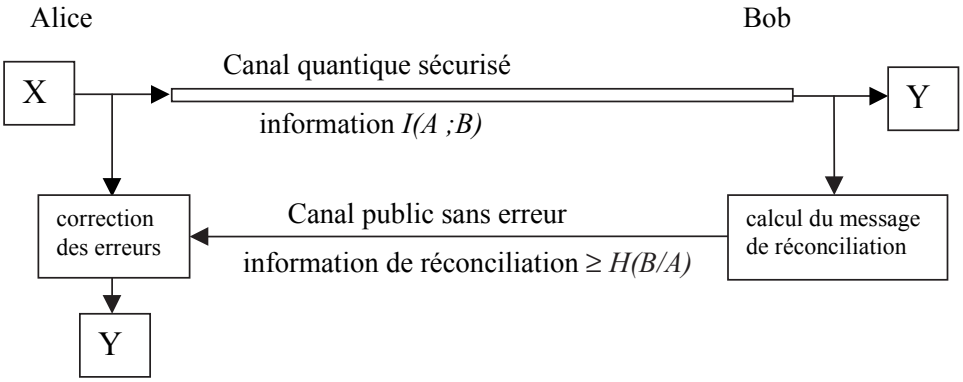

Figure 1.5: *Schéma de principe de la réconciliation mono-directionnelle inverse. Bob envoie des données de réconciliation à Alice. Le message réconcilié est Y.*

La capacité du canal est définie comme:

$$C = \max_{p(a)} I(A;B) \tag{1.13}$$

et la source dont la loi de probabilité $p(a)$ permet d'atteindre la capacité du canal est dite

adaptée à ce canal.

Remarquons sur les figures 1.4 et 1.5 que l'information de réconciliation est transmise à travers un canal public sans erreur. Ce canal n'est a priori pas sécurisé, et cette information est donc accessible à l'espion Eve. Comme il s'agit a priori de données complexes, il est difficile d'estimer l'usage qu'elle pourra en faire. Un moyen pour contourner cette difficulté consiste à crypter[106] ces données à l'aide d'une clé secrète de taille r partagée au préalable par Alice et Bob. On peut admettre l'existence de cette clé préalable, puisqu'Alice et Bob doivent de toute façon partager initialement une certaine quantité d'information secrète à des fins d'authentification. Mais il peut paraître paradoxal d'utiliser une clé de cryptage pour un protocole destiné justement à distribuer une clé de cryptage. Cette démarche est cependant pertinente si la clé distribuée est plus grande que la clé de cryptage utilisée: Alice et Bob retranchent alors une clé de taille r de cette clé distribuée, pour une utilisation ultérieure. On parlera alors de protocole d'amplification de clé secrète plutôt que de protocole de distribution de clé secrète.

Qu'en est-il de la mise en pratique de ces concepts. Il se trouve qu'il existe maintenant différents protocoles de réconciliation mono-directionnelle, tels que les Turbo-codes[22] ou les codes LDPC[32], qui affichent des performances proches des limites prévues par la théorie de l'information de Shannon. Ces protocoles sont toutefois très récents, et ce ne sont pas ceux que nous avons utilisé dans les travaux exposés au cours de ce mémoire. Nous avons utilisé un autre schéma de réconciliation: la réconciliation interactive, ou bidirectionnelle, dont nous allons maintenant aborder le principe.

1.2.3 La réconciliation interactive

Nous avons donc été amenés à utiliser la reconciliation interactive binaire, avec des alphabets binaires $\mathbf{A}$ et $\mathbf{B}$ identiques pour Alice et Bob: $\mathbf{A} = \mathbf{B} = \mathbb{F}_2$. Nous avons notamment adopté ce type de réconciliation pour implémenter le protocole BB84 avec notre source de photons uniques déclenchée (chapitre 2). Dans le cas du protocole BB84, on se touve dans la situation particulière d'un canal à bruit additif: l'erreur $E = Y - X$ est indépendante de X.

Nous avons vu au 1.2.2 qu'Alice et Bob devaient, pour corriger leurs erreurs, s'échanger un message de réconciliation de taille r supérieure à l'ambiguïté:

$$r \gtrsim H(X|Y) = nH(A|B) \tag{1.14}$$

Ouvrons ici une petite parenthèse concernant les bruits additifs: comme le bruit additif E est indépendant de X, on aura[1]

$$H(Y|X) = H(X + E|X) = H(E) = nh(e) \tag{1.15}$$

où $h(e)$ est l'entropie associée au taux d'erreur e:

$$h(e) = -e \log_2 e - (1 - e) \log_2 (1 - e) \tag{1.16}$$

Si de plus les bits 0 et 1 sont équiprobables dans X, ils seront également équiprobables dans Y; on aura donc dans ce cas $H(X) = H(Y) = n$, et (1.12) implique alors directement

$$H(X|Y) = H(Y|X) = nh(e) \tag{1.17}$$

[1] Les couples de messages (X, Y) sont en correspondance biunivoque avec les couples (X, E), ce qui implique $H(X, Y) = H(X, E)$. Si E est indépendant de X, on montre simplement que $H(X, E) = H(X) + H(E)$, d'où ce résultat.

La minoration 1.14 devient ainsi:

$$r \gtrsim nh(e) \tag{1.18}$$

Alice et Bob peuvent donc corriger leurs erreurs en s'échangeant au moins $nh(e)$ bits d'information. Pour concrétiser cette phase de réconciliation, nous avons utilisé le logiciel de réconciliation intéractive "Cascade", développé par G. Brassard et L. Savail[34]. Ce logiciel corrige les erreurs par révélation de parité, et voici brièvement son principe:

La parité d'un bloc est simplement la somme de ses bits. Si les parités de x et y diffèrent, il y a forcément une erreur qui pourra être précisée par dichotomie: on coupe les messages en deux parties, et l'on désigne la seule de ces parties pour laquelle les parités d'Alice et Bob vont encore différer. Par itération, cette procédure permet de désigner l'emplacement exact de l'erreur. Le logiciel Cascade va appliquer cette procédure de dichotomie non aux messages eux-mêmes, mais à des blocs issus d'une partition de ces messages: L'algorithme comprendra ρ étapes, et utilisera pour l'étape i une partition aléatoire des messages en blocs de taille k_i , où $k_{i+1} = 2k_i$ et où k_1 est déterminé empiriquement en fonction du taux d'erreurs par $k_1 \approx 0.73/e$. Dès qu'une erreur est repérée, une détection dichotomique est effectuée de nouveau sur tous les blocs qui contenaient cette erreur lors des étapes précédentes, cette dernière ayant été masquée par au moins une autre erreur. Typiquement, on démarre donc avec des blocs qui contiennent en moyenne un peu moins d'une erreur, et au fur et à mesure que les erreurs sont corrigées, on considère des blocs de plus en plus gros. Le nombre total d'étapes à effectuer vérifie $2^\rho k_1 > n$.

Ce logiciel affiche de bonnes performances, avec un nombre de bits de parité révélés par Alice égal à:

$$r = nf(e)h(e) \tag{1.19}$$

où $f(e) \approx 1.16$ pour un taux d'erreurs inférieur à 5%[34, 113]. Il faut toutefois remarquer que, pour chaque bit de parité révélé par Alice, Bob annonce si sa propre parité est correcte ou non, ce qui revient à révéler son propre bit de parité. A l'issue de la réconciliation, Alice aura donc transmis un message R_A de taille r contenant les parités qu'elle a calculées, et Bob aura transmis un message R_B de même taille et contenant ses propres parités. On a donc au final $2r$ bits échangés. Pour définir une clé secrète, il faudra donc savoir quelle quantité d'information est vraiment utile à Eve.

Comme dans le cas de la réconciliation mono-directionnelle, on pourra crypter les messages de réconciliation. L'usage de deux clés de codage différentes pour R_A et R_B conduirait effectivement à un coût peu performant de $2r$ bits d'information pour la phase de réconciliation. Mais nous allons maintenant supposer qu'Alice et Bob utilisent une même clé Q de taille r pour coder à la fois R_A et R_B: si le code de Vernam est utilisé pour ce cryptage, l'espion ne pourra connaître que $(Q + R_A) + (Q + R_B) = R_A + R_B$. L'espion sait donc si les parités d'Alice et Bob sont égales ou non et, connaissant Cascade, il peut exactement savoir sur quels blocs ces parités ont été calculées. Il peut donc connaître, avec le processus de dichotomie, la position de toutes les erreurs $\varepsilon = x+y$, où ε, x et y sont respectivement des réalisations de E, X et Y. Réciproquement, la connaissance de ε permet de calculer R_A+R_B. Donc si l'on crypte les messages d'Alice et Bob avec une seule clé Q de taille r, la seule information pour l'espion sera la position des erreurs ε.

Dans le cas du protocole $BB84$ il apparaît clairement que ε n'apporte pour l'espion aucune information pertinente, puisque les erreurs de Bob sont indépendantes des données envoyées par Alice. Dans ce cas précis, on peut donc effectivement comptabiliser l'information révélée lors

de la réconciliation comme valant $r = nf(e)h(e)$ bits (qui ont été utilisés pour le cryptage des données). On ne sera cependant pas toujours dans ce cas, et nous aurons à reprendre cette discussion au chapitre 3, où il faudra alors explicitement calculer l'information apportée par ε.

1.2.4 Théorie de l'information avec des variables continues

Avant d'aborder la suite de ce chapitre, qui sera plus particulièrement consacrée à l'étude d'alphabets binaires, voyons ce que deviennent les notions que nous venons d'exposer dans le cas d'un alphabet défini sur un continuum, tel que nous pourrons en rencontrer dans les expériences de cryptographie à variables continues présentées au chapitre 3.

Considérons par exemple une variable aléatoire A à valeurs réelles, associée à une densité de probabilité $\pi(a)$. Si l'on discrétise l'axe réel en cellules de taille δa, on peut introduire:

$$p_i = p(A \in [a, a + \delta a[) \approx \pi(a)\delta a \tag{1.20}$$

ainsi que

$$H_{\delta a}(A) = -\sum_i p_i \log_2 p_i \approx -\int \pi(a) \log_2 \pi(a) da - \log_2 \delta a \tag{1.21}$$

L'entropie est donc a priori infinie lorsque $\delta a \to 0$, ce qui n'a rien d'étonnant s'agissant d'un continuum. On peut cependant associer à A l'entropie différentielle :

$$H_d(A) = -\int \pi(a) \log_2 \pi(a) da \tag{1.22}$$

Cette quantité n'est définie qu'à une constante près et n'est donc plus nécessairement positive, mais on peut lui donner un sens comme nous allons le voir. Signalons également qu'à variance fixée ($V_A =< A^2 > - < A >^2$), la distribution qui maximise $H_d(A)$ est une gaussienne, et on a alors:

$$H_d(A) = H_{V_A}^{max} = \frac{1}{2} \log_2(2\pi e V_A) \tag{1.23}$$

(le fait qu'une gaussienne maximise $H_d(A)$ se démontre simplement[80] en optimisant $H_d(A)$ sous les contraintes $\int \pi(a)da = 1$ et V_A fixée, en utilisant la méthode des multiplicateurs de Lagrange).

Il est à noter que ce résultat se généralise au cas d'une variable gaussienne $\overrightarrow{X}$ définie dans un espace de dimension n avec [80]:

$$H_d(\overrightarrow{X}) = \frac{1}{2} \log_2((2\pi e)^n |K|) \tag{1.24}$$

où K est la matrice de covariance[2] de la distribution.

Pour une variable continue B, on aura de façon équivalente à (1.21) et (1.22):

$$H_{\delta b}(B) = H_d(B) - \log_2 \delta b \tag{1.25}$$

avec pour l'entropie conjointe:

$$H_{\delta a, \delta b}(A, B) = H_d(A, B) - \log_2 \delta a - \log_2 \delta b \tag{1.26}$$

[2]La matrice de covariance K est définie pour des variables centrées par $K_{ij} =< X_i X_j >$. La distribution $\pi(\overrightarrow{X})$ d'une variable gaussienne s'écrit $\pi(\overrightarrow{X}) \propto exp(-{}^t\overrightarrow{X} K^{-1} \overrightarrow{X}/2)$

et, pour l'information mutuelle:

$$I(A;B) = H_d(A) + H_d(B) - H_d(A,B) \tag{1.27}$$

Ainsi, contrairement à l'entropie, l'information mutuelle $I(A;B)$ ne dépend pas de δa et δb, et est donc parfaitement définie dans la limite du continuum.

Donc, même si la quantité d'information contenue dans une variable continue est potentiellement infinie, l'information mutuelle reste finie après transmission par un canal bruité.

Fort de ces considérations, voyons maintenant le cas simple des canaux à bruit additif gaussien qui nous sera particulièrement utile par la suite. On a dans ce cas $B = A + N$, où N est un bruit indépendant de A. On a alors $H_d(B|A) = H_d(N)$ et $I(A;B) = H_d(B) - H_d(N)$. Comme le bruit est fixé par les caractéristiques physiques du canal, optimiser $I(A;B)$ revient à optimiser $H_d(B)$. Si l'on considère des signaux centrés et que l'on fixe l'énergie moyenne $< B^2 >$ du signal reçu, cette dernière quantité est maximale pour une distribution gaussienne, et d'après (1.23) on obtient pour la capacité de canal :

$$C = \frac{1}{2}\log_2 \frac{< B^2 >}{< N^2 >} = \frac{1}{2}\log_2[1 + \frac{< A^2 >}{< N^2 >}] \tag{1.28}$$

Nous avons supposé ici que le bruit N était indépendant de A, ce qui a considérablement simplifié l'évaluation de $H_d(B|A)$. On peut cependant reformuler le problème de façon à ne pas utiliser cette hypothèse, ce qui est par exemple nécessaire pour calculer $H_d(A|B)$:

Le couple de variable (A,B) peut être vu comme une variable gaussienne dans un espace de dimension 2. D'après (1.24) on a alors:

$$H_d(A,B) = \frac{1}{2}\log_2((2\pi e)^2|K|) = \frac{1}{2}\log_2((2\pi e)^2[< A^2 >< B^2 > - < AB >^2]) \tag{1.29}$$

d'où l'on tire

$$H_d(A|B) = H_d(A,B) - H_d(B) = \frac{1}{2}\log_2(2\pi e V_{A|B}) \tag{1.30}$$

où l'on a défini la variance conditionnelle:

$$V_{A|B} =< A^2 > - \frac{< AB >^2}{< B^2 >} \tag{1.31}$$

La variance conditionnelle peut s'interpréter de la manière suivante: Lorsque Bob fait sa mesure B, il en déduit une estimation αB du signal A émis par Alice, α étant un nombre réel, et commet une erreur $\epsilon = A - \alpha B$. La variance conditionnelle est la valeur minimale de la variance de cette erreur obtenue, pour des variables centrées, pour :

$$\alpha = \frac{< AB >}{< B^2 >} \tag{1.32}$$

La variance conditionnelle est relative à l'ambiguïté sur A sachant B, ce qui justifie (1.30) à posteriori. L'information mutuelle s'écrit quant à elle :

$$I(A;B) = H_d(A) - H_d(A|B) = \frac{1}{2}\log_2 \frac{< A^2 >}{V_{A|B}} \tag{1.33}$$

On vérifiera aisément sur cet exemple l'équivalence des relation (1.28) et (1.33). Tous ces résultats (1.28-1.33) sont valables pour des signaux centrés. Dans le cas général, on introduira simplement les variables centrées $A' = A - < A >$, $B' = B - < B >$.

1.3 La transmission d'une clé secrète

1.3.1 Introduction

Nous avons vu différentes voies pour corriger les erreurs lors d'une transmission; il s'agit maintenant de reprendre notre objectif, qui est la distribution d'une clé secrète K. Par clé secrète, on entend avec Shannon que malgré l'information Z dont il dispose, l'espion n'a aucune information sur cette clé:

$$I(K;Z) = 0 \Leftrightarrow H(K|Z) = H(K) \tag{1.34}$$

Comme $I(X;Y)$ correspond à l'information que Bob a des données d'Alice, et comme $I(X;Z)$ correspond à l'information qu'Eve a des données d'Alice, on pourrait croire en la possibilité qu'ont Alice et Bob d'extraire une clé secrète binaire de taille :

$$k_f \lesssim I(X;Y) - I(X;Z) \tag{1.35}$$

Imre Csiszár et János Körner ont concrétisé cette intuition en construisant[50] un codage de canal réalisant cette objectif pour des attaques individuelles[3]. Cette construction n'est pas applicable en pratique, mais permet de montrer que cette borne est accessible. Elle ne permet cependant pas de montrer que cette borne est une borne supérieure pour le système de communication utilisé, et il se trouve que ce n'est généralement pas le cas, comme le note Ueli Maurer[118]:

Si Alice envoie un message binaire X dans un canal à bruit additif E, Bob recevra $Y = X+E$. Si le canal d'écoute d'Eve est également à bruit additif, Eve recevra $Z = X + D$. Supposons maintenant que Bob renvoie à Alice un message aléatoire V codé par Y dans un canal classique sans erreur: Alice recevra $W = Y + V$. Comme $W + X = V + E$ et $W + Z = V + E + D$, tout se passe comme si Bob avait envoyé à Alice un message V avec une erreur E, Eve cumulant quant à elle ses propres erreurs à celles de Bob dans sa tentative d'espionnage. Ces considérations permettent à Ueli Maurer de conclure que l'on peut également extraire une clé secrète de taille $I(Y;X) - I(Y;Z)$. Ce résultat s'interprète très simplement en terme de réconciliation inverse: si la clé secrète est extraite à partir des données de Bob et non de celles d'Alice, c'est la connaissance qu'Eve a des données de Bob qui est pertinente, et qui doit être retranchée. Ce point est crucial en cryptographie, car cette seconde borne est généralement plus élevée, Eve ayant moins d'informations qu'Alice sur les données de Bob. C'est ce type de résultat qui a été utilisé dans nos protocoles à réconciliation inverse, que nous développerons au chapitre 3.

Résumons la situation: comme nous l'avons vu, le principe de la réconciliation interactive est d'échanger une information R sur un canal public de façon à corriger les erreurs de Bob; on a alors $H(X|Y,R) = 0$ et $I(X;Y,R) = H(X)$. Considérons que, comme il est préférable, l'information R est cryptée et n'est donc pas connue de l'espion. La relation (1.35) s'écrit alors simplement dans ce cas:

$$k \lesssim I(X;Y,R) - I(X;Z) = H(X) - I(X;Z) = H(X|Z) \tag{1.36}$$

[3]Les canaux de communication sont supposés 'sans mémoire'. Dit autrement, on considère ici que les symboles échangés sont indépendants.

ou, dans le cas de la réconciliation inverse:

$$k \lesssim I(Y;X,R) - I(Y;Z) = H(Y) - I(Y;Z) = H(Y|Z) \tag{1.37}$$

Nous cherchons donc, pour tout k vérifiant l'une ou l'autre de ces relations, à extraire une clé K vérifiant (1.34), à savoir $H(K|Z) = H(K)$. Comme $H(K|Z) \leq H(K) \leq k$, cet objectif sera atteint si

$$H(K|Z) \approx k \tag{1.38}$$

1.3.2 L'amplification de confidentialité

La technique que nous allons maintenant présenter s'applique à des données binaires, n étant la taille du message X réconcilié[4] et k étant celle de la clé K que l'on cherche à extraire. Le processus d'amplification de confidentialité revient à appliquer à X une fonction $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$, soit $f(X) = K$. L'espion peut connaître cette fonction f, mais ne doit avoir aucune information sur la clé K, soit d'après (1.38): $H(K|Z) \approx k$.

C. Bennett, G. Brassard et J.-M. Robert proposent pour cela[18] de choisir des fonctions qui ont un comportement essentiellement aléatoire, en utilisant la notion de classe universelle de fonction de hachage introduite par J.L. Carter et M.N. Wegman[43]:

Une classe $\mathbf{F}$ de fonctions de $\mathbf{A} \to \mathbf{B}$ est dite simplement universelle si, pour toute paire x_1, x_2 d'éléments distincts de $\mathbf{A}$, la probabilité que $f(x_1) = f(x_2)$ pour $f \in \mathbf{F}$ est au plus $1/|\mathbf{B}|$. C. Bennett et ses collaborateurs[21] ont quantifié l'efficacité de ces fonctions en utilisant non pas l'entropie de Shannon, mais l'entropie de Rényi d'ordre 2:

$$H_s(X) = -\log_2 \sum_x p^2(x) = -\log_2 p_c(x) \tag{1.39}$$

où $p_c(X)$ est la probabilité de collision, à savoir la probabilité pour que deux événements pris aléatoirement dans $\mathbf{X}$ soient égaux. C. Bennett et ses collaborateurs ont montré que, pour une réalisation $Z = z$ de la mesure de l'espion, on a:

$$H(K|Z=z) \;\geq\; k - 2^{k-H_2(X|Z=z)}/\ln 2 \tag{1.40}$$

On a donc $H(K|Z=z) \approx k$ si $H_2(X|Z=z) > k$. On peut facilement montrer que $H(K|Z)$ est la moyenne de $H(K|Z=z)$ sur l'ensemble des réalisations de Z. La condition de sécurité (1.38), $H(K|Z) \approx k$, est donc vérifiée si $H_2(X|Z=z) > k$ pour toute réalisation de Z (ou pour la plupart de ces réalisations[21]). On prendra de plus une petite marge de sécurité s (négligeable devant n) de façon à ce que $2^{k-H_2(X|Z)}$ soit suffisamment proche de 0:

$$H_2(X|Z=z) \;\geq\; k + s \tag{1.41}$$

Rappelons que l'on doit ôter de la clé finale une clé de même taille r que le message de réconciliation R, afin de compenser la clé qui a été utilisée pour crypter ce message. La clé finale devra donc vérifier :

$$k_f = k - r \leq H_2(X|Z=z) - r - s \tag{1.42}$$

La condition (1.41) est plus restrictive que la condition (1.36) $H(X|Z) > k$, car l'entropie de Shannon est supérieure à l'entropie de Rényi. Une minoration de l'entropie de Shannon n'est

[4] Dans le cas de la réconciliation inverse, on prendra simplement Y pour désigner le message réconcilié.

donc a priori pas suffisante pour assurer la sécurité de l'amplification de confidentialité. Nous avons vu cependant que lorsque l'on considère un grand nombre n de symboles indépendants, on pouvait réduire les ensembles de messages étudiés aux seules suites typiques, la probabilité d'avoir une suite atypique étant arbitrairement faible pour les grandes valeurs de n. Ces suites typiques ont par ailleurs une distribution quasiment uniforme (du moins sur une échelle logarithmique). Comme les entropies de Rényi et de Shannon sont égales pour une distribution uniforme, on peut écrire[119]:

$$\overline{H}_2(X|Z=z) \geq H(X|Z) - \epsilon = H(X) - I(X;Z) - \epsilon \tag{1.43}$$

avec $\epsilon \to 0$ aux grands n, et où l'entropie de Rényi $\overline{H}_2$ est restreinte aux suites typiques: on a $\overline{H}_2 > H_2$ car, contrairement au cas de l'entropie de Shannon, les suites atypiques ont une contribution non négligeable dans l'entropie de Rényi. Donc dans le cas d'un grand nombre de symboles indépendants la condition (1.36), à savoir

$$k_f = k - r \leq H(X) - r - I(X;Z) - s \quad , \tag{1.44}$$

peut garantir, dans le cadre de l'amplification de confidentialité par des fonctions de hachage, la sécurité au sens de Shannon (1.34). Précisons que le fait de considérer des symboles indépendants suppose qu'Eve se limite à des attaques individuelles des symboles émis par Bob. Pour un algorithme de réconciliation parfait, $r = H(X|Y)$ et (1.44) devient $k_f < I(X;Y) - I(X;Z)$, qui est la taille de clé donnée par Csiszár et Körner. Tout ce qui vient d'être exposé s'applique au cas de la réconciliation inverse en échangeant simplement les rôles de X et Y, ce qui permet d'extraire une clé de taille:

$$k_f = k - r \leq H(Y) - r - I(Y;Z) - s \tag{1.45}$$

1.3.3 Sécurité des protocoles de cryptographie à variables discrètes

Nous allons maintenant nous intéresser à l'analyse de la sécurité du protocole $BB84$, en fonction des différentes caractéristiques physiques de la transmission, et notamment du taux d'erreur e qu'il est d'usage d'appeler QBER (Quantum Bit Error Rate) afin d'éviter toute confusion avec le taux d'erreur final[72] (après réconciliation).

Un critère de sécurité a été proposé par N. Lütkenhaus[113, 112], dans le cas d'une attaque individuelle, en reprenant le critère (1.42) que nous venons de voir au 1.3.2, basé sur l'entropie de Rényi. L'attaque individuelle consiste pour Eve à appliquer une stratégie d'espionnage indépendante pour chaque symbole envoyé par Alice. Il n'y a donc aucune corrélation entre les données d'Alice, Eve et Bob concernant des symboles différents. On peut donc écrire :

$$p_c(X|Z=z) = \prod_{i=1}^{n} p_c(A_i|C_i=c_i) \tag{1.46}$$

où A_i et C_i sont les lettres des messages X et Z. Le nombre de bits reçus par Bob est noté n, et n'inclue pas les impulsions éliminées lorsque les bases d'Alice et Bob diffèrent: le nombre d'impulsions réellement transmises est donc $2n$. N. Lütkenhaus montre que, si un unique photon a été envoyé par Alice, et pour un QBER $e < 1/2$, on peut majorer la probabilité de collision par :

$$p_c(A_i|C_i=c_i) \leq \frac{1}{2} + 2D - 2D^2 \tag{1.47}$$

où D est l'erreur introduite par l'espion. La preuve de Lütkenhaus est très complète et nous ne la développerons pas ici. On remarquera cependant que la borne supérieure de 1.47 est atteinte avec l'attaque individuelle présentée en section 1.1.2; le fait d'utiliser un alphabet binaire permet en effet d'écrire:

$$p_c(A_i|C_i = c_i) = p^2(A_i = c_i|C_i = c_i) + p^2(A_i \neq c_i|C_i = c_i) = p_E^2 + (1 - p_E)^2 \tag{1.48}$$

p_E étant la probabilité pour Eve d'avoir la bonne estimation des données d'Alice. En prenant la valeur $p_{E,opt}$ de l'attaque, donnée par (1.3), on obtient la borne (1.47): cette attaque individuelle est donc optimale.

Pour parfaire cette analyse de sécurité, il fallait également étudier le cas correspondant à l'émission de plusieurs photons. Eve peut en effet détecter les impulsions contenant plusieurs photons par une mesure non destructive, prélever l'un des photons qu'elle placera dans une mémoire quantique (l'autre étant renvoyé vers Bob à travers un canal sans pertes), et mesurer l'état de polarisation de ce photon lorsqu'Alice et Bob révèlent les bases utilisées[35, 113]. Une telle attaque PNS (Photon Number Splitting) est irréalisable à l'heure actuelle, mais elle est possible en théorie, et l'objectif de la cryptographie quantique est de ne se baser que sur des limitations purement théoriques, liées aux lois de la physique, et non sur d'éventuelles limitations de la technologie de l'espion. On pourra donc considérer dans la suite que toute impulsion contenant plusieurs photons correspond à un bit parfaitement connu d'Eve, et ce sans qu'aucune erreur n'ait été introduite dans les données de Bob. On a donc dans ce cas $p_E = p_c = 1$. Mais l'existence des photons multiples a également une incidence dans l'évaluation de l'erreur D pouvant être introduite par l'espion:

Supposons en effet que les seules erreurs possibles soient celles introduites par l'espion. Cette hypothèse, qui signifie que l'espion a les moyens techniques d'éliminer toute autre source d'erreur, est un peu forte puisque l'espion n'est pas supposé pouvoir intervenir sur le système de Bob (nous reviendrons sur ce point au chapitre suivant). Il s'agit cependant d'une hypothèse de sécurité maximale. Dans ce cas, le nombre ne d'erreurs dans les données reçues est égal au nombre $n_1 D$ d'erreurs introduites par l'espion sur les n_1 acquisitions correspondant à l'émission d'un photon unique. On prendra donc:

$$D = \frac{n}{n_1} e \tag{1.49}$$

Il s'ensuit la minoration suivante de l'entropie de Rényi:

$$H_2(X|Z = z) \geq -n_1 \log_2(\frac{1}{2} + 2D - 2D^2) \tag{1.50}$$

minoration qui peut être utilisée dans (1.42) pour majorer la taille de la clé finale :

$$k_f \leq -n_1 \log_2(\frac{1}{2} + 2D - 2D^2) - nf(e)h(e) - s \tag{1.51}$$

où l'on a pris $r = nf(e)h(e)$ pour la taille du message de réconciliation (voir section 1.2.3). On peut reformuler cette équation en écrivant avec Lütkenhaus[113]:

$$n_1 = n - n_m \tag{1.52}$$

où n_m est le nombre d'acquisition correspondant à l'émission de plusieurs photons. n_m correspond en fait au nombre d'impulsions à photons multiples émises par la source, puisqu'Eve recense toutes ces impulsions et les envoie à Bob à travers un canal sans pertes:

$$n_m = \frac{1}{2} S_m N_{acq} \tag{1.53}$$

où N_{acq} est le nombre d'impulsions émises par la source et où S_m est la probabilité pour la source d'émettre 2 photons ou plus (le facteur 1/2 correspond aux impulsions éliminées lorsque les bases d'Alice et Bob diffèrent). Le nombre total de photons reçus dépend quand à lui du gain η_L du canal de transmission et l'on a, en négligeant les coups d'obscurité des détecteurs de Bob:

$$n = \frac{1}{2} \eta_L \Pi_e N_{acq} \tag{1.54}$$

où Π_e est la probabilité pour la source d'émettre au moins un photon. Ainsi, en introduisant le taux de fuite d'information f_{il} (fractional information leakage), caractéristique de l'émission de la source:

$$f_{il} = \frac{\text{Proba. d'émettre 2 photons ou plus}}{\text{Proba. d'émettre au moins 1 photon}} = \frac{S_m}{\Pi_e} \tag{1.55}$$

on déduit de (1.51) le taux de bits sûrs par impulsion:

$$BS = \frac{k_{f,max}}{N_{acq}} = \frac{\eta_L \Pi_e}{2} [(\eta_L^{-1} f_{il} - 1) \log_2(\frac{1}{2} + 2D - 2D^2) - f(e)h(e)] \tag{1.56}$$

avec

$$D = \frac{e}{1 - \eta_L^{-1} f_{il}} \tag{1.57}$$

Ces deux dernières équations, où f_{il} n'intervient que sous la forme $(1 - \eta_L^{-1} f_{il})$, appellent quelques commentaires. Tout d'abord, comme on a généralement $f_{il} \ll 1$, l'influence des photons multiples n'est visible que pour les fortes pertes ($\eta_L^{-1} \gg 1$). De plus, si $\eta_{L,min}$ est la valeur minimale du gain de canal permise par cette méthode, obtenue en posant $BS = 0$, il apparaît directement sur ces équations que si f_{il} est atténué d'un certain facteur, $\eta_{L,min}$ sera atténué du même facteur. On a ainsi intérêt à travailler avec un petit f_{il} pour augmenter l'atténuation permise sur le canal de transmission, et donc la portée du dispositif de cryptographie. Nous utiliserons ce paramètre pour quantifier les performances de notre source de photons uniques au chapitre 2, même si les performances prévues par (1.56) ne sont plus forcément accessibles lorsque l'on prend en compte les coups d'obscurité, comme nous le verrons au chapitre 2.

1.3.4 De la sécurité inconditionnelle

Finissons ce rapide tour d'horizon en abordant succinctement les démarches visant à montrer la sécurité inconditionnelle du protocole $BB84$. L'objectif de la cryptographie quantique est en effet de pouvoir disposer au final d'un dispositif parfaitement sûr quelles que soient les capacités technologiques de l'espion, y compris contre les attaques collectives ou cohérentes. Les premières idées sur ce sujet datent de 1996 [120, 121, 31, 105]. Ces preuves sont aujourd'hui généralement acceptées, grâce notamment aux travaux de P.Shor et J.Preskill[152] qui ont exhibé une preuve remarquable par son élégance et sa simplicité, et dont voici les grandes lignes.

Le point de départ de cette démonstration reprend l'idée suivante: si Alice et Bob partagent k paires EPR, ils obtiendront une clé parfaitement sûre simplement en mesurant les différentes paires dans une base $\{|0\rangle, |1\rangle\}$ donnée[60]. Pour comprendre ce point, il suffit de remarquer que les paires partagées par Alice et Bob sont dans un état pur. La matrice densité ρ_{ABE} décrivant l'état partagé par Alice, Bob et Eve est donc nécessairement factorisable en $\rho_{ABE} = \rho_{AB} \otimes \rho_E$:

les mesures d'Eve sont rigoureusement indépendantes de celles d'Alice et Bob (on se reportera à [105] pour une formulation plus quantitative de ce fait). Le fait qu'Alice et Bob puissent s'échanger une information qui n'existe pas a priori, à partir d'une mesure commune sur un état pur, montre toute l'étrangeté de la mécanique quantique et forme le cœur du paradoxe EPR. Alice pourrait donc générer k paires EPR, et envoyer un membre de chaque paire à Bob: ce faisant, les erreurs liées à la transmission devront être corrigées pour avoir au final un partage de paires EPR. Un tel protocole est donc lié de très près à la correction d'erreurs quantiques.

Les erreurs quantiques différent profondément des erreurs classiques en ce qu'elle englobent toute transformation unitaire appliquée aux qubits. Elles se ramènent en fait à deux erreurs types: les erreurs de bit ($|0\rangle \rightarrow |1\rangle$ et $|1\rangle \rightarrow |0\rangle$) qui sont le pendant des erreurs classiques, et les erreurs de phase ($|0\rangle \rightarrow |0\rangle$ et $|1\rangle \rightarrow -|1\rangle$). Il est tentant de vouloir corriger ces erreurs indépendamment par des techniques de réconciliation mono-directionnelles, et c'est justement ce que permet de réaliser le codage CSS[42] (Calderbank-Shor-Steane).

Ce dispositif de correction d'erreurs peut être appliqué au protocole suivant: Alice génère n paires EPR, garde un membre de chaque paire et envoie les autres à Bob. Si les taux d'erreurs de bit et de phase ne sont pas trop importants, le codage CSS permettra de corriger les erreurs introduites par le canal. Une fois les erreurs corrigées, Alice et Bob partageront k paires parfaitement corrélées, et pourront obtenir une clé de taille k parfaitement sûre.

Shor et Preskill démontrent alors l'équivalence entre ce protocole inconditionnellement sûr et BB84. Cette démonstration s'appuie essentiellement sur le fait qu'Alice peut mesurer l'état de ses photons avant même d'avoir envoyé les photons de Bob: ce qui compte est alors l'état dans lequel sont les photons de Bob après les mesures d'Alice, et non le fait que cet état ait été généré à partir de paires EPR. L'utilisation d'une source EPR n'est donc pas essentielle à la sécurité du protocole: seule la capacité de la ligne à transmettre l'intrication est vraiment importante. Signalons que le protocole EPR ne nécessite pas a priori l'utilisation de 2 bases de codage. En fait, la base diagonale n'est utilisée dans ce protocole que pour estimer le taux d'erreurs de phase, ces erreurs de phase devenant des erreurs de bit dans la base diagonale. Dans la preuve d'équivalence, et du fait que Bob ne dispose pas de mémoire quantique, l'utilisation de 2 bases devient primordiale pour BB84.

Cette preuve de Shor et Preskill n'est pas complètement satisfaisante dans la mesure où elle ne prend pas en compte tous les défauts expérimentaux: elle suppose notamment une source parfaite capable d'envoyer des photons uniques, et l'on sait que c'est justement l'un des points qui posent problème avec l'attaque PNS. Cette démonstration utilise néanmoins des concepts intéressants, notamment le fait que l'on puisse utiliser les propriétés quantiques d'une source EPR sans disposer vraiment d'une telle source: nous avons été amenés à utiliser des concepts de ce type pour l'analyse de nos protocoles à variables continues que nous développerons au chapitre 3.

Signalons pour finir la publication récente de nouveaux critères de sécurité, plus robustes, qui reprennent les notions évoquées à la section 1.3 dans le cadre plus général de la théorie de l'information quantique: Igor Devetak et Andreas Winter[54] ont ainsi montré qu'un codage de canal avec une condition de sécurité appropriée permettait de se prémunir contre les attaques collectives; Renato Renner et ses collaborateurs[144, 145] ont quant à eux repris la notion d'amplification de confidentialité par fonctions de hachage et ont montré, avec une version quantique de l'entropie de Rényi, qu'elle permettait d'atteindre la sécurité inconditionnelle. Ces résultat suscitent de nombreux travaux théoriques, mais dépassent le cadre de ce manuscrit.

1.4 Dispositifs de cryptographie quantique: état de l'art et applications

La première expérience de cryptographie quantique[19] fut suivie d'un foisonnement d'idées et de prototypes[72], débouchant même sur la création de start-ups[116, 95].

L'un des objectifs poursuivis est d'adapter ces systèmes aux réseaux de communication par fibres optiques, ce qui ne va pas sans poser de nombreux défis expérimentaux pour compenser les fluctuations de polarisation dues à la biréfringence des fibres[65, 123, 23] ou, dans le cas du codage en phase, pour stabiliser le chemin optique[161, 73]. Par ailleurs, il n'est pas possible d'amplifier le signal dans la fibre sans briser la sécurité liée à l'unicité des photons transmis[180]. Ce dernier point va considérablement limiter la portée de ces protocoles, l'atténuation étant de l'ordre de $0,25$ dB/km dans les fibres des télécommunications optiques.

La source de photons généralement utilisée est une simple source cohérente fortement atténuée, pour laquelle le taux de fuite d'information vaut $f_{il} = \Pi_e/2$. En utilisant cette expression dans (1.56,1.57), et pour un QBER de 4%, il vient que le taux de bit sûr maximal est de 6% pour une ligne sans perte (obtenu avec $\Pi_e = 0,42$), 4.10^{-3} pour 6 dB de pertes (soit approximativement 25 km) et 7.10^{-7} pour 25 dB de pertes (100 km de fibres). Qu'en est-il du débit ? Il se trouve que le temps mort des détecteurs, ainsi que le temps de commutation des électro-optiques destinés à coder les bits d'information, vont limiter la fréquence d'émission à la dizaine de MHz, et l'estimation précédente conduit à un débit de 40 kbits/s pour une atténuation de 6 dB (600 kbits/s pour une ligne sans pertes).

En fait, les performances atteintes pour des atténuations de cet ordre (6 dB) sont plutôt[159] de l'ordre du kbit/s; l'évaluation (1.56,1.57) est en effet très optimiste, et ne prend notamment pas en compte les coups d'obscurités des détecteurs, sur lesquels nous reviendrons au chapitre 2. Il faut toutefois signaler la possibilité d'augmenter sensiblement le débit en utilisant de l'électronique rapide, mise en évidence récemment[30] par une expérience réalisée à l'air libre, de nuit, entre deux bâtiments du NIST à Gaithesburg distants de moins d'un kilomètre.

La cryptographie en transmission directe, à l'air libre et sans fibre optique, est un deuxième sujet d'étude, non dénué d'applications puisqu'il est susceptible de s'appliquer aux transmissions vers les satellites. Les records de distance de transmission se sont succédés[66, 41, 93], pour atteindre[100] une distance de 23 km entre deux sommets des alpes. On peut désormais envisager un échange de clé quantique entre un satellite et une station terrestre[140].

Une telle transmission avec un satellite pose bien sûr de nombreux problèmes, tels que le pointé d'un faisceau de très faible intensité sur plusieurs dizaines de kilomètres, à travers les turbulences atmosphériques. Mais l'on peut se montrer optimiste à ce sujet, avec notamment le développement des techniques d'optique adaptative, même si l'on doit s'attendre à travailler avec des pertes importantes. La communication par satellite ouvre d'interessantes perspectives, puisqu'une fois franchie la barrière atmosphérique, on pourra considérer des transmissions satellite-satellite sur des milliers de kilomètres.

Chapitre 2

Réalisation d'une source de photons uniques déclenchée

Sommaire

Comme nous l'avons vu au chapitre précédent, l'un des points faibles des protocoles à photons uniques de type $BB84$ réside dans la possibilité d'attaquer les impulsions contenant 2 photons ou plus. Dans l'hypothèse où l'espion (Eve) pourrait sélectionner ces impulsions et les transmettre au destinataire (Bob) par une ligne sans pertes, la portée de ce type de protocole s'en trouve fortement diminuée. L'intérêt d'une source capable d'émettre périodiquement un photon unique apparaît donc tout naturellement.

Le principe des premières sources de photons uniques[76] reposait sur l'émission de paires EPR, la détection de l'un des photons de la paire impliquant la présence de l'autre photon sur la voie de sortie. La source EPR doit cependant être faiblement excitée afin de limiter l'émission

simultanée de plusieurs paires: pour une application en cryptographie de telles sources sont en fait moins efficaces, en terme de débit, que les sources atténuées.

L'excitation d'un centre fluorescent individuel est une autre voie permettant d'obtenir une source de photons uniques: si un tel centre est excité par une impulsion suffisamment courte et suffisamment intense, il pourra être transféré vers l'état excité de façon presque certaine sans avoir le temps d'émettre de photon; le système reviendra ensuite dans son état fondamental en émettant un photon unique. Si les premières expériences consacrées à l'étude de la statistique d'émission d'émetteurs individuels ont été réalisées avec des atomes ou des ions[97, 55], elles nécessitaient une spectroscopie fine, à basse température, pour séparer l'émission de fluorescence de l'impulsion excitatrice. Il est donc préférable de travailler avec des systèmes plus complexes, pour avoir à température ambiante des spectres d'excitation et d'émission bien séparés. L'objet de ce chapitre est d'exposer nos travaux sur le système que nous avons choisi d'exploiter, à savoir les centres colorés du diamant. Mais avant d'exposer les raisons de ce choix, voyons de façon un peu plus quantitative ce que l'on peut attendre d'une source fonctionnant selon ce principe.

2.1 Une source de photons uniques déclenchée

Pour déterminer l'avantage quantitatif des sources déclenchées par rapport aux sources atténuées, on pourra comparer leur taux de fuite d'information f_{il} (fractional information leakage, voir chapitre 1) pour une même probabilité d'émission P_e. Nous avons effectué ce calcul, détaillé dans la référence [2.1], en considérant un système à deux niveaux régi par des équations de taux: les niveaux intermédiaires et les cohérences sont négligés de par leur très faible durée de vie. Ces niveaux sont représentés sur la figure 2.1 avec les taux de transfert ainsi qu'un éventuel état métastable. On notera donc r le taux de pompage, Γ^{-1} la durée de vie de l'état excité, et on supposera nul dans un premier temps le taux de branchement β vers l'état métastable.

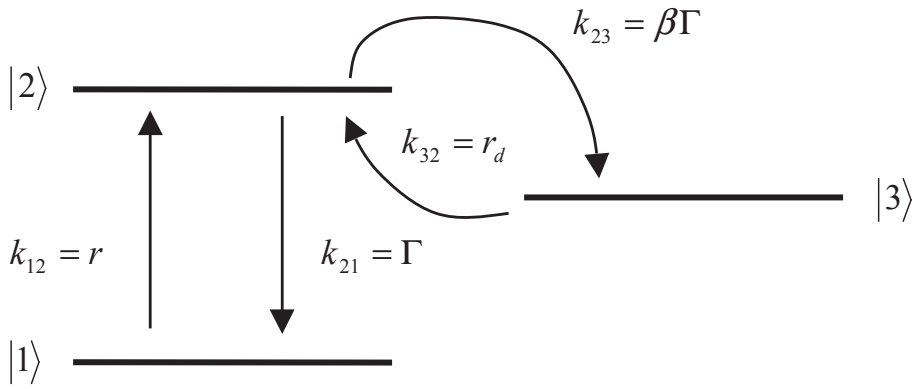

Figure 2.1: *Modélisation du centre fluorescent.*

Rappelons que f_{il} est défini comme étant le rapport S_m/Π_e, où Π_e est donc la probabilité pour la source d'émettre au moins 1 photon, tandis que S_m est la probabilité d'en émettre 2 ou plus. Pour estimer ces quantités il faut tout d'abord calculer les probabilités $P_n^{(g)}$ pour le centre fluorescent d'émettre n photons dans l'intervalle T séparant deux impulsions. L'indice (g) signifie que ces probabilités sont calculées en supposant que le système est initialement dans l'état fondamental, ce qui n'a de sens que si $T \gg \Gamma^{-1}$. Voici la valeur trouvée pour $P_1^{(g)}$ lorsque

cette condition est réalisée, δT étant la durée de l'impulsion lumineuse utilisée pour l'excitation:

$$P_1^{(g)} = (\frac{r}{r-\Gamma})^2[\exp(-\Gamma\delta T) - \exp(-r\delta T)] - \frac{r\Gamma\delta T}{r-\Gamma}\exp(-r\delta T) \tag{2.1}$$

L'expression de $P_e^{(g)}$, probabilité pour le centre d'émettre au moins un photon, est quand à elle beaucoup plus intuitive, et s'écrit (toujours avec $T \gg \Gamma^{-1}$) :

$$P_e^{(g)} = 1 - P_0^{(g)} = 1 - \exp(-r\delta T) \tag{2.2}$$

Il se trouve que si l'impulsion est suffisamment courte ($r\delta T < 10$) on pourra négliger la probabilité d'émettre plus de 2 photons et écrire simplement $P_2^{(g)} \approx P_e^{(g)} - P_1^{(g)}$.

Pour maintenant caractériser complètement la source et calculer f_{il} il est nécessaire d'introduire l'efficacité de collection η des photons émis par le centre fluorescent, ainsi que les probabilités $\Pi_n^{(g)}$ pour la source d'émettre n photons. On peut donc écrire, en limitant à 2 les photons pouvant simultanément être émis par le centre et en notant $\overline{\eta} = 1 - \eta$:

$$\Pi_0^{(g)} = P_0^g + \overline{\eta}P_1^g + \overline{\eta}^2 P_2^g \tag{2.3}$$

$$\Pi_1^{(g)} = \eta P_1^g + 2\eta\overline{\eta}P_2^g \tag{2.4}$$

On pourra alors calculer la probabilité $\Pi_e = 1 - \Pi_0^{(g)}$ d'émettre au moins un photon, ainsi que la probabilité $S_m = \Pi_e - \Pi_1^{(g)}$ d'émettre 2 photons ou plus, et l'on pourra enfin comparer $f_{il} = S_m/\Pi_e$ à sa valeur dans le cas d'une source atténuée: $f_{il} \approx \Pi_e/2$. Les sources atténuées (WCS) généralement utilisées dans les expériences de cryptographie[72] ont typiquement un Π_e de $0,1$. Pour obtenir une telle valeur avec une source à photons uniques (SPS), l'efficacité de collection doit atteindre 10%: les résultats présentés sur la figure 2.2, présentées en fonction[1] de Π_e, sont obtenus avec $\eta = 0.1$, pour différentes valeurs de la durée δT de l'impulsion d'excitation: on peut donc s'attendre à gagner plus d'un ordre de grandeur sur f_{il}, sachant que ce gain est d'autant plus important que l'impulsion est courte (les courbes calculées en utilisant la valeur de $\Gamma\delta T$ qui sera utilisée dans l'expérience sont indiquées en gras).

Pour une même valeur de Π_e, les performances d'une source de photons uniques sont donc supérieures à celles d'une source atténuée. Mais cette comparaison n'a plus de sens pour des valeurs de Π_e qui seraient inaccessibles aux sources de photons uniques; et comme notre rendement de collection sera plus proche de 2% que de 10%, ce point n'est pas sans importance (voir fig. 2.2). Alors comment comparer effectivement les performances de différentes sources pour la cryptographie? Cette question n'a en fait pas de réponse directe car elle dépend du cahier des charges. Nous avons vu au chapitre 1, équations (1.56,1.57), que les attaques PNS sur les impulsions à 2 photons posaient surtout problème pour les fortes atténuations η_L de la ligne de transmission. On peut donc s'attendre à ce que les sources à photons uniques soient surtout intéressantes pour les fortes atténuations avec, par rapport aux sources atténuées et pour Π_e fixé, un gain sur l'atténuation maximale autorisée équivalant au gain sur f_{il}. La figure 2.3 présente une estimation du taux de bits sûrs en fonction de l'atténuation du canal de transmission, pour un taux d'erreur de 4% ($f(e) \approx 1,16$) et sans prise en compte des coups d'obscurité. Les paramètres utilisés pour les sources à photons uniques sont $\Gamma\delta T = 0,032$ et $r\delta T = 8$, tandis que les sources atténuées équivalentes sont ajustées pour avoir la même valeur de Π_e que les sources à photons uniques.

[1] Fixer la valeur de Π_e revient en fait à fixer celle de $r\delta T$, à savoir l'énergie d'excitation.

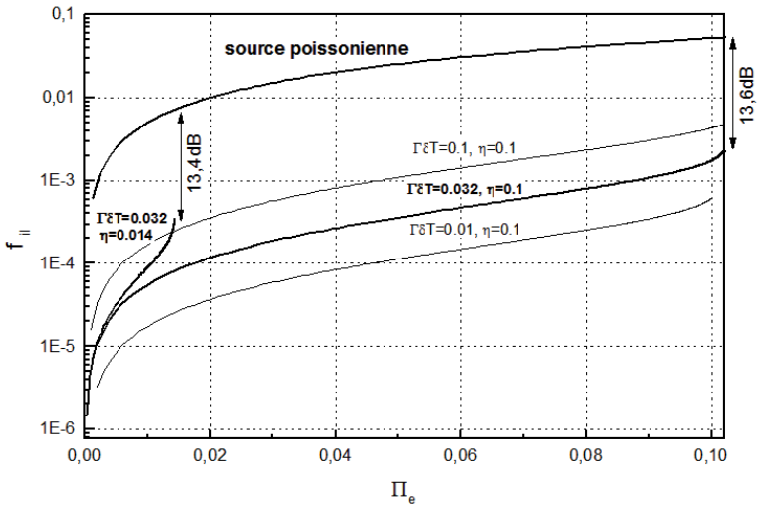

Figure 2.2: *Calcul de f_{il} en fonction de Π_e pour une source à photons uniques (avec $\eta = 0,1$ et $\eta = 0,014$) ainsi que pour une source atténuée.*

Les résultats présentés sur les figures 2.2 et 2.3 illustrent le fait que l'on peut attendre un gain sur l'atténuation maximale autorisée qui soit de l'ordre du gain sur f_{il} (de l'ordre de 13 dB sur ces exemples). L'emploi d'une source à photons uniques pourra donc être particulièrement intéressante pour les applications présentant une forte atténuation de la transmission (longues distances, transmission satellite). Certes, nous n'avons pas pris en compte ici l'influence des coups d'obscurités, qui comptent parmi les phénomènes qui vont dégrader ces performances et sur lesquels nous reviendrons. On peut néanmoins s'attendre à un gain tout-à-fait conséquent.

2.2 Etude des centres colorés N-V du diamant

2.2.1 Les centres colorés N-V du diamant

A l'époque où nous avions commencé à envisager cette thématique de recherche, des premiers travaux avaient déjà été réalisés sur des molécules[13, 40, 98]. Le principal problème de l'utilisation des molécules est le phénomène de photo-blanchiment, transformation chimique irréversible qui rend la molécule inutilisable. Il existe également une famille de semi-conducteurs que l'on peut utiliser à température ambiante: les nanocristaux de CdSe, qui présentent les caractéristiques d'émission d'un centre unique[122]. Cette émission présente cependant un clignotement de grande période qui est un obstacle pour l'utilisation de ces nanocristaux en tant que source de photons uniques. Par rapport à tous ces candidats, il nous est apparu que les centres N-V du diamant[86] présentaient de nombreux avantages.

Les centres N-V (Nitrogen-Vacancy) sont des défauts naturellement présents dans le cristal de diamant. Ils sont constitués d'un atome d'azote en substitution d'un atome de carbone à coté d'une lacune, la direction N-V étant parfaitement définie par rapport à la maille cristalline (figure 2.4). Leurs spectres d'absorption et d'émission s'étalent sur une centaine de nanomètres autour de la raie à zéro phonons (637 nm), et sont suffisamment séparés pour permettre un filtrage simple et efficace de la lumière d'excitation (figure 2.5). Leur structure électronique se ramène au schéma de la figure 2.1, avec notamment la présence d'un état métastable. La

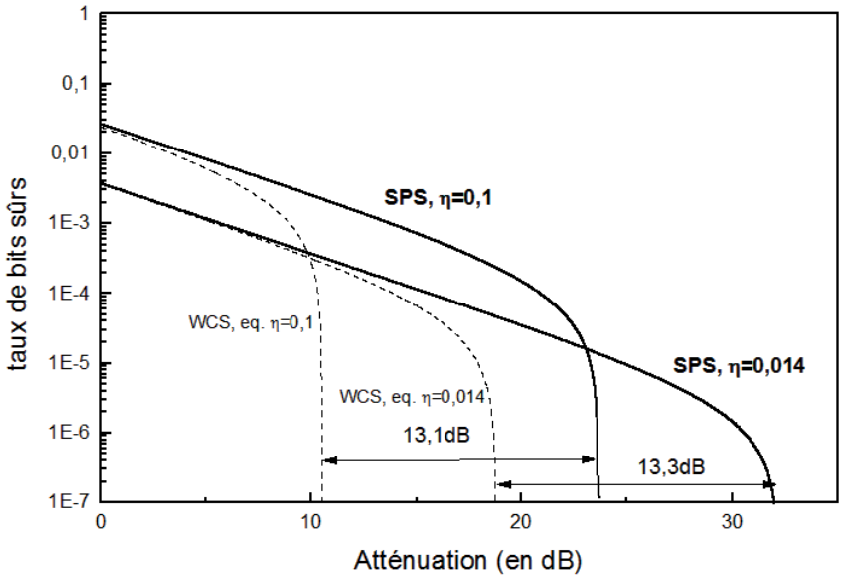

Figure 2.3: *Taux de bits sûrs en fonction de l'atténuation, pour* $\eta = 0,1$ *et* $\eta = 0,014$.

désexcitation est essentiellement radiative, ce qui garantira l'émission d'un photon pour chaque impulsion d'excitation.

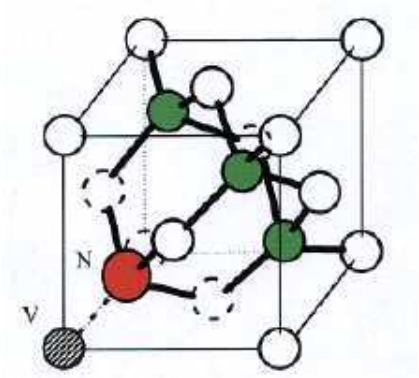

Figure 2.4: *Structure d'un centre NV à l'intérieur d'une maille de cristal de diamant.*

Le principal avantage de ces centres est leur photostabilité: nous n'avons observé aucune modification de la lumière de fluorescence, aussi bien sous excitation continue qu'impulsionnelle. De plus, outre le fait qu'ils sont naturellement fixés dans une matrice solide, ce qui facilite leur manipulation, la faible durée de vie du niveau excité ($\Gamma^{-1} = 11,6$ ns) permet d'envisager un taux de répétition relativement élevé (≈ 10 MHz), compatible avec ce qui est faisable en prenant en compte le temps mort des détecteurs.

2.2.2 Observation des centres colorés

Nous cherchons donc à exciter et collecter la fluorescence d'un centre N-V unique dans un cristal de diamant, et nous avons pour cela développé un système de microscopie confocale,

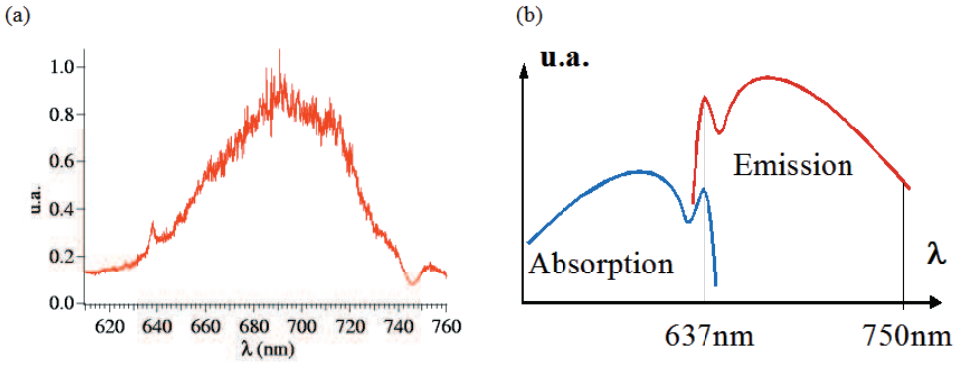

Figure 2.5: *(a) Spectre d'émission de centres NV excités à 532 nm dans le diamant massif. (b) Les spectres d'absorption et d'émission sont bien séparés.*

schématisé sur la figure 2.6. La particularité d'un microscope confocal réside dans la présence d'un trou de filtrage sur la voie de détection, placé de telle façon que son image sur l'échantillon coïncide avec le spot d'excitation. Il est ainsi possible de sélectionner la lumière en provenance des centres excités dans cette zone, et d'éliminer une grande partie de la lumière parasite. Le faisceau d'excitation proviendra soit d'un laser Argon (514 nm) ou d'un YAG doublé (532 nm), soit d'une source impulsionnelle qui sera décrite ultérieurement. Ce faisceau est amené sur le montage par une fibre optique, et une lame demi-onde associée à un cube polariseur permettent d'en ajuster la puissance. Un filtre passe bande interférentiel (centré sur 514 nm ou 532 nm) est utilisé pour éliminer toute lumière parasite pouvant être générée lors du passage dans la fibre, notamment par effet Raman.

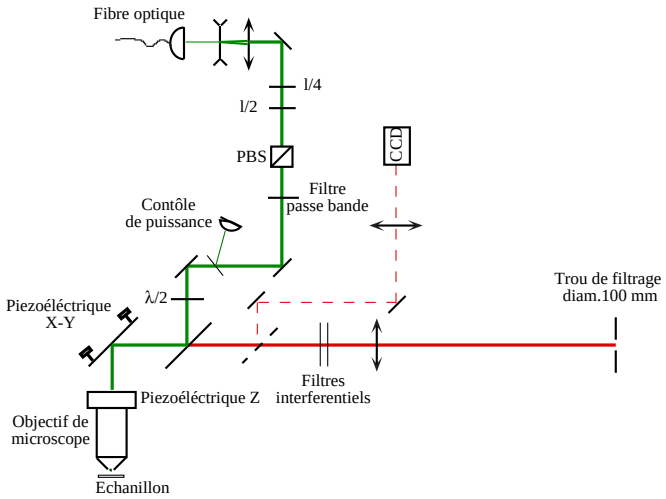

Figure 2.6: *Schéma expérimental du microscope confocal.*

Pour exciter un très faible volume tout en collectant le maximum de lumière, nous utilisons un objectif à immersion de très grande ouverture numérique (typiquement $ON = 1,3$). Par ailleurs, pour simplifier le montage, nous avons choisi un objectif corrigé d'aberrations à l'infini, avec un grossissement $G = 100$. Nous l'avons monté sur une bague piézo-électrique afin de pouvoir ajuster

sa distance à l'échantillon. Nous pouvons ainsi contrôler la position Z du spot d'excitation, sa position $X-Y$ étant quant à elle contrôlée par un miroir à 45° monté sur une cale piézo-électrique 2 axes. Enfin, une lame dichroïque ainsi qu'une série de filtres interférentiels placés sur la voie de détection éliminent la lumière d'excitation et filtrent la lumière de fluorescence.

Les premières expériences que nous avons effectuées ont été réalisées sur des échantillons de diamant massif de taille $1,5 \times 1,5 \times 0,1$ mm. Il est possible d'augmenter artificiellement le nombre de centres N-V en irradiant les échantillons, mais il s'est avéré que les échantillons non-irradiés présentaient des concentrations suffisamment importantes de ces centres. Ces échantillons sont placés entre une lame de verre et une lamelle de microscope, une goutte d'huile assurant le contact optique entre les différentes interfaces. La figure 2.7 présente un balayage en Z d'un échantillon: on distingue clairement les différentes interfaces, et l'on peut donc sans difficulté placer le spot d'excitation au milieu de l'échantillon.

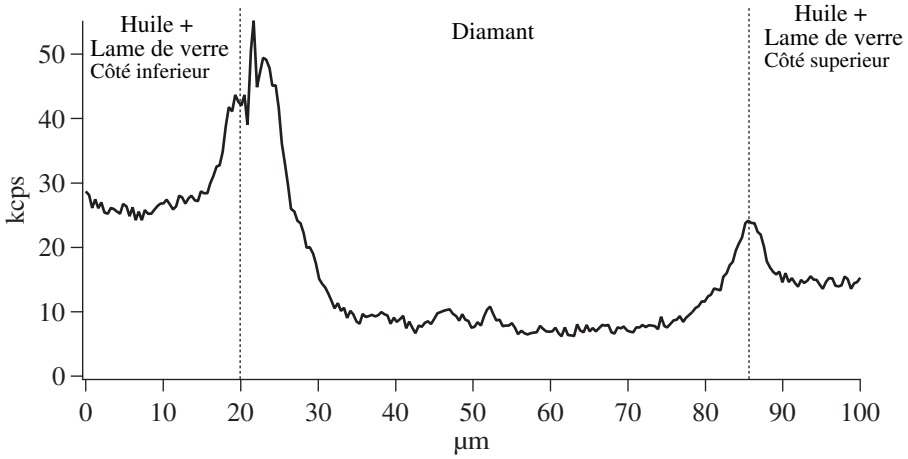

Figure 2.7: *Balayage en Z d'un échantillon de diamant massif.*

La figure 2.8 présente quant à elle un balayage en $X-Y$, ainsi qu'une coupe de ce balayage selon l'axe indiqué en pointillés. Nous pouvons clairement isoler différents centres, chaque centre correspondant à un grain dont la taille est en bon accord avec la valeur théorique de la taille du spot d'excitation (600 nm). Ce type d'enregistrement permet, en comparant la valeur au sommet à la ligne de base, de déterminer le contraste $\rho = S/(S+B)$, où S est le signal utile et B le bruit de fond lié à la lumière de fluorescence parasite, qui est de l'ordre de 85% dans nos expériences sur le diamant massif.

Ce système nous permet donc de repérer et de pointer un centre fluorescent. Nous avons ainsi pu asservir la position du spot d'excitation sur un centre et collecter une lumière de fluorescence très stable pendant plusieurs heures. Il s'agit ensuite d'analyser cette lumière pour caractériser le centre et, surtout, s'assurer qu'il est bien unique.

2.2.3 Caractérisation des centres dans le diamant massif

Pour conclure sur l'unicité du centre nous mesurons l'autocorrélation $g^{(2)}(\tau)$ de l'intensité de fluorescence. En régime de comptage de photons, cette fonction d'autocorrélation s'interprète simplement comme le rapport:

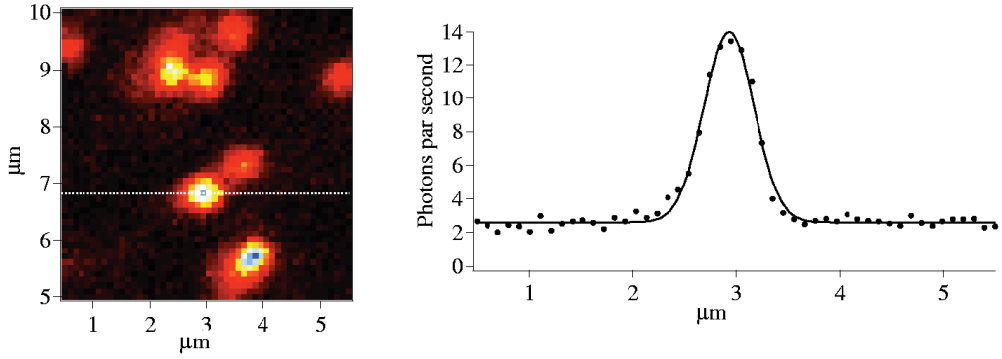

Figure 2.8: *Balayage en $X-Y$ d'un échantillon de diamant massif, et coupe selon l'axe en pointillés.*

$$g^2(\tau) = \frac{P(\tau)}{P(\infty)} = \frac{\sigma_2(\tau)}{\sigma_2(\infty)} \tag{2.5}$$

où $P(\tau) = \eta_d \Gamma \sigma_2(\tau)$ est la densité de probabilité de détecter un photon en $t = \tau$ sachant qu'un photon a été détecté en $t = 0$, η_d prenant en compte les efficacités de collection et de détection, et $\sigma_2(\tau)$ étant la population de l'état excité (voir figure 2.1). Dans le cas d'un système à 2 niveaux on montre simplement que l'on a[2.1]:

$$g^2(\tau) = 1 - \exp[(r + \Gamma)\tau] \tag{2.6}$$

où l'on rappelle que r est le taux de pompage (voir figure 2.1). La fonction d'autocorrélation est donc nulle en $t = 0$: la probabilité d'émettre 2 photons en même temps est nulle. C'est justement cette propriété de dégroupement de photons, signature de l'émission par un centre unique, que nous cherchons à exploiter pour réaliser une source de photons uniques. Si par contre plusieurs centres sont observés en même temps, on aura $g^{(2)}(0) = 1 - N^{-1}$, N étant le nombre de centres observés. On a donc $g^{(2)}(0) \geq 1/2$ si plus d'un centre est présent, ce qui laisse une confortable marge d'erreur pour vérifier l'unicité du centre.

Pour mesurer cette fonction d'autocorrélation nous avons utilisé le montage classique proposé par Hanbury-Brown et Twiss [89] et présenté sur la figure 2.9 (voir également la référence [2.2]): après le trou de filtrage du microscope confocal (voir figure 2.6), le faisceau est séparé en deux par une séparatrice 50/50, une photodiode à avalanche (PDA) en régime de comptage de photons étant placée sur chacune des deux voies. L'une des photodiodes est connectée à l'entrée 'start' d'un convertisseur temps-amplitude (CTA), qui contrôle le déclenchement d'une rampe de tension. L'autre photodiode est connectée à l'entrée 'stop' qui va bloquer cette rampe: la valeur finale de la tension du CTA, proportionnelle à l'intervalle de temps τ séparant les deux photons détectés, est ensuite numérisée et enregistrée dans un histogramme.

Des filtres ainsi que des trous de filtrage permettent de limiter les problèmes de diaphonie optique, liée à une émission infrarouge lors de l'avalanche dans la PDA. Pour symétriser le rôle des PDA 'start' et 'stop', une ligne à retard introduit un délai d'une vingtaine de nanosecondes sur la ligne 'stop'. Enfin, en retirant un miroir amovible, le montage permet d'effectuer un enregistrement du spectre de fluorescence (voir figure 2.9), qui permet de s'assurer que l'on observe bien un centre NV.

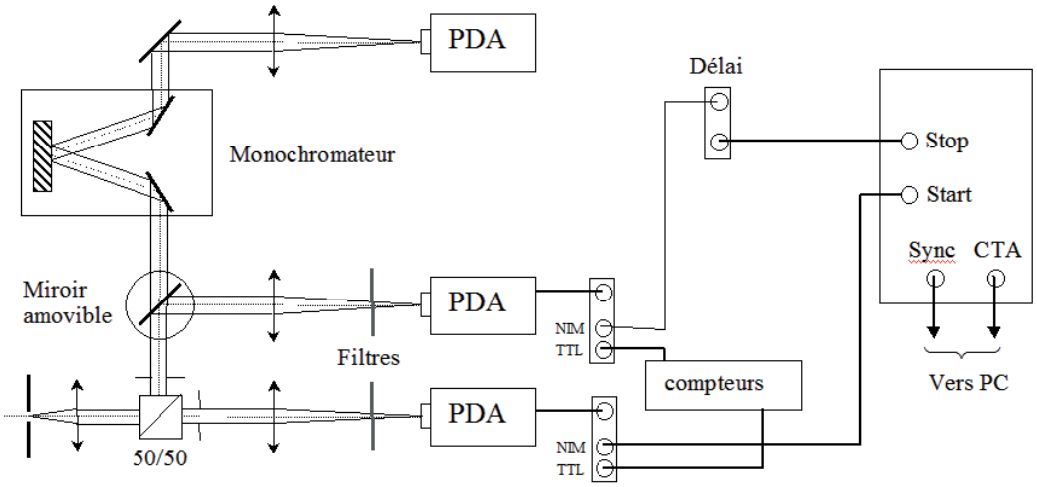

Figure 2.9: *Schéma expérimental du montage Hanbury-Brown et Twiss.*

La figure 2.10 présente un exemple de résultat obtenus avec le diamant massif en utilisant pour l'excitation un YAG doublé ($\lambda = 532$ nm) avec une puissance de $1,3$ mW. Les données brutes $C(\tau)$ correspondent à l'échelle de gauche: il s'agit du nombre de coups enregistrés dans les canaux de l'histogramme, chaque canal correspondant à $w = 1$ ns. Le temps d'acquisition est ici $T_{acq} = 667$ s, les nombres de photons enregistrés chaque seconde par les PDA étant $N_1 = 16620\ s^{-1}$ et $N_2 = 18440\ s^{-1}$. Dans le cas des faibles taux de comptage, l'histogramme $C(\tau)$ est proportionnel à la densité de probabilité $P(\tau)$, et il suffit donc a priori de le normaliser par[2] $C(\infty) = N_1 N_2 w T_{acq}$ pour obtenir $g^{(2)}(\tau)$.

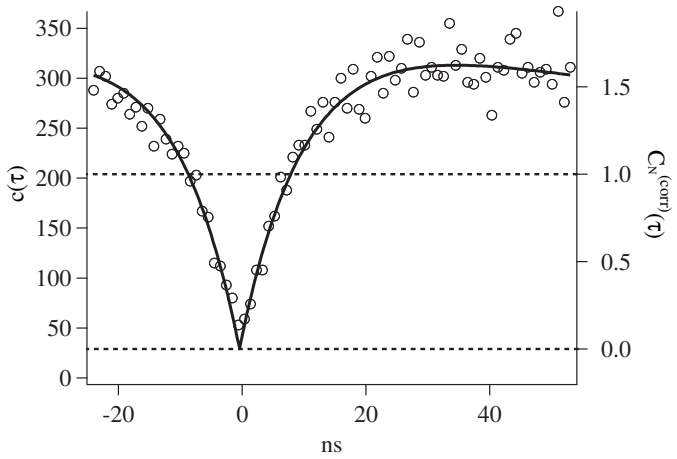

Figure 2.10: *Exemple d'histogramme enregistré, montrant le dégroupement de photons.*

[2] $C(\infty)$ doit être compris comme $C(\tau_\infty)$, avec τ_∞ suffisamment grand pour que $P(\tau_\infty) \approx P(\infty)$, c'est-à-dire pour que les évènements soient décorrélés, et suffisamment petit pour que $C(\tau) \propto P(\tau)$. En toute rigueur on a $C(\infty) = 0$ puisque la probabilité d'avoir 2 évènements de détection successifs séparés par un intervalle de temps arbitrairement grand est asymptotiquement nulle.

En fait, il apparaît sur la figure que le signal ne descend pas tout-à-fait à 0 en $\tau = 0$, tout en atteignant une valeur suffisamment faible pour exclure la présence de plusieurs centres. Ce fait peut être interprété très simplement par la présence du fond de lumière parasite, et il est possible de le corriger en utilisant le contraste ρ introduit précédemment (figure 2.8). On définit ainsi la quantité $C_N^{corr}(\tau)$, qui sera la quantité mesurée devant être comparée à $g^{(2)}(\tau)$:

$$C_N^{corr}(\tau) = \frac{C(\tau)/C(\infty) - (1-\rho^2)}{\rho^2} \tag{2.7}$$

Cette quantité peut être lue sur la figure 2.10 en utilisant l'échelle de droite. Le signal atteint maintenant la valeur 0 en $\tau = 0$, mais par contre il est supérieur à 1 aux temps plus longs ($\tau \approx 40$ ns), ce qui est en désaccord avec le modèle à deux niveaux (2.6). Nous avons ici la signature d'un phénomène de groupement de photons, lié à la présence de l'état métastable: les photons sont émis par bouffées, avec une interruption de l'émission lorsque le système est bloqué dans l'état métastable. Ce phénomène se produit sur une échelle de temps plus grande que le dégroupement de photons, et l'on aura bien sûr $g^{(2)}(\infty) = 1$, comme attendu de (2.5). L'étude systématique de ce type d'enregistrements que nous allons maintenant présenter nous a permis d'accéder à certains paramètres photophysiques d'un centre NV, et notamment de connaître un peu mieux les propriétés de l'état métastable.

2.2.4 Etude photophysique des centres NV dans le diamant massif

Nous avons effectué des enregistrements d'histogrammes ($C_N^{corr}(\tau)$) dans la configuration que nous venons de décrire (diamant massif, YAG doublé), pour différentes valeurs de la puissance d'excitation (voir la référence [2.3]). Nos résultats sont présentés sur la figure 2.11, où l'on retrouve l'histogramme de la figure 2.10 pour une puissance de 1,3 mW. La dynamique du groupement de photons est ici mieux visible, notamment pour les puissances d'excitation importantes.

En étudiant la dynamique de la population $\sigma_2(\tau)$ de l'état excité du système à 3 niveaux de la figure 2.1, et en utilisant l'expression (2.5) de la fonction d'autocorrélation, on montre que de façon générale cette dernière peut se mettre sous la forme[2.3]:

$$g^2(\tau) = 1 - \frac{1+g_e}{2}\exp[-\frac{k_{tm}+k_{1m}}{2}\tau] - \frac{1-g_e}{2}\exp[-\frac{k_{tm}-k_{1m}}{2}\tau] \tag{2.8}$$

les paramètres g_e, k_{tm} et k_{1m} étant fonction des paramètres physiques k_{12}, k_{21}, k_{23} et k_{32} du modèle utilisé. Les courbes en trait gras sur la figure 2.11 correspondent à des ajustements individuels de chaque courbe par cette expression (ainsi d'ailleurs que la courbe de la figure 2.10). Il n'est cependant pas possible de déduire les 4 paramètres du modèle à partir des 3 coefficients de l'ajustement. Pour effectuer cette inversion, on peut ajouter une donnée expérimentale supplémentaire qui est le taux de comptage N: ce taux est en effet directement lié à $\sigma_2(\infty)$ par:

$$N = \eta_d k_{21} \sigma_2(\infty) \tag{2.9}$$

σ_∞ pouvant lui-même être exprimé en fonction des paramètres recherchés. L'inversion peut ainsi être réalisée en utilisant une estimation de l'efficacité de détection, mais l'imprécision de cette estimation va introduire une erreur importante sur les résultats. Une telle démarche aboutit notamment à une dépendance linéaire de k_{21} en fonction de la puissance d'excitation qui n'est pas physiquement acceptable (l'excitation est à 100 nm de la longueur d'onde d'émission, ce qui exclut tout phénomène d'émission stimulée). Nous avons donc ajouté une condition supplémentaire en

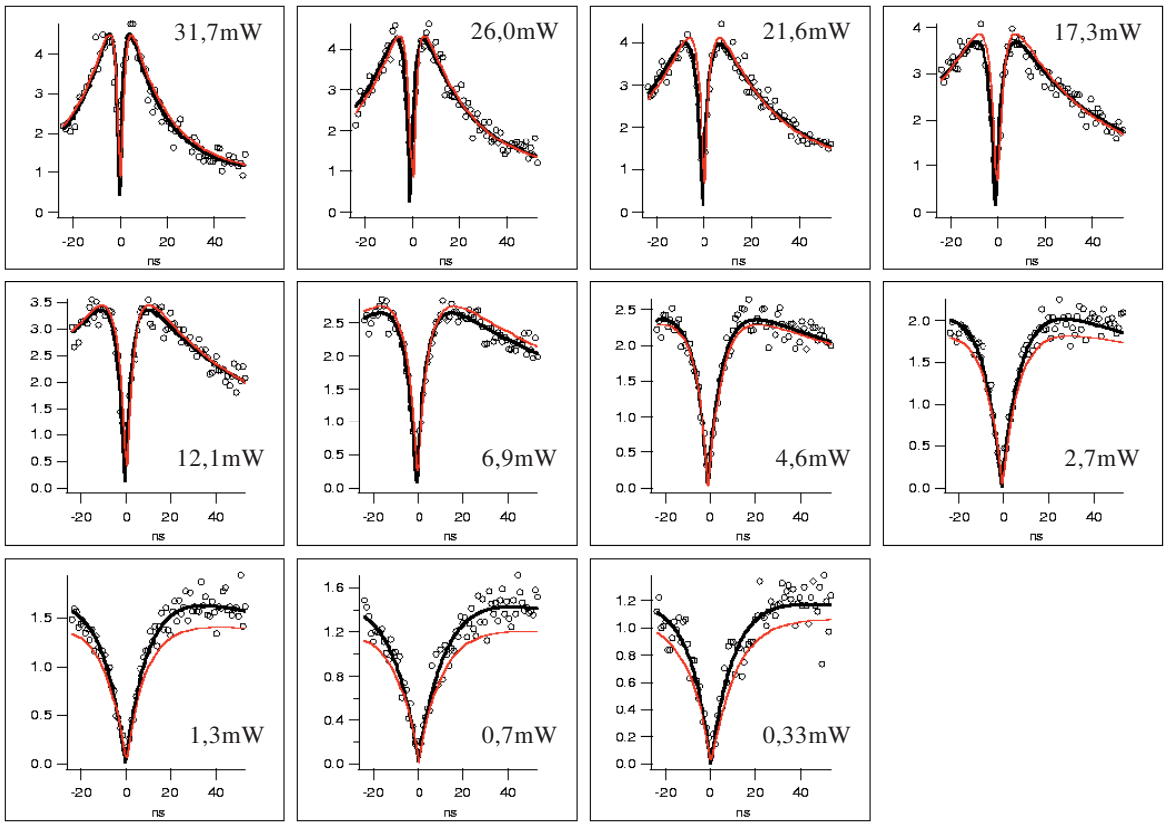

Figure 2.11: *Histogrammes ($C_N^{corr}(\tau)$) enregistrés pour différentes puissances d'excitation.*

imposant que le coefficient directeur de k_{21} soit nul, ce qui se produit pour $\eta_d = 1,27.10^{-3}$. On obtient ainsi les résultats de la figure 2.12:

Un ajustement linéaire peut être effectué pour toutes les quantités de la figure 2.12, et les courbes en trait fin sur la figure 2.11 ont été calculées en utilisant les valeurs obtenues à partir de ces ajustements linéaires. La valeur de $k_{21} = \Gamma$ est constante par hypothèse, et nous trouvons $\Gamma^{-1} \approx 12$ ns, en bon accord avec la durée de vie donnée dans la littérature[49] qui est de $11,6$ ns. Concernant le taux de pompage $k_{12} = r$, nous le trouvons proportionnel à la puissance d'excitation, avec $r\Gamma^{-1} \approx 5$ pour une puissance d'excitation de 30 mW. Nous avons vu à la section 2.1 que l'on cherche à avoir pour l'excitation impulsionnelle $r\delta T \approx 0,03 r\Gamma^{-1} \approx 10$, ce qui nécessite une puissance crête d'excitation 60 fois supérieure, de l'ordre du Watt.

Nous pouvons également estimer le taux de branchement vers l'état métastable $\beta = k_{23}/k_{21}$, qui dépend peu de la puissance d'excitation et qui vaut environ 1/15 à puissance nulle: le centre fluorescent a une chance sur 16 de passer de l'état excité vers l'état métastable. Nous trouvons pour ce dernier une durée de vie $k_{32}^{-1} \approx 430$ ns à puissance nulle, durée de vie qui se réduit avec la puissance d'excitation. Ces données ne sont toutefois plus forcément valables pour des valeurs plus importantes de la puissance d'excitation. De plus, comme nous allons maintenant le voir, il est en fait préférable de travailler avec des nanocristaux de diamants. Nous reprendrons donc ultérieurement l'étude de l'influence de l'état métastable.

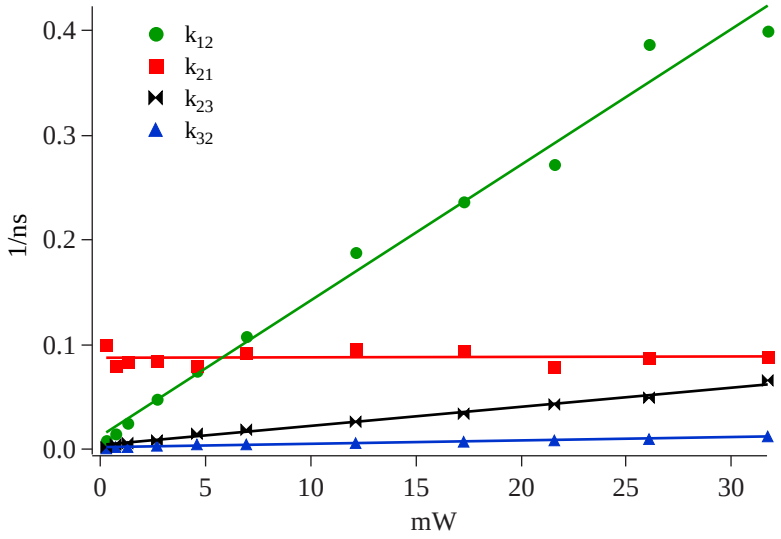

Figure 2.12: *Evolution des paramètres photophysiques en fonction de la puissance d'excitation.*

2.2.5 Des nanocristaux de diamant pour augmenter les performances de la source

Nous avons donc montré la possibilité de collecter la lumière de fluorescence d'un centre NV unique, avec toutefois une efficacité de collection assez faible. Nous venons d'estimer l'efficacité de détection $\eta_d = 1,27.10^{-3}$; en prenant en compte le rendement quantique des PDA qui est de 0.7, ainsi que la séparatrice 50/50 et les différents filtres du montage qui ont un coefficient de transmission global de 25%, on en déduit une efficacité de collection de l'objectif égale à $1,45\%$. Nous avions pourtant utilisé un objectif de grande ouverture numérique $ON = 1.3$ capable, avec un angle de collection maximal $\alpha_{max} = 61.5°$, de collecter 26% des photons émis par une source ponctuelle dans un milieu d'indice de réfraction constant. Le fait de travailler dans le diamant massif induit en fait deux difficultés:

- une diminution de l'angle de collection liée à la réfraction au passage de l'interface huile/diamant (figure 2.13a), ainsi que des pertes par réflexion, faisant passer l'efficacité de collection de 26% à 7%.
- des aberrations géométriques dues à la présence de cette interface (figure 2.13b), qui vont réduire l'intensité d'excitation au niveau du centre NV, mais qui vont également réduire l'efficacité de détection d'un facteur 5 (estimé par le logiciel code V).

Nous avions donc beaucoup à gagner à passer à des objets émetteurs ponctuels placés dans un milieu d'indice de réfraction $n = 1.5$, c'est-à-dire à utiliser des nanocristaux de diamant plutôt que du diamant massif. Les nanocristaux de diamant sont couramment utilisés dans l'industrie du verre pour le polissage des surface. Nous sommes donc partis d'une de ces poudres de diamant pour préparer nos échantillons, en collaboration avec Thierry Gacoin, du Laboratoire de Physique de la Matière Condensée de l'Ecole Polytechnique. Nous créons tout d'abord artificiellement des centres NV en procédant à une irradiation électronique suivie d'un recuit. Cette poudre est ensuite lavée dans un bain d'acide nitrique concentré, puis dispersée au moyen d'ultrasons dans une solution possédant de bonnes propriétés de mouillage (1% de Poly-Vinyl-Pyrrolidone dans

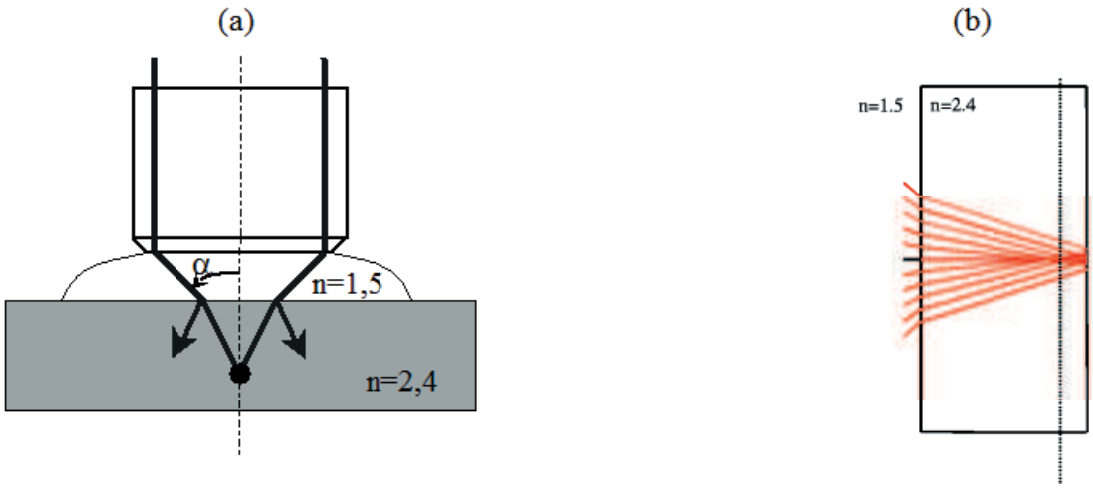

Figure 2.13: *Problèmes liés à l'interface huile/diamant : (a) diminution de l'angle de collection, pertes par réflexion. (b) aberrations géométriques, calculées ici pour le faisceau d'excitation.*

de l'isopropanol). La poudre est ensuite sélectionnée en taille par centrifugation, puis étalée sur un substrat, par centrifugation également. Nous obtenons ainsi, après évaporation de la solution de mouillage, des nanocristaux dont la taille est petite devant la longueur d'onde, déposés sur un substrat qui est en l'occurrence une lamelle de microscope en silice de 170 mm d'épaisseur. La disposition que nous avons utilisée pour l'observation des nanocristaux est présentée sur la figure 2.14, les nanocristaux adhérant simplement à la lamelle.

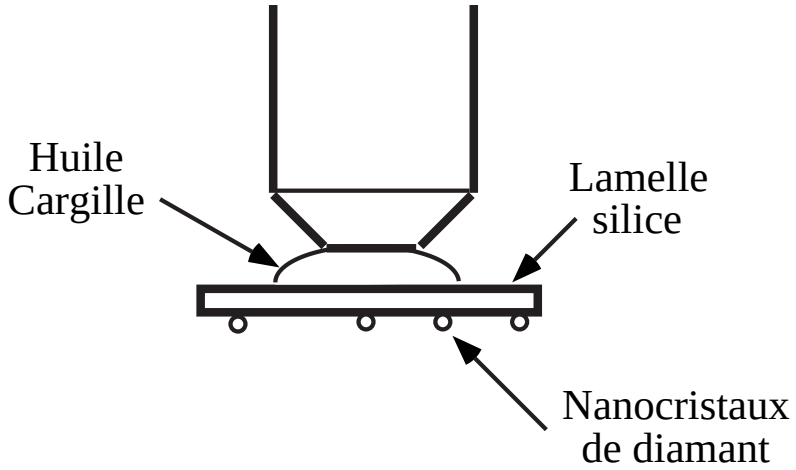

Figure 2.14: *Montage expérimental pour l'observation des nanocristaux de diamant.*

Nous avons pu ainsi observer à nouveau une émission de fluorescence en provenance d'un centre NV unique (voir également la référence [2.4]). Par contre, nous avons observé une diminution du taux de comptage à saturation par rapport au diamant massif, d'un facteur environ égal à 2/3. On ne peut cependant tirer de conclusion directe de ce constat quant à l'efficacité de collection: en effet, le nombre de photons détectés, donné par (2.9), dépend de l'environnement

au travers des paramètres photophysiques. Notamment, le taux d'émission spontanée $\Gamma = k_{21}$ dépend de la densité de modes électromagnétiques de l'environnement, et l'on peut montrer[2.4] qu'il est proportionnel à l'indice de réfraction du milieu, qui varie énormément lorsque l'on passe du diamant massif aux nanocristaux.

Nous n'avons pas repris avec les nanocristaux une étude photophysique complète analogue à celle du diamant massif (des mesures, effectuées avec une excitation impulsionnelle, seront cependant présentées au paragraphe suivant), mais nous avons mesuré la durée de vie en nous plaçant à faible puissance d'excitation pour trouver $\Gamma^{-1} = 25 \pm 4$ ns, soit un facteur $2,1$ par rapport au diamant massif. Le problème de l'évaluation théorique de la durée de vie est tout-à-fait non-trivial dans le cas des nanocristaux, car nous sommes en présence d'une géométrie complexe avec un nanocristal de diamant qui émet dans un demi-espace de silice et dans un demi-espace d'air. Un modèle naïf, consistant à introduire un indice effectif égal à la moyenne des indices de réfraction de la silice et de l'air, prévoit une durée de vie de 23 ns, en bon accord avec la valeur mesurée. Il faut cependant noter ici que des mesures récentes[5, 162] ont révélé une grande dispersion de ces durées de vie, montrant les limites de ce modèle.

Quoiqu'il en soit, les durées de vie avec lesquelles nous avons travaillé sont de cet ordre, et impliquent une diminution d'un facteur 2 du taux d'émission par rapport au cas du diamant massif. Dans ce cadre la diminution d'un facteur 2/3 du taux de comptage correspond à une augmentation d'un facteur $1,3$ de l'efficacité de collection, très petite devant le gain espéré. Nous attribuons ces mauvaises performances à une dégradation de l'objectif (qui faisait partie du "fond historique" de l'Institut d'Optique). En fait, dans la version finale de la source impulsionnelle que nous allons maintenant décrire, nous avons placé les nanocristaux sur un miroir diélectrique et utilisé un objectif métallographique neuf: nous avons alors observé une augmentation du nombre de photons collectés à saturation d'un facteur proche de 10. C'est cette possibilité, de part leur petite taille, de placer les microcristaux sur des miroirs ou dans des cavités, jointe à la potentialité d'augmenter fortement l'efficacité de collection, qui nous a conduit à persévérer dans le choix des nanocristaux pour le développement de notre sources de photons uniques.

2.3 Développement d'une source de photons uniques polarisés

2.3.1 Le laser impulsionnel d'excitation

Nous avons montré que l'on pouvait collecter et analyser la lumière de fluorescence d'un centre NV unique du diamant. Conformément à ce que nous avons vu au début de ce chapitre, il "suffit" maintenant d'utiliser une source impulsionnelle pour l'excitation du centre. Il n'existait cependant pas de sources commerciales possédant toutes les caractéristiques requises, ce qui nous a amené à développer notre propre source. Son principe est schématisé sur la figure 2.15.

Nous partons d'un laser Nd-YAG continu monomode, émettant 100 mW à $\lambda = 1064$ nm, dans lequel nous découpons des impulsions à l'aide d'un modulateur électro-optique fibré. Ce modulateur intégré est en fait un interféromètre de Mach-Zender dont la différence de marche est fonction de la tension de commande: il suffit d'une variation de tension très faible, de 4 V environ, pour basculer de l'extinction à la transmission totale. Pour garantir un haut niveau d'extinction, nous lui appliquons une tension continue asservie sur une frange sombre, à laquelle il suffit de superposer une tension de modulation pour le découpage des impulsions. Nous arrivons ainsi à émettre un train d'impulsions dont la taille peut varier de $\delta T = 0,8$ ns à $\delta T = 4$ ns pour une fréquence de 10 MHz ou plus.

Les impulsions sont ensuite amplifiées dans un amplificateur à fibre dopée Ytterbium pour pouvoir être doublées efficacement par simple passage dans un cristal de PPKTP (Periodically

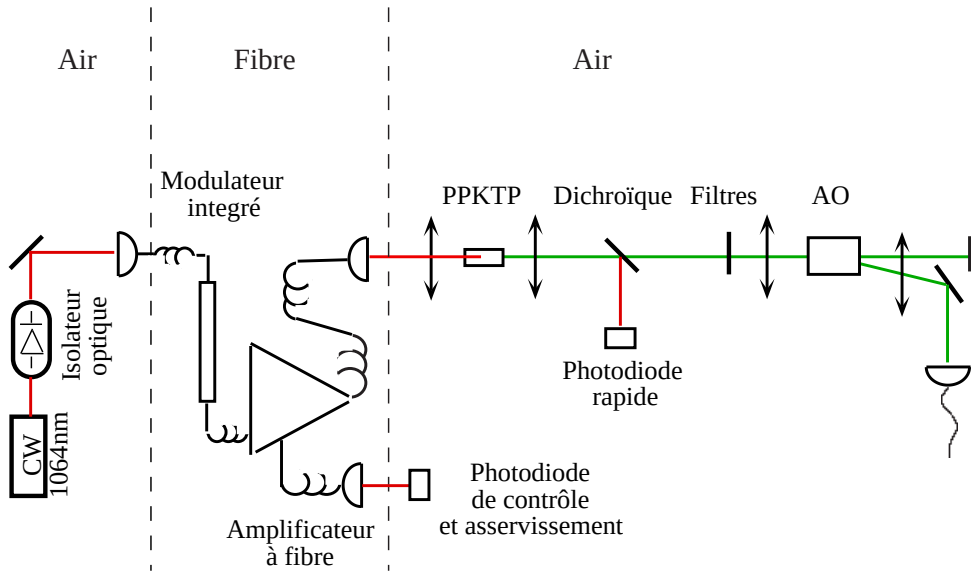

Figure 2.15: *Principe de la source laser impulsionnelle pour l'excitation des centres NV.*

Poled KTP). Il a ainsi été possible, avec une efficacité de doublage de 15%, de générer des impulsions à 532 nm, polarisées linéairement, avec une puissance crête pouvant atteindre plusieurs centaines de milliwatts. Ce faisceau est ensuite séparé de la pompe à 1064 nm par une lame dichroïque et une série de filtres. Enfin, lorsqu'une fréquence de répétition inférieure à 10 MHz est nécessaire, un modulateur acousto-optique est utilisé en bout de chaîne comme diviseur de fréquence, en ne sélectionnant qu'une impulsion sur 2 ou une impulsion sur 3. Le faisceau est ensuite couplé à la fibre optique destinée à l'amener sur le dispositif de microscopie confocale (figure 2.6). La figure **??** montre la fonction d'autocorrélation mesurée, après atténuation, par notre dispositif Hanbury-Brown et Twiss.

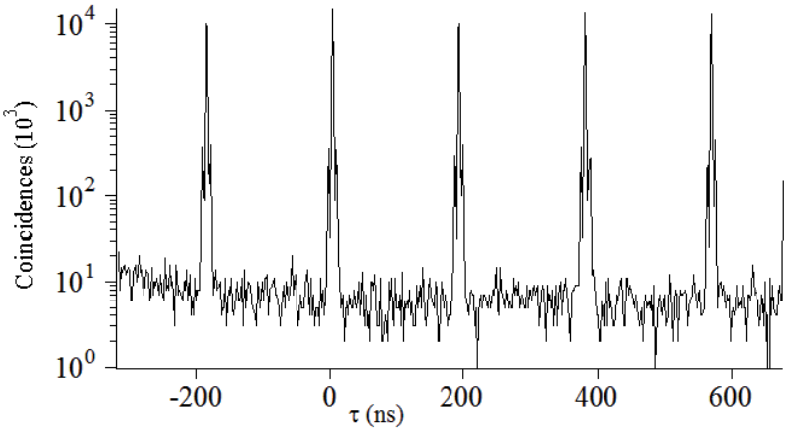

Figure 2.16: *Fonction d'autocorrélation de la source impulsionnelle sur une échelle logarithmique, la période du train d'impulsions étant de* 200 *ns, la taille des impulsions étant de* $1,2$ *ns et le temps d'intégration de* 595 *s.*

Les impulsions émises ont donc un faible piédestal, avec un rapport en amplitude de 10^4, le rapport entre l'aire d'un pic et l'aire entre 2 pics successifs étant de 37. Nous pouvons donc légitimement négliger la probabilité d'excitation du centre entre 2 impulsions. Par ailleurs, cette trace d'autocorrélation est caractéristique d'une source impulsionnelle atténuée, et appelle à ce titre quelques commentaires :

Tout d'abord, plutôt que de s'intéresser au nombre de coïncidences $C(\tau)$, enregistrées dans un canal de largeur w centré sur τ, la nature impulsionnelle du problème invite à considérer le nombre de coïncidences $C(m)$ associé à la m^{ieme} impulsion suivant le premier événement de détection. Le coefficient $C(m)$ ainsi défini correspond à l'aire du m^{ieme} pic d'autocorrélation, et on peut le normaliser de manière analogue à ce qui a été fait au 2.2.3, en le divisant par la valeur C_∞ obtenue[3] en considérant des évènements décorrélés, soit dans le cas des faibles taux de comptage:

$$\begin{aligned} C_N(m) &= C(m)/C_\infty \\ C_\infty &= P^2 N_{acq} \\ P &= \frac{a}{2}\Pi_1 \end{aligned} \tag{2.10}$$

où N_{acq} est le nombre d'impulsions laser émises durant l'acquisition, où P est la probabilité de détecter un événement, Π_1 est la probabilité pour la source d'émettre un photon, et où a est le rendement quantique des PDA (le facteur 1/2 rend compte de la séparatrice du dispositif Hanbury-Brown et Twiss). Nous n'effectuons plus ici de correction liée au fond de fluorescence (equ. 2.7), car il s'agit maintenant de caractériser non pas l'émission d'un centre unique, mais une source pour la cryptographie, où l'on ne pourra plus différencier un photon provenant du centre d'un photon provenant du bruit de fond.

Si maintenant on reprend la trace d'autocorrélation de la figure 2.16, qui correspond donc au cas d'une source cohérente atténuée, les pics ont tous la même amplitude et la même surface: $C_N(m) = 1$ y compris en $m = 0$. Pour bien comprendre ce point, rappelons que le cas $m = 0$ est lié à l'émission d'au moins 2 photons pour une même impulsion: $C(0) = a^2 N_{acq}\Pi_2/2$ (dans le cas des faibles taux de comptage), Π_2 étant la probabilité pour la source d'émettre deux photons. Le facteur 1/2 correspond toujours à la présence de la séparatrice, et représente la probabilité pour que les deux photons incidents soient équitablement distribuées sur les deux PDA *start* et *stop*. Dans le cas d'une source atténuée, on a $\Pi_2^{att} = \Pi_1^2/2$, ce qui donne effectivement $C_N(0) = 1$. Pour une source quelconque, la valeur de $C_N(0)$ est directement reliée au Π_2 de la source avec $\Pi_2 = C_N(0)\Pi_1^2/2$, soit pour le taux de fuite d'information:

$$f_{il} \approx C_N(0) f_{il}^{att} \approx C_N(0)\Pi_1/2 \tag{2.11}$$

Tous ces points étant posés, nous pouvons maintenant passer à l'analyse de la lumière émise par un centre NV sous excitation impulsionnelle.

2.3.2 Analyse de l'émission d'un centre NV sous excitation impulsionnelle

La figure 2.17 présente une trace d'autocorrélation réalisée avec la lumière émise par un centre NV dans un nanocristal de diamant, sous excitation impulsionnelle. Le laser d'excitation a ici une puissance moyenne de $0,94$ mW, avec un taux de répétition de 10 MHz et une durée d'impulsions de $1,2$ ns (soit une puissance crête de 80 mW, conditions proches de la saturation du centre).

[3] Même remarque que la note 2 de la page 37

La première remarque concernera la faible valeur du pic en $\tau = 0$, ce qui est comme nous venons de le voir la signature d'une source de photons uniques.

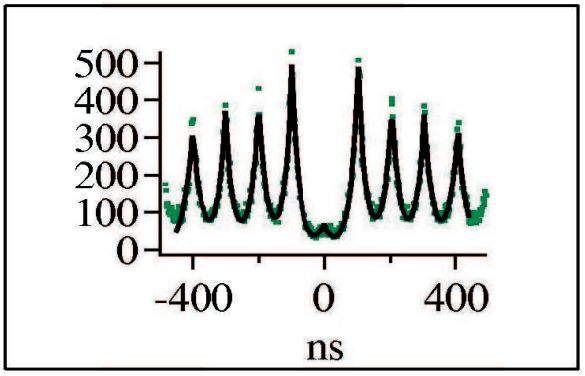

Figure 2.17: *Fonction d'autocorrélation d'un centre NV unique.*

Contrairement au cas de la source atténuée, le taux de recouvrement entre pics adjacents est ici important, et l'aire $C(m)$ de chaque pic ne peut être évaluée directement. Plutôt que cette évaluation directe nous avons réalisé un ajustement prenant en compte la forme théorique de ces pics:

$$C(\tau) = w\frac{\Gamma}{2}\sum_m C(m)exp(-\Gamma|\tau - mT|) \tag{2.12}$$

Le premier coefficient issu de cet ajustement est la durée de vie du niveau excité. En moyenne sur 5 centres nous trouvons ainsi $\Gamma^{-1} = 23,4 \pm 0,5$ ns pour les nanocristaux, en bon accord avec les résultats exposés au 2.2.5. Les valeurs obtenues pour $C_N(m)$ sont présentées sur la figure 2.18:

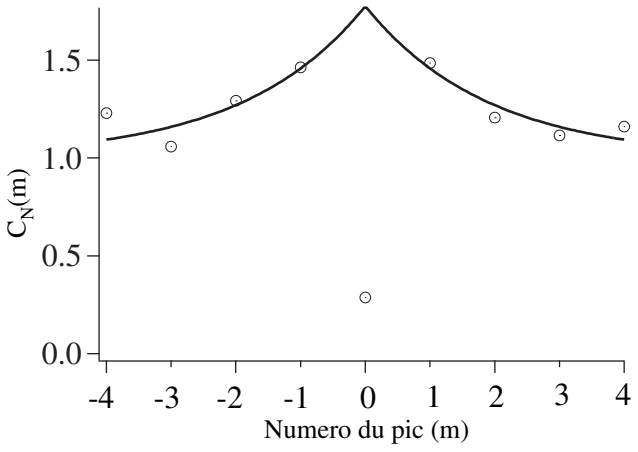

Figure 2.18: *Valeurs de $C_N(m)$ pour chacun des pics.*

Nous avons ici des valeurs de $C_N(m)$ supérieures à 1, ce qui est comme nous l'avons déjà vu la signature du groupement de photons liés à la présence de l'état métastable. On se reportera

à la référence [2.5] pour plus de détails sur cette expérience et les analyses associées. Le point essentiel est de bien comprendre l'impact de ce niveau métastable sur le fonctionnement de la source: cette dernière va émettre un train d'impulsion tant que le système n'est pas piégé dans l'état métastable, pendant une durée moyenne T_{on}. Le système est ensuite piégé dans cet état pendant une durée moyenne T_{off} au cours de laquelle il n'émet plus. La source émet donc des trains d'impulsions, à l'origine du groupement de photons observé, et le flux émis est réduit d'un facteur égal au rapport cyclique $\eta_{cycl} = T_{on}/(T_{on} + T_{off})$, qui vaut ici $0,54$. Ce facteur sera par la suite incorporé dans l'efficacité de collection ($\eta \rightarrow \eta_{cycl}\eta$).

Concernant maintenant le cas $m = 0$, nous obtenons $C_N(0) = 0,21$, soit pour f_{il} un gain d'un facteur 5 environ par rapport à la source atténuée équivalente, ce qui n'est pas aussi bon que les performances attendues: le diagramme de la figure 2.2 laisse entrevoir un facteur 10 minimum. Le fond de fluorescence collecté est donc encore trop important. Le nombre d'évènements de détection à saturation permet quant à lui d'évaluer l'efficacité de détection $\eta_d = 1,85.10^{-3}$, valeur qui, comme nous l'avons vu au paragraphe 2.2.5, est légèrement supérieure à celle obtenue dans le cas du diamant massif, mais en restant loin de la valeur 10 fois plus grande qui était attendue.

2.3.3 Source de photons uniques polarisés pour la cryptographie

Nous avons donc cherché à améliorer les performances qui viennent d'être décrites afin d'avoir une source qui puisse légitimement être utilisée en cryptographie. Nous avons ainsi remplacé notre objectif à immersion d'ouverture numérique $1,3$ par un objectif métallographique d'ouverture numérique $0,95$ (optimisé pour fonctionner à l'air libre). Par ailleurs, nous avons placé les nanocristaux sur un miroir diélectrique de façon à potentiellement doubler l'efficacité de collection. Nous obtenons ainsi une efficacité de détection $\eta_d = 1,1\%$, soit une amélioration par un facteur 6 du résultat précédent. Cette valeur n'atteint pas encore la limite théorique du système, mais elle est suffisante pour proposer raisonnablement une expérience de cryptographie: elle correspond en effet, avec un rapport cyclique $\eta_{cycl} = 0,71$, à une efficacité de collection $\eta = 2,6\%$, qui sera ramenée à $1,4\%$ après polarisation.

Pour s'assurer que l'intervalle de temps entre deux impulsions est suffisamment grand par rapport à la durée de vie du niveau excité (typiquement $T > 6\Gamma^{-1}$, avec $\Gamma^{-1} = 23$ ns), nous avons utilisé une fréquence de répétition de $5,3$ MHz. La durée d'impulsion sera désormais fixée à $0,8$ ns. L'analyse par autocorrélation de cette source nous permet d'obtenir $C_N(0) = 0,07$, qui correspond à un taux de fuite d'informations $f_{il} = 5.10^{-4}$, beaucoup plus proche des performances attendues (voir figure 2.2). La probabilité d'émettre plus d'un photon se limite ainsi à $S_m = 7.10^{-6}$, soit moins de 40 paires par seconde. Pour obtenir ce résultat nous avons accordé un soin particulier au choix du miroir diélectrique afin de minimiser sa fluorescence. Un balayage préalable du voisinage du centre étudié peut notamment permettre de diminuer encore, par photoblanchiment, cette fluorescence.

Enfin, cette source est polarisée par l'adjonction d'une lame demi-onde et d'un cube séparateur de polarisation. Il se trouve que la lumière émise par le centre est déjà fortement polarisée, avec un taux de polarisation de typiquement 70%. Le polariseur introduit donc peu de pertes nouvelles (moins de 20%). Par contre, pour pouvoir être utilisée en cryptographie, cette source doit permettre le codage en polarisation des photons émis. Ceci est obtenu par un modulateur électro-optique, utilisant la biréfringence générée par effet Kerr dans un cristal d'ADP. Ce modulateur est compensé de façon à présenter, sur une plage spectrale de plus de 200 nm, un déphasage nul pour une tension de commande nulle. Je passerai tous les aspects techniques concernant la synchronisation, ainsi que la réalisation d'un commutateur Haute Tension Haute Fréquence[29].

Au final, nous pouvons choisir aléatoirement la polarisation du photon émis (dans $\{H, V, G, D\}$), avec une erreur maximale de 1% sur la polarisation produite, et en introduisant 35% de pertes supplémentaires. L'efficacité de collection du système complet est donc de $1,4\%$. Cette source peut maintenant, avec ces performances, être utilisées pour une expérience de cryptographie (voir également la référence [2.6]).

2.4 Application à la cryptographie quantique

2.4.1 Le dispositif expérimental

Nous venons de décrire le dispositif d'Alice, qui est donc une source impulsionnelle de photons polarisés aléatoirement dans $\{H, V, G, D\}$. Bob doit donc effectuer une mesure de la polarisation dans la base $\{H, V\}$ ou dans la base $\{G, D\}$. Pour effectuer le choix aléatoire de cette base, il suffit d'utiliser une simple séparatrice 50/50, envoyant avec une probabilité 1/2 le photon dans un dispositif de mesure $\{H, V\}$ ou $\{G, D\}$. Ce dispositif de mesure, présenté sur la figure 2.19, nécessite l'utilisation de 4 PDA, mais présente l'avantage de ne pas utiliser de dispositif actif nécessitant une procédure complexe de synchronisation.

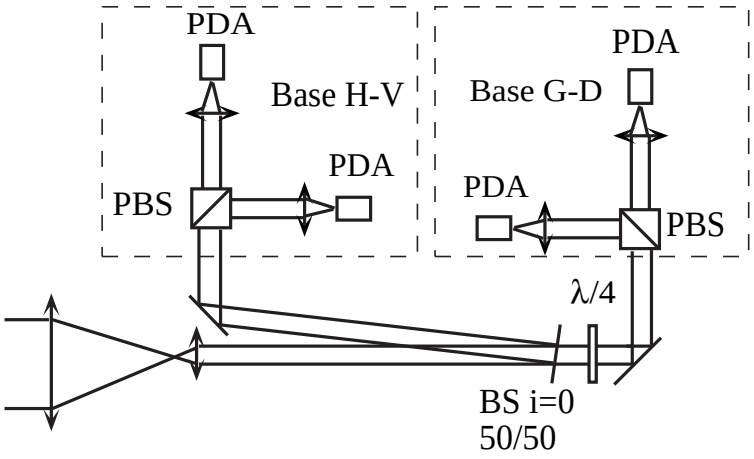

Figure 2.19: *Montage expérimental de Bob.*

Nous avons essayé notre système dans un couloir de l'Institut d'Optique, avec une distance de 50 m entre Alice et Bob (figure 2.20). La transmission des systèmes optiques, de la sortie de la source jusqu'aux PDA, est d'environ 90%, le rendement quantique des PDA étant de $0,6$. En rappelant que la source utilisée par Alice émet 75000 photons polarisés chaque seconde, Bob peut donc potentiellement détecter 40000 photons par seconde.

Nous avons pris soin d'éliminer toute lumière parasite, mais les coups d'obscurité constituent une source d'erreur incontournable. Sur l'ensemble des 4 photodiodes, 870 coups d'obscurités sont émis chaque seconde, ce qui n'est pas négligeable devant le nombre de photons détectés. Pour réduire les erreurs potentielles liées à ce phénomène, nous post-sélectionnons les photons détectés dans une fenêtre de 50 ns synchronisée sur l'émission d'Alice: de par la durée de vie du niveau excité, à savoir 23 ns, cela implique une probabilité de détection d'un photon émis par Alice proche de 90%, tandis que la probabilité de déclenchement sur un coup d'obscurité est divisée par 4.

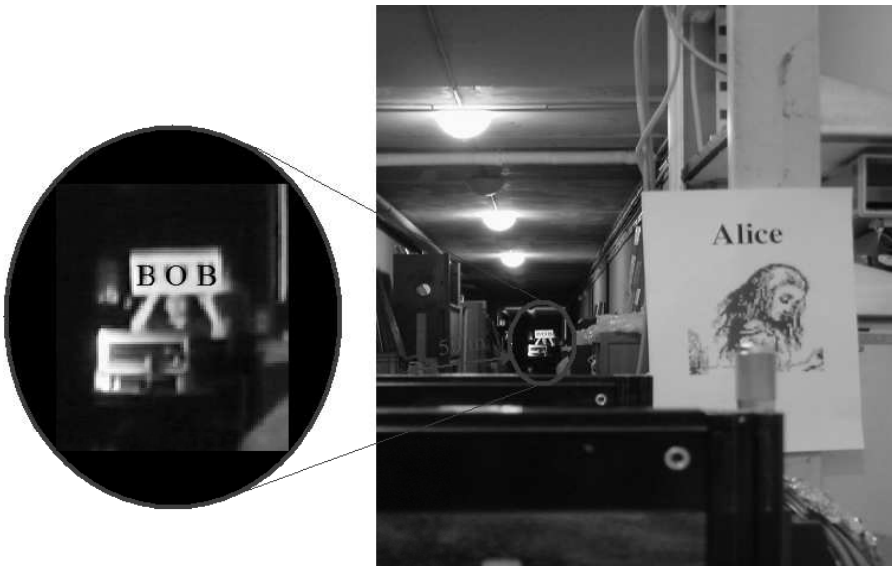

Figure 2.20: *Une distance de* 50 *m sépare Alice et Bob.*

L'expérience a consisté en trois acquisitions de 10 ms, qui ont permis de détecter 1180 évènements, en bon accord avec les performances attendues. Après post-sélection par la fenêtre temporelle et comparaison des bases utilisées par Alice et Bob, il reste 473 bits utilisables pour la génération de la clé. Sur ces bits, le taux d'erreurs est de $4,6\%$. Nous avons attribué ce taux relativement élevé à des imperfections dans le signal de commande du modulateur électro-optique.

Enfin, l'utilisation des formules (1.49-1.53) permet de prévoir un débit de distribution de 8000 bits sûrs par seconde. Les coups d'obscurités ne sont ici pris en compte que dans l'évaluation du nombre n d'évènements de détection enregistrés par Bob ainsi que dans celle du QBER e. L'application concrète des algorithmes de réconciliation (Cascade) et d'amplification de confidentialité, réunis au sein du logiciel QuCrypt développé par Louis Savail et ses collaborateurs[130], sur les 473 bits utilisables ne nous a en fait permis d'extraire qu'une clé secrète de 158 bits, soit 5300 bits sûrs par seconde. Il se trouve que l'échantillon traité est ici trop petit pour profiter de toute la potentialité de notre système, avec notamment une difficulté pour évaluer de façon fiable le QBER. Cette première démonstration n'avait d'autre objectif que de mettre en œuvre un système complet de cryptographie utilisant notre source de photons uniques, et a permis de clore avec succès la thèse d'Alexios Beveratos (voir également la référence [2.6]). Nous avons ensuite repris ce système pour une deuxième série d'expériences, réalisées en collaboration avec le Laboratoire de Photonique Quantique et Moléculaire de l'ENS de Cachan et dans le cadre de la thèse de Romain Alléaume, en faisant cette fois-ci varier le gain du canal de transmission (référence [2.7]).

2.4.2 Performances du dispositif avec un canal présentant des pertes

Les performances du dispositif ont tout d'abord été améliorées par rapport à sa première version, notamment celles du modulateur électro-optique dont la transmission est passée de 65% à 90%. Le rendement de collection de la source est ainsi passé, toujours avec une fréquence de répétition de $5,3$ MHz, de $1,4\%$ à $2,35\%$, tandis que le QBER a été ramené à $1,65\%$ pour une ligne sans perte. Les coups d'obscurité ont été réduits à 620 coups par seconde pour les 4

photodiodes. Seule la valeur de $C_N(0)$ a légèrement augmenté: nous avons désormais $C_N(0) = 0,13$.

Ce système a été utilisé pour une expérience de transmission réalisée de nuit, dans l'espace libre, entre deux ailes en regard de l'Institut d'optique. La distance séparant Alice et Bob est ici de 30 m. En prenant en compte les pertes dans les télescopes de transmission et dans le système de réception, le rendement de collection de Bob est d'approximativement $\eta_B = 30\%$. La durée de la fenêtre utilisée pour la post-sélection est de 60 ns.

Des essais de transmission ont donc été réalisés pour différentes valeur du gain η_T du canal de transmission (le rendement de détection global est $\eta_B\eta_T$). Les débits obtenus sont présentés sur la figure 2.21: les ronds sont les débits réellement obtenus, comparés au résultat théorique (trait gras) issu de (1.49-1.53). Les croix correspondent aux débits qui auraient été obtenus, dans les mêmes conditions, par une source atténuée (avec la courbe théorique correspondante).

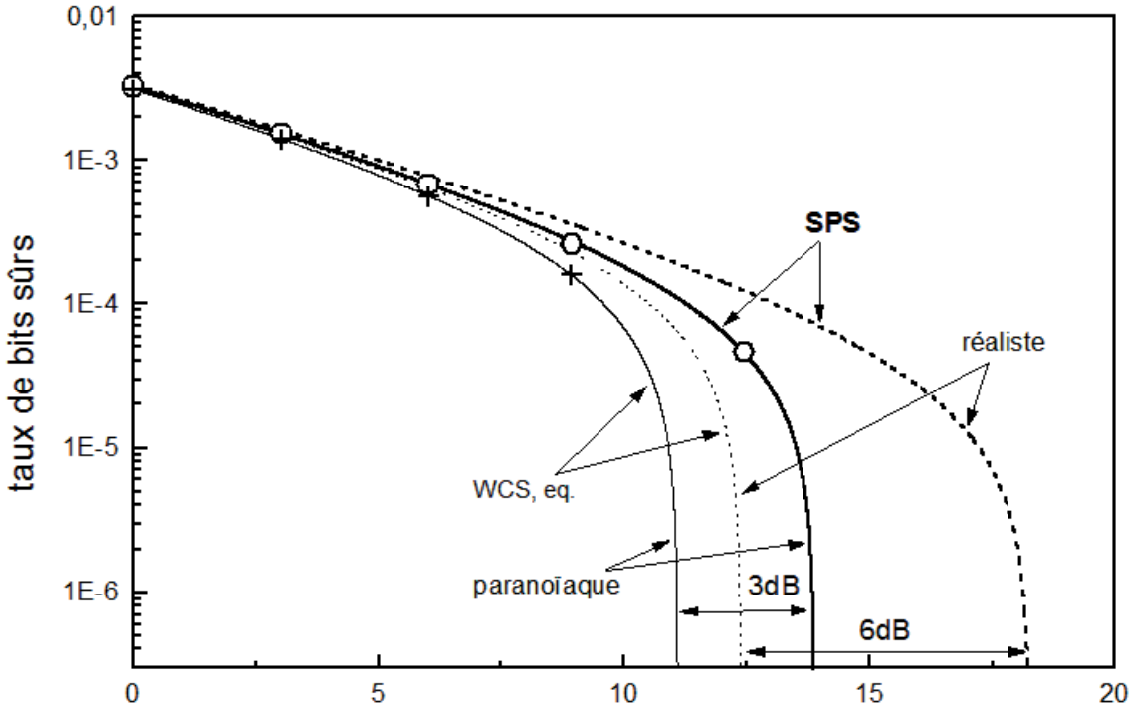

Figure 2.21: *Taux de bits sûrs en fonction de l'atténuation.*

Cette figure démontre l'intérêt de notre source lorsque les pertes sont importantes, même si nous n'atteignons pas ici les performances annoncées au début de ce chapitre: les coups d'obscurités sont le principal facteur limitant la portée de notre dispositif. Il faut cependant remarquer que les critères de sécurité qui ont été appliqués ici sont particulièrement restrictifs, puisqu'il a été implicitement supposé qu'Eve pouvait contrôler et annuler les coups d'obscurité de Bob. Nous avons en effet écrit que $n = n_1 + S_m N_{acq}/2$ (1.52,1.53): les coups d'obscurité sont pris en compte dans l'évaluation de n par Alice et Bob, mais la formule dont il est question ici correspond à une stratégie d'attaque d'Eve qui consiste à renvoyer vers Bob toutes les impulsions contenant plusieurs photons, et à compléter par des impulsions contenant un photon unique; cette stratégie suppose donc l'élimination des coups d'obscurités, qui n'apparaissent pas dans le bilan qui lui est associé (on peut faire la même remarque pour la formule (1.49) qui lie l'erreur D

introduite par l'espion au QBER e). Ce point de vue est en fait paranoïaque: si Eve possède une telle technologie, elle peut espionner Bob en amont de la procédure de codage. Je conclurai donc ce paragraphe par une approche réaliste, qui ne suppose plus cette capacité de contrôle des coups d'obscurité. Nous écrirons donc à la place de (1.52,1.53):

$$n = n_1 + S_m N_{acq}/2 + n_d \tag{2.13}$$

où n_d est le nombre d'évènements détectés correspondant aux coups d'obscurité.

Par ailleurs, si D est le taux d'erreur introduit par Eve sur l'espionnage des photons uniques, on aura pour le QBER:

$$en = Dn_1 + n_d/2 \tag{2.14}$$

La probabilité de collision est toujours donnée par 1.47 dans le cas d'un photon unique, et vaut 1 dans le cas de l'émission de photons multiples. Dans le cas d'un coup d'obscurité, Eve n'a aucune information particulière et la probabilité de collision vaut 1/2. L'entropie de Rényi s'écrit dans ce cas:

$$H_2(X|Z) = n_d - n_1 \log_2(\frac{1}{2} + 2D - 2D^2) \tag{2.15}$$

Le taux de bits sûrs qui en découle (donné par 1.42) est présenté sur la figure 2.21, avec des performances améliorées en terme de portée, ainsi qu'un avantage pour la source de photons uniques, dont la portée est de 6 dB supérieure à celle de la source atténuée. Ceci démontre l'importance des hypothèses de sécurité et du traitement de l'information pour les performances obtenues.

2.5 Conclusion

Nous avons donc pu mettre au point une source de photons uniques fiable, présentant un réel avantage compétitif pour la transmission de clé secrète en présence de fortes pertes. Les performances de notre source pourraient par ailleurs être encore améliorées, en augmentant par exemple les facteurs de transmission des différents filtres utilisés. L'efficacité de collection de l'objectif pourrait être également améliorée par l'insertion des nanocristaux de diamant dans des microcavités, permettant ainsi une émission plus directive vers l'objectif. Ainsi, la possibilité d'obtenir un rendement de collection global de la source dépassant 10 ou 20% est tout-à-fait envisageable. Cette source dont, rappelons-le, la longueur d'onde d'émission se situe aux alentours de 700 nm, peut trouver une application dans la transmission codée par satellite, l'atmosphère présentant une fenêtre de transmission à cette longueur d'onde.

Cette conclusion doit toutefois être modérée par la possibilité de contrecarrer les attaques PNS[94, 107, 168] en utilisant des états leurre ('decoy state'): Alice peut remplacer, de manière aléatoire, certaines impulsions signal par des impulsions leurres; dans le cas d'un protocole utilisant une source cohérente atténuée, ces impulsions leurre peuvent consister en des impulsions cohérentes générées avec une atténuation différente de celle des impulsions signal. Eve ne peut pas distinguer les deux types d'impulsions, et devra appliquer la même stratégie d'attaque dans tous les cas. Par contre, Bob sera informé par Alice, à l'issue de transmission des qubits, de la position des impulsions leurre. Il pourra ainsi calculer les propriétés de transmission du canal (pertes, taux d'erreurs) associées à ces impulsions. On peut montrer[94] qu'une attaque PNS va modifier ces propriétes de transmission, et que leur mesure permet de majorer le nombre d'impulsions à deux photons attaquées par Eve. Cette stratégie pourrait limiter l'avantage de

notre source à photons uniques, puisqu'elle permet de se protéger des attaques PNS en utilisant de simples sources atténuées. On pourrait cependant envisager d'utiliser également ces états leurre avec des sources à photons uniques, et peut-être redonner ainsi l'avantage à ces dernières.

2.6 Articles annexés au chapitre

[2.1] R. Brouri, A. Beveratos, J. P. Poizat, P. Grangier, Single photon generation by pulsed excitation of a single dipole, *Phys. Rev. A* **62**, 063814 (2000).

[2.2] R. Brouri, A. Beveratos, J.-Ph. Poizat et P. Grangier, Photon antibunching in the fluorescence of individual color centers in diamond, *Opt. Lett.* **25**, 1294 (2000).

[2.3] A.Beveratos, R.Brouri, J.P. Poizat et P.Grangier, Bunching and antibunching from single NV color centers in diamond, *QCM&C 3 Proceedings (Kluver Academic/Plenum Publisher)*.

[2.4] A.Beveratos, R.Brouri, T.Gagoin, J.P. Poizat et P.Grangier, Nonclassical radiation from diamond nanocrystals, *Phys. Rev. A* **64**, 061802 (2001).

[2.5] A.Beveratos, S.Kühn, R.Brouri, T.Gagoin, J.P. Poizat et P.Grangier, Room temperature stable single photon source, *EPJ D* **18**, 191 (2002).

[2.6] A.Beveratos, R.Brouri, T.Gacoin, A.Villing, H.P.Poizat et P.Grangier, Single photon quantum cryptography, *Phys. Rev. Lett.* **89**, 187901 (2002).

[2.7] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle et P. Grangier, Experimental open air quantum key distribution with a single photon source, *New J. Phys* **6**, 92 (2004).

Chapitre 3

Cryptographie avec des variables continues

Sommaire

Parallèlement à nos expériences de cryptographie utilisant notre source de photons uniques, nous nous sommes intéressé à la possibilité de faire de la cryptographie quantique avec des mesures à valeurs dans un continuum. Nous reviendrons dans un instant sur la potentialité de cette thématique, après de brefs rappels d'optique quantique introduisant les mesures en question.

3.1 Rappels d'optique quantique

Dans toute la suite de ce manuscrit, et de manière générale dans tous les travaux que nous avons publié jusqu'à présent sur la question, nous travaillons sur un unique mode du champ électromagnétique, correspondant à une impulsion lumineuse. Classiquement et en notation complexe, le champ électromagnétique dans cette impulsion va s'écrire:

$$\overrightarrow{E}(\overrightarrow{r},t) = \alpha\,\overrightarrow{e}(\overrightarrow{r},t), \qquad \overrightarrow{B}(\overrightarrow{r},t) = \alpha\,\overrightarrow{b}(\overrightarrow{r},t) \tag{3.1}$$

où $\overrightarrow{e}$ et $\overrightarrow{b}$ sont des champs normalisés, correspondant à une impulsion d'énergie E_0. Toute mesure dépendra uniquement de l'amplitude complexe α, cette grandeur ne pouvant toutefois pas être mesurée directement. L'énergie E de l'impulsion est ainsi égale à $|\alpha|^2 E_0$. En utilisant une image semi-classique, si l'impulsion contient n photons et si l'on définit E_0 comme étant l'énergie moyenne d'un photon, on aura $E = nE_0$, soit:

$$n = |\alpha|^2 \tag{3.2}$$

Remarquons qu'avec la plupart des photodétecteurs, qui convertissent les photons en électrons, c'est cette quantité qui est mesurée. Pour accéder maintenant à la phase de α, il faut envisager un dispositif interférométrique. C'est typiquement le rôle d'une détection homodyne, dont le principe est décrit sur la figure 3.1. On fait interférer à l'aide d'une séparatrice 50/50 une impulsion 'signal' d'amplitude α avec une impulsion de référence d'amplitude α_{ol} , également appelée oscillateur local. Ces deux impulsions sont supposées se recouvrir parfaitement, si bien que les amplitudes des impulsions transmises, α_A et α_B, s'expriment simplement en fonction des amplitudes d'entrée (voir figure).

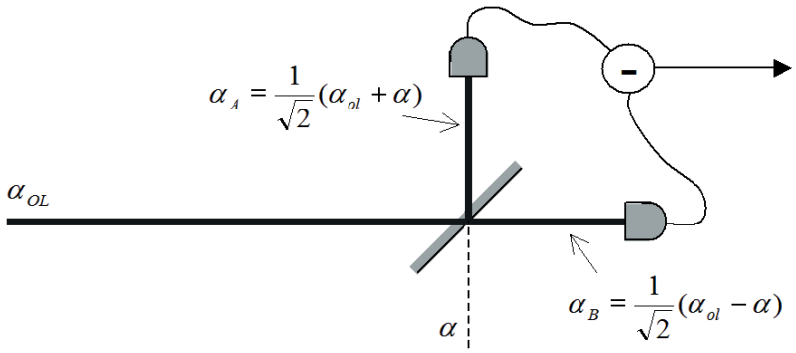

Figure 3.1: *Principe d'une détection homodyne.*

Le signal mesuré correspond ainsi à la différence des mesures effectuées sur chacune des voies, ce qui permet d'isoler le signal d'interférence:

$$\Delta n = |\alpha_A|^2 - |\alpha_B|^2 = \alpha_{ol}^* \alpha + \alpha_{ol}\alpha^* \tag{3.3}$$

ou encore, en notant $\alpha_{ol} = |\alpha_{ol}| \exp(i\varphi) = \sqrt{n_{ol}} \exp(i\varphi)$, n_{ol} étant le nombre de photons dans l'oscillateur local:

$$\Delta n = \sqrt{n_{ol}}\ [\exp(-i\varphi)\alpha + \exp(i\varphi)\alpha^*] \equiv \sqrt{\frac{n_{ol}}{N_0}}\ x(\varphi) \tag{3.4}$$

où l'on a introduit la quadrature $x(\varphi)$ du champ signal. Nous introduisons ici le préfacteur N_0 arbitraire afin de lever toute ambiguïté dans la définition des quadratures, qui peut varier selon les auteurs (nous verrons que cette quantité représente en fait la variance des fluctuations quantiques des quadratures d'un état vide).

Ce dispositif a donc pour fonction essentielle de mesurer une quadrature. Si l'oscillateur local est suffisamment intense, on pourra ainsi étudier des signaux très faibles, même en utilisant de simples photodiodes pour la détection. La phase φ peut quant à elle être ajustée en contrôlant le chemin optique de l'oscillateur local. On peut en effet écrire, pour des impulsions qui ne sont pas trop larges spectralement et dans le cadre d'une approximation d'enveloppe lentement variable:

$$\overrightarrow{E}(z+\delta L) \approx \exp[-2\pi i \frac{\delta L}{\lambda_0}] \overrightarrow{E}(z) \tag{3.5}$$

λ_0 étant la longueur d'onde centrale de l'impulsion.

On peut visualiser la quadrature $x(\varphi)$ comme étant la projection, dans le plan complexe, de $2N_0^{1/2}\alpha$ sur une droite faisant un angle φ avec l'axe réel (figure 3.2a). α est d'ailleurs complètement déterminée par la mesure des deux quadratures $q = x(0)$ et $p = x(\pi/2)$:

$$\alpha = \frac{q+ip}{2\sqrt{N_0}} \tag{3.6}$$

La procédure de quantification conduit à associer l'opérateur a à l'amplitude α, opérateur qui, n'étant pas une observable, est distinct de son adjoint $a^\dagger$. Pour décrire les interactions on se placera en représentation de Heisenberg: les opérateurs quantiques évoluent de la même façon que leurs homologues classiques, et les états quantiques ne sont pas modifiés. Ces opérateurs $a^\dagger$ et a sont interprétés comme les opérateurs création et annihilation d'un oscillateur harmonique, les photons étant les différents modes d'excitation de cet oscillateur. On a donc:

$$[a, a^\dagger] = 1 \tag{3.7}$$

l'état vide $|0\rangle$ vérifiant:

$$a|0\rangle = 0 \tag{3.8}$$

L'observable associée au nombre de photons (3.2) est $N = a^\dagger a$, dont les états propres sont les états de Fock $|n\rangle$ (états à n photons):

$$N|n\rangle = n|n\rangle \tag{3.9}$$

Concernant la détection homodyne, si l'oscillateur local est suffisamment intense pour être traité classiquement ($a_{ol} \approx \alpha_{ol},\ a_{ol}^\dagger \approx \alpha_{ol}^*$), l'observable mesurée sera l'opérateur de quadrature:

$$X(\varphi) = \sqrt{N_0}[\exp(-i\varphi)a + \exp(i\varphi)a^\dagger] \tag{3.10}$$

ou plus précisément

$$\Delta N = \sqrt{\frac{n_{ol}}{N_0}}\ X(\varphi) \tag{3.11}$$

qui est la version quantifiée de (3.4).

Nous nous intéresserons plus particulièrement par la suite à la paire conjuguée $Q = X(0)$, $P = X(\pi/2)$), qui vérifie la relation de commutation:

$$[Q, P] = 2N_0 i \tag{3.12}$$

Ces observables ont donc un comportement analogue à celui des opérateurs position et impulsion: ce sont des opérateurs à spectre continu, dont on notera q et p les valeurs propres correspondant aux vecteurs propres $|q\rangle$ et $|p\rangle$. L'opérateur P vérifiant (3.12) s'écrit en représentation q:

$$P = -2N_0 i \frac{d}{dq} \tag{3.13}$$

Cette dernière relation peut notamment être utilisée pour exprimer les états de Fock dans l'espace des quadratures. La relation (3.12) implique également des inégalités de Heisenberg: si V_Q et V_P sont les variances respectives de Q et P, on aura en effet:

$$V_Q V_P \geq N_0^2 \tag{3.14}$$

On ne peut donc connaître exactement les quadratures Q et P, ni faire correspondre à un état quantique un point du plan complexe (figure 3.2a). Pour représenter un état quantique, on pourra par exemple introduire la fonction de Wigner $W(q, p)$ de cet état, fonction réelle directement reliée à la matrice densité de l'état, dont la projection sur une droite permet d'obtenir la distribution de probabilité de la quadrature correspondante (figure 3.2b). Nous reviendrons plus en détails au chapitre 4 sur cette fonction, qui peut être vue comme une distribution de probabilité dans l'espace des phases.

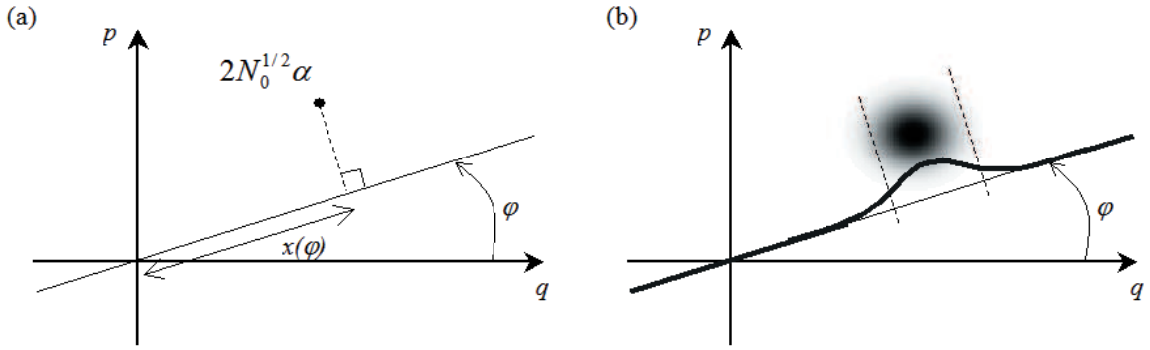

Figure 3.2: *(a) positionnement de l'amplitude classique α dans l'espace des quadratures. La quadrature $x(\varphi)$ correspond à la projection de ce point sur un axe faisant un angle φ avec l'axe q. (b) cas quantique: la projection de la fonction de Wigner sur cet axe reproduit la distribution de probabilité de $x(\varphi)$.*

La borne minimale de l'inégalité de Heisenberg (3.14) est atteinte pour des états gaussiens: leur fonction de Wigner est une gaussienne dont les axes propres sont les axes q et p. Ce sont des états comprimés ('squeezed states' en anglais), caractérisés par un facteur de compression $s \leq 1$: pour un état comprimé suivant la quadrature q, on aura $V_Q = sN_0$, $V_P = N_0/s$. On pourra écrire la fonction d'onde d'un tel état en représentation q:

$$\psi_s(q) = (2\pi s N_0)^{-\frac{1}{4}} \exp[-\frac{1}{4}\frac{(q-q_0)^2}{sN_0} + i\frac{pq}{2N_0}] \tag{3.15}$$

A titre indicatif, on aura pour sa fonction de Wigner:

$$W_s(q,p) = (2\pi N_0)^{-1} \exp[-\frac{1}{2}\frac{(q-q_0)^2}{sN_0} - \frac{s}{2}\frac{(p-p_0)^2}{N_0}] \tag{3.16}$$

La cas s=1 correspond aux états cohérents, qui vérifient:

$$V_Q = V_P = N_0 \tag{3.17}$$

quel que soit le couple de quadratures Q et P considéré. A toute valeur de l'amplitude complexe $\alpha = (q_0 + ip_0)/\sqrt{4N_0}$ correspond l'état cohérent $|\alpha\rangle$, dont la fonction d'onde est donnée par (3.15) avec $s = 1$. On a notamment:

$$a|\alpha\rangle = \alpha|\alpha\rangle \tag{3.18}$$

Les états cohérents sont les états qui correspondent au mieux à une impulsion cohérente dont l'amplitude et la phase sont bien déterminées. Remarquons avec (3.8) que l'état vide peut être considéré comme un état cohérent d'amplitude nulle. Ainsi, si aucun signal n'est envoyé dans la détection homodyne, des fluctuations seront tout de même observées (voir 3.17), liées à la nature quantique de l'observation effectuée. D'après (3.4,3.17), la variance de ces fluctuations est exactement n_{ol}, le nombre de photons de l'oscillateur local, ce qui pourrait conduire à interpréter ce bruit quantique comme un bruit de grenaille relatif à la distribution des photons au niveau de la séparatrice. Il faut cependant remarquer que n_{ol} n'est qu'un simple facteur d'échelle dans (3.11), l'observable considérée étant uniquement caractérisée par l'impulsion signal: les fluctuations observées sont donc bien des fluctuations quantiques. On parle de fluctuations du vide, que l'on peut d'ailleurs considérablement réduire en utilisant un vide comprimé.

Nous venons donc d'introduire les concepts et les notations que nous allons utiliser. Pour revenir à la cryptographie quantique, la question maintenant et de voir s'il est possible de transmettre une clé en codant l'information sur les quadratures d'une impulsion lumineuse.

3.2 Les protocoles de cryptographie à variables continues

3.2.1 Introduction

L'idée de coder l'information sur les quadratures d'une impulsion lumineuse plutôt que sur l'état d'un photon unique est très séduisante: disposant d'un continuum de canaux, on peut en effet espérer pouvoir coder beaucoup plus d'informations sur une impulsion lumineuse que sur un photon unique. Par ailleurs, une détection homodyne peut être plus rapide et moins chère qu'une photodiode à avalanche, ce qui n'est pas sans intérêt pour une application commerciale.

De nombreuses propositions de protocoles[92, 138, 139, 143, 75, 16, 154] ont ainsi vu le jour à partir de 1999, mais la plupart de ces protocoles étaient conçus comme des analogues de BB84, cherchant à coder un unique bit d'information dans les variables continues. Nicolas Cerf et ses collaborateurs[44, 45] ont été les premiers à proposer un protocole exploitant la théorie de l'information avec des variables continues. Dans ce protocole, Alice code une variable aléatoire gaussienne et centrée $\overline{X}_A$ en utilisant une impulsion comprimée (figure 3.3): elle utilise pour cela soit la quadrature Q, en envoyant une impulsion centrée sur $(Q = \overline{X}_A, P = 0)$ soit la quadrature P, avec une impulsion centrée sur $(Q = 0, P = \overline{X}_A)$, l'impulsion étant dans tous

les cas comprimée selon la quadrature choisie. Bob mesure aléatoirement la quadrature P ou Q, et rejette a posteriori sa mesure s'il a fait le mauvais choix. Le choix d'une distribution gaussienne pour $\overline{X}_A$ peut se comprendre puisque, à variance $\langle \overline{X}_A^2 \rangle \equiv V_A N_0$ fixée, c'est-à-dire à énergie moyenne fixée, la distribution gaussienne maximise la quantité d'information envoyée (voir section 1.2.4 du chapitre 1).

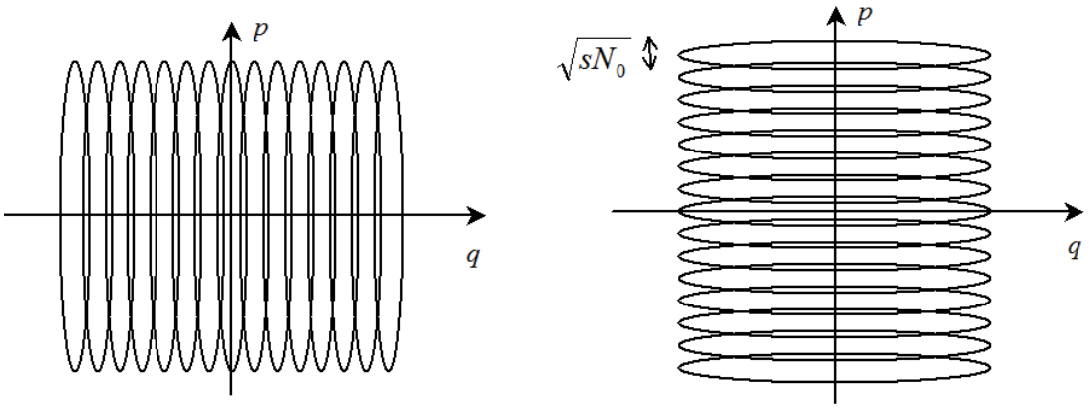

Figure 3.3: *Protocole de codage utilisant des états comprimés.*

Le fait que l'état soit comprimé permet de limiter le bruit quantique sur la mesure, et donc de transférer un grand nombre d'informations. Si Eve mesure la mauvaise quadrature, elle va introduire une erreur importante sur les données de Bob.

Pour quantifier toutes ces affirmations, il est nécessaire de modéliser le canal reliant Alice et Bob. Nous supposerons que les propriétés de ce canal sont symétriques[1] pour P et Q. Le canal va introduire des pertes, et nous noterons G son gain en energie ($G < 1$). Les quadratures suivent un comportement analogue à celui des amplitudes complexes, qui seront atténuées d'un facteur $\sqrt{G}$ à la traversée du canal, et l'on modélisera[78, 80] l'action du canal en écrivant pour les quadratures reçues par Bob:

$$Q_B = \sqrt{G}Q + B_Q \tag{3.19}$$

$$P_B = \sqrt{G}P + B_P \tag{3.20}$$

où B_Q et B_P sont les bruits ajoutés par le canal, qui ne sont pas corrélés au signal d'entrée. Considérons pour simplifier le choix de Q comme quadrature de codage (un raisonnement équivalent s'appliquera au choix de P). B_Q n'est pas corrélé à Q, et donc commute avec lui. Toutes les observables de (3.19) sont donc compatibles, et on peut les considérer comme de simples variables aléatoires, que nous supposerons par ailleurs gaussiennes. Ce dernier point est évident pour Q, que l'on peut réécrire $Q = \overline{X}_A + \delta Q$, où δQ correspond au bruit quantique sur l'état émis par Alice, de distribution gaussienne et de variance sN_0. Q est donc associé à une distribution gaussienne de variance:

$$\langle Q^2 \rangle = \langle \overline{X}_A^2 \rangle + \langle \delta Q^2 \rangle = (V_A + s)N_0 \equiv VN_0 \tag{3.21}$$

[1] On se reportera aux références [44], [80], [3.1] et [3.2] pour un traitement plus complet, qui n'apporte aucune modification fondamentale.

Par contre, il est beaucoup moins évident que B_Q corresponde également à une distribution gaussienne, puisque le bruit de canal comprend le bruit dû à l'espionnage d'Eve, qui n'est pas forcément gaussien. Il se trouve cependant que les attaques gaussiennes sont optimales pour Eve[84], et nous reviendrons sur ce point au 3.4.1. Nous poserons donc que tous les opérateurs de (3.19,3.20) ont une statistique gaussienne. On se rapproche ainsi du cas des canaux additifs gaussiens abordé au chapitre 1, où le signal B reçu par Bob était relié au signal A émis par Alice par $B = A + N$, N étant un bruit additif gaussien. Dans le cas présent, on pourra écrire (3.19) sous la forme:

$$B = G^{-\frac{1}{2}} Q_B = \overline{X}_A + (\delta Q + B_{Q,eq}) = A + N \tag{3.22}$$

où $B_{Q,eq} = G^{-1/2} B_Q$ est le bruit de canal ramené à l'entrée. On obtient ainsi, en posant $\langle B^2_{Q,eq} \rangle = \chi N_0$ et en utilisant (1.28) pour l'évaluation de l'information mutuelle:

$$I^{(Q)}_{AB} = \frac{1}{2} \log_2 [1 + \frac{< A^2 >}{< N^2 >}] = \frac{1}{2} \log_2 (1 + \frac{V_A}{s + \chi}) = \frac{1}{2} \log_2 (\frac{V + \chi}{s + \chi}) \tag{3.23}$$

Cette expression correspond à l'information transmise à Bob si celui-ci a choisi de mesurer la quadrature correcte. Si ce n'est pas le cas, aucune information n'est transmise, et l'expression (3.23) doit être divisée par deux pour prendre en compte ce fait:

$$I_{AB} = \frac{1}{4} \log_2 (\frac{V + \chi}{s + \chi}) \tag{3.24}$$

La variance χ du bruit ajouté est donc une donnée essentielle pour caractériser la capacité du canal à transmettre de l'information. Sa valeur peut être facilement déterminée dans le cas d'un canal présentant de simples pertes: cette valeur est en effet indépendante du signal, et comme une impulsion vide en entrée amène à une impulsion vide en sortie il vient:

$$\chi \equiv \chi_0 = \frac{1 - G}{G} \tag{3.25}$$

On écrira dans un cadre plus général:

$$\chi = \chi_0 + \epsilon \tag{3.26}$$

où l'"excès de bruit" ϵ est a priori positif. Cet excès de bruit peut avoir diverses origines, allant des bruits techniques dans la source laser au bruit électronique dans le système de détection homodyne, en passant par le bruit éventuellement ajouté par l'espion. En fait, il est difficile de déterminer expérimentalement χ avec une très haute précision, aussi le protocole doit-il être robuste par rapport à ce bruit pour avoir une marge d'erreur.

Il s'agit maintenant de quantifier la quantité d'information obtenue par Eve. Le modèle utilisé pour le canal d'écoute d'Eve est analogue à celui de Bob:

$$Q_E = \sqrt{H}(Q + C_{Q,eq}) \tag{3.27}$$

$$P_E = \sqrt{H}(P + C_{P,eq}) \tag{3.28}$$

C'est à ce niveau que la nature quantique des opérateurs va entrer en jeu, afin de minorer le bruit sur l'écoute d'Eve en utilisant les relations de Heisenberg. Les observables Q_E et P_B correspondent à des mesures effectuées sur des systèmes physiques différents (à savoir 2 impulsions laser), donc elles commutent :

$$[Q_E, P_B] = \sqrt{GH}([Q, P] + [C_{Q,eq}, B_{P,eq}]) = 0 \tag{3.29}$$

d'où l'on déduit que:

$$[C_{Q,eq}, B_{P,eq}] = -2iN_0 \tag{3.30}$$

et donc que:

$$\langle C^2_{Q,eq}\rangle\langle B^2_{P,eq}\rangle \geq N_0^2 \Rightarrow \langle C^2_{Q,eq}\rangle \geq N_0/\chi \tag{3.31}$$

Dit autrement, même si Eve et Bob coopèrent pour mesurer l'état émis par Alice, ils restent limités par le principe d'incertitude. La variance minimale de bruit sur l'écoute d'Eve est donc N_0/χ d'où l'on tire, en reprenant la démonstration de (3.24) avec $\chi \leftrightarrow \chi^{-1}$, l'information mutuelle optimale pour Eve:

$$I_{AE} = \frac{1}{4}\log_2(\frac{V+\chi^{-1}}{s+\chi^{-1}}) \tag{3.32}$$

On peut donc au final espérer un taux de secret par impulsion:

$$\Delta I = I_{AB} - I_{AE} = \frac{1}{4}\log_2(\frac{V+\chi}{s+\chi}\cdot\frac{s+\chi^{-1}}{V+\chi^{-1}}) \tag{3.33}$$

Comme $s < V$ par définition de V (3.21), cette expression est positive pour $\chi < 1$. Au vu de ce qui a été exposé au chapitre 1, on peut donc espérer extraire une clé secrète à partir des informations collectées par Bob.

3.2.2 Cryptographie avec des états cohérents

A ce niveau, Frédéric Grosshans et Philippe Grangier ont soulevé[79, 81] deux points fondamentaux. Le premier de ces points[79] concerne le fait que la condition $s < 1$ n'a pas été utilisée dans le raisonnement précédent. Cela signifie qu'une information secrète peut être également transférée en utilisant la quadrature amplifiée, à condition que $1/s < V$. Il est donc dommage d'abandonner la moitié des impulsions en ne codant aucune information sur la quadrature amplifiée.

On peut donc considérer un nouveau protocole dans lequel Alice envoie toujours des impulsions comprimées selon Q ou P, mais centrées sur $(\overline{Q}_A, \overline{P}_A)$, $\overline{Q}_A$ et $\overline{P}_A$ étant deux variables aléatoires gaussiennes et centrées, non corrélées, de variances respectives, pour un faisceau comprimé selon Q (figure 3.4) :

$$N_0^{-1}\langle\overline{Q}_A^2\rangle = V - s, \quad N_0^{-1}\langle\overline{P}_A^2\rangle = V - \frac{1}{s} \tag{3.34}$$

Ces variances sont déterminées de façon à avoir la même variance VN_0 pour les quadratures Q et P émises par Alice:

Rien n'est donc modifié si Bob mesure la quadrature comprimée. Par contre, s'il a mesuré la quadrature amplifiée, il pourra tout de même extraire une clé secrète avec un débit par impulsion (voir 3.33 avec $s \leftrightarrow 1/s$) :

$$\Delta I^{ampl} = I_{AB} - I_{AE} = \frac{1}{4}\log_2(\frac{V+\chi}{s^{-1}+\chi}\cdot\frac{s^{-1}+\chi^{-1}}{V+\chi^{-1}}) \tag{3.35}$$

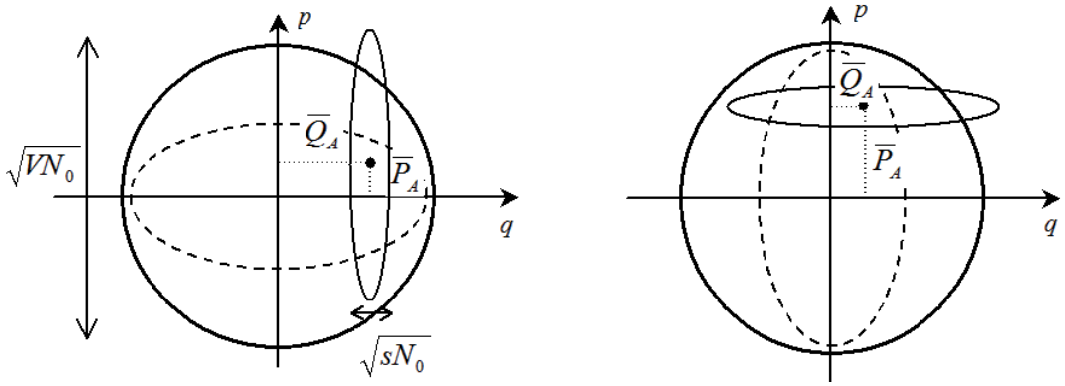

Figure 3.4: *Autre protocole de codage: $\overline{Q}_A$ et $\overline{P}_A$ sont choisies aléatoirement selon une statistique gaussienne (ligne de niveau pointillée). Les quadratures émises par Alice (Q et P) ont également une statistique gaussienne (ligne de niveau circulaire noire).*

On obtiendra le taux de secret global en faisant la somme de (3.33) et (3.35), qui se trouve être indépendante de s:

$$\Delta I^{tot} = \frac{1}{2}\log_2\left(\frac{V+\chi}{\chi V+1}\right) \tag{3.36}$$

L'usage d'impulsions cohérentes devient donc tout à fait légitime, ce qui est un point extrêmement important puisque ces impulsions sont beaucoup plus simples à produire que les impulsions comprimées.

Le seul point négatif concernant ce protocole est la condition $\chi < 1$ nécessaire pour avoir $\Delta I^{tot} > 0$. D'après (3.26,3.25), cette condition implique en effet un gain de canal supérieur à 1/2. Ce protocole est donc peu résistant aux pertes de canal, ce qui se comprend très bien puisque dans ce cas une attaque conceptuellement très simple est applicable: Eve utilise une lame séparatrice de transmission G, envoie la lumière transmise vers Bob en utilisant un canal sans pertes, et conserve une impulsion réfléchie avec un coefficient $R = 1 - G$, plus intense que l'impulsion reçue par Bob, lui permettant ainsi d'avoir plus d'informations sur les données d'Alice.

C'est ici qu'intervient le second point soulevé par Frédéric Grosshans et Philippe Grangier[81], qui va permettre de contourner cette difficulté par l'utilisation d'un protocole de réconciliation inverse.

3.2.3 Utilisation de la réconciliation inverse

Comme nous l'avons vu au chapitre 1(1.3.1), Ueli Maurer[118] montre que l'on peut également transmettre une clé secrète si $I_{BA} > I_{BE}$. Un moyen pour atteindre cet objectif consiste à utiliser la réconciliation inverse: la clé n'est plus construite à partir des données envoyées par Alice, mais avec les données reçues par Bob, et c'est Alice qui corrigera son message pour s'accorder sur celui de Bob. Il faut alors prendre en compte dans l'analyse de sécurité l'information que possède Eve sur les données de Bob, qui est généralement plus faible que l'information que possède Alice sur ces même données, puisqu'Eve cumule ses propres erreurs aux erreurs de Bob. Il est donc intéressant d'étudier les performances du protocole précédent avec la réconciliation inverse[81].

Pour quantifier ces performances, il est préférable d'utiliser l'expression (1.33) de l'information mutuelle, basée sur la notion de variance conditionnelle: si Alice emploie l'estimateur $\alpha\overline{Q}_A$ (resp. $\alpha\overline{P}_A$), elle commettra sur Q_B (resp. P_B) l'erreur:

$$\delta Q_{B|A,\alpha} = Q_B - \alpha\overline{Q}_A \quad (resp. \quad \delta P_{B|A,\alpha} = P_B - \alpha\overline{P}_A) \tag{3.37}$$

La variance de cette erreur est minimale pour $\alpha = \langle Q_B|\overline{Q}_A\rangle/\langle\overline{Q}_A^2\rangle = \sqrt{G}$, la valeur minimale obtenue étant, par définition, la variance conditionnelle:

$$V_{Q_B|\overline{Q}_A} = \langle Q_B^2\rangle - \frac{\langle Q_B\overline{Q}_A\rangle^2}{\langle\overline{Q}_A^2\rangle} = G[s+\chi]N_0 \quad (resp. \quad V_{P_B|\overline{P}_A} = G[s^{-1}+\chi]N_0) \tag{3.38}$$

dans le cas d'une impulsion comprimée suivant Q. L'information mutuelle s'obtient simplement par (1.33):

$$I_{BA} = \frac{1}{2}\log_2(\frac{\langle Q_B^2\rangle}{V_{Q_B|\overline{Q}_A}}) = \frac{1}{2}\log_2(\frac{V+\chi}{s+\chi}) \tag{3.39}$$

en parfait accord avec l'expression (3.23).
On écrira de même pour Eve:

$$\delta Q_{B|E,\beta} = Q_B - \beta Q_E, \quad \delta P_{B|E,\beta} = P_B - \beta P_E \tag{3.40}$$

Comme pour le cas du protocole direct, P_B et Q_E correspondent à des impulsions différentes et donc commutent. Comme $\overline{P}_A$ est un simple nombre qui commute avec tout opérateur, on peut écrire en utilisant (3.37):

$$[\delta Q_{B|E,\beta}, \delta P_{B|A,\alpha}] = [Q_B, P_B] = 2iN_0 \tag{3.41}$$

et

$$\langle\delta Q_{B|E,\beta}^2\rangle\langle\delta P_{B|A,\alpha}^2\rangle \geq N_0^2 \tag{3.42}$$

Il vient, comme cette dernière inégalité doit être satisfaite pour tout α, β:

$$V_{Q_B|Q_E}V_{P_B/\overline{P}_A} \geq N_0^2 \tag{3.43}$$

Alice et Eve ne peuvent connaître l'état de Bob avec une précision supérieure à celle autorisée par le principe d'incertitude. On peut ainsi minorer la variance conditionnelle d'Eve, et ainsi majorer la connaissance qu'elle a des données de Bob. Mais cette borne n'est pas la plus contraignante.

Pour obtenir la borne la plus contraignante, il est nécessaire de faire les remarques suivantes[82, 80]:

Tout d'abord, Alice n'envoie pas un état comprimé déterminé puisque cet état est centré sur un point $(\overline{Q}_A, \overline{P}_A)$ choisi aléatoirement selon la distribution gaussienne $p(\overline{Q}_A, \overline{P}_A)$. Elle envoie un mélange statistique d'états décrit par la matrice densité:

$$\rho_A = \int p(\overline{Q}_A, \overline{P}_A)\rho_{\overline{Q}_A,\overline{P}_A,s}d\overline{Q}_A d\overline{P}_A \tag{3.44}$$

où $\rho_{\overline{Q}_A,\overline{P}_A,s}$ est la matrice densité d'un état pur, comprimé suivant Q, centré sur $(\overline{Q}_A, \overline{P}_A)$. Il se trouve que, par construction, ρ_A ne dépend pas du facteur de compression s. On peut facilement

s'en convaincre en introduisant les fonctions de Wigner, qui dépendent linéairement des matrices densités et sont en correspondance biunivoque avec elles:

$$W_A(q,p) = \int p(\overline{Q}_A, \overline{P}_A) W_{\overline{Q}_A, \overline{P}_A, s}(q,p) d\overline{Q}_A d\overline{P}_A = (2\pi V N_0)^{-1} \exp(-\frac{q^2+p^2}{2VN_0}) \tag{3.45}$$

où l'on a utilisé l'expression (3.16) pour la fonction de Wigner d'un état comprimé (voir également la figure 3.4).

Nous pouvons ensuite utiliser l'argument suivant: les variances conditionnelles $V_{Q_B|Q_E}$ et $V_{P_B|P_E}$ ne dépendent que de la matrice densité des états reçus par Bob et Eve. Cette dernière ne dépend elle-même que de la matrice densité ρ_A du mélange statistique envoyé par Alice, ainsi que de la stratégie d'espionnage d'Eve. Certes, Eve peut modifier sa stratégie d'espionnage en fonction du facteur de compression s utilisé; mais on peut tout-à-fait considérer, pour les besoins de la démonstration, un cas d'école où Eve n'utilise qu'une seule stratégie optimisée pour des états cohérents ($s = 1$). Dans ce cas, comme ρ_A ne dépend pas de s, $V_{Q_B|Q_E}$ et $V_{P_B|P_E}$ sont également indépendant de s. Ils doivent cependant vérifier l'inégalité (3.43) pour toutes les valeurs de ce facteur, y compris pour celles qui minimisent $V_{P_B|\overline{P}_A}$ et $V_{Q_B|\overline{Q}_A}$ (respectivement $s = V$ et $s = V^{-1}$). On en déduit la minoration:

$$V_{Q_B|Q_E} \geq \frac{N_0^2}{V^{min}_{P_B|\overline{P}_A}} = \frac{N_0}{G(V^{-1}+\chi)} \tag{3.46}$$

avec une relation identique pour $V_{P_B|P_E}$. Ces relations doivent être vérifiées dans tous les cas, même si Alice n'utilise que des états cohérents: cette démonstration ne repose pas sur le fait qu'Alice utilise des états comprimés, mais uniquement sur le fait qu'elle puisse le faire.

On peut donc utiliser (3.46) même avec des états cohérents, pour lesquels on obtient le taux de secret:

$$\Delta I^{inverse} = I_{BA} - I_{BE} = \frac{1}{2}\log_2(\frac{V_{Q_B|Q_E}}{V_{Q_B|\overline{Q}_A}}) = -\frac{1}{2}\log_2[G^2(1+\chi)(V^{-1}+\chi)] \tag{3.47}$$

On aura donc un taux de secret positif pour:

$$G^2(1+\chi)(V^{-1}+\chi) < 1 \tag{3.48}$$

condition qui peut être réalisée pour des valeurs de G arbitrairement proche de 0. En effet, en re-introduisant l'excès de bruit ϵ avec (3.26), cette expression devient pour $G \ll 1$:

$$\epsilon < \frac{1}{2} - \frac{1}{2V} \tag{3.49}$$

C'est donc l'excès de bruit qui peut ici limiter l'application de ce protocole. Il est ainsi possible de développer un protocole de cryptographie à variables continues, n'utilisant que des états cohérents, et valable dans un régime de fortes pertes: il s'agit là d'un résultat tout à fait fondamental. Pour une analyse détaillée de ces résultats on se reportera à [81], ainsi qu'aux articles [3.1] et [3.2] joints à la fin de ce chapitre.

3.2.4 Exemple de stratégie d'espionnage optimale

Pour fixer les idées, nous allons développer une stratégie d'attaque d'Eve (voir également la référence [3.2]). Reprenons tout d'abord l'attaque de la séparatrice: Eve utilise une séparatrice dont les coefficients de réflexion et de transmission en amplitude sont respectivement $r = \sqrt{1-G}$ et $t = \sqrt{G}$. La figure 3.5 explicite les quadratures de sortie en fonction des quadratures d'entrée, relations directement déduites du cas classique (on obtient des relations similaires pour la quadrature P).

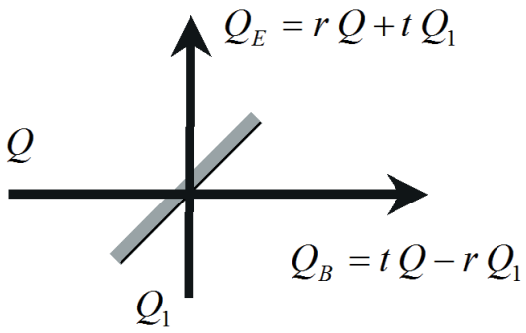

Figure 3.5: *Attaque utilisant une séparatrice. On obtient des relations similaires pour P.*

L'impulsion transmise est directement envoyée à Bob par une ligne sans perte, qui reçoit donc une quadrature vérifiant (3.19) avec $B_Q = -rQ_1$. On a ainsi:

$$\chi = \frac{\langle B_{Q,eq}^2 \rangle}{N_0} = \frac{r^2 \langle Q_1^2 \rangle}{GN_0} \tag{3.50}$$

Si Eve se contente d'intercaler sa séparatrice, l'impulsion entrant sur la voie Q_1 sera dans l'état vide du champ:

$$\langle Q_1^2 \rangle = N_0\ , \quad \chi = \frac{1-G}{G} = \chi_0 \tag{3.51}$$

où l'on retrouve sans surprise la valeur du bruit ajouté introduit du seul fait de l'atténuation du signal. L'examen de la figure 3.5 fait apparaître assez naturellement le fait que, pour améliorer sa connaissance des données de Bob, Eve a tout intérêt à injecter dans la voie Q_1 un état qu'elle connaît au mieux. Pour cela, la stratégie qui semble optimale consiste à utiliser une paire de faisceaux intriqués générée par une source EPR. Nous reviendrons plus en détails au chapitre 4 sur la description et la mise en œuvre de telles sources, et nous n'en ferons ici qu'une description succincte. Comme les observables $Q_1 - Q_2$ et $P_1 + P_2$ commutent, il est possible de disposer d'une paire de faisceaux vérifiant $Q_1 \approx Q_2$ et $P_1 \approx -P_2$: on peut alors connaître Q_1 (ou P_1) par la mesure de Q_2 (ou P_2). Eve peut donc injecter l'un des membres de la paire EPR dans la séparatrice et conserver l'autre dans une mémoire quantique, de façon à en faire ultérieurement la mesure Q_2 ou P_2. La relation avec Q_1 ou P_1 ne sera bien sûr pas exacte et l'on écrira:

$$Q_1 = Q_2 + Q_{inconnu} \quad (\Leftrightarrow Q_{inconnu} = Q_1 - Q_2) \tag{3.52}$$

où $Q_{inconnu}$ est un bruit centré, et avec une relation analogue pour les quadratures P. Le commutateur $[Q_{inconnu}, P_1]$ valant $2iN_0$, l'inégalité de Heisenberg qui en découle implique que l'on aura au mieux:

$$\langle Q^2_{inconnu}\rangle = \frac{N_0^2}{\langle P_1^2\rangle} = \frac{1-G}{G\chi}N_0 = \frac{\chi_0}{\chi}N_0 \quad \text{, avec} \quad \langle P_1^2\rangle = \langle Q_1^2\rangle = \frac{G\chi}{1-G}N_0 \tag{3.53}$$

où l'on a utilisé la relation (3.50) liant χ à la variance de Q_1. Donc, Eve a la possibilité de bien connaître les données de Bob, mais au prix d'un grand excès de bruit introduit dans le canal.

Une fois Q_2 mesurée et fixée, la valeur moyenne de Q_1 vaut Q_2 et l'on a $\langle Q_E\rangle = tQ_2$, $\langle Q_B\rangle = -rQ_2$. Nous avons ainsi affaire à des variables qui ne sont plus centrées et il nous faut, pour estimer l'information que possède Eve sur les données de Bob, introduire les variables centrées (voir 1.2.4):

$$Q'_E = Q_E - \langle Q_E\rangle = rQ + tQ_{inconnu} \tag{3.54}$$
$$Q'_B = Q_B - \langle Q_B\rangle = tQ - rQ_{inconnu} \tag{3.55}$$

Et l'on pourra en déduire la variance conditionnelle:

$$V_{Q'_B|Q'_E} = \langle Q'^2_B\rangle - \frac{\langle Q'_B Q'_E\rangle}{\langle Q'^2_E\rangle} = \frac{N_0}{G(V^{-1}+\chi)} \tag{3.56}$$

Ainsi, en utilisant ce que nous appellerons une cloneuse intriquante, il est possible pour Eve d'atteindre la limite (3.46): Cette stratégie d'attaque est donc optimale par rapport à l'analyse de sécurité précédemment effectuée. Nous reviendrons sur cette analyse au paragraphe 3.4, le paragraphe 3.3 étant dédié à la mise en œuvre expérimentale de notre protocole à états cohérents.

3.3 Réalisation expérimentale du protocole de cryptographie

3.3.1 Détection homodyne en régime impulsionnel

Le cœur de notre procédé consiste donc à coder l'information sur les quadratures d'une impulsion lumineuse. Le fait de travailler avec des impulsions, et donc de déterminer parfaitement le système quantique sur lequel nous effectuons le codage, est la principale originalité de l'ensemble de nos travaux sur les variables continues. Et la principale difficulté qu'il nous a fallu résoudre pour cela a été la conception de la détection homodyne (figure 3.1): il est en effet impossible, en mode impulsionnel, d'éliminer l'oscillateur local à l'aide d'un filtre passe-haut, comme on le fait habituellement en mode continu. Certes, l'oscillateur local n'apparaît pas dans (3.3), car l'énergie est équitablement distribuée sur chacune des deux voies de la détection homodyne; mais il faut un très bon équilibrage pour éliminer cette composante qui est beaucoup plus intense que le signal d'interférence.

Nous avons donc particulièrement soigné le montage[175]. Chaque voie est munie d'une lame demi-onde et d'un cube séparateur pour un réglage fin de la puissance lumineuse, et comporte deux miroirs réglables afin d'ajuster la position du faisceau selon la dépendance spatiale en sensibilité de la photodiode. Des lentilles permettent également d'optimiser la dimension des taches de focalisation (figure 3.10). Les photodiodes ont été triées de façon à offrir des caractéristiques optoélectroniques voisines. Elles sont indépendamment polarisées par des tensions ajustables pour équilibrer les capacités parasites. La soustraction des photocourants est réalisée par application directe de la loi des nœuds en sortie des photodiodes (figure 3.6).

Nous avons ainsi pu obtenir un taux de réjection de l'ordre de 85 dB, correspondant à un déséquilibrage des voies inférieur au $1/10000^e$. Malgré ces performances, l'oscillateur local devra tout de même ne pas être trop intense pour être correctement éliminé: nous travaillerons avec un

oscillateur local de l'ordre de quelques dizaines de μW, c'est-à-dire avec des impulsion contenant quelques centaines de millions de photons. Le signal d'interférence utile sera alors de l'ordre du nW. La détection homodyne doit donc être très sensible pour détecter correctement un signal qui n'est pas si intense que cela, avec un bruit électronique qui soit le plus faible possible, tout en conservant une bande passante importante afin d'isoler chaque impulsion avec une haute cadence d'émission. Nous avons pour cela utilisé deux amplificateurs faible bruit, amplifiant chacun d'un facteur 10 la tension aux bornes de la résistance de $4,7$ kΩ placée à la sortie des photodiodes.

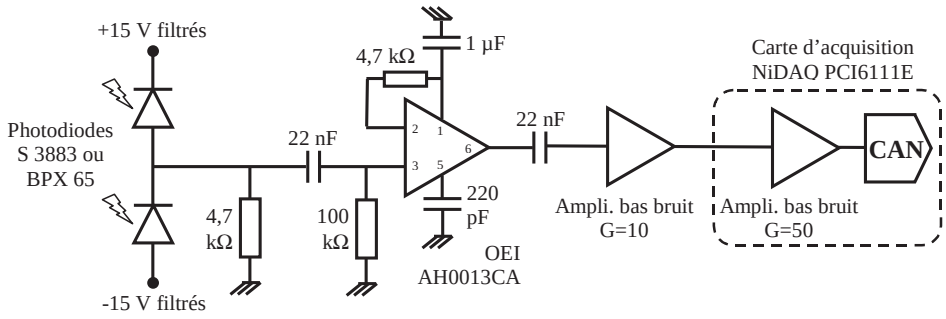

Figure 3.6: *Schéma électronique de la détection à amplification de tension.*

Le signal en sortie du dispositif de la figure 3.6 sera donc le produit de convolution du profil temporel de l'impulsion par la réponse impulsionnelle du système de détection, qui s'étale sur plusieurs centaines de nanosecondes. Avec des impulsions suffisamment courtes, le signal de sortie sera donc proportionnel à cette réponse impulsionnelle et à la différence d'énergie des impulsions des deux voies de la détection homodyne. Un échantillonnage du signal de sortie, convenablement synchronisé, permet donc d'obtenir une tension proportionnelle à cette différence d'énergie, ou de manière équivalente au nombre de photons Δn de l'équation (3.3). Nous avons pu atteindre un gain de $\kappa = 0,54$ μV par électron pour une bande passante de $6,5$ MHz.

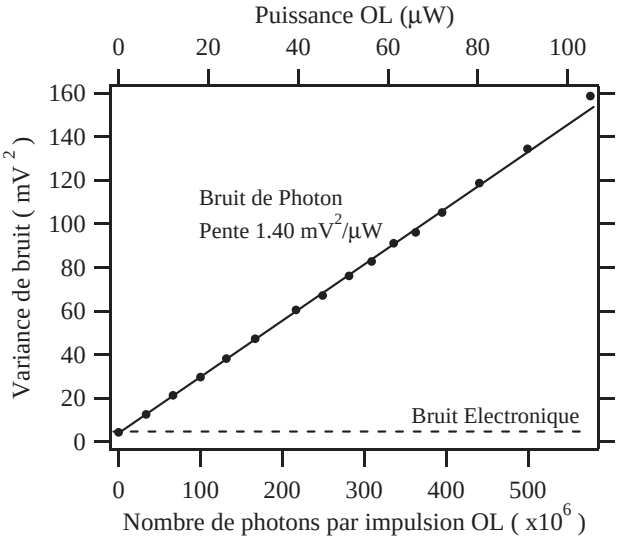

Figure 3.7: *Variance du bruit de la détection en fonction de la puissance de l'oscillateur local.*

La figure 3.7 présente, pour une mesure effectuée sur le vide quantique (sans impulsion signal), l'évolution de la variance du signal mesuré (en mV^2) en fonction de la puissance de l'oscillateur local. On obtient un comportement linéaire, conformément à (3.4). Le niveau du bruit électronique est indiqué par la ligne en pointillés. Ces données permettent de calibrer les mesures pour avoir au final une mesure de quadrature, indépendante de la puissance de l'oscillateur local.

Nous avons donc utilisé cette détection homodyne pour nos premières expériences de cryptographie, décrites dans cette section 3.3. Nous avons également développé par la suite une autre détection homodyne, qui fonctionne globalement selon le même principe, mais avec un amplificateur de charge, au lieu d'une simple résistance, pour l'analyse des photocourants. Le schéma de principe de ce dispositif, largement inspiré du travail de Hauke Hansen et de ses collaborateurs[90, 91, 114], est présenté sur la figure 3.8. Il permet, à bruit électronique équivalent, d'atteindre un gain de $\kappa = 2,24\ \mu$V par électron pour une bande passante de 10 MHz, soit un gain d'un facteur 20 pour le rapport signal à bruit en variance. Ce second montage a été utilisé dans toutes les expériences du chapitre 4, ainsi que pour les expériences de cryptographie plus récentes, mentionnées en section 3.5.

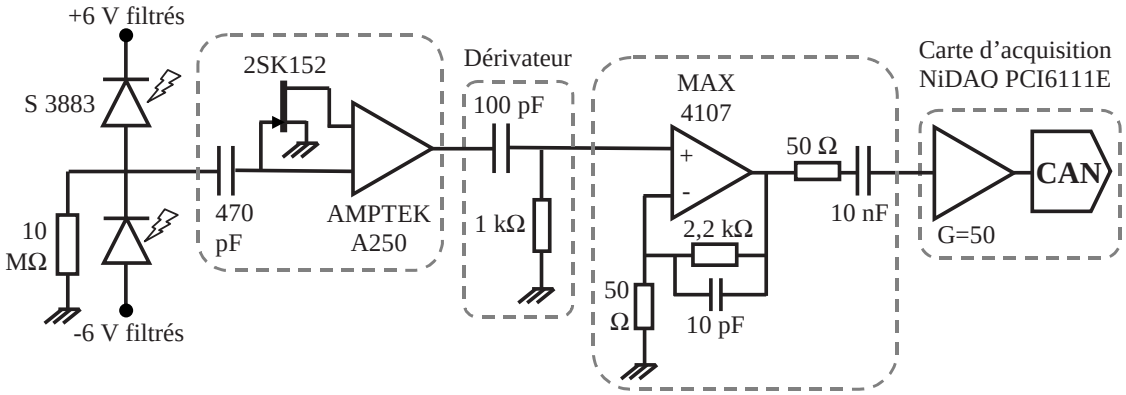

Figure 3.8: *Schéma électronique de la détection à amplification de charge.*

3.3.2 Modélisation des imperfections de la détection homodyne

Si les performances présentées au paragraphe précédent répondent au cahier des charges, d'autres données sont nécessaires pour une caractérisation complète du détecteur. Jusqu'à présent nous n'avons en effet pas pris en compte l'effet des pertes dans les optiques, de l'efficacité quantique des détecteurs, ni celui du recouvrement imparfait du signal et de l'oscillateur local. Pour évaluer ce dernier point, il est intéressant d'utiliser le produit scalaire naturellement introduit par la définition de l'énergie électromagnétique[2]. Classiquement, le champ signal $\overrightarrow{E}(\overrightarrow{r},t) = \alpha\,\overrightarrow{e}(\overrightarrow{r},t)$ et l'oscillateur local $\overrightarrow{E}_{ol}(\overrightarrow{r},t) = \alpha_{ol}\,\overrightarrow{e}_{ol}(\overrightarrow{r},t)$ vérifient :

$$\langle\overrightarrow{E}|\overrightarrow{E}\rangle = |\alpha|^2\langle\overrightarrow{e}|\overrightarrow{e}\rangle = |\alpha|^2 E_0\ ,\ \ \langle\overrightarrow{E_{ol}}|\overrightarrow{E_{ol}}\rangle = |\alpha_{ol}|^2 E_0 \tag{3.57}$$

où l'on rappelle que E_0 est l'énergie moyenne d'un photon dans l'impulsion.

[2]On pourra utiliser dans le cadre de l'approximation paraxiale $\langle\overrightarrow{E}_1|\overrightarrow{E}_2\rangle = \frac{\varepsilon_0}{2}\int \overrightarrow{E}_1(\overrightarrow{r},t)\cdot\overrightarrow{E}_2^*(\overrightarrow{r},t)d^3r$, $\langle\overrightarrow{E}|\overrightarrow{E}\rangle$ représentant ainsi l'énergie de l'impulsion.

Introduisons le taux de recouvrement:

$$\eta_{mod} = \langle \overrightarrow{e}_{ol} | \overrightarrow{e} \rangle / E_0 \tag{3.58}$$

quantité qui peut être rendue réelle par un choix adéquat des phases de $\overrightarrow{e}$ et $\overrightarrow{e}_{ol}$. L'énergie sur chaque voie s'écrit alors:

$$\frac{1}{2}\langle \overrightarrow{E} \pm \overrightarrow{E}_{ol} | \overrightarrow{E} \pm \overrightarrow{E}_{ol} \rangle = \frac{E_0}{2}\{|\alpha|^2 + |\alpha_{ol}|^2 \pm \eta_{mod}(\alpha_{ol}^* \alpha + \alpha_{ol}\alpha^*)\} \tag{3.59}$$

Dans une expérience classique d'interférométrie, avec $\alpha = \alpha_{ol}\exp(i\varphi)$, il vient simplement $I_0(1 + \eta_{mod}\cos(\varphi))$: le taux de recouvrement η_{mod} est alors égal au contraste des franges d'interférences. Pour maintenant évaluer l'influence du recouvrement dans le traitement quantique du problème, il faut prendre en compte tous les modes susceptibles d'avoir un recouvrement non nul avec l'oscillateur local: nous avons en effet vu qu'un mode, même vide, présente toujours des fluctuations de quadrature. Introduisons ainsi le mode $\perp$ défini par:

$$\overrightarrow{e}_{\perp} = \frac{\overrightarrow{e}_{ol} - \eta_{mod}\overrightarrow{e}}{\sqrt{1-\eta_{mod}^2}} \Leftrightarrow \overrightarrow{e}_{ol} = \eta_{mod}\overrightarrow{e} + \sqrt{1-\eta_{mod}^2}\,\overrightarrow{e}_{\perp} \tag{3.60}$$

Avec (3.57,3.58), on a $\langle \overrightarrow{e}_{\perp} | \overrightarrow{e}_{\perp} \rangle = E_0$ et $\langle \overrightarrow{e} | \overrightarrow{e}_{\perp} \rangle = 0$. De plus tout mode orthogonal à $\overrightarrow{e}$ et $\overrightarrow{e}_{\perp}$ est également orthogonal à $\overrightarrow{e}_{ol}$, et ne produira donc aucun signal d'interférence sur la détection homodyne. Au final seuls les modes $\overrightarrow{e}$ et $\overrightarrow{e}_{\perp}$ vont donc contribuer au signal homodyne, et la quadrature mesurée s'écrira après quantification:

$$X_m(\varphi) = \eta_{mod}X(\varphi) + \sqrt{1-\eta_{mod}^2}\,X_{\perp}(\varphi) \tag{3.61}$$

L'expression (3.61) est équivalente à l'action sur les quadratures d'une lame séparatrice de transmission (en énergie) η_{mod}^2. On peut donc modéliser l'imperfection du recouvrement en introduisant une séparatrice dans le bras amenant le signal d'entrée. Cette séparatrice aura un effet analogue à (3.61), le rôle du mode parasite $X_{\perp}$ étant joué par le mode X_0 incident sur l'autre voie de la séparatrice. On pourra de même prendre en compte le rendement quantique η_{phot} des photodiodes en plaçant une séparatrice de transmission η_{phot} devant chaque photodiode, et l'on peut montrer[80, 175] que ceci est également équivalent à placer une séparatrice de même transmission sur le bras amenant le signal d'entrée. Au final, on placera donc sur la voie d'entrée une séparatrice de transmission η, avec pour l'efficacité homodyne η:

$$\eta = \eta_{mod}^2\eta_{phot}\eta_{opt} \tag{3.62}$$

η_{opt} représentant les pertes au niveau des optiques. Dans notre expérience de cryptographie, nous avons obtenu $\eta_{phot} = \eta_{opt} = 92\%$, $\eta_{mod} = 96,5\%$, soit une efficacité homodyne $\eta = 79\%$. Au final, le signal homodyne mesuré s'écrit donc, en reprenant notamment (3.4):

$$v = \kappa\Delta n = \frac{v_0}{\sqrt{N_0}}[\sqrt{\eta}\,X(\varphi) + \sqrt{1-\eta}\,X_0(\varphi)] + v_{el} \tag{3.63}$$

où κ est le gain en tension par électron, où v_0 est l'écart-type (en mV) de mesures effectuées sur le vide quantique, et où v_{el} est le bruit électronique sur la tension mesurée. De cette mesure, Bob veut en déduire une estimation de $X(\varphi)$, et va donc calculer :

$$X_B(\varphi) = \sqrt{\frac{N_0}{\eta}}\,\frac{v}{v_0} = X(\varphi) + \sqrt{\frac{1-\eta}{\eta}}\,X_0(\varphi) + \frac{v_{el}}{v_0} \tag{3.64}$$

Les imperfections de la détection homodyne vont donc essentiellement se traduire par un bruit supplémentaire sur les mesures de Bob, de variance $(\chi_{hom} + \chi_{el})N_0$, avec:

- $\chi_{hom} = \frac{1-\eta}{\eta}$ pour l'excès de bruit lié à l'efficacité homodyne, soit $\chi_{hom} = 0,27$ pour nos conditions expérimentales.
- $\chi_{el} = \frac{1}{\eta}\frac{v_{el}^2}{v_0^2}$ pour l'excès de bruit lié aux bruits électroniques. Comme nous travaillerons avec $v_0 = 4,23$ mV, nous poserons par la suite $\chi_{el} = 0,33$.

Ces variances devront bien sûr être divisées par le gain de ligne G si on considère les bruits ramenés à l'entrée.

3.3.3 Influence des imperfections sur les performances du protocole

La détection homodyne introduit donc un excès de bruit important puisque $\chi_{hom} + \chi_{el}$ est supérieur à $N_0/2$. Au vu de (3.49), on peut donc s'attendre à ce qu'il réduise fortement les performances du protocole, notamment en terme de portée. Cependant, utiliser les formules (3.47,3.48) avec:

$$\chi = \chi_{ligne} + \frac{\chi_{hom} + \chi_{el}}{G} \tag{3.65}$$

revient à considérer qu'Eve peut manipuler ces excès de bruit. Nous avons déjà vu qu'une telle hypothèse était paranoïaque, puisque si Eve a une avance technologique qui lui permet ainsi de manipuler les instruments de Bob, elle peut espionner Bob directement, annulant l'intérêt même de la cryptographie. Il est donc nécessaire d'effectuer une étude réaliste de la sécurité, dans laquelle l'attaque d'Eve s'arrête à la quadrature Q_e (ou P_e) du champ à l'entrée de la détection homodyne. A ce niveau, les résultats précédents s'appliquent et l'on peut écrire en reprenant (3.46):

$$V_{Q_e|Q_E} \geq \frac{N_0}{G(V^{-1} + \chi_{ligne})} \tag{3.66}$$

où χ_{ligne} reprend le bruit de ligne χ_0, ainsi que l'excès de bruit ϵ lié à la présence du canal. En écrivant d'après (3.64): $Q_B = Q_e + B_{hom} + B_{el}$, et en utilisant la définition (1.31) de la variance conditionnelle, il vient:

$$V_{Q_B|Q_E} \geq \frac{N_0}{G(V^{-1} + \chi_{ligne})} + \chi_{hom}N_0 + \chi_{el}N_0 \tag{3.67}$$

et, en terme d'information mutuelle (1.33):

$$I_{BE} = \frac{1}{2}\log_2(\frac{\langle Q_B^2\rangle}{V_{Q_B|Q_E}}) \leq \frac{1}{2}\log_2[\frac{G^2(V+\chi)(V^{-1}+\chi_{ligne})}{1+G(\chi_{hom}+\chi_{el})(V^{-1}+\chi_{ligne})}] \tag{3.68}$$

Les informations mutuelles I_{AB}, I_{AE} et I_{BE} sont tracées sur la figure 3.9, dans les conditions de l'expérience et pour $V = 40$, dans le cas d'une approche paranoïaque ainsi que dans celui d'une approche réaliste. Cette dernière approche permet donc de préserver les performances du protocole, et notamment la possibilité en réconciliation inverse d'échanger une clé malgré un gain de canal arbitrairement faible.

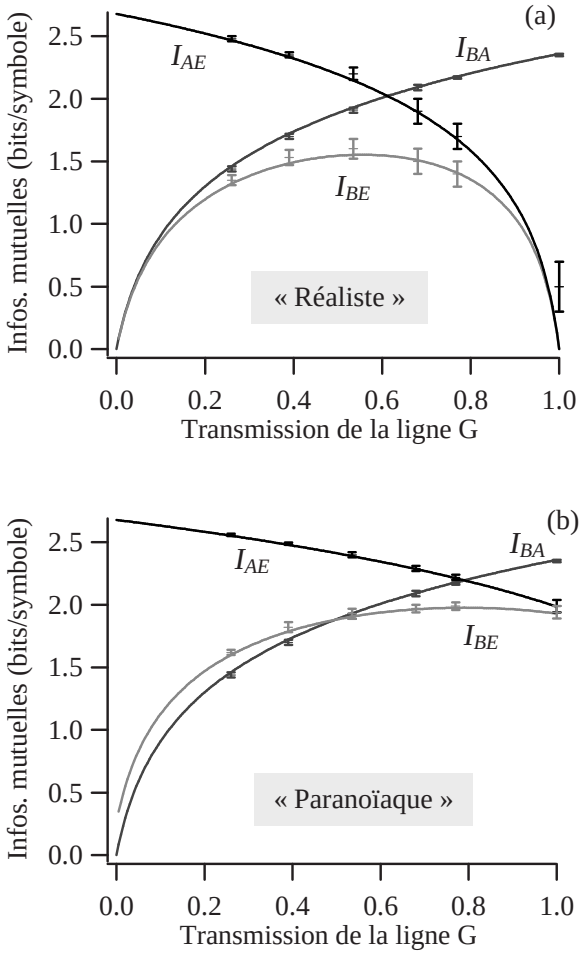

Figure 3.9: *Informations mutuelles calculées, dans les conditions de l'expérience et pour* $V = 40$*, dans le cas d'une approche réaliste et dans celui d'une approche paranoïaque.*

3.3.4 Le dispositif expérimental

L'ensemble de l'expérience est présenté sur la figure 3.10. Nous avons travaillé à 780 nm, en utilisant une diode laser montée en cavité étendue afin de disposer d'une raie laser étroite et stable. Un modulateur acousto-optique (AOM) permet l'émission d'impulsions courtes (FWHM 120 ns) à une cadence de 800 kHz. Une fibre à maintient de polarisation (MF) est utilisée pour le filtrage spatial du mode laser. Une partie du faisceau sera ensuite utilisée en tant qu'oscillateur local, tandis qu'un modulateur électro-optique (EOM) de très large bande passante (2 GHz) permet de contrôler l'amplitude de l'impulsion signal.

Pour pouvoir, selon le protocole proposé, émettre des impulsions selon une distribution gaussienne dans l'espace des quadratures, il faudrait également disposer d'un modulateur de phase rapide à 780 nm, et nous n'avons malheureusement pas pu nous procurer un tel dispositif: étant donné qu'il ne s'agit ici que d'une étape de démonstration de faisabilité, nous avons contourné ce problème en balayant linéairement la phase à l'aide du PZT normalement utilisé pour sélectionner la quadrature mesurée. Une permutation aléatoire des mesures permet ensuite de simuler une distribution aléatoire de la phase.

Enfin une lame séparatrice permet de simuler les pertes du canal de transmission. Le principe de la détection homodyne, qui constitue le dispositif de réception de Bob, a été décrit précédemment. La figure 3.11a présente un exemple de correspondance obtenue entre la quadrature $\overline{Q}_A$ émise par Alice et la quadrature Q_B mesurée par Bob, pour un bloc de 60000 impulsions échangées. On peut facilement extraire de ces données la valeur du bruit χ, puis celle de χ_{ligne}, après soustraction des composantes χ_{hom} et χ_{el}. Les valeurs obtenues pour χ_{ligne} sont présentées sur la figure 3.11b, et sont en bon accord avec la prédiction théorique $(1-G)/G$ (3.25) (nous n'avons pas introduit dans cette expérience de bruit de canal ajouté).

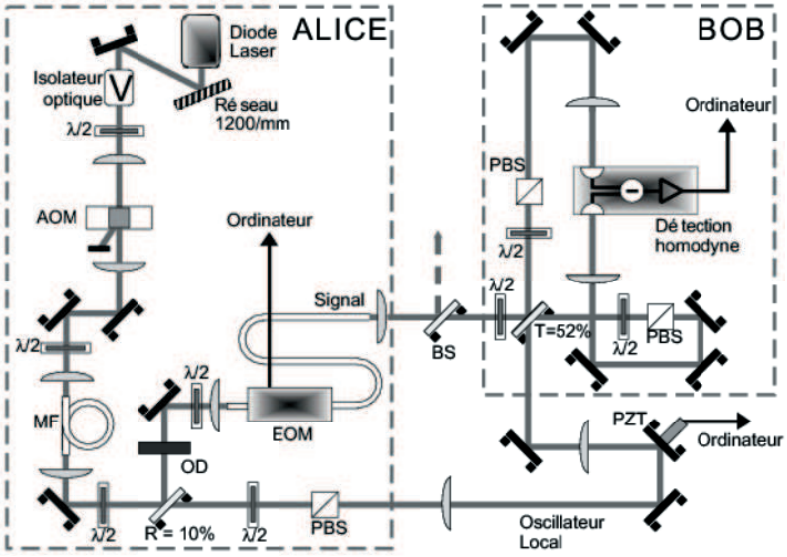

Figure 3.10: *Dispositif expérimental complet.*

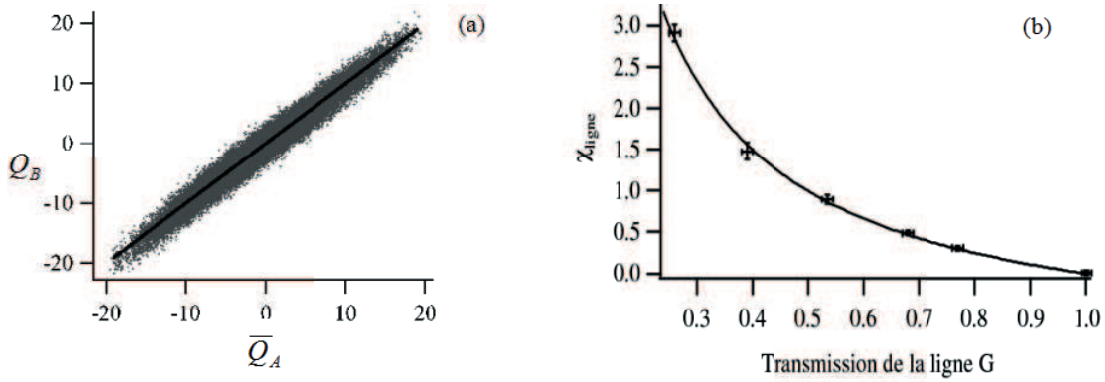

Figure 3.11: *(a) Quadrature Q_B mesurée par Bob en fonction de la quadrature $\overline{Q}_A$ envoyée par Alice, pour 60000 impulsions échangée et un gain de canal unité. (b) Variance expérimentale χ_{ligne} en fonction du gain G.*

3.3.5 Echange de clé secrète

Après la communication par le canal quantique, Alice et Bob partagent donc un ensemble de valeurs réelles corrélées, l'erreur sur les mesures de Bob étant liée à un bruit gaussien bien caractérisé. Pour obtenir une clé secrète, il va falloir maintenant passer par les étapes de réconciliation et d'amplification de confidentialité. Comme il existe pour cela des algorithmes aux performances éprouvées, mais fonctionnant sur des données binaires, une étape préliminaire va consister à discrétiser ces valeurs réelles: l'axe réel est partagé en un certain nombre d'intervalles, en l'occurrence une puissance de 2, et le numéro de l'intervalle dans lequel se trouve la valeur réelle fournira un mot binaire (figure 3.12). Bob va ainsi discrétiser toutes les valeurs codées sur les n impulsions envoyées par Alice, et obtenir n mots binaires. Ces mots peuvent être considérés comme les valeurs successives d'une variable aléatoire que nous noterons B, dans la continuité des notations du chapitre 1.

Selon le protocole de réconciliation inverse, Alice doit ensuite corriger ses propres valeurs pour partager avec Bob les mêmes mots binaires. La stratégie qui consisterait pour Alice à discrétiser d'abord les valeurs de quadratures qu'elle a envoyées, pour corriger ensuite les mots obtenus, n'est en fait pas optimale. Nous avons entrepris une collaboration avec l'équipe de Nicolas Cerf, à l'Université Libre de Bruxelle, sur ce sujet délicat de la réconciliation de variables continues: cette équipe a justement travaillé[163] à la conception d'un protocole, dit de "réconciliation par tranches" , optimisé pour ce problème particulier. L'idée est qu'une connaissance partielle des données de Bob contient en elle-même une information sur les données restantes. Concrètement imaginons que, sur chacun des n mots, Alice et Bob aient réconcilié les i premiers bits de poids faible. Alice peut alors utiliser cette connaissance pour donner une estimation plus fiables des bits de rang $i+1$ mesurés par Bob. Les n bits de cette tranche sont ensuite réconciliés avant de passer à la tranche suivante, et ce en utilisant un échange moins important d'information.

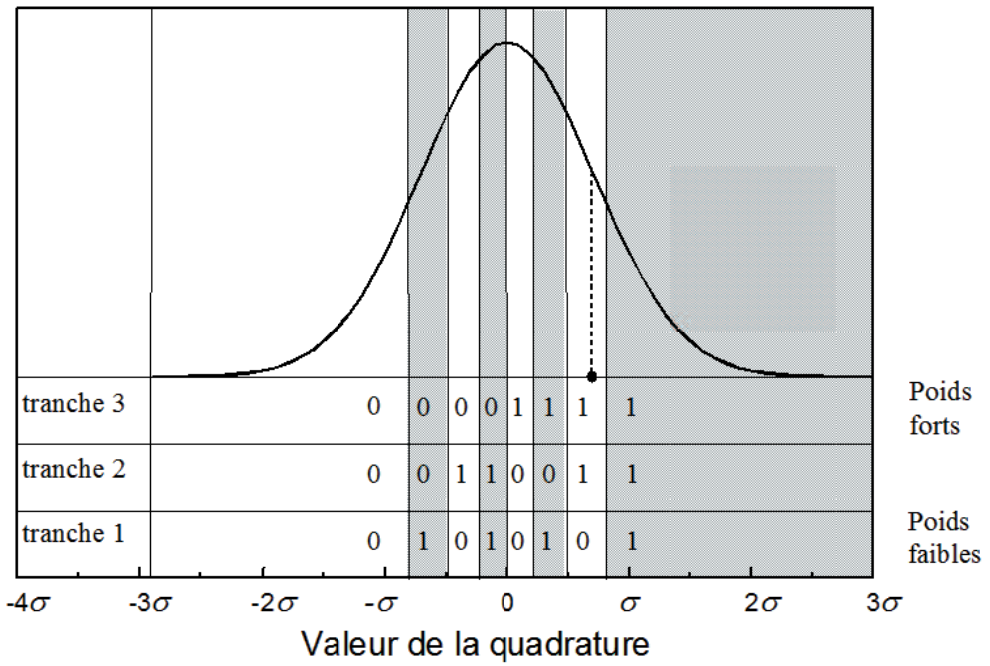

Figure 3.12: *Discrétisation des quadratures sur 3 bits. Sur l'exemple d'une quadrature valant 0,7σ (point noir), le codage binaire correspondant sera '110'.*

Le nombre d'intervalles utilisés pour la discrétisation, ainsi que leur distribution, est optimisé selon les paramètres expérimentaux pour garantir un transfert d'information maximal[127, 165]. Nous avons ainsi été amenés à utiliser 5 bits pour coder 32 intervalles. Les 2 premières tranches sont très bruitées, avec un taux d'erreur proche de 50%: la réconciliation est ici inefficace, et ces bits sont en fait directement révélés par Bob. Ces bits ne pourront donc pas contribuer directement à la clé secrète mais, dans l'esprit de la réconciliation par tranche, cette connaissance va permettre à Alice de diminuer son taux d'erreur sur les tranches suivantes, augmentant ainsi la taille de la clé finale. Les 3 tranches suivantes ont été réconciliées en utilisant le logiciel Cascade succinctement décrit au chapitre 1.

Nous avions notamment soulevé au chapitre 1 les problèmes liés à la bi-directionnalité de Cascade, et au fait que l'espion connaît la position ε des différences entre les données d'Alice et Bob. Ainsi, pour estimer la taille de la clé secrète, c'est l'information mutuelle $I(B;E,\varepsilon)$, et non $I(B;E)$, qui devra être prise en compte pour estimer la connaissance de l'espion. Ces deux quantités sont reliées par:

$$I(B;E,\varepsilon) = I(B;E) + I(B;\varepsilon|E) \tag{3.69}$$

où l'on a introduit la notation:

$$I(B;\varepsilon|E) \equiv H(B|E) - H(B|\varepsilon,E) \tag{3.70}$$

Et contrairement au cas du protocole BB84, cette quantité $I(B;\varepsilon|E)$ n'a ici aucune raison d'être nulle, et il faut pouvoir l'estimer. Nous l'avons calculée dans le cas d'une attaque par cloneuse intriquante (voir 2.2.5): toutes les distributions de probabilités sont en effet parfaitement connues dans le cadre de ce modèle, ce qui permet un calcul complet de (3.70) (on se reportera à la thèse de Gilles Van Assche[165] pour les détails de ce calcul). La taille de la clé secrète est ensuite fixée par une formule analogue à (1.45):

$$\frac{k_f}{n} < H(B) - \frac{r}{n} - I(B;\varepsilon|E) - I(B;E) \tag{3.71}$$

où l'on rappelle que r est la taille du message de réconciliation. La table 3.3.5, tirée de la référence [3.1] ainsi que de la thèse de Gilles Van Assche[165], résume les résultats obtenus à partir de nos données expérimentales (pour des blocs de 60000 impulsions).

G	V	$H(B)$	r/n	$I(B;\varepsilon\|E)$	η_{rec}	$I(B;E)$	bits sûrs /symbole	bits sûrs /seconde (kbits/s)	limite théorique (kbits/s)
1	41,7	4,63	2.50	0,000	89,0%	0,00	2,13	1 700	1 920
0,79	38,6	4,48	2,56	0,039	86,9%	1,23	0,65	520	730
0,68	32,3	4,33	2,64	0,082	83,2%	1,30	0,31	250	510
0,49	27	4,70	3,32	0,092	77,8%	1,20	0,09	75	370

Tableau 3.1: *performances obtenues à partir des données expérimentales.*

Dans cette table, le coefficient η_{rec} est l'efficacité de réconciliation, qui compare la taille du message réconcilié à l'information mutuelle I_{AB} (3.39):

$$\eta_{rec} = \frac{H(B) - r/n - I(B;\varepsilon|E)}{I_{AB}} \tag{3.72}$$

La quantité $I(B;\varepsilon|E)$ a été intégrée dans la définition de ce paramètre puisqu'elle est directement reliée à l'algorithme de réconciliation utilisé. L'information $I(B;E)$ qu'a l'espion sur les données de Bob a quant à elle été estimée avec (3.68).

Le premier point que l'on peut souligner concernant ces résultats est la performance obtenue en l'absence de pertes dans le canal de transmission ($G = 1$): nous avons en effet plus de 2 bits sûrs par symbole, avec un débit relativement proche de la limite théorique; ceci concrétise l'avantage des variables continues pour la transmission de l'information. Nous avons également obtenu un transfert de clé secrète pour un gain $G = 0.49$, inférieur à 0.5, avec un débit non négligeable de 75 kbits par seconde. La réconciliation inverse permet donc effectivement d'utiliser les variables continues, pour la distribution de clé secrète, lorsque les pertes sont supérieures au gain.

Alors on pourra objecter que la sécurité de ce protocole n'est assurée que contre une attaque par cloneuse intriquante, qui est certes optimale par rapport à I_{BE}, mais qui ne l'est plus nécessairement lorsque l'on prend en compte la connaissance que l'espion peut avoir de ε. Il s'agit ici essentiellement d'une limitation de l'algorithme de réconciliation: ce problème disparaît avec l'utilisation d'un algorithme mono-directionnel de réconciliation, les turbo-codes figurant parmi les plus prometteurs de ces algorithmes. L'équipe de l'ULB a ainsi tenté une implémentation de ce type[128, 165]: les deux première tranches sont toujours simplement révélées, tandis que la troisième tranche est réconciliée à l'aide d'un turbo-code. Cascade est toujours utilisé pour les deux dernières tranches, les turbo-codes étant actuellement peu efficaces lorsque le taux d'erreur est trop faible (ces deux dernières tranches ont un taux d'erreur très inférieur à 1%, à comparer au taux de 7% de la troisième tranche). Cette stratégie s'est révélée payante à faible gain, puisqu'un taux de 80 kbits/s a pu être obtenu pour $G = 0,49$.

La qualité de la réconciliation est donc une composante essentielle du protocole, et c'est la raison pour laquelle nous continuons de travailler en étroite collaboration avec l'équipe de l'ULB. Nous sommes ici encore assez loin des limites théoriques pour les faibles valeurs de gain, et il nous fallait donc travailler à l'amélioration de ces performances pour atteindre des débits plus importants et des valeurs encore plus faibles du gain (un gain de $0,49$ correspond à 15 km pour les fibres optiques habituellement utilisées en télécommunication). Il nous fallait également délimiter exactement le niveau de sécurité garanti par ce protocole, et nous allons maintenant revenir sur ce point.

3.4 Analyse de la sécurité du protocole

Ce protocole, qui utilise les techniques classiques d'amplification de confidentialité décrites au chapitre 1, n'est garanti que contre des attaques individuelles. Tel que nous l'avons présenté, ce protocole n'est donc pas inconditionnellement sûr. De plus, nous avons fait l'hypothèse que les attaques gaussiennes étaient optimales pour Eve, et nous allons commencer par la discussion de ce dernier point.

3.4.1 Optimalité des attaques gaussiennes

La réponse à cette question a en fait été donnée postérieurement à la référence [3.1], par Frédéric Grosshans et Nicolas Cerf[84]. Le point central pour la sécurité de notre protocole à réconciliation inverse est l'inégalité de Heisenberg (3.43):

$$V_{Q_B|Q_E} V_{P_B|\overline{P}_A} \geq N_0^2 \tag{3.73}$$

En utilisant la relation (1.30) qui lie, pour des variables aléatoires gaussiennes, la variance conditionnelle à l'entropie conditionnelle, on obtient facilement:

$$H_d(Q_B|Q_E) + H_d(P_B|\overline{P}_A) \geq 2H_0 \tag{3.74}$$

où $H_0 = \log_2(2\pi e N_0)/2$ est l'entropie différentielle associée aux quadratures d'un état vide. Cette inégalité signifie que la connaissance conjointe qu'ont Alice et Eve de l'état de Bob ne peut permettre de déterminer cet état avec une précision supérieure à celle autorisée par le principe d'incertitude. Cette inégalité a été établie ici pour des variables gaussiennes, mais elle dépasse en fait largement ce cadre: il s'agit d'une forme entropique du principe d'incertitude. Quelle que soit la stratégie d'attaque (individuelle) utilisée par Eve, quelle que soit la mesure E qu'elle choisit d'effectuer, l'état reçu au final par Bob devra toujours vérifier [88]:

$$H_d(Q_B|E) + H_d(P_B|\overline{P}_A) \geq 2H_0 \tag{3.75}$$

Cette expression très générale peut maintenant être utilisée pour minorer la taille de la clé secrète:

$$\Delta I = I_{BA} - I_{BE} = H_d(Q_B|E) - H_d(Q_B|\overline{Q}_A) \geq 2H_0 - H_d(Q_B|\overline{Q}_A) - H_d(P_B|\overline{P}_A) \tag{3.76}$$

Il suffit donc à Alice et Bob, en comparant une partie de leurs données pour caractériser le canal de transmission, d'estimer $H_d(Q_B|\overline{Q}_A)$ et $H_d(P_B|\overline{P}_A)$ pour borner la connaissance de l'espion et obtenir une valeur minimale pour la taille de la clé secrète. Mais on peut aller plus loin, puisque l'on sait que, à variance fixée, l'entropie est maximale pour une distribution gaussienne:

$$H_d(Q_B|\overline{Q}_A) \leq H_{gauss}(Q_B|\overline{Q}_A) \tag{3.77}$$

avec une inégalité analogue pour la quadrature P. La borne inférieure de ΔI est donc minimale lorsqu'une stratégie d'attaque gaussienne est envisagée. On peut donc considérer que cette attaque est optimale dans la mesure où toute autre attaque permettrait à Alice et Bob d'extraire une clé de taille supérieure. On peut montrer par une démarche analogue que les attaques individuelles sont optimales par rapport à des attaques sur un nombre limité d'impulsions. On se reportera à l'article de F. Grosshans et N. Cerf[84] pour un exposé complet de ces arguments, ou pour comprendre comment (3.76) et (3.77) permettent effectivement de retrouver la minoration (3.47) précédemment établie pour ΔI.

Ce travail montre donc la sécurité de notre protocole contre des attaques individuelles. Peut-on pousser plus loin cette analyse de sécurité ? Nous avons vu que la démonstration de sécurité inconditionnelle de Shor et Preskill[152] pour BB84 reposait sur l'existence d'un protocole utilisant l'intrication de paires EPR, lui-même inconditionnellement sûr. En fait, l'intrication est un pré-requis indispensable pour la sûreté d'un protocole de distribution de clé[1, 51]. Nous allons maintenant montrer comment notre protocole dérive effectivement d'un protocole utilisant une source EPR, amenant ainsi à la notion d'intrication virtuelle.

3.4.2 Intrication virtuelle sous-jacente au protocole

Nous allons dans cette section reprendre succinctement les arguments de l'article [3.2] annexé à ce chapitre. Le principal résultat développé dans cet article est que le dispositif de la figure 3.13 est rigoureusement équivalent à notre protocole à états cohérents.

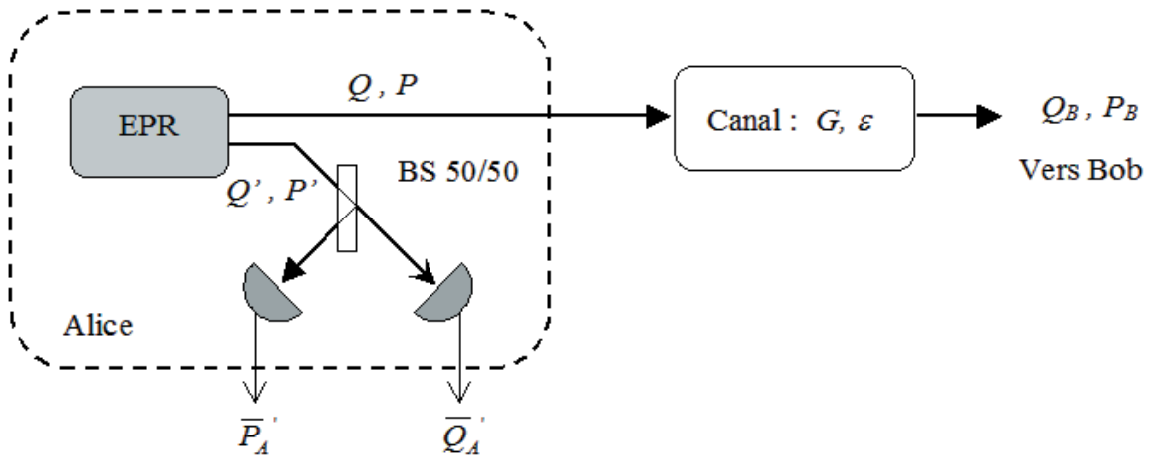

Figure 3.13: *Exemple de dispositif de cryptographie utilisant une source EPR.*

La source EPR utilisée dans ce dispositif émet un état gaussien centré, complètement caractérisé par:

$$\langle Q^2 \rangle = \langle P^2 \rangle = \langle Q'^2 \rangle = \langle P'^2 \rangle = V N_0 \tag{3.78}$$

et:

$$\langle QQ' \rangle = -\langle PP' \rangle = \sqrt{V^2 - 1}\ N_0 \tag{3.79}$$

On peut montrer que cette source présente, à variance fixée (équation 3.78), une corrélation maximale des impulsions jumelles.

Le protocole sous-tendu par ce dispositif se déroule de la manière suivante: Alice conserve l'une des impulsions de la paire EPR émise, et effectue une mesure des quadratures $\overline{Q}'_A$ et $\overline{P}'_A$ après passage par une séparatrice 50/50. Cette mesure va bien sûr conditionner l'autre membre de la paire EPR, et nous avons plus précisément montré qu'elle projetait l'impulsion envoyée à Bob sur un état cohérent bien défini: il s'agit de l'état cohérent centré sur les estimateurs[3] $\overline{Q}_A = \alpha \overline{Q}'_A$ et $\overline{P}_A = \alpha \overline{P}'_A$ qu'Alice a de Q et P. Ces estimateurs $\overline{Q}_A$ et $\overline{P}_A$ sont par ailleurs tous deux des variables aléatoires gaussiennes de variance $(V-1)N_0$, et ont donc exactement la même statistique que les variables $\overline{Q}_A$ et $\overline{P}_A$ utilisées dans notre protocole pour définir la position des impulsions dans l'espace des quadratures.

Tout se passe donc comme si Alice avait envoyé un état cohérent centré sur $(\overline{Q}_A, \overline{P}_A)$: ce dispositif est complètement équivalent à celui que nous avons utilisé, à l'instar de l'équivalence entre le protocole $BB84$ et les protocoles à paires EPR. Rien ne permet de discerner le moment où Alice mesure l'élément de la paire qu'elle conserve, et donc de savoir si finalement elle a envoyé un système dans un état particulier, ou si elle a utilisé une paire EPR. Au final, c'est donc plutôt la capacité de la ligne à transmettre l'intrication qui est pertinente.

Nous avons cherché à analyser cette capacité à transmettre l'intrication en quantifiant le niveau d'intrication entre l'impulsion (Q_B, P_B) reçue par Bob et l'impulsion (Q', P') conservée

[3] avec $\alpha = \langle \overline{Q}'_A Q \rangle / \langle \overline{Q}'^2_A \rangle = \sqrt{2(V-1)/(V+1)}$

par Alice. En utilisant[3.2] un critère de non-séparabilité introduit par Duan[59] et Simon[156], nous avons montré que ces deux impulsions étaient effectivement intriquées pour un excès de bruit $\epsilon < 2$, et ce quelles que soient les pertes du canal de transmission. Ce critère est à comparer avec le critère (3.49) de sécurité de notre protocole: $\epsilon < 1/2$. Notre critère de sécurité est plus restrictif, ce qui est bien cohérent avec l'idée que la sécurité des protocoles est reliée à la capacité du canal à transmettre l'intrication. Ceci dit, il y a également intrication pour $1/2 < \epsilon < 2$, et il pourrait donc très bien exister des protocoles fonctionnant dans cette plage. Ainsi par exemple, les protocoles à états squeezés, avec lesquels nous avons introduit ce chapitre, sont plus robustes par rapport au bruit ajouté, et peuvent fonctionner pour $\epsilon < 1$.

Bien sûr, l'intrication virtuelle exposée ici n'est pas en soi une preuve de sécurité inconditionnelle, mais c'est un pas dans cette direction, comme nous allons maintenant le voir.

3.4.3 Sécurité inconditionnelle

Peut-on maintenant appliquer un raisonnement analogue à celui de Shor et Preskill[152] pour BB84 ? L'équipe de l'ULB que dirige Nicolas Cerf a tenté de répondre par l'affirmative à cette question[164, 165]. Pour cela, ils ont transformé le protocole de réconciliation par tranche en protocole de correction d'erreurs quantiques pour les variables continues.

Nous avons vu que le protocole de réconciliation que nous avons utilisé fonctionnait sur des données binaires, obtenues après discrétisation, et non sur les quadratures mesurées. Ces données binaires sont en fait équivalentes à la quadrature mesurée, à condition d'introduire une variable continue permettant de situer cette dernière à l'intérieur de l'intervalle dans lequel elle se trouve. L'idée développée par le groupe de l'ULB est de généraliser cette équivalence au niveau quantique: l'état quantique $|\psi\rangle$ de l'impulsion lumineuse est équivalent à la donnée d'un certain nombre de qubits $|s_i\rangle$ ainsi que d'une variable continue $|\overline{s}\rangle$. Concrètement, cette équivalence signifie qu'il existe une transformation unitaire (un ordinateur quantique) permettant de passer de l'une à l'autre de ces représentations. Dans le cas d'une paire EPR intriquée en quadrature, il se trouve que cette transformation unitaire va générer des qubits intriqués, et à partir de ce point il est possible de suivre une démarche analogue à celle de Shor et Preskill:

Alice et Bob partagent des paires de qubits intriqués, cette intrication n'étant que partielle à cause des erreurs introduites par le canal. Il est donc nécessaire de disposer d'un protocole de correction d'erreurs quantiques adapté à cette expérience, et une étape importante du travail de Nicolas Cerf et ses collaborateurs[164, 165] a justement été de développer un protocole de corrections d'erreurs quantiques basé sur la réconciliation par tranche. Ce protocole peut bien sûr échouer si les erreurs introduites par le canal sont trop nombreuses, mais dans le cas contraire Alice et Bob partagent après cette correction des qubits parfaitement intriqués, qu'il leur suffit de mesurer pour obtenir une clé de façon inconditionnellement sûre. La dernière étape de ce travail a été de montrer, de manière analogue à la démonstration de Shor-Preskill, l'équivalence de ce protocole avec un protocole utilisant un traitement classique de l'information sur les quadratures mesurées.

Alors, ce travail permet-il de conclure à la sûreté inconditionnelle de notre protocole? Une difficulté subsiste[166], qui consiste a estimer les taux d'erreurs quantiques sur les qubits virtuels, et notamment le taux d'erreurs de phase. Si ce taux est simple à estimer pour BB84, il faut ici une connaissance particulièrement fine des propriétés de transmission du canal pour l'obtenir: nous sommes incapables à l'heure actuelle de l'évaluer dans nos expériences. L'analyse tomographique de ces propriétés reste à étudier, au plan théorique comme au plan expérimental.

Nous ne pouvons donc conclure actuellement sur la sécurité inconditionnelle de notre protocole. Ces travaux sur les variables continues sont encore très récents par rapport aux travaux

sur les protocoles à variables discrètes, et nous n'avons pas le même recul. Nous disposons cependant d'un certain nombre d'éléments qui nous appellent à l'optimisme. Ainsi, les nouveaux critères de sécurité évoqués à la fin de la section 1.3.4, introduits par Igor Devetak et Andreas Winter[54] ainsi que par Renato Renner et ses collaborateurs[144, 145], suscitent déjà de nombreux travaux[85, 125, 126, 46] afin d'en étudier les implications sur notre protocole.

3.5 Conclusion et perspectives

Nous avons donc réalisé un premier démonstrateur pour valider la distribution de clés secrètes avec des variables continues. La méthode a fait l'objet d'un dépôt de brevet[37]. Confortés par ces résultats nous avons entrepris de développer, en collaboration avec la société Thalès, un système compatible avec les normes des télécommunications optiques, fonctionnement notamment à 1550 nm, et totalement fibré. Ce travail fait maintenant l'objet de la thèse de Jérôme Lodewyck, dans le cadre du projet européen SECOQC (Secure Communication based on Quantum Cryptography). De nombreux problèmes expérimentaux restent à résoudre, et notamment celui de la transmission simultanée par fibre optique du signal et de l'oscillateur local: les fibres optiques peuvent en effet introduire des fluctuations de phase et de polarisation qui vont nuire aux performances du protocole. L'une des voies pouvant permettre de pallier à cette difficulté consiste à multiplexer le signal et l'oscillateur local sur une même fibre (figure 3.14) : les deux impulsions subissent alors les mêmes perturbations, qui sont donc naturellement compensées. Ce dispositif a fait l'objet d'un dépôt de brevet[108], déposé conjointement avec la société Thalès. Sa réalisation est actuellement bien avancée, avec de très bonnes performances obtenues sur le bruit ajouté[109].

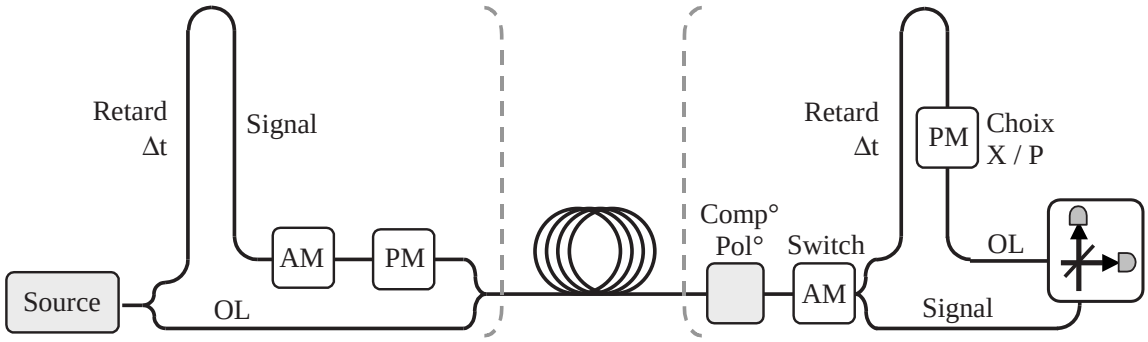

Figure 3.14: *Exemple de dispositif de cryptographie avec transmission fibrée.*

Ce prototype fibré, dans son état actuel, permet potentiellement d'atteindre un taux de secret de 1 kbit/s pour une distance de 25 km et un taux de répétion de 1 MHz; cette performance est suffisamment compétitive pour que nous ayons été sélectionnés par SECOQC pour une implémentation à taille réelle de notre dispositif. Ceci dit, notre prototype pourrait permettre d'atteindre 55 kbit/s sur 25 km s'il n'était pas limité par le temps de calcul des algorithmes de réconciliation.

De nombreux efforts restent donc à fournir en ce qui concerne le traitement de l'information: nous avons déjà vu que l'efficacité des algorithmes de réconciliation était un point névralgique de notre protocole. Ils doivent non seulement être plus efficaces, mais également plus rapides pour ne pas limiter le débit d'information. L'équipe de l'ULB a pour objectif d'étudier différentes possibilités d'amélioration de ses algorithmes. Nous avons également démarré une collaboration

avec Matthieu Bloch et ses collaborateurs, qui ont obtenu de très bons résultats avec les codes LDPC[32].

D'autres possibilités pourront également être explorées, telles que les algorithmes à post-sélection[154, 110]. Sans entrer dans les détails ces algorithmes, d'une mise en œuvre beaucoup plus simple pour le traitement de l'information, pourraient être plus efficaces pour les faibles valeurs du gain de canal, mais leur sécurité, et notamment leur robustesse par rapport au bruit ajouté, n'est pas encore validée.

Enfin, une autre voie à explorer est la possibilité de faire effectivement de la purification d'intrication avec des variables continues. Plus généralement, le fait de travailler en régime impulsionnel ouvre la possibilité d'étudier des états "exotiques" de la lumière: ce travail fait l'objet du quatrième chapitre de ce manuscrit.

3.6 Articles annexés au chapitre

[3.1] 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).

[3.2] 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).

Chapitre 4

Génération et tomographie d'états non-gaussiens en régime impulsionnel

Sommaire

La principale limitation de notre protocole de cryptographie à variables continues, surtout dans le cas de lignes à fortes pertes, c'est-à-dire dans le cas d'une transmission longue distance, réside dans l'efficacité de nos protocoles de réconciliation. Nous pouvons certainement compter à l'avenir sur des améliorations de ces protocoles, et nos partenaires de l'université libre de Bruxelle (ULB) y travaillent[128, 165]. Il existe cependant une autre voie à explorer, plus proche des thématiques de notre groupe, qui concerne la possibilité de faire effectivement de la purification d'intrication avec des variables continues: peut-on, en partant d'un certain nombre de paires EPR faiblement intriquées, obtenir un nombre plus petit de paires plus fortement intriquées ?

Il se trouve qu'un tel processus est impossible[62, 69] en partant d'un état gaussien (dont la fonction de Wigner est gaussienne) et en utilisant des opération gaussiennes (qui transforment un

état gaussien en un autre état gaussien). Et comme les paires EPR intriquées en quadratures que l'on génère par les méthodes classiques (voir section 4.4) sont des états gaussiens, il va falloir sortir du domaine gaussien en utilisant une opération non-gaussienne. Plusieurs solutions théoriques ont déjà été proposées pour purifier des paires EPR[58, 38]. Notre objectif dans l'immédiat n'est absolument pas d'essayer de mettre en œuvre de telles solutions, mais de s'intéresser dans un premier temps à la maîtrise de différentes opérations de base pouvant être impliquées dans ces protocoles, et notamment des opérations conditionnées qui sont à la base du protocole proposé par D. Browne et ses collaborateurs[38].

Nous verrons comment ces opérations conditionnées permettent effectivement de sortir du domaine gaussien, et quelles peuvent en être les applications en dehors de la purification. En effet nous abordons ici un domaine de l'optique quantique dont l'intérêt scientifique dépasse amplement le cadre de la communication quantique, avec notamment la possibilité de produire des états particulièrement exotiques de la lumière, ou celle de tester les inégalités de Bell par une voie nouvelle, ne permettant plus aucune échappatoire.

4.1 Production de vide comprimé en régime impulsionnel

La première étape de la série d'expériences présentée dans ce chapitre consiste en la production d'impulsion de vide comprimé. La production de vide comprimé[157, 158, 99, 96, 6, 53] n'est pas en soi originale; la nouveauté ici est d'avoir réalisé cette expérience en régime impulsionnel, avec une analyse résolue en temps, ce qui pose différentes difficultés tant au niveau de la génération des impulsions qu'au niveau de leur détection. Cette section, consacrée à cette problèmatique, sera l'occasion de présenter le dispositif expérimental utilisé par la suite. On pourra également se reporter à la référence [4.1] pour un exposé plus détaillé.

4.1.1 Introduction

Parmi les différentes possibilités[167, 117, 87, 11] permettant la production d'états comprimés, l'amplification paramétrique d'impulsions ultrabrèves lors d'un simple passage dans un cristal non-linéaire apparaît comme étant une solution simple et efficace. Nous avons ainsi utilisé une configuration d'amplification paramétrique dégénérée, avec une impulsion pompe à 2ω qui n'interagit qu'avec une seule impulsion à ω. Considérons la propagation d'une impulsion signal dans le cristal, repérée par sa position z: si cette impulsion est convenablement superposée à la pompe, et si l'on note $\alpha(z)$ son amplitude, on pourra écrire classiquement, dans le cadre d'une approximation d'enveloppe lentement variable[150]:

$$\frac{d\alpha}{dz} = \frac{\alpha^*}{L_{NL}} \tag{4.1}$$

où L_{NL} est la longueur caractéristique de l'interaction:

$$L_{NL} = \sqrt{\varepsilon_0 c^3 n_\omega^2 n_{2\omega} \omega^{-2}} \times \frac{1}{d_{eff}\sqrt{2I}} \tag{4.2}$$

où l'on a utilisé les notations usuelles, d_{eff} étant le coefficient de non-linéarité du cristal et I l'intensité de la pompe. En optique classique, un facteur i est généralement introduit[150] dans l'équation (4.1); il ne s'agit ici que d'une pure convention, correspondant à un déphasage de $\pi/4$ des amplitudes complexes.

Par contre, une autre approximation se cache dans cette expression (4.1): on considère ici que L_{NL} est une constante, et comme cette longueur caractéristique dépend de l'intensité de la

pompe, cela revient à considérer que l'extension spatiale et temporelle de l'impulsion de pompe est grande devant celle de l'impulsion signal. La forme globale de cette dernière impulsion est donc conservée au cours de l'interaction, et l'on peut considérer que l'on n'a affaire qu'à un unique mode du champ. Cette approximation monomode néglige tous les effets liés à la diffraction induite par le gain[101], et nous verrons que si elle permet de comprendre nos expériences, elle reste d'une validité limitée, sur laquelle nous reviendrons. Cette mise au point étant faite, la quantification de (4.1) est aisée en introduisant les opérateurs de création et d'annihilation dans le mode considéré:

$$\frac{da}{dz} = \frac{a^\dagger}{L_{NL}} \tag{4.3}$$

On peut alors simplement relier les opérateurs en entrée et en sortie du cristal:

$$a_{out} = \cosh r \; a_{in} + \sinh r \; a_{in}^\dagger \tag{4.4}$$

où l'on a introduit le paramètre de compression $r = L/L_{NL}$. On peut également écrire:

$$a_{in} = \cosh r \; a_{out} - \sinh r \; a_{out}^\dagger \tag{4.5}$$

Dans l'esprit de la représentation de Heisenberg, l'état initial n'est pas modifié par l'interaction, et doit simplement être exprimé dans la base de Fock $|n\rangle_{out}$. On obtient ainsi pour un état initial vide[104]:

$$a_{in}|0\rangle_{in} = 0 \quad \Leftrightarrow \quad |0\rangle_{in} = \frac{1}{\sqrt{\cosh r}} \sum_{m=0}^{\infty} [C_{2m}^m (\frac{1}{2} \tanh r)^{2m}]^{1/2} |2m\rangle_{out} \tag{4.6}$$

Cette expression nous sera utile par la suite pour mieux comprendre le principe de la préparation conditionnelle. Mais l'utilisation des quadratures simplifie en fait considérablement le problème et permet de bien saisir ce qu'est l'amplification paramétrique; on obtient ainsi en introduisant les quadratures dans (4.4):

$$Q_{out} = e^{+r} Q_{in} \; , \quad P_{out} = e^{-r} P_{in} \tag{4.7}$$

L'amplification paramétrique revient donc simplement à appliquer une dilatation pour la quadrature Q, et une contraction pour la quadrature P. Elle peut ainsi nous permettre, avec un état initial vide, de produire un vide comprimé sur la quadrature P (étant données les conventions introduites). Elle permet également d'amplifier une impulsion cohérente dont le centre est sur l'axe Q, avec un gain e^{+r} en amplitude, et donc e^{+2r} en énergie. Une impulsion dont le centre est sur l'axe P sera quant à elle dé-amplifiée d'un facteur inverse: l'amplification dépend donc ici de la phase de l'impulsion incidente.

4.1.2 Le dispositif expérimental

Pour obtenir une amplification conséquente, c'est-à-dire une valeur élevée du paramètre de compression r, on peut jouer sur la longueur du cristal et l'importance de l'effet non-linéaire. Ces deux leviers ne sont toutefois pas indépendants: l'effet non-linéaire dépend entre autres de l'intensité de la pompe, qui est d'autant plus importante que les faisceaux sont focalisés et que les impulsions sont courtes; et ces derniers paramètres sont limités par la taille du cristal, si l'on veut éviter les problèmes posés par la diffraction, ainsi que par le désaccord de vitesse de groupe. Le désaccord de vitesse de groupe (GVM: Group Velocity Mismatch) est en effet problématique

en régime impulsionnel: les impulsions à ω et à 2ω ne se déplacent pas à la même vitesse dans le cristal, et ne doivent donc pas être trop courtes pour se recouvrir jusqu'à la sortie du cristal. Par ailleurs la longueur du cristal doit être inférieure à la longueur de Rayleigh, ce qui limite la taille du waist dans le cristal. En faisant le bilan de toutes ces contraintes, il apparaît que la qualité de l'amplification dépend essentiellement de l'énergie des impulsions.

Il nous fallait donc un laser délivrant des impulsions de grande énergie, avec une haute cadence et une bonne qualité de mode. Les oscillateurs femtoseconde standards avaient une cadence de l'ordre de 100 MHz, trop élevée pour notre détection homodyne, et les impulsions émises avaient une énergie un peu trop faible (< 10 nJ). Les amplificateurs régénératifs commerciaux avaient quant à eux une cadence trop lente (≈ 10 kHz). Après examen des différentes solutions, la source finalement retenue a été le laser commercial Tiger-CD de la société Time-Bandwidth.

Ce laser est un oscillateur femtoseconde titane-saphir muni d'un 'cavity dumper': il s'agit d'une cellule de Bragg permettant de prélever périodiquement l'énergie accumulée dans la cavité. Ce dispositif permet à la fois de diminuer la fréquence d'émission et d'augmenter l'énergie des impulsions. Nous obtenons ainsi, à une fréquence de 780 kHz, des impulsions de 150 fs pouvant atteindre 75 nJ, soit une puissance crête de 500 kW. La longueur d'onde centrale de l'émission est 846 nm.

Vient ensuite le choix du cristal non-linéaire. Nous avons opté pour le niobate de potassium (KNbO3), dont le coefficient non-linéaire important[57] ($d_{eff} \approx 12$ pm/V à 850 nm, 9 fois supérieur à celui du BBO) est un avantage précieux. Le désaccord de vitesse de groupe est certes élevé (1.2 ps/mm) et impose une longueur de cristal de l'ordre de 100 μm, mais cette petite taille est compensée par la possibilité de focaliser plus fortement les faisceaux. Enfin et surtout, ce cristal permet à 850 nm d'obtenir un accord de phase non-critique de type I par simple contrôle de la température.

Les 3 axes cristallographiques du $KNbO_3$ sont notés a, b et c, le cristal étant taillé normalement à la direction a. Le faisceau pompe et le faisceau sonde sont alignés sur cet axe, la sonde étant polarisée suivant b, la pompe suivant c. Pour $\lambda = 846$ nm, l'accord de phase de type I, $n_{b,\omega} = n_{c,2\omega} = 2,281$, est obtenu pour une température de l'ordre de $-12°$C. Cette configuration est donc idéale pour travailler en mode dégénéré. Pour atteindre cette température de $-12°$C nous avons conçu une cellule de refroidissement, fonctionnant sous vide pour éliminer les problèmes de condensation (figure 4.1): le refroidissement est obtenu par un élément Peltier, lui-même refroidi par une circulation d'eau.

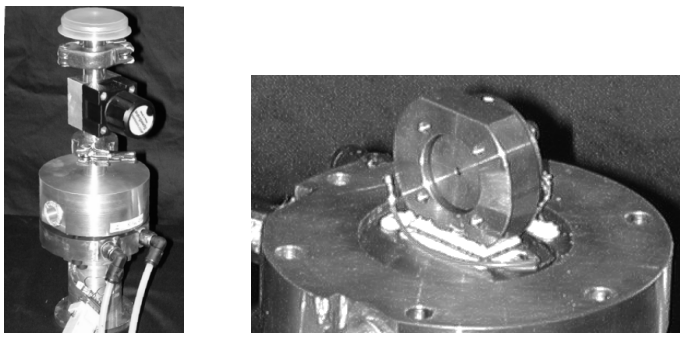

Figure 4.1: *Enceinte à vide réfrigérante pour le cristal de $KNbO_3$.*

Le schéma du dispositif complet est présenté sur la figure 4.2. Le faisceau pompe à 2ω est généré par doublage de fréquence (SHG) dans un cristal de $KNbO_3$, dans une configuration iden-

tique à celle de l'amplification paramétrique. Nous avons pu typiquement obtenir un rendement de doublage de $20-25\%$, correspondant à des impulsions d'une dizaine de nanojoules à 423 nm. Ce rendement n'est pas des plus élevés, et nous pensons que des effets thermiques locaux sont à l'origine de cette limitation; mais il faut garder à l'esprit qu'il est obtenu par simple passage dans un cristal de 100 μm d'épaisseur.

La pompe est ensuite soigneusement filtrée pour éliminer tout résidu à ω, avant d'être injectée dans l'amplificateur paramétrique dégénéré (DOPA). Une sonde peut également être injectée dans l'amplificateur pour en caractériser le fonctionnement ainsi que pour l'alignement de l'ensemble du dispositif.

Le signal issu de l'amplificateur est ensuite filtré, puis analysé par la détection homodyne impulsionnelle à amplificateur de charge décrite au chapitre 3 (10% du faisceau initial sont prélevés pour constituer l'oscillateur local). Nous avons estimé l'efficacité homodyne dans ce montage à $\eta = 75\%$, soit une valeur un peu plus faible qu'au chapitre 3 de par un moins bon recouvrement de l'oscillateur local et du signal.

Enfin, deux transducteurs piézo-électriques (PZT) sont utilisés pour ajuster la phase de l'oscillateur local ainsi que celle de la sonde. Une impulsion de 150 fs de durée a une largeur de 45 μm: un ajustement extrêmement précis est donc nécessaire pour superposer toutes ces impulsions.

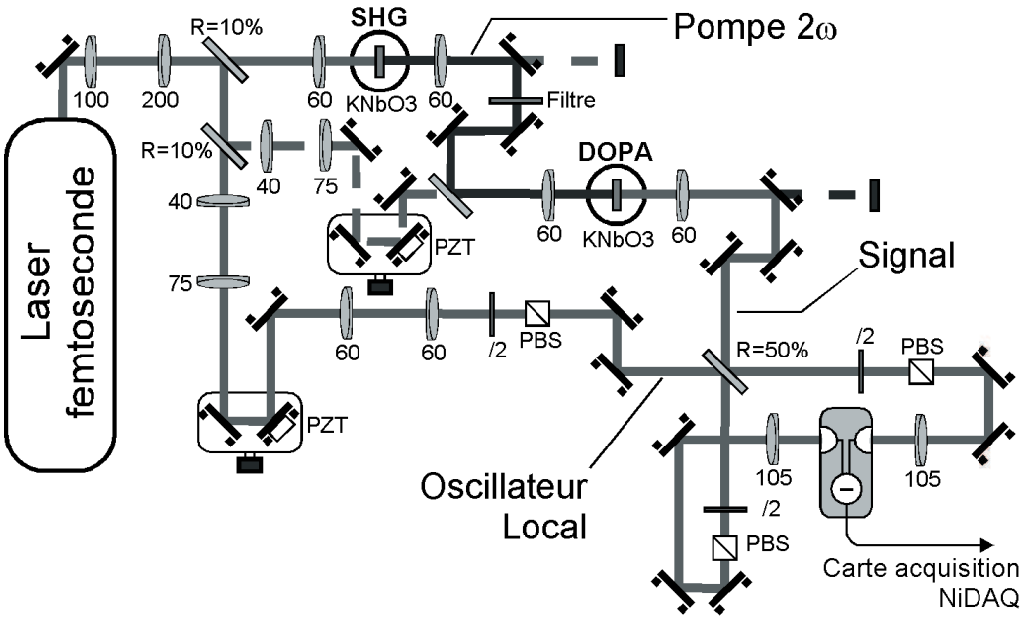

Figure 4.2: *Dispositif complet pour la génération d'états comprimés. Les focales sont indiquées en millimètres.*

4.1.3 Analyse des résultats

Nous avons commencé par mesurer le gain paramétrique en énergie sur un faisceau sonde. Sont présentés sur la figure 4.3 le gain maximal (losanges pleins) ainsi que le gain minimal (disques pleins) obtenus en fonction de la puissance de pompe en faisant varier la phase de la sonde [1]. Les

[1] rappelons que la quadrature Q est amplifiée, tandis que la quadrature P est dé-amplifiée.

cercles correspondent à l'inverse du gain de dé-amplification et sont, contrairement à la théorie, légèrement en deçà du gain d'amplification. Nous sommes dés à présent confrontés aux limites du modèle monomode, la diffraction induite par le gain jouant un rôle qui n'est pas forcément complètement négligeable. Il est cependant possible avec ce modèle d'obtenir un ajustement satisfaisant (courbes en trait plein, l'ajustement a été effectué pour des puissances de pompe inférieures à $0,5$ mW).

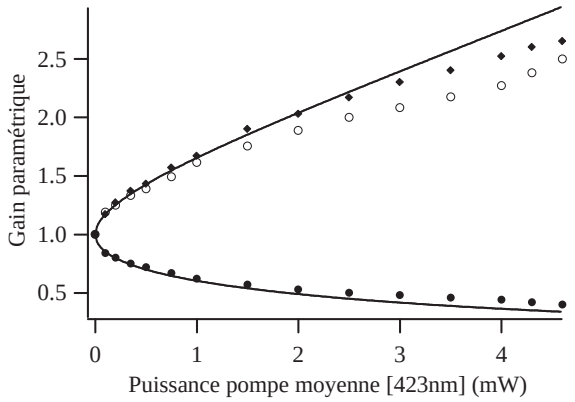

Figure 4.3: *Gain paramétrique en fonction de la puissance de pompe moyenne à 423 nm. Les disques et losanges pleins correspondent à la dé-amplification et à l'amplification, les cercles à l'inverse du gain de dé-amplification, tandis que les courbes en trait plein sont un ajustement par le modèle monomode.*

Le faisceau sonde est ensuite coupé afin de permettre la génération de vide comprimé et son analyse par la détection homodyne. La figure 4.4 présente l'évolution de la variance du signal homodyne mesuré pour un balayage linéaire de la phase de l'oscillateur local. Chaque variance est calculée pour un bloc de 2500 mesures. Le niveau du bruit quantique standard (SNL : Shot Noise Level) est indiqué, ainsi que la variance du bruit électronique. Comme on peut le voir sur cette figure, nous pouvons clairement obtenir un vide comprimé, dont la variance est inférieure au bruit quantique standard.

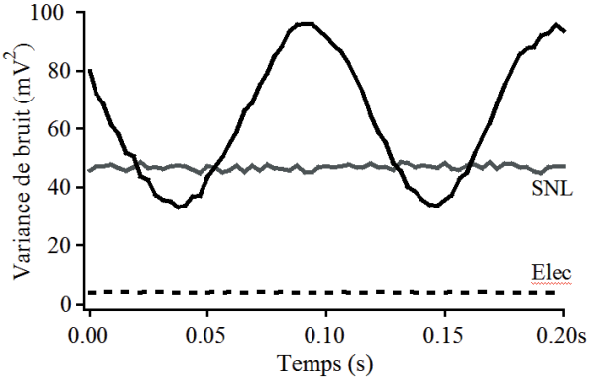

Figure 4.4: *Mesures homodynes du vide comprimé pour un balayage linéaire de la phase de l'oscillateur local.*

Pour notre meilleur résultat, qui correspond aux histogrammes de la figure 4.5, la variance minimale du signal est à $-1,87 \pm 0,06$ dB sous le bruit quantique standard (facteur $0,65$), tandis que la quadrature amplifiée est à $3,32 \pm 0,04$ dB au dessus de ce niveau (facteur $2,15$). Ces résultats sont en bon accord avec ce que l'on pouvait attendre du gain paramétrique en énergie ($0,53 \pm 0,01$ pour la dé-amplification et $2,51 \pm 0,05$ pour l'amplification): en effet, le gain en variance est identique au gain en énergie (voir 4.7), et en prenant en compte l'efficacité homodyne ainsi que le bruit électronique (voir 3.63), on déduit du gain paramétrique une variance de $-1,92 \pm 0,06$ dB pour la quadrature comprimée, et de $3,32 \pm 0,06$ dB pour la quadrature amplifiée. Inversement, en corrigeant nos mesures de variances du bruit électronique et de l'efficacité homodyne, nous pouvons conclure à une compression de $-2,68$ dB (facteur $0,54$) et une amplification de $4,0$ dB (facteur $2,51$).

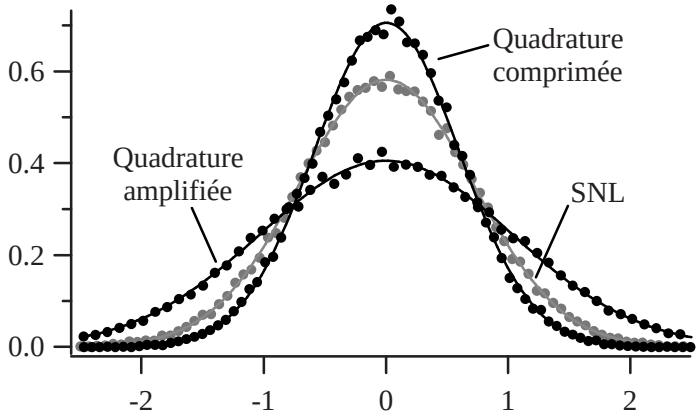

Figure 4.5: *Distributions de probabilité des quadratures mesurées, avec la convention* $N_0 = 1/2$.

Rappelons ici que l'ensemble de ces résultats sont l'aboutissement d'une étude statistique sur les mesures de quadratures effectuées individuellement sur chaque impulsion. Aucun analyseur de spectre n'est ici utilisé pour observer la réduction des fluctuations sur une plage étroite de fréquence, et ceci constitue la principale originalité de ce travail et ouvre la porte aux mesures conditionnées que nous aborderons au paragraphe 4.3. Avant cela, analysons plus en détails l'état produit.

4.1.4 Tomographie du vide comprimé

Un état quantique est complètement caractérisé par sa matrice densité ρ ou, dans la base des quadratures, par les éléments de matrice $\rho(q, q')$. Nous avions succinctement introduit la fonction de Wigner au chapitre 3, comme étant en correspondance bi-univoque avec la matrice densité. Cette fonction est en fait définie par:

$$W(q,p) = \frac{1}{4\pi N_0} \int \rho(q - \frac{x}{2}, q + \frac{x}{2}) \exp(\frac{ixp}{2N_0}) dx \tag{4.8}$$

Il apparaît de manière évidente qu'en intégrant cette fonction sur p, on obtient la distribution de probabilité de la quadrature Q. Dit autrement, la distribution de probabilité de la quadrature Q est donnée par la projection de la fonction de Wigner sur l'axe q. Comme nous l'avions déjà indiqué au chapitre 3, cette propriété est en fait très générale[104]: La distribution $P_\varphi(q)$ d'une quadrature $X(\varphi)$ est donnée par la projection de la fonction de Wigner sur une droite faisant

un angle φ avec l'axe q. Cette propriété est formellement plus simple à écrire dans l'espace de Fourier[104]:

$$\tilde{P}_\varphi(\xi) = \int P_\varphi(q) e^{-iq\xi} dq = \tilde{W}(\xi\cos\varphi, \xi\sin\varphi) \tag{4.9}$$

où $\tilde{W}(\mu,\nu)$ est la transformée de Fourier de la fonction de Wigner.

Ainsi, la connaissance des distributions de probabilité des différentes quadratures permet, par (4.9), de reconstruire la fonction de Wigner. Ce procédé est analogue aux méthodes de tomographie utilisées en imagerie médicale, où l'on reconstruit une image à partir de ses projections sur différents axes, et l'on parle pour cette raison de tomographie quantique. Pour le mettre en œuvre[104] on écrira ainsi[2]:

$$W(q,p) = \frac{1}{4\pi^2} \int \tilde{P}_\varphi(\xi) e^{i\xi(q\cos\varphi + p\sin\varphi)} \xi d\varphi d\xi \tag{4.10}$$

Pour régulariser ce qui va suivre, on tronquera cette intégrale au delà d'une fréquence de coupure k_c (imposant ainsi $|\xi| < k_c$). Cette fréquence de coupure doit être convenablement choisie pour conserver l'information pertinente dans $\tilde{P}_\varphi$ tout en éliminant le bruit haute fréquence. En écrivant $\tilde{P}_\varphi(\xi)$ en fonction de $P_\varphi(x)$, et en utilisant la symétrie de cette dernière pour $\varphi \to \varphi+\pi$, $x \to -x$, on obtient la relation suivante, connue sous le nom de transformation de Radon inverse:

$$W(q,p) = \frac{1}{2\pi^2} \int_0^\pi d\varphi \int P_\varphi(x) K(q\cos\varphi + p\sin\varphi - x) dx \tag{4.11}$$

avec

$$K(X) = \frac{1}{2} \int_{-k_c}^{k_c} |\xi| e^{i\xi X} d\xi \tag{4.12}$$

Nous avons réalisé la tomographie du vide comprimé généré par notre expérience en enregistrant 6 histogrammes pour 6 déphasages régulièrement répartis entre 0 et π ($\varphi = 0$, $\pi/6$, $\pi/3$, $\pi/2$, $2\pi/3$, $5\pi/6$), et en échantillonnant en conséquence l'intégrale (4.11). Le résultat est présenté sur la figure 4.6, où l'on observe sans surprise une gaussienne dont les axes propres sont q et p.

La fonction visualisée sur cette figure ne correspond en fait pas exactement à la fonction de Wigner de l'état généré, car les mesures n'ont pas été corrigées de l'influence de l'efficacité homodyne, ni de celle du bruit électronique. Il est a priori difficile de corriger ces artefacts expérimentaux directement sur la fonction de Wigner, et nous verrons au 4.3.4 comment il est possible de les prendre en compte. Toujours est-il que l'on a ici affaire à un état gaussien. La fonction de Wigner d'un état gaussien centré s'écrit de manière très générale:

$$W(q,p) = \frac{1}{2\pi N_0 \sqrt{\det\gamma}} \exp[-\frac{{}^t\mathbf{X}\gamma^{-1}\mathbf{X}}{2N_0}] \tag{4.13}$$

où ${}^t\mathbf{X} = (q,p)$ et où γ est la matrice de covariance, qui peut être diagonalisée en choisissant convenablement les axes q et p:

$$\gamma = \frac{1}{N_0} \begin{pmatrix} V_{max} = \langle Q^2 \rangle & 0 \\ 0 & V_{min} = \langle P^2 \rangle \end{pmatrix} \tag{4.14}$$

[2] $W(q,p) = \frac{1}{4\pi^2} \int \tilde{W}(X,Y) e^{i(qX+pY)} dX dY$, ou $W(q,p) = \frac{1}{4\pi^2} \int \tilde{W}(\xi\cos\varphi, \xi\sin\varphi) e^{i\xi(q\cos\varphi + p\sin\varphi)} \xi d\varphi d\xi$ en coordonnées polaires. Le reste découle de (4.9).

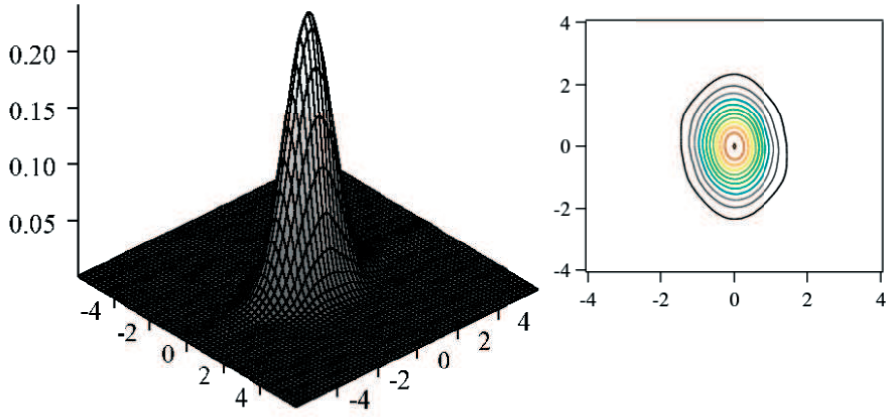

Figure 4.6: *Tomographie quantique d'un état comprimé, obtenue par la transformation de Radon inverse à partir de 6 histogrammes enregistrés pour 6 phases différentes. On a utilisé la convention* $N_0 = 1/2$.

La fonction de Wigner est donc complètement définie par V_{min} et V_{max}, variances issues de mesures homodynes après correction de l'efficacité homodyne et du bruit électronique.

On peut introduire un système physique idéal très simple capable de produire ce type d'états[135, 2]: il suffit d'ajouter un amplificateur non-dégénéré devant l'amplificateur dégénéré idéal qui produit le vide comprimé (figure 4.7). Nous décrirons plus en détails au 4.4 les amplificateurs non-dégénérés, qui ont un gain $H = \cosh^2 r$ indépendant de la phase, et amènent un bruit ajouté.

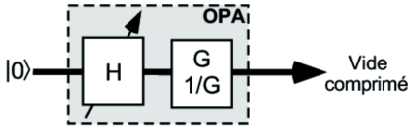

Figure 4.7: *Système idéal permettant la génération d'un état gaussien centré quelconque.*

On a à la sortie de ce système:

$$\begin{aligned} Q_{out} &= \sqrt{G}(\sqrt{H}\ Q_{vac} + \sqrt{H-1}\ Q_{aux}) \\ P_{out} &= \frac{1}{\sqrt{G}}(\sqrt{H}\ P_{vac} - \sqrt{H-1}\ P_{aux}) \end{aligned} \tag{4.15}$$

où les états vac et aux sont deux états vides introduits dans l'amplificateur non dégénéré. Ce système produit un état gaussien caractérisé par les variances:

$$\begin{aligned} V_{max} &= G(2H-1)N_0 \\ V_{min} &= (2H-1)N_0/G \end{aligned} \tag{4.16}$$

et il est toujours possible d'ajuster G et H pour obtenir n'importe quel couple de variances, du moment que ces dernières vérifient l'inégalité de Heisenberg ($V_{max}V_{min} \geq N_0^2$). L'intérêt de ce

modèle est que G et H sont directement reliés aux gains d'amplification et de dé-amplification classiques d'un faisceau sonde:

$$G_{max} = GH \ , \quad G_{min} = H/G \tag{4.17}$$

Il est donc a priori possible de caractériser le vide comprimé émis par l'amplificateur réel d'une manière indirecte, par la mesure de ces gains. La figure (4.8) montre les valeurs obtenues pour G et H par une mesure homodyne directe et par cette méthode, et les résultats obtenus sont en bonne adéquation. Ces valeurs ont été ajustées en reprenant les dépendances de G et H en fonction de la puissance de pompe ($G = \exp(2\alpha\sqrt{P_{pompe}})$, $H = \cosh^2(\beta\sqrt{P_{pompe}})$).

On peut remarquer que $H \neq 1$, ce qui correspond au fait déjà signalé que G_{max} n'est pas exactement l'inverse de G_{min}, ce que nous avions attribué aux limites du modèle monomode. Nous pouvons trouver ici une confirmation de cette interprétation, puisque l'on a pour la pureté modale du vide comprimé[4.2]:

$$P = Tr\rho^2 = \frac{1}{\sqrt{\det\gamma}} = \frac{1}{2H-1} < 1 \tag{4.18}$$

Pour finir, signalons une méthode alternative de caractérisation, par une mesure directe, des états gaussiens centrés, que nous avons expérimentée sur une idée originale de Jaromír Fiurášek et Nicolas Cerf[64]. Cette méthode consiste simplement à introduire dans le faisceau analysé une lame séparatrice de transmission T_j, puis à effectuer une mesure à l'aide d'une simple photodiode à avalanche (APD) en régime de comptage de photons. La quantité statistique ainsi mesurée est la probabilité P_{nc} de ne rien détecter ('no click'), qui est une fonction de $Tr\gamma$, $\det\gamma$, T_j ainsi que du rendement quantique η^{APD} de la photodiode. En effectuant plusieurs mesures pour différentes valeurs de T_j il est théoriquement possible de déterminer ainsi $Tr\gamma$ et $\det\gamma$. En fait, si de bons résultats ont été obtenus pour $Tr\gamma$ (figure 4.9), nous n'avons pas réussi à déterminer $\det\gamma$ par cette méthode. Tout juste avons nous pu avoir l'encadrement suivant, lié à l'inégalité de Heisenberg ainsi qu'au fait que la matrice de covariance est définie positive:

$$1 \leq \det\gamma \leq (Tr\gamma/2)^2 \tag{4.19}$$

On pourra se reporter à la référence [4.2] pour plus de détails à ce sujet.

4.2 Source d'états quantiques non-gaussiens

Nous en arrivons maintenant au cœur de ce chapitre, qui consiste en la préparation conditionnelle d'états non gaussien. La possibilité de générer des états exotiques par préparation conditionnelle [52, 102, 103] a déjà été utilisée pour la production d'états à un photon[76]: partant d'une source EPR de faible intensité, qui émet des paires de photons uniques de manière aléatoire, il est possible de s'assurer de la présence d'un photon unique sur l'une des voies en détectant l'autre photon de la paire. Ce procédé a notamment permis à Lvovsky et ses collaborateurs[114, 3] de réaliser la tomographie de l'état à 1 photon. Notre ambition a donc été de tester la préparation conditionnelle sur un état plus complexe, en l'occurrence le vide comprimé décrit à la section précédente, qui implique plusieurs photons et qui n'est plus indépendant de la phase d'observation. Le travail exposé ici a fait l'objet de la publication [4.3].

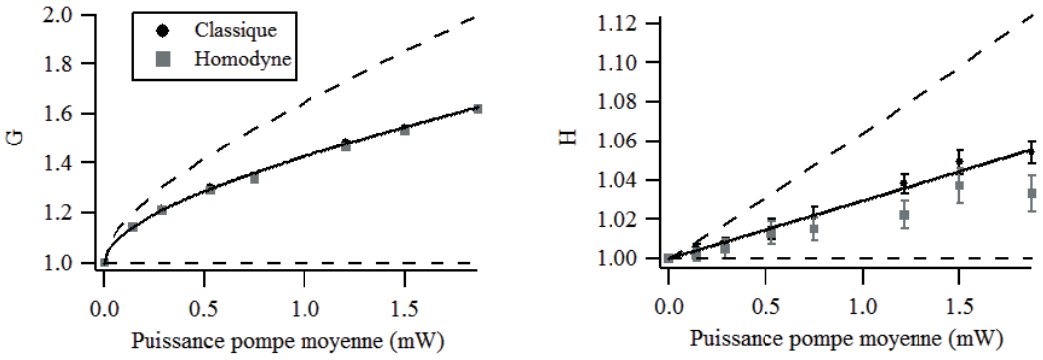

Figure 4.8: *Paramètres G et H déterminés en fonction de la puissance de pompe par deux méthodes différentes. Les courbes en trait plein correspondent à des ajustements des données obtenues avec la méthode classique par un modèle simple basé sur les dépendances de G et H en fonction de la puissance de pompe. Les lignes en pointillés sont déduites de l'inégalité 4.19 déterminée par la méthode de comptage de photons.*

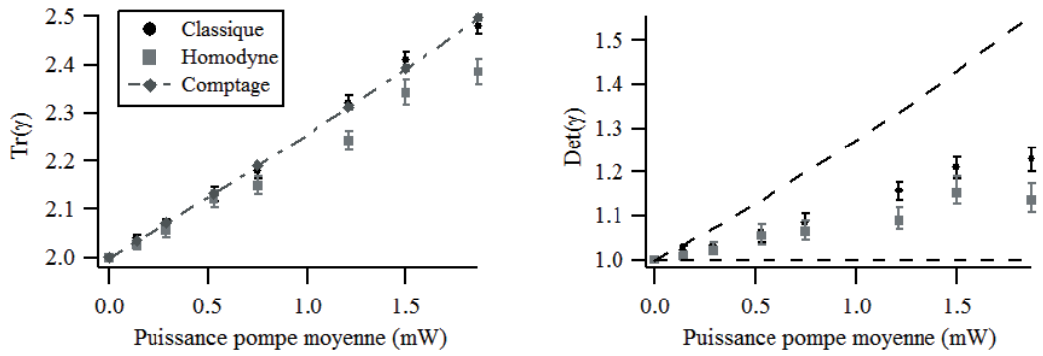

Figure 4.9: *Gauche: Paramètre $Tr\gamma$ déterminé en fonction de la puissance de pompe par les trois méthodes. La ligne en trait mixte joint les points obtenus par la méthode de comptage. Droite: Paramètre $\det\gamma$ déterminé par deux méthodes, la méthode de comptage fournissant l'encadrement en pointillés par 4.19.*

4.2.1 Présentation de l'expérience

Le principe de cette expérience est schématisé sur la figure 4.10: nous partons d'une impulsion de vide comprimée, dont la source a été présentée au paragraphe précédent, et nous l'envoyons sur une lame de faible réflectivité R. En utilisant les notations de la figure, on a:

$$\begin{aligned} a_1 &= \sqrt{R}\, a_3 + \sqrt{1-R}\, a_4 \\ a_2 &= \sqrt{1-R}\, a_3 - \sqrt{R}\, a_4 \end{aligned} \tag{4.20}$$

Il se trouve que l'espace de Fock est particulièrement bien adapté pour donner une idée intuitive de cette expérience. Rappelons en préliminaire l'action de la lame séparatrice dans cet espace[167]; on a, en introduisant l'état vide $|0\rangle$ commun à tous les opérateurs a_i et en utilisant (4.20):

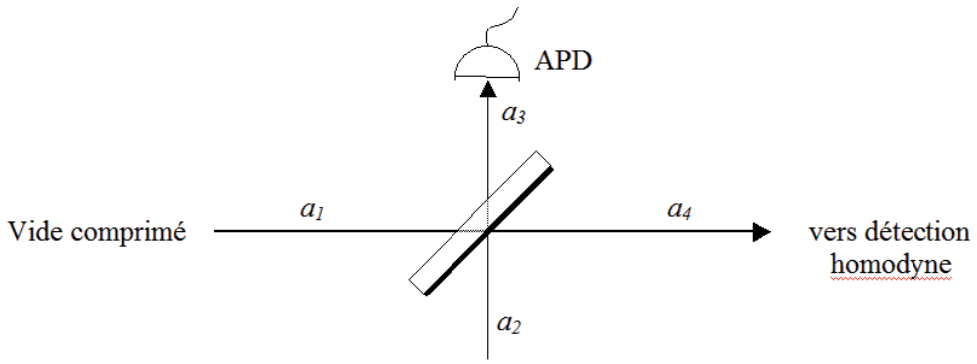

Figure 4.10: *Schéma de principe de l'expérience.*

$$|n\rangle_1|0\rangle_2 = \frac{1}{\sqrt{n!}}a_1^{\dagger n}|0\rangle = \sum_{k=0}^{n}\sqrt{C_n^k R^k(1-R)^{n-k}}\;|k\rangle_3|n-k\rangle_4 \tag{4.21}$$

On retrouve ainsi une simple loi binomiale, caractéristique d'une distribution aléatoire de particules indépendantes.

Si maintenant on envoie le vide comprimé, dont la décomposition dans l'espace de Fock a été donnée en (4.6), on obtient en sortie:

$$|\psi\rangle_{out} = \frac{1}{\sqrt{\cosh r}}\sum_{m=0}^{\infty}\sum_{k=0}^{2m}[C_{2m}^m C_{2m}^k(\frac{1}{2}\tanh r)^{2m}R^k(1-R)^{2m-k}]^{1/2}|k\rangle_3|2m-k\rangle_4 \tag{4.22}$$

Si la réflectivité R de la lame est suffisamment faible, on pourra négliger les termes d'ordre $k>1$ dans ce développement (évènements correspondant à la présence de plusieurs photons sur la voie 3). Si maintenant la photodiode à avalanche (APD) détecte un photon sur cette voie, on aura en sortie sur la voie 4 l'état:

$$|\psi\rangle_{cond} = \frac{1}{N}\sum_{m=1}^{\infty}[2mC_{2m}^m(\frac{1}{2}(1-R)\tanh r)^{2m}]^{1/2}|2m-1\rangle_4 \tag{4.23}$$

L'état ainsi conditionné correspond à ce que l'on aurait obtenu en appliquant l'opérateur d'annihilation a_1 au vide comprimé ou, plus précisément, à un vide comprimé avec un paramètre de compression ζ vérifiant $\tanh\zeta = (1-R)\tanh r$: on réalise ainsi la soustraction d'un photon.

On peut noter également que cet état correspond[117, 111] à un état à un photon amplifié par l'amplificateur dégénéré, avec le même paramètre de compression ζ. Ceci se démontre simplement en écrivant[3] $|1\rangle_{in} = a_{in}^{\dagger}|0\rangle_{in}$ (ce qui, au passage, permet de déterminer la constante de normalisation $N^2 = \tanh^2\zeta\cosh^3\zeta$). La préparation conditionnelle permet donc de synthétiser un état à un photon amplifié, et ce avec un dispositif expérimental beaucoup plus simple que celui qui aurait consisté à préparer d'abord un état à un photon que l'on aurait ensuite amplifié.

La figure 4.11(a et b) représente les densités de probabilité théoriques des quadratures amplifiées et comprimées, calculées à partir de (4.22) pour différentes valeur de R, et pour le paramètre

[3] en suivant une démarche analogue à la démonstration de (4.6).

de compression $r = 0,43$ utilisé dans l'expérience. Lorsque R est suffisamment faible (1%), on retrouve la distribution caractéristique de l'état à 1 photon (amplifiée ou comprimée), avec une valeur nulle à l'origine et une fonction de Wigner négative en ce point[4.3]. Lorsque R est plus élevé, l'état conditionné sur la voie 4 n'est plus un état pur, et même pour $R = 11,5\%$ (valeur qui sera utilisée dans l'expérience) on commence à s'éloigner sensiblement du résultat prédit par (4.23).

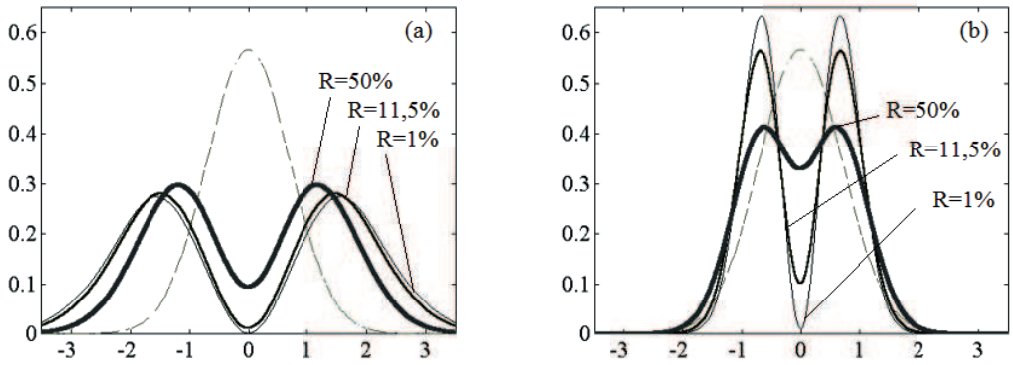

Figure 4.11: *Densité de probabilité théorique des données conditionnées pour les quadratures amplifiées (a) et comprimées (b) pour différentes valeurs de la réflectivité R de la lame et pour $r = 0,43$ (avec la convention $N_0 = 1/2$). La courbe en tirets indique le mode vide de référence. La détection homodyne est supposée parfaite.*

L'efficacité de la détection homodyne va également dégrader les résultats, comme le montre la figure 4.12, où les densités de probabilité théoriques sont calculées pour $R = 11,5\%$, $r = 0,43$, et pour différentes valeurs de l'efficacité η_{hom} de la détection homodyne. Nous verrons toutefois au 4.3.4 que l'on peut corriger cet effet, qui n'est pas relatif à l'état produit mais qui est uniquement dû au système de détection. Ce n'est pas le cas d'un autre écart au cas idéal présenté ici, lié à la nature multimode de la fluorescence paramétrique, que nous allons maintenant aborder.

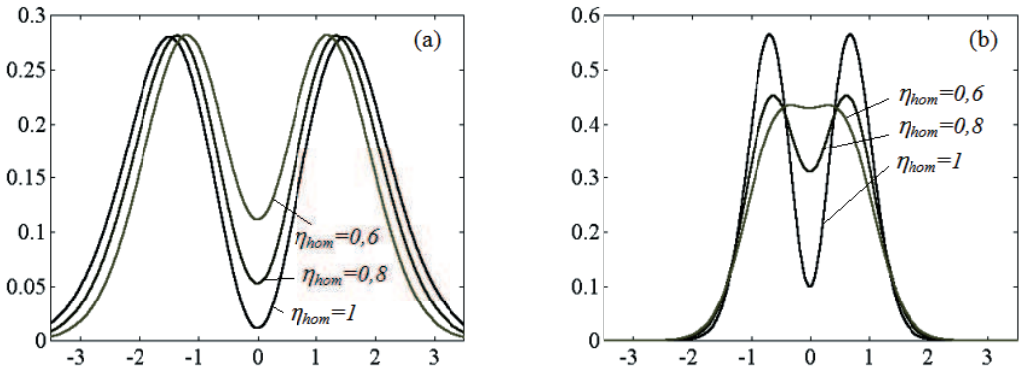

Figure 4.12: *Densité de probabilité théorique des données conditionnées pour les quadratures amplifiées (a) et comprimées (b) pour différentes valeurs de l'efficacité η_{hom} de la détection homodyne, pour $R = 11,5\%$ et $r = 0,43$ (avec la convention $N_0 = 1/2$).*

4.2.2 Dispositif expérimental de conditionnement

L'objet de cette expérience est donc de réaliser la soustraction conditionnelle d'un photon sur l'état vide comprimé décrit au 4.2. Le problème est que cet état est loin d'être le seul à être généré par la fluorescence paramétrique: tout mode vide vérifiant les conditions d'accord de phase, y compris dans une configuration d'amplification non dégénérée, peut être amplifié. On observe ainsi une lumière de fluorescence sur un spectre étendu (200nm) dans un cône de plusieurs degrés d'ouverture. Cette lumière parasite n'est pas trop gênante pour la détection homodyne, qui ne détecte essentiellement qu'un mode unique. Par contre, l'APD est sensible à un très grand nombre de modes, et un filtrage drastique est nécessaire[77, 114].

Le dispositif de conditionnement est détaillé sur la figure 4.13, avec son système de filtrage spatial et spectral: un trou de 50 μm de diamètre, situé dans le plan focal image d'une lentille, sélectionne les modes émis le long de l'axe optique. Un autre trou de 3 mm de diamètre, placé en amont, sélectionne le mode TEM00. Un système de spectroscopie optique à réseau est ensuite utilisé pour réaliser un filtrage spectral sur une bande de 3 nm autour de 846 nm. L'ensemble a un taux de transmission de 3% pour le faisceau sonde soit, en prenant en compte le rendement quantique de l'APD, une efficacité de détection de 1,5%. La conséquence essentielle de cette faible efficacité est un faible taux de comptage, mais la qualité de la préparation conditionnelle n'en est que très peu affectée.

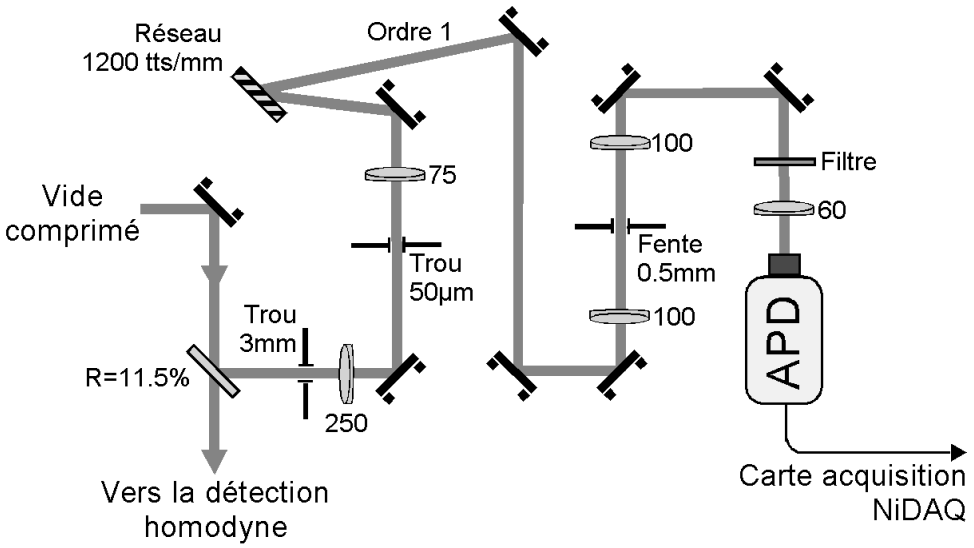

Figure 4.13: *Dispositif expérimental de conditionnement. Un système de filtrage spatial et spectral permet d'éliminer les modes parasites générés par l'amplification paramétrique.*

Bien sûr, ce système de filtrage n'est pas d'une efficacité absolue, et il subsiste une contribution non négligeable des modes parasites sur le signal APD. Nous atteignons ici les limites du modèle monomode utilisé. Un modèle multimode plus approprié a été introduit[77, 114] pour l'étude de l'état à 1 photon obtenu par préparation conditionnelle, qui prend en compte de manière plus détaillée les performances du dispositif de filtrage. Mais il faut rappeler que notre expérience se distingue par un nombre plus important de photons dans l'état généré, compliquant ce type d'étude. Nous ne renonçons pas au développement d'un modèle plus complexe, adapté à notre expérience, mais nous avons dans un premier temps introduit un modèle simplifié pour interpréter nos résultats, schématisé sur la figure 4.14:

Nous avons ainsi considéré les modes émis par amplification paramétrique comme indépendants, en supposant par ailleurs que les modes parasites ne contribuaient pas au signal homodyne. Le mode signal et les modes parasites ont respectivement des poids ξ et $1-\xi$ en ce qui concerne leur probabilité d'être détectés par l'APD. Ce paramètre ξ décrit en quelque sorte la pureté modale de l'état détecté par l'APD, mais prend également en compte d'autres évènements parasites tels que les coups d'obscurité.

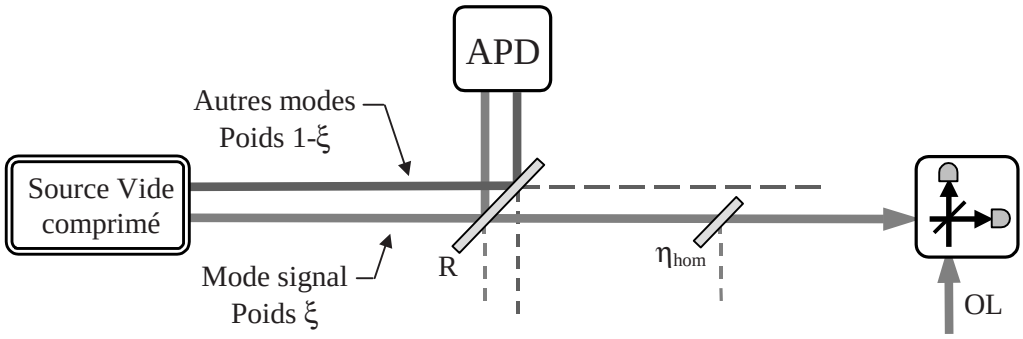

Figure 4.14: *Modèle simplifié pour la prise en compte de la nature multimode de la fluorescence paramétriques: des modes parasites peuvent déclencher l'APD avec une probabilité* $1-\xi$ *, mais ne contribuent pas au signal homodyne.*

Dans le cadre de ce modèle, un déclenchement parasite de l'APD entraîne une contribution du mode signal non-conditionné dans l'histogramme enregistré:

$$Pr = \xi Pr_{cond} + (1-\xi) Pr_{non-cond} \tag{4.24}$$

Le paramètre ξ peut être grossièrement estimé par l'excès du taux de comptage enregistré sur l'APD. Le modèle monomode permet en effet d'estimer ce taux de comptage pour le mode signal, à condition de connaître précisément le taux de transmission des filtres pour ce mode. Nous avons ainsi obtenu dans notre expérience l'estimation suivante: $0,6 < \xi < 0,8$.

4.2.3 Analyse des résultats expérimentaux

Les distributions de probabilités expérimentales, enregistrées pour les quadratures amplifiées et comprimées des impulsions conditionnées, sont présentées sur la figure 4.15 avec la convention $N_0 = 1/2$. La réflectivité de la séparatrice utilisée est $R = 11,5\%$, de façon à disposer d'une statistique de comptage acceptable. Le paramètre de compression $r = 0,43$ ainsi que l'efficacité homodyne $\eta_{hom} = 0,75$ sont conjointement vérifiées par l'analyse de mesures effectuées sur un faisceau sonde et par celle de la tomographie du vide comprimé.

On observe une claire dépendance des statistiques observées par rapport à la phase de l'oscillateur local, caractéristique du fort taux de compression utilisé et du nombre important de photons émis dans l'impulsion[4]. Les données expérimentales sont ajustées par (4.24), avec une valeur $\xi = 0,7$ de la pureté modale en bon accord avec l'encadrement prévu à la section précédente.

Nous avons réalisé la tomographie de cet état en appliquant la transformation de Radon inverse à 6 histogrammes enregistrés pour 6 phases régulièrement répartis entre 0 et $\pi(\varphi = 0,$

[4]On ne peut tronquer les développements dans l'espace de Fock en deçà d'une dizaine de photons.

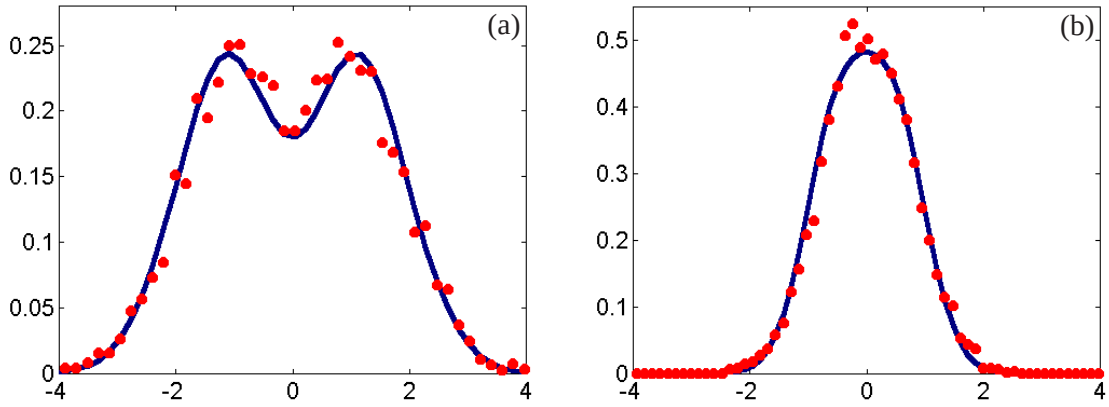

Figure 4.15: *Distributions de probabilités ($N_0 = 1/2$) pour les quadratures amplifiées et comprimées des données conditionnées. Les courbes correspondent au modèle théorique avec $r = 0,43$, $R = 11,5\%$ et $\xi = 0,7$.*

$\pi/6$, $\pi/3$, $\pi/2$, $2\pi/3$, $5\pi/6$), d'une manière analogue à la tomographie du vide comprimé de la section 4.2.4. La fonction de Wigner obtenue est présentée sur la figure 4.16, avec 2 coupes suivant ses axes propres. Comme on peut le voir sur cette figure, nous avons un état clairement non gaussien, avec un creux net à l'origine de l'espace des phases ($W_exp(0,0) = 0,067$ alors que le maximum de W est à $0,12$).

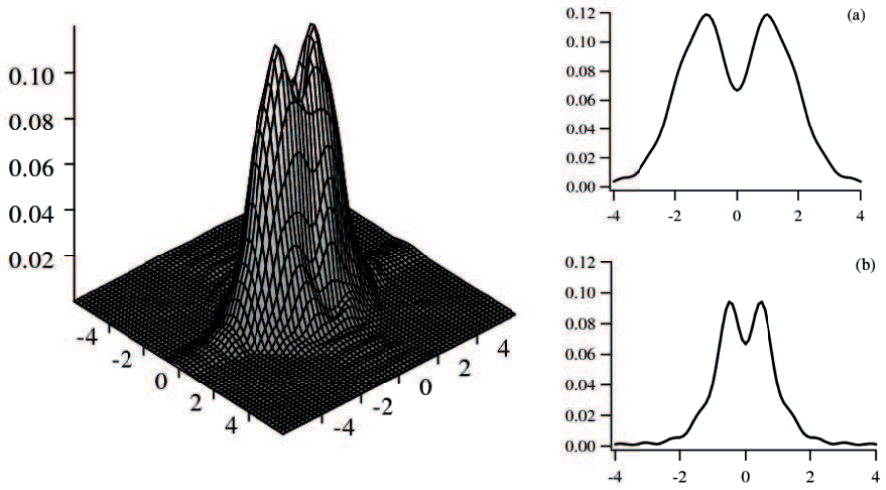

Figure 4.16: *Fonction de Wigner de l'état conditionné reconstruite par la transformation de Radon inverse ($N_0 = 1/2$). Deux coupes selon les quadratures amplifiée (a) et comprimée (b) sont également présentées.*

Une simulation à partir du modèle théorique (4.24) prévoit toutefois une fonction de Wigner atteignant presque $-0,06$ avec les paramètres de l'expérience, à condition de disposer d'une détection homodyne parfaite ($\eta_{hom} = 1$). Et il n'est absolument pas illégitime de vouloir corriger mathématiquement les imperfections du système de détection, qui ne sont pas caractéristiques de l'état produit. Nous allons maintenant voir comment il est possible de réaliser une telle

opération, en utilisant une reconstruction numérique de la fonction de Wigner par maximum de vraisemblance.

4.2.4 Reconstruction de la fonction de Wigner par maximum de vraisemblance

L'objectif ici n'est en fait pas la reconstruction de la fonction de Wigner, mais celle de la matrice densité. Ces deux entités sont toutefois équivalentes, et l'on peut facilement obtenir la fonction Wigner à partir de la matrice densité. Nous allons représenter cette matrice dans l'espace de Fock, en utilisant une troncation adéquate. Cette troncation doit bien sûr être convenablement choisie de façon à ne pas déformer le résultat final (typiquement 20 photons); le fait de limiter le nombre de photons va jouer le rôle d'un filtre éliminant les bruits hautes fréquences.

Nous avons utilisé, pour faire cette reconstruction, la méthode du maximum[141, 115] de vraisemblance. Cette méthode consiste à maximiser la vraisemblance $L(\rho)$, qui est la probabilité d'obtenir le résultat observé lorsque la matrice densité de l'état incident est ρ:

$$L(\rho) = \prod_j [Pr_j(\rho)]^{f_j} \tag{4.25}$$

où j balaye l'ensemble des canaux des 6 histogrammes, où Pr_j est la probabilité de tomber dans le canal j, et où f_j est le nombre d'occurrences effectivement enregistrées dans ce canal.

La probabilité $Pr_j(\rho)$ est facilement reliée à la matrice densité en introduisant le projecteur Π_j sur l'état j: $Pr_j(\rho) = Tr\{\Pi_j \rho\}$. En écrivant que le logarithme de (4.25) est stable pour toutes variations $\rho_0 \to \rho_0 + d\rho$ autour de l'optimum ρ_0 (avec $d\rho$ de trace nulle pour préserver la normalisation de la matrice densité), il vient que:

$$Tr\{R(\rho_0) d\rho\} = 0 \tag{4.26}$$

pour tout $d\rho$ de trace nulle, où R est définie par:

$$R(\rho) = \sum_j \frac{f_j}{Pr_j(\rho)} \Pi_j \tag{4.27}$$

On peut déduire[115] de la condition (4.26) que R est proportionnel à l'identité au maximum de vraisemblance, et donc que ce maximum est un point fixe de la suite:

$$\rho^{(k+1)} = N[R(\rho^{(k)}) \rho^{(k)} R(\rho^{(k)})] \tag{4.28}$$

où N est l'opérateur de normalisation garantissant l'unité de la trace de ρ. Une suite peut parfois converger vers son point fixe, et c'est le cas ici lorsque l'on prend l'identité pour condition initiale.

Il se trouve qu'il est très simple de corriger les imperfections du détecteur par cette méthode. Rappelons que l'on peut prendre en compte l'efficacité η_{hom} de la détection homodyne en considérant une détection parfaite, et en intercalant une séparatrice de transmission η_{hom}. Il suffit de prendre en compte la traversée de cette lame dans le calcul de Π_j, Pr_j et R pour obtenir une estimation de la matrice densité de l'état avant cette traversée, corrigée de l'influence de cette imperfection. Nous avons adapté cette méthode pour corriger également le bruit électronique. La figure 4.17 présente la fonction de Wigner ainsi obtenue pour notre état conditionné, après 4000 itérations de (4.28), corrigée de l'efficacité $\eta_{hom} = 0,75$ et du bruit électronique.

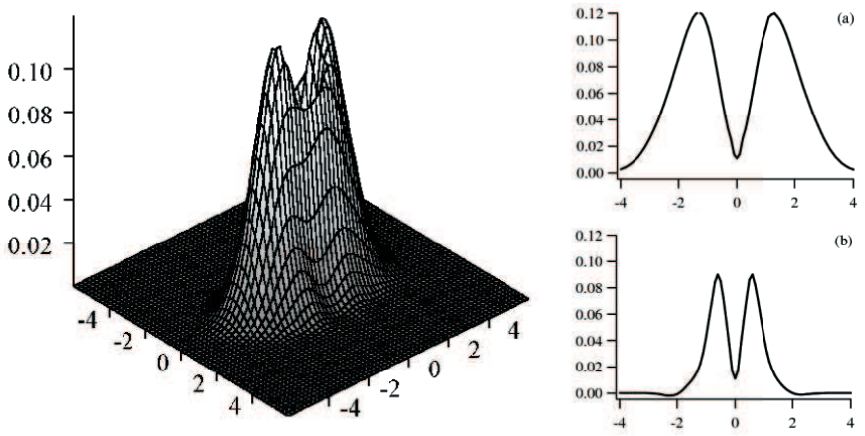

Figure 4.17: *Fonction de Wigner de l'état conditionné reconstruite par maximum de vraisemblance (pour $N_0 = 1/2$), avec correction de η_{hom} et du bruit électronique. Deux coupes selon les quadratures amplifiée (a) et comprimée (b) sont également présentées.*

La correction appliquée permet d'obtenir un creux plus profond, mais qui n'atteint pas les valeurs négatives prédites par la simulation. Nous sommes donc forcés de constater ici les limites de notre modèle monomode, même agrémenté du paramètre ξ (4.24).

4.2.5 Conclusion et perspectives

Nous avons donc pu, avec la préparation conditionnelle, synthétiser un état non gaussien. Un modèle relativement simple a permis une interprétation raisonnable des résultats obtenus. Il s'agit maintenant de mieux comprendre théoriquement l'influence de la nature multimode de notre expérience. Au plan expérimental, nous devons nous rapprocher du régime monomode pour améliorer nos résultats; on pourra pour cela utiliser un filtrage plus efficace (par l'utilisation d'une fibre monomode par exemple), ainsi qu'une taille plus importante du faisceau pompe.

Ce travail fait désormais l'objet de la thèse d'Alexei Ourjoumtsev. Un filtrage par fibre monomode a déjà permis d'améliorer considérablement les résultats, avec l'observation d'une fonction de Wigner négative avant même la prise en compte de l'efficacité homodyne[133]. Cette amélioration nous a également permis de réaliser la première reconstruction tomographique d'un état à 2 photons, obtenu avec une détection conditionnelle à 2 évènements[134]. Par ailleurs, la simple prise en compte de la pureté modale du vide comprimé utilisé, par l'introduction du paramètre H (voir 4.15,4.18), a permis d'améliorer l'adéquation de notre modèle théorique avec les résultats expérimentaux[133, 134].

Concernant la possibilité d'utiliser une taille plus importante du faisceau pompe, nous avons démarré la conception d'un amplificateur Ti-Sa, afin de disposer de plus d'énergie dans nos impulsions pompe. Cet amplificateur est maintenant quasiment réalisé, et devrait nous permettre d'étudier la dépendance de la pureté modale ξ avec la taille de la pompe. Il nous reste donc encore un important travail à réaliser pour maîtriser tous les aspects de cette expérience.

Comme nous l'avons déjà souligné, la préparation conditionnelle est un ingrédient indispensable de certains protocoles de purification d'intrication[38]. Nous poursuivrons nos efforts dans l'étude de la faisabilité de ce type de protocole avec peut-être, à la clé, de nouveaux dispositifs de cryptographie longues distances. Mais l'état à 1 photon amplifié (4.23) peut avoir d'autres

applications, et notamment la génération de chats de Schrödinger :

Rappelons tout d'abord qu'un état lumineux macroscopique, d'amplitude complexe α, est associé à un état cohérent $|\alpha\rangle$. Suivant l'expérience de pensée de Schrödinger, dans laquelle un système macroscopique se retrouve dans une superposition d'états, on introduit en optique quantique l'état chat:

$$|chat : \alpha\rangle = \frac{1}{N}(|\alpha\rangle - |-\alpha\rangle) \tag{4.29}$$

Cet état présente la particularité de ne comporter que des termes impairs dans sa décomposition de Fock, à l'instar de l'état conditionné (4.23). Il se trouve que ce dernier, calculé pour une réflectivité $R = 1\%$ de la séparatrice de conditionnement avec $r = 0.43$, présente une fidélité $F > 99\%$ avec le chat (4.29) pour $\alpha = 1.16$, où l'on définit la fidélité par:

$$F = |\langle chat : \alpha|\psi_{cond}\rangle|^2 \tag{4.30}$$

Ainsi, nos expériences de conditionnement les plus récentes[134] nous ont permis de synthétiser un état présentant une fidélité de 70% avec un chat pour $\alpha = 0,89$. Alors il est vrai qu'avec des valeurs de α proches de l'unité, qui correspondent à peine à un photon par impulsion, on ne peut pas vraiment parler de superposition d'états macroscopiques. Mais ce "chaton" peut ensuite être utilisé pour produire un chat de plus grande amplitude, en suivant une technique d'amplification conditionnelle[111] qui semble réalisable avec les technologies actuelles. La production de tels états pourra se révéler très intéressante pour approfondir l'étude du monde quantique, et notamment de la décohérence.

Pour finir, signalons que nous verrons au 4.5 une autre application de la préparation conditionnelle, pour un test sans échappatoires des inégalités de Bell. Nous allons avant cela exposer un autre savoir-faire indispensable: la génération d'états intriqués en quadrature.

4.3 Génération d'états intriqués en quadrature

4.3.1 Introduction

Des paires de faisceaux intriquées en quadratures ont déjà été produites par différentes techniques [131, 132, 179, 153], et ont même été utilisées pour la téléportation quantique[67] de quadratures. Comme dans le cas du vide comprimé, notre originalité réside ici dans le fait de travailler en régime impulsionnel, avec une détection homodyne impulsionnelle. Ce travail est détaillé dans la référence [4.4]. Nous utiliserons le même cristal que précédemment, mais en travaillant cette fois-ci en configuration non-dégénérée: le signal et l'idler ne sont plus confondus (figure 4.18).

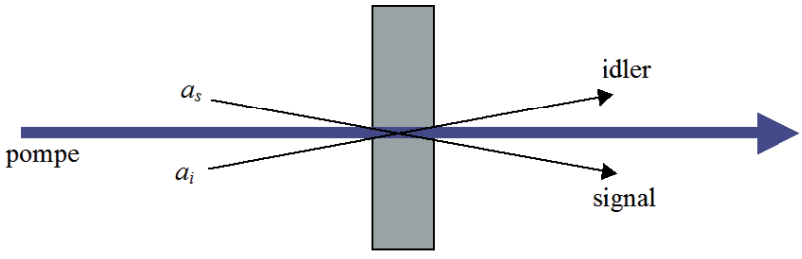

Figure 4.18: *Amplificateur paramétrique en configuration non dégénérée (NOPA).*

L'équation de propagation (4.3) devient[150]:

$$\frac{da_s}{dz} = \frac{a_i^\dagger}{L_{NL}} \ , \quad \frac{da_i}{dz} = \frac{a_s^\dagger}{L_{NL}} \tag{4.31}$$

avec pour solution:

$$\begin{aligned} a_{s,out} &= \cosh r a_{s,in} + \sinh r a_{i,in}^\dagger \\ a_{i,out} &= \cosh r a_{i,in} + \sinh r a_{s,in}^\dagger \end{aligned} \tag{4.32}$$

ou, dans l'espace des quadratures:

$$\begin{aligned} Q_{s,out} &= \cosh r Q_{s,in} + \sinh r Q_{i,in} \ , \quad P_{s,out} = \cosh r P_{s,in} - \sinh r P_{i,in} \\ Q_{i,out} &= \cosh r Q_{i,in} + \sinh r Q_{s,in} \ , \quad P_{i,out} = \cosh r P_{i,in} - \sinh r P_{s,in} \end{aligned} \tag{4.33}$$

Ces dernières relations montrent que l'on a affaire ici à un amplificateur indépendant de la phase (le coefficient d'amplification est identique pour toutes les quadratures), avec un bruit quantique ajouté par le couplage signal/idler en relation avec l'impossibilité du clonage quantique. On peut noter que ce sont ces relations qui ont été utilisées dans le modèle (4.15) de production d'un état gaussien centré quelconque. Le gain de cet amplificateur est toujours supérieur à 1, et reste toujours inférieur au gain d'amplification du même système en configuration dégénérée. Dans toutes ces relations, on retrouve évidemment le cas dégénéré en posant l'égalité du signal et de l'idler.

On obtient l'expression dans l'espace de Fock du vide amplifié par ce système de la même manière que pour le vide comprimé:

$$a_{s,in}|0\rangle_{in} = a_{i,in}|0\rangle_{in} = 0 \Leftrightarrow |0\rangle_{in} = \sqrt{1-\lambda^2} \sum_n \lambda^n |n\rangle_{s,out}|n\rangle_{i,out} \tag{4.34}$$

où l'on a posé $\lambda = \tanh r$. On peut ainsi générer par fluorescence paramétrique des paires de photons intriquées. Les impulsions correspondantes sont également intriquées en quadrature, comme on peut le voir à partir de (4.33) en écrivant:

$$\begin{aligned} Q_{s,out} - Q_{i,out} &= e^{-r}(Q_{s,in} - Q_{i,in}) \\ P_{s,out} + P_{i,out} &= e^{-r}(P_{s,in} + P_{i,in}) \end{aligned} \tag{4.35}$$

et l'on a, pour des valeurs élevées du paramètre de compression, $Q_{s,out} \approx Q_{i,out}$ et $P_{s,out} \approx -P_{i,out}$. En fait, cette source est exactement la source d'états maximalement intriqués en quadrature introduite au chapitre 3 : on peut en effet directement vérifier les équations (3.78,3.79) à partir des équations (4.33), avec $V = cosh(2r)$.

4.3.2 Résultats expérimentaux

Pour la réalisation expérimentale de ce dispositif, il a fallu réaligner les optiques en utilisant cette fois-ci un faisceau sonde qui n'est plus aligné sur la pompe, mais fait un petit angle avec lui. Le système de détection a également du être modifié, puisque nous avons une paire de faisceaux à analyser. Nous aurions donc idéalement du utiliser 2 détections homodynes; ne disposant que

d'une détection fonctionnelle lors de ces expériences, nous avons utilisé une méthode alternative, schématisée sur la figure 4.19:

Les deux faisceaux issus de la source EPR sont recombinés à l'aide d'une séparatrice 50/50, et seul l'un des deux faisceaux issu de cette recombinaison est analysé par la détection homodyne. Un transducteur piezo-électrique (PZT) permet de contrôler le déphasage θ entre les faisceaux au niveau de la séparatrice. Lorsque $\theta = 0$, la détection homodyne va mesurer:

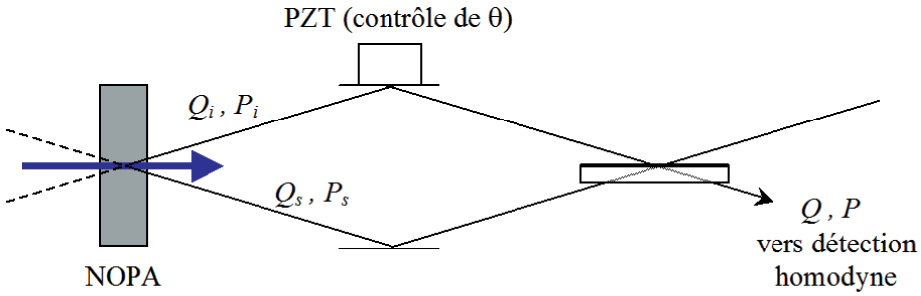

Figure 4.19: *Procédure utilisée pour la caractérisation des deux états intriqués.*

$$Q = \frac{1}{\sqrt{2}}(Q_s + Q_i) \ , \quad P = \frac{1}{\sqrt{2}}(P_s + P_i) \tag{4.36}$$

tandis que l'on aura pour $\theta = \pi$:

$$Q = \frac{1}{\sqrt{2}}(Q_s - Q_i) \ , \quad P = \frac{1}{\sqrt{2}}(P_s - P_i) \tag{4.37}$$

On voit apparaître dans ces expressions les quantités (4.35) qui caractérisent l'intrication en quadrature. Ces quantités vont nous permettre de quantifier le niveau d'intrication des paires d'impulsions produites, comme nous le verrons à la section suivante.

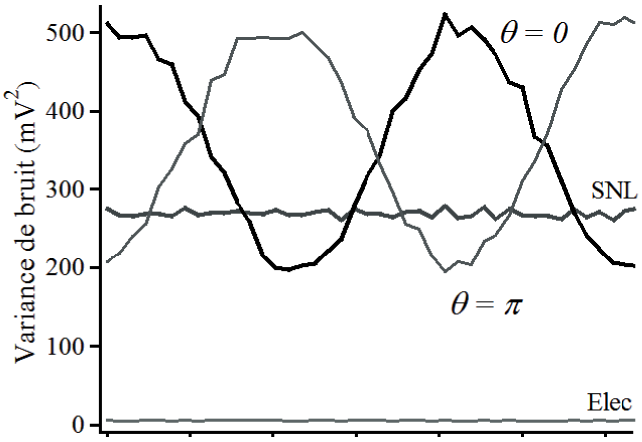

Figure 4.20: *Variance du signal homodyne mesuré, pour $\theta = 0$ et $\theta = \pi$, lors d'un balayage de la phase de l'oscillateur local. Les niveaux du bruit quantique standard (SNL) et du bruit électronique sont également représentés.*

La variance du signal homodyne mesuré est présenté sur la figure 4.20, pour un balayage linéaire de la phase φ de la détection homodyne, et pour $\theta = 0$ et π. La variance du bruit quantique standard est également présentée, ainsi que celle du bruit électronique. En $\theta = 0$ la variance est minimale pour la quadrature P, tandis qu'elle est minimale pour la quadrature Q en $\theta = \pi$: il est donc logique d'observer deux sinusoïdes en opposition.

Ces deux courbes ont des propriétés symétriques pour le niveau de précision de l'expérience $(0,01N_0)$, avec une compression des fluctuations quantiques à $0,70N_0$ ($-1,55$ dB), et une amplification à $1,96N_0$ (2,92 dB). Après correction par (3.63) de l'influence du bruit électronique et de l'efficacité de la détection homodyne (évaluée ici à $\eta_{hom} = 68\%$) nous obtenons, en notant $\Delta^2 X$ la variance de l'opérateur X:

$$\frac{1}{2}\Delta^2(Q_s - Q_i) = \frac{1}{2}\Delta^2(P_s + P_i) = 0,56N_0 \tag{4.38}$$

On observe donc une corrélation entre Q_s et Q_i , ainsi qu'entre P_s et $-P_i$, caractéristique de l'intrication en quadrature.

4.3.3 Conclusion

Nous avons donc mis en évidence l'intrication en quadrature d'une paire d'impulsions produite par amplification paramétrique non dégénérée. L'originalité de cette expérience réside dans le fait d'avoir travaillé d'un bout à l'autre en régime impulsionnel, une mesure de quadrature étant associée de façon non équivoque à chaque impulsion. L'idéal aurait bien sûr été d'utiliser deux détections homodynes, pour mesurer directement les corrélations entre les quadratures des faisceaux émis. Nous avons cependant réussi à mesurer les quantités (4.38), qui sont en soit caractéristiques de l'intrication. Un critère de non-séparabilité utilisant ces quantités a été formulé de façon indépendante par L.M. Duan[59] et R. Simon[156]:

$$I_{DS} = \frac{1}{2}[\Delta^2(Q_s - Q_i) + \Delta^2(P_s + P_i)] < 2N_0 \tag{4.39}$$

et il vient directement que dans notre cas $I_{DS} = 1,12N_0$, et que l'état produit ne peut donc pas être factorisé. La quantité I_{DS} ne peut toutefois pas, a priori, être utilisée comme une mesure de l'intrication, car elle ne possède pas les propriétés adéquates[63]. La mesure d'intrication couramment admise pour un état quelconque est l'entropie de formation[177], qui est une entité théorique que l'on ne sait en général pas calculer. Il existe cependant une exception pour les états gaussiens symétriques, et l'on a dans ce cas[70]:

$$E_F = f(\frac{I_{DS}}{2N_0}) \tag{4.40}$$

où f est une fonction donnée explicitement dans la référence [4.4]. Nous obtenons pour notre expérience $E_F = 0,44$ ebit, ce que l'on peut interpréter comme la quantité d'information qu'Alice et Bob pourront partager en exploitant l'intrication de chaque paire d'impulsions.

Ceci est une expérience préliminaire très encourageante, et nous projetons d'améliorer ces performances en vue de tester sur ces paires des protocoles de dégaussification par préparation conditionnelle, et d'établir dans quelle mesure la purification d'intrication est expérimentalement réaliste. Mais nous allons maintenant aborder une autre application potentielle de ce type d'expériences.

4.4 Intrication en quadrature et inégalités de Bell

La théorie quantique a bouleversé notre conception du monde, en prétendant que le résultat d'une mesure n'a de sens qu'une fois cette dernière effectuée. L'univers quantique est intrinsèquement probabiliste, et l'on ne peut connaître que la probabilité d'obtenir tel ou tel résultat: vouloir aller plus loin dans la connaissance du monde, même de manière abstraite, serait invariablement voué à l'échec. Cet aspect paradoxal de la mécanique quantique a été souligné en 1935 dans le célèbre article d'Einstein, Podolsky et Rosen[61], dont les noms sont maintenant emblématiques de la notion d'intrication.

Car cette notion d'intrication exacerbe de façon aiguë toute les difficultés conceptuelles de cette théorie. Les mesures effectuées sur deux particules intriquées, c'est-à-dire préparées par une source commune dans un état quantique non factorisable, peuvent en effet présenter des corrélations, même lorsque ces particules sont très éloignées l'une de l'autre. Ces corrélations peuvent même être maximales si les deux quantités mesurées sont en adéquation: le résultat de l'une des mesures fixe alors de façon certaine, et instantanément, le résultat de l'autre. Comment alors expliquer de telles corrélations, dans le cadre d'une théorie locale interdisant toute transmission super-luminique, sans introduire un "élément de réalité", une variable commune, transportant l'information nécessaire à ces corrélations ?

Une telle théorie réaliste et locale, à variables cachées, permettrait d'aborder la mécanique quantique de manière beaucoup plus intuitive. Le résultat d'une mesure ne dépendrait alors que de la quantité α mesurée, et d'un paramètre λ extérieur à la théorie quantique. En 1964 John Bell[15] a apporté une contribution majeure à ce débat en le quantifiant: il a en effet montré que ces théories devaient satisfaire à certaines contraintes désormais connues sous le nom d'inégalités de Bell. Supposons que deux opérateurs A et B disposent chacun de l'une des particules d'une paire EPR, et qu'ils effectuent indépendamment une mesure sur leur particule. Dans le cadre d'une théorie à variable cachée, le résultat de la mesure de la quantité α par l'opérateur A sera $A(\alpha, \lambda)$: ce résultat est parfaitement déterministe, l'aléa ne résidant que dans la valeur de λ. De même, l'opérateur B va mesurer $B(\beta, \lambda)$. On a considéré ici une théorie locale, où le résultat de la mesure B ne dépend pas de la quantité mesurée en A, et réciproquement. Le paramètre λ peut être n'importe quelle entité mathématique, à partir du moment où elle est définie dans un espace probabilisé: cette description est donc très générale. Dans ce cadre théorique, la corrélation entre les deux mesures va s'écrire:

$$E(\alpha, \beta) = \int A(\alpha, \lambda) B(\beta, \lambda) p(\lambda) d\lambda \tag{4.41}$$

On pourrait croire que l'on peut interpréter toutes les corrélations, classiques ou quantiques, avec une relation de ce type, mais ce n'est pas le cas. On peut s'en rendre compte en introduisant par exemple l'inégalité suivante, dite inégalité CHSH (Clauser-Horne-Shimony-Holt[47]). Si le résultat des mesures de A et B est binaire, ne pouvant prendre que les valeurs $+1$ ou -1, la formulation (4.41) implique nécessairement:

$$S = |E(\alpha, \beta') + E(\alpha', \beta') + E(\alpha', \beta) - E(\alpha, \beta)| \leq 2 \tag{4.42}$$

où α,α' et β,β' sont deux couples de quantités pouvant être mesurées respectivement par A et B. Cette relation peut être établie simplement, puisqu'il suffit de remarquer que si A,A',B et B' sont 4 variables pouvant prendre les valeurs $+1$ ou -1, alors $(A + A')B' + (A' - A)B$ ne peut prendre que les valeur $+2$ ou -2. La violation par une expérience de cette inégalité, ou d'une autre du même type[48], suffit donc pour rejeter toute théorie locale et réaliste.

Dés lors le débat pouvait être tranché expérimentalement, la théorie quantique prévoyant des situations violant ces inégalités. Ainsi, au début des années 80, les expériences menées par Alain Aspect, Jean Dalibard, Philippe Grangier et Gérard Roger[7, 8, 9] ont permis de vérifier de manière très claire les prévisions de la mécanique quantique. Alors, ces expériences permettaient-elles de disqualifier définitivement les théories à variables cachées? Il existe en fait deux "échappatoires" pour la survie de ces théories:

La première de ces échappatoires concerne la localité, et le fait que les évènements de mesure doivent, pour être concluants, être séparés d'un intervalle de genre espace pour exclure toute communication entre ces points. Alain Aspect et ses collaborateurs[9] ont réalisé en 1982 une première expérience permettant de clore cette échappatoire. Cette expérience a depuis été reprise par Anton Zeilinger et son équipe[170] avec une séparation des détecteurs de 400 m, menant aux mêmes conclusions. Ces expériences ne permettent toutefois pas d'écarter une seconde échappatoire, qui concerne l'efficacité de détection: les détecteurs de photons uniques utilisés ont un rendement quantique limité, et la statistique des évènements mesurés peut être différente de la statistique de l'ensemble[136, 71]. David Wineland et son équipe ont pu clore cette échappatoire en mesurant les corrélations quantiques entre deux ions de Beryllium[147] avec une efficacité de détection de près de 80%; la distance entre les ions (8 μm) était cependant trop faible pour clore l'échappatoire de localité.

En fait, aucune expérience n'a permis à ce jour de clore simultanément les deux échappatoires. Il y a certes peu de raisons de s'attendre à des surprises, mais il est intéressant de pousser ce débat dans ses derniers retranchements. C'est ici que nos expériences sur les variables continues peuvent jouer un rôle: il s'agit d'expériences d'optique pour lesquelles il est assez facile de clore l'échappatoire de localité. Mais l'avantage majeur des variables continues est que toute mesure de la détection homodyne fournit un résultat qui pourra être pris en compte dans les statistiques. L'efficacité imparfaite de cette détection va uniquement jouer sur la distribution statistique de ces évènements de mesure, et il n'existe aucun 'non-événement' pouvant fausser cette distribution. La violation des inégalités de Bell par des variables continues pourrait donc permettre de clore définitivement le débat.

Dans ce contexte, le problème consiste à trouver une inégalité de Bell qui puisse être violée par une expérience à variables continues. Ainsi, les états intriqués en quadrature présentés dans la section précédente ne peuvent être candidats: ce sont des états gaussiens, et leur fonction de Wigner positive, qui peut être interprétée comme une probabilité dans l'espace de phase, permet de construire une théorie à variable cachée quelles que soient les mesures considérées. W.J. Munro fut le premier à proposer[124] un état permettant d'obtenir une violation des inégalités de Bell avec des variables continues: il prévoit ainsi une violation $S = 2,076$ de CHSH à partir d'un état de la forme $|\psi\rangle = \sum c_n|n\rangle|n\rangle$, les coefficients c_n étant pertinemment choisis pour maximiser S. Par la suite, G. Auberson et ses collaborateurs[10] ont proposé un état permettant une violation maximale de CHSH, à savoir $S = 2\sqrt{2} \approx 2,83$. L'état proposé est toutefois singulier, incluant une forme régularisée de $1/\sqrt{q}$. Nous nous sommes attaqués à ce problème, et avons proposé un état plus régulier permettant également d'obtenir une violation maximale de CHSH. Cet état, comprenant entre autres une superposition multiple d'états cohérents, reste toutefois peu accessible à l'expérience, et l'on se reportera à la référence [4.5] pour plus de détails à ce sujet.

L'idée que je vais maintenant exposé est issue d'une réunion avec nos collaborateurs de l'Université Libre de Bruxelles, alors que nous exposions nos projets concernant la dégaussification de paires intriquées. Le schéma du dispositif proposé est donné sur la figure 4.21 : un dispositif de préparation conditionnelle, analogue à ce qui a été présenté en section 4.3, est placé sur chacune des voies de sorties de la source EPR, et l'état final n'est accepté que si les APD sont simultanément déclenchées sur les deux voies. On obtient en sortie un état dont la fonction de

Wigner présente des valeurs négatives (figure 4.22a) et, mieux, permet une violation de CHSH.

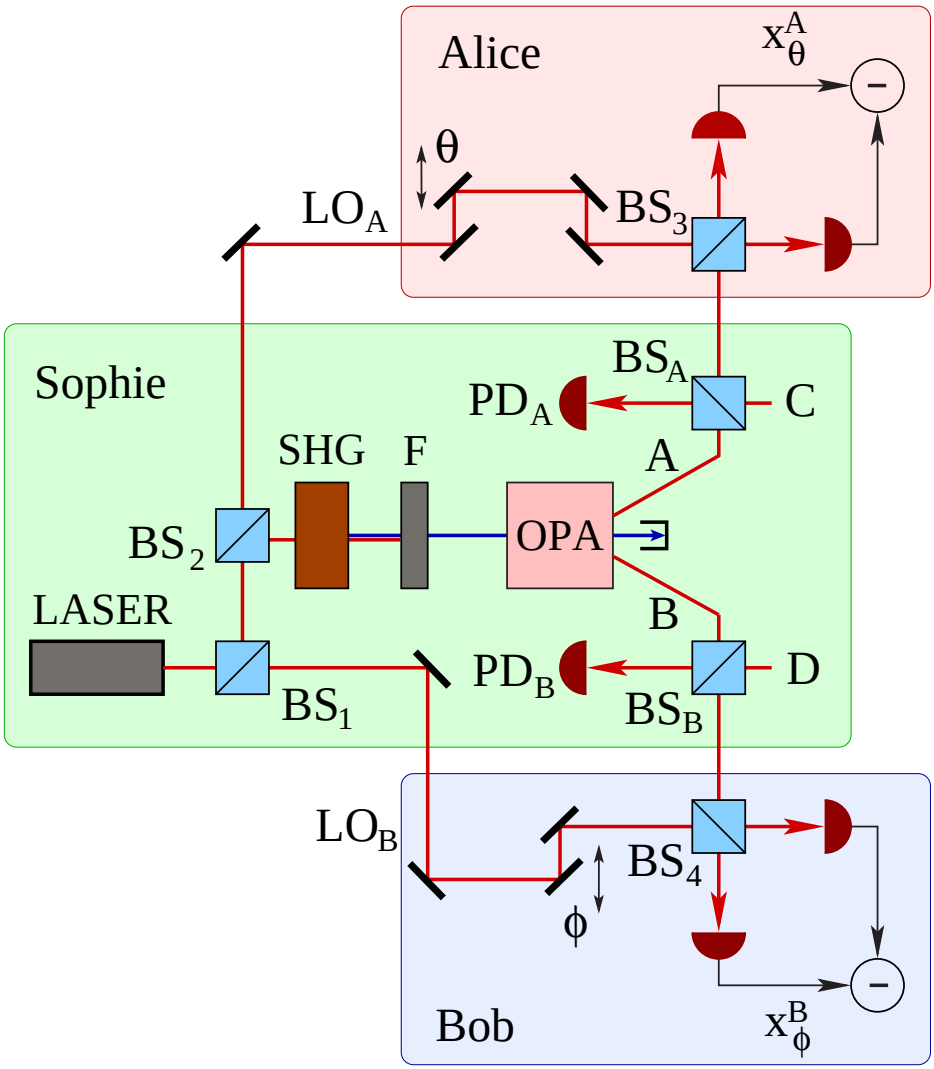

Figure 4.21: *Proposition d'expérience test des inégalités de Bell utilisant des variables continues.*

Il suffit à Alice et Bob, pour chaque état validé par la préparation conditionnelle, de mesurer au choix la quadrature P ou Q, et de prendre pour résultat le signe de cette mesure. Chaque mesure donnera un résultat qui sera pris en compte dans le calcul des corrélations, pour la détermination de la quantité:

$$S = |E(P_A, Q_B) + E(Q_A, Q_B) + E(Q_A, P_B) - E(P_A, P_B)| \leq 2 \tag{4.43}$$

Nous prédisons ainsi une violation $S \approx 2,046$ pour une transmission $T = 99\%$ des lames de conditionnement, et pour $\lambda = \tanh r \approx 0,57$ (figure 4.22b). Ce résultat est obtenu pour des détecteurs parfaits, et la figure 4.22 présente les variations de S en fonction du rendement quantique des APD de conditionnement (4.22c, pour une détection homodyne parfaite) et de l'efficacité des détections homodynes (4.22d, pour un rendement quantique des APD $\eta = 30\%$), pour différentes valeurs du taux de transmission T, et pour $\lambda T \approx 0,57$.

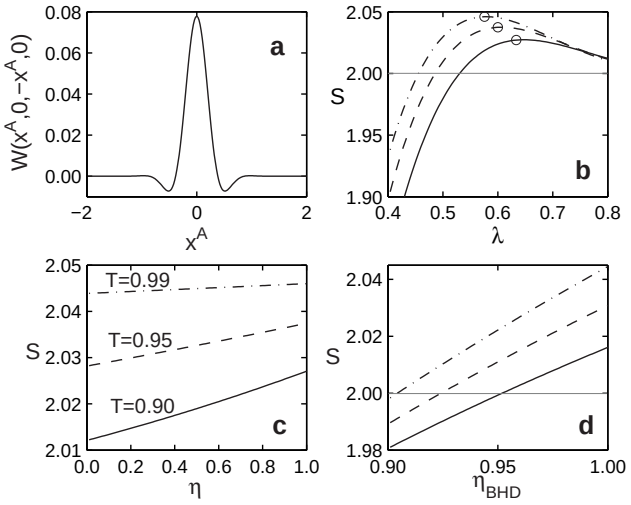

Figure 4.22: *(a) Coupe de la fonction de Wigner de l'état conditionné avec* $\lambda = 0.5$, $T = 0.95$, *et* $\eta = 30\%$ *pour la ligne* $q_B = -q_A$, $p_A = p_B = 0$. *(b) Paramètre de Bell* S *en fonction de la compression* λ *du faisceau EPR initial, pour des détections parfaites* ($\eta = \eta_{hom} = 100\%$), *avec* $T = 0.9$ *(trait plein),* $T = 0.95$ *(tirets), et* $T = 0.99$ *(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).*

Une faible violation des inégalités de Bell paraît donc accessible, même si les performances requises ($r \approx 0,7$, $\eta_{hom} > 0,9$) relèvent du challenge technologique. Il faut bien comprendre que dans ce dispositif, le fait que la préparation conditionnelle élimine un grand nombre de paires n'est en rien un handicap pour la clôture de l'échappatoire liée à l'efficacité de détection: il s'agit ici d'une sélection à la source, rigoureusement indépendante du choix des quantités mesurées par Alice et Bob. On peut voir la source comme une boîte noire, qui émet de temps en temps des paires EPR en les annonçant. Ceci place notre expérience dans le formalisme 'event-ready' selon John Bell[15]. Toutes les paires ainsi émises feront l'objet d'une mesure.

Il semble donc que les variables continues puissent mener à un test définitif, sans échappatoire, des inégalités de Bell, par un procédé qui n'est pas inaccessible aux technologies actuelles.

4.5 Articles annexés au chapitre

[4.1] 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).

[4.2] J. Wenger, J. Fiurášek, R. Tualle-Brouri, N.J. Cerf et P. Grangier, Pulsed squeezed vacuum characterization without homodyning, *Phys. Rev. A* **70** 053812 (2004).

[4.3] J. Wenger, R. Tualle-Brouri et P. Grangier, Non-gaussian statistics from individual pulses of squeezed light, *Phys. Rev. Lett.* **92**, 153601 (2004).

[4.4] J. Wenger, A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Time-resolved homodyne characterization of individual quadrature-entangled pulses, *Eur. Phys. J. D* **32** 391-396 (2005).

[4.5] 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).

[4.6] 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, *Phys. Rev. Lett.* **93** 130409 (2004).

Conclusion générale

L'ensemble du travail abordé dans ce manuscrit s'inscrit dans une thématique actuellement en pleine effervescence. Au niveau expérimental, de nombreux dispositifs sont en train de voir le jour, affichant des performances toujours plus élevées. Au niveau théorique, il y a encore actuellement une intense activité de recherche sur les protocoles ainsi que sur leurs preuves de sécurité. Il est délicat dans un tel contexte de tenter de conclure sur la viabilité de tel ou tel dispositif.

Nous avons développé dans notre équipe deux dispositifs pour la distribution quantique de clés secrètes. Le premier utilise le codage discret de l'information sur les états de polarisation de photons uniques. Son originalité réside dans la source de photons uniques que nous avons conçue.

Cette dernière utilise l'émission de fluorescence de centres individuels dans un cristal de diamant. Ses performances apportent clairement un avantage par rapport à une simple source cohérente atténuée utilisée dans les mêmes conditions. Il est clair que sa faible efficacité de collection peut constituer un handicap, mais cette efficacité peut être encore améliorée en travaillant sur les optiques de collection et de filtrage, ou en plaçant les nanocristaux de diamant dans des cavités pour canaliser leur émission de fluorescence.

Une autre limitation de cette source réside peut-être dans la durée de vie du niveau excité des centres que nous avons étudiés. Celle-ci limite le taux de répétition à $\approx$ 10 MHz, ce qui n'est certes pas négligeable. Mais la voie la plus directe pour augmenter le débit de clé secrète consiste à augmenter ce taux de répétition, et de nombreux groupes[30, 160, 74] travaillent maintenant sur des systèmes dépassant 1 GHz, annonçant déjà[160] des débits de clé secrète dépassant 100 kbits/s à travers 25 km de fibre optique. Ceci dit, nos collègues de l'ENS de Cachan, qui continuent de travailler sur cette expérience, ont mis en évidence[178] d'autres centres colorés du diamant qui ont une durée de vie plus courte, de l'ordre de 2 ns. Cette limitation semble donc pouvoir être contournée.

Le second dispositif que nous avons développé présente l'originalité de coder l'information sur des variables continues, à savoir les quadratures d'une impulsion lumineuse. Ce dispositif peut être intégré en utilisant les composants fibrés standards des télécommunications optiques, et permet d'atteindre des débits intéressants. Sur une distance de 25 km de fibre optique, nos résultats expérimentaux nous laissent ainsi attendre un débit de 1 kbit/s. Cette performance est tout-à-fait compétitive, puisqu'elle nous a permis d'être sélectionnés par le consortium européen SECOQC pour une implémentation grandeur nature de notre prototype. Il faut cependant souligner que notre principale limitation réside dans le temps de calcul des logiciels de réconciliation, et que l'on atteindrait un débit de 50 kbits/s sans cette limitation. Il faut également souligner que ce débit est annoncé pour un taux de répétition de 1 MHz seulement, et que nous pouvons raisonnablement envisager des cadences de 10 voire 100 MHz.

Ce procédé est donc très prometteur; il a la potentialité d'atteindre des débits très supérieurs à ceux des protocoles à variables discrètes, du moins sur des distances inférieures à une quarantaine de kilomètres. Notre dispositif est en effet moins robuste aux pertes que les protocoles à variables discrètes, ces derniers pouvant fonctionner sur une distance d'une centaine de kilomètres.

Pour augmenter la portée de notre dispositif de cryptographie à variables continues, nous avons décidé d'explorer la possibilité de réaliser des répéteurs quantiques. Notre objectif dans un premier temps n'est pas de mettre en œuvre une telle technologie, mais d'étudier la faisabilité des différentes opérations impliquées dans un tel projet.

Il est ainsi nécessaire de maîtriser la téléportation de variables continues en régime impulsionnel, ce qui implique une source d'états intriqués en quadratures qui soit très performante dans ce régime. Pour augmenter le niveau d'intrication après la traversée d'un canal de transmission, il est impératif de sortir du domaine gaussien, ce qui nous a conduit à explorer les opérations de dégaussification par préparation conditionnelle.

Nous avons déjà obtenu sur ces sujets de nombreux résultats intéressants. Il nous faudra maintenant améliorer globalement les performances de notre dispositif expérimental, en amplifiant par exemple les impulsions femtosecondes utilisées. Ce projet est soutenu par le réseau européen COVAQIAL, ainsi que par l'ANR à travers le projet IRCOQ.

Nous pourrons ainsi envisager des objectifs ambitieux, mais pas inaccessibles, tels la génération d'un chat de Schrödinger, ou la violation sans échappatoire d'inégalités de Bell. De tels résultats ne seraient pas sans lien avec la problématique de l'information quantique; un lien a ainsi été mis en évidence, du moins pour les variables discrètes, entre la violation des inégalités de Bell et la sécurité des protocoles de cryptographie[148] ou la performance de certains protocoles de communication[39]. Mais ces objectifs ont en eux-même un intérêt scientifique qui justifie que l'on s'y intéresse...

Informations complémentaires

Curriculum vitæ

Rosa BROURI épouse TUALLE
Née le 30 Juillet 1970
Mariée, 1 enfant
rosa.tualle-brouri@iota.u-psud.fr

depuis 2000	Maître de Conférences à l'IUT d'Orsay
1999-2000	CDD d'Enseignant-Chercheur à l'Institut d'Optique Théorique et Appliquée (Université Paris XI, Orsay)
1998-1999	Poste d'**ATER** à l'Ecole Normale Supérieure de Cachan
1997-1998	Poste d'**ATER** à mi-temps à l'université Paris 13
1995-1998	**Thèse de Doctorat** dans le groupe d'Interférométrie Atomique du Laboratoire de Physique des Lasers (Université Paris 13) soutenue le 30 Septembre 1998. titre: *Interaction d'atomes neutres métastables avec des ondes optiques évanes--centes : diffraction, interférences.*
1993-1994	**D.E.A.** "Lasers et Matière" (Université Paris XI, Orsay)

Activités d'enseignement

Depuis mon recrutement à l'IUT d'Orsay, en tant que Maître de Conférences, en Septembre 2000, j'enseigne essentiellement l'optique et l'optronique au département Mesures Physiques. J'ai notamment pris en charge la responsabilité de l'option " optronique " proposée en deuxième année de DUT, avec la conception d'un nouveau cours/TD et l'introduction de nouveaux TP.

Cette option a été le prélude à une option de licence MMIC (Métiers de la Mesure, de l'Instrumentation et de Contrôle) qui a ouvert en Septembre 2005. Je me suis beaucoup impliquée dans le dossier de demande d'habilitation à délivrer cette licence, avec la conception du programme de l'option optronique et la recherche de soutiens industriels. Je me suis occupée de la mise en place des enseignements de l'option optronique, à laquelle 200 heures d'enseignement sont consacrées, et j'ai moi-même assuré 90 de ces heures.

année scolaire (service)	enseignement	niveau
1997-1998 (96h)	TP d'électronique analogique	Licence d'électronique
	TD de mécanique du point	DEUG
1998-1999 (192h)	TP d'électronique	$1^{ère}$ année ENS Cachan
	Montages d'agrégation	
1999-2000 (192h)	TP d'électronique	$1^{ère}$ année ESO
	TP d'optique	$3^{ème}$ année ESO
	TP système	$3^{ème}$ année ESO
2000-2001 (192h)	TP et TD d'optique	DUT $1^{ère}$ et $2^{ème}$année
2001-2002 (192h)	TP et TD d'optique	DUT $1^{ère}$ et $2^{ème}$année
	TD traitement du signal	DUT $2^{ème}$année
2002-2003 (192h)	TD et TP d'optique géométrique et ondulatoire	DUT $1^{ère}$
	cours, TD et TP d'optique physique	DUT $2^{ème}$année
	cours, TD traitement du signal	DUT $2^{ème}$année
	cours, TD et TP d'optronique	DUT $2^{ème}$année
2003-2004 (192h)	TD et TP d'optique géométrique et ondulatoire	DUT $1^{ère}$
	cours, TD et TP d'optique physique	DUT $2^{ème}$année
	TD traitement du signal	DUT $2^{ème}$année
	cours, TD et TP d'optronique	DUT $2^{ème}$année
2004-2005 (192h)	cours d'optique géométique, TD et TP d'optique	DUT $1^{ère}$
	cours et TD d'optique physique	DUT $2^{ème}$année
	cours, TD et TP d'optronique	DUT $2^{ème}$année
2005-2006 (192h)	TP et TD d'optique	DUT $1^{ère}$année
	cours et TD d'optique physique	DUT $2^{ème}$année
	TD probabilités/statistiques	DUT $2^{ème}$année
	cours, TD et TP d'optronique	Licence MMIC

Expérience d'encadrement

stagiaires **DEA**	période	% encadrement
Alexios Beveratos	01/04/1999 - 30/06/1999	70%
Jérôme Wenger	01/04/2001 - 30/06/2001	80%
Mohammad Hafezi	01/04/2002 - 30/06/2002	50%
Jérôme Lodewyck	01/04/2003 - 30/06/2003	80%
Alexei Ourjoumtsev	01/04/2005 - 30/06/2005	80%
étudiants **Thèse**	période	% encadrement
Alexios Beveratos	01/09/1999 - 30/12/2002	45%
Frédéric Grosshans	01/09/1999 - 30/12/2002	50%
Jérôme Wenger	01/09/2001 - 30/09/2004	75%
Jérôme Lodewyck	Depuis le 01/09/2003	20%
Alexei Ourjoumtsev	Depuis le 01/09/2004	75%

Publications

Articles dans des revues avec comité de lecture

[P1] R. Brouri ,R. Asimov, M. Gorlicki, S. Feron, J. Reinhardt, V. Lorent et H. Haberland, Thermal atom beam splitting by an evanescent standing wave, *Optics Communications* **124** 448 (1996).

[P2] R. Brouri, F. de Tomasi , J. Robert, J. Baudon, J. Reinhardt, V. Lorent et M. Gorlicki, A Fresnel Bi-Prism Device for Atomic Matter Waves, *Optics Communications* **141** 329 (1997).

[P3] R. Mathevet, K. Brodsky, J. Baudon, R. Brouri, B. Viaris de Lesegno, et J. Robert, Double atom interferometer, *Phys. Rev. A* **58** (1998).

[P4] R. Brouri, A. Beveratos, J. P. Poizat, P. Grangier, Single photon generation by pulsed excitation of a single dipole, *Phys. Rev. A* **62**, 063814 (2000).

[P5] R. Brouri, A. Beveratos, J.-Ph. Poizat et P. Grangier, Photon antibunching in the fluorescence of individual color centers in diamond, *Opt. Lett.* **25**, 1294 (2000).

[P6] A. Beveratos, R. Brouri, T. Gagoin, J.P. Poizat et P. Grangier, Nonclassical radiation from diamond nanocrystals, *Phys. Rev. A* **64**, 061802 (2001).

[P7] A. Beveratos, S. Kühn, R. Brouri, T. Gagoin, J.P. Poizat et P. Grangier, Room temperature stable single photon source, *EPJ D* **18**, 191 (2002).

[P8] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, H.P. Poizat et P. Grangier, Single photon quantum cryptography, *Phys. Rev. Lett.* **89**, 187901 (2002).

[P9] 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).

[P10] 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).

[P11] 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).

[P12] 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).

[P13] J. Wenger, R. Tualle-Brouri et P. Grangier, Non-gaussian statistics from individual pulses of squeezed light, *Phys. Rev. Lett.* **92**, 153601 (2004).

[P14] 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, *Phys. Rev. Lett.* **93** 130409 (2004).

[P15] J. Wenger, J. Fiurášek, R. Tualle-Brouri, N.J. Cerf et P. Grangier, Pulsed squeezed vacuum characterization without homodyning, *Phys. Rev. A* **70** 053812 (2004).

[P16] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle et P. Grangier, Experimental open air quantum key distribution with a single photon source, *New J. Phys* **6**, 92 (2004).

[P17] J. Wenger, A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Time-resolved homodyne characterization of individual quadrature-entangled pulses, *Eur. Phys. J. D* **32** 391-396 (2005).

[P18] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, et P. Grangier, Controlling excess noise in fiber-optics continuous-variable quantum key distribution, *Phys. Rev. A* **72**, 050303 (2005).

[P19] T. Briant, P. Grangier, R. Tualle-Brouri, A. Bellemain, R. Brenot et B. Thédrez, Accurate Determination of the Noise Figure of Polarization-Dependent Optical Amplifiers: Theory and Experiment, *J. of Lightwave Tech. A* **24** (3), 1499 (2006).

[P20] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat et P. Grangier, Generating Optical Schrödinger Kittens for Quantum Information Processing, *Science* **312**, 83-86 (2006).

[P21] A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Quantum homodyne tomography of a two-photon Fock state, *Phys. Rev. Lett.* **96**, 213601 (2006).

Brevets

[P22] R. Brouri-Tualle, N.J. Cerf, P. Grangier, F. Grosshans, G. Van Assche, J. Wenger, *High-rate quantum key distribution relying on continuously phase- and amplitude-modulated coherent light pulses*, Regular US patent application filed on July 7, 2003 by Office Van Malderen as application serial number 10/615,490.

[P23] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, P. Grangier, *Système de distribution quantique de clé de cryptage à variables continues*, patent application n° FR 0413337 (2005).

Proceeding avec comité de lecture

[P24] A.Beveratos, R.Brouri, J.P. Poizat et P.Grangier, Bunching and antibunching from single NV color centers in diamond, *QCM&C 3 Proceedings (Kluver Academic/Plenum Publisher).*

Diffusion de l'information scientifique

[P25] Rosa Tualle-Brouri, Proposition expérimentale pour une violation sans échappatoire des inégalités de Bell, *Lumière* **20** (2005).

Communications dans des Congrès

[C1] **R.Brouri**, R.Asimov, M.Gorlicki, S.Feron, J.Reinhardt an V.Lorent, Second Meeting of the Young Atom Opticians, Oxford, (1996).

[C2] R.Brouri, F.de Tomasi, S.Feron, J.Reinhardt, **V.Lorent** and M.Gorlicki, III Workshop "Optics and Interfermetry With Atom", Marciana Marina(Elba Island, Italy) (1996).

[C3] **R. Brouri**, A. Beveratos, J-Ph. Poizat, et Ph. Grangier, GDR Information quantique (2000)

[C4] A. Beveratos, R. Brouri, J-Ph. Poizat, et **Ph. Grangier**, International conference on quantum information, measurement and computing, QCM&C Capri 2000.

[C5] R. Brouri, A. Beveratos, **J-Ph. Poizat**, et Ph. Grangier, IQEC 2000 (Nice) (invité)

[C6] **R. Brouri**, A. Beveratos, J-Ph. Poizat, et Ph. Grangier, Colloque Buissy, Orsay (2001)

[C7] **R. Brouri**, A. Beveratos, J.-Ph. Poizat, and P. Grangier, Euroconference QUICK, 7-12 avril 2001, Cargèse.

[C8] **A. Beveratos**, S. Kühn , R. Brouri, T. Gacoin, J.-Ph Poizat and P. Grangier, CLEO/Europe-EQEC Quantum Information and communications Munich (June 2001).

[C9] **Frédéric Grosshans**, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and Philippe Grangier " Quantum cryptography with coherent states " , ESF workshop on Continuous Variable Quantum Information Processing (CVQIP'02), Brussels, Apr. 5-8, 2002.

[C10] J. P. Poizat, A. Beveratos, R. Brouri, and **P. Grangier**, " Quantum Cryptography using single photons on demand ", JST Meeting, Paris, 19-21 juin 2002.

[C11] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, **P. Grangier**, "Quantum key distribution using modulated coherent states", QCMC conference, Boston, (2002).

[C12] **Frédéric Grosshans**, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and Philippe Grangier, Cryptographie quantique à haut débit avec des états cohérents, 2nd meeting of the french GdR Information et Communication Quantiques, Les Houches, May 21-23, 2003.

[C13] **Frédéric Grosshans**, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and Philippe Grangier, "Quantum key cryptography with coherent states", Plenary meeting of the belgian IAP-PHOTON project, Ghent University, May 7, 2003.

[C14] Frédéric Grosshans, Gilles Van Assche, Jérôme, Wenger, Rosa Brouri, **Nicolas J. Cerf** and Philippe Grangier, "Quantum cryptography with continuous variables", 3rd International Workshop of Classical and Quantum Interference, Research center for Optics, Olomouc, Czech Republic, Oct.23-24, 2003.(Invité)

[C15] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J.Cerf and **Philippe Grangier**, "High bit rate quantum key distribution using coherent states", École d'été des Houches, Jul. 20-25, 2003. (Invité)

[C16] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and **Philippe Grangier**, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables", QIPC Oxford, "Hot Topics" session, Jul. 13-17, 2003 (Invité).

[C17] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf and **Philippe Grangier**, "High rate quantum key distribution using Gaussian-modulated coherent states", 2nd ESF workshop on Continuous Variable Quantum Information Processing (CVQIP'03), Aix-en-Provence, Apr. 11-13, 2003. (Invité)

[C18] J. Wenger, M. Hafezi, F. Grosshans, **R. Tualle-Brouri** et Ph. Grangier. "Maximal violation of Bell inequalities using continuous variable measurements", Continuous Variables Quantum Information Processing, 2003 Workshop, Aix en Provence 11-14 April 2003.

[C19] J. Wenger, R. Tualle-Brouri et **P. Grangier**."Non gaussian statistics from individual pulses of squeezed light CLEO/IQEC, San Francisco, California, USA, 16-21 Mai 2004.(invité)

[C20] Frédéric Grosshans , Jérome Wenger , Alexei Ourjoumtsev , Rosa Tualle-Brouri , Gilles Van Assche, Raul Sanchez, Jaromir Fiurášek, Nicolas Cerf , and **Philippe Grangier**, "Non-Gaussian statistics and entanglement using femtosecond pulses of squeezed light", Conférence "Quantum Optics", Olomouc 20-24 octobre (2004).(invité)

[C21] **G. Messin** , A. Beveratos, J.-P. Poizat, R. Tualle-Brouri, P. Grangier (Institut d'Optique), R. Alleaume, Y. Dumeige, F. Treussart, J.-F. Roch (ENS Cachan)." Experimental open air quantum cryptography with single photons Post-deadline paper, communication effectuée lors de l' "International Quantum Electronics Conference (CLEO/IQEC)", en mai 2004, à San Francisco, USA.

[C22] J. Wenger, **R. Tualle-Brouri** et P. Grangier, "Non-gaussian statistics from individual pulses of squeezed light", 3nd ESF workshop on Continuous Variable Quantum Information Processing (CVQIP'04), Veilbronn 2-5 April 2004.(invité)

[C23] Frédéric Grosshans, Jérome Wenger, Rosa Tualle-Brouri, Gilles Van Assche, Raul Patron-Sanchez, Jaromir Fiurášek, Nicolas Cerf, and **Philippe Grangier**, "Key distribution and non-gaussian statistics with quantum continuous variables", Ecole d'été Cargèse 16-29 aout 2004 (invité).

[C24] **J. Wenger**, R. Tualle-Brouri et P. Grangier. "Non-Gaussian statistics from individual pulses of squeezed light". Latsis symposium on quantum communication and computing, Lausanne (Suisse), 2004.

[C25] J. Wenger, **R. Tualle-Brouri** et P. Grangier, "Non-Gaussian statistics from individual pulses of squeezed light", the seventh International Conference on Quantum Communication, Measurement and Computing", Glasgow, 24-29 july 2004.

Bibliographie

[1] A. Acin, N. Gisin et L. Masanes, Equivalence between two-qubit entanglement and secure key distribution, *Phys. Rev. Lett.* **91**, 167901 (2003).

[2] G. Adam, Density matrix elements and moments for generalized Gaussian state fields, *J. Mod. Opt.* **42**, 1311 (1995).

[3] 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).

[4] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle et P. Grangier, Experimental open air quantum key distribution with a single photon source, *New J. Phys* **6**, 92 (2004).

[5] R. Alléaume, *Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique*, Thèse, Université Paris 6 (2004).

[6] 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).

[7] A. Aspect, P. Grangier, et G. Roger, Experimental Tests of Realistic Local Theories via Bell's Theorem, *Phys. Rev. Lett.* **47**, 460 (1981).

[8] 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).

[9] A. Aspect, J. Dalibard, et G. Roger, Experimental Test of Bell's Inequalities Using Time- Varying Analyzers, *Phys. Rev. Lett.* **49**, 1804 (1982).

[10] 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).

[11] H.A. Bachor, *A guide to experiments in quantum optics*, Wiley-VCH, Weinheim (1998).

[12] H.Barnum, C.M. Caves, C.A. Fuchs, R. Jozsa et B. Schumacher, Noncommuting mixed states cannot be broadcast,*Phys. Rev. Lett.* **76**(15), 2828 (1996).

[13] Th. Bashé, W.E. Moerner, M. Orrit, et H. Talon, Photon antibunching in the fluorescence of a single dye molecule trapped in a solid, *Phys. Rev. Lett.* **69**, 1516 (1992).

[14] G. Battail, *Théorie de l'information – Application aux techniques de communication*, Masson, Paris (1997).

[15] J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, 1988.

[16] K. Bencheikh, T. Symul, A. Jankovic et J.A. Levenson, Quantum key distribution with continuous variables, *J. Mod. Optics* **48**, 1903 (2001).

[17] 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).

[18] C.H. Bennett, G. Brassard et J.-M. Robert, Privacy amplification by public discussion, *SIAM Journal on Computing* **17** (2), 210-229 (1988).

[19] C.H. Bennett, F.Bessette, G. Brassard, L. Salvail, et J. Smolin, Experimental Quantum Cryptography, *J. of Cryptology* **5**,3 (1992).

[20] C.H. Bennett, Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).

[21] C.H. Bennett, G. Brassard, C. Crépeau et U.M. Maurer, Generalized privacy amplification, *IEEE Trans. Inform. Theory* **41**, 1915 (1995).

[22] 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.

[23] D.S. Bethune et W.P. Risk, An autocompensating fiber-optic quantum cryptography system based on polarisation splitting of light, *IEEE Journal of Quantum Electronics***36**, 340-347 (2000).

[24] R. Brouri, A. Beveratos, J.-Ph. Poizat et P. Grangier, Photon antibunching in the fluorescence of individual color centers in diamond, *Opt. Lett.* **25**, 1294 (2000).

[25] A.Beveratos, R.Brouri, J.P. Poizat et P.Grangier, Bunching and antibunching from single NV color centers in diamond, *QCM&C 3 Proceedings (Kluver Academic/Plenum Publisher).*

[26] A.Beveratos, R.Brouri, T.Gagoin, J.P. Poizat et P.Grangier, Nonclassical radiation from diamond nanocrystals, *Phys. Rev. A* **64**, 061802 (2001).

[27] A.Beveratos, S.Kühn, R.Brouri, T.Gagoin, J.P. Poizat et P.Grangier, Room temperature stable single photon source, *EPJ D* **18**, 191 (2002).

[28] A.Beveratos, R.Brouri, T.Gacoin, A.Villing, H.P.Poizat et P.Grangier, Single photon quantum cryptography, *Phys. Rev. Lett.* **89**, 187901 (2002).

[29] A.Beveratos, *Réalisation expérimentale d'une source de photons uniques par fluorescence de centres colorés dans le diamant; application à la cryptographie quantique.*, Thèse, Université Paris-Sud 11, (Orsay, 2002).

[30] J.C. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley et J. Wen, Quantum key distribution with 1.25Gbps clock synchronization, *Optics Express***12**, 2011-2016 (2004).

[31] E. Biham, M. Boyer, P.O. Boykin, T. Mor et V. Roychowdhury, A proof of the security of quantum key distribution, *quant-ph/9912053* (1999).

[32] M. Bloch, A. Thangaraj et S. McLaughlin, *e-print arxiv/cs.IT/0509041.*

[33] D. Bouwmeester, A. Ekert et A. Zeilinger (Eds.), *The physics of quantum information*, Springer, Berlin (2000).

[34] 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).

[35] G. Brassard, N. Lütkenhaus, T. Mor, et B. Sanders, *e-print quant-ph/9911054*

[36] R. Brouri, A. Beveratos, J. P. Poizat, P. Grangier, Single photon generation by pulsed excitation of a single dipole, *Phys. Rev. A* **62**, 063814 (2000).

[37] R. Brouri-Tualle, N.J. Cerf, P. Grangier, F. Grosshans, G. Van Assche, J. Wenger, *High-rate quantum key distribution relying on continuously phase- and amplitude-modulated coherent light pulses*, Regular US patent application filed on July 7, 2003 by Office Van Malderen as application serial number 10/615,490.

[38] 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).

[39] C. Brukner, M. Zukowski, J.-W. Pan et A. Zeilinger, Violation of Bell's inequality: criterion for quantum communication complexity advantage, *Phys. Rev. Lett.* **92**, 127901 (2004).

[40] C. Brunel, B. Lounis, P. Tamarat, et M. Orrit, Triggered source of single photons based on controlled single molecule fluorescence, *Phys. Rev. Lett.* **83**, 2722 (1999).

[41] W. Buttler, R. Hughes, S. Lamoreaux, G. Morgan, J. Nordholt et C. Peterson, Daylight Quantum Key Distribution over 1.6km, *Phys. Rev. Lett.***84**, 5652 (2000).

[42] A.R. Calderbank and P. Shor, *Phys. Rev. A* **54**, 1098-1105 (1996); A.M. Steane, Proc. R. Soc. London A **452**, 2551-2577 (1996).

[43] J.L. Carter et M.N. Wegman, Universal classes of hash functions, textitJournal of Computer and System Sciences textbf18, 143-154 (1979)

[44] N.J. Cerf, M. Lévy et G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, *Phys. Rev. A* **63**, 052311 (2001).

[45] N.J. Cerf, S. Iblisdir et G. Van Assche, Cloning and cryptography with quantum continuous variables, *Eur. Phys. J. D* **18**, 211 (2002).

[46] N.J. Cerf et R. Garcia-Patron, *Gaussian, or not Gaussian: that is the question*, CVQIP 06, Copenhague (mai 2006).

[47] 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).

[48] J. F. Clauser et M. A. Horne, Experimental consequences of objective local theories, *Phys. Rev. D* **10**, 526 (1974).

[49] A. Collins, M. Thomaz et M. Jorge, Luminescence decay time of the 1.945 eV center in type Ib diamond, *J. Phys. C* **16**, 2177 (1983).

[50] I. Csiszár et J. Körner, Broadcast channel with confidential messages, *IEEE Trans. Inform. Theory* **24**, 339 (1978).

[51] M. Curty, M. Lewenstein et N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, *Phys. Rev. Lett.* **92** (21), 217902 (2004).

[52] 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).

[53] 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).

[54] I. Devetak et A. Winter, Distillation of secret key and entanglement from quantum states, *Phys. Rev. Lett.* **93**, 080501 (2004).

[55] F. Diedrich, H. Walter, Nonclassical radiation of a single stored ion, *Phys. Rev. Lett.* **58**, 203 (1987).

[56] D. Dieks, Communication by EPR devices, *Phys. Rev. A* **92**(6), 271-272 (1982)

[57] V.G Dmitriev, G.G. Gurzadyan et D.N. Nikogosyan, *Handbook of nonlinear optical crystals*, 3e édition, Springer, Berlin (1999).

[58] 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).

[59] L.M. Duan, G. Giedke, J.I. Cirac et P. Zoller, Inseparability criterion for continuous variable systems, *Phys. Rev. Lett.* **84**, 2722 (2000).

[60] A.K. Ekert, Quantum cryptography based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).

[61] A. Einstein, B. Poldolsky et N. Rosen, Can quantum mechanical description of physical reality be considered complete ?, *Phys. Rev.* **47**, 777 (1935).

[62] J. Eisert, S. Scheel et M.B. Plenio, Distilling Gaussian states with Gaussian operations is impossible, *Phys. Rev. Lett.* **89**, 137903 (2002).

[63] J. Eisert et M.B. Plenio, Introduction to the basics of entanglement theory in continuous-variable systems, *Int. J. Quant. Inf.* **1**, 479 (2003).

[64] J. Fiurášek et N.J. Cerf, How to measure squeezing and entanglement of gaussian states without homodyning, *Phys. Rev. Lett.* **93**, 063601 (2004).

[65] J.D. Franson et B. Jacobs, Operational system for quantum cryptography, *Electronics Letters* **31**, 232-234 (1995).

[66] J.D. Franson et B. Jacobs, Quantum cryptography in free space, *Optics Letters* **21**, 1854-1856 (1996).

[67] A. Furusawa, J. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble et E. Polzik, Unconditionnal quantum teleportation, *Science* **282**, 706 (1998).

[68] 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, *Phys. Rev. Lett.* **93** 130409 (2004).

[69] G. Giedke et J.I. Cirac, Characterization of Gaussian operations and distillation of Gaussian states, *Phys. Rev. A* **66**, 032316 (2002).

[70] 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).

[71] N. Gisin et B. Gisin, A local hidden variable model of quantum correlation exploiting the detection loophole, *Phys. Lett. A* **260**, 323 (1999).

[72] N. Gisin, G. Ribordy, W. Tittel et H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

[73] C. Gobby, Z.L. YUAN et A.J. Shield, Quantum key distribution over 122km of standard telecom fiber, *Appl. Phys. Lett.***84**(19), 3762 (2004).

[74] K.J. Gordon, V. Fernandez, R.J. Collins, I. Rech, S.D. Cova, P.D. Townsend et G.S. Buller, 3.3 gigahertz clocked quantum key distribution system, *ECOC 2005, 31st European Conference,* **4**, 913 (2005).

[75] D. Gottesman et J. Preskill, Secure quantum key distribution using squeezed states, *Phys. Rev. A* **63**, 022309 (2001).

[76] P. Grangier, *Etude expérimentale de propriétés non-classiques de la lumière : interférence à un seul photon.* , Thèse, Université Paris-Sud 11 (Orsay).

[77] 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).

[78] F. Grosshans et Ph. Grangier, No-cloning theorem and teleportation criteria for quantum continuous variables, *Phys. Rev. A* **64**, 010301(R) (2001).

[79] F. Grosshans et Ph. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).

[80] F. Grosshans, *Communication et cryptographie quantiques avec des variables continues*, Thèse, Université Paris-Sud 11 (2002).

[81] 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).

[82] 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).

[83] 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.

[84] F. Grosshans et N.J. Cerf, Security of continuous-variable quantum cryptography against non-gaussian attacks, *Phys. Rev. Lett.* **92**, 047905 (2004).

[85] F. Grosshans, Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 020504 (2005).

[86] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup et C. von Borczyskowki, Scanning confocal optical microscopy and magnetic resonance on single defect centers, *Science* **276**, 2012 (1997).

[87] G. Grynberg, A. Aspect et C. Fabre, *Introduction aux lasers et à l'optique non-linéaire*, Ellipses, Paris (1997).

[88] M.J.W. Hall, Information excusion principle for complementary observables, *Phys. Rev. Lett.* **74**,3307-3310 (1995).

[89] R. Hanbury Brown et R.Q. Twiss, Correlation between photons in two coherent beams of light, *Nature* **177**, 22 (1956).

[90] H. Hansen, *Generation and characterization of new quantum states of the light field.* , Thèse, Universität Konstanz, Allemagne (2000).

[91] 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).

[92] M. Hillery, Quantum cryptography with squeezed states, *Phys. Rev. A* **61**, 022309 (2000).

[93] R.J. Hughes, J.E. Nordholt, D. Derkacs, C.G. Peterson, Practical free-space quantum key distribution over 10km in daylight and at night, *New Journal of Physics***4**, 43.1-43.14 (2002).

[94] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).

[95] idQuantique SA (Genève, Suisse), http://www.idquantique.com

[96] C. Kim et P. Kumar, Quadrature-squeezed light detection using a self-generated matched local oscillator, *Phys. Rev. Lett.* **73**, 1605 (1994).

[97] H.J. Kimble, M. Dagenais, L. Mandel, Photon Antibunching in Resonance Fluorescence, *Phys. Rev. Lett.* **39**, 691 (1977).

[98] S. C. Kitson, P. Jonsson, J. G. Rarity, et P. R. Tapster, Intensity fluctuation spectroscopy of small numbers of dye molecules in a microcavity, *Phys. Rev. A* **58**, 620 (1998).

[99] P. Kumar, O. Aytur et J. Huang, Squeezed light generation with an incoherent pump, *Phys. Rev. Lett.* **64**, 1015 (1990).

[100] C. Kurtsiefer, P. Zarda, M. Hanlder, H. Weinfurter, P.M. Gorman, P.R. Tapster et J.G. Rarity, Quantum cryptography; A step towards global key distribution, *Nature* **419**,450 (2002).

[101] A. Laporta et R.E. Slusher, Squeezing limits at high parametric gain, *Phys. Rev. A* **44**, 2013 (1991).

[102] 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).

[103] 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).

[104] U. Leonhardt, *Measuring the quantum state of light*, Cambridge University Press, Cambridge, (1997).

[105] H.-K. Lo et H.F. Chau, Unconditionnal security of quantum key distribution over arbitrary long distances, *Science* **283**, 2050-2056 (1999).

[106] H.-K. Lo, Method for decoupling error correction from privacy amplification, arXiv quant-ph/ 0201030 (2002).

[107] H.-K. Lo, X. Ma et K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).

[108] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, P. Grangier, *Système de distribution quantique de clé de cryptage à variables continues*, patent application n° FR 0413337 (2005).

[109] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, et P. Grangier, Controlling excess noise in fiber-optics continuous-variable quantum key distribution, *Phys. Rev. A* **72**, 050303 (2005).

[110] S. Lorenz, N. Korolkova, G. Leuchs, Continuous-variable quantum key distribution using polarization encoding and post selection, *Appl. Phys. B* **79**, 273-277 (2004).

[111] 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).

[112] N. Lütkenhaus, Estimates for practical quantum cryptography, *Phys. Rev. A* **59**(5), 3301-3319 (1999).

[113] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, *Phys. Rev. A* **61**, 052304-1-10 (1999).

[114] 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).

[115] A.I. Lvovsky, Iterative maximum-likelihood reconstruction in quantum homodyne tomography, arXiv quant-ph/0311097 (2003).

[116] MAGIQ, http://www.magiqtech.com (1999).

[117] L. Mandel et E. Wolf, *Optical coherence and quantum optics*, Cambridge University Press, Cambridge (1995).

[118] U.M. Maurer, Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory* **39**, 733 (1993).

[119] U. Maurer et S. Wolf, Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free, in *Advances in Cryptology-Eurocrypt 2000, Lecture Notes in Computer Science*, B. Preneel, p.351 (2000).

[120] D. Mayers, Quantum key distribution and string oblivious transfer in noisy channels, *Advances in Cryptology-Proceedings of Crypto '96*, Springer-Verlag, 343-357 (1996).

[121] D. Mayers, Unconditional security in quantum cryptography, textitquant-ph/9802025 (1998).

[122] P. Michler, A. Imamoğlu, M.D. Mason, P.J. Carson, G.F. Strouse, S.K. Buratto, Quantum correlation among photons from a single CdSe quantum dot at room temperature, *Nature* **406**, 968 (2000).

[123] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden et N. Gisin, "Plug and play" systems for quantum cryptography, *Applied Physics Letters* **70**, 793-795 (1997).

[124] W. J. Munro, Optimal states for Bell inequality violations using quadrature-phase homodyne measurements, *Phys. Rev. A* **59**, 4197 (1999).

[125] M. Navascués and A. Acín, Security Bounds for Continuous Variables Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 020505 (2005).

[126] M. Navascués, F. Grosshans and A. Acín, Key Rates for Continuous Variables Quantum Key Distribution protocols, *to be submitted* (2005).

[127] K. Nguyen, *Extension des Protocoles de Réconciliation en Cryptographie Quantique*, rapport de stage, Univ. Libre de Bruxelles (2002).

[128] 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*.

[129] M.A. Nielsen et I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge (2000).

[130] P.M. Nielsen, C. Schori, J.L. Sorensen, L. Salvail, I. Damgard, et E. Polzik, *J. Mod. Opt.* **48**, 1921 (2001); http://www.cki.au.dk/experiment/qrypto/doc/

[131] 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).

[132] 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).

[133] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat et P. Grangier, Generating Optical Schrödinger Kittens for Quantum Information Processing, *Science* **312**, 83-86 (2006).

[134] A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Quantum homodyne tomography of a two-photon Fock state, *Phys. Rev. Lett.* **96**, 213601 (2006).

[135] 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).

[136] Philip M. Pearle, Hidden-Variable Example Based upon Data Rejection, *Phys. Rev. D* **2**, 1418 (1970).

[137] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht (1997).

[138] T.C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* **61**, 010303(R) (2000).

[139] T.C. Ralph, Security of continuous-variable quantum cryptography, *Phys. Rev. A* **62**, 062306 (2000).

[140] J. Rarity, P. Tapster, P. Gorman et P. Knight, Ground to satellite secure key exchange using quantum cryptography, *New Journal of Physics* **4** 82 (2002).

[141] J. Rehacek, Z. Hradil et M. Jesek, Iterative algorithm for reconstruction of entangled states, *Phys. Rev. A* **63**, 040303 (2001).

[142] M.D. Reid, Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification, *Phys. Rev. A* **40**, 913 (1989).

[143] M.D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, *Phys. Rev. A* **62**, 062308 (2000).

[144] R. Renner and R. König, Universally Composable Privacy Amplification Against Quantum Adversaries, arXiv:quant-ph/0403133v2 (2004).

[145] R. Renner, Security of Quantum Key Distribution, arXiv:quant-ph/0512258v2, Thèse, Swiss Federal Institute of Technology, Zurich (2006).

[146] R.L. Rivest, A. Shamir et L.M. Adleman, A method of obtaining digital signatures and public-key cryptosystems, *Comm. ACM* **21**(2),120-126 (1978).

[147] 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).

[148] V. Scarani et N. Gisin, Quantum Communication between N-partners and BellŠs Inequalities, *Phys. Rev. Lett.* **87**, 117901 (2001).

[149] C.E. Shannon, A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 623-656 (1948).

[150] Y.R. Shen, *Principles of nonlinear optics*, Wiley Classics Library, New York (1983).

[151] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J.Comp.* **26**(5),1484-1509 (1997).

[152] P.W. Shor et J. Preskill, Simple proof of security of the $BB84$ Quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441-444 (2000).

[153] 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).

[154] C. Silberhorn, N. Korolkova, et G. Leuchs, Quantum key distribution with bright entangled beams, *Phys. Rev. Lett.* **88**, 167902 (2002).

[155] 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).

[156] R. Simon, Peres-Horodecki separability criterion for continuous variable systems, *Phys. Rev. Lett.* **84**, 2726 (2000).

[157] 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).

[158] R.E. Slusher, P. Grangier, A. LaPorta, B. Yurke et M.J. Potasek, Pulsed squeezed light, *Phys. Rev. Lett.* **59**, 2566 (1987).

[159] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy et H. Zbinden, Quantum key distribution over 67km with a plug&play system, *New Journal of Physics* **4**, 41.1-41.8 (2002).

[160] R.T. Thew, S. Tanzilli, L. Krainer, S.C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden et N. Gisin, GHz QKD at telecom wavelengths using up-conversion detectors, *arXiv:quant-ph/0512054v1* (2005).

[161] P.D. Townsend, J.G. Rarity et P.R. Tapster, Enhance single photon fringe visibility in a 10km-long prototype quantum cryptography channel, *Elec. Lett.* **29**, 1291 (1993).

[162] F. Treussart, V. Jacques, E. Wu, T. Gacoin, P. Grangier et J.-F. Roch, Photoluminescence of single colour defects in 50nm diamond nanocrystals, *arXiv:cond-mat/0509512v1* (2005).

[163] 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).

[164] G. Van Assche, S. Iblisdir et N.J. Cerf, Secure Coherent-state Quantum Key Distribution Protocols with Efficient Reconciliation, arXiv:quant-ph/0410031v1 (2004).

[165] G. Van Assche, *Information-Theoretic Aspects of Quantum Key Distribution*, Thèse, Univ. Libre de Bruxelles (2005).

[166] G. Van Assche, communication personnelle.

[167] D.F. Walls et G.J. Milburn, *Quantum Optics*, Springer, Berlin (1994).

[168] X.-B. Wang, Beating the PNS attack in practical quantum cryptography, *arXiv:quant-ph/0410075v5* (2005).

[169] M.N. Wegman et J.L. Carter, New hash functions and their use in authentification and set equality, *Journal of Computer and System Sciences* **22**, 265-279 (1981).

[170] 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).

[171] 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).

[172] 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).

[173] J. Wenger, J. Fiurášek, R. Tualle-Brouri, N.J. Cerf et P. Grangier, Pulsed squeezed vacuum characterization without homodyning, *Phys. Rev. A* **70** 053812 (2004).

[174] J. Wenger, R. Tualle-Brouri et P. Grangier, Non-gaussian statistics from individual pulses of squeezed light, *Phys. Rev. Lett.* **92**, 153601 (2004).

[175] J. Wenger, *Dispositifs impulsionnels pour la communication quantique à variables continues*, Thèse, Université Paris-Sud 11 (2004).

[176] J. Wenger, A. Ourjoumtsev, R. Tualle-Brouri et P. Grangier, Time-resolved homodyne characterization of individual quadrature-entangled pulses, *Eur. Phys. J. D* **32** 391-396 (2005).

[177] W.K. Wooters, Entanglement of formation and concurrence, *Quantum. Inf. Comput.* **1**, 27 (2001).

[178] E. Wu, V. Jacques, F. Treussart, H. Zeng, P. Grangier et J.-F. Roch, Single-photon emission in the near infrared from diamond colour centre, *arXiv:cond-mat/0509516* (2005).

[179] 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).

[180] W.K. Wooters et W.H. Zurek, A single quantum state cannot be cloned, *Nature* **299**, 802 (1982).