Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique

Romain Alleaume

Laboratoire de Photonique Quantique et Moléculaire

École Normale Supérieure de Cachan

Université Pierre et Marie Curie

Thèse de doctorat de l'Université Paris VI

Spécialité : Physique Quantique

présentée et soutenue publiquement par

Romain ALLÉAUME

Pour obtenir le grade de
Docteur de l'Université PARIS VI

Le 30 Novembre 2004

Sujet :

RÉALISATION EXPÉRIMENTALE DE SOURCES DE PHOTONS UNIQUES, CARACTÉRISATION ET APPLICATION À LA CRYPTOGRAPHIE QUANTIQUE

devant le jury composé de :

M. Jean-François ROCH ..... *Directeur de thèse*
M. Brahim LOUNIS ..... *Rapporteur*
M. Juan-Ariel LEVENSON ..... *Rapporteur*
M. Philippe GRANGIER ..... *Examinateur*
M. François TREUSSART ..... *Examinateur*
M. Jean-Michel RAIMOND ..... *Examinateur*
M. Alexei TRIFONOV ..... *Membre invité*

Table des matières

Remerciements

J'ai effectuée ma thèse au Laboratoire de Photonique Quantique et Moléculaire de l'ENS Cachan. Je remercie Monsieur Joseph ZYSS, directeur du laboratoire, de m'y avoir accueilli.

Pour mener ce travail à son terme, j'ai bénéficié d'un aménagement de scolarité auprès du Corps des Télécommunications durant les deux dernières années de ma thèse. Je remercie Marc OBERLÉ, ainsi que les responsables de la formation initiale à Télécom Paris, de rendre ce cursus possible. Je remercie également Jean-Michel RAIMOND qui m'a fait l'honneur de présider mon jury de thèse, ainsi qu' Ariel LEVENSON et Brahim LOUNIS qui ont acceptés d'être rapporteurs de ce travail.

C'est bien sûr à Jean-François ROCH que je souhaite présenter mes plus vifs remerciements pour avoir dirigé ma thèse et lui présenter l'expression de ma profonde gratitude pour la façon dont il l'a fait. Manifestant une attention quotidienne aux progrès comme aux éventuelles difficultés qui se sont présentées, Jean-François a été un directeur de thèse extrêmement présent et disponible, tout en me laissant une grande liberté d'initiative et de choix. J'ai été très sensible aux rapports de confiance qu'il sait instaurer ainsi qu'a sa générosité humaine. L'atmosphère conviviale qui en découle rend le travail dans son équipe formidablement agréable et motivant. Jean-François est de plus un physicien d'une grande culture, avec une vision personnelle toujours éclairante et souvent enthousiaste des questions sur lesquelles nous nous sommes penchées. Sa façon, calme et réfléchie d'aborder les problèmes, son grand sens de la pédagogie ont constitué des repères essentiels au cours de ma thèse, et, je l'espère, m'inspireront dans mon début de carrière scientifique. Enfin, que ce soit pour avoir envisagé avec compréhension et humour ma facheuse tendance à revenir blessé des matchs de rugby, pour ses conseils scientifiques et extra-scientifiques toujours précieux - surtout quand arrivent les angoisses de la fin de la thèse - ou pour son soutien sans faille lors ces inoubliables nuits passées sur le plateau d'Orsay à s'envoyer des photons uniques, c'est aussi pour son optimisme communicatif que je souhaite le remercier.

Je tiens également à remercier François TREUSSART qui a très activement encadré ma thèse et avec lequel bon nombre des expériences décrites dans ce manuscrit ont été réalisées. La grande maîtrise expérimentale de François, alliée à son sens de l'organisation restera pour moi un exemple. J'avoue même que lors des premières semaines de travail en commun, son énergie et son efficacité me fit si forte impression que je me demandais comment être utile à mon tour ! Le dévouement, la fiabilité, mais également la personnalité extrêmement sympathique de François m'a cependant mis à l'aise et permis de trouver mes marques rapidement. J'ai énormément apprécié le travail avec lui et je crois avoir beaucoup appris à ses côtés. Je garde notamment d'excellents souvenirs des longs mais souvent ludiques moments passés à aligner l'expérience pour finalement réussir à apprivoiser ensemble les éphémères lueurs émises par nos molécules fluorescentes. Un grand merci donc, pour ces photons mais surtout pour tout le reste !

L'arrivée de Yannick DUMEIGE dans l'équipe fut une grande chance et le travail effectué en commun sur les émetteurs en cavité un réel plaisir. Alors même qu'il effectuait également une importante charge d'enseignement en tant qu' ATER, son implication fut extrêmement précieuse et fructueuse. Je tiens à le remercier pour l'excellente atmosphère de ces moment passés ensemble et lui souhaite beaucoup de succès dans son nouveau poste.

Je voudrais aussi à remercier sincèrement Véronique LE FLOC'H qui avait grandement avancé « la chasse aux molécules » lors de son stage de DEA, pour les conseils et les informations échangées tout aux long de nos thèses, et pour la cohabitation agréable sur l'expérience.

La venue de Vincent JACQUES au laboratoire lors de son stage de maîtrise nous a permis de travailler ensemble, dans une atmosphère chaleureuse et amicale dont je voudrais le remercier. Je lui souhaite beaucoup de réussite pour sa thèse, pour laquelle je suis persuadé que son énergie et sa créativité feront merveille.

Je remercie Jean-Michel COURTY pour son coup de main efficace concernant les analyses de la statistique d'émission des molécules uniques ainsi pour ses conseils et sa bonne humeur.

Je voudrais aussi remercier André CLOUQUEUR pour ses réalisation de circuits électroniques ainsi que Jean-Pierre MADRANGE, pour avoir assuré avec une grande compétence la réalisation de pièces mécaniques pour nos expériences.

Les échanges fréquents avec Philippe GRANGIER et son équipe ont considérablement enrichi cette thèse. Je tiens à le remercier pour l'intérêt qu'il a porté à ce travail et pour la collaboration qu'il nous a proposé, ainsi que pour ses nombreux conseils. Je lui suis également très reconnaissant pour ses interventions stimulantes, mêlant exigence, inventivité et passion scientifique, tout au long de ces trois années, depuis le moment où j'ai poussé la porte de son bureau durant mon DEA, et où il m'orienta vers le groupe de Jean-François ROCH, jusqu'à sa participation à mon jury de thèse.

Un grand merci bien sûr également à Alexios BEVERATOS pour m'avoir formé aux « arcanes de la manip diamant » et pour tous les échanges durant nos thèses respectives qui ont été une grande source de motivation et d'idées. Je tiens aussi à remercier Alexios pour ses conseils et son aide extrêmement précieuse alors que nous prenions sa relève sur le dispositif de cryptographie quantique.

Merci à Isabelle LEDOUX pour nous avoir prêté pendant plusieurs mois une grande place dans sa salle de manip, afin d'y déménager le montage installé initialement à l'Institut d'Optique.

J'ai travaillé durant quatre mois dans le laboratoire de l'entreprise MagiQ, et je tiens à remercier Alexei TRIFONOV pour son accueil et de sa disponibilité à mon égard. Ses grandes connaissances en information quantique ont rendu passionnant les discussions et le travail effectué sous sa supervision. J'ai par ailleurs eu la chance de travailler aux côtés de Darius SUBACIUS et d'Anton ZAVRIYEV, dont les compétences en optique fibrée et en photodétection ont été très utiles, et tiens à les remercier pour l'ambiance de travail chaleureuse ainsi que l'atmosphère inoubliable des repas partagés ensemble et des discussions qui les animaient.

Je voudrais enfin remercier mes proches pour avoir écouté avec patience et amusement mes histoires de photons uniques avant de les voir se muer en d'étranges communications entre Alice et Bob. Je remercie enfin du fond du coeur mes parents pour toute l'aide et le soutien qu'ils m'ont apporté durant mes études.

Chapitre 1

Introduction

Du photon unique aux communications quantiques

Les réflexions sur la nature de la lumière et l'introduction de la quantification du rayonnement sont aux origines même de l'élaboration de la physique quantique. C'est en effet en cherchant à expliquer l'effet photoélectrique et le caractère discret des échanges d'énergie entre le rayonnement et un métal conducteur, qu'Albert EINSTEIN fit en 1905 l'hypothèse des quantas de lumière [1]. Les succès et les découvertes expérimentales liés à la théorie quantique ont été considérables dès les années 1920[2, 3] mais, cette théorie, dont les prédictions n'ont cessées d'être confirmées tout au long du vingtième siècle [4], nécessite de renoncer à un certain nombre d'images héritées du « sens commun ». Elle propose en particulier une description de la lumière où coexistent des propriétés de type ondulatoire avec un caractère corpusculaire. Ainsi, si la description quantique de la lumière renoue avec l'image très ancienne des « grains de lumière » utilisée en particulier par les philosophes de l'Antiquité [5] les quanta élémentaire d'énergie lumineuse - qui prendront en 1926 le nom de photons [6] - restent difficiles à penser à et à décrire en dehors du cadre formel de la physique quantique.

Il est raisonnable de penser que la génération et la détection de photons uniques n'était pas encore envisagée lorsque le concept de photon fut introduit. Ainsi, jusqu'à l'émergence des idées et des méthodes de l'optique quantique, le « régime du photon unique » était atteint en atténuant fortement une source lumineuse, jusqu'à s'assurer que la probabilité d'observer plus d'un photon soit négligeable [1].

Néanmoins, les états du champ lumineux que l'on obtient en procédant de la sorte diffèrent fondamentalement de « vrais » photons uniques par le fait que même pour de fortes atténuations, la probabilité d'observer simultanément plus d'un photon n'est jamais rigoureusement nulle.

Les progrès techniques associés à la naissance de l'optique quantique dans les années soixante, c'est-à-dire la mise au point des lasers et de systèmes physiques capables de détecter les photons avec une bonne efficacité, ont finalement rendu possible l'observation directe d'états non classiques du rayonnement [34, 35]. Un peu plus tard, ces travaux ont conduit à la première réalisation d'une véritable source de photons uniques [40, 41].

Le travail que nous présentons dans cette thèse est consacré à la réalisation expérimentale de sources de photons uniques. Il appartient donc, d'un point de vue disciplinaire à l'*optique quantique*, dont nous avons utilisé à la fois les méthodes expérimentales et les outils théoriques.

[1] C'est ainsi que furent observées des franges d'interférence « photon par photon »[8].

L'optique quantique est aujourd'hui un domaine en pleine évolution, ses thèmes de recherche « traditionnels » étant maintenant souvent considérés et problématisés sous le jour nouveau des *communications et du calcul quantiques*. Cette discipline émergente regroupe des problématiques issues de différents domaines de recherche et mobilise des savoirs provenant de branches scientifiques généralement considérées de façon disjointes, telles que la physique quantique, l'algorithmique, la théorie de l'information et la cryptographie [21].

Comme nous l'expliquons dans le deuxième chapitre du mémoire, les enjeux liés à la mise au point de sources de photons uniques entrent en forte résonance avec les préoccupations de l'information quantique puisque de telles sources constituent un jalon essentiel pour la réalisation d'un bon nombre des tâches liées aux communications ou au calcul quantique. Parmi celles-ci, la *cryptographie quantique* apparaît comme l'application qui est aujourd'hui la plus accessible expérimentalement, et pour laquelle l'utilisation de sources de photons uniques est susceptible d'apporter d'importants gains de performance. Nous nous sommes attachés à étudier ce dernier point, en travaillant sur la réalisation expérimentale d'un système de cryptographie quantique fondé sur une source de photons uniques, dont nous avons ainsi pu démontrer le fonctionnement et discuter les performances.

Les types de source de photons uniques étudiés dans cette thèse

J'ai effectué mes trois années de doctorat au sein de l'équipe de recherche « Nanophotonique Quantique », du Laboratoire de Photonique Quantique et Moléculaire, équipe dirigée par Jean-François ROCH. J'ai eu la chance, au cours de ces trois années de bénéficier de l'encadrement et du soutien constant de Jean-François ROCH et de François TREUSSART, pour lesquels ma reconnaissance ne saurait se cantonner au chapitre « Remerciements ». De plus, la relation privilégiée qu'entretient notre équipe avec le groupe dirigé par Philippe GRANGIER, ainsi le stage que j'ai effectué dans le cadre de mon cursus d'ingénieur élève au sein du Corps des Télécommunications, nous ont fournit l'occasion de développer des activités de recherche en collaboration avec d'autres équipes. Ces liens ont contribué à enrichir mon travail initial, en y intégrant d'autres approches expérimentales et en en élargissant les horizons thématiques.

Ainsi, après avoir étudié la production de photons uniques par une molécule unique à température ambiante au sein de l'équipe de Jean-François ROCH [75], la collaboration avec l'équipe de Philippe GRANGIER nous a permis d'élargir la mise en œuvre des résultats et des méthodes utilisées avec les molécules uniques, en étudiant l'émission de photons uniques par un centre coloré NV du diamant. En outre, la collaboration avec Philippe GRANGIER nous a amené à poursuivre le travail remarquable effectué par Alexios BEVERATOS durant sa thèse de doctorat [86] et nous avons réalisé, à l'Institut d'Optique les premiers échanges quantiques de clé avec une source de photons uniques en propagation libre [234]. Enfin, le stage en entreprise du Corps des Télécommunications m'a fourni l'opportunité de travailler dans les laboratoires de recherche de l'entreprise MAGIQ [273], et d'y développer une source asymétrique de photons « annoncés » bien adaptée à la cryptographie quantique à grande distance dans un réseau optique fibré [235].

L'objet de cette section est de présenter les deux « familles » de sources de photons uniques auxquelles nous avons ainsi pu nous intéresser au cours de cette thèse, à savoir d'une part les sources déclenchées de photons uniques, basées sur le contrôle de la fluorescence d'un émetteur individuel, et d'autre part les sources asynchrones de photons « annoncés » fondées sur l'utilisation de paires de photons émis par fluorescence paramétrique

dans un cristal non-linéaire $\chi^{(2)}$

Source déclenchée de photons uniques

L'idée physique sans doute la plus simple pour réaliser une source pouvant émettre les photons un par un, à la demande de l'utilisateur, est d'adresser un centre émetteur individuel et de lui appliquer une excitation impulsionnelle adaptée. Pour chaque impulsion d'excitation, un tel système, une fois porté dans son état excité, conduit alors à l'émission d'un photon et d'un seul, de manière synchrone des tops d'horloge correspondants aux excitations impulsionnelles [122, 166].

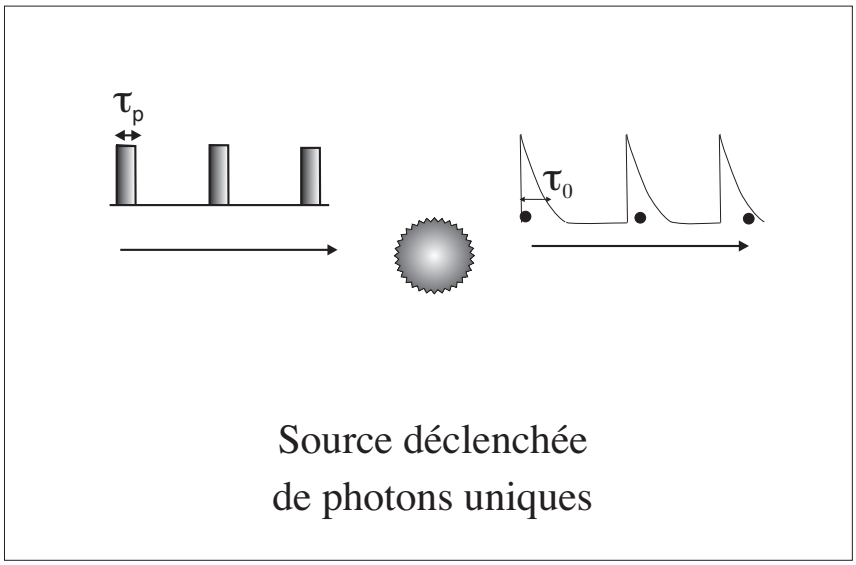

FIG. 1.1 – Schéma de principe d'une source de photons uniques déclenchée : un émetteur unique est porté dans son état excité par une impulsion de pompe, dont la durée τ_p doit être très brève devant la durée de vie de l'état excité τ_0. L'émetteur unique va alors générer, sur une durée typique de l'ordre de τ_0, un photon et un seul, dont l'émission a été « déclenchée » par l'impulsion excitatrice.

Nous avons mis en œuvre ce principe, représenté schématiquement sur la figure 1.1, pour la réalisation de sources de photons uniques à partir d'une molécule unique et d'un centre coloré unique du diamant. Ces expériences sont décrites respectivement aux chapitres 3, 4 et 5, où les protocoles, les performances expérimentales ainsi que les notions génériques telles que « excitation impulsionnelle adaptée », - volontairement employé ici - seront précisées.

Source de photons uniques « annoncés »

Le processus de fluorescence paramétrique dans un cristal non linéaire $\chi^{(2)}$ permet de génèrer, à partir d'un photon de pompe, une paire de photons, appelés « signal »et « réplique » émise durant un intervalle de temps qui est typiquement de la centaine de femtosecondes

[42]. Leonard MANDEL a le premier montré qu'il est possible d'utiliser l'information temporelle portée par l'un des deux photons d'une paire paramétrique afin de conditionner la préparation d'un état à un photon [41].

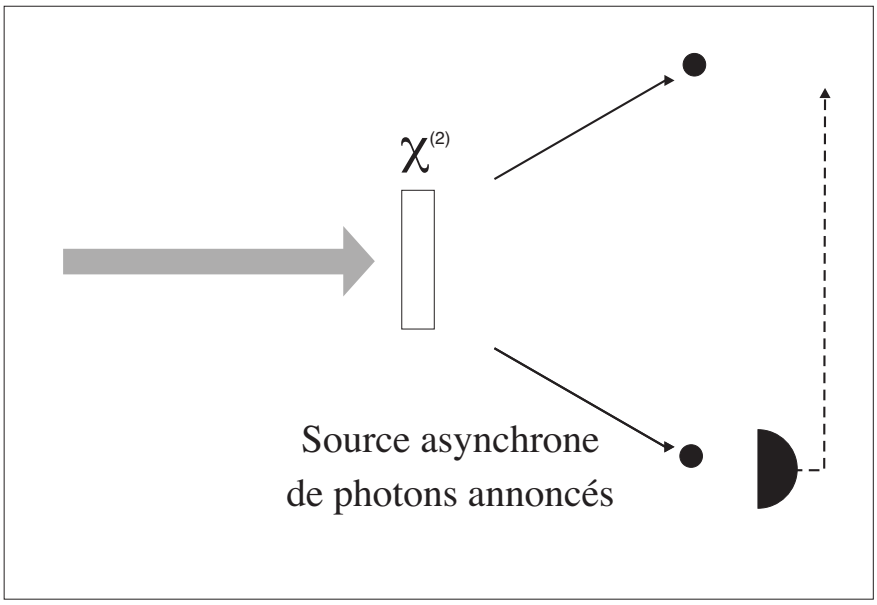

FIG. 1.2 – Schéma de principe d'une source de photons uniques « annoncés » : la photodétection, dans un mode spatial fixé, d'un des photons (signal) issue d'une paire de photons émis par fluorescence paramétrique « annonce » l'existence du photon réplique qui lui est associé. Ce photon unique a été émis simultanément dans le mode spatial conjugué de celui du photon signal. Ainsi, l'information portée par le clic de photodétection sur la voie signal conditionne et annonce l'observation d' états à un photon dans un mode spatial et sur une fenêtre temporelle bien définis.

Le processus de fluorescence paramétrique étant un phénomène spontané [2], les instants d'émission des paires de photons sont aléatoires et une telle source sera qualifiée d'asynchrone. En revanche, les lois de conservation de l'énergie et de l'impulsion imposent des relations bien définies entre les vecteurs d'ondes des photons signal et réplique. En particulier, les mode spatiaux dans lesquels ces photons sont émis sont corrélés.

Le principe de fonctionnement d'une source à « photon unique annoncé » , pouvant être désigné en anglais sous le terme d'« heralded single photon », est représenté sur la figure 1.2. Le photon « signal » , idéalement couplé à un seul mode spatial de propagation est envoyé sur un photodétecteur. Un clic de photodétection agit alors comme un témoin de l'émission complémentaire du photon « réplique » dans le mode spatial corrélé avec celui du photon « signal ». Comme on connaît à la fois l'information spatiale et temporelle associée à ce photon unique, un tel état correspond à ce que Leonard MANDEL a dénommé un « état à un photon localisé » [41], annoncé par le clic de photodétection sur la voie « signal ». On peut réaliser, à l'aide de ce « témoin », un fenêtrage temporel efficace des photons émis, limitant fortement la possibilité d'observer deux paires pour le même signal de déclenchement. L'état lumineux conditionné auquel on s'intéresse peut ainsi être rendu très proche de celui d'un

[2] Les efficacités maximales reportées dans une expérience de génération de paires de photons par fluorescence paramétrique sont de l'ordre de 10^{-6} [268]

photon unique.

Plan de la thèse

Ce manuscrit est composé de deux parties, qui font suite à ce chapitre d'introduction.

La première partie regroupe quatre chapitres et est consacrée aux travaux sur les sources déclenchées de photons uniques. Elle débute au chapitre 2, où nous décrivons différentes applications envisageables pour une source de photons uniques. Nous nous intéresserons spécifiquement aux applications mettant en jeu les propriétés quantiques d'une telle source de lumière et commençons en évoquant les applications faisant suite à l'observation d'états non-classiques du rayonnement. Nous discutons ensuite de l'apport d'une réelle source de photons uniques dans les expériences de cryptographie quantique, dont nous rappelons brièvement le principe. Nous évoquons dans une dernière section les applications potentielles de ces systèmes aux communications et au calcul quantique. Nous dressons enfin un état de l'art des sources de photons uniques existantes, sans nous limiter aux systèmes expérimentaux sur lesquels nous avons travaillé. Ce tableau général permet ainsi de conclure le chapitre 2 par une discussion qualitative des avantages et des inconvénients relatifs aux différentes sources de photons uniques dans le cadre des différentes applications que nous avons présentées .

Le chapitre 3 présente les principes et le protocole expérimental pour la réalisation d'une source de photon unique à partir d'une molécule unique, à température ambiante. Nous y décrivons tout d'abord les paramètres importants pour la détection optique d'une molécule individuelle. Nous détaillons ensuite le montage expérimental que nous avons utilisé, en évoquant le fonctionnement en régime d'excitation continue, puis le régime de fonctionnement en excitation impulsionnelle. C'est dans ce dernier régime que l'on peut obtenir l'émission régulière de photons uniques.

Le chapitre 4 présente les outils d'analyse des propriétés statistiques de l'intensité émise par cette source moléculaire de photons unique. Nous y détaillons également la mise en œuvre d'une méthode d'acquisition et de traitement de la distribution statistique des photons ainsi émis, fondée sur l'enregistrement de tous les instants successifs de photodétection. Ces outils sont ensuite appliqués à un échantillon statistique de référence, pour évaluer la qualité statistique de la source de photons uniques ainsi que ses différents paramètres, puis nous nous intéressons aux fluctuations d'intensité de cette même source sur une large gamme d'échelles de temps. Les données expérimentales sont comparées à un modèle analytique, permettant de relier le comportement statistique observé à la dynamique interne de la molécule et à ses propriétés d'intermittence dans la fluorescence.

Le chapitre 5 décrit le travail et les résultats relatifs à l'utilisation de centres colorés NV du diamant comme source de photons uniques. Ces résultats s'appuient très largement sur le travail de thèse d'Alexios BEVERATOS [86], que nous avons complété par une étude du rayonnement de centres uniques couplés à une microcavité planaire, ainsi que par la mise en évidence du phénomène de photocréation de centres colorés dans des nanocristaux de diamant en régime d'excitation femtoseconde.

La deuxième partie du mémoire traite des applications des sources de photons uniques à la cryptographie quantique. Elle débute par le chapitre 6, dont l'objectif est de présenter les enjeux généraux liés à la cryptographie quantique. Nous mettons pour cela l'accent sur les différentes approches expérimentales qui ont été développées, avant de nous intéresser au statut et à l'interprétation des différents travaux théoriques portant sur les preuves de

sécurité en cryptographie quantique. Le chapitre 7 présente l'expérience de cryptographie quantique en espace libre avec une source de photons uniques, réalisée en octobre 2003 à l'Institut d'Optique à partir de la source de photons uniques décrite au chapitre 5. La discussion des résultats expérimentaux nous permettra de faire clairement apparaître les avantages apportés par une source de photons uniques par rapport à l'utilisation d'impulsions laser fortement atténuées. Enfin, le chapitre 8 décrit une partie du travail effectué lors du stage de recherche au sein de la startup MAGIQ [235], à savoir la mise au point d'une source de photons uniques annoncés fonctionnant à la longueur d'onde de 1550 nm. Nous débuterons ce chapitre en discutant spécifiquement des enjeux technologiques liés au développement de la cryptographie quantique à grande distance dans un réseau optique fibré, nous décrirons ensuite le fonctionnement de cette source, puis nous illustrerons son intérêt en présentant des résultats préliminaires, démontrant sa capacité à assurer des échanges quantiques de clé sur des distances de propagation inaccessibles de manière réaliste avec des impulsions laser atténuées.

Chapitre 2

Sources de photons uniques et applications

Sommaire

2.1 Introduction

Disposer d'une source de lumière capable de produire des photons un par un est actuellement un enjeu important en optique quantique, motivé d'une part par la réalisation de tests fondamentaux de la physique quantique et d'autre part par ses applications potentielles au traitement quantique de l'information. Citons par exemple la mise en œuvre de dispositifs de cryptographie quantique apportant une sécurité accrue par rapport aux systèmes de cryptographie classique [28] ainsi que la réalisation de fonctions logiques élémentaires fondées sur des non-linéarités induites directement par le processus de photodétection [152].

Nous présenterons dans ce chapitre les caractéristiques souhaitées pour une source de photons uniques et décrirons trois familles d'applications des sources de photons uniques dans le domaine de l'optique quantique. Nous montrerons ainsi comment la mise au point de telles sources s'articule avec différents thèmes de recherche et avec des travaux antérieurs. Enfin, nous tenterons de brosser un rapide état de l'art en matière de réalisations expérimentales de sources de photons uniques à la demande, sans toutefois prétendre à l'exhaustivité tellement ce domaine de recherche est actuellement actif au plan international [26]

2.2 Considérations générales sur les « sources de photons uniques »

On désigne par « source de photons uniques » un dispositif capable de délivrer, des impulsions lumineuses contenant un et un seul photon. Comme nous allons le voir en examinant les applications potentielles d'une source de photons uniques, les critères d'évaluation des performances d'une telle source dépendent étroitement de l'application visée. Il est cependant possible de dégager quelques critères « transversaux » . Ainsi, l'utilisateur pourra souhaiter bénéficier d'une source présentant les caractéristiques suivantes :

- Une grande efficacité dans l'émission de photons. Une source idéale aura notamment la propriété de pouvoir émettre un photon pour chaque signal de déclenchement.

- Une bonne efficacité de collection des photons. En effet, la performance effective de la source dépend de la proportion de photons uniques disponibles à l'endroit où ceux-ci sont utiles. L'efficacité de collection, combinée avec l'efficacité d'émission, se répercutera directement sur le rapport signal à bruit des expériences fondées sur l'utilisation de la source de photons uniques.

- Un taux de répétition élevé, permettant d'obtenir une bonne précision statistique lors des acquisitions expérimentales. Ce taux de répétition fixe également le débit d'information qui pourra être codé sur le flux de photons émis par la source.

- Une émission dans un seul mode spatial, de préférence avec une polarisation définie. Le caractère monomode spatial peut *a priori* être obtenu de deux manières différentes :
  - Par filtrage spatial, *après l'émission* du faisceau émis par la source. Il est pour cela possible d'utiliser un dispositif de microscopie confocale adapté à la détection optique de nano-objets uniques [271] ;
  - En forçant l'émission des photons dans le mode d'une microcavité par l'effet Purcell [12], ce mode étant ensuite efficacement couplé à une ligne de transmission.

- Une utilisation aisée et fiable. Ainsi, la possibilité de faire fonctionner la source à température ambiante sera un point très positif, tandis que la stabilité au cours du temps des propriétés d'émission est une condition indispensable pour la plupart des utilisations.

- Enfin, la statistique du nombre de photons dans l'impulsion émise est une caractéristique évidemment primordiale, la proportion d'impulsions contenant plus d'un photon devant être aussi faible que possible.

Trois grandes familles d'applications des sources de photons uniques peuvent être envisagées. Nous évoquerons dans un premier temps comment une telle source peut être utilisée dans des expériences de physique fondamentale. Nous verrons en particulier qu'une source capable de produire des photons uniques à la demande possède des propriétés statistiques tout-à-fait singulières et qu'elle constitue ainsi un outil intéressant pour générer des états non-classiques du rayonnement.

Nous expliquerons ensuite comment l'utilisation de sources de photons uniques peut être mise au service de la distribution de clés secrètes, à travers la technique de la cryptographie quantique. Nous montrerons qu'en terme de sécurité, une source de photons uniques présente des avantages par rapport à l'utilisation d'impulsions lumineuses atténuées, les-

quelles ne correspondent que de manière approchée à une impulsion à un photon.

Enfin, nous évoquerons l'importance que revêt la réalisation de sources de photons uniques pour les développements futurs des communications et du calcul quantique. Une source de photons uniques est en effet capable de constituer une « brique de base » en vue de la construction d'un ordinateur quantique, les interférences quantiques entre états à un photon pouvant être mises à profit pour réaliser des portes logiques photoniques [152].

2.3 Applications à la génération d'états de la lumière non-classiques

Le développement de l'optique quantique a été depuis ses débuts étroitement relié aux travaux théoriques et expérimentaux permettant de mettre en évidence la nature non-classique du rayonnement. Ainsi, les travaux de GLAUBER, menés à partir des années soixante [33], ont permis d'établir une formulation quantique de la cohérence en optique et de la photodétection, jetant alors les fondements théoriques de l'optique quantique. Dans le chapitre 4 où seront examinées les propriétés de bruit d'une source de photons uniques, nous développerons les liens entre la théorie de la photodétection de Glauber et la mesure du bruit d'intensité lié à la répartition statistique des photons dans l'émission d'une molécule unique.

Il a fallu attendre une quinzaine d'années après les travaux de Glauber, et la fin des années soixante-dix, pour observer une des premières manifestations expérimentales de la nature non-classique de la lumière. Ainsi, dès 1974, John CLAUSER, travaillant sur les statistiques d'émission de lumière produite par effet photoélectrique dans un métal, a pu réaliser l'un des tous premiers test mettant en évidence les divergences de prédictions entre théories classique et quantique [34]. Quelques années plus tard, H. J. KIMBLE, L. MANDEL et M. DAGENAIS réalisèrent l'une des expériences fondatrices de l'optique quantique, [35]. En envoyant sur une lame séparatrice la lumière de fluorescence d'un atome individuel excité par un faisceau laser résonnant en interaction avec un jet atomique très dilué, ils observèrent un phénomène de « dégroupement de photons » . Leur résultat, fondé sur l'impossibilité de « couper en deux un photon » , ne peut être expliqué autrement qu'à l'aide de la quantification du champ électromagnétique.

La réalisation d'expériences avec des sources de lumière elles-mêmes non classiques a constitué un tournant majeur dans l'histoire de l'optique quantique. Ainsi, il est frappant de remarquer qu'une des expériences pionnières dans ce domaine, menée par A. ASPECT, P. GRANGIER et G. ROGER a été en même temps la première réalisation d'une source capable de produire des états quantiques à un photon [162]. La source quantique utilisée dans ces travaux est basée sur l'émission consécutive de deux photons à partir d'un état doublement excité de l'atome de calcium ; la détection d'un premier photon de la cascade radiative, « annonce » de façon conditionnelle l'émission d'un état à un photon par l'atome. La cascade atomique utilisée par A. ASPECT et P. GRANGIER constitue ainsile premier exemple de source de photons uniques « annoncés » dont nous verrons un autre exemple au chapitre 8. Cette expérience a permis d'illustrer de façon spectaculaire un des aspects les plus fascinants de la mécanique quantique : la dualité onde – corpuscule [39].

Une autre possibilité pour « annoncer » l'émission d'un photon consiste à utiliser la fluorescence paramétrique dans un cristal non-linéaire de type χ^2 [41, 25].

Par rapport à la cascade atomique utilisée par P. GRANGIER et A. ASPECT, l'usage de cristaux non-linéaires offre davantage de souplesse et conduit à une meilleure efficacité. Dans les deux cas, si l'on s'intéresse à la distribution de probabilité du nombre de photons dans

l'impulsion « annoncée » par une autre photodétection, on peut montrer que cette distribution de probabilité est sub-poissonnienne. Comme nous le verrons au chapitre 8, un tel dispositif permet de réaliser une source de photons uniques efficace pour la cryptographie quantique.

Depuis les années quatre-vingt, d'autres états non-classiques de la lumière ont été étudiés et observés expérimentalement. Un des axes de recherche très important pour l'optique quantique a ainsi été l'étude d'états du rayonnement électromagnétique dont les propriétés de bruit permettent de contourner la limite classique du bruit de photons. On parle alors d'états « comprimés » de la lumière, ou de « squeezing » du champ lumineux, le caractère spécifiquement quantique de ces états apparaissant sur les fluctuations du champ électromagnétique.

Pour des observables qui ne commutent pas, la mécanique quantique conduit aux inégalités d'HEISENBERG, correspondant à l'existence d'une borne inférieure sur le produit des variances de la répartition statistique des résultats de mesure de ces observables. On dénote couramment par P et Q les composantes de quadrature d'un champ électromagnétique, observables qui ne commutent pas [15]. Si l'on considère les valeurs $\Delta^2 P$, respectivement $\Delta^2 Q$, des variances associées aux fluctuations quantiques des composantes de quadrature du champ, la relation d'incertitude d'HEISENBERG peut s'écrire, après une normalisation correctement choisie :

$$\Delta^2 P \times \Delta Q^2 \geq 1 \tag{2.1}$$

Les fluctuations quantiques apparaissent sous la forme de bruit lorsqu'on effectue une mesure sur le champ électromagnétique correspondant. Il est important de remarquer que l'inégalité (2.1) conduit à une limite inférieure sur le *produit* des variances, sans pour autant fixer la variance de l'une ou l'autre des quadratures.

Dans le cas d'un champ classique (état cohérent), les variances $\Delta^2 P$ et $\Delta^2 Q$ sont égales et proportionnelles à l'intensité du champ. On peut de plus montrer que la variance $\Delta^2 N_T$ du nombre de photons détectés pendant une temps de mesure T est égale à $\langle N \rangle_T$, nombre moyen de photons détectés pendant le temps de mesure. Ce niveau de bruit correspond à la « limite quantique standard », aussi appelée bruit de photons. Il est néanmoins possible de générer des états non-classiques, dits états « comprimés » de la lumière où le bruit quantique est « concentré » sur une quadrature permettant ainsi à la quadrature complémentaire d'avoir des fluctuations inférieures au bruit de photons sans pour autant violer les relations de dispersion d'HEISENBERG. Nous avons représenté sur la figure 2.1 la forme que peut avoir un état comprimé dans l'espace des phases pour les coordonnées P et Q. Ces états comprimés sont usuellement produits à l'aide d'interactions non-linéaires dépendantes de la phase entre les modes du champ électromagnétique [16]. Une autre méthode de production d'un état comprimé de la lumières a été introduite par Y. YAMAMOTO. Considérons en effet un émetteur à semi-conducteur idéal, pour lequel chaque paire électron-trou injectée dans la jonction émettrice conduit à l'émission d'un photon. En pilotant l'émission par un flux régulier d'électrons, obtenu en pratique en mettant en série une résistance suffisamment grande, il est possible de générer un faisceau lumineux dans lequel la distribution temporelle des photons reproduit la régularité du courant d'injection [172, 173]. Y. YAMAMOTO et A. IMAMOGLU ont alors proposé de contrôler l'injection de paires électron-trou au niveau individuel, en se plaçant pour cela dans le régime de blocage de Coulomb [164]. La source a alors un fonctionnement de type « turnstile », : elle produit un photon unique pour chaque paire electron–trou injectée au sein de la jonction émettrice. Cependant,l'extrême complexité expérimentale de ce système n'a pu pour l'instant être totalement maîtrisée. Les contraintes

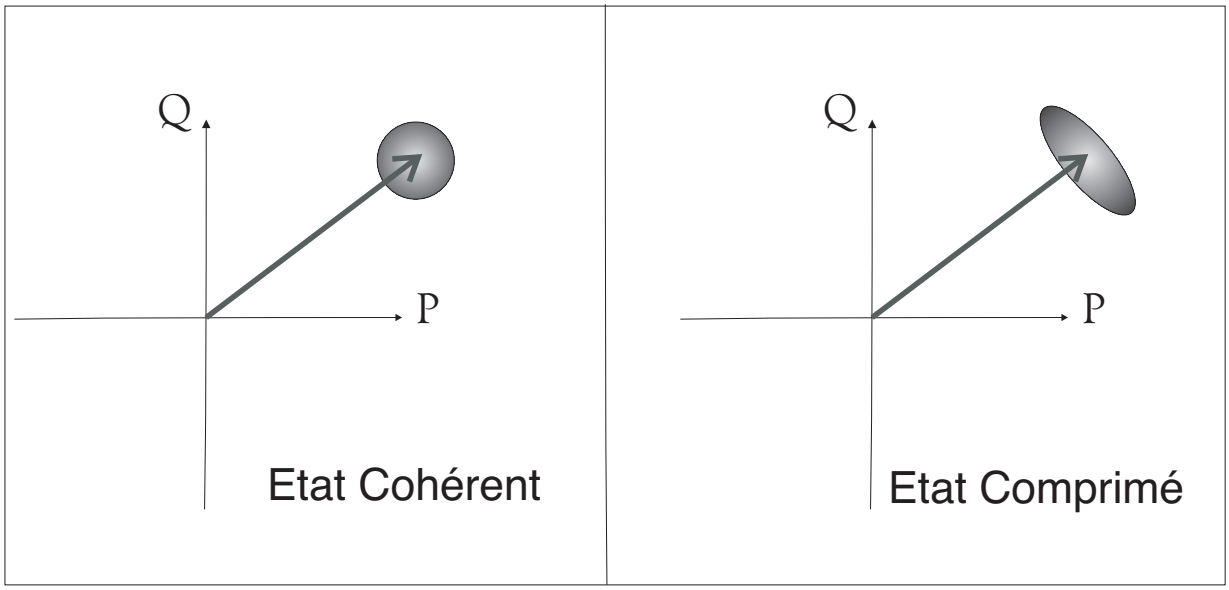

FIG. 2.1 – Représentation, dans l'espace des phase des quadratures P et Q, d'un état cohérent et d'un état comprimé. À gauche, l'état cohérent est un état classique pour lequel les fluctuations ΔP et ΔQ sont identiques et correspondent à la « limite quantique standard ». À droite, nous avons représenté un état dit « comprimé en intensité » pour lequel les fluctuations des deux quadratures ne sont pas symétriques. Pour un tel état, l'incertitude de mesure due au bruit quantique sur l'intensité du champ est inférieure à la limite du bruit de photons, tandis que l'incertitude se reporte en quelque sorte sur la phase relative des deux quadratures.

de fonctionnement sont en effet redoutables : les expériences doivnet être réalisées à des températures de l'ordre du millikelvin et la fabrication des échantillons est particulièrement critique. Dans les résultats publiés en 1999 [107] les contraintes inhérentes à ce système ont limité l'efficacité de collection des photons émis par la source à environ 10^{-4} et aucune mesure directe de dégroupement de photons n'a été relatée.

Ce rapide tour d'horizon des relations entre les sources de photons uniques et la mise en évidence de la nature non-classique du rayonnement peut être conclu en évoquant l'intérêt que présentent les sources de photons uniques « à la demande », obtenues en isolant et en contrôlant la lumière rayonnée par un émetteur individuel. De telles source permettent à la fois d'observer le phénomène de dégroupement de photon et d'émettre un flux lumineux dont les fluctuations d'intensité sont inférieures à la limite quantique standard. En effet, si l'on garde à l'esprit l'image corpusculaire des photons comme étant des grains élémentaires de lumière, il est facile de se représenter un flux lumineux sub-poissonnien, où la répartition des instants d'arrivée des photons est régulière, comme cela est représenté sur la figure 2.2. Nous étudierons dans le chapitre 4 les limites de validité de cette image élémentaire.

2.4 Application à la cryptographie quantique

L'une des motivations essentielles pour la réalisation d'une source de photons uniques est liée à son utilisation dans un système de cryptographie quantique, ou plus exactement

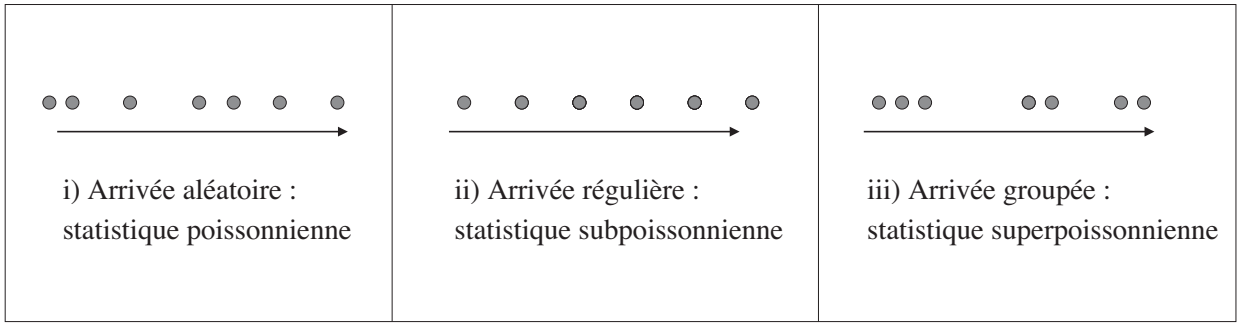

FIG. 2.2 – Représentation corpusculaire du flux de photons dans un faisceau lumineux, distinguant trois cas de figures : i) Source « classique » de lumière, conduisant à une statistique de Poisson des photons émis, tous les instants d'émission étant équiprobables. ii) Émission régulière de photons, correspondant à des fluctuations d'intensité sub-poissonniennes. iii) Groupement de photons, caractéristique par exemple d'une lumière chaotique ou thermique ; les fluctuations d'intensité sont alors supérieures à celles de la référence poissonnienne.

pour la distribution quantique de clés secrètes. Nous allons en rappeler rapidement ici les idées sous-jacentes, en expliquant comment les lois de la physique quantique peuvent être mises à profit pour garantir la confidentialité d'un partage de secret. Nous verrons que pour toute une classe de protocoles, dans lesquels l'information est codée sur des objets quantiques individuels, l'usage d'une véritable source de photons uniques - par opposition à des sources cohérentes atténuées qui ne correspondent que de manière approchée à un état à un photon - permet une amélioration des performances en terme de distance maximale atteignable pour un niveau de sécurité donné. Une étude plus approfondie de cet avantage sera présentée dans les chapitres 7 et 8.

2.4.1 La physique quantique au service de la confidentialité

La cryptographie quantique vise à exploiter les lois de la physique quantique afin de réaliser une tâche cryptographique. Comme l'utilisation de la physique quantique à des fins cryptographiques se limite pour l'instant essentiellement à la distribution de clés secrète, on opère bien souvent un glissement sémantique, en désignant la *distribution quantique de clé* sous le terme générique de *cryptographie quantique*. Cet abus de langage sera fait dans cette thèse, principalement pour des raisons de commodité, mais aussi parce la distribution quantique de clé est actuellement le seul type de protocole cryptographique ayant été réalisé expérimentalement.

La théorie de l'information et la cryptographie conventionnelle prennent pour acquis que les communications numériques peuvent toujours être espionnées de façon passive ou enregistrées pour éventuel usage futur, même par une personne qui ne peut en comprendre le sens au moment de l'interception. Ainsi, l'enregistrement d'une communication chiffrée peut s'avérer utile à quelqu'un qui espère ensuite pouvoir découvrir la clé cryptographique utilisée pour le chiffrage à une date ultérieure, après avoir réussi à accumuler suffisamment de texte chiffré pour faciliter la cryptanalyse ou bien par des voies moins nobles telles que l'espionnage ou la corruption... En revanche, les relations de dispersion d'HEISENBERG, qui

sont au cœur de la physique quantique, permettent d'imaginer des méthodes cryptographiques inédites, irréalisables avec des dispositifs de cryptographie conventionnels. Elles conduisent en particulier à l'existence de canaux de communication que nul ne peut espionner sans risquer simultanément de perturber la transmission de façon ensuite détectable par ses usagers légitimes, et cela indépendamment de la technologie dont peut disposer l'espion[1].

Pour reprendre le jargon habituel des cryptographes, nous supposons que deux protagonistes, communément appelés Alice et Bob, cherchent à communiquer de manière secrète, tandis qu'une tierce personne, dénommé Eve [2] va déployer les moyens les plus machiavéliques pour espionner leurs confidences. Á l'aide de protocoles s'appuyant sur un codage de l'information sur des états quantiques, une chaîne binaire secrète et aléatoire peut être partagée entre Alice et Bob. Cette succession de bits peut ensuite être utilisée comme clé secrète pour le chiffrage de messages transmis via un canal public. La puissance de la cryptographie quantique réside essentiellement dans le fait que les clés ainsi distribuées sont invulnérables à l'espionnage sur le canal quantique ainsi qu'à la puissance de calcul dont pourrait disposer Eve.

Comme nombre de propositions scientifiques originales, la découverte et la diffusion des concepts de la cryptographie quantique ont été quelque peu chaotiques. On peut en effet faire remonter la naissance de l'idée de cryptographie quantique aux propositions de Stephen WIESNER, dans son article « *Conjugate coding* » [11] rédigé à la fin des années soixante. Cet article ne fut que très peu remarqué et, refusé pour publication, resta longtemps non publié. Stephen WIESNER y propose deux applications futuristes des spécificités des systèmes quantiques : il imagine des billets de banque impossibles à contrefaire, ainsi que le multiplexage de plusieurs messages de sorte que la lecture de l'un d'entre eux conduise à une destruction irrémédiable des autres messages. Charles H. BENNETT et Gilles BRASSARD appliquèrent ensuite ces idées au partage de clé secrète [3]. En collaboration avec Stephen WIESNER et Seth BREIDBART, ils jetèrent les bases de la cryptographie quantique en proposant un moyen permettant de combiner les techniques de cryptographie à clé publique avec le codage quantique, pour aboutir à la fabrication de jetons de métro infalsifiables [176] correspondant à un stockage quantique de l'information [4]. Quelques années plus tard, C. BENNETT et G. BRASSARD allaient véritablement ouvrir la voie à la distribution quantique de clé, en se rendant compte qu'il n'était pas nécessaire de *stocker* l'information de manière quantique, mais seulement de pouvoir la *transmettre*. Ils ont pour cela adapté leurs idées précédentes au cas où Alice et Bob échangent des photons uniques, polarisés suivant deux bases non orthogonales. Le protocole correspondant est désormais connu sous le sigle « BB84 », rappelant les initiales des noms de ses deux inventeurs ainsi que l'année où il fut proposé [175]. « BB84 » est jusqu'à aujourd'hui le protocole de cryptographie quantique

[1] On suppose en particulier que cet espion dispose d'ordinateurs arbitrairement puissants, capables de casser instantanément les messages protégés par la cryptographie conventionnelle.

[2] Comme « eavesdropper » qui en anglais signifie « celui qui écoute aux portes »

[3] Pour la petite histoire [29], on peut préciser que Charles BENNETT connaissait bien Stephen WIESNER. Ayant entendu parler de son idée, il n'eut l'intuition de l'appliquer au partage de clé secrète qu'après avoir partagé ses reflexions avec Gilles BRASSARD, lors d'une conférence sur l'information quantique à Puerto Rico en 1979.

[4] On peut rétrospectivement trouver amusant l'accueil que ces idées avaient alors reçu au sein de la communauté scientifique. En effet, cette proposition semblait totalement hors d'atteinte au niveau expérimental et était perçue comme un rêve de théoricien relevant plus de la science-fiction que d'une découverte applicable. Ce jugement était notamment lié au fait que l'on pensait alors que la mise en œuvre de la cryptographie quantique nécessitait de pouvoir stocker de l'information dans des mémoires quantiques. Une telle fonctionnalité reste, en dépit d'importants progrès dans cette direction [144, 143] , aujourd'hui encore non démontré expérimentalement.

qui a été le plus étudié tant du point de vue théorique qu'expérimental. Jusqu'au début des années quatre vingt dix, seule une poignée de chercheurs s'occupaient de cryptographie quantique et ce n'est véritablement que grâce à l'idée d'Artur EKERT, proposant d'utiliser la non-localité de la physique quantique à des fins cryptographiques [225], que l'engouement pour la cryptographie quantique s'est répandu dans la communauté des physiciens. Aux dires de Gilles BRASSARD lui-même [29], l'entrée dans « l'âge d'or » de la cryptographie quantique coïncide avec l'organisation par Artur EKERT, de la première conférence internationale sur ce sujet, en 1993, à Broadway en Angleterre.

2.4.2 Une sécurité basée sur les lois de la physique et la théorie de l'information

La distribution quantique de clé repose sur un schéma global de fonctionnement commun à l'ensemble des protocoles, à savoir l'utilisation conjuguée d'un canal classique et d'un canal quantique (figure 2.3). Alice et Bob sont reliés par un canal quantique public à l'aide duquel ils vont établir une information partagée. Ils vont pour cela échanger des bits quantiques codés sur des photons uniques, sur lesquels ils effectuent des opérations d'encodage et de mesure.

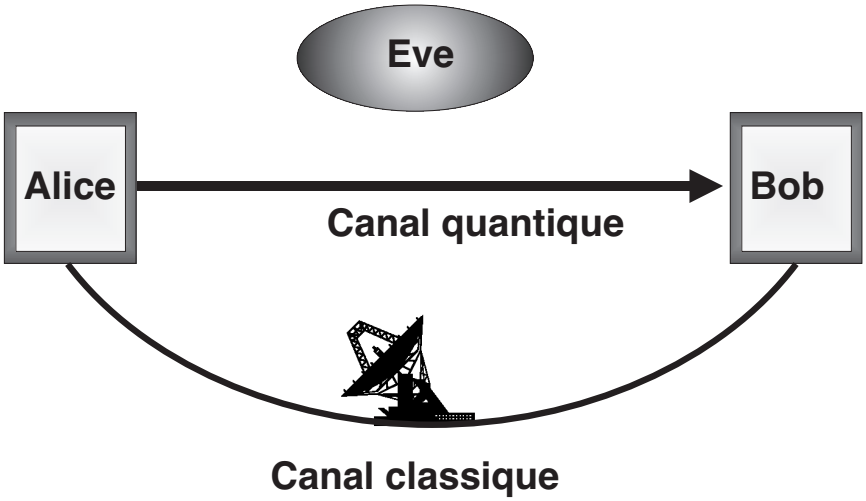

FIG. 2.3 – Cas de figure envisagé en cryptographie quantique : Alice et Bob souhaitent communiquer de façon confidentielle. À cette fin, ils utilisent un canal classique et un canal quantique afin d'établir une clé secrète. Eve, l'espion, tente d'obtenir de l'information sur la clé. Si elle peut écouter librement le canal classique, l'espionnage du canal quantique introduit en revanche des perturbations qu'Alice et Bob peuvent repérer. Alice et Bob vont ainsi pouvoir limiter l'information qu'Eve peut recueillir.

La nature quantique du support de l'information assure à Alice et à Bob que l'information véhiculée sur le canal quantique ne pourra être espionnée qu'en effectuant des mesures, et donc en introduisant des perturbations. Cette sensibilité du canal quantique à l'espionnage s'appuie sur différents points :

- Il est impossible de dupliquer un état quantique arbitraire, comme cela a été démontré par W. ZUREK et W. K. WOOTTERS en 1982 [157]. Ce théorème de « non-clonage » implique que l'on ne peut obtenir de l'information sur l'état d'un objet quantique individuel autrement qu'en effectuant une mesure sur ce dernier, conduisant du même

coup à une projection de l'objet quantique mesuré dans l'état propre correspondant au résultat obtenu pour la mesure.

- L'encodage des bits quantiques peut être rendu sensible à l'espionnage dès lors que l'information est codée sur au moins deux états non-orthogonaux. En effet, toute mesure d'un objet quantique effectuée dans une base autre que celle dont il est état propre aura une action en retour sur l'objet mesuré. Ainsi, dès lors que l'on introduit de l'ambiguïté sur l'encodage, en utilisant des états non orthogonaux, un espion, qui quant à lui ignore la base d'états propres sur laquelle est codée l'information, ne pourra effectuer de mesures sans introduire d'erreurs.

Le partage « quantique » d'information n'est cependant pas suffisant pour aboutir directement à une clé secrète. En effet, après cette étape, Alice et Bob possèdent certes une certaine quantité d'information en commun, mais celle-ci comporte encore beaucoup de défauts :
- une partie des bits acquis ne sont pas significatifs ;
- l'information commune est entachée d'erreurs, dues par exemple à l'encodage imparfait des bits par Alice ou au bruit dans les systèmes de photodétection utilisés par Bob ;
- un espion a éventuellement été en mesure d'obtenir une partie de cette information et aura lui aussi induit des erreurs.

Pour qu'Alice et Bob puissent aboutir à une clé réellement secrète, il est donc nécessaire de recourir à un ensemble de protocoles, dits de réconciliation et d'amplification de confidentialité. Les algorithmes mathématiques correspondants sont issus de la théorie de l'information classique et leur application requiert l'utilisation d'un canal de communication classique pouvant être écouté librement par l'espion. En pratique, cette communication classique entre Alice et Bob peut être véhiculée avec n'importe laquelle des techniques de télécommunications dont nous disposons aujourd'hui : système téléphonique, radio, optique, Internet, etc...

La force des protocoles de cryptographie quantique est par conséquent de combiner les contraintes qu'un canal quantique fait peser sur un espion potentiel avec la puissance héritée des protocoles classiques de partage de secret. On est en effet en mesure de prouver rigoureusement, dans le cadre de la théorie de l'information de SHANNON , que les corrélations partagées à la suite de la communication quantique associées à un traitement classique de l'information permettent à Alice et Bob de « se mettre d'accord » sur une clé secrète commune, tout en étant certains qu'un espion ne peut en connaître qu'une fraction que l'on peut rendre arbitrairement petite [179, 180].

La garantie de sécurité de la cryptographie quantique, apportée par les lois de la physique quantique, est ainsi à prendre au sens de « sécurité inconditionnelle au sens de la théorie de l'information ».

Le type de sécurité offert par la cryptographie quantique est par conséquent fondamentalement « incomparable » avec celui obtenu avec les solutions utilisées en cryptographie traditionnelle, comme par exemple le protocole de cryptographie asymétrique RSA [249, 251], aujourd'hui communément utilisé pour échanger des clés secrètes, notamment sur Internet. En effet, la cryptographie traditionnelle ne s'appuie pas sur des preuves « inconditionnelles » de sécurité en terme de théorie de l'information, mais sur des conjectures mathématiques non prouvées. Elle repose ainsi sur ce que l'on appelle des hypothèses « computationnelles », c'est-à-dire sur l'idée que certains problèmes sont difficiles à résoudre

et que l'on peut contrôler la borne inférieure du temps nécessaire à la résolution de ces problèmes, de façon à rendre *en pratique* impossible de « casser » ces méthodes de cryptage en un temps de calcul raisonnable avec les moyens informatiques actuels. Nous préciserons ces notions dans le chapitre 6 en détaillant les principes d'un codage dont la sécurité est garantie par la théorie de l'information : le code de Vernam.

2.4.3 Avantage procuré par une source de photons uniques

La distribution quantique de clé nécessite l'utilisation de photons uniques afin de garantir la sensibilité du canal quantique à toute tentative d'écoute par l'espion Eve. En pratique, la « sensibilité à l'espionnage » est diminuée par les erreurs expérimentales et il apparaît une limite sur le taux d'erreur de la transmission entre Alice et Bob au-delà de laquelle la sécurité des clés ne peut plus être garantie. De façon similaire, l'utilisation d'une source de photons uniques n'est pas rigoureusement indispensable. Dans le cas où la source produit des impulsions vides, celles-ci ne contribuent pas à engendrer des données partagées entre Alice et Bob ; à l'inverse, les impulsions multiphotoniques constituent une source potentielle de fuite d'information vers l'espion [183]. Dans le cas où la quantité d'information concédée ainsi à l'espion n'est pas prépondérante, la fuite d'information peut être compensée grâce aux techniques d'amplification de confidentialité.

Il est par conséquent possible de réaliser une expérience de cryptographie quantique à l'aide d'une source de photons uniques imparfaites. C'est en pratique très commode, car cela permet de se contenter d'approximations d'états à un photons que sont des impulsions cohérentes atténuées [5]. Celles-ci offrent l'avantage d'être faciles à obtenir à partir d'un laser fonctionnant directement en régime impulsionnel, ou bien à partir d'un faisceau continu dans lequel on « découpe » des impulsions au moyen de modulateurs électro-optiques ou acousto-optiques.

En dépit de cet aspect pratique, l'utilisation d'impulsions laser atténuées présente des inconvénients. Pour une telle source, la distribution statistiquedu nombre n de photons par impulsion obéit à une loi de Poisson, fonction d'un paramètre μ correspondant au nombre moyen $\langle n \rangle$ de photons par impulsion et qui s'écrit :

$$P(n) = \frac{\mu^n}{n!} \mathrm{e}^{-\mu} \tag{2.2}$$

Remarquons tout d'abord dans le cas d'une source fortement atténuées, on vérifie $\langle n \rangle \equiv \mu \ll 1$ et que par conséquent les probabilités respectives de trouver un et deux photons dans l'impulsion sont $P(1) \simeq \mu$ et $P(2) \simeq \mu^2/2$. Ainsi, si l'on souhaite limiter le nombre d'impulsions contenant deux photons afin de réduire potentiellement les fuites d'information vers Eve, il est nécessaire de limiter le nombre moyen de photons par impulsion, et donc le taux de transmission d'information. Á l'inverse, une source de photons uniques conduit essentiellement à des avantages qui sont le pendant des défauts des impulsions cohérentes atténuées. Puisqu'il n'existe plus de fuite d'information due aux impulsions comportant plus de deux photons, la cadence de transmission et l'efficacité de la source n'ont pas à être diminuées pour optimiser le niveau de sécurité de la clé entre Alice et Bob. Comme nous le montrerons aux chapitres 7 et 8, c'est avant tout dans le régime des grandes pertes en ligne et des grandes distances de propagation qu'une source de photons uniques révélera tout son intérêt pour la cryptographie quantique.

[5] En anglais : WCP pour « Weak Coherent Pulses ».

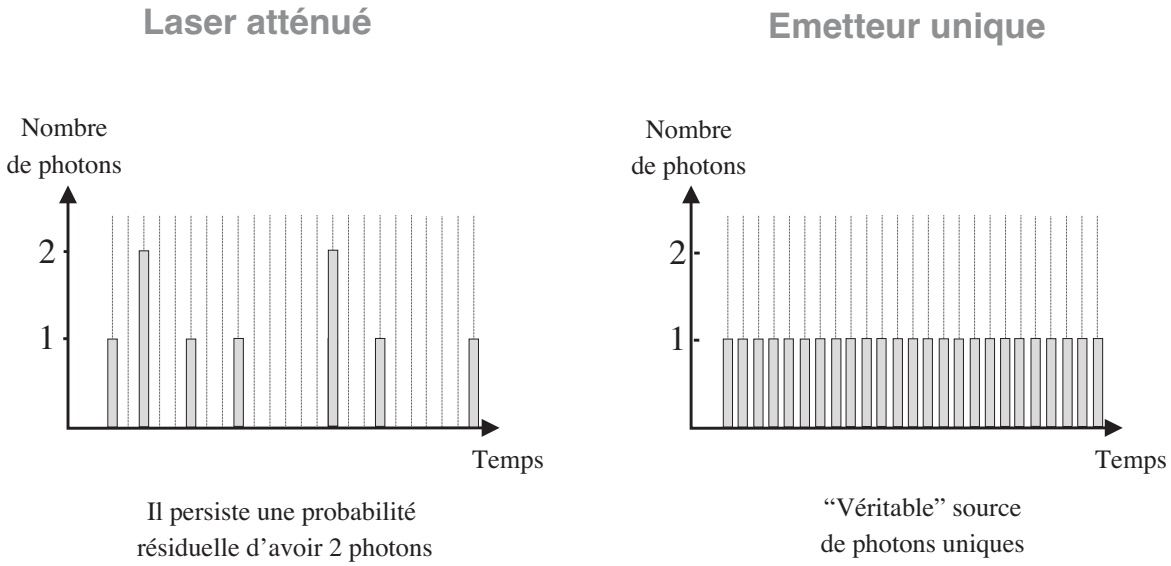

FIG. 2.4 – Différence entre une source poissonnienne atténuée et une vraie source de photons uniques. Dans le cas d'une source atténuée, on doit prendre $\langle n \rangle \ll 1$ pour limiter le nombre d'impulsions contenant deux photons, qui restent néanmoins présentes de manière résiduelle. Dans le même temps, l'atténuation diminue la quantité d'impulsions « remplies » et par là même le débit des communications réalisables. A l'inverse, une source de photons uniques déclenchée idéale ne souffre pas de ces deux défauts : pour chaque impulsion d'excitation, elle conduit à l'émission d'un photon et un seul.

Nous pouvons conclure cette section en dégageant les différents paramètres pouvant servir de « facteurs de mérite » pour une source de photons uniques dans l'optique d'une application à la cryptographie quantique. Ces critères pourront servir de grille de lecture pour l'analyse de notre travail et ils fourniront également des d'éléments de comparaison avec d'autres systèmes expérimentaux. Bien que cette discussion soit abordée plus en détail dans les chapitres 7 et 8, nous pouvons dès à présent établir une liste de paramètres qui ont une influence importante sur les performances de la distribution quantique de clé :

- Les propriétés statistiques d'émission de la source. L'écart à une statistique idéale de photons uniques, que ce soit à cause d'un taux résiduel d'impulsions à deux photons ou à cause de la proportion d'impulsions vides de photons, affectera fortement les performances du partage de clé secrète, en terme de taux de transmission et de niveau de sécurité.

- Les caractéristiques spectrales de la source. Si la *longueur d'onde d'émission* de la source détermine le canal optique utilisable en pratique (fibre optique ou espace libre) la *largeur spectrale* et la *stabilité du profil spectral* vont jouer un grand rôle sur l'évolution du taux d'erreur au fur et à mesure de la propagation. Pour les systèmes de cryptographie quantique reposant sur des mesures interférométriques, les propriétés de cohérence des photons émis jouent également un rôle crucial. Nous verrons enfin que la longueur d'onde et la largeur spectrale des impulsions émises par la source influencent les performances du système de photodétection, lesquelles vont être cruciales pour le fonctionnement du système QKD (cf chapitre 8).

- Le taux de répétition de la source. Ce paramètre expérimental est directement relié au débit d'information lors du partage quantique de clé. Son optimisation peut s'avérer complexe, car il existe en pratique de nombreux facteurs limitants, de nature parfois contradictoires : énergie des impulsions de pompe pour saturer l'émission, durée des impulsions fournies par la source, rapidité des détecteurs et de l'électronique d'acquisition, temps mort du système de photodétection, etc.

- La durée des impulsions à un photon. Ce paramètre est directement relié à la dynamique du processus d'émission. On préférera disposer d'impulsions à un photon de courte durée, de sorte qu'il soit ensuite possible d'établir un fenêtrage temporel étroit au niveau du système de détection, de manière à limiter l'influence des coups d'obscurité des détecteurs et à diminuer ainsi le taux d'erreur dans la transmission.

- Le contrôle de l'émission de la source. Comme nous le verrons, une source capable de fournir un photon unique à la demande, telle que celle étudiée aux chapitres 3 et 4, est sensiblement plus pratique qu'une source asynchrone de photons uniques « annoncés » (décrite au chapitre 8) pour laquelle on dispose effectivement d'un signal de déclenchement pour chaque impulsion, mais où l'instant d'émission de la paire de photons reste aléatoire dans le temps.

2.5 Applications potentielles au calcul et aux communications quantiques

Les perspectives ouvertes par la manipulation d'objets quantiques individuels dans le domaine du traitement de l'information ont tout d'abord été entrevues par Richard FEYNMAN. Il avait suggéré dès 1982 qu'il était possible de contourner les difficultés rencontrées dans la simulation « classique » de systèmes quantiques en utilisant un ordinateur dont le fonctionnement même serait basé sur les lois de la physique quantique [9]. L'idée de l'ordinateur quantique était née et, quelques années plus tard, elle sera formalisée de façon plus précise par David DEUTSCH. Le fonctionnement d'un ordinateur quantique est ainsi basé celui d'un registre de systèmes quantiques à deux niveaux appelés *qubits* ou bits quantiques, dont l'évolution est contrôlée par des opérations unitaires et sur lesquels les transformations sont effectuées à l'aide de portes logiques appelées « portes quantiques », par analogie avec les portes logiques binaires de l'électronique numérique.

David DEUTSCH fut le premier à montrer qu'un ordinateur quantique permettait de résoudre certains problèmes de façon plus efficace qu'un ordinateur classique [155]. Durant les années 90, deux résultats majeurs d'algorithmique quantique allaient illustrer les capacités prometteuses d'un ordinateur quantique, d'abord avec la découverte de l'algorithme de SHOR [154] permettant la factorisation de nombres premiers en un temps polynomial[6], puis avec celle de l'algorithme de GROVER, permettant d'accélèrer de façon quadratique la recherche dans une liste non ordonnée [153]. Ces deux résultats ont fortement renforcé l'attention autour de l'information quantique, la réalisation d'un ordinateur quantique devenant en quelque sorte le nouveau Graal sinon de la recherche fondamentale en physique, tout du moins de sa vulgarisation [7].

[6] C'est à dire avec un accroissement exponentiel des performances par rapport aux algorithmes classiques

[7] En dépit de l'enthousiasme et de l'optimisme soulevé par les progrès des expériences de « Quantum Com-

Les défis à relever, tant théoriques qu'expérimentaux, afin de fabriquer un ordinateur quantique sont néanmoins très importants, ce qui justifie l'ampleur des efforts déployés depuis quelques années. Nous n'entrerons pas ici dans le détail de l'activité foisonnante [8] et des progrès effectués en direction de l'ordinateur quantique et nous nous limiterons à une simple évocation des possibilités offertes par l'utilisation d'états quantiques à un photon dans les communications et le calcul quantique. Cette voie de recherche est activement explorée car elle pourrait permettre de relever plusieurs des défis considérables auxquels se heurtent la réalisation d'un ordinateur quantique.

L'un des obstacles majeurs à la réalisation d'un ordinateur quantique est le problème de la *décohérence* [145], terme qui désigne la disparition des propriétés quantiques d'interférence du fait de l'interaction avec l'environnement [151]. Il apparaît cependant que parmi les supports physiques susceptibles de constituer des bits quantiques, la lumière, ou plus exactement son constituant ultime, le photon, est l'un des plus résistants à la décohérence. En effet, au cours de sa propagation que ce soit en espace libre ou dans une fibre optique, l'état quantique d'un photon sera peu perturbé. Cela en fait un candidat de choix pour servir de support à l'information quantique. L'une des difficultés inhérentes à l'utilisation de photons vient revanche du fait que pour l'instant, on ne sait pas stocker l'état quantique d'un photon, en dépit de résultats intéressants sur les mesures quantique non-destructives sur un photon unique [124], le ralentissement de la lumière [142] ou la réalisation de mémoires quantiques dans un nuage d'atomes [144] .

En dépit de ces limitations, il a été montré récemment que l'on peut utiliser les photons afin de réaliser des calculs quantiques. KNILL, LAFLAMME, et MILLBURN en 2001 ont ainsi proposé dans un article très remarqué [152] un modèle d'ordinateur quantique « optique » reposant sur l'utilisation d'une source de photons uniques spectralement cohérente, associée à des éléments d'optique linéaire et à des photodétecteurs. Le système qu'ils envisagent permet de réaliser les principales actions logiques nécessaires pour le calcul quantique et il se positionne dès lors comme un candidat prometteur en vue de la réalisation d'un ordinateur quantique.

L'un des aspects a priori surprenants dans cette proposition est qu'elle semble impliquer la possibilité d'effectuer des calculs à partir d'opérations exclusivement linéaires [9]. Cependant le principe de fonctionnement de cet d'ordinateur quantique « optique » est en fait bien basé sur des non-linéarités, qui sont associées à la photodétection et à la post-sélection des résultats. En effet, les résultats des mesures de photodétection y sont réinjectés dans le calcul sur les bits quantiques à l'aide d'un système de bouclage, ce qui conduit aux fonctions logiques nécessaires à la réalisation d'un calcul. Le phénomène dit de « coalescence » de photons est l'un des éléments de base sur lesquels reposent cette proposition. Ce terme désigne le phénomène intervenant quand deux photons indiscernables sont incidents de par et d'autre d'une lame séparatrice. Il se produit alors une interférence entre les différents « chemins quantiques » (figure 2.5), se traduisant par une annulation de la probabilité d'avoir simultanément un photon transmis et un photon réfléchi des deux côtés de la lame séparatrice en sortie de ce coupleur linéaire. On observe donc un groupement des photons dans le même mode du champ, compatible avec leur caractère bosonique. Ce

puting », il existe des arguments scientifiques amenant à mettre en doute ne serait-ce que la possibilité qu'un ordinateur quantique puisse nous être un jour utile [27].

[8] L'ouvrage, désormais classique, de NIELSEN et CHUANG [21] constitue une formidable introduction à ce domaine de recherche.

[9] Une telle possibilité semble en effet en contradiction avec le fait que certaines des opérations nécessaires dans la grand majorité des calculs, notamment la mesure et la mise en mémoire, sont des opérations irréversibles, qui ne peuvent par conséquent pas être décrites dans le cadre d'un formalisme linéaire basé sur des transformations unitaires des opérateurs quantiques ou des fonctions d'onde.

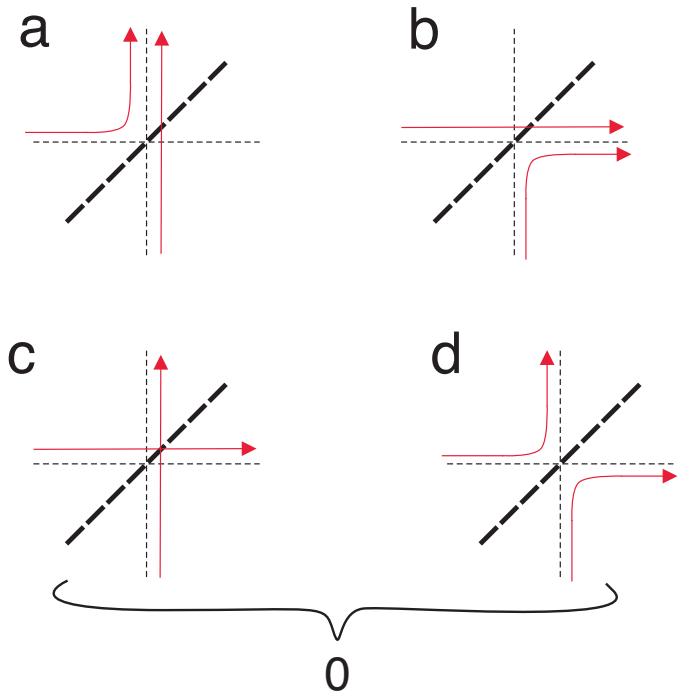

FIG. 2.5 – Deux photons indiscernables, particules bosoniques, semblent se « regrouper » en sortie d'une lame séparatrice. Dans le cas où la lame séparatrice est une lame pour laquelle les coefficients de réflexion et de transmission sont égaux à 50 %, les amplitudes de probabilité correspondant aux termes c et d, pour lequels les deux photons sont soit transmis soit réfléchis, sont de signes opposés. Ils s'annihilent en interférant destructivement. On observe donc expérimentalement que les photons sortent du même coté de la lame séparatrice (termes a et b).

phénomène de coalescence a été prédit et observé par HONG, OU et MANDEL en 1987, au moyen de paires de photons produits par fluorescence paramétrique [42].

Comme nous l'avons mentionné au début de ce chapitre, l'observation de la coalescence nécessite de produire des photons pouvant être décrits par un paquet d'onde dont la cohérence temporelle et spatiale permet d'observer des interférences avec un contraste proche de l'unité. Parmi les expériences portant sur la réalisation d'une source de photons uniques dont nous donnons un aperçu dans la section suivante, très peu de dispositifs ont pour l'instant permis de produire directement des photons uniques sous la forme de paquets d'onde cohérents. A notre connaissance, seules les expériences fondées sur l'émission d'atomes [39, 123, 133] et celles portant sur les boîtes quantiques semi-conductrices en microcavité [105, 96] permettent actuellement d'atteindre ce régime [10]. Concernant les avancées récentes des travaux menés sur les boîtes quantiques InAs/GaAs , il a été possible, à l'aide de ce type de système expérimental d'observer pour la première fois le phénomène de coalescence entre deux photons émis consécutivement par la même source de photons uniques

[10] On peut préciser ce point en indiquant que si la cohérence spatiale, qui peut augmenter au cours de la propagation, n'est pas a priori un facteur limitant, la cohérence temporelle des photons émis est en revanche extrêmement critique. Elle est directement liée au mécanisme d'émission, et au temps de cohérence T_2 du dipôle émetteur vis-à-vis de sa durée de vie radiative T_1. Ainsi, le critère assurant un bon contraste dans le phénomène de coalescence est le rapport entre la durée de vie radiative T_1 et le temps de cohérence T_2. Le cas optimal où $T_2/2T_1 = 1$ correspond à des photons « limités par Fourier » [140].

[140]. Il a également été démontré qu'une telle source de photons uniques peut servir de point de départ à la formation d'états intriqués [149], ainsi qu'à la réalisation d'expériences de téléportation quantique [150].

2.6 Réalisations expérimentales de sources de photons uniques à la demande

Les enjeux liés à la réalisation de sources de photons uniques sont actuellement poursuivis par un grand nombre de groupes de par le monde, et de très nombreux résultats sur la production de photons uniques ont été obtenus au cours des dernières années [31, 26]. Une grande diversité de voies expérimentales sont activement explorées et nous nous attacherons dans cette section à en présenter les grandes familles, en tentant de discuter brièvement les points forts et les points faibles des différents types d'émetteurs.

Comme nous l'avons expliqué en introduction, nous avons abordé deux types de sources de photons uniques dans le cadre de ce travail de thèse, à savoir les sources de photons uniques à la demande et les sources de photons annoncés. Nous nous limiterons ici à un panorama des systèmes expérimentaux pouvant constituer des source de photons uniques à la demande [11]. La réalisation d'une source de photons uniques à la demande implique de pouvoir contrôler temporellement l'émission spontanée d'un émetteur unique afin de « déclencher » l'émission d'un photon. On peut schématiquement répartir les systèmes expérimentaux en deux catégories :

- Les sources de photons uniques déclenchées obtenues par *excitation cohérente* d'un dipôle unique. C'est par exemple le cas des sources réalisées à partir d'un atome,d'un ion piégé, ou d'une molécule unique à basse température.
- Les sources de photons uniques déclenchées fonctionnant par *excitation incohérente* d'un dipôle placé dans une matrice solide. De nombreux émetteurs uniques fluorescents ont été utilisés pour réaliser de telles sources de photons uniques et nous évoquerons les travaux relatifs aux molécules uniques, aux centres colorés du diamant et aux boîtes quantiques colloïdales de CdSe avant de détailler les résultats obtenus à partir d'excitons semi-conducteurs dans les boîtes quantiques.

2.6.1 Excitation cohérente d'un dipôle unique

Molécules à basse température

Les premières études concernant les propriétés de fluorescence d'un dipôle unique ont été réalisées à l'aide de molécules uniques placées à basse température. Une molécule fluorescente unique insérée dans un substrat solide constitue en effet un émetteur individuel dont les propriété d'émission sont fondamentalement non classiques, et dont on peut résoudre spectralement les niveaux d'absorption de bord de bande en se plaçant à des températures de quelques kelvin, où l'élargissement inhomogène des raies d'absorption dû à l'interaction avec les phonons est limité.

On doit à William Esco MOERNER la première observation d'un signal de molécule uniques [44]. Dans une expérience réalisée à une température de 1.6 K, une molécule de pentacène insérée dans un cristal de paraterphényl est pompée de façon résonnante sur la

[11] Le contexte bibliographique relatif aux sources de photons annoncés sera quant à lui développé au chapitre 8.

raie à zéro phonon (λ = 592.32 nm). La détection est effectuée en mesurant *l'absorption* du faisceau, lorsque sa fréquence est balayée de part et d'autre de la résonance.

Le coefficient d'absorption correspondant à une molécule unique étant très faible, une telle détection en absorption conduit à un rapport signal à bruit proche de l'unité [131]. De manière presque simultanée [45], Michel ORRIT et Jacky BERNARD ont montré qu'une détection par fluorescence était bien mieux adaptée, conduisant à des rapports signal à bruit bien supérieurs. Dans ce nouveau schéma expérimental, la molécule est toujours excitée de façon résonnante sur la raie à zéro phonon. Le niveau peuplé peut alors se désexciter vers la suite de niveaux vibrationnels du niveau fondamental et la lumière de fluorescence ainsi produite, décalée spectralement de la longueur d'onde d'excitation, peut être détectée de manière spécifique au moyen de filtres spectraux adaptés. Une remarquable série d'expériences ont ensuite permis de montrer qu'à basse température, un petit nombre de molécules bien choisies se comportent comme des systèmes à deux niveaux, la raie à zéro phonon ayant une largeur spectrale limitée par la durée de vie radiative du niveau excité [76].

Que ce soit la mise en évidence du déplacement lumineux ou du doublet Autler-Townes [51], de transitions mutiphotoniques [52], ou l'observation d'oscillations de Rabi radiofréquences entre les « états habillés » de la molécule par le champ laser [53], l'analogie entre molécule et système à deux niveau va au-delà d'une simple similitude. Elle est en particulier validée par un excellent accord entre les résultats expérimentaux et l'applications des équations de Bloch optiques.

Enfin, le contrôle cohérent de l'excitation d'une molécule unique fluorescente par transfert adiabatique conduit à la réalisation de la première source de photons uniques déclenchée. Publié en 1999, le travail de C. BRUNEL *et al* [54] a démontré la possibilité d'émettre des photons uniques à la demande à partir d'une molécule unique fluorescente immergée dans l'hélium superfluide à une température de 1.6 K [12]. Le passage dans l'état excité est obtenu par passage adiabatique rapide, à l'aide d'une modulation périodique de l'effet Stark quadratique induit par l'application d'un champ électrique sinusoïdal appliqué à la molécule, en plus d'un faisceau laser résonnant. Le balayage de la résonance est ajusté de façon à correspondre à une impulsion π, créant l'inversion de population dans le système à deux niveaux.

Il est important de noter qu'afin de s'affranchir de la lumière diffusée par la matrice à la fréquence du laser d'excitation, lumière qui vient masquer les photons émis sur la raie à zéro phonon, seule l'absorption, et donc l'excitation de la molécule s'effectue de façon résonnante. Les photons émis par la molécule et réellement détectés sont issus d'une multiplicité de transitions, entre le niveau de bord de bande de S_1 et les niveaux vibrationnels de S_0. Dès lors, *ces photons ne correspondent plus à des paquets d'onde parfaitement cohérents*. Ils ne remplissent donc pas les conditions nécessaires pour une application aux communications et au calcul quantique.

Electrodynamique en cavité

Les expériences d'électrodynamique en cavité, illustrant les propriétés les plus fondamentales de l'interaction entre matière et rayonnement, ont en même temps été parmi les premiers systèmes expérimentaux aptes à générer des états à un photon à la demande.

Le schéma général de ces expérience a été proposé en 1997 par C. K. LAW et H. J. KIMBLE [122]. Il se fonde sur l'utilisation du couplage fort entre un atome et une cavité ainsi que sur le transfert cohérent de l'état quantique de l'atome vers les états quantiques du champ.

[12] Cette expérience a été réalisée avec une molécule de DBATT (dibenzantranthrène) insérée dans une matrice de n-hexadecane.

Les expériences de l'équipe de Gerhard REMPE réalisées à Münich ont ainsi démontré la possibilité de contrôler l'émission de photons uniques d'un atome fortement couplé à une cavité optique de grande finesse. L'impulsion excitatrice de pompe provoque le passage adiabatique de l'atome vers l'état excité fortement couplé à la cavité optique par émission Raman stimulée. En ajustant la durée de l'impulsion excitatrice, on peut s'assurer que le système, pour chaque impulsion de déclenchement, émet un unique photon dans le mode spatial de résonance de la cavité auquel l'atome est couplé [123, 121].

Ce type d'expérience a également été réalisé dans le domaine micro-onde, à partir d'un atome de rubidium, dans le groupe d'Herbert WALTHER. Un jet peu dense d'atomes de rubidium, excités dans un état de Rydberg circulaire est envoyé dans une cavité supraconductrice de très haute finesse, refroidie à 300 mK et résonnante avec une transition des atomes dans le domaine micro-onde. Le temps d'interaction atome - cavité, qui dépend en partie du nombre de photons dans la cavité, peut être contrôlé par la sélection en vitesse des atomes et un tel système peut générer à la demande un état de Fock à n photons dans le mode de la cavité micro-onde [125, 126].

Atome ou ion unique piégé

Les expériences évoquées au paragraphe précédent, fondées sur le contrôle cohérent d'un système atome-photon en régime de couplage fort, peuvent également être réalisées avec des ions ou des atomes uniques piégés. Ceci présente un important avantage dans le cadre de la réalisation d'une source de photons uniques, puisque l'on s'affranchit ainsi des contraintes liées à des temps d'arrivée aléatoires et aux possibles fluctuations du nombre d'atomes dans la zone d'interaction [126].

Un ion unique peut être efficacement confiné spatialement à l'aide de pièges magnétiques [130]. L'utilisation d'un tel ion piégé afin d'émettre des photons uniques a été réalisé avec succès à partir d'ions calcium piégés, dans les équipes de Rainer BLATT et Herbert WALTHER [128, 126]. Ce type de source, à même d'émettre à la demande des paquets d'onde à un photon cohérents, permet d'envisager des applications intéressantes dans le domaine des communications quantiques [158]

Plus récemment encore, le piégeage d'atomes neutres à l'aide de pièges dipolaires a également ouvert de nouvelles perspectives en ce qui concerne la réalisation de source de photons uniques indiscernables. Ce type d'expérience est rendu possible par les progrès considérables réalisés ces dernières années pour la mise au point de pièges dipolaires capables de capturer quelques atomes [136] et plus récemment un seul atome grâce au phénomène de blocage collisionnel découvert dans l'équipe de Philippe GRANGIER [135]. Un système légèrement différent a ensuite été mis en place dans le groupe de Jeff KIMBLE [134] et ce système a très récemment permis de réaliser une source de photons uniques à la demande à partir d'atomes uniques de césium piégés, en interaction forte avec une cavité de grande finesse [133]

2.6.2 Excitation incohérente d'un émetteur fluorescent individuel

Francesco DE MARTINI a proposé la réalisation d'une source de photons déclenchée, fondée sur l'excitation incohérente d'une molécule unique *à température ambiante* [166]. Au cours de ces dernières années, cette idée a ouvert la voie à un très grand nombre de réalisations expérimentales. Son application à des molécules uniques fluorescentes ainsi qu'à un centre coloré unique du diamant a constitué une part importante de ce travail de thèse, et les éléments bibliographiques afférents seront développés aux chapitres 3 et 5.

Boîtes quantiques semi-conductrices

Le développement des nanostructures semi-conductrices a également ouvert de nouvelles possibilités quant au choix d'émetteurs individuels pouvant être utilisés pour produire des photons uniques. Les boîtes quantiques sont des structures semiconductrices nanométriques dont la taille et la forme peuvent être contrôlées avec précision. Leur étude suscite depuis quelques décennies un engouement particulier dans la communauté scientifique internationale, du fait de leurs propriétés physiques originales [120], qui découlent essentiellement du fort confinement électronique tridimensionnel des porteurs. Une boîte quantique individuelle est ainsi caractérisée par une densité d'états électroniques discrète et peut être considérée comme un « atome artificiel », chaque désexcitation d'une paire électron-trou conduisant ainsi à l'émission d'un photon. Ces systèmes présentent de très bonnes caractéristiques en vue de la réalisation de sources de photons uniques. En effet, ils sont facilement isolables, photostables et ont une durée de vie assez courte, typiquement de l'ordre de la dizaine de picosecondes. Nous évoquerons ici brièvement trois approches expérimentales assez différentes ayant conduit à la réalisation de sources de photons uniques à partir de boîtes semi-conductrices uniques. On trouvera une discussion plus complète des propriétés des différents systèmes en se rapportant à la référence [102].

Boîtes quantique InAs dans des micropiliers

Une boîte quantique individuelle d'InAs placée au sein d'une microcavité résonnante, constitue un système physique bien adapté à la réalisation d'une source déclenchée de photons uniques. De tels objets sont réalisés en plusieurs étapes [120]. La structure semiconductrice de type III-V est obtenu grâce à des dépôts successifs de couches par épitaxie par jet moléculaire. Les boîtes quantiques d'InAs se forment par auto-organisation lors du dépôt de la couche d'InAs sur une couche de GaAs. Autour de la couche contenant les boîtes quantiques, on ajoute une alternance de couches GaAs / AlAs de façon à obtenir une microcavité planaire, on a alors une structure confinée à deux dimensions, ou « puit quantique ». L'obtention du confinement à trois dimensions nécessite une étape supplémentaire : la « gravure » des micropiliers. Ceci apparaissent, pour les boîtes quantiques qui y sont confinées, comme des microcavités tridimensionnelles dont le facteur de qualité peut atteindre 10^3. La résonance correspondante permet d'obtenir un couplage très important avec l'émetteur et donc de forcer, par effet Purcell, l'émission de photons dans le mode de la cavité [110] [13].

Si l'excitation d'une boîte quantique aboutit à la création de plusieurs excitons, il a été observé que lors de la cascade radiative liée aux désexcitations successives, les photons sont émis à des longueurs d'onde différentes [96, 97]. Ainsi, en utilisant un filtre approprié, il est possible d'isoler le photon émis par le mono-exciton (noté X sur la figure 2.6), à la toute fin du processus de cascade radiative ce qui conduit ainsi à l'émission d'un seul photon dans le mode de la microcavité. Il a été montré récemment qu'en se plaçant à basse température, les paquets d'onde correspondants ont une très bonne cohérence temporelle [140], se prétant ainsi à une utilisation pour l'information quantique [149, 150].

Le dispositif expérimental nécessaire pour produire des photons uniques est assez élaboré, et nécessite l'utilisation de basses températures, ce qui limite pour l'instant l'efficacité globale de ces sources aux alentours de 1 %.

[13] On notera que d'autres types de microcavités peuvent être envisagées. Ainsi, l'équipe de A. IMAMOGLU s'est quant à elle intéressée à l'étude de ces boîtes quantiques InAs dans des microcavités en forme de microdisques [103, 104].

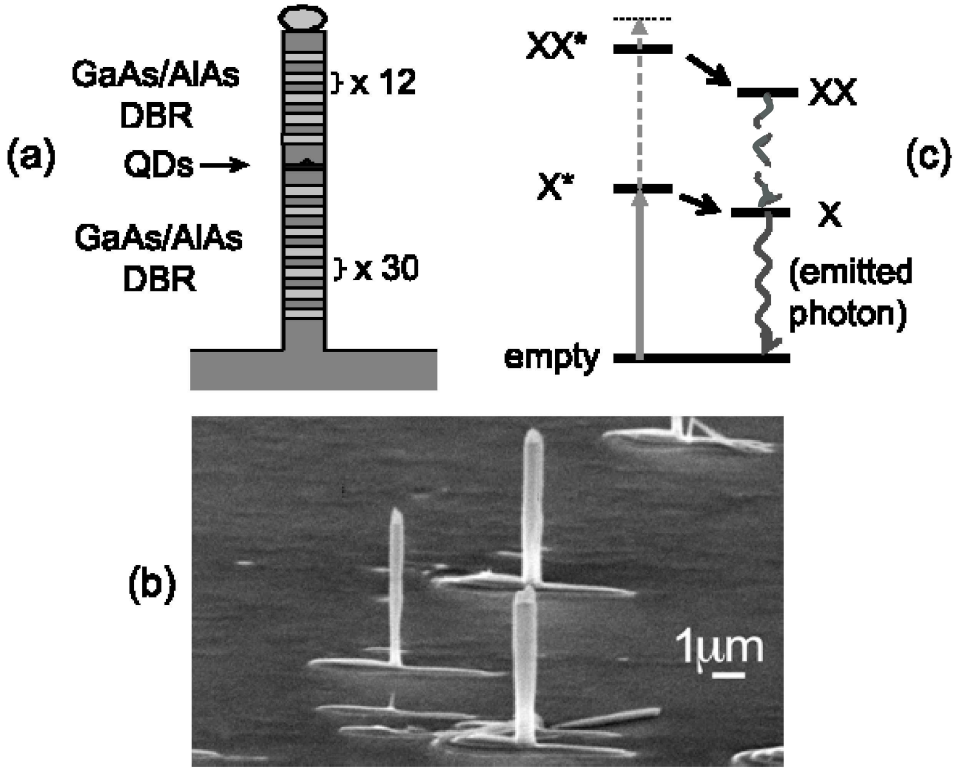

FIG. 2.6 – Emission de photon suniques dans les boîtes quantiques InAs en micropiliers. (a) Diagramme schématique de la structure d'une boîte quantique unique dans un micropilier et principe de fonctionnement de la source de photons uniques par un processus de cascade radiative. (b) Image des micropiliers enregistrée par microscopie électronique à balayage. Les micropiliers ont une hauteur d'environ 5 μm et un diamètre qui peut varier de 0.3 à quelques microns. Ces figures sont extraites de la référence [112].

Nanocristaux colloïdaux de CdSe

Les nanocristaux colloïdaux de sélénure de cadmium CdSe appartiennent à une autre famille : ce sont des semi-conducteurs de type II-VI, produits par synthèse chimique. Pour diminuer le réactivité et éviter une oxydation trop rapide, ces nanoparticules dont le cœur a un diamètre moyen de l'ordre du nanomètre, sont « passivées » à l'aide d'une couche de sulfure de zinc ZnS. Ces nanocristaux ont des propriétés de fluorescence intéressantes, car la longueur d'onde d'émission située dans le visible peut être fixée de façon relativement précise lors de la fabrication [14]. Compte tenu de leur photostabilité et de leur taille nanométrique, ces nanocristaux constituent de très bons candidats pour des utilisations en tant que sondes fluorescentes en biologie [116]. Par ailleurs, en bon accord avec l'image d'« atome artificiel », le dégroupement de photons a été observé avec ces émetteurs [119] et il a été montré récemment [115] que l'on pouvait réaliser une source de photons uniques déclenchée fonctionnant à température ambiante à partir de l'émission d'un nanocristal unique.

[14] L'élargissement inhomogène mesuré sur une assemblée de boîtes quantiques de CdSe / ZnS est de l'ordre d'une dizaine de nm [111].

Emission de photons uniques contrôlée électriquement

Les sources de photons uniques évoquées précédemment reposent sur l'excitation optique d'une boîte quantique unique. Il a récemment été démontré qu'il était possible de contrôler électriquement l'émission de photons par une boîte quantique unique.

L'équipe d'Andrew SHIELDS, à Cambridge (UK) a ainsi pu obtenir des résultats prometteurs en réussissant à faire fonctionner à 5 K, par excitation électrique, une diode électroluminescente composée d'une jonction $p - n$ dans laquelle est plongée une boîte quantique nanométrique d'arsenure d'indium. Un tel dispositif est capable d'émettre des photons uniques pour chaque impulsion électrique de pompe [99].

2.7 Synthèse

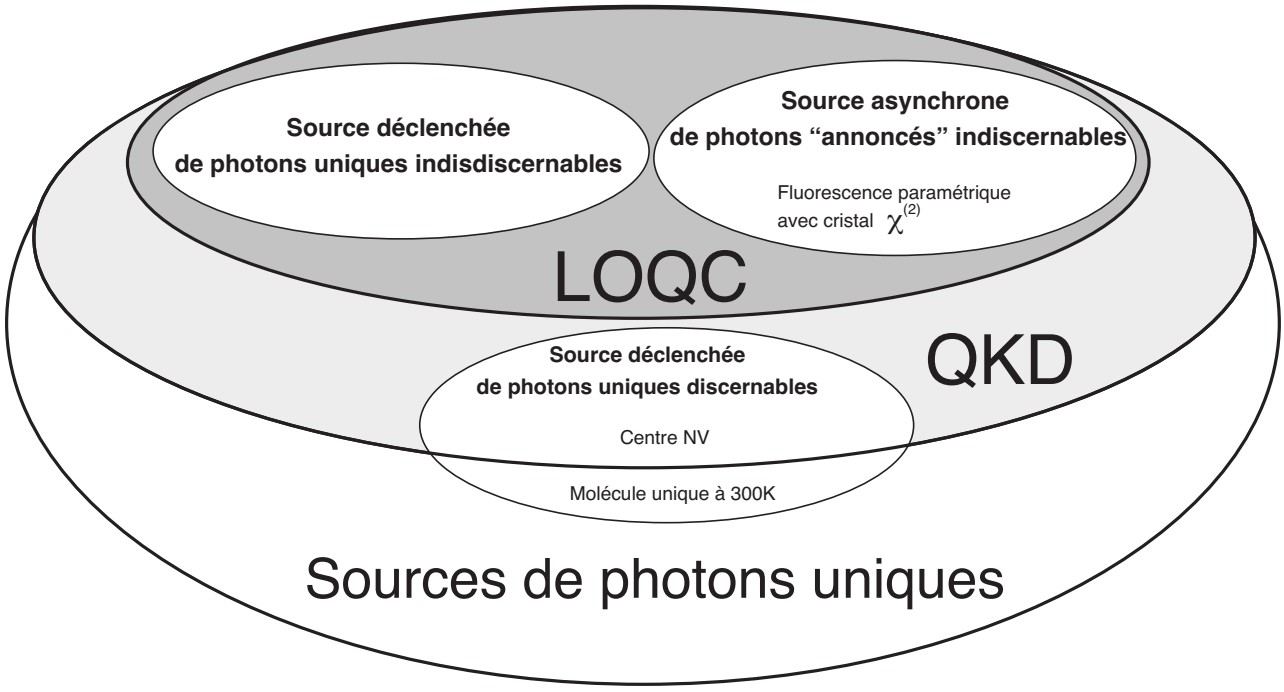

FIG. 2.7 – Classification des sources de photons uniques en fonction des applications pour lesquelles elles sont adaptées. Nous avons placé sur ce schéma les trois systèmes expérimentaux sur lesquels nous avons travaillé dans le cadre de cette thèse : molécule fluorescente unique, centre coloré unique du diamant et source de photons annoncés basée sur la fluorescence paramétrique dans un cristal non-linéaire.

La figure 2.7 propose une synthèse des différents systèmes expérimentaux utilisés jusqu'à présent afin de produire des états à un photon. Nous distinguons parmi ces systèmes d'une part ceux qui sont adaptés au calcul et aux communications quantiques (LOQC) et d'autre part ceux qui ne sont applicables qu'à la cryptographie quantique (QKD), qui ne fait pas nécessairement intervenir les propriétés de cohérence des paquets d'onde. Toutes les sources de photons uniques ont également la propriété d'exhiber une statistique d'émission sub-poissonnienne et se prêtent à l'observation de propriétés non-classiques du rayonne-

ment. On notera cependant que la photostabilité est en pratique nécessaire pour envisager de manière réaliste une application à la cryptographie quantique (notée **QKD**) ce qui impose d'écarter les molécules, tout du moins quand elles sont utilisées à température ambiante.

Chapitre 3

Source moléculaire de photons uniques

Sommaire

3.1 Introduction

Nous évoquons dans ce chapitre les aspects expérimentaux du travail que nous avons effectué autour de la réalisation d'une source moléculaire de photons uniques. Ainsi, après avoir expliqué les enjeux liés à la détection optique d'objets individuels, nous nous intéressons plus spécifiquement aux principes et aux réalisation expérimentales qui structurent les recherches sur l'observation de la fluorescence de molécules uniques. Nous détaillerons ensuite le dispositif expérimental que nous avons réalisé, en présentant tout d'abord son fonctionnement en régime d'excitation continue, où l'on peut observer le phénomène de « dégroupement de photons », avant d'en venir à la constitution et au mode opératoire de la source moléculaire déclenchée de photons uniques.

3.2 Détection optique d'objets individuels : généralités

Si l'élaboration d'une source de photons uniques est un travail qui s'inscrit naturellement dans le champ de l'optique quantique, les techniques sur lesquelles elle repose, liées à l'étude et à l'utilisation des propriétés optiques d'objets individuels, entrent en résonance avec de nombreux autres domaines de recherche. Rendue possible grâce aux progrès conjugués de la microscopie et des techniques de microfabrication, la réalisation d'expériences à l'échelle d'un objet quantique individuel ouvre des perspectives radicalement nouvelles aussi bien pour la physique fondamentale que pour des applications inédites. On peut ainsi mentionner l'apport considérable de ces techniques au domaine de la biologie, notamment à travers l'utilisation d'émetteurs individuels comme marqueurs fluorescents [116, 257]. On peut également faire référence à un grand nombre d'autres applications, comme par exemple l'observation de nouvelles propriétés de transport électronique [255], ou encore l'utilisation des techniques de détection de fluorescence de molécules uniques afin d'étudier une dynamique réactionnelle à l'échelle de l'objet individuel [57].

Qu'il soit obtenu par adressage optique d'une molécule, d'une boîte quantique ou d'une nanoparticule métallique unique, le signal relatif à un émetteur individuel offre des informations souvent inaccessibles dans les mesures d'ensemble pour lesquelles de nombreux émetteurs participent au signal détecté. Outre l'application au traitement quantique de l'information, dont nous avons donné un aperçu au chapitre précédent, un certain nombre d'avantages en découlent directement :

- Lorsqu'il s'agit de mettre en évidence un comportement statistique non-classique, la possibilité d'isoler le signal relatif à un seul émetteur permet de s'affranchir de l'élargissement inhomogène des distributions statistiques lié aux mesures effectuées sur un grand ensemble d'emetteurs différents. L'obtention et l'observation de comportement non-classique du rayonnement en sont ainsi facilitées, et les mesures détaillées au chapitre 4, permettant de discuter le caractère non-classique de l'émission d'une source déclenchée de photons uniques en sont une illustration.

- Un émetteur individuel permet par ailleurs d'obtenir des informations sur l'environnement local dans lequel il est placé. Des objets sub-longueur d'onde tels qu'une molécule unique ou une nano-particule d'or, peuvent en effet constituer des sondes locales très précises, possédant une grande sensibilité au champ électromagnétique local, ou à la présence éventuelle dans leur voisinage d'autres molécules, d'ions voire de surfaces métalliques. Ainsi, couplée aux techniques de spectroscopie non-linéaire comme l'absorption à deux photons la diffusion Raman ou la génération de second harmonique, la détection optique d'objet unique est aujourd'hui une technique de caractérisation extrêmement puissante [254].

- L'excitation d'un émetteur individuel et la détection du signal optique correspondant rend également possible l'étude de la dynamique de systèmes uniques sans pour cela recourir à une synchronisation externe. Les techniques de détection de nano-objets individuels ont ainsi apporté un éclairage nouveau sur les processus de diffusion ou de transfert de charge au sein de systèmes biologiques [60].

La détection optique de molécules uniques, ce « vieux rêve » déjà évoqué par Perrin au début du XX^{eme} siècle [10], est désormais une technique appliquée en spectroscopie et plus largement dans les expériences portant sur l'étude des caractéristiques de fluorescence

de molécules individuelles et qui recouvre un domaine d'activité qui s'est en développé de façon remarquable, en particulier au cours des dix dernières années. Après les premières observations expérimentales effectuées d'abord à basse température [44, 45] puis à température ambiante [46, 47], les expériences sur la fluorescence de molécules uniques se sont multipliées.

Le développement et la diffusion de ces techniques dans la communauté ont fait apparaître clairement les potentialités offertes par de tels émetteurs fluorescents individuels, que l'on peut placer en matrice solide et dont on sait isoler et détecter l'émission aussi bien à basse température qu'à température ambiante. En particulier, les molécules uniques apparaissent comme un système bien adapté en vue de la réalisation d'une source de photons uniques. Les caractéristiques chimiques et spectrales sont en effet bien connues, et beaucoup d'entre elles présentent une efficacité quantique de fluorescence satisfaisante ainsi qu'une force d'oscillateur proche de l'unité pour une section efficace d'absorbtion de l'ordre de l'angström. Enfin, il est relativement aisé de préparer des échantillons de fluorophores de faible concentration en matrice solide.

3.3 Observation de la fluorescence de molécules uniques à température ambiante

Nous introduisons dans cette section les notions et propriétés photophysiques jouant un rôle important dans les expériences portant sur la détection de la fluorescence de molécules uniques.

3.3.1 Système des niveaux d'énergie d'une molécule de colorant

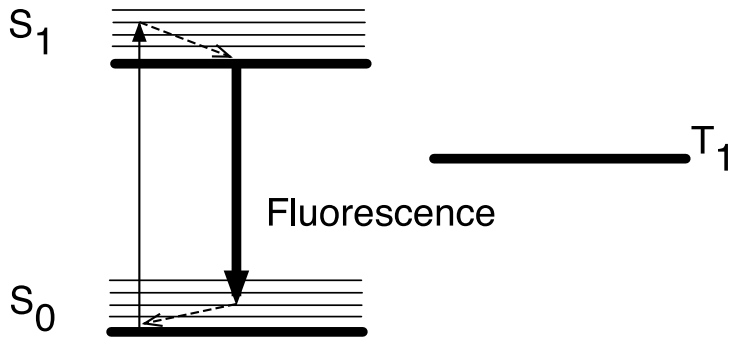

FIG. 3.1 – Diagramme de JABLONSKI des niveaux d'énergie d'une molécule de colorant. Les niveaux S_0 et S_1 correspondent à des états singulet de spin, tandis que le niveau T_1 est associé à une structure triplet. Nous avons représenté en traits plus fins les états vibrationels excités de S_0 et S_1. La *fluorescence* provient de la transition de l'état vibrationnel de plus basse énergie du niveau excité S_1, vers un état quelconque du niveau fondamental S_0. Les flèches en tirets représentent des désexcitations non radiatives. Enfin, la transition $T_1 \rightarrow S_0$, qui correspond à une transition interdite pour l'opérateur dipolaire électrique donne lieu au phénomène de *phosphorescence*.

Les propriétés d'absorption et d'émission des molécules de colorant peuvent être interprétées à l'aide de la représentation schématique des niveaux d'énergie électronique de

JABLONSKI [48, 49] (figure 3.1). Trois types de niveaux sont mis en jeu : deux niveaux singulets de spin S_0 et S_1 et un niveau triplet T_1. La *fluorescence* provient de transitions entre les niveaux singulets. Il arrive cependant que la molécule puisse changer d'état de spin alors qu'elle se trouve dans l'état excité S_1 ; elle passe alors dans le niveau triplet T_1, ce qui correspond à un *croisement inter-système* [1]. La transition $T_1 \rightarrow S_0$ étant interdite, la molécule reste alors dans ce niveau « piège » pendant une durée très grande devant la durée de vie du niveau excité S_1 ; le niveau triplet est ainsi métastable. Le retour de T_1 vers le niveau fondamental S_0 se fait par l'émission d'un photon de *phosphorescence* à des longueurs d'onde que nous ne détectons pas.

Sur la figure 3.1, nous avons également représenté, en traits plus fin, les sous-niveaux d'énergie plus élevée qui sont ceux des états vibrationnels de la molécule. Imaginons que le laser d'excitation, continu ou impulsionnel, porte la molécule dans l'un des états vibrationnels excités du niveau S_1. Celle-ci se désexcite ensuite de façon *non radiative* vers l'état vibrationel de plus basse énergie. Dans le cas où la molécule est insérée dans une matrice solide, ce processus de relaxation se déroule à une échelle de temps de l'ordre de la picoseconde, très courte devant la durée de vie radiative de la transition dipolaire considérée qui est typiquement de l'ordre de quelques nanosecondes. En faisant abstraction du croisement inter-système, on peut ainsi simplifier le diagramme des niveaux d'énergie de la molécule pour aboutir à un simple schéma à quatre niveaux, comme nous l'avons représenté sur la figure 3.11.

3.3.2 Excitation et détection de la fluorescence

La détection d'un émetteur unique fluorescent à température ambiante tire profit du décalage vers le rouge du spectre de fluorescence par rapport au spectre d'absorption (« décalage Stokes ») tel qu'on peut le voir sur la figure 3.4(b). Grâce à ce décalage, il est en effet possible d'exciter la fluorescence à une longueur d'onde λ_{exc} qui ne chevauche que très peu le spectre de fluorescence. La lumière émise par la molécule peut ensuite être séparée spectralement de la lumière de pompage à l'aide d'un simple filtre passe haut ne laissant passer que les longueurs d'onde plus grandes que λ_{exc}.

Par ailleurs, l'utilisation de la microscopie de fluorescence confocale [82] s'est avérée être une technique expérimentale très performante pour observer des molécules uniques à température ambiante. En effet, un microscope confocal couplé à un faisceau laser limité par la diffraction et à un système de photodétection efficace, permet d'atteindre une très grande sensibilité et un très bon rapport signal à bruit dans les acquisitions expérimentales. Un dispositif confocal, dont le principe est détaillé sur la figure 3.3.2 offre en effet l'avantage de présenter une très bonne résolution spatiale et permet d'obtenir un grand rapport signal à bruit dans les expériences de détection de la fluorescence d'un objet unique. Ce point sera illustré par un calcul d'ordre de grandeur dans la section 3.4.1.

Enfin, des photodiodes à avalanche, fonctionnant en régime de comptage de photon, sont généralement utilisées dans le cadre d'expériences relatives à l'étude de la fluorescence de molécules uniques. Les photodiodes à avalanche au silicium dont le pic de sensibilité est situé à 700 nm, sont à cet égard particulièrement bien adaptées. En effet, leur fenêtre de sensibilité spectrale (450 - 900 nm) s'accorde bien avec le spectre de fluorescence de la plupart des molécules, et l'efficacité quantique de ces photodétecteurs commerciaux atteint 70 % autour de 700 nm.

[1] Nous utiliserons parfois la notation ISC en référence au terme anglais d' *inter-system crossing*.

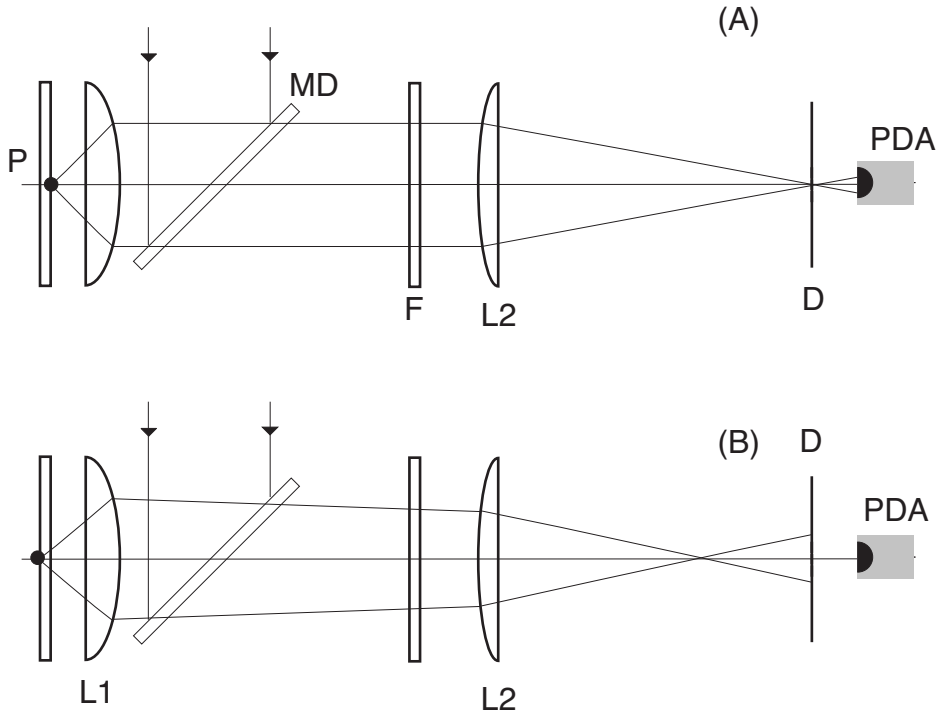

FIG. 3.2 – Schéma expliquant le principe du microscope confocal. (A) La lumière d'excitation est réfléchie sur un miroir dichroïque vers un objectif de microscope, puis focalisée sur l'échantillon. La lumière rayonnée en retour par l'échantillon (en particulier la lumière de fluorescence) est collectée par le même objectif, filtrée spectralement de la lumière de pompe puis focalisée sur un trou de faible diamètre, qui joue le rôle de filtre spatial. On peut se convaincre, à l'aide du schéma (B) que seuls les rayons lumineux provenant d'une région spatiale limitée autour du plan objet de l'objectif de microscope seront détectés efficacement, ce qui d'isoler la lumière provenant d'un faible volume de l'échantillon[271]. E : échantillon ; L1, L2 : lentilles ; MD : Miroir dichroïque ; F : filtre spectral ; D : diaphragme ; PDA : détecteur (photodiode à avalanche dans notre expérience).

3.3.3 Le problème du photoblanchiment

Comme nous venons de l'expliquer, les molécules uniques paraissent « concentrer » les propriétés qui en font des émetteurs fluorescents idéaux pour une grande variété d'usages et en particulier la réalisation d'une source de photons uniques. Néanmoins, la photo-stabilité réduite des molécules fluorescentes à température ambiante constitue une limitation majeur pour l'utilisation de ces émetteurs. Sous excitation lumineuse, les molécules subissent en effet une transformation chimique après avoir émis un certain nombre de photons, qui altère de manière irréversible leurs propriétés fluorescentes. De manière générale, et pour des conditions usuelles d'excitation optique en régime continu, la probabilité de photoblanchiment varie entre 10^{-5} pour les molécules de colorant en solution [66] et 10^{-6} pour les molécules en matrice polymère [64].

Les processus physico-chimiques à l'origine du photoblanchiment sont à l'heure actuelle encore relativement mal compris. On l'associe généralement à des réactions d'oxydation irréversible intervenant à partir d'états multi-excités de la molécule [63]. On pense par conséquent que les réactions associées au photoblanchiment sont activées par la présence

de dioxygène, hypothèse confirmée par l'exceptionnelle photostabilité observée pour des molécules placées dans un cristal moléculaire tel que le p-terphényl [67] pour lequel la probabilité de photoblanchiment est de l'ordre de 10^{-8} [2]. Des résultats récents [69] ont rapporté l'observation de rendements de photoblanchiment réduits d'un facteur de l'ordre de 60 en passant de l'air à une atmosphère constituée par un flux de diazote. Cette augmentation de la durée de vie de la molécule s'accompagne cependant de modifications de la transition vers l'état triplet T_1, où la molécule cesse alors de fluorescer. Les deux effets conjugués aboutissent au final à un nombre total de photons émis par la molécule (jusqu'au photoblanchiment) sensiblement égal avec ou sans flux de diazote.

Pour notre part, nous n'avons par cherché à axer notre travail sur l'amélioration de la photostabilité des molécules uniques, nous contentant simplement d'une démarche pragmatique permettant de maximiser le nombre total de photons détectés pour notre dispositif expérimental.

3.4 Dispositif expérimental pour l'excitation et la détection de la fluorescence d'une molécule unique

Molécule unique dans un film mince polymère transparent

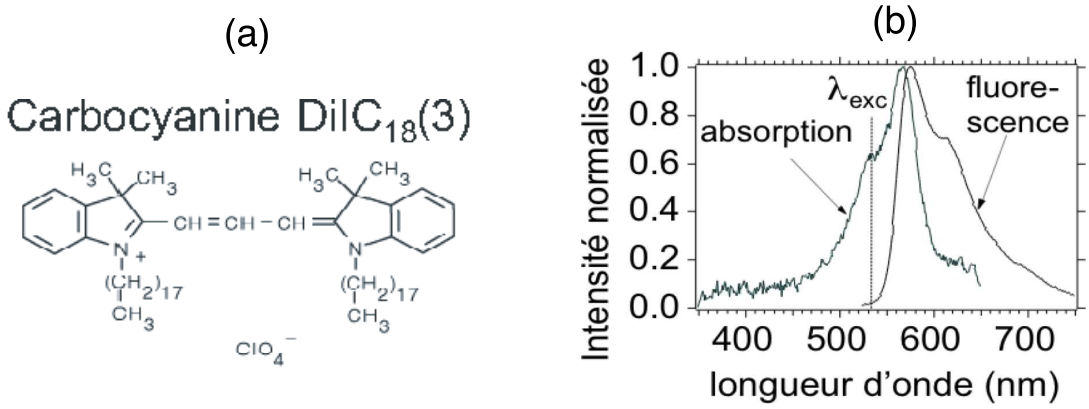

FIG. 3.3 – (a) Structure chimique de la molécule de carbocyanine, de formule $\mathrm{DiIC}_{18}(3)$. (b) Spectres de fluorescence et d'absorption de cette molécule. Le décalage vers le rouge du spectre de fluorescence par rapport au spectre d'absorption, communément appelé *décalage de* STOKES, se comprend aisément à partir de la figure 3.1. Ce décalage permet de réaliser une excitation de la molécule à l'aide d'un laser à 532 nm, en dehors de la bande de fluorescence. Ainsi, les photons « parasites »à la longuer d'onde d'excitation, dus essentiellement à la diffusion Rayleigh par l'échantillon, pourront être supprimés de manière sélective au moyen d'un filtre spectral adapté.

Les résultats présentés dans ce chapitre ainsi que dans le chapitre suivant, ont été obtenus avec des molécules de carbocyanine $\mathrm{DiIC}_{18}(3)$ dont nous présentons la structure chimique sur la figure 3.4. Ce choix de colorant a été déterminé en raison de sa forte efficacité quantique, et de sa bonne photostabilité.Ce colorant présente de plus une section efficace d'absorption de l'ordre de 2 Å^2 [74] (ce qui correspond à l'ordre de grandeur « standard »)

[2] Des observations similaires ont également été reportées en utilisant une matrice de cristaux liquides [65]

et une durée de vie radiative relativement courte (environ 3 ns) ce qui est un critère important pour les expériences que nous souhaitons mener.

Nous avons également choisi d'incorporer ces molécules fluorescentes dans un film mince de polymère, déposé sur une lamelle de microscope[3].

Les échantillons dont nous donnons une vue schématisée sur la figure 3.4 sont intégralement préparés au laboratoire LPQM, en utilisant pour cela sa salle blanche et les facilités de fabrication et de caractérisation qui y sont associées. Voici les principales étapes de la préparation des échantillons :

- Les lamelles de microscope sont décapées en étant plongées pendant plusieurs heures dans un « bain piranha » composé d'un mélange d'acide sulfurique et d'eau oxygénée, qui dégrade efficacement toute impureté de type « biologique »
- On prépare une solution de PMMA dans le toluène ainsi que des solutions graduellement diluées de carbocyanine que l'on mélange ensuite à la solution de PMMA.
- On rince abondamment les lames de verre à l'eau distillée, jusqu'à obtenir un pH proche de 7 pour l'eau de rinçage.
- Le dépôt du polymère PMMA dopé en molécules de cyanine sur les lames de verres est effectué à la tournette, dont la vitesse est fixée de façon à produire des couches uniformes d'environ 30 nm d'épaisseur, mesurée à l'aide d'un profilomètre optique.
- Les échantillons sont ensuite placés à l'étuve à 120°C pendant plusieurs heures afin d'assurer la polymérisation du PMMA.
- On teste les différents échantillons sur notre montage de microscopie confocale à balayage afin de s'assurer de la propreté du dépôt et de déterminer les échantillons pour lesquels la concentration surfacique en molécule est satisfaisante, de l'ordre de une molécule par μm^2. Seuls ces échantillons seront ensuite utilisés.

Après des premiers tests effectués sur des molécules de terrylène dispersées dans des cristaux de p-terphényl, nous avons ainsi pu gagner près d'un ordre de grandeur sur le rapport signal à fond en insérant les molécules dans un mince film polymère, les échantillons correspondant typiquement à un rapport signal à bruit de fond de l'ordre de 30 dans les expériences de détection de la fluorescence d'une molécule unique.

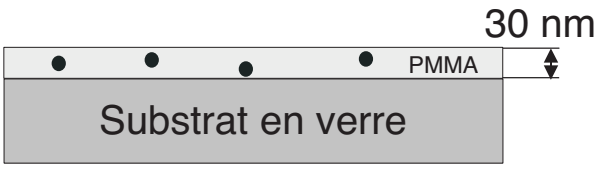

FIG. 3.4 – Échantillons réalisées pour l'observation de molécules uniques, obtenus par dépôt sur une lamelle de verre d'une solution de colorant dilué dans du PMMA

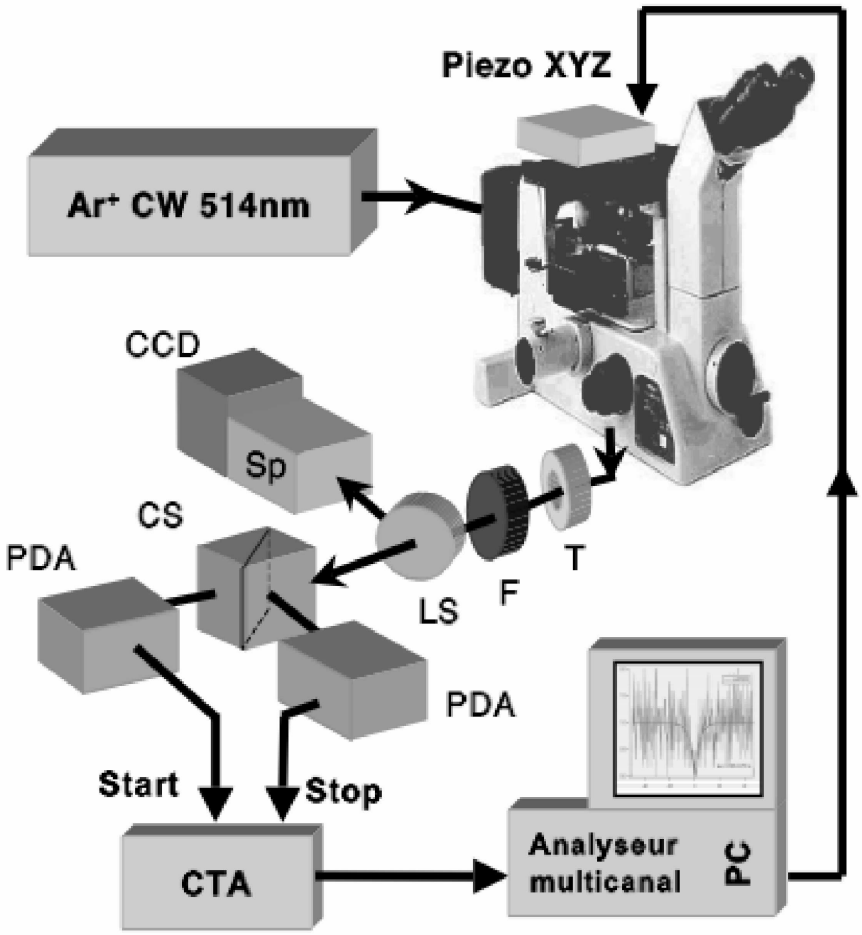

FIG. 3.5 – Schéma de l'expérience en régime d'excitation continue, effectuée avec un laser argon à la longueur d'onde λ_p=514.5 nm. Piezo XYZ : platine de translation 3-D piézoélectrique ; T : diaphragme (diamètre 30-50 μm) assurant la « confocalité » de la détection optique ; F : filtre réjecteur de type « Notch » centré sur λ_p, ou filtre passe-haut pour $\lambda > \lambda_p$; LS : lame séparatrice ; CS : cube séparateur 50/50 insensible à l'état de polarisation de la lumière ; PDA : photodiode à avalanche en régime de comptage de photons ; CTA : convertisseur temps-amplitude ; Sp : spectrographe imageur utilisant un réseau concave ; CCD : matrice CCD silicium de 1024×128 pixels, refroidie à $\approx -60°$C.

Microscope confocal à balayage

Fonctionnant en régime d'excitation continue représenté sur la figure 3.5, le montage expérimental repose sur l'utilisation d'un microscope commercial en configuration inversée[4]. La fluorescence de l'échantillon est excitée continûment à l'aide d'un laser argon à la longueur d'onde de 514.5 nm, dont le faisceau est injecté dans le microscope après son épuration par passage dans une fibre optique monomode. Ce faisceau est réfléchi par un miroir dichroïque incliné à 45°, avant d'être focalisé sur l'échantillon à l'aide d'un objectif de microscope à immersion de grande ouverture numérique[5]. La fluorescence d'une zone de l'échantilllon d'une taille d'environ 10×10 μm est étudiée en déplaçant pas à pas ce dernier. Ce déplacement est obtenu au moyen d'une platine piézoélectrique pouvant assurer un déplacement dans les trois directions de l'espace avec une résolution nanométrique [6].

Les photons de fluorescence sont collectés par le même objectif de microscope qui en fait un faisceau parallèle. Ce faisceau est focalisé dans un diaphragme qui assure la « confocalité » de la détection optique (cf. figure 3.3.2). Cette configuration permet de sélectionner la lumière provenant sélectivement d'un volume de l'échantillon de l'ordre de 1 μm^3, réduisant ainsi, par rapport à la microscopie classique, la lumière parasite due à la fluorescence de toute la zone de substrat illuminé par le faisceau d'excitation laser. Le faisceau est ensuite collimaté, filtré spectralement, puis focalisé sur des photodiodes à avalanche au silicium fonctionnant en régime de comptage de photons. Ces dernières sont reliées à une chaîne de comptage et toute l'électronique est pilotée par un ordinateur. Les systèmes de scan de l'échantillon et de comptage des coups de photodétection ont été réalisés par André CLOUQUEUR, ingénieur électronicien au LPQM.

Pour certaines expériences, nous avons également eu besoin d'analyser spectralement la lumière de fluorescence. Pour cela, nous avons construit un spectrographe imageur constitué d'un réseau concave qui produit l'image du spectre sur une matrice CCD au silicium. Ce capteur peut être refroidi à une température de -60°C afin de diminuer son bruit d'obscurité.

Scan de l'échantillon

L'échantillon contenant les molécules uniques est solidaire du déplacement de la platine de translation, dont le mouvement est piloté par ordinateur et synchronisé avec notre système de photodétection. Nous pouvons ainsi effectuer des scans de l'échantillon, correspondant au déplacement de celui-ci par rapport au faisceau laser et, pour chaque pas de la platine nanométrique, enregistrer l'intensité du signal détecté.

Quand les réglages optiques sont satisfaisants, c'est-à-dire notamment quand la couche contenant les molécules est confondue avec le plan focal objet de l'objectif et quand l'axe optique est centré sur le diaphragme de confocalité, le signal enregistré au cours d'un scan fait apparaître un certain nombre de pics de fluorescence, comme sur la figure 3.6. Cette première étape permet de juger de la qualité d'un échantillon, par le rapport signal à bruit des pics de fluorescence, et de repérer la position des centres émetteurs.

[3] Notons, qu'à la fin des années quatre vingt dix, les molécules uniques étaient étudiées à température ambiante essentiellement dans des matrices hôtes cristallines apportant une grande photostabilité [67]. La matrice hôte est cependant à l'origine d'un bruit de fond bien plus important que celui généré par un film mince polymère. Ce bruit de fond vient en partie masquer les propriétés d'émission de photon unique par la molécule ce qui constitue une limitation importante lorsque l'on souhaite pouvoir observer une statistique de photons

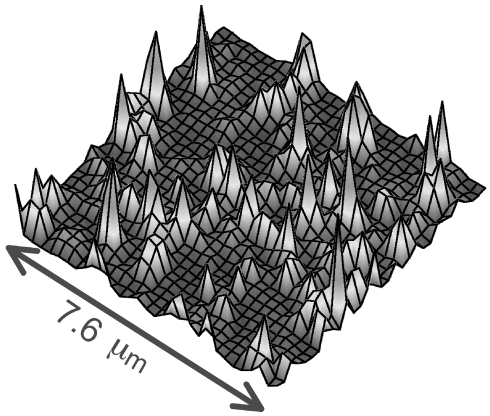

FIG. 3.6 – Pics de fluorescence tels qu'ils apparaissent lors du scan d'un échantillon à l'aide du dispositif de microscopie confocale.

Photodétection

Nous utilisons pour détecter les photons émis par les molécules fluorescentes, deux photodiodes à avalanche au silicium de type AQR 14, manufacturées par Perkin-Elmer, que nous faisons fonctionner en régime de comptage « libre » dit aussi mode GEIGER, où aucune information temporelle complémentaire n'est fournie pour un éventuel fenêtrage temporel des photodiodes. Ces photodiodes sont caractérisées par un taux de coups d'obscurité d'environ 100 coups/s , un temps mort de 30 ns et une gigue de 700 ps. À la longueur d'onde d'émission de la molécule de carbocyanine $\mathrm{DiIC}_{18}(3)$, l'efficacité des détecteurs est d'environ 60% (cf figure 3.7)

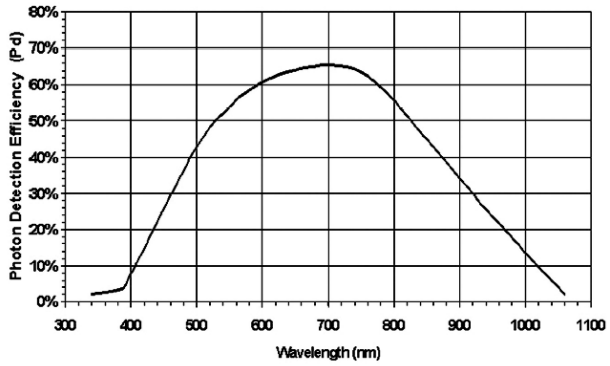

FIG. 3.7 – Efficacité quantique des photodiodes à avalanche AQR14 en fonction de la longueur d'onde (source : Perkin Elmer).

Les expériences de type Start – Stop, utilisant les signaux de photodétection des deux photodiodes à avalanches s'appuient sur la grande précision temporelle de ces dernières

fortement non-classique.

[4]Ce dispositif a été mis en place par François TREUSSART et Jean-François ROCH avant le début de ma thèse.

[5]Objectif $\times 60$ ou $\times 100$, avec une ouverture numérique ON=1.3 ou ON=1.4 respectivement.

[6]Cette platine est asservie dynamiquement en position par l'intermédiaire de jauges de contrainte.

et nécessitent par ailleurs de recourir à des précautions particulières pour limiter les effets de diaphonie. Même si le nombre d'événements causés par ce phénomène est faible, le fait qu'ils apparaissent toujours en coïncidence sur les deux détecteurs peut être à l'origine d'artefacts importants dans les mesures d'autocorrélation en intensité. On peut distinguer deux types de diaphonie :

- Diaphonie électrique
  La diaphonie électrique apparaît typiquement lorsque les signaux électriques issus des photodiodes à avalanche sont traités dans le même circuit électronique. Une impulsion sur la voie Start peut alors entraîner une réplique électronique déclenchant la voie Stop, ce qui va donc toujours provoquer une coïncidence Start/Stop. Nous avons résolu ce problème en prêtant un soin particulier à l'isolement électrique des voies d'entrée Start et Stop du circuit de conversion temps-amplitude dont nous avons adapté les impédances d'entrée de façon à éviter les phénomènes de rebonds. Le problème de diaphonie électrique semble en revanche ne pas se poser lors des acquisitions à l'aide de la carte TIA (cf. après pour une description de cette carte).

- Diaphonie optique
  La diaphonie optique est dûe au fait que l'avalanche d'électron associé à une photodétection s'accompagne également d'une émission de photons [237] dont le spectre, d'environ 300 nm de largeur, est centré sur la longueur d'onde 850 nm. Même si le nombre de photons ainsi émis est relativement faible (approximativement 43 photons par avalanche [237]), ces photons si ils parviennent à la deuxième photodiode à avalanche, sont systématiquement à l'origine de coïncidences et perturbent donc fortement la précision des mesures de corrélations d'intensité au temps courts. Nous avons résolu ce problème en plaçant devant l'une des photodiodes à avalanche un filtre interférentiel ne laissant passer que les longueurs supérieures à 750 nm.

Enfin, il convient de mentionner que dans le cadre des expériences décrites au chapitre suivant, où notre méthode d'acquisition est basée sur une carte numérique de type TIA, le temps mort de chacune des voies du système de photodétection est limité par le temps de réponse électronique de la carte. Nous avons mesuré ce temps en testant les coïncidences avec lui-même du signal détecté sur une photodiode et envoyé sur la carte TIA, lors d'une excitation à l'aide d'un laser continu fortement atténué. Comme on peut le voir sur la figure 3.8, le temps mort électronique apparaît ainsi clairement : il est de 240 ns et domine donc le temps mort « physique » des détecteurs, qui est de 30 ns.

3.4.1 Évaluation du rapport signal à bruit

De simples ordres de grandeur permettent d'évaluer le rapport signal à bruit pour la détection de la fluorescence d'une molécule unique dans une matrice solide à température ambiante [50], au moyen de l'expression suivante :

$$\frac{S}{\text{Bruit}} = \frac{(\eta_{\text{tot}}\phi_F\sigma_p P_0 T)/(Ah\nu)}{\sqrt{(\eta_{\text{tot}}\phi_F\sigma_p P_0 T)/(Ah\nu) + C_b P_0 \tau + N_d T}}, \tag{3.1}$$

où S représente le nombre de coups de photodétection dus à la fluorescence d'une seule molécule pendant une durée d'intégration T, ϕ_F représente l'efficacité quantique de la molécule, σ_p est la section efficace d'absorption à résonance, P_0 la puissance d'excitation laser, A l'aire

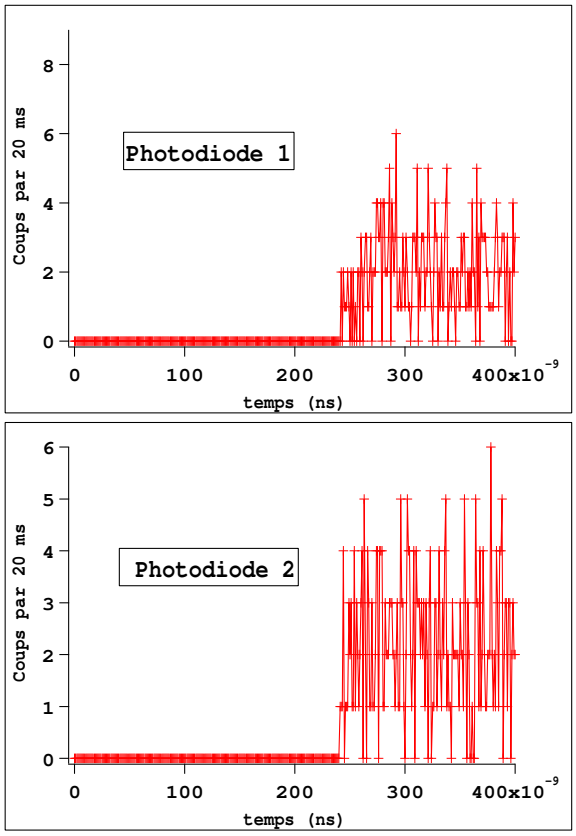

FIG. 3.8 – Autocorrélation avec lui-même du signal de photodétection d'une photodiode à avalanche en régime d'excitation continu. L'absence de coïncidences pour un temps inférieure à 240 ns est la signature d'un temps mort de nature électronique, causé par le TIA.

de la tache de focalisation, $h\nu$ l'énergie des photons de pompe, N_d le nombre de coups d'obscurité des détecteurs par unité de temps. Enfin, le paramètre C_b correspond au nombre de coups d'obscurité par seconde et par unité de puissance d'excitation et est dû au fond de fluorescence, tandis que η_{tot} représente l'efficacité totale de collection et de détection des photons émis, prenant en compte l'efficacité quantique des photodétecteurs.

Les trois termes qui s'ajoutent au dénominateur de la relation (3.1), sous la racine carrée, sont associés respectivement au bruit de grenaille de la lumière de fluorescence, à celui du fond de fluorescence dû à la matrice hôte et enfin aux coups d'obscurité des détecteurs. D'après cette relation, on constate que le rapport S/Bruit est d'autant plus grand que l'efficacité quantique de l'émetteur et sa section efficace d'absorption sont grandes, et que l'aire du spot d'excitation est petite. Si l'on prends les ordres de grandeurs propres à notre expérience : $A \approx 10^{-9}$ cm^2, $\eta_{\text{tot}} \approx 0.05$, $\phi_F \approx 0.8$, $P_0 \approx 100$ μW à $\lambda = 514.5$ nm (ce qui fait $h\nu \approx 3.9 \times 10^{-19}$ J), $\sigma_p \approx 2 \times 10^{-16}$ cm^2 (d'après [74]), une contribution du fond de fluorescence[7] pour $1/30^{\text{e}}$ de celle du nombre de coups de fluorescence, et finalement $N_d = 100$ coups/s, alors $S/\text{Bruit} \approx 100$ pour un temps d'intégration T de 20 ms. Ce résultat est ainsi très voisin du bruit de photon associé au signal de fluorescence, le fond et les courants d'obscurité des détecteurs n'ayant qu'une faible contribution à des échelles de temps

[7] Dans ce fond, on prend également en compte la diffusion RAYLEIGH de la lumière de pompage.

de l'ordre de la vingtaine de millisecondes.

On voit donc qu'il est non seulement aisé de détecter une molécule individuelle à température ambiante et que toute modification de la statistique du bruit de cette source pourra être aisément détectée, comme nous le ferons par la suite.

3.5 Unicité de l'émetteur et dégroupement de photon

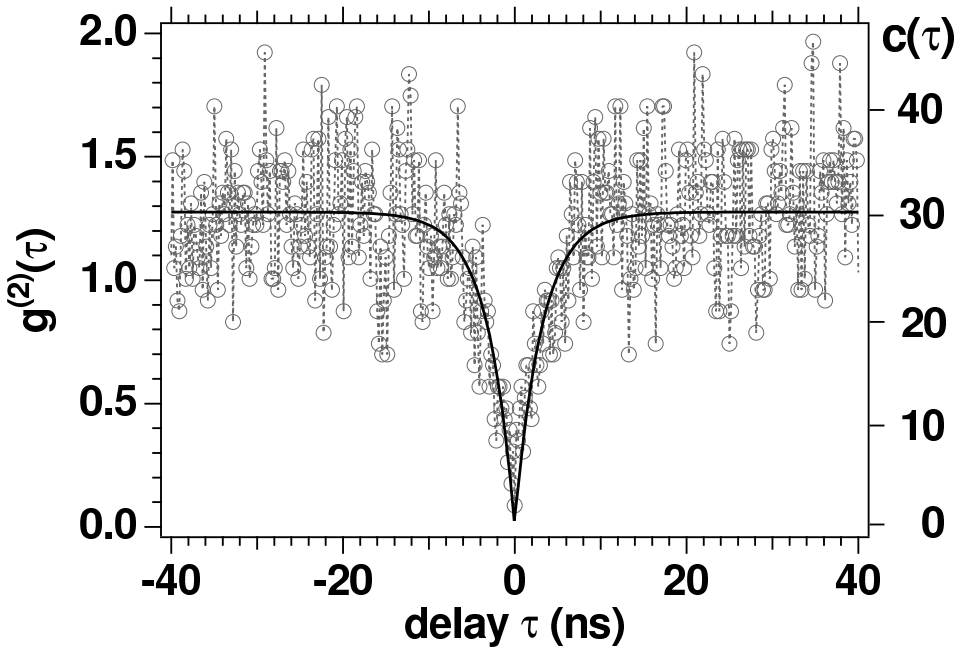

FIG. 3.9 – -○- : fonction d'autocorrélation en intensité $g^{(2)}(\tau)$ obtenue pour une molécule de terrylène dans un film mince de polymère PMMA [71]. Les valeurs de $g^{(2)}(\tau)$ sont déduites du nombre de coïncidences $c(\tau)$ (échelle de droite) enregistrées pendant la durée de l'expérience. Temps d'intégration : 100.4 s. On observe le « dégroupement de photons » correspondant à l'absence de coïncidences au retard $\tau = 0$ et caractéristique de l'unicité de l'émetteur. Le fait que pour $|\tau| \geq 40$ ns, la fonction d'autocorrélation $g^{(2)}(\tau)$ prenne une valeur supérieure à l'unité – valeur correspondant à ce que donnerait une source de lumière dont les fluctuations d'intensité suivant une statistique poissonienne – est dû au passage de la molécule par le niveau triplet métastable. Dès que la molécule quitte ce niveau piège, elle peut de nouveau se mettre à fluorescer. À l'échelle de temps de la durée de vie du niveau triplet, les photons semblent être émis par paquets (« groupement de photons ») . En trait plein : ajustement des données expérimentales par un modèle faisant intervenir les trois niveaux S_0, S_1 et T_1 du diagramme de JABLONSKI.

La caractérisation de l'unicité de l'émetteur est effectuée grâce à la mesure des corrélations temporelles de l'intensité de fluorescence $I(t)$, correspondant au nombre de photons détectés par seconde à l'instant t. Si l'émetteur est un objet quantique individuel, il ne peut en effet fluorescer qu'en émettant un seul photon à la fois [167, 88]. En construisant alors l'histogramme des retards entre deux photons consécutivement détectés en provenance de l'émetteur, il apparaît un « trou » dans la distribution des coïncidences aux temps « courts » dû au fait que deux photons émis à la suite l'un de l'autre sont au moins séparés d'une durée de l'ordre de la durée de vie de l'état excité de l'émetteur [36]. Ce phénomène de

dégroupement de photons a été une des premières propriétés non-classiques de la lumière mise en évidence [35], en utilisant des atomes dans un jet atomique de très faible intensité. Depuis cette première réalisation, il a été observé et il a été observé avec de très nombreux types d'émetteurs autres que les atomes : ion isolé dans un piège magnétique [130], molécules isolées [77, 43], centres colorés dans le diamant [88, 85], boîtes quantiques de semiconducteur [100, 118]. Le phénomène de dégroupement de photon est *caractéristique* de la lumière produite par un émetteur individuel, et son observation constitue donc un diagnostic direct de l'unicité de l'émetteur.

En pratique, chaque photodétection est suivie d'un temps mort d'une durée d'environ 30 ns, nécessaire à la repolarisation de la photodiode aprés le processus d'avalanche. Ainsi, pour mesurer les corrélations d'intensité aux retards courts il est nécessaire de recourir à l'utilisation de deux détecteurs.

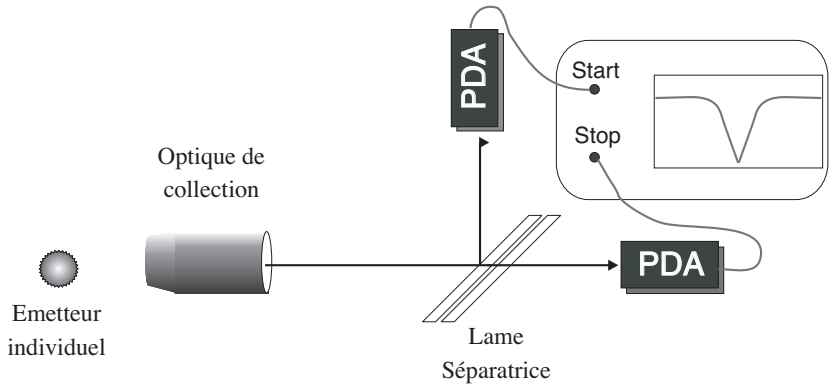

FIG. 3.10 – Représentation schématique d'un montage de type HANBURY-BROWN et TWISS permettant la mesure de la fonction d'autocorrélation en intensité d'un champ lumineux, en régime de comptage de photons. La lame séparatrice 50 / 50 répartit aléatoirement les photons vers les deux photodiodes à avalanche (PDA) et le signal provenant des deux détecteurs est envoyé à un corrélateur

Afin de caractériser de façon non ambiguë le caractère dégroupé de l'émission des photons par la source, on évalue la fonction d'autocorrélation en intensité de la lumière à l'aide du montage de type HANBURY-BROWN et TWISS [32], où les deux détecteurs sont placés de part et d'autre d'une lame séparatrice 50 /50 (cf. figure 3.10). En procédant à des mesures de l'intervalle de temps séparant une photodétection sur une voie de la photodétection suivante sur l'autre voie (méthode dite START - STOP), on peut s'affranchir de l'effet des temps mort et accéder à une statistique non biaisée même à des retards proches de zéro. Les deux photodiodes, produisant une impulsion de tension à chaque photodétection, sont reliées à un convertisseur temps-amplitude (CTA) dont la sortie alimente un analyseur multicanal. Ce système trace « en temps réel » l'histogramme des intervalles de temps entre deux photons consécutivement détectés sur l'un puis l'autre des deux détecteurs. Sous certaines

conditions de validité [38], cet histogramme est directement relié, via une normalisation adéquate [88], à la fonction d'autocorrélation en intensité $g^{(2)}(\tau) \equiv \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle^2}$. Nous préciserons ces notions statistiques et les hypothèses afférentes au chapitre suivant.

Les données présentées sur la figure 3.9, correspondant à l'enregistrement de la fonction d'autocorrélation en intensité illustrent cette mesure, pour une molécule de terrylène dans un film polymère de PMMA [71]. L'absence de coïncidence à l'intervalle de temps nul constitue en effet une preuve directe que l'on détecte bien la fluorescence provenant d'un seul émetteur quantique, en l'occurrence ici d'une molécule isolée de terrylène.

Remarquons enfin que l'immobilisation des émetteurs dans la matrice solide est absolument nécessaire à l'observation de ce dégroupement de photon. Pour des molécules en solution, le mouvement d'agitation thermique et les fluctuations du nombre de molécules dans la zone d'interaction avec le faisceau laser excitateur font disparaître cet effet, la fonction $g^{(2)}(\tau)$ prenant alors des valeurs toujours supérieures à l'unité [73], même pour le délai nul.

3.6 Source déclenchée de photons uniques

3.6.1 Principe de la génération de photon un par un

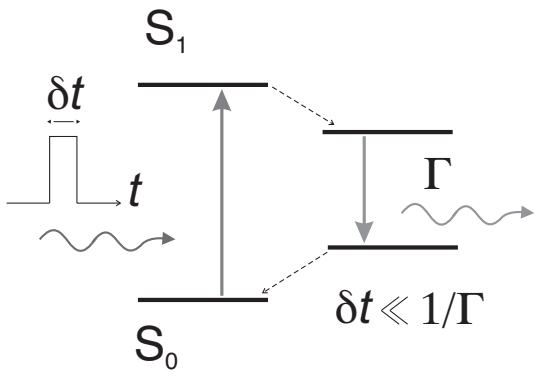

FIG. 3.11 – Schéma de principe d'une source de photons uniques déclenchée, fondée sur la modélisation des niveaux d'énergie d'un fluorophore par un système à quatre niveaux. Une impulsion excitatrice suffisamment brève et intense porte le système dans un état vibrationel du niveau excité S_1. De là, il se désexcite d'abord rapidement de façon non-radiative (flèches en pointillés), puis émet un photon unique dans la durée de vie $\tau_0 \equiv 1/\Gamma$ du niveau S_1 avant de revenir dans l'état fondamental du niveau S_0. Dans la limite où la durée de l'impulsion d'excitation δt est très courte devant la durée de vie de fluorescence $\tau_0 = 1/\Gamma$, le système ne peut émettre qu'un seul photon par impulsion d'excitation.

Afin de réaliser une source déclenchée de photons uniques à partir de la fluorescence d'un molécule, nous avons utilisé le principe proposé et mis en œuvre pour le première fois par Francisco DE MARTINI [167]. Il consiste à piloter de manière incohérente l'excitation d'une molécule unique, au moyen d'impulsions brèves permettant de déclencher l'émission de photons uniques.

Le principe d'une telle source déclenchée de photons uniques est illustré sur la figure 3.11. On porte, par une excitation brève, un émetteur unique de son état fondamental vers un état excité. Dans la limite où l'impulsion excitatrice est à la fois suffisamment intense et

en même temps suffisamment brève, on assure conjointement une importante probabilité de transition vers l'état excité, tout en limitant fortement la probabilité que l'émetteur effectue un double cycle « absorption –émission – absorption ». Nous verrons dans les paragraphes suivants comment quantifier plus précisément ces conditions sur la puissance et la durée des impulsions. Pour qu'au plus un photon soit produit pour chaque impulsion d'excitation, il faut en outre que ces dernières soient séparées temporellement les unes des autres d'une période beaucoup plus grande que la durée de vie τ_0 de l'état excité afin de garantir que le système moléculaire soit bien revenu dans son état fondamental avant l'application de l'impulsion suivante. Dans notre cas, la cadence du laser est choisie égale à 8 ou 2 MHz suivant l'électronique utilisée et dans les deux cas le taux de désexcitation radiative $1/\tau_0 \approx 300$ MHz, correspondant à une durée de vie de la molécule $\tau_0 \approx 3$ ns, est très grand devant cette cadence d'excitation.

La première source déclenchée de photons uniques opérant à température ambiante a été réalisée en 2000 par Brahim LOUNIS , alors dans le groupe de W.E MOERNER [43]. Cette première expérimentale, fondée sur l'observation de la fluorescence d'une molécule unique de terrylène dans un cristal de p-terphenyl, placée sous excitation impulsionnelle, a en quelque sorte ouvert la voie tracée par la proposition de Francisco DE MARTINI [167], vers l'obtention de photons uniques à l'aide d'émetteurs uniques à température ambiante. Les travaux que nous décrivons dans ce chapitre se placent dans le prolongement direct de cette première expérience, effectuée dans notre cas à partir d'une molécule d'une molécule fluorescente de carbo-cyanine [75, 171].

Conditions sur la durée des impulsions excitatrices

Afin d'éviter qu'un deuxième photon soit émis pour la même impulsion d'excitation, il est nécessaire que le système moléculaire soit encore dans son état excité à la fin de l'impulsion [88]. Ainsi, il lui sera impossible de réabsorber de la lumière de pompe pour émettre un second photon. Cette condition est d'autant mieux réalisée que l'impulsion est d'une durée δt très courte devant la durée de vie τ_0 du niveau excité . Dans notre expérience, nous avons utilisé des impulsions femtosecondes de durée $\delta t \approx 150$ fs. La probabilité que le photon soit émis avant la fin de l'impulsion est inférieure à $1 - \exp(-\delta t/\tau) \approx 5 \times 10^{-5}$. La molécule est donc encore dans son état excité, avec une probabilité très proche de l'unité, à la fin de l'impulsion.

En pratique, la « qualité statistique » de la lumière émise par une telle source de photons uniques n'est pas limitée par la durée des impulsions excitatrices mais par le fond résiduel de fluorescence qui vient se superposer à la fluorescence de la molécule unique.

Conditions sur la puissance des impulsions excitatrices

Afin d'obtenir une source de photons uniques la plus efficace possible, nous avons cherché à nous placer dans un régime de saturation de la transition $S_0 \rightarrow S_1$ [8]. Travailler dans ce régime d'excitation pose des problèmes spécifique. Par son influence sur l'environnement local de la molécule, elle conduit très certainement à une modification des propriétés photophysiques telles que la probabilité de basculer vers l'état triplet ou la probabilité de photoblanchiment [64]. Aussi en pratique avons-nous simplement cherché à travailler avec une puissance d'excitation juste suffisante pour assurer une probabilité de transition $S_0 \rightarrow S_1$ proche de l'unité.

[8] On notera que notre approche se distingue ainsi de travaux tels que [56, 68].

Afin d'évaluer l'énergie par impulsion nécessaire pour saturer cette transition, nous avons enregistré la variation du taux de comptage en fonction de l'énergie par impulsion d'excitation. Nous avons représenté sur la figure 3.6.1 une courbe caractéristique obtenue lors de ces mesures. Les brusques variations d'intensité sont dues à des passages de la molécule dans le niveau triplet et nous avons cherché à corriger nos données de cette influence du triplet. En utilisant un modèle d'équations cinétiques entre deux niveaux simplement couplés par des processus d'absorption et d'émission, nous pouvons calculer le taux de population σ de l'état excité à l'instant τ_{p} suivant l'arrivée de l'impulsion excitatrice :

$$\sigma = \frac{E_{\mathrm{p}}/E_{\mathrm{sat}}}{(1+E_{\mathrm{p}}/E_{\mathrm{sat}})}\left(1-e^{-\frac{\tau_{\mathrm{p}}}{\tau_0}\left(1+\frac{E_{\mathrm{p}}}{E_{\mathrm{sat}}}\right)}\right). \tag{3.2}$$

Dans cette équation, l'interprétation du paramètre E_{sat} n'est pas immédiate. On peut l'expliciter en considérant qu'il faut déployer, durant le temps de vie τ_0 de la molécule, une puissance E_{sat}/τ_p afin d'assurer la saturation de la transition $S_0 \rightarrow S_1$.

Les données $R(E_{\mathrm{p}})$ présentées sur la figure 3.6.1 sont exprimées sous la forme de la fonction $R = R_0 \times \sigma$ à l'aide d'une procédure d'ajustement en deux temps. Après un premier ajustement effectué sur les données brutes, les points inférieurs de plus d'une déviation standard à la première équation d'ajustement sont attribués à l'influence de l'état triplet et sont supprimés. L'ajustement sur les donnée restantes permet de calculer : $R_0 = 160 \times 10^3$ coups/s et $E_{\mathrm{sat}} = 5.6 \times 10^{-5}$ pJ.

Afin d'optimiser le nombre de photons émis par la source et éviter ainsi un blanchiment trop rapide, nous avons ensuite fixé la valeur maximale de l'excitation à placés à une énergie par impulsion d'excitation $E_{\mathrm{p}}^{\mathrm{max}} = 5.6$ pJ. D'après l'équation (3.2), cette valeur correspond à une probabilité de transition vers l'état excité de 97%.

3.6.2 Dispositif expérimental impulsionnel

Le dispositif d'excitation et détection en régime impulsionnel est représenté sur la figure 3.13. Il a été mis au point et utilisé durant ma thèse. Nous avons remplacé le laser argon continu du montage de la figure 3.5 par une source laser femtoseconde, accordable en longueur d'onde (laser saphir dopé titane) et pompé par diodes. La cadence de ce laser est réduite de 82 MHz à 8.2, 4.1 ou 2.05 MHz selon nos besoins, à l'aide d'un sélecteur d'impulsion. Le faisceau infrarouge produit par ce laser à une longueur d'onde de 1028 ou 1064 nm, est ensuite doublé par un cristal non-linéaire $\chi^{(2)}$ de $LiIO_3$, avant d'être focalisé sur l'échantillon par l'objectif de microscope.

Les corrélations temporelles entre les photons détectés sont ensuite enregistrées à l'aide de deux dispositifs. Le premier identique à celui utilisé dans le régime d'excitation continue, et correspond à l'association standard d'un convertisseur temps-amplitude et d'un analyseur multi-canal. Le second correspond à une carte d'acquisition TIA, pour « Time Interval Analyser » , permettant d'enregistrer tous les instants de détections de photons sur les deux photodétecteurs, avec une très grande résolution temporelle de l'ordre de 75 ps.

3.6.3 Test de l'unicité de l'émetteur en régime impulsionnel

La première étape dans la réalisation de la source de photons uniques déclenchée, consiste à repérer quels « spots » fluorescents dans le balayage de l'échantillon correspondent effectivement à une seule molécule bien isolée. Pour ce faire, on positionne le laser d'excitation sur chacun de ces spots puis on enregistre l'histogramme des retards entre photons

consécutivement détectés sur l'une puis l'autre photodiode comme dans le régime d'excitation continue. Cette caractérisation préliminaire est effectuée à une énergie d'excitation E_{p} « faible » devant celle de saturation (typiquement $E_{\mathrm{p}}^{\max}/100$), afin de ne pas risquer de photoblanchir la molécule prématurément.

L'histogramme des retards obtenus est représenté sur la figure 3.14(a), dans le cas où l'on excite effectivement la fluorescence d'une seule molécule. Il est composé de pics régulièrement espacés de la période de répétition du laser d'excitation. On remarque qu'au retard nul, le pic a une aire très petite devant celle des autres. Ce résultat découle directement du phénomène de dégroupement de photons caractéristique de l'émission par un objet quantique individuel [36]. Notons que la mesure précise de cette aire permet de quantifier la probabilité que plus d'un photon soit émis dans la fluorescence. Précisons également que dans ce régime d'excitation à faible énergie, la fluorescence de la molécule n'est pas déclenchée pour chaque impulsion d'excitation et l'efficacité de la source est par conséquent très limitée.

Si l'on enregistre les corrélations temporelles entre photons provenant d'une source laser atténuée, nous obtenons l'histogramme de la figure 3.14(b). L'aire du pic de retard nul est alors identique à celle des autres pics ; c'est le comportement attendu pour des photons provenant d'une source de lumière classique, avec une distribution poissonnienne du nombre de photons dans l'impulsion lumineuse [77].

On peut d'ailleurs justifier l'allure de la courbe 3.14(b) à l'aide d'un raisonnement élémentaire basé sur la statistique de photons d'une source cohérente fortement atténuée, de paramètre μ (cf. section 2.4.3 pour la définition de μ et de la statistique de Poisson associée). En effet, lorsque l'on enregistre la fonction d'autocorrélation en intensité pour une telle source à l'aide d'un montage de type Start – Stop, le nombre de coïncidences autour du délai nul est fixé par la probabilité $P(2)$ d'avoir deux photons dans la même impulsion, divisée par un facteur 2 qui vient du fait que l'on ne compte pas de coïncidences quand les deux photons vont sur le même détecteur. Ainsi :

$$\text{Aire du pic autour du delai nul} \propto P(2) \times 1/2 \simeq \mu^2/2 \times 1/2 = \mu^2/4. \tag{3.3}$$

Les autres pics de la fonction d'autocorrélation sont essentiellement dus au fait de détecter, dans un impulsion donnée, un photon sur la voie Start puis de détecter, lors d'une autre impulsion, sur la voie Stop. Chacun de ces deux événements interviennent avec une probabilité $P(1) \times 1/2$, où le facteur $1/2$ est dû à la lame séparatrice équilibrée utilisée dans un montage de type HANBURY-BROWN et TWISS. On a donc :

$$\text{Aire des autres pics} \propto (P(1) \times 1/2)^2 \simeq (\mu/2)^2 = \mu^2/4. \tag{3.4}$$

Ceci montre bien que les différents pics de la fonction d'autocorrélation d'une source impulsionnelle poissonnienne sont de même aire.

3.7 Fonctionnement de la source moléculaire de photons uniques

L'objectif de notre expérience est de réaliser une source de photons uniques la plus efficace possible, à partir de la fluorescence d'une molécule unique excitée de manière impulsionnelle . Nous précisons ici le mode opératoire que nous avons élaboré pour atteindre cet objectif.

3.7.1 Protocole d'excitation de la molécule

Nous avons décrit dans le chapitre précédent le dispositif expérimental permettant le repérage et l'identification d'émetteurs uniques au sein de l'échantillon. Rappelons que cette

étape préliminaire est effectuée à faible puissance d'excitation afin de limiter au maximum la probabilité d'un photoblanchiment de la molécule. En revanche, les propriétés de la source de photons uniques doivent être quant à elles étudiées à saturation, afin de maximiser le taux d'émission des photons. Ainsi, après avoir repéré les pics de fluorescence à l'aide d'un balayage de l'échantillon et s'être assuré qu'un pic choisi correspond bien à un émetteur individuel, on positionne cet émetteur au foyer de l'objectif de microscope et on applique une rampe d'excitation (cf. figure 3.15) qui porte progressivement l'énergie par impulsion à une valeur de 5.6 pJ, assurant alors la saturation de la transition $S_0 \rightarrow S_1$.

3.7.2 Enregistrement en régime d'émission saturée

Le nombre total de photons que peut émettre une molécule fluorescente unique à température ambiante est limité par sa photostabilité [63]. Ainsi, sous excitation continue à faible puissance, une molécule de cyanine $\mathrm{DiIC}_{18}(3)$ émet typiquement 10^6 photons avant de photoblanchir [64]. Cherchant à étudier les propriétés d'émission dans le régime où la molécule est saturée avec une excitation impulsionnelle femtoseconde, nous nous sommes heurtés au fait que le photoblanchiment intervenait très rapidement dans le cas de l'application abrupte de l'énergeie maximale $E^p_{\max}$.

Le photoblanchiment, est usuellement attribué à des transitions vers des niveaux multiexcités de la molécule [63]. Nous avons donc penser qu'il était préférable de limiter l'énergie par impulsion excitatrice pour ne pas souffrir d'un photoblanchiment trop rapide. Par ailleurs, en étudiant le phénomène de saturation de la molécule, nous avons été amenés à introduire un système permettant de moduler rapidement l'intensité du faisceau d'excitation. Ce système est constitué d'un modulateur électro-optique (LINOS LM 0202) suivi d'un cube polariseur. Nous avons programmé un générateur de tension arbitraire, placé en commande de la haute tension appliquée sur le modulateur, afin de réaliser une rampe d'excitation (cf. figure 3.15) débutant par une augmentation progressive de l'intensité d'excitation sur 50 ms, suivie d'un plateau d'excitation de 300 ms et se terminant par une décroissance linéaire de l'intensité à une valeur nulle.

Afin de déclencher à coup sûr l'émission d'un photon par la molécule unique préalablement repérée, on augmente l'énergie de l'impulsion excitatrice E_{p} jusqu'à la valeur de saturation de la molécule, $E_{\mathrm{p}}^{\max} \approx 5.6$ pJ, au delà de laquelle l'intensité de fluorescence cesse de croître. Insistons sur le fait que si, partant d'une intensité d'excitation nulle, nous appliquions brutalement des impulsions d'énergie $E_{\mathrm{p}}^{\max}$ à la molécule repérée, nous ne collections alors qu'au plus un millier de photons avant que cette dernière ne blanchisse. La procédure décrite précédemment nous a permis d'augmenter le nombre de photons collectés d'un ordre de grandeur, et nous avons ainsi pu collecter un peu plus de 10^4 photons avant le photoblanchiment de la molécule. En outre, les intensités de fluorescence, définies comme le nombre de photons émis par seconde, obtenues par cette méthode sont aussi plus grandes d'environ un ordre de grandeur que dans le cas d'une illumination directe par des impulsions d'énergie $E_{\mathrm{p}}^{\mathrm{sat}}$. Ces observations suggèrent qu'une illumination « brutale » envoie la molécule plus souvent dans son niveau triplet (état « noir »), d'où il semblerait (selon certains modèles [78, 79]) que le photoblanchiment se produise. Nous n'avons pas fait une étude détaillée de ces observations, certes troublantes, mais en marge du but principal que nous nous étions fixés pour cette expérience.

Le démarrage de l'acquisition de l'ensemble des instants de photodétection à l'aide de la carte TIA est synchronisé sur le lancement de la rampe d'excitation. Cependant, afin d'étudier le comportement de notre source de photons uniques dans le régime d'émission saturée, nous sélectionnons au sein de la séquence des instants de photodétection, ceux qui

sont intervenus durant le plateau de saturation. Nous avons ainsi représenté sur la figure 3.16 l'évolution du nombre de photons détectés durant des fenêtres d'intégration de 500 μs, ainsi que le profil en intensité de la rampe d'excitation. La période sélectionnée est délimitée par des lignes verticales pointillées ; elle débute quand l'énergie d'excitation atteint sa valeur maximale et se termine lorsque la molécule disparaît par photoblanchiment. On peut remarquer la variation caractéristique du signal de fluorescence lors du photoblanchiment d'une molécule unique, qui se traduit par un effondrement brusque et en une seule étape du niveau de signal qui rejoint le niveau correspondant au bruit des détecteurs.

3.8 Conclusion

Nous avons présenté dans ce chapitre le contexte scientifique ainsi que les aspects expérimentaux liés à l'observation de la fluorescence d'une molécule unique, avant de détailler la réalisation et le mode opératoire de la source moléculaire déclenchée de photons uniques.

Le chapitre suivant sera consacré à l'analyse statistique des données de photodétection associée à cette source. On notera, que dans un soucis de cohérence, un unique « jeu » de donnée expérimentales, statistiquement représentatif de la centaine d'acquisition effectuées, sera utilisé pour ces analyses. Il s'agit des instants de photodétection acquis en régime d'excitation saturée, correspondant aux données représentées la fréquence sur la figure 3.16.

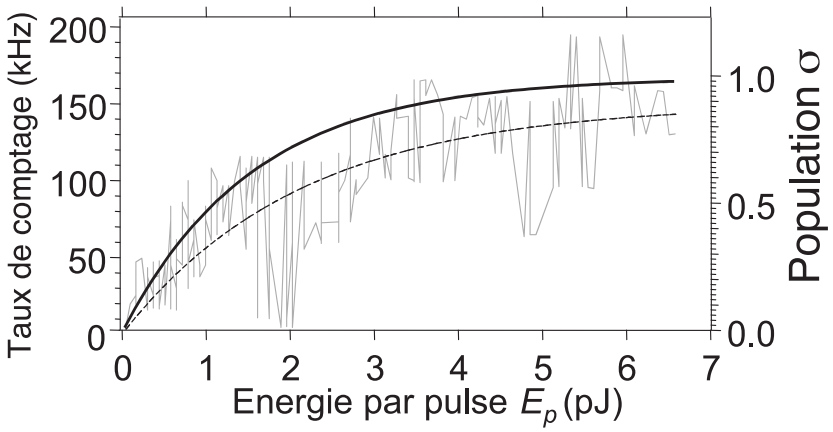

FIG. 3.12 – Taux de comptage mesuré pour une molécule unique, en fonction de l'énergie par impulsion excitatrice. L'enregistrement d'une telle courbe est rendue difficile à cause du photoblanchiment accéléré des molécules à forte puissance d'excitation dans un régime femtoseconde. Par ailleurs, l'existence du niveau triplet induit des fluctuations d'intensité importantes due à l'arrêt de la fluorescence tant que la molécule est dans ce niveau « noir ». La courbe en pointillé est un ajustement des données brutes réalisé à partir de l'équation (3.2) tandis que la courbe en trait plein est un ajustement réalisé après suppression des points associés au passage par le niveau triplet.

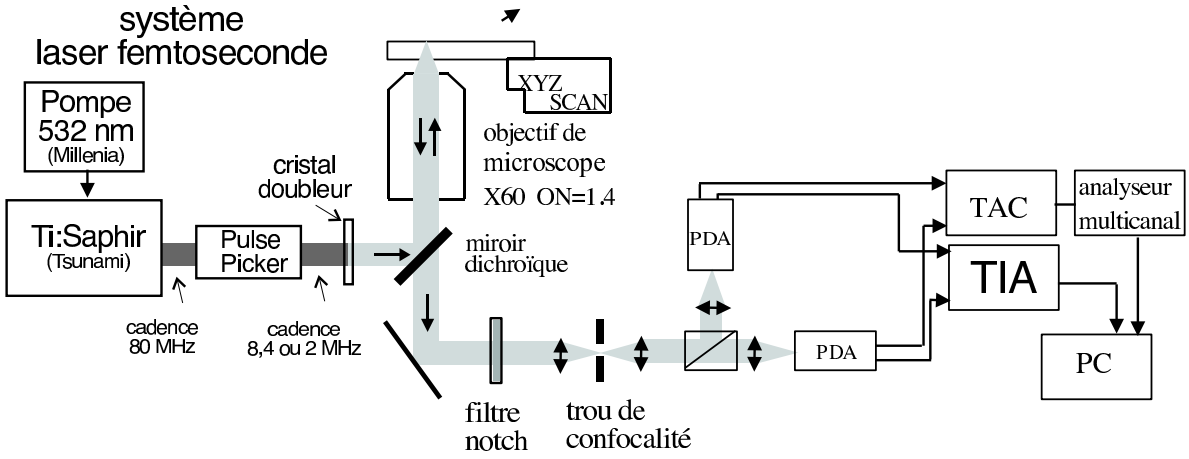

FIG. 3.13 – Schéma de l'expérience en régime d'excitation impulsionnelle. *Système d'excitation laser* : Ti :Sa : laser impulsionnel saphir dopé titane délivrant des impulsions de durée $\simeq$ 150 fs ; PP : sélecteur d'impulsions réduisant la cadence d'excitation de la molécule ; S : cristal doubleur de fréquence $LiIO_3$; EO : cristal électro-optique suivi d'un polariseur P. *Système d'excitation/détection confocal* : PZT : platine trois axes piézoélectrique sur laquelle est posée l'échantillon ; Obj. : objectif de microscope à immersion $\times 60$, ON=1.4 ; DM : miroir dichroïque ; PH : trou de confocalité ; NF : filtre réjecteur Notch ; BS : séparateur 50/50 de faisceau insensible à la polarisation ; SPAD : photodiode à avalanche en régime de comptage de photons. TAC : convertisseur temps-amplitude relié à l'analyseur multi-canal MA ; TIA : analyseur d'intervalles temporels (« Time Interval Analyser ») ; PC : ordinateur.

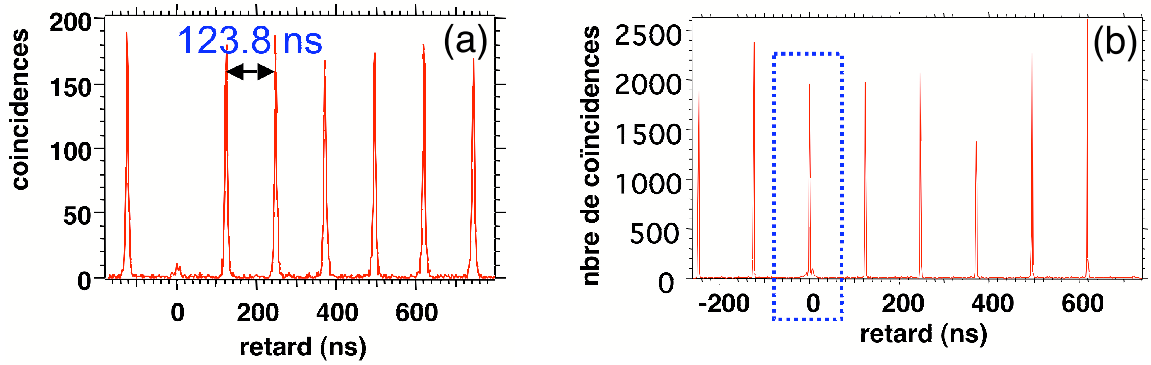

FIG. 3.14 – (a) Histogramme des retards entre photons consécutivement détectés sur l'une puis l'autre photodiode. La lumière provient d'une molécule unique excitée à la cadence de 8 MHz, à la longueur d'onde $\lambda = 514$ nm, et dans le régime des faibles énergies par impulsion d'excitation. Dans ce régime d'excitation impulsionnelle, la très petite aire du pic au retard nul traduit le dégroupement de photons caractéristique de la lumière provenant d'un seul émetteur quantique. (b) Cas où la lumière provient d'une source classique atténuée. Il s'agit en l'occurrence, d'une fraction du faisceau de pompage réfléchie sur l'échantillon, et ayant été au préalable légèrement décalé en longueur d'onde de la valeur centrale du filtre réjectif « notch » utilisé dans le système de microscopie confocale.

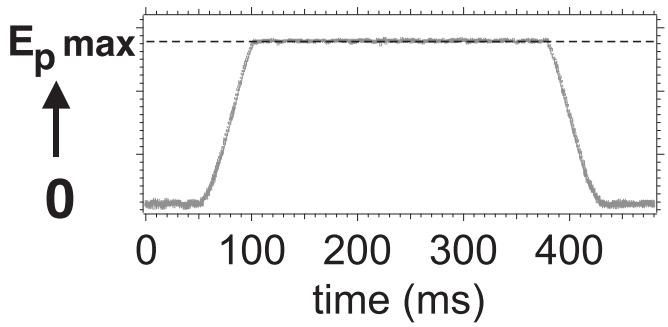

FIG. 3.15 – Rampe d'excitation appliquée pour l'excitation d'une molécule unique. L'acquisition des données est effectuée durant le plateau d'énergie E_p^{max} = 5.6 pJ. Cette énergie permet d'assurer la saturation de la transition $S_0 \rightarrow S_1$ de la molécule pour chaque impulsion de pompe appliquée.

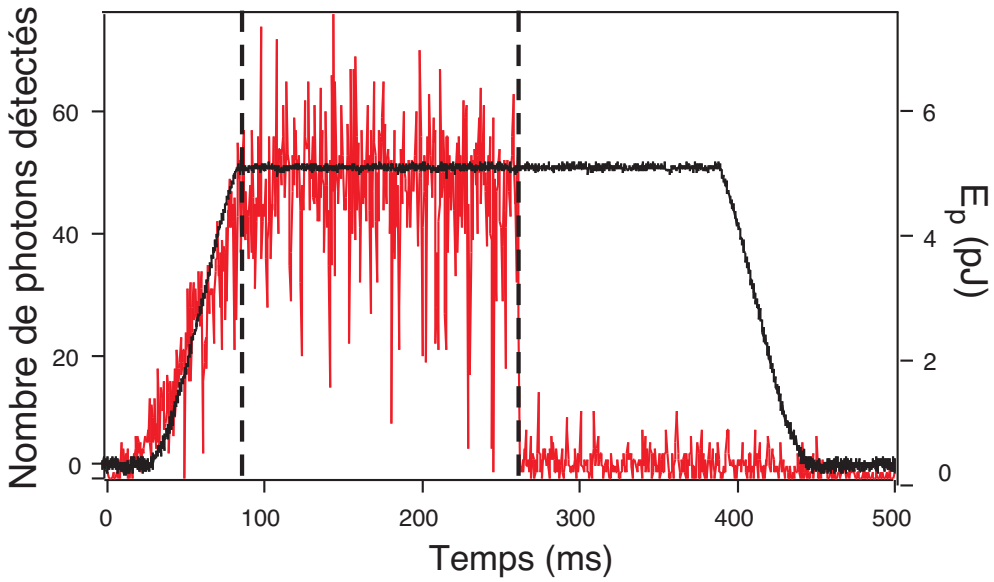

FIG. 3.16 – *En trait plein noir* (échelle de droite) : variation de l'énergie E_{p} de l'impulsion d'excitation en fonction du temps, lors d'une séquence d'acquisition des photons de fluorescence. E_{p} est augmenté linéairement en fonction du temps, jusqu'à la valeur $E_{\mathrm{p}}^{\mathrm{max}} = 5.6$ pJ pour laquelle la fluorescence de la molécule est saturée. *En trait gris foncé* (échelle de gauche) : nombre de photons de fluorescence détectés pendant une durée d'intégration de 500 μs. Les fluctuations de ce signal, plus grandes que les fluctuations statistiques, proviennent du passage intermittent de la molécule par le niveau triplet non fluorescent. L'interruption brutale de la fluorescence légèrement au-delà de la moitié du palier d'excitation correspond à la disparition de la molécule par photoblanchiment. Durant la période délimitée par les deux traits pointillés verticaux, d'une durée de l'ordre de 162 ms, la molécule peut délivrer des photons un par un à la cadence de l'excitation de 2 MHz. Au total 15138 photons seront détectés durant cette phase et constitueront les « données de références » étudiées au chapitre 4.

Chapitre 4

Caractérisation statistique de la source de photons uniques

Sommaire

La source de photon unique moléculaire décrite au chapitre 3 présente une flexibilité et une simplicité qui lui confère un certain nombre de propriétés intéressantes. Cette source fonctionne à température ambiante et est basée sur un dispositif optique conduisant à une détection efficace des photons de fluorescence émis par la molécule. Par ailleurs, la molécule fluorescente offre a priori une grande souplesse, que ce soit pour le choix de la longueur d'onde d'émission ou de la durée de vie radiative. Ces caractéristiques nous ont permis de réaliser une source de photons uniques pour laquelle on peut non seulement *produire* mais aussi *détecter* les photons avec une très bonne efficacité.

Une telle source de photons uniques constitue ainsi un système adapté à la mise en évidence des propriétés statistiques non-classiques de la lumière de fluorescence d'un émetteur unique. C'est dans cette direction que nous avons orienté notre travail, en nous intéressant

tout particulièrement aux fluctuations d'intensité du faisceau de photons uniques ainsi produit et à sa comparaison par rapport au niveau de référence classique correspondant au bruit de photons.

4.1 Introduction : Statistiques de photons

Cette section d'introduction a pour but d'introduire quelques résultats de la théorie développée par Roy GLAUBER, qui fixe un cadre théorique adapté à l'étude des corrélations statistiques en optique quantique [18]. Ces éléments de la théorie quantique de la photodétection nous permettront ensuite d'introduire les outils que nous avons utilisés pour caractériser la statistique de notre source de photons uniques. Par ailleurs, nous tenterons également de porter l'accent sur les points de divergence existant entre les prédictions de la théorie classique du rayonnement et ceux de la théorie quantique.

4.1.1 Eléments de théorie quantique de la photodétection

Description quantique du champ

La description du rayonnement dans le cadre de l'optique quantique nécessite d'introduire des opérateurs afin de décrire le champ électromagnétique. On peut montrer que la combinaison des équations de Maxwell, d'un choix de jauge approprié (jauge de Coulomb), et d'un volume de quantification V assorti de conditions aux limites permet de quantifier le champ sous la forme de modes de vibration [19].

Dans le cas où l'on considère l'expression du champ à grande distance de la source de rayonnement, la solution dans le vide des équations de Maxwell peut se décomposer sur la base des ondes planes monochromatiques, chaque mode noté k correspondant à une onde plane de fréquence ω_k, de vecteur d'onde $\mathbf{k}$ et de vecteur polarisation $\mathbf{e}_k$. La quantification du rayonnement permet de dériver l'expression suivante pour l'opérateur champ électrique libre en fonction d'opérateurs de création et d'annihilation [14] :

$$\hat{\mathbf{E}}(\mathbf{r},t) = i\sum_k \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}}[\hat{a_k}\,\mathbf{e}_k e^{i(\mathbf{k}.\mathbf{r}-\omega_k t)} - \hat{a_k}^\dagger\,\mathbf{e}_k^* e^{-i(\mathbf{k}.\mathbf{r}-\omega_k t)}] \tag{4.1}$$

et l'on pose usuellement :

$$\hat{\mathbf{E}}(\mathbf{r},t) = \hat{\mathbf{E}}^{(+)}(\mathbf{r},t) + \hat{\mathbf{E}}^{(-)}(\mathbf{r},t) \tag{4.2}$$

où le terme $\hat{E}^{(+)}$ regroupe les termes correspondant aux opérateurs d'annihilation $\hat{a_k}$ et $\hat{E}^{(-)}$ aux opérateurs de création $\hat{a}_k^\dagger$.

Probabilité de photoionisaton d'un atome détecteur

La théorie de la photodétection de GLAUBER est fondée sur un modèle simple de photodétecteur constitué par un atome irradié par une onde incidente et susceptible d'être ionisé en libérant un électron. La première étape consiste à calculer l'amplitude de probabilité pour la transition correspondant à l'ionisation de l'atome, c'est-à-dire le passage de son état fondamental à l'un des états du continuum des états excités, accompagné du passage du champ électromagnétique incident de son état initial $|i\rangle$ à un état final $|f\rangle$.

On se place pour cela dans le cadre de l'approximation où le rayonnement est émis ou absorbé par des atomes de tailles très inférieures à la longueur d'onde, justifiant l'utilisation de l'expression du champ libre de l'hamiltonien d'interaction dipolaire électrique :

$$\hat{W} = -\hat{\mathbf{D}}.\hat{\mathbf{E}}(\mathbf{r_0}, t) \tag{4.3}$$

où $\mathbf{r_0}$ correspond à la position de l'atome et $\hat{\mathbf{D}}$ est l'opérateur dipolaire. Dès lors, l'application de la règle d'or de Fermi permet de calculer la probabilité d'ionisation P_{if} d'un atome par unité de temps, placé à la position $\mathbf{r}$, au temps t, dans le cas où $|i\rangle$ et $|f\rangle$ correspondent respectivement aux états initial et final du champ électromagnétique. On montre alors que :

$$P_{if} = |\langle f|\hat{E}^{(+)}(\mathbf{r}, t)|i\rangle|^2 \tag{4.4}$$

la probabilité totale d'ionisation étant ensuite données par la somme des probabilités de transition sommée sur tous les états $|f\rangle$ du champ accessibles à partir de l'état $|i\rangle$ au cours du processus d'absorption.

Ainsi, si l'état quantique du champ peut être décrit par la matrice densité $\hat{\rho}$, on peut montrer que la probabilité d'ionisation par unité de temps est donnée par [14] :

$$I(\mathbf{r}, t) = \sum_f P_{fi} = \mathrm{Tr}\{\hat{\rho}\hat{E}^{(-)}(\mathbf{r}, t)\hat{E}^{(+)}(\mathbf{r}, t)\} \tag{4.5}$$

Enfin, dans le cas d'un photodétecteur « large bande » dont la réponse spectrale varie lentement avec la fréquence ω du champ, on peut montrer que le taux de comptage est directement proportionnel à la probabilité d'ionisation par unité de temps $I(\mathbf{r}, t)$. Cette grandeur peut être identifiée, à une constante multiplicative près, au taux de comptage d'un photodétecteur fonctionnant en régime de comptage, comme par exemple un photomultiplicateur ou une photodiode à avalanche.

Nous voyons ainsi apparaître un résultat important : le taux de comptage est proportionnel à la valeur moyenne d'un produit d'opérateurs rangés dans l'ordre « normal » c'est-à-dire au sein duquel les opérateurs de création $\hat{a}^\dagger$ sont placés à gauche des opérateurs d'annihilation $\hat{a}$.

4.1.2 Fonctions de corrélation du champ électromagnétique

L'expression (4.5) a une portée plus générale que le calcul du taux de comptage d'un photodétecteur. En effet, la corrélation du champ entre les points $x = (\mathbf{r}, t)$ et $x^{'} = (\mathbf{r}^{'}, t^{'})$ peut être exprimée à l'aide de la fonction de corrélation de premier ordre du champ électromagnétique, définie selon la relation :

$$G^{(1)}(x, x^{'}) = Tr\{\hat{\rho}\hat{E}^{(-)}(x)\hat{E}^{(+)}(x^{'})\} \tag{4.6}$$

Comme en optique classique, cette fonction caractérise les propriétés de cohérence du champ électromagnétique et permet en particulier de rendre compte des phénomènes d'interférences du champ électromagnétique. Ainsi, le taux de comptage d'un photodétecteur, exprimé dans l'expression (4.5) peut s'interpréter comme le résultat de l'interférence du champ électromagnétique avec lui-même au point $x = (\mathbf{r}, t)$.

Plus généralement, la fonction de corrélation du premier ordre $G^{(1)}(x, x^{'})$ quantifie le degré de cohérence spatio-temporelle du champ électromagnétique décrit par la matrice densité $\hat{\rho}$. Cette cohérence peut être « testée » expérimentalement par les montages traditionnels d'interférence à un photon, comme par exemple l'expérience des trous d'Young

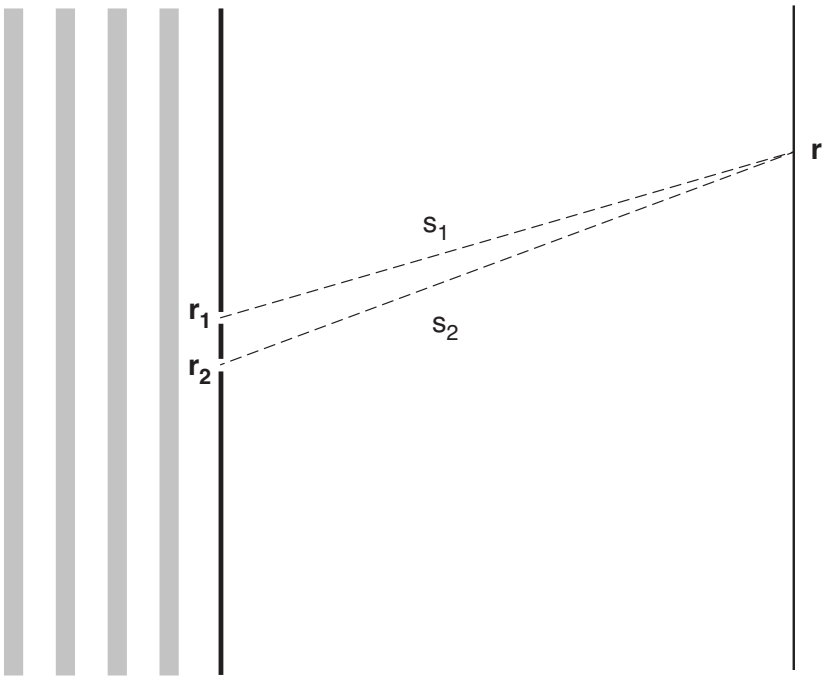

FIG. 4.1 – Représentation schématique et notations attachées à la description de l'expérience d'interférence des fentes d'Young.

[14].

On montre d'ailleurs que le contraste des franges d'interférences est déterminé par le niveau de cohérence entre les chemins optiques qui interfèrent. Dans le cas d'un interféromètre à deux voies, comme par exemple les fentes d'Young représenté à la figure 4.1, et dans le cas où les deux voies de l'interféromètre correspondent à la même intensité lumineuse, le calcul de la figure d'interférence sur un écran placé derrière les fentes permet de donner une interprétation physique à la fonction de corrélation $G^{(1)}$.

Ainsi, en reprenant les notations induites par la figure 4.1, on paramètre par $x_1 = (\mathbf{r_1}, t - s_1/c)$ et $x_2 = (\mathbf{r_2}, t - s_2/c)$ les coordonnées, au point $x = (\mathbf{r}, t)$ des champs secondaires rayonnés par les deux fentes. Ces coordonnées dépendent de la position $\mathbf{r_i}$ des trous d'Young et des chemins optiques $|\mathbf{r_i} - \mathbf{r}|$ (cf. figure 4.1). On montre [14] que l'enveloppe des franges d'interférence au point $\mathbf{r}$ est décrite par la fonction de corrélation $G^{(1)}(x_1, x_2)$.

En particulier, dans le cas où les champs incidents sur chacun des trous d'Young ont la même intensité, on montre que le contraste est égal à la fonction de correlation normalisée, définie comme :

$$g^{(1)}(x_1, x_2) = \frac{G^{(1)}(x_1, x_2)}{[G^{(1)}(x_1, x_1)\, G^{(1)}(x_2, x_2)]^{1/2}} \tag{4.7}$$

La quantité $|g^{(1)}(x_1, x_2)|$ a la propriété d'être bornée par 1 valeur correspondant à un niveau de cohérence « totale » .

Il est important à ce stade de remarquer que les propriétés « interférentielles » du rayonnement, dont on peut rendre compte à l'aide de la fonction de corrélation du premier ordre,

sont *identiques* à celles que l'on pourrait dériver dans le cadre d'un formalisme purement classique de l'électromagnétisme.

En revanche, pour décrire des expériences mettant en jeu des *corrélations d'intensité* du champ électromagnétiques [1], il est nécessaire de définir des fonctions de corrélation d'ordre supérieur. Ainsi, la fonction de corrélation d'ordre n du champ électromagnétique sera donnée par la relation :

$$G^{(n)}(x_1 \cdots x_n, x_{n+1} \cdots x_{2n}) = \mathrm{Tr}\{\hat{\rho}\hat{E}^{(-)}(x_1) \cdots \hat{E}^{(-)}(x_n)\hat{E}^{(+)}(x_{n+1}) \cdots \hat{E}^{(+)}(x_{2n})\} \quad (4.8)$$

4.1.3 Mesures de corrélations d'intensité

La première expérience d'optique quantique réalisée en dehors du domaine des phénomènes à un photon a été l'expérience d' HANBURY BROWN et TWISS [32]. Depuis, leurs noms sont associés aux les dispositifs expérimentaux permettant de mesurer la probabilité conjointe de détecter l'arrivée d'un premier photon à l'instant t, puis d'un second photon à l'instant $t+\tau$. La figure 3.10 du chapitre précédent en décrit le principe, basé sur le calcul des corrélations d'intensité entre les deux faisceaux en sortie d'une lame séparatrice 50 / 50.

Les corrélations d'intensité du champ électromagnétique mesurées dans ce type d'expérience, peuvent être interprétées comme des corrélations de nombres de photons. Ainsi, pour reprendre le formalisme de la théorie de GLAUBER, on peut montrer qu'une expérience de corrélation d'intensité est associée à une mesure de la fonction de corrélation du second ordre :

$$\begin{aligned} G^{(2)}(t, t+\tau) &= \langle \hat{E}^{(-)}(t)\hat{E}^{(-)}(t+\tau)\hat{E}^{(+)}(t+\tau)\hat{E}^{(+)}(t)\rangle & (4.9)\\ &= \langle : I(t)I(t+\tau) : \rangle & (4.10)\\ &\propto \langle : n(t)n(t+\tau) : \rangle & (4.11)\\ & & (4.12) \end{aligned}$$

où : : désigne l'ordonnancement des opérateurs dans l'ordre normal, où l'opérateur intensité est défini comme : $\hat{I} \equiv \hat{E}^{(-)}\hat{E}^{(+)}$ et enfin ou $\hat{n}$ désigne l'opérateur nombre de photons.

À partir de maintenant et jusqu'à la fin de ce chapitre, on effectuera une distinction de notation entre les grandeurs relatives au nombre de photons dans le champ électromagnétique, notées par un « petit » n, et les grandeurs liées à une statistique de comptage, auxquelles on associera des symboles majuscules[2].

Il est utile, pour caractériser les corrélations d'intensité du champ électromagnétique, d'introduire la fonction de corrélation normalisée du second ordre, définie comme :

$$g^{(2)}(t, t+\tau) = \frac{G^{(2)}(t, t+\tau)}{G^{(1)}(t)\, G^{(1)}(t+\tau)} \quad (4.13)$$

Cette fonction, dont nous avons ici limité la définition à la variable temporelle qui porte donc le nom de « fonction d'autocorrélation d'intensité » et permet de quantifier les corrélations temporelles d'intensité du champ électromagnétique. Afin d'illustrer les propriétés de cette

[1] Ainsi que plus généralement des processus à plus d'un photon.

[2] On désignera, par exemple le nombre moyen de photodétections intervenant durant des fenêtres d'acquisitions de durée T, par la notation $\langle N \rangle_T$.

fonction, nous pouvons comparer le cas de figure d'un champ classique dont les fluctuations d'intensité peuvent être décrites à l'aide d'une distribution de probabilité, avec les valeurs prises par $g^{(2)}(t, t+\tau)$ pour des états du champ électromagnétique spécifiquement quantiques.

Corrélations d'intensité d'un champ classique

Un champ classique fluctuant peut être décrit à l'aide d'une distribution de probabilité $P(\epsilon)$, où ϵ désigne l'amplitude du champ, de sorte que :

$$\hat{E}^{(+)}(\epsilon, t) = -i\sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}}\epsilon e^{-i\omega t} \tag{4.14}$$

On peut alors montrer [14] que, dans le cas d'un champ monomode, on a :

$$g^{(2)}(0) = 1 + \frac{\int P(\epsilon)(|\epsilon|^2) - \langle|\epsilon|^2\rangle)^2 d^2\epsilon}{(\langle|\epsilon|^2\rangle)^2} \tag{4.15}$$

Ainsi, la distribution de probabilité $P(\epsilon)$ étant toujours positive dans le cas d'un champ classique, on obtient un premier résultat important :

Pour un champ électromagnétique classique, $g^{(2)}(0) \geq 1$.

Par ailleurs, dans le cas d'un champ classique, on n'a plus de question à se poser quant à l'ordre dans lequel sont placés les opérateurs associés au champ. Ainsi, il est possible d'utiliser l'inégalité de CAUCHY-SCHWARZ afin de comparer $\langle I(t)I(t+\tau)\rangle$ et $\langle I^2(t)\rangle$, et à l'aide de l'équation (4.12) d'en déduire une autre propriété importante :

Pour un champ électromagnétique classique, $g^{(2)}(0) \geq g^{(2)}(|\tau|)$.

Ainsi, la fonction d'aucorrélation d'intensité classique est maximale en $\tau = 0$. Cette propriété correspond au phénomène de « groupement de photons » et est observable avec de la lumière thermique ou lorsque l'on s'intéresse à l'émission d'une assemblée d'atomes dans un gaz dense au sein duquel la largeur de raie d'émission est fixée par les collisions [32].

Corrélations d'intensité des états quantiques du champ

Nous venons de voir qu'une description classique du rayonnement se traduisait par deux propriétés spécifiques de la fonction d'autocorrélation d'intensité : $g^{(2)}(0) \geq 1$ et $g^{(2)}(0) \geq g^{(2)}(|\tau|)$.

Ces propriétés peuvent néanmoins ne pas être vérifiées pour des états quantique du champ, ouvrant ainsi la voie à la mise en évidence expérimentale de propriétés non-classiques qui correspondent à la violation de ces inégalités. Ainsi, la description quantique de la fluorescence d'un atome conduit à un phénomène de dégroupement de photons fondé sur l'impossibilité pour l'atome d'émettre immédiatement un deuxième photon juste après une première absorption [36]. Ce phénomène se traduit par une pente positive de la fonction de d'autocorrélation d'intensité du second ordre au voisinage du délai nul et idéalement par la propriété $g^{(2)}(0) = 0$. Ce résultat est en complète contradiction avec les prédictions de la théorie classique, et permet d'affirmer que la lumière rayonnée par un atome unique a une essence fondamentalement quantique.

A la différence d'un champ classique, les différents termes dans l'équation (4.9) ne commutent pas, et les propriétés dérivées pour le champ classique peuvent être violées. Nous allons illustrer ce propos en calculant $g^{(2)}(\tau)$ pour différents états du champ, en se limitant par simplicité au cas d'un champ monomode. Une telle approche présente l'avantage de simplifier les calculs sans restreindre la généralité des résultats qui peuvent être facilement généralisés au cas d'un champ multimode.

Ainsi, en adoptant les notations propres à un champ monomode, il est facile de relier la valeur de la fonction d'autocorrélation à délai nul $g^{(2)}(0)$ à la distribution du nombre de photons :

$$g^{(2)}(0) = \frac{\langle \hat{a}^\dagger \hat{a}^\dagger \hat{a}\hat{a} \rangle}{\langle \hat{a}^\dagger \hat{a} \rangle^2} = \frac{\langle \hat{n}(\hat{n}-1) \rangle}{\langle \hat{n} \rangle^2} \tag{4.16}$$

La formule (4.16), que l'on peut facilement étendre au cas de la lumière multimode, montre que l'on peut relier de manière directe la valeur de $g^{(2)}(0)$ à la distribution de probabilité du nombre de photons. Ceci justifie que la valeur de $g^{(2)}(0)$ soit souvent utilisée comme paramètre caractéristique de la « qualité statistique » d'une source de photons uniques, sachant que pour une source de photons uniques idéale, $g^{(2)}(0) = 0$.

Dans le cas d'un état cohérent $\rho = |\alpha\rangle\langle\alpha|$, dont nous rappelerons la définition un peu plus tard et dont le comportement est essentiellement classique, l'équation (4.16) donne $g^{(2)}(0) = 1$ résultat compatible avec les propriétés « classiques » énoncées au paragraphe précédent consacré aux corrélations d'intensité d'un champ classique. En revanche, il est facile de voir que des états purement quantiques, comme la famille des états nombre de photons $\{|n\rangle\}$, conduisent à des résultats radicalement différents. Ainsi, pour l'état $|n\rangle$, l'application de l'équation (4.16) permet de calculer $g^{(2)}(0) = 1 - 1/n$. Ce résultat viole l'inégalité $g^{(2)}(0) \geq 1$ vérifiée par un champ électromagnétique classique. Ainsi, si l'on voulait définir une description de probabilité capable de décrire les corrélations d'intensité du champ électromagnétique pour un tel état nombre, on peut montrer que l'on serait amener à considérer des distributions de probabilité non définies, prenant des valeurs négatives. Ces résultats sont la signature du caractère fondamentalement non-classique de tels états.

Le cas particulier des états à un photon, produits par fluorescence d'un émetteur unique est directement relié à notre travail. Le caractère quantique de l'émission d'un système fluorescent unique veut qu'à des temps courts devant τ_0 ; où τ_0 désigne la durée de vie de fluorescence de l'émetteur, un photon au plus peut être émis. Par conséquent, pour $|\tau| \ll \tau_0$ la fonction de corrélation en intensité $g^{(2)}(\tau)$ d'un émetteur unique, est proche de 0, ce qui est une traduction directe du phénomène de dégroupement de photons. Aux temps longs devant τ_c , les corrélations temporelles entre les photons émis deviennent négligeables et la fonction de corrélation en intensité peut être factorisée en termes indépendants, entraînant alors la limite $g^{(2)}(\tau) \to 1$ pour $\tau \to \pm\infty$. Là encore, cette variation est en contradiction avec les inégalités « classiques » devant être vérifiées par la fonction de corrélation en intensité.

Corrélation d'intensité et statistique de comptage de photons : facteur de Mandel

Comme nous l'avons évoqué au début de cette section à travers l'expression de $g^{(2)}(0)$ dans le cas d'un champ monomode (cf. équation 4.16), on peut relier la fonction de corrélation d'intensité à délai nul au nombre $\langle n \rangle = \mathrm{Tr}\{\hat{\rho}\,\hat{n}\}$, nombre moyen de photons dans le champ décrit par la matrice densité $\hat{\rho}$: $g^{(2)}(0) = \frac{\langle \hat{n}(\hat{n}-1) \rangle}{\langle \hat{n} \rangle^2}$.

Pour l'état monomode du champ considéré ici, la valeur de $g^{(2)}(0)$ est directement reliée à la variance $V(n) = \langle n^2 \rangle - \langle n \rangle^2$ du nombre de photons dans le mode considéré :

$$g^{(2)}(0) = \frac{V(n)}{\langle n \rangle^2} \tag{4.17}$$

Ainsi, dans le cas d'expériences réalisées en régime de comptage de photons, on peut également dériver un lien direct entre les fluctuations du nombre N de photodétections enregistrées pendant une durée T déterminée et la fonction de corrélation d'intensité. Ces fluctuations peuvent être caractérisées par la dispersion $\langle \Delta N^2 \rangle_T = \langle N - \langle N \rangle_T \rangle_T^2$, où la notation $\langle \rangle_T$ se réfère aux statistiques de comptage moyennées sur un grand nombre d'acquisitions, chacune d'entre elles ayant été de la même durée T.

On peut alors montrer [161, 17] que le moment factoriel d'ordre deux, $\langle N(N-1) \rangle_T$ est relié à $g^{(2)}(t_1, t_2)$ par :

$$\langle N(N-1) \rangle_T = \int_0^T \int_0^T dt_1 dt_2 \, g^{(2)}(t_1, t_2) \tag{4.18}$$

Dans le cas où l'on peut faire l'hypothèse de la stationnarité de l'émission $g^{(2)}(t_1, t_2)$ ne dépend alors que de la différence $(t_2 - t_1)$ et :

$$\frac{\langle \Delta N^2 \rangle_T - \langle N \rangle_T}{\langle N \rangle_T} = \frac{\langle N \rangle_T}{T^2} \int_{-T}^{T} d\tau \, (T - |\tau|) g^{(2)}(\tau) \tag{4.19}$$

Cette dernière quantité $\frac{\Delta N^2 - \overline{N}}{\overline{N}}$, qui caractérise les fluctuations d'intensité sur une période de durée T, est notée $Q(T)$ et est appelée **facteur de Mandel** [17]. Comme nous allons l'expliquer, ce paramètre permet de comparer les fluctuations d'intensité d'une source lumineuse classique ou quantique, avec celles correspondant à une distribution des photons selon une loi de Poisson.

Etats cohérents et statistique poissonnienne

Les états cohérents de la lumière correspondent au champ électromagnétique émis par une source classique non bruitée, comme par exemple un laser fonctionnant très au-dessus de son seuil. On peut formellement décrire ces états comme les vecteurs propres de l'opérateur annihilation $\hat{a}$ [3]. Ainsi, si $|\alpha\rangle$ désigne l'état cohérent d'amplitude complexe α :

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{4.20}$$

relation permettant de décomposer les états cohérents sur la base des états nombres :

$$|\alpha\rangle = \sum_n e^{-|\alpha|^2/2} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{4.21}$$

Cette dernière expression permet de calculer la statistique de photons d'un état cohérent. Ainsi, si on note $P(n)$ la probabilité qu'un état cohérent de nombre moyen de photons $\langle n \rangle$ contienne n photons, on a :

$$P(n) = e^{-\langle n \rangle} \frac{\langle n \rangle^n}{n!} \tag{4.22}$$

[3] Il convient de noter que $\hat{a}$ et $\hat{a}^\dagger$ ne sont pas à proprement parlé des opérateurs, puisque ces transformations linéaires ne sont pas hermitiques.

où $\langle n \rangle = |\alpha|^2$. Cette loi est une distribution de Poisson, dont la statistique de photons est entièrement caractérisée par le nombre $\langle n \rangle$.

Cette distribution a un certain nombre de propriétés intéressantes.

Tout d'abord, un faisceau poissonnien, de nombre moyen de photons $\langle n \rangle$ reste un faisceau poissonnien après une atténuation linéaire. La statistique de photons du faisceau atténué est une loi de Poisson de paramètre $\eta \times \langle n \rangle$ où η est le coefficient de transmission. Cette propriété découle directement de l'équation (4.24) et de la loi binomiale de paramètre η, qui relie les distributions $P^{in}(n)$ et $P^{\text{out}}(n)$ correspondant aux statistiques de photon *avant* et *après* l'atténuation.

$$P^{\text{out}}(n) = \sum_{m=n}^{\infty} \binom{m}{n} \eta^n (1-\eta)^{m-n} P^{in}(m) \tag{4.23}$$

Par ailleurs, l'équation (4.24) permet également de calculer la variance du nombre de photons pour une distribution poissonnienne,

$$\Delta n^2 = \langle n \rangle \tag{4.24}$$

Pour une statistique de Poisson, la variance du nombre de photons est égale à la valeur moyenne $\langle n \rangle$ du nombre de photons dans l'état cohérent considéré. .

Cette relation a une conséquence directe sur l'amplitude des fluctuations d'intensité du nombre de photons N détectés lors d'une expérience de comptage de photons pendant une durée T. La relation entre la statistique du champ et celle des photodétections étant supposée linéaire, on aura :

$$Q(T)_{\text{Poisson}} = \frac{\langle \Delta N^2 \rangle_T - \langle N \rangle_T}{\langle N \rangle_T} \text{ soit } Q(T)_{\text{Poisson}} = 0 \tag{4.25}$$

Une statistique de photons poissonnienne se caractérise par un facteur de Mandel $Q(T)$ égal à zéro, quelle que soit l'échelle de temps associée à la mesure.

Les propriétés énoncées dans cette section à propos de la statistique de Poisson permettent de mieux comprendre l'influence des pertes vis à vis du facteur de Mandel. Ainsi, une atténuation linéaire d'un facteur η du nombre moyen de photons, c'est-à-dire de l'intensité moyenne du faisceau, conduit à la relation entrée $\rightarrow$ sortie :

$$Q^{\text{out}} = \eta\, Q^{\text{in}} \tag{4.26}$$

Il est dès lors clair que la propriété d'avoir un facteur de Mandel égal à zéro, caractéristique d'une statistique de Poisson, est *stable* au cours d'une atténuation linéaire. Il apparaît en outre qu'une atténuation linéaire fait tendre le facteur de Mandel vers zéro. Ceci est la conséquence du fait qu'atténuer un faisceau « écrase » les corrélations d'intensité dont il peut être le siège, faisant converger la statistique des photons vers une distribution de Poisson et le facteur de Mandel vers la valeur nulle.

Le fait que le facteur de Mandel est affecté par l'efficacité globale de détection de la lumière va entraîner de fortes contraintes sur les dispositifs expérimentaux visant à mesurer une statistiques non-classique du flux de photons. Nous voyons ainsi apparaître l'intérêt que présente notre source de photons uniques moléculaire, qui constitue une source non-classique de lumière pour laquelle l'efficacité de détection est importante.

Statistiques sub-poissonniennes et super-poissonniennes

On désigne par sub-poissonniennes (respectivement super-poissonniennes) des distributions statistiques de photons dont la variance est inférieure (respectivement supérieure) au nombre moyen de photons. Ainsi, une distribution sub-poissonnienne est caractérisée par une facteur de Mandel $Q < 0$ tandis qu'une statistique super-poissonnienne implique $Q > 0$. Notons cependant que le caractère sub/super-poissonnien est relié à la statistique de comptage pour un temps de mesure T donné, et qu'il est ainsi directement attaché à une certaine échelle de temps. Une statistique de photons peut par conséquent être sub-poissonnienne pour une échelle de temps et devenir super-poissonnienne à une autre.

En termes plus intuitifs, une statistique sub-poissonnienne indique des fluctuations d'intensité réduite à l'échelle de temps considéré et donc une certaine régularité dans l'arrivée des photons. Une telle statistique est fondamentalement non-classique ; comme on peut s'en convaincre à l'aide de la relation (4.19), une valeur négative du paramètre de Mandel est nécessairement reliée à une fonction d'autocorrélation $g^{(2)}(\tau)$ inférieure à l'unité sur un certain intervalle de temps, et ceci est impossible dans le cas d'un état classique de la lumière.

Ainsi, nous avons établi que pour des échelles de temps $|\tau|$ très inférieures à la durée de vie τ_0 de fluorescence d'un émetteur unique, la fonction $g^{(2)}(|\tau|)$ était proche de zéro. L'équation (4.19) montre que l'on peut, en pilotant un émetteur unique à cette échelle de temps, générer une statistique sub-poissonnienne de photons, corroborant ainsi l'intuition selon laquelle les instants d'émission des photons par l'émetteur unique présentent une certaine régularité. À l'inverse, une statistique super-poissonnienne, caractérisée par un facteur de Mandel $Q > 0$ est liée non pas à un agencement régulier des photons, mais à une arrivée de ces derniers « par paquets ». Ce phénomène de groupement de photons (en anglais « bunching ») est compatible avec une description classique de l'émetteur. Un tel régime peut être observé pouor des systèmes physiques macroscopique associés à des processus d'émission thermiques ou chaotiques [15].

4.2 Expériences mettant en évidence une statistique de photons sub-poissonnienne

Mettre en évidence expérimentalement le caractère sub-poissonnien d'une statistique de photon requiert de limiter les pertes qui interviennent entre la source de photons et le système de photodétection, pertes qui ont pour effet de rapprocher la statistique de photodétection d'une classique loi de Poisson . À l'inverse, les systèmes physiques susceptibles de générer des statistiques de photons sub-poissonniennes (émetteur unique ou fluorescence paramétrique) nécessitent d'isoler et de contrôler le système physique étudié en le plaçant par exemple à basse température dans un cryostat, et en utilisant des techniques de filtrage spatial, spectral ou temporel, autant d'impératifs qui limitent l'efficacité de collection que l'on peut obtenir en pratiquie. Dès lors, les mesures expérimentales d'une déviation négative du paramètre de Mandel sont restée limitées à des valeurs toujours proches de zéro.

La première expérience portant sur ce paramètre a été réalisée par SHORT et MANDEL en 1983 [160] et était basée sur la fluorescence de résonance d'atomes de sodium, à partir d'un montage proche de celui de la référence [35]. On détecte la lumière lors du passage d'un atome au sein d'un jet atomique, durant un temps de mesure limité à 200 ns. La lumière de fluorescence est bien sub-poissonnienne, et la statistique de photodétection correspond à un paramètre de Mandel $Q = (-1.8 \pm 0.38) \times 10^{-}3$. On notera que cet article précise explicitement que l'observation d'une déviation négative du paramètre de Mandel requiert d'im-

portantes précautions expérimentales. Parmi les différentes caractéristiques du protocole expérimental utilisé, deux conditions, s'avérant cruciales sont soulignées par les auteurs :

- Le jet atomique est fortement atténué afin d'avoir une très faible probabilité d'observer simultanément deux émetteurs dans une même fenêtre de détection ;

- L'utilisation d'un fenêtrage temporel étroit, correspondant à une durée de 200 ns, permet d'éliminer un partie du bruit parasite généré notamment par les coups d'obscurité des photodétecteurs.

Comme nous l'avons exposé dans le chapitre 3 décrivant notre source moléculaire de photons uniques, les choix expérimentaux que nous avons effectué sont bien conformes à ces critères.

Le développement des techniques de piégeage d'ions a permis de réaliser des expériences où il s'avère possible de capturer un ion unique pendant plusieurs minutes et d'observer son émission de fluorescence de résonance. Les travaux menés dans l'équipe d'Herbert WALTHER en 1987 [130] ont ainsi permis d'observer le dégroupement de photons pour un ion unique excité à résonance et d'en inférer le caractère sub-poissonnien de la lumière détectée, correspondant à un facteur de Mandel $Q = -7 \times 10^{-5}$. Là encore, l'efficacité de détection apparaît comme un facteur fortement limitant.

Lorsqu'on évoque les expériences visant à mesurer un facteur de Mandel négatif, on est frappé de la similitude entre cette problématique et celle de la mise en évidence du « squeezing », c'est-à-dire de l'observation de la réduction des fluctuations quantiques d'un faisceau lumineux en dessous du bruit de photons [16]. Tout comme pour la mise en évidence expérimentale d'une statistique sub-poissonnienne, la mesure d'une réduction des fluctuations d'une quadrature du champ en deçà du bruit de photon est directement affectée par les pertes du système expérimental, rendant ainsi particulièrement délicate l'observation directe d'importantes déviations.

Ainsi, jusque dans les années quatre-vingt dix, les expériences effectuées afin de mettre en évidence des fluctuations sub-poissonniennes à l'aide de mesures de corrélations d'intensité [160, 168, 130, 169] se sont toutes heurtées aux limites imposées par l'efficacité de détection, et la plus grande déviation du facteur de Mandel directement mesurée était d'environ 7×10^3

Par rapport aux expériences indiquées précédemment, les techniques de réalisation de sources déclenchées de photons uniques à partir d'un émetteur unique à température ambiante, que nous avons décrites au chapitre 3, permettent de gagner presque un ordre de grandeur en terme d'efficacité globale de détection. Elles se prètent donc bien à l'observation directe de la statistique sub-poissonnienne du faisceau lumineux ainsi [75].

Nous pouvons enfin discuter le cas de la fluorescence paramétrique. Ce phénomène est fondamentalement non-classique [4], non seulement du fait des corrélations quantiques qui peuvent exister entre les photons « signal » et « réplique », mais également au vu de la répartition temporelle des photons. En effet, la production des photons de la paire de photons issue du même photon de pompe est quasi-simultanée, la largeur temporelle de l'état à deux photons étant fixée par les conditions d'accord de phase dans le cristal non-linéaire, et inversement proportionnelle à la largeur spectrale de l'émission de fluorescence. Cette largeur temporelle correspond typiquement à quelques centaines de femtosecondes pour des

[4] On en trouvera par exemple une brillante illustration expérimentale dans le récent article [165].

cristaux non-linéaires de quelques millimètres de long.

Dans le cas des photons uniques « annoncés », il convient cependant d'établir une différence entre le caractère sub-poissonnien de la statistique *conditionnelle* obtenue et la statistique de la lumière directement émise par la source. En effet, en régime d'excitation continue, l'émission de paires de photons par fluorescence paramétrique est un processus spontané dont la répartition temporelle est aléatoire, tandis que la distribution statistique du nombre de paires émises est thermique, associée à une distribution de Bose-Einstein. Dès lors, le flux de photons dans le mode spatial correspondant aux photons « signal » (ou « idler ») possède une statistique poissonnienne voire super-poissonnienne. Ce n'est qu'au niveau des corrélations temporelles entre les deux faisceaux ainsi générés qu'apparaissent les corrélations non-classiques.

4.3 Acquisition de la statistique de photons et mise en forme des données

Nous avons cherché à tirer partie des fonctionnalités de la carte TIA[5], en terme d'acquisition des données. Cette carte est adaptée à l'acquisition d'informations sur une large gamme d'échelles de temps et ellepermet d'enregistrer sur deux voies l'ensemble des instants de photodétection des deux photodiodes à avalanche avec une résolution temporelle de 75 ps et un temps mort électronique de 240 ns pour chaque voie. En limitant la cadence d'excitation du centre émetteur à la valeur de 2 MHz, toute l'information temporelle au sujet de la dynamique d'émission de notre source de photons uniques peut alors être enregistrée, permettant une caractérisation statistique sur une large gamme d'échelles de temps. Cette méthode permet ainsi d'effectuer une analyse globale de la statistique de photons de la source, ce qui constitue un avantage si on la compare à la caractérisation plus communément effectuée et reposant sur l'enregistrement de l'histogramme $c(\tau)$ des intervalles de temps séparant deux détections consécutives. On notera également que cette dernière technique, basée sur un montage de type Start – Stop, ne permet d'évaluer simplement la fonction d'autocorrelation $g^{(2)}(\tau)$ qu'à la limite des temps courts et des faibles efficacités de détection [38, 68].

Les données que nous allons considérer dans la suite de ce chapitre sont issues d'un échantillon statistique unique. Elles correspondent aux mêmes données d'acquisition – et par conséquent à la même molécule unique – que celles qui ont été utilisées pour réaliser la figure 3.16. La séquence $\{t_i\}$ des instants de photodétection y est signalée à l'aide des deux barres verticales, espacées d'une durée de 162 ms, qui délimitent les données que nous avons sélectionnées pour le post-traitement effectué après l'enregistrement complet de l'émission de la molécule.

L'information contenue dans cette séquence $\{t_i\}$ est dans un premier temps transformée en une information sur le nombre de photodétections intervenues pour chacune des impulsions excitatrices appliquées à la molécule. Pour cela, les instants de photodétections sont resynchronisés par rapport à une horloge numérique, la procédure complète étant décrite dans l'Annexe A. La valeur de la période d'excitation est reconstituée à partir de l'ensemble des instants de photodétection au moyen d'une méthode s'apparentant aux techniques de récupération d'horloge. Une fois les instants de photodétection synchronisés sur cette horloge, on peut effectuer une discrimination temporelle. On applique pour cela un

[5]GT 653 GuideTech

fenêtrage débutant avec l'impulsion excitatrice, durant lequel on compte le nombre de photodétections intervenues. Nous avons choisi une durée de fenêtrage de 30 ns, plus de dix fois supérieure au temps de vie de fluorescence de la cyanine dans le PMMA. Ainsi, plus de 99.9 % des événements de fluorescence sont conservés. Les événements situés en dehors des fenêtres sont rejetés car nous pouvons estimer qu'ils sont dus au bruit de fond et aux coups d'obscurité des photodétecteurs. Cette procédure permet d'améliorer légèrement le rapport signal à bruit de la détection de fluorescence. À l'issue de ce traitement préliminaire, on associe à chaque impulsion excitatrice p, un nombre $n_p = 0, 1, 2$ de photons détectés. On remarquera que notre système d'acquisition, composé uniquement de deux photodiodes à avalanche, ne nous permet pas d'enregistrer plus de deux photodétections par fenêtre de 30 ns.

Durant la durée d'émission de 162 ms que nous considérons ici, la molécule a été excitée à énergie constante, donnant lieu à 15 332 photodétections durant les 325 313 périodes d'excitation. Le filtrage temporel que nous venons de mentionner retient finalement 15 138 événements. Nous aboutissons donc à une représentation de nos données en fonction d'une discrétisation des instants de photodétection, que nous allons ensuite utiliser pour quantifier les paramètres statistiques de la source de photons uniques.

4.4 Statistiques à l'échelle d'une impulsion et comparaison avec une distribution poissonnienne

La répartition statistique du nombre de photodétections par impulsion excitatrice est résumée dans le tableau 4.1. Ces chiffres, calculés directement à partir de la liste $\{n_p\}$, vont permettre de quantifier le caractère sub-poisonnien des impulsions lumineuses produites par notre source.

n	0	1	2
nombre d'impulsions avec n photodétections	310190	15108	15
probabilité P(n)	0.95351	0.04644	4.6×10^{-5}

TAB. 4.1 – Répartition statistique du nombre de photodétections par impulsion excitatrice. Ces données, correspondant à la source moléculaire de photons uniques représentée sur la figure 3.16, seront dénotées par l'indice (S). Le nombre total de photons détectés est 15138 pour 325313 impulsions d'excitation. Le nombre moyen de photons détectés par impulsion est $\langle n \rangle = 0.04653$.

Nous pourrons chercher à interpréter directement les chiffres du tableau 4.1, afin de comparer la statistique de la source à celle d'une source cohérente servant de référence. Une manière simple de procéder consiste ainsi à prendre comme paramètre de comparaison le rapport entre $P(2)$ et $P(1)^2/2$. En effet, pour une statistique de photons d'une source poissonnienne présentant en moyenne un faible nombre de photons par impulsion $\langle n \rangle \ll 1$, ce

rapport est proche de l'unité tout en étant indépendant de l'intensité de la source et donc de $\langle n \rangle$. On a en effet, $P(2) = e^{-\langle n \rangle} \langle n \rangle^2 / 2 \simeq P(1)^2/2 = (e^{-\langle n \rangle} \langle n \rangle)^2/2$.

Nous allons cependant voir qu'il serait erroné de comparer directement la statistique des photons avec la statistique des photodétections. Il existe en effet un écart entre ces deux distributions, dû aux imperfections du système d'acquisition telles que les pertes, le bruit ajouté ou les non-linéarités des détecteurs associées à des phénomènes de saturation ou au temps mort. Si l'on considère le cas de la source de photons uniques et l'interprétation de la statistique des photodétections, l'évaluation rigoureuse de la réduction du taux d'impulsions à plusieurs photons nécessite une prise en compte de l'influence des caractéristiques expérimentales du système de détection.

4.4.1 De la statistique de photons à celle des photodétections

Les clics de photodétection enregistrés avec la carte d'acquisition TIA sont obtenus au moyen de deux photodiodes à avalanche, placées de par et d'autre d'une lame séparatrice dans le montage d'HANBURY BROWN et TWISS. Ces deux voies d'acquisition présentant un temps mort électronique de 240 ns (cf. figure 3.8), chacune des photodiodes ne peut « cliquer » plus d'une fois pendant une fenêtre d'acquisition, dont nous avons fixé la durée à une valeur de 30 ns. L'influence des temps morts des photodiodes à avalanche s'apparente donc à une saturation du système de détection ; puisqu'il est impossible de détecter plus de deux photons pour chaque impulsion lumineuse. En revanche, le montage d'HANBURY BROWN et TWISS permet d'étudier la statistique des photons, jusqu'à des temps bien inférieurs à la limite imposée par le temps mort de chacun des détecteurs. En particulier, nous allons pouvoir évaluer la statistique de photons à l'intérieur d'une même impulsion, ce qui correspond à des intervalles de temps compris entre 0 et 30 ns.

La relation entre le nombre de photons incidents et le nombre de photodétections à l'échelle d'une impulsion dépend des caractéristiques du système expérimental. Nous pouvons séparer les différentes contributions au moyen de la modélisation présentée sur la figure 4.2 que nous allons maintenant expliciter.

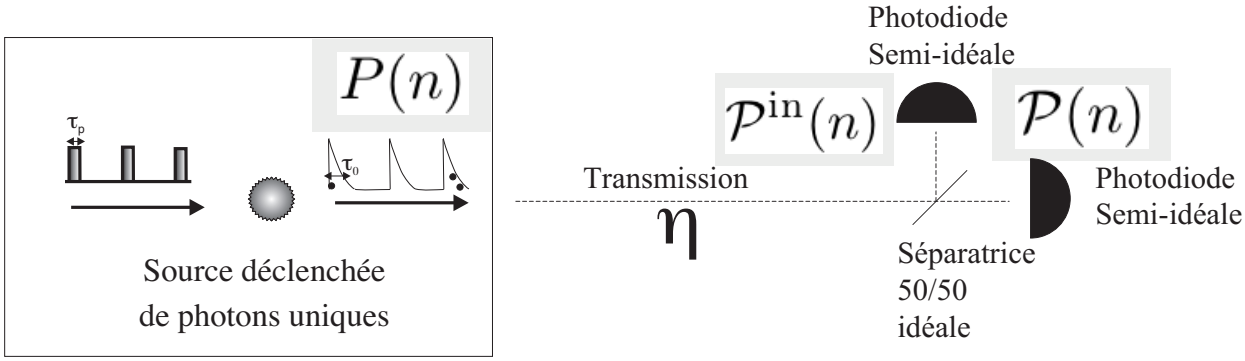

FIG. 4.2 –

Considérons tout d'abord la source de photons fonctionnant en régime d'excitation impulsionnelle périodique. On s'intéresse au nombre total de photons n émis par la source durant ce que nous appelons une « impulsion », c'est-à-dire les 30 ns suivant l'excitation de la molécule par le laser. Cette fenêtre temporelle est suffisamment longue devant le temps de vie de fluorescence de la molécule pour que l'on soit sûr qu'elle contient tous les photons

de fluorescence. Nous désignerons par la notation cursive $\mathcal{P}(n)$ la distribution du nombre de photons émis par la source dans une impulsion afin de la distinguer de la statistique des photocoups $P(n)$, laquelle est mesurée et correspond à la somme des « clics » des photodétecteurs enregistrés durant la fenêtre temporelle d'acquisition.

On combine dans un facteur unique η les atténuations linéaires placées sur le signal, c'est-à-dire le produit de l'efficacité de collection des photons, de l'efficacité de transmission et de l'efficacité de détection des photodétecteurs. Toutes ces pertes, regroupées dans le seul facteur η, peuvent être modélisées par une lame séparatrice idéale de transmission η. De même, on adopte un modèle de photodétecteur « semi-idéal » dont l'efficacité de détection est égale à l'unité mais qui est néanmoins affecté d'un temps mort et qui par conséquent ne peut cliquer plus d'une fois par impulsion. Notre modélisation va permettre de calculer séparément les effets dus à l'atténuation et ceux dus au temps mort de photodétection.

La relation entre la statistique $\mathcal{P}(n)$ des photons émis par la source et la statistique des photons incidents sur la lame séparatrice $\mathcal{P}^{\text{in}}$ est donnée par une loi binomiale, dont le paramètre est la transmission linéaire η du système. Nous avons ainsi :

$$\mathcal{P}^{\text{in}}(n) = \sum_{m=n}^{\infty} \binom{m}{n} \eta^n (1-\eta)^{m-n} \mathcal{P}(m) \tag{4.27}$$

Connaissant $\mathcal{P}^{\text{in}}(n)$, distribution statistique du nombre de photons incidents sur la lame 50/50, il reste à la relier à la distribution $P(n = 0, 1, 2)$ du nombre n de photons *détectés*. La transformation non-linéaire correspondante peut être calculée au moyen de notre modélisation de la réponse des photodiodes. Considérons tout d'abord le cas où la lumière est envoyée directement sur un seuls photodétecteur « semi-idéal ». Celui-ci va saturer dès qu'il y a plus d'un photon incident par impulsion ; soit :

$$P(0) = \mathcal{P}^{\text{in}}(0) \quad \text{et} \quad P(1) = \sum_{n\geq 1}^{\infty} \mathcal{P}^{\text{in}}(n) \tag{4.28}$$

Pour notre système expérimental à deux photodétecteurs, nous devons considérer le partage aléatoire des photons de part et d'autre de la lame séparatrice 50/50 du montage d'HANBURY BROWN et TWISS. On obtient ainsi :

$$P(0) = \mathcal{P}^{\text{in}}(0) \tag{4.29}$$

$$P(1) = \sum_{n\geq 1}^{\infty} \mathcal{P}^{\text{in}}(n) \, \frac{1}{2^{n-1}} \tag{4.30}$$

$$P(2) = \sum_{n\geq 2}^{\infty} \mathcal{P}^{\text{in}}(n) \left(1 - \frac{1}{2^{n-1}}\right) \tag{4.31}$$

La combinaison des équations (4.29), (4.30), (4.31) et (4.27) permet finalement d'établir une relation analytique complète entre $\mathcal{P}(n)$ et $P(n = 0, 1, 2)$. On remarquera que la saturation imposée par l'existence de temps mort est sans effet sur la statistique de photodétection dans le cas d'une source idéale de photons uniques pour laquelle $\mathcal{P}(n \geq 2) = 0$. A l'opposé, pour une source « réelle », , pouvant émettre plus d'un photon par impulsion, le nombre d'événements multiphotoniques détectés est systématiquement sous-évalué. Ainsi, dans la limite expérimentale qui nous intéresse, c'est-à-dire quand l'efficacité globale de collection est faible, la probabilité d'enregistrer deux « clics » de photodétection dans la même impulsion est dominée par le terme en $\eta^2\mathcal{P}(2)$. La probabilité d'une photodétection conjointe est

cependant divisée par un facteur deux par rapport à celle des événements à deux photons de sorte que : $P(2) = \mathcal{P}^{\text{in}}(2)/2 \simeq \mathcal{P}(2)\eta^2/2$. En effet, pour chaque impulsion correspondant à deux photons incidents sur la lame séparatrice, il y une chance sur deux pour qu'ils empruntent la même voie, arrivent sur la même photodiode et ne provoquent dans ce cas qu'un seul « clic » de photodétection. L'existence du temps mort entraîne ainsi une réduction *artificielle* de la variance de la distribution du nombre de photodétection. Il est nécessaire de prendre en compte ce biais pour comparer de manière correcte la statistique des photons émis par la source à une référence « classique » correspondant au bruit de photons.

4.4.2 Comparaison avec une source poissonnienne

L'un des critères essentiels pour évaluer les performances d'une source de photons uniques réside dans la réduction effective de la probabilité d'émission d'impulsions contenant plusieurs photons. Cette réduction est évaluée en comparaison avec une source de référence « classique » de même intensité, dont la statistique obéit à une loi de Poisson. Nous avons effectué cette comparaison de manière analytique, en tenant compte de la relation calculée précédemment entre la statistique $\mathcal{P}(n)$ de photons et la statistique $P(n)$ des photodétections. Nous avons de plus validé cette comparaison par une vérification expérimentale consistant à enregistrer la statistique des photodétections associées à l'émission d'une source cohérente.

Statistique de photodétection d'une source poisonnienne

On peut montrer [19] que le flux de photons rayonnés par une source classique suit une loi de Poisson. Cette distribution statistique a la particularité d'être un point « fixe » vis à vis de l'atténuation ; ainsi une statistique poissonnienne atténuée reste une statistique poissonnienne dont seul le nombre moyen de photons par impulsion est changé. Si on note α le nombre moyen de photons dans une impulsion, la loi de distribution de Poisson s'écrit

$$\mathcal{P}(n) = e^{-\alpha}\alpha^n/n! \tag{4.32}$$

Si l'on veut mesurer la statistique de photons d'une source poissonnienne de paramètre α à l'aide du montage décrit dans la figure 4.2, l'atténuation linéaire de paramètre η, dont l'effet est décrit par l'équation (4.27), transforme la distribution précédente en une distribution poissonnienne de paramètre $\eta \times \alpha$ laquelle va correspondre à $\mathcal{P}^{\text{in}}(n)$. La statistique de photodétection associée, que nous noterons $P_{\text{P}}(n)$, peut alors être dérivée à partir des équations (4.29), (4.30) et (4.31)), soit :

$$P_{\text{P}}(0) = e^{-\eta\alpha} \tag{4.33}$$
$$P_{\text{P}}(1) = 2e^{-\eta\alpha/2}(1 - e^{-\eta\alpha/2}) \tag{4.34}$$
$$P_{\text{P}}(2) = (1 - e^{-\eta\alpha/2})^2, \tag{4.35}$$

Étalonnage du système de mesure

Afin de nous assurer de la validité des expressions analytiques fondées sur la modélisation du système de photodétection, nous avons effectué une mesure expérimentale de la statistique des photocoups associée à une source poissonnienne. Nous avons utilisé pour cela les impulsions du laser de pompe soumis à une très forte atténuation, et obtenues en pratique en décalant légèrement la longueur d'onde d'émission du laser Ti :Sa par rapport à la bande de réjection du filtre « notch » utilisé pour la détection de molécules uniques. La lumière de pompe est alors réfléchie sur un miroir métallique qui remplace l'échantillon, puis une

faible fraction résiduelle est transmise à travers le miroir dichroïque et le filtre « notch ». Les taux de comptage associés à cette référence expérimentale (notée R) sont ajustés de façon à être le plus proche possible de ceux enregistrés pour la source de photons uniques (S) précédemment décrite. On aboutit ainsi à une mesure complémentaire des probabilités $P_{\mathrm{P}}(n)$ que l'on peut confronter aux résultats 4.33, 4.34 et 4.35 utilisés pour dériver les expressions de $P_{\mathrm{P}}(n)$.

Résultats

Le tableau 4.2 présente la comparaison des résultats obtenus pour la statistique de photodétection de la source de photons uniques (S) avec les prédictions analytiques (P) et les mesures expérimentales (R) effectuées pour une référence poissonnienne correspondant au même nombre moyen de photons par impulsion.

Notons que la précision statistique sur les mesures des probabilités $P(n = 0, 1, 2)$ est fixée par la taille des données analysées, c'est-à-dire les nombres d'événements N_0, N_1 et N_2 correspondant à respectivement à 0, 1 ou 2 photons enregistrés. Dans le cas d'une molécule unique, le nombre d'événements enregistrés est limité par le photoblanchiment et l'incertitude relative sur la valeur calculée de $P(n)$ à partir des données de l'expérience, varie comme $1/\sqrt{N_n}$. Elle peut atteindre 0.25 dans le cas de $P(2)$, en raison du faible nombre d'événements collectés, comme on peut le voir à partir des chiffres présentés dans le tableau 4.1. L'incertitude sur la mesure de P(1) est quant à elle inférieure à 10^{-2}.

	$n = 1$	$n = 2$	$\langle n \rangle$
$P_{\mathrm{S}}(n)$	0.0464	$(5 \pm 1) \times 10^{-5}$	0.0465
$P_{\mathrm{R}}(n)$	0.0452	$(50 \pm 5 \times 10^{-5}$	0.0462
$P_{\mathrm{P}}(n)$	0.04514	53×10^{-5}	0.0462

TAB. 4.2 – Probabilités de photodétection $P(n)$ pour la source moléculaire de photons uniques (S), une référence de Poisson expérimentale (R) puis théorique (P). La colonne de droite correspond au nombre moyen $\langle n \rangle$ de photodétections par impulsion.

Le tableau 4.2 montre également qu'un bon accord est obtenu entre les prédictions analytiques et les résultats expérimentaux, pour ce qui concerne la statistique de photodétection de la référence poissonnienne. Cet accord quantitatif indique que l'approche que nous avons développée pour prendre en compte les temps morts est satisfaisante. À partir des équations présentées dans la section 4.4.1 nous pouvons également noter que pour une source poissonnienne dont le nombre moyen de photodétection par impulsion est faible, alors $P(2) \simeq P(1)^2/4$. La confrontation de cette référence statistique avec les résultats concernant notre source de photons uniques fait apparaître que la réduction du taux d'impulsions à plusieurs photons atteint un facteur de l'ordre de 10 par rapport à une référence de Poisson. Le taux résiduel d'impulsions contenant plusieurs photons peut être attribué au fond de fluorescence excité par les impulsions du laser de pompe. En faisant une hypothèse supplémentaire, à savoir que la statistique des photons correspondant à ce fond de fluorescence est poissonnienne, nous pouvons caractériser de façon plus précise la source que nous avons réalisée.

4.4.3 Efficacité de collection et bruit de fond de la source moléculaire

Le bruit de fond qui se superpose à l'émission de photons uniques par la molécule unique est dû au taux résiduel de fluorescence du substrat, composé d'une lamelle de verre de 0.17 mm d'épaisseur et d'un dépôt de polymère PMMA d'environ 30 μm d'épaisseur. D'intensité faible par rapport à l'émission de fluorescence d'une molécule unique, ce bruit de fond n'est pas le fait d'un émetteur individuel mais d'un nombre macroscopique d'émetteurs. Il est par conséquent approprié de supposer que la répartition statistique du nombre de photons associés à cette émission parasite suit une loi de Poisson. Nous pouvons ainsi décrire l'émission de la source de photons unique comme la superposition d'une source idéale et d'un bruit de fond poissonnien. Comme on l'a fait dans le § 4.4.1, l'ensemble des pertes linéaires sont ensuite regroupées dans le facteur de transmission global η. Dans le cas d'une source idéale, c'est-à-dire sans bruit de fond, la statistique des photons incidents sur le système de photodétection est :

$$\begin{aligned} \mathcal{P}^{\text{in}}_{\text{perf.SPS}}(0) &= 1-\eta \\ \mathcal{P}^{\text{in}}_{\text{perf.SPS}}(1) &= \eta \\ \mathcal{P}^{\text{in}}_{\text{perf.SPS}}(n\geq 2) &= 0. \end{aligned} \tag{4.36}$$

Nous pouvons par ailleurs écrire le nombre moyen de photons correspondant bruit de fond sous la forme $\eta \times \gamma$, la distribution de probabilité correspondante étant :

$$\mathcal{P}^{\text{in}}_{\text{backgnd.}}(n) = \frac{e^{-\eta\gamma}(\eta\gamma)^n}{n!}, \text{ pour } n \geq 0. \tag{4.37}$$

Enfin, si l'on applique les équations (4.29) à (4.31) à la superposition de ces deux contributions, nous pouvons obtenir des expressions analytiques pour la statistique de photodétection associée à la source « réelle » notée (S) dans le tableau 4.2 :

$$\begin{aligned} P_{\text{S}}(0) &= e^{-\eta\,\gamma}\,(1-\eta) \\ P_{\text{S}}(1) &= 2\,(e^{-\eta\,\gamma/2}-e^{-\eta\,\gamma}) + \eta\,(2e^{-\eta\,\gamma}-e^{-\eta\,\gamma/2}) \\ P_{\text{S}}(2) &= (1-e^{-\eta\,\gamma/2})^2 + \eta\,(e^{-\eta\,\gamma/2}-e^{-\eta\,\gamma}). \end{aligned} \tag{4.38}$$

Les valeurs respectives de l'efficacité globale de collection η et du rapport signal à bruit $1/\gamma$ peuvent être calculées à partir de la statistique de photodétection mesurée P_{S} (cf tableau 4.1) et des équations (4.38). On en déduit la valeur de $\eta \simeq 0.04456$ et de $\eta \times \gamma \simeq 2.02 \times 10^{-3}$. Ceci correspond à un rapport signal à bruit de 22, en bon accord avec le contraste observé lors du balayage de l'échantillon pour lequel le bruit de fond était de l'ordre de 5 kHz, en comparaison avec un signal de l'ordre de e 100 kHz lorsque l'on observe la fluorescence d'une molécule.

4.4.4 Paramètre de Mandel des impulsions lumineuses

Le paramètre de Mandel, $Q \equiv \frac{\langle n^2\rangle - \langle n\rangle^2}{\langle n\rangle} - 1$, qui permet de caractériser les fluctuations du nombre n de photons émis par la source dans une impulsion lumineuse, est un critère d'évaluation des performances d'une source de photons uniques permettant de quantifier son écart à l'idéalité, c'est-à-dire la capacité à délivrer en sortie du dispositif et avec une efficacité unité, exactement un photon. D'un point de vue statistique, cet écart réside dans deux caractéristiques principales : une efficacité inférieure à l'unité, et une proportion non nulle d'impulsions contenant plus d'un photon. Une source idéale aurait pour facteur de Mandel

$Q = -1$ valeur indiquant le caractère rigoureusement sub-poissonnien d'un train d'impulsions dont chacune contient exactement un photon. Les limites expérimentales sur l'efficacité de collection ainsi que sur la réduction d'impulsions multiphotoniques rapprochent la statistique observée d'une distribution de Poisson. Elles ramènent par conséquent le facteur de facteur vers la limite classique correspondant à $Q = 0$.

La mesure et l'interprétation de la valeur du paramètre de Mandel est un problème équivalent à la connaissance de la distribution $P(n)$ des probabilités de photodétection. Nous avons ainsi choisi de travailler directement à partir des données expérimentales correspondant à tous les instants de photodétection, et d'en évaluer directement le paramètre de Mandel *mesuré*, Q_m. Cette valeur peut être calculée à partir des distributions de probabilités $P_{\{S,P,C\}}(n)$:

$$Q_m = [P(1) + 2P(2)] \left\{ \frac{2P(2)}{[P(1) + 2P(2)]^2} - 1 \right\} \tag{4.39}$$

ce qui donne, en utilisant les chiffres du tableau 4.1 liés à la source expérimentale de photons uniques (S), un paramètre de Mandel mesuré $Q_{\mathrm{m}}^{(\mathrm{S})} = -0.04455$. La valeur négative de $Q_{\mathrm{m}}^{(\mathrm{S})}$ confirme que les impulsions produites par cette source ont bien un caractère sub-poissonnien. Cette fois encore, il importe de comparer $Q_{\mathrm{m}}^{(\mathrm{S})}$ à une référence poissonnienne, car le système de photodétection introduit un biais statistique du fait des temps morts des photodiodes à avalanche. En reprenant les équation (4.33) à (4.35) ainsi que l'équation (4.39), nous pouvons calculer l'expression du paramètre de Mandel $Q^{(\mathrm{P})}$ des photons détectés pour une source poissonnienne (P) émettant en moyenne α photons par impulsion. En remarquant que le nombre moyen de photons détectés est donné par $\langle n \rangle_{\mathrm{P}} = 2\,(1 - e^{-\alpha/2})$ on montre ainsi que :

$$Q^{(\mathrm{P})} = \langle n \rangle_{\mathrm{P}} \left[\frac{2P_{\mathrm{P}}(2)}{\langle n \rangle_{\mathrm{P}}^2} - 1 \right] = \langle n \rangle_{\mathrm{P}} \left[\frac{2(1 - e^{-\alpha/2})^2}{4(1 - e^{-\alpha/2})^2} - 1 \right] = -\frac{\langle n \rangle_{\mathrm{P}}}{2}. \tag{4.40}$$

La statistique de photodétection de cette référence poissonnienne apparaît donc sub-poissonnienne en raison de la saturation des photodétecteurs. Néanmoins, la valeur mesurée pour notre source expérimentale, $Q_{\mathrm{m}}^{(\mathrm{S})}$, diffère de façon significative de la limite correspondant à une statistique poissonnienne de même nombre moyen de photons par impulsion $Q^{(\mathrm{P})} = \langle n \rangle_{\mathrm{P}} = \langle n \rangle = 0.04653$. Une telle source correspondrait en effet à un paramètre de Mandel $Q_{\mathrm{P}} = -0.02327 > Q_{\mathrm{m}}^{(\mathrm{S})}$.

Par ailleurs, comme la proportion d'événements à plus d'un photon est fortement réduite par rapport à celle d'une source cohérente, la valeur mesurée pour $Q_{\mathrm{m}}^{(\mathrm{S})}$ est essentiellement limitée par l'efficacité globale de détection, qui impose une limite inférieure : $Q_{\mathrm{m,lim}} = -\eta = -0.04456$ pour le facteur de Mandel.

Notons qu'il est en général difficile d'obtenir de fortes déviations négatives du paramètre de Mandel, car une telle observation nécessite la réunion de conditions presque antithétiques : avoir un système quantique bien isolé de son environnement et pouvoir l'observer avec une grande efficacité. L'observation par microscopie confocale de la fluorescence d'une molécule unique apparaît de ce point de vue comme un mode opératoire très intéressant, qui permet de conjuguer une bonne efficacité de collection (de l'ordre de 10% dans notre expérience) et un bon rapport signal à bruit optique. Ainsi la valeur mesurée pour le paramètre de Mandel dans notre expérience dépasse de plus d'un ordre de grandeur les valeurs obtenues lors des expériences précédentes portant sur l'observation de statistiques sub-poissonniennes de photons [160, 130, 68].

4.4.5 Lien entre la statistique de photons et la valeur de $g^2(0)$

La méthode que nous avons développée pour analyser les propriétés statistiques de la source de photons uniques repose sur l'enregistrement, à l'aide d'une carte d'acquisition « TIA », de l'ensemble de la distribution des instants de photodétection. Cet enregistrement nous a permis de calculer les distributions statistiques relatives à l'émission de la source. Cette méthode présente l'avantage de rendre « naturel » le calcul de la distribution de probabilité $P(n = 0, 1, 2)$ du nombre de photons détectés par impulsion et permet une analyse relativement exhaustive des données enregistrées, ainsi que la prise en compte des biais statistiques propres au système de photodétection utilisé [171]. Elle diffère cependant de la méthode basée sur l'enregistrement de l'histogramme des intervalles de temps entre deux photodétections consécutives dans le dispositif d'HANBURY BROWN et TWISS, couramment employée dans les expériences sur les sources de photons uniques [38, 87, 105]. Il apparaît ainsi intéressant de comparer le lien entre la mesure de « $g^2(0)$ »[6] et la distribution statistique du nombre de photodétections par impulsion.

Nous avons ainsi recalculé, à partir des données enregistréds par le TIA, l'histogramme des délais afin de érifier la cohérence entre la caractérisation de notre caractérisation de la source de photon unique basée sur la mesure de $P(n = 0, 1, 2)$) et la valeur de $g^2(0)$ évaluée à partir des mêmes données. L' histogramme obtenu par exploitation numérique des données est représenté sur la figure 4.3.

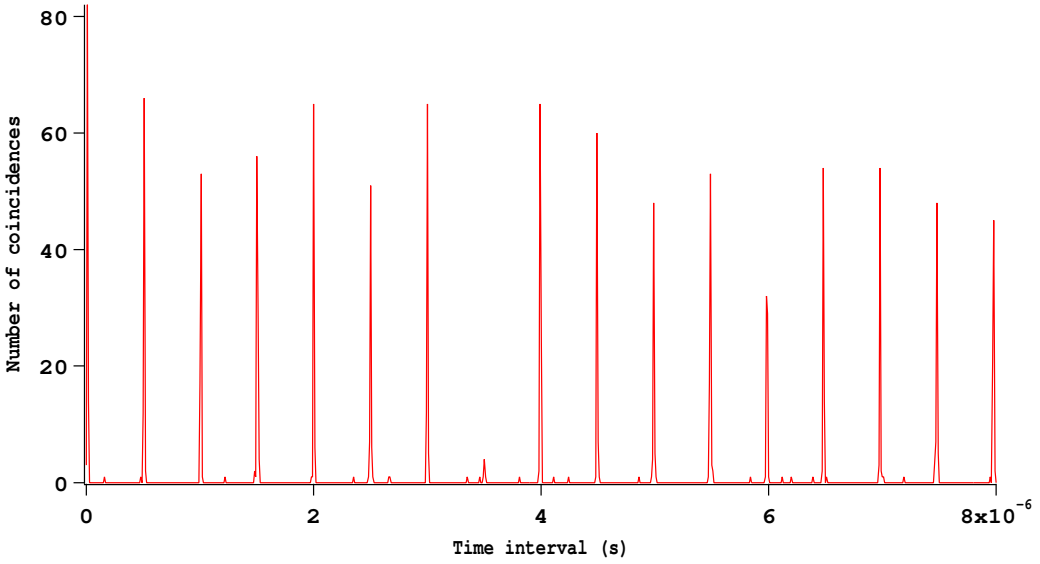

FIG. 4.3 – Histogramme des intervalles de temps séparant deux photodétections, au voisinage du délai nul. Cet histogramme a été calculé numériquement à partir des données $\{t_i\}$ enregistrée par le TIA. La fenêtre temporelle associée a pas de l'histogramme (« timebin ») est de 10 ns.

Comme nous l'avons expliqué au §4.1.3, les paramètres $g^{(2)}(0)$ et Q sont eux-mêmes reliés à la distribution de probabilité $P(0, 1, 2)$ du nombre de photodétections par impulsion. Dans le cadre d'une mesure Start – Stop on doit ainsi obtenir :

[6] Ce terme désigne, par abus de langage, l'aire normalisée de la fonction d'autocorrélation d'intensité $g^{(2)}(\tau)$ au voisinage du délai nul. Il constitue le paramètre qui est généralement évalué à partir de l'acquisition de la fonction d'autocorrélation.

$$g^{(2)}(0) = \frac{P(2)}{\langle n/2 \rangle^2} = \frac{4P(2)}{[P(1)+2P(2)]^2} \qquad \text{soit} \qquad g^2(0) = 8.5 \times 10^{-2} \tag{4.41}$$

Par ailleurs, la valeur de $g^{(2)}(0)$ peut être directement évaluée à partir de l'histogramme des retards représenté sur la figure 4.3. En normalisant le nombre de coïncidences intervenues sur une fenêtre de durée 500 ns autour du délai nul, pendant le temps d'acquisition de durée T = 162 ms (cf. § 3.16), nous obtenons : $g^{(2)}(0) = 8.2 \times 10^{-2}$, valeur en bon accord avec celle calculée à partir de l'équation (4.41).

Les équations (4.39) et (4.41) montrent qu'il existe une relation analytique directe entre le facteur de Mandel mesuré, Q_m et la mesure de $g^{(2)}(0)$:

$$Q_m = \langle n \rangle \Big(\frac{g^{(2)}(0)}{2} - 1 \Big), \tag{4.42}$$

justifiant ainsi a posteriori le fait que l'essentiel de notre analyse ait été limitée à la mesure du facteur de Mandel.

4.5 Etude des fluctuations d'intensité

La plupart des réalisations expérimentales de sources de photons uniques, présentent un phénomène d'intermittence, observé aussi bien avec des molécules uniques [43], des centres colorés dans le diamant [87], que des boîtes quantiques InAs/GaAs [105] ou des nanocristaux semi-conducteurs [118]. De multiples phénomènes physiques sont à l'origine de cette intermittence ; comme par exemple la fuite du système vers un état « noir »(état triplet des molécules de colorant) ou une perturbation du dipôle émetteur conduisant à un arrêt momentané de son émission. Ainsi, dan les nanocrsitaux de CdSe, le phénomène de scintillement (ou « blinking ») est dû à une ionisation par effet Auger [100] et présente une particularité statistique : la distribution des durées des périodes noires suit une loi de puissance (vols de Lévy, [23]) pour laquelle le temps d'émission « ON » du dipôle n'admet pas de valeur moyenne [118].

De façon générale, l'intermittence entre des périodes d'émission et des périodes noires est un phénomène qui diminue l'efficacité de la source et perturbe son utilisation du fait des interruptions aléatoires. L'analyse statistique que nous avons développée permet de relier les fluctuations d'intensité aux paramètres photophysiques de la molécule étudiée, et à sa dynamique interne.

4.5.1 Comment quantifier les fluctuations d'intensité

Afin d'étudier les effets de l'intermittence sur l'émission de photons uniques par notre source, nous avons analysé les données enregistrées au moyen de notre système de comptage de photons résolu en temps. On s'intéresse aux fluctuations statistiques du nombre de photodétections intervenant durant des fenêtres d'intégration de tailles variables, l'un des intérêts de notre méthode d'acquisition étant de rendre possible ce type d'étude sur une très large gamme d'échelles de temps.

Nous avons pour cela prolongé l'analyse développée au § 4.4.4 et avons étudié l'évolution du facteur de Mandel à l'échelle de plusieurs impulsions lumineuses. Nous pouvons ainsi caractériser l'amplitude des fluctuations d'intensité pour les échelles de temps supérieures à la période de répétition des impulsions d'excitation.

Calcul du facteur de Mandel dépendant du temps

La liste du nombre de photodétections en fonction de l'indice de l'impulsion d'excitation $\{n_p\}$ est une transcription sur une échelle de temps discrète des variations d'intensité de la source. Comme nous avons pu le voir en calculant les paramètres statistiques de la source de photons uniques, la relation entre les fluctuations statistiques de la source et celles des photodétections est essentiellement déterminée par le facteur de transmission η du système. Le calcul du paramètre de Mandel, sur lequel l'effet d'une atténuation linéaire se traduit par un simple facteur multiplicatif, apparaît donc d'autant plus pertinent dans cette situation.

La variable à laquelle nous allons nous intéresser pour cette étude est le nombre total $N(T)$ de photons détectés durant une durée d'intégration $T \equiv \mathcal{M} \times \tau_{\text{rep}}$, multiple de la période de répétition τ_{rep} du laser d'excitation. Plus précisément, la liste $\{n_p\}_{p=1,\ldots,\mathcal{N}}$ du nombre de photocoups enregistrés durant $\mathcal{N}$ périodes consécutives est découpée en sous-ensembles consécutifs, chacun de taille $\mathcal{M}$. Nous obtenons ainsi $\mathcal{N}_{\text{sample}} = E[\mathcal{N}/\mathcal{M}]$ sous-ensembles et appelons $N_k(T)$ le nombre de photodétections enregistrées durant la k^{e} fenêtre d'intégration. Ainsi :

$$N_k(T) \equiv \int_{k\,\tau_{\text{rep}}}^{(k+1)\tau_{\text{rep}}} I(t)dt = \sum_{p=k\mathcal{M}}^{(k+1)\mathcal{M}-1} n_p, \tag{4.43}$$

et l'on note $\langle\,\rangle_T$ la moyenne statistique sur les $\mathcal{N}_{\text{sample}}$ échantillons de durée T. :

$$\langle N\rangle_T = \frac{1}{\mathcal{N}_{\text{sample}}} \sum_{k=0}^{\mathcal{N}_{\text{sample}}-1} N_k(T)\,. \tag{4.44}$$

Le paramètre de Mandel mesuré pour un temps d'intégration T est alors défini comme :

$$Q_m(T) \equiv \frac{\langle(\Delta N)^2\rangle_T}{\langle N\rangle_T} - 1, \tag{4.45}$$

Incertitude statistique sur le facteur de Mandel

L'une des difficultés d'une analyse sur des échelles de temps longues vient du nombre limité de mesures statistiquement significatives. On peut vérifier que l'incertitude sur la mesure du facteur de Mandel, c'est-à-dire la variance des mesures effectuées sur un nombre limité de points, varie comme comme $1/\sqrt{N}$ où N est le nombre de points de mesure. Pour cela fixons le nombre N ainsi que les probabilités de photodétection (P_0, P_1, P_2) puis évaluons la variance de mesures successives du facteur de Mandel, c'est-à-dire la quantité

$$Q_m = \frac{\sum_{i=1}^{N} n_i^2}{\sum_{i=1}^{N} n_i} - 1/N \sum_{i=1}^{N} n_i - 1 \tag{4.46}$$

On s'interesse donc au comportement asymptotique de $\langle Q_m^2\rangle - \langle Q_m\rangle^2$ pour N grand, ou $\langle ...\rangle$ dénote la moyenne sur des réalisations successives indépendantes, avec les mêmes probabilités $P_0, P_1 et P_2$.

Pour N grand on a $\langle \sum_{i=1}^{N} n_i^2 / \sum_{i=1}^{N} n_i\rangle \simeq \langle \sum_{i=1}^{N} n_i^2\rangle / \langle \sum_{i=1}^{N} n_i\rangle$.

En utilisant de plus l'hypothèse que les variables n_i sont indépendantes, on peut évaluer les valeurs moyennes des sommes $S_n = \sum_{i=1}^{N} n_i$ et $S_{n^2} = \sum_{i=1}^{N} n_i^2$ à l'aide de fonctions génératrices :

$$\Pi_{S_n}(z) = (P_0 + P_1 z + P_2 z^2)^N \quad \text{et} \tag{4.47}$$
$$\Pi_{S_{n^2}}(z) = (P_0 + P_1 z + P_2 z^4)^N \tag{4.48}$$

On a en effet :

$$\langle S_n \rangle = \frac{\partial}{\partial z}\Pi_{S_n}(z)\Big|_{z=1} \quad \text{et} \quad \langle \mathrm{S_{n^2}} - \mathrm{S_n} \rangle = \frac{\partial^2}{\partial \mathrm{z}^2}\Pi_{\mathrm{S_n}}(\mathrm{z})\Big|_{\mathrm{z}=1} \tag{4.49}$$

Nous avons effectué ces calculs avec Mathematica, et l'on s'assure ainsi que pour N grand, la variance associée aux mesures du facteur de Mandel varie comme $1/\sqrt{N}$:

$$\langle Q_m^2 \rangle - \langle Q_m \rangle^2 \sim \mathrm{O(1/N)} \tag{4.50}$$

4.5.2 Lien entre le bruit d'intensité et l'intermittence dans la fluorescence

Nous avons développé un modèle qui permet de relier les fluctuations d'intensité observées sur la statistique de la source, aux paramètres physiques de la molécule.

Nous supposons pour cela que la source peut se trouver dans deux états : ON ou OFF . Le phénomène d'intermittence, observé aussi bien dans le cas d'une molécule unique [75] que d'un centre coloré NV du diamant [87] est dû à l'existence d'un état triplet métastable non-fluorescent, vers lequel l molécule peut basculer depuis l'état excité fluorescent S_1. La dynamique du comportement ON - OFF en régime d'excitation saturée périodique peut être expliquée à partir du schéma représenté sur la figure 4.5. On note p le taux de transition de l'état ON l'état OFF et q celui de l'état OFF vers l'état ON.

- Les transitions ON $\rightarrow$ OFF consistent en une relaxation de l'état excité S_1 vers l'état triplet métastable T_1. La probabilité correspondante, probabilité de croisement intersystème, notée $\mathcal{P}_{\mathrm{ISC}}$ pour « Inter System Crossing ». Cette probabilité est faible dans le cas des molécules de cyanine $\mathrm{DiIC_{18}(3)}$ utilisées dans notre expérience [64] : ($\mathcal{P}_{\mathrm{ISC}} \simeq 10^{-4}$). En régime d'excitation saturée, chaque impulsion excitatrice porte la molécule dans l'état S_1 si bien que l'on peut définir un taux p de branchement vers l'état triplet. Le facteur $1/p$ s'interprète alors comme la durée de vie de l'état ON, donnée par $1/p = \tau_{\mathrm{rep}}/\mathcal{P}_{\mathrm{ISC}}$.
- Les transitions OFF $\rightarrow$ ON correspondent à la désexcitation non-radiative de l'état triplet T_1 vers le fondamental S_0, associée au phénomène de phosphorescence, et correspondent à une durée de vie $\tau_{\mathrm{T}} = 1/q$. Les règles de sélection interdisant une transition dipolaire entre un état S et un état T, cette durée de vie est bien supérieure à la durée de vie associée à la fluorescence. Ainsi, dans le cas de la cyanine $\mathrm{DiIC_{18}(3)}$, $\tau_{\mathrm{T}} \simeq 200$ μs [64].

.

Dynamique du système ON- OFF

En régime d'excitation pulsée, la dynamique du système ON-OFF peut être évaluée en discrétisant le temps. Nous associons une variable stochastique r_k à l'état du système à l'instant $t_k = (k \times \tau_{\mathrm{rep}})$, où r_k peut prendre deux valeurs : $r_k = 1$ si la source est dans l'état ON à l'instant t_k et $r_k = 0$ si la source est dans l'état OFF à ce même instant t_k.

Nous appelons de plus u_k la probabilité pour que la molécule soit dans l'état ON à l'instant t_k. Comme la source de photons uniques émet uniquement lorsqu'elle est dans l'état

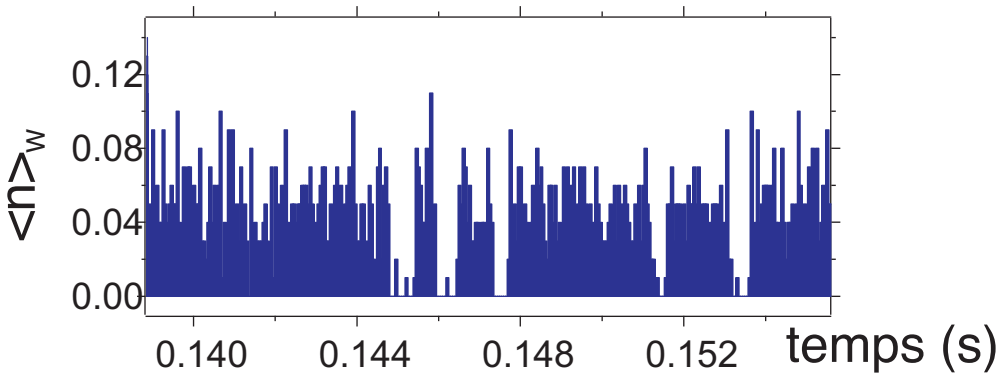

FIG. 4.4 – Périodes « noires » dans l'émission de la source moléculaire de photons uniques. On a représenté le nombre moyen de photons détectés par impulsion, la durée sur laquelle est effectuée la moyenne étant de 100 périodes d'excitation, soit environ 50 μs. À cette échelle de temps, le phénomène d'intermittence dans la fluorescence de la molécule apparaît clairement.

ON, u_k coïncide avec la probabilité d'émission à l'instant t_k. En remarquant que les durées de vie $1/p$ et $1/q$ des état ON et OFF sont beaucoup plus longues que la période de répétition $\tau_{\rm rep}$, on peut limiter les calculs de probabilité aux transitions intervenant entre deux impulsions successives ; ainsi, l'état de la source à l'impulsion $k+1$ ne dépend que de son état à l'impulsion k. Par ailleurs, les probabilités de transition en temps discret sont des grandeurs sans dimension : la probabilité de transition ON→OFF vaut $p\tau_{\rm rep}$ tandis que la probabilité de transition OFF→ON vaut $q\tau_{\rm rep}$. L'équation de récurrence sur u_{k+1}, probabilité d'être dans l'état ON au temps t_{k+1}, peut donc s'écrire :

$$u_{k+1} = (1 - p\tau_{\rm rep})\, u_k + q\tau_{\rm rep}\ (1 - u_k)\,, \tag{4.51}$$

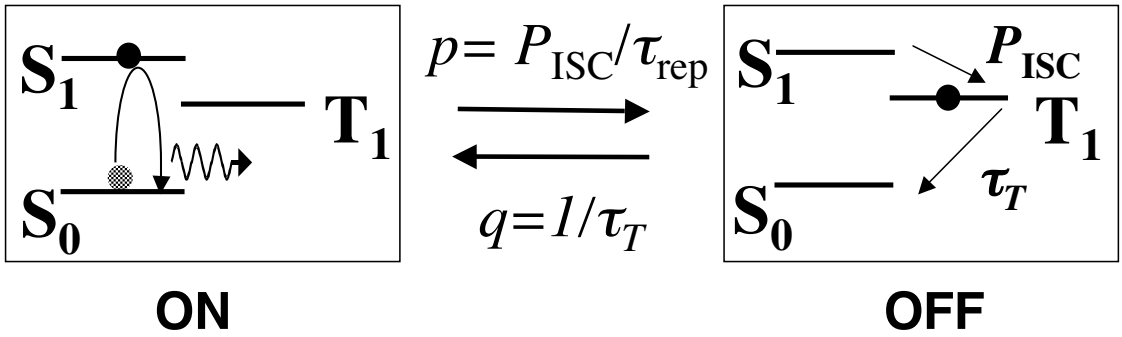

FIG. 4.5 – Structure à trois niveaux utilisée pour modéliser l'intermittence ON - OFF de la molécule. Dans l'état ON, la molécule effectue des cycles d'excitation-émission entre l'état fondamental S_0 et l'état excité S_1. Dans l'état OFF, la molécule est piégée dans l'état « noir » métastable T_1. Les transitions de S_1 vers T_1 ont lieu avec une probabilité $\mathcal{P}_{\rm ISC}$ après chaque excitation et correspondent à un taux de transition ON→OFF $p = \mathcal{P}_{\rm ISC}/\tau_{\rm rep}$. Les transitions inverses, OFF→ON, ont lieu à un taux $q = 1/\tau_{\rm T}$, où $\tau_{\rm T}$ est la durée de vie de l'état triplet T_1.

conduisant à la solution générale :

$$u_k = \left(u_0 - \frac{q}{p+q}\right)\,(1 - p\,\tau_{\rm rep} - q\,\tau_{\rm rep})^k + \frac{q}{p+q}. \tag{4.52}$$

Cette équation donne l'évolution de la probabilité d'émission de la source en fonction de la condition initiale u_0. Elle est associée à un effet de mémoire sur une durée $1/(p+q)$ et correspond aux solutions stationnaires :

$$P_{\rm on} = \frac{q}{(p+q)} \qquad \text{et} \qquad P_{\rm off} = 1 - P_{\rm on} = \frac{p}{(p+q)}$$

.

Paramètre de Mandel dépendant du temps

D'après notre modèle, la lumière émise par la source consiste en une succession d'impulsions émises aux temps $t_k = k \times \tau_{\rm rep}$ avec la probabilité u_k, correspond à une intensité :

$$I(t) = \sum_{k=-\infty}^{+\infty} \delta(t - k\tau_{\rm rep}) \times r_k, \qquad \text{avec } r_k = 0 \text{ ou } 1. \tag{4.53}$$

L'équation (4.52) permet de calculer les propriétés statistiques du flux de photons. En particulier, nous pouvons obtenir l'expression de la variance de $N(T)$, nombre de photodétections intervenues pour une durée T, et en déduire l'expression du paramètre de Mandel dépendant du temps. Les calculs correspondants sont détaillés dans l'Annexe B.

La solution analytique complète, qui correspond à l'équation (B.5), se simplifie dans le régime où $\beta = (p+q)\tau_{\rm rep} \ll 1$, comme c'est le cas pour l'émission de la molécule. Le paramètre de Mandel d'une source de photons uniques intermittente « idéale » est alors donné par :

$$Q_{\rm perf.SPS}(\mathcal{M}\tau_{\rm rep}) = \frac{2p \times \tau_{\rm rep}}{\beta^2}\left\{1 - \frac{1}{\mathcal{M}\beta}\left[1 - (1-\beta)^{\mathcal{M}}\right]\right\} - 1 \tag{4.54}$$

tandis que le paramètre de Mandel « réel » de la statistique de photodétection, est lui affecté par l'efficacité η qui agit comme un simple facteur multiplicatif. Le paramètre de Mandel pour la source réelle est ainsi donné par :

$$Q_{\rm S}(T) = \eta\, Q_{\rm perf.SPS}(T). \tag{4.55}$$

4.5.3 Analyse des données expérimentales

Disposant d'un modèle reliant les fluctuations d'intensité, caractérisées par la valeur du paramètre de Mandel dépendant du temps $Q(T)$, aux paramètres photophysiques de la source, nous pouvons le confronter aux données expérimentales déjà étudiées à la section 4.4. Comme expliqué dans le § 4.5.1, nous pouvons évaluer le paramètre de Mandel des impulsions lumineuses à partir de la liste de données expérimentales de photodétection $\{n_p\}_{p=1,\ldots,\mathcal{N}}$. La courbe correspondante est reproduite sur l'insert de la figure 4.6 et représente la variation du facteur de Mandel $Q^S_{\rm m}(T)$ pour des échelles de temps T variant de la microseconde aux dizaines de millisecondes, soit sur plus de quatre ordres de grandeur.

La fenêtre principale de la figure 4.6 détaille le comportement de $Q^S_{\rm m}(T)$ pour les temps d'intégration courts. Elle fait nettement apparaître l'existence de deux régimes distincts en ce qui concerne les fluctuations statistiques de la source :

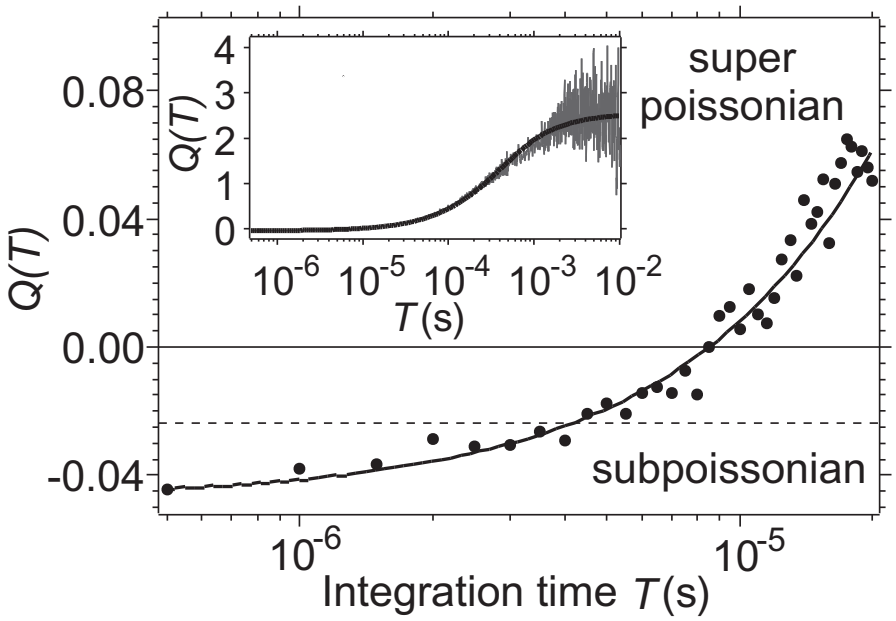

FIG. 4.6 – Paramètre de Mandel de la source moléculaire de photons uniques en fonction de la durée d'intégration T. La courbe est présentée dans son intégralité dans l'insert, tandis que la figure principale correspond à un agrandissement du comportement aux temps courts. La courbe en trait plein représente le résultat de l'ajustement des formules analytiques aux données du modèle ON - OFF. Le trait horizontal pointillé matérialise la limite poissonnienne du facteur de Mandel compte tenu de la saturation introduite par les temps morts des photodétecteurs.

- Sur des échelles de temps inférieures à une durée de l'ordre de $8 \times \tau_{\mathrm{rep}}$, le paramètre de Mandel $Q_{\mathrm{m}}^{S}(T)$ de la source reste en dessous de la limite poissonnienne $Q_{lim} = -\langle n \rangle / 2$. La régularité de l'émission de la source de photons unique, imposée par l'excitation périodique, est alors le phénomène dominant et les fluctuations statistiques de la lumière émise reproduisent le caractère régulier de la lumière d'excitation

- Aux échelles de temps supérieures à une durée de l'ordre de 10 μs, l'intermittence dans l'émission de fluorescence due au basculement de la molécule dans son état triplet, influe fortement sur la statistique de photon. L'alternance de périodes d'émission et de périodes « noires » a pour effet de « grouper » les photons émis par la source [70]. La statistique devient ainsi super-poissonnienne, ce qui se traduit par un excès de bruit et par conséquent une valeur positive du paramètre de Mandel.

Comme on peut le voir sur la figure 4.6, les données expérimentales s'accordent bien avec l'ajustement effectué à partir des formules (4.54) et (4.55). La procédure d'ajustement permet ainsi de déterminer les paramètres physiques liés au constantes de couplage du modèle ON - OFF. Dans le cas des données présentées dans ce chapitre, l'ajustement, obtenu sur plus de quatre ordres de grandeurs temporels, est réalisé en fixant la valeur de l'efficacité globale de détection à la valeur $\eta = 0.04456$ précédemment déterminée. Les paramètres p et q sont eux laissés libres pour l'ajustement, on déduit de leurs valeurs celles correspondant à la de la durée de vie de l'état triplet $\tau_{\mathrm{T}} = 250\,\mu$s, ainsi qu'à la probabilité de croisement

inter-système probabilité d'intersystem crossing : $\mathcal{P}_{\mathrm{ISC}} = p\tau_{\mathrm{rep}} = 2.1\times10^{-4}$. Ces valeurs sont en bon accord avec les mesures réalisées précédemment sur des molécules individuelles de cyanine dispersées dans une matrice polymère [64]. Notre méthode d'acquisition et d'analyse « photon par photon » de l'émission de la molécule, apparaît ainsi pouvoir compléter utilement e les méthodes de caractérisation statistique d'objets individuels.

4.6 Conclusion

La source de photon unique moléculaire que nous avons mise au point nous a permis d'atteindre des efficacités quantiques globales parmi les meilleures alors atteintes en 2002, date à laquelle ces résultats ont été obtenus. Depuis, les boîtes quantiques semi-conductrice dans des micropilliers ont permis d'atteindre de beaucoup plus grandes efficacités quantiques, jusqu'à 37% dans certaines conditions [117], en particulier pour la photodiode au contact du composant, à l'intérieur du cryostat)

Nous avons caractérisé complètement, par une méthode originale, la statistique du nombre de photons détectés en provenance de cette source sur plusieurs ordres de grandeur de la durée d'observation. La molécule agit effectivement comme un « régulateur »de l'intensité en émettant les photons un par un : le bruit d'intensité de la lumière de fluorescence détecté est plus faible que le bruit de photons, et présente un caractère sub-poissonien. Ce résultat n'est cependant valable qu'aux temps courts, inférieur à la μs. Sur les plus longues périodes d'observation, au delà de cette échelle de temps, la dynamique interne de la molécule conduit à un excès de bruit par rapport à la référence de Poisson[7].

Notons que nous avions initialement développé cette source en vue de son application à un système de distribution quantique de clés de cryptage. Cependant, à cause de leur photoblanchiment trop rapide, ces systèmes moléculaires se sont avérés inadaptés à de telles applications. C'est pourquoi, nous avons préféré les centres colorés dans le diamant, ayant une photostabilité à température ambiante bien meilleure, aux molécules pour la réalisation pratique d'expérience de cryptographie quantique : c'est l'objet du chapitre suivant.

[7] Notons que la plupart des systèmes utilisés pour produire des photons uniques présente ce même type de comportement d'intermittence, dû à l'existence d'états "noirs".

Chapitre 5

Centres colorés du diamant comme source de photons uniques

Sommaire

Nous présentons dans ce chapitre les études que nous avons effectuées sur la fluorescence d'un centre coloré du diamant, le centre NV, correspondant à l'association d'une impureté d'azote et d'une lacune dans la maille cristalline. À température ambiante, ce centre coloré possède une structure de niveaux qui, en première approximation, est analogue à celle des molécules de colorant. Ainsi, le schéma d'excitation incohérente utilisé pour les molécules afin de leur faire émettre des photons un par un va s'appliquer à ce système. Contrairement aux systèmes moléculaires précédemment étudiés, le centre NV est parfaitement photostable [94]. Il est par conséquent adapté à une mise en œuvre dans un dispositif de cryptographie quantique à photons uniques [233].

Le travail que nous avons mené prolonge celui réalisé par Alexios BEVERATOS entre 1999 et 2002 dans le cadre de sa thèse, dirigeé par Philippe GRANGIER, au Laboratoire Charles Fabry de l'Institut d'Optique (LCFIO) [86].

Nous débuterons ce chapitre par une description des caractéristiques générales des centres NV et du dispositif permettant de réaliser une source de photon unique à partir de tels émetteurs. Nous effectuerons ensuite une synthèse des résultats obtenus par Alexios BEVERATOS concernant les performances de la source déclenchée de photons uniques reposant sur la fluorescence d'un centre NV unique.

L'objet de notre collaboration avec l'équipe de Philippe GRANGIER a porté sur deux aspects. Nous avons cherché à améliorer les performances de la source de photons uniques fonctionnant à partir de la fluorescence d'un centre NV unique, et nous présentons ici les premiers résultats que nous avons obtenus. En couplant un centre coloré NV unique au mode de résonance d'une microcavité planaire, nous sommes parvenus à réduire la largeur de son spectre d'émission. Le couplage de l'émetteur aec le mode de résonance de la microcavité a par ailleurs la propriété de rendre le diagramme de rayonnement de l'émetteur fortement directionnel dans l'axe de la cavité, facilitant ainsi une collection efficace des photons émis par un objectif de microscope d'ouverture numérique modérée, placé au-dessus de la cavité. Nous évoquerons également le phénomène de photocréation de centre que nous avons pu mettre en évidence en régime d'excitation femtoseconde. Un autres aspect de notre collaboration a été la mise en oeuvre d'une système de cryptographie quantique, avec une transmission des photons en espace libre. Ce travail sera décrit dans le chapitre 7.

5.1 Le centre coloré NV dans le diamant

Le terme « centres colorés du diamant » désigne une famille de défauts optiquement actifs au sein de la matrice cristalline du diamant. L'intérêt des centres colorés du diamant est d'associer les propriétés d'une « molécule fluorescente artificielle » avec une très grande photostabilité et la possibilité d' adresser facilement ces émetteurs individuels en matrice solide. Ils se prêtent donc très bien à la réalisation d'une source déclenchée de photons uniques à température ambiante.

Ces aspect ayant été étudiés en détail dans le cadre de la thèse d'Alexios BEVERATOS, nous nous contenterons ici d'une brève description des propriétés des centres colorés du diamant, renvoyant le lecteur désireux d'en savoir plus au manuscrit correspondant [86].

L'existence de centres NV uniques dans le diamant a été mise en évidence pour la première fois en 1997 dans le groupe de Jörg WRACHTRUP [94] sans néanmoins observer directement la signature du dégroupement de photons. Cet effet fut démontré de manière indépendante trois années plus tard par l'équipe de Philippe GRANGIER à Orsay , [91] et par l'équipe de Harald WEINFÜRTER à Münich [84].

5.1.1 Structure des niveaux d'énergie

Le centre NV correspond à l'association dans deux sites adjacents dans la maille cristalline du diamant d'une impureté atomique ^{14}N d'azote en substitution, et d'une lacune notée V, pour « vacancy » (figure 5.1(a)). La substitution d'un atome de carbone par un atome d'azote apporte un électron excédentaire non apparié, pouvant rester localisé sur ce défaut. Un tel système correspond au centre NV^-, chargé négativement et se comporte comme un *défaut paramagnétique* du fait de l'électron non apparié. Cette propriété le distingue fortement des molécules fluorescentes de colorant, pour lesquelles le niveau fondamental est un niveau singulet de spin, tous les électrons de la molécule étant appariés deux à deux.

Comme on peut le lire sur la figure 5.1(b), les niveaux fondamental et excité sont fortement couplés par une transition dipolaire électrique, dont la raie à zéro phonon est située à une énergie de 1.945 eV correspondant à une longueur d'onde de 637.7 nm. Le couplage de cette transition dipolaire avec les phonons de la matrice diamant est à l'origine d'un important élargissement du spectre d'émission d'un centre coloré NV à température ambiante. Ainsi, à cause des répliques de phonons, la largeur spectrale du spectre d'émission est de l'ordre de 100 nm. Le spectre d'absorption est le symétrique de celui d'émission autour de 637 nm. Ainsi, la longueur d'onde d'excitation peut être choisie indifféremment entre 514

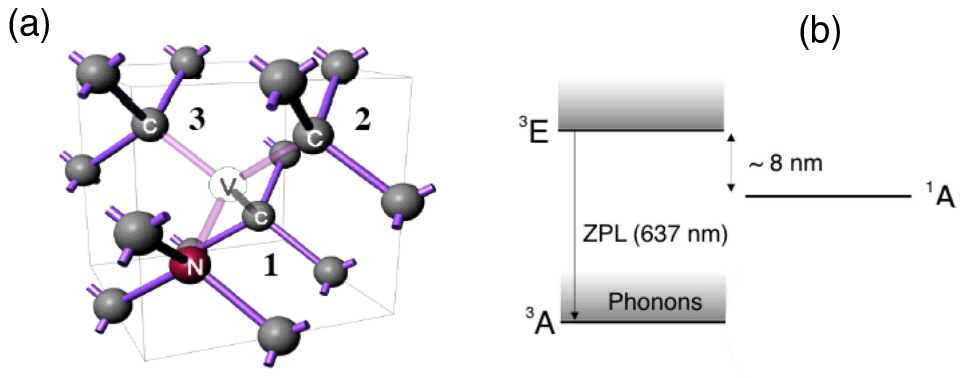

FIG. 5.1 – **(a)** Centre coloré NV dans la maille cristalline du diamant, formé d'un défaut d'azote (N) voisin d'une lacune (V=« vacancy »). **(b)** Représentation schématique des niveaux d'énergie du centre coloré NV. Les états fondamental et excité sont des état triplet, respectivement dénotés ^{3}A et ^{3}E dans la nomenclature associée à la symétrie cristalline C_{3v}. En grisé sont représentés les niveaux vibrationnels excités. La raie « zéro phonon » (ZPL) correspondant à une transition entre les états vibrationnels de plus basse énergie des deux niveaux, est à la longueur d'onde $\lambda = 637$ nm. Le troisième niveau ^{1}A correspond à un état singulet vers lequel peut basculer le centre NV excité, par croisement inter-système. Dans l'état ^{1}A, le centre NV cesse de fluorescer.

nm et 637 nm, sans recouvrement avec le spectre d'émission. Nous avons représenté sur la figure 5.2 le spectre de fluorescence, à température ambiante, d'un centre NV unique dans un nanocristal de diamant tel que nous avons pu l'enregistrer [90].

Notons enfin que de les centres colorés « optiquement actifs » que nous utilisons existent naturellement dans le diamant de type Ib[1], mais en très faible proportion. Afin d'augmenter leur concentration, il est nécessaire de créer des lacunes supplémentaires par irradiation électronique. Un dosage adéquat de la dose d'irradiation permet de créer des centres NV uniques suffisamment séparés les uns des autres pour être observés individuellement par microscopie confocale à température ambiante [94]. La stabilisation des centres colorés est ensuite obtenue par un recuit d'une durée de deux heurs à une température de 800 °C. Tous les échantillons de diamant que nous avons utilisés ont été obtenus en suivant cette procédure, à savoir irradiation électronique puis recuit.

5.1.2 Détection d'un centre NV et fabrication des échantillons

Efficacités de détection

Le groupe d'Optique Quantique du LCFIO a testé différentes associations « échantillon - objectif de microscope », afin d'optimiser l'efficacité de collection de la fluorescence provenant d'un centre NV unique. Le tableau 5.1.2 en présente un récapitulatif. Des « wafers » de diamant massif Ib d'épaisseur 100 μm ont d'abord été utilisés. Cependant, compte tenu

[1]Ce type de diamant contient des impuretés d'azote placées de façon prédominante en substitution, dans des proportions pouvant aller jusqu'à 500 ppm. Très peu (environ 0.1%) de diamant naturel appartiennent à cette catégorie. En revanche, presque tous les diamants synthétiques sont de type Ib.

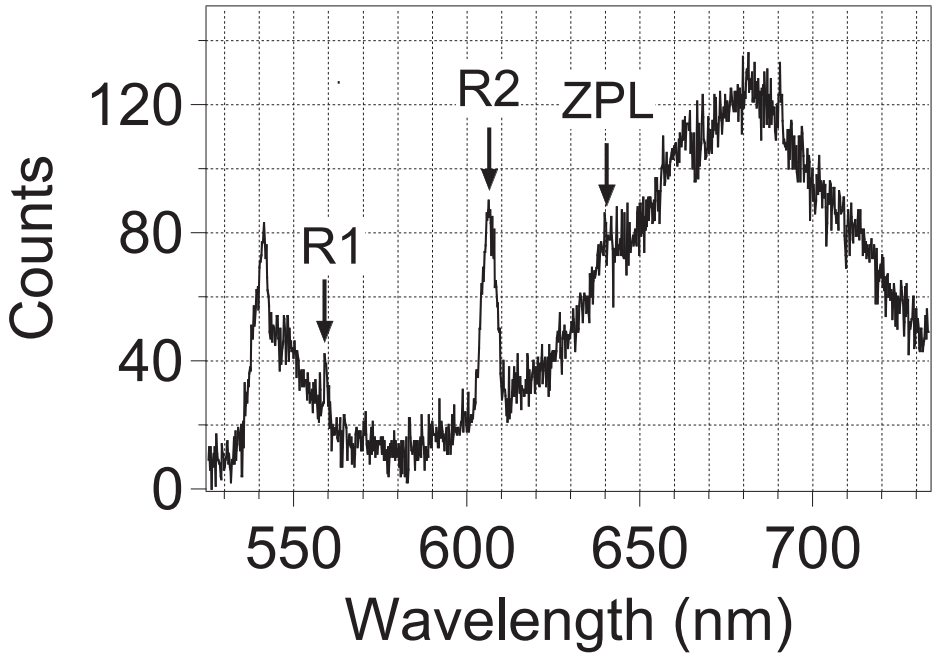

FIG. 5.2 – Spectre de fluorescence d'un centre NV unique dans un nanocristal de diamant. Le centre coloré est excité en éclairage continu à la longueur d'onde $\lambda = 514.5$ nm et à une puissance d'excitation de 10 mW. Ce spectre a été obtenu à l'aide du spectrographe imageur + matrice CCD représenté sur la figure 3.5. On devine la raie à zéro phonon (ZPL) et plus nettement les raies de diffusion Raman à un phonon R1 et à deux phonons R2 provenant de la matrice cristalline de diamant. Le pic étroit qui apparaît en dessous de 550 nm provient de lumière parasite du laser d'excitation, à 514.5 nm ,diffusée dans le spectrographe.

de l'indice de réfraction de n=2.4 du diamant, la réflexion totale à l'interface diamant-air a lieu pour un angle d'incidence de seulement 24.6°, si bien que la lumière de fluorescence d'un centre unique situé dans le diamant massif en sort difficilement par les faces parallèles de l'échantillon, au dessus desquelles nous plaçons l'objectifs de microscope.

Pour palier à ce défaut, le groupe d'Optique Quantique a eu l'idée remplacer les « wafers » de diamant massif par des nanocristaux dont la dimension est très inférieure à la longueur d'onde. Les nanocristaux, de diamètre moyen ≈ 90 nm, sont mélangés à une concentration nanomolaire à un polymère transparent puis déposés en couche ultra-mince sur le substrat, comme nous l'expliquons plus en détail dans le § 5.1.2 suivant. À cette échelle, tout se passe comme si le centre NV rayonne dans le milieu diélectrique qui entoure le nanocristal et la lumière n'est plus affectée par une réflexion diamant-air. L'angle solide sous lequel est collectée la lumière de fluorescence est par conséquent fixé par l'ouverture numérique de l'objectif de microscope, sans être affecté par la forte réfraction qui précédemment avait lieu à l'interface diamant-air [92].

La meilleure efficacité de collection, de l'ordre de 1.6%, est obtenue lorsque les nanocristaux sont déposés sur un miroir de Bragg « $R_{\max}$ » constitué d'une alternance de couches de silice SiO_2 et d'oxyde de niobium Nb_2O_5, matériaux qui s'avèrent être les moins fluorescents pour fabriquer de tels miroirs. Ce miroir, fabriqué selon nos spécifications par la société LAYERTEC (Allemagne), a une réflectivité maximale de 99.99% à la longueur d'onde

Type d'échantillon	Type d'objectif de microscope	Efficacité totale de détection
Diamant massif (« wafer » de dimensions 1.5 mm$\times$1.5 mm$\times$0.1 mm) déposé sur une lamelle de silice	à immersion (Zeiss,$\times$100, ON=1.3)	$\approx 0.5\%$ ([86],p.67)
Nanocristaux de diamant dans une couche mince polymère, déposés sur une lamelle de silice	à immersion (Zeiss, $\times$100, ON=1.3)	$\approx 0.7\%$ ([86],p.67)
Nanocristaux de diamant dans une couche mince polymère **déposés sur un miroir de Bragg** (Réflectivité $R = 99.99\%$ à 690 nm)	à air (sans liquide d'indice) « métallographique » (Olympus, $\times$100, ON=0.95)	$\approx \mathbf{1.6}\%$ ([86],p.104)

TAB. 5.1 – Diverses configurations testées au laboratoire LCFIO en vue d'une optimisation de la collection de la fluorescence d'un centre NV unique.

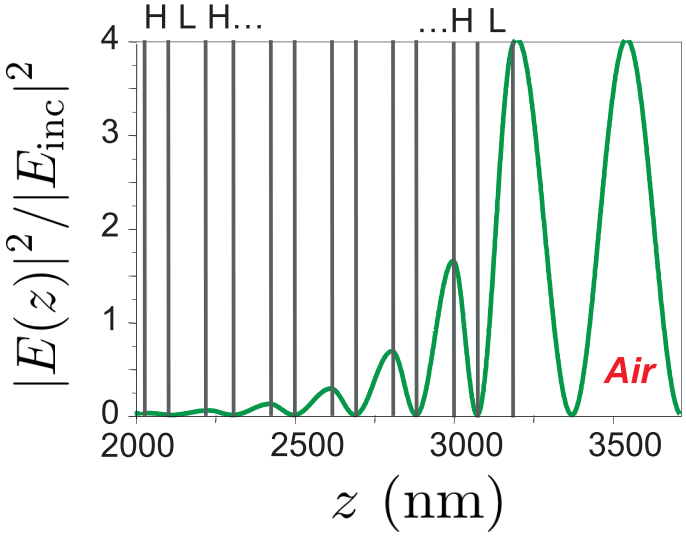

FIG. 5.3 – Structure du miroir de Bragg sur lequel sont déposés les nanocristaux de diamant. Ce miroir est formé d'une alternance d'une couche diélectrique d'indice de réfraction élevé d'oxyde de niobium(H=Nb_2O_5, $n_H = 2.39$) et d'une couche de silice d'indice de réfraction plus faible (L=SiO_2, $n_L = 1.45$). La coube en trait plein représente le module au carré du champ électrique en fonction de la position z sur un axe perpendiculaire à la surface du miroir. Cette courbe résulte d'une modélisation de la structure utilisant la technique des matrices de transfert. La réflectivité théorique du miroir ainsi prédite par le modèle est de 99.9996% à 690 nm, le fabricant garantissant une valeur minimale de 99.99%.

de 690 nm qui correspond au pic d'émission du centre NV (fig.5.2). La structure du miroir, représenté schématiquement sur la figure 5.3, permet d'optimiser la collection des photons émis, dans la configuration de microscopie inversée où l'excitation et la détection sont effectuées à travers le même objectif de microscope. Avec un objectif métallographique à air[2],

[2]Objectif $\times$100 de la marque OLYMPUS, d'ouverture numérique ON=0.95 et de distance de travail$\approx$ 0.1 mm

les taux de comptage typiques obtenus à saturation de l'excitation d'un centre NV unique sont de l'ordre de 80 kcoups/s pour une cadence d'excitation de 5.3 MHz. Ces valeurs correspondent à une efficacité de détection globale $\eta \approx 1.6\%$.

Nous pouvons remarque que cette efficacité est sensiblement inférieure à celle de 4.5% obtenue pour la collection de la fluorescence d'une molécule avec une molécule individuelle. Les raisons d'un tel écart ne sont pas encore clairement identifiés.

Préparation des échantillons utilisant des nanocristaux de diamant

La technique de préparation des échantillons sous forme de nancristaux déposés sur un utilisée a été mise au point par Thierry GACOIN du Groupe de Chimie Physique au Laboratoire de Physique de la Matière Condensée (LPMC, Ecole Polytechnique). Un gramme de poudre commerciale de diamant synthétique Ib, de taille « 0.5 μm ») est tout d'abord irradié pour y créer des lacunes, puis recuit[3]. Comme nous l'avons déjà indiqué, cette procédure conduit à la formation de centres NV stable dans la maille cristalline des nanocristaux de diamant. La poudre est ensuite dispersée dans un polymère en solution (ployvinylpyrrolidone à 1% en masse dans le propanol) à l'aide d'ultrasons. Le polymère utilisé a été choisi pour ses propriétés stabilisatrices de la solution colloïdale de nanocristaux ainsi formée. Cette étape de désagrégation constitue la principale difficulté pour pouvoir disposer de nanocristaux bien isolés les uns des autres. Une centrifugation à 11000 tours/min, effectuée pendant 30 minutes permet ensuite de sélectionner en taille les plus petits cristaux, aboutissant à une distribution en taille de 90 ± 30 nm, mesurée par les techniques usuelles de diffusion de la lumière. La solution centrifugée est finalement déposée à la tournette en film mince d'épaisseur de l'ordre de 30 nm, sur une lamelle de silice ou bien directement sur le miroir de Bragg (fig.5.3).

Durée de vie radiative et milieu diélectrique

Le groupe d'Optique Quantique a remarqué qu'il apparaissait une modification de la durée de vie de l'état excité du centre NV entre le diamant massif dans lequel elle vaut environ 11 ns et les nanocristaux de taille sub-longueur d'onde [92] où elle vaut en moyenne 20 ns. Notons qu'il existe cependant une grande dispersion de cette durée de vie d'un centre coloré à l'autre [4], comme le montre la figure 5.4.

Cette modification de durée de vie est attribuée au changement d'indice de réfraction du milieu diélectrique entourant le centre NV, paramètre intervenant directement dans l'expression du taux d'émission spontanée. Ainsi, le taux d'émission spontanée $\Gamma_{\rm n}$ d'un centre NV dans le nanocristal vaut $\Gamma_{\rm n} = n\Gamma_{\rm v}$, où $\Gamma_{\rm v}$ est son taux d'émission spontanée dans le vide. Compte tenu de la taille sub-longueur d'onde des nanocristaux, on peut considérer que l'émission des centres NV qu'ils contiennent se fait comme dans le milieu qui entoure les nanocristaux, à savoir un demi-espace d'air et l'autre de silice (ou de multicouches diélectriques, si le dépôt a été réalisé sur un miroir de Bragg décrit précédemment). Cette interprétation conduit à un bon accord pour la modification de la durée de vie [88].

Compte tenu de la grande dispersion des durées de vie observées pour les centres NV dans les nanocristaux, des études plus approfondies semblent cependant nécessaires pour totalement valider cette interprétation Ces études pourraient en particulier révéler la nécessité

[3] La dose d'irradiation appliquée est de l'ordre de 3×10^{17} $\mathrm{e}^-/\mathrm{cm}^2$, avec des électrons d'énergie 1.5 MeV. Le recuit est fait à une température de l'ordre de $\approx 800°$C, pendant 2 heures.

[4] Cette large distribution rend probablement compte de la dispersion en position du centre NV au sein des nanocristaux, ainsi que de la dispersion en taille de ces cristaux.

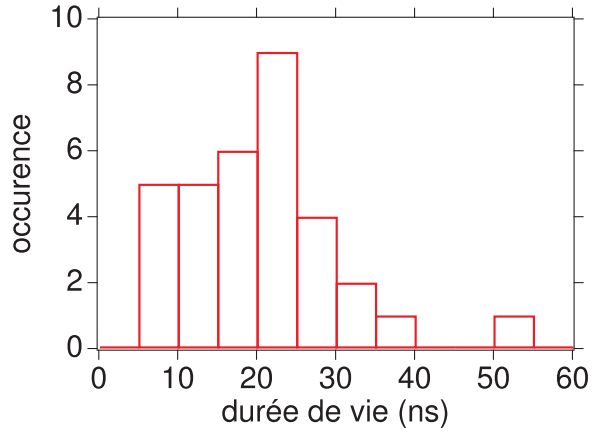

FIG. 5.4 – Distribution de durée de vie de l'état excité de centres NV uniques dans des nanocristaux de diamant déposés sur le miroir de Bragg décrit sur la figure 5.3 . Pour les 33 centres uniques étudiés, la valeur moyenne de la durée de vie est de 20 ns avec une dispersion de l'ordre de 10 ns.

de prendre également en compte un facteur modificatif de *champ local*., ayant pour but de corriger le champ électromagnétique afin d'estimer la valeur effectivement « vue » par les émetteurs. Cette correction dépend de l'environnement immédiat, à l'échelle des liaisons inter-atomques du centre émetteur. Dans l'analyse présentée dans la référence [88] le groupe d'Optique Quantique avait estimé que ce facteur ne changeait pas en passant du matériau massif aux nanocristaux. Nous avons complété cette étude en étudiant la dispersion de durée de vie pour un échantillon de centres NV déposé sur un miroir de Bragg. La valeur moyenne obtenue pour cette distribution est en bon accord avec l'analyse présentée dans la référence [88]. Les résultats de cette étude, effectuée par Robin SMITH étudiante en stage dans notre groupe, sont résumés sur la figure 5.4. Ce travail préliminaire va ensuite être complété en étudiant la modification de la durée de vie de centres NV dans des nanocristaux déposés sur des substrats d'indice de réfraction variés (de 1.45 à 1.7), étude qui devrait permettre de cerner plus clairement l'impact du facteur éventuel de champ local.

5.2 Source de photon unique utilisant le centre NV

Dispositif expérimental

Compte tenu de ses spectres d'absorption et d'émission (figure 5.2), le centre NV absorbe efficacement dans le vert (autour de 500 nm) et émet sa fluorescence sur une large bande centrée autour de 690 nm avec une largeur total à mi-hauteur d'environ 70 nm.

Les photons uniques déclenchés utilisant le centre coloré du diamant sont produits selon le même schéma d'excitation que celui utilisé pour la source moléculaire décrite au § 3.6.1. Le dispositif expérimental combine un microscope en configuration confocale, dont on peut « balayer » le point de focalisation sur l'échantillon et une source laser impulsionnelle nanoseconde, de longueur d'onde égale à 532 nm. Les impulsions de pompe nécessaires à la saturation de la transition du centre NV, doivent être cependant plus énergétiques ($E_{\mathrm{p}} \approx 1$ nW) que celles utilisées pour les molécules, probablement à cause d'une plus faible section ef-

ficace d'absorption du centre coloré. De telles énergies étant difficilement accessibles avec des lasers commerciaux émettant dans le vert, l'équipe du LCFIO a développé une source à 532 nm adaptée à l'excitation impulsionnelle à saturation des centres colorés NV [86], avec une durée d'impulsion de 0.8 ns et une cadence de répétition de l'ordre de ≈ 5 MHz.

Aux puissances d'excitation utilisées pour atteindre le régime de saturation d'un centre NV, on observe lors des premiers « balayages »de l'échantillon, un bruit de fond élevé, dû à la fluorescence résiduelle du miroir diélectrique et à l'émission d'éventuelles impuretés au sein du film polymère. Alors que ces niveaux de bruit de fond auraient été rédhibitoires dans le cadre de nos expériences sur la source moléculaire de photons uniques, la photostabilité des centres colorés NV permet de résoudre ce problème ; on observe en effet, sous excitation impulsionnelle prolongée, un photoblanchiment quasi total du fond de fluorescence tandis que centre NV reste lui parfaitement stable ! La figure 5.5 illustre le bon niveau de rapport signal à bruit (supérieur à 10) que l'on peut ainsi atteindre, après avoir pris le temps de « blanchir » pendant plusieurs dizaines de minutes la zone de l'échantillon située autour du centre coloré sélectionné.

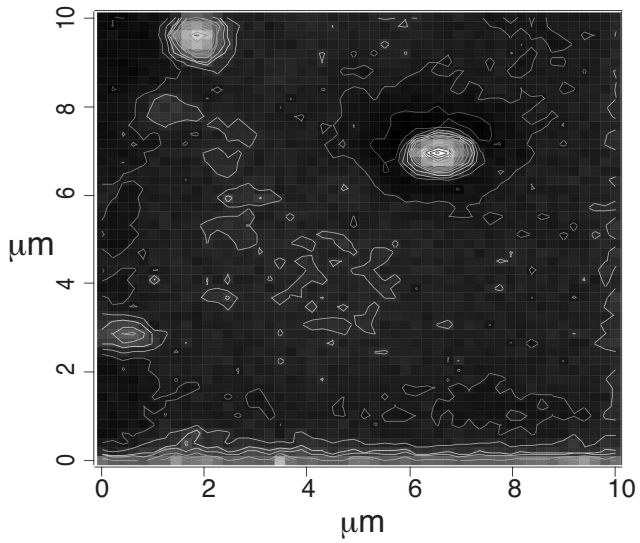

FIG. 5.5 – « Scan »faisant apparaître les variations de niveau de fluorescence lors du balayage par le faisceau laser d'un échantillon de nanocristaux déposés sur un miroir diélectrique. Cette image, a été enregistrée après avoir préalablement « blanchi » le fond de fluorescence du miroir diélectrique et du film polymère entourant les nanocristaux. Elle illustre le fait que seuls les centres colorés NV survivent à cette irradiation, qui permet d'améliorer considérablement le rapport signal à bruit dans la détection des photons émis par le centre coloré.

Fonction d'autocorrélation en intensité

La « qualité statistique » d'un émetteur est ensuite évaluée en enregistrant la fonction d'autocorrélation en intensité $g^{(2)}$ en régime impulsionnel. Le protocole expérimental pour cette mesure est similaire à celui décrit au chapitre 3, avec un montage de corrélations en

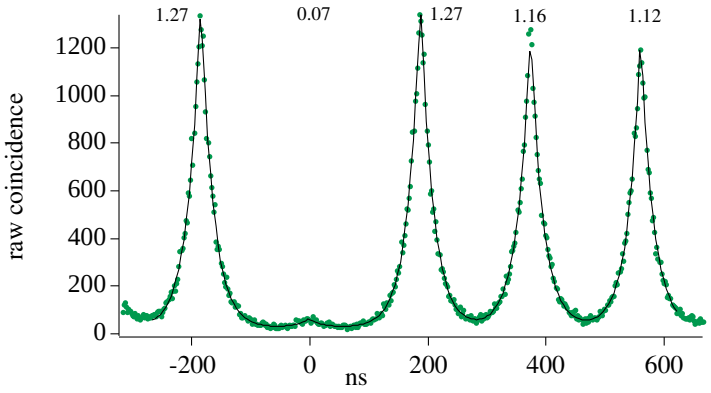

FIG. 5.6 – Fonction d'autocorrélation d'un centre NV unique

intensité de type Start – Stop. La courbe d'autocorrélation est également constituée de pics, espacés de la période de répétition du laser d'excitation, comme on le voit sur la figure 5.6.

L'aire normalisée du pic autour du délai nul $\tau = 0$ nous renseigne sur la « qualité statistique » de la source de photons uniques et est directement reliée aux probabilité $P(1)$ et $P(n \geq 2)$ de la distribution statistique de photons dans les impulsions émises par la source (cf. chapitre 4). Cette valeur n'est pas accessible directement à partir de l'histogramme des délais entre photodétections consécutives. Afin de comparer la statistique des photons à la distribution de Poisson servant de référence, il est nécessaire de normaliser les résultats bruts présentés sous la forme d'un histogramme de délais entre les photodétections successives. On mesure à l'aide d'un compteur digital, les valeurs N_1 et N_2 du nombre de photocoups enregistrés par chacune des photodiodes à avalanche durant le temps total d'acquisition T. Pour une source poissonnienne périodique, de période θ, le nombre moyen de coïncidences intervenant durant une fenêtre temporelle de largeur θ pour une durée totale d'acquisition T est lié aux coïncidences accidentelles N_{acc} :

$$N_{\text{acc}} = N_1 N_2 \frac{\theta}{T} \tag{5.1}$$

Cette dernière expression nous permet de calculer le facteur de normalisation. Si l'on note $c(m)$ le nombre total d'événements dans une fenêtre de largeur θ autour du délai $m \times \theta$, cette valeur est proportionnelle à l'aire des pics de la fonction d'autocorrélation qu'il faut diviser par le facteur de normalisation.

L'aire normalisée du m^{e} pic de la fonction d'autocorrélation est alors donnée par la relation [87] :

$$C_N(m) = \frac{c(m)}{N_1 N_2 \theta / T} \tag{5.2}$$

Dans le cas d'une source poissonnienne, l'aire normalisée de tous les pics est égale à l'unité. L'écart à l'unité de l'aire du pic à $\tau = 0$ donné par le facteur $C_N(0)$, quantifie donc la qualité de la source de photons uniques.

Avec l'objectif métallographique et les échantillons de nanocristaux sur le miroir diélectrique Layertech, nous avons obtenu des valeurs « minimales typiques » de $C_N(0)$ situées autour de 0.1, c'est à dire une réduction d'un facteur 10 du nombre d'événements multiphoniques par rapport à une source cohérente de même taux de comptage.

Nous avons représenté sur la figure 5.6 un enregistrement réalisé en Octobre 2002 dans le cadre de l'expérience de cryptographie quantique avec une source de photons uniques,

décrite au chapitre 7.

5.3 Fluorescence de centres colorés dans une microcavité monomode

Afin d'accroître l'efficacité de collection de la fluorescence provenant d'un centre NV unique, nous avons étudié le couplage des photons émis par le centre coloré au mode de résonance d'une microcavité planaire. Cette dernière doit conduire à une réduction de la largeur angulaire de rayonnement d'un centre unique convenablement orienté, tout en donnant également un affinement spectral des photons transmis par la cavité.

5.3.1 Diagramme de rayonnement

Poser les nanocristaux sur le miroir de Bragg, a pour effet de diriger le diagramme de rayonnement des centres colorés NV qu'ils contiennent vers l'objectif de microscope, comme le montre la simulation réalisée par Yannick DUMEIGE qui a assuré une partie importante des travaux théoriques et expérimentaux liés à la microcavité planaire et notamment les calculs permettant d'établir les diagrammes de rayonnement (cf. figure 5.7).

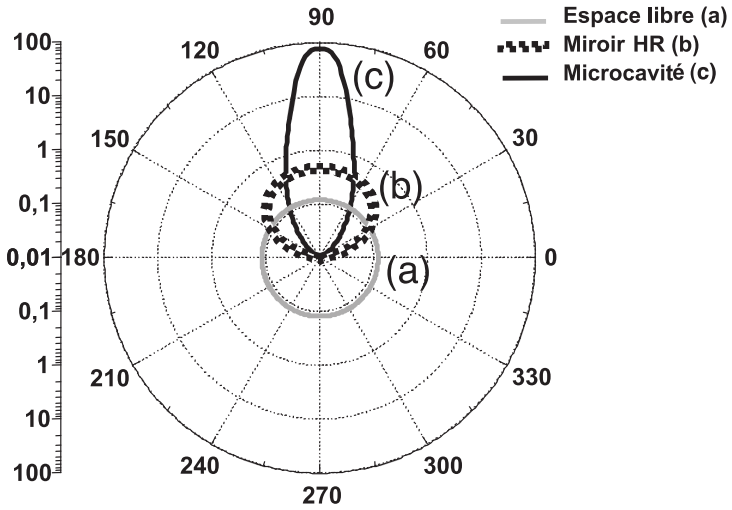

FIG. 5.7 – Simulation du diagramme de rayonnement d'un centre coloré NV assimilé à un dipôle couché dans le plan du miroir. (a) Cas où le centre NV est dans un nanocristal posé sur un miroir de Bragg « $R_{\max} \approx 99.99\%$ » alternant des couches de SiO_2 (couches d'indice de réfraction faible) et de Nb_2O_5 (indice de réfraction fort), (b) Cas où, face au miroir de la configuration (a) on place un miroir de plus faible réflectivité $R \approx 90\%$, en laissant enre eux une couche d'air dont le contrôle de l'épaisseur permet d'obtenir une cavité résonante monomode autour de 690 nm .

Ce diagramme de rayonnement est encore modifié lorsque le dipôle est placé dans une microcavité dont la structure est schématisée sur la figure 5.8(a).

Les miroirs composant cette cavité ont été optimisés en collaboration avec la société LAYERTECH, afin que l'amplitude du champ de l'onde de fluorescence soit maximale au niveau du centre coloré, assimilé dans les simulation à un dipôle orienté parallèlement à la

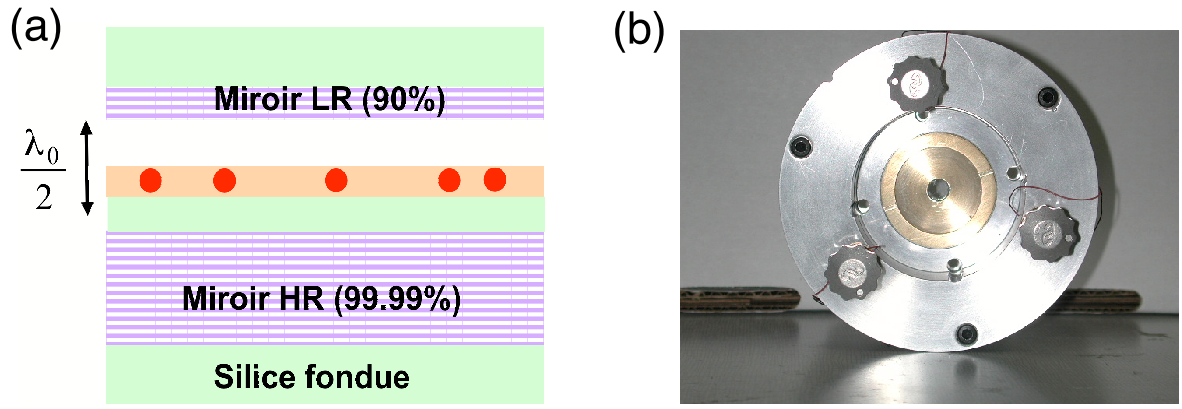

FIG. 5.8 – **(a)** Configuration testée pour étudier les modifications de la fluorescence de centres colorés, représentés par points gris foncés dans une microcavité dissymétrique plane monomode. Les nanocristaux sont déposés sur le miroir de Bragg de haute-réflectivité (HR) identique à celui utilisé dans la fabrication des échantillons décrite au §5.2. Un miroir de plus faible réflectivité est placé parallèlement au miroir (HR) à environ $\lambda_{\text{fluo}}/2$ à l'aide de micro- et nano-positionnement. **(b)** Photographie de la microcavité dont la conception et la fabrication ont été entièrement assurés à l'ENS CACHAN. Les supports de miroirs en laiton, sont amovibles et peuvent être placés sur la partie mobile aussi bien que sur la partie fixe de la cavité. On aperçoit trois vis qui permettent l'ajustement micrométrique ainsi que les fils qui amènent la tension sur les trois cales piézoélectriques permettant d'obtenir un réglage fin de l'épaisseur de la cavité.

surface du miroir[5]. Pour ce faire, nous réutilisons les dépôts de nanocristaux effectués sur le miroir (HR) de réflectivité $R_{\max}$ à 690 nm .

Ce miroir dispose également d'une couche supplémentaire de silice déposée sur sa surface, afin que l'amplitude du champ de la fluorescence soit maximale à une distance d'environ 25 nm au dessus de sa surface, là où se trouvent, en moyenne, les centres colorés dans les nanocristaux. Le second miroir de la microcavité est choisi de plus faible réflectivité $R_2 = 90\%$ (LR), afin de laisser sortir la lumière de fluorescence. Ce miroir est positionné parallèlement au miroir (HR), les deux miroirs étant séparés par un interstice d'air dont nous sommes parvenu à faire diminuer l'épaisseur jusqu'à des valeurs de l'ordre de $\lambda_{\text{fluo}}/2$. Le réglage de la cavité est réalisé à l'aide de trois vis micrométriques et de cales piézoélectriques.

5.3.2 Caractérisation et réglage de l'épaisseur de la cavité

La cavité, dont nous avons dessiné les plans au laboratoire et dont la fabrication a été entièrement assurée par Jean-Pierre MADRANGE, ingénieur mécanicien à l'ENS Cachan, a été utilisée dans une configuration dissymétrique des miroir : un miroir de haute réflectivité ($R_1 = 99.99\%$) faisant face à un miroir de plus faible réflectivité ($R_2 = 90\%$), comme représenté sur la figure 5.8(a).

La cavité est optimisée pour fonctionner « en configuration $\lambda/2$ », c'est-à-dire, avec une

[5]Cette configuration d'orientation est évidemment la plus favorable pour collecter le plus efficacement possible la lumière de fluorescence. Notons cependant que l'orientation des centres colorés NV n'est pas contrôlée, et que d'autre part la lumière de fluorescence d'un centre NV n'est que partiellement polarisée linéairement (au mieux à 80%). Nous pouvons ainsi pense que l'hypothèse d'un comportement dipolaire n'est qu'une approximation assez grossière.

épaisseur d'air entre les miroirs d'environ $690/2 \simeq 350$ nm. L'épaisseur de la cavité est réglable à l'aide de 3 vis micrométriques et nous avons procédé à la caractérisation puis au « réglage » de l'épaisseur de la cavité, en jouant sur ces vis micrométriques, tout en contrôlant le spectre de transmission de la cavité *en lumière blanche*[6].

La figure 5.9 montre les résultats obtenus en faisant varier progressivement la position relative des deux miroirs, tout en ayant le soucis de maintenir leur parallélisme. On observe un spectre caractéristique de transmition de la cavité en fonction de la fréquence optique ν, décrit par une fonction d'Airy :

$$f(\nu) = \frac{I_0}{1 + m * (sin^2(\Pi(\nu - \nu_0)/ISL))} \tag{5.3}$$

Les paramètres importants de cette équations sont :

- L'intensité maximale en transmission I_0.
- Le paramètre m, qui est directement relié à la réflectivité des miroirs (voir par exemple la référence [20]). On montre que dans notre cas, où le miroir HR peut être assimilé à un miroir à réflectivité totale, l'expression de m se simplifie à : $m = 4R_2/(1-R_2)^2$, soit m = 360.
- L'intervalle spectrale libre de la cavité (ISL). Le réglage en « configuration$\lambda/2$ », correspond au cas où $ISL = c/\lambda \simeq 4.3\ 10^{14}$ Hz.

Comme on peut le voir sur les différents spectres présentés sur la figure 5.9, nous sommes capables de contrôler l'épaisseur de la cavité jusqu'à des épaisseurs inférieures à la longueur d'onde, et c'est dans ce régime que nous avons optimisé les réglages de façon à maximiser la lumière collectée. Nous présentons, sur la figure 5.9, une série de 8 spectres, en partant de la configuration où les miroirs sont les plus éloignés (ISL faible), jusqu'à la configuration où leur écartement est inférieur à la longueur d'onde. Un ajustement, basé sur l'équation 5.3 est effectué sur chacune de ces courbes expérimentales et les paramètres de cet ajustement sont indiqués sur le graphique correspondant. On notera tout d'abord que les courbes obtenues à l'aide de la procédure d'ajustement convergent avec précision vers les courbes expérimentales.

Par ailleurs, ces données nous ont permis de mesurer l'évolution de la finesse $\mathcal{F}$ de la cavité, en fonction du réglage. Cette finesse peut être définie à partir du paramètre m par

$$\mathcal{F} \equiv \frac{\Pi}{2}\sqrt{m} \tag{5.4}$$

Ainsi, la finesse théorique de notre cavité est de $\frac{\Pi}{2}\sqrt{360} \simeq 29.8$, ce qui est en bon accord (cf. figure 5.10) avec les mesures que nous avons effectuées. L'accord en finesse théorique et finesse « expérimentale » est d'autant meilleur que la cavité se « referme » c'est à dire que les miroirs se rapprochent et que l'ISL augmente. Ceci est d'ailleurs le régime qui nous intéresse pour l'observation de la fluorescence de centres colorés NV uniques en cavité, la cavité étant optimisée pour fonctionner en « configuration$\lambda/2$ ».

[6]Nous avons également placé des cales piezo-électriques afin de contrôler électriquement l'épaisseur de la cavité, cependant, aux faibles épaisseur de la cavité, les contraintes subies par les cales piezo-électriques sont trop importantes et un réglage manuel, à l'aide des vis micrométriques s'est avéré nécessaire.

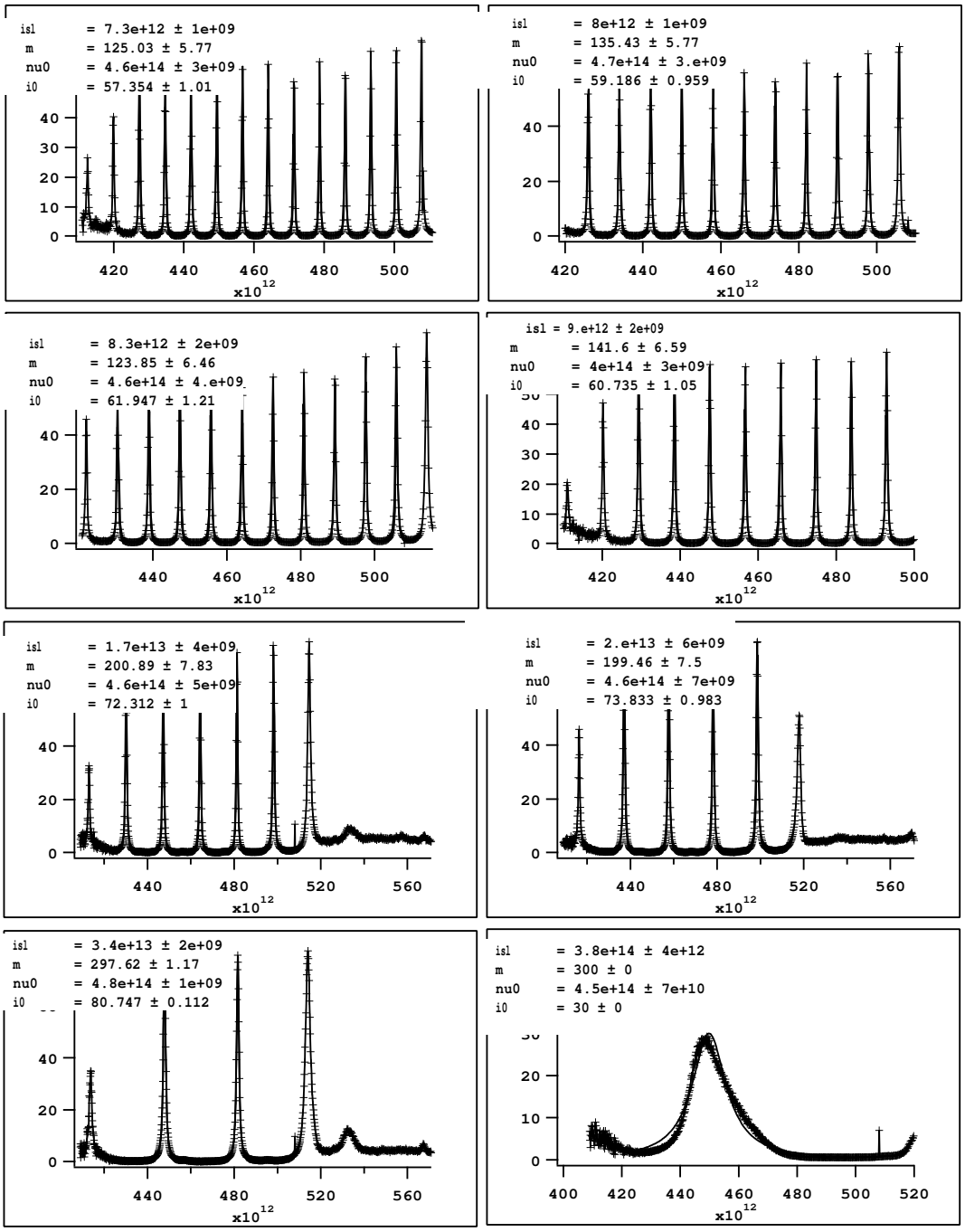

FIG. 5.9 – Spectres de transmition de la cavité planaire, mesurés pour un éclairage normal en lumière blanche. Les différents spectres correspondent à différentes épaisseurs d'air entre les deux miroirs. Chacune de ces courbes est ajustée à partir de l'équation 5.3 et les paramètres de l'ajustement sont portés sur le graphique correspondant. En haut à gauche, le spectre présente de nombreux pics, l'intervalle spectral libre (ISL) est faible car les miroirs sont éloignés d'une distance égale à plusieurs multiples de la longueur d'onde. En bas à droite, l'intervalle spectral libre correspond à un réglage proche de la « configuration $\lambda/2$ ».

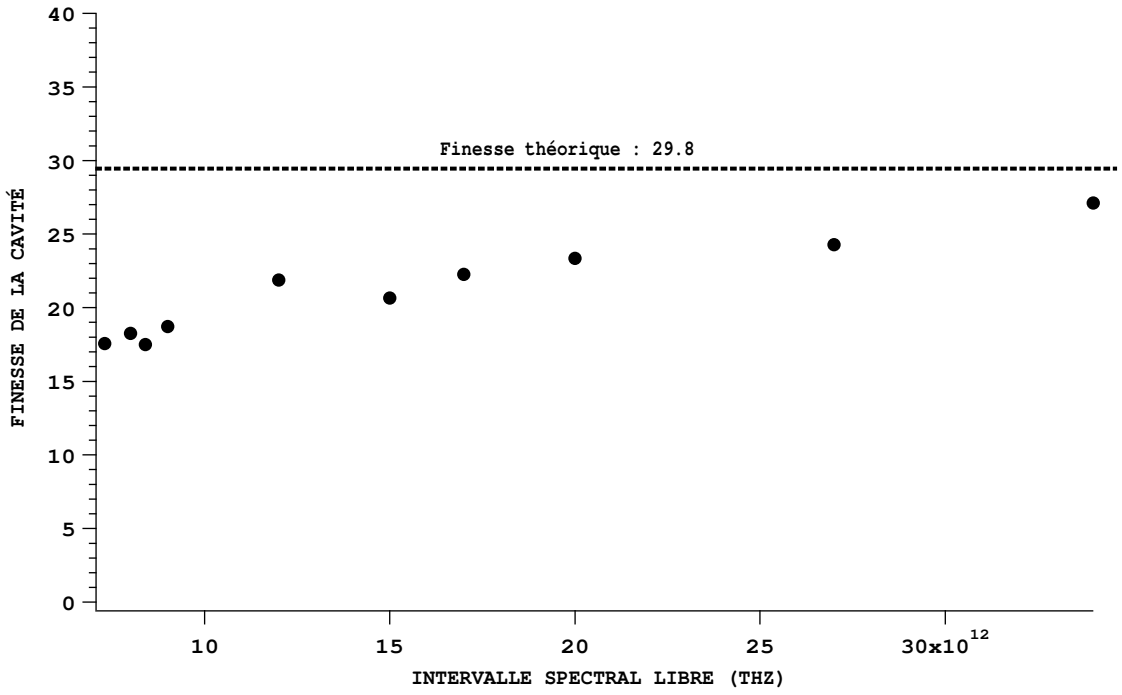

FIG. 5.10 – Evolution de la finesse de la cavité, mesurée à partir des ajustement de la figure 5.9, en fonction de l'intervalle spectral libre (ISL). Les valeurs mesurées sont compatibles avec la finesse théorique, qui est de 29.8.

5.3.3 Affinement spectral de le fluorescence

L'excitation des centres NV est effectuée en focalisant le faisceau continu d'un laser argon à 514.5 nm à travers le miroir (LR)[7]. On utilise pour cela un objectif de microscope de grande distance de travail, permettant de corriger les aberrations optiques induites par la traversée de l'épaisseur du substrat du miroir (LR). La fluorescence d'un centre coloré est ensuite collectée à travers ce même miroir à l'aide du même objectif de microscope.

Afin de réaliser un accord fin de la longueur d'onde de résonance de la cavité autour de la longueur d'onde $\lambda = 690$ nm, où la fluorescence du centre NV est maximale, nous avons tout d'abord enregistré *in situ* le spectre en transmission de la cavité « froide », c'est-à-dire sans émetteur. Compte tenu de l'asymétrie de la cavité, la transmission attendue autour de 690 nm est très faible[8] et nous avons dû accumuler pendant plusieurs minutes les photons détectés sur la matrice CCD du spectrographe, afin d'obtenir le spectre de la figure 5.11(a) dont la largeur totale à mi-hauteur est de l'ordre de 20 nm. Une fois le mode de résonance de la cavité accordé sur la bande spectrale où l'on détecte le plus de photons, qui coïncide avec la zone spectrale autour de 690 nm où se situe le pic d'émission des centres NV, cf. figure 5.2, nous avons cherché une centre NV unique, puis enregistré son spectre de fluorescence dans les mêmes conditions de collection de la lumière que pour la cavité « froide » (fig.5.11(b)). Nous obtenons un spectre disymétrique, ayant une largeur totale à mi-hauteur de 22 nm,

[7] La réflectivité de ce miroir à 514.5 nm vaut environ 30% : il transmet donc convenablement le laser de pompage.

[8] En théorie, compte tenu de la structures des miroirs, ($R_{HR} = 99.9996\%$ et $R_{LR} = 90\%$) la transmission de la cavité est donnée par $4\frac{(1-R_{HR})}{1-R_{LR}}$. Elle vaut ainsi 1.6×10^{-4}.

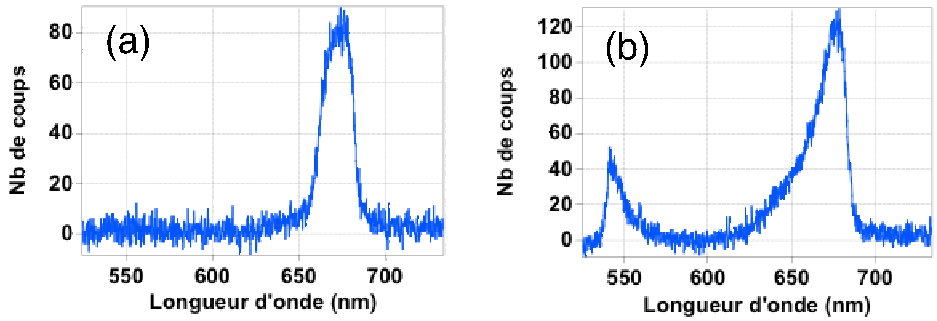

FIG. 5.11 – (a) Spectre en transmission de la microcavité « froide » éclairée en lumière blanche. Ce spectre est obtenu en focalisant dans la cavité un faisceau parallèle de lumière blanche à l'aide d'un autre objectif de microscope de longue distance de travail placé au dessus du miroir « $R_{\max}$ ». La lumière transmise est collectée par l'objectif principal (distance de travail maximale 3.1 mm, $\times 40$, ouverture numérique 0.60) et envoyée vers le spectrographe imageur représenté sur la figure §3.5. Le spectre obtenu a une largeur à mi-hauteur d'environ 20 nm. (b) Spectre de la fluorescence d'un centre NV unique. Le pic autour de 550 nm est un artefact dû au spectrographe (lumière de pompe à 514.5 nm diffusée à l'intérieur du spectrographe) et n'a pas de rapport avec le spectre du centre NV. Ces spectres sont obtenus après une accumulation d'une durée d'intégration de 10 minutes sur la matrice CCD refroidie à -60°C.

comparable à celle du spectre mesuré en transmission pour la cavité « froide ». L'extension vers les basses longueurs d'ondes est attribué à une structure de modes transverses de la cavité planaire. Celle-ci a donc bien pour effet d'affiner le spectre de fluorescence du centre NV, le faisant passer d'une largeur totale à mi-hauteur de l'ordre de 70 nm (fig.5.1(b)) à une valeur d'environ 20 nm.

Nous pouvons également noter que la cavité n'a pas eu un simple effet de filtrage, mais que la fluorescence semble également avoir été exaltée dans la bande de résonance de la microcavité, comme le montre l'augmentation de la densité spectrale de fluorescence observée dans la comparaison entre un centre NV dans un nanocristal déposé sur le miroir de Bragg (fig.5.2) et un centre NV situé dans la microcavité (fig.5.11(b)). Cette densité spectrale est définie comme le nombre de coups comptés par la matrice CCD au maximum du spectre de fluorescence, soit à $\lambda \approx 690$ nm, par unité de longueur d'onde et par unité de temps d'intégration du spectre. Les résultats obtenus sont résumés dans le tableau 5.2.

Configuration	Puissance continue de pompage à 514.5 nm (mW)	taux de comptage (coups/s)	densité spectrale à $\lambda_{\max} = 690$ nm (coup/nm/min)
Sans cavité	11.5	140×10^3	31
Avec cavité	10.2	63×10^3	60

TAB. 5.2 – Tableau récapitulant l'effet de la cavité sur les taux de comptage et les densités spectrales d'intensité. Un gain d'un facteur deux dans la densité spectrale est obtenu grâce à la microcavité. C'est le facteur que l'on gagne sur le nombre de photons collectés en utilisant la cavité au lieu du simple miroir combiné à un filtre interférenciel de même spectre de transmission, placé par exemple devant les détecteurs.

Notons cependant quel'intensité totale de la lumière de fluorescence collectée est par contre réduite d'un facteur 2.2 lorsqu'on utilise la microcavité. Nous pensons qu'il peut exister trois causes à cette réduction :

- La première est géométrique. Malgré l'affinement du diagramme de rayonnement, la fluorescence n'est pas aussi bien collectée par l'objectif de microscope utilisé pour le couplage au mode de sortie la microcavité, qu'elle l'est lorsqu'on utilise l'objectif de grande ouverture numérique placé quasiment au contact du miroir seul.
- La deuxième raison tient à ce que, dans notre expérience, nous ne détectons pas la lumière couplée aux modes guidés dans l'interstice entre les deux miroirs, modes inhérents à la structure planaire de la microcavité. Un confinement transverse de la lumière comme dans les structures de micropilliers semiconductrices [96, 117] résoudrait en grande partie se problème, le prix à payer étant une réalisation technologique plus lourde.
- Enfin, la troisième raison est liée à ce que les transitions entre états vibrationnels du niveau excité et du niveau fondamental sont pour la plupart non résonantes avec la microcavité, dont le spectre est plus étroit que celui de la fluorescence du centre coloré NV. La fluorescence pourrait ainsi être inhibée pour toutes les transitions hors résonance, ayant pour effet de rallonger la durée de vie de l'état excité[9]. Des données préliminaires ont montré que cette dernière était de l'ordre de 35 ns, alors qu'en moyenne sur un miroir, la durée de vie de l'état excité est de l'ordre de 20 ns (cf. fig.5.4). La distribution des durées de vie de centres uniques dans la microcavité doit cependant être étudiée pour obtenir des données plus significatives et affiner cette interprétation

5.3.4 Prolongements

La modélisation réalisée jusqu'à présent des propriétés de la microcavité est fondée sur l'utilisation de matrices de transfert [270]. Elle ne tient pas encore compte de la présence de modes non-propagatifs, ou modes guidés, situés dans l'interstice entre les deux miroirs. Signalons également que ces simulations ont été effectuées pour un rayonnement monochromatique à la longueur d'onde du maximum de fluorescence du centre NV. Afin d'estimer quantitativement la contribution des modes guidés, nous avons simulé la propagation au cours du temps, du champ émis par le dipôle situé dans la cavité. Nous avons utilisé pour cela la méthode des éléments finis, afin de résoudre l'équation de propagation (méthode 2D FDTD = « Finite Difference Time Domain »). Cette simulation préliminaire révèle qu'une proportion non négligeablede la lumière « fuit » effectivement dans les modes guidés.

Le prolongement du travail décrit ici consiste d'une part à prendre en compte l'émission large bande du centre coloré, et d'autre part à introduire l'effet des modes guidés dans la modélisation des spectres, des diagrammes de rayonnement et des durées de vie radiatives du dipôle couplé à la microcavité, pour tenter d'expliquer quantitativement les observations expérimentales.

5.4 Photocréation de centres colorés dans le diamant

Dans l'expérience initialement réalisée dans le groupe de Philippe GRANGIER à l'Institut d'Optique, les centres NV étaient excités à l'aide d'impulsions nanosecondes, dont la durée

[9]Notons que cette explication est envisageable à condition que le couplage de la fluorescence aux modes guidés soit suffisamment faible pour ne pas, à l'inverse, réduire la durée de vie de l'état excité en offrant de nouvelles voies de désexcitation au dipôle excité.

$\tau_p \approx 0.8$ ns, correspond à environ $1/30^e$ de la durée de vie τ_0 de l'état excité du centre NV. Dans le § 3.6.1, nous avons cependant expliqué que l'émission d'un seul photon pour chaque impulsion d'excitation était d'autant mieux garantie que $\tau_0 \gg \tau_p$. Nous avons donc décidé d'étudier la génération de photons uniques par des centres NV lorsque ceux-ci sont excités par les impulsions femtosecondes du laser saphir dopé titane dont nous disposons au LPQM. Cette expérience n'a pas donné les résultats escomptés, mais elle nous a permis de mettre en évidence un phénomène qui a notre connaissance n'avait jamais été observé sur les nanocristaux de diamant : la photocréation dans un nanocristal de nouveaux centres fluorescents à l'émission intermittente, ainsi que la probable photoionisation de centres NV individuels réputés être chargés négativement, en centres NV^0 neutres [90].

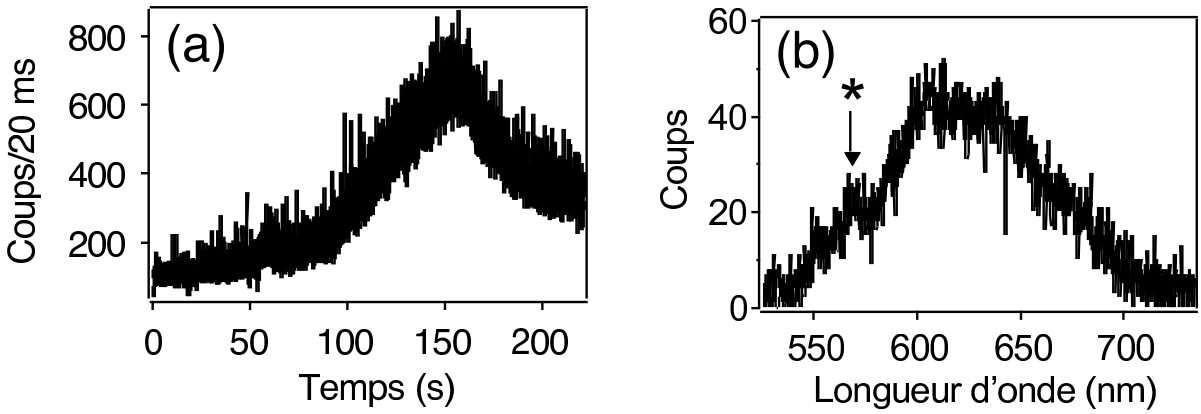

FIG. 5.12 – **(a)** Variation de l'intensité de la fluorescence collectée en fonction du temps, sous illumination laser femtoseconde focalisée sur l'échantillon. Longueur d'onde 500 nm, énergie par impulsion ≈ 55 pJ, fréquence de répétition 8.2 MHz. L'intensité lumineuse au foyer de l'objectif de microscope utilisé pour la focalisation du faisceau d'excitation sur l'échantillon est de l'ordre de 20 GW / cm^2. Le bruit associé à cette acquisition est en grand partie imputable au phénonène d'intermittence. **(b)** Spectre de la fluorescence enregistré par le spectrographe imageur, pendant l'éclairage du nanocristal par le faisceau laser femtoseconde et pour une durée d'intégration de 20 minutes. Le spectre a subi un décalage vers le bleu par rapport à celui du centre NV et il est apparu une raie (marquée de l'étoile) autour de 570 nm, caractéristique de la raie zéro-phonon du centre NV^0 neutre.

Nous avons en effet observé que sous excitation laser femtoseconde à la longueur d'onde de 500 nm, l'intensité de fluorescence provenant d'un nanocristal de diamant contenant initialement un seul centre coloré NV se mettait à croître au bout d'un centaine de secondes, comme cela apparaît sur la figure 5.12(a). La valeur de l'intensité de fluorescence après être montée jusqu'à sept fois celle de départ, se stabilise finalement à environ deux ou trois fois la valeur initiale. Il semble donc qu'à l'issue de l'expérience il y ait un ou deux centres colorés supplémentaires qui fluorescent dans le nanocristal illuminé. Cette hypothèse est corroborée par l'enregistrement de la fonction d'autocorrélation en intensité, dont la profondeur du « trou » autour du retard nul est en accord avec l'émission d'un ou deux centres supplémentaires (cf. figure 5.13) de la réf.[90]). Précisons que la fluorescence provenant de ces centres supplémentaire est en général très intermittente.

Notons qu'en plus de la photo-création de centre colorés, l'illumination laser femtoseconde modifie le spectre de fluorescence, déplaçant le maximum de 680-690 nm à 630 nm comme on peut le voir en comparant les figures 5.2 et 5.12(b). Dans ce dernier spectre, il

apparaît un pic centré sur 570-575 nm, que nous attribuons à la raie zéro-phonon du centre NV^0 neutre. Nous interprétons donc l'évolution de la fluorescence dans le nanocristal contenant initialement un centre NV^- comme, d'une part une ionisation de ce centre en centre NV neutre, et d'autre part l'apparition de nouveaux centres fluorescents, du type NV.

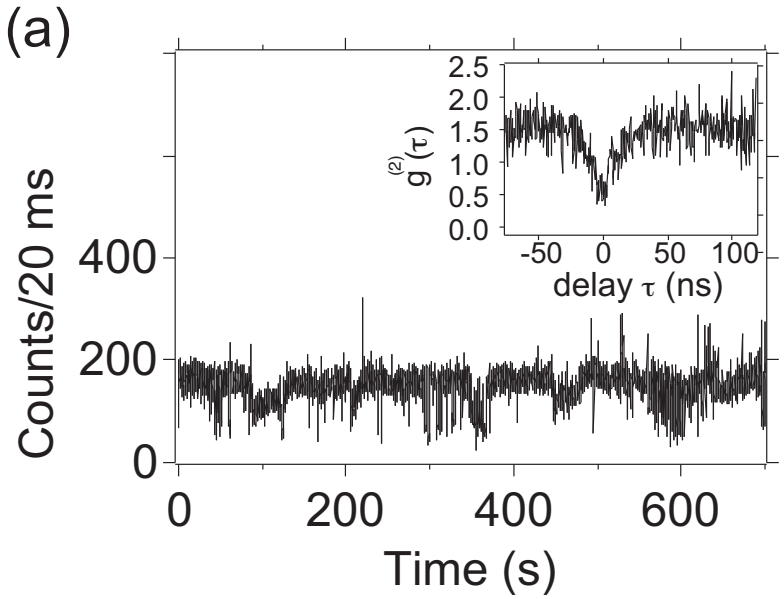

FIG. 5.13 – Enregistrement simultané, en régime d'excitation continue, de l'intensité du signal de fluorescence et de la fonction d'autocorrélation en intensité. Cette acquisition a été effectuée *immédiatement après l'illumination d'un centre unique à l'aide du laser femtoseconde*. Il apparaît clairement que l'intensité de fluorescence est stable dans ce régime d'excitation. En revanche le « creux » de l'ordre de 0.5 dans la courbe de dégroupement indique que l'on est en présence d'un nanocristal contenant deux centres émetteurs, et donc qu'il y a eu création d'un centre durant l'illumination par le laser femtoseconde ?

Interprétation possible du phénomène de photocréation

Nous pensons qu'une augmentation très localisée de la température pendant une durée brève devant les temps caractéristiques de diffusion de la chaleur par conduction ou convection, pourrait être à l'origine de l'apparition de nouveaux centres fluorescents, telle que nous l'avons observé. En effet, une augmentation de température de quelques centaines de degrés peut faire migrer des lacunes au sein des nanocristaux, les rapprochant d'impuretés d'azote et conduisant alors à l'apparition de nouveaux centres colorés fluorescents. Le caractère non photostable des premiers centres ainsi créés (maximum de la courbe 5.12) provient de ce qu'il n'y a pas eu le recuit habituellement réalisé après l'irradiation électronique.

Cette interprétation nous semble être confortée par une autres observation. Nous avons en effet constaté le même phénomène de photocréation de centres colorés avec le laser d'excitation nanoseconde, lorsque l'échantillon, à température ambiante, est placé dans un vide correspondant à une pression inférieure à 10^{-2} mbar. La baisse de pression réduit en

effet le mécanisme de transport de chaleur par convection qui aidait auparavant à dissiper plus rapidement la chaleur produite par les processus non radiatifs mis en jeu dans l'illumination laser du nanocristal. Ces explications requièrent cependant d'autres confirmations expérimentales ainsi qu'une évaluation des facteurs d'échauffement au sein de notre échantillon. Une mesure de l'échauffement local, effectué par la technique photothermique [257] mise au point au CPMOH (Bordeaux) pourrait compléter utilement cette étude.

5.5 Conclusion

Les centres colorés NV du diamant sont des émetteurs fluorescents parfaitement photostables à température ambiante à partir desquels on peut réaliser une source de photon unique stable et efficace [87]. La largeur spectrale relativement importante de l'émission de fluorescence des centres NV, si elle n'est pas compatible avec les applications nécessitant des photons uniques indiscernables, n'est en revanche pas un obstacle à la réalisation d'expériences de distribution quantique de clés, que nous décrirons au chapitre 7. Enfin, nous avons obtenu des résultats préliminaires indiquant que l'on peut réduire la largeur spectrale d'émission des centres colorés NV en couplant leur émission de fluorescence à une microcavité résonnante.

Chapitre 6

Cryptographie quantique : théorie et pratique

Sommaire

6.1 Introduction

Nous avons introduit au chapitre 2 les idées principales sur lesquelles reposent la distribution quantique de clé, en insistant sur les avantages que procure l'utilisation d'une source de photons uniques. Ce chapitre a quant à lui pour objet de définir avec plus de précision les questions ainsi que les résultats théoriques et expérimentaux relatifs à la cryptographie quantique.

Nous débuterons par une description du protocole BB84, qui permet d'introduire l'ensemble des ingrédients techniques en relation avec le partage d'information secrète à l'aide de la cryptographie quantique. Nous décrirons ensuite les différents types de réalisations expérimentales de distribution quantique de clé, avant de conclure par une section consacrée aux preuves de sécurité et aux applications envisagées pour la cryptographie quantique.

Comme nous allons le voir, la cryptographie quantique est est devenue un thème de recherche extrêmement actif au cours de ces dernière années. Devant l'ampleur des sujets

abordés dans ce chapitre, nous tenterons de rester relativement concis, en revoyant le lecteur à la référence [28] pour une revue plus détaillée des principes et des enjeux de la cryptographie quantique.

6.2 Le protocole BB84

Nous avons brièvement retracé au chapitre 2 l'historique de la cryptographie quantique et la génèse du protocole BB84 [175]. C'est ce protocole que nous avons mis en œuvre dans l'expérience de distribution quantique de clé à l'air libre avec une source de photons uniques qui sera décrite dans le chapitre suivant [234]. Nous en exposons ici le principe, en détaillant les différentes étapes permettant d'aboutir à une clé secrète, et expliquons l'intérêt que présente ce protocole pour effectuer des distributions quantiques de clé.

6.2.1 Principe

Le protocole BB84 permet à deux protagonistes, Alice et Bob, de construire ensemble une clé de cryptage connue d'eux seuls. Il repose sur le codage par Alice et la mesure par Bob de la polarisation d'une séquence de photons uniques. Le codage est effectué sur quatre états correspondant aux axes de deux bases perpendiculaires au faisceau : la base droite (Horizontale-Verticale) et la base oblique (45°-135°). Il existe ainsi une ambiguïté sur la base de codage, et les mesures de Bob sont effectuées aléatoirement dans l'une ou l'autre de ces bases. Une alternative à la base oblique est la base de polarisation circulaire (cf fig. 6.1), dont les état propres sont les polarisations circulaires droite (D) et gauche (G).

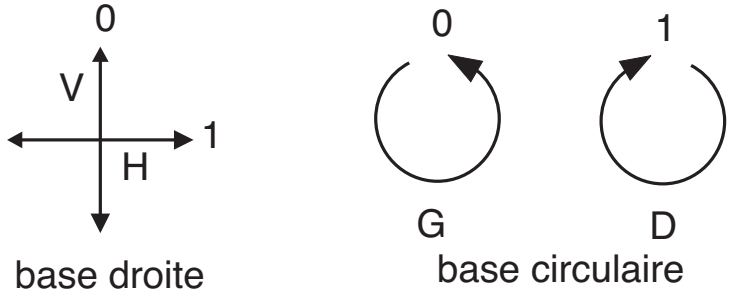

FIG. 6.1 – Bases de polarisation rectilignes et circulaires et bits codés. Ce choix de base, sera utilisé dans l'expérience de cryptographie quantique décrite dans le chapitre suiivant pour la réalisation du protocole BB84.

Comme tous les systèmes de cryptographie quantique, le protocole BB84 repose sur l'utilisation d'un canal quantique utilisé pour partager de l'information entre Alice et Bob ainsi que d'un canal classique (cf section 2.4). Même si l'on est amené à employer le terme de « sécurité inconditionnelle »[1], le cadre de raisonnement de la distribution quantique s'appuie en fait sur plusieurs hypothèses, souvent utilisées de façon implicite :

[1]Ce terme est essentiellement utilisé pour distinguer le type de sécurité offert par la cryptographie quantique de celle offerte par la cryptographie « traditionnelle ». Dans le cas de l'échange de secret entre Alice et Bob, on qualifie d'inconditionnelles les méthodes où l'ignorance d'une tierce partie se démontre directement dans le cadre de la théorie de l'information.

- La capacité de calcul de l'espion, Eve, est supposée illimitée. Eve peut donc « casser » toute primitive cryptographique dont la sécurité repose sur la difficulté d'effectuer certaines opérations mathématiques, comme la factorisation des grands nombres. En revanche, l'espion reste néanmoins contraint par les lois de la physique et ses conséquences comme la théorie quantique de la mesure et le théorème de non-clonage [157].

- Alice et Bob disposent chacun d'un espace sécurisé, inaccessible à l'espion. Ainsi, la source de photons, les détecteurs et les dispositifs de modulation ne peuvent être ni manipulés ni observés par Eve, de même que les mémoires classiques utilisées par ces deux protagonistes.

- Si le canal classique peut être écouté à loisir par Eve, il importe en revanche que l'intégrité des messages échangés entre Alice et Bob par ce biais puisse être garantie. Dans le cas contraire, la distribution quantique de clé deviendrait vulnérable à une attaque de type « man in the middle » couramment considérée en cryptographie classique [240]. Une telle attaque peut consiste à usurper l'identité des utilisateurs légitimes. Ainsi Eve se fait passer pour Bob auprès d'Alice et pour Alice auprès de Bob, partage des clés avec eux et est à même de pirater toute communication entre eux. On peut se prémunir de ce type d'attaque à l'aide d'une authentification « inconditionnelle », toujours à comprendre au sens de la théorie de l'information [248]. Appliquée à la cryptographie quantique, cette authentification permet de garder les mêmes prérogatives de sécurité sur les clés finales. En pratique, il faut disposer d'une petite quantité de bits secrets, initialement partagés par Alice et Bob, afin de réaliser l'authentification [186]. Dès lors, il serait nécessaire, comme le fait d'ailleurs remarquer G. BRASSARD [175], de ne pas parler de *distribution quantique de clé*, mais *d'amplification quantique de clé* qui au final serait inconditionnellement sûre au sens de la théorie de l'information.

Le partage d'une clé secrète suivant le protocole BB84 s'effectue en trois étapes consécutives :

1. Une étape « physique » correspondant à l'envoie par Alice de photons par Alice de photons uniques codés de façon aléatoire sur quatre états de polarisation et sur lesquels Bob effectue une mesure de polarisation dans une base choisie elle aussi aléatoirement. Le principe du protocole BB84 est d'introduire de l'ambiguïté dans le codage des bits, en utilisant deux bases d'états de polarisations, non orthogonales. Cette ambiguïté va rendre impossible l'espionnage du signal quantique sans introduction d'erreurs.

2. L'annonce par Bob des impulsions pour lesquelles il a détecté un photon et du choix de la base de mesure correspondante. Alice répond à son tour en dévoilant les choix de base qu'elle a effectuées pour le codage. Seuls les résultats de mesures effectués quand les bases d'Alice et Bob coïncidaient sont conservés. Cette étape correspond formellement à une phase d' « advantage distillation » [244] : Alice et Bob partageant une information supérieure à celle d'Eve, ils peuvent, à l'aide du canal classique, augmenter la corrélation entre leurs informations au détriment d'Eve.

3. La dernière étape du protocole consiste en un traitement purement numérique des données, conduisant à la distillation d'une clé secrète à partir des informations partagées par Alice et Bob. La construction de la clé s'effectue en deux phases. Elle com-

mence par la phase de correction d'erreurs réalisée au moyen d'une communication bidirectionnelle sur le canal classique. À l'issue de cette étape, Alice et Bob disposent de chaînes de bits identiques, sur lesquelles Eve peut encore posséder une certaine quantité d'information.
La deuxième phase, dite d' « amplification de confidentialité » , permet à Alice et Bob d'extraire de la chaîne de bits une séquence plus courte sur laquelle l'information d'Eve peut être rendue arbitrairement petite. C'est finalement cette séquence de bit qui va constituer la clé secrète partagée par Alice et Bob.

La figure 6.2 illustre ces trois étapes du protocole BB84. Alice commence par tirer une séquence de bits aléatoires, à la cadence de production des photons uniques de la source. Pour chacun de ces bits, Alice effectue un nouveau tirage au hasard qui détermine le choix de la base de polarisation. La polarisation du photon est alors codée dans cette base, en utilisant la convention choisie pour la représentation des bits « 0 » , et « 1 » (cf. figure 6.2). Ce photon est envoyé à Bob sur un canal (fibre optique, air libre ...) que l'on appelle « canal de communication quantique » , puisque l'information est portée par des photons uniques, dont la natures est fondamentalement quantique.

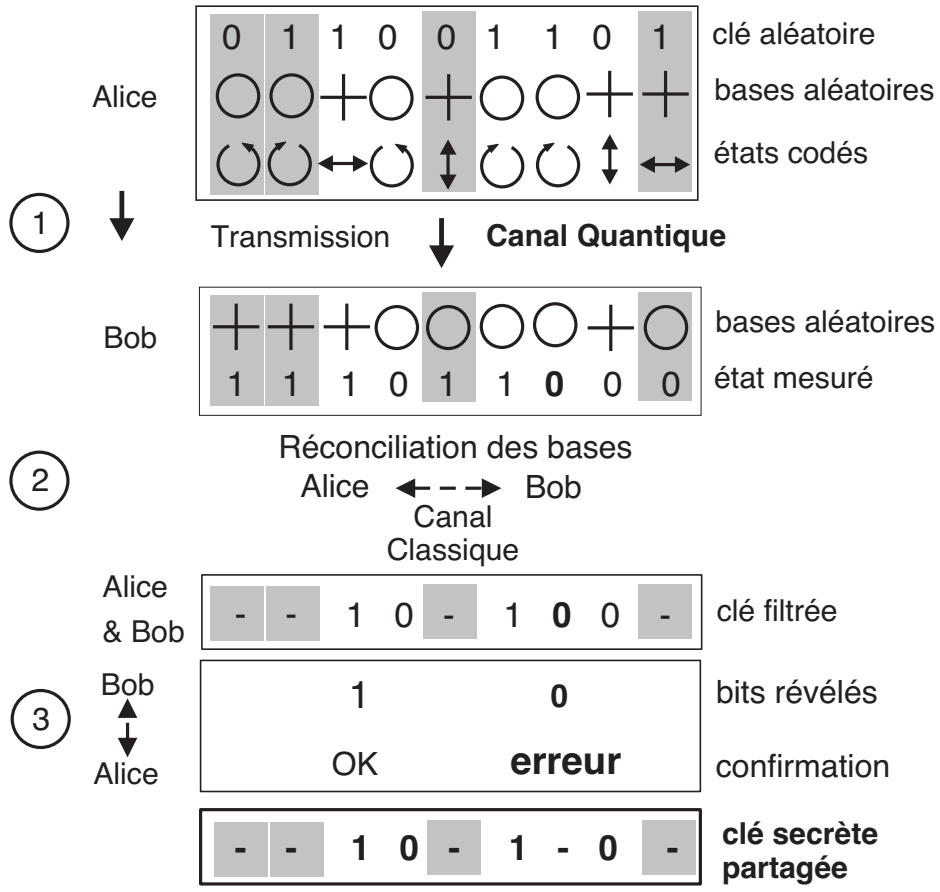

FIG. 6.2 – Résumé des différentes étapes du protocole BB84 conduisant au partage d'une clé secrète entre Alice et Bob.

Pour chaque photon susceptible d'être reçu, Bob choisit aléatoirement la base de mesure. Il obtient ainsi une séquence de bits qui diffère de celle envoyée par Alice pour plusieurs raisons. Tout d'abord, parce que sa base de mesure n'est pas forcément celle utilisée par Alice pour le codage en polarisation du photon, mais aussi parce que sa mesure peut donner un résultat inexact du fait des imperfections des photodétecteurs, d'un mauvais fonctionnement du modulateur utilisé par Alice, d'un espionnage de la ligne de transmission des photons, etc.

En communiquant publiquement leur choix respectifs de base, Alice et Bob excluent dans la deuxième étape tous les bits de la séquence pour lesquels les polarisations des photons n'ont pas été codées et mesurées dans les mêmes bases. Il ne persiste dans cette *clé filtrée* que les erreurs de mesure ou de codage, qu'on ne peut distinguer des erreurs introduites par un espion. C'est par exemple le cas du bit « 0 » signalé en caractère gras dans la figure 6.2. Dans la troisième étape, Alice et Bob corrigent les erreurs avec des algorithmes de la théorie de l'information. Pour ce faire ils doivent d'abord estimer le taux d'erreur dans leur clé en comparant publiquement une fraction de leur séquence respective, qui sera ainsi sacrifiée. Bob annonce son résultat mesure et Alice confirme si c'est bien le bit envoyé. Lorsque le taux d'erreur est de l'ordre de quelques pour cents, les codes correcteurs d'erreur sont efficaces et divulguent peu d'information supplémentaire à Eve, tout en produisant une clé sans erreur chez Bob et Alice. Dans la dernière phase, Alice et Bob réalisent une *amplification de confidentialité*, laquelle réduit encore la taille de la clé mais permet de réduire le niveau d'information acquis par Eve à un niveau arbitrairement faible. Cette phase consiste en l'application d'une fonction appelée « fonction de hachage », choisie aléatoirement puis annoncée publiquement [246]. À la fin de toutes ces opérations, Alice et Bob partagent une clé totalement secrète.

6.2.2 Intérêt du protocole BB84

Le protocole BB84 de distribution quantique de clé est adapté aux communications quantiques où l'information est codée sur des variables discrètes. Il reste aujourd'hui encore le plus utilisé des protocoles de cryptographie quantique. Ce succès s'explique par une combinaison de facteurs qui dépasse la simple renommée héritée de son statut de « précurseur historique ».

Tout d'abord, au point de vue théorique, de nombreux travaux ont permis d'établir la sécurité inconditionnelle de ce protocole [2] [179, 180, 181, 187]. Ces preuves ne sont cependant valables que sous des hypothèses relativement fortes, comme par exemple l'utilisation d'une véritable source de photons uniques. Elles ont été complétées par une étude de la sécurité pouvant être atteinte avec des schémas plus proches des réalisations expérimentales. Moyennant quelques hypothèses supplémentaires, il est possible de prouver, dans un cadre moins général, mais compatible avec les réalisations expérimentales, que BB84 demeure un protocole sûr [183, 186, 185]. Nous discuterons des aspects liés à la sécurité des protocoles de façon plus approfondie dans la section 6.4.

D'un point de vue pratique, le protocole BB84 correspond à un codage des bits quan-

[2] La notion de sécurité inconditionnelle est à comprendre au sens de la théorie de l'information : quelle que soit la stratégie d'attaque choise par Eve, on peut prouver qu'Alice et Bob sont capables, de partager une clé commune sur laquelle l'information d'Eve peut être rendue arbitrairement petite, à condition cependant que la transmission respecte certains critères.

tiques sur un alphabet de 4 états, relativement aisé à mettre en œuvre. [3] Par ailleurs, le protocole BB84 rend quasiment « naturelles » les étapes classiques permettant l'obtention d'une clé à partir des données partagées à l'issue de la communication quantique. C'est en pratique un avantage considérable si on le compare aux protocoles à variables continues qui nécessitent des algorithmes classiques plus sophistiqués [194], mais aussi par rapport à d'autres protocoles à variables discrètes proposés récemment [190] [4].

Par ailleurs, il a été montré [192] que dans le protocole BB84, la nature des corrélations entre les données dont disposent Alice et Bob à l'issue de la communication quantique sont équivalentes aux distributions de probabilité pouvant être obtenues avec des protocoles alternatifs basés sur l'intrication [225]. Ce résultat apporte un éclairage nouveau sur les relations entre communications quantiques et distributions classiques de probabilité, et conforte l'intérêt du protocole BB84 en lui conférant une plus grande généralité.

6.3 Systèmes expérimentaux et sources de photons pour la distribution quantique de clé

Le premier prototype expérimental de cryptographie quantique mettant en œuvre le protocole BB84 fut réalisé en 1989, au IBM J. Watson Research Centre, dans le laboratoire de Charles BENNETT [201]. Les performances de ce système étaient alors modestes, avec un taux de transmission de la clé sûre de 10 bits/s et une distance de 30 cm distance entre Alice et Bob. La première réalisation expérimentale « complète » du protocole BB84 fut effectuée quelques années plus tard, au sein d'une équipe menée par « les pères fondateurs » , Charles BENNETT et Gilles BRASSARD [202].

Comme nous l'avons expliqué au chapitre 2, l'engouement des expérimentateurs pour la cryptographie quantique a fait suite à l'article d'Artur EKERT publié en 1991 [225], proposant de baser la sécurité de la distribution quantique de clé sur l'intrication de paires EPR de photons. Il est ensuite difficile de garder le fil de la chronologie des réalisations expérimentales et de la circulation des idées, tellement les recherches ont été soutenues et les travaux nombreux, débouchant notamment sur le dépôt publication d'un grand nombre de brevets [5] et même la création de start-ups [273, 274].

Nous présenterons ici un rapide panorama des différents systèmes expérimentaux existant actuellement, en renvoyant d'une part à la référence [28] pour une revue détaillée et d'autre part à la récente *Feuille de Route* commandée par l'ARDA [30] [6]. Nous avons classé les expériences en fonction du type de source de photons utilisée : impulsions cohérentes atténuées, paires de photons intriqués, impulsions cohérentes contenant un grand nombre de photons pour les expériences dites de « cryptographie à variable continues », et enfin cryptographie quantique avec une source de photons uniques.

[3] La distance maximale (distance mesurée sur la sphère de Bloch) entre ces 4 états facilite le décodage et rend le codage relativement robuste aux erreurs.

[4] Il convient cependant de modérer cette comparaison, qui ne se veut pas un jugement définitif mais seulement un constat fondé sur l'état de nos connaissances en 2004. En effet, les nouvelles classes de protocoles de cryptographie quantique sont encore jeunes et n'ont pas atteint la maturité de BB84. Elles progressent cependant très rapidement et seront très vraisemblablement porteuses de progrès importants pour la distribution quantique de clé, comme en témoignent ses développements récents [232, 196].

[5] Il y a actuellement plus d'une centaine de brevets relatifs à la cryptographie quantique, dont 10 brevets « mondiaux »

[6] Ce document fournit une comparaison très documentée des différents systèmes de cryptographie quantique ainsi qu'une évocation de leurs perspectives de développement.

6.3.1 Systèmes utilisant une source d'impulsions cohérente atténuée

La façon la plus simple de simuler des impulsions à un photon est bien évidemment d'atténuer la lumière émise par une source laser impulsionnelle. Cette solution, expérimentalement de loin la plus commode si on la compare à la réalisation de sources de photons uniques ou de photons intriqués, a été adoptée dans un grand nombre d'expériences de cryptographie quantique, principalement celles axées sur les aspects « système » et sur le développement industriel.

Comme nous l'avons expliqué au chapitre 2, la distribution $P(n)$ du nombre n de photons dans de telles impulsions classiques obéit à la loi de Poisson :

$$P(n) = \frac{\mu^n}{n!}\mathrm{e}^{-\mu} \tag{6.1}$$

Ainsi, la probabilité d'avoir plus d'un photon par impulsion est données par :

$$P(n \geq 2) = 1 - P(1) - P(2) = 1 - \mathrm{e}^{-\mu}(1+\mu) \tag{6.2}$$

$$\text{soit } P(n \geq 2) \simeq \tfrac{\mu^2}{2} + O(\mu^3) \text{ pour } \mu \ll 1 \tag{6.3}$$

tandis que la probabilité conditionnelle d'avoir plus d'un photon dans les impulsions non vides est :

$$P(n \geq 2 | n > 0) = \frac{1 - P(1) - P(2)}{1 - P(0)} = \frac{1 - \mathrm{e}^{-\mu}(1+\mu)}{1 - \mathrm{e}^{-\mu}} \simeq \frac{\mu}{2} + O(\mu^2) \tag{6.4}$$

Ainsi, dans les cas $\mu = 0.1, 0.2, 1$, les probabilités d'avoir plus d'un photon par impulsion transportant de l'information sont respectivement de 5%, 10% et 58%, c'est-à-dire des valeurs loin d'être négligeables. Le choix de la valeur du paramètre μ relève d'un compromis : des valeurs de μ élevées permettent d'augmenter le débit de la transmission quantique et de diminuer le taux d'erreur et, par la même le recours, aux algorithmes de correction d'erreur. À l'inverse, des valeurs élevées de μ vont permettre à l'espion d'acquérir une grande quantité d'information durant la phase communication quantique, ce qui nécessite de sacrifier beaucoup de bits lors de la phase d'amplification de confidentialité.

Systèmes fonctionnant à l'air libre

Il est possible d'utiliser une ligne de vision directe, en espace libre pour la transmission de photons nécessaire à l'établissement entre Alice et Bob de corrélations de nature quantique . La propagation en espace libre ne pose pas de problèmes majeurs dans la mesure où elle ne perturbe pas ou très peu les degrés de liberté des photons sur lesquels sont codés l'information. C'est notamment le cas pour un codage en polarisation, la biréfringence de l'atmosphère étant suffisamment faible pour ne pas induire de dépolarisation notable pour des distances de transmission de plusieurs dizaines de kilomètres [204]. La propagation dans l'atmosphère se prête par ailleurs particulièrement bien à l'utilisation des longueurs d'onde visibles, et particulièrement de la fenêtre spectrale $750 - 850$ nm, pour lesquelles les photodiodes à avalanche au silicium sont des détecteurs de photons uniques performants.

En revanche, l'un des défis essentiels liés à ce mode de propagation provient de l'influence de l'absorption et de la diffusion dans l'atmosphère, (cf. figure 6.3). Une autre difficulté expérimentale sévère est liée à la suppression de la lumière parasite, particulièrement si les expériences sont envisagées en plein jour.

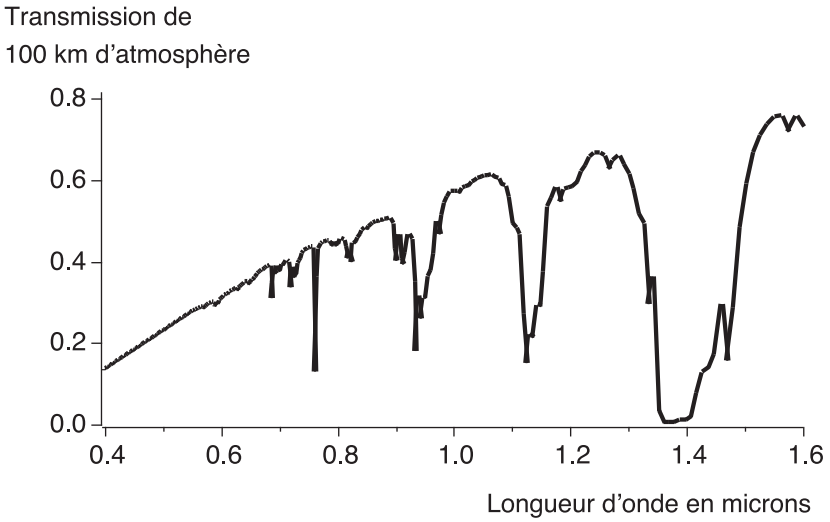

FIG. 6.3 – Transmission de l'atmosphère terrestre sur 100 km (mesurée en pointé vertical), en fonction de la longueur d'onde. On voit apparaître de nettes diminutions dues notamment aux bandes d'absorption de l'eau et des autres composés chimiques présents dans l'atmosphère. Autour de 700 nm, (émission d'un centre coloré NV), l'atténuation est de l'ordre de 4.5 dB pour 100 km.

Enfin, même si les distances théoriques maximales atteignables sont de plusieurs centaines de kilomètres, une des limitation essentielle des systèmes de cryptographie à grande distance réside dans le pointé d'un faisceau de très faible intensité sur plusieurs dizaines de kilomètres. On doit alors compenser l'effet des turbulences atmosphériques, ce qui impose d'établir une rétroaction sur le signal détecté, opération délicate quand il s'agit d'un faisceau de photons uniques [209]. Compte tenu des performances sans cesse améliorées des systèmes d'optique adaptative [272], on peut néanmoins se montrer optimiste quant à la possibilité de surmonter de tels obstacle techniques.

Du point de vue des réalisations expérimentales, le perfectionnement des dispositifs a permis de repousser au fur et à mesure les limites de distance et de conditions de fonctionnement soit diurne, soit nocturne. La première expérience de cryptographie quantique [202] a été réalisée en 1992 à travers environ 30 cm d'air, tandis que la possibilité de réaliser des communications quantiques en espace libre était testée et démontrée la même année [203]. Ensuite, en 1996, une expérience réalisée initialement en optique fibrée fut adaptée pour démontrer la faisabilité de la cryptographie quantique en espace libre, sur une distance d'environ 70 m [205], ouvrant la voie à l'optimisation des performances. Depuis, une série d'expériences ont démontré la possibilité d'échanger des clés sur des distances de plus en plus grandes : de 1.6 km durant la journée en 2000 [206] , la distance a ensuite été portée à 10 km par l'équipe de R. HUGHES à Los Alamos [207]. Le « record » de distance est pour l'instant détenu par une expérience réalisée de nuit entre deux sommets dans les Alpes autrichiennes sur une distance de 23 km [208]. Une telle expérience permet d'envisager la réalisation d'échange de clé quantique entre un satellite et des stations réceptrices placées sur la Terre [209]. Enfin, une expérience récente, réalisée de nuit entre deux bâtiments du NIST à Gaithesburg, distants de moins d'un kilomètre, a démontré la possibilité d'augmenter sensiblement le débit d'échange de clé en utilisant de l'électronique rapide [210].

Systèmes utilisant des impulsions cohérentes atténuées envoyées dans une fibre optique

L'utilisation d'optique fibrée permet d'éviter un certain nombre des problèmes liés à la propagation en espace libre. Ainsi, la propagation sur un réseau de fibres optiques offre un support stable et fiable à la transmission de photons uniques, bénéficiant de l'expérience héritée des télécommunications par voie optique et en particulier de la faible absorption linéique des fibres optiques pour des longueurs d'ondes correspondant aux « fenêtres télécoms »[7].

Envoyer et recevoir de l'information codée sur des impulsions de très faible intensité dans des fibres optiques présente néanmoins des difficultés très spécifiques, et il est impossible de transposer directement le fonctionnement de « l'optique télécom » aux expériences de cryptographie quantique. En particulier, le maintien des propriétés quantiques des photons quasi-uniques impose de n'utiliser que des réseaux fibrés passifs, sans dispositifs d'amplification, qui bien évidemment perturberaient de façon irréversible la communication quantique [157] Nous évoquerons au chapitre 8 les défis expérimentaux associés au développement de la cryptographie quantique à grande distance sur des réseaux fibrés, en détaillant les deux approches expérimentales principales qui sont actuellement poursuivies :

- Le codage en phase sur un dispositif « à un passage », (« One-Way » en anglais) utilisant un interféromètre de MACH-ZEHNDER dont la longueur des bras est stabilisée de manière active [218, 223].
- Le codage en polarisation en utilisant un dispositif « à aller-retour » (« Round-Trip » en anglais) permettant de compenser activement [212] ou de façon automatique [216, 213], le brouillage en polarisation dû aux fluctuations de la biréfringence de la fibre.

6.3.2 Systèmes utilisant des paires de photons intriqués

C'est Artur EKERT qui a le premier suggéré d'utiliser l'intrication comme une ressource pour la distribution quantique de clé. Dans le protocole proposé [225], le partage d'information secrète corrélée entre Alice et Bob résulte des corrélations quantiques portées par des paires de photons intriqués dont l'un est mesuré par Alice et l'autre par Bob (figure 6.4).

Il est possible d'utiliser différents types de degrés de liberté pour produire des paires de photons intriqués, que l'on peut ainsi classer très schématiquement par type :

– Les paires de photons intriqués en polarisation ;
– Les paires de photons intriqués en temps – énergie ;
– Les paires de photons intriqués en impulsion.

Au-delà de ces différentes catégories de paires de photons intriqués, l'expression du vecteur d'état quantique restera formellement le même. En particulier, pour les états à deux photons dits « maximalement intriqués », ceux-ci correspondent aux quatre états de Bell pour lesquels les corrélations entre les résultats de la mesure effectuée par Alice et de celle effectuée par Bob sont maximales [21]. En revanche, l'espionnage de la transmission quantique va se traduire par l'introduction d'erreurs, et donc par un abaissement de ce taux de corrélation [228].

L'un des intérêts de la cryptographie quantique avec des photons intriqués est que ses bases théoriques sont très bien établies. Il a par ailleurs été démontré récemment qu'il existe un lien profond entre le partage quantique de corrélations préalable à la distillation d'une clé secrète, et l'intrication quantique [191, 192].

[7] Les standards actuels pour les fibres optiques produites par l'industrie correspondent à des atténuations inférieures à 0.39 dB/km à 1310 nm et à 0.24 dB/km à 1550 nm (source : ALCATEL).

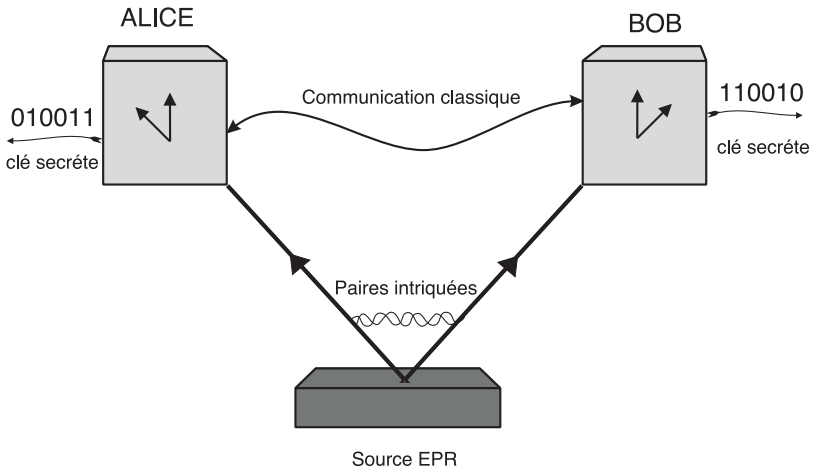

FIG. 6.4 – Représentation schématique d'un système de distribution quantique de clé fondé sur l'usage d'une source de paires de photons intriqués. Alice et Bob mesurent l'arrivée des photons dans l'une des deux bases non orthogonales, comme dans le protocle BB84. Une partie des résultats de mesure permet de vérifier que la source présente bien des corrélations non-locales conduisant à une violation des inégalités de Bell et de s'assurer ainsi de l'absence d'un éventuel espion. Les chaînes des clés brutes obtenues par Alice et par Bob sont utilisées pour obtenir des clés secrètes après les étapes de correction d'erreur et d'amplification de confidentialité.

Par ailleurs, l'un des avantages pratique est que la distribution quantique basée sur l'usage de paires de photons intriqués ne nécessite pas de tirage aléatoire de la base de codage, puisque le caractère aléatoire provient des trajets des photons lors des détections chez Alice et Bob. En revanche, l'une des limitations principales de cette méthode réside actuellement dans la brillance des sources de paires de photons intriqués [8].

Des expériences de cryptographie quantique utilisant des paires de photons intriquées ont été été réalisées en espace libre avec un codage en polarisation [226, 228]. Des paires de photons intriquées en temps – énergie ont également été utilisées pour réaliser des expériences de distribution quantique de clé [227]. On notera que ce type d'intrication est bien adapté à la propagation sur fibre optique. Ainsi, les progrès réalisés au niveau des sources, et en particulier l'amélioration des taux de couplage des faisceaux intriqués produits par fluorescence paramétrique dans un cristal non-linéaire dans des fibres monomodes [258, 264], ont permis de réaliser des expériences sur des distances de plusieurs kilomètres, [229], utilisant des paires de photons intriqués en temps – énergie.

6.3.3 Cryptographie à variables continues avec des impulsions cohérentes

Une nouvelle famille de protocoles et de réalisations expérimentales d'expériences de cryptographie quantique, fondée sur la manipulation de variables quantiques continues, a vu le jour récemment [193, 232]. Pour ces protocoles, l'information est codée sur une modulation de faible amplitude des quadratures du champ d'une impulsion lumineuse cohérente intense, tandis que la mesure de l'une ou l'autre des quadratures de champ est assurée au

[8] Les taux de coïncidence les plus importants mesurés à ce jours sont de l'ordre de 10^7 coïncidences par seconde [258, 265].

moyen d'une détection homodyne impulsionnelle. Les étapes de réconciliation font appel à des algorithmes plus sophistiqués que dans le cas des variables discrètes. Elles reposent sur une méthode de « réconciliation par tranche » [195] tandis que l'un des résultats théoriques majeurs [232] vient de la possibilité de réaliser ces protocoles de manière « inverse » c'est-à-dire en utilisant la clé brute de Bob comme référence secrète et en limitant les communications classiques lors de la réconciliation à des messages envoyés de Bob vers Alice .

L'intérêt majeur de la cryptographie quantique avec des variables continues est qu'elle peut s'effectuer expérimentalement avec des dispositifs (sources de photons, modulateurs, photodétecteurs) efficaces et rapides, ce qui permet d'envisager des débits de transmission importants, bien supérieurs au MHz [232]. En revanche, même si l'utilisation des protocoles inverses de réconciliation permet théoriquement d'envisager la distribution quantique de clé sur une distance arbitrairement grande, les performances des protocoles à variables continues restent sensiblement moins résistantes aux pertes optiques que les protocoles basés sur des variables discrètes. Pour l'instant, les distances maximales d'utilisation envisageables pour de tels systèmes sont d'une quinzaine de kilomètres.

6.3.4 Cryptographie quantique avec des photons uniques

Comme allons le voir dans les deux chapitres qui vont suivre, une partie significative du travail effectué au cours de cette thèse a été consacrée à la réalisation d'expériences de cryptographie quantique avec des sources de photons uniques, ou pour être plus exact, avec des sources d'impulsions lumineuses fortement sub-poissonniennes, l'une étant adaptée à la propagation en espace libre [234] et l'autre à l'utilisation sur un réseau optique fibré [235].

La première démonstration expérimentale d'un dispositif de cryptographie quantique reposant sur une source de photons uniques a été réalisée par A. BEVERATOS *et al.* en 2002 [233], à partir de l'émission de la source décrite au chapitre 5. Par ailleurs, une autre démonstration expérimentale de l'intérêt des sources de photon uniques en cryptographie quantique a été réalisée dans le groupe de Y. YAMAMOTO, à Stanford, en utilisant cette fois l'émission d'une boîte quantique unique en microcavité [106].

6.4 Les preuves de sécurité en cryptographie quantique

6.4.1 Cryptographie quantique et sécurité inconditionnelle

Comme nous l'avons évoqué au chapitre 2, la cryptographie quantique a pour objet le partage d'une clé secrète avec une sécurité dite inconditionnelle, c'est-à-dire en particulier indépendante de la puissance de calcul d'un espion et plus généralement de la technologie dont il dispose ou des stratégies qu'il adopte. On parle plus précisémment de sécurité « inconditionnelle au sens de la théorie de l'information » pour notifier le fait que l'information maximale – définie au sens de la théorie de Shannon [247, 249], – qu'un espion peut obtenir sur la clé finale, peut être rendue arbitrairement faible.

Si le caractère fondamentalement nouveau des tâches cryptographiques rendues possibles par l'échange d'information codée sur des états quantiques individuels est une idée qui a été rapidement acceptée au fur et à mesure que les propositions de Charles BENNETT et Gilles BRASSARD se sont diffusées au sein de la communauté scientifique, [9] il a fallu at-

[9] La citation [13] qui leur est attribuée est à cet égard particulièrement éclairante.

tendre plus d'une dizaine d'années avant que des preuves de la sécurité inconditionnelle du protocole BB84 soient établies [179, 180].

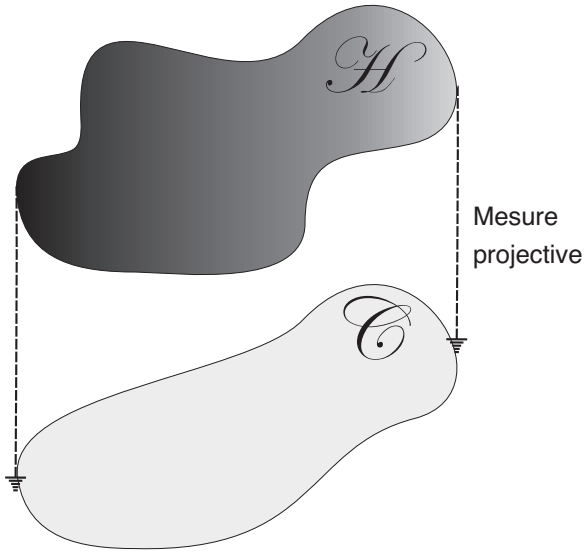

FIG. 6.5 – Représentation schématique de la relation entre le monde quantique, où l'espace des états possibles $\mathcal{H}$ est un espace de Hillbert, et l'espace classique $\mathcal{C}$ qui correspond à l'espace des distributions de probabilités des résultats des mesures, résultats qui sont stockés sous forme classique. La nature projective des mesures effectuées sur les objets quantiques implique que la « taille » de l'espace $\mathcal{C}$ est très inférieure à celle de l'espace $\mathcal{H}$. Dès lors, seules les preuves dérivées dans l'espace $\mathcal{H}$ peuvent revêtir un caractère de généralité.

L'une des raisons qui explique en grande partie l'important laps de temps qui s'est écoulé entre la proposition datant de 1984 [175] et la découverte d'une preuve de sécurité [179], vient précisément de la complexité d'une telle démonstration. En effet, la notion de sécurité inconditionnelle implique que cette sécurité doit pouvoir « couvrir » *l'ensemble* des attaques réalisables par un espion dont les pouvoirs sont uniquement limités par les lois de la physique. En particulier, si l'on considère la transmission de N photons uniques successifs, chacun porteur d'un bit quantique, on se doit de considérer des stratégies d'espionnage « collectives », pour lesquelles on suppose que l'espion Eve intervient directement en réalisant des opérations dans l'espace $\mathcal{H}$ à N bits quantique (cf. figure 6.5). Par opposition, Alice et Bob réalisent des mesures projectives sur des bits quantiques individuels transposant ainsi le problème à une distillation de secret dans l'espace classique $\mathcal{C}$, c'est-à-dire à un problème qui connaît une solution dans le cadre de la théorie de l'information [244]. Ainsi, toute la difficulté de l'élaboration d'une preuve de sécurité inconditionnelles en cryptographie quantique réside dans la nécessité de conserver un caractère de généralité suffisant, lequle peut être uniquement obtenu en se plaçant dans l'espace des N bits quantiques.

La première preuve de sécurité inconditionnelle du protocole BB84 fut annoncée en 1996 par Dominic MAYERS et publiée en 1998. Cette preuve générale reprend les éléments développés par Eli BIHAM et ses collaborateurs [188] concernant la sécurité du protocole BB84 contre une classe d'attaques appelées « collective attacks ». La preuve établie par Dominic MAYERS fait appel à des raisonnement complexes basés sur les propriétés des mesures en physique quantique et garantit la sécurité de l'échange de clé contre l'ensemble des at-

taques autorisées par la mécanique quantique. Il faut cependant noter que cette preuve se limite au cas idéal d'un canal quantique sans bruit et sans erreurs.

Deux ingrédients essentiels ont ensuite permis d'étendre la généralité de cette première preuve : les codes correcteurs d'erreur quantiques [159] ainsi que le « principe de réduction » entre l'espace « quantique » $\mathcal{H}$ et l'espace « classique » $\mathcal{C}$ [178]. Le développement de la théorie des codes correcteurs d'erreur quantiques a en effet fourni des outils permettant de réaliser *directement dans l'espace quantique*, l'étape de correction des erreurs permettant à Alice et à Bob de distiller des paires parfaitement intriquées à partir de paires de photons qui ne sont que partiellement intriquées. Ainsi la preuve de sécurité établie par H. K. LO et H. F. CHAU est fondée sur l'utilisation par Alice et Bob d'ordinateurs quantiques capable de mettre en œuvre des étapes de correction d'erreurs quantiques. Ils ont prouvé qu'il était alors possible de réaliser le partage d'une clé quantique sur un canal bruité de manière réaliste et sur une distance arbitraire. Ils ont également démontré qu'après la phase de correction quantique d'erreurs, on peut applique une « réduction » de l'espace quantique $\mathcal{H}$ vers l'espace $\mathcal{C}$. On peut alors envisager directement dans l'espace classique $\mathcal{C}$ l'ensemble des distributions classiques de résultats associés à n'importe laquelle des stratégies qu'Eve peut adopter. On peut ainsi ramener le problème de l'obtention d'une clé parfaitement secrète à un problème classique, pour lequel il existe des solutions connues [250].

Enfin, les preuves du protocole BB84 ont été simplifiées et approfondies grâce au travail de Peter SHOR et John PRESKILL fondé sur l'utilisation de protocoles de distillation de l'intrication, lequels ne nécessitent pas le recours à un ordinateur quantique [181]. Les codes correcteurs quantiques utilisés dans la distillation de l'intrication sont appelés codes CSS du nom de leurs inventeurs : Robert CALDERBANK, Peter SHOR et Andrew STEANE. C'est au final la performance de ces codes qui fixe le taux d'erreur maximal acceptable, de l'ordre de 11 $\%$ pour lequel on peut garantir une sécurité inconditionnelle de la cryptographie quantique avec le protocole BB84. Plus récemment, un travail complémentaire de Daniel GOTTESMAN et Hoi-Kwong LO a démontré quela garantie de sécurité inconditionnelle du protocole BB84 pouvait être étendue jusqu'à un taux d'erreur de 18.9 $\%$, grâce à l'utilisation de communications classiques bidirectionnelles d'Alice vers Bob et de Bob vers Alice [182].

6.4.2 Sécurité des systèmes réels utilisant le protocole BB84

Même lorsque l'on parle de sécurité inconditionnelle de la cryptographie quantique, il subsiste un certain nombre d'hypothèses implicites. Ainsi, on suppose en particulier que :

- La physique quantique est une bonne théorie [10].
- Alice et Bob disposent d'un environnement parfaitement sécurisé, de sorte que les appareils de codage et de mesure, ainsi que les mémoires classiques utilisées pour le stockage d'informations, sont totalement inaccessibles à un espion.
- La modélisation des systèmes physiques ne comporte par de biais. C'est en fait le point le plus délicat puisque les systèmes physiques vont nécessairement différer des caractéristiques « idéales » que l'on suppose vérifiées pour établir les preuves de sécurités. Citons ainsi la description des impulsions lumineuses comme un paquet d'onde à un photon parfaitement cohérent du point de vue temporel et spatial ou encore l'absence de canaux cachés vers les dispositifs d'Alice ou de Bob [11].

[10] Nous n'avons pas tenté d'aborder ce point dans cette thèse... !

[11] On entend par là des failles de sécurité dues aux imperfections matérielles des systèmes expérimentaux. On peut alors imaginer des attaques, de type « Cheval de Troie » cherchant à tirer partie de ces défauts [237, 238]

Compte tenu de l'écart à l'idéalité des systèmes physiques, il est difficile de transposer rigoureusement les résultats des preuves de sécurité inconditionnelle au cas des réalisations expérimentales. Il existe néanmoins une démarche pragmatique permettant d'évaluer la sécurité des systèmes expérimentaux, et qui rejoint d'une certaine façon la démarche des preuves en cryptographie traditionnelle : définir entièrement certains types d'attaques, jugées dangereuses et réalisables puis démontrer quelles sont les limites induites par ces attaques sur la sécurité du protocole de cryptographie quantique.

On notera qu'un tel raisonnement diffère fondamentalement d'une preuve inconditionnelle, puisqu'il permet seulement *d'exclure* de la « zone sécurisée » certains régimes de fonctionnement pour lesquels la sécurité est défaillante vis-à-vis de certaines attaques. En revanche, en deçà des limites fixées pour les attaques considérées, on ne peut garantir une sécurité inconditionnelle, mais seulement un fonctionnement qui sera en pratique « potentiellement sûr ».

Nous avons représenté sur la figure 6.6, les différents statut associés à la sécurité des systèmes réels de cryptographie quantique : d'abord la sécurité inconditionnelle pour une certaine gamme de paramètres comme par exemple la distance entre Alice et Bob, puis la sécurité potentielle lorsque cette distance augmente et enfin l'absence de sécurité au-delà d'une certaine distance.

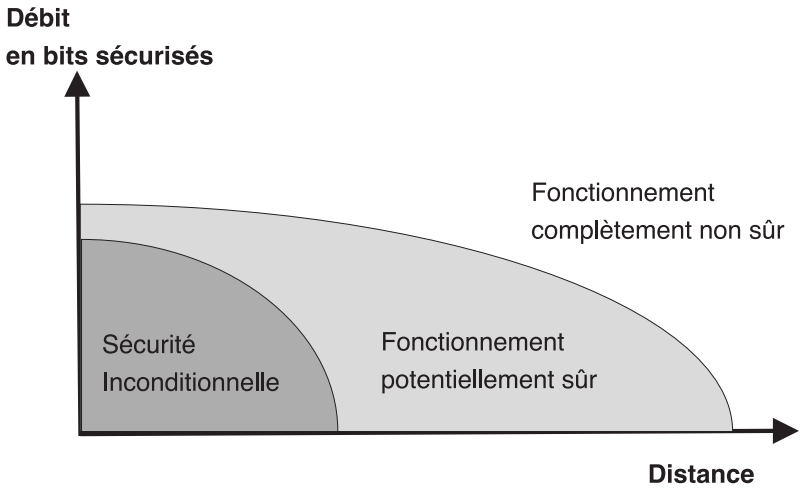

FIG. 6.6 – Les différents régimes de sécurité pour le fonctionnement d'un systèmes réel de distribution quantique de clé. Nous avons choisi la distance entre Alice et Bob comme paramètre de sécurité, avec l'hypothèse implicite que les autres paramètres comme le taux d'erreur ou le nombre moyen de photons par impulsions peuvent être optimisés pour une distance donnée afin de permettre le débit maximal de bits sûrs. Le régime de sécurité inconditionnelle permet de garantir la sécurité des clés indépendamment de toute stratégie d'attaque adoptée par un espion. Le régime de sécurité potentielle correspond au régime pour lequel il n'a pas été exhibé d'attaque suffisamment puissante pour empêcher le partage de clés secrètes. Pour le régime de fonctionnement « complètement non sûr », il existe des attaques rendant impossible l'établissement d'une clé secrète.

6.4.3 Les principales attaques sur le protocole BB84

Nous venons de voir que l'examen des attaques que peut entreprendre un espion sur les systèmes de distribution quantique de clé constitue un élément essentiel dans l'évaluation

de la sécurité du protocole. Nous n'envisagerons ici que deux types d'attaques, renvoyant le lecteur aux références [28, 214, 30] pour des discussions plus détaillées.

Attaque de type « Interception – Renvoi »

Ce type d'attaque correspond à celles qui sont les plus immédiates à mettre en œuvre, et consiste pour Eve, à mesurer indivuellement les impulsions lumineuses émises par Alice, puis à renvoyer vers Bob un photon codé dans l'état correspondant au résultat de mesure qu'elle a obtenu. Il est facile de se convaincre que, dans le cas du protocole BB84, si Eve mesure au hasard dans l'une des deux bases de codage en polarisation, elle a une chance sur quatre d'introduire une erreur, tandis quelle obtient ainsi 75% de l'information codée sur le photon mesuré [214]. Eve peut faire baisser le taux d'erreur qu'elle introduit à seulement 15%, en réalisant des mesures dans la base dite de BREIDBART [177], orientée à 22.5 $^\circ$ par rapport aux bases choisies par Alice et Bob.

Attaque « Photon-Number-Splitting »

L'une des attaques les plus puissanes d'une mise en œuvre expérimentale du protocole BB84 a été imaginée et étudiée par Norbert LÜTKENHAUS [186]. Couramment désignée par l'acronyme d'attaque « PNS », elle a permis de définir ce qui est aujourd'hui considéré comme les limites « pratiques » de la cryptographie quantique avec des impulsions cohérentes atténuées [183].

Cette attaque s'applique à la quasi-totalité des expériences de distribution quantique de clé utilisant des impulsions cohérentes atténuées, qui ne sont, comme nous l'avons rappelé à la section précédente, que des approximations d'états à un photon.

L'existence d'une probabilité résiduelle que deux photons soient présents dans l'impulsion émise par Alice est à l'origine d'une faille de sécurité qui peut être mises à profit par Eve pour obtenir de l'information sans pour autant risquer d'être détectée par Alice ou Bob. La figure 6.7 détaille comment Eve peut procéder pour obtenir *toute* l'information acheminée par les impulsions contenant deux photons ou plus. Ainsi, la sécurité de la transmission n'est plus parfaitement garantie par la seule mesure du taux d'erreur et cette attaque impose à Alice de limiter la probabilité d'impulsions multi-photoniques en contrôlant le paramètre μ correspondant au nombre moyen de photons par impulsion. Comme d'autre part Eve peut exploiter les pertes afin de bloquer les impulsions à un photon [183], on montre qu'Alice doit en pratique diminuer le paramètre μ jusqu'à atteindre la valeur $\mu = T$ où T désigne la transmission en intensité du canal quantique. L'attaque PNS va donc limiter de manière drastique la distance maximale sur laquelle il est possible de réaliser de manière sécurisée la distribution quantique de clé . À titre d'exemple, pour d'excellentes performances expérimentales telles qu'une probabilité de coups d'obscurité par impulsion de 10^{-6} et une efficacité de détection de l'appareil de Bob de 0.1, les pertes maximales que peut supporter le protocole BB84 sont de 20 dB [183]. Un chiffre plus réaliste correspond à une limite des pertes d'environ 13 dB au-delà de laquelle il est en pratique impossible d'assurer la sécurité de la distribution de clé [184].

On comprend dès lors tout l'intérêt d'utiliser des sources de photons réellement uniques pour une mise en œuvre du protocole BB84, puisque ces systèmes ne seront pas affectés par les attaques de type PNS. Les publications de Norbert LÜTKENHAUS [186, 185] donnent à cet égard un cadre théorique complet permettant de comparer les performances de la distri-

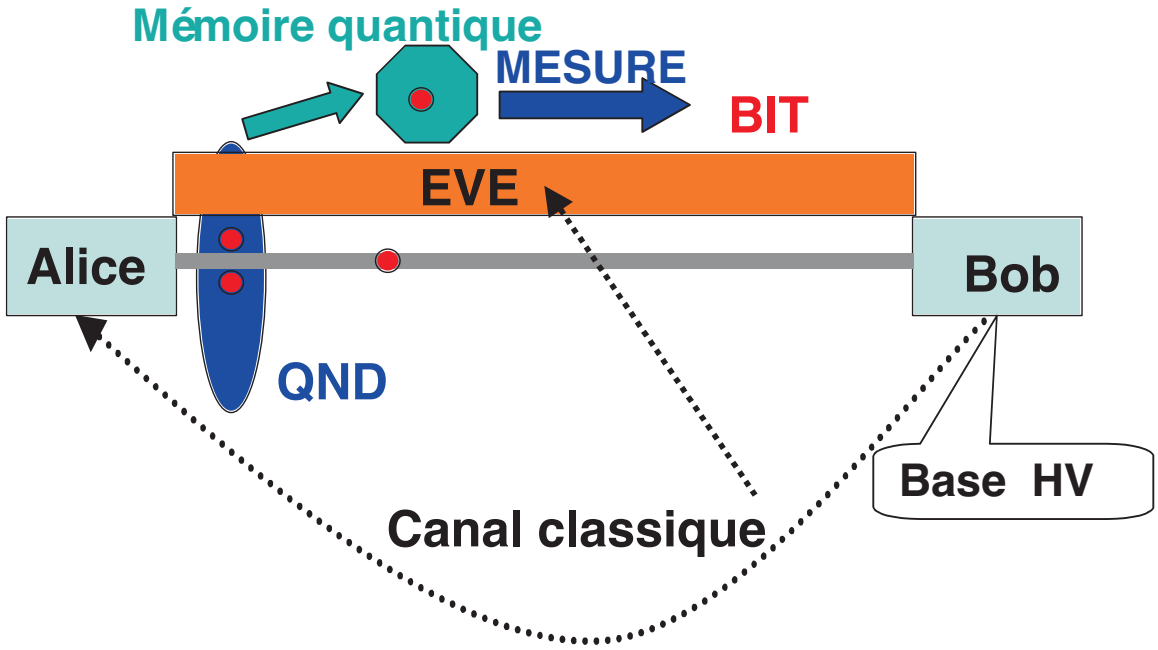

FIG. 6.7 – Principe de l'attaque PNS. Eve réalise une mesure quantique non-destructive (QND) du nombre de photon. Si l'impulsion contient plus d'un photon, Eve en conserve un dans une mémoire quantique et transmet l'autre photon à Bob. Eve attend ensuite que Bob annonce sa base de mesure pour faire la mesure a posteriori, dans la *même* base. De cette façon, Eve peut acquérir, sans introduire aucune erreur, la totalité de l'information contenue sur les impulsions à deux photons. Une telle attaque suppose qu'Eve est capable de réaliser une mesure QND du nombre de photons et qu'elle dispose d'une mémoire quantique. Une telle hypothèse est en pratique très hardie, mais elle est autorisée par la physique quantique [124, 144].

bution quantique de clé en fonction des paramètres expérimentaux, en faisant l'hypothèse que l'espion est limité à des attaques individuelles sur chacune des impulsions, dont l'attaque PNS fait partie. Nous nous sommes basés sur ces travaux pour l'analyse théorique de la sécurité des expériences décrites dans les chapitres 7 et 8. En pratique, les sources de photons uniques que nous avons réalisées sont des sources d'impulsions avec une statistique *sub-poissonnienne* du nombre de photons, pour lesquelles on peut montrer [198], s'appuyant sur les références [186, 185], qu'un important gain de performance est obtenu dans le régime des fortes atténuations.

On mentionnera pour conclure cette section que le groupe de Nicolas GISIN a récemment proposé un nouveau protocole, parfois désigné par l'acronyme « SARG » et qui semble beaucoup plus robuste contre l'attaque PNS [184]. L'idée directrice de ce travail est de modifier la phase classique du protocole BB84, correspondant à l'annonce des bases de codage et de mesure et qui permet d'établir une correspondance entre les résultats de mesure (à savoir quel photodétecteur a produit un « clic ») et la succession des bits dans la clé brute partagée par Alice et Bob. Ils ont montré qu'en établissant une correspondance non pas « impulsion par impulsion » mais en regroupant les impulsions par bloc de deux, on peut imposer que Eve, même en écoutant l'annonce du choix des bases effectué par Bob, soit contrainte de discriminer des états non-orthogonaux. L'efficacité de l'attaque PNS se trouve

alors fortement réduite. Les auteurs estiment pouvoir gagner en pratique 10 dB de pertes à l'aide de tels protocoles, avec des impulsions cohérentes atténuées [184].

6.4.4 Cryptographie quantique contre cryptographie classique ?

Après être née au sein de la communauté des cryptographes, la distribution quantique de clé est devenue un thème de recherche très actif au sein de la communauté de l'optique quantique. Les systèmes expérimentaux et leurs performances ont progressé à grand pas, pour atteindre ces dernières années un stade de développement suffisamment avancé pour motiver des investissements et la naissance de start-ups cherchant à commercialiser des systèmes de cryptographie quantique [273, 274].

L'une des conséquences naturelles du basculement de la cryptographie quantique vers la physique expérimentale est que les aspects cryptographiques à proprement parler qui accompagnent la distribution quantique de clé ont cessé d'être au centre des préoccupations des acteurs du domaine, et qu'en particulier il a persisté un certain flou quant aux potentialités de la distribution quantique de clé en comparaison avec la cryptographie classique traditionnelle. Cette question reste d'ailleurs relativement controversée, les réserves des cryptographes classiques [252] faisant écho aux promesses parfois un peu trop enthousiastes des physiciens.

Il convient tout d'abord d'affirmer clairement qu'il serait erroné de décrire la cryptographie quantique comme « l'avenir de la cryptographie » . Une telle postion relève d'une profonde méconnaissance de cette science, qui intervient aujourd'hui dans une variété considérable d'applications et couvre un champ disciplinaire extrêmement vaste. A l'opposé, il est important de bien comprendre que les potentialités cryptographiques offertes par la mécanique quantique sont de nature fondamentalement différentes de celles dont on dispose avec les méthodes classiques.

En pratique, la cryptographie quantique est en mesure de proposer une méthode de distribution inconditionnelle de clé secrètes. Ces clés peuvent ensuite être utilisées de différentes manières, en reprenant pour cela les méthodes et les techniques établies par les cryptographes classiques.

C. SHANNON [243] a en particulier montré qu'il existe une méthode de codage qui permet de garantir une sécurité inconditionnelle des communications entre deux protagonistes partageant une clé arbitrairement sûre : il s'agit du Code de VERNAM, aussi appelé « One Time Pad » qui impose de disposer d'une clé aléatoire aussi longue que le message et de n'utiliser cette clé qu'une seule fois. Voici le principe de cet algorithme de cryptage :

Pour tranmettre un message binaire (M), Alice et Bob disposent d'une clé secrète aléatoire (K), connue d'eux seuls, et aussi longue que le message. Pour coder le message Alice applique un « Ou Exclusif » $\oplus$ entre le message et la clé $M \oplus K = M_c$. Elle peut maintenant diffuser le message crypté par n'importe quel moyen à sa convenance. Bob de son côté reçoit le message crypté et applique de nouveau un « Ou Exclusif » entre le message crypté et la même clé, ce qui reconstitue le message original $M_c \oplus K = (M \oplus K) \oplus K = M$, puisque $K \oplus K = 0$.

La sécurité absolue de cet algorithme repose sur le fait que la clé secrète est aléatoire et n'est utilisée qu'une seule fois. En effet si un espion intercepte deux messages codés avec la même clé, il est capable de restituer la somme des deux messages originaux en appliquant de nouveau un ou exclusif, cette fois entre les deux messages cryptés :

$$(A \oplus K) \oplus (B \oplus K) = (A \oplus B) \oplus (K \oplus K) = (A \oplus B) \tag{6.5}$$

La distribution quantique de clé est à même de fournir des clés aléatoires dont la sécurité est inconditionnelle, et qui, combinée avec le Code de VERNAM, permet d'obtenir une technique de cryptage inconditionnelle. Néanmoins une telle méthode de cryptage est très « gourmande » puisqu'elle nécessite des clés aussi longues que les messages à protéger.

On peut, dans la pratique, obtenir une excellente sécurité en utilisant les clés distribuée à l'aide de la cryptographie quantique pour mettre en œuvre des techniques de chiffrage symétrique, comme par exemple l'algorithme AES [249]. Cette méthode est la solution la plus couramment retenue pour les applications « commerciales » de la cryptographie quantique [273, 274], et permet d'envisager de chiffrer des flux de plusieurs centaines de Mbits/s. On peut en outre penser que la sécurité ainsi obtenue surpasse encore largement celle des méthodes cryptographiques traditionnellement mise en œuvre [253].

6.5 Conclusion

La cryptographie quantique est un domaine de recherche qui évolue à un rythme très rapide. Au cours des vingt dernières années, les réalisations expérimentales ont évolué du stade d' expériences de démonstration à la mise au point des premiers prototypes et à leur commercialisation [273, 274]. Les bases théoriques en sont par ailleurs maintenant solidement ancrées. Grâce aux preuves de sécurité inconditionnelles [179, 180], il est clairement établi que l'utilisation des ressources quantiques donne accès à des tâches cryptographiques qui sont impossibles à réaliser au moyen de communications classiques.

Les progrès rapides des systèmes expérimentaux et des protocoles permettent d'envisager une progression importante des performances globales de la cryptographie quantique durant les années à venir. À cet égard, la mise au point de sources de photons uniques apparaît comme un enjeu majeur, susceptible de contribuer de façon importante à l'amélioration des dispositifs de cryptographie quantique, tant en terme de débit de transmission qu'au niveau de la sécurité.

Les deux prochains chapitres vont décrire l'application de sources de photons uniques à la mise en œuvre d'une distribution quantique de clé, pour des conditions réalistes de fonctionnement.

Chapitre 7

Cryptographie quantique en espace libre avec une source de photons uniques

Sommaire

7.1 Introduction

Prolongeant le travail d'Alexios BEVERATOS *et al* ayant conduit à la première démonstration de principe d'une distribution quantique de clés de cryptage utilisant une source de photons uniques [233], nous avons entrepris de réaliser à nouveau une telle expérience, mais avec des conditions plus réalistes de fonctionnement. La transmission a eu lieu en espace libre, entre les deux ailes du bâtiment de l'Institut d'Optique (figure 7.1). Alice et Bob correspondaient ainsi à deux entités totalement séparées, reliées entre elles par le canal quantique constitué par une « ligne directe » en espace libre, et un canal classique de connection via Internet. Chez Alice, nous utilisons la source de photons uniques polarisés reposant sur le centre coloré NV, dont le fonctionnement a été décrit au chapitre 5 . L'expérience s'est déroulée de nuit, avec un léger éclairage publique et la lumière diffusée par la Lune.

Par comparaison avec l'expérience décrite dans la référence [233], nous sommes parvenus à réduire le taux d'erreur à $1.7\ \%$ et à diminuer le niveau des pertes optiques chez Alice.

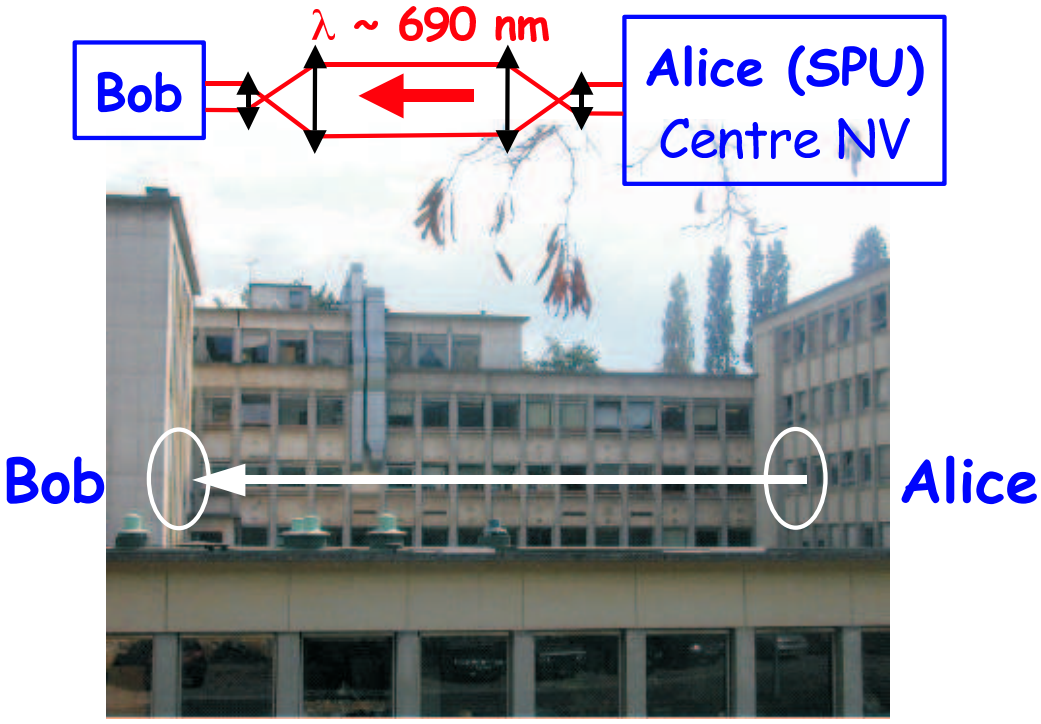

FIG. 7.1 – Disposition relative d'Alice et Bob à l'Institut d'Optique, dans l'expérience, réalisée en octobre 2003, de distribution quantique de clé de cryptage en espace libre. Les deux protagonistes sont séparés par une distance de 30 m.

Nous avons ainsi pu augmenter d'un facteur deux le débit de bits sécurisés. Par ailleurs, nous avons travaillé avec un nombre de photons par session d'échange de clé suffisamment important pour que les algorithmes de correction d'erreur soient proches de leur efficacité optimale. Enfin, nous avons simulé expérimentalement l'accroissement de la distance de transmission entre Alice et Bob en ajoutant des densités neutres sur le canal quantique. Nous avons ainsi pu tester la résistance du système de distribution quantique de clé jusqu'au régime des fortes atténuations.

Nous débuterons ce chapitre par une description du montage et des paramètres expérimentaux utilisés pour les sessions d'échange de clé. La section suivante détaillera comment les résultats bruts, issus de l'étape de « communication quantique », sont exploités pour générer une clé et s'assurer de se sécurité. Enfin, la dernière section est consacrée à l'étude de la sécurité dans le régime des fortes atténuations. Nous montrerons que ce système expérimental, basé sur une source de photons uniques, conduit à des performances quantitativement supérieures à celles obtenues avec des impulsions laser atténuées.

7.2 Montage expérimental

Le montage expérimental comporte deux entités distantes, Alice et Bob, chacune étant située dans l'une des ailes du bâtiment de l'Institut d'Optique (cf. photo figure 7.1).

La figure 7.2 donne une vision synthétique de l'ensemble du dispositif expérimental.

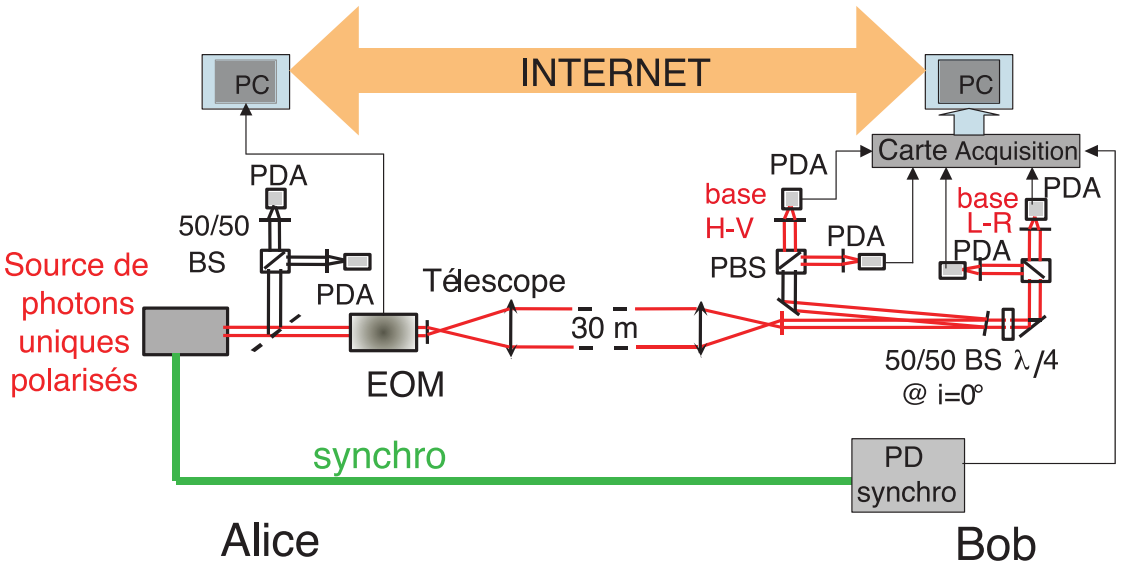

FIG. 7.2 – Schéma du dispositif expérimental permettant la distribution quantique de clés en espace libre entre les deux ailes du batiment de l'Institut d'Optique (cf. figure 7.1).

7.2.1 Alice

Alice détient la source de photons uniques, basée sur l'émission d'un centre coloré NV unique en régime impulsionnel dont le fonctionnement a été décrit au chapitre 5. La configuration expérimentale retenue associe un objectif de microscope métallographique (d'ouverture numérique égale à 0.95) et un échantillon de centres colorés NV déposés sur le miroir de Bragg LAYERTECH dont les caractéristiques sont également données dans le chapitre 5. Il s'agit de la configuration expérimentale qui, de façon pargmatique, a permis d'optimiser l'émission de photons uniques [86].

La chaîne d'excitation laser est celle mise au point par Alexios BEVERATOS durant sa thèse [86]. Elle permet de générer des impulsions vertes à la longueur d'onde de 532 nm, d'une durée de 0.8 ns et répétées à une cadence de 5.3 MHz. Ce taux de répétition permet de s'assurer que les désexcitations successives d'un centre coloré sont suffisamment bien séparées dans le temps.

La lumière collectée par l'objectif de microscope est filtrée spectralement au moyen d'un filtre passe-haut transmettant les longueurs d'onde supérieures à 645 nm, puis spatialement, par focalisation dans un diaphragme de confocalité de diamètre égal à 100 μm. L'émission des centres colorés NV étant seulement partiellement polarisée, on obtient des photons uniques *polarisés rectilignement* en plaçant un cube polarisant sur le trajet du faisceau. Une lame $\lambda/2$ placée en amont du cube polarisant permet de séparer la fluorescence du centre coloré en deux voies, la première correspondant à la transmission vers Bob, et la deuxième étant un dispositif de Hanburry Brown et Twiss permettant de s'assurer de l'unicité du centre émetteur et d'asservir le microscope confocal sur son émission.

Nous avons mis en œuvre une transcription aussi fidèle que possible du protocole BB84, décrit dans la section 6.2, utilisant le codage des photons uniques sur deux bases de polarisation : la base Horizontale Verticale (H - V) et la base circulaire Droite et Gauche (D - V). L'encodage de la polarisation des photons s'effectue au moyen d'un modulateur électro-optique placé chez Alice . Il s'agit d'un modulateur LINOS LM0202, compensé à l'ordre zéro et com-

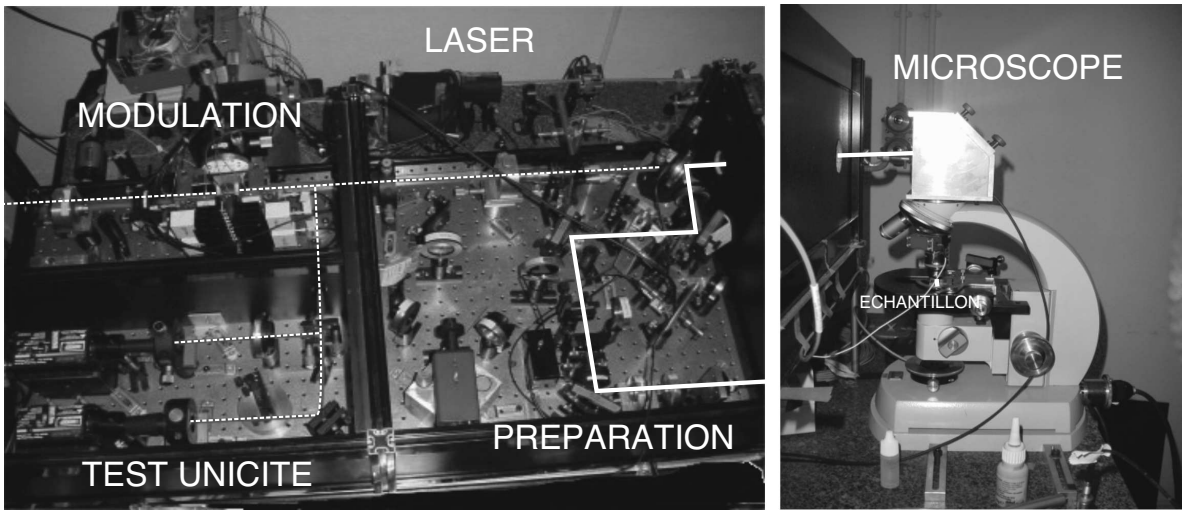

FIG. 7.3 – Photographie du dispositif expérimental utilisé chez Alice.

posé de 4 cristaux de KDP [1]. L'alimentation du modulateur est effectuée au moyen d'une d'électronique de commutation rapide développée par Frédéric MORON et André VILLING, ingénieurs électroniciens à l'Institut d'Optique. Basé sur des composants électroniques de puissance, l'alimentation du modulateur est capable de commuter une tension de l'ordre de 300 V en 30 ns. Les quatre états de polarisations (H - V - L - R) correspondent à quatre valeurs différentes de la tension appliquée au modulateur électro-optique. Deux registres à décalage programmables sont utilisés pour générer deux séquences de bits pseudo-aléatoires crée au moyen de suites de Fibonacci [86]. L'association de 20 portes logiques permet de coder 2^{20} - 1 = 1 048 575 bits et les 4 états du protocole « BB84 » sont générés à l'aide de deux bits, provenant de chacune des séquences pseudo-aléatoires.

Après leur encodage par le modulateur, les photons uniques sont envoyés par la fenêtre de la pièce où se trouve Alice vers celle où est située Bob(cf. figure 7.1). Afin de minimiser les pertes liées à la diffraction, le faisceau est préalablement étendu à l'aide d'un dispositif afocal composé de deux lentilles. Le faisceau qui traverse les 30.5 mètres d'air séparant Alice de Bob a ainsi un diamètre d'environ 2 cm.

7.2.2 Bob

Le dispositif de Bob était situé dans une pièce faisant face à celle où Alice avait été installée, Madame Françoise CHAVEL nous ayant gracieusement autorisé à occuper la partie de son bureau située à côté de la fenêtre durant les quelques mois nécessaires à la réalisation de notre expérience, et à investir les lieux à la nuit tombée...

Les photons transmis sont collectés par Bob, à l'aide d'un dispositif afocal identique à celui placé en sortie du dispositif d' Alice, permettant ainsi de ramener la taille du faisceau à son diamètre d'origine. Le dispositif expérimental associé à Bob, assure la détection, dans une base de polarisation déterminée aléatoirement, des photons uniques encodés par Alice.

[1] Notons que l'utilisation de deux cristaux biréfringents en configuration croisée suffit théoriquement à assurer la compensation du modulateur. Dans le cas du modèle LM0202, l'utilisation de quatre cristaux permet de diminuer de moitié la valeur de la tension demi-onde permettant de basculer de 90° une polarisation rectiligne.

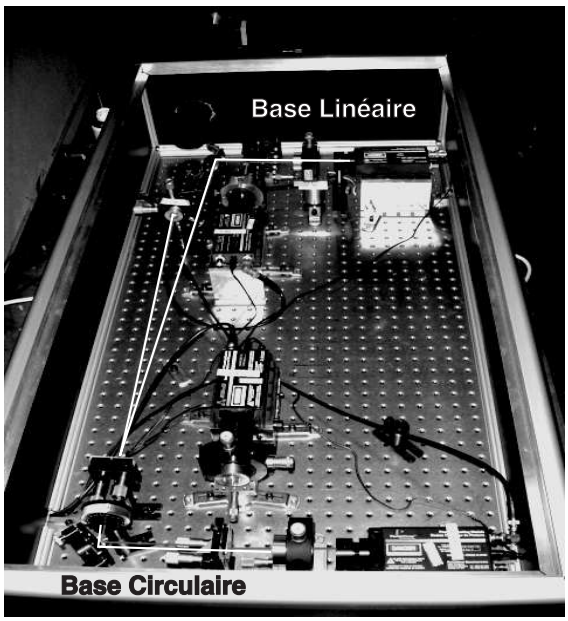

FIG. 7.4 – Photographie du dispositif expérimental utilisé chez Bob.

Bob est constitué de deux blocs d'analyse de polarisation des photons envoyés par Alice, correspondant soit à la base linéaire H-V, soit à la base circulaire G-D (cf. figure 7.2). La sélection entre les deux bases de mesure s'effectue de manière passive. Comme l'a fait remarquer John RARITY à propos de cette configuration, « Dieu joue au dé » : chaque fois qu'un photon unique arrive sur la lame séparatrice 50 / 50 il « choisit » aléatoirement d'être envoyé vers l'une ou l'autre des bases de détection. La lame séparatrice est utilisée en incidence quasi normale, de façon à minimiser la dépendance du coefficient de réflection vis-à-vis de la polarisation du photon incident. Dans la base linéaire H-V, les états de polarisation H et V sont simplement discriminés à l'aide d'un cube polarisant dont chacune des sorties est envoyée en direction d'une photodiode à avalanche. Dans la base de détection G-D des états de polarisation circulaires, une lame quart d'onde achromatique permet de faire basculer les états incidents polarisés circulairement en états polarisés linéairement lesquels peuvent ensuite être discriminés à l'aide d'un cube polarisant puis détectés par deux photodiodes à avalanche. Les photodiodes à avalanche utilisées dans l'expérience sont pour deux d'entre elles des modèles AQR-14, les deux autres étant des modèles AQR-13.

Le résultat de chaque mesure de polarisation, associé à un clic d'une des quatre photodiodes à avalanche chez Bob, est enregistré à l'aide d'une carte numérique d'acquisition rapide (NATIONAL INSTRUMENT, PCI-6534). Afin de supprimer partiellement les clics correspondant à des coups d'obscurité et générés de façon non synchrone avec le train de photons uniques produit par Alice, l'acquisition des données s'effectue en mode « fenêtré », synchronisée avec les tops d'horloge utilisés pour déclencher l'émission des photons uniques chez Alice. Cette synchronisation est réalisée en transmettant d'Alice vers Bob, une fraction des impulsions laser vertes utilisées pour exciter la source de photons uniques. Ces impulsions sont détectées à l'aide d'une photodiode rapide placée chez Bob. Le signal de sortie de la photodiode est remis en forme pour générer une impulsion TTL de durée 30 ns (signal S), cette forme de signal étant adaptée à la carte d'acquisition utilisée pour l'expérience. Par ailleurs, les impulsions correspondant aux clics des photodiodes à avalanche, sont également remises en forme pour produire en sortie des impulsions TTL de durée 60 ns (signal A). Le

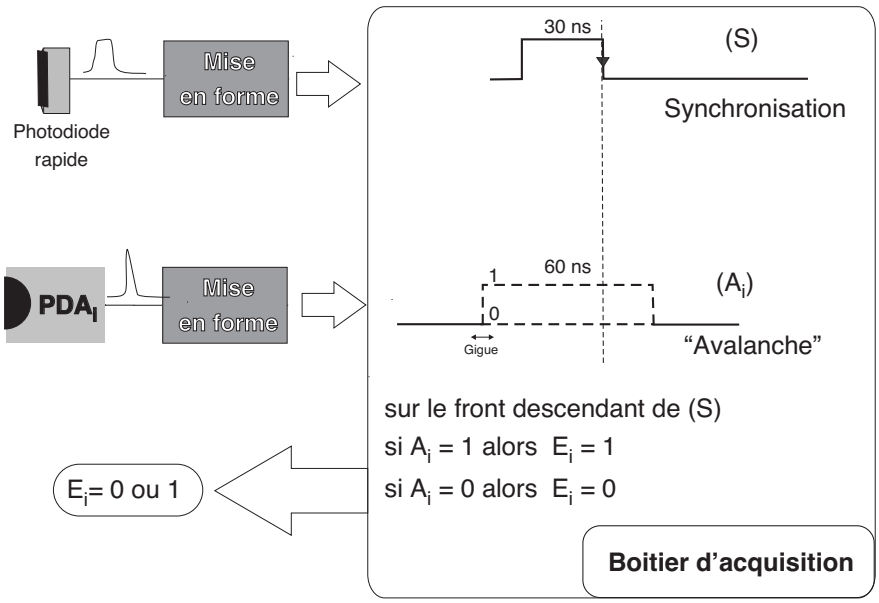

FIG. 7.5 – Schéma détaillant le principe de la mise en forme des signaux de photodétection obtenus chez Bob. Le signal de synchronisation (S) est fourni par une photodiode rapide détectant les impulsions nanosecondes prélevées sur le faisceau d'excitation et envoyées par Alice. Ces impulsions correspondent ainsi à une horloge à 5.3 MHz, cadence d'excitation de la source de photons uniques. Le signal (A_i) de chacune des quatre photodiodes à avalanche (PDA$_i$) placées chez Bob est transformé en une impulsion TTL de durée égale à 60 ns. Le boîtier d'acquisition permet de régler le décalage temporel relatif de ces deux signaux et d'assurer ainsi une détection « fenêtrée » des clics des photodiodes à avalanche. Chacune des sorties du boîtier d'acquition fournit les signaux E$_i$ pour $i = 1, ..., 4$, lesquels sont ensuite envoyés à une carte d'acquisition « TIA » à quatre voies d'entrées, placée dans un micro-ordinateur (cf. figure 7.2).

schéma électronique adopté, décrit sur la figure figure 7.5, permet d'éliminer les fluctuations sur la durée des impulsions générées par les photodiodes à avalanche [2]. Pour chacune des quatres voies de détection, la carte d'acquisition est programmée pour lire l'état du signal A_i, à chaque front descendant du signal de synchronisation S. En jouant sur le retard électronique du signal A_i vis à vis du signal S, nous assurons ainsi un fenêtrage temporel d'une largeur de 60 ns pour la détection des photons uniques.

Chaque session d'échange de clé aboutit chez Bob à une suite de résultats de mesure d'états de polarisation, c'est-à-dire à la clé brute (cf. section 6.2 pour le détail des étapes du protocole BB84). Il s'agit de la « phase de communication quantique » dont la durée totale est de 0.2 s. Les étapes suivantes du protocole BB84 vont être purement classiques. Il s'agit en effet de tirer avantage des corrélations existant entre les données correspondant à la clé brute de Bob et celles d'Alice, afin de distiller une clé secrète connue uniquement d'Alice et de Bob. Comme nous le détaillerons dans la section 7.4, l'ensemble de ces opérations a été réalisée sous la forme de communications bidirectionnelles classiques, effectuées par échange de paquets IP sur le réseau Internet de l'Institut d'Optique, au moyen du logiciel

[2] Ces fluctuations sont essentiellement dues à la gigue de 700 ps associée au signal de sortie des photodiodes à avalanche au silicium.

libre QUCRYPT développé par Louis SALVAIL à l'Université d' Aahrus (Danemark) [214].

7.3 Paramètres expérimentaux pour les échanges de clé

L'objectif principal de l'expérience que nous avons réalisée était d'effectuer une démonstration en conditions réelles de la distribution quantique de clé en espace libre avec la source de photons uniques correspondant à l'émission du centre coloré NV. Les acquisitions expérimentales ont été effectuées à la fin de l'été 2003, entre le mois d'août et le mois d'octobre. Elles ont été réalisées de nuit afin de maintenir le niveau de lumière parasite – dans notre cas la Lune et l'éclairage public – à un niveau suffisamment bas. Notons en effet que le système de photodétection est adapté au spectre d'émission relativement large (environ 70 nm de largeur totale à mi-hauteur) des centres colorés NV, et n'est par conséquent pas adapté à un fonctionnement diurne, nécessitant une grande sélectivité spectrale [207].

La source de photons uniques basée sur la fluorescence d'un centre coloré NV unique a fait la preuve, dans ce cadre, de sa stabilité et de sa fiabilité. En particulier, nous avons été en mesure de poursuivre les acquisitions relatives à un même centre émetteur durant plusieurs jours d'affilée, sans noter une quelconque modification de son comportement radiatif. Pour des raisons de cohérence, toutes les données présentées dans ce chapitre ont été enregistrées durant la même soirée et sont relatives à l'émission du même centre coloré NV.

7.3.1 Performance de la source de photons uniques

Le repérage et les tests préliminaires liés à la statistique d'un centre émetteur sont effectués du côté d'Alice. En effet, l'un des préalables à la réalisation de sessions d'échange de clé est de disposer d'un centre émetteur qui possède des propriétés satisfaisantes, c'est-à-dire :

- Une efficacité d'émission élevée ;
- Une forte réduction de la probabilité d'émission multi-photonique par rapport à une référence poissonnienne.

Ainsi, ces deux paramètres sont dans un premier temps évalués directement à partir d'expériences de mesure d'autocorrélation en intensité, qui permettent d'évaluer simultanément le taux d'émission de la source ainsi que la qualité du dégroupement de photons, comme nous l'avons expliqué au chapitre 5. Cependant, afin de caractériser au mieux la distribution statistique des photons réellement détectée par Bob, nous avons décidé de la déterminer de façon directe à partir de l'enregistrement des instants de photodétection intervenant chez Bob. Cette approche est en tout point similaire à celle adoptée dans le travail décrit au chapitre 4, en tirant profit de l'électronique d'acquisition mise en place chez Bob.

Commençons tout d'abord par les données relatives à l'efficacité d'émission de la source de photons uniques, lesquelles sont enregistrées directement à partir des taux de comptage au niveau des deux photodiodes placées chez Alice. Ainsi, pendant une séquence d'acquisiton de 0.2 s, durant laquelle la cadence d'excitation de la source est de 5.3 MHz, un total de 8.8×10^4 événements ont été détectés. Si l'on corrige ces données en supposant que l'efficacité de détection des photodiodes à avalanche est $\eta_{\mathrm{APD}} = 0.6$ (cf. figure 3.7), on obtient alors une évaluation de l'efficacité globale de l'émission photons polarisés, d'environ $\approx 2.8\%$. Par ailleurs, afin d'être à même de détailler l'origine des pertes optiques dans le montage, nous avons mesuré la transmission optique de l'ensemble de la chaîne optique allant d'Alice à Bob à l'aide d'un laser HeNe et d'un mesureur de puissance calibré. Ces données permettent

d'évaluer l'efficacité globale de la source de photons uniques placée chez Alice, qui constitue un paramètre capital pour l'évaluation de la sécurité des échanges de clés. Ainsi, après l'encodage en polarisation effectué par passage à travers le modulateur électro-optique de transmission $T_{\mathrm{EOM}} = 0.90$ et la traversée des optiques du dispositif confocal de transmission $T_{\mathrm{afocal}} = 0.94$, le nombre moyen de photons polarisés envoyés sur le canal quantique à chaque impulsion est $\mu = 0.0235$.

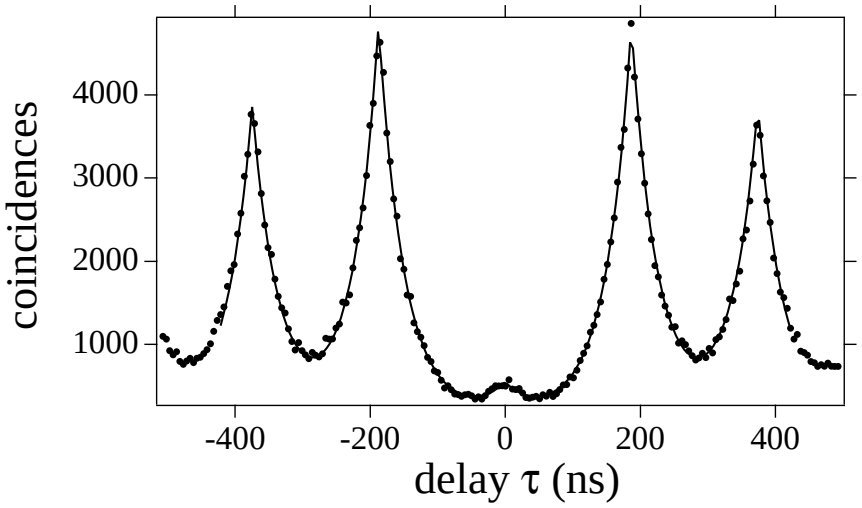

FIG. 7.6 – Histogramme des intervalles de temps entre deux photodétections consécutives enregistrées au niveau d'Alice à l'aide du dispositif de mesure des corrélations d'intensité, de type HANBURY BROWN ET TWISS. Le temps d'intégration est de 175 s. La courbe en trait plein correspond à un ajustement des données expérimentales par un de décroissance exponentiel de chacun des pics, modèle prenant en compte le bruit de fond. Cet ajustement permet d'évaluer à 35 ns la durée de vie radiative du centre coloré NV utilisé. La forte réduction du nombre de coïncidences au voisinage du délai nul est signature du fait que ce centre coloré NV est bien un émetteur individuel qui produit des photons uniques.

La figure 7.6 fait clairement apparaître le fait que le taux d'émission multiphotonique de la source est très inférieur à celui d'une source cohérente atténuée de même efficacité d'émission. Comme nous l'avons expliqué au chapitre 5, le calcul de l'aire normalisée du pic de la fonction d'autocorrélation autour du délai nul constitue une mesure du taux de réduction des impulsions multiphotoniques par rapport à une distribution de Poisson du nombre de photons par impulsion. La statistique de la source peut être caractérisée de façon plus complète en mesurant directement la distribution de probabilité des clics intervenant sur les quatre photodiodes à avalanche placées chez Bob, pour des fenêtres d'acquisition de 60 ns (cf. § 7.2). Une telle mesure présente l'avantage de constituer simultanément une calibration du paramètre $\mathcal{R}$, de réduction de l'émission multiphotonique, qui joue un rôle direct dans les performances du système de distribution quantique de clé. Nous avons pour cela rassemblé les données correspondant à environ 4×10^7 impulsions, pour lesquelles le nombre de photodétections associées a été enregistré à l'aide de la carte d'acquisition placée chez Bob. Ainsi, les probabilités de détecter respectivement un photon ou deux photons, par fenêtre d'acquisition, sont respectivement de : $P_d(1) = 7.6 \times 10^{-3}$ et $P_d(2) = 2.7 \times 10^{-6}$.

Ces chiffres nous permettent d' évaluer le facteur $\mathcal{R}$ de réduction du taux d'impulsions contenant plus d'un photon vis à vis de ce que serait ce taux pour une source cohérente

atténuée équivalente [88]. Il convient cependant de prendre en compte à l'influence du temps mort des photodiodes à avalanche sur cette mesure, comme nous l'avons expliqué au chapitre 4. A partir d'un raisonnement élémentaire de probabilités, on montre en effet que pour la configuration particulière adoptée dans notre expérience, la probabilité $P_d(2)$ de détecter deux photons de polarisation identique est affectée d'un facteur $5/8$ par rapport à la probabilité que deux photons soient incidents sur le système de photodétection [3]. Par conséquent, le facteur $\mathcal{R}$ mesurant la probabilité de réduction de l'émission multiphotonique vaut :

$$\mathcal{R} = \frac{5}{8} \times \frac{P_d(1)^2/2}{P_d(2)} \, . \tag{7.1}$$

soit une valeur $\mathcal{R} = 6.7$ pour le centre coloré étudié. Ce résultat est en bon accord avec la valeur de $\mathcal{R} = 6.1$ obtenue à partir de l'aire normalisée du pic central de la figure 7.6, en tenant compte de la durée de vie de l'émetteur et en prenant une durée de 60 ns comme valeur de la base d'intégration [87]. Lors de l'analyse de la sécurité présentée à la fin de ce chapitre, nous utiliserons la valeur $\mathcal{R} = 6.7$ comme taux de réduction des impulsions multi-photoniques, car cette valeur est directement déduite de l'enregistrement des clics de photodétections sur le montage expérimental.

Nous nous sommes placés dans le cadre d'un modèle de sécurité inconditionnelle contre les « attaques individuelles » [185], dont nous avons évoqué les hypothèses et le domaine de validité au chapitre précédent. Ce modèle implique en particulier que l'attaque optimale est de type « Photon Number Splitting », laquelle permet à un espion de déterminer entièrement le bit d'information porté par les impulsions à plus d'un photons. Ainsi, la probabilité $S^{(\mathrm{m})}$ d'émission d'une impulsion contenant plus d'un photon, est un paramètre qui influe de façon significative sur la performance du système de cryptographie quantique en terme de taux de bits sûr finalement partagés par Alice et Bob. Nous pouvons calculer ce paramètre pour notre source, ainsi que pour une source poissonnienne ayant le même nombre moyen de photons par impulsion, et quantifier ainsi la quantité d'information potentiellement cédée à un espion par le seul fait de la présence de ces impulsions. Dans le cadre de la source de photons uniques utilisée pour l'expérience, nous avons ainsi :

$$S^{(\mathrm{m})}_{\mathrm{SPS}} = \frac{1}{6.7} \times \left[1 - (1+\mu)\mathrm{e}^{-\mu}\right] = 4.1 \times 10^{-5} \, . \tag{7.2}$$

compte tenu de la valeur $\mu = 0.0235$ du nombre moyen de photons par impulsion, déterminée au début de cette section.

Notons que dans le cas d'impulsions cohérentes de même nombre moyen de photons par impulsion, on aurait :

$$S^{(\mathrm{m})}_{\mathrm{WCP}} = 1 - (1+\mu)\mathrm{e}^{-\mu} = 2.7 \times 10^{-4} \tag{7.3}$$

7.3.2 Paramètres expérimentaux du système de détection de Bob

Nous pouvons calculer, à partir des valeurs mesurées de $P_d(1)$ et de $P_d(2)$, la probabilité $p_{\mathrm{exp}} \simeq 7.6 \times 10^{-3}$ correspondant à la probabilité moyenne d'enregistrer un clic de photodétection sur l'un des détecteurs de Bob durant une fenêtre d'acquisition de 60 ns.

Si l'on fait l'hypothèse – a priori fort raisonnable – que le facteur d'absorption lié à la traversée des 30 m d'air qui sépare Alice de Bob est négligeable, la valeur de p_{exp} nous permet d'évaluer l'efficacité globale η_{Bob} associée au système de détection de Bob puisque

[3] Ceci vient du fait que la probabilité que ces photons aboutissent au même détecteur et ne provoquent donc qu'un seul clic est de $3/8$.

celle-ci doit vérifier $\eta_{\mathrm{Bob}} \times T_{\mathrm{air}} \times \mu = p_{\mathrm{exp}}$. Pour notre expérience, où $\mu = 0.0235$ et $T_{air} \simeq 1$, nous avons ainsi $\eta_{\mathrm{Bob}} \simeq 0.3$.

Les coups d'obscurité des photodiodes à avalanche ainsi que les photodétections provoquées par la lumière parasite sont en partie responsables des erreurs de détection au niveau de Bob. De façon plus générale, le niveau de bruit et les erreurs associés au système de photodétection contribuent à fixer les limites de performance d'un système expérimental de distribution quantique de clé, et vont contribuer de façon significative au taux d'erreur dans le cas où le signal est soumis à une atténuation importante sur le canal quantique. Ainsi, nous avons veillé à isoler le mieux possible les photodiodes avalanches de toute lumière parasite, en plaçant pour cela Bob dans un caisson noir dont on a refermé le couvercle et isolé les éventuelles fuites à l'aide de chiffon noir avant chacune des acquisitions (cf. photographie de la figure 7.4). Par ailleurs, au-delà de ces protections contre la lumière parasite, des filtres spectraux sont placés chez Bob afin de « couper » les longueurs d'onde inférieures à 580 nm. On notera que l'on ne peut cependant pas placer des filtres spectraux étroits dans notre montage car ceux-ci ne seraient pas adaptés au spectre d'émission des centres colorés NV. C'est en particulier la raison pour laquelle ce système de distribution de clés quantiques n'a pu fonctionner en plein jour, la lumière venant du soleil constituant alors un signal parasite trop important. Nous avons mesuré les taux de coups d'obscurité des quatre photodiodes à avalanche placées chez Bob, dans des conditions expérimentales identiques à celles des sessions d'échange de clés. On peut désigner chacune des photodiodes par la base de mesure à laquelle elle correspond : Horizontale (H), Verticale (V), circulaire Gauche (G) et circulaire Droite (D). Les niveaux correspondants des coups d'obscurité mesurés sont notés (d_H, d_V, d_G, d_D) et valent respectivement (60,70, 350, 150) s^{-1} [4].

Compte tenu des valeurs des paramètres expérimentaux (fenêtre temporelle de 60 ns, durée de vie du centre coloré de 35 ns, péridoe de répétition des impulsions de de 188 ns) nous pouvons évaluer que 82% des photons émis par la source de photons uniques le seront dans la fenêtre temporelle de photodétection, contre seulement 32% des coups d'obscurité des photodétecteurs. Le fenêtrage temporel permet ainsi d'améliorer sensiblement le rapport signal à bruit et relève d'un compromis entre la part de signal que l'on doit sacrifier et la diminution des contributions des coups d'obscurité. Nous pouvons enfin calculer la probabilité globale p_{dark} d'observer un coup d'obscurité durant une fenêtre de détection de 60 ns : $p_{\mathrm{dark}} = 3.8 \times 10^{-5}$ s^{-1}. Ce paramètre sera important pour l'évaluation des performances de la distribution quantique de clé.

7.3.3 Evaluation du taux d'erreur

Comme nous l'avons vu au chapitre précédent, il n'est possible de distribuer des clés secrètes que dans la mesure où le taux d'erreur sur le canal quantique, généralement noté QBER pour « Quantum Bit Error Rate », est inférieur à une certaine borne, dont la valeur est fixée par le modèle de sécurité. Ce taux d'erreur, lié aux erreurs de codage ou de détection et aux coups d'obscurité, fixe en particulier la limite de sensibilité d'Alice et Bob par rapport à l'intervention d'un espion sur la ligne quantique. Il influence donc de façon importante les performances du système de distribution quantique de clé.

Nous avons apporté un soin particulier à limiter le taux d'erreur « systématique », lié

[4] Les photodiodes à avalanche sont triées par le fabricant en fonction de leur niveau de coups d'obscurité, puis vendues selon différents standards de qualité. Les photodiodes à avalanches de type AQR-14 ont un bruit d'obscurité garanti inférieur à 100 coups/s tandis que pour les modèles de type AQR-13, seul un niveau de coups d'obscurité inférieur à 250 coups/s est garanti. Dans notre expérience, les photodiodes à avalanche H et V sont de type AQR-14 tandis que les photodiodes à avalanche G et D sont de type AQR-13.

aux erreurs d'encodage en polarisation par le modulateur électro-optique. Nous avons pour cela effectué un premier réglage du dispositif de modulation à l'aide d'un laser HeNe, puis nous avons ajusté les quatre valeurs des tensions appliquées sur le modulateur, de façon à minimiser le taux d'erreur pour chacun des quatre états de polarisations codés à l'aide du modulateur. Ce réglage fin a été effectué directement sur les photons uniques émis par Alice et détectés par Bob, et nous sommes ainsi parvenus à un taux d'erreur inférieur à 2% sur chacun des états encodés, avec une valeur du taux moyen d'erreur de 1.7%. Ces taux d'erreur sont calculés directement en comparant les registres correspondant d'une part à la clé d'Alice et d'autre part aux données brutes enregistrées par Bob , en limitant bien sûr la comparaison aux cas où les bases de polarisation correspondant au codage et à la détection coïncident. On peut identifier deux contributions majeurs au taux d'erreur [185] :

- Le caractère imparfait de la modulation et de la détection des états de polarisation des photons. Le nombre de ces erreurs « optiques » est proportionnel au flux de photons de photons détectés par Bob. On peut ainsi définir un facteur de proportionnalité α et écrire que le taux d'erreurs « optiques » correspond à $\alpha \times \mu \times \eta_{\mathrm{T}}\, \eta_{\mathrm{Bob}}$, où η_{T} désigne la transmission optique du canal quantique entre Alice et Bob.
- Les coups d'obscurité des photodiodes. Contrairement aux erreurs de type « optique » le taux d'erreurs correspondant aux coups d'obscurité est constant, égal au paramètre p_{dark} et par conséquent ne varie pas avec le niveau de signal détecté par Bob. Ce type d'erreur devient donc prépondérant dans le régime des fortes atténuations sur le canal quantique.

On peut définir le taux d'erreur e comme le rapport entre le nombre de « clics erronés par unité de temps » et le taux de photodétection p_{exp}. Pour le système expérimental que nous avons utilisé, ce paramètre est alors donné par :

$$e = \alpha \frac{\mu\, \eta_{\mathrm{T}}\, \eta_{\mathrm{Bob}}}{p_{\mathrm{exp}}} + \frac{p_{\mathrm{dark}}}{p_{\mathrm{exp}}}. \tag{7.4}$$

Nous avons mesuré le taux d'erreur e pour différents niveaux η_T de transmission du canal quantique. Les résultats de ces mesures sont présentée dans le tableau 7.1. Par ailleurs, nous avons pu constater que les variations du nombre total d'erreur par unité de temps, $e \times p_{\mathrm{exp}}$ sont bien décrites, par une loi affine dont la variable est η_{T}. Un ajustement linéaire nous a permis de déterminer les paramètres de cette loi affine à partir des données du tableau 7.1 conduisant à $\alpha = (13 \pm 2) \times 10^{-3}$ et $p_{\mathrm{dark}} = (35 \pm 6) \times 10^{-6}$. Ce dernier résultat est compatible avec les mesures décrites précédemment et nous avons par la suite utilisé cette valeur dans les simulations numériques.

7.3.4 Caractéristiques du canal classique

Au cours des sessions de démonstration expérimentales de la distribution quantique de clé avec une source de photons uniques, afin de présenter un travail où *l'ensemble* des étapes de la distribution quantique de clé, sont mis en oeuvre, depuis l'échange de photons uniques polarisés jusqu'aux communications classiques nécessaires à la correction d'erreur et l'amplification de confidentialité.

En particulier, les communications classiques entre Alice et Bob, qui sont dans le dispositif expérimental deux entités physiquement distinctes, ont été effectuées à travers le réseau Internet TCP/IP de l'Institut d'Optique.

Comme nous l'avons expliqué au chapitre précédant, dans la section consacrée au protocole BB84, les phases de codage en polarisation et de détection de photons uniques polarisés permettent à Alice et Bob de disposer de données brutes corrélées. Il est ensuite nécessaire

η_T	Taille moyenne des données brutes (bits)	$p_{\exp}$	QBER
1	8000	7.6×10^{-3}	1.65 %
0.498	4250	4.0×10^{-3}	2.2 %
0.25	2100	2.0×10^{-3}	3.2 %
0.128	1025	9.8×10^{-4}	4.15 %
0.057	395	3.8×10^{-4}	9.4 %

TAB. 7.1 – Mesures des paramètres expérimentaux correspondant au taux de photodétection chez Bob $p_{\exp}$ et au taux d'erreur QBER, en fonction de la transmission η_T du canal quantique. Afin de limiter les fluctuations statistiques sur ces mesures, ces valeurs ont été calculées sur des échantillons statistiques contenant au moins 3000 bits. Dans le cas des fortes atténuations sur le canal quantique, ces échantillons ont été obtenus par concaténation des données issues de plusieurs séquences successives d'échange de photons entre Alice et Bob
.

d'appliquer des algorithmes classiques afin d'aboutir au partage d'une clé secrète identique, connue seulement d'Alice et de Bob. Nous avons effectué l'ensemble de ce traitement informatique à l'aide du logiciel libre QUCRYPT écrit par Louis SALVAIL [214]. Ce programme Java, dont nos présentons une image d'écran à la figure 7.7 est parfaitement adapté au fonctionnement sur deux serveurs distants reliés à travers le réseau Internet.

7.4 Mise en oeuvre du protocole « BB84 »

Chaque session d'échange de clé, consiste en une phase d'environ 0.2 s de communication quantique, au cours de laquelle une séquence de 1048575 bits est codée chez Alice. Compte tenu de l'efficacité de la source de photons uniques $\mu = 2.35\%$, et de l'efficacité du système de détection chez Bob $\eta_{\text{Bob}} \simeq 0.3$, Bob détecte, en l'absence d'atténuation sur le canal quantique, environ 8000 photons pour chaque session. Il dispose donc d'une clé brute d'environ 8000 bits.

La première étape des communications classiques est alors de se mettre d'accord sur la position des impulsions pour lesquelles Bob a enregistré un clic de photodétection. Ensuite, Alice et Bob révèlent publiquement leurs choix de base pour le codage, respectivement la détection des photons échangés. Les impulsions pour lesquelles plus d'une photodétection a eu lieu sont quant à elles éliminées, car elles sont considérées comme ambigües [5]. À la suite de l'annonce des bases, Alice et Bob ne conservent que les bits pour lesquels ils avaient fait un choix de base identique, c'est-à-dire en moyenne un bit sur deux. On aboutit ainsi à la « clé filtrée » dont la taille $N_{\text{filtree}} \approx 4000$ bits est environ la moitié des données brutes initiales.

7.4.1 Distillation d'une clé secrète à partir de la clé filtrée

Correction d'erreur et amplication de confidentialité

Les clés filtrées d'Alice et Bob ne sont pas parfaitement corrélées, car elles restent en-

[5] On montre néanmoins qu'il est important de fixer une borne supérieure sur le nombre d'impulsions dont on défausse ainsi le résultat, sans quoi l'on peut introduire une faille de sécurité dans le protocole. En pratique, dans les expériences que nous avons menées, le nombre d'événements correspondant est très faible, de sorte que leur suppression pure et simple n'introduit aucune limitation pratique aux performances des échanges de clé en terme de débit et de sécurité.

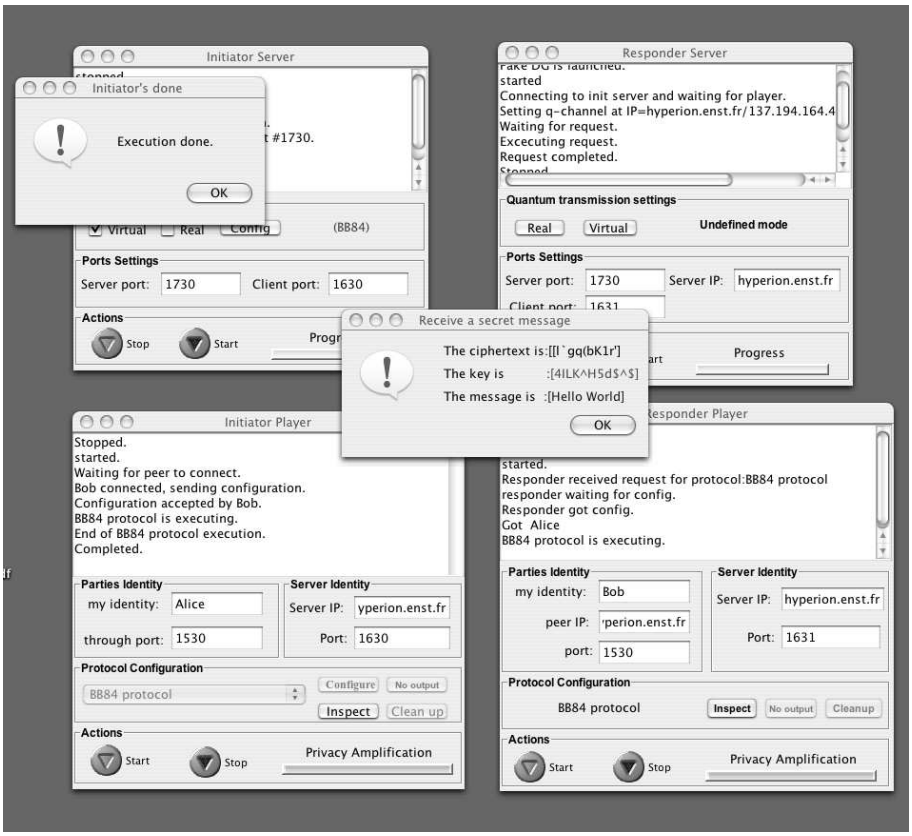

FIG. 7.7 – Fenêtres du programme QUCRYPT permettant de configurer des serveurs distants afin de réaliser les protocoles de communication classique de correction d'erreur et d'amplification de confidentialité permettant l'établissement et le partage d'une clé secrète à partir des données brutes issues de la phase de communication quantique.

tachées d'erreurs. En outre, un espion potentiel a pu éventuellement être en mesure d'en découvrir une partie au cours de la transmission quantique. Les techniques de correction d'erreur et d'amplification de confidentialité sont donc mises en œuvre à travers l'utilisation du logiciel QUCRYPT [214]. QUCRYPT utilise tout d'abord l'algorithme CASCADE afin de réaliser la première étape de correction d'erreurs [245]. Cet algorithme consiste à la recherche dichotomique itérative des erreurs, à l'intérieur des blocs de données que constituent les clés filtrées, en effectuant pour cela des contrôles de parité. Il s'agit d'un algorithme de correction d'erreur qui requiert des communications bi-directionnelles entre Alice et Bob, et qui est optimisé pour corriger *toutes* les erreurs tout en révélant un nombre de bits aussi faible que possible.

Pour un taux d'erreur e la théorie de Shannon [243] nous permet de fixer une borne inférieure $f(e)$à la quantité d'information qu'il est nécessaire d'échanger sur le canal quantique afin de permettre la correction d'une erreur.

$$f(e) = -\log_2 e - (1-e)\log_2(1-e) \tag{7.5}$$

Nous avons vérifié que pour la taille des clés utilisées dans l'expérience, correspondant en pratique à plusieurs milliers de bits, l'algorithme CASCADE fonctionne de façon efficace : l'information échangée nécessaire à la correction d'un bit ne dépasse que d'environ 10% la borne de Shannon fixée par l'équation (7.5).

Pour que l'établissement d'une clé secrète soit possible, Alice et Bob doivent commencer par s'assurer que le taux d'erreur e n'est pas trop élevé . À cet effet, 1% des données de la clé filtrée sont sacrifiées afin d'effectuer l'évaluation du taux d'erreur dans les données brutes. Nous nous sommes assuré que cette proportion de 1% était suffisante, en vérifiant que la taille finale des clés secrètes obtenues au final fluctue de moins de 5% d'une exécution à l'autre de CASCADE.

Faisant suite à cette phase de correction d'erreur, une deuxième étape, dite d'amplification de confidentialité est également assurée à l'aide de QUCRYPT. Elle consiste à fabriquer, grâce à une fonction de hachage, une sorte de « condensé » à partir des données partagées par Alice et Bob, qui ont certes été rendues identiques après la phase de correction d'erreur mais sur lesquelles l'espion Eve peut avoir acquis de l'information. La fonction de hachage est choisie au hasard parmi une classe de fonction vérifiant de « bonnes » propriétés cryptographiques (cf. par exemple la référence [249] pour une définition mathématique de ces notions), puis est annoncées publiquement. On peut prouver, dans le cadre de la théorie de l'information, que l'application de la fonction de hachage permet de rendre évanescente l'information résiduelle d'Eve sur le condensé généré symétriquement par Alice et Bob. On fixe pour cela un paramètre s dit « paramètre de sécurité » qui désigne le nombre de bits supplémentaires d'information mutuelle entre Alice et Bob I_{AB} que l'on consomme dans la phase d'amplification de confidentialité de façon à rendre l'information résiduelle d'Eve $I_E^{(finale)}$ proportionnelle à 2^{-s}.

Les paramètres de l'amplification de confidentialité sont directement liés au modèle de sécurité et en particulier à la quantité d'information qu'un hypothétique espion a pu se procurer. Ainsi, l'information I_E dont peut disposer Eve avant la phase d'amplification de confidentialité, est la somme de l'information qu'elle a potentiellement pu obtenir en écoutant la communication quantique et de l'information rendue publique durant la phase de correction d'erreur. On peut montre que I_E est bornée : connaissant le taux d'erreur de la communication quantique, QBER, le modèle de sécurité nous permet d'évaluer une borne supérieure à la première des contributions à I_E ; par ailleurs, l'équation 7.5 montre que la quantité d'information divulguée durant la phase de correction d'erreur est asymptotiquement bornée par la limite de Shannon multipliée par un facteur correctif tenant compte de l'efficacité de l'algorithme utilisé (Le coefficient 1.1 vaut pour notre expérience et l'utilisation de CASCADE).

7.4.2 Modèle de sécurité

En fixant à l'intérieur de QUCRYPT une borne supérieure au QBER « admissible », on s'assure que toutes les sessions d'échanges de clé aboutissant à l'établissement symétrique d'une clé commune sont sûre face à une certaine classe d'attaques. Nous avons ainsi fixé cette borne à 12.5%, valeur qui correspond à la probabilité minimale qu'a Eve d'introduire une erreur en réalisant des mesures impulsion par impulsion, sans connaître la base de mesure choisie par Bob [214].

Comme nous l'avons expliqué au chapitre précédent, des attaques plus raffinées et complexes sont cependant envisageables et la simple donnée du taux d'erreur e ne suffit pas à évaluer la sécurité de la distribution quantique de clé. Nous avons ainsi adopté l'approche de Norbert LÜTKENHAUS qui a développé un cadre théorique général permettant de démontrer la sécurité d'une réalisation expérimentale de distribution quantique de clé contre les attaques « individuelles » [185]. Si les hypothèses liées à ce modèle de sécurité ont été présentées au chapitre précédent, nous rappellerons ici qu'il établit une preuve for-

melle « d'existence », : tout en tenant compte des imperfections expérimentales des sources de photons et des détecteurs, il indique qu'il est possible de garantir un échange de clé secrète entre Alice et Bob, pour une certaine « région » des paramètres expérimentaux telles que le taux d'erreur ou la proportion d'impulsions à plusieurs photons [6]

Dans le cadre de ce modèle de sécurité, la performance du système d'échange quantique de clé peut être caractérisée par la valeur du gain G, désignant la proportion moyenne de bits secrets partagés par impulsion encodée. La référence [185] fournit explicitement la variation de G, en fonction des paramètres expérimentaux p_{exp}, e et $S^{(\mathrm{m})}$ de notre expérience :

$$G = \frac{1}{2}\, p_{\mathrm{exp}} \left\{ \frac{p_{\mathrm{exp}} - S^{(\mathrm{m})}}{p_{\mathrm{exp}}} \left(1 - log \left[1 + 4e \frac{p_{\mathrm{exp}}}{p_{\mathrm{exp}} - S^{(\mathrm{m})}} - 4 \left(e \frac{p_{\mathrm{exp}}}{p_{\mathrm{exp}} - S^{(\mathrm{m})}} \right)^2 \right] \right) \right. \\ \left. + 1.1 \left[\log_2 e + (1-e) \log_2 (1-e) \right] \right\} \tag{7.6}$$

7.5 Performances du système et résistance aux pertes

La figure 7.8 présente les mesures expérimentales de G ainsi que les courbes théoriques des variations de ce paramètre en fonction de l'atténuation introduite sur le canal quantique. Les taux de bits sûrs mesurés expérimentalement sont calculés à partir d'échantillons de données suffisamment grands pour garantir des fluctuations statistiques inférieures à 5 %. On notera que ces valeurs sont en très bon accord avec les courbes théoriques, ce qui prouve que les paramètres expérimentaux ont été mesurés avec une précision suffisante et que les échantillons statistiques considérés contiennent suffisamment de points pour ne pas observer de limitation dans l'efficacité des algorithmes utilisés par QUCRYPT. En l'absence d'atténuation entre Alice et Bob, le nombre moyen de bits sûrs échangés au cours d'une session de 0.2 s est de 3200 bits, ce qui correspond à un taux de 16 kbits/s. Cette valeur est plus de deux fois supérieure à celle obtenue lors de la première réalisation expérimentale de distribution quantique avec une source de photons uniques [233]. Comme on peut le voir sur la figure 7.8, la réduction de la proportion $S^{(m)}$ d'impulsions multiphotoniques vis-à-vis d'une source d'impulsions cohérentes atténuées (WCP sur la figure 7.8) donne à la source de photons uniques un avantage significatif dans le régime des atténuations importantes. Néanmoins, comme notre système présente un taux de coups d'obscurité relativement importants [7], et comme de plus nous avons adopté un modèle de sécurité relativement sévère, l'atténuation maximale que peut supporter notre système est de l'ordre de

[6] On notera qu'il serait bien sûr possible d'adopter des hypothèses de sécurité moins strictes que celles utilisées dans [185], augmentant ainsi de façon quelque peu artificielle les performances en terme de taux d'échange de bits sécurisés. Par ailleurs, les protocoles alternatifs proposés récemment, comme par exemple celui de la référence [**?**] peuvent s'avérer être une manière efficace d'augmenter, à performance expérimentale équivalente, la portée maximale sur laquelle peuvent être réalisés des échanges sécurisés. Il serait donc intéressant de comparer les performances relatives des sources de photon uniques et des sources laser atténuées dans le cadre de ces nouveaux protocoles. Cependant, ne disposant pas d'éléments de comparaison aussi bien établis que ceux développés dans la référence [185], nous avons volontairement remis ce travail à une date ultérieure, sachant que Valerio SCARANI travaille actuellement à établir les dérivations analytiques liées au SARG [**?**].

[7] Il y a plusieurs raisons à cela. La raison principale est que la durée de vie de la source de photons unique ne nous permet pas d'effectuer un fenêtrage trop sélectif vis à vis des coups d'obscurité. On pourrait néanmoins diminuer sensiblement le niveau des coups d'obscurité d'au moins deux façons. La première solution serait d'utiliser des photodiodes à avalanches présentant des niveaux de coups d'obscurité bien inférieurs telles que les AQR-15, pour lesquelles taux de coups d'obscurité d est inférieur à 70 Hz. Nous pourrions également choisir de façon active la base de photodétection au niveau de Bob, ce qui diminuerait le niveau de bruit d'un facteur deux.

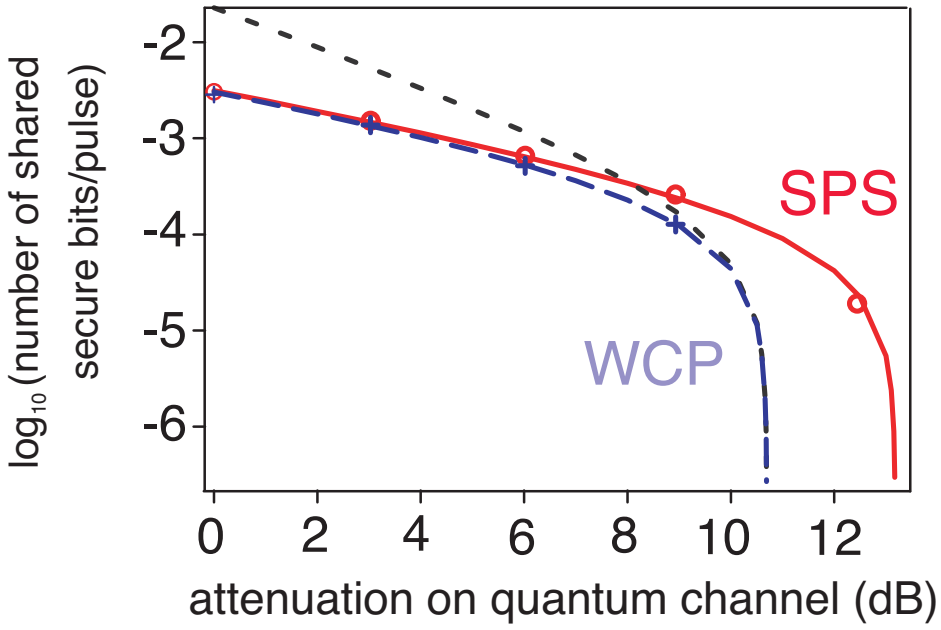

FIG. 7.8 – Taux de clé sûr par impulsion mésuré en bit et présenté sur une échelle logarithmique, en fonction de l'atténuation sur le canal quantique exprimée de décibels. Les courbes sont calculées à partir de l'équation (7.6) et les points sont directement issus des réalisations expérimentales d'échange de clé, en présence d'atténuation sur le canal quantique. La courbe en trait plein et la courbe en tirets larges correspondent respectivement aux performances de la source de photon uniques et d'une source d'impulsions cohérentes atténuées de même taux de comptage. La courbe en tirets courts est obtenue en optimisant G par rapport au paramètre μ dans l'équation (7.6).

13 dB. Cette valeur est inférieure aux performances publiées par l'équipe de Y. YAMAMOTO [106]. L'expérience que nous avons effectuée montre cependant clairement les avantages à utiliser une source de photons uniques dans le régime des fortes atténuations.

Le premier élément de comparaison consiste à calculer le taux G de bits sûrs par impulsion, pour la source de photons uniques et pour une référence poissonnienne de même paramètre $\mu = 0.0235$ (courbe notée « WCP »). Néanmoins, lorsqu'on utilise une source d'impulsions cohérentes atténuées, le paramètre μ peut être facilement ajusté à l'aide d'un atténuateur optique variable. C'est pour cette raison que nous avons également calculé les performances optimales que l'on pourrait obtenir à l'aide d'une source d'impulsions cohérentes atténuées, pour les mêmes conditions expérimentales, en optimisant le paramètre μ pour chaque valeur de l'atténuation. Cependant, même avec cette stratégie correspondant à la courbe en pointillés sur la figure 7.8, il apparaît clairement que la source de photons uniques SPS dépasse en performance la source WCP, dès lors que le niveau d'atténuation sur le canal quantique dépasse 9 dB.

On notera que la comparaison entre la source de photons uniques SPS et une source d'impulsions cohérentes atténuées WCP a été effectuée pour le même niveau de coups d'obscurité p_d. Ceci présente l'avantage de permettre de relier directement le gain en terme de performance avec la réduction du taux d'impulsions multiphotoniques décrite par le paramètre$S^{(\mathrm{m})}$. On peut cependant objecter qu'une telle comparaison n'est pas à l'avantage

des sources d'impulsions atténuées, pour lesquelles le niveau de coups d'obscurité peut être réduit au moyen d'un fenêtrage temporel plus étroit. Nous ne sommes pas rentrés ici dans ces considérations, en grande partie parce que nous pensons que la durée de vie d'émission ne constitue pas une limitation intrinsèque de la cryptographie quantique avec une source de photons uniques. En effet, des systèmes alternatifs présentent des durées de vie bien inférieures à la nanoseconde [106], tandis que d'autres centres colorés du diamant, dont l'observation a été reportée récemment [93], présentent des caractéristiques d'émission bien adaptées à un fenêtrage temporel et spectral plus sélectif.

7.6 Conclusion

Pour cette expérience, nous avons choisi de suivre de manière fidèle le protocole de transmission proposé par C. BENNETT et G. BRASSARD en 1984 [175]. Nous nous sommes attachés à obtenir de très faibles taux d'erreur de codage et de détection des quatre états choisis pour le codage en polarisation des photons. Nous avons ainsi obtenu un QBER de 1.7%, le plus bas ayant été obtenu à ce jour dans une expérience de cryptographie quantique utilisant une source de photons uniques.

Nous avons de plus étudié l'évolution du taux de bits sûrs en fonction d'une atténuation ajoutée sur la ligne de transmission entre Alice et Bob. Cette atténuation permet de simuler une propagation dans l'air sur une plus grande distance que celle utilisée dans l'expérience. Nous avons montré que lorsque la transmission du canal quantique est de l'ordre de 6%, l'utilisation de photons uniques conduit à des performances impossibles à obtenir à l'aide d'impulsion cohérentes atténuées [234]. On notera que cette valeur caractéristique de l'atténuation correspond à une propagation des photons sur une distance de 300 km à travers l'atmosphère, dans le domaine spectral d'émission des centres colorés NV. Ainsi, un tel dispositif de cryptographie quantique à photons uniques pourrait de manière peut être un peu futuriste, fonctionner entre Alice sur la Terre, et Bob embarqué sur un satellite [209].

Chapitre 8

Source de photons annoncés pour la cryptographie quantique longue distance

Sommaire

8.1 Introduction

Une source de photons annoncés, dont nous avons brièvement expliqué le principe de fonctionnement dans le chapitre d'introduction, est caractérisée par le fait que l'émission de chaque photon s'accompagne d'un « signal témoin » que l'on peut utiliser pour fenêtrer temporellement les systèmes de détection, ce qui permet d'obtenir de façon conditionnelle une statistique proche de celle d'une source à un photon.

Dans le cadre d'une expérience de distribution quantique de clé, les avantage résultant de l'utilisation d'une telle source plutôt que d'impulsions cohérentes atténuées résident

dans la forte réduction de la proportion d'impulsions vides envoyées par Alice, ainsi que dans le caractère sub-poissonnien de la statistique des photons annoncés. Comme dans le cas des sources de photons uniques déclenchées, on peut ainsi augmenter significativement les performances des systèmes expérimentaux dans le régime des fortes atténuations [106, 234].

De plus, si la longueur d'onde de la source de photons annoncés est compatible avec la propagation sur une fibre optique télécom, alors cette source est particulièrement adaptée pour la distribution quantique de clé sur de grandes distances . Une première mise en oeuvre expérimentale de cette idée dans le cadre de la cryptographie quantique a été réalisée en 2001 dans le groupe de Nicolas Gisin où ont été réalisés les premiers travaux avec une source de photons annoncés à 1550 nm [229], mettant à cette occasion en lumière certaines contraintes expérimentales spécifiques, liées notamment à la largeur spectrale de la source ainsi qu'aux limites sur l'efficacité de collection.

En stage dans l'équipe de recherche dirigée par Alexei Trifonov, au sein de la startup MagiQ, nous avons également travaillé à la mise au point d'une source de photons uniques annoncés émettant à 1550 nm, optimisée pour les longues distances, c'est à dire de faible largeur spectrale. Nous avons de plus effectué les premières étapes permettant la réalisation d'un système opérationnel de cryptographie quantique fonctionnant avec cette source.

Nous débuterons ce chapitre en évoquant les enjeux spécifiques liés à la réalisation d'expérience de distribution quantique de clé sur de grandes distances, effectuant un bref rappel des travaux déjà effectués avant d'analyser les barrières technologiques existantes. Nous décrirons ensuite la réalisation et les performances de la source de photons annoncés que nous avons réalisée avant de conclure en présentant les premiers résultats obtenus en intégrant notre source dans un dispositif de crypographie quantique composé d'un interféromètre « à un passage » et de 76 km de fibre optique commerciale. Ces résultats préliminaires démontrent l'intérêt du type de source que nous avons développé pour la cryptographie quantique à longue distance [235].

8.2 Cryptographie quantique à longue distance

La cryptographie quantique et plus généralement les communications quantiques présentent des particularités qui les rendent irréductibles aux méthodes utilisées dans les télécommunications dites classiques. Ces particularités, telles que le principe de non-clonage [157], les propriétés non-locales des corrélations quantiques [37], le caractère probabiliste des résultats de mesure... sont à l'origine même des potentialités nouvelles offertes par les communications quantiques. En revanche, la nature de l'information transmise impose également des contraintes nouvelles, qui ont une importance considérable quand on s'attache à la mise en oeuvre des protocoles de communication quantique puisqu'ils en déterminent les limites expérimentales.

Ainsi, l'un des impératifs d'une communication quantique est la préservation de la cohérence des états quantiques véhiculés. L'une des conséquences importantes liées à cette contrainte est que le signal quantique ne peut être ni mesuré, ni même amplifié par des méthodes classiques, qui ont pour effet d'ajouter du bruit et donc de ne pas maintenir la cohérence quantique [157]. En termes pratiques, des techniques telles que l'amplification optique dans des fibres dopées à l'erbium ou l'amplification électronique, couramment utilisées dans les télécommunications traditionnelles, ne peuvent être utilisées dans une communication quantique. Il s'ensuit que l'atténuation et la décohérence du signal au cours de sa propa-

gation constitue une limite physique intrinsèque des communications quantiques, qui sont donc par leur nature même limitées en distance.

La cryptographie quantique, qui constitue la technologie la plus mature en terme de communication quantique, a naturellement été le premier champ d'expérimentation pour les communications quantiques à grandes distances. Nous évoquons quelques jalons essentiels des progrès effectués sur cette voie, tout en reliant les performances actuelles des systèmes de cryptographie quantique aux barrières technologiques et aux contraintes imposées par le maintien d'une sécurité démontrable.

8.2.1 Allongement des distances de transmission et verrous technologiques

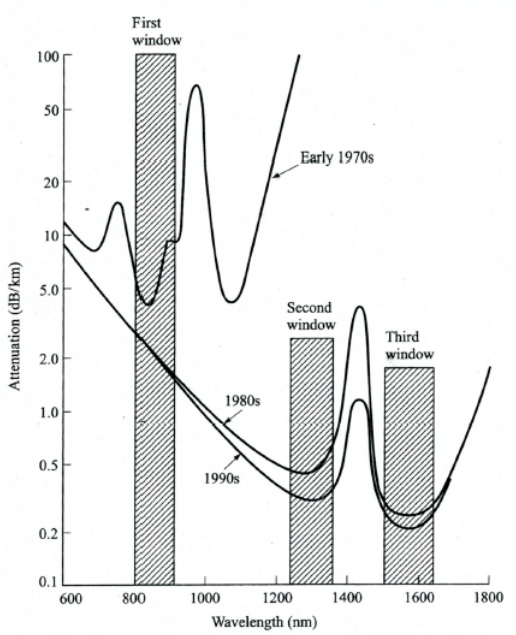

FIG. 8.1 – Transmission des fibres optiques commerciales en fonction de la longueur d'onde. On voit clairement apparaître l'existence de deux « fenêtres » respectivement autour de 1.3 et 1.55 μm.

Du fait d'une moindre atténuation des fibres optiques dans la fenêtre de longueur d'onde située autour de 1550 nm (cf. figure 8.1) l'utilisation de grandes distances de propagation impose de réaliser les expériences à cette longueur d'onde, même si les photodiodes à avalanche à InGaAs, qui sont les mieux adaptées à la détection de photons uniques à cette longueur d'onde, ont des performances nettement moins bonnes que les détecteurs disponibles pour des longueurs d'onde inférieures [211].

D'autre part, comme nous l'avons expliqué au chapitre 6, la prise en compte de l'attaque « PNS » [183, 185] impose des compromis sévère quant à la limitation du nombre moyen μ de photons par impulsion et la quantité de pertes tolérables. En particulier, si le taux de photodétection varie comme $O(\eta_T)$ où η_T désigne la transmission du canal quantique, le taux de bits sûrs varie lui comme $O(\eta_T^2)$.

On voit donc apparaître deux types de limites :

1. La limite « expérimentale » qui correspond à l'atténuation maximale pour laquelle on peut encore détecter un photon unique, c'est à dire pour laquelle le signal de photodétection est de l'ordre du bruit causé par les coups d'obscurité. Cette limite est donc de la forme η_{B}/p_d où p_d désigne le taux de coups d'obscurité et η_{B} correspond à l'efficacité de l'appareil de Bob (notamment des photodétecteurs).
2. Une limite « théorique » discutée par exemple dans la référence [183] et imposée en particulier par l'attaque PNS. La limite en terme d'atténuation maximale est alors de $\eta_{\mathrm{B}}/2\sqrt{p_d}$, bien inférieure à la limite expérimentale définie dans le point précédent.

La plupart des expériences publiées à ce jour et utilisant des impulsions cohérentes atténuées fonctionnaient avec une valeur de μ comprise entre 0.1 et 0.2, en suivant des modèles de sécurité souvent moins restrictifs que celui développé dans la référence [185]. Elles fonctionnaient en quelque sorte essentiellement dans le régime correspondant aux « limitations expérimentales » que nous venons d'évoquer. Dans ce régime, la proportion d'information qu'un espion est théoriquement capable de se procurer est largement sous-estimée et les distances maximales atteintes, sur lesquelles ces expériences fondent généralement leur « publicité » , doivent être considérées avec prudence. Si les distances annoncées donnent bien sûr une indication des progrès effectués dans la mise au point des systèmes de cryptographie quantique, les paramètres de fonctionnement expérimentaux sont parfois situés en dehors de la « zone » à l'intérieur de laquelle la sécurité de la distribution de clé peut être démontrée.

Comme cela apparaît clairement dans les limites 1. et 2. que nous venons de d'évoquer, ce sont avant tout les performances des photodétecteurs et donc leurs améliorations qui ont permis de repousser les limites des distances sur lesquelles les expériences de cryptographie quantique ont pu être effectuées.

On peut d'ailleurs citer quelques jalons essentiels de cette progression en commençant par évoquer les travaux précurseurs menés par Paul TOWNSEND au milieu des années 90, effectués à la longueur d'onde de 1.3 μm [218, 219].

Le passage à la longueur d'onde de 1.5 μm et le perfectionnement des interféromètres utilisés [216], ont permis d'accroître les distances de transmission, avec des publications faisant état d'une distance de 48 km en 2000 [220], de 67 km en 2002 [221] pour une expérience effectuée sous le lac de Genève tandis que plus récemment, une équipe japonaise de l'entreprise NEC ayant centré ses efforts sur l'améliorations des photodiodes à avalanche InGaAs a annoncé avoir atteint des distances supérieures à 100 km [222].

Les progrès très récents apparus au niveau des protocoles de distribution de clé quantique [184, 200] sont susceptibles de permettre de faire se rejoindre les limites expérimentales et théoriques. Le protocole proposé quelques jours avant la fin de la rédaction de ce manuscrit par H. K. LO annonce en effet pouvoir contourner les limitations dues à l'attaque PNS, ce qui permettrait d'atteindre des distances limites de l'ordre de 150 km pour la distribution quantique de clé, tout en conservant la sécurité. L'expérience de la référence [223] a mis à profit ce nouveau protocole pour démontrer une transmission sur 122 km.

8.3 Réalisation expérimentale d'une source de photons annoncés à 1550 nm

Comme l'ont montré C. K. HONG et L. MANDEL dès la fin des années 80 [41] il est possible d'obtenir une bonne approximation d' états à un photon à partir de paires de photons produites par fluorescence paramétrique, en utilisant l'un des photons comme signal de déclenchement. Le temps de cohérence d'une paire de photons étant typiquement inférieur à

la picoseconde, la détection d'un des photons annonce en effet avec une très bonne précision temporelle l'existence du deuxième photon qui lui est associé par le processus d'émission paramétrique, ce qui motive notre utilisation du terme de « photons annoncés ». Cette technique présente un fort intérêt dans le cadre de la réalisation d'un système de cryptographie quantique car elle rend possible l'utilisation de photons annoncés aux longueurs d'onde télécom, permettant d'envisager une propagation à longue distance dans une fibre optique, tandis que le photon « témoin » est émis à une longueur d'onde efficacement détectée par les photodiodes à avalanche au silicium.

Nous avons en effet opté pour la réalisation d'une source dissymétrique, émettant par fluorescence paramétrique, à partir de la lumière de pompe à la longueur d'onde de 532 nm, des paires de photons dont les longueurs d'ondes sont respectivement de 810 nm pour le photon signal et de 1550 nm pour le photon réplique.

L'intérêt d'un tel choix de longueur d'onde est triple :

1. On dispose de lasers intenses, monomodes et de de très grande pureté spectrale à 532 nm ;
2. Les photons « signal » émis 810 nm, peuvent être détectés à l'aide de photodiodes à avalanche au silicium, dont les performances sont très bonnes ;
3. Les photons « répliques » émis à 1550 nm, « annoncés » par les clics de photodétection des photodiodes à avalanche au silicium, sont adaptés à la propagation sur de longues distances dans des fibres optiques.

8.3.1 Source de photons annoncés : principe

C'est dans l'équipe de Nicolas GISIN qu'ont été effectués les premiers travaux soulignant l'intérêt d'une source de photons annoncés 810/1550 nm optimisée pour la cryptographie à grande distance. La première expérience fut réalisée par Grégoire RIBORDY *et al.* [229], et ces travaux sont actuellement poursuivis dans le cadre de la thèse de Sylvain FASEL [230, 231].

Le principe d'utilisation d'une telle source pour la cryptographie quantique consiste à obtenir une très bonne efficacité d'émission d'un photon réplique à 1550 nm conditionnée par un clic de photodétection sur la voie signal à 810 nm. Si l'on cherche à établir une comparaison avec le fonctionnement traditionnel d'une source d'impulsions déclenchées, la probabilité conditionnelle d'émettre un photon sur la voie à 1550 nm par clic de photodétection sur la voie à 810 nm s'apparente au paramètre μ, nombre moyen de photons par impulsions :

$$P(\text{photon sur la voie 1550 nm} \mid \text{clic sur la voie 810 nm}) \sim \mu \tag{8.1}$$

L'une des difficultés expérimentales majeures réside donc dans d'un bon couplage des faisceaux dans des fibres, sachant en outre que la fibre optique à 1550 nm est une fibre monomode (c'est le standard pour les télécommunications optiques à 1.55 μm.). Comme nous allons le voir, une autre difficulté provient de la nécessité de limiter la largeur spectrale de la source, car ce paramètre va déterminer l'importance de l'élargissement temporel des impulsions lors de la propagation dans les fibres et donc le rapport signal à bruit lors de la photodétection. Nous montrerons donc ici comment nous avons optimisé ces paramètres avant de présenter, dans la section suivante les résultats obtenus en janvier 200 dans les laboratoire de MagiQ en terme de taux d'erreur pour une propagation à longue distance.

8.3.2 Choix du cristal et géométrie de l'accord de phase

Le choix du cristal non linéaire adapté à la réalisation de notre source de paires de photons paramétriques est extrêmement contraint. On cherche en effet d'une part à coupler efficacement les photons émis dans des fibres monomodes, en utilisant l'intrication spatiale entre les vecteurs d'ondes des photons à 810 nm et à 1550 nm ; et d'autre part à obtenir un spectre d'émission le plus étroit possible afin de limiter les effets de la dispersion liés à la propagation du signal quantique sur de longues distances dans une fibre.

Après avoir travaillé sur un cristal de BBO en juillet 2003, pour lequel une très bonne efficacité de couplage (plus de 60 $\%$ pour la probabilité de détection conditionnelle) avait été obtenue, nous avons opté, pour les expériences réalisées en janvier 2004, pour un cristal de 20 mm de $LiNbO_3$, dont le l'accord de phase est de type 1, non critique, afin de limiter la largeur spectrale d'émission et de pouvoir ainsi sélectionner une bande spectrale très étroite au niveau des photons à 810 nm sans trop réduire l'efficacité de la source.

Le premier élément guidant le choix du cristal est lié aux longueurs d'onde envisagées. Ce choix est bien sûr contraint par le fait que l'on veuille obtenir des photons annoncés à 1550 nm et par la conservation de l'énergie dans le processus paramétrique. D'autre part, la longueur d'onde des photons témoins doit être adaptée à la détection par des photodiodes à avalanche au silicone. En dernier lieu, le processus de conversion non-linéaire nécessite l'usage d'un laser de pompe monomode, à la longueur d'onde stable et de faible largeur spectrale.

En utilisant un laser de pompe de type Verdi, émettant à 532 nm, l'ensemble de ces conditions peuvent être remplies. Ce laser YAG doublé présente en effet une largeur spectrale inférieure à 5 MHz et une très bonne stabilité. Comme $\frac{1}{532} = \frac{1}{1550} + \frac{1}{810}$, la conservation de l'énergie implique que les photons témoins sont produits à la longueur d'onde de 810 nmn.

Nous avons choisi un cristal de niobate de lithium, $LiNbO_3$ car celui-ci présente de larges coefficients non-linéaires et une acceptance angulaire réduite, et est donc bien adapté pour obtenir une émission paramétrique sur une bande spectrale relativement réduite. Comme on souhaite obtenir une efficacité de conversion non-linéaire importante on a de plus opté pour un cristal de 20mm de long (et de section 4 mm $\times$ 4 mm) .

La géométrie adoptée pour la source obéit par ailleurs à un certain nombre de contraintes. Afin que les paires de photons produites dans la totalité du cristal contribuent au même mode du champ, nous nous somme placés en configuration d'accord de phase colinéaire non-critique [261]. La géométrie colinéaire assure que les photons paramétriques créés tout au long du cristal sont alignés sur le faisceau de pompe, ce qui maximise la proportion de lumière paramétrique émise suivant un vecteur d'onde donné. Pour que cette condition soit effectivement réalisée, il est de plus nécessaire que la dispersion angulaire du faisceau de pompe soit faible afin que le faisceau pompe puisse être considéré comme une onde plane sur toute la longueur du cristal. Enfin, il faut également que le walk-off (angle entre le vecteur d'onde et le vecteur de Poynting du faisceau pompe au sein du cristal) soit réduit. Ce problème est résolu en adoptant une géométrie d'accord de phase dite non critique, correspondant au cas où le faisceau pompe fait un angle de 90° avec l'axe optique du cristal. Dans cette configuration le walk-off s'annule.

On règle la température du cristal de $LiNbO_3$ de manière à assurer l'accord de phase dans la configuration colinéaire. La configuration d'accord de phase colinéaire non critique présente des avantages remarquables : elle permet non seulement de maximiser la longueur de cristal participant efficacement à l'accord de phase mais facilite également considérablement les étapes d'alignement qui sont très critiques en ce qui concerne le couplage de la lumière dans des fibres monomodes. En dernier lieu, une telle géométrie permet de rendre le mon-

tage compact en séparant sur une distance réduite les faisceaux paramétriques destinés à être couplés dans deux fibres optiques monomodes indépendantes. En effet, du fait de leur différence en longueur d'onde, photons signal (810 nm) et réplique (1550 nm) peuvent être séparés efficacement à l'aide d'un miroir dichroïque.

8.3.3 Conditions d'accord de phase

Pour un mélange à trois onde, la conservation de l'énergie s'écrit

$$\omega_3 = \omega_1 + \omega_2 \tag{8.2}$$

tandis que la condition d'accord de phase s'écrit :

$$\overrightarrow{k_3} = \overrightarrow{k_1} + \overrightarrow{k_2} \tag{8.3}$$

Dans le cas de l'accord de phase colinéaire, cette dernière condition se résume à une équation scalaire que l'on peut écrire :

$$\mathrm{n}_3\,\omega_3 = \mathrm{n}_1\,\omega_1 + \mathrm{n}_2\,\omega_2 \tag{8.4}$$

Cette condition est automatiquement satisfaite dans un milieu non dispersif car elle est alors équivalente à la condition (8.2). En revanche, dans un milieu dispersif tel que le niobate de lithium cette dernière équation impose une contrainte sur les indices de réfraction, qui peut être satisfaite en jouant soit sur l'orientation de la polarisation des faisceaux vis-à-vis des axes du cristal soit sur le contrôle des indices en fonction de la température. Travaillant en géométrie d'accord de phase colinéaire, nous avons donc utilisé le contrôle de la température pour optimiser l'accord de phase en plaçant notre cristal de $LiNbO_3$ dans un four thermostaté.

On peut calculer la température correspondant à l'accord de phase colinéaire à l'aide des équations de Sellmeier pour le niobate de lithium :

$$\mathrm{n_o}(\lambda,\mathrm{T}) = \sqrt{4.9130 + \frac{0.1173 + 1.65\,10^{-8}\,\mathrm{T}^2}{\lambda^2 - (0.212 + 2.7\,10^{-8}\,\mathrm{T}^2)^2} - 0.0278\,\lambda^2} \tag{8.5}$$

$$\mathrm{n_e}(\lambda,\mathrm{T}) = \sqrt{4.5567 + \frac{0.0970 + 2.7\,10^{-8}\,\mathrm{T}^2}{\lambda^2 - (0.201 + 5.4\,10^{-8}\,\mathrm{T}^2)^2} - 0.0224\,\lambda^2} \tag{8.6}$$

Pour l'accord de phase de type I les photons signaux et idler sont polarisés dans la direction ordinaire tandis que la pompe est polarisée suivant la direction extraordinaire. L'équation d'accord de phase colinéaire (8.4) intégrant la température s'écrit donc :

$$\mathrm{n_e}(0.532\mu\mathrm{m},\mathrm{T})/0.532 = \mathrm{n_o}(0.81\mu\mathrm{m},\mathrm{T})/0.81 + \mathrm{n_o}(1.55\mu\mathrm{m},\mathrm{T})/1.55 \tag{8.7}$$

On peut alors, à l'aide des équations de Sellmeier, calculer la température correspondant à l'accord de phase recherché . On a représenté sur la figure 8.2 la valeur des deux termes de l'égalité (8.7) en fonction de la température.

Le croisement des courbes illustre l'existence d'une température, T = 427 K soit 154 ° C pour laquelle la condition d'accord de phase colinéaire est obtenue et à laquelle on doit donc maintenir le cristal. Expérimentalement, l'efficacité optimum de la source a été obtenue lorsque l'asservissement de température indiquait 142.5 °C. L'écart avec la valeur théorique attendue peut être dû aussi bien à un défaut de calibrage des capteurs thermiques qu'à

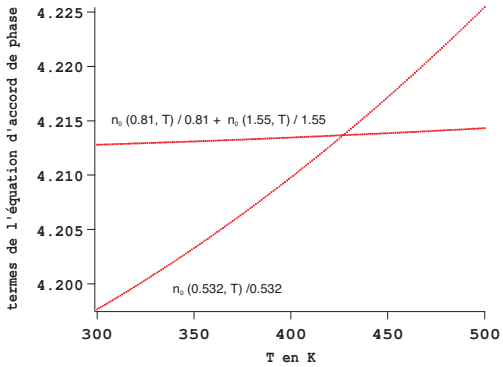

FIG. 8.2 – Dépendance des deux termes de l'équation (8.7) en fonction de la température

la non homogénéité de la température du cristal en présence du laser de pompe. Ce dernier effet, bien que difficilement quantifiable, est clairement présent car la température de consigne doit être ajustée de quelques dixièmes de degrès en fonction de la puissance du laser de pompe.

8.3.4 Optimisation du couplage et efficacité de collection

Nous présentons ici les calculs ayant été effectués afin d'optimiser l'efficacité de collection et d'évaluer la largeur spectrale de la source. Ces paramètres vont rentrer en ligne de compte pour l'échange de bits entre Alice et Bob car ils seront liés aux pertes des différents éléments du montage, au contraste de l'interféromètre utilisé et au rapport signal à bruit de la photodétection des photons annoncés à l'aide de photodiodes à avalanche InGaAs fonctionnant en mode déclenché.

Le paramètre que l'on cherchera à optimiser est la probabilité conditionnelle de détecter un photon à 1550 nm à partir d'un signal de déclenchement produit par une photodiode à avalanche détectant un photons 810 nm. Cette probabilité va constituer le nombre effectif moyen de photons par impulsion, et peut être atteindre une valeur proche de 1 sans mettre en danger la sécurité, assurant une importante amélioration du rapport signal à bruit par rapport au cas d'une source de photons basée sur un laser atténué [229]. Nous avons obtenu des résultats préliminaires avec une optique sub-optimale en juillet 2003, et avons ensuite effectué une étude plus précise des paramètres optiques de l'expérience.

Notre approche est calquée sur celle proposée par C. KURSIEFER *et al* [258], et nous avons basé nos calculs sur le papier de M.H RUBIN [261]. Le cristal est un cristal de 20 mm de $LiNbO_3$, dont l'accord de phase est de type 1. Ce cristal est placé dans un four, à la température de 380 K pour laquelle on obtient un accord de phase colinéaire. On fait de plus l'hypothèse (raisonnable dans notre cas ou les dimensions transverses des faisceaux ne sont pas trop faibles) que l'on peut négliger les effets transverses dans le calcul de l'accord de phase pour le processus de conversion paramétrique : 532 nm $\rightarrow$ 810 nm + 1550 nm.

Nous avons utilisé le logiciel SNLO [275] comme base de données concernant les propriétés optiques du $LiNbO_3$. Reprenant les notations du papier de Rubin, on a pu calculer :

$$\overline{K} = 12.03\mu m^{-1} \quad et \quad cD = 0.092 \tag{8.8}$$

où $\overline{K}$ est le vecteur d'onde « moyen » et où D désigne la différence entre les inverses des vitesses de groupes ordinaire et extraordinaires.

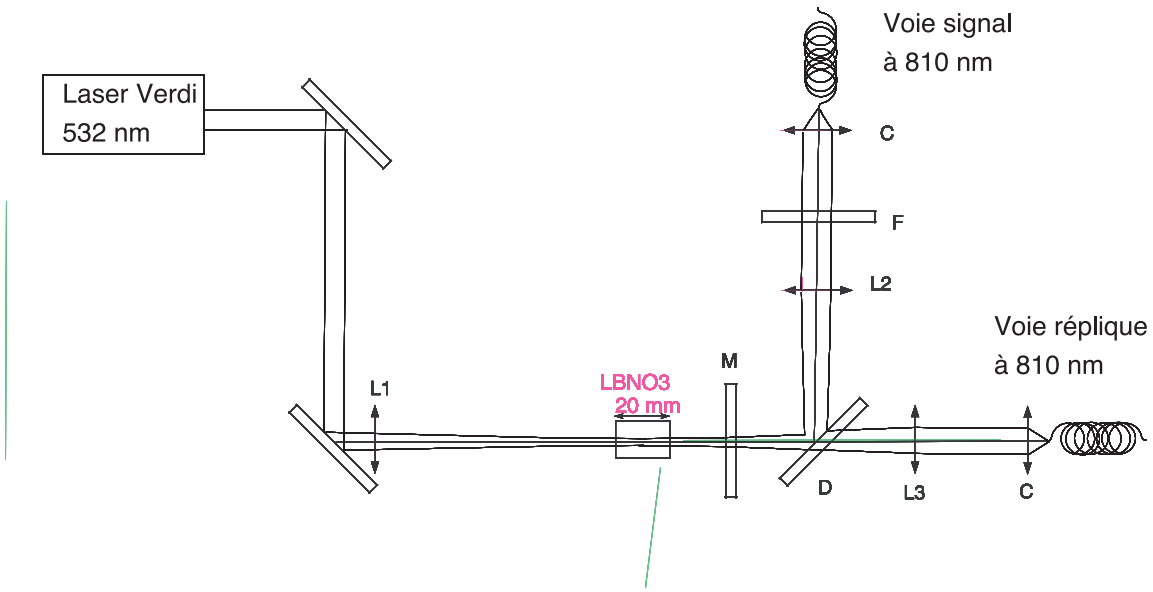

FIG. 8.3 – Montage expérimental : couplage des faisceaux signal (810 nm) et idler (1550 nm) dans des fibres monomodes. L1 : lentille de focale 100 cm, L2 et L3 : lentilles de focale 25 cm. D : miroir dichroïque de coefficient de réflexion 99 % à 810 nm et de transmission 85 % à 1550 nm. M : miroir interférentiel de haute reflectivité à 532 nm, utilisé pour bloquer la lumière de pompe. F : Filtre passe haut. C : coupleur basé sur une lentielle asphérique de focale 11 mm. Le waist du faisceau de pompe au niveau du cristal de $LiNbO_3$ est de 170 μm.

A partir de ces données et sachant que le laser de pompe est monochromatique à 532 nm, (laser Verdi de la marque Coherent), la largeur naturelle d'émission $\delta\lambda$ des photons paramétriques peut être calculée. On trouve respectivement :

$$\delta\lambda_{810} = \frac{2\lambda_{810}^2}{cDL} = 0.71\,\mathrm{nm} \tag{8.9}$$

et

$$\delta\lambda_{1550} = \frac{2\lambda_{1550}^2}{cDL} = 2.6\,\mathrm{nm} \tag{8.10}$$

Ainsi, le filtre de largeur 0.11 nm placé sur la voie à 810 nm réduit le spectre d'un facteur qui reste raisonnable, et préserve la possibilité d'avoir un flux de photons importants. Par ailleurs, sachant que la largeur spectrale du laser de pompe est très faible, la condition d'accord de phase (cf. equation 8.2) implique que le fait de filtrer spectralement la lumière sur la voie à 810 nm se répercute sur la largeur spectrale de la voie à 1550 nm.

Afin d'optimiser le couplage du faisceau à 1550 nm dans la fibre monomode, il convient ensuite d'évaluer l'ouverture angulaire du faisceau jumeau de celui des photons « trigs » à 810 nm. Là encore nos calculs se basent sur la référence [261]. Pour une largeur spectrale de 0.11 nm sur la voie à 810 nm, on calcule ainsi une ouverture angulaire de

$$\Delta\theta_{810} = 21.4\,\mathrm{mrad} \tag{8.11}$$

et

$$\Delta\theta_{1550} = 11.2\,\mathrm{mrad} \tag{8.12}$$

Nous avons calculé les valeurs des focales des différentes optiques en prenant en compte ces différents résultats. Le waist du faisceau de pompe au niveau du cristal de $LiNbO_3$ étant de 170 μm.

Comme espéré, nous avons obtenu une amélioration très significative des efficacité de collection et mesuré une probabilité conditionnelle de détection d'un photon à 1550 nm de près de 60 %, c'est-à-dire comparable aux meilleurs résultats reportés jusqu'à présent [229, 230].

Les taux de comptages étaient alors les suivants : pour 100 mW de pompe on détectait environ 100 000 photons / s sur la voie à 810 nm et 6000 coups/s sur la voie à 1550 nm (sachant que l'efficacité quantique de détection de la photodiode InGaAs avait préalablement été calibrée et valait alors 10 %).

L'efficacité conditionnelle de production de photons annoncés à 1550 nm est donc :

$$P(\text{photon sur la voie 1550 nm} \mid \text{clic sur la voie 810 nm}) \simeq \frac{6000}{100000 \times 0.1} = 60\% \qquad (8.13)$$

On peut néanmoins mentionner que l'importance des effets photoréfractifs dans les cristal de $LiNbO_3$ perturbe quelque peu le profil transverse des faisceaux qui le traversent et par la même l'efficacité de couplage, rendant instable notre efficacité de couplage. Un nouveau cristal, dopé au plomb va être utilisé prochainement afin de pouvoir s'affranchir de ces effets.

8.4 Système de distribution quantique de clé basé sur la source asymétrique

8.4.1 Photodétection à 1550 nm

La fenêtre télécom autour de 1550 nm s'impose naturellement pour la réalisation de cryptographie quantique à grande distance, en raison de la très faible atténuation dans les fibres optiques commerciales à cette longueur d'onde (environ 0.2 dB/ km pour les fibres récentes). En revanche, la limite technologique majeure des systèmes de cryptographie quantique actuelle provient des performances pour l'instant encore très imparfaites des détecteurs de photons uniques à 1550 nm. Ces derniers sont constitués de photodiodes à avalanche InGaAs, pour lesquels le courant d'obscurité est élevé.

Beaucoup d'efforts de recherche ont été menés pour améliorer la performance des détecteurs et, si l'on ne cherchera pas à rentrer dans le détail du fonctionnement des photodiodes à avalanche ici, on retiendra que les meilleurs rapport signal à bruit sont obtenus en refroidissant les photodiodes et en opérant en « gated mode », c'est à dire en mode déclenché, ou les photodiodes ne sont portées au voisinage de leur tension d'avalanche que durant un temps court, afin de limiter le taux de coups d'obscurité [239].

Un important travail d'ingénierie sur la photodétection à 1,55 μm a été effectué au sein de MagiQ, et nous sommes donc en mesure de détecter les photons uniques propagés à travers une fibre optique avec un rapport signal à bruit d'environ 50 dB, en opérant à -80° C, ce qui correspond à une efficacité quantique QE $\simeq$ 10 % et un taux de coups d'obscurité par fenêtre de 2 ns : $p_d \simeq 2 \times 10^{-6}$.

C'est dans ce régime de fonctionnement qu'on été réalisées les mesures présentées dans la section 8.5

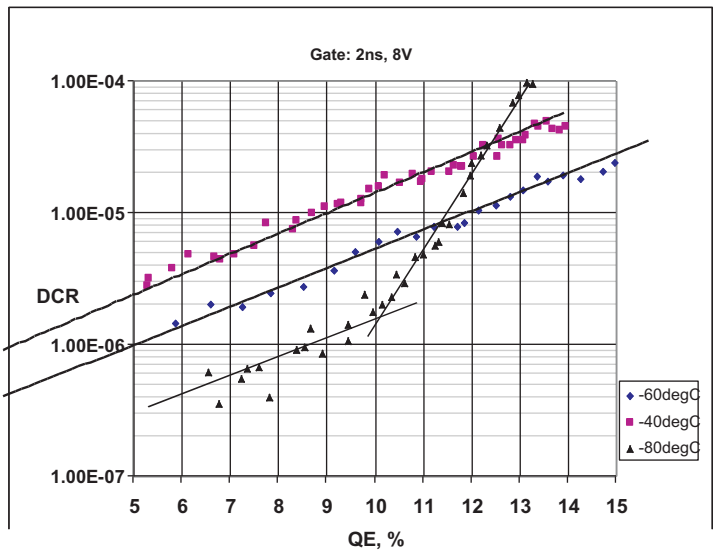

FIG. 8.4 – Performance des photodiodes à avalanche utilisées dans notre expérience : probabilité d'avoir un coup d'obscurité par timeslot, de 2 ns pour différentes valeurs de l'efficacité quantique (Données MAQIQ issues du travail de Darius SUBACIUS)

8.4.2 Mesure du spectre et influence de la dispersion

Une autre des clés de la réussite de l'expérience réside dans la limitation des effets de dispersion sur le signal quantique : en effet, du fait de la biréfringence, couplée à la dispersion des modes de polarisation les paquets d'onde s'élargissent au fur et à mesure de leur propagation. On évalue l'élargissement temporelle à typiquement 17 ps/nm/km, et l'effet est donc important pour les distances sur lesquelles nous souhaitons opérer, de l'ordre de 100 km.

Il y a deux raisons pour lesquels on souhaite limiter cet élargissement

- L'interféromètre utilise un codage phase-temps, avec des différences de chemin optique de l'ordre de 10 ns, si l'élargissement devient comparable à 10 ns, la visibilité des interférences de phase va s'effondrer ;
- Il est très important de limiter autant que possible la durée des fenêtres durant lesquelles les photodiodes InGaAs sont activées, afin de préserver un faible niveau de bruit et donc les performances de notre système.

Nous avons ainsi mesuré l'enveloppe temporelle des paquets d'onde avant et après la fibre optique afin de mesurer l'élargissement dû à la dispersion. Ceci constitue une mesure indirecte, mais néanmoins relativement précise de la largeur spectrale de notre source. L'élargissement mesuré, de l'ordre de 600 ps nous indique que la largeur spectrale des photons à 1550 nm est de 0.47 nm, valeur tout à fait en accord avec ce que l'on attendait (i.e un spectre environ 4 fois plus large que la bande spectrale sélectionnée sur le faisceau à 810 nm, qui est elle de 0.11 nm). En sortie de fibre, l'enveloppe de 1.3 ns reste compatible avec un fonctionnement efficace des photodiodes à avalanche.

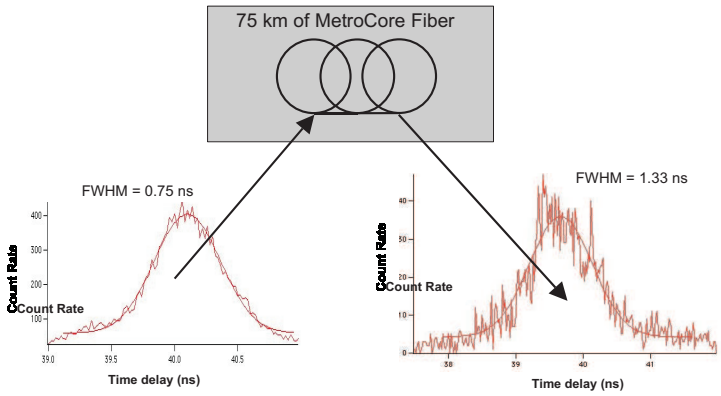

FIG. 8.5 – Enveloppe temporelle des photons sur le canal quantique avant et après propagations dans 76 km de fibre optique. L'enveloppe temporelle des coïncidences 810 nm / 1550 nm est mesurée en variant le retard électronique relatif entre les deux voies. Sur la figure de droite, l'enveloppe temporelle est mesurée directement en sortie de la source de photons annoncés. Sa largeur est limitée par la gigue de 700 ps de la photodiode au silicium placée sur la voie à 810 nm. La figure de gauche est mesurée après 76 km de propagation dans une fibre monomode SMF -28. L'élargissement temporel mesuré est en très bon accord avec la dispersion causée par la fibre, typiquement de 17 ps/nm/km.

8.5 Application à la cryptographie quantique et évaluation des performances envisageables

8.5.1 Statistique de la source

Il est important de comprendre que la statistique conditionnelle du nombre de photons annoncés par impulsion est fortement sub-poissonnienne. Reprenons pour cela les chiffres relatifs à notre expérience :

Pour 100 mW de pompe on détecte environ 100 000 photons/s sur la voie à 810 nm et 6000 coups/s sur la voie à 1550 nm, pour une efficacité quantique de détection de la photodiode InGaAs mesurée de 10 % et une largeur de fenêtrage de 2 ns. La statistique des photons émis par émission paramétrique est thermique [25] et, pour un temps d'intégration donné, la probabilité $\mathcal{P}(2)$ d'émettre deux photons vaut approximativement $\mathcal{P}(1)^2$ tant que $\mathcal{P}(0)$ est proche de 1, comme c'est le cas dans notre réalisation de source de photons annoncés.

Dès lors, sachant qu'une impulsion lumineuse n'est pas vide, la probabilité pour que deux paires soient émises dans la fenêtre de photodétection correspondante est d'environ $10^5 \times 2\,.10^{-9} = 0.02\%$. Il a d'ailleurs été récemment mis en évidence expérimentalement que la statistique du nombre de photons dans des impulsions conditionnées permet d'obtenir des valeurs de $g^{(2)}(0)$ extrêmement basses [231].

8.5.2 Cryptographie quantique à l'aide d'un interféromètre en phase « One - Way »

Nous avons utilisé un interféromètre de type Mach-Zehnder, pour effectuer un codage en phase de l'information quantique sur les photons uniques produits par notre source. Cet interféromètre a été entièrement réalisé par Anton ZAVRIYEV et Darius SUBACIUS avant

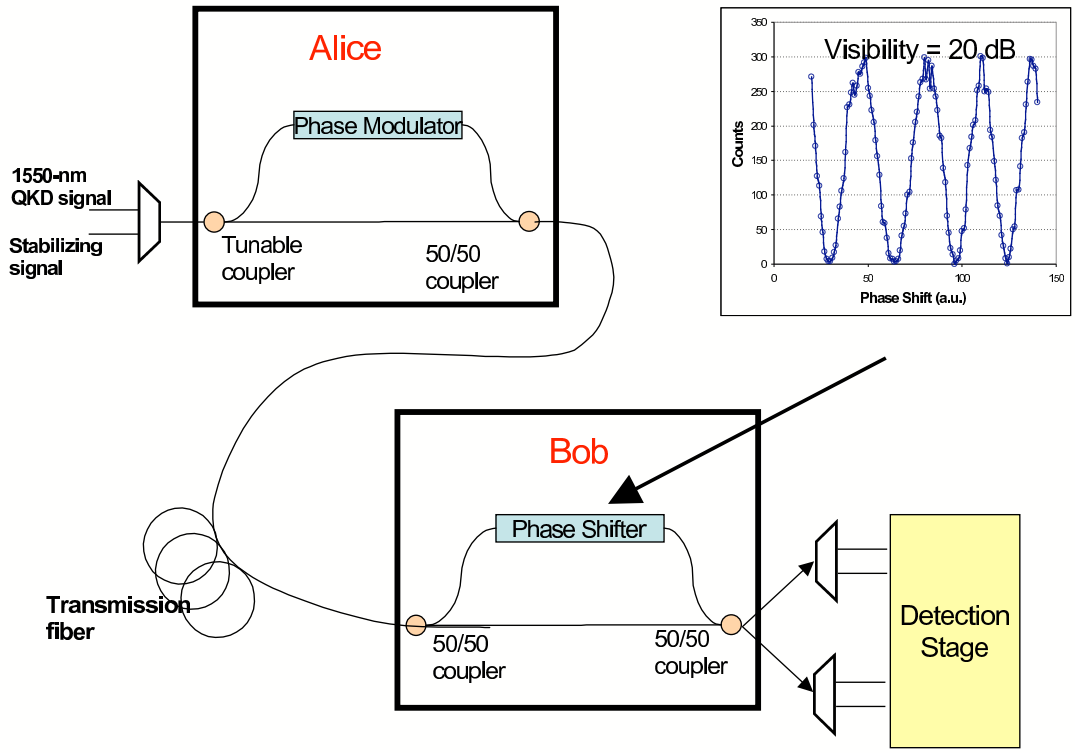

FIG. 8.6 – Interféromètre utilisant un codage en phase et muni d'un dispositif de stabilisation active. En l'absence d'atténuation sur le canal quantique, nous avons mesuré un contraste de plus de 20 dB, directement sur les photons produits par la source de photons annoncés.

mon arrivée à MagiQ. Un tel interféromètre « à un passage » nécessite une stabilisation active des deux bras, également mise au point par Anton ZAVRIYEV et Darius SUBACIUS .

Le schéma de l'interféromètre est représenté à la figure 8.6 et l'on reverra le lecteur à la référence [28] pour une explication plus détaillée de son principe.

L'idée est qu'Alice peut choisir 2 bits aléatoires correspondant à un choix de base et à un codage binaire, la combinaison de ces deux bits codant pour l' une des quatre valeurs $\{0, \Pi/2, \Pi, 3\Pi/2\}$ de la modulation en phase tandis que Bob décode en choisissant aléatoirement la base dans laquelle il effectue sa détection à l'aide du « phase shiflter »dont la modulation de phase est choisie aléatoirement parmi $\{0, \Pi/2\}$. La valeur binaire enregistrée par Bob dépend alors de l'indice de la photodiode qui clique. Les pertes totales de l'interféromètres ont été mesurées sur le signal quantique et sont de 14 dB, ce qui est relativement élevé étant donnée que les pertes intrinsèques de cet interféromètre sont de 6 dB.

Nous avons caractérisé le taux d'erreur de notre interféromètre de phase *sur notre signal quantique* et mesuré un taux d'extinction supérieur à 20 dB, i.e correspondant à un taux d'erreur en l'absence de pertes de moins de 1 % (cette mesure est réalisée pour une faible longueur de fibre).

8.5.3 Fonctionnement du système pour 76 km de propagation et évaluation des performances

Nous concluerons cette partie en décrivant les mesures de taux d'erreur effectuée en utilisant un canal quantique de 76 km de fibre optique. Cette mesure permet de discuter des performances envisageables d'un système de cryptographie quantique basé sur notre source de photons uniques.

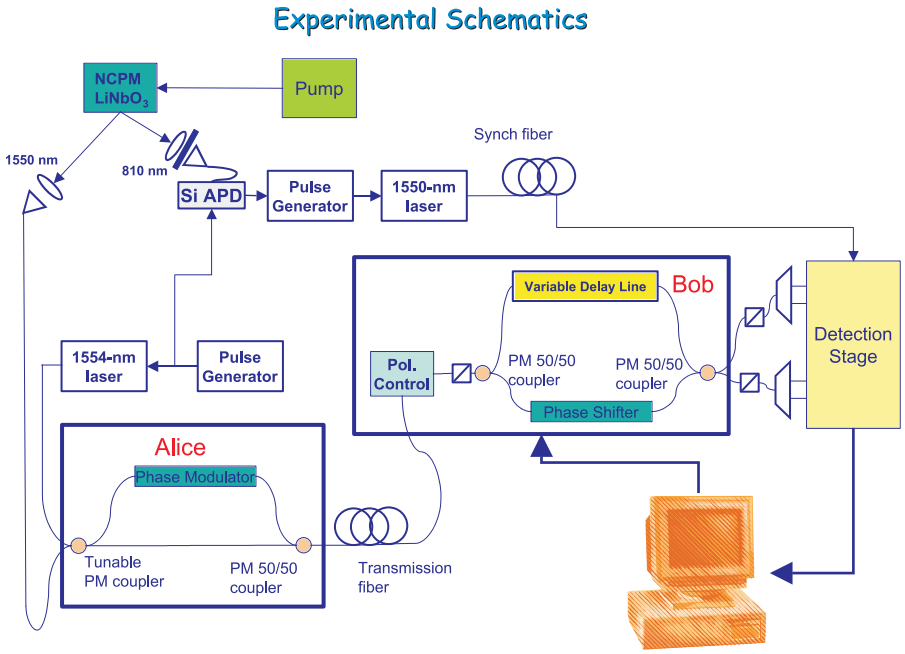

FIG. 8.7 – Dispositif expérimental pour la mesure du taux d'erreur sur une distance de 76 km

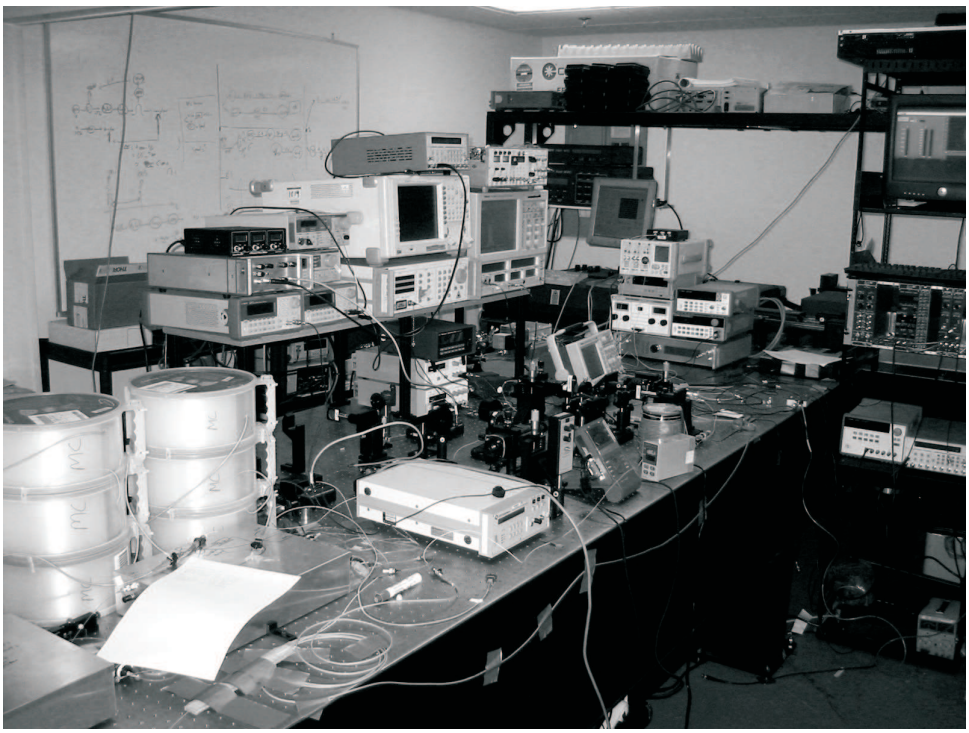

FIG. 8.8 – Photo de l'expérience réalisée sur une distance de 76 km de fibre optique (on voit les rouleaux de 3 bobines de 25 km, l'un des rouleaux étant utilisé pour envoyer le signal de synchronisation).

Nous avons échangé de l'information codée sur les photons annoncés issus de la source décrite précédemment à l'aide de l'interféromètre à un passage stabilisé activement et du système de photodétection construit à cet effet par Darius SUBACIUS. Nous sommes parvenus à échanger de l'information avec un taux d'erreur de l'ordre de 10 %, à une cadence de l'ordre de 3 Hz, pour une distance de propagation de 76 km. On peut montrer [185], qu'un tel régime de fonctionnement permet d'assurer la distribution quantique de clé de façon sécurisée contre l'attaque PNS. Nous avons utilisé ce même modèle de sécurité pour comparer les performances du *même système de modulation et de détection* utilisant soit une source de photons annoncés (SPS), soit une source d'impulsions cohérentes atténuées. Nous avons pour cela utilisé une valeur $\mu = 0.1$ pour notre source de photons uniques, correspondant au nombre moyen de photons par impulsion annoncées, *à la sortie du dispositif d'Alice*, dont les pertes sont de 7.5 dB. Les résultats de cette comparaison sont présentés sur la figure 8.6.

8.6 Conclusion

Il apparaît clairement sur la figure 8.6 que l'utilisation d'une source de photons uniques permet d'obtenir, à grande distance, des performances substantiellement supérieures à celles autorisées par l'utilisation d'impulsions laser atténuées. L'option que nous avons choisie – si l'on compare notre travail à celui effectué dans le groupe de Nicolas GISIN – c'est-à-dire l'utilisation de filtres spectraux très sélectifs, permet de limiter les effets dus à la dispersion chromatique dans la fibre. Une approche alternative consisterait à compenser la dispersion à l'aide de fibre à coefficient de dispersion negatif [230].

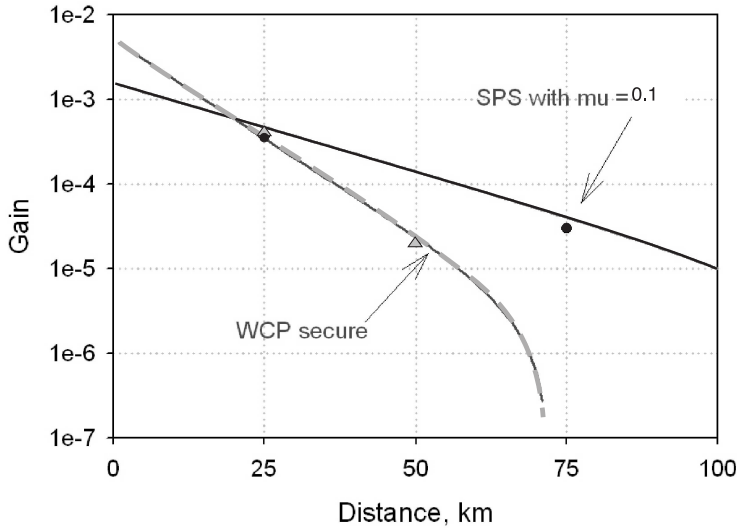

FIG. 8.9 – Comparaison des performances du dispositif décrit dans la figure 8.5.3 en fonction de la distance de propagation, dans le cadre du modèle de sécurité décrit dans la référence [185]. La courbe noire en trait plein représente la performance de la source de photons uniques (SPS) dont le nombre moyen équivalent de photons par impulsion est de 0.1 (voir texte). La courbe grisée, en pointillé, représente les performances accessibles à l'aide d'impulsions cohérentes atténuées. Ces courbes théoriques sont calculées à partir des mesures expérimentales correspondant aux point placés sur la figure : triangles gris pour les impulsions cohérentes atténuées et cercles noirs pour les mesures réalisées à partir de la source de photons annoncés.

Chapitre 9

Conclusion générale et perspectives

Au cours de ces dernières années, les idées novatrices mises en jeu dans le domaine du *traitement quantique de l'information* [21] ont conduit à de nombreux développements théoriques et expérimentaux pour les *communications quantiques*, permettant de transmettre de l'information à distance – essentiellement par voie optique – d'une façon qui n'a pas d'analogue dans le domaine des communications classiques. La progression et les découvertes des techniques associées à ces communications quantiques sont conditionnées par les résultats des recherches obtenues à différents niveaux. Elles nécessitent en particulier :

1. Des éléments matériels permettant de produire des états spécifiquement quantiques, support d'information, et de les détecter de façon efficace.
2. Des dispositifs de codage de l'information sur ces états quantiques, adaptés au milieu envisagé pour la propagation.
3. L'établissement de protocoles de communication spécifiques, accompagnés de l'évaluation théorique de leurs capacités.

Les différents travaux abordés au cours de cette thèse, sont essentiellement consacrés au premier de ces points et plus particulièrement à la réalisation expérimentale de sources de photons uniques dont nous avons présenté les applications potentielles aux communications quantiques au chapitre 2. Nous avons ainsi travaillé à la mise au point de sources de photons uniques fonctionnant à température ambiante. Nous avons ainsi montré qu'il était possible, en contrôlant temporellement la fluorescence d'un émetteur individuel, d'émettre efficacement, de façon déclenchée, des impulsions contenant un seul photon. Nous avons également travaillé à la mise au point d'une source de photons annoncés, fondée sur la préparation conditionnelle d'états à un photon à partir de paires de photons émises par fluorescence paramétrique dans un cristal non-linéaire $\chi^{(2)}$. Nous avons complété ces travaux expérimentaux sur les sources de photons uniques par une étude des propriétés statistiques de la lumière émise par de telles sources, en développant une méthode d'analyse des enregistrement expérimentaux effectués en régime de comptage de photons [75].

Les collaborations avec l'équipe de Philippe GRANGIER au laboratoire Charles Fabry de l'Institut d'Optique, ainsi que le stage de recherche effectué au sein de la start-up MAGIQ nous ont permis d'élargir notre travail de thèse. Nous avons appliqué les sources de photons uniques réalisées à la mise en œuvre de dispositifs de distribution quantique de clé, technologie qui constitue l'application la plus mûre des recherches effectuées sur les communications quantiques. En prolongeant le travail de thèse d'Alexios BEVERATOS [86], nous avons ainsi étudié, en conditions « réelles » d'utilisation, les performances d'un système

complet de distribution de clé fonctionnant en espace libre avec une source déclenchée de photons uniques. Nous avons ainsi démontré sa fiabilité et son intérêt en vue d'un échange de clé à grande distance [234]. Le travail réalisé chez MAGIQ nous a quant à lui permis d'optimiser les performances d'une source de photons annoncés pour un système de cryptographie quantique à grande distance sur des fibres optiques. Les résultats préliminaires obtenus démontrent les gains de performance autorisés par l'usage d'une telle source, par rapport à l'emploi de simples impulsions laser atténuées [235].

Quelques perspectives pour les sources de photons uniques

Comme nous l'avons expliqué au chapitre 2, la plupart des applications des sources de photons uniques aux communications et au calcul quantique – en dehors de la cryptographie quantique– nécessitent que les photons émis par la source soient indiscernables. En outre, même si cette condition n'est pas strictement nécessaire pour effectuer des distributions quantiques de clé, l'utilisation de paquets d'onde cohérents à un photon permettrait de se rapprocher des hypothèses sur lesquelles se basent les preuves de sécurité inconditionnelle en cryptographie quantique. Il est donc raisonnable de penser que l'un des défis importants est bien de réaliser des sources de photons uniques indiscernables, comme le confirment dès à présent les premiers résultats obtenus avec des boîtes quantiques d'InAs en microcavité [112] ou avec des atomes piégés [133].

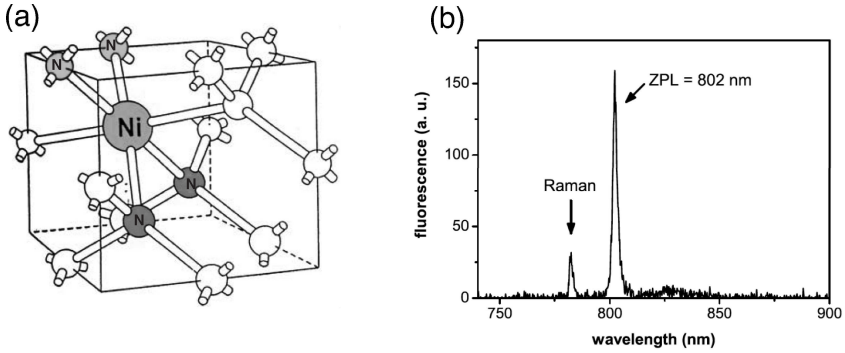

FIG. 9.1 – **(a)** Centre coloré NE8 dans la maille cristalline du diamant. Le centre NE8 est un complexe associant un atome de nickel et 4 atomes d'azote voisins. **(b)** Spectre de fluorescence du centre NE8 excité par un laser continu à la longueur d'onde de 710 nm. Ces figures sont extraites de la référence [93] .

En ce qui concerne l'utilisation de la fluorescence de systèmes moléculaires, le travail très récent mené dans le groupe d'Adreas ZUMBUSCH à Munich montre qu'il est possible d'obtenir une émission cohérente par une molécule unique, en excitant de façon non-résonnante une molécule unique de terrylène à basse température et en filtrant l'émission de fluorescence sur la raie à zéro phonon [80]. Les centres colorés du diamant pourraient conduire à l'émission de photons uniques indiscernables. En effet, un nouveau centre coloré du diamant a été détecté récemment comme nano-objet unique. Il s'agit plus précisément du centre NE8, correspondant à un défaut dans la maille cristalline du diamant composé d'un complexe nickel-azote. Nous avons représenté sur la figure 9.1 la structure chimique ainsi que le spectre d'un centre coloré NE8, enregistré à température ambiante. La caractéristique la plus frappante de ce centre est sa très faible largeur spectrale d'émission, de seulement 1.2

nm, concentrée même à température ambiante dans la raie à zéro phonon [93]. Cette caractéristique permet d'envisager la génération de photons uniques indiscernables à basse température, par une excitation non-résonnante de la photoluminescence.

Quelques perspectives de recherche en cryptographie quantique

La rapidité avec laquelle progressent les expériences et les systèmes consacrés à la distribution quantique de clé rendrait probablement caduque toute tentative d'en prédire aujourd'hui le devenir. La feuille de route [30], rédigée en 2004 par des spécialistes du domaine, permet néanmoins de dégager quelques lignes directrice, aussi renvoyons-nous le lecteur à cette référence pour ce qui est des probables étapes futures du développement de ce domaine de recherche.

Il est par ailleurs récemment apparu que de très importants gains de performances sont possibles d'une part grâce aux progrès des preuves théoriques de sécurité et d'autre part en imaginant de nouveaux protocoles ou des variantes permettant de contourner certaines difficultés. C'est en particulier le cas pour le protocole BB84 avec des impulsions cohérentes atténuées qui, grâce à une modification de l'étape de réconciliation, peut être rendus beaucoup plus résistants aux attaques envisagées jusqu'à présent [184]. Enfin, nous avons pris connaissance, peu de temps avant la fin de la rédaction de ce manuscrit, d'un nouveau protocole, utilisant des états baptisés « Decoy States », obtenus en variant aléatoirement l'intensité d'impulsions cohérentes de faible nombre moyen de photons. Ce protocole semble être en mesure de faire progresser de façon significative les performances expérimentales des systèmes de distribution quantique de clé, rendant accessibles des distances de propagation de l'ordre de 150 km tout en maintenant le critère de sécurité inconditionnelle [200].

Une autre perspective de recherche en cryptographie quantique est de dépasser le cadre simple du partage de clé entre deux utilisateurs et d'élargir les protocoles et les systèmes expérimentaux à la distribution de secret au sein d'un réseau comportant plusieurs utilisateurs. Un tel travail, pour lequel quelques propositions ont déjà été formulées [199], est au cœur du projet européen SECOQC (SEcure COmmunication based on Quantum Cryptography). Ce programme de recherche, qui regroupe 41 unités de 12 pays vise à doter l'Union Européenne d'un réseau global de communication sécurisées fondé sur la cryptographie quantique.

Annexe A

Source déclenchée : resynchronisation des instants de photodétection

Nous avons mis au point un traitement numérique adapté des données brutes relatives à la statistique d'émission d'une source de photons uniques, telles qu'elles sont collectées par le TIA (cf chapitres 3 et 4) qui enregistre la liste chronologique des instants de photodétection.

En régime d'excitation impulsionelle, les instant d'émission ne sont pas entièrement aléatoires : la périodicité de la lumière excitatrice se répercute sur le train de photons émis par la molécule unique. On peut donc tirer partie de cette caractéristique dans l'analyse des données enregistrées à l'aide du TIA. Les données consistent en une liste d'instants de photodétection $\{t_i\}$ dont l'acquisition débute à l'ouverture de l'obturateur placé sur le faisceau d'excitation. Nous décrivons ici la procédure de traitement de ces données brutes que nous avons élaboré. Elle permet de synchroniser les $\{t_i\}$ sur une horloge correspondant aux impulsions excitatrices, puis de construire la liste $\{n_p\}$ du nombre de photons détectés pour chaque impulsion p.

Le laser d'excitation joue le rôle d'une horloge de période $\tau_{\mathrm{rep}} \simeq 488$ ns (pour une excitation à 2.05 MHz, comme dans le cas des données traitées dans le chapitre 4). On peut donc écrire les instants correspondants à l' impulsions d'excitation p sous la forme $t_{\mathrm{start}} + p \times \tau_{\mathrm{rep}}$. t_{start} dénote l'instant d'émission de l'impulsion laser pour laquelle la première photodétection intervient ($p = 0$).

Les valeurs t_{start} and τ_{rep} doivent être déterminées pour chaque nouvel ensemble de données car la période de répétition du laser Ti :Sa peut fluctuer légérèment entre deux acquisitions. On peut néanmoins considérer que la période τ_{rep} est stable à l'échelle d'une acquisition (dont la durée est inférieure à la seconde).

L'émission de photons uniques par la molécule suit l'impulsion d'excitation avec un délai aléatoire distribué suivant la durée de vie de l'état excité de la molécule. Il existe de plus des événements non synchrones, imputables aux coups d'obscurité des photodiodes à avalanche. De tels événements sont cependant rares dans les expériences décrites dans cette thèse où le rapport signal à bruit est très supérieur à 1, si bien que la quasi totalité des photodétections sont dues à l'émission de photons uniques par la molécule et dans une moindre mesure au fond de fluorescence. Comme par ailleurs la durée de vie de la molécule (2-3 ns) est courte devant la période de répétition du laser ($\simeq$ 488 ns), la seule donnée des $\{t_i\}$ est suffisante pour effectuer une post-synchronisation, c'est à dire déterminer t_{start} et τ_{rep} à partir de $\{t_i\}$.

Le i [e]instant de photodétection, t_i peut être exprimé sous la forme :

$$t_i = t_{\text{start}} + (p_i \times \tau_{\text{rep}}) + \delta\tau_i, \tag{A.1}$$

L'entier $p_i \in \{1, \ldots, \mathcal{N}\}$ est l'indice de l'impulsion excitatrice précédant la détection du i^{eme} photon et les données analysées s'étendent sur $\mathcal{N}$ périodes d'excitation. Par ailleurs, $\delta\tau_i$ représente l'intervalle de temps séparant l'impulsion excitatrice de l'instant de photodétection ($0 \leq \delta\tau_i < \tau_{\text{rep}}$).

Ainsi, la donnée de l'ensemble $\{t_i\}$ peut être exprimée de façon équivalente sous la forme des ensembles $\{p_i\}$ et $\{\delta\tau_i\}$ à partir du moment où la valeur τ_{rep} est connue avec suffisamment de précision. On aura d'ailleurs $\delta\tau_i \ll \tau_{\text{rep}}$ pour les événement autres que les coups d'obscurité.

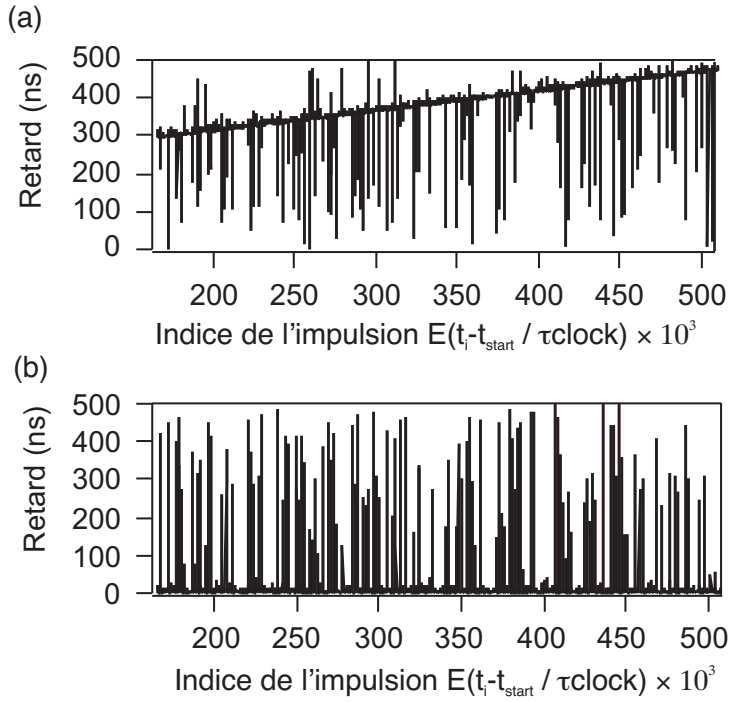

FIG. A.1 – Procédure de synchronisation des instants de photodétection $\{t_i\}$: on s'intéresse à la valeur du retard $\text{Delay}(t_i)$ en fonction de l'indice de l'impulsion excitatrice $E[(t_i - t_{\text{start}})/\tau_{\text{clock}}]$ pour un couple de paramètres t_{start} et τ_{clock}. (a) Cas où τ_{clock} est proche de τ_{rep}, ce qui entraine une petite dérive linéaire de la valeur du retard. En revanche la valeur de t_{start} est incorrecte. (b) Cas où $\tau_{\text{clock}} = \tau_{\text{rep}}$ avec un précision relative atteignant 10^{-9} et où t_{start} est correctement évalué.

Comme la période de répétition du laser n'est pas connue avec précision, nous procédons à une première évaluation du décalage des instants de photodétection par rapport à une horloge de période τ_{clock} proche de la valeur attendue (488 ns). Nous introduisons pour cela un fonction "retard" qui dépend des paramètres t_{start} et τ_{clock} et qui permet d'évaluer l'intervalle de temps séparant chaque instant de photodétection du top d'horloge qui l'a précédé (la notation $E()$ désigne la fonction partie entière).

$$\text{Retard}_{t_{\text{start}},\tau_{\text{clock}}}(t_i) = t_i - t_{\text{start}} - E\left(\frac{t_i - t_{\text{start}}}{\tau_{\text{clock}}}\right) \times \tau_{\text{clock}}, \tag{A.2}$$

L'intérêt de l'évaluation de la fonction Retard dans le processus d'ajustement vient du fait que pour un petit écart entre la période de répétition du laser et de de l'horloge, cette fonction Retard va dériver linéairement, comme le montre l'équation A.3. On retrouve ce comportement sur la figure A(a).

$$\mathrm{Retard}_{t_{\mathrm{start}},\tau_{\mathrm{clock}}}(t_i) \simeq p_i(\tau_{\mathrm{rep}} - \tau_{\mathrm{clock}}) \simeq \frac{t_i}{\tau_{\mathrm{rep}}}\left(\tau_{\mathrm{rep}} - \tau_{\mathrm{clock}}\right). \tag{A.3}$$

Dès lors, la pente de la fonction retard permet d'inférer une nouvelle valeur de τ_{clock} se rapprochant de la valeur réelle de τ_{rep}. En pratique, la valeur initiale choisie pour τ_{clock} est généralement assez éloignée de la période de répétition du laser, si bien que la fonction retard a une forme en dents de scie et que seule une fraction des données peuvent être utilisées pour évaluer une nouvelle valeur. Lors des étapes suivantes, réalisées de manière itérative l'estimation de τ_{rep} s'affine et permet d'utiliser une fraction plus importantes des données, jusqu'a atteindre la situation de la figure A(a) ou l'évaluation se fait sur la totalité des données, amenant alors à la situation de la figure A(b) où la valeur τ_{rep} est fixée avec une précision relative supérieure à 10^{-9}.

Une fois que les valeurs τ_{rep} et t_{start} sont connues, le calcul de $\{p_i\}$ et $\{\delta\tau_i\}$ se fait de manière directe :

$$p_i = E\left(\frac{t_i - t_{\mathrm{start}}}{\tau_{\mathrm{rep}}}\right) \text{ and } \delta\tau_i = \mathrm{Retard}_{t_{\mathrm{start}},\tau_{\mathrm{rep}}}(t_i). \tag{A.4}$$

A ce stade du traitement des données nous pouvons éliminer les évènements de photodétection intervenants à des retards très supérieurs à la durée de vie de l'état excité de la molécule. Cette procédure de filtrage consiste en un fenêtrage de durée $\Delta T_{\mathrm{window}}$ qui doit être choisi plus court que la période de répétition du laser et beaucoup plus long que la durée de vie des molécules(on a $1/\Gamma \simeq 2.5$ ns pour les molécules du colorant DiIC_{18}(3)). Nous avons choisi de fixer comme valeur $\Delta T_{\mathrm{window}} = 30$ ns, éliminant ainsi 94 $\%$ des coups d'obscurité tout en conservant plus de 99,9 $\%$ des évènements de photodétection "réels".

Au final, les données traitées se résument à une série de valeurs discrètes $\{n_i, p_i\}$ désignant le nombre de photodétections intervenues dans chaque fenêtre de 30 ns suivant une impulsion d'excitation. Ces données traitées, que l'on notera aussi $\{n_p\}$ serviront de point de départ pour caractériser la statistique de notre source de photons uniques sur une large gamme temporelle (de $\tau_{\mathrm{rep}} \simeq 500$ ns jusqu'à des échelles de temps de plusieurs millisecondes).

Annexe B

Dérivation de l'expression de la variance du nombre de photons produits par une source intermittente pulsée

B.1 Paramètres du modèle

On s'interesse ici à l'effet de l'intermittence de l'émission lumineuse d'une molécule unique sur les fluctuations du nombre de photons qu'elle produit pendant une durée T, i.e un nombre N de pulses ($T = N * \tau$).
On considère le cas d'une excitation et d'une détection parfaite (100 %).
Ainsi le système est entièrement décrit à l'aide d'un système à 2 niveaux, ON et OFF, couplés entre eux. Les paramètres du couplage, pour le système "physique" moléculaire sont :

- **K** qui est la probabilité de *croisement inter-système* , probabilité pour que la molécule passe de l'état excité et optiquement actif S^1, à l'état triplet noir T quittant ainsi l'état ON.
- le temps de vie du triplet, noté ici **1/q** caractérisant le retour de l'état OFF à l'état ON.

En régime pulsé, le temps est discrétisé et les pulses ont lieu aux temps $t_k = k * \tau$. On peut alors symétriser la description de la molécule, et la considérer comme une source qui passe de ON à OFF avec une probabilité **p** par unité de temps (avec $p * \tau = K$) et de OFF vers ON avec une probabilité **q** par unité de temps.

On choisit comme variable décrivant l'état du système, la probabilité u_k pour que la molécule soit dans l'état ON *juste après l'arrivée du kième pulse*.

On peut alors écrire l'intensité de fluorescence de la molécule sous la forme :

$$I(t) = \sum_{k=-\infty}^{+\infty} \delta(t - k * \tau) * r_k \tag{B.1}$$

Où l'on a introduit la variable aléatoire r_k qui prend la valeur 1 avec la probabilité u_k, et 0 avec la probabilité $1 - u_k$. Dans notre modèle sans bruit de fond, r_k est le nombre de photons produits par la source au pulse k.

B.2 Evolution du système

On peut facilement écrire une équation de récurrence sur les probabilités u_k :

$$u_{k+1} = (1 - p\tau) * u_k + q\tau * (1 - u_k)$$

Rigoureusement il faudrait remplacer $q\tau$ par $1 - e^{-q\tau}$ mais comme on travaille dans un régime où $q\tau << 1$ cela changerait peu les résultats.

On résoud cette équation en se fixant une condition initiale u_0 :

$$u_k = (u_0 - \frac{q}{p+q}) * (1 - p\tau - q\tau)^k + \frac{q}{p+q}$$

On posera $\alpha = 1 - p\tau - q\tau$ dans la suite du calcul. Le système présente un effet de mémoire de la valeur de u_0 sur une durée $1/ln(\alpha)$.

B.3 Nombre moyen de photons détectés durant une fenêtre de durée T

On note ce nombre $< n >=< \int_0^T dtI(t) >$.
En utilisant l'expression (B.1), et comme ($T = N * \tau$), on a

$$< n >=< \sum_{k=0}^{N-1} r_k >$$

$<>$ désigne la valeur moyenne prise sur un ensemble statistique de fenêtres de taille T, c'est à dire la moyenne sur un ensemble supposé infini (ceci ne peut être le cas dans l'expérience où les molécules blanchissent, mais la limite trouvée dans ce calcul s'appliquera à l'expérience si le nombre de fenêtres indépendantes que l'on peut extraire des données est suffisamment grand).

Comme il existe un élément de cohérence entre les valeurs de u_k et donc de r_k pour une même fenêtre, on commence par moyenner sur la valeur de u_0 (qui vaut 1 avec une proba $\frac{q}{p+q}$ et 0 avec une proba $\frac{p}{p+q}$). Puis on utilise le fait que l'espérance de r_k, $< r_k >$ est u_k (supposant connue la valeur u_0).

Ainsi,

$$
\begin{aligned}
< n >=< \textstyle\sum_{k=0}^{N-1} r_k > &= \frac{p}{p+q} < \sum_{k=0}^{N-1} r_k >_{|u_0=0} + \frac{q}{p+q} < \sum_{k=0}^{N-1} r_k >_{|u_0=1} \\
&= \frac{p}{p+q}(-\frac{q}{p+q})\frac{1-\alpha^n}{1-\alpha} + N\frac{pq}{(p+q)^2} + \frac{q}{p+q}(\frac{p}{p+q})\frac{1-\alpha^n}{1-\alpha} + N\frac{q^2}{(p+q)^2} \\
&= N\frac{q}{p+q}
\end{aligned}
\tag{B.2}
$$

B.4 Calcul de la variance

On connaît la valeur de $< n >$, il reste à calculer $< n^2 >$. De façon similaire à $< n >$, on aura :

$$< n^2 >=< \sum_{k,k'=0}^{N-1} r_k\, r_{k'} >$$

On distinguera dans la somme les termes indentiques :

$$< \sum_{k=k'=0}^{N-1} r_k\, r_{k'} >=< \sum_{k=0}^{N-1} r_k^2 >=< n > \qquad\qquad (r_k^2 = r_k)$$

Il reste donc à calculer :

$$< \sum_{k\neq k'}^{N-1} r_k\, r_{k'} >$$

Choisir une fenêtre dans une distribution statistique de fenêtres revient à choisir des fenêtres où l'on $u_0 = 0$ avec une probabilité $\frac{p}{p+q}$ et des fenêtres où l'on $u_0 = 1$ avec une probabilité $\frac{q}{p+q}$.

$$
\begin{aligned}
< \textstyle\sum_{k\neq k'}^{N-1} r_k\, r_{k'} > &= \frac{p}{p+q} < \sum_{k\neq k'}^{N-1} r_k\, r_{k'} >_{|u_0=0} + \frac{q}{p+q} < \sum_{k\neq k'}^{N-1} r_k\, r_{k'} >_{|u_0=1} \\
&= \frac{p}{p+q} \sum_{k\neq k'}^{N-1} < r_k\, r_{k'} >_{|u_0=0} + \frac{q}{p+q} \sum_{k\neq k'}^{N-1} < r_k\, r_{k'} >_{|u_0=1}
\end{aligned}
\tag{B.3}
$$

Il reste à calculer les termes de correlation $< r_k\, r_{k'} >_{|u_0=0,1}$. Pour $k' > k$ on pose $k' = k+l$ et l'on peut écrire exactement les différents termes sachant que le produit $r_k\, r_{k'}$ ne prend une valeur non nulle que si r_k et $r_{k'}$ sont égaux à 1 :

$$< r_k\, r_{k+l} >_{|u_0=0} = \; u_{k\,|u_0=0} * u_{k+l\,|u_k=1} = \frac{q(1-\alpha^k)}{p+q} * \frac{p\alpha^l + q}{p+q}$$

et

$$< r_k\, r_{k+l} >_{|u_0=1} = \; u_{k\,|u_0=1} * u_{k+l\,|u_k=1} = \frac{p\alpha^k + q}{p+q} * \frac{p\alpha^l + q}{p+q}$$

Il reste à effectuer la sommation :

$$< \sum_{k\neq k'}^{N-1} r_k\, r_{k'} >= \frac{p}{p+q} \sum_{k=0}^{N-1} 2 \sum_{l=1}^{N-1-k} \{\frac{q(1-\alpha^k)}{p+q} * \frac{p\alpha^l + q}{p+q}\} \; + \; \frac{q}{p+q} \sum_{k=0}^{N-1} 2 \sum_{l=1}^{N-1-k} \{\frac{p\alpha^k + q}{p+q} * \frac{p\alpha^l + q}{p+q}\}$$
$$= N(N-1)\frac{q^2}{(p+q)^2} + 2\frac{pq}{(p+q)^2}\{N\frac{\alpha}{1-\alpha} - \frac{\alpha}{1-\alpha}\frac{1-\alpha^N}{1-\alpha}\} \tag{B.4}$$

Finalement, en regroupant les termes et en soustrayant le carré de la valeur moyenne, on en déduit l'expression de la variance

$$< n^2 > - < n >^2 = \frac{pq}{(p+q)^2} \;\; \{N\frac{1+\alpha}{1-\alpha} - -2\alpha\frac{1-\alpha^N}{(1-\alpha)^2}\}$$

Finalement, en posant $\beta = (p+q)\tau_{\mathrm{rep}}$, on obtient la forme exact du paramètre de Mandel dépendant du temps pour le système ON-OFF :

$$Q_{\mathrm{S}}(\mathcal{M}\tau_{\mathrm{rep}}) = \frac{p}{p+q}\big(\frac{2-\beta}{\beta} - \frac{2(1-\beta)}{\mathcal{M}}\frac{1-(1-\beta)^{\mathcal{M}}}{\beta^2}\big) - 1 \tag{B.5}$$

Bibliographie

Références historiques

[1] F. Balibar, *Einstein 1905*, Editeur : Presses Universitaires de France, (1992).

[2] W. Gerlach et O. Stern, *Der experimentelle Nachweis des magnetischen Moments des Silberatoms*, Zeitschrift für Physik **8**, 110-111 (1921).

[3] A. H. Compton, *A Quantum Theory of the Scattering of X-rays by Light Elements*, Phys. Rev. **21**, 483–502 (1923).

[4] Emilio Segré, *Les physiciens modernes et leurs découvertes : des rayons X aux quarks*, Fayard (1984).

[5] V. Ronchi, *Histoire de la lumière*, Editions J. Gabay (1956).

[6] « *I therefore take the liberty of proposing for this hypothetical new atom, which is not light but plays an essential part in every process of radiation, the name photon.* »
Citation extraite de la lettre de Gilbert N. Lewis à l'éditeur Nature ; Nature **118**, 18 Décembre 1926, page 874-875.

[7] R. Feynman, *Lumière et matière une étrange histoire*, Interéditions (1987).

[8] G.I Taylor, *Interference Fringes with Feeble Light*, Proc. Cambridge Philos. Soc. **15**, 114 (1909).

[9] R.P. Feynman, *Simulating physics with computers*, Int. J. Theor. Phys. **21**, 467 (1982).

[10] J. Perrin, Annales de Physique (Paris), **9**, 133, (1948)

[11] S. Wiesner, *Conjugate coding*, Sigact News, **15-1**, 78-88 (1983) le manuscrit original date de 1970 environ mais, refusé pour publication à cette date, est resté non publié jusqu'en 1983.

[12] E. M. Purcell, *Spontaneous emission probabilities at radio frequencies*, Phys. Rev., *69*, p. 681, (1946).

[13] *When elementary quantum systems . . . are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media.* Charles H. Bennett et Gilles Brassard (1984).

Manuels de référence et articles de revue

[14] D.F. Walls, G.J. Milburn, *Quantum Optics*, Editeur : Springer-Verlag, (1994).

[15] R. Loudon, *The Quantum Theory of Light*, Ed : Oxford University Press, (2000).

[16] H. Bachor et T.C. Ralph, *Experiments in Quantum Optics*, Ed. Wiley, New York, (2004).

[17] L. Mandel et E. Wolf, *Optical coherence and quantum optics*, Cambridge University Press, (1995).

[18] R. J Glauber, *Optical Coherence and Photon Statistics*, Cours de l'école des Houches, ed : C. deWitt, A. Blandin, et C. Cohen-Tannoudji, (Gordon and Breach Science Publishers), (1964).

[19] C. Cohen-Tannoudji, J. Dupont-Roc et G. Grynberg, *Photons et atomes, Introduction à l'Électrodynamique Quantique*, InterEditions et Éditions du C.N.R.S., Paris (1987).

[20] M. Born et E. Wolf, *Principle of Optics*, Pergamon Press (1986).

[21] P. M. Nielsen et I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2002).

[22] H.-K. Lo, S. Popescu,et T. Spiller (eds.), *Introduction to quantum computation and information*, World Scientific, Singapore, (1998).

[23] F. Bardou, J.-P. Bouchaud, A. Aspect et C. Cohen-Tannoudji, *Lévy Statistics and Laser Cooling*, Cambridge University Press (2002).

[24] B. Chu, *Laser Light Scattering. Basic Principles and Practice* (Boston : Academic Press) (1991).

[25] D.N. Klyshko, *Photons and Nonlinear optics*, Gordon and Breach, New York (1988).

[26] P. Grangier, I. Abram, *Single photons on demand*, Physics World, Février 2003.

[27] S. Haroche et J.-M. Raimond, *L'ordinateur quantique : rêve ou cauchemar ?*, La Recherche, nov. 1996.

[28] N.Gisin, G. Ribordy, W. Tittel et H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145 (2002), `Eprint quant-ph/0101098v2`.

[29] G. Brassard, C. Crépeau, *25 years of quantum cryptography* Proceeding d' ACM SIGACT, **27** , Issue 3 (Septembre 1996).

[30] *Quantum Cryptography Roadmap*, Rapport de synthèse réalisé par un panel d'experts composé de C. Bennett, D. Bethune, G. Brassard, N. Donnangelo, A. Ekert, C. Elliott, J. Franson, C. Fuchs, M. Goodman, R. Hughes, P. Kwiat, A. Migdall, S. W. Nam, J. Nordholt, J. Preskill, J. Rarity,
`Disponible sur http ://qist.lanl.gov/qcrypt_map.shtml` (2004).

[31] Un panorama récent de la recherche sur les photons uniques peut être trouvé dans le numéro spécial dans :
Philippe Grangier et al, *Focus on Single Photons on Demand*, New J. Phys. **6** (2004). `http ://www.iop.org/EJ/abstract/1367-2630/6/1/E04`

Articles de référence en optique quantique

[32] R.H. Brown et R. Twiss, *Correlation between photons in two coherent beams of light*, Nature, **177**, 22 (1956).

[33] R. J. Glauber, *Coherent and Incoherent States of the Radiation Field*, Phys. Rev. **1**, 2766 (1963).

[34] J. F. Clauser, *Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect*, Phys. Rev. D **9**-4, 853-860 (1974).

[35] J. Kimble, M. Dagenais et L. Mandel, *Photon antibunching in fluorescence resonance*, Phys. Rev. Lett. **39**, 691 (1977).

[36] H. J. Carmichael, P. Drummond, P. Meystre et D. F. Walls, *Intensity correlations in resonance fluorescence with atomic number fluctuations*, J. Phys. A : Math. Gen., **11**, 121-126, (1978).

[37] A. Aspect, P. Grangier, G. Roger, *Experimental realization of Einstein-Podolsky-Rosen gedankenexperiment ; a new violation of Bell's inequalities*, Phys. Rev. Lett. **49**, 91(1982).

[38] S. Reynaud, *La fluorescence de résonance : Etude par la méthode de l'atome habillé*, Ann. Phys. Fr. **8** 315, (1983).

[39] P. Grangier, A. Aspect, J. Vigué, *Quantum interference effect for two atoms radiating a single photon*, Phys. Rev. Lett., **54**, 418 (1985).

[40] P. Grangier, G. Roger et A. Aspect, *Experimental evidence for a photon anticorrelation effect on a beam splitter : a new light on single-photon interferences*, Europhysics Letters **1**, 173-179 (1986).

[41] C. K. Hong et L. Mandel *Experimental realization of a localized one-photon state* Phys. Rev. Lett. **56**, 56-80 (1986)

[42] C. K. Hong, Z. Y. Ou et L. Mandel, *Measurement of Subpiconsecond Time Intervals between Two Photons by Interference* Phys. Rev. Lett. **59**, 2044–2047 (1987).

Molécules uniques

[43] B. Lounis et W.M. Moerner, *Single photons on demand form a single molecule at room temperature*, Nature, **407**, 491, (2000).

[44] W.E Moerner, L. Kador, *Optical detection and spectroscopy of single molecules in a solid* Phys. Rev. Lett. **62** (1989) 2535.

[45] M. Orrit, J. Bernard, *Single pentacene molecules detected by fluorescence excitation in a p-terphenyl crystal*, Phys. Rev. Lett. **65**, 2716, (1990).

[46] E.B. Shera, N.K. Seitwinker, L. Davis, R.A. Keller, S.A. Soper, *Detection of single fluorescent molecules Chem. Phys. Lett.* **65** (1990) 2716.

[47] R. Rigler, J. Widengren, U. Mets, *Fluorescence Spectrosopy* ed. E. Wolbeis, Springer, Berlin **65** (1992) 13.

[48] B. Valeur, *Molecular Fluorescence : An Introduction - Principles and Applications*, Publié par Wiley-VCH, (2002).

[49] J.R. Lakowicz, *Principles of Fluorescence Spectroscopy*, Ed. Kluwer Academic, (1999).

[50] W.E. Moerner, *Single photon based on single molecules in solids*, New J. Phys., **6**, 88 (2004).

[51] Ph. Tamarat, B. Lounis, J. Bernard, M. Orrit, S. Kummer, R. Kettner, S. Mais et Th. Basché, *Pump-Probe Experiments with a Single Molecule : ac-Stark Effect and Nonlinear Optical Response*, Phys. Rev. Lett. **75** (1995) 1514.

[52] B. Lounis, F. Jelezko, Ph. Tamarat, M. Orrit, *Single Molecules Driven by Strong Resonant Fields : Hyper-Raman and Subharmonic Resonances*, Phys. Rev. Lett. **78** (1997) 3673.

[53] C. Brunel, B. Lounis, Ph. Tamarat, M. Orrit, *Rabi Resonances of a Single Molecule Driven by rf and Laser Fields*, Phys. Rev. Lett. **81** 2679, (1998).

[54] C. Brunel, *Optique non linéaire et quantique sur des molécules individuelles*Thèse de doctorat , Université de Bordeaux I, Juillet 2000.

[55] T. Bashé, W. 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).

[56] J. Bernard, L. Fleury, H. Talon et M. Orrit, *Photon bunching in the fluorescence from single molecules : a probe for intersystem crossing*, J. Chem. Phys., **98**, 850, (1993).

[57] H. Yang, S. Xie, *Statistical Approaches for Probing Single-molecule Dynamics Photon-by-Photon*, Chem. Phys. **284**, 423 (2002).

[58] H. Yang, G. Luo, P. Karnchanaphanurach, T.-M. Louie, I. Rech, S. Cova, L. Xun, et X. S. Xie, *Protein Conformational Dynamics Probed by Single-Molecule Electron Transfer*, Science, **302**, 262-266 (2003).

[59] V. Barsegov, S. Mukamel, *Probing Single Molecule Kinetics by Photon Arrival Trajectories*, J. Chem. Phys., **116**, 9802-9811 (2002)

[60] A. Berglund, A. Doherty et H. Mabuchi, *Photon statistics and dynamics of Fluorescence Resonance Energy Transfer*, Phys. Rev. Lett., **89**, 068101 (2002).

[61] T. Basché, W. E. Moerner, M. Orritt et H. Talon, *Photon antibunching in the fluorescence of a single dye molecule trapped in a solid*, Phys. Rev. Lett., **69** 1516 (1992).

[62] C. G. Hübner, G. Zumofen, A. Renn, A. Herrmann, K. Müllen et T. Basché, *Photon Antibunching and Collective Effects in the Fluorescence of Single Bichromophoric Molecules*, Phys. Rev. Lett. **91** 093903, (2003).

[63] C.Eggeling, J.Widengren, R. Rigler, C. A. M. Seidel, *Photobleaching of Fluorescent Dyes under Conditions Used for Single-Molecule Detection : Evidence of Two-Step Photolysis*, Anal. Chem. **70**, pp. 2651-2659 (1998).

[64] J. A. Veerman, M. F. Garcia-Parajo, L. Kuipers et N. F. Van Hulst, *Time-varying triplet state lifetimes of single molecules*, Phys. Rev. Lett. **83** 2155, (1999).

[65] S. G. Lukishova, A. W. Schmid, A. J. McNamara, R. W. Boyd et C. R. Stroud, *Room temperature single-photon source : Single-dye molecule fluorescence in liquid crystal host*, IEEE J. Selected Topics Quant. Electron. **9**, 1512 (2003).

[66] P.S.Dittrich et P.Schwille, *Photobleaching and stabilization of fluorophores used for single-molecule analysis with one- and two-photon excitation*, Appl.Phys.B **73**), 829-837 (2001).

[67] L. Fleury, B. Sick, G. Zumofen, B. Hecht et U. Wild, *High photostability of single molecules in an organic crystal at room temperature observed by scanning confocal optical microscopy*, Molecular Physics, **95**, 1333, (1998).

[68] L. Fleury, J.M. Segura, G. Zumofen, B. Hecht et U. Wild, *Nonclassical Photon Statistics in Single-Molecule Fluorescence at Room Temperature*, Phys. Rev. Lett. **84**, 1148, (2000).

[69] Y. Lill et B. Hecht, *Single dye molecules in an oxygen-depleted environment as photostable organic triggered single-photon sources*, Appl. Phys. Lett., **84**, 1665-1667, (2004).

[70] J. Bernard, L. Fleury, H. Talon, et M. Orrit, *Photon bunching in the fluorescence from single molecules : A probe for intersystem crossing*, J. Chem. Phys. **98**-2, 850 (1993).

[71] F. Treussart, A. Clouqueur, C. Grossman et J.F. Roch, *Photon antibunching in the fluorescence of a single dye molecule embedded in a thin polymer film*, Opt. Lett. **26** 1504 (2001).

[72] P.W Atkins et R.S. Friedman, *Molecular Quantum Mechanics* (Oxford : Oxford University Press, Oxford) (1997)

[73] 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, 620-627 (1998).

[74] La section efficace d'absorption de la molécule de carbocyanine est évaluéé à partir du coefficient d'extinction molaire de 125 000 cm^{-1} indiqué sur le site de Molecular Probes. `http ://www.probes.com/handbook/sections/1404.html`

[75] F. Treussart, R. Alléaume, V. Le Floc'h, L.T. Xiao, J.M. Courty et J.F. Roch, *Direct Measurement of the Photon Statistics of a Trigerred Single Photon Source Phys. Rev. Lett.* **89** 093601, (2002).

[76] Ph. Tamarat, A. Maali, B. Lounis et M. Orrit, *Ten Years of Single-Molecule Spectroscopy*, J. Phys. Chem. A, **104**-1, (2000).

[77] 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).

[78] R. Zondervan, F. Kulzer, S.B. Orlinskii et M. Orrit, *Photoblinking of Rhodamine 6G in Poly(vinyl alcohol) : Radical Dark State Formed through the Triplet*, J. Phys. Chem. A, **107**, 6770, (2003).

[79] R. Zondervan, F. Kulzer, M.A. Kol'chenko et M. Orrit", *Photobleaching of Rhodamine 6G in Poly(vinyl alcohol) at the Ensemble and Single-Molecule Levels*, J. Phys. Chem. A, **108**, 1657, (2003).

[80] A. Kiraz, M. Ehrl, C. Bräuchle et A. Zumbusch *Ultralong coherence times in the purely electronic zero-phonon line emission of single molecules*, Appl. Phys. Lett. **85**, 920, (2004).

[81] J.J. Macklin, J.K. Trautma, T.D. Harris et L.E. Brus, *Imaging and Time-Resolved Spectroscopy of Single Molecules at an Interface*, Science, **272**, 255, (1996).

[82] S. Nie, D. T. Chiu et R. N. Zare, *Probing individual molecules with confocal fluorescence microscopy*, Science *266*, 1018-1021 (1994).

Centres colorés du diamant

[83] R. Brouri, A. Beveratos, J.P. Poizat et P. Grangier, *Single photon emission from colored centers in diamond* Opt. Lett. **25** 1294.

[84] C. Kurtsiefer, S. Mayer, P. Zarda, S. Mayer et H. Weinfurter, *A robust all-solid-state source for single photons*, Phy. Rev. Lett., **85**, 290, (2000).

[85] C. Kurtsiefer, S. Mayer, P. Zarda et H. Weinfurter, *A stable solid-state source of single photons*, Phys. Rev. Lett. **85** 290 (2000).

[86] A. Beveratos, *Réalisation expérimentale d'une source de photons uniques par fluorescence de centres colorés individuels dans le diamant ; application à la cryptographie quantique*, Thèse de doctorat, Université Paris XI, Décembre 2002.

[87] A. Beveratos, S. Kühn, R. Brouri, T. Gacoin, J.-P. Poizat et P. Grangier, *Room temperature stable single-photon source* Eur. Phys. J. D 18, 191-196 (2002).

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

[89] A. M. Zaitsev, *Optical Properties of Diamond, A Data Handbook*, Springer (2001)

[90] Y. Dumeige, F. Treussart, R. Alléaume, T. Gacoin, J.-F. Roch et P. Grangier, *Photo-induced creation of nitrogen-related color centers in diamond nanocrystals under femtosecond illumination*, Journal of Luminescence, **109**, **61**, (2004).

[91] R. Brouri, A. Beveratos, J.P. Poizat et P. Grangier, *Single photon emission from colored centers in diamond* Opt. Lett. **25** 1294 (2000).

[92] A. Beveratos, R. Brouri, T. Gacoin, J.-P. Poizat, and P. Grangier, *Nonclassical radiation from diamond nanocrystals*, Phys. Rev. A **64**, 061802(R) (2001).

[93] T. Gaebel, I. Popa, A. Gruber, M. Domhan, F. Jelezko et J. Wrachtrup, *Stable single-photon source in the near infrared*, New J. Phys. **6**, 98, (2004).

[94] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup et C. von Borczyskowski, *Scanning confocal optical microscopy and magnetic resonance on single defect centres*, Science **276** 2012 (1997).

[95] F. Jelezko, T. Gaebel, I. Popa, A. Gruber, et J. Wrachtrup, *Observation of Coherent Oscillations in a Single Electron Spin*, Phys. Rev. Lett. **92**, 076401 (2004).

Boîtes quantiques semi-conductrices

[96] E. Moreau, I. Robert, L. Manin et V. Thierry-Mieg, J.M. Gérard et I. Abram, *Quantum cascade of photons in semiconductor quantum dots*, Phys. Rev. Lett., **87** 183601 (2001).

[97] E. Moreau, I. Robert, J.M. Gérard, I. Abram, L. Manin et V. Thierry-Mieg, *Single-mode solid-state single photon source based on isolated quantum dots in pillar microcavities*, Appl. Phys. Lett., **79** 2865 (2001).

[98] K. Brunner, U. Bockelmann, G. Abstreiter, M. Walther, G. Böhm, G. Tränkle et G. Weimann, *Photoluminescence from a singe GaAs/AlGaAs quantum dot*, Phys. Rev. Lett. **69**, 3216 (1992).

[99] Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N.S. Beattie, D. A. Ritchie et M. Pepper, *Electrically driven single-photon source*, Science **295**, 102 (2002).

[100] B. Lounis, H. A. Bechtel, D. Gerion, P. Alivisatos et W. E. Moerner, *Photon antibunching in single CdSe/ZnS quantum dot fluorescence*, Chem. Phys. Lett., **329**, 399, (2000).

[101] V. Zwiller, H. Blom, P. Jonsson, N. Panev, S. Jeppesen, T. Tsegayer, E. Goobar, M. Pistol, L. Samuelson et G. Björk, *Single quantum dots emit single photons at a time : Antibunching experiments*, Appl. Phys. Lett. **78**, 2476 (2001).

[102] V. Zwiller, T. Aichele et O. Benson, *Quantum optics with single quantum dot devices*, New J. Phys. **6**, 96 (2004).

[103] P. Michler, A. Kiraz, C. Becher, W.V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu et A. Imamoğlu, *A quantum dot single photon turnstile device* Science **290** 2282 (2000).

[104] C. Becher, A. Kiraz, A. Imamoğlu, W.V. Schoenfeld, P. M. Petroff et L. Zhang, *Nonclassical radiation from a single self-assembled InAs quantum dot*, Phys. Rev. B, **63**, (2001).

[105] C. Santori, M. Pelton, G. Solomon, Y. Dale et Y. Yamamoto, *Triggered Single Photons from a Quantum Dot*, Phys. Rev. Lett. **86** 1502 (2001).

[106] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, et Y. Yamamoto, *Quantum Cryptography with a PhotonTurnstile*, Nature, **420**, pp. 762, (2002).

[107] J. Kim, O. Benson, H. Kan, Y. Yamamoto, *A single-photon turnstile device*, Nature, **397** 500-503 (1999).

[108] E. Moreau, *Etude d'une source solide monomode de photons uniques constituée par une boîte quantique semi- conductrice dans un microcavité optique*, Thèse de Doctorat (2002).

[109] J.-Y. Marzin, J.-M. Gérard, A.Izraël, D.Barrier, G.Bastard, *Photluminescence of single InAs quantum dots obtained by self-organized growth on GaAs*, Phys.Rev. Lett **.73**, 716, (1994).

[110] J.-M. Gérard, b. Sermage ; B. Gayral ; B. Legrand, E. Costard et V. Thierry-Mieg, *Enhance spontaneaous emission by quantum boxes in a monolithic optical microcavity*, Phys. Rev. Lett., **81**, 1110, (1998).

[111] E. M. Chan, R. A. Mathies et A. P. Alivisatos, *Size-controlled growth of CdSe nanocrystals in microfluidic reactors* Nano Letters **3**-2, 199-201, (2003).

[112] C. Santori, D. Fattal, J. Vuckovic, G. Solomon, et Y, Yamamoto, *Single-photon generation with InAs quantum dots*, New J. Phys., special issue on "Single-photon sources" **6**, 89 (2004).

[113] M. H. Baier, E. Pelucchi, E. Kapon, S. Varoutsis, M. Gallart, I. Robert-Philip, et I. Abram, *Single photon emission from site-controlled pyramidal quantum dots*, Appl. Phys. Lett., **84**, pp. 648-650, (2004)

[114] M. Kuno, D. P. Fromm, H. F. Hamann, A. Gallagher, et D. J. Nesbitt, *« On » / « Off » fluorescence intermittency of single semiconductor quantum dots*, J. Chem. Phys., **115**, pp. 1028-1040, (2001).

[115] X. Brokmann, E. Giacobino, M. Dahan, et J. P. Hermier, *Highly efficient triggered emission of single photons by colloidal CdSe/ZnS nanocrystals* , Appl. Phys. Lett., **85**, pp. 712-714. (2004).

[116] M. Dahan, S. Lévi, C. Luccardini, P. Rostaing, B. Riveau et A. Triller, *Diffusion dynamics of glycine receptors revealed by single quantum dot tracking*, Science **302**, 442 (2003).

[117] J. Vučković, D. Fattal, C. Santori, G.S. Solomon et Y. Yamamoto, *Enhanced single-photon emission from a quantum dot in a micropost microcavity*, Appl. Phys. Lett., **82**, 3596, (2003).

[118] X. Brokmann, J.-P. Hermier, G. Messin, P. Desbiolles, J.-Ph. Bouchaud et M. Dahan, *Statistical Aging and Non Ergodicity in the Fluorescence of Single Nanocrystals* Phys. Rev. Lett. **90**, 120601 (2003).

[119] P. Michler, A. Imamoglu, M. D. Mason, P. J. Carson, G. F. Strouse, S. K. Buratto, *Quantum Correlation Between Photons from a Single CdSe Quantum Dot at Room Temperature*, Nature, **406**, 968-970 (2000).

[120] M. Grundman, *Nano-Optoelectronics : Concepts, Physics and Devices*, Ed. Springer, ISBN 3-540-43394-5 ; (2002).

Electrodynamique en cavité

[121] A. Kuhn, M. Hennrich et G. Rempe, *Deterministic Single-Photon Source for Distributed Quantum Networking*, Phys. Rev. Lett., **89**, 067901 (2002) .

[122] C. K. Law et H. J. Kimble, *Deterministic generation of a bit-stream of single-photon pulses*, J. Mod. Opt., **44**, 2067, (1997).

[123] A. Kuhn, M. Henrich, T. Bondo et G. Rempe, *Controlled generation of single photons from a strongly coupled atom-cavity system*, Appl. Phys. B **69**, 373 (1999).

[124] G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J.-M. Raimond et S. Haroche, *Seeing a Single Photon Without Destroying It*, Nature **400** 239-242, (1999).

[125] S. Brattke, B. T. H. Varcoe et H. Walther, *Generation of photon number states on demand via cavity quantum electrodynamics*, Phys. Rev. Lett. **86**, 3534-3537 (2001).

[126] B. T. H. Varcoe, S. Brattke et H. Walther, *The creation and detection of arbitrary photon number states using cavity QED*, New J. Phys., special issue on "Single-photon sources" **6**, 97 (2004).

[127] P. Goy, J.-M. Raimond, M. Gross et S. Haroche, *Observation of cavity-enhanced single-atom spontaneous emission*, Phys. Rev. Lett **50**, 1903, (1983).

Atome ou ion unique

[128] C. Maurer, C. Becher, C. Russo, J. Eschner et R. Blatt, *A single-photon source based on a single Ca+ ion*, New J. Phys. **6**, 94 (2004).

[129] M. Keller, B. Lange, K. Hayasaka, W. Lange et H. Walther, *A calcium ion in a cavity as a controlled single-photon source*, New J. Phys. **6**, 95 (2004).

[130] F. Diedrich et H. Walther, *Nonclassical Radiation of a Single Stored Ion* Phys. Rev. Lett., **58** 203 (1987).

[131] D. J. Wineland, Wayne M. Itano, and J. C. Bergquist, *Absorption spectroscopy at the limit : detection of a single atom*, Optics Letters, **12**, 389, (1987).

[132] N. Schlosser, G. Reymond, I. Protsenko et P. Grangier,*Sub-poissonian loading of single atoms in a microscopic dipole trap*, Nature **404** ,1024 (2001).

[133] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich et H. J. Kimble, *Deterministic Generation of Single Photons from One Atom Trapped in a Cavity*, Science **303**, 1992 (2004).

[134] J. McKeever, J. R. Buck, A. D. Boozer, A. Kuzmich, H.-C. Nägerl, D. M. Stamper-Kurn et H. J. Kimble, *State-Insensitive Cooling and Trapping of Single Atoms in an Optical Cavity*, Phys. Rev. Lett. **90**, 133602 (2003).

[135] N. Schlosser, G. Reymond, I.E. Protsenko et P. Grangier, *Sub-poissonian loading of single atoms in a microscopic dipole trap*, Nature **411**, 1024 (2001).

[136] D. Frese, B. Ueberholz, S. Kuhr, W. Alt, D. Schrader, V. Gomer et D. Meschede, *Single Atoms in an Optical Dipole Trap : Towards a Deterministic Source of Cold Atoms*, Phys. Rev. Lett. **85**, 3777–3780 (2000).

Systèmes expérimentaux pour le calcul et l'information quantique

[137] C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano et D.J. Wineland, *Demonstration of a Fundamental Quantum Logic Gate*, Phys. Rev. Lett. **75**, 4714 (1995)

[138] I.L. Chuang, N. Gershenfeld, M. Kubinec, *Experimental Implementation of Fast Quantum Searching* Phys. Rev. Lett. **80**, 3408 (1998)

[139] W. Tittel, J. Brendel, H. Zbinden et N. Gisin, *Violation of Bell inequalities by photons more than 10 km apart*, Phys. Rev. Lett., **81**, 3563, (1998).

[140] C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon et Y.Yamamoto, *Indistinguishable photons from a single-photon device*, Nature **419**, 594–597 (2002).

[141] P. Grangier, *Single photons stick together*, Nature **419**, 577 (2002).

[142] C. Liu, Z. Dutton, C. H. Behroozi, L. V. Hau, *Observation of coherent optical information storage in an atomic medium using halted light pulses*, Nature **409**, 490-493 (2001).

[143] R. M. Gingrich, P. Kok, H. Lee, F. Vatan, J. P. Dowling, *An All Linear Optical Quantum Memory Based on Quantum Error Correction*, Phys. Rev. Lett. **91**, 217901 (2003).

[144] J. M. Taylor, C. M. Marcus, and M. D. Lukin, *Long-Lived Memory for Mesoscopic Quantum Bits*, Phys. Rev. Lett. **90**, 206803 (2003).

[145] M. B. Plenio et P. L. Knight, *Decoherence limits to quantum computation using trapped ions*, Proceedings : Mathematical, Physical and Engineering Sciences, **453**, 1965, pp. 2017-2041, (1997).

[146] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, et D. J. Wineland, *Demonstration of a Fundamental Quantum Logic Gate* Phys. Rev. Lett. 75, 4714–4717 (1995).

[147] Y. Nakamura, Y. A. Pashkin et J. S. Tsai, *Coherent control of macroscopic quantum states in a single-Cooper-pair box*, Nature **398**, 1999, pp. 786-788.

[148] L. B. Ioffe, V. B. Geshkenbein, M. V. Feigelman, A. L. Fauchère et G. Blatter, *Environmentally decoupled sds-wave Josephson junctions for quantum computing*, Nature, **398**, pp. 679-681, (1999).

[149] David Fattal, Kyo Inoue, Jelena Vukovi, Charles Santori, Glenn S. Solomon, and Yoshihisa Yamamoto, *Entanglement Formation and Violation of Bell's Inequality with a Semiconductor Single Photon Source*, Phys. Rev. Lett. **92**, 037903 (2004).

[150] D. Fattal, E. Diamanti, K. Inoue, et Y. Yamamoto, *Quantum Teleportation with a Quantum Dot Single Photon Source*, Phys. Rev. Lett. **92**, 037904 (2004).

Information quantique : articles théoriques

[151] W.H. Zurek, *Decoherence and the Transition from Quantum to Classical*, Physics Today, **44**, 36-34, (1991). `Eprint quant-ph/030672`.

[152] E. Knill, L. Laflamme et G. J. Milburn, *Efficient linear optics quantum computation*, Nature **409**, 46 (2001).

[153] L. Grover, A fast quantum mechanical algorithm for database search, Proc. 28th Annual ACM Symposium on the Theory of Computation, 212-219, (1996). Disponible à : `http ://www.bell-labs.com/user/lkgrover` .

[154] P. W. Shor, *Polynomial time algorithms for prime factorization and discrete logarithm on a quantum computer*, Proceedings of the 35th Annual Symposiumon Foundations of Computer Science, Santa Fe, NM,1994, éditeur : Shafi Goldwasser (IEEE Computer Society-Press, Los Alamitos, CA, 1994), 124 (1994) ; SIAM J. Comput. **26**, 1484 (1997). `Eprint quant-ph/9508027v2` .

[155] D. Deutsch, *Quantum theory, the church-turing principle and the universal quantum computer*, Proc. R. Soc. Lond. A, **400** 97-117 (1985). Disponible à : `http ://www.qubit.org/oldsite/resource/deutsch85.pdf`.

[156] D.P. DiVincenzo, D. Loss, *Superlattices and Microstructures* **23**, 419 (1998)

[157] W. K. Wootters et W. H. Zurek, *A single quantum cannot be cloned*, Nature, **299**, 802 (1982).

[158] S. van Enk, J. I. Cirac, P. Zoller, H. J. Kimble, et H. Mabuchi, *Quantum state transfer in a quantum network : a quantum optical implementation*, J. Mod. Opt. *44*, 1727 (1997).

[159] D. Gottesman, An Introduction to Quantum Error Correction `http ://arxiv.org/abs/quant-ph/0004072`

Observation d'états non-classiques du rayonnement

[160] R. Short et L. Mandel, *Observation of Sub-Poissonian Photon Statistics* Phys. Rev. Lett. **51** 384 (1983)

[161] L. Mandel, *Sub-Poissonian photon statistics in resonance fluorescence*, Opt. Lett. **4** 205, (1979).

[162] P. Grangier, *Etude expérimentale de propriétés non-classiques de la lumière : interférence à un seul photon*, Thèse de doctorat, Université Paris XI, (1986).

[163] W.H. Richarson, S. Machida et Y. Yamamoto, *Squeezed photon-number noise and sub-Poissonian electrical partition noise in a semiconductor laser* , Phys. Rev. Lett. , **66**, 2867 (1991).

[164] A. Imamoḡlu et Y. Yamamoto, *Noise Suppression in Semiconductor p-i-n Junctions ; Transition from Macroscopic Squeezing to Mesoscopic Coulomb Blockade of Electron Emission Process* , Phys. Rev. Lett. , **70**,3327 (1993).

[165] E.Waks, E. Diamanti, B.C. Sanders, S.D. Barlett, Y. Yamamoto, *Direct observation of nonclassical photon statisitcs in parametric downconversion*, ; `Eprint quant-ph/0307162`.

[166] F. De Martini, O. Jedrkiewicz et P. Mataloni, *Generation of quantum photon states in an active microcavity trap*, J. Mod. opt., **44**, 2053, (1997).

[167] F. De Martini, G. Di Giuseppe et M. Marrocco, *Single-mode generation of quantum photon states by excited single molecules in a microcavity trap*, Phys. Rev. Lett., **76**, 900, (1996).

[168] M. C. Teich et B. E. A. Saleh, *Observation of sub-Poisson Franck-Hertz light at 253.7 nm*, J. Opt. Soc. Am.B, **2**, pp. 275-285, (1985).

[169] M. A. Finn, G. W. Greenlees, T. W. Hodapp et D. A. Lewis, *Sub-Poisson, two-level behavior of three-level atoms prior to quantum jumps*, Phys. Rev. A **40**, 1704–1706 (1989).

[170] B. G. Oldaker, P. J. Martin, P. L. Gould, M. Xiao et D. E. Pritchard, *Experimental study of sub-Poissonian statistics in the transfer of momentum from light to atoms*, Phys. Rev. Lett. **65**, 1555–1558 (1990).

[171] R. Alléaume, F. Treussart, J.-M. Courty et J.-F. Roch, *Photon statistics characterisation fo a single-photon source*, New Journal of Physics, **6**, 85 (2004).

Squeezing

[172] Y. Yamamoto, S. Machida et O. Nilsson, *Amplitude squeezing in a pump-noise-suppressed laser oscillator*, Phys. Rev. A **34**, 4025–4042 (1986).

[173] Y. Yamamoto, N. Imoto, et S. Machida, *Amplitude squeezing in a semiconductor laser using quantum nondemolition measurement and negative feedback*, Phys. Rev. A, **33**, 3243–3261 (1986).

[174] R. E. Slusher, L. Hollberg, B. Yurke, J. C. Mertz, et J. F. Valley, *Squeezed states in optical cavities : A spontaneous-emission-noise limit*, Phys. Rev. A **31**, 3512–3515 (1985).

Cryptographie quantique : publications théoriques

[175] C. Bennett, G. Brassard, *Quantum cryptography : public key distribution and coin tossing*, Int. conf. Computers, Systems and Signal Processing, Bangalore, India pp 175-179 (1984).

[176] C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, *Quantum cryptography or unforgeable subway tokens*, Advances in Cryptology : Proc of Crypto 82,pp. 267-275, Plenum Press (1982)

[177] C. H. Bennett, G. Brassard, S. Breidbart, et S. Wiesner, *Eavesdrop-Detecting Quantum Communications Channel* in IBM Technical Disclosure Bulletin **26**, 3153-3163, (1984).

[178] H. K. Lo, *Quantum Cryptology*, article paru dans la référence [22] (1998).

[179] D. Mayers, *Unconditionnal Security in Quantum Cryptography*, J. Assoc. Comput. Math. **48**, 351, (1998), `Eprint quant-ph/9802025` . (Preliminary version in 1996 Advances in Cryptography : Proc. of Crypto '96 (New York : Springer) p 343).

[180] H. K. Lo et H. F. Chau, *Unconditionnal Security of Quantum Key Distribution Over Arbitrarily Long Distances*, Science, **283**, (1999), 2050–2056.

[181] P. W. Shor et J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett., **85** (2000), 441–444 ; `Eprint quant-ph/0003004`.

[182] D. Gottesman, H.-K. Lo, *Proof of Security of Quantum Key Distribution With Two-Way Classical Communications*, IEEE Trans. Info. Theory **49**, 457-475 (2003).

[183] G. Brassard, N. Lütkenhaus, T. Mor et C. Sanders, *Security Aspects of Practical Quantum Cryptography*, Phys. Rev. Lett., **85**, 1330 (2000).

[184] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against number splitting attacks for weak laser pulse implementations*, Phys. Rev. Lett. **92**, 057901 (2004).

[185] N. Lütkenhaus, *Security against individual attacks for realistic quantum key distribution*, Phys. Rev. A **61** 052304, (2000).

[186] N. Lütkenhaus, *Estimates for practical quantum cryptography*, Phys. Rev. A **59**-5, 3301, (1999).

[187] H. Inamori, N. Lütkenhaus et D. Mayers, *Unconditional Security of Practical Quantum Key Distribution*, (2001) `Eprint quant-ph/0107017`.

[188] E. Biham, M. Boyer, G. Brassard, E. Biham et T. Mor *Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. Lett. **78**, 2256–2259 (1997).

[189] N. Lütkenhaus, *Quantum Key Distribution : Ho do we know it's secure ?*, Optics and Photonics News, p.24, Mars 2004.

[190] J. M. Renes, *Spherical Code Key Distribution Protocoles for Qubits*, (2004) `Eprint quant-ph/0402135`.

[191] A. Acìn, L. Masanes et N. Gisin, *Equivalence between Two-Qubit Entanglement and Secure Key Distribution*, Phys. Rev. Lett. , **91**, 167901, (2003).

[192] M. Curty, M. Lewenstein, N. Lütkenhaus, *Entanglement as a Precondition for Secure Quantum Key Distribution* Phys. Rev. Lett. , **92**-21, 217903 (2004) ; `Eprint quant-ph/0307151`.

[193] F. Grosshans et P. Grangier, *Continuous variable quantum cryptography using coherent states*, Phys. Rev. Lett. **88**-5, 057902 (2002). Une version étendue est disponible sur le site de Los Alamos : `Eprint quant-ph 0109084`.

[194] F. Grosshans et P. Grangier, *Reverse reconciliation protocols for quantum cryptography with continuous variables*. Proceeding of the 6^{th} International Conference Quantum Communication, Measurement and Computing, Rinton Press, (2002). *Eprint quant-ph/0204127*.

[195] G. Van Assche, J. Cardinal, N. Cerf, *Reconciliation of a quantum-distributed Gaussian key*, IEEE Transactions on Information Theory **50**(2), 394-400, (2004).

[196] Frederic Grosshans, *Collective attacks and unconditional security in continuous variable quantum key distribution*, `Eprint : quant-ph/0407148`.

[197] B. Huttner, N. Imoto, N. Gisin et T. Mor, *Quantum cryptography with coherent states*, Phys. Rev. A **51**, 1863, (1995).

[198] E. Waks, C. Santori et Y. Yamamoto, *Security aspects of quantum key distribution with sub-Poisson light*, Phys. Rev. A **66**, 042315 (2002).

[199] P. D. Townsend, S. J. D. Phoenix, K. J. Blow et S. M. Barnett, *Quantum cryptography for multi-user passive optical networks*, Electronics Letters, **30**, pp. 1875-1877 (1994).

[200] L'idée originale est dans : W.-Y. Hwang, *Quantum Key Distribution with High Loss :Toward Global Secure Communication*, Phys. Rev. Lett. **91**, 057901 (2003).
H.-K. Lo et son équipe ont développé cette idée :
H.-K. Lo, X. Ma, K. Chen, *Decoy State Quantum Key Distribution*, `Eprint : quant-ph/0411004` (posté le 31 Octobre 2004).

Cryptographie quantique expérimentale

Publications historiques

[201] C. H. Bennett et G. Brassard, *The dawn of a new era for quantum cryptography : the experimental prototype works !*, SIGACT News, **20**(4), 1989.

[202] C. Bennett, F. Bessette, G. Brassard, L. Salvail, et J. Smolin, *Experimental Quantum Cryptography*, J. of Cryptology, **5**, 3 (1992).

Cryptographie quantique en espace libre

[203] S. F. Seward, P. R. Tapster, J. G. Walker et J. G. Rarity, *Daylight demonstration of a lowlight- level communication system using correlated photon pairs*, JOSA B : Quantum and Semiclassical Optics **3**, 201–207 (1991).

[204] A. Saleh, *An investigation of laser wave depolarization due to atmospheric transmission* IEEE J. Quantum Electronics, **3**, 540- 543 (1967).

[205] J. D. Franson et B. Jacobs, *Quantum cryptography in free space*, Opt. Lett. **21**, 1854-1856 (1996).

[206] W. Buttler, R. Hughes, S. Lamoreaux, G. Morgan, J. Nordholt et C. Peterson, *Daylight Quantum Key Distribution over 1.6 km*, Phys. Rev. Lett., **84**, 5652 (2000).

[207] R. J. Hughes, J. E. Nordholt, D. Derkacs, C. G. Peterson, *Practical free-space quantum key distribution over 10 km in daylight and at night*, New Journal of Physics, **4** 43.1-43.14, (2002).

[208] 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).

[209] 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).

[210] 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 1.25 Gbps clock synchronization*, Optics Express, **12**, 2011 - 2016 (2004).

Cryptographie quantique sur une fibre optique

[211] H. Zbinden, *Experimental quantum cryptography*, article paru dans la référence [22] (1998).

[212] J. D. Franson, B. C. Jacobs, *Operational system for quantum cryptography*, Electronics Letters, **31**, 232-234, (1995).

[213] D.S. Bethune, W.P. Risk, *An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light*, IEEE Journal of Quantum Electronics, **36**, 340-347, (2000).

[214] P.M. Nielsen, C. Schori, J.L. Sorensen, L. Salvail, I. Damgard, E. Polzik, J. Mod. Opt. **48**, 1921 (2001) ; Disponible à `http ://www.cki.au.dk/experiment/qcrypto/doc`.

[215] A. Muller, J. Breguet et N. Gisin, *Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km*, Europhys. Lett. **23**, 383 (1993).

[216] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, et N. Gisin, *« Plug and play » systems for quantum cryptography* Applied Physics Letters, **70**, pp. 793-795, (1997).

[217] C. Gobby, Z. L. Yuan, and A. J. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett., **84**(19), 3762 (2004)

[218] P. D. Townsend, J. G. Rarity, et P. R. Tapster, *Enhance single photon fringe visibility in a 10 km-long prototype quantum cryptography channel*, Elec. Lett., **29**, 1291 (1993).

[219] P.D. Townsend, *Secure key distribution system based on quantum cryptography*, Electronic Letters, **30**, No. 10, pp 809-811 (1994).

[220] R. Hughes, G. Morgan et C. Peterson, *Quantum key distribution over a 48 km optical fibre network*, J. Mod. Opt., *47*, 553 (2000).

[221] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy et H. Zbinden, *Quantum key distribution over 67 km with a plug & play system*, New J. Physics, **4**, 41 (2002).

[222] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, K. Nakamura, *Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector*, Electron. Lett., **39**, No. 16, pp. 1199-1201(2003).

[223] C. Gobby, Z. L. Yuan, and A. J. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett., **84**(19), 3762 (2004)

[224] J. Merolla, Y. Mazurenko, J. Goedgebuer, L. Duraffourg, H. Porte et W. T. Rhodes, *Quantum cryptographic device using single-photon phase modulation*, Phys. Rev. A, **60**, 1899 (1999).

Cryptographie quantique avec des paires de photons intriqués

[225] A. K. Ekert, *Quantum cryptography based on Bell's Theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[226] T. Jennenwein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, *Quantum Cryptography with entangled photons*, Phys. Rev. Lett. **84**, 4729 (2000).

[227] W. Tittel, J. Brendel, H. Zbinden et N. Gisin *Quantum Cryptography using Entangled Photons in Energy-Time Bell states*, Phys. Rev. Lett., **84**, 4737 (2000).

[228] D. S. Naik and C. G. Peterson and A. G. White and A. J. Berglund and Paul G. Kwiat, *Entangled State Quantum Cryptography : Esavesdropping on the Ekert Protocol*, Phys. Rev. Lett., *84*, 4733, (2000).

[229] G. Ribordy, J. Brendel, J.D. Gautier, N. Gisin et H. Zbinden, *Long-distance entanglement-based quantum key distribution* Phys. Rev. A **63**, 042301 (2001)

[230] S. Fasel, N. Gisin, G. Ribordy et H. Zbinden, *Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs : a comparison of two chromatic dispersion reduction methods*, (2004), `Eprint. quant-ph/0403144`.

[231] S. Fasel, O. Alibart, A. Beveratos, S. Tanzilli, H. Zbinden, P. Baldi et N. Gisin, *High quality asynchronous heralded single photon source at telecom wavelength*, `Eprint quant-ph/0408136`.

Cryptographie quantique à variables continues

[232] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf et P. Grangier, *High-rate quantum key distribution using gaussian-modulated coherent states*, Nature, **421** (6920),

238-241, (2003).

Cryptographie quantique avec des photons uniques

[233] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat et P. Grangier, *Single photon quantum cryptography* Phys. Rev. Lett. **89** 187901 (2002). `Eprint quant-ph/0206136`.

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

[235] R. Alléaume, J.-F. Roch, D. Subacius, A. Zavriyev et A. Trifonov, *Fiber-optics quantum cryptography with single photons*, Proceedings de la 7^{eme} Conférence Internationale QCMC, Glasgow. Accepté pour publication (décembre 2004).

Publications connexes

[236] C. Elliott, *Building the quantum network*, New J. Phys. **4** (July 2002) 46.

[237] C. Kurtsiefer, P. Zarda, S. Mayer et H. Weinfurter, *The breakdown flash of Silicon Avalanche diodes - backdoor for eavesdropper attacks ?*, J. Mod. Opt., **48**, 2039, (2001).

[238] A. Vakhitov, V. Makarov et D. R. Hjelme, *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography*. Journal of Modern Optics, **48**, 2023-2038 (2001).

[239] D. Stücki, G. Ribordy, A. Stefanov, H. Zbinden, J.G. Rarity, T. Wall, *Photon counting for QKD with Peltier Cooled InGaAs/InP APD's* J.Mod.Opt **48**, n°13 1967-1981 (2001).

Théorie de l'Information et cryptographie

[240] G.Brassard, Cryptologie Contemporaine, *Collection Logique, Mathématiques, Informatique*, Masson (1993).

[241] G.S. Vernam, *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, Journal of the American Institute of Electrical Engineers, **45**, pp. 109–115, (1926).

[242] I. Csisžar et Körner, *Broadcast channel with confidential message*, IEEE Transactions on Information Theory, **24** ; 339-348, (1978).

[243] C.E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, **28-4**, 656-715, 1949. Disponible sous une forme rééditées à `http ://www.cs.ucla.edu/ jkong/research/security/shannon.html`.

[244] U. Maurer, *Secret key agreement by public discussion from common information*, IEEE Transactions on Information Theory, **39**, 733-742(1993). Disponible à : `http ://www.crypto.ethz.ch/ maurer/publications.html`.

[245] G. Brassard et L. Salvail, *Secret key reconciliation by public discussion*, Advances in cryptology - Eurocrypt'93, **765** in Lectures Notes in Computer Science, 411-423, New-York, Ed Springer Velag, (1993).

[246] C. Crépeau, *Réconciliation et distillation publiques de secret*. Disponible à : `http ://www.cs.mcgill.ca/ crepeau/theses.html`, (1995).

[247] C. Shannon, *A mathematical theory of communication*, Bell System Technical Journal **27**, 379 (1948).

[248] J. L. Carter et M. N. Wegman, *New hash functions and their use in authentication and set equality*, J. of Comp. and Syst. Sci., **22**, 265-279, (1981).

[249] G. Zémor, *Cours de Cryptographie*, Editeur : Cassini, (2001).

[250] C. H. Bennett, G. Brassard, C. Crepeau et U. M. Maurer, *Generalized privacy amplification*, IEEE Trans. Inf. Theo. **41**, 1915 (1995).

[251] R. Rivest, A. Shamir et L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, **21**, pp. 120-126, (1978).

[252] K. G. Paterson, F.Piper et R. Schack, *Why Quantum Cryptography ?*, `Eprint quant-ph/0406147` (2004).

[253] Louis Salvail et Grégoire Ribordy, discussion privée (2004)

Nanophysique

[254] S. Brasselet, V. Le Floc'h, F. Treussart, J.-F. Roch, J. Zyss, E. Botzung-Appert, A. Ibanez, *In situ diagnostics of the crystalline nature of single organic nanocrystals by nonlinear microscopy*, Phys. Rev. Lett. **92**, 207401 (2004).

[255] H. Park, J. Park, A. K. L. Lim, E. H. Anderson, A. P. Alivisatos et P. L. McEuen, *Nanomechanical oscillations in a single-C60 transistor*, Nature **407** , 57 (2000).

[256] A. Imamoğlu et Y. Yamamoto, *Turnstile device for heralded single photons : Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions*, Phys. Rev. Lett. **72**, 210 (1994).

[257] D. Boyer, P. Tamarat, A. Maali, B. Lounis, et M. Orrit, *Photothermal Imaging of Nanometer-Sized Metal Particles Among Scatterers* Science **297**, 1160, (2002).

Production de paires de photons par fluorescence paramétrique

[258] C. Kurtsiefer, M. Oberparleiter et Harald Weinfurter, *High-efficiency entangled photon pair collection in type-II parametric fluorescence*, Phys. Rev. A, **64**, 023802, (2001).

[259] A. Valencia, M. V. Checkhova, A. Trifonov et Yanhua Shih, *Entangled Two-Photon Wave Packet in a Dispersive Medium*, Phys. Rev. Lett., **88**, 183601, (2002).

[260] B. E. A. Saleh, A. Joobeur, M. C. Teich, *Spatial effects in two- and four-beam interference of partially entangled biphotons*, Phys. Rev. A, **57**, 3991, (1998).

[261] M. H. Rubin, *Transverse correlation in optical spontaneous parametric down-conversion*, Phys. Rev. A, **54**, 5349, (1996).

[262] W. Tittel, J. Brendel, N. Gisin et Hugo Zbinden, *Long-distance Bell-type tests using energy-time entangled photons*, Phys. Rev. A, **59**, 4150, (1999)

[263] S. Tanzilli, H. de Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. de Micheli, D. B. Ostrowsky et N. Gisin, *Highly efficient photon-pair source using a Periodically Poled Litium Niobate waveguide*, Electron. Lett. **37**, 26 (2001).

[264] A. B. U'Ren, C. Silberhorn, K. Banaszek et I. A. Walmsley, *Efficient Conditional Preparation of High-Fidelity Single Photon States for Fiber-Optic Quantum Networks*, Phys. Rev. Lett. **93**, 093601 (2004).

[265] M. Pelton, P. Marsden, D. Ljunggren, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, F. Laurell, *Bright, single-spatial-mode source of frequency non-degenerate, polarization-entangled photon pairs using periodically poled KTP*, Optics Express, **12**, 15, 3573-3580, (2004).

[266] S. Castelletto, I. P. Degiovanni, A. Migdall et M. Ware, *On the measurement of two-photon mode coupling efficiency in parametric down-conversion sources*, New Journal of Physics, **6** 87.

[267] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. Di Giuseppe, A. V. Sergienko, *Effective fibre-coupling of entangled photons for quantum communication*, (2003), `Eprint quant-ph/0303126`.

[268] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowski, et N. Gisin, *Highly efficient photon-pair source using periodically poled lithium niobate waveguide*, Electron. Lett. **37**, 26-28 (2001).

Références et notes diverses

[269] W. L. Barnes, G. Björk, J.-M. Gérard, P. Jonssn, J. A. A. Wasey, P. T. Worthing et V. Zwiller, *Solid-state single photon sources : light collection strategies*, European J. Phys. D **18**, (2002).

[270] P. Yeh, A. Yariv et C.-S. Hong, *Electromagnetic propagation in periodic stratified media. I. General theory.*, J. Opt. Soc. Am., **67**, 423, (1977).

[271] R. H. Webb, *Theoretical basis of confocal microscopy*, pp 3-20 du livre Confocal microscopy, **307**, Academic Press, San Diego, CA, (1999).

[272] F. Roddier, *Adaptive Optics in Astronomy* (recueil d'articles), Cambridge University Press, Cambridge, 1999. voir aussi `http ://www.onera.fr/dota/oa-soo/index.html`.

[273] MAGIQ est une startup fondée en 1999 par Bob Gelfond. Cette entreprise commercialise un système de distribution quantique de clé et mène un politique active en matière de propriété intellectuelle dans le domaine de l'information quantique. Plus d'information est disponible sur leur site internet : `http ://www.magiqtech.com`

[274] IDQUANTIQUE SA (Genève, Switzerland), `http ://www.idquantique.com`

[275] Logiciel freeware de calculs d'optique non-linéaire développé au SANDIA NATIONAL LABORATORIES, `http ://www.sandia.gov/imrl/XWEB1128/snloftp.htm`.

Résumé

Une source de photons uniques est un émetteur lumineux capable de produire des impulsions contenant exactement un photon. Nous présentons le travail lié à la réalisation expérimentale et à la caractérisation statistique de deux types de sources de photons uniques :

- Les sources déclenchées de photons uniques, reposant sur la contrôle de la fluorescence d'un émetteur individuel. Nous avons utilisé des molécules uniques ainsi que des centres colorés NV uniques du diamant comme émetteurs individuels.
- Les sources de photons « annoncés », reposant sur la préparation conditionnelle d'états à un photon à partir de paires de photons produites par fluorescence paramétrique dans un cristal non-linéaire.

Deux des sources de photons uniques réalisées ont été utilisées dans des expériences de distribution quantique de clé, dont les résultats illustrent les avantages que procure l'utilisation d'une source de photons uniques vis-à-vis de systèmes reposant sur des impulsions cohérentes atténuées.

Mots Clés :

Information quantique – Cryptographie quantique – Source de photons uniques – Statistique de photons – Molécules uniques – Diamant – NV – Fluorescence paramétrique – Photons annoncés.

Abstract

A single photon source is an emitter that is able to produce light plses containing exactly one photon. We present the work related to the experimental realisation and the statistical characterisation of single photon sources of two kinds :

- Triggerred single photon sources, based on the temporal control of a single fluorescent emitter. We used single molecules and single NV coloured centres of diamond as single emitters.
- Sources of « heralded » single photons, based on the conditionnal preparation of one-photon states, obtained from photon pairs produced by parametric down-conversion in a non-linear crystal.

Two of the single photon sources we have realised have been used in experimental quantum key distribution test-beds. The measured experimental performances indicate that a potential gain can be obtained bu using a single photon source instead of weak coherent pulses.

Keywords :

Quantum information – Quantum cryptography – Single photon sources – Photon statistics – Single molecules – Diamond – NV – Parametric down-conversion – Heralded photons.